天融信下一代防火墙
管理手册

天融信
TOPSEC®
北京市海淀区上地东路 1 号华控大厦 100085
电话：+8610-82776666
传真：+8610-82776677
服务热线：+8610-8008105119
http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

目　录

1 前言

本管理手册主要介绍天融信下一代防火墙（Next Generation Firewall，本文档简称为 NGFW）的配置、使用和管理。通过阅读本文档，管理员可以了解 NGFW 的基本设计思想，并根据实际应用环境配置 NGFW。

本章内容主要包括：

- 文档目的
- 读者对象
- 约定
- 相关文档
- 扩展功能
- 技术服务体系
- 文档意见反馈

1.1 文档目的

本文档主要介绍如何配置 NGFW。通过阅读本文档，管理员能够正确地安装和配置 NGFW，并综合运用安全设备提供的多种安全技术有效地保护用户网络，控制网络的非法访问和抵御网络攻击，实现高效可靠的安全通信。

1.2 读者对象

本管理手册适用于具有基本网络知识的系统管理员和网络管理员阅读，通过阅读本文档，他们可以独自完成以下一些工作：

- NGFW 的基本管理
- 制定各个防火区之间的包过滤策略
- 制定地址转换策略
- 制定访问控制策略
- 设置 NGFW 的各种附加安全引擎，如防病毒安全引擎等。
- 管理与配置 NGFW 的附加功能模块，如备份系统、系统高可用性配置、IDS、QoS 等。

1.3 约定

本文档遵循以下约定。

1）命令行格式采用以下约定：

格式	说明
粗体	命令行关键字（命令中保持不变，必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	方括号表示可选项。
< >	尖括号表示手工输入的参数。
{ }	大括号表示命令或参数组合。
|	竖线表示隔开多个相互独立的关键字或参数。
-	短线表示数字形式的参数范围，如 1-20。
,	逗号分割参数表示参数个数不确定的参数格式。比如向用户组添加若干个用户，每个用户间用“，”分隔。

注意

- ✧ 命令行的参数顺序应该与 WebUI 的显示相对应。
- ✧ 关于术语缩写的规范：当用引号括起来时，与界面显示内容保持一致；否则，按照业界约定俗成的说法进行描述。

2）图形界面操作的描述采用以下约定：

格式	说明
【XX】	表示按钮。如：点击【XX】按钮。
『』	表示带链接的文字。如：点击『添加』。
“”	表示页面内容引用。如：激活“XX”页签，弹出“XX”窗口，在下拉框中选择“XX”参数。
>	分隔多个菜单项，且此时菜单项采用“菜单命令”格式。 如：点击（选择） **高级管理** > **特殊对象** > **用户**。
< >	带尖括号表示键盘按钮名。如：按 <Ctrl> + <Alt> 即可。

3）章节标识符采用以下约定：

格式	说明
带*号	表示该章节内容非标准配置内容，为附加说明内容。

为了叙述方便，本文档采用了大量网络拓扑图，图中的图标用于指明天融信和通用的网络设备、外设和其他设备，以下图标注释说明了这些图标代表的设备：

4）文档中出现的说明、注意、示例等标志，是关于管理员在安装和配置 NGFW 过程中需要特别注意的部分，请管理员在明确可能的操作结果后，再进行相关配置。这些标志的意义如下：

格式	说明
说明	对操作内容的描述进行必要的补充和说明。
注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或设备损坏。
示例	对相关描述进行举例说明。

1.4 相关文档

NGFW 配套资料包括如下文档：

文档类型	文档名称	内容介绍
安装手册	《NGFW 安装手册》	帮助您了解 NGFW 系统的组成和外观，指导您对设备进行安装及初始化配置。
配置案例	《NGFW 配置案例》	以典型应用环境及典型功能配置为例，介绍不同部署环境下配置不同功能的具体步骤及注意事项。

1.5 技术服务体系

天融信公司对于自身所有安全产品提供远程产品咨询服务，广大用户和合作伙伴可以通过多种方式获取在线文档、疑难解答等全方位的技术支持。

公司主页

http://www.topsec.com.cn

服务支持

http://www.topsec.com.cn/fwzc/index.htm

服务机构及联系方式

http://www.topsec.com.cn/fwzc/fwjgjqlxfs/index.htm

文档中心

http://www.topsec.com.cn/fwzc/wdzx/index.htm

天融信全国安全服务热线

800-810-5119　400-610-5119

1.6 文档意见反馈

如果您在使用过程中发现文档的任何问题，可通过服务热线或在线客服的方式进行反馈。感谢您的反馈，让我们做得更好！

2 NGFW 简介

天融信下一代防火墙（Next Generation Firewall，本文档简称 NGFW），以天融信公司具有自主知识产权的 NGTOS 操作系统（Next Generation Topsec Operation System）为系统平台，具有用户访问控制、应用层安全防护、高性能业务处理、多层级冗余设计、全网可视化及多业务融合等特点，支持用户认证、DDoS 防御、应用识别和控制、入侵防御、病毒过滤、文件过滤和 URL 过滤等功能，可为用户网络提供全面的安全防护。

NGTOS 操作系统是天融信自主研发的新一代系统平台，采用全模块化设计、中间层理念，具有高效性、高安全性、高健壮性、扩展性、可移植性、模块化、标准化等特征。

本章主要内容包括：

- 功能和特点：介绍天融信下一代防火墙的主要功能和特点。
- 工作原理：介绍天融信下一代防火墙的工作原理。
- 工作模式：介绍天融信下一代防火墙的路由、透明以及混合工作模式。

2.1功能和特点

天融信下一代防火墙本身可以提供完整的访问控制功能，可以自由地采用路由、透明及混合等多种方式集成到客户网络环境中，并通过与天融信的其他安全产品相配合，为客户网络提供强大的安全保护功能。

同时，客户还可以通过网络管理平台（如 SNMP 管理器或日志服务器）对天融信下一代防火墙的运行状况进行查询、监控和日志分析。另外，天融信下一代防火墙还提供了与其他厂家 VPN 产品建立 IPSec VPN 静态隧道，极大加强了网络安全性能。

天融信下一代防火墙具有如下基本功能：

- 支持透明、路由和混合三种工作模式。
- 支持基于对象的网络访问控制，包括网络层、应用层等多层次的访问控制；支持 URL、HTTP 脚本、关键字、邮件等多种形式的内容过滤、入侵防御和防病毒过滤。

- 支持基于对象的应用和 QoS。
- 支持多种网络地址转换（NAT）方式。
- 支持多种认证方式，如密码认证、证书认证、短信认证，并且支持本地认证，以及第三方 Radius、TACACS 和 LDAP 等认证服务器认证。
- 支持标准 IPSec VPN。
- 能够自防御 Land、Smurf、TearOfDrop、SynFlood、Targa3 和 IPSweep 等攻击，具有抗 DoS/DDoS 攻击功能。
- 支持与天融信下一代防火墙双机热备。
- 支持 IPX、NETBEUI、VOD、H.323v1/v2、SSH 等协议。
- 支持 DHCP，包括 DHCP Server、DHCP Client 以及 DHCP Relay。
- 支持接口联动和聚合接口。
- 支持智能 DNS 和服务器负载均衡。

天融信下一代防火墙具有如下特点：

- 采用多接口设计，具有良好的网络应用可扩展性。
- 高效的访问控制。天融信下一代防火墙采用核检测技术，应用深度过滤策略在系统内核实现应用层深度过滤，可对网络流量进行细粒度控制。
- 灵活的管理。实现了 TOPSEC 防火墙管理协议，管理员可以从天融信下一代防火墙的多种接口登录天融信下一代防火墙，实现类似交换机设备的中央管理。
- 高性能的应用层威胁分析能力。系统核心层实现应用层内容的还原、安全检测，深入洞察网络流量，实现高性能的 TOPSEC 内容安全协议，保证网络安全可靠。
- 强大的可视化功能。采用多维度实时图表展示产品运行状态、网络流量组成、应用构成、IPSec 流量、安全威胁等统计信息，并提供分析报表，让用户全方位感知网络运行状况。
- 系统升级与容错。天融信下一代防火墙可以通过命令行和 WebUI 方式进行系统升级，同时天融信下一代防火墙采用双系统设计，在主系统发生故障时，用户可以在启动时选择 BACKUP 方式，用备份系统引导系统。

2.2工作原理

防火墙的作用是控制外部的非信任网络（如 Internet）对内部信任网络的访问、内部网络中不同区域之间的相互访问、以及内网网络访问外部非信任网络，为网络构建全面的安全保护屏障。天融信下一代防火墙所使用的 NGTOS 操作系统平台是基于模块设计的高稳定性操作系统，通过调用防火墙模块、深度过滤模块、乃至 VPN 模块、DDoS 防御模块、入侵防御模块、防病毒模块等一系列功能模块，防火墙可深度控制穿越安全设备的数据流。

调用各个功能模块后，天融信下一代防火墙处理数据包的基本过程如下。

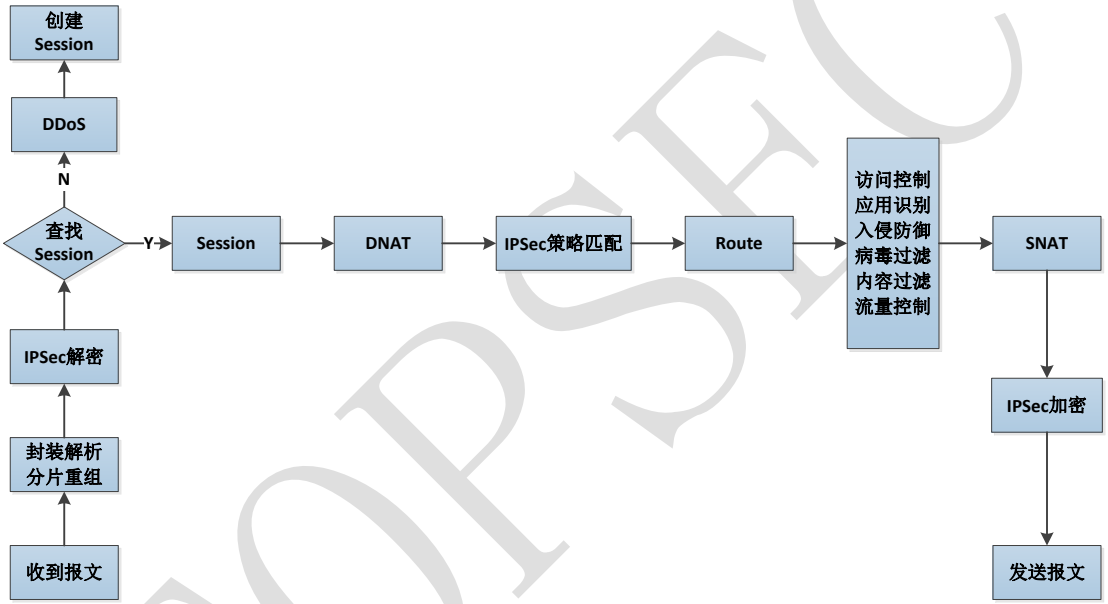


图 2-1 天融信下一代防火墙数据包处理流程图

1）接收处理

防火墙接收到数据报文后进行解析，如果为分片数据报文，且防火墙的分片重组功能开启，则重组数据报文，并区分出报文类型（本地报文、广播报文、二层透明转发报文、路由转发报文）。如果接收的数据包为 IPSec 协议保护的报文，则还需进行 IPSec 解密。

2）会话查询

对于一个新接收的报文，防火墙将根据五元组查询会话表，判断该报文是否属于某个已经存在的会话。如果存在，直接转至 3）处理。如果不存在，则说明此报文属于

一个新的会话，防火墙将调用 DDoS 防御模块检测报文是否合法，如果报文合法，则在会话表中创建一条新的会话记录。

3）DNAT 规则匹配

如果数据报文满足 DNAT（目标地址转换）规则条件，天融信下一代防火墙则将报文的目的 IP 地址（或端口），转换为规则中预先设置的 IP 地址或端口（真实的 IP 地址或端口）；否则，不进行地址转换。关于地址转换策略的设置具体请参见 7.3 地址转换。

4）路由查询

报文类型为路由转发报文时才进行路由查询。如果是新建连接，则查找路由表，并记录查询结果在会话表中；如果不是新建连接，则仅仅检查路由年龄是否变化（即路由是否发生变化），有变化时才查路由，重新确定下一跳。数据包如果经过了地址转换操作，防火墙将根据转换后的地址查询路由表。关于路由的设置具体请参见 6.5 路由。

5）IPSec 策略匹配

根据报文的源 IP 地址与目的 IP 地址匹配 IPSec VPN 策略中所保护隧道子网，如果匹配成功，则记录信息，在防火墙发送数据报文之前，根据相应 IPSec VPN 策略加密数据报文。关于 IPSec VPN 的配置具体请参见 6.9IPSec VPN。

6）访问控制策略匹配

访问控制规则描述了防火墙能否允许符合相关条件的报文通过。防火墙接收到报文后，将按策略的编号顺序逐条匹配访问规则表中所设定规则，一旦寻找到完全匹配的规则，则按照该策略所规定的操作（允许或丢弃）处理该报文。关于访问控制规则的设置具体请参见 7.2 访问控制。

7）SNAT 规则匹配

如果数据报文满足 SNAT（源地址转换）规则条件，将接收的报文的源 IP 地址（或端口）转换为规则中预先设定的 IP 地址（或端口）；否则，不进行地址转换。关于地址转换策略的设置具体请参见 7.3 地址转换。

8）发送前处理

对于发送 IPSec VPN 报文，系统将对其进行加密。IPSec VPN 加密后的报文目的地址有可能改变，此时，重新查询路由表，确定发送数据报文的下一跳，然后根据下

一跳将数据报文转发出去。对于非 VPN 报文，则直接根据路由查询阶段查询到的下一跳转发报文。

2.3工作模式

天融信下一代防火墙可以在三种模式下工作：透明模式、路由模式以及混合模式。

2.3.1 路由模式

在这种模式下，天融信下一代防火墙具备路由器转发数据包的功能，将接收到的数据包的源 MAC 地址替换为相应接口的 MAC 地址，然后转发。该模式适用于每个区域都不在同一个网段的情况。和路由器一样，天融信下一代防火墙的每个接口均要根据区域规划配置 IP 地址。

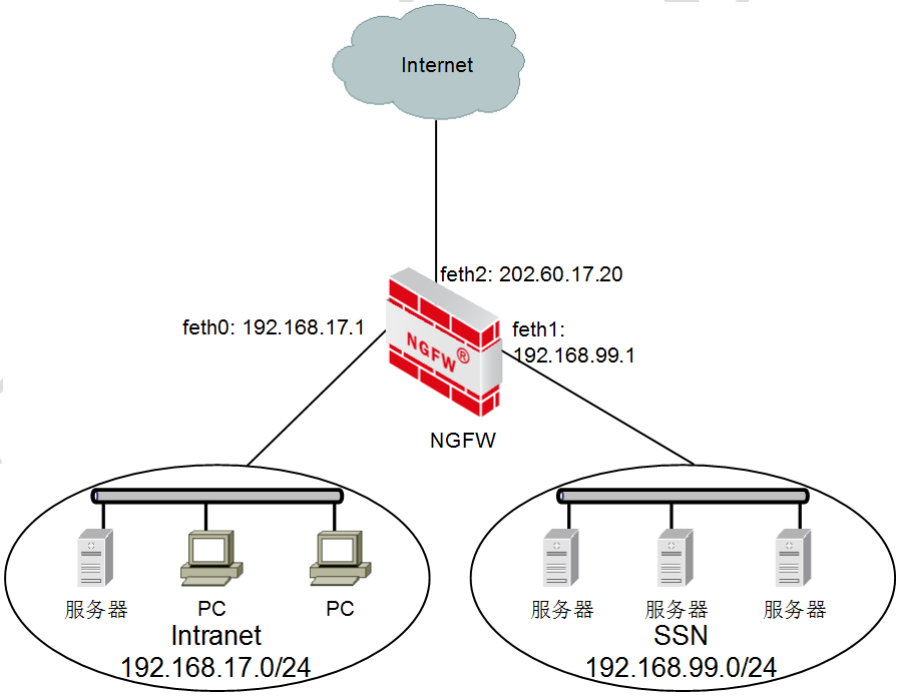


图 2-2 路由工作模式示意图

2.3.2 透明模式

在这种模式下，天融信下一代防火墙的所有接口均作为交换接口工作。也就是说，对于同一 VLAN 的数据包在转发时不作任何改动，包括 IP 和 MAC 地址，直接把包转发出去。同时，天融信下一代防火墙可以在设置了 IP 的 VLAN 之间进行路由转发。

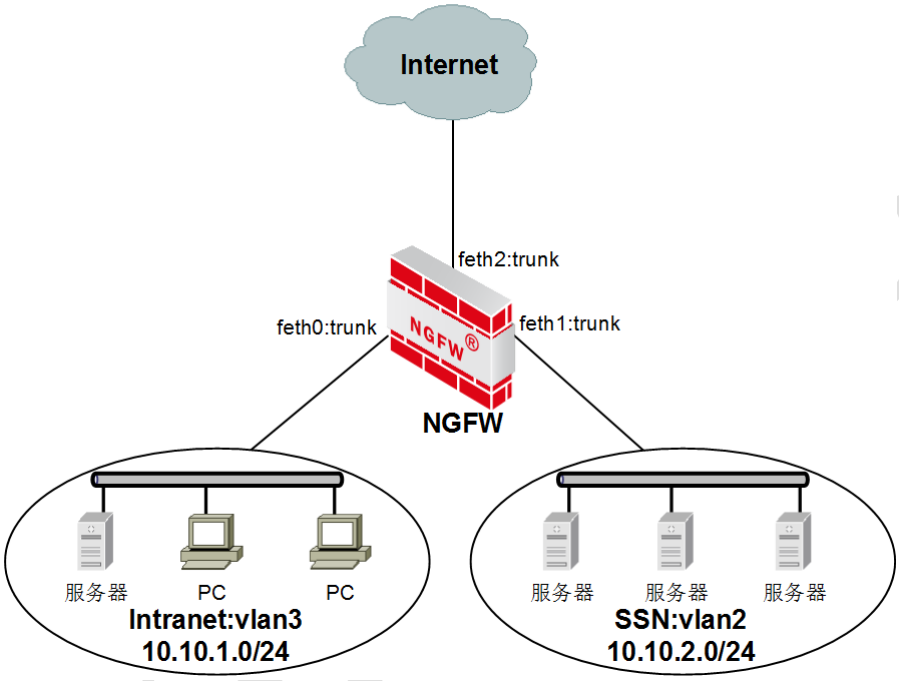


图 2-3 透明工作模式示意图

2.3.3 混合模式

顾名思义，这种模式是前两种模式的混合。也就是说某些区域（接口）工作在透明模式下，而其他的区域（接口）工作在路由模式下。该模式适用于较复杂的网络环境。如下图所示，feth1 接口为路由接口，配置了 IP 200.96.10.69，feth2 和 feth3 为交换接口，feth1 属于 Internet 区域，feth2 属于区域 intranet；feth3 属于 SSN 区域。

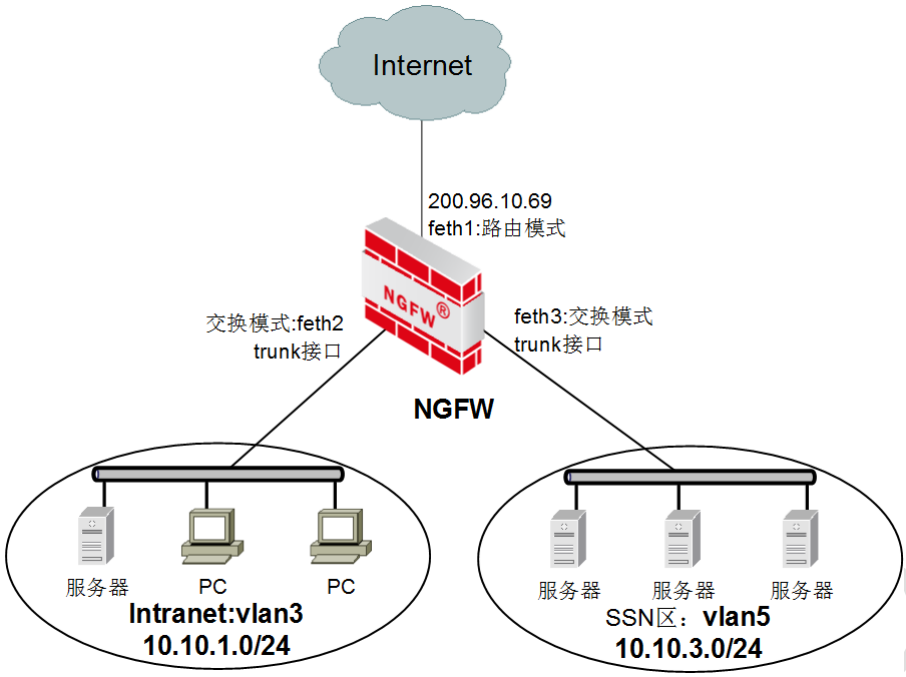


图 2-4 混合工作模式示意图

3 WEB 管理

管理员在登录系统前应首先安装部署 NGFW，安装成功后开启电源开关，才能通过管理主机登录并对系统进行管理。本章主要介绍登录界面、管理界面及常用图标说明。

3.1 登录界面

管理员在管理主机的浏览器上输入防火墙的管理 URL，例如：https://192.168.1.254，弹出如下的登录页面。

输入用户名密码（天融信下一代防火墙一员管理模式下默认出厂用户名/密码为：superman/talent，三员管理模式下的用户名/密码请参见 4.4*管理员（三权分立）），点击【登录】按钮，就可以进入管理页面。

说明

- ✧ 在输入 URL 时要注意以“https://”作为协议类型，例如 https://192.168.1.254。
- ✧ 天融信下一代防火墙对于用户名和密码大小写敏感。
- ✧ 管理主机的浏览器建议使用 IE8.0 以上版本。

3.2 管理界面

WEB 管理界面由一级标签栏、二级标签栏、页签、内容区及工具条组成。管理界面如下图所示。

对上图的说明如下：

图标	说明
20	每页显示信息条数，如“20”表示每页最多可显示 20 条信息。
	显示第一页。
	显示上一页。
	显示下一页。
	显示最后一页。
	刷新当前页面数据。
	保存当前配置。
	退出登录。
	右侧快捷方式存放区可自定义存放常用模块的快捷方式。如果需要存放某个模块的快捷方式，只需用鼠标将模块拖至快捷方式存放区后放开即可。该图标表示“删除”。如果需要删除某个模块的快捷方式，将该快捷方式拖至该图标后放开即可。

3.3 图标说明

管理页面中有很多图标帮助用户进行配置操作。当鼠标停留在可操作的图标上时，会出现提示信息以帮助理解图标的含义。下表将对页面中出现频率较高的图标进行说明。

图标	名称	说明
查看	查看	选中需要查看的条目，点击该图标即可查看该条目的详细信息。
添加	添加	点击该图标，添加新条目。
编辑	编辑	选中需要修改的条目，点击该图标即可对该条目重新进行编辑。
删除	删除	选中需要删除的条目，点击该图标即可将该条目删除。
	刷新	点击该图标，刷新当前管理页面。
搜索	搜索	输入查询关键子，点击该图标即可查询带有关键字信息的条目。
清空	清空	选中需要清空的条目，点击该图标即可以清空该条目的统计或者配置信息。
启用	启用	选中需要启用的条目，点击该图标即可启用该条目。
禁用	禁用	选中需要启用的条目，点击该图标即可禁用该条目，此时该配置项所在行变为深灰色。
移动	移动	选中需要移动的条目，在弹出的对话框中，选中该条目移动的目的位置。
显示统计	显示统计	选中需要显示统计信息的条目，点击该图标即可显示统计信息。
克隆	克隆	选中需要复制的条目，点击该图标即可复制该条目。
属性	属性	选中需要修改属性的条目，点击该图标，即可修改该条目的属性。
查询	查询	选中需要移动的条目，在弹出的对话框中，输入查询条件，即可查询符合条件的条目。
保存	保存	点击该图标，保存配置。
另存为	另存为	点击该图标，备份配置信息。
导入	导入	点击该图标，在弹出的对话框中，配置导入信息，即可完成导入。
导出	导出	选中需要导出的条目，点击该图标，在弹出的对话框中，选择条目的保存地址，即可完成导出。

4 系统管理

NGFW 的系统模块用于关联各功能模块，并可协调、控制各个功能模块的功能和性能，保证系统正常稳定运行。系统的稳定性是 NGFW 稳定、高效运作的基础。本章主要介绍如何管理、配置、维护、优化系统的基本操作，主要包括以下内容：

- 系统设置：介绍查看及配置系统的基本信息、系统参数、系统时间，以及诊断系统的连通性、配置 SNMP 功能和配置本地域名解析服务器。
- 系统维护：介绍维护配置文件、升级固件、获取健康记录、重启系统和升级规则库。
- 管理员（一员管理）：介绍一员模式下管理员及其权限管理方法。
- *管理员（三权分立）：介绍三员模式下管理员及其权限管理方法。
- 系统日志：介绍配置日志记录条件、配置日志服务器以及查看日志信息。
- 告警：介绍设备报警方式及触发条件配置方法。
- 高可用性：介绍 NGFW 的双机热备、负载均衡和连接保护功能的实现方法。

4.1 系统设置

系统设置包括查看系统基本信息、设置系统参数、设置系统时间、诊断系统连通性、修改当前管理员密码、配置 SNMP 管理主机、配置 SNMP 陷阱主机、配置 SNMPv3 用户、设置本地 DNS 服务器以及开放本地服务。

4.1.1 系统信息

“系统信息”界面显示了 NGFW 的硬件组成部分和软件组成部分的详细信息。

WEBUI 查看方式

选择 **系统管理** > **系统设置** > **系统信息**，如下图所示。

界面中显示了 NGFW 的产品型号、产品序列号、操作系统、软件版本、许可证版本号、系统名称、终端超时时间、系统时间和系统运行时间。关于系统名称、终端超时和系统时间的配置具体请参见 4.1.2 系统参数。

CLI 查看方式

system product model <cr>

命令描述：

查看系统产品型号。

以下是查看系统产品型号的示例：

```
TopsecOS # system product model
TOPSEC-XX
```

system product sn <cr>

命令描述：

查看系统产品序列号。

以下是查看系统产品序列号的示例：

```
TopsecOS # system product sn
001631ffccd4.001
```

system version <cr>

命令描述：

显示系统版本信息。

以下是显示系统版本的示例：

```
TopsecOS# system version
VERSION: v3.1130.1243.1_ngfw
PSN: Unkonw
```

system devname show <cr>

命令描述：

该命令用于查看 NGFW 名称。

以下是显示已配置 NGFW 名称的示例：

```
TopOS# system devname show
system devname set TopsecOS
```

system terminal show <cr>

命令描述：

显示终端空闲超时时间。

以下是设置终端超时时间的示例：

```
TopsecOS# system terminal show
terminal idle timeout: 60 seconds
```

system time show <cr>

命令描述：

显示系统日期。

以下是显示系统日期的示例：

```
TopsecOS # system time show
+08 2014-09-09 06:09:32
```

system uptime <cr>

命令描述：

显示系统启动后运行的总时间。

以下是显示系统运行总时间的示例：

```
TopsecOS # system uptime
UP 1 day, 00:19:56
```

4.1.2 系统参数

“系统参数”界面包括标识设备的名称、设备在处理数据报文时的基本网络参数、以及流量统计开关。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **系统参数**，如下图所示。

步骤 2 配置系统参数。

在设置系统参数时，各项参数的具体说明如下表所示。

参数	说明
设备名称	设置 NGFW 的设备名称，默认为 TopsecOS。
终端空闲超时	设置管理员通过 WebUI 方式对 NGFW 进行管理的空闲超时时间，超过该空闲时间，如果管理员没有对 NGFW 执行任何操作，该管理连接自动中断。 单位：秒；取值范围：0，30-3600；默认值：180，设置为 0，表示永不超时。
长连接超时	设置长连接的超时时间。 单位：秒；取值范围：3600-8388607；默认值：86400。
握手时 TCP 连接超时	设定建立 TCP 连接的三次握手的超时时间。 单位：秒；取值范围：10-200；默认值：100。
关闭时 TCP 超时时间	设置关闭 TCP 连接的超时时间。 单位：秒；取值范围：3-800；默认值：20。
TCP 超时时间	设置建立 TCP 连接后的空闲超时时间。TCP 连接建立后，在空闲超时时间内，如果无相同五元组的 TCP 连接通过 NGFW，NGFW 则将该建立的连接删除。 单位：秒；取值范围：10-7200；默认值：1800。
UDP 超时时间	设置建立 UDP 连接后的空闲超时时间。UDP 连接建立后，在空闲超时时间内，如果没有相同五元组的 UDP 连接通过 NGFW，NGFW 则将该建立的连接删除。 单位：秒；取值范围：10-7200；默认值：60。

参数	说明
其他连接超时	设置除 TCP、UDP 连接外其他类型连接的超时时间。 单位：秒；取值范围：10-7200；默认值：20。
长连接占总连接的百分比	设置长连接占总连接百分比的上限。单位：%；取值范围：5-90。 说明： 当长连接占总连接的百分比超过此处设置的值，NGFW 将自动删除存在时间较长的长连接，以避免大量的长连接一直占用内存。
TCP reset	对于违反安全策略的 TCP 连接，设定是否允许 NGFW 发送 TCP Reset 报文以中断连接。
包校验和	设置是否对 IP/TCP/UDP/ICMP 数据包进行校验。
分片重组	设置是否支持对接收到的分片 IP 数据包进行重组。
连接完整	是否启用 TCP 连接完整性状态检测开关。 说明： 1）TCP 连接完整性状态检测开关处于开启状态下时，NGFW 会跟踪 TCP 连接的状态，TCP 连接必须通过完整的三次握手，NGFW 才允许其建立连接；TCP 连接经过四次结束握手或者收到 RST 数据包，NGFW 才终结其连接。 2）在特殊情况下，对于某种 TCP 连接，如果建立的时候并没有经过 NGFW，连接建立以后需要经过 NGFW，则需要关闭状态检测开关，否则，该种连接会因不符合 NGFW 的 TCP 连接完整性标准而被丢弃。
快速连接重用	是否启用快速连接重用开关。 说明： 当源到目的的连接已经存在，源向目的发送 SYN 包时，如果快速连接重用开关处于开启状态，NGFW 会将已建立的连接删除并重新建立连接；否则，NGFW 直接将该 SYN 包丢弃。
非 syn 包建立连接	对于 TCP 连接，设置是否允许第一个报文不是 SYN 报文的连接建立新连接。
流量统计开关设置	是否开启 NGFW 统计各种类型流量的开关.。流量类型包括：会话流量、用户及应用流量、服务器流量、威胁事件及 VPN 隧道流量。

步骤 3 系统参数设置完成后，点击【应用】按钮完成系统参数的配置。

CLI 方式配置配置

system devname set <*string*>

命令描述：

该命令用于配置 NGFW 名称。

参数说明：

system devname set	必选项。配置 NGFW 名称。
string	字符串类型，默认值：TopsecOS。

以下是配置 NGFW 名称的示例：

修改系统名称为 TopOS。

TopsecOS# **system devname set** *TopOS*

system terminal idle-timeout <*number*>

命令描述：

设置终端空闲超时时间。

参数说明：

system terminal idle-timeout	必选项。设置终端空闲超时时间。
number	数值类型。单位：秒；取值范围：0，30-3600；默认值：60，0 表示永不超时。

以下是设置终端超时时间的示例：

设置终端空闲超时时间为 60 秒。

TopsecOS# **system terminal idle-timeout** *60*

network session timeout never-expire <*number*|default>

命令描述：

设置长连接的超时时间。

参数说明：

network session timeout never-expire	必选项，设置长连接的超时时间。
number	数值类型，单位：秒；取值范围：3600-8388607；默认值：24 小时。
default	设定为默认超时值。

以下为设置长连接超时时间的示例：

设置长连接的超时时间为 2 天。

TopsecOS#**network timeout never-expire** *172800*

network session timeout handshake <*number*|default>

命令描述：

设置 TCP 三次握手的超时时间。

参数说明：

network session timeout handshake	必选项，指定三次握手阶段 TCP 连接的超时时间。
number	数值类型，单位：秒；取值范围：10-200；默认值：100。
default	设定为默认超时值。

以下为设定 TCP 三次握手超时时间的示例：

设定三次握手阶段 TCP 连接的超时时间为 150 秒。

TopsecOS#**network session timeout handshake** *150*

设定三次握手阶段 TCP 连接的超时时间为默认值。

TopsecOS# **network session timeout handshake** default

network session timeout close <*number*|default>

命令描述：

设置关闭 TCP 连接的超时时间。

参数说明：

network session timeout close	必选项，指定关闭 TCP 连接的超时时间。
number	数值类型，单位：秒；取值范围：3-800；默认值：20。
default	设定为默认超时值。

以下为设置关闭 TCP 连接超时时间的示例：

设定关闭 TCP 连接的超时时间为默认值 20 秒。

TopsecOS#**network session timeout close** default

设定关闭 TCP 连接的超时时间为 200 秒。

TopsecOS#**network session timeout close** *200*

network session timeout established <*number*|default>

命令描述：

设置建立 TCP 连接后的空闲超时。

参数说明：

network session timeout established	必选项，设定建立 TCP 连接后的空闲超时时间。
number	数值类型，单位：秒；取值范围：10-7200；默认值：1800。
default	设定为默认超时值。

以下为设定建立 TCP 连接后的空闲超时时间命令示例：

设定已建立 TCP 连接的超时时间为默认值。

```
TopsecOS# network session timeout established default
```

network session timeout udp <*number*|default>

命令描述：

设置 UDP 连接的超时时间。

参数说明：

network session timeout udp	必选项，指定 UDP 连接的超时时间。
number	数值类型，单位：秒；取值范围：10-7200；默认值：60。
default	设定为默认超时值。

以下为 UDP 连接超时时间的示例：

设定 UDP 连接的超时时间为默认值 60 秒。

```
TopsecOS#network session timeout udp default
```

设定 UDP 连接的超时时间为 200 秒。

```
TopsecOS#network session timeout udp 200
```

network session timeout other <*number*|default>

命令描述：

设置除 TCP、UDP 连接外其他类型连接的超时时间。

参数说明：

network session timeout other	必选项，指定其他类型连接的超时时间。
number	数值类型，单位：秒；取值范围：10-7200；默认值：20。
default	设定为默认超时值。

以下为设定其他类型连接超时时间的示例：

设定其他类型连接的超时时间为默认值 20 秒。

TopsecOS#**network session timeout other** default

设定其他类型连接的超时时间为 200 秒。

TopsecOS#**network session timeout other** *200*

network session timeout default <cr>

命令描述：

将所有连接的超时参数设置为默认值。

以下为将所有连接超时参数设置为默认值的示例：

TopsecOS#**network session timeout default**

network session never-expire-percent <*number*>

命令描述：

设置长连接占总连接百分比的上限。

参数说明：

network session never-expire-percent	必选项，设置长连接占总连接百分比的上限。
number	数值类型，单位：%；取值范围：5-90；默认值：10。

以下为设置长连接占总连接百分比上限的示例：

设置长连接占总连接百分比的上限为 20%。

TopsecOS# **network session never-expire-percent** *20*

network session tcp-reset <on|off>

命令描述：

设定是否允许设备发送 TCP Reset 报文。

参数说明：

network session tcp-reset	必选项，设定是否允许设备发送 TCP Reset 报文。默认不允许。
on|off	是|否

以下为设置允许发送 TCP Reset 报文的示例：

```
TopsecOS# session tcp-reset on
```

network session packet-checksum <on|off>

命令描述：

设定是否对 TCP、UDP、ICMP 的 IP 数据报文进行校验。

参数说明：

network session packet-checksum	必选项，设定是否对数据报文进行校验。
on|off	是|否

以下为设置对数据报文进行校验的示例：

```
TopsecOS# network session packet-checksum on
```

network session defrag <on|off>

命令描述：

设置 NGFW 是否支持对分片的 IP 报文具有重组的功能，默认情况下，NGFW 的重组开关处于开启状态。

参数说明：

network session defrag	设置 NGFW 是否支持对分片的报文进行重组。
on|off	开|关

以下为关闭 NGFW 对分片报文重组功能的示例：

```
TopsecOS# network session defrag off
```

network session session-integrity <on|off>

命令描述：

TCP 连接完整性状态检测开关设置。

参数说明：

network session session-integrity	必选项，设定是否对数据报文的 TCP 连接完整性进行检测。
on|off	是|否

以下为不进行 TCP 连接完整性检测的示例：

```
TopsecOS# network session session-integrity off
```

network session syn-reset <on|off>

命令描述：

快速连接重用设置。

参数说明：

network session syn-reset	必选项，设置是否开启快速连接重用功能，默认为关闭。
on|off	开启|关闭

以下为开启快速连接重用的示例：

```
TopsecOS# network session syn-reset on
```

network session only-syn-create <on|off>

命令描述：

NGFW 对接收的 TCP 数据包的第一个 TCP 报文进行限定，如果第一个报文为 SYN 报文才允许建立连接。

参数说明：

network session only-syn-create	设置是否只允许第一个报文为 SYN 报文建立新连接。
on|off	开启|关闭

以下为只允许 SYN 报文建立新连接的示例：

TopsecOS# **network session only-syn-create** on

stat switch session <on|off>

命令描述：

是否开启 NGFW 的会话流量统计开关。

参数说明：

stat switch session	设置是否开启 NGFW 的会话流量统计开关。
on|off	开启|关闭

以下为开启会话流量统计开关的示例：

TopsecOS#**stat switch session** on

stat switch user_app <on|off>

命令描述：

是否开启用户及应用流量统计开关。

参数说明：

stat switch user_app	设置是否开启用户及应用流量统计开关。
on|off	开启|关闭

以下为开启用户及应用流量统计开关的示例：

TopsecOS# **stat switch user_app** on

stat switch server <on|off>

命令描述：

是否开启服务器流量统计开关。

参数说明：

stat switch server	设置是否开启服务器流量统计开关。
on|off	开启|关闭

以下为开启服务器流量统计开关的示例：

```
TopsecOS# stat switch server on
```

stat switch threat <on|off>

命令描述：

是否开启威胁事件流量统计开关。

参数说明：

stat switch threat	设置是否开启威胁事件流量统计开关。
on|off	开启|关闭

以下为开启威胁事件流量统计开关的示例：

```
TopsecOS# stat switch threat on
```

stat switch vpn_tunnel <on|off>

命令描述：

是否开启 VPN 隧道流量统计开关。

参数说明：

stat switch vpn_tunnel	设置是否开启 VPN 隧道流量统计开关。
on|off	开启|关闭

以下为开启 VPN 隧道流量统计开关的示例：

```
TopsecOS# stat switch vpn_tunnel on
```

stat switch show <cr>

命令描述：

查看统计功能开关信息。

以下是查看统计功能开关信息的示例：

```
TopsecOS# stat switch show
session flow statistics switch is on
user_app flow statistics switch is off
```

server flow statistics switch is off
qos channel flow statistics switch is off
vpn tunnel flow statistics switch is off
threat flow statistics switch is off

stat switch reset <cr>

命令描述：

重置统计功能开关。

4.1.3 系统时间

NGFW 内置时钟，是记录日志信息、安全策略、监控系统等事件的时间基准，因此，NGFW 时间对具有时间戳的策略发生作用产生直接影响。NGFW 为确保时间的精准性提供了系统时间管理功能，管理员可以手动修改系统时间，可以简单地根据管理主机的内置时钟对 NGFW 时钟进行同步，也可以启动 NTP（Network Time Protocol，网络时间协议）服务根据设定的 NTP 服务器上的时间来同步 NGFW 的系统时钟。其中，通过 NTP 可使用户网络中的应用服务器、其他安全产品及网络管理系统等保持系统时间的严格一致，使 NGFW 几乎零时差防护用户网络成为可能。

NTP 基于 UDP 传输，使用端口号 123，是为网络设备向参考时间源提供高精准度时间同步的协议。NGFW 既可以作为 NTP 服务器也可作为 NTP 客户端，NTP 服务器提供参考时间可为网络设备提供授时服务，为整个网络传递统一、标准的时间；NTP 客户端周期向 NTP 服务器设备发送 NTP 报文以同步其时间。

假设 NGFW 作为 NTP 客户端，NGFW 系统时间为 11:00:00am，NTP 服务器系统时间为 12:00:00am，NTP 数据包在 NGFW 与 NTP 服务器间单向传输需要 1s，NGFW 和 NTP 服务器处理 NTP 数据包的时间均为 1s，NTP 同步时间实现原理简要描述如下图所示。

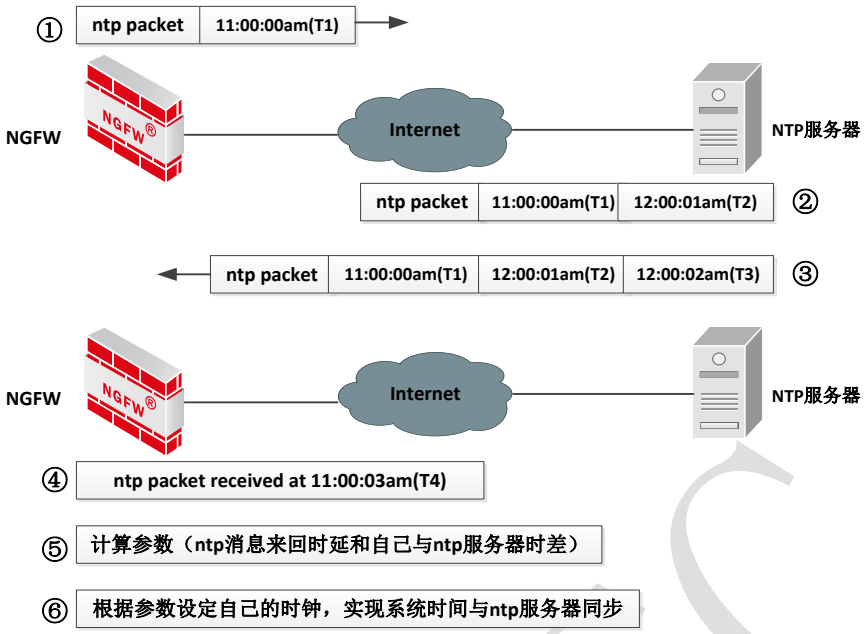


图 4-1 NTP 实现过程图

- NGFW 向 NTP 服务器发送 NTP 报文，报文中带有报文离开 NGFW 时的时间戳 11:00:00am（T1）。
- NTP 服务器接收到该 NTP 报文，在该报文中加上报文到达时间戳 12:00:01am（T2），然后再加上其向 NGFW 回复确认 NTP 报文的时间戳 12:00:02am（T3），发送给 NGFW。
- NGFW 接收到该 NTP 报文时，加上接收到该报文的时间戳 11:00:03am（T4）。至此，NGFW 获取了 NGFW 相对于 NTP 服务器的时间差为（（T2-T1）+（T3-T4））/2 和 NTP 消息来回一个周期的时延为（T4-T1）-（T3-T2），最后 NGFW 根据获取的其与 NTP 服务器的时间差及 NTP 消息来回时延设定自己的时钟，实现其与 NTP 服务器的时钟同步。

NGFW 作为 NTP 客户端时，会向 NTP 服务器定期发送 NTP 报文以同步时间，同步时间时，首先向主 NTP 服务器同步时间，如果主 NTP 服务器不可达时，则向备份 NTP 服务器同步时间。

本节主要介绍系统时间的配置。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **系统时间**。

步骤 2 设置时区。在“时区”下拉框中选择 NGFW 设备所处区域的时区。

步骤 3 设置系统时间。修改系统时间的方式有三种，下面分别予以详细介绍。

- 手动修改：选中“手动设置”，点击“系统日期时间”右侧文本框后的时间设置工具设置系统时间。
- 与管理主机时间同步：选中“本地同步”。
- 与 NTP 服务器时间同步：选中“NTP 设置”，在服务器地址文本框中输入 NTP 服务器的 IP 地址。在设置 NTP 服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器地址 1	输入首选的 NTP 服务器的 IP 地址。
服务器地址 2	在有备用 NTP 服务器的情况下，输入备用 NTP 服务器的 IP 地址。 说明： NGFW 无法通过首选 NTP 服务器同步时间时，将尝试与备用 NTP 服务器的时间同步。
同步地址	需通过 NTP 服务器手动即时同步系统时间时，该参数为必选项。输入 NTP 服务器的 IP 地址，点击【立即同步】按钮，NGFW 立即与该 NTP 服务器时间同步。 说明： “同步地址”处配置的 NTP 服务器为 NGFW 一次同步时间 NTP 服务器。

说明

- ✧ 通过 NTP 服务器周期性同步系统时间之前，建议尽可能先将系统时间设置为接近正确的时间。
- ✧ 在“NTP 服务器地址 1”/“NTP 服务器地址 2”处配置了 NTP 服务器地址，NGFW 即作为 NTP 客户端周期性发送 NTP 报文向 NTP 服务器地址 1”/“NTP 服务器地址 2”处配置的 NTP 服务器同步时间，也同时作为 NTP 服务器为其他网络设备提供时间基准。

步骤 4 时区和时间设置完成后，点击【应用】按钮完成 NGFW 系统时间的修改。

CLI 方式配置

system time set [**clock** <*string1*>] [**date** <*string2*>] [**timezone** <*string3*>]

命令描述：

手工设置系统日期。

参数说明：

system time set	设置系统时间。
colck	可选项，设置时间，时、分、秒。
string1	字符串类型，形为 HH:MM:SS。
date	可选项，设置日期，年、月、日。
string2	字符串类型，形为 YYYY-MM-DD。
timezone	可选项，设置时区。
string3	字符串类型，格式为 <+|->TZ，“+”表示东区，“-”表示西区，“TZ”取值范围：1-12。

以下是设置系统日期的示例：

设置时间为 2013-10-01 的 12:00:00，时区为东八区。

```
TopsecOS# system time set clock 12:00:00 date 2013-10-01 timezone +8
```

system ntp start [**ip** <*ipaddress1*>] [**ip2** <*ipaddress2*>]

命令描述：

当不指定 IP 参数时，启动 NGFW 作为 NTP 服务器。当指定 IP 参数时，启动 NGFW 作为 NTP 客户端与 IP 参数设置的 NTP 服务器进行时间同步。

参数说明：

system ntp start	启动 NTP 同步进程。
ip	可选项，当 NGFW 作为 NTP 客户端时，设定 NTP 服务器 IPv4 地址。
ipaddress1	IPv4 地址字符串，形为 A.B.C.D。
ip2	可选项，当 NGFW 作为 NTP 客户端时，设定备份 NTP 服务器 IPv4 地址。
ipaddress2	IPv4 地址字符串，形为 A.B.C.D。

以下是启动 NTP 同步的示例：

启动 NTP 同步，服务器为 192.168.90.20。

```
TopsecOS# system ntp start ip 192.168.90.20
```

启动 NTP 服务器。

```
TopsecOS# system ntp start
```

system ntp show <cr>

命令描述：

显示 NTP 的配置信息和状态。

以下是显示 NTP 配置的示例：

```
TopsecOS# system ntp show
Ntp Client mode running, ntp server ip1: 192.168.90.224 ip2: 192.168.90.20
```

system ntp stop <cr>

命令描述：

停止 NTP 同步进程。

以下是停止 NTP 同步进程的示例：

```
TopsecOS# system ntp stop
TopsecOS# system ntp show
Ntp stopped
```

system ntp update ip <*ipaddress*>

命令描述：

NGFW 上的时间和 NTP 服务器立即同步时间。

参数说明：

system ntp update	NGFW 上的时间和 NTP 服务器进行时间同步。
ip	必选项。设定 NTP 服务器的 IPv4 地址。
ipaddress	IPv4 地址字符串，格式为 A.B.C.D。

以下是通过 NTP 服务器立即同步时间的示例：

通过 NTP 服务器 172.16.1.23 立即同步时间。

```
TopsecOS# system ntp update ip 172.16.1.23
```

4.1.4 系统诊断

根据网络传输的原理，NGFW 分别针对网络层、传输层和应用层提供诊断系统网络连通性的工具，包括 PING、TRACEROUTE、TCP、HTTP 和 DNS。

- PING，探测 NGFW 到目的主机的网络层是否可达。
- TRACEROUTE，探测 NGFW 到达目的主机所经过的路由设备。
- TCP，探测 NGFW 与目标主机建立三次握手所花费的时间，以诊断网络连通状态。
- HTTP，探测 NGFW 与使用 HTTP 协议的服务器是否可达。
- DNS，探测 DNS 服务器是否能成功解析某域名。

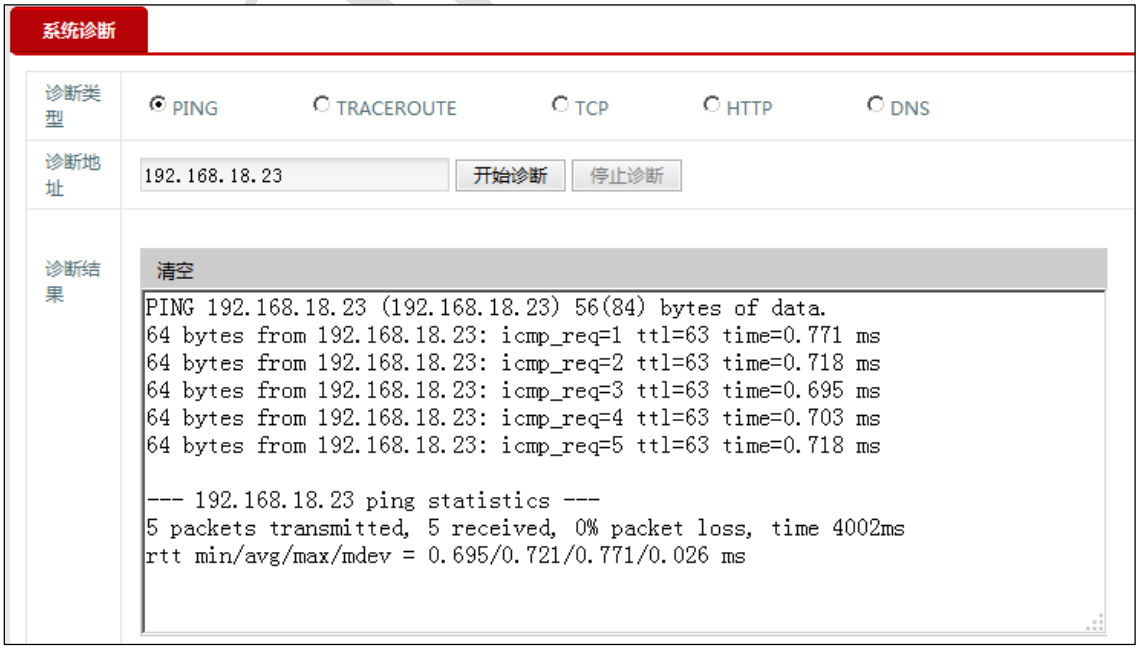
WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **系统诊断**。

步骤 2 诊断。

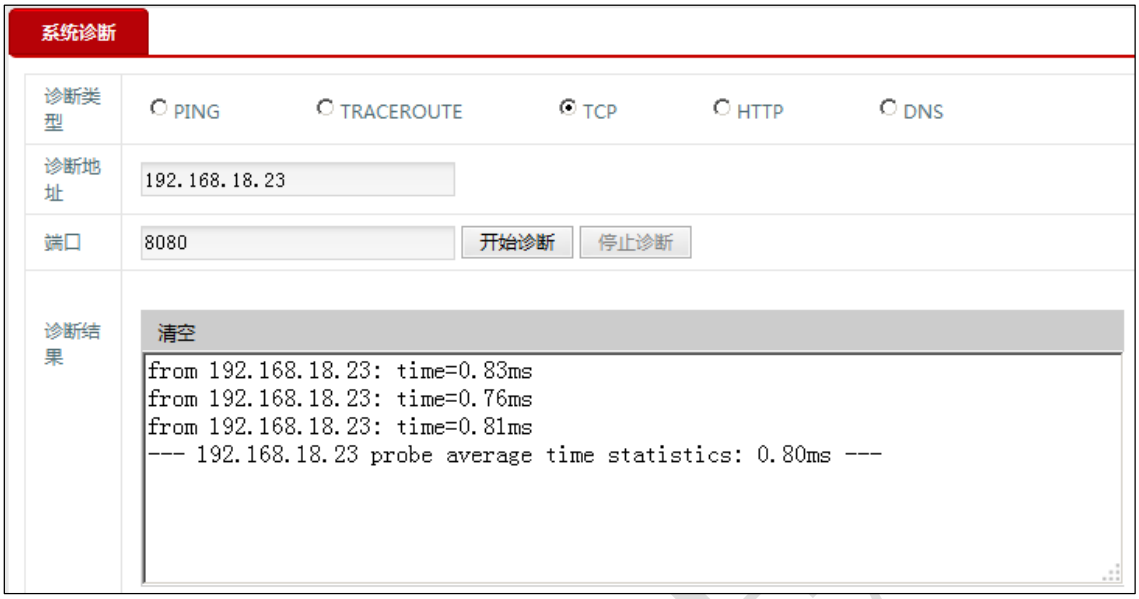
- 网络层诊断

选择“PING”或“TRACEROUTE”，然后在“诊断地址”文本框中输入目的 IP 地址，点击【开始诊断】按钮执行目的可达性检测，如下图所示。



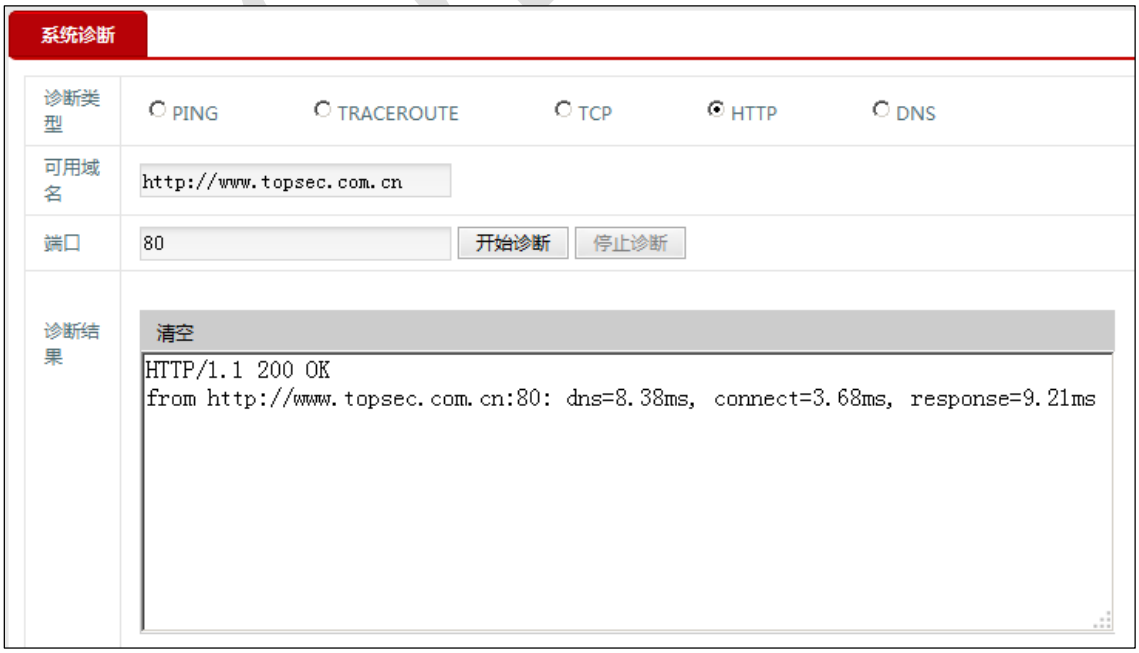
- 传输层诊断

选择“TCP”，然后在“诊断地址”文本框中输入目的 IP 地址，“端口”文本框中配置端口号，点击【开始诊断】按钮执行目的可达性检测，如下图所示。



➢ 应用层诊断

选择“HTTP”，在“可用域名”文本框中输入域名，在“端口”文本框中输入端口号；选择“DNS”，则在“诊断地址”文本框中输入 DNS 服务器地址，然后在“可用域名”文本框中配置域名。点击【开始诊断】按钮执行目的可达性检测，如下图所示。



步骤 3 点击【停止诊断】按钮可以停止命令执行，如点击『清空』可以将命令的执行结果从 WEBUI 界面中删除。

CLI 方式配置

ping <*string1*> [**interface** <*string2*>] [**count** <*number1*>] [**size** <*number2*>]

命令描述：

验证 NGFW 与 IPv4 主机或网络设备的连接情况。

参数说明：

ping	验证 NGFW 与 IPv4 主机或网络设备的连接情况。
string1	字符串类型，表示 IPv4 地址或者域名。如果为 IPv4 地址字符串，格式为 A.B.C.D。如果为域名，格式为 www.topsec.com.cn。
interface	可选项，数据报文传出时通过的接口名称或 IPv4 地址。
string2	字符串类型，物理接口名称或 IPv4 地址。
count	可选项，设定发送 ping 包的次数。
number1	数值类型，表示次数数值。
size	可选项，设定发送 ping 包的字节长度。
number2	数值类型。单位：字节；取值范围：0-65492。

以下是目的 IPv4 地址诊断的示例：

目的 IPv4 地址为 192.168.90.79，出接口 IPv4 地址为 192.168.90.70，数据包大小为 30000 字节，接收包的次数为 100。

TopsecOS # **ping** *192.168.90.79* **interface** *192.168.90.70* **count** *100* **size** *30000*

PING 192.168.90.79(192.168.90.79) 30000(30028) bytes of data

30008 bytes from 192.168.90.79: icmp_req=1 ttl=64 time=0.101 ms

30008 bytes from 192.168.90.79: icmp_req=2 ttl=64 time=0.052 ms

ping6 <*string1*> [**interface** <*string2*>] [**count** <*number1*>] [**size** <*number2*>]

命令描述：

验证 NGFW 与 IPv6 主机或网络设备的连接情况。

参数说明：

ping6	必选项。验证 NGFW 与 IPv6 主机或网络设备的连接情况。
string1	字符串类型，表示 IPv6 地址或者域名。格式为 IPv6 地址字符串或 www.topsec.com.cn。
interface	可选项，数据报文传出时通过的接口名称或 IPv6 地址。

string2	字符串类型，物理接口名称或 IPv6 地址。
count	可选项，设定发送 ping 包的次数。
number1	数值类型，表示次数数值。
size	可选项，设定发送 ping 包的字节长度。
number2	数值类型。单位：字节；取值范围：0-65492。

以下是目的 IPv6 地址诊断的示例：

目的 IPv6 地址为 2200::1。

```
TopsecOS # ping6 2200::1

PING 2200::1(2200::1) 56 data bytes

64 bytes from 2200::1: icmp_seq=1 ttl=64 time=0.059 ms

64 bytes from 2200::1: icmp_seq=2 ttl=64 time=0.100 ms

64 bytes from 2200::1: icmp_seq=3 ttl=64 time=0.036 ms

64 bytes from 2200::1: icmp_seq=4 ttl=64 time=0.067 ms

64 bytes from 2200::1: icmp_seq=5 ttl=64 time=0.045 ms

64 bytes from 2200::1: icmp_seq=6 ttl=64 time=0.037 ms
```

system traceroute <*string*> [**maximum** <*number1*>] [**port** <*port*>] [**count** <*number2*>] [**wait** <*number3*>]

命令描述：

显示路由封包到达目的 IPv4 地址的信息。

参数说明：

system traceroute	必选项。显示路由封包到达目的地址的信息。
string	字符串类型，表示目标 IPv4 地址，格式为 A.B.C.D。
maximum	可选项，设置目的可达的最大路由跳数。
number1	数值类型，TTL 大小的数值。
port	可选项，设置 UDP 传输协议的通信端口。
port	通信端口。取值范围：0-65535。
count	可选项，探测包的个数。
number2	数值类型，默认值：3。
wait	可选项，设置等待远端主机响应的最大时间，超过该时间还未收到远端主机的响应，则表示该远端主机不可达。
number3	数值类型，代表时间长短。

以下是显示路由封包到达目的 IPv4 地址信息的示例：

目的 IPv4 地址为 192.168.90.70。

```
TopsecOS # system traceroute 192.168.90.70
traceroute to 192.168.90.70 (192.168.90.70), 30 hops max, 60 byte packets
 1  192.168.90.70 (192.168.90.70)  0.353 ms * *
```

system traceroute6 <*string*> [**maximum** <*number1*>] [**port** <*port*>] [**count** <*number2*>] [**wait** <*number3*>]

命令描述：

显示路由封包到达目的 IPv6 地址的信息。

参数说明：

system traceroute6	必选项。显示路由封包到达目的地址的信息。
string	字符串类型，表示目标 IPv6 地址，格式为 x:x:x:x:x:x:x:x，其中 x 为一个 4 位十六进制整数。
maximum	可选项，设置目的可达的最大路由跳数。
number1	数值类型，TTL 大小的数值。
port	可选项，设置 UDP 传输协议的通信端口。
port	通信端口。取值范围：0-65536。
count	可选项，探测包的个数。
number2	数值类型。
wait	可选项，设置等待远端主机响应的最大时间，超过该时间还未收到远端主机的响应，则表示该远端主机不可达。
number3	数值类型，表示时间。

以下是显示路由封包到达目的 IPv6 地址信息的示例：

目的 IPv6 地址为 2100::1。

```
TopsecOS# system traceroute6 2100::1
traceroute to 2100::1 (2100::1), 30 hops max, 80 byte packets
 1  2100::1 (2100::1)  0.031 ms  0.006 ms  0.004 ms
```

system probe tcp serverip <*ipaddress*> **port** <*port*> [**count** <*number1*>] [**interval** <*number2*>]

命令描述：

通过 TCP 协议探测网络状况。

参数说明：

system probe tcp	通过 TCP 协议探测网络状况。
serverip	必选项，指定目标主机 IP 地址。
ipaddress	IP 地址字符串，格式 x.x.x.x。

port	必选项，设置通信端口。
port	数值类型，表示端口号。
count	可选项，探测包的个数。
number1	数值类型，单位：次；默认值：3。
interval	可选项，探测包的间隔。
number2	数值类型，单位：秒；默认值：0。

以下是通过 TCP 协议探测主机 192.168.18.23 的 8080 端口的示例：

TopsecOS# **system probe tcp serverip** *192.168.18.23* **port** *8080*

from 192.168.18.23: time=1.29ms

from 192.168.18.23: time=0.77ms

from 192.168.18.23: time=0.84ms

--- 192.168.18.23 probe average time statistics: 0.97ms ---

system probe http domain <*string*> [**count** <*number1*>] [**interval** <*number2*>]

命令描述：

通过 http 协议探测网络状况。

参数说明：

system probe http	通过 http 协议探测网络状况。
domain	必选项，指定域名地址。
string	字符串类型。
count	可选项，探测包的个数。
number1	数值类型，单位：次；默认值：1。
interval	可选项，探测包的间隔。
number2	数值类型，单位：秒；默认值：0。

以下是探测 http://www.topsec.com.cn 是否可达的示例：

TopsecOS#**system probe http domain** *http://www.topsec.com.cn*

HTTP/1.1 200 OK

from http://www.topsec.com.cn: dns=2.89ms, connect=3.79ms, response=2.79ms

system probe dns serverip <*ipaddress*> **domain** <*string*> [**count** <*number1*>] [**interval** <*number2*>]

命令描述：

诊断 DNS 服务器是否可解析某域名。

参数说明：

system probe dns	诊断 DNS 服务器是否可解析某域名。
serverip	必选项，指定域名服务器 IP 地址。
ipaddress	字符串类型。
domain s	必选项，指定域名。
string	字符串类型。
count	可选项，探测包的个数。
number1	数值类型，单位：次；默认值：3。
interval	可选项，探测包的间隔。
number2	数值类型，单位：秒；默认值：0。

以下是探测域名服务器 172.16.1.254 是否可解析 www.topsec.com 的示例：

TopsecOS#**system probe dns serverip** *172.16.1.254* **dns** *www.topsec.com*

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=6.20ms

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=4.53ms

48 bytes from 172.16.1.254, www.topsec.com has ipv4 address: 195.218.116.139, dns=1.64ms

--- sum data: 144 bytes, average time statistics: 4.12ms ---

4.1.5 密码设置

为降低管理员管理管理员账号的难度，并保障普通管理员账号的安全，NGFW 支持管理员修改其自身密码。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **密码设置**。

说明

✧ 在管理员模块的设置界面中配置好密码强度，在此处提示出选择的强度。关于密码强度的设置具体请参见 4.3.3 设置。

在修改管理员自身密码时，各项参数的具体说明如下表所示。

参数	说明
输入原始密码	输入管理员账号当前密码。
输入密码	设置新密码，新密码不能与旧密码相同，密码的复杂度的设置具体请参见 4.3.3 设置。
再次输入	再次输入新密码，需与“输入密码”文本框中输入的密码完全一致。

步骤 2 点击【应用】按钮完成密码的修改。

CLI 方式配置

password old-password <*string1*> **new-password** <*string2*> **new-repeat** <*string3*>

命令描述：

修改当前管理员的密码。

参数说明：

password	修改当前管理员密码。
old-password	必选项。输入管理员的当前密码。
string1	字符串类型。

new-password	必选项，输入管理员新密码。
string2	字符串类型。
new-repeat	必选项，重新输入管理员的新密码。
string3	字符串类型。

以下是修改当前管理员的密码的示例：

TopsecOS# **password old-password** *talent* **new-password** *topsec123* **new-repeat** *topsec123*

4.1.6 SNMP

SNMP（Simple Network Management Protocol，简单网络管理协议），是 TCP/IP 网络基于 UDP 协议的网络管理标准协议，用于网络管理员集中管理网络中的网络设备。其网络管理模型包括以下部件：SNMP 管理站、SNMP 代理、被管理设备、MIB，各部件的联系如下图所示。

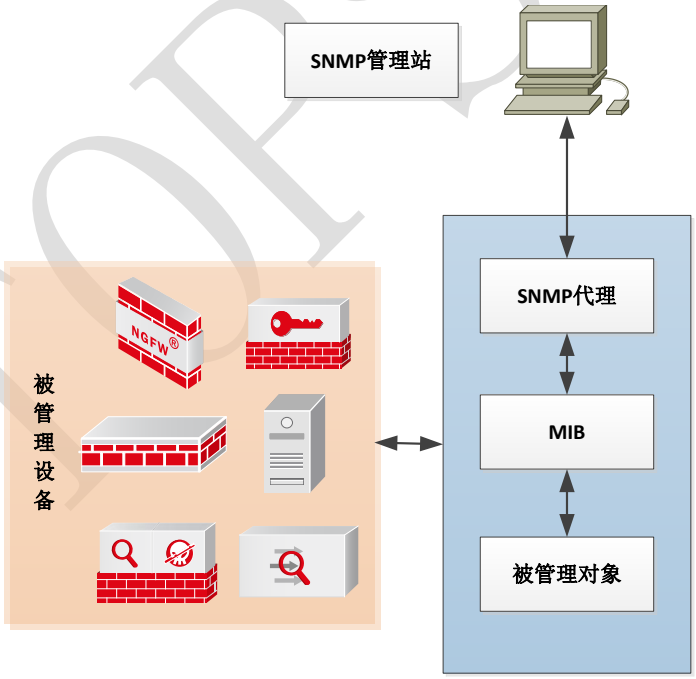


图 4-2 SNMP 网络管理模型

1）SNMP 管理站，是运行 SNMP 网络管理软件的独立设备（一般为 PC），作为网络管理员集中管理网络设备的接口。其基本构成包括：一组具有分析数据、发现故

障等功能的管理程序；一个用于监控网络的接口；一个从被管网络实体的 MIB 中抽取信息的数据库。管理站可以实现以下功能：

- 向网络设备发送“读”请求报文。
- 接收网络设备的响应报文、Trap 消息以及报警消息。

2）SNMP 代理，嵌入到网络设备中的功能模块，即指网络上设备支持的 SNMP 代理服务。通过在某网络设备上启动 SNMP 服务，网络管理员则可通过 SNMP 管理站远程获取网络设备的配置信息和实时信息。SNMP 代理可以实现以下功能：

- 接收来自 SNMP 管理站的请求报文。
- 响应来自 SNMP 管理站的“读”请求。
- 根据系统内部设定，主动地向 SNMP 管理端发送 TRAP 消息。

3）被管理设备，指运行 SNMP 代理服务的网络设备，如计算机、路由器、交换机、防火墙、VPN、IPS 等支持 SNMP 代理服务的网络设备。

4）MIB（Management Information Base，管理信息库），提供了标识网络设备所有可能被管理对象的集合，向管理站表明被管理设备的哪些部件可被管理。SNMP 管理站通过读取 MIB 中具体的对象来获取设备配置或运行状况进行网络监控，并可以通过修改 MIB 中对象的变量值改变 SNMP 代理处资源的配置。

网络设备中任何一个可被管理的对象都用 MIB 集合中的一个元素表示，为唯一标识设备中的可被管理对象，MIB 采用树形结构命名方案来标识网络对象。网络对象由 MIB 中从根开始的路径唯一识别，根据如下 MIB 结构图，interface 由{1.3.6.1.2.1.2}唯一表示。

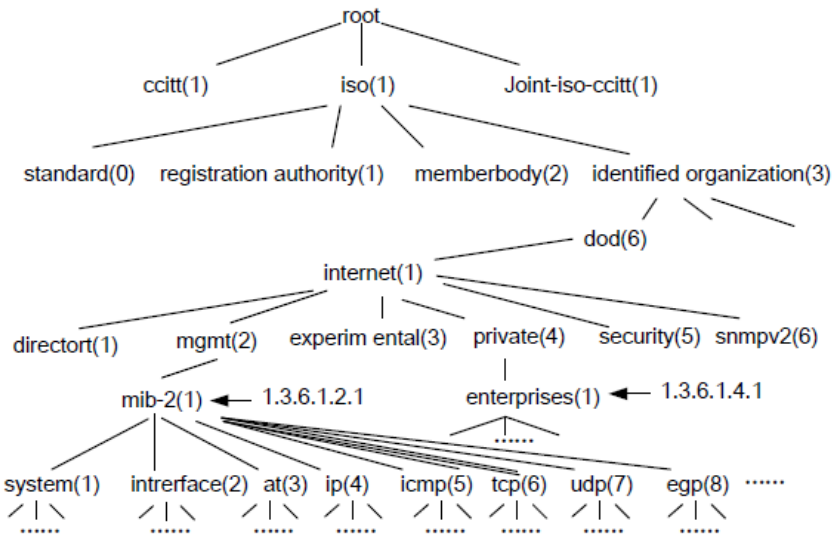


图 4-3 MIB 结构图

MIB 包括公有标准 MIB 库和厂商私有 MIB 库，天融信根据自身产品的特点自定义了 TOPSEC MIB 库，方便网络管理员获取天融信产品各功能模块的“读”权限。

NGFW 内嵌 SNMP 代理服务功能模块，兼容 SNMPv1、SNMPv2 以及 SNMPv3，支持主流的 SNMP 管理软件（如 PRTG Network Monitor、SolarWinds、HP 的 Open View 等等）对其进行管理，也可以响应 SNMP 管理站的查询请求，并可主动向 SNMP 陷阱主机发送 TRAP 消息及报警信息，其可实现功能如下图所示。

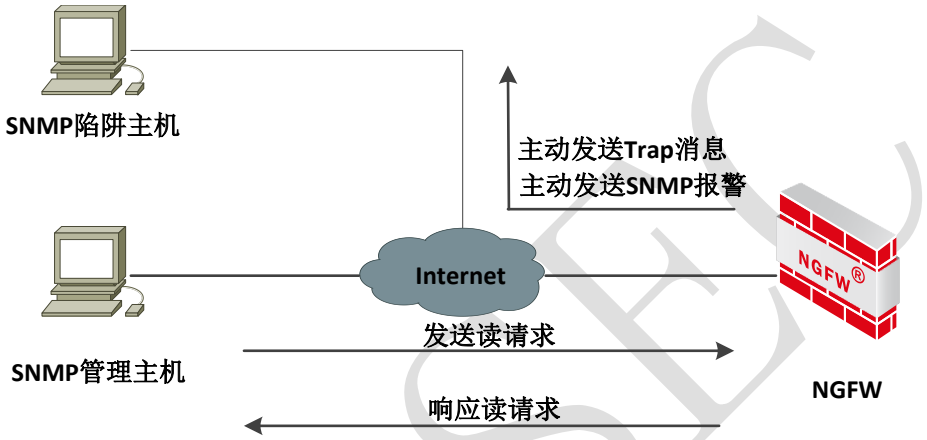


图 4-4 NGFW 的 SNMP 功能示意图

网络管理员要通过 SNMP 管理软件管理 NGFW，以及能接收 NGFW 能主动发送其 Trap 消息及报警信息，需要进行如下设置：

WEBUI 方式配置

步骤 1 配置管理主机/陷阱主机。

1）在管理主机/陷阱主机上安装 SNMP 管理软件（比如 PRTG Network Monitor、SolarWinds、HP OPENVIEW 软件）。

2）导入公有 MIB 库或 TOPSEC MIB 库（可从随机光盘中获得）并做简单配置，关于 SNMP 管理软件的安装及相关配置具体请参考相关管理软件的使用手册。

步骤 2 配置 NGFW。

1）对 SNMP 管理区域的管理/陷阱主机开放 SNMP 服务。

2）添加管理主机对象。

3）添加陷阱主机对象。

4）可选。如果采用 SNMPV3 版本，需添加 SNMP V3 用户。

5）启动 SNMP 服务。

4.1.6.1 SNMP 服务控制

NGFW 上必须启动 SNMP 服务才能支持 SNMP 管理主机管理以及向 SNMP 陷阱主机主动发送 Trap 消息。下面介绍 NGFW 如何启动 SNMP 服务。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **SNMP**，“SNMP 服务控制”界面如下图所示。

步骤 2 设置参数。

在配置 SNMP 服务控制的参数时，各项参数的具体说明如下表所示。

参数	说明
位置	记录设备在网络环境中的位置。设备出现故障问题时，方便管理员快速定位设备存放地点，默认显示天融信公司官方网站地址。
联系	记录设备直接责任人的联系方式，可以为电话号码或 Email 地址。通过配置此参数，将重要信息存储在 NGFW 中，以便出现紧急问题时查询使用。默认显示天融信公司客服的邮件地址。

说明

✧ 修改参数的配置后，管理员必须重新启动 SNMP 服务才能使参数生效。

步骤 3 点击【应用】按钮保存参数修改。如果没有修改默认参数，略去此步骤。

步骤 4 点击【启动】按钮，启动 SNMP 服务；点击【停止】按钮，则停止 SNMP 服务。

CLI 方式配置

system snmp set location <*string*>

命令描述：

设置启用了 SNMP 服务的 NGFW 在网络环境中的位置。

参数说明：

snmp set location	必选项，设置 NGFW 在网络中的位置。
string	字符串类型。

以下为设置 NGFW 提供 SNMP 服务时其位置的示例：

设置 NGFW 位置为 www.topsec.com.cn。

TopsecOS# **system snmp set location** *www.topsec.com.cn*

system snmp set contact <*string*>

命令描述：

设置 NGFW 设备直接责任人的联系方式。

参数说明：

snmp set contact	必选项，设置 NGFW 启用了 SNMP 服务后，管理这个设备的联系人信息。
string	字符串类型。可为电话号码、邮箱地址等信息。

以下为设置 NGFW 设备负责人信息的示例：

设置 NGFW 设备负责人信息为 support@topsec.com.cn。

TopsecOS# **system snmp set contact** *support@topsec.com.cn*

system snmp start <cr>

命令描述：

启动 NGFW 的 SNMP 服务，启动 SNMP 服务后，将不能配置管理主机、陷阱主机以及 SNMPV3 用户。

以下为启动 NGFW 的 SNMP 服务的示例：

TopsecOS# **system snmp start**

system snmp stop <cr>

命令描述：

停止 NGFW 的 SNMP 服务。

以下为停止 NGFW 的 SNMP 服务的示例：

```
TopsecOS# system snmp stop
```

system snmp show <config|status>

命令描述：

查看 SNMP 配置和运行状态信息。

参数说明：

system snmp show	查看 SNMP 配置和运行状态信息。
config|status	配置信息|状态信息

以下为查看 SNMP 服务状态信息的示例：

```
TopsecOS# system snmp show status
snmpd is not running!
```

4.1.6.2 SNMP 管理主机

SNMP 采用 C/S 架构，管理站使用知名端口号 162 接收 Trap 消息及报警消息，客户端使用知名端口号 161 接收查询设备信息。网络管理员通过 SNMP 管理主机管理 NGFW 的原理图如下。

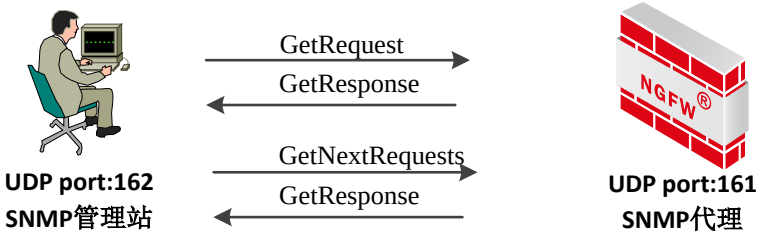


图 4-5 SNMP 管理主机管理网络设备示意图

网络管理员通过管理主机查询 NGFW 的操作命令说明如下：

- GetRequest：管理站向网络设备某功能节点发起“读”请求，获取设备某功能节点的配置信息或实时状态信息。
- GetNextRequests：管理站向网络设备某功能节点发起“读”请求，在 GetRequest 的基础上获取其相邻另一个功能节点的配置信息或实时状态信息。
- GetBulk：管理站向网络设备发起“读”请求，相当于连读多次执行 GetNextRequests 操作，方便管理员批量查询网络设备信息，提示管理效率。
- GetResponse：网络设备响应管理站发起的 GetRequest、GetNextRequests、GetBulk 操作。

管理主机安装 SNMP 管理软件并导入了公有 MIB 库或 TOPSEC MIB 库后，还需要在 NGFW 上添加管理主机信息。下面介绍如何在 NGFW 上添加 SNMP 管理主机。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤 2 激活“SNMP 管理主机”页签，点击『添加』，如下图所示。

在添加 SNMP 管理主机时，各项参数的具体说明如下表所示。

参数	说明
主机名称	必选项，添加该管理主机的名称。
本地地址	设置管理主机的类型，可选项：主机和子网。 “主机”指设定 SNMP Manager 为一台主机；“子网”指设定 SNMP Manager 为一个子网，该子网内的主机都可以配置为 SNMP 管理主机。 说明：

参数	说明
	1）当管理主机只有一个时，添加“主机”类型的管理主机对象； 2）当管理主机具有多个且正好位于一个子网时，可以添加多个“主机”类型的管理主机对象，也可以添加一个“子网”类型的管理主机对象。
子网 IP	管理主机类型选择“主机”时，用于指定 SNMP 管理主机对象的 IP 地址；管理主机类型选择“子网”时，用于指定 SNMP 管理子网对象的子网地址及其掩码。
Community	必选项，指定 SNMP 管理主机访问 NGFW 时的团体名。 说明： SNMPv1 和 SNMPv2c 的管理主机与设备使用团体名认证，管理主机端配置的团体名必须此处设置的团体名一致，否则，网络管理员不能通过管理主机管理该 NGFW。

步骤 3 点击【确定】按钮完成管理主机对象的添加。

CLI 方式配置

system snmp managehost add name <*string1*> **hostip** <*ipaddress*> **community** <*string2*>

命令描述：

增加 SNMP 管理主机对象。

参数说明：

system snmp managehost add	增加 SNMP 管理主机对象。
name	必选项，指定 SNMP 管理主机对象的名称。
string1	字符串类型，表示 SNMP 管理主机对象的名称。
hostip	必选项，指定 SNMP 管理主机对象的 IP 地址。
ipaddress	IP 地址字符串，格式为 A.B.C.D。
community	必选项，指定 SNMP 管理主机访问 NGFW 时的团体名。 说明： SNMP V1/V2 支持团体名认证方案，与 NGFW 认可的团体名不符的 SNMP 报文将被丢弃。
string2	字符串类型，表示团体名。

以下为新增 SNMP 管理主机的示例：

新增一个名称为 abc，IP 地址为 192.168.10.11，团体名为 public 的 SNMP 管理主机。

TopsecOS# **system snmp managehost add name** *abc* **hostip** *192.168.10.11* **community** *public*

system snmp managehost delete name <*string*>

命令描述：

删除 SNMP 管理主机。

参数说明：

system snmp managehost delete	删除 SNMP 管理主机。
name	必选项，指定待删除 SNMP 管理主机对象的名称。
string	字符串类型，表示 SNMP 管理主机对象的名称。

以下为删除 SNMP 管理主机的示例：

删除名称为“manage_host1”的 SNMP 管理主机对象。

```
TopsecOS# system snmp managehost delete name manage_host1
```

system snmp managehost show <cr>

命令描述：

显示所有的 SNMP 管理主机对象。

以下为显示所有 SNMP 管理主机的示例：

```
TopsecOS# system snmp managehost show
```

system snmp managehost clean <cr>

命令描述：

清空所有的 SNMP 管理主机对象。

以下为清空所有 SNMP 管理主机的示例：

```
TopsecOS# system snmp managehost clean
```

system snmp managesubnet add name <*string1*> **subnet** <*string2*> **community** <*string3*>

命令描述：

增加 SNMP 管理子网对象。

参数说明：

system snmp managesubnet add	增加 SNMP 管理子网对象。
name	必选项，指定 SNMP 管理子网对象的名称。
string1	字符串类型，表示新增 SNMP 管理子网对象的名称。
subnet	必选项，指定 SNMP 管理子网对象的地址。
string2	设定子网地址及子网掩码，格式为 A.B.C.D/E。
community	必选项，指定 SNMP 管理子网访问 NGFW 时的团体名。 说明： SNMP V1/V2 支持团体名认证方案，与 NGFW 认可的团体名不符的 SNMP 报文将被丢弃。
string3	字符串类型，表示团体名。

以下为新增 SNMP 管理子网的示例：

增加一个名称为 manage_subnet1，子网地址为 192.168.83.0，子网掩码为 255.255.255.0，团体名为“community2”的 SNMP 管理子网对象。

```
TopsecOS# system snmp managehost add name manage_subnet1 subnet
192.168.83.0/24 community community2
```

system snmp managesubnet delete name <*string*>

命令描述：

删除 SNMP 管理子网对象。

参数说明：

system snmp managesubnet delete	删除 SNMP 管理子网对象。
name	必选项，指定 SNMP 管理子网对象的名称。
string	字符串类型，输入要删除的 SNMP 管理子网对象的名称。

以下为删除 SNMP 管理子网对象的示例：

删除名称为“manage_subnet1”的 SNMP 管理子网对象。

```
TopsecOS# system snmp managesubnet delete name manage_subnet1
```

system snmp managesubnet show <cr>

命令描述：

显示所有的 SNMP 管理子网对象。

以下为显示所有 SNMP 管理子网对象的示例：

```
TopsecOS#system    snmp managesubnet show
```

system snmp managesubnet clean <cr>

命令描述：

清空所有的 SNMP 管理子网对象。

以下为清空所有 SNMP 管理子网对象的示例：

```
TopsecOS# system snmp managesubnet clean
```

4.1.6.3 SNMP 陷阱主机

陷阱主机是指接收 NGFW 发出 SNMP Trap 消息或 SNMP 报警消息的主机，但根据其使用的 SNMP 版本不同，可接收的消息类型有所不同，SNMPv1 和 SNMPv3 的陷阱主机只支持接收 Trap 消息，只有 SNMPv2c 的陷阱主机可同时接收 Trap 消息和 SNMP 报警消息。NGFW 主动向陷阱主机发送 Trap 消息及报警消息如下所示。

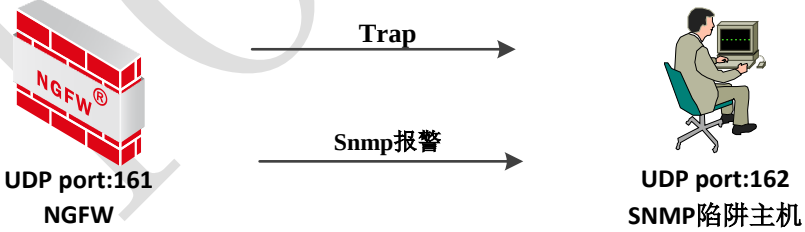


图 4-6 NGFW 向陷阱主机主动发送 Trap 或报警信息示意图

- Trap 消息：NGFW 主动发送给陷阱主机表明系统出现异常的信息，以提醒网络管理员设备已出现异常。NGFW 已经预定义了 TRAP 事件，关于 TRAP 事件的设置具体请参见 4.6 告警。

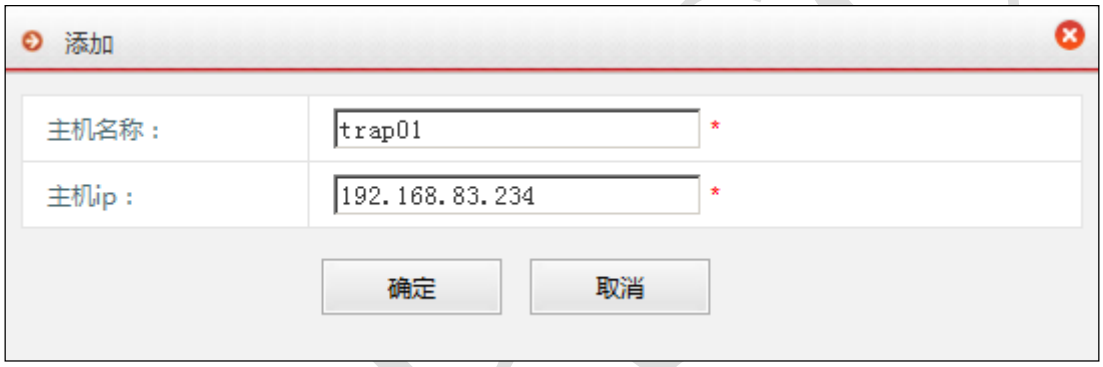
- 报警消息：通过设备的流量触发报警规则时，NGFW 自动以 SNMP 报警方式向陷阱主机发送报警信息。关于报警规则及报警方式的配置具体请参加 4.6 告警。

陷阱主机安装 SNMP 管理软件并导入了公有 MIB 库或 TOPSEC MIB 库后，还需要在 NGFW 上添加陷阱主机信息，网络管理员才可接收 NGFW 主动发送的 Trap 消息及 SNMP 报警消息，下面介绍如何在 NGFW 上添加陷阱主机。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤 2 激活“SNMP 陷阱主机”页签，点击『添加』，如下图所示。



步骤 3 配置陷阱主机的名称和 IP 地址。

步骤 4 点击【确定】按钮完成陷阱主机对象的添加。

CLI 方式配置

system snmp traphost add name <*string*> **hostip** <*ipaddress*>

命令描述：

增加 SNMP 陷阱主机对象。

参数说明：

system snmp traphost add	增加陷阱主机对象。
name	必选项，指定陷阱主机对象的名称。
string	字符串类型，表示要增加的陷阱主机对象的名称。
hostip	必选项，指定陷阱主机的 IP 地址。
ipaddress	IP 地址字符串，格式为 A.B.C.D。

以下为新增 SNMP 陷阱主机对象的示例：

增加一个陷阱主机对象，名称为“trap_host1”，陷阱主机的 IP 地址为“192.168.83.223”。

```
TopsecOS# system snmp traphost add name trap_host1 hostip 192.168.83.223
```

system snmp traphost delete name <*string*>

命令描述：

删除陷阱主机对象。

参数说明：

snmp traphost delete	删除陷阱主机对象。
name	必选项，指定陷阱主机对象的名称。
string	字符串类型，表示要删除的陷阱主机对象的名称。

以下为删除 SNMP 陷阱主机对象的示例：

删除名称为“trap_host1”的陷阱主机对象。

```
TopsecOS# system snmp traphost delete name trap_host1
```

system snmp traphost show <cr>

命令描述：

显示所有的陷阱主机对象。

以下为显示所有 SNMP 陷阱主机的示例：

```
TopsecOS# system snmp traphost show
Name                    Host
trap_host1              192.168.83.223
```

system snmp traphost clean <cr>

命令描述：

清空所有的陷阱主机对象。

以下为清空所有 SNMP 陷阱主机的示例：

TopsecOS# **system snmp traphost clean**

4.1.6.4 SNMPV3 用户

NGFW 支持 SNMP V3 版本，同时兼容 V1 和 V2 版本。网络管理员使用 SNMP V1、SNMP V2 对 NGFW 进行查询或配置时，只需在管理主机设置时设置“community”即可，但存在的最大问题是传输的认证和管理数据没有加密、数据的收发缺乏鉴别机制，因此对网络的管理缺乏安全保障。

SNMP V3 版本引入了三个安全级别：1）不需要认证，不提供机密性；2）基于 HMAC-MD5 或 HMAC-SHA 认证，不提供加密；3）不仅提供认证，还提供 CBC-DES 加密算法的加密机制。网络管理员使用 SNMP V3 对 NGFW 设备进行查询或配置时，不仅可将传送的报文使用 DES 算法进行加密，NGFW 还通过 SNMPV3 用户的密钥验证网络管理员身份的合法性，因此，进一步提高了对 NGFW 设备被 SNMP 管理软件管理的安全性。下面介绍如何配置 SNMPv3 用户。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **SNMP**。

步骤 2 激活“SNMPV3 用户”页签，点击『添加』，如下图所示。

步骤 3 添加 SNMPV3 用户。

在添加 SNMPV3 用户时，各项参数的具体说明如下表所示。

参数	说明
用户名称	必选项，设置网络管理员通过 SNMP 网管软件访问 NGFW 所使用的用户名。
安全级别	设置是否对 SNMP 认证和管理信息进行加密。可选项：加密，不加密。 说明： 1）当设置加密时，同时使用加密和认证技术，先对数据进行加密，然后进行认证技术的消息摘要计算。 2）设置不加密时，只使用认证技术。
认证密码	必选项，指定管理站通过 SNMPV3 用户账号向 NGFW 进行身份认证时使用的认证密码。必须为 8 位字符。 说明： 1）NGFW 支持的 SNMP 认证算法为 MD5。 2）SNMP 认证，可保证只有拥有设备访问权限的用户才可访问该设备。
私有密码	安全级别选择“加密”时，该参数为必选参数。指定消息加密时使用的密码。必须为 8 位字符。 说明： 1）NGFW 支持的 SNMP 加密算法为 DES。 2）SNMP 加密，使管理主机与被管理设备间的数据以密文方式传输，避免数据被非法用户窃取。

步骤 4 点击【确定】按钮完成 SNMPv3 用户的创建。

CLI 方式配置

system snmp snmpv3user add name <*string1*> **authpass** <*string2*> **securitylevel** <authnopriv|authpriv> [**privpass** <*string3*>]

命令描述：

增加 SNMPV3 用户对象。

参数说明：

system snmp snmpv3user add	增加 SNMPV3 用户对象。
name	必选项，指定 SNMPV3 用户对象的名称。
string1	字符串类型，表示新增 SNMPV3 用户对象的名称。
authpass	必选项，指定 SNMPV3 用户对象进行认证时使用的密码，加密方式为 MD5。 说明： 必须为 8 位字符。
string2	字符串类型，表示 SNMPV3 用户对象的认证密码。
securitylevel	必选项，设置安全级别。
authnopriv|authpriv	不加密|加密
privpass	可选项，在安全级别为加密时，该参数有效。私有密

	码，指定消息加密时使用的密码，加密方式为 DES。 说明： 必须为 8 位字符。
string3	字符串类型，表示消息加密使用的密码。

以下为新增 SNMPV3 用户的示例：

增加一个 SNMPV3 用户对象，其中该用户名称为 v3_user1，安全级别为加密，认证密码为 11111111，私有密码为 22222222。

TopsecOS# **system snmp snmpv3user add name** *v3_user1* **authpass** *11111111* **privpass** *22222222* **securitylevel** authpriv

system snmp snmpv3user delete name <*string*>

命令描述：

删除 SNMPV3 用户对象。

参数说明：

system snmp snmpv3user delete	删除 SNMPV3 用户对象。
name	必选项，指定 SNMPV3 用户对象的名称。
string	字符串类型，表示要删除的 SNMPV3 用户对象的名称。

以下为删除 SNMPV3 用户的示例：

删除名称为“v3_user1”的 SNMPV3 用户对象。

TopsecOS# **system snmp snmpv3user delete name** *v3_user1*

system snmp snmpv3user show <cr>

命令描述：

显示所有的 SNMPV3 用户对象。

以下为显示所有 SNMPV3 用户的示例：

TopsecOS# **system snmp snmpv3user show**

system snmp snmpv3user clean <cr>

命令描述：

清空所有的 SNMPV3 用户对象。

以下为清空 SNMPV3 用户的示例：

```
TopsecOS# system snmp snmpv3user clean
```

4.1.7 本地域名解析

TCP/IP 协议使用 IP 地址实现网络的连接和通信，而 IP 地址由点分十进制组成，对用户而言，记住众多网络主机对应的 IP 地址难度非常大。针对此问题，专门设计了域名（一种字符串形式的主机命名机制）以及 DNS（Domain Name System，域名系统），其中，DNS 提供域名与 IP 地址间的查询机制，自动实现域名地址与 IP 地址的映射，用户只需知道某网络服务的域名而无需知道其 IP 地址即可访问该网络服务。

为在 Internet 中通过域名唯一标识某台主机，并为网络服务指定一个有意义的名字，方便用户记忆，域名采用树形结构的命名方案。每个申请 Internet 域名的国家都需向 NIC（Network Information Center，网络信息中心）注册一个顶级域名，NIC 将顶级域名的管理权分配给指定的管理机构，这些管理机构再对其被授权管理的域继续进行划分，以此下去，便形成层次结构的域名体系，域名树形结构如下图所示。

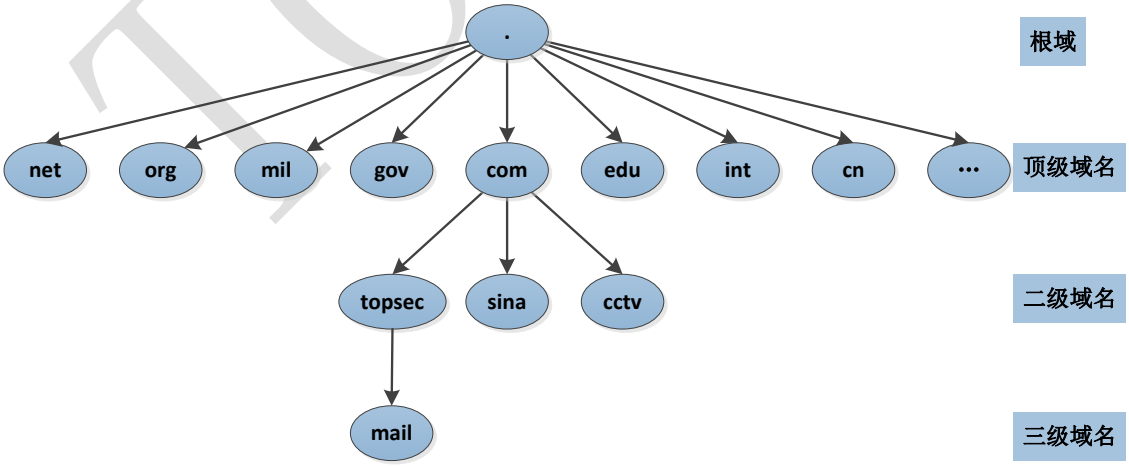


图 4-7 域名层次结构图

域名级别包括根域、顶级域名、二级域名、三级域名等等，不同级别的域名用点号分隔，级别最低的域名写在最左边，级别最高的域名则写在最右边。域名体系的层次结构说明如下：

域名级别	说明
根域	根域用点号（.）表示，以点号结尾的域名为完全合格域名。
顶级域名	包括国际顶级域名和国内顶级域名。 举例： 1）cn：供中国使用；us：供美国使用；jp：供日本使用。 2）net：供网络提供商使用；com：供商业组织使用；edu：供教育机构使用；gov：供政府机构使用；org：供非商业非盈利单位使用；mil：供军事机构使用。
二级域名	顶级域名之下的域名。由字母、数字和连接符（-）组成，各级域名之间用实点（.）连接。
……	……

DNS 域名系统采用 C/S 架构，传输层协议为 TCP 或 UDP，服务器端口号 53，DNS 服务器负责域名解析，DNS 客户端提出查询请求。NGFW 可作为 DNS Client，当其通过域名访问网络资源时，通过向 DNS 服务器发送域名解析请求，获取域名对应的 IP 地址，进而通过 IP 地址访问具体的网络服务。NGFW 访问 www.topsec.com.cn.时，DNS 域名解析完整过程如下图：

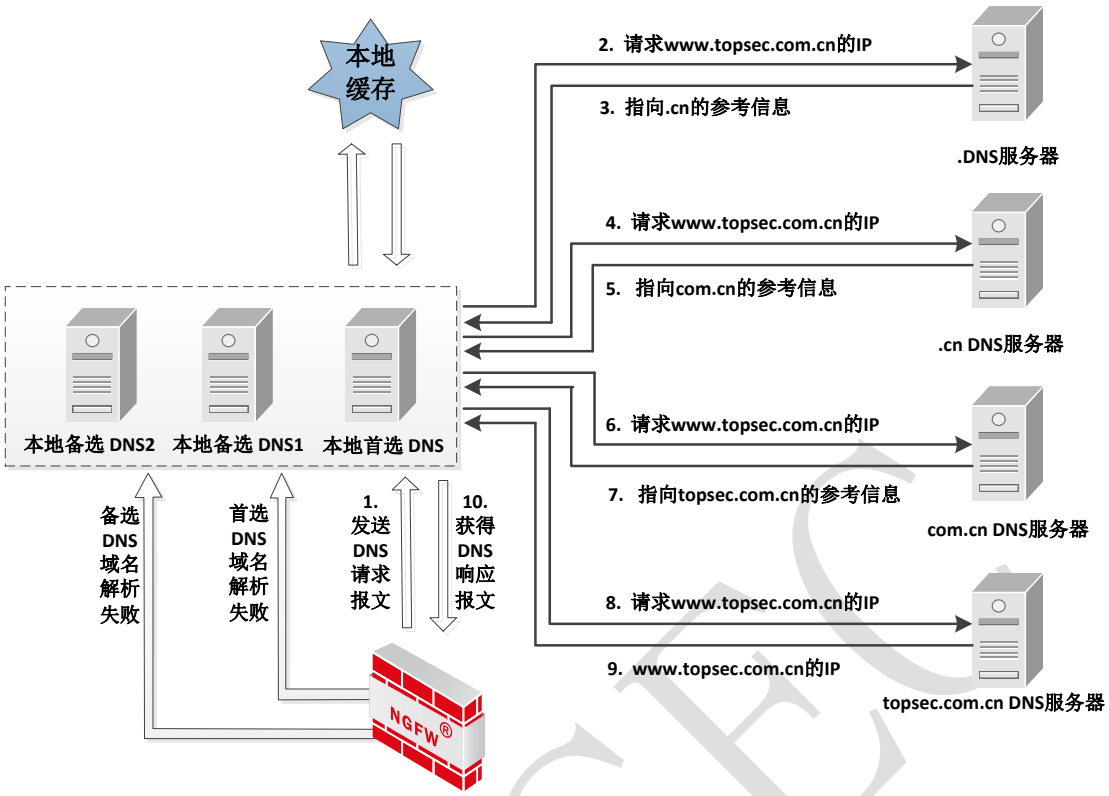


图 4-8 域名解析原理图

NGFW 首先向本地首选 DNS 服务器发起域名解析请求，如果本地首选 DNS 服务器进行域名解析失败，则向本地备选 DNS 服务器发起域名解析请求。

本地 DNS 服务器接收域名请求后的处理流程如下：

1）本地 DNS 服务器进行域名解析时，首先查询其缓存表，如果查找到域名对应的 IP 地址，本地 DNS 服务器向 NGFW 返回该域名对应的 IP 地址；否则，向根域服务器发起请求报文。

2）根域服务器查询其映射表项，然后向本地 DNS 服务器返回指向.cn 服务器的 IP 地址；本地 DNS 服务器获取.cn 服务器 IP 地址后，向.cn 服务器发起域名请求。

3）流程同 3）逐级查询，直到查询到最后一个域名服务器 topsec.com.cn，最后一个域名服务器将域名 www.topsec.com.cn 对应的 IP 返回给本地 DNS 服务器。

4）本地 DNS 服务器接收到.topsec.com.cn 服务器解析成功的响应报文，将域名与 IP 地址的映射关系缓存至本地，并将域名解析结果发送给 NGFW。

下面介绍 NGFW 作为 DNS 客户端时，如何配置其本地 DNS 服务器。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **域名解析**，如下图所示。

步骤 2 配置 DNS 服务器。在“首选 DNS 服务器”文本框中输入优先级最高的 DNS 服务器的 IP 地址；如果有备用的 DNS 服务器，则在“备选 DNS1”/“备选 DNS2”文本框中输入其 IP 地址。

步骤 3 点击【应用】按钮完成 DNS 服务器的配置；点击【重置】按钮则恢复系统出厂配置。

说明

✧ NGFW 支持 IPv4 和 IPv6 域名服务器。

CLI 方式配置

network dns set dns1 <*ipaddress1*> [**dns2** <*ipaddress2*>] [**dns3** <*ipaddress3*>]

命令描述：

设置域名服务器的地址，最多可设三个 DNS 服务器。

参数说明：

network dns set	设置域名服务器的地址。
dns1	必选项，设置主域名服务器的地址。
ipaddress1	IP 地址字符串，设置 IPv4 域名服务器，格式：A.B.C.D； 设置 IPv6 域名服务器，格式：x:x:x:x:x:x:x:x。
dns2	可选项，设置第二域名服务器的地址。
ipaddress2	IP 地址字符串，设置 IPv4 域名服务器，格式：A.B.C.D； 设置 IPv6 域名服务器，格式：x:x:x:x:x:x:x:x。
dns3	可选项，设置第三域名服务器的地址。
ipaddress3	IP 地址字符串，设置 IPv4 域名服务器，格式：A.B.C.D； 设置 IPv6 域名服务器，格式：x:x:x:x:x:x:x:x。

使用说明：

DNS 服务器设置多个时，当主 DNS 服务器失效时，采用第二域名服务器，当前两个域名服务器均失效时采用第三域名服务器。

network dns reset <cr>

命令描述：

重启 DNS 客户端服务。

network dns show <cr>

命令描述：

查看域名服务器的设置。

以下是查看 DNS 服务器的示例：

```
TopsecOS# network dns show
network dns set dns1 114.114.114.114 dns2 8.8.8.8
```

4.1.8 本地服务设置

本地服务就是管理员对设备的访问权限控制，NGFW 支持通过 WEBUI、Telnet、SSH 方式进行远程访问。

通过本地服务模块，管理员可设置允许访问 NGFW 的方式，提高设备的安全性。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统设置** > **本地服务设置**。

步骤 2 设置 NGFW 允许的登录方式。

在设置本地服务时，各项参数的具体说明如下表所示。

参数	说明
sshd 服务	设置是否允许通过 SSH 方式远程访问 NGFW。可选项：开启和关闭。
telnet 服务	设置是否允许通过 Telnet 方式远程访问 NGFW。可选项：开启和关闭。
httpd 服务	设置是否允许通过 WEBUI 方式远程访问 NGFW。可选项：开启和关闭。

步骤 3 配置完成后，点击【应用】按钮，完成本地服务设置。

步骤 4 （可选）点击【重置】按钮，可以恢复本地服务的设置为出厂配置，此时将关闭通过 WEBUI、Telnet、SSH 方式进行远程访问 NGFW。

CLI 方式配置

system service sshd <on|off>

命令描述：

设置是否允许通过 SSH 方式远程访问 NGFW。

参数说明：

system service sshd	设置是否允许通过 SSH 方式远程访问 NGFW。
on|off	开启|关闭

以下设置通过 SSH 方式远程访问 NGFW 的示例：

```
TopsecOS# system service sshd on
```

system service telnetd <on|off>

命令描述：

设置是否允许通过 Telnet 方式远程访问 NGFW。

参数说明：

system service telnetd	设置是否允许通过 Telnet 方式远程访问 NGFW。
on|off	开启|关闭

以下设置允许通过 Telnet 方式远程访问 NGFW 的示例：

```
TopsecOS# system service telnetd on
```

system service httpd <on|off>

命令描述：

设置是否允许通过 WEBUI 方式远程访问 NGFW。

参数说明：

system service httpd	设置是否允许通过 WEBUI 方式远程访问 NGFW。
on|off	开启|关闭

以下设置允许通过 WEBUI 方式远程访问 NGFW 的示例：

```
TopsecOS# system service httpd on
```

system service default <cr>

命令描述：

恢复本地服务的设置为出厂配置，此时将关闭通过 WEBUI、Telnet、SSH 方式进行远程访问 NGFW。

以下恢复本地服务的设置为出厂配置的示例：

```
TopsecOS# system service httpd default
```

4.2 系统维护

NGFW 为管理员提供了排除系统故障、优化系统性能的功能，包括：配置备份、配置替换、固件升级、获取健康记录、重启系统和规则库升级。

4.2.1 配置维护

NGFW 的配置信息保存在配置文件中，设备中可同时存在多个配置文件，但是只有一个生效。设备中存在以下配置信息。

- 出厂配置：设备在出厂时，带有基本功能的配置信息。配置文件损坏时，可使用出厂配置正常启动。
- 启动配置：设备在启动时，自动加载的配置文件，如果设备未找到启动配置文件加载出厂配置。
- 当前配置：设备当前正在运行的配置，包括设备的启动配置及管理员新增的配置信息。如果不保存当前配置，设备重启后，会丢失当前配置。

系统支持配置文件的备份、替换和删除等功能，可大大降低管理员批量配置设备的工作量。另外，管理员可通过导入不同配置文件实现设备在不同网络中的配置，自由切换 NGFW 在网络环境中的功能，并可在设备配置出现问题时帮助管理员轻松将配置恢复到正常状态。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统维护** > **配置维护**。

界面中状态栏中图标为“  ”，表示配置文件是系统当前的运行配置文件；“  ”表示该配置文件是存储到系统中的备份配置文件。

步骤 2 保存配置文件。

点击『保存』，在弹出的确认对话框中，点击【确定】按钮，即可将系统中的配置文件保存。

步骤 3 备份系统运行配置文件。

点击『另存为』，弹出“配置文件另存为”窗口。输入另存的配置文件文件名和描述信息，点击【确定】按钮即可将系统当前运行配置文件备份到设备中。

步骤 4 导出配置文件。

1）选择一个或多个系统中存储的配置文件，点击『导出』。如果选择了多个配置文件，NGFW 将多个配置文件打包导出。

2）在弹出的提示窗口，点击【确定】按钮，完成将系统中存储的配置文件导出至管理主机中。

步骤 5 导入配置文件。

1）点击『导入』，弹出“导入配置文件”窗口。

在导入配置文件时，各项参数的具体说明如下表所示。

参数	说明
文件	选择配置文件。点击【浏览】按钮，在管理主机中选择配置文件。
描述	输入配置文件的必要描述信息。
替换当前的系统配置	如果勾选“替换当前的系统配置”该项表示将该导入的配置文件作为系统的运行配置文件。

2）点击【确定】按钮完成配置文件的导入，点击【取消】按钮撤销本次操作。

步骤 6 替换配置文件。

选择一个备份的配置文件，点击其状态栏中的“”，选择的配置将替换为系统当前运行配置文件，配置文件的状态图标转变为“”，表示替换完成。

步骤 7 删除备份配置文件。

选择备份的配置文件，点击『删除』，在弹出的提示窗口中，点击【确定】按钮，完成备份配置文件的删除。

注意

- 配置文件显示为“”时，不可进行删除操作。

步骤 8 恢复设备出厂配置。

点击『恢复默认』，在弹出的提示窗口中，点击【确定】按钮，恢复出厂设置。

CLI 方式配置

步骤	配置命令	配置说明
1	**system config_file save_as** <*string1*> **comment** <*string2*>	保存系统配置文件。
2	**system config_file load** <*string*>	下载系统配置文件。
3	**system config_file delete** < *string* >	删除系统配置文件。
4	**system config reset**	恢复系统出厂配置。
5	**system config_file show** <cr>	查看系统配置文件

system config reset <cr>

命令描述：

恢复设备的配置文件为出厂设置。

使用说明：

恢复出厂设置会删除设备的配置信息，在恢复出厂设置前，请先导出必要的配置信息。

恢复出厂设置会造成网络中断，请谨慎操作。

system config_file delete < *string* >

命令描述：

删除未被使用的系统配置维护文件。

使用说明：

删除系统配置维护文件时，如果文件前显示为“*”，表示该文件当前正在被使用，如果文件前显示为“-”，表示该文件当前没有被使用。

以下是删除未被使用的系统配置维护文件的示例：

```
TopsecOS# system config_file show
FLAG  FILE_NAME  SIZE  ADMIN_NAME  VERSION  SAVE_TIME
COMMENT
-  config  20010  superman  v3.1130.1235.1_ngfw  2014-10-22
07:05:45  default config
```

```
-       1234            19117    superman    v3.1130.1202.1_ngfw    2014-09-15
02:38:14      copy
*       20151022        24701    superman    v3.1130.1235.1_ngfw    2014-11-03
07:02:02      1212 备份
TopsecOS# system config_file delete file2
delete config success!!

TopsecOS# system config_file show
FLAG   FILE_NAME   SIZE   ADMIN_NAME   VERSION     SAVE_TIME
COMMENT
-       config          20010    superman    v3.1130.1235.1_ngfw    2014-10-22
07:05:45      default config
*       20151022        24701    superman    v3.1130.1235.1_ngfw    2014-11-03
07:02:02      1212 备份
```

system config_file load <*string*>

命令描述：

下载系统配置维护文件。

参数说明：

system config_file load	必选项。下载系统配置维护文件。
string	字符串类型，系统配置维护文件的名称。

以下是下载系统配置维护文件的示例：

```
TopsecOS # system config_file load file1
load config success!!
```

system config_file save_as <*string1*> [**comment** <*string2*>]

命令描述：

保存系统配置维护文件。

参数说明：

system config_file save_as	必选项。保存系统配置维护文件。
string1	字符串类型，系统配置维护文件的名称。
comment	可选项。设置对该系统配置维护文件的说明。
string2	字符串类型，相关的说明信息。

以下是保存系统配置维护文件的示例：

```
TopsecOS # system config_file save_as file1 comment firstfile
config save as success!
```

system config_file show <cr>

命令描述：

显示系统配置文件。其中“*”表示当前正在使用的配置文件，“-”表示存储在设备中的备份配置文件。

以下是显示系统配置文件的示例：

```
TopsecOS # system config_file show
FLAG    FILE_NAME    SIZE    ADMIN_NAME      VERSION
 SAVE_TIME        COMMENT
*          config          18381     superman          v3.1130.1202.1_ngfw    2014-09-
15 00:27:18      default config
-          backup          19117     superman          v3.1130.1202.1_ngfw    2014-09-
15 02:38:14      copy
```

4.2.2 固件维护

NGFW 支持基于 TFTP 服务器、FTP 服务器和本地方式升级设备的系统软件，并支持将升级包备份到设备中，在设备需要升级时进行升级，可方便用户根据天融信发布的升级包及时对设备的性能和功能进行扩充。系统软件升级前将会首先检查升级包与设备的硬件平台是否匹配，如果不匹配，系统会提示管理员不能进行升级操作。

TFTP 和 FTP 服务器方式通过下载远程服务器的升级包进行升级，而本地方式则通过管理主机中的升级包进行升级，即采用本地方式升级前，需将升级包下载到管理主机中，下面分别予以详细介绍。

WEBUI 方式配置

在固件维护之前，需要先进行如下步骤：

- 建议用户在升级前先保存系统的配置。
- 通过本地进行升级时，请尽量退出串口登录。
- 通过 TFTP/FTP 进行升级时，在升级之前需要事先配置好 TFTP/FTP 服务器及其工作目录，并保证升级文件存放在工作目录中。
- 通过 TFTP/FTP 进行升级时，确保 TFTP/FTP 服务器和设备之间有路由可达。

步骤 1 选择 **系统管理** > **系统维护** > **固件维护**。

界面中状态栏中图标为“ ”，表示当前运行的系统软件；“ ”表示存储到系统中的备份系统软件。

步骤 2 升级系统软件。

- TFTP 升级方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“TFTP”。

采用 TFTP 方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项。输入存放升级包的 TFTP 服务器的 IP 地址。
文件名称	必选项。输入升级包的名称。
描述	输入简单的描述信息。
替换当前的系统固件	勾选“替换当前的系统固件”，NGFW 会升级固件；否则，NGFW 并不升级固件，只是将 TFTP 服务器中相应的升级包下载到设备中进行备份。

- FTP 服务器方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“FTP”。

采用 FTP 方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项。输入存放升级包的 FTP 服务器的 IP 地址。
文件名称	必选项。输入升级包的名称。

参数	说明
用户名	FTP 服务器不支持匿名登录时为必选项。输入 FTP 服务器的合法登录账号名称。
密码	FTP 服务器不支持匿名登录时为必选项。输入 FTP 服务器的合法登录账号名称对应的密码。
描述	输入简单的描述信息。
替换当前的系统固件	勾选“替换当前的系统固件”，NGFW 会升级固件；否则，NGFW 并不升级固件，只是将 FTP 服务器中相应的升级包下载到设备中进行备份。

➢ 本地方式

点击『导入』，弹出“导入”窗口，在“升级方式”下拉框中选择“本地”。

采用本地方式升级固件时，各项参数的具体说明如下表所示。

参数	说明
描述	输入简单的描述信息。
文件名称	点击【浏览】按钮，选择管理主机中存放的升级包，然后点击【确定】按钮导入升级包。
替换当前的系统固件	勾选“替换当前的系统固件”，NGFW 会升级固件；否则，NGFW 并不升级固件，只是将管理主机中相应的升级包下载到设备中进行备份。

步骤 3 升级方式设置完成后，点击【确定】按钮，完成升级包的导入或系统升级，点击【取消】按钮撤销本次操作。

说明

✧ 远程升级时，建议利用 FTP 或 TFTP 服务器进行升级，最好不要选择 WEBUI 方式升级。

✧ 升级系统软件需要一定的时间，升级过程中，请耐心等待，不要在界面中进行任何操作，否则升级可能中断。如系统长时间显示“正在升级，请稍等”对话框，则表明升级不成功，请点击【确定】按钮返回。升级不成功，请重点考虑和检查以下几方面的原因：

1）是否正确配置了 TFTP/FTP 服务器；

2）是否输入了正确的文件名称或选择了正确的升级包。

CLI 方式配置

步骤	配置命令	配置说明
1	**system firmware import filename** <*string1*> **get-method** ftp **serverip** <*ipaddress*> [**ftp-user** <*string2*>] [**ftp-password** <*string3*>] [**comments** <*string4*>]	使用 FTP 方式将升级包导入 NGFW 系统。

步骤	配置命令	配置说明
	system firmware import filename <*string1*> **get-method** tftp **serverip** <*ipaddress*> [**comments** <*string2*>]	使用 TFTP 方式将升级包导入 NGFW 系统。
2	**system firmware load filename** <*string*> [**sysdisk** <normal>]	加载系统文件。
3	**system firmware update filename** <*string1*> **get-method** ftp **serverip** <*ipaddress*> [**ftp-user** <*string2*>] [**ftp-password** <*string3*>] [**sysdisk** <normal>] [**comments** <*string4*>]	使用 FTP 方式升级系统文件。
	system firmware update filename <*string1*> **get-method** tftp **serverip** <*ipaddress*> [**comments** <*string2*>]	使用 TFTP 方式升级系统文件。
4	**system firmware delete filename** <*string*>	删除指定的未使用系统文件。
5	**system firmware clean** <cr>	清除所有未使用的升级文件。

system firmware clean <cr>

命令描述：

清空所有未使用的升级文件。

以下是清空所有未使用的升级文件的示例：

```
TopsecOS # system firmware clean
```

system firmware delete filename <*string*>

命令描述：

删除指定的未使用升级文件。

以下是显示删除未使用的升级文件的示例：

```
TopsecOS # system firmware delete filename ngfw-v1.0.23.2-default_upt
```

system firmware import filename <*string1*> **get-method** <ftp|tftp> [**ftp-user** <*string2*>] [**ftp-password** <*string3*>] **serverip** <*ipaddress*> [**comments** <*string4*>]

命令描述：

将升级包导入 NGFW 系统。该条命令用于非即时升级的情况。此时系统升级在执行该命令后，还需执行 **system firmware load** 加载命令。

参数说明：

system firmware import	将升级包导入 NGFW 系统。
filename	必选项。升级包文件名。
string1	字符串类型，升级包名称，字符串长度为 1-64 位。
get-method	必选项。选择对系统进行升级的方式。
ftp|tftp	通过 FTP 升级|通过 TFTP 升级
serverip	必选项。远端存放升级包的服务器 IPv4 地址。
ipaddress	IPv4 地址字符串，格式为 A.B.C.D。
ftp-user	可选项。FTP 服务器上的用户名。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
string2	字符串类型，用户名。
ftp-password	可选项。FTP 服务器上的用户密码，与 FTP 用户名对应。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
string3	字符串类型，与用户名对应的密码。
comments	可选项。对升级包的说明描述。
string4	字符串类型，字符串长度为 1-256 位。

以下是导入升级包的示例：

TopsecOS # **system firmware import filename** *ngfw-v1.0.23.2-default_upt*

getmethod *ftp* **serverip** *192.168.91.99* **ftp-user** *superman* **ftp-password** *123456*

comments *updatefile*

.....

Data pacakge become effective, The device must reboot.

system reboot.....

system firmware load filename <*string*> [**sysdisk** <normal>]

命令描述：

根据文件名加载 NGFW 设备上的升级包。

参数说明：

system firmware load	加载 NGFW 设备上的升级包。
filename	必选项。升级包文件名。
string1	字符串类型，升级包名称，字符串长度为 1-64 位。
sysdisk	可选项，设置升级的系统。
normal	主系统。

以下是根据文件名从 NGFW 设备上加载升级包的示例：

```
TopsecOS # system firmware load filename ngfw-v1.0.23.2-default_upt
```

system firmware show <cr>

命令描述：

显示升级包的信息。

以下是显示升级包信息的示例：

```
TopsecOS # system firmware show
```

system firmware update filename <*string1*> **get-method** <ftp|tftp> **serverip** <*ipaddress*> [**ftp-user** <*string2*>] [**ftp-password** <*string3*>] [**sysdisk** <normal>] [**comments** <*string4*>]

命令描述：

设置升级系统软件。该条命令用于即时升级系统的情况。此时系统升级只需执行该命令即可。

参数说明：

system firmware update	升级 NGFW 系统软件。
filename	必选项。升级包文件名。
string1	字符串类型，升级包名称，字符串长度：1-64。
get-method	必选项。选择对系统进行升级的方式。
ftp|tftp	通过 FTP 升级|通过 TFTP 升级
serverip	必选项。远端存放升级包的服务器 IPv4 地址。
ipaddress	IPv4 地址字符串，格式为 A.B.C.D。
ftp-user	可选项，FTP 服务器上的用户名。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
string2	字符串类型，用户名。
ftp-password	可选项，FTP 服务器上的用户密码，与 FTP 用户名对应。 说明： 当采用 FTP 方式升级时，该参数才需要填写。
string3	字符串类型，与用户名对应的密码。
sysdisk	必选项，选择升级的系统。
normal	主系统。
comments	可选项，对升级包的说明描述。
string4	字符串类型，字符串长度：1-256。

使用说明：

升级过程需要几分钟，请耐心等待。避免对 NGFW 平台进行任何操作。

以下是升级系统的示例：

TopsecOS # **system firmware update filename** *ngfw-v1.0.23.2-default_upt*

getmethod *tftp* **serverip** *192.168.1.4* **comments** *updatefile*

4.2.3 健康记录

管理员可以下载设备的健康记录，包括设备的配置信息，运行状态等信息，以便当设备出现异常时，可以帮助天融信的技术支持人员快速地定位并解决故障。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统维护** > **健康记录**。

步骤 2 点击【保存】按钮可将健康记录保存到管理主机。

说明

- ✧ 健康记录已加密，仅供调试人员使用。

4.2.4 系统重启

当系统升级、设备工作不正常或部分新配置需要生效时，需对系统进行重启，管理员可以远程重启系统。

注意

- ✧ 重启前应保存系统的配置信息，否则，重启后将丢失全部未保存的配置。
- ✧ 系统重启将会造成业务中断，请谨慎使用。
- ✧ 系统重启后，管理员需要重新登录。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统维护** > **系统重启**。

步骤 2 点击【重启系统】按钮，在弹出的对话框中，选择是否保存当前配置信息，点击【确定】按钮保存；点击【取消】按钮放弃保存。

步骤 3 在弹出的对话框中，点击【确定】按钮，即可重新启动 NGFW。

CLI 方式配置

步骤	配置命令	配置说明
1	**system reboot** <cr>	重启 NGFW 系统。

system reboot <cr>

命令描述：

重新启动 NGFW 设备。

以下为重新启动 NGFW 设备的示例：

```
TopsecOS# system reboot
Save system config?[y/n]:y
system config save.....
save config success.
```

```
Reboot system [y/n]:y
reboot.....
```

4.2.5 规则库升级

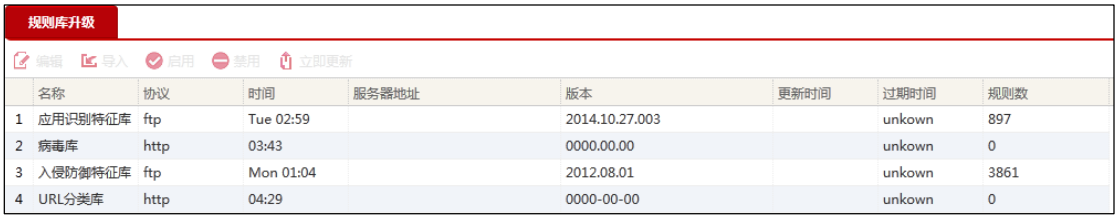
当前网络中入侵手段、病毒类型和应用类型的复杂多变，用户对设备的识别效率和识别能力的需求也在随之增强。为了使设备可以及时的识别新的应用，防御新的攻击和病毒，设备需要及时升级规则文件。

规则库升级功能可以升级规则库，可以提高设备对入侵行为、病毒和应用的识别能力和识别效率。升级规则文件有：自动升级、立即升级和本地升级 3 种方式。管理员可以根据需要选择合适的升级方式。

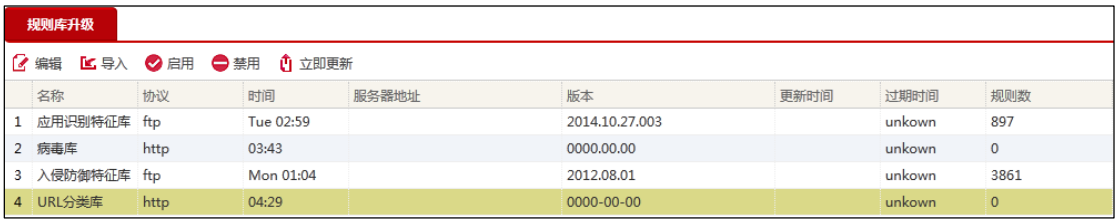
- 自动升级：自动升级指设备根据管理员设置的时间和目的地址，定期从目的地址处自动下载并更新规则库。
- 立即升级：当管理员发现网络上出现新的攻击方式、病毒或应用，升级中心已发布新的规则库，而此时未到设备的自动升级时间，可立即升级操作，及时升级规则库。立即升级方式与自动升级使用相同的规则库下载地址。
- 本地升级：当 NGFW 与 Internet 物理隔离，且没有部署升级服务器时，可以采用本地升级方式。升级前将需要升级的规则文件保存到管理主机，再通过 WebUI 登录到 NGFW 设备，进行选择规则文件进行升级。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统维护** > **规则库升级**。

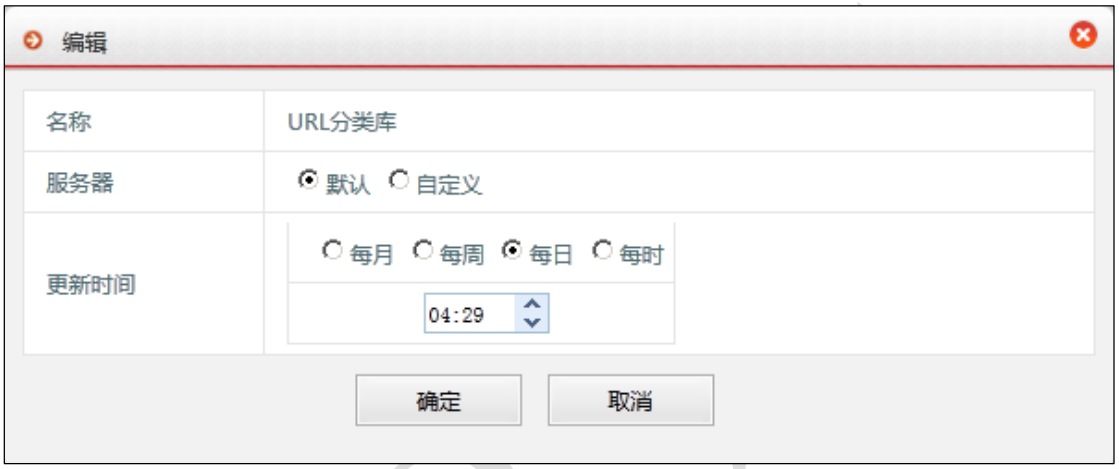


步骤 2 点击界面中需要更新规则类型所在行，此时操作菜单变为可编辑状态。



步骤 3 配置自动升级规则文件。

1）点击『编辑』，在弹出的“编辑”对话框中，配置自动更新策略。



在配置自动升级规则文件时，各项参数的具体说明如下表所示。

参数	说明
名称	显示自动更新规则名称。
服务器	设置规则文件升级的服务器类型。可选项：默认和自定义。 服务器设置为“默认”时，规则库升级如下： AI：服务器地址为 topsec.com.cn/ngfw-ai/，更新周期为“每周二”。 IPS：服务器地址为 ftp.topsec.com.cn，更新周期为“每周一”。 URL：服务器地址为 webfilter.topsec.com.cn，更新周期为“每天”。 AV：服务器地址为 avse.topsec.com.cn/fast-av，更新周期“每天”。
方式	设置服务器为自定义时，该项可配置。设置自动更新方式。可选项：HTTP 和 FTP。 HTTP：从指定的 URL 地址下载规则文件。 FTP：从指定的 FTP 服务器地址下载规则文件。
用户名	设置服务器为自定义且升级方式为 FTP 时需要配置该选项。输入 FTP 服务器的合法登录账号名称，字符类型，取值范围：1-63。
密码	设置服务器为自定义且升级方式为 FTP 时需要配置该选项。输入 FTP 服务器的合法登录账号名称对应的密码，字符类型，取值范围：1-63。

参数	说明
更新时间	配置自动更新的时间间隔。可选择的更新间隔有：每月、每周、每日和每时。并可通过更新间隔下方的参数详细配置更新时间。
服务器地址	设置服务器为自定义时，该项可配置。配置自动更新获取规则文件的服务器地址。 HTTP 方式升级时，服务器地址为字符串类型，最大长度为 63 个字符，支持多个升级服务器地址，可点击右侧『＋』输入多个地址，最多支持 5 个服务器地址。格式为：域名形式或点分十进制形式 X.X.X.X。 FTP 方式升级时字符串类型，最大长度为 63 个字符，支持多个服务器地址，可点击右侧『＋』输入多个地址，最多支持 5 个服务器地址。格式为：域名形式或点分十进制形式 X.X.X.X。

2）设置完成后，点击【确定】按钮，完成自动更新策略配置。

步骤 4 （可选）禁用自动升级规则。

配置完成自动升级规则后，该规则默认为启用，如果需要取消自动更新策略到规则文件，可点击『禁用』，此时界面对应的规则文件所在行显示为深灰色。可点击『启用』，重新开启自动升级规则功能。

步骤 5 配置立即升级规则文件。

1）设置自动更新策略。同步骤 3 中的操作。

2）点击『立即更新』，完成规则文件升级。

步骤 6 配置本地升级规则文件。

1）选择规则文件所在行，点击『导入』，弹出“规则文件导入”窗口。

在配置手动更新规则文件时，各项参数的具体说明如下表所示。

参数	说明
名称	显示规则文件名称。
文件名称	点击【浏览】按钮，选择管理主机上保存的规则文件。

2）配置完成后，点击【确定】按钮，完成规则文件升级。

CLI 方式配置

步骤	配置命令	配置说明
1	**system rules-update enable** <aise|av|ips |url>	开启规则文件自动升级功能。
2	**system rules-update disable** <aise|av|ips |url>	（可选）关闭规则文件自动升级功能。

步骤	配置命令	配置说明
3	**system rules-update modify-time** <aise|av|ips|url> **period-time** <*string1*>[**period-date** <*string2*>|**period-week** <*string3*>]	修改自动更新策略的时间。
4	**system rules-update modify-server** <aise|av|ips|url> **type ftp serverip** <*ipaddress*> [**ftpuser** <*string1*>] [**ftppass** <*string2*>]	修改 FTP 方式升级规则文件的服务器信息。
	system rules-update modify-server <aise|av|ips|url> **type http url** <*string*>	修改 HTTP 方式升级规则文件的服务器信息。
5	**system rules-update update** <aise|av|ips|url>	设置立即升级规则文件。
6	**system rules-update reset** <aise|av|ips|url>	恢复规则文件升级为出厂配置。
7	**system rules-update show** <cr>	查看升级规则文件的配置信息。
8	**system rules-update version** <cr>	查看规则文件的版本信息。

system rules-update enable <aise|av|ips|url>

命令描述：

开启规则文件自动升级功能。

可使用 **system rules-update disable** <aise|av|ips |url>命令关闭规则文件自动升级功能。

参数说明：

system rules-update enable	开启规则文件自动升级功能。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库

system rules-update modify-time <aise|av|ips|url> **period-time** <*string1*>[**period-date** <*string2*>|**period-week** <*string3*>]

命令描述：

修改规则文件自动更新策略的更新时间。

参数说明：

system rules-update modify-time	修改自动升规则文件的时间。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库
period-time	自动更新的时间间隔。以每日或者每小时时形式设置。
string1	设置每日或者每小时自动更新的时间。格式为“小时：分钟”或“分钟”，如 11:12 或 12
period-date	自动更新的时间间隔。以每月形式设置。

string2	设置每月自动更新的时间。格式为“月-日”或“日”，如 01-01 或者 01。
period-week	自动更新的时间间隔。以每周形式设置。
string3	设置每周自动更新的时间。数值类型，取值范围 0-6，表示星期日-星期六。

system rules-update modify-server <aise|av|ips|url> **type ftp serverip** <*ipaddress*> [**ftpuser** <*string1*>] [**ftppass** <*string2*>]

命令描述：

修改 FTP 方式升级规则文件的服务器信息。

参数说明：

system rules-update modify-server	修改升级规则文件的服务器信息。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库
type	自动升级方式。
ftp	从指定的 FTP 服务器地址下载规则文件。
serverip	FTP 服务器 IP 地址。
ipadress	IP 地址，格式为：域名形式或点分十进制形式 X.X.X.X。
ftpuser	FTP 服务器用户名。
string1	字符串类型，长度范围：1-63。
ftppass	FTP 服务器密码。
string2	字符串类型，长度范围：1-63。

system rules-update modify-server <aise|av|ips|url> **type http url** <*string*>

命令描述：

修改 HTTP 方式升级规则文件的服务器信息。

参数说明：

system rules-update modify-server	修改升级规则文件的服务器信息。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库
type	自动升级方式。
http	从指定的 URL 地址下载规则文件。
url	规则库服务器域名。
string	字符串类型，格式为：域名形式或点分十进制形式 X.X.X.X。

system rules-update reset <aise|av|ips|url>

命令描述：

恢复规则文件升级为出厂配置。规则文件的升级服务器地址及升级周期如下所示。

- AI：服务器地址为 topsec.com.cn/ngfw-ai/，更新周期为“每周二”。
- IPS：服务器地址为 ftp.topsec.com.cn，更新周期为“每周一”。
- URL：服务器地址为 webfilter.topsec.com.cn，更新周期为“每天”。
- AV：服务器地址为 avse.topsec.com.cn/fast-av，更新周期“每天”。

参数说明：

system rules-update reset	修改升级规则文件的服务器信息。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库

system rules-update show <cr>

命令描述：

查看自动更新策略配置信息。

以下为显示自动更新策略的配置信息示例：

```
TopsecOS# system rules-update show
Module      UpdateWay    State      Time      Server     User:Passwd
aise        ftp          disable    Tue 02:59
av          http         enable     03:43
ips         ftp          enable     Mon 01:04
url         http         disable    04:29
```

system rules-update update <aise|av|ips|url>

命令描述：

立即更新规则库。

配置立即更新规则库前，需要先开启规则文件自动升级功能。

参数说明：

rules-update update	配置规则库自动升级。
aise|av|ips|url	应用识别规则库|病毒过滤规则库|入侵防御规则库|URL 过滤规则库

system rules-update version <cr>

命令描述：

查看规则文件版本信息。

以下为查看规则文件版本信息的示例。

TopsecOS# **system rules-update version**

Module	Version	Expire	UpdateTime	RulesNum
ips	2012.08.01	unkown	never update	3861
aise	2014.10.27.003	unkown	never update	897
av	0000.00.00	unkown	never update	0
url	0000-00-00	unkown	never update	0

4.2.6 License 升级

License 是许可证，用来管理和控制天融信 NGFW 的部分功能以及服务的使用。对于非所有用户都有权涉及的受限制模块，许可证可授予相关权限。通过升级 License 可修改产品的功能开启状态。客户在购买 License 后，可使用 License 升级功能，将 License 写入设备，激活相应的功能。

License 升级方式有：FTP 升级、TFTP 升级和本地升级 3 种方式。管理员可以根据需要选择合适的升级方式。

- FTP 升级：FTP 升级指从指定的 FTP 服务器升级，如果 FTP 服务器设置了密码，需要填写用户名和密码。
- TFTP 升级：TFTP 升级指从指定的 TFTP 服务器升级。
- 本地升级：当 NGFW 与 Internet 物理隔离，且没有部署升级服务器时，可以采用本地升级方式。升级前将需要升级的 License 文件保存到管理主机，再通过 WebUI 登录到 NGFW 设备，选择 License 文件进行升级。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统维护** > **license 升级**。

步骤 2 配置升级 license 文件。

在配置升级 license 文件时，各项参数的具体说明如下表所示。

参数	说明
升级方式	设置自动更新方式。可选项：HTTP 和 FTP。 本地：从管理主机上获取 License 文件。 HTTP：从指定的 URL 地址下载 License 文件。 FTP：从指定的 FTP 服务器地址下载 License 文件。
服务器地址	配置自动更新获取 license 文件的服务器地址。字符串类型。格式为：http://...或 ftp://...。
文件名称	当升级方式为“本地”时，点击【浏览】按钮，选择主机上保存的 License 文件。 当升级方式为“FTP”或者“TFTP”时，设置 license 文件名称。
用户名	设置升级方式为 FTP 时需要配置该选项。输入 FTP 服务器的合法登录账号名称。
密码	设置升级方式为 FTP 时需要配置该选项。输入 FTP 服务器的合法登录账号名称对应的密码。

步骤 3 设置完成后，点击【应用】按钮，完成 License 文件升级配置。

CLI 方式配置

步骤	配置命令	配置说明
1	**system license update filename** <*string1*> **serverip** <*ipaddress*> **sysdisk normal** [**ftp yes** [**ftpuser** <*string2*>] [**ftppass** <*string3*>]]	配置 License 文件升级策略。

步骤	配置命令	配置说明
2	**system license show** <cr>	查看升级 License 文件的配置信息。
3	**system license version** <cr>	查看 License 文件的版本信息。

system license update filename <*string1*> **serverip** <*ipaddress*> **sysdisk normal** [**ftp yes** [**ftpuser** <*string2*>] [**ftppass** <*string3*>]]

命令描述：

设置 License 文件的升级策略。

参数说明：

system rules-update add	设置 License 文件的升级策略。
filename	必选项。License 文件名称。
string1	字符串类型，License 文件名称。
server-ip	FTP 服务器 IP 地址。
ipaddress	IP 地址，格式为：ftp://...。
sysdisk normal	升级主盘。
ftp	从指定的 FTP 服务器地址下载 license 文件。
yes	升级。
ftpuser	FTP 服务器用户名。
string2	字符串类型，长度范围：1-63。
ftppass	FTP 服务器密码。
string3	字符串类型，长度范围：1-63。

system license show <cr>

命令描述：

查看 License 文件配置信息。

以下为查看 License 文件示例：

```
TopsecOS# system license show
SERIALNO=xxxxxxxxxxxx.001
PRODUCT=TOPSEC-XX
BOARDTYPE=000
COPYRIGHT=TOPSEC
MAXSESSION=900000
```

```
ROUTE_TABLE=8000
POLICY_ROUTE=2000
VS_MAX_NUM=128

NGTOS=enable
PLAT=.100
TOTAL_OBJ_NUM=5000
TYPE_OBJ_NUM=2000
FW_COUNTS_MAX=10000
LICENSE_VER=2.0
NTP=enable
DHCP=enable
DHCP_CLIENT=enable
DHCP_RELAY=enable
DHCP_SERVER=enable
QINQ=enable
VLINE=enable
BOND=enable
VIRTUAL_SERVER=enable
BYPASS=enable
……
```

system license version <cr>

命令描述：

查看 License 文件的版本信息。

以下为查看 License 文件示例：

```
TopsecOS# system license version
001
```

4.3 管理员（一员管理）

管理员是用来登录并对设备进行管理配置的特殊用户，管理员可以通过 CLI、WEB 等方式登录设备，对设备进行网络以及安全策略等相关配置，使设备按用户需求工作。每台 NGFW 设备可以有多个管理员，不同的管理员对设备可以有不同的管理权限。

设备出厂后，第一次启动过程中将初始化预置管理员。按照职能和管理范围的不同，管理员可以分为超级管理员 superman、配置管理员，虚拟系统管理员。所有的管理员不允许重名。

1）超级管理员具有 NGFW 中所有的管理权限；

2）配置管理员具有查看和设定规则的权限，以及部分 NGFW 管理权限，但没有分配管理员的权限，只能修改自身的登录密码；

3）虚拟系统管理员不具备全局权限，只能查看、配置有限的公共信息和本虚拟系统的配置信息。

超级管理员可以添加、删除、修改配置管理员并对他们进行相应的授权。在开启虚系统功能开关后，超级管理员可以在添加配置管理员时为其指定一个已经存在的虚系统，如此，该配置管理员就是一个虚系统管理员，可以在授权范围内管理其关联虚系统的配置。如果超级管理员在添加配置管理员时没有为其指定关联的虚系统，这个配置管理员就是一个全局管理员，在授权范围内进行设备的全局配置。

除一员管理员外，NGFW 还支持三权管理员管理模式，关于管理员三权管理模式的配置具体请参见 4.4*管理员（三权分立）。

管理员登录方式的具体说明如下表所示。

登录方式	说明
Web	即通过 HTTPS 登录 Web 界面。管理员可利用任意以太网接口，只要登录 PC 与设备路由可达即可，一般优先选择管理口进行登录。 说明： 1）设备默认开启 HTTPS 服务。 2）管理员通过 Web 界面对设备进行操作，这种操作方式比命令行方式更直观。

登录方式	说明
CLI	即通过命令行方式登录，可选项：Console 口、Telnet、SSH。Telnet 和 SSH 方式默认为关闭。 1）Console 口方式是其他命令行登录方式的基础，同一时刻只允许一个人操作。使用场景有： （a）首次登录设备 CLI 界面； （b）无法远程登录设备时，通过 Console 口进行本地登录； （c）设备无法正常启动时，通过 Console 口进入并加载系统软件。 2）Telnet 方式便于对设备进行远程管理和维护，同一时刻允许多人操作。 3）SSH 方式需要进行密码认证，与 Telnet 方式相比更安全。

4.3.1 管理员

NGFW 支持预置管理员对其进行管理，也支持新添加的管理员对其进行管理。新添加的管理员的权限由其继承的管理权限模板控制，关于管理权限模板的设置具体请参见 4.3.2 管理权限。

管理员登录成功后，登记在一个在线管理员列表里，在线管理员信息包括：管理员名称、登录 IP 地址、登录时间、在线时间、登录方式。

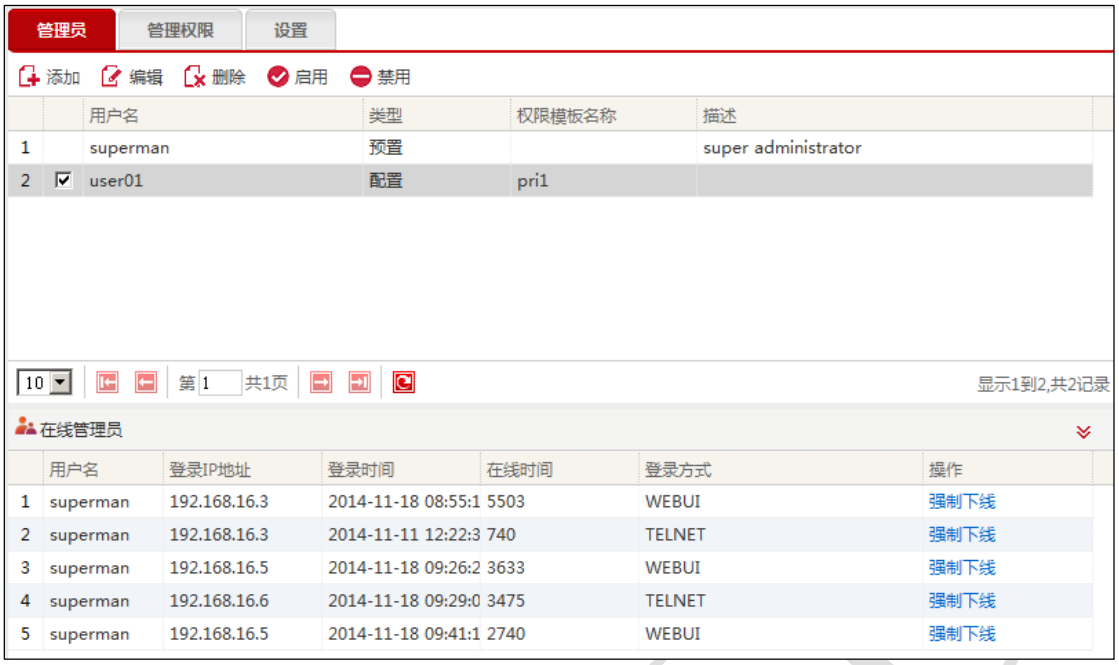
具备管理员管理权限的管理员可新添不同访问控制类型的管理员，还可远程监控登录 NGFW 的所有管理员，并可强制在线管理员退出系统。

说明

- ✧ 预置管理员不能被删除、被修改权限，只限于对预置管理员的操作只限于修改自身密码，预置管理员不能被删除、被修改权限。
- ✧ 不同的管理模式决定系统初始状态的管理员及其权限，如果管理模式发生改变，管理员相关配置将被清空并按新管理模式重新初始化。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **管理员**，激活“管理员”页签，进入管理员功能界面，如下图所示。

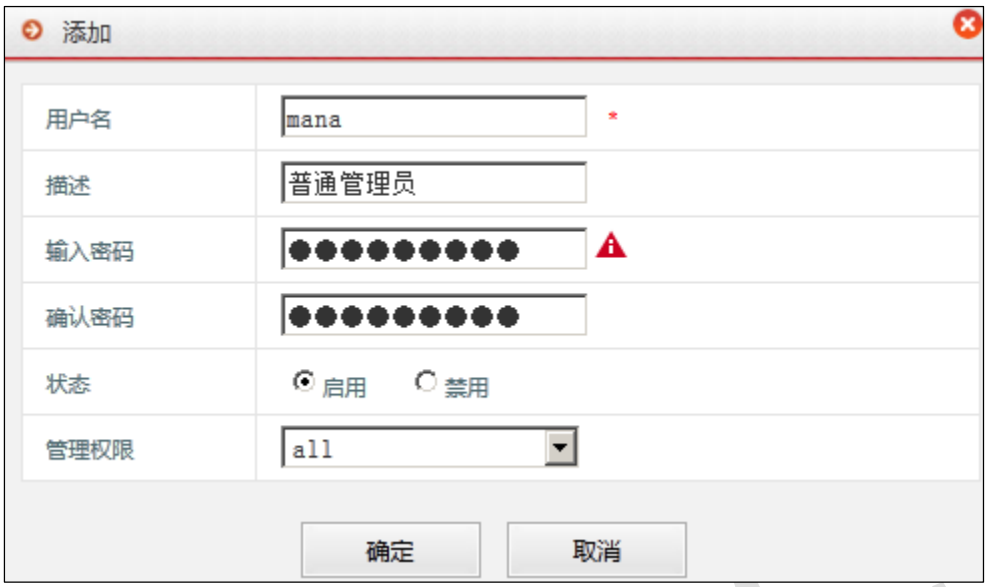


界面中上半部分显示了所有管理员账号信息，包括管理员名称、类型和管理权限等信息。选中已有管理员，点击菜单栏中的『启用』，弹出确定启用当前管理员的提示对话框，然后点击【确定】按钮表示该管理员账号启用；点击菜单栏中的『禁用』，弹出确定禁用当前管理员的提示对话框，然后点击【确定】按钮表示该管理员账号被禁用。界面下半部分显示了目前所有登录 NGFW 的在线管理员信息，包括名称、登录 IP 地址、最近登录时间、在线累积时间和登录方式。

注意

✧ 管理员列表中，若管理员账号被禁用，则显示为深灰色，如上图红框内所示的策略，非深灰色的管理员账号均处于启用状态。

步骤 2 点击『添加』，弹出“添加”窗口，如下图所示。



在添加管理员时，各项参数的具体说明如下表所示。

参数	说明
用户名	必选项，设置管理员的用户名称，需为除“!@#$%^&+=|?\"\\'> <`~”以外的字符。
描述	设置管理员的相关描述。
输入密码	必选项，设置管理员名称对应的密码，关于密码的复杂度具体请参见 4.3.3 设置。
确认密码	必选项，再次输入管理员名称对应的密码。
状态	设置管理员的启用状态。可选项：启用、禁用。
管理权限	设置管理员具备管理 NGFW 的权限。关于管理权限的设置具体请参见 4.3.2 管理权限。

点击【确定】按钮完成管理员的添加。

步骤 3 选择在线管理员列表中任一管理员，点击相应的『强制下线』，强制管理员下线。

CLI 方式配置

system admin add name <*string1*> **passwd** <*string2*> [**comment** <*string3*>] [**vsys-name** <*string4*>]

命令描述

添加系统管理员。

参数说明

system admin add	添加管理员。
name	必选项，设置管理员名称。
string1	字符串类型，表示管理员名称。
passwd	必选项，设置管理员登录密码。
string2	字符串类型。
comment	可选项，设置对添加的管理员的具体说明。
string3	字符串类型。
vsys-name	可选项，设置虚系统号。
string4	字符串类型。

以下是添加管理员的示例：

添加名称为“zmz”，登录密码为“talent”的管理员。

```
TopsecOS # system admin add name zmz passwd talent
```

system admin modify-info name <*string1*> [**passwd** <*string2*>] [**comment** <*string3*>]

命令描述

修改系统管理员基本信息。

参数说明

system admin modify-info	修改系统管理员基本信息。
name	必选项，指定管理员名称。
string1	字符串类型，表示管理员名称。
passwd	可选项，设置管理员登录密码。
string2	字符串类型。
comment	可选项，设置对添加的管理员的具体说明。
string3	字符串类型。

system admin modify-priv admin-name <*string1*> [**map-name** <*string2*>] [**status** <valid|invalid>]

命令描述

修改系统管理员权限。

参数说明

system admin modify- priv	修改系统管理员权限。
admin-name	必选项，指定管理员名称。
string1	字符串类型，表示管理员名称。
map-name	可选项，设置管理权限的模板名称。
string2	字符串类型。
status	可选项，设置系统管理员的状态。

valid|invalid	启用|禁用

system admin forced-offline session-id <*number*>

命令描述

强制管理员下线配置。

参数说明

system admin forced-offline	强制管理员下线。
session-id	必选项，设置在线管理员的编号。
number	数值类型。

system admin show <cr>

命令描述

显示系统管理员。

以下是显示系统管理员的示例：

```
TopsecOS # system admin show
-----------------------------------------------------
admin-name: superman
admin-type: default
privilege-map:
comment:super administrator
status: valid
-----------------------------------------------------
admin-name: 1
admin-type: config
privilege-map: all
comment:
status: valid
-----------------------------------------------------
admin-name: vsys01
admin-type: vsys-admin
```

```
privilege-map: KJH
comment:
status: valid
-----------------------------------------------------
admin-name: user1
admin-type: config
privilege-map:
comment:
status: valid
```

system admin online <cr>

命令描述

显示系统在线管理员。

以下是显示系统在线管理员的示例：

```
TopsecOS # system admin online
-----------------------------------------------------------
session-id: 1     admin-name: superman     logon-ip: 192.168.16.5     logon-type:
TELNET logon-time: 2014-09-10 00:41:20     online-time: 4312
-----------------------------------------------------------
session-id: 2     admin-name: superman     logon-ip: 192.168.16.6     logon-type:
WEBUI    logon-time: 2014-09-10 00:41:36     online-time: 4296
-----------------------------------------------------------
session-id: 3     admin-name: superman     logon-ip: 192.168.16.5     logon-type:
WEBUI    logon-time: 2014-09-10 01:10:31     online-time: 2561
-----------------------------------------------------------
session-id: 4     admin-name: superman     logon-ip: 192.168.16.6     logon-type:
TELNET logon-time: 2014-09-10 01:49:46     online-time: 206
```

4.3.2 管理权限

管理权限指管理员对 NGFW 各功能模块的操作权限，包括“无”、“只读”和“读写”，“无”指管理员无查看和设置权限；“只读”指管理员具备查看的权限；“读写”指管理员具备设置权限。NGFW 基于管理权限模板对非预定义的管理员赋予管理权限，关于为管理员赋予管理权限的操作具体请参见 4.3.1 管理员。

说明

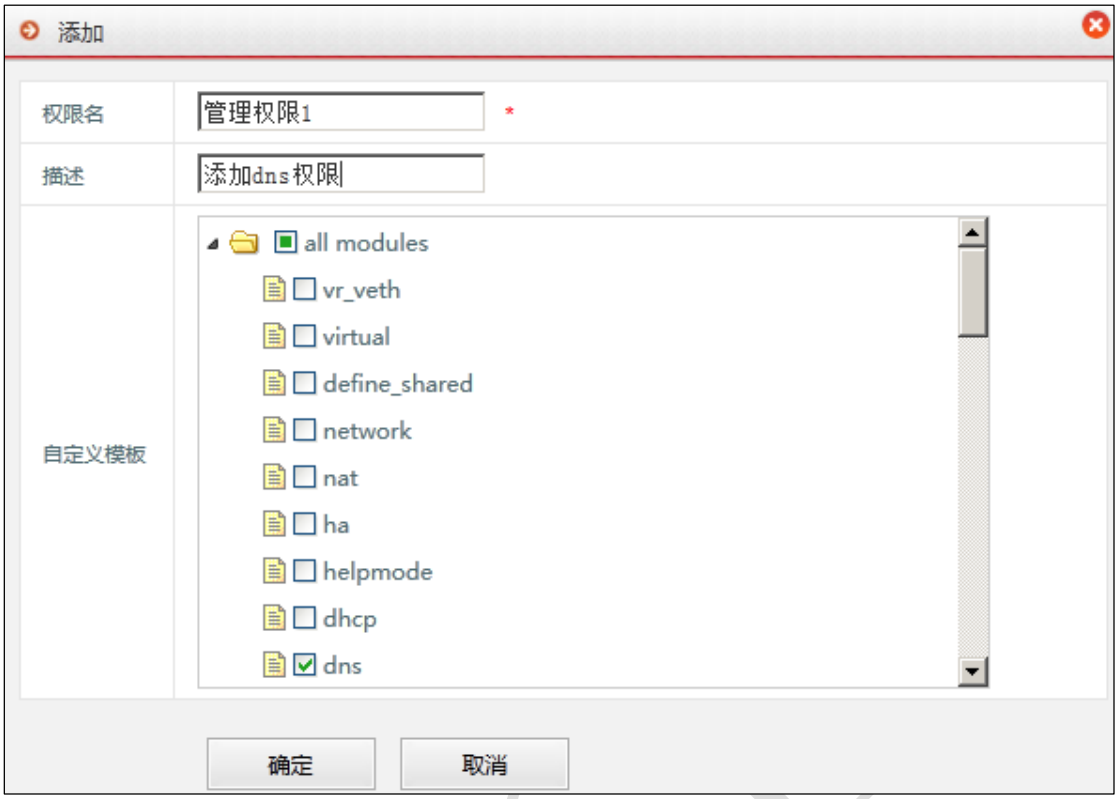
- ✧ 创建管理员账号和为管理员赋权可由相同的管理员完成，也可由不同的管理员完成。例如在一员管理模式下，可由 superman 完成管理员创建及赋权的操作；三员管理模式下，可由 admin 创建管理员账号，grantor 为管理员赋权。

NGFW 基于管理权限模板对非预置管理员赋予管理权限，管理权限模板可实现划分 NGFW 的部分功能为不同的访问控制类型，以控制不同管理员的管理权限，进而对管理 NGFW 进行合理分工。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **管理员**，激活“管理权限”页签。

步骤 2 点击『添加』，弹出“添加”窗口，如下图所示。



在添加权限模板时，各项参数的具体说明如下表所示。

参数	说明
权限名	必选项，设置权限模板名称。
描述	设置权限模板必要的描述信息。
自定义模块	设置权限模板的访问权限。 说明： 勾选相应模块的复选框，则具有查看及配置该模块相关配置的功能。

点击【确定】按钮完成权限模板的添加。

CLI 方式配置

system privilege show-modules <cr>

命令描述

显示系统管理权限及其对应的 ID。

以下是显示系统管理权限及其对应的 ID 的示例：

```
TopsecOS # system privilege show-modules
64   vr_veth                    65   virtual
66   define_shared              128  network
129  nat                        130  ha
131  helpmode                   132  dhcp
133  dns                        134  global
135  snmp                       136  ai
137  memory                     138  pf-service
139  local-service              140  pki
141  vpn                        142  super
256  alarm                      257  show-running
258  show                       259  ping
260  network-show               261  global-ai
320  define                     321  firewall
322  user_manage                323  proxy
324  vsys                       325  stat
326  qos                        327  alg
896  ddos                       897  ips
898  av                         899  file_block
900  url_filter                 901  data_filter
```

system privilege map create name <*string1*> [**comment** <*string2*>] [**module-select** <*string3*>]

命令描述

添加管理权限模板。

参数说明

system privilege map create	添加管理权限模板。
name	必选项，设置管理权限模板的名称。
string1	字符串类型，表示管理权限模板的名称。
comment	可选项，设置权限模板必要的描述信息。
string2	字符串类型。
module-select	可选项，设置权限模板包含的功能。 说明：

	权限功能用功能编号表示，并用逗号分隔，比如 1,2,129,321。
string3	数值类型。表示系统功能模块对应的 ID 号。

以下是添加管理权限模板的示例：

添加名称为“map1”，包含功能模块“901”的管理权限模板。

```
TopsecOS# system privilege show-modules
64   vr_veth                    65   virtual
66   define_shared              128  network
129  nat                        130  ha
131  helpmode                   132  dhcp
133  dns                        134  global
135  snmp                       136  ai
137  memory                     138  pf-service
139  local-service              140  pki
141  vpn                        142  super
256  alarm                      257  show-running
258  show                       259  ping
260  network-show               261  global-ai
320  define                     321  firewall
322  user_manage                323  proxy
324  vsys                       325  stat
326  qos                        327  alg
896  ddos                       897  ips
898  av                         899  file_block
900  url_filter                 901  data_filter
TopsecOS# system privilege map create name map1 module-select 901
```

system privilege map show-single name <*string*>

命令描述

显示指定的管理权限模板的功能信息。

参数说明

system privilege map show-single	显示管理权限模板。
name	必选项，指定管理权限模板的名称。
string	字符串类型，表示管理权限模板的名称。

system privilege map show <cr>

命令描述

显示所有的功能权限。

以下是显示所有的功能权限的示例：

```
TopsecOS# system privilege map show
name: KJH
type: custom
describtion:
privilege:
id          module_name                 status
64          vr_veth                     enable
65          virtual                     enable
66          define_shared               enable
128         network                     enable
129         nat                         enable
130         ha                          enable
131         helpmode                    enable
132         dhcp                        enable
133         dns                         enable
134         global                      enable
135         snmp                        enable
136         ai                          enable
137         memory                      enable
138         pf-service                  enable
```

139	local-service	enable
140	pki	enable
141	vpn	enable

---

system privilege map add-module name <*string1*> [**module-select** <*string2*>]

命令描述

添加功能模块到管理权限中。

参数说明

system privilege map add-module	添加自定义功能模板。
name	必选项，设置自定义模板名称。
string1	字符串类型。
module-select	可选项，设置自定义模板的访问权限。
string2	数值类型。

system privilege map sub-module name <*string1*> [**module-select** <*string2*>]

命令描述

减少管理员权限中的功能。

参数说明

system privilege map sub-module	减少管理员权限中的功能。
name	必选项，指定管理员权限模板。
string1	字符串类型。
module-select	可选项，设置要删除的权限模块对应的 ID。
string2	数值类型。

4.3.3 设置

管理员负责 NGFW 的管理与配置，因此为保证 NGFW 的安全性，管理员的登录会话必须设置一定的安全保护机制，以防止非法人员窃取管理员账号。具备管理员模块读写权限的管理员可以通过设置管理员账号的密码复杂度、允许最大登录失败次数、最大在线数，防止管理员账号被暴力破解，提高管理员管理设备的安全性。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **管理员**，激活“设置”页签，进入管理员账号安全设置界面。

在设置管理员账号安全保护机制时，各项参数的具体说明如下表所示。

参数	说明
密码复杂度	为适应管理员密码安全性、易用性的不同需求，NGFW 提供密码复杂度的设置功能。 设置添加管理员时口令密码的复杂程度。可选项：高、中、低。 说明： “高”表示密码设置要大于 16 个字符，小于等于 128 个字符，必须包含大小写、数字、特殊英文字符“!@#$%^&*_+-=)”，不包含自身信息（用户名、描述）。 “中”表示密码设置要大于 12 个字符、小于等于 128 个字符，必须包含大小写、数字。 “低”表示密码设置要大于 8 个字符，小于等于 128 个字符。
防暴力破解	设置是否启用防暴力破解开关。勾选复选框表示防暴力破解开关处于开启状态。
首次登录是否强制修改密码	为适应管理员密码安全性、易用性的不同需求，NGFW 提供首次登录强制修改密码的设置功能。 勾选复选框表示开启首次登录强制修改密码功能。
允许最大登录失败次数	设置允许同一管理员连续登录 NGFW 的最大失败次数。单位：次；取值范围：3-100；默认值：5。 说明： 同一管理员登录失败次数超过最大失败次数后，NGFW 的登录界面将被锁定一段时间。
账号锁定时间	设置 NGFW 的 WEBUI 界面因管理员超过最大登录失败次数后仍未成功登录的锁定时间。单位：秒；取值范围：30-3600；默认值：60。
管理员最大在线数	设置所有管理员登录 NGFW 的最大连接数。单位：个；取值范围：1-5000；默认值：100。
同一个管理员最大在线数	设定使用同一管理员账号同时管理 NGFW 的最大连接数。单位：个；取值范围：1-5000；默认值：5。
webui 方式登录最大并发管理数	设置所有管理员使用 WEBUI 界面方式同时管理 NGFW 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。
ssh 方式登录最大并发管理数	设置所有管理员使用 SSH 方式同时管理 NGFW 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。
telnet 方式登录最大并发管理数	设置所有管理员使用 Telnet 方式同时管理 NGFW 的最大连接数。单位：个；取值范围：0-5000，0 表示不限制；默认值：0。

步骤 2 参数设置完成后，点击【应用】按钮完成账号安全机制的配置，点击【重置】按钮将管理员账号保护机制的各参数值恢复为出厂配置。

CLI 方式配置

system admin-auth-policy set [**password-complexity** <high|medium|low>] [**anti-crack** <on|off>] [**first-login** <yes|no>] [**maxnum-admin-online** <*number1*>] [**maxnum-same-admin-online** <*number2*>] [**maxnum-auth-fail** <*number3*>] [**account-locked-time** <*number4*>]

命令描述

管理员账号安全设置。

参数说明

system admin-auth-policy set	设置管理员账号安全参数。
password-complexity	可选项，设置添加管理员时口令密码的复杂程度。
high|medium|low	高|中|低
anti-crack	可选项，设置是否启用防暴力破解开关。
on|off	启动|禁用
first-login	可选项，设置是否开启首次登录强制修改密码功能。
yes|no	是|否
maxnum-admin-online	可选项，设置所有管理员登录 NGFW 的最大连接数。
number1	数值类型，单位：个；取值范围：1-5000；默认值：100。
maxnum-same-admin-online	可选项，设定使用同一管理员账号同时管理 NGFW 的最大连接数。
number2	数值类型，单位：个；取值范围：1-5000；默认值：5。
maxnum-auth-fail	可选项，设置允许同一管理员连续登录 NGFW 的最大失败次数。
number3	数值类型，单位：次；取值范围：3-100；默认值：5。
account-locked-time	可选项，设置 NGFW 的 WEBUI 界面因管理员超过最大登录失败次数后仍未成功登录的锁定时间。
number4	数值类型，单位：秒；取值范围：30-3600；默认值：60。

以下是设置管理员账号安全的示例：

TopsecOS # **system admin-auth-policy set password-complexity** high **anti-crack** on **first-login** yes **maxnum-admin-online** *100* **maxnum-same-admin-online** *5* **account-locked-time** *60*

system admin-auth-policy show <cr>

命令描述

显示管理员账号安全设置信息。

以下是设置管理员账号安全的示例：

```
TopsecOS # system admin-auth-policy show
password-complexity: high
anti-crack: on
maxnum-auth-fail: 100
account-locked-time: 3000(seconds)
maxnum-admin-online: 200
maxnum-same-admin-online: 200
password-need-change-first-login: yes
online number limit of login type:
webui: 0 ;ssh: 0 ;telnet: 0
```

system admin-auth-policy reset <cr>

命令描述

重置管理员账号安全设置信息。

4.4 *管理员（三权分立）

为满足不同用户的保密使用需求，NGFW 支持多个管理员对其进行管理操作，不同的管理员可以设置不同的操作权限。用户可以根据实际需求，订购不同管理模式的 NGFW。当 NGFW 出厂配置为三权分立管理模式时，系统预置了三个管理员：admin、grantor 和 auditor，密码为 talent。

- admin：预置系统管理员，具有创建管理员的权限，新创建的管理员默认没有任何权限；
- grantor：预置安全保密员，具有对系统管理员已创建的管理员进行赋权的权限；
- auditor：预置审计员，则具有设置和查看所有管理员的行为日志以及网关业务日志，并提供报警提示的权限。

三权分立管理员，将一元管理的 superman 预配置管理员权限分散到三个预配置管理员，并且不能对设备进行功能配置，不同管理员的权限分明，提高设备的安全性。三个管理员管理权限相互独立，相互制约。另外，系统内置一个预置管理员 operator，具有配置命令的权限。NGFW 系统可根据实际需要配置新的管理员账号及管理权限。

说明

- admin、grantor 和 auditor 的密码都是 talent，成功登录防火墙后，可通过 **系统管理** > **系统设置** > **密码设置**，修改管理员自身的密码。
- 对预置管理员的操作只限于修改自身密码，预置管理员不能被删除、被修改权限。

不同管理员具有不同的管理权限，当使用 WEBUI 进行设备管理时，预配置管理员权限及配置的功能入口如下表所示。

功能入口	功能说明位置	admin	grantor	auditor
安全策略 > **ALG**	7.6ALG	支持	支持	支持
网络管理 > **接口** > **接口联动**	6.2.6 接口联动	支持	支持	支持
系统管理 > **系统设置** > **系统信息** **系统管理** > **系统设置** > **系统参数** **系统管理** > **系统设置** > **系统诊断** **系统管理** > **系统设置** > **密码设置**	4.1 系统设置	支持	支持	支持
系统管理 > **系统维护** > **配置维护** **系统管理** > **系统维护** > **健康记录** **系统管理** > **系统维护** > **license 升级**	4.2 系统维护	支持	支持	支持
系统管理 > **系统日志** > **日志查看** **系统管理** > **系统日志** > **日志配置** **系统管理** > **系统日志** > **日志服务器配置**	4.5 系统日志	不支持	不支持	支持
系统管理 > **管理员**，管理员页签	4.3 管理员（一员管理）	支持（创建）	支持（赋权）	不支持
系统管理 > **管理员**，设置页签	4.3 管理员（一员管理）	支持	不支持	不支持
系统管理 > **管理员**，管理权限页签	4.3 管理员（一员管理）	不支持	支持	不支持

具体功能详细说明与一元管理时配置步骤相同，请参见网络管理和系统管理对应的功能章节，具体请参见 4.3 管理员（一员管理）。以下仅介绍如何在三权分立管理模式下，创建配置管理账户并配置管理权限。

WEBUI 方式配置

步骤 1 使用 admin 预配置管理员创建配置管理员。

只有 admin 管理员具有配置管理员账号的权利，其他类型的管理员登录系统后只能修改自身的登录密码。

1）使用 admin 预配置管理登录防火墙，选择 **系统管理** > **管理员**，进入如下界面。

2）添加配置管理员账号。

点击『添加』，弹出“添加管理员”对话框，在对话框中配置管理员账号。

在添加管理员时，各项参数的具体说明如下表所示。

参数	说明
用户名称	必选项，设置管理员的用户名称，需为除“!@#$%^&+=|?\"\\'> <`~”以外的字符。
描述	设置管理员的相关描述。
输入密码	必选项，设置管理员名称对应的密码，关于密码的复杂度具体请参见 4.3.3 设置。
确认密码	必选项，再次输入管理员名称对应的密码。

配置完成后，点击【确定】按钮，完成配置。

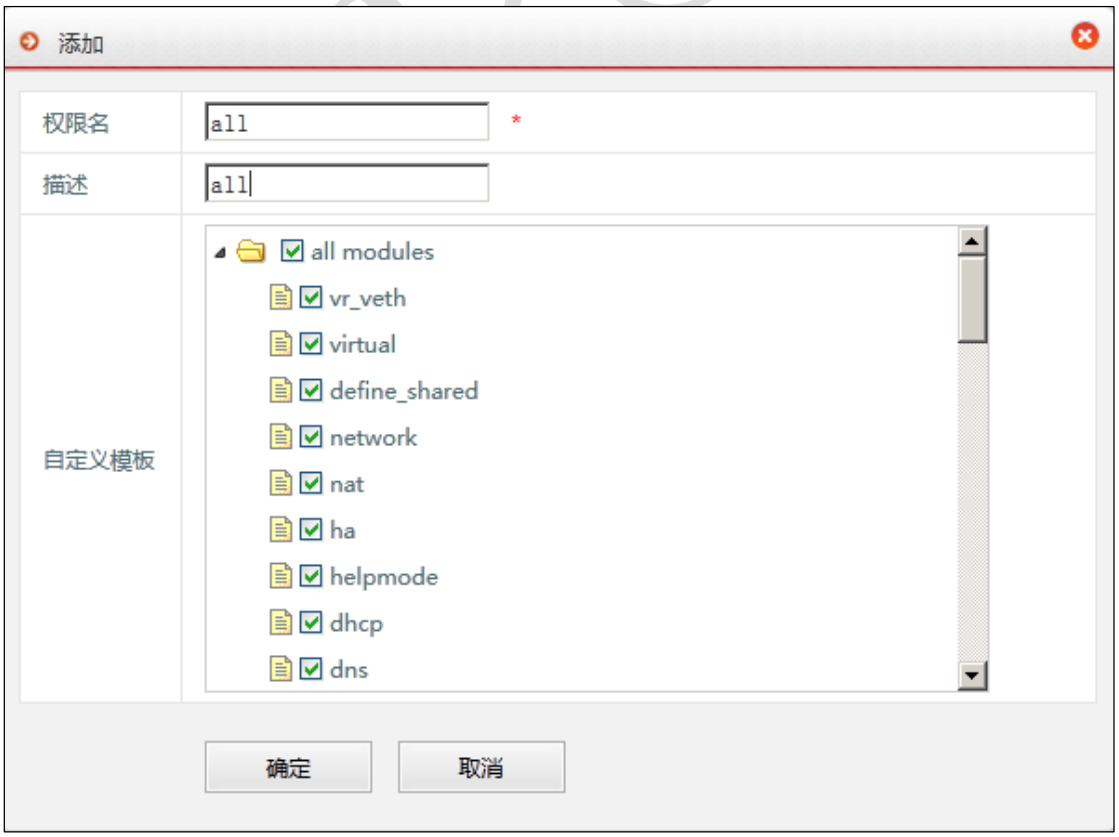
3）（可选）选择 **系统管理** > **管理员**，激活“设置”页签，可设置管理员账号的安全配置信息，具体参数说明请参见 4.3.3 设置。

步骤 2 使用 grantor 预配置管理员修改配置管理员的管理权限。

只有预置保密员 grantor 具有对系统管理员 admin 已创建的配置管理员进行授权的权限。

1）使用 grantor 登录防火墙，选择 **系统管理** > **管理员**，进入如下界面。

2）激活“管理权限”页签，点击『添加』，弹出“添加权限模板”对话框。



在添加权限模板时，各项参数的具体说明如下表所示。

参数	说明
权限名	必选项，设置权限模板名称。
描述	设置权限模板必要的描述信息。
自定义模块	必选项。设置权限模板的访问权限。 说明： 所有管理员均具有查看系统“首页”、“监控”、“接口联动”、“系统设置”和“系统维护”的功能。勾选相应模块的复选框，则具有查看及配置该模块相关配置的功能。

3）激活“管理员”页签，双击由 admin 创建的配置管理员所在行，弹出“编辑用户”对话框。

在编辑管理员时，各项参数的具体说明如下表所示。

参数	说明
用户名	显示需要修改的管理员用户名。
状态	设置配置管理员账号是否可用。可选项：启用和禁用；默认值：启用。
管理权限	设置管理员的管理权限模板，通过下拉列表选择。

配置完成后，点击【确定】按钮，完成配置。

CLI 方式配置

使用 admin 预配置管理员创建配置管理员，grantor 预配置管理员为配置管理员配置管理权限。

步骤	配置命令	配置说明
1	**system admin add name** <*string1*> **passwd** <*string2*> [**comment** <*string3*>] [**vsys-name** <*string4*>]	使用 admin 预配置管理员创建配置管理员。
2	**system admin-auth-policy set** [**password-complexity** <high|medium|low>] [**anti-crack** <on|off>] [**first-login** <yes|no>] [**maxnum-admin-online** <*number1*>] [**maxnum-same-admin-online** <*number2*>] [**maxnum-auth-fail** <*number3*>] [**account-locked-time** <*number4*>]	（可选）使用 admin 预配置管理员设置管理员安全选项。
3	**system privilege map create name** <*string1*> [**comment** <*string2*>] [**module-select** <*string3*>]	使用 grantor 预配置管理员创建管理权限模板。
4	**system privilege map add-module name** <*string1*> [**module-select** <*string2*>]	使用 grantor 预配置管理员添加功能模块到管理权限中。
5	**system admin modify-priv admin-name** <*string1*> [**map-name** <*string2*>] [**status** <valid|invalid>]	使用 grantor 预配置管理员修改系统管理员权限。

4.5 系统日志

NGFW 提供完善的系统日志功能，方便管理员及时跟踪防火墙的工作状态，比如管理员登录、系统事件、出错信息等反映系统当前或一段时间内的运行状况，及时对生成的日志进行综合分析，发现安全隐患，从而提高被保护网络的安全性和设备安全系统的管理成效。

管理员可根据用户的实际需求，在日志配置界面灵活配置 NGFW 需要记录的日志，并可以从日志查看界面中查看设备上记录的日志。系统日志按时间先后顺序保存至本地缓存中，设备上记录的日志过多会导致系统缓存区容量达到最大，此时当新的日志产生时，系统将删除缓存区中最旧的日志，显示当前最新的日志。如果管理员想要查看历史日志信息，可以利用 NGFW 提供的日志服务器配置功能，将设备日志上传至配置好的日志服务器中，在日志服务器中进行查看。

4.5.1 日志服务器配置

日志服务器能够集中负责日志的收集、分析、报告和日志安全管理，能够有效地协助管理员进行系统管理维护、攻击定位，发现安全风险。

NGFW 可以按照 Welf 或 Syslog 格式来记录日志。系统日志可保存在本地缓存中，当本地存储的日志数量越来越多，本地磁盘大小有限导致设备存储不够时，可考虑通过 TCP 或 UDP 协议将记录的日志传送到日志服务器上，从而实现对设备日志进行统计与分析，并及时发现攻击等安全隐患，提高 NGFW 的安全管理。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **系统日志** > **日志服务器配置**。

在配置日志服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器地址	必选项，设置日志服务器的 IP 地址，格式：x.x.x.x，默认地址：192.168.1.254。可最多设置 16 个日志服务器。
服务器端口	必选项，设置日志服务器接收日志的服务端口。取值范围：1-65535；默认值：514。 说明： 日志服务器端口必须和设备日志服务器配置页面所指定的端口一致。
传输协议	必选项，设置 NGFW 传输日志至日志服务器中所使用的协议，可选项：TCP、UDP。
传输类型	必选项，设置 NGFW 记录日志的格式，可选项：Welf、Syslog。 说明： NGFW 可以按照 Welf 格式或者 Syslog 格式记录日志，并通过 Syslog 协议传送到已设定的日志服务器上，并可采用第三方软件来对日志进行统计与分析。
日志开关	设置是否记录日志。
传输至	设置传输日志到日志服务器的位置，可选项：控制台、文件。 传输至“控制台”：表示传输到通过 console 口连接的主机上； 传输至“文件”：表示传输到设备上指定的位置。 若配置了日志服务器，则将日志同时传输到日志服务器上。
传输日志	必选项。设置是否传输日志至所配置的日志服务器中。
传输加密	必选项。设置是否加密传输至日志服务器中的日志。
加密密码	“传输加密”开关处于开启状态下时，该参数为必选项。设置加密日志的密码。 说明： 加密密码为 8 位。

说明

- ✧ 配置好日志服务器后，系统记录的日志除了被发送到设定的日志服务器中外，也在 NGFW 中缓存部分日志。在 NGFW 中缓存的日志可以通过 **系统日志** > **日志查看**

进行查看，关于日志查看具体请参见 4.5.3 日志查看。

步骤 2 点击【确定】按钮完成日志服务器的配置。

CLI 方式配置

log config set [**ipaddr** <*string1*>] [**port** <*string2*>] [**logtype** <syslog|welf>] [**log_switch** <on|off>] [**to_console** <on|off>] [**to_file** <on|off>] [**trans** <enable|disable>] [**trans_gather** <yes|no>]

命令描述

配置日志服务器。

参数说明

log config set	设置日志服务器。
ipaddr	可选项，设置日志服务器的 IP 地址。
string1	字符串类型，表示 IP 地址，格式为 A.B.C.D。
port	可选项，设置日志服务器接收日志的端口号。
string2	字符串类型，表示端口号，格式为 udp:端口号或 tcp:端口号，端口号取值范围：1-65535；默认值：514。
logtype	可选项，设置日志服务器传输日志的传输类型，有 2 种：syslog 和 welf。
syslog|welf	默认值：syslog。
log_switch	可选项，设置是否开启日志开关。
on|off	打开|关闭
to_console	可选项，设置是否传输日志到控制台。
on|off	是|否
to_file	可选项，设置是否传输日志到文件。
on|off	是|否
trans	可选项，设置是否传输日志。
enable|disable	传输日志|不传输日志
trans_gather	可选项，设置是否要合并日志的传输。
yes|no	合并|不合并

以下是设置日志服务器参数的示例：

TopsecOS# **log config set ipaddr** *192.168.1.25* **logtype** syslog **port** *udp:80* **trans** enable **trans_gather** yes log_**switch** on

log config set mode retry <on|off>

命令描述

设置重试模式。

参数说明

log config set mode	设置日志服务器的重试模式。
retry	必选项，设置是否开启重试模式。
on|off	打开|关闭

log config crypt <enable|disable>

命令描述

设置是否进行日志加密。

参数说明

log config crypt	设置是否加密日志。
enable|disable	加密日志|不加密日志

以下是设置日志加密信息的示例：

TopsecOS# **log config crypt** enable

log config key_set <*string*>

命令描述

设置日志的密钥。

参数说明

log config key_set	设置日志信息传输时使用的加密密码。
string	字符串类型，8 个字符。

以下是设置日志密钥的示例：

TopsecOS# **log config key_set** *11111111*

log config key_set clean <cr>

命令描述

清除日志的密钥。

4.5.2 日志配置

NGFW 日志的功能主要是记录系统运行时的各种信息，如用户登录，系统事件，出错信息等，能够反映系统当前和一段时间内的运行状况。管理员可通过配置系统日志生成条件控制系统日志的数量，以获取定位系统问题时具备参考价值的日志。

日志所属级别包括：

- 紧急：造成严重错误导致系统不可用。
- 告警：警报信息。
- 严重：严重错误信息，可能会造成某些功能无法正常工作。
- 错误：一般错误信息。
- 警示：所有攻击行为以及非授权访问（除通信日志外）。
- 通知：非错误信息，但需要管理员特殊处理。
- 信息：普通事件。
- 调试：开发人员调试信息，包括正常的使用信息。

其中，级别为紧急、告警、严重的日志属于高级别的日志，级别为错误、警示、通知的日志属于中级别的日志，级别为信息、调试的日志属于低级别的日志。

WEBUI 方式配置

在配置日志之前，需要先进行日志服务器的配置，关于日志服务器的介绍具体请参见 4.5.1 日志服务器配置。

步骤 1 选择 **系统管理** > **系统日志** > **日志配置**。

在配置系统日志记录条件时，各项参数的具体说明如下表所示。

参数	说明
全部日志	必选项。全局日志开关。开启该开关，NGFW 会根据“自定义配置”处的日志开关记录相应的日志；关闭该开关，NGFW 不会记录系统日志。
级别严重程度	在“全部日志”开关处于开启状态下，为必选项。设置所记录的系统日志的级别严重程度，可选项：高、中、低。 说明： 系统只会记录所选级别及其以上级别的日志信息。若选择“高”，则系统只记录高级别的日志信息，若选择“中”，则系统将记录级别为高、中的日志信息。

参数	说明
日志服务器	显示 NGFW 所配置的日志服务器的 IP 地址，关于日志服务器的配置具体请参见 4.5.1 日志服务器配置。
自定义配置	在“全部日志”开关处于开启状态下，为必选项。用于管理员控制是否生成相应类型事件的日志，以及生成的日志所属级别。

注意

- ✧ 系统记录和传输日志是根据日志类型和日志级别。如日志级别为“严重”，日志类型为“阻断策略”，系统将记录紧急、告警和严重级别的阻断策略日志。
- ✧ 若日志配置发生变化，则系统读取新的参数，建立新的连接，同时关闭与客户端的连接，并通知客户端配置发生了改变。

步骤 2 点击【应用】按钮完成日志信息的配置。

CLI 方式配置

log config type_set
<mgmt|system|pf|conn|ac|secure|dpi|vpn|portflow|user_auth|ips|asse|ai|ids|ddos_inspect|ddos_clean|anti_virus|url_filter|data_filter|file_block|ha> **level_set** <*number*>

命令描述

设置日志的类型和级别。

参数说明

log config type_set	设置日志的类型。
mgmt|system|pf|conn|ac|secure|dpi|vpn|portflow|user_auth|ips|asse|ai|ids|ddos_inspect|ddos_clean|anti_virus|url_filter|data_filter|file_block|ha	管理日志|系统日志|包过滤日志|连接日志|访问策略/地址转换策略日志|安全日志|深度内容检测日志|VPN 日志|统计日志|用户认证日志|IPS 日志|反垃圾邮件日志|应用识别日志|IDS 日志|DDOS 检测日志|DDOS 清洗日志|防病毒日志|URL 过滤日志|内容过滤日志|文件过滤日志|高可用性日志
level_set	必选项，设置日志的级别。系统将会记录所选级别及其以上级别的日志信息。如选择严重，则系统将记录紧急、告警和严重级别的日志信息。 日志级别如下： 紧急——造成严重错误导致系统不可用，该日志被传送到日志服务器； 告警——警报信息，需要通知管理员，该日志被传送到日志服务器； 严重——严重错误信息，可能会造成某些功能

	无法正常工作； 错误——一般错误信息； 警示——所有攻击行为以及非授权访问（除通信日志外）； 通知——管理员操作； 信息——普通事件； 调试——开发人员调试信息。
number	数值类型，0：EMERG 表示紧急，1：ALERT 表示告警，2：CRITICAL 表示严重，3：ERROR 表示错误，4：WARN 表示警示，5：MANAG 表示通知，6：INFO 表示信息，7：DEBUG 表示调试，8：OFF 表示关闭。

以下是设置日志的类型和级别的示例：

```
TopsecOS# log config type_set ac level_set 1
```

log config show <cr>

命令描述

显示日志配置信息。

以下是显示日志配置信息的示例：

```
TopsecOS# log config show
log config set ipaddr '192.168.1.254 192.168.92.112' port UDP:514 logtype syslog
  trans enable trans_gather yes log_switch on
log config crypt disable
log config key_set clean
log config set to_console off
log config set to_file off
log config set mode retry on
log config type_set mgmt level_set 7
log config type_set system level_set 8
log config type_set pf level_set 8
log config type_set conn level_set 8
log config type_set ac level_set 8
```

```
log config type_set secure level_set 8
log config type_set dpi level_set 8
log config type_set vpn level_set 8
log config type_set portflow level_set 8
log config type_set user_auth level_set 8
log config type_set ips level_set 8
log config type_set asse level_set 8
log config type_set ai level_set 8
log config type_set ids level_set 8
log config type_set ddos_inspect level_set 8
log config type_set ddos_clean level_set 8
```

4.5.3 日志查看

日志查看主要用于查看具体的日志情况，例如可以查看安全区域内的哪些对象受到了 DDoS 攻击，并可以查看攻击的源 IP 和端口等详细信息。日志记录了 NGFW 处理的所有流量的源地址、目的地址、所匹配的防护策略、攻击类型、开始阻断时间和是否已自动将该流量的源地址加入到黑名单等信息。

WEBUI 方式配置

在查看日志之前，需要先进行日志类型、日志级别等配置，关于日志参数的配置具体请参见 4.5.2 日志配置。

步骤 1 选择 **系统管理** > **系统日志** > **日志查看**，进入日志查看界面。

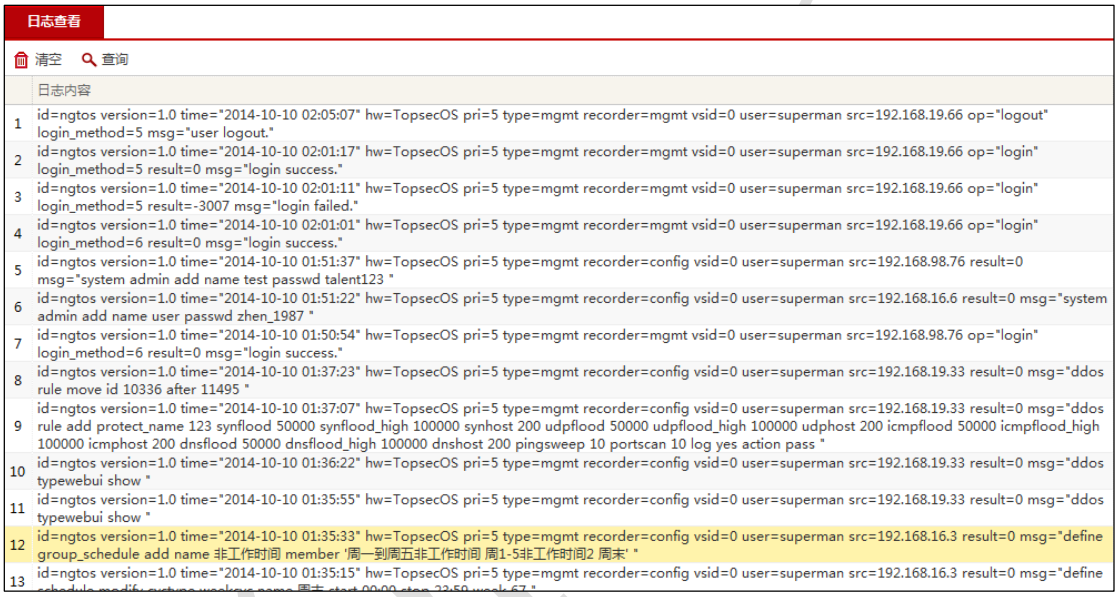
步骤 2 点击『查询』，弹出“搜索”窗口。

在设置搜索信息时，各项参数的具体说明如下表所示。

参数	说明
起始位置	设置日志查询的起始位置，取值范围：1-2048。
结束位置	设置日志查询的结束位置，取值范围：1-2048。
关键词	设置日志查询的关键词。

参数	说明
日志类型	设置日志包含的类型。关于日志类型的设置具体请参见 4.5.2 日志配置。
日志级别	设置日志的级别。关于日志级别的设置具体请参见 4.5.2 日志配置。
起始时间	设置日志产生的起始时间。
结束时间	设置日志产生的结束时间。

点击【确定】按钮完成查询的参数设置，同时与查询条件匹配的日志信息显示在日志查看列表中，如下图所示。



CLI 方式配置

log message count <cr>

命令描述

查看当前日志的数量。

以下是查看当前日志的数量的示例：

```
TopsecOS# log message count

Total log : 21
```

log message show from <*number1*> **to** <*number2*> [**keyword** <*string1*>] [**level** <*number3*>] [**type** <mgmt|system|pf|conn|ac|secure|dpi|vpn|portflow|user_auth|ips|asse|ai|ids|ddos_inspect|ddos_clean|anti_virus|url_filter|data_filter|file_block|ha>] [**vsid** <*number4*>] [**date_range** <*string2*>]

命令描述

查看日志的内容。

参数说明

log message show	查看日志的内容。
from	必选项，设置读取日志的起始位置。
number1	数值类型，取值范围：1-2048。
to	必选项，设置读取日志的结束位置。
number2	数值类型，取值范围：1-2048。
keyword	可选项，设置检索日志的关键词。
string1	字符串类型。
level	可选项，设置当前日志的级别。
number3	数值类型，取值范围：0-7。
type	可选项，设置当前日志的类型。
mgmt|system|pf|conn|ac|secure|dpi|vpn|portflow|user_auth|ips|asse|ai|ids|ddos_inspect|ddos_clean|anti_virus|url_filter|data_filter|file_block|ha	管理日志|系统日志|包过滤日志|连接日志|访问策略/地址转换策略日志|安全日志|深度内容检测日志|VPN 日志|统计日志|用户认证日志|IPS 日志|反垃圾邮件日志|应用识别日志|IDS 日志|DDOS 检测日志|DDOS 清洗日志|防病毒日志|URL 过滤日志|内容过滤日志|文件过滤日志|高可用性日志
vsid	可选项，设置当前日志的虚系统号。
number4	数值类型，表示虚系统号。
date_range	可选项，设置查看当前日志的时间范围。
string2	字符串类型，格式为 YYYYMMDD-YYYYMMDD。其中，Y 表示年，M 表示月，D 表示日。

以下是查看当前日志的内容的示例：

TopsecOS# **log message show from** *1* **keyword** *name* **level** *3* **to** *2048* **type** system **vsid** *2* **date_range** *20131011-20141010*

log message clean <cr>

命令描述

清除日志的缓存。

log stat <cr>

命令描述

设置日志计数功能。

以下是显示日志计数功能的示例：

```
TopsecOS# log stat
log statistic:
sended:0
droped:97
failed/retryed:0
```

log stat reset <cr>

命令描述

设置日志重置计数功能。

4.6 告警

NGFW 报警模块的功能是为系统提供报警服务，通过 WEBUI 或 CLI 为各种报警事件类型指定某种报警方式，当模块调用接口时启动指定的报警方式进行处理。

NGFW 具有完善的报警提示功能，支持邮件报警、声音报警、NETBIOS 报警、控制台报警和 SNMP 报警五种报警方式：

- 邮件报警（发送电子邮件到用户指定的电子邮件地址）
- 声音报警（通过 NGFW 的内置扬声器报警）
- NETBIOS 报警（发送 NETBIOS 消息）
- 控制台报警（发送报警信息到 TOPSEC 管理中心）
- SNMP 报警（通过发送 SNMP TRAP 消息到 SNMP 陷阱主机报警）

管理员首先需要添加报警规则，设置报警的对象和参数。然后设定触发报警规则的安全事件，包括设备本身发生故障和发生管理员预先定义的安全事件两种。这样当安全事件发生时，NGFW 就会根据规则触发相应的报警信息。

告警对象是设置各种审计策略时需要匹配的对象之一，比如当内网用户在论坛发帖涉及敏感关键字或外发邮件附件涉及重要信息时，若匹配了相应的审计策略，而该策略引用了报警对象，则系统发出报警信号。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **告警**。

步骤 2 点击『添加』，弹出“报警配置”窗口，如下图所示。

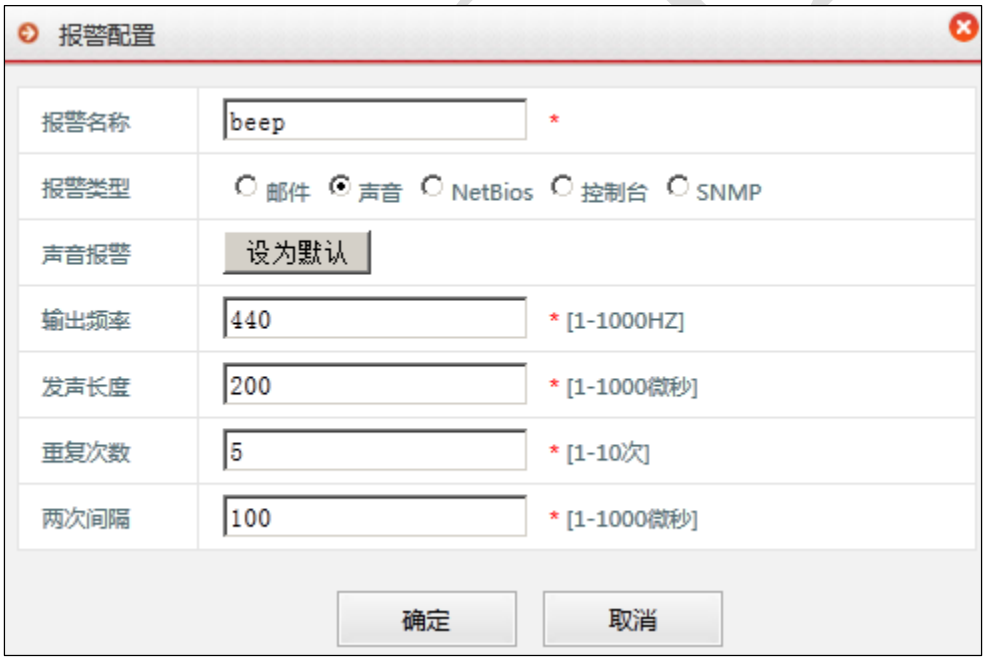
在“报警类型”选择报警方式：“邮件”、“声音”、“NetBios”、“控制台”以及“SNMP”，选择不同的报警方式将出现不同的参数项。

1）选择“邮件报警”，界面如上图所示。

在设置邮件报警信息时，各项参数的具体说明如下表所示。

参数	说明
报警名称	必选项，设置邮件报警规则的名称。
服务器地址	必选项，设置要使用的发送邮件的 SMTP 服务器的 IP 地址。
服务器端口	必选项，设置 SMTP 服务器端口号。取值范围：1-65535。
收件人地址	设置接收报警信息的电子邮件地址，如 xx@topsec.com.cn。NGFW 支持同时设置多个收件人地址。
邮件主题	设置电子邮件主题。
身份认证	如果服务器要求验证用户身份后才会发送电子邮件，则必须启动“身份认证”。其中，“  ”表示开启，“  ”表示关闭。
发件人	启动“身份认证”后才能设置该参数值。用于发送报警信息的电子邮件地址，必须是 SMTP 服务器的合法帐户。
用户密码	启动“身份认证”后才能设置该参数值。 设置发件人帐户对应的密码。

2）选择“声音报警”，界面如下图所示。

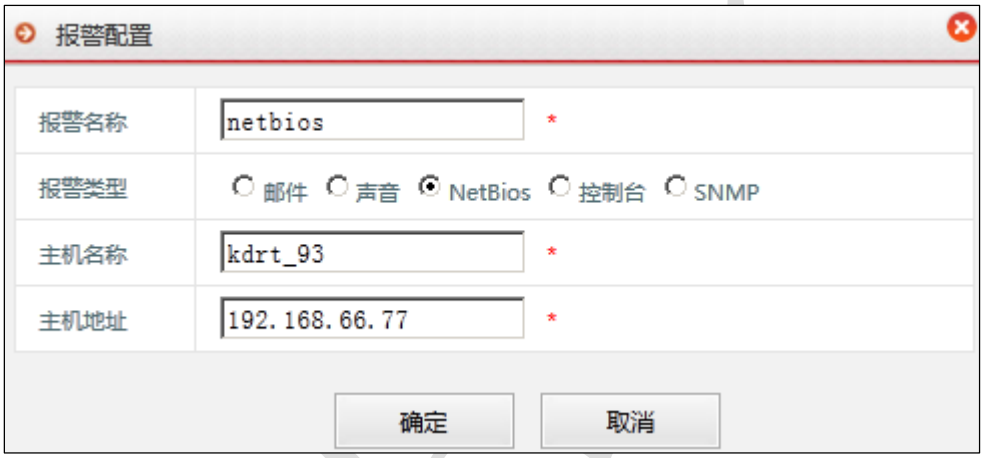


在设置声音报警信息时，各项参数的具体说明如下表所示。

参数	说明
报警名称	必选项，设置声音报警规则的名称。
声音报警（设为默认）	若希望使用 NGFW 的默认参数，可以点击【设为默认】按钮，声音报警的各参数值自动显示为默认值，即输出频率为 440HZ、报警声音长 200 微秒、报警重复 5 次、两次报警间隔时间为 100 微秒。

参数	说明
输出频率	必选项，设置报警声音的频率，单位：HZ；取值范围：1-1000；默认值：440。
发声长度	必选项，设置报警声音延续的时间，单位：微秒；取值范围：1-1000；默认值：200。
重复次数	必选项，设置报警声音重复多少次后停止，单位：次；取值范围：1-10；默认值：5。
两次间隔	必选项，设置两次声音报警之间的间隔，单位：微秒；取值范围：1-1000；默认值：100。

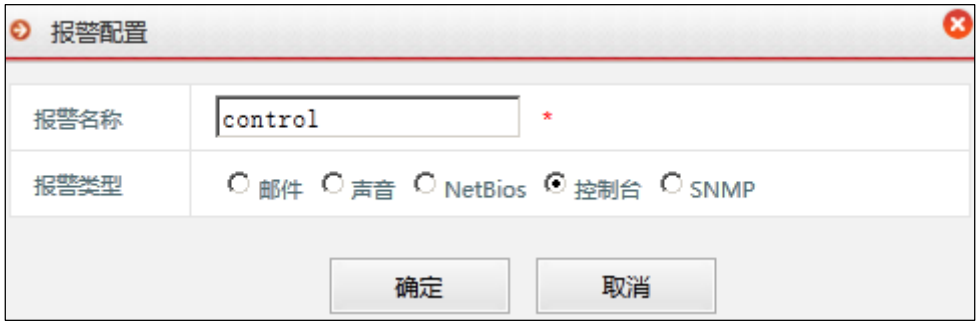
3）选择“NetBios”报警，界面如下图所示。



在设置 NetBios 报警信息时，各项参数的具体说明如下表所示。

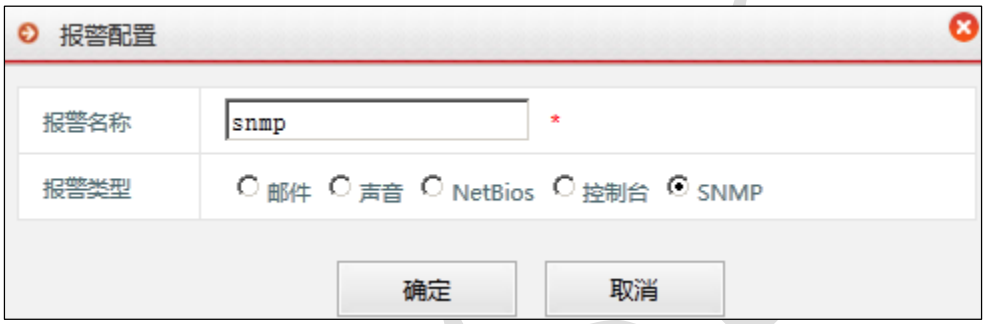
参数	说明
报警名称	必选项，设置 NetBios 报警规则的名称。
主机名称	必选项，设置接受 NetBios 报警信息的主机的真实名称。 说明： NetBios 主机命名要符合规范，只能由数字、字母、下划线“_”和中横线“-”组成，其他字符均为非法字符。
主机地址	必选项，设置接受 NetBios 报警信息的主机的 IP 地址。 说明： 接收 NetBios 消息的主机必须启动 Messenger 服务。

4）选择“控制台”报警，界面如下图所示。



在“报警名称”处填写用户指定的报警规则的名称。

5）选择“SNMP”报警，界面如下图所示。



在“报警名称”处填写用户指定的报警规则的名称，点击【确定】按钮，NGFW 即可将报警信息发送到 SNMP 陷阱主机，具体请参见 4.1.6SNMP。

说明

✧ 由于 SNMP 报警是通过发送 SNMP Trap 消息到能够接收 Trap 消息的 SNMP 陷阱主机报警，因此需要选择 **系统管理** > **SNMP**，启动 SNMP 服务，具体操作请参见 4.1.6.1SNMP 服务控制；然后设置 SNMP 陷阱主机地址，具体操作请参见 4.1.6.3SNMP 陷阱主机。

步骤 3 参数设置完成后，点击【确定】按钮完成告警规则的添加。界面如下图所示。

上图中规则的红色框部分为触发该报警规则的安全事件，蓝色框部分的内容为该报警规则的参数。新添加的规则没有和任何安全事件关联，关于将报警规则与安全事件关联的设置具体请参见 设置触发报警的安全事件。

步骤 4 设置触发报警的安全事件。

报警安全事件包括设备本身的故障和管理员定义的安全事件，如：

- 管理：指管理员对设备进行配置。
- 系统：用户登录、管理设备，系统启动或停止、系统升级、管理员进行日志设置、HA 状态切换、网络环路、网卡掉线等事件。
- 安全：系统根据 IDS 和 IPS 攻击策略监测到攻击发生。
- 策略：在添加访问控制策略时选择“系统报警”选项后，每当有匹配的访问控制策略起效时将会报警。
- 通讯：通过设备建立会话、会话断开、IP 地址冲突等关键通信事件。
- 硬件：系统 CPU、内存资源不足。
- 容错：系统恢复。
- 测试：用户对报警规则进行测试。

当成功添加一条告警规则到天融信下一代防火墙后，还需要设置触发报警的安全事件。设置方法是在已添加的告警规则的右侧窗口选择相应的安全事件，如下图所示。

在上图报警规则中，安全事件选择了“系统”、“硬件”和“容错”作为可触发报警的安全事件，在“分类”中可以看出报警方式采用的是声音报警。这条规则成功设置后，当系统出现了“系统”、“硬件”的事件时，就会触发一个报警，天融信下一代防火墙会通过声音报警来提醒管理员。

CLI 方式配置

alarm event set <manage|system|security|policy|communication|hardware|recover|noticetest| all> <**noticeid** <*number*>| **noticename** <*string*>| <empty>>

命令描述

根据类别设置事件的报警方式。

参数说明

alarm event set	必选项，设置事件的报警方式。
manage|system|security|policy|communication|hardware|recover|noticetest|all	manage 表示管理系统时报警，system 表示系统报警，security 表示安全报警，policy 表示策略报警，communication 表示通信报警，hardware 表示硬件报警，recover 表示恢复报警，noticetest 表示测试报警，all 表示所有事件都报警。
noticeid	必选项，设置报警方式的 ID 号。
number	数值类型，表示报警方式 ID 号。
noticename	必选项，设置报警方式的名称。
string	字符串类型，表示报警方式名称。
empty	表示不报警。

以下是根据类别设置事件的报警方式的示例：

设置报警规则，当硬件发生变化时，采用 beep1 报警（beep1 是定义的声音报警方式）。

```
TopsecOS#alarm event set hardware noticename beep1
```

alarm event show

<manage|system|security|policy|communication|hardware|recover|noticetest|all>

命令描述

查看某报警事件。

参数说明

alarm event show	必选项，查看某报警事件。
manage|system|security|policy|communication|hardware|recover|noticetest|all	manage 表示管理系统时报警，system 表示系统报警，security 表示安全报警，policy 表示策略报警，communication 表示通信报警，hardware 表示硬件报警，recover 表示恢复报警，noticetest 表示测试报警，all 表示查看所有报警事件。

以下是查看安全报警事件的示例：

```
TopsecOS# alarm event show security

alarm event set security noticeid '9044 9039'
```

alarm event show <cr>

命令描述

查看系统中所有的报警事件。

以下是查看系统中所有的报警事件的示例：

```
TopsecOS# alarm event show
alarm event set system noticeid '9044'
alarm event set security noticeid '9044 9039'
alarm event set policy noticeid '9039'
alarm event set communication noticeid '9044'
alarm event set recover noticeid '9044 9039'
```

alarm notice add <beep> **name** <*string*> **freq** <*number1*> **length** <*number2*> **reps** <*number3*> **delay** <*number4*>

alarm notice add <beep> **name** <*string*> default <cr>

命令描述

添加一个声音报警。

参数说明

alarm notice add	添加一个声音报警。
beep	表示报警方式为声音报警。
name	必选项，设置报警名称。
string	字符串类型，表示报警名称。
default	使用声音报警的默认值，选择此项后不再需要设置下面的参数。
freq	可选项，设置声音输出频率。
number1	数值类型，表示声音输出频率，单位：HZ；取值范围：1-1000。
length	可选项，设置声音长度。
number2	数值类型，表示声音长度，单位：微秒；取值范围：1-1000。
reps	可选项，设置声音的重复次数。
number3	数值类型，表示声音重复次数，单位：次；取值范围：1-100。
delay	可选项，设置两次发声的间隔。
number4	数值类型，表示发声间隔，单位：微秒；取值范围：1-1000。

使用说明：

声音报警属性设为 default 时，各参数默认值见下表。

freq	440HZ
length	200 微秒
reps	5 次
delay	100 微秒

以下是添加声音报警的示例：

添加一个缺省的声音报警 beep1。

```
TopsecOS# alarm notice add beep name beep1 default
```

alarm notice add <mail> **name** <*string1*> **srvaddr** <*ipaddress*> **srvport** <*number*> **mailaddr** <*string2*> **auth** <on|off> [**username** <*string3*> **password** <*string4*>] [**subject** <*string5*>]

命令描述

添加一个邮件报警。

参数说明

alarm notice add	添加一个邮件报警。
mail	表示报警方式为邮件报警。
name	必选项，设置报警名称。
string1	字符串类型，表示报警名称。
srvaddr	必选项，设置要使用的发送邮件的 SMTP 服务器的 IP 地址。
ipaddress	字符串类型，表示 IP 地址，格式为 192.168.83.6。
srvport	必选项，设置 SMTP 发件服务器的端口。
number	数值类型，表示端口号。
mailaddr	必选项，设置接收报警邮件的邮件帐户。
string2	字符串类型，表示电子邮件地址，例如 abc@topsec.com.cn。
auth	必选项，设置邮件服务器要求进行认证。
on|off	是|否
username	可选项，当邮件服务器需要认证时，输入用户名。当“auth”设置为 off 时不需要设置该项。
string3	字符串类型。
password	可选项，当邮件服务器需要认证时，输入用户密码。当“auth”设置为 off 时不需要设置该项。
string4	字符串类型。
subject	可选项，设置报警邮件的主题。
string5	字符串类型，表示邮件主题。

以下是添加邮件报警的示例：

添加一个发送到 user@topsec.com.cn 的邮件报警 mail1，SMTP 邮件服务器的 IP 地址为 192.168.1.2，端口为 25，设置报警邮件主题为“邮件报警”。

TopsecOS# **alarm notice add** mail **name** *mail1* **srvaddr** *192.168.1.2* **srvport** *25* **mailaddr** *user@topsec.com.cn* **auth** off **subject** *邮件报警*

alarm notice add <netbios> **name** <*string1*> **hostname** <*string2*> [**ipaddr** <*ipaddress*>]

命令描述

添加一个 netbios 报警。

参数说明

alarm notice add	添加一个 netbios 报警。
netbios	表示报警方式为 netbios 报警。
name	必选项，设置报警名称。
string1	字符串类型，表示报警名称。
hostname	必选项，设置接收报警信息的主机名称。
string2	字符串类型，表示 netbios 主机名称。netbios 主机命名必须符合规范，只能由数字、字母、下划线“_”和中横线“-”组成，其他字符均为非法字符。
ipaddr	可选项，设置接收报警信息的主机 IP 地址。
ipaddress	字符串类型，表示 IP 地址，格式为 192.168.83.6。

以下是添加 netbios 报警的示例：

添加一个发送到 host1（IP：192.168.1.6）的 netbios 报警 netbios1。

TopsecOS# **alarm notice add** netbios **name** *netbios1* **hostname** *host1* **ipaddr** *192.168.1.6*

alarm notice add <console|snmp> **name** <*string*>

命令描述

添加一个控制台或 SNMP 报警。

参数说明

alarm notice add	必选项，添加一个报警。
console|snmp	表示报警方式为控制台报警或者 SNMP 报警。
name	必选项，设置报警名称。
string	字符串类型，表示报警名称。

以下是添加一个控制台报警 console1 的示例：

```
TopsecOS# alarm notice add console name console1
```

alarm notice delete name <*string*>| **id** <*number*>

命令描述

删除一个报警。

参数说明

alarm notice delete	删除一个报警。
name	必选项，指定要删除的报警的名称。
string	字符串类型，表示报警名称。
id	必选项，指定要删除的报警的 ID 号。
number	数值类型，表示 ID 号。

使用说明：

只有当该报警规则的报警事件为空时才可以删除，否则会提示错误信息。

以下是删除指定报警的示例：

删除报警 beep1。

```
TopsecOS# alarm notice delete name beep1
```

alarm notice clean <cr>

命令描述

清除所有报警规则。只有当报警规则中包含的报警事件均为空时才可以操作成功。

alarm notice show [**name** <*string*>]| [**id** <*number*>]

命令描述

查看报警。

参数说明

alarm notice show	查看报警。
name	可选项，指定要查看的报警的名称。

string	字符串类型，表示报警名称。
id	可选项，指定要查看的报警的 ID 号。
number	数值类型，表示 ID 号。

以下是查看报警的示例：

查看名称为 mail1 的报警。

```
TopsecOS# alarm notice show name mail1
```

查看所有的报警。

```
TopsecOS# alarm notice show
```

alarm notice test <cr>

命令描述

测试报警。

使用说明：

为了方便用户，天融信下一代防火墙提供了报警测试功能。成功添加报警方式和设置触发报警的安全事件后，用户可以通过测试来验证报警规则的有效性。

4.7 高可用性

4.7.1 简介

在数据通信过程中，各种软件或硬件错误都可能导致网络连接异常中断，造成数据传输失败或防护网络功能失效。如下图所示，所有的网络流量都从 NGFW 设备进行转发，如果 NGFW 设备故障，整条链路的业务将中断。

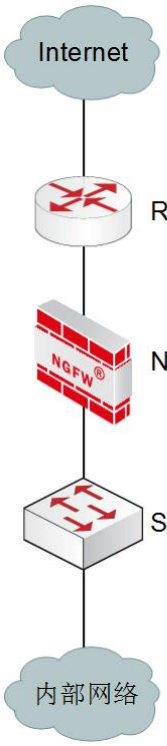


图 4-9 单链路网络示意图

为了保证网络的可靠性，NGFW 提供了冗余备份功能，以确保在 NGFW 通信线路或设备故障时，也能保障业务网络数据的正常运转，提高设备的可用性。

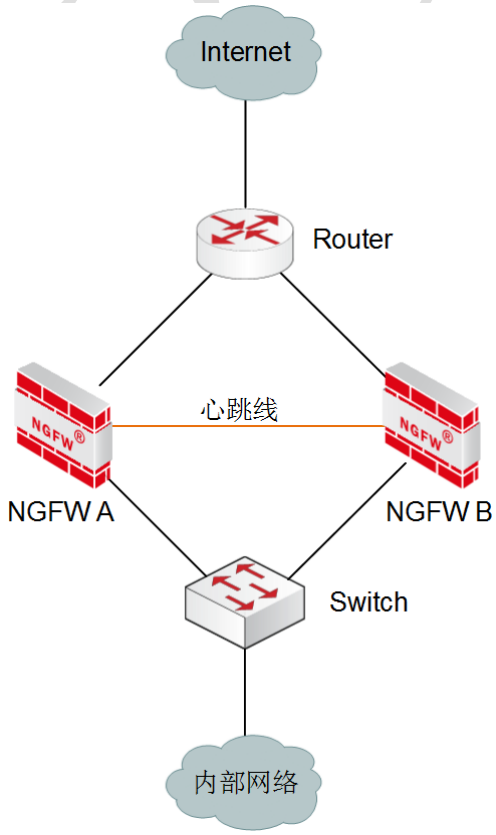


图 4-10 双链路网络示意图

如上图所示，NGFW A 和 NGFW B 之间通过心跳口同步状态信息、连接信息和配置信息。

NGFW 通过配置热备组实现高可用性，同一 NGFW 设备支持多个热备组，可在不同的热备组中作为主设备或者备设备，如下图所示。如果配置为双机热备工作场景，仅需配置热备组 1 即可，如果配置为负载均衡工作场景，则需要配置热备组 1 和热备组 2。

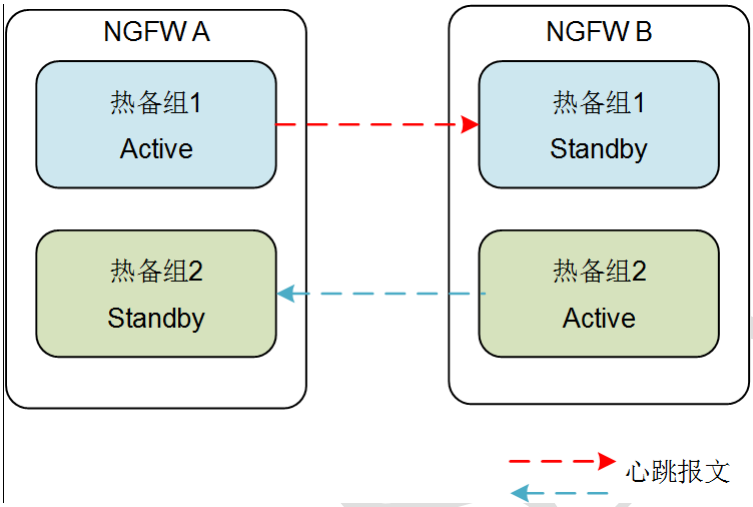


图 4-11 热备组示意图

热备组中的设备有如下 4 种工作状态：

- INIT：初始化状态，热备组未启用。
- ACTIVE：主用状态，当前设备为主用设备。
- STANDBY：备用状态，当前设备为备用设备。
- PREEMPT：抢占状态，当前设备已从故障中恢复，且已启用抢占模式，如果抢占延时时间内，设备正常工作，则设备将抢占为主用状态。

NGFW 的高可用性支持 3 种工作模式：主备模式（AS，Active-to-Standby）、负载均衡模式（AA，Active-to-Active）、连接保护模式（SP，Session Protect）。

主备模式

NGFW 以主备模式部署时，由 2 台 NGFW 设备组成热备组，设备有 2 种工作状态主设备和备设备，有一台主设备处于工作状态，另外一台设备处于备份状态。

如下图所示，主备模式由正常情况到故障情况的工作流量。

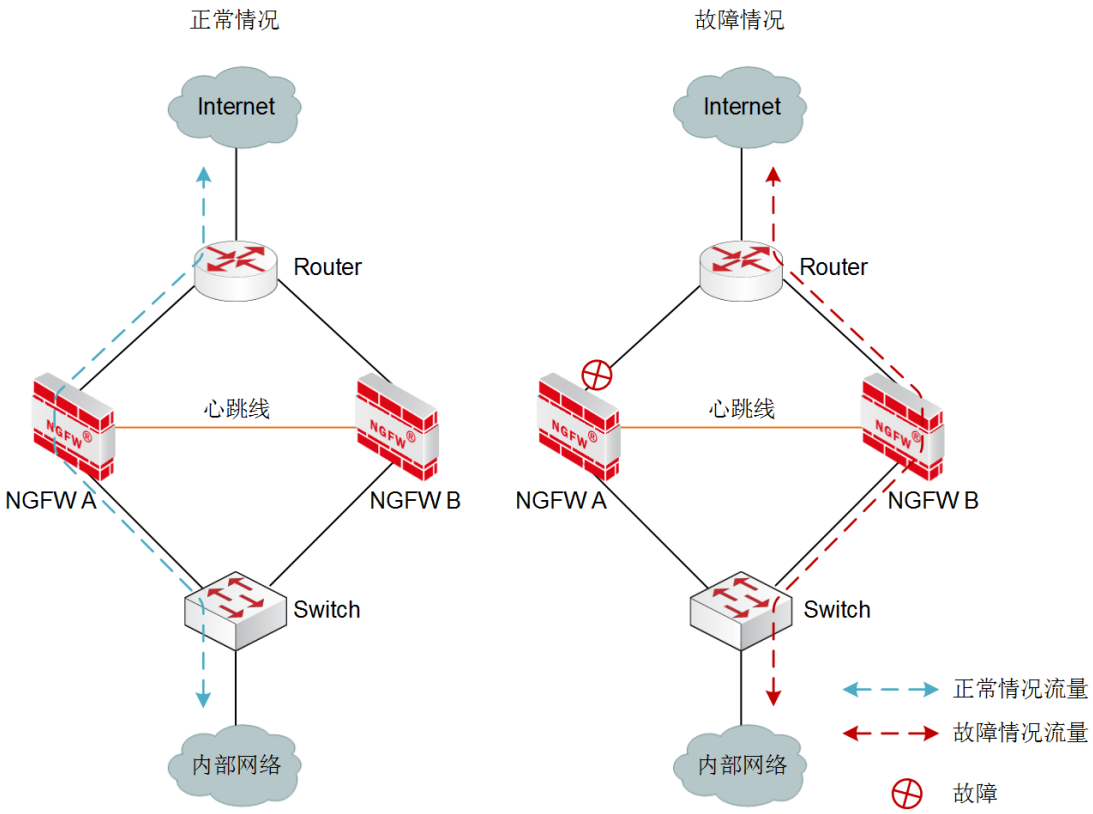


图 4-12 双机热备工作场景示意图

1）正常情况下，主设备承担报文的转发、检测、清洗或回注等任务，主设备通过心跳口实时同步处于工作状态的 NGFW 的状态和配置信息到备设备。

2）当主设备的软件或硬件（不包括心跳口）出现故障时，处于备份状态的 NGFW 立即对用户完全透明的情况下接替主设备的工作。

3）当主设备故障恢复时，则根据 NGFW 是否为抢占模式，决定设备是否由备设备切换回主设备。热备组配置为抢占模式时，主设备故障恢复后，恢复原来的主设备为工作状态，为了防止因设备运行不稳定，导致其热备组中设备的角色频繁切换，需要配置适当的延迟时间，主设备工作稳定后再从备设备切换回主设备。

负载均衡模式

NGFW 以负载均衡模式部署时，有 2 种工作状态主设备和备设备。NGFW 设备组成 2 个热备组，每个热备组中有一台主设备处于工作状态，另外一台设备处于备份状态。

如下图所示，负载均衡工作场景正常情况到故障情况的工作流量。

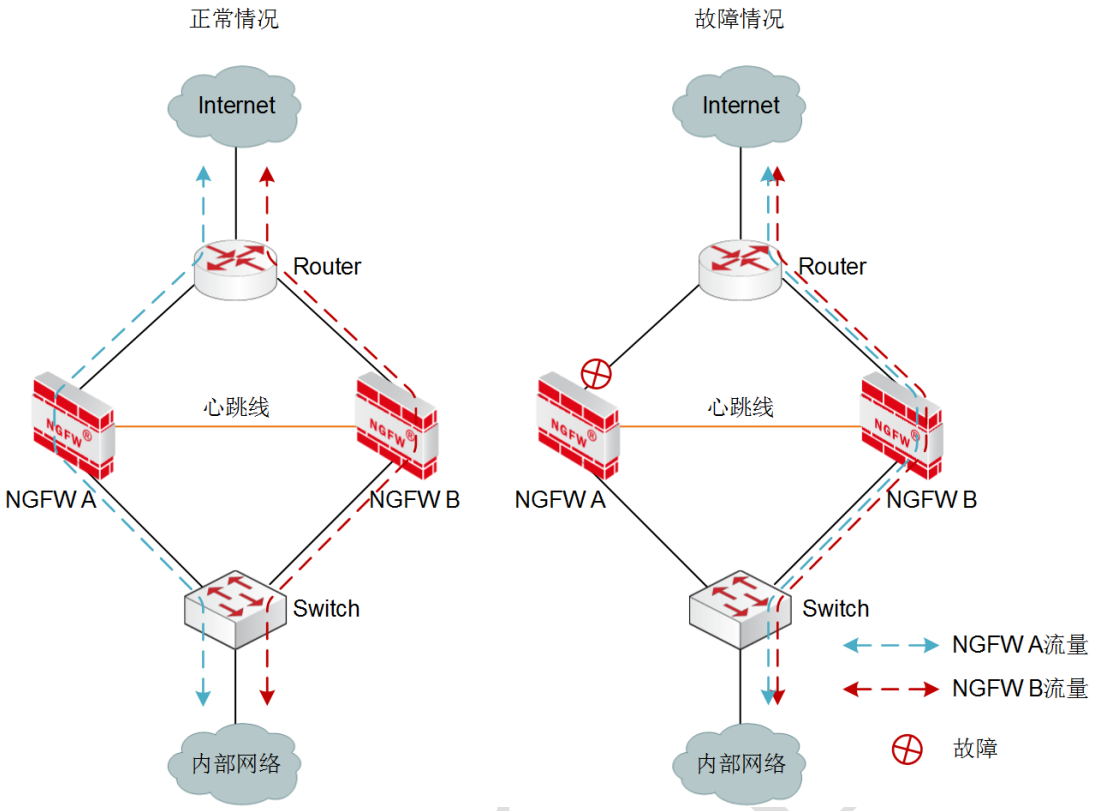


图 4-13 负载均衡工作场景示意图

- 正常情况下，热备组的 2 台设备独立工作，各自承担报文的转发、检测、清洗或回注等任务，通过心跳口相互同步对方的状态和配置信息，互为对方的备设备。
- 当其中一台设备的软件或硬件（不包括心跳口）出现故障时，处于同一热备组中的另外一台 NGFW 立即对用户完全透明的情况下接替故障设备的工作。
- 当主设备故障恢复时，则根据 NGFW 是否为抢占模式，决定设备是否由备设备切换回主设备。热备组配置为抢占模式时，主设备故障恢复后，恢复原来的主设备为工作状态，为了防止因设备运行不稳定，导致其热备组中设备的角色频繁切换，需要配置适当的延迟时间，主设备工作稳定后再从备设备切换回主设备。

连接保护模式

在连接保护模式下，所有防火墙均处于工作状态并且在网络部署层面相互独立，不区分主备，如下图所示。

- 当两台防火墙均正常工作时，由上下游的设备进行选路。如果内部网络在发送数据报文时，选择从 NGFW A 发送，在 NGFW A 上将建立数据报文的连接，如果从网络中返回的数据报文选择从 NGFW B 上返回，在没有开启连接保护模式时，NGFW B 上没有建立该网络连接，将丢弃该报文；在开启连接保护模式后，NGFW A 通过心跳口将连接信息同步到 NGFW B 上，将该连接的报文正常转发到内部网络。
- 当其中一台防火墙发生故障时，上下游设备经过协商后会将其上的数据流通过另外的防火墙转发。

NGFW 工作在连接保护模式下支持透明和路由模式。连接保护模式下不需要添加热备组，只需配置本地和对端地址即可。

连接保护模式下的部署示意图如下所示。

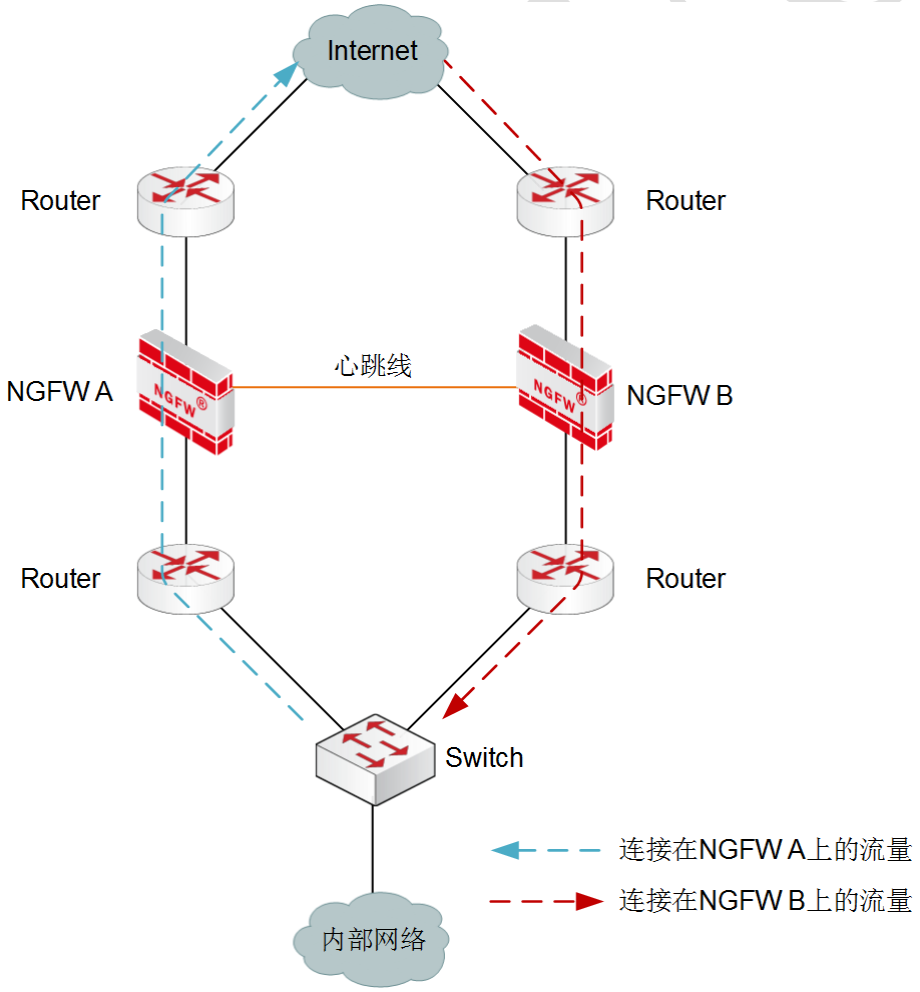


图 4-14 NGFW 连接保护模式示意图

说明

- ✧ 高可用性中的防火墙，必须使用心跳口交换状态监测及探测信息，NGFW 上的任何以太网接口都可以做为心跳接口。
- ✧ 利用高可用性进行冗余备份时，两台防火墙型号、软件版本必须一致，否则在其中一台故障时，无法保证将业务正常切换到另外一台设备。

4.7.2 配置主备模式

在配置主备模式前，需要先进行如下步骤：

- ➢ 配置心跳口属性。所有心跳口的地址必须配置在同一网段，而且接口属性必须要勾选“非同步地址”选项，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。
- ➢ 配置其他通信接口。互为备份的接口必须配置相同的 IP 地址。
- ➢ 配置双机热备的相关参数，并启用双机热备功能。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **高可用性**。

步骤 2 配置全局参数。

在配置全局属性时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“主备模式”。
心跳口	设置同步主设备工作状态的通信接口。
本端 IP	设置本端设备心跳口的 IP 地址。IP 地址必须为心跳口上已经配置的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。 说明： 对端 IP 地址和本地 IP 地址必须在同一子网内。

全局参数设置完成后，点击【应用】按钮保存配置。

步骤 3 配置热备组参数。

1）点击“管理组设置”下的『添加』，弹出“添加”窗口。

在配置 NGFW 在热备组中的属性时，各项参数的具体说明如下表所示。

参数	说明
组 ID	设置 NGFW 通信接口（除心跳口以外）所属热备组的组号，该组号用于确定处于同一热备组的设备，取值范围：1-255。 说明： 1）处于同一热备组的 NGFW 设备组 ID 需配置相同。 2）热备组的虚拟 MAC 地址由 NGFW 的组号映射而生成。
角色	设置本机在热备组中所处的工作状态，可选项：主、备。 主：管理组处于工作状态 备：管理组处于备份状态
抢占	设置是否开启“抢占”模式，即作为主设备的本机出现通信故障时，热备组中的其他设备担任主设备的角色，当本机的故障解除后，是否重新夺回主设备的地位。 说明： 只有当主设备与从设备相比有明显的性能差异时，才需要配置主设备工作在“抢占”模式，否则，当原主设备恢复工作时主从设备的再次切换浪费系统资源。
抢占延时	设置抢占的推迟时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。单位：秒；取值范围：1-120。
监控接口	从可用接口中选择接口添加到管理组，并监控其工作状态。

说明

✧ 防火墙工作在主备模式时，只能添加一个管理组。

2）点击【确定】按钮完成本机在热备组中角色属性的设置；点击【取消】按钮撤销本次操作。

步骤 4 启动双机热备功能。

点击【启动】按钮，可以启动 NGFW 的双机热备功能。

步骤 5 同步配置。

点击【立即同步】按钮，可将本机除 HA 之外的所有的配置信息同步到对端机上。

步骤 6 停止双机热备功能。

点击【停止】按钮，可以停止 NGFW 的双机热备功能。

CLI 方式配置

步骤	配置命令	配置说明
1	**ha mode set** aa	设置 HA 为负载均衡模式。
2	**ha interface add** <*string*> **local** <*ipadress1*> **remote** <*ipadress2*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha group** <*number1*> **mode** <master|backup>	添加热备组，并配置设备在热备组中的角色为主设备/备设备。
4	**ha group** <*number*> **preempt** <enable|disable>	（可选）设置热备组是否启用抢占模式。
5	**network interface** <*string*> **tgid** <*number*>	将接口添加到管理组。
6	**ha group** <*number1*> **preempt delay** <*number2*>	（可选）设置热备组的抢占延时时间。
7	**ha start** <cr>	启动 HA 功能。
8	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

4.7.3 配置负载均衡模式

在配置负载均衡模式前，需要先进行如下步骤：

- 配置心跳口属性。所有心跳口的地址必须配置在同一网段，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。
- 配置其他通信接口。互为备份的接口必须配置相同的 IP 地址。
- 配置双机热备的相关参数，并启用双机热备功能。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **高可用性**。

步骤 2 配置全局参数。

在配置全局属性时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“负载均衡”。
心跳口	设置同步主设备工作状态的通信接口。
本端 IP	设置本端设备心跳口的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。 说明： 对端 IP 地址和本地 IP 地址必须在同一子网内。

全局参数设置完成后，点击【应用】按钮保存配置。

步骤 3 配置热备组参数。

1）点击“管理组设置”下的『添加』，弹出“添加”窗口。

在配置 NGFW 在热备组中的属性时，各项参数的具体说明如下表所示。

参数	说明
组 ID	设置 NGFW 通信接口（除心跳口以外）所属热备组的组号，该组号用于确定处于同一热备组的设备，取值范围：1-255。 说明： 1）处于同一热备组的 NGFW 设备组 ID 需配置相同。 2）热备组的虚拟 MAC 地址由 NGFW 的组号映射而生成。
角色	设置本机在热备组中所处的工作状态，可选项：主、备。 主：管理组处于工作状态 备：管理组处于备份状态
抢占	设置是否开启“抢占”模式，即作为主设备的本机出现通信故障时，热备组中的其他设备担任主设备的角色，当本机的故障解除后，是否重新夺回主设备的地位。 说明： 只有当主设备与从设备相比有明显的性能差异时，才需要配置主设备工作在“抢占”模式，否则，当原主设备恢复工作时主从设备的再次切换浪费系统资源。
抢占延时	设置抢占的推迟时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。单位：秒；取值范围：1-120。
监控接口	从可用接口中选择接口添加到管理组，并监控其工作状态。

说明

✧ 防火墙工作在主备模式时，可以添加两个管理组。

2）点击【确定】按钮完成本机在热备组中角色属性的设置；点击【取消】按钮撤销本次操作。

步骤 4 启动双机热备功能。

点击【启动】按钮，可以启动 NGFW 的双机热备功能。

步骤 5 同步配置。

点击【立即同步】按钮，可将本机除 HA 之外的所有的配置信息同步到对端机上。

步骤 6 停止双机热备功能。

点击【停止】按钮，可以停止 NGFW 的双机热备功能。

CLI 方式配置

步骤	配置命令	配置说明
1	**ha mode set** aa	设置 HA 为负载均衡模式。
2	**ha interface add** <*string*> **local** <*ipadress1*> **remote** <*ipadress2*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha group** <*number1*> **mode** master	添加热备组，并配置设备在热备组 1 中的角色为主设备。
4	**ha group** <*number*> **mode** backup	添加热备组，并配置设备在热备组 2 中的角色为备设备。
5	**network interface** <*string*> **tgid** <*number*>	将接口添加到管理组。
6	**ha group** <*number*> **preempt** <enable|disable>	（可选）设置热备组是否启用抢占模式。
7	**ha group** <*number1*> **preempt delay** <*number2*>	（可选）设置热备组的抢占延时时间。
8	**ha start** <cr>	启动 HA 功能。
9	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

4.7.4 配置连接保护模式

在配置连接保护模式前，需要先进行如下步骤：

- 配置心跳口属性。所有心跳口的地址必须配置在同一网段，否则心跳口的 IP 地址信息会在主从设备运行状态同步时被对方覆盖。
- 配置其他通信接口。互为备份的接口必须配置相同的 IP 地址。
- 配置双机热备的相关参数，并启用双机热备功能。

WEBUI 方式配置

步骤 1 选择 **系统管理** > **高可用性**。

步骤 2 配置全局参数。

在配置全局属性时，各项参数的具体说明如下表所示。

参数	说明
模式	设置为“连接保护”。
心跳口	设置同步主设备工作状态的通信接口。
本端 IP	设置本端设备心跳口的 IP 地址。
对端 IP	设置对端设备心跳口的 IP 地址。 说明： 对端 IP 地址和本地 IP 地址必须在同一子网内。

点击【应用】按钮完成连接保护功能的全局配置。

步骤 3 启用连接保护模式。

点击【启动】按钮即可启动连接保护模式。

步骤 4 手工同步配置。

当主网关或从网关配置发生变更后，手工同步配置可以保证主从网关配置的一致性。

点击【立即同步】按钮，可以从本机同步配置到对端机上，包括除 HA 之外的所有配置信息。

步骤 5 停止连接保护模式。

点击【停止】按钮，可以停止连接保护模式。

CLI 方式配置

步骤	配置命令	配置说明
1	**ha mode set** sp	设置 HA 为连接保护模式。
2	**ha interface add** <*string*> **local** <*ipadress1*> **remote** <*ipadress2*>	设置 HA 的心跳口，本端 IP 地址及对端 IP 地址。
3	**ha start** <cr>	启动 HA 功能。
4	**ha sync-config-to-peer** <cr>	HA 同步，同步本端配置到对端。

4.7.5 高可用性相关命令

ha clean <cr>

命令描述：

清除 HA 的配置信息。

ha interface add <*string*> **local** <*ipaddress1*> **remote** <*ipaddress2*>

命令描述：

设置心跳接口。

使用 **ha interface delete** <*string*>命令删除心跳口配置。

参数说明：

ha interface add	设置设备的心跳口。
string	字符串类型，表示接口名称。
local	本端设备。
ipaddress1	本端设备的 IP 地址，A.B.C.D 形式。
remote	对端设备。
ipaddress2	对端设备的 IP 地址，A.B.C.D 形式。

以下是设置心跳口的示例：

设置 feth3 为心跳口，本端的 IP 地址为 192.168.1.3，对端的 IP 地址为 192.168.1.6。

TopsecOS# **ha interface add** feth3 **local** 192.168.1.3 **remote** 192.168.1.6

ha group <*number*> **delete** <cr>

命令描述：

删除备份组。

参数说明：

ha group	配置热备组的主从模式
number	AS 模式下的管理组号，取值范围：1-255。

ha group <*number*> **mode** <master|backup>

命令描述：

用于防火墙主备工作状态切换，执行该命令之前需开启防火墙的 HA 功能。

如果 HA 功能已经启用，切换主备工作状态前，需要先停止 HA 功能。

参数说明：

ha group	配置热备组的主从模式。
number	AS 模式下的管理组号，取值范围：1-255。
mode	防火墙工作状态设置。
master|backup	主设备|备设备。

ha group <*number*> **preempt** <enable|disable>

命令描述：

配置备份组抢占模式。用户应当首先设定 HA 的工作模式，然后再设置该参数，否则会有错误提示信息。

参数说明：

ha group	必选项，HA 备份组 ID。
number	数值类型，表示 ID 号，取值范围：1-255。
preempt	必选项，HA 抢占设置。
enable|disable	抢占|不抢占

以下是进行备份组抢占配置的示例：

设置备份组抢占。

```
TopsecOS# ha vrid 1 preempt enable
```

ha group <*number1*> **preempt delay** <*number2*>

命令描述：

设置抢占的延时时间，以防止本机运行不稳定而导致其热备组中设备的角色频繁切换。

参数说明：

group	必选项，HA 备份组 ID。
number1	数值类型，表示 ID 号，取值范围：1-255。
preempt	必选项，HA 抢占设置。
number2	抢占延时时间，单位：秒；取值范围：1-120。

以下是进行备份组抢占配置的示例：

设置备份组抢占延时时间为 100s。

```
TopsecOS# ha group 1 preempt delay 100
```

ha mode set <aa|as|sp>

命令描述：

配置 HA 模式。

参数说明：

mode	必选项，HA 模式配置。
aa|as|sp	负载均衡模式|双机热备模式|连接保护模式

以下是进行 HA 模式配置的示例：

配置 HA 模式为负载均衡模式。

```
TopsecOS# ha mode set aa
```

配置 HA 模式为双机热备模式。

```
TopsecOS# ha mode set as
```

ha show <config|status|session-statistic>

命令描述：

查看 HA 的配置信息。

参数说明：

show	必选项，指定查看 HA 的配置信息。
config	查看当前 HA 的参数配置。
status	查看本设备 HA 的运行状态。
session-statistic	查看备份组会话的统计信息。

以下是查看 HA 的配置信息的示例：

查看当前 HA 参数配置。

```
TopsecOS# ha show configuration
ha clean
ha mode set aa
ha group 255 mode master
ha group 255 preempt enable
ha group 255 preempt-delay 10
```

查看当前 HA 参数配置。

```
TopsecOS #ha show status
```

```
Group 255
State          Preempt      Priority     Interface
INIT           enable       65000
```

查看备份组的会话统计信息。

```
TopsecOS#ha show session-statistic
ha_statistic_config.ha_HA_get_pktbuff_DP_enter is 0
ha_statistic_config.ha_HA_send_pkt_DP_enter is 0
ha_statistic_config.xmit_error_statistic is 0
ha_statistic_config.ha_HA_COMM_bulidDpMessage_enter is 0
ha_statistic_config.ha_HA_COMM_bulidDpMessage_success is 0
ha_statistic_config.ha_HA_COMM_recvDpMessage_call_session is 0
ha_statistic_config.ha_HA_COMM_recvDpMessage_enter is 0
ha_statistic_config.ha_HA_COMM_sendDpMessage_enter is 0
ha_statistic_config.ha_HA_COMM_sendDpMessage_success is 0
```

ha start <cr>

命令描述：

启动 HA。HA 默认为停止状态，需要手工启动。

可使用 **ha stop** <cr>命令停用 HA。

ha sync-config-to-peer <cr>

命令描述：

HA 同步（从同步配置到对端设备上）。

使用说明：

HA 同步前需要先使用 **ha start** 命令启动 HA 功能。

以下是进行 HA 同步的示例：

同步配置到对端机上。

```
TopsecOS# ha sync-config-to-peer
```

network interface <*string*> **tgid** <*number*>

命令描述：

将接口添加到管理组。

参数说明：

network interface	将接口添加到管理组。
string	查看当前 HA 的参数配置。
tgid	必选项，设置高可用性管理组 ID。
number	数值类型，取值范围：0-255，0 表示取消 tgid。

以下为添加接口到管理组的示例：

```
TopsecOS#network interface feth11 tgid 1
```

查看管理组的监视接口的示例：

```
TopsecOS# ha show status
HA-Status: ha disable
Heartbeat-Local IP: 0.0.0.0

Group 1
State          Preempt       Priority      Interface
INIT           enable        65000         feth11
```

5 用户管理

用户是互联网活动主体，是 NGFW 防护网络的目标对象。NGFW 提供了用户统一管理和认证系统，不仅可作为认证服务器验证用户合法性，还可联动第三方 Radius、Ldap 以及 Tacacs 认证服务器验证用户的合法性，更进一步实现基于用户进行细粒度访问控制的管理维度。其中，NGFW 上的用户包括：本地用户和接入用户。

- 本地用户：NGFW 所防护内网中的活动主体，如企业内部员工。通过在防火墙上添加本地用户信息，本地用户访问网络资源时，NGFW 可基于用户细粒度控制用户的网络行为。
- 接入用户：外部网络中通过 NGFW 访问内部网络资源的活动主体，如企业出差员工、合作伙伴等。接入用户需通过 NGFW 的认证，才能根据其权限访问内网资源。

本章内容主要包括：

- 用户管理：主要介绍如何在 NGFW 上管理用户信息。
- 认证服务器：主要介绍如何使 NGFW 与外部认证服务器建立连接。
- 门户配置：主要介绍如何配置用户向 NGFW 认证的登录界面。
- PKI：主要介绍如何配置 NGFW 的 PKI 功能。

5.1 用户管理

用户管理模块提供全面的用户管理功能。用户由 NGFW 本地认证时（关于认证的介绍具体请参见 5.2 认证服务器），需管理员在 NGFW 本地用户数据库中添加用户信息，NGFW 对用户进行认证和授权；用户由第三方认证服务器认证时，NGFW 向第三方认证服务器转发用户认证请求并对认证通过的用户进行授权。

为实现对用户进行灵活、分类、规范化管理，NGFW 提供了基于用户组集中管理用户的机制，因此，“用户管理”功能包括用户组管理和用户管理两部分。

5.1.1 管理用户组

用户组是用户的集合，管理员可以根据用户间的联系将若干用户分为一个用户组，如可以将区域、部门、访问规则或认证方式等相同的用户添加到同一用户组中。

NGFW 采用树形结构的用户组管理系统。下面介绍如何管理用户组。

WEBUI 方式配置

步骤 1 选择 **用户管理** > **用户管理**。界面左侧为用户组管理界面，点击某个用户组，界面右侧的列表中将显示此用户组中包含的子组和用户信息。

步骤 2 添加新用户组。

1）点击用户组管理界面区域的『添加』，如下图所示。

在添加用户组时，各项参数的具体说明如下表所示。

参数	说明
用户组名	必选项。设置用户组的名称，可为汉字、数字和字母的组合。
描述	设置用户组的描述信息。
所属用户组	设置用户组隶属的父组。
选择成员	设置该用户组所包含的成员。 说明： 1）“成员”中显示 NGFW 中添加的所有用户和用户组信息，“已选成员”中显示添加到该用户组的用户和用户组信息。管理员可以在“成员”中选择一个或多个用户，点击【>】添加到“已选成员”中。 2）在搜索栏中输入关键字，点击“🔍”图标可以快速查找某个成员。

2）设置完成后，点击【确定】按钮，完成新用户组的添加。

步骤 3 查找用户组。

在查找框中输入待查找组名称的部分关键字，然后点击“🔍”图标，则名称中包含该关键字的用户组将被筛选出来。

CLI 方式配置

user manage group add name <*string1*> [**address-name** <*string2*>] [**area-name** <*string3*>] [**auth-server** <*string4*>] [**description** <*string5*>] [**group** <*string6*>] [**inherit-policy** <yes|no>] [**notice-url** <*string7*>] [**timer-name** <*string8*>] [**force-inherit** <yes|no>]

命令描述：

添加用户组。

参数说明：

user manage	添加用户组。

group add	
name	必选项，设置用户组的名称，可为字母和数字的组合。
string1	字符串类型。不能超过 31 个字节，一个汉字占两个字节空间；一个字母占一个字节空间。
address-name	可选项，限定用户组中用户所使用的 IP 地址范围。
string2	字符串类型，表示 IP 地址对象名称。
area-name	可选项，限定用户组中用户访问 NGFW 的来源区域。
string3	字符串类型，表示区域对象名称。
auth-server	可选项，设置为该用户组中用户认证的认证服务器。
string4	字符串类型，表示认证服务器名称。
description	可选项，设置描述用户组的信息。
string5	字符串类型，描述信息。
group	可选项，设置用户组隶属的父组名称。
string6	字符串类型。表示父组名称。
inherit-policy	可选项，设置用户组是否继承父组的属性。
yes|no	是|否，默认选项为是。
notice-url	可选项，设置用户通过 NGFW 认证后，弹出的通知消息页面的 URL。
string7	字符串类型。
timer-name	可选项，限定当前用户组中用户可访问 NGFW 的时间段名称。
string8	字符串类型。
force-inherit	可选项，设置是否强制隶属于此用户组的子组或用户继承该用户组的认证策略属性。
yes|no	是|否，默认选项为否。

以下是添加一个用户组的示例：

添加一个名称为“group1”的用户组，并限定该用户组中用户访问 NGFW 的来源区域为“area1”。

TopsecOS# **define area add name** *area1* **interface** *feth0* **comment** *comment_content*

TopsecOS# **user manage group add name** *group1* **area-name** *area1*

user manage group search <number> **key-word** <id|name|description|group> **key-value** <*string*>

命令描述：

搜索与相应关键字匹配的用户组的数量。

参数说明：

user manage group search number	搜索与相应关键字匹配的用户组的数量。
key-word	必选项，根据关键字搜索用户组数量。
id|name|description|group	用户组的 ID|用户组名称|描述信息|用户组的父组名称
key-value	必选项，设置与用户组相关的关键字的值。

string	字符串类型。

以下是通过关键字搜索用户组的数量的示例：

根据用户组名称查找用户组的数量信息。

TopsecOS# **user manage group search** number **key-word** name **key-value** *group2*

matching result 1

user manage group search <page> **key-word** <id|name|description|group> **key-value** <*string*> [**begin-num** <*number1*> [**end-num** <*number2*>]]

命令描述：

查找用户组。

参数说明：

user manage group search page	查找用户组信息。
key-word	必选项，根据关键字查找用户组。
id|name|description|group	用户组名称|描述信息|用户组的父组
key-value	必选项，设置与用户组相关的关键字的值。
string	字符串类型。
begin-num	可选项，指定显示搜索结果的起始位置。
number1	数值类型。
end-num	可选项，指定显示搜索结果的终止位置。
number2	数值类型。

以下是显示用户组的信息的示例：

TopsecOS# **user manage group search** page **key-word** name **key-value** *group2*

ID 8013 user manage group add name group2 notice-url null max-users 1024 total-users 0 max-son-group 64 total-son-group 0 description null group null auth-server null address-name null area-name null timer-name sche inherit-policy no force-inherit yes

user manage group show <number>

命令描述：

显示用户组的数量信息。

以下是显示用户组的数量信息的示例：

TopsecOS# **user manage group show** number Current has total of group is 2

user manage group show <all> [**begin-num** <*number1*> [**end-num** <*number2*>]]

命令描述：

显示用户组信息。

参数说明：

user manage group show all	显示所有或部分用户组的信息。
begin-num	可选项，指定显示搜索结果的起始位置。
number1	数值类型。
end-num	可选项，显示搜索结果的终止位置。
number2	数值类型。

以下是显示用户组信息的示例：

TopsecOS# **user manage group show** all ID 8012 user manage group add name group notice-url null max-users 1024 total-users 0 max-son-group 64 total-son-group 0 description null group null auth-server null address-name null area-name null timer-name null inherit-policy no force-inherit no ID 8013 user manage group add name group2 notice-url null max-users 1024 total-users 0 max-son-group 64 total-son-group 0 description null group null auth-server null address-name null area-name null timer-name sche inherit-policy no force-inherit yes

user manage group show name <*string*>

命令描述：

根据用户组名显示用户组信息。

参数说明：

user manage group show	显示指定用户组名的用户组信息。
name	必选项，指定用户组。
string	字符串类型，表示用户组名称。

以下是显示用户组“group2”的示例：

```
TopsecOS# user manage group show name group2
ID 8013 user manage group add name group2 notice-url null max-users 1024 total-users
0 max-son-group 64 total-son-group 0 description null group null auth-server null
address-name null area-name null timer-name sche inherit-policy no force-inherit no
```

user manage group delete index-key <name|id> **index-value** <*string*>

命令描述：

根据用户组的名称或者 ID 删除用户组。

参数说明：

user manage group delete	删除用户组。
index-key	必选项，选择指定用户组的索引关键字。
name|id	用户组名|用户组的 ID 号
index-value	必选项，指定用户组的索引关键字的值。
string	字符串类型。

以下是根据用户组的名称或者 ID 删除用户组的示例：

删除名称为“group1”的用户组。

```
TopsecOS# user manage group delete index-key name index-value group1
```

user manage group clean <cr>

命令描述：

清空用户组。

以下是清空用户组的示例：

```
TopsecOS# user manage group clean
```

5.1.2 管理用户

用户经过 NGFW 访问网络资源前，首先需通过 NGFW 的认证，对于通过认证的用户，NGFW 还会检查用户的属性，如用户账号是否可用、账号过期时间、用户访问策略等信息，只有认证和用户限制策略都通过的用户，才可访问其被授权的网络资源。

用户能被 NGFW 进行认证，必须首先在 NGFW 中创建相关用户的账号信息。管理员可通过三种方式在 NGFW 上创建用户：1）手动逐条创建；2）手动批量创建，将用户信息按照模板写入 TXT 或 CSV 文件中，再将 TXT 或 CSV 文件导入到 NGFW 中；3）设备自动发现，NGFW 通过扫描网络中指定 IP 地址范围的主机，自动添加用户至 NGFW 中。

用户通过 NGFW 进行认证时，具体认证方式如下：

- 按照用户服务器认证方式，可以分为免认证、本地认证和外部认证。
  - 免认证：NGFW 根据用户登录地址、登录时间和来源区域自动识别用户，进而确定该用户是否合法。
  - 本地认证：表示在 NGFW 上进行认证。
  - 外部认证：表示在外部认证服务器上进行认证。
- 按照用户身份认证的方式，可以分为用户名本地密码认证和证书认证两种。
  - 用户名密码认证：根据认证服务器是否为 NGFW 设备，分为本地密码认证和外部密码认证（Radius、LDAP 或 TACACS）。
  - 证书认证：根据签发证书的 CA 是否是设备本身，分为本地证书认证、第三方 CA 离线认证、第三方 CA 在线认证三种。

下面介绍如何在 NGFW 上管理用户信息。

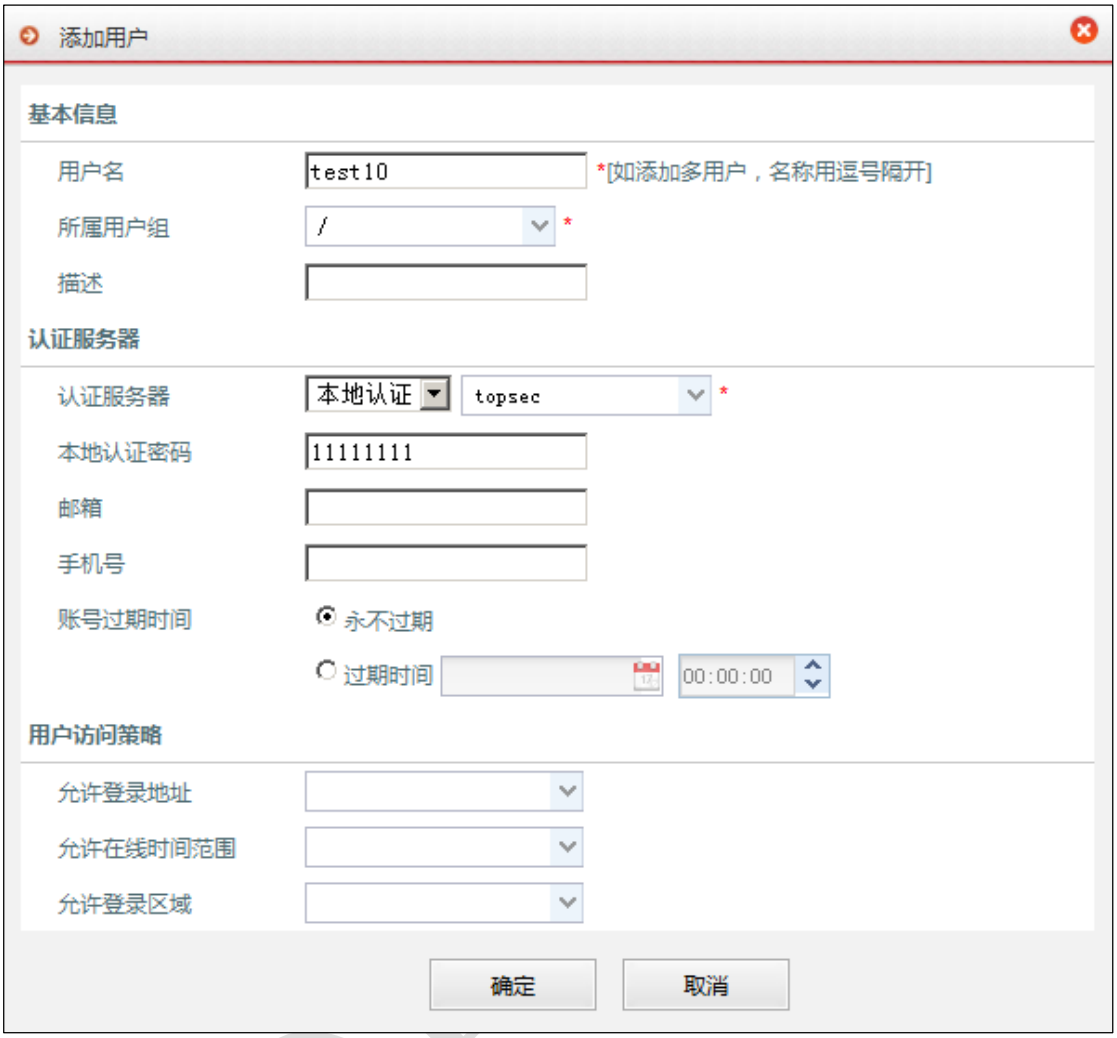
WEBUI 方式配置

步骤 1 选择 **用户管理** > **用户管理**。界面左侧为用户组管理界面，右侧为用户管理界面，点击某个用户组，界面右侧的列表中将显示此用户组中包含的子组和用户信息。

步骤 2 添加新用户。

1）手动方式。

（a）点击用户管理界面的『添加』，如下图所示。



在添加用户时，各项参数的具体说明如下表所示。

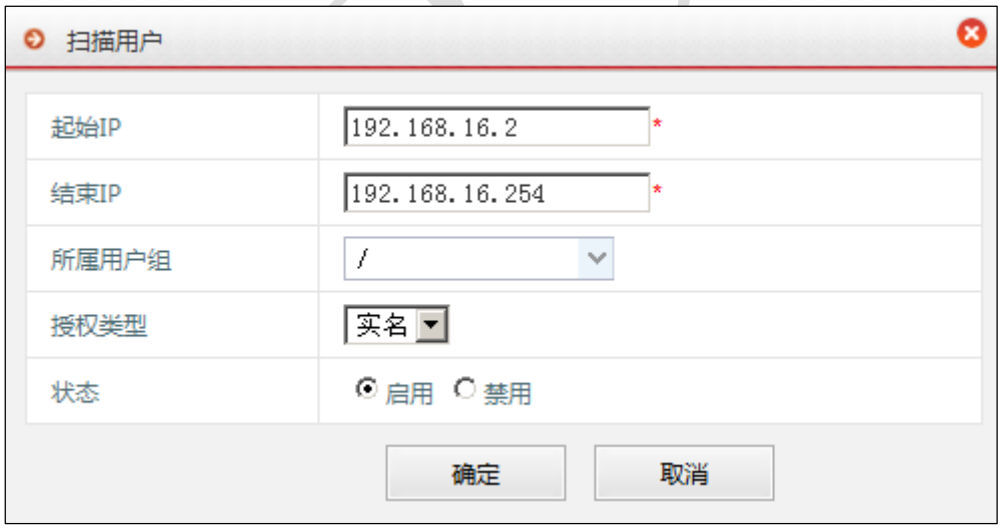
参数	说明
用户名	必选项。指认证用户的名称，可为中文、数字、字母以及逗号“,”的组合。 说明： 可以同时添加多个用户，名称之间用逗号隔开。
所属用户组	从下拉框中选择用户所属的父组。
描述	输入用户的描述信息。
认证服务器	选择新添加用户的认证方式并填写相应的认证服务器地址，可选项：免认证、本地认证、外部认证、未关联。 1）免认证：表示不需要选择认证服务器认证用户，NGFW 根据用户登录地址、登录时间和来源区域自动识别用户，进而确定是否允许该用户通过认证； 2）本地认证：表示在 NGFW 上进行认证，需选择 NGFW 本地认证服务器；

参数	说明
	3）外部认证：表示在外部认证服务器上进行认证，需选择指定第三方认证服务器； 4）未关联：表示在添加该用户时并不指定其认证服务器，管理员需后续指定认证该用户的认证服务器。
本地认证密码	采用“本地认证方式”时，设置与用户名对应的密码。
邮箱	采用“本地认证方式”时，设置认证用户的电子邮件地址信息。
手机号	采用“本地认证方式”时，设置认证用户的手机号码。
账号过期时间	采用“本地认证方式”时，可以限制认证用户的有效时间。可设置为永不过期或者某个时间段内有效。
用户访问策略	设置是否允许同一用户多点登录。
允许登录地址	设置允许用户登录的地址范围。
允许在线时间范围	设置允许用户登录的时间范围。
允许登录区域	设置允许用户从防火墙的哪个区域登录。

（b）参数设置完成后，点击【确定】按钮即可完成新用户的添加。

2）自动获取。

（a）点击『扫描』，如下图所示。



在配置自动发现用户参数时，各项参数的具体说明如下表所示。

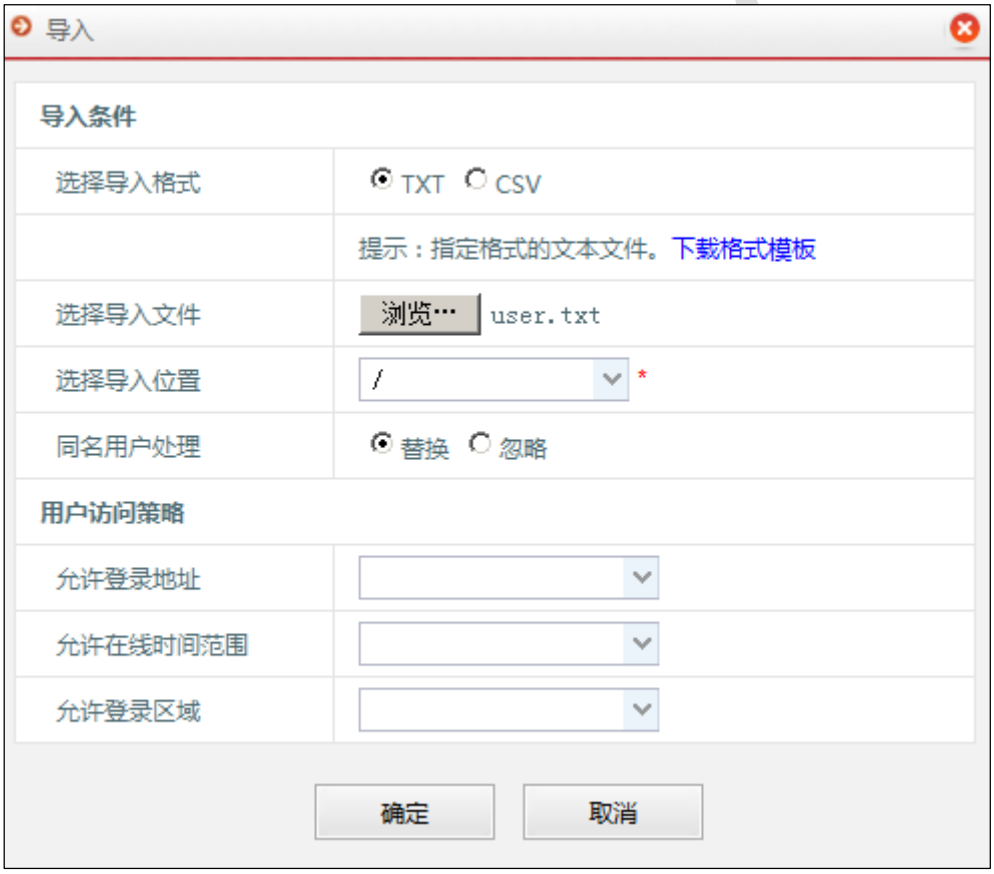
参数	说明
起始 IP	设置扫描用户的起始主机 IP 地址。
结束 IP	设置扫描用户的结束主机 IP 地址。
所属用户组	设置 NGFW 自动扫描出的用户添加到哪个用户组中。
授权类型	可选项：实名和匿名。

参数	说明
	说明： 实名：需指定具体认证服务器对用户进行认证，用户添加完成后，管理员后续需指定用户的认证服务器。 匿名：不需指定具体认证服务器对用户进行认证，NGFW 根据用户登录 IP 地址自动识别用户，进而确定是否允许该用户通过认证。
状态	可选项：启用和禁用。

（b）参数设置完成后，点击【确定】按钮完成用户的添加。

3）导入用户。

（a）点击『导入』，如下图所示。



在导入用户条件时，各项参数的具体说明如下表所示。

参数	说明
选择导入格式	选择导入用户配置文件的格式。可选项为：TXT 和 CSV 两种。 说明： 点击“下载格式模板”可以下载对应的 TXT 或 CSV 格式的模板。
选择导入文件	点击【浏览】按钮，在本地主机中选择待导入的文件。
选择导入位置	设置导入的用户属于哪个用户组。

参数	说明
同名用户处理	设置导入用户名称与 NGFW 上已有用户同名时的处理方式，可选项：替换、忽略。 说明： 替换：导入同名用户时，导入的新用户替换 NGFW 上已配置的用户。 忽略：导入同名用户时，跳过该用户的导入。
用户访问策略	设置导入的用户的访问策略。包括： 1）允许登录地址。 用户的主机 IP 地址只有在设定范围内，才能访问 NGFW。不设置该项，用户访问 NGFW 不受其主机 IP 地址的限制。 2）允许在线时间范围。 只能在设定的时间范围内，用户才能访问 NGFW。不设置该项，用户访问 NGFW 不受时间的限制。 3）允许登录区域。 用户只有通过特定的区域访问 NGFW，才可登录 NGFW。不设置该项，用户登录 NGFW 不受区域的限制。

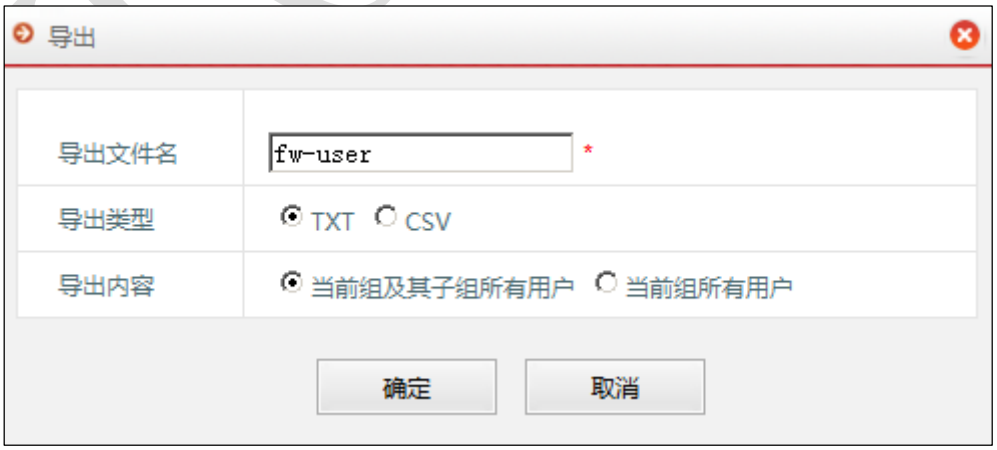
2）参数设置完成后，点击【确定】按钮即可完成用户导入。

步骤 3 启用/禁用用户。

用户所在行背景显示为白色，表示用户处于“启用”状态；所在行背景显示为深灰色，表示用户处于禁用状态。新添加用户默认处于“启用”状态。选择用户，点击『启用』可启用用户，点击『禁用』可禁用用户。

步骤 4 导出用户。

1）点击『导出』，如下图所示。



在设置导出用户条件时，各项参数的具体说明如下表所示。

参数	说明
导出文件名	设置导出的用户配置文件的名称。
导出类型	选择导出用户配置文件的格式。可选项为：TXT、CSV。
导出内容	设置待导出的用户。可选项：当前组及其子组所有用户、当前组所有用户。

2）参数设置完成后，点击【确定】按钮可导出相应用户组的用户信息。

CLI 方式配置

user manage user add name <*string1*> [**address-name** <*string2*>] [**area-name** <*string3*>] [**auth-server** <*string4*>] [**description** <*string5*>] [**group** <*string6*>] [**invalid** <yes|no>] [**type** <actuality|anonymity>] [**timer-name** <*string7*>]

命令描述：

手动逐个添加用户。

参数说明：

user manage user add	手动逐个添加用户。
name	必选项，设置用户的名称。
string1	字符串类型。不允许重名用户存在。用户名可以为数字、字母和逗号“,”的组合。
address-name	可选项，限定用户可通过哪些 IP 地址访问 NGFW。
string2	字符串类型。
area-name	可选项，限定用户可通过哪些区域访问 NGFW。
string3	字符串类型，表示区域名称。
auth-server	可选项，设置认证用户的认证服务器。
string4	字符串类型，表示认证服务器名称。
description	可选项，设置用户的描述信息。
string5	字符串类型。
group	可选项，设置用户所属的用户组。
string6	字符串类型，表示用户组名称。
invalid	可选项，设置是否禁用当前用户。
yes|no	是|否
type	可选项，设置授权用户的类型。
actuality|anonymity	实名授权用户|匿名授权用户
timer-name	可选项，设置用户可访问 NGFW 的时间段。
string7	字符串类型，表示时间对象名称。

以下是手动逐个添加一个用户的示例：

添加名称为“user1”的用户，所属用户组为“group2”，可通过区域 “area1”访问 NGFW。

TopsecOS# **user manage user add name** *user1* **area-name** *area1* **group** *group2*

user manage scan-host find begin-ip <*ipaddress1*> **end-ip** <*ipaddress2*> **group** <*string*> **type** <actuality|anonymity> **invalid** <yes|no>

命令描述：

通过扫描主机方式添加用户。

参数说明：

user manage scan-host find	通过扫描方式添加用户。
begin-ip	设置扫描用户的起始主机 IP 地址。
ipaddress1	IP 地址字符串。
end-ip	设置扫描用户的结束主机 IP 地址。
ipaddress2	IP 地址字符串。
group	设置 NGFW 自动扫描出的用户添加到哪个用户组中。
string	字符串类型。
type	设置根据主机 IP 地址扫描出的用户的授权类型，可选项：实名和匿名。
actuality|anonymity	实名|匿名 说明： 实名：需指定具体认证服务器对用户进行认证，用户添加完成后，管理员后续需指定用户的认证服务器。 匿名：不需指定具体认证服务器对用户进行认证，NGFW 根据用户登录地址、登录时间和来源区域自动识别用户，进而确定是否允许该用户通过认证。
invalid	设置添加的用户是否禁用。
yes|no	是|否

以下通过扫描主机方式自动添加用户的示例：

扫描主机地址范围为 192.168.16.10 至 192.168.16.100 内的用户，并将扫描出的用户添加到用户组“/”下，且授权类型设置为实名授权。

TopsecOS# **user manage manage scan-host find begin-ip** *192.168.16.1* **end-ip** *192.168.16.100* **group** **/** **type** actuality **invalid** no

user manage user import filename <*string1*> **file-format** <txt|csv> [**address-name** <*string2*>] [**cognominal** <overwrite|ignore>] [**group** <*string3*>] [**timer-name** <*string4*>] [**type**

<actuality|anonymity>] [**area-name** <*string5*>]

命令描述：

导入用户。

参数说明：

user manage user import	导入用户。
filename	必选项，设置导入文件的文件名。
string1	字符串类型。
file-format	必选项，选择导入配置文件的文件格式。
txt|csv	文本文件类型|纯文本文件类型
address-name	可选项，设置用户允许登录的 IP 地址。
string2	字符串类型。
cognominal	可选项，选择同名用户的处理方式。
overwrite|ignore	覆盖|忽略
group	可选项，选择导入到的用户组。
string3	字符串类型，表示用户组名称。
timer-name	可选项，设置用户允许登录的时间。
string4	字符串类型。
type	设置用户授权类型。
actuality|anonymity	实名|匿名
area-name	设置用户允许访问 NGFW 的区域。
string5	字符串类型。

user manage user export file-format <txt|csv> **group** <*string1*> [**filename** <*string2*>]

命令描述：

导出指定用户组的授权用户数据信息。

参数说明：

user manage user export	导出用户。
file-format	必选项，选择要生成的文件格式。
txt|csv	文本文件类型|纯文本文件类型
group	必选项，选择导出用户的用户组。
string1	字符串类型，表示用户组名称。
filename	可选项，设置要生成的文件名称。
string2	字符串类型。

user manage user search <number> **key-word** <name|group> **key-value** <*string*>

命令描述：

查询匹配相应关键字的用户的数量。

参数说明：

user manage user search number	查询匹配相应关键字的用户的数量。
key-word	必选项，设置与用户相关的关键字。
name|group	用户的名称|用户隶属的用户组
key-value	必选项，指定与用户相关的关键字的值。
string	字符串类型。

以下是查询用户名称为“user2”的用户数量的示例：

TopsecOS# **user manage user search** number **key-word** name **key-value** *user2*

matching result 1

user manage user search <page> **key-word** <id|name|ip|group> **key-value** <*string*> [**begin-num** <*number1*>] [**end-num** <*number2*>]

命令描述：

根据关键字查询用户信息。

参数说明：

user manage user search page	根据关键字查询用户信息。
key-word	必选项，与用户相关的关键字。
id|name|ip|group	用户 ID|用户名称|用户的 IP|用户隶属的用户组名
key-value	必选项，与用户相关的关键字的值。
string	字符串类型。
begin-num	可选项，指定显示搜索结果的起始位置。当选择 page 参数时设置此项。
number1	数值类型。
end-num	可选项，指定显示搜索结果的终止位置。当选择 page 参数时设置此项。
number2	数值类型。

以下是查询用户名称为“user3”的用户信息的示例：

TopsecOS# **user manage user search** page **key-word** name **key-value** *user3*

ID 8010 user manage user add name user3 description null invalid no type actuality group null auth-server null address-name null area-name null timer-name null

user manage user show <number>

命令描述：

显示当前用户的数量。

以下是显示当前用户的数量的示例：

```
TopsecOS# user manage user show number
current has total of users is 1
```

user manage user show <all> [**begin-num** <*number1*> [**end-num** <*number2*>]]

命令描述：

显示当前用户信息。

参数说明：

user manage user show all	显示所有或部分用户信息。
begin-num	可选项，指定显示搜索结果的起始位置。
number1	数值类型。
end-num	可选项，指定显示搜索结果的终止位置。
number2	数值类型。

以下是显示当前所有用户信息的示例：

```
TopsecOS# user manage user show all
ID 8009 user manage user add name user description null invalid no type anonymity
group null auth-server null address-name area1 area-name area1 timer-name sche
```

user manage user show name <*string*>

命令描述：

根据用户名称显示用户信息。

参数说明：

user manage user show	根据用户名称显示用户信息。
name	必选项，指定指定用户名。
string	字符串类型。

以下是显示用户名称为“user”的用户信息的示例：

```
TopsecOS# user manage user show name user
```

```
ID 8009 user manage user add name user description null invalid no type anonymity
group null auth-server null address-name area1 area-name area1 timer-name sche
```

user manage user delete index-key <name|id> **index-value** <*string*>

命令描述：

删除用户。删除用户的同时删除用户在线信息。

参数说明：

user manage user delete	删除用户。
index-key	必选项，选择指定用户的索引关键字。
name|id	用户名|用户的 ID 号
index-value	必选项，指定用户的索引关键字的值。
string	字符串类型。

以下是删除用户的示例：

删除名称为“user1”的用户。

```
TopsecOS# user manage user delete index-key name index-value user1
```

user manage user clean <cr>

命令描述：

清空用户信息。

以下是清空用户信息的示例：

```
TopsecOS# user manage user clean
```

user manage online-user show <cr>

命令描述：

查看在线用户。

以下是查看在线用户的示例：

```
TopsecOS# user manage online-user show
user_name      address        server_name   client_type   online_time(hh:mm:ss)
```

'zhmezhe'　　192.168.16.6　　topsec　　cgi　　2:48:1

user manage online-user < num>

命令描述：

查看在线用户的数量。

以下是查看在线用户数量的示例：

TopsecOS# **user manage online-user** num

user manage online-user delete-by-name <*string*>

命令描述：

根据用户名称删除在线用户。

参数说明：

user manage online-user	根据用户名称删除在线用户。
delete-by-name	必选项，通过名称删除在线用户。
string	字符串类型。

以下是删除在线用户的示例：

删除名称为“user1”的在线用户。

TopsecOS# **user manage online-user delete-by-name** *user1*

user manage online-user delete-by- addr addr <*ipaddress*>

命令描述：

根据登录地址删除在线用户。

参数说明：

user manage online-user	根据登录地址删除在线用户。
delete-by- addr	必选项，通过登录地址删除在线用户。
addr	必选项，指定 IP 地址。
ipaddress	IP 地址字符串。

以下是删除在线用户的示例：

删除登录地址为“10.10.10.10”的在线用户。

TopsecOS# **user manage online-user delete-by- addr addr** *10.10.10.10*

user manage online-user clean <cr>

命令描述：

清除在线用户。

以下是清除在线用户的示例：

TopsecOS# **user manage online-user clean**

5.2 认证服务器

NGFW 不仅能作为认证服务器接受用户的认证请求，验证用户的合法性，还可以向外部认证服务器转发用户的认证请求，由外部认证服务器验证用户是否合法，NGFW 支持的外部认证协议包括 Radius、Ldap 和 Tacacs。

远程用户登录 NGFW 进行认证时，NGFW 将查询存储在 NGFW 上的用户信息，进而确定用户的认证方式，对于需由外部认证服务器认证的用户，NGFW 向相应的认证服务器转发用户认证请求，如果认证服务器验证该用户合法，且符合用户访问策略，则允许放行。

注意

- ✧ 用户通过外部认证服务器进行认证，以获取访问 NGFW 权限时，NGFW 需与外部认证服务器建立连接。

5.2.1 添加本地认证服务器

WEBUI 方式配置

步骤 1 选择 **用户管理** > **认证服务器**。

步骤 2 点击『添加』，进入“添加服务器”界面。

步骤 3 添加本地认证服务器。

1）服务器类型选择“本地服务器”，如下图所示。

在添加本地服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器名称	必选项。输入本地认证服务器的名称。
关联用户/组	设置该服务器所涉及的网关上的用户和用户组成员。 说明： 1）“成员”中显示所有用户及用户组信息，“已选成员”中显示需通过本地认证服务器认证的用户。管理员可以在“成员”中选择一个或多个用户或用户组，点击【>】添加到“已选成员”中。 2）在搜索栏中输入关键字，点击“🔍”图标可以快速查找某个用户或用户组成员。

2）参数设置完成后，点击【确定】按钮，完成本地认证服务器的添加。

CLI 方式配置

user auth server add protocol <localdb> **name** <*string1*> [**user-group-name** <*string3*>]

命令描述：

添加本地认证服务器。

参数说明：

user auth server add	添加认证服务器。
protocol	必选项，指定使用的认证协议。
localdb	认证使用的协议类型。
name	必选项，指定认证服务器名称。
string1	字符串类型，表示认证服务器名称。
user-group-name	可选项，指定由该本地认证服务器认证的用户所属组的名称。
string3	字符串类型。

使用说明：

各种服务器均有缺省认证端口，localdb 的缺省认证端口为“3306”。

以下是添加本地认证服务器的示例：

添加一个本地认证服务器 topsec01。

```
TopsecOS# user auth server add protocol localdb name topsec01
```

5.2.2 添加 Radius 服务器

WebUI 方式配置

步骤 1 选择 **用户管理** > **认证服务器**。

步骤 2 点击『添加』，进入“添加服务器”界面。

步骤 3 添加 Radius 服务器。

1）服务器类型选择“Radius 服务器”，如下图所示。

在设置 Radius 服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器名称	必选项。输入外部认证服务器的名称。
服务器地址	必选项。指认证服务器的 IP 地址。
服务器端口	必选项。指认证服务器的监听认证请求的服务端口。
认证方法	指 Radius 认证协议的认证方法，可选项：PAP、CHAP。
共享密钥	指 Radius 认证服务器端的共享密钥。
客户端 IP	指网关与 Radius 服务器连接的出接口的 IP 地址。
超时时间	为判断某个服务器是否失效，网关会向服务器周期性地发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。单位：秒；取值范围：1-180；默认值：5。

参数	说明
认证重试次数	网关向服务器发送认证请求失败时，可以重复认证的次数。单位：次；取值范围：1-10；默认值：3。
属性值字符集	Radius 外部认证服务器返回的自定义属性的值的格式。可选项为 GBK 和 UTF-8。
自动增加用户到本地	设置是否自动增加 Radius 服务器上的用户到本地。
计费功能	设置是否开启 Radius 计费功能。
属性值的分隔符	表示当 Radius 服务器的一个属性值被分隔成多个时，每个值之间的分隔符号。 说明： 属性值分隔符只针对资源、ACL、组。

2）参数设置完成后，点击【确定】按钮完成 Radius 外部认证服务器的添加。

CLI 方式配置

user auth server add protocol <radius> **name** <*string1*> **host** <*string2*> **port** <*port1*> **radius-sharesecret** <*string3*> [**radius-authmode** <pap|chap>] [**radius-clientip** <*string4*>] [**time-out** <*number1*>] [**retry-times** <*number2*>] [**charset** <gbk|utf-8>] [**auto-add-user** <yes|no>] [**radius-useaccount** <yes|no>] [**radius-account-port** <*port2*>] [**attr-separator** <*string5*>]

命令描述：

添加 Radius 认证服务器。

参数说明：

user auth server add	添加认证服务器。
protocol	必选项，指定使用的认证协议。
radius	认证使用的协议类型。
name	必选项，指定认证服务器名称。
string1	字符串类型，表示认证服务器名称。
host	必选项，设置认证服务器的 IP 地址。
string2	字符串类型，表示认证服务器的 IP 地址。
port	必选项，指定认证服务器的监听认证请求的服务端口，不同协议的默认值不同。Radius 协议的默认值为 1812。
port1	数值类型，表示端口号，取值范围：0-65535。
radius-sharesecret	可选项，设置 Radius 的共享密钥。
string3	字符串类型。
radius-authmode	可选项，设置 Radius 认证协议的认证方法。
pap|chap	可选项：PAP、CHAP。

radius-clientip	可选项，设置 Radius 的客户端 IP 地址
string4	字符串类型。
time-out	可选项，设置认证服务器的失效时间。 说明： NGFW 会向服务器周期性的发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。
number1	数值类型，单位：秒；取值范围：1-180；默认值：5。
retry-times	可选项，设置认证失败后重新认证的最大次数。
number2	数值类型，取值范围：0-10；默认值：0 次。
charset	可选项，选择认证服务器返回的自定义属性的格式，可选项为 GBK 和 UTF-8。
gbk|utf-8	GBK 字符集和 UTF-8 字符集。
auto-add-user	可选项，设置是否自动增加认证服务器上的用户到本地。
yes|no	是|否
radius-useaccount	可选项，是否启动 Radius 计费功能。
yes|no	是|否
radius-account-port	可选项，设置 Radius 计费的端口号。
port2	数值，表示端口号，取值范围：0-65535。
attr-separator	可选项，属性值的分隔符。
string5	字符串类型。

以下是添加认证服务器的示例：

添加一个 radius 认证服务器，认证服务器的名称为“radius01”，地址为“192.168.1.10”，端口为“1812”，共享密钥为“11111111”。

TopsecOS# **user auth server add protocol** radius **name** *radius01* **host** *192.168.1.10* **port** *1812* **radius-sharesecret** *11111111*

5.2.3 添加 Ldap 服务器

WEBUI 方式配置

步骤 1 选择 **用户管理** > **认证服务器**。

步骤 2 点击『添加』，进入“添加服务器”界面。

步骤 3 添加 Ldap 服务器。

1）服务器类型选择“Ldap 服务器”，如下图所示。

在设置 Ldap 服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器名称	必选项。输入外部认证服务器的名称。
服务器地址	必选项。指认证服务器的 IP 地址。
服务器端口	必选项。指认证服务器的监听认证请求的服务端口。

参数	说明
服务器 DN	必选项。LDAP 服务器的域名。需要输入域名分解格式，不同厂家的 LDAP 服务器需要设置不同的关键字。例如：假设 AD 服务器域名为“sina.com”则此处应输入“dc=sina, dc=com”。 说明： 在 LDAP 服务器上可以通过“我的电脑”右键菜单的 **属性** > **计算机名** 来查看服务器所在的域。
服务器类型	LDAP 是一个开放的协议，不同的公司有不同的实现方法，因此需要选择 LDAP 服务器的类型，可选项为 MS-AD、SUN ONE、NOVELL 和 other。分别表示微软公司的 AD 服务器、SUN ONE 公司的 LDAP 服务器、NOVELL 公司的 LDAP 服务器和其他公司的 LDAP 服务器。
查询账号	设置是否启用 LDAP 查询账号。LDAP 查询账号是指 LDAP 服务器上具有用户查询权限的用户。
查询密码	必选项。设置 LDAP 服务器查询账号密码。启用 LDAP 查询账号时需要设置此参数。
用户过滤条件	必选项。设置 LDAP 用户过滤条件。
查询范围	设置以服务器 DN 为起点，查询 LDAP 目录的范围。可选项为：subtree、one level，默认值为 subtree。subtree 表示对包含服务器 DN 的所有子节点都进行查询；one level 表示只对服务器 DN 的直接子节点进行查询。
用户名	在下拉列表中选择一个属性的值作为 LDAP 服务器上用户名属性，也可选择自定义。
关联用户组	在下拉列表中选择一个属性的值作为 LDAP 服务器上用户所关联的用户组，也可选择自定义。
超时时间	为判断某个服务器是否失效，网关会向服务器周期性地发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。单位：秒；取值范围：1-180；默认值：5。
属性值字符集	LDAP 外部认证服务器返回的自定义属性的值的格式。可选项为 GBK 和 UTF-8。
自动添加用户到本地	设置是否自动添加 LDAP 服务器上的用户到本地。
属性值的分隔符	表示当 Ldap 用户的一个属性值被分隔成多个时，每个值之间的分隔符号。 说明： 属性值分隔符只针对资源、ACL、组。

2）参数设置完成后，点击【确定】按钮完成 LDAP 外部认证服务器的添加。

CLI 方式配置

user auth server add protocol <ldap> **name** <*string1*> **host** <*string2*> **port** <*port*> **ldap-dn** <*string3*>[**ldap-subtype** <ad|sun|novell|other>] [**ldap-usequeryaccount** <yes|no>] [**ldap-queryname** <*string4*>] [**ldap-querypasswd** <*string5*>] [**ldap-filterinfo** <*string6*>] [**ldap-scope** <onelevel|subtree>] [**ldap-searchpath** <*string7*>] [**time-out** <*number*>] [**charset** <gbk|utf-8>] [**auto-add-user** <yes|no>] [**attr-separator** <*string8*>]

命令描述：

添加 Ldap 认证服务器。

参数说明：

user auth server add	添加认证服务器。
protocol	必选项，指定使用的认证协议。
ldap	认证使用的协议类型。
name	必选项，指定认证服务器名称。
string1	字符串类型，表示认证服务器名称。
host	必选项，设置认证服务器的 IP 地址。
string2	字符串类型，表示认证服务器的 IP 地址。
port	必选项，指定认证服务器的监听认证请求的服务端口，不同协议的默认值不同。
port	数值类型，表示端口号，取值范围：0-65535。
ldap-dn	可选项，LDAP 认证服务器 DN。 说明： 需要输入域名分解格式，不同厂家的 ldap 服务器需要设置不同的关键字。例如：假设 AD 服务器域名为“sina.com”则此处应输入“dc=sina,dc=com”。
string3	字符串类型。
ldap-subtype	可选项，设置 LDAP 服务器类型。
ad|sun|novell|other	可选项为 ad、sun、novell 或其他类型。
ldap-usequeryaccount	可选项，设置是否将 LDAP 查询账户启动。
yes|no	是|否
ldap-queryname	可选项，LDAP 认证服务器上具有用户查询权限的用户 DN（一般为管理员 DN）。 说明： 在配置管理员 DN 时，需要输入完全管理员的 DN，比如管理员 Administrator，由于 Administrator 也属于 Users 用户组，则管理员 DN 为：cn=Administrator,cn=users,dc=cams,dc=com。
string4	字符串类型。
ldap-querypasswd	可选项，LDAP 查询账户密码。
string5	字符串类型。
ldap-filterinfo	可选项，设置从 LDAP 认证服务器上同步用户时的过滤条件。例如：在 Active Directory 中，用户名属性标识通常为：

	saMAccountName。输入“saMAccountName=u*”时，只导入 LDAP 服务器上用户名以 u 开头的用户。 说明： 当设置多个过滤条件时，设置“或”关系时的格式为：(|（…）（…))；设置“与”关系时的格式为：(&（…）（…))。内层括号内设置具体的过滤条件。
string6	字符串类型。
ldap-scope	可选项，设置以服务器 DN 为起点，查询 LDAP 目录的范围。
onelevel|subtree	onelevel 表示只对服务器 DN 的直接子节点进行查询； subtree 表示对包含服务器 DN 的所有子节点都进行查询。
ldap-searchpath	可选项，LDAP 搜索路径。
string7	字符串类型。
time-out	可选项，设置认证服务器的失效时间。 说明： NGFW 会向服务器周期性的发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。
number	数值类型，单位：秒；取值范围：1-180；默认值：5。
charset	可选项，选择认证服务器返回的自定义属性的格式，可选项为 GBK 和 UTF-8。
gbk|utf-8	GBK 字符集和 UTF-8 字符集。
auto-add-user	可选项，设置是否自动增加认证服务器上的用户到本地。
yes|no	是|否
attr-separator	可选项，属性值的分隔符。
string8	字符串类型。

以下是添加认证服务器的示例：

添加一个 LDAP 认证服务器 ldap01，认证服务器地址为 172.16.1.2，端口为 389，DN 为 sina.com。

TopsecOS#**user auth server add protocol** ldap **name** *ldap01* **host** *172.16.1.2* **port** *389* **ldap-dn** *dc=sina,dc=com*

5.2.4 添加 Tacacs 服务器

WEBUI 方式配置

步骤 1 选择 **用户管理** > **认证服务器**。

步骤 2 点击『添加』，进入“添加服务器”界面。

步骤 3 添加 Tacacs 服务器。

1）服务器类型选择“Tacacs 服务器”，如下图所示。

在设置 Tacacs 服务器时，各项参数的具体说明如下表所示。

参数	说明
服务器名称	必选项。输入外部认证服务器的名称。
服务器地址	必选项。指认证服务器的 IP 地址。
服务器端口	必选项。指认证服务器的监听认证请求的服务端口。
认证方法	指 Tacacs 认证协议的认证方法。 可选项：PAP、CHAP。

参数	说明
共享密钥	必选项。指 Tacacs 认证服务器端的共享密钥。
超时时间	为判断某个服务器是否失效，NGFW 会向服务器周期性地发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。单位：秒；取值范围：1-180；默认值：5。
属性值字符集	TACACS 外部认证服务器返回的自定义属性的值的格式。可选项：GBK 和 UTF-8。
自动添加用户到本地	设置是否自动增加 TACACS 服务器上的用户到本地。

2）参数设置完成后，点击【确定】按钮完成 Tacacs 外部认证服务器的添加。

CLI 方式配置

user auth server add protocol <tacacs> **name** <*string1*> **host** <*string2*> **port** <*port*> **tacacs-key** <*string3*> [**tacacs-mode** <pap|chap>] [**time-out** <*number*>] [**charset** <gbk|utf-8>] [**auto-add-user** <yes|no>]

命令描述：

添加 Tacacs 认证服务器。

参数说明：

user auth server add	添加认证服务器。
protocol	必选项，指定使用的认证协议。
tacacs	认证使用的协议类型。
name	必选项，指定认证服务器名称。
string1	字符串类型，表示认证服务器名称。
host	必选项，设置认证服务器的 IP 地址。
string2	字符串类型，表示认证服务器的 IP 地址。
port	必选项，指定认证服务器的监听认证请求的服务端口，不同协议的默认值不同。
port	数值类型，表示端口号，取值范围：0-65535。
tacacs-key	可选项，设置 TACACS 的共享密钥。
string3	字符串类型。
tacacs-mode	可选项，设置 TACACS 的认证方法。
pap|chap	可选项：PAP、CHAP。
time-out	可选项，设置认证服务器的失效时间。 说明： NGFW 会向服务器周期性的发送请求报文，如果在规定的时间内未得到服务器发回的应答，需重传请求报文。
number	数值类型，单位：秒；取值范围：1-180；默认值：5。
charset	可选项，选择认证服务器返回的自定义属性

	的格式，可选项为 GBK 和 UTF-8。
gbk|utf-8	GBK 字符集和 UTF-8 字符集。
auto-add-user	可选项，设置是否自动增加认证服务器上的用户到本地。
yes|no	是|否

以下是添加 Tacacs 认证服务器的示例：

添加一个 Tacacs 认证服务器 tacacs01，认证服务器地址为 192.168.77.10，端口号为 9000，共享密钥为 11111111。

TopsecOS# **user auth server add protocol** tacacs **name** *tacacs01* **host** *192.168.77.10* **port** *9000* **tacacs-key** *11111111*

5.2.5 全局认证属性配置

全局认证属性配置用于设置用户登录的全局参数以及认证参数，从而对用户登录网关认证进行安全限制。

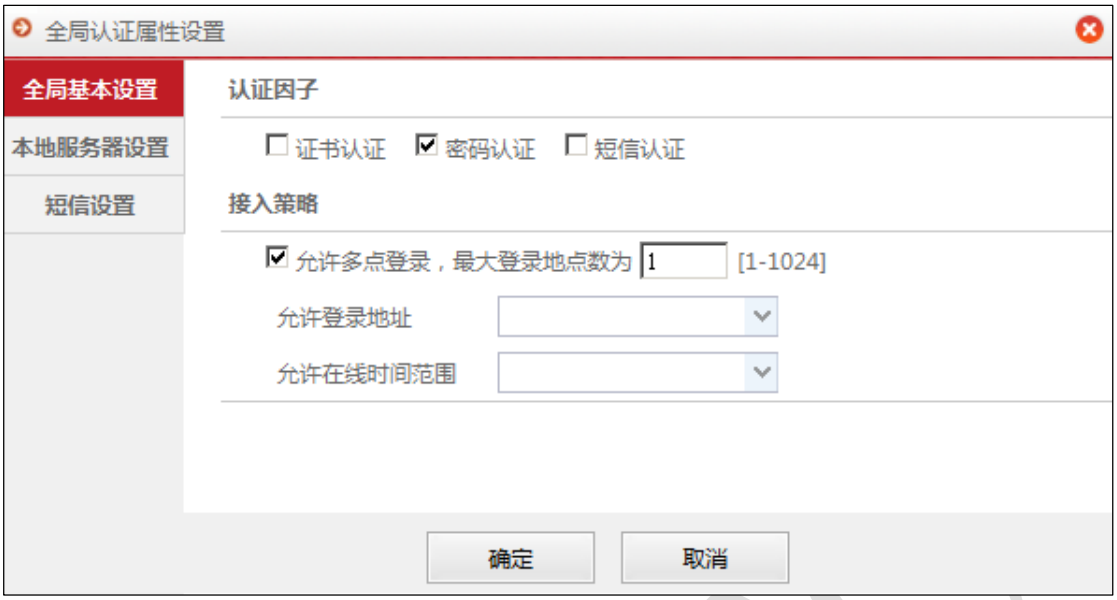
WEBUI 方式配置

步骤 1 选择 **用户管理** > **认证服务器**。

步骤 2 点击『全局认证属性配置』，进入“全局认证属性配置”界面。

步骤 3 设置用户全局属性。

激活“全局基本配置”页签，如下图所示。



在设置全局基本参数时，各项参数的具体说明如下表所示。

参数	说明
认证因子	设定用户认证的方式。可选项：证书认证、密码认证、短信认证。
接入策略	设置用户登录的限制。包括： 1）允许多点登录，最大登录地点数。 设置是否允许同一用户账号在不同地址同时进行登录。 2）允许登录地址。 用户登录的主机 IP 只能在设定范围内才能正常登录。默认不对用户使用的 IP 地址进行限制。 3）允许在线时间范围。 用户只能在设定的时间范围内在线。默认不对用户的允许在线时间进行限制。

参数设置完成后，点击【确定】按钮即可完成全局基本参数的设置。

步骤 4 设置本地服务器属性。

激活“本地服务器设置”页签，如下图所示。

在设置本地服务器属性时，各项参数的具体说明如下表所示。

参数	说明
防暴力破解	预防暴力破解用户密码采取的措施。包括以下几个方面： 1）本地密码认证失败次数：允许用户认证失败的最大次数，超过此设定，账号将被锁定一定时间。失败次数取值范围：1-255；默认值：5 次。 2）认证失败锁定时间：若用户认证失败，失败次数超过允许失败的最大次数，则在设定的锁定时间内，不得进行认证操作。锁定时间单位：秒；取值范围：60-100*86400；默认值：180。 3）24 小时内最多重置密码次数：若忘记密码，允许用户每天重置密码的最大次数，取值范围：1-255；默认值：3 次。 4）密码找回间隔：每次找回密码之间必须间隔的时间。单位：秒；取值范围：60-100*86400；默认值：180。 5）重置密码方式：用户忘记密码时，是否允许重置密码以及重置密码的方式。可选项有禁止、邮件以及短信三种，默认为禁止。

参数	说明
	说明： 用户进行密码重置的次数受“24 小时内最多重置密码次数”参数设置的控制，超出此限制后系统将拒绝执行密码重置操作。
密码复杂度	设置用户密码的复杂程度。可选项为： 新旧密码不同、不包含用户信息（用户名、手机、邮箱、注释）、密码包含大写字母、密码包含小写字母、密码包含数字、密码包含特殊字符、最小/大口令长度（密码长度范围：1-64，默认最小长度和最大长度分别为 6 和 32）以及口令复杂度修改后，已有帐户如果不符合新策略，是否在下次登录时强制修改口令使其符合新的口令策略。
密码有效性	设置用户密码有效性选项。包括： 1）禁止用户修改密码：是否禁止用户修改密码。若禁止则用户登录后不能自行修改密码。 2）首次登录修改密码：是否要求用户首次登录时修改管理员分配的密码。 3）密码修改间隔时间：在密码有效期内前后两次密码修改之间必须间隔的时间。单位：天；取值范围：1-120；默认值：30。 4）密码有效期时间：密码的有效期限，超过设置的有效期，用户再次登录将提示修改密码。单位：天；取值范围：120-360；默认值：120。
用户信息	禁止修改账号邮箱：禁止用户自行修改邮箱地址。 禁止修改账号电话：禁止用户自行修改联系电话号码。

参数设置完成后，点击【确定】按钮即可完成本地服务器参数的设置。

步骤 5 设置短信认证服务器

激活“短信设置”页签，如下图所示。

在设置短信认证服务器时，各项参数的具体说明如下表所示。

参数	说明
短信类型	根据短信网关是否直接连接 NGFW，设置发送短信的模式。可选项：topsec、local、none。 说明： 当设备所在的机房屏蔽无线电信号时，需要通过网络先将短信发送到短信中转发送服务器，再发送短信。此时需要选择“topsec”；否则，选择“local”即可，表示短信网关直接连接在 NGFW 的 USB 口。
短信猫制式	设置 NGFW 支持的短信猫类型。可选项：GSM 和 CDMA，“GSM”表示支持经纬星航移动或联通短信猫，“CDMA”表示仅支持经纬星航电信 CDMA 短信猫。 只有当“发送短信方式”选择“local”时才需要设置该项。

参数	说明
服务器地址	设置短信中转发送服务器的 IP 地址。 只有当“发送短信方式”选择“topsec”时才需要设置该项。
服务器端口	设置短信中转发送服务器接收 NGFW 设备发送的短信的端口。 只有当“发送短信方式”选择“topsec”时才需要设置该项。
当前网关 ID	设置由短信中转服务器指定的用于标识 NGFW 的 ID 号。只有当“发送短信方式”选择“topsec”时才需要设置该项。
共享密钥	设置由短信中转服务器指定的认证共享通行串，必须与短信中转发送服务器的设置一致。 只有当“发送短信方式”选择“topsec”时才需要设置该项。
密码长度	设置短信网关发送的动态口令的密码长度。单位：字符；取值范围 1-10；默认值：6。
密码有效期	设置短信网关发送的动态口令的有效期限。单位：秒；取值范围：60-255；默认值：60。
密码错误次数	允许 VRC 用户错误输入短信网关发送的动态口令的次数。单位：次；取值范围 1-10；默认值 3。
超时时间	设置认证超时时间。当发送短信时间达到此处设定的值后，密钥需要重新协商。
短信内容要求	可选项：num、character、both。num 表示短信内容只包含数字，character 表示短信内容只包含字母，both 表示短信内容包含数字和字母。
短信提示语	发送的短信提示语。

参数设置完成后，点击【确定】按钮完成短信服务器参数的设置。

CLI 方式配置

user auth global-config modify [**accept-reset-type** <no|mail|sms>] [**access-ip-range** <*string1*>] [**access-time-range** < *string2*>] [**account-locked-time** <*number1*>] [**attr-authorise** <global|condition|attribute>] [**cert-auth** <yes|no>] [**cert-search-action** <success|failure>] [**cert-search-user** <yes|no>] [**cert-search-attr** <*string3*>] [**change-pass-interval** <*number2*>] [**deny-change-mail** <yes|no>] [**deny-change-pass** <yes|no>] [**deny-change-phone** <yes|no>] [**diff-from-old-pass** <yes|no>] [**exclude-account-info** <yes|no>] [**fail-login-limit** <yes|no>] [**first-login** <yes|no>] [**force-change-pass** <yes|no>] [**hwid-bind** <yes|no>] [**include-char-digit** <yes|no>] [**include-char-lower** <yes|no>] [**include-char-punct** <yes|no>] [**include-char-upper** <yes|no>] [**invalid-password** <yes|no>] [**limit-access-ip** <yes|no>] [**limit-access-time** <yes|no>] [**limit-pass-**

len <yes|no>] [**max-pass-len** <*number3*>] [**maxnum-auth-fail** <*number4*>] [**maxnum-login-addr** <*number5*>] [**maxnum-reset** <*number6*>] [**maxnum-seccode** <*number7*>] [**min-pass-len** <*number8*>] [**multi-login** <yes|no>] [**pass-valid-period** <*number9*>] [**passwd-auth** <yes|no>] [**reset-pass-interval** <*number10*>] [**reset-pass-limit** <yes|no>] [**sms-auth** <yes|no>] [**termly-change-pass** <yes|no>]

命令描述：

配置全局认证策略。

参数说明：

user auth global-config modify	配置认证服务器的全局认证策略。
accept-reset-type	可选项，设置认证服务器允许重置的密码类型。
no|mail|sms	禁止重置密码|邮件重置密码|短信重置
access-ip-range	可选项，设置认证服务器允许登录的 ip 范围。
string1	字符串类型，例如 192.168.1.1-192.168.1.254,172.16.1.1-172.16.1.25，最多支持 16 种组合。
access-time-range	可选项，设置认证服务器允许登录的时间范围。
string2	数值类型，例如 12-00:00:00-23:59:59,4-00:00:00-11:59:59，最多 4 种组合，表示星期 1，2 全天，星期 4 的半天。
account-locked-time	可选项，设置认证服务器认证失败的锁定时间。
number1	数值类型，单位：分钟；取值范围：3-180；默认值：3。
attr-authorise	可选项，设置认证服务器的授权属性类型。
global|condition|attribute	全局授权|条件授权|属性授权
cert-auth	可选项，设置认证服务器是否需要证书认证。
yes|no	是|否
cert-search-action	可选项，查找结果是否成功。
success|failure	成功|失败
cert-search-user	可选项，设置认证服务器是否采用用户的属性值搜索本地授权用户。
yes|no	是|否
cert-search-attr	可选项，设置证书认证成功后，从证书相关属性中取值，搜索同名用户的属性值。
string3	字符串类型。
change-pass-interval	可选项，设置认证服务器密码修改的间隔时间。
number2	数值类型，单位：天；取值范围：1-120；默认值：30。如果未达到间隔期限，修改密码进行友好提示。
deny-change-mail	可选项，设置认证服务器是否禁止修改帐号邮箱。
yes|no	是|否
deny-change-pass	可选项，设置认证服务器是否禁止修改密码。
yes|no	是|否
deny-change-phone	可选项，设置认证服务器是否禁止修改帐号电话。
yes|no	是|否

diff-from-old-pass	可选项，设置认证服务器新旧密码是否不同。
yes|no	是|否
exclude-account-info	可选项，设置认证服务器认证时是否不包含帐号信息。
yes|no	是|否
fail-login-limit	可选项，设置认证服务器认证时是否限制失败登录。
yes|no	是|否
first-login	可选项，设置认证服务器是否在首次登录时修改密码。
yes|no	是|否
force-change-pass	可选项，设置认证服务器是否在不符合口令策略帐号下次登录时强制修改口令。
yes|no	是|否
hwid-bind	可选项，设置认证服务器是否使用硬件特征码绑定功能，特征码是按照特定计算机硬件计算出来的特征值，不同计算机特征码不同。启动该功能后，将用户名和特定机器绑定在一起，减少内网资源被非授权访问的风险。
yes|no	是|否
include-char-digit	可选项，设置认证服务器的密码中是否包含数字。
yes|no	是|否
include-char-lower	可选项，设置认证服务器的密码中是否包含小写字母。
yes|no	是|否
include-char-punct	可选项，设置认证服务器的密码中是否包含特殊字符。
yes|no	是|否
include-char-upper	可选项，设置认证服务器的密码中是否包含大写字母。
yes|no	是|否
invalid-password	可选项，设置认证服务器是否进行密码有效期设定。
yes|no	是|否
limit-access-ip	可选项，设置认证服务器是否限制登录的 ip。
yes|no	是|否
limit-access-time	可选项，设置认证服务器是否限制登录的时间。
yes|no	是|否
limit-pass-len	可选项，设置认证服务器是否限制密码的长度。
yes|no	是|否
max-pass-len	可选项，设置认证服务器的最大密码长度。
number3	数值类型，最大支持 128，最小长度为 6。
maxnum-auth-fail	可选项，设置认证服务器的最大认证失败次数。
number4	数值类型，取值范围：4-16；默认值：4。
maxnum-login-addr	可选项，设置认证服务器的最大登录地点数。
number5	数值类型，最大登录次数 1024。
maxnum-reset	可选项，设置认证服务器的密码每天的最大重置次数。
number6	数值类型，单位：次；取值范围：1-32；默认值：1。
maxnum-seccode	可选项，设置认证服务器的最大特征码数目。

number7	数值类型，表示进行登录地点的主机个数，最多支持 16 个主机的特征码信息。
min-pass-len	可选项，设置认证服务器的最小密码长度。
number8	数值类型，默认值：6。
multi-login	可选项，对于 SSL VPN 用户，设置是否允许多个人使用同一账号在不同地点登录，默认为“yes”。 说明： 当设备不包含 SSL VPN 模块时，界面不会显示该选项。
yes|no	是|否
pass-valid-period	可选项，设置认证服务器的密码有效期时间。
number9	数值类型，单位：天；取值范围：120-360；默认值：120。
passwd-auth	可选项，设置认证服务器是否需要密码认证。
yes|no	是|否
reset-pass-interval	可选项，设置认证服务器的密码重置间隔时间。
number10	数值类型，单位：分钟；取值范围：3-180；默认值：3。
reset-pass-limit	可选项，设置认证服务器是否限制密码的重置。
yes|no	是|否
sms-auth	可选项，设置认证服务器是否使用短信认证。
yes|no	是|否
termly-change-pass	可选项，设置认证服务器是否定期修改密码。
yes|no	是|否

以下是修改认证服务器全局认证策略的参数的示例：

修改认证服务器认证过程中允许以短信形式重置密码，最大密码长度设置为 10，允许使用短信认证，并允许多点登录。

```
TopsecOS# user auth global-config modify accept-reset-type sms max-pass-len 10
sms-auth yes multi-login yes
```

user auth global-config show <cr>

命令描述：

显示认证服务器全局配置信息。

以下是显示认证服务器全局配置信息的示例：

```
TopsecOS# user auth global-config show
Auth-gene:
    cert-auth    yes                    passwd-auth    yes
```

```
    hwid-bind    yes                    sms-auth    yes
Auth_strategy:
    fail-login-limit    yes          maxnum-auth-fail    5
account-locked-time    300          reset-pass-limit    yes
……
```

user auth global-config reset <cr>

命令描述：

恢复认证服务器的全局默认策略。

以下是恢复认证服务器的全局默认策略的示例：

```
TopsecOS# user auth global-config reset
```

user auth sms modify type <none|local|topsec> [**error-count** <*number1*>] [**id** <*string1*>] [**info** <*string2*>] [**ip** <*string3*>] [**passwd-length** <*number2*>] [**passwd-type** <num|character|both>] [**port** <*port*>] [**share-secret** <*string4*>] [**timeout** <*number3*>] [**validtime** <*number4*>] [**support-mode** <gsm|cdma>]

命令描述：

修改短信认证服务器的配置属性。

参数说明：

user auth sms modify	修改短信认证服务器的类型。
type	设置短信认证服务器的类型。
none|local|topsec	topsec 是短信中转发送服务器； local 表示短信猫直接连接在 NGFW 的 USB 口。
error-count	可选项，修改短信认证服务器的密码错误次数。
number1	数值类型，取值范围：1-10；默认值：3。
id	可选项，修改由短信中转服务器指派给当前网关的 ID 号。
string1	字符串类型，表示 ID 号。
info	可选项，修改自定义的短信提示语。
string2	字符串类型。
ip	可选项，修改短信中转服务器的 IP 地址。
string3	IP 地址字符串。
passwd-length	可选项，修改短信密码长度。
number2	数值类型，取值范围：1-8；默认值：6。

passwd-type	可选项，修改生成短信内容的要求。
num|character|both	数字|字母|数字和字母
port	可选项，修改短信中转服务器接收 NGFW 设备发送的短信的端口。
port	数值，表示端口，取值范围：0-65535。
share-secret	可选项，修改由短信中转服务器指定的认证共享通行串，必须与短信中转发送服务器的设置一致。
string4	字符串类型。
timeout	可选项，修改认证超时时间。当发送短信时间达到此处设定的值后，密钥需要重新协商。
number3	数值类型，单位：秒；取值范围：1-180；默认值：5。
validtime	可选项，修改短信密码有效期。
number4	数值类型，单位：秒；取值范围：60-86400；默认值：60。
support-mode	可选项，修改支持短信猫制式。
gsm|cdma	GSM 或者 CDMA。

以下是修改短信认证服务器的配置的示例：

设置短信服务器的短信类型为“topsec”，短信密码错误次数为“3 次”，短信中转服务器的 IP 地址为“192.168.92.132”，短信中转服务器的端口为“1812”，短信密码的超时时间为“5 秒”，并且支持 GSM 短信猫制式。

TopsecOS# **user auth sms modify type** topsec **error-count** *3* **ip** *192.168.92.132* **passwd-type** both **port** *1812* **timeout** *5* **support-mode** gsm

user auth sms show <cr>

命令描述：

显示短信认证服务器的配置信息。

以下是显示短信认证服务器的配置信息的示例：

TopsecOS# **user auth sms show**

user auth sms modify type 'topsec' ip '192.168.92.132' port 1812 id '0' share-secret null info null passwd-type 'both' timeout 5 validtime 60 passwd-length 6 error-count 3

5.3 门户配置

门户是一个校验用户 ID 的入口，同时关联一种认证服务器，具有认证属性的控制功能。门户管理提供数据的存储和实现认证服务器的各种认证协议。管理员通过门户配置模块，配置用户向 NGFW 认证的登录界面，实现将不同的认证用户分配到认证服务器上。

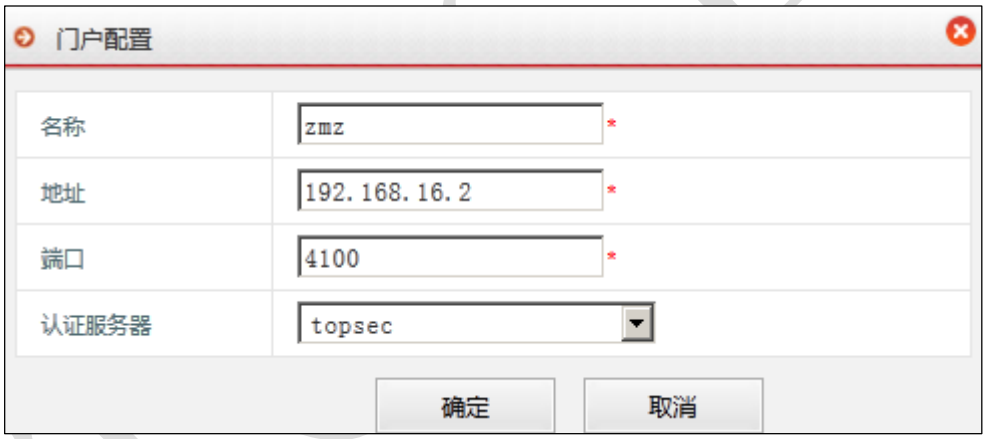
WEBUI 方式配置

在进行门户配置之前，需要先进行以下配置：

- 配置认证服务器，关于认证服务器的配置具体请参见 5.2 认证服务器。
- 配置用户信息，关于用户信息的配置具体请参见 5.1 用户管理。

步骤 1 选择 **用户管理** > **门户配置**。

步骤 2 点击『添加』，弹出“门户配置”窗口。

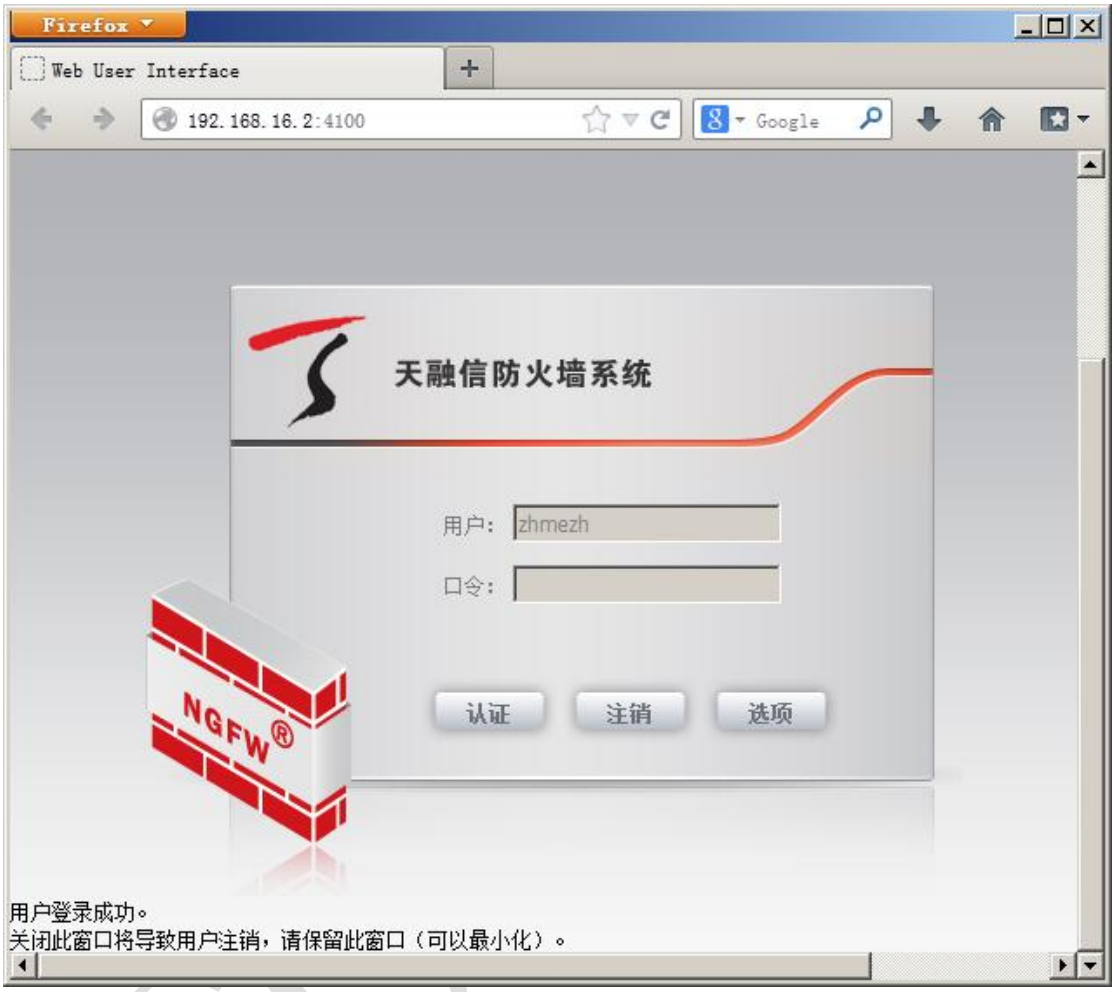


在设置门户配置信息时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置门户的名称。
地址	必选项，设置 NGFW 的接口 IP 地址。格式为：A.B.C.D。
端口	必选项，设置端口号。取值范围：1-65535。
认证服务器	选择认证服务器。

步骤 3 点击【确定】按钮完成门户的配置。

管理员可通过浏览器输入自定义的认证地址及端口进入自定义认证界面，如192.168.16.2:4100，然后输入已配置的用户名和密码，点击【认证】按钮，NGFW 即可对该用户进行身份认证，如下图所示。



CLI 方式配置

步骤	配置说明
1	配置认证服务器，具体请参见 5.2 认证服务器
2	配置门户策略

user auth portal add name <*string1*> **server-name** <*string2*> **address** <*string3*> **port** <*port*>

命令描述

添加一条门户策略。

参数说明

user auth portal add	添加门户策略。
name	必选项，设置门户策略名称。
string1	字符串类型，表示门户名称。
server-name	必选项，指定已存在的认证服务器。
string2	字符串类型，表示认证服务器的名称。
address	必选项，设置 NGFW 的接口 IP 地址。
string3	字符串类型，表示 IP 地址。
port	必选项，设置 NGFW 的端口号。
port	数值类型，表示端口号。取值范围：0-65535。

以下是添加门户信息的示例：

添加用户名称为“portal”、认证服务器为“radius”、NGFW 的接口 IP 地址为 172.16.16.2，端口号为 231 的门户策略。

TopsecOS# **user auth server add name** *radius* **protocol** radius **port** *1812* **time-out** *100* **host** *192.168.83.231* **radius-sharesecret** *topsec* **radius-authmode** pap **radius-clientip** *192.168.16.6*

TopsecOS# **user auth portal add name** *portal* **server-name** *radius* **address** *172.16.16.2* **port** *231*

user auth portal modify name <*string1*> [**server-name** <*string2*>] [**address** <*string3*>] [**port** <*port*>]

命令描述

修改门户配置信息。

参数说明

user auth portal modify	修改门户。
name	必选项，指定门户。
string1	字符串类型，表示门户名称。
server-name	可选项，修改门户所属的认证服务器。
string2	字符串类型，表示认证服务器的名称。
address	可选项，修改门户地址。
string3	字符串类型，表示 IP 地址。
port	可选项，修改门户端口号。
port	数值类型，表示端口号。取值范围：0-65535。

以下是修改门户配置信息的示例：

修改门户策略 portal 的端口号为 1813。

TopsecOS# **user auth portal modify name** *portal* **port** *1813*

user auth portal show <cr>

命令描述

显示门户信息。

以下是显示门户配置信息的示例：

TopsecOS# **user auth portal show** user auth portal add name 'uuu' server-name 'topsec' address '1.1.1.1' port 2323

user auth portal delete name <*string*>

命令描述

删除指定名称的门户配置信息。

以下是删除门户配置信息的示例：

TopsecOS# **user auth portal delete name** *portal*

user auth portal clean <cr>

命令描述

清空门户配置信息。

以下是清空门户配置信息的示例：

TopsecOS# **user auth portal clean**

5.4 PKI

PKI（Public Key Infrastructure，公钥基础设施）是建立于公钥密码体制上提供信息安全的一套体系和规范，可解决广大用户要求互联网上通信具备身份认证、数据防篡改、机密性和抗抵赖的安全需求。作为网络安全的核心技术，PKI 目前已广泛应用于电

子商务和电子政务，如 Web 服务器和浏览器间的安全通信、电子邮件源认证和机密性、网上信用卡交易、网上银行交易和 VPN 通信等。

PKI 系统的核心技术围绕着数字证书的申请、签发、存储、发布和撤销整个生命周期展开，通过为网络中的用户及网络设备颁发并验证证书，确保网络的可信任性。NGFW 内置 PKI 系统，可以为设备及用户签发证书，并支持对远程用户和隧道对端设备进行数字证书认证，甚至还支持对由第三方 CA 签发的证书进行合法性认证。

证书生命周期

数字证书的生命周期包括：申请、签发、存储、颁发、使用、验证和撤销，防火墙远程用户或对端设备证书的整个生命周期均由防火墙 PKI 系统主导完成。

1）申请证书。远程用户或对端设备管理员向防火墙管理员发起获取证书请求。

2）签发证书。防火墙管理员经审核该证书请求通过后，为该远程用户或对端设备签发证书，关于证书的签发具体请参见 5.4.4.2 管理证书。

4）存储证书。防火墙管理员将签发的证书下载至其管理主机中，关于证书的下载具体请参见 5.4.4.2 管理证书。

5）颁发证书。防火墙管理员通过邮件或 USBKey 等方式将签发的证书发送给远程用户或对端设备管理员。

6）使用证书。远程用户申请人员获取证书后将证书导入其计算机，设备管理员申请人员获取证书后将证书导入设备中。

7）验证证书。远程用户或证书使用过程中用户或设备根据本端保存的 CA 证书验证对端合法性。

8）撤销证书。证书私钥泄露、证书服务过期，证书执有者向防火墙提交证书撤销申请，此时，防火墙管理员则需撤销该证书并更新其 CRL。关于证书的撤销具体请参见 5.4.4.3 维护证书撤销列表，关于 CRL 的更新具体请参见 5.4.4.2 管理证书。

PKI 系统组成

PKI 系统组成部分主要包括：公钥密码技术、证书认证中心 CA、数字证书等。

1）公钥密码技术：即非对称加密技术，使用成对的公钥和私钥（公钥无法推导出私钥，而私钥可推导出公钥），公钥在网络上公开，而私钥需由用户谨慎保管，一旦私钥

泄露，为防止非法人员使用该证书实施网络欺骗，用户需向证书颁发机构声明证书丢失以更新证书。公钥密码技术可实现功能包括数据加密和数字签名。

（a）数据加密（保障数据的机密性，防止第三方窃听）：发送方使用接收方公钥加密，接收方使用自身的私钥解密，使用公钥密码技术加密数据的详细过程如下。

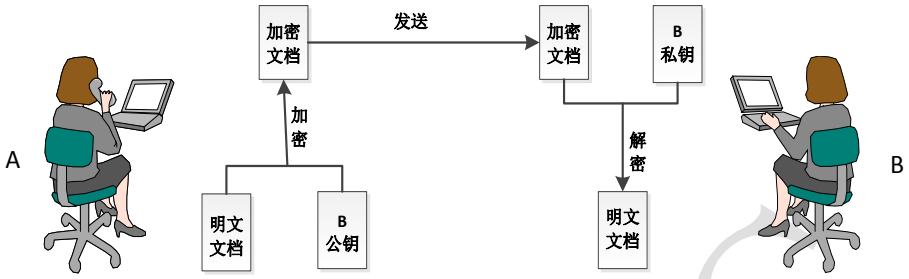


图 5-1 使用公钥密码技术加密数据

（b）数字签名（不对数据进行加密，但可确定来源是否可靠，数据是否被篡改）：发送方使用自身的私钥加密，接收方使用发送方的公钥解密。使用公钥密码技术进行签名实现源认证和数据完整性的详细过程如下。

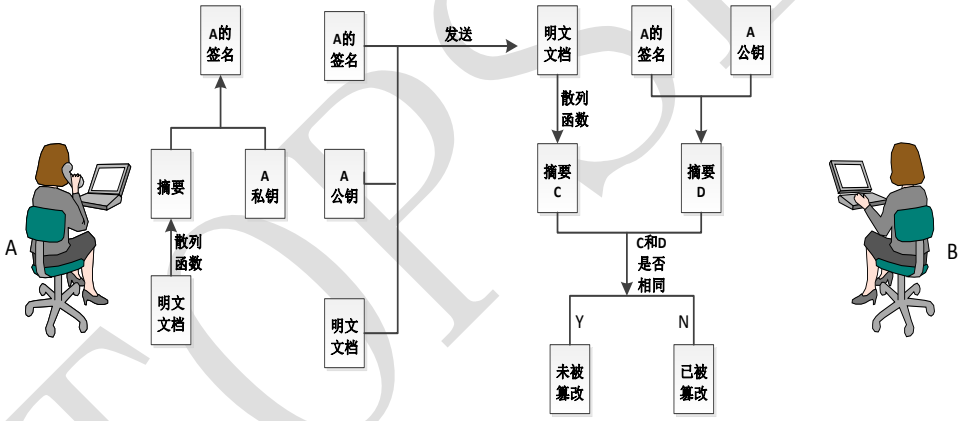


图 5-2 使用公钥密码技术签名

2）证书认证中心 CA（Certificate Authority）：负责签发、存储、撤销证书，是具有可信赖性、公证性特征的权威性机构，相对于互联网通信双方为可信任的第三方。CA 采用树形体系结构，除可签发和撤销证书外，还能为下级 CA 签名，总之，只要某个 CA 相信权威性认证机构的根 CA，由该 CA 签发的证书即可被互联网中用户认可。

3）数字证书（Digital Certificate）：又称为电子证书，是因特网上用来标志和证明网络通信双方身份的数字信息文件，网络中的用户或设备通信时，双方互相验证对方证书的有效性，从而实现保护电子邮件消息、向通信对端证明身份、保证 Internet 上安全通信等作用。证书示意图如下。

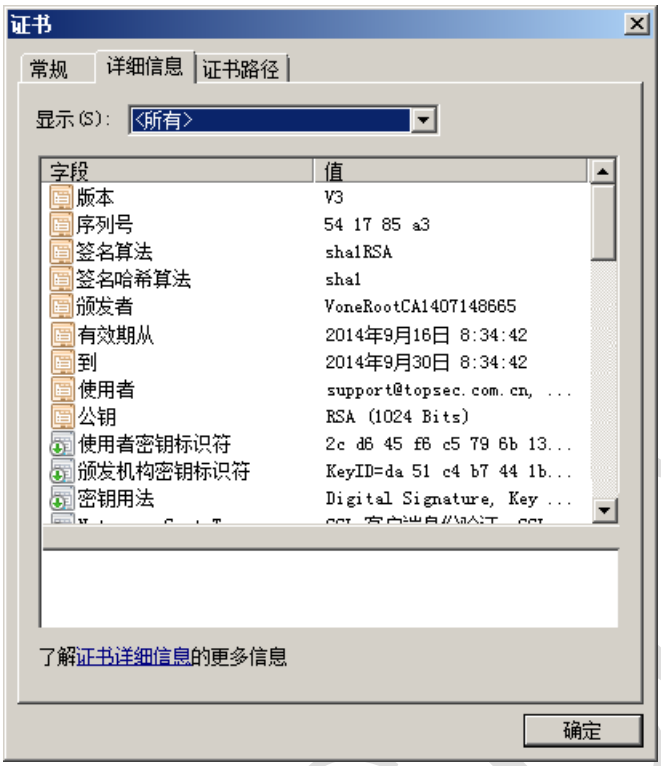


图 5-3 数字证书文件示意图

数字证书信息包括：公钥、颁发者、使用者、有效期、签名算法、证书序列号等。NGFW 支持以 DER、PEM、PKCS12、TAR 格式颁发证书，DER、PEM、PKCS12 格式证书包括证书文件和私钥文件，TAR 格式证书包括证书文件、私钥文件和根证书。

- 证书文件：证书文件中包含证书持有者的身份信息、公钥、有效期、证书序列号、及 CA 发行机构的数字签名等信息，在网络通讯中标识证书持有者的身份。
- 私钥文件：私钥文件是证书持有人的私有文件，与证书中的公钥组成一对互相匹配的公私钥对，是基于证书的加密体系的重要部分，私钥可推到出公钥，因此需要妥善保管，私钥一旦泄露，证书执有者需向证书颁发机构提出撤销或更新证书申请。
- 根证书：根证书是证书发行机构的自身证书，可以用来验证该发行机构所发行的证书的合法性。

5.4.1 本机证书

本机证书是本防火墙设备的证书。设备之间采用数字证书认证时，需根据对方的本机证书信息验证对方身份的合法性。由于出厂配置中，NGFW 没有本机证书，因此需由管理员手工导入。

NGFW 的本机证书可由 TopPolicy 或专门的 CA 中心下发，下发后的证书以文件形式存在磁盘或 USBKey 等存储载体中，管理员需要将它从存储载体中导入到防火墙中设备才可以使用。

证书导入可以有 3 种方式：

- 普通文件导入：包括一个证书文件，一个私钥文件。
- pkcs12 格式证书导入：包括一个证书文件，一个私钥文件。
- 打包文件方式导入：可以把证书文件、私钥文件、证书颁发机构的根证书打成一个.tar 的包，再导入。

说明

- NGFW 本机证书的导入需要将证书文件和私钥导入到 NGFW 中。NGFW 证书分为主证书和从证书
- 主证书只能导入 RSA 证书，从证书只能导入 ECC 证书。

下面介绍如何导入防火墙的本机证书。

WEBUI 方式配置

步骤 1 选择 **用户管理** > **PKI** > **本机证书**。

步骤 2 点击『添加』，如下图所示。

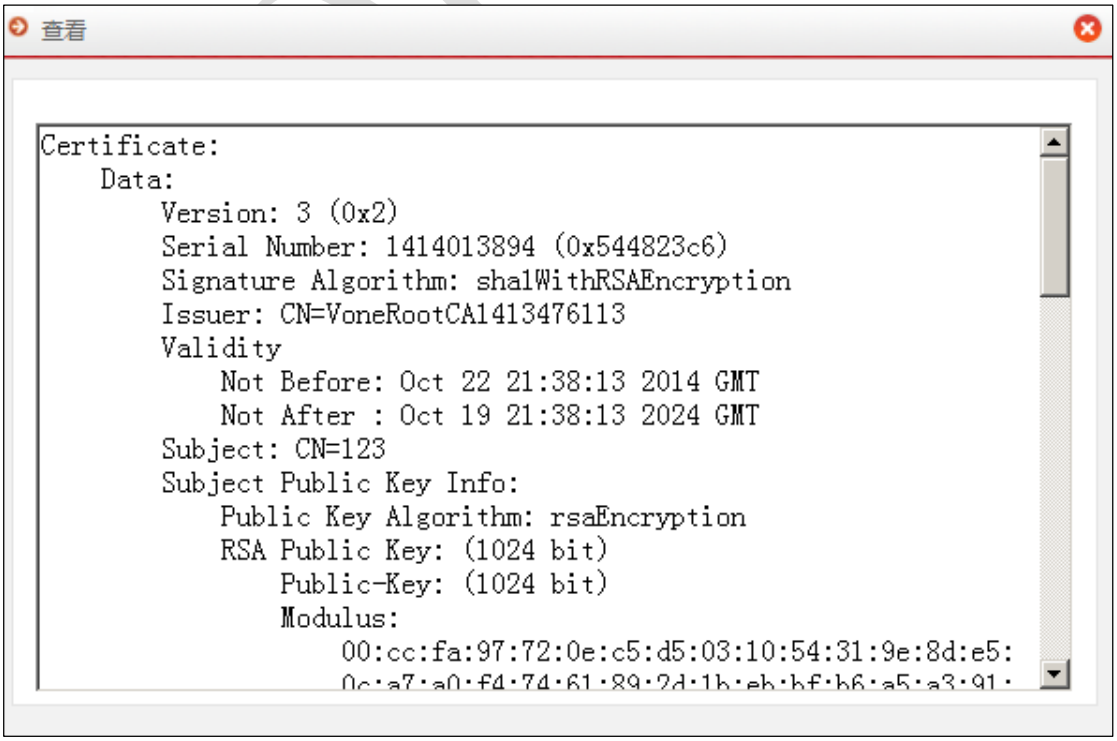
选择管理员管理主机中保存的本机证书的类型，点击【浏览】按钮导入证书，最后点击【确定】按钮完成证书的导入。

证书导入成功后，将会在“本机证书”中显示新导入的证书信息，如下图所示。

说明

- ✧ 每台设备只能有一份证书以验证其身份。如果管理员导入第二份证书，将自动覆盖以前所导入的证书。
- ✧ 以 TAR 文件格式导入本机证书的同时也导入了该证书颁发机构的 CA 根证书，因此无须再单独导入 CA 证书。

步骤 3 点击“详细”栏的『详细』，可以查看该证书的详细信息，如下图所示。



CLI 方式配置

pki localcert getbyfile certfile <*string1*> **keyfile** <*string2*> [**passwd** <*string3*>]

命令描述：

以普通文件方式导入证书。

参数说明：

pki localcert getbyfile	文件方式导入本机证书及私钥。
certfile	必选项。指定证书文件名。
string1	字符串类型。证书文件名。
keyfile	必选项。指定证书私钥文件名。
string2	字符串类型。私钥文件名，上传至/tmp 目录下，不需要全路径。
passwd	可选项。指定打开文件的密码。
string3	字符串类型。

pki localcert getbypkcs12 certfile <*string1*> [**passwd** <*string2*>]

命令描述：

以 pkcs12 格式导入证书。

参数说明：

pki localcert getbypkcs12	以 pkcs12 文件格式导入本机证书及私钥。
certfile	必选项，指定 pkcs12 证书文件名。
string1	字符串类型。加密证书文件名，上传至/tmp 目录下，不需要全路径。
passwd	可选项，指定打开证书文件的密码。
string2	字符串类型。密钥。

pki localcert getbytar certfile <*string*>

命令描述：

以 tar 文件方式导入本机证书及私钥。

参数说明：

pki localcert getbytar	以 tar 文件方式导入本机证书及私钥。
certfile	必选项，指定 tar 证书文件名。
string	字符串类型。打包证书文件名，上传至/tmp 目录下，不需要全路径符串。

pki localcert show <cr>

命令描述：

查看本机证书。

pki localcert delete <cr>

命令描述：

删除本机证书。

pki localcert type-set <primary|secondary>

命令描述：

本地证书类型设置。

参数说明：

pki localcert type-set	本地证书类型设置。
primary|secondary	主证书|从证书

pki localcert type-show <cr>

命令描述：

显示本地证书类型。

5.4.2 对端证书

对端证书指与 NGFW 通信的对端设备的证书文件，用于 NGFW 向对端设备发送加密的数据报文，以防止非法人员截获 NGFW 与对端设备的通信内容。对端证书的内容包含对端设备的公钥、颁发者、使用者、有效期等信息。

NGFW 向对端设备发送数据报文时，使用对端证书中的公钥加密数据报文（只有拥有该公钥对应的私钥的人员才可解密该数据报文），对端设备接收到该数据包报文，则通过自身的私钥可将数据报文解密，进而查看数据报文的具体内容。

NGFW 与 IPSec VPN 设备采用证书方式进行认证时，需在 NGFW 上导入对端 IPSec VPN 设备的证书文件。下面介绍如何在 NGFW 上添加对端设备的证书文件。

WEBUI 方式配置

步骤 1 选择 **用户管理** > **PKI** > **对端证书**。

步骤 2 点击『添加』。

点击【浏览】按钮，选择隧道对端证书的证书文件（DER 格式），然后点击【确定】按钮即可导入对端证书。

对端证书导入成功后，如下图所示。

步骤 3 点击“详细”栏中的『详细』，可以查看该证书的详细信息。

CLI 方式配置

pki remotecert import certfile <*string*>

命令描述：

导入对端设备证书。

参数说明：

pki remotecert import	导入证书。
certfile	必选项，指定证书文件。
string	字符串类型。

pki remotecert show [**index** <*number*>]

命令描述：

查看对端设备证书。

参数说明：

pki remotecert show	查看证书。
index	可选项，指定证书序号。
number	数值类型。

pki remotecert delete index <*number*>

命令描述：

删除对端设备证书。

参数说明：

pki remotecert delete	删除证书。
index	必选项，指定证书序号。
number	数值类型。

5.4.3 第三方 CA 证书

CA 基于树形结构进行组织管理，任何 CA 可添加其子 CA 并为用户颁发证书，且子 CA 由其上级 CA 认证，用户只要相信某权威机构认证中心 CA，即信任由该权威认证机构颁发或由其任意级别子 CA 颁发的证书。因此，企业或事业单位可只向互联网上的权威认证中心申请一个数字证书，通过 NGFW 的内置 CA 功能，即可为内网中的所有用户签发公认合法的数字证书。CA 树形结构如下图所示。

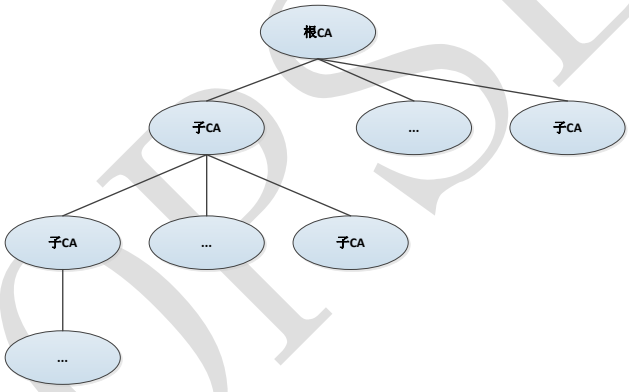


图 5-4 CA 树形结构图

隧道对端设备或移动用户的数字证书由第三方 CA 颁发时，NGFW 同样可根据其数字证书对对端设备或移动用户进行本地认证。

对于第三方 CA 签发的证书，天融信下一代防火墙验证证书是否有效性的方式包括离线验证和在线验证。

- 离线认证：是指利用第三方 CA 的根证书（RootCA）和证书撤销列表（CRL）来验证证书的有效性，防火墙通过该方式验证证书时，需要导入第三方 CA 的根证书和 CRL。
- 在线认证：是指通过第三方 CA 的根证书以及向轻目录访问协议（LDAP）服务器和 HTTP 协议服务器在线查询证书是否有效。

下面介绍如何在 NGFW 上添加第三方 CA 根证书以及如何更新第三方 CA 的 CRL。

说明

- ✧ 如果证书不是根 CA 签发的，则在此需要导入上一级 CA 证书直到根 CA 的证书。
- ✧ NGFW 支持导入**多个** CA 根证书，可对由不同 CA 机构颁发的证书进行认证。

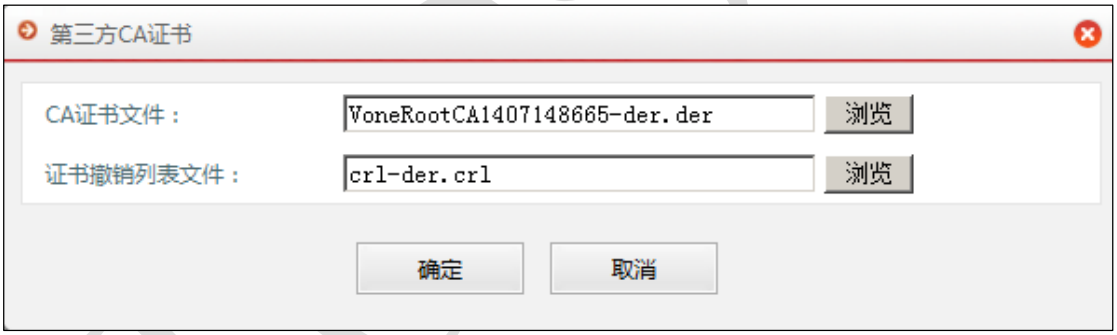
5.4.3.1 配置 CA 根证书

管理员可以在 NGFW 上添加第三方 CA 证书的根证书，下面介绍如何添加和查看第三方 CA 根证书。

WEBUI 方式配置

步骤 1 选择 **用户管理 > PKI > 第三方 CA 证书**。

步骤 2 点击『添加』，如下图所示。



点击【浏览...】按钮选择管理主机上存放的 CA 证书文件和证书撤销列表文件，然后点击【确定】按钮完成第三方 CA 证书的导入。

证书导入成功后，如下图所示。

步骤 3 查看第三方 CA 证书。

点击详细栏中的『详细』，可以查看该证书的详细信息。

CLI 方式配置

pki cacert import certfile <*string1*> [**crlfile** <*string2*>]

命令描述：

从文件中导入 CA 证书及 CRL。

参数说明：

pki cacert import	从文件中导入 CA 证书及 CRL。
certfile	必选项，指定证书文件名。
string1	字符串类型。CA 证书文件名。
crlfile	可选项，指定 CRL 文件名。
string2	字符串类型。CRL 文件名，上传至/tmp 目录下，不需要全路径。

pki cacert show [**index** <*number*>]

命令描述：

查看 CA 证书及相关信息。

参数说明：

pki cacert show	查看 CA 证书及相关信息。
index	可选项，指定 CA 证书序号。
number	数值类型，表示证书序号。

以下是查看 CA 证书及相关信息的示例：

```
TopsecOS# pki cacert show
INDEX:    1
CN:       sdf
Version:          3
NotBefore:        Nov 11 05:12:25 2014 GMT
NotAfter:         Nov    8 05:12:25 2024 GMT
Issuer: CN=VoneRootCA1415758784
Subject:CN=sdf
haveCrl:          no
```

pki cacert delete index <*number*>

命令描述：

删除一个 CA 证书及其相关信息。

参数说明：

pki cacert delete	删除一个 CA 证书及其相关信息。
index	必选项，指定 CA 证书序号。
number	数值类型。

pki cacert clean <cr>

命令描述：

清空 CA 证书及相关信息。

5.4.3.2 管理 CRL

NGFW 支持第三方 CA 的 CRL 手工更新，也支持 CRL 自动下载，启用 NGFW 自动下载 CRL 后，NGFW 将会定时自动下载更新第三方 CRL 文件。

下面介绍如何管理第三方 CA 的 CRL。

WEBUI 方式配置

步骤 1 选择 **用户管理** > **PKI** > **第三方 CA 证书**，如下图所示。

步骤 2 更新证书撤销列表 CRL。

1）手动更新 CRL。

点击“CRL 导入”栏中的导入图标“ ”，可手动导入第三方 CA 对应的 CRL。

2）周期更新 CRL。

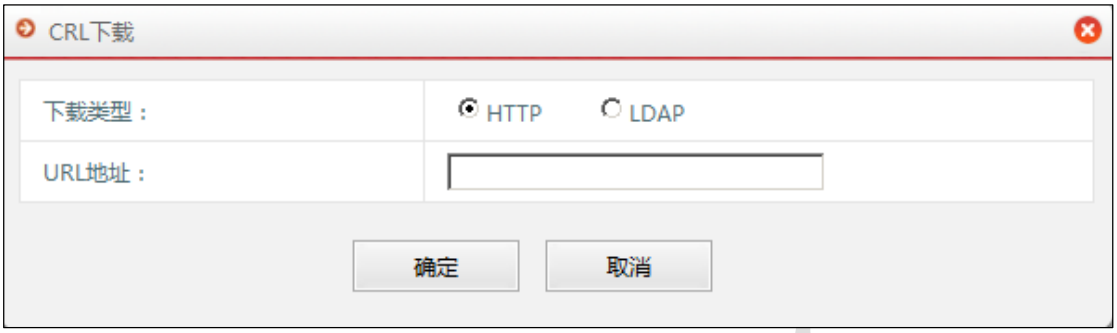
（a）配置自动下载 CRL 的周期。

点击『CRL 自动下载配置』，可配置 NGFW 自动下载 CRL 的周期，单位：秒；取值范围：60-172800；默认值：86400。

（b）配置自动下载 CRL 的服务器。

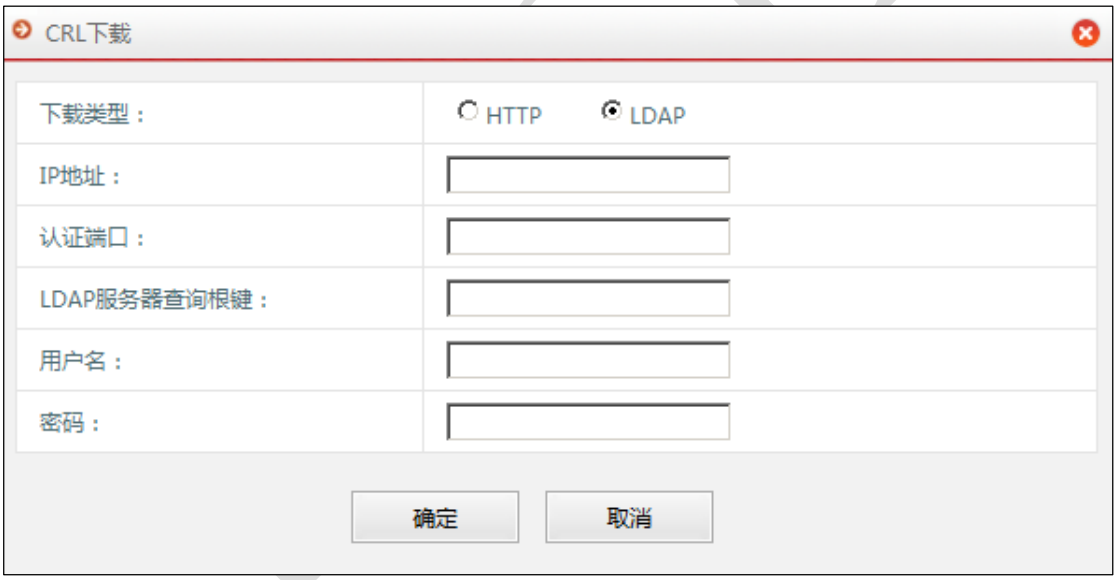
点击“CRL 下载设置”栏中的设置图标“ ”。

① 如果下载类型选择“HTTP“时，如下图所示。



输入使用 HTTP 协议向第三方 CA 发送下载请求时，指向 CA 服务器 CRL 信息的链接，然后点击【确定】按钮。

② 如果下载类型选择“LDAP”时，如下图所示。



在设置以 LDAP 方式下载 CRL 时，各项参数的具体说明如下表所示。

参数	说明
IP 地址及认证端口	使用 LDAP 协议向第三方 CA 发送下载 CRL 请求时，指定 LDAP 服务器的 IP 地址（或域名）及查询端口号。
LDAP 服务器查询根键	设置 LDAP 服务器进行证书查找的根域，关于 LDAP 服务器配置的具体操作步骤请参见 5.2.3 添加 Ldap 服务器。
用户名及密码	指定登录 LDAP 服务器时使用的用户名和密码。

参数设置完成后，点击【确定】按钮完成 CRL 自动更新服务器的配置。

3）即时自动更新 CRL 文件。

点击“CRL 下载”栏中的下载图标“  ”，NGFW 立即从设定的 LDAP 服务器或 HTTP 服务器上下载 CRL 文件。

CLI 方式配置

pki cacert loadcrl index <*number*> **crlfile** <*string*>

命令描述：

手动导入第三方 CA 的 CRL 列表。

参数说明：

pki cacert loadcrl	导入 CRL 列表。
index	必选项，指定 CA 证书序号。
number	数值类型。
crlfile	必选项，指定 CRL 文件名。
string	字符串类型。

pki cacert downcrl index <*number*>

命令描述：

向 HTTP 或 LDAP 服务器手动立即更新第三方 CA 的 CRL。

参数说明：

pki cacert downcrl	手动下载 CA 的 CRL。
index	必选项，指定 CA 证书序号。
number	数值类型。

pki cacert modifycrlproto index <*number*> **proto** <ldap|http>

命令描述：

修改下载第三方 CRL 所使用的协议。

参数说明：

pki cacert modifycrlproto	修改 CA 的 CRL 下载协议。
index	必选项，指定 CA 证书序号。
number	数值类型。
proto	必选项，指定通过哪种协议下载 CRL 文件。
ldap|http	LDAP 协议|HTTP 协议

pki cacert modifyhttpconf index <*number*> **httpconf** <*string*>

命令描述：

修改通过 http 协议下载第三方 CRL 的地址。

参数说明：

pki cacert modifyhttpconf	修改 CA 通过 http 协议下载 CRL 的地址。
index	必选项，指定 CA 证书序号。
number	数值类型。
httpconf	必选项。指定使用 http 协议向第三方 CA 发送下载 CRL 请求时，指定指向 CA 服务器的 CRL 信息的链接。
string	字符串类型。

pki cacert modifyldapconf index <*number1*> **ip** <*ipaddress*> **port** <*number2*> **basedn** <*string1*>

[**userid** <*string2*>] [**passwd** <*string3*>]

命令描述：

修改通过 LDAP 协议下载第三方 CRL 的配置。

参数说明：

pki cacert modifyldapconf	修改 CA 通过 LDAP 协议下载 CRL 的配置。
index	必选项，指定 CA 证书序号。
number1	数值类型。
ip	必选项，指定 LDAP 服务器的 ip 地址（或域名）。
ipaddress	ip 地址字符串。
port	必选项，指定 LDAP 服务器的查询端口号。
number2	数值类型。
basedn	必选项，指定 LDAP 服务器的查询根键。
string1	字符串类型。
userid	可选项，指定登录 LDAP 服务器的用户帐号。
string2	字符串类型。
passwd	可选项，指定登录 LDAP 服务器的用户密码。
string3	字符串类型。

pki cacert showcrl index <*number*>

命令描述：

查看 CA 证书的 CRL 详细信息。

参数说明：

pki cacert showCRL	查看 CA 证书的 CRL 详细信息。
index	必选项，指定 CA 证书序号。
number	数值类型。

pki cacert showcrlproto index <*number*> [**proto** <ldap|http>]

命令描述：

查看一个第三方 CA 的 CRL 下载配置。

参数说明：

pki cacert showcrlproto	查看一个第三方 CA 的 CRL 下载配置。
index	必选项，指定 CA 证书序号。
number	数值类型。
proto	可选项，指定下载 CRL 文件所使用的协议类型。
ldap|http	LDAP 协议|HTTP 协议

pki cacert delcrl index <*number*>

命令描述：

删除一个第三方 CA 证书的 CRL。

参数说明：

pki cacert delcrl	删除一个第三方 CA 证书的 CRL。
index	必选项，指定 CA 证书序号。
number	数值类型。

pki cacert crltimer [**interval** <*number*>]

命令描述：

指定自动下载第三方 CA 的 CRL 周期。

参数说明：

pki cacert crltimer	指定 CRL 信息更新周期。
interval	可选项，指定下载间隔，单位：秒。
number	数值类型。

5.4.4 本地 CA 策略

NGFW 内置 CA，可签发、存储、发布和撤销证书，因此，企业或者事业单位可通过 NGFW 自建 CA 中心，不必购买单独的认证体系，为内部局域网构建完善的证书管理系统。

NGFW 为远程用户及对端设备颁发证书及认证的大体结构如下图所示。

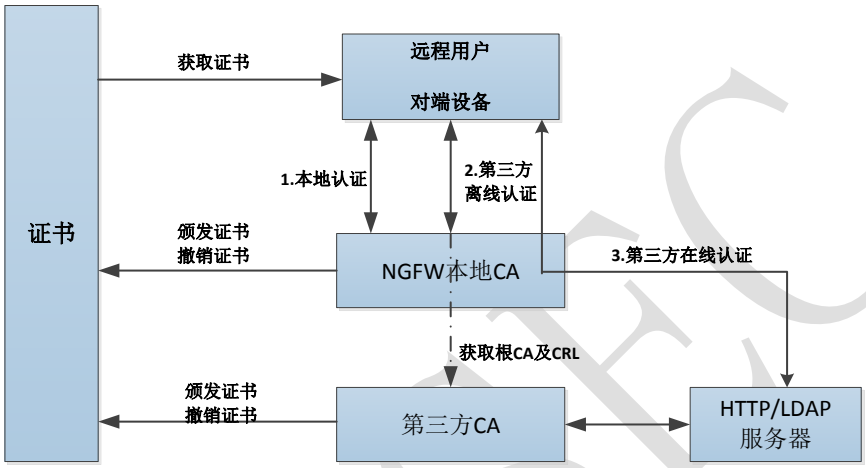


图 5-5 本地 CA 工作流程图

管理 NGFW 内置 CA 的步骤为：

1）构建本地 CA。管理员导入或生成 NGFW 的根证书和私钥，即成功建立本地 CA，关于 CA 根证书的导入具体请参见 5.4.4.1 构建本地 CA。

2）管理证书。对设备或移动用户进行数字证书的签发、存储、撤销操作，关于证书的管理具体请参见 5.4.4.2 管理证书。

3）CRL 列表维护。构建内置 CA 时导入 CRL 列表，证书撤销后重新发布 CRL 列表，以对证书的有效性进行验证。关于 CRL 列表的重新发布具体请参见 5.4.4.3 维护证书撤销列表。

5.4.4.1 构建本地 CA

内置 CA 根证书和私钥可以通过以下几种方式导入：本地生成、使用 NGFW 的本机证书、导入其它 CA 签发的根证书和私钥。

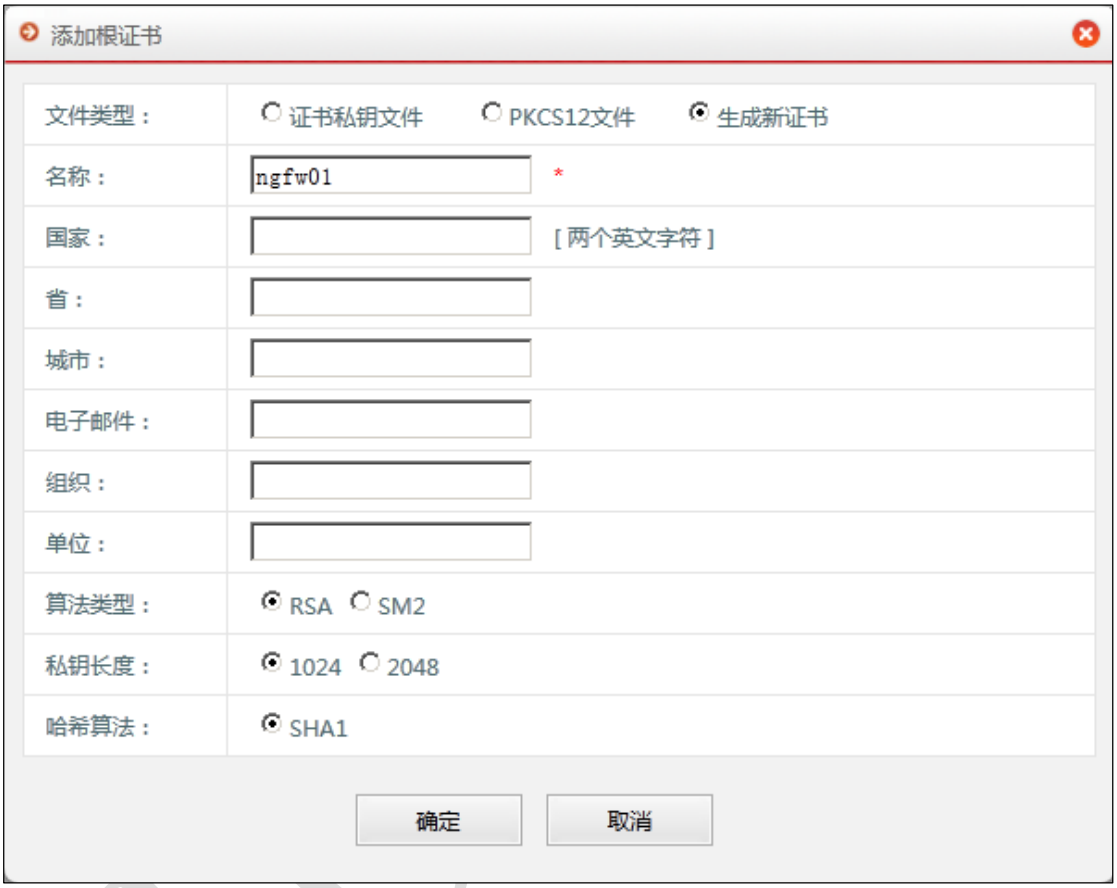
管理员支持内置 CA 根证书的导出，用于和第三方 CA 签发的证书进行交叉认证。

WEBUI 方式配置

步骤 1 选择 **用户管理 > PKI > 本地 CA 策略**。

步骤 2 添加根证书。

点击“根证书”区域的『添加』，如下图所示。



在获取根证书时，各项参数的具体说明如下表所示。

参数	说明
证书秘钥文件	当内置 CA 根证书为上一级 CA 签发，且证书文件的证书文件和私钥文件分开存储时，需要分别设置证书和私钥文件在管理主机上的存放路径。上传的证书和私钥两个文件的大小之和不能超过 10M。
PKCS12 文件格式导入	当内置 CA 根证书为上一级 CA 签发，且证书文件采用 PKCS12 的格式存储时，需要设置证书文件的存放路径和证书文件的密码。
生成新证书	NGFW 作为根 CA 为自身生成一个新证书作为根证书。必须要设置证书的名称，其他属性为可选项 。
名称	必选项。生成新的根证书的名称。

参数	说明
	说明： 最多输入 31 个字符。
国家	生成新的根证书的网关设备的属性。 说明： 限两个英文字符。
省、城市、电子邮件、组织、单位	生成新的根证书的网关设备的属性。
算法类型	设置加解密数据包时使用的算法类型。 可选项：RSA、SM2。
密钥长度	设置公钥的密钥长度。 说明： “RSA”算法对应的公钥密钥长度可选择 1024 或 2048。 “SM2”算法对应的公钥密钥长度只可选择 256。
哈希算法	设置作校验的签名使用的哈希算法。 说明： “RSA”算法对应的签名哈希算法只可选择 SHA1。 “SM2”算法对应的签名哈希算法只可选择 SM3。

其中选择“生成新证书”时，参数“算法类型”、“密钥长度”、“哈希算法”的可选项对应关系如下表所示。

算法类型	密钥长度	哈希算法
RSA	1024|2048	SHA1
SM2	256	SM3

设置完成后，点击【确定】按钮完成证书的导入。根证书导入成功后，如下图所示。

说明

- ✧ 每台设备只能有一份客户端根证书用来生成移动用户所用的客户端证书。如果管理员导入第二份证书，将自动覆盖以前所导入的证书。
- ✧ 当更新客户端根证书后，以前发放的移动用户的客户端证书将全部失效，需要管理员重新为移动用户发放证书。

步骤 3 查看根证书。

点击详细栏中的『详细』，可以查看该证书的详细信息。

步骤 4 导出根证书。

NGFW 支持以两种文件格式导出根证书：DER 格式和 PEM 格式。

勾选根证书文件，点击『导出』可以将 NGFW 的根证书导出到本地。

CLI 方式配置

pki localca rootcert create name <*string1*> [**algtype** <rsa|sm2>] [**city** <*string2*>] [**country** <*string3*>] [**email** <*string4*>] [**len** <256|1024|2048>] [**organization** <*string5*>] [**province** <*string6*>] [**revokedate** <*string7*>] [**unit** <*string8*>] [**hash** <sm3|sha1>]

命令描述：

创建客户端认证 CA 根证书。

参数说明：

pki localca rootcert create	创建客户端认证根证书。
name	必选项，指定证书名。
string1	字符串类型。必填项。
algtype	可选项，设置加解密数据包时使用的算法类型。
rsa|sm2	RSA|SM2
city	可选项，城市名称。
string2	字符串类型。
country	可选项，国家名称。
string3	字符串类型。仅可输入两位英文字符。
email	可选项，电子邮件地址
string4	字符串类型。
len	可选项，设置公钥的密钥长度。
256|1024|2048	256bit|1024bit|2048bit
organization	可选项，组织名称。
string5	字符串类型。
province	可选项，省或州名称。
string6	字符串类型。

revokedate	可选项，指定证书最后有效日期。
string7	字符串类型。格式为 yyyy/mm/dd。
unit	可选项，单位名称。
string8	字符串类型。
hash	可选项，设置作校验的签名使用的哈希算法。
sm3|sha1	SM3|SHA1

pki localca rootcert getbyfile certfile <*string1*> **keyfile** <*string2*> [**passwd** <*string3*>]

命令描述：

以文件方式导入客户端认证 CA 根证书。

参数说明：

pki localca rootcert getbyfile	以文件方式导入客户端认证根证书。
certfile	必选项，指定证书文件名。
string1	字符串类型。
keyfile	必选项，指定证书私钥文件名。
string2	字符串类型。
passwd	可选项，设置打开私钥文件的密码。
string3	字符串类型。

pki localca rootcert getbypkcs12 certfile <*string1*> [**passwd** <*string2*>]

命令描述：

以 pkcs12 文件方式导入客户端认证根证书。

参数说明：

pki localca rootcert getbypkcs12	以 pkcs12 文件方式导入客户端认证根证书。
certfile	必选项，指定 pkcs12 证书文件名。
string1	字符串类型。
passwd	可选项，指定打开证书文件的密码。
string2	字符串类型。

pki localca rootcert show <cr>

命令描述：

查看客户端认证 CA 根证书。

以下是查看客户端认证 CA 根证书的示例：

```
TopsecOS# pki localca rootcert show
```

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=VoneRootCA1415758784
        Validity
            Not Before: Nov 12 02:19:44 2014 GMT
            Not After : Nov  9 02:19:44 2024 GMT
        Subject: CN=VoneRootCA1415758784
```

pki localca rootcert export type <der|pem|pkcs12> [**password** <*string*>]

命令描述：

导出客户端认证 CA 根证书。

参数说明：

pki localca rootcert export	导出客户端认证 CA 根证书。
type	必选项，指定证书类型。
der|pem|pkcs12	支持四种格式导出，根据需要选择。
password	必选项，指定打开证书文件的密码。
string	字符串类型。

5.4.4.2 管理证书

为内置 CA 的导入根证书后，NGFW 即可为设备或移动用户签发证书，签发的证书采用证书名称来唯一标识证书。天融信下一代防火墙本地 CA 签发的数字证书可为 DER、PEM、PKCS12、TAR 格式。

1）DER 格式：内容为二进制编码的 ASCII 文件，扩展名为.der，数字证书的公钥和私钥分盘存储。

2）PEM（Privacy Enhanced Mail）格式：内容为 Base64 编码的 ASCII 码文件，扩展名为.pem，数字证书的公钥和私钥分盘存储。

3）PKCS12（Personal Information Exchange ）格式：以加密的二进制形式存储证书的公钥和私钥，扩展名为.p12，数字证书的公钥和私钥分盘存储。通常用于用户在 windows 计算机中导入/导出数字证书公钥和私钥。

4）TAR 格式：为打包过后的证书文件，文件内容包括证书、私钥和证书颁发机构的根证书。与其他证书文件不同之处 TAR 格式文件包括根证书，以 TAR 方式导入数字证书的同时，也导入了该证书颁发机构的 CA 根证书。

对于已经生成的证书，管理员可以查看证书属性、将证书导出到管理员所在主机上，也可以将证书撤销、删除或一次性清空，下面介绍管理员如何签发、撤销、查看证书。

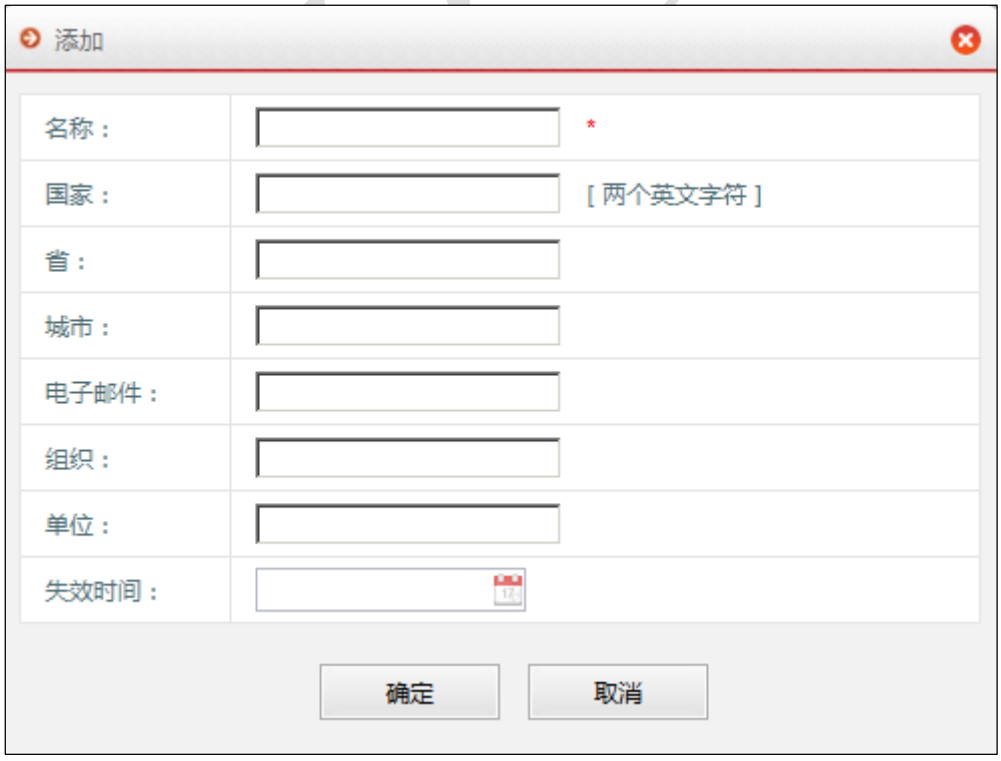
WEBUI 方式配置

步骤 1 选择 **用户管理 > PKI > 本地 CA 策略**。

步骤 2 签发证书。

1）签发证书。

点击“签发证书”区域的『添加』，如下图所示。

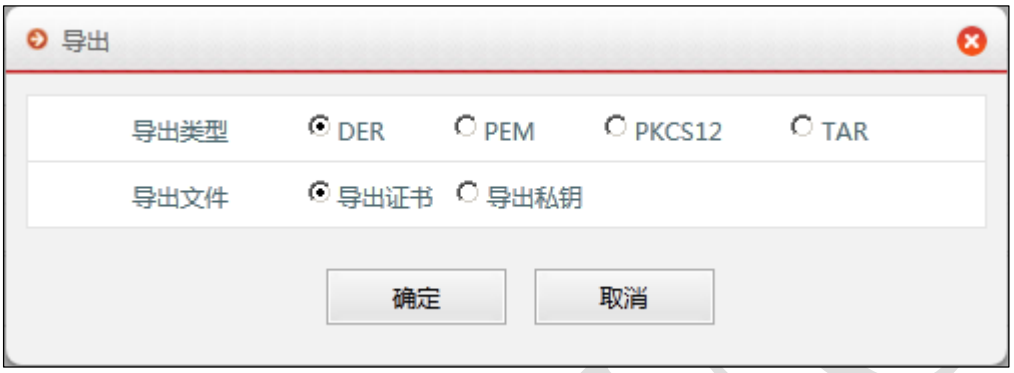


在“名称”处输入新证书的名称，该名称唯一地标识证书。国家、省、城市、电子邮件、组织、单位，以及证书的失效时间均为证书的属性字段，为可选输入项。

参数设置完成后，点击【确定】按钮完成生成证书。

步骤 3 导出证书。

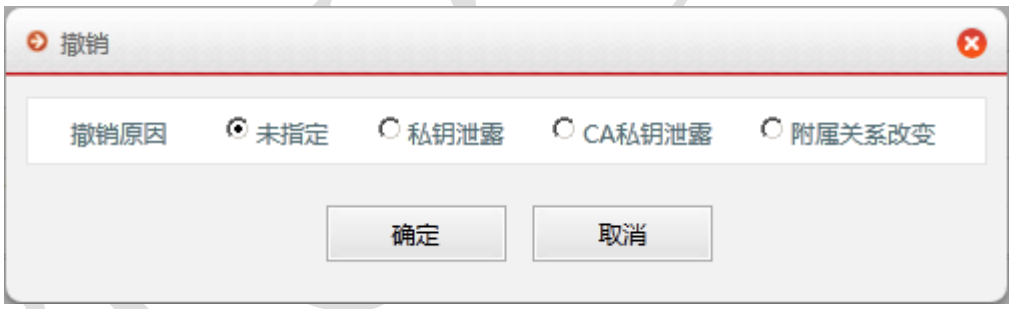
选择待导出的证书，点击『导出』，如下图所示。



选择证书导出格式，点击【确定】按钮可将用户证书导出到管理员的管理主机上。

步骤 4 撤销证书。

选择待撤销的证书，点击『撤销』，如下图所示。



选择撤销证书的原因，点击【确定】按钮完成证书的撤销。证书撤销后，证书状态栏显示“revoked”。

说明

- ✧ 客户端证书密钥长度与根证书密钥长度相同，即当根证书的密钥长度为 1024 位时，签发的证书密钥长度也为 1024 位；当根证书的密钥长度为 2048 位时，签发的证书密钥长度也为 2048 位。
- ✧ 签发的证书类型与根证书的类型一致，即 RSA 类型的根证书只能签发 RSA 类型的证书，ECC 类型的根证书只能签发 ECC 类型的证书。

CLI 方式配置

pki localca clientcert create name <*string1*> [**city** <*string2*>] [**country** <*string3*>] [**email** <*string4*>] [**organization** <*string5*>] [**province** <*string6*>] [**unit** <*string7*>] [**revokedate** <*string8*>]

命令描述：

创建客户端认证证书。

参数说明：

pki localca clientcert create	创建客户端认证根证书。
name	必选项，指定证书名。
string1	字符串类型。
city	可选项，城市名称。
string2	字符串类型。
country	可选项，国家名称。
string3	字符串类型。仅可输入两位英文字符。
email	可选项，电子邮件地址。
string4	字符串类型。
organization	可选项，组织名称。
string5	字符串类型。
province	可选项，省或州名称。
string6	字符串类型。
unit	可选项，单位名称。
string7	字符串类型。
revokedate	可选项，指定证书最后有效日期。
string8	字符串类型。格式为 yyyy/mm/dd。

pki localca clientcert show [**name** <*string*>]

命令描述：

查看客户端认证证书。

参数说明：

pki localca clientcert show	查看客户端认证根证书。
name	可选项，证书名称（客户端用户名）。
string	字符串类型。

pki localca clientcert delete [**name** <*string*>]

命令描述：

删除客户端认证根证书。

参数说明：

pki localca clientcert delete	删除客户端认证证书。
name	可选项，指定证书名称（客户端用户名）。
string	字符串类型。

pki localca clientcert clean <cr>

命令描述：

清空客户端认证根证书。

pki localca clientcert export name <*string1*> **type** <der|pem|pkcs12|tar> [**password** <*string2*>]

命令描述：

导出客户端认证证书。

参数说明：

pki localca clientcert export	导出客户端认证证书。
name	必选项，指定客户端证书名称。
string1	字符串类型。
type	必选项，指定证书类型。
der|pem|pkcs12|tar	支持四种格式导出，根据需要选择。 pkcs12：网关支持该种格式。
password	可选项，指定打开证书文件的密码。
string2	字符串类型。

pki localca clientcert batch-export type <der|pem|pkcs12|tar> [**password** <*string*>]

命令描述：

批量导出客户端认证证书。

参数说明：

pki localca clientcert batch-export	批量导出客户端认证证书。
type	必选项，指定证书类型。
der|pem|pkcs12|tar	支持四种格式导出，根据需要选择。 pkcs12：网关支持该种格式。
password	可选项，指定打开证书文件的密码。

string	字符串类型。

pki localca signcertreq revoke name <*string*> [**reason**

<unspecified|keycompromise|cacompromise|affiliationchanged>]

命令描述：

撤销证书文件。

参数说明：

pki localca signcertreq revoke	撤销证书文件。
name	必选项，指定证书文件的名称。
string	字符串类型。
reason	可选项，设置撤销该证书文件的原因。
unspecified|keycompromise| cacompromise|affiliationchanged	未指定|密钥泄露|CA 密钥泄露|附属关系改变

5.4.4.3 维护证书撤销列表

证书撤销列表 CRL 指定了所有被撤消证书的唯一序列号，当防火墙签发的数字证书失效后，防火墙作为 CA 需要对 CRL 列表进行更新，以当防火墙作为其他 CA 的第三方 CA 时，供其他 CA 更新防火墙的 CRL，以验证由防火墙颁发的证书是否合法。下面介绍管理员如何维护证书撤销列表。

WEBUI 方式配置

步骤 1 选择 **用户管理** > **PKI** > **本地 CA 策略**。

步骤 2 查看撤销列表。

点击『查看撤销列表』，可以查看 NGFW 最新的 CRL。

步骤 3 发布新撤销列表。

点击『发布新撤销列表』，则 NGFW 将更新其 CRL。

步骤 4 导出撤销列表。

点击『导出撤销列表』，可以将 NGFW 作为 CA 的 CRL 以 DER 或 PEM 格式导出到管理员所在主机上。

CLI 方式配置

pki localca crl creat <cr>

命令描述：

创建客户端认证 CA 根证书文件撤销列表 CRL 文件。

pki localca crl export type <der|pem>

命令描述：

导出客户端认证 CA 根证书的 CRL 文件。

参数说明：

pki localca crl export	导出客户端认证 CA 根证书文件撤销列表 CRL 文件。
type	指定证书类型。
der|pem	根据需要选择。

pki localca crl show <cr>

命令描述：

查看客户端认证 CA 根证书文件撤销列表 CRL 文件。

pki localca crl revoke name <*string*> [**reason**

<unspecified|keycompromise|cacompromise|affiliationchanged>]

命令描述：

导出客户端认证 CA 根证书的 CRL 文件。

参数说明：

pki localca crl revoke	吊销客户端认证 CA 签发的客户端证书。
name	必选项，设置证书名称。
string	字符串类型，根据需要选择。
reason	吊销原因。
unspecified|keycompromise|cacompromise|affiliationchanged	unspecified：未指定； keycompromise：密钥泄露； cacompromise：CA 密钥泄露； affiliationchanged：附属关系改变。

6 网络管理

NGFW 作为一种网关型产品，通常部署在各个安全区域的入口或交点，可以通过交换机或 HUB 将安全区收缩为一个入口，并将此入口点连接到防火墙的网络接口。因此在安装 NGFW 之前，网络管理人员应根据网络应用的实际情况以及网络中主机、服务器等设备的安全属性来规划安全区域，合理的设置防火墙的网络管理功能。

本章主要内容包括：

- 网络规划：主要介绍如何根据网络实际情况进行网络规划。
- 接口：主要介绍如何设置 NGFW 上的物理接口、子接口以及端口聚合，包括接口属性和 IP 地址设置等。
- VLAN：主要介绍如何在 NGFW 上设置 VLAN。
- 链路聚合：主要介绍如何在 NGFW 上设置聚合接口。
- 路由：主要介绍 NGFW 路由的设置方式。
- 邻居：主要介绍如何在 NGFW 上设置 ARP 和 Neighbour 信息。
- MAC：主要介绍如何在 NGFW 上设置 MAC。
- DHCP：主要介绍如何将 NGFW 作为 DHCP 服务器、DHCP 客户端、DHCP 中继使用。
- IPSec VPN：主要介绍 IPSec 协议原理及相关术语，并介绍介绍如何中配置静态隧道。
- GRE：主要介绍如何利用 GRE 协议与远端设备建立 GRE 隧道进行数据传输。
- 智能 DNS：主要介绍智能 DNS 的工作原理，如何在 NGFW 上配置智能 DNS。

6.1 网络规划

在网络规划时，一般分为两种情况：

1）在当前运行的网络中添加 NGFW，安装 NGFW 的目的通常是增强现有网络的防御能力。

部署防火墙时，往往要求尽可能少地改动或禁止改动网络节点的网络属性，如网络拓扑结构、网络设备地址等，并要求防火墙的接入对网络通信造成的影响最少，尽可能地做到防火墙部署透明。此时部署的 NGFW 最好采用透明模式或者虚拟线方式。

- 在透明模式下，如果在同一 VLAN 中转发数据报文，NGFW 将不改变通信数据包的包头信息，这样可以避免各个防火区域中应用设备的物理地址的刷新。同时，NGFW 可以在设置了接口 IP 地址的不同 VLAN 之间路由转发数据报文。
- 在虚拟线模式下，将防火墙的 2 个物理接口加入一个虚拟线组后，从一个接口接收包时，除了目的地址是防火墙地址的数据报文外，会直接从另一个接口转发出去，不经过二层交换以及三层路由的检查过程。

2）在设计网络结构和部署网络设备的初始阶段，充分考虑了网络的安全问题，并已将 NGFW 的安全和通信等功能融入网络设计方案。

在这种情形下，通常可以启用防火墙的通信功能，如路由、地址转换等。最佳的工作模式为混合模式，即同时使用防火墙的透明功能和路由功能。

- 透明模式支持把同一网段的网络区域划分为不同的防火区，主要适用于基于业务的 IP 分配方案，可以将同一应用业务的服务器和客户机通过同一网段连接起来，以提高整体网络的通信性能。
- 路由模式支持将路由信息转发到其它防火区，减少防火墙应用带来的网络管理的工作量。NGFW 路由模式提供完整的静态路由功能，对于中小规模的内部网络完全可以代替内网路由器。该工作模式下，NGFW 可以友好地支持网络扩展，如可以对防火墙原有的配置不作改变或少量修改，实现在原有网络基础上增加网段或主机的功能。

网络规划实例

下面以一个 NGFW 部署案例说明网络的划分：

方案中设计了 4 个防火区，分别是：

- 公共网络防火区和安全服务防火区：LAN-1：202.100.100.0/24
- 千兆服务网络防火区：LAN-2：202.100.101.0/24
- 内部网络防火区：LAN-3：192.168.1.0/24；192.168.2.0/24

其中内部网络防火区包括两个子网：安全子网 A 和安全子网 B；LAN-1 跨两个防火区：公共网络防火区和安全服务防火区。

下图为规划好的网络拓扑图。

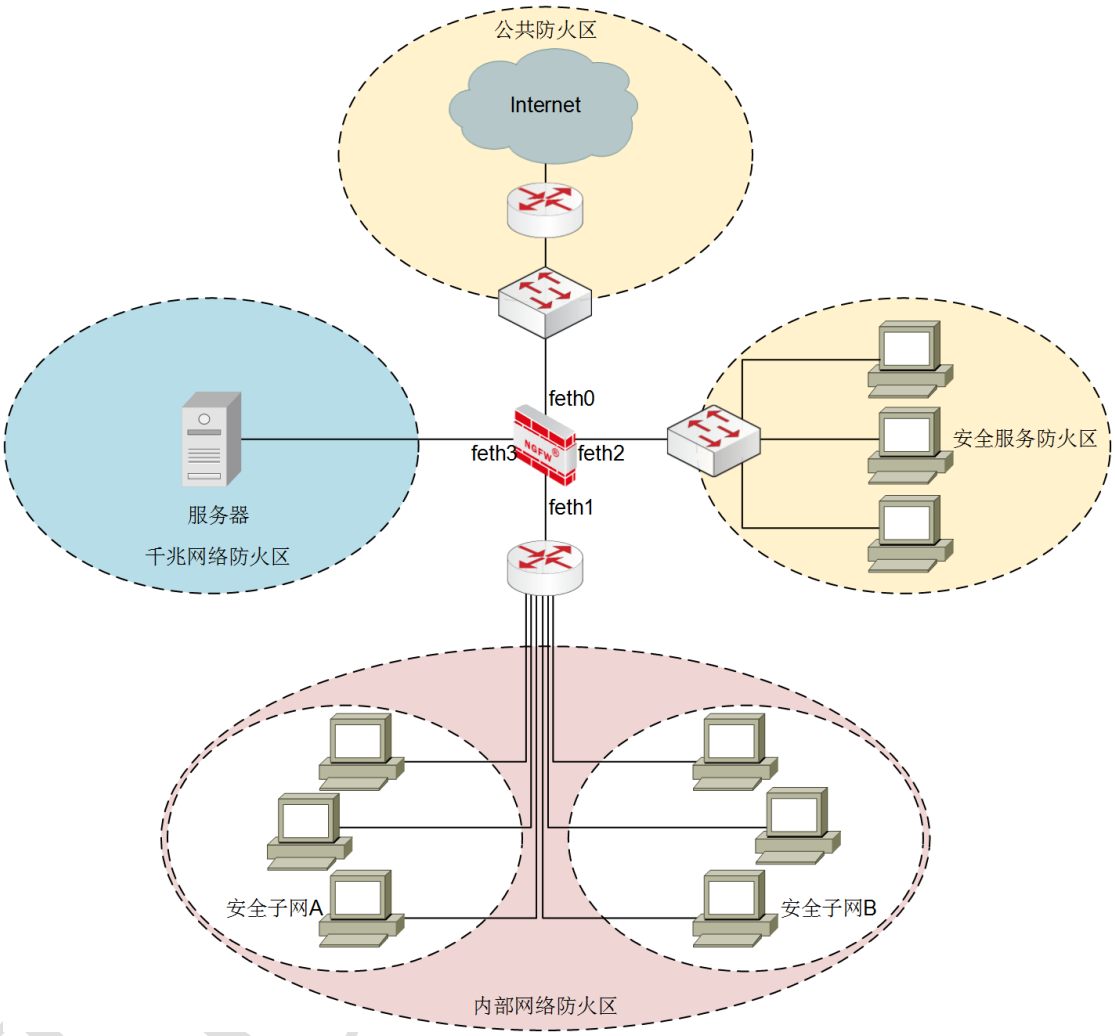


图 6-1 NGFW 部署案例示意图

6.2 接口

6.2.1 简介

接口是设备与网络中其他设备交换数据并相互作用的枢纽，按照性质分为物理接口和逻辑接口。

- 物理接口是指真实存在于设备上的接口，如设备上的以太网接口 feth0 等，广义的物理接口包括 Console 口等。

- 逻辑接口是指能够实现数据交换功能但物理上不存在，并且需要通过配置建立的接口。

NGFW 的物理接口仅指以太网接口，逻辑接口包括子接口和 VLAN 虚接口。

- 子接口是在路由模式的单个物理接口上配置的多个逻辑接口。子接口共用物理接口的物理参数配置，但有各自独立的链路层和网络层配置参数，如 MAC 地址和 IP 地址。在不增加物理接口的情况下，子接口是扩展路由接口的方案。
- VLAN 虚接口是 VLAN 内所有设备对外通信的出口。VLAN 虚接口是 VLAN 内所有以太网接口的集合，只要 VLAN 内有一个以太网接口处于 UP 状态，该 VLAN 虚接口就处于 UP 状态。
- 聚合接口是将多个物理接口聚合成一个逻辑端口，可以使设备之间的带宽成倍增加、增强端口灵活性并提供链路冗余。当聚合接口内的某条链路出现故障时，该链路的流量将自动转移到其余链路上。

接口模式

根据设备型号的不同，物理接口支持快速以太网接口（速率为 10/100Mbit/s）和千兆以太网接口（速率为 1000Mbit/s）。

NGFW 的物理接口支持四种工作模式：路由模式、交换模式、虚拟线模式和 SLAVE 模式。在实际应用中，用户可根据需求进行配置。

- 路由模式

在路由模式下，接口为三层接口，工作在网络层，可配置 IPv4 或 IPv6 地址，对不同网段间的数据进行三层路由和转发。

- 交换模式

在交换模式下，接口为二层接口，工作在数据链路层。处于同一个交换域的主机加入 VLAN 后，可以互相通过该 VLAN 进行通信，实现对数据二层转发。接口工作模式可分为 Access 模式和 Trunk 模式。

  - Access 模式：在 Access 模式下，同一接口可发送一个 VLAN 的报文，通常用于连接终端设备，如 PC、服务器等。
  - Trunk 模式：在 Trunk 模式下，同一接口可发送多个 VLAN，通常用于网络设备间互联，如交换机，路由器，防火墙等。

➢ 虚拟线模式

如图 6-2 所示，在 NGFW 设备中，一条虚拟线只有接口 A 和接口 B 两个工作接口，接口 A 接收到的数据包，除了目的地址为 NGFW 的数据报文外，直接从接口 B 转发出去。

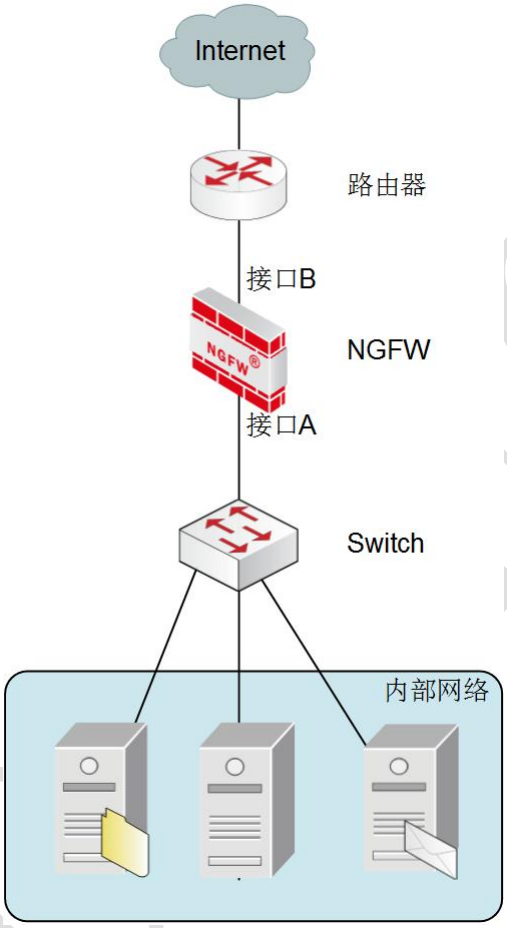


图 6-2 接口工作在虚拟线模式示意图

➢ SLAVE 模式

工作在路由模式的物理接口加入到聚合接口后，该物理接口将工作在 SLAVE 模式。关于聚合接口的配置具体请参见 6.4 链路聚合。

IP 地址

设备如果需要连接到网络中，并能正常通信，必须配置接口的 IP 地址。目前 IP 地址有 2 个版本：IPv4 和 IPv6。

➢ IPv4 地址

IPv4 地址长度为 32 位，共 4 个字节，形式为点分十进制，每个字节的取值范围是 0-255，如 101.2.1.1。IPv4 地址由网络位和主机位组成，为了在网络中区分网络位和主机位，IPv4 地址由 IP 地址+子网掩码表示，子网掩码表示地址中的网络位位数，如 100.2.2.3/24，表示当前网络地址二进制表示方式中的前 24 位为网络位，后 8 位为主机位。子网掩码也可表示为点分十进制，如 100.2.2.3/24，可表示为 IP 地址为 100.2.2.3，子网掩码为 255.255.255.0。

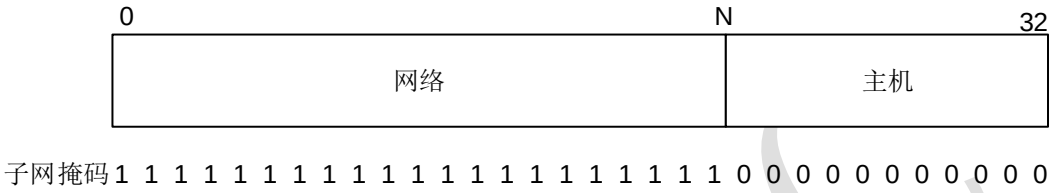


图 6-3 IP 地址的子网掩码

- IPv6 地址

IPv4 地址由 32 位组成，随着网络中的设备增多，出现了 IPv4 地址短缺的问题。为解决该问题 IETF 设计了新的 IP 地址形式 IPv6。

IPv6 地址长度为 128 位，共 16 个字节，形式为冒分十六进制，如 9000:0000:0000:0023:4567:78AB:CEDF。如果地址中有多个 0，则可省略数字前的零，如果该字节都为零，则可省略为一对冒号。因此以上的 IP 地址可简写为 9000::23:4567:78AB:CEDF。但是一个 IPv6 地址中仅可有一对冒号，以免引起歧义。

由于目前网络中大部分设备为 IPv4 地址，为实现网络由 IPv4 到 IPv6 的平滑过渡，IPv6 地址还支持兼容 IPv4 地址和映射 IPv4 地址，表示方式分别为：0:0:0:0:0:0:IPv4-add 或者 0:0:0:0:0:FFFF:IPv4-add，其中 IPv4-add 为点分十进制形式的 IPv4 地址。

IPv6 地址由网络前缀和接口标示组成，IPv6 地址由 IP 地址+前缀表示，前缀表示地址中的网络前缀位数，如 9000::0123:4567:78AB:CEDF/80，表示当前网络地址二进制表示方式中的前 80 位为网络前缀，后 48 位为接口标示。

6.2.2 配置接口工作模式

NGFW 的接口支持四种工作模式：路由模式、交换模式、虚拟线模式和 SLAVE 模式，默认情况下，所有接口均工作在路由模式下。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **物理接口**。

步骤 2 点击某接口对应的操作图标“”，可设置该接口的相关属性参数。

1）设置接口的基本属性：包括接口工作模式、是否启用该接口以及接口描述信息。

在设置基本属性时，各项参数的具体说明如下表所示。

参数	说明
名称	显示接口名称及其 MAC 地址。
状态	配置接口是否启用，可选项：启用、禁用。
描述	输入对该接口的简要描述。
模式	设定接口工作在路由模式、交换模式、虚拟线模式或 SLAVE 模式。接口默认工作在路由模式。当该接口加入到聚合组后时，“模式”参数显示为“SLAVE”且不可编辑，关于聚合组的配置具体请参见 6.4 链路聚合。

2）设置接口在不同工作模式下的属性。

（a）路由模式

当在“基本信息”处设置接口工作在“路由”模式时，需要设置接口的 IP 地址及其掩码。

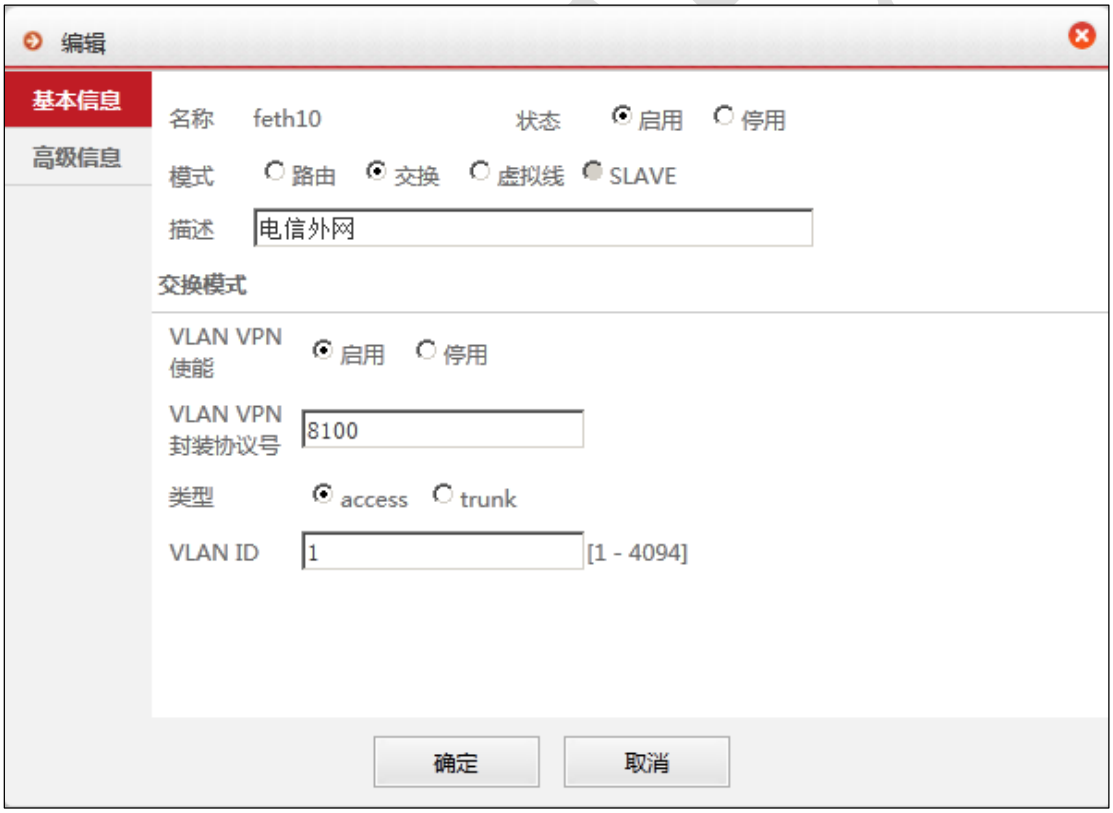
在设置接口地址时，各项参数的具体说明如下表所示。

参数	说明
IPv4 地址/掩码	输入接口的 IPv4 地址及其子网掩码。 说明： 1）可以为路由接口设置多个 IPv4 地址。 2）NGFW 不支持不同的物理接口配置相同的 IPv4 地址或 IPv4 地址在同一子网内。
非同步地址	如果在网络中配置了高可用性功能，则设置心跳口 IP 时必须要选择“非同步地址”，否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。热备组中的备设备的管理 IP 必须选择“非同步地址”，否则无法对备设备进行管理。关于高可用性的配置具体请参见 4.7 高可用性。
添加	如果“地址/掩码”设置正确，点击【添加】按钮，则新添加接口的 IPv4 地址会显示在列表中。
删除	点击 IPv4 地址操作栏对应的删除按钮，然后在确认提示框中点击【确定】按钮，可以删除已添加的 IPv4 地址。

参数	说明
IPv6 地址	输入接口的 IPv6 地址/前缀长度，若添加链路本地地址则不需要提供前缀长度。 说明： 1）可以为路由接口设置多个 IPv6 地址，最多不超过 53 个。 2）NGFW 不支持不同的物理接口配置相同的 IPv6 地址或 IPv6 地址在同一子网内。
添加	如果“IPv6 地址”设置正确，点击【添加】按钮，则新添加接口的 IPv6 地址会显示在列表中。
删除	点击 IPv6 地址对应的“删除”，然后在确认提示框中点击【确定】按钮，可以删除已添加的 IPv6 地址。

（b）交换模式

当在“基本信息”处设置接口工作在“交换”模式时，需要设置接口类型为“access”或“trunk”的接口，及其所属 VLAN 的 ID 号。



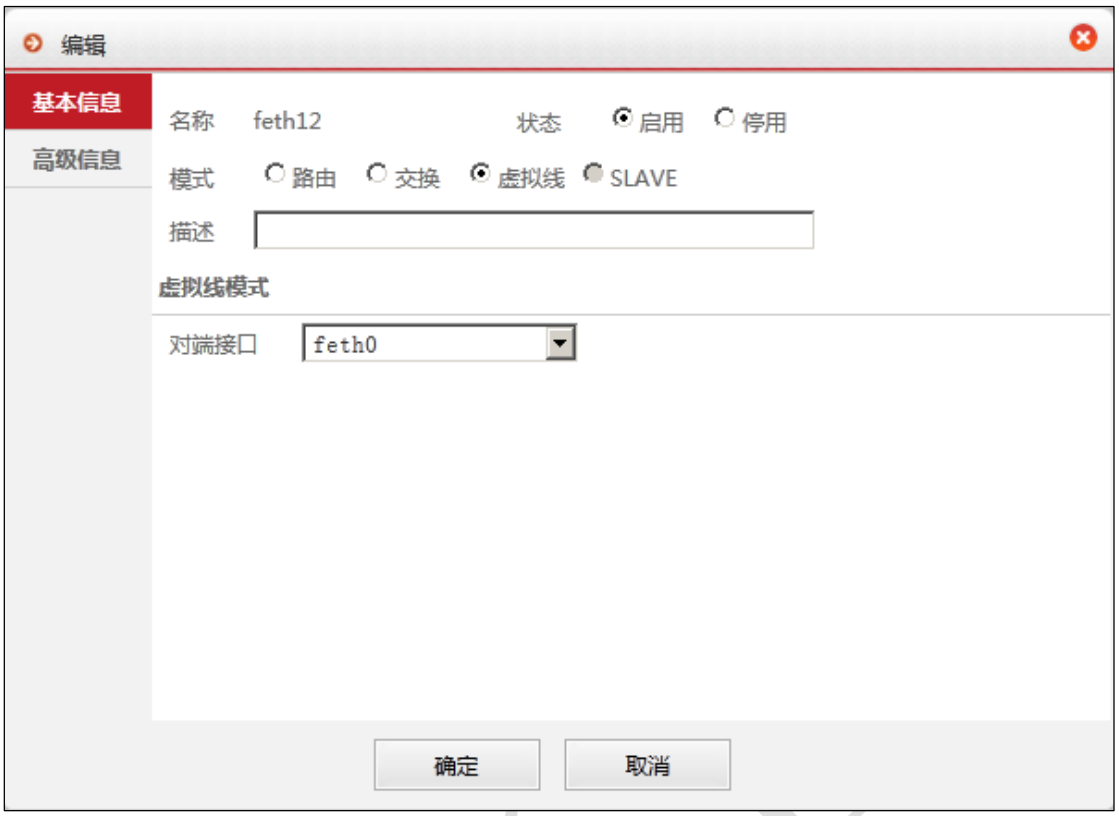
在设置接口交换模式基本属性时，各项参数的具体说明如下表所示。

参数	说明
VLAN VPN 使能	默认接口为“停用”，表示关闭 QinQ 功能；如果选择“启用”，则表示已开启 QinQ 功能。关于 QinQ 的说明具体请参见 6.3VLAN。

参数	说明
VLAN VPN 封装协议号	设置 QinQ 功能使用的协议类型，数值类型，十六进制形式，默认为 0x8100。 为了实现不同厂商的设备互通，接口 QinQ 外层 VLAN Tag 的协议类型应该配置为和该接口连接的设备能够识别的协议类型。关于 QinQ 的说明具体请参见 6.3VLAN。 VLAN VPN 封装协议号一般只在网络侧接口配置，用于指定运营商采用的协议类型。
类型	设置该交换接口的类型。可选项：access 和 trunk。
VLAN ID	设置接口的所属的 VLAN ID，取值范围：1-4094。 当“类型”为“access”时，此参数用于指定 Access 口所属的 VLAN ID 号码。 当“类型”为“trunk”时，此参数用于指定 Trunk 接口的 Native VLAN。
VLAN 范围	仅当“类型”为“trunk”时，需要设置该项。 用于设置该 Trunk 接口允许哪些 VLAN 的报文通过。VLAN 值的取值范围：1-4094。 格式举例： 1-10 表示属于 VLAN1 到 VLAN 10； 1，10 表示属于 VLAN1 和 VLAN10。

（c）虚拟线模式

当在“基本信息”处设置接口工作在“虚拟线”模式时，需要设置虚拟线的对端接口。设置完成后对端接口的工作模式自动设置为虚拟线模式。



（d）SLAVE 模式

当工作在路由模式的物理接口加入到聚合接口后，其工作模式为 SLAVE，关于聚合接口的配置具体请参见 6.4 链路聚合。

步骤 3 设置完成后，点击【确定】按钮完成接口属性设置。

CLI 方式配置

设置接口为路由模式，并配置相关属性。

说明

✧ 默认情况下，NGFW 的所有物理接口均工作在路由模式。如果接口被设置成工作在监听模式、交换模式或虚拟线模式时，通过执行如下命令，可以使接口工作在路由模式。

步骤	配置命令	配置说明
1	**network interface** <*string*> **no listening** <cr>	取消设置接口的工作模式为监听模式。
2	**network interface** <*string*> **no switchport** <cr>	取消设置某物理接口的工作模式为交换模式。

步骤	配置命令	配置说明
3	**network virtual-line delete id** <*number*>	删除与物理接口相关的虚拟线。
4	**network interface** <*string1*> **ip add** <*ipaddress*> [**mask** <*string2*>]	配置接口的 IPv4 地址。
	network interface <*string1*> **ipv6 add** <*string2*> **prefix** <*number*>	配置接口的 IPv6 地址。

设置接口为交换模式，并配置相关属性。

步骤	配置命令	配置说明
1	**network interface** <*string*> **switchport** <cr>	设置接口为交换模式。
2	**network interface** <*string*> **switchport mode** <access|trunk>	设置交换接口的工作模式。
3	**network interface** <*string1*> **switchport trunk allowed-vlan** <*string2*>	设置 Trunk 接口的属性。即该 Trunk 端口属于哪些 VLAN。
4	**network interface** <*string*> **switchport trunk native-vlan** <*number*>	设置该 Trunk 接口的本地 VLAN。
5	**network interface** <*string*> **switchport access-vlan** <*number*>	设置 Access 接口所属的 VLAN。

network interface <*string1*> **ip add** <*ipaddress*> [**mask** <*string2*>] [ha-static]

命令描述：

给接口添加 IPv4 地址，一个接口可添加多个 IPv4 地址。

参数说明：

network interface	必选项，指定待添加的接口。
string1	字符串类型，表示接口名称，可为物理接口或虚接口。
ip add	必选项，添加 IPv4 地址。
ipaddress	IPv4 地址字符串，IPv4 地址格式为 A.B.C.D。
mask	可选项，设置子网掩码。
string2	子网掩码字符串。
ha-static	可选项，设置接口 IP 地址是否为高可用性的同步地址。

使用说明：

如果在添加接口 IPv4 地址时，只设置了 IPv4 地址并没有设置掩码，系统根据 IPv4 地址自动为该 IPv4 添加主类子网掩码。

以下为添加接口 IPv4 地址的示例：

给 feth0 添加 IPv4 地址为：192.168.90.75。

```
TopsecOS# network interface feth0 ip add 192.168.90.75
```

network interface <*string*> **ip clean** <cr>

命令描述：

清空某接口所有的 IPv4 地址。

参数说明：

network interface	必选项，指定待清空 IPv4 地址的接口。
string	字符串类型，表示接口名称，可为物理接口和虚接口。
ip clean	必选项，清空指定接口所有的 IPv4 地址。

以下为清空指定接口 IPv4 地址的示例：

清空 feth2 接口上所有的 IPv4 地址。

```
TopsecOS# network interface feth2 ip clean
```

NGFW 的物理接口支持 IPv4 地址和 IPv6 地址，虚接口不支持 IPv6 地址。

network interface <*string*> **ip delete** <*ipaddress*>

命令描述：

删除某接口指定的 IPv4 地址。

参数说明：

network interface	必选项，指定待删除 IPv4 地址的接口。
string	字符串类型，表示接口名称，可为物理接口或虚接口。
ip delete	必选项，删除指定接口指定的 IPv4 地址。
ipaddress	IPv4 地址字符串，IPv4 地址格式为 A.B.C.D。

以下为删除接口 IPv4 地址的示例：

删除 feth0 接口上为 192.168.90.75 的 IPv4 地址。

```
TopsecOS# network interface feth0 ip delete 192.168.90.75
```

network interface <*string1*> **ipv6 add** <*string2*> **prefix** <*number*> [ha-static]

命令描述：

添加接口的 IPv6 地址。

可使用 **network interface** <*string1*> **ipv6 delete** <*string2*>命令删除接口的 IPv6 地址。

参数说明：

network interface	必选项，指定待添加地址的接口。
string1	字符串类型，表示物理接口名称，可为物理接口和虚接口。
ipv6 add	必选项，添加 IPv6 地址。
string2	IPv6 地址字符串，IPv6 地址格式为 X:X:X:X:X:X:X:X，其中 X 为一个四位十六进制整数。
prefix	必选项，设置 IPv6 地址网络前缀。
number	数值类型。取值范围：0-128。
ha-static	可选项，设置接口 IP 地址是否为高可用性的同步地址。

以下为添加接口 IPv6 地址的示例：

添加 feth0 接口的 IPv6 地址为 12AB::CD30/64。

```
TopsecOS# network interface feth0 ipv6 add 12ab::cd30 prefix 64
TopsecOS# network interface feth0 show configuration
network interface feth0 vsid 0
network interface feth0 mtu 1500
network interface feth0 ip add 192.168.90.78 mask 255.255.255.0      label 0
network interface feth0 ipv6 add 12ab::cd30 prefix 64
network interface feth0 speed auto
network interface feth0 duplex auto
network interface feth0 no switchport
network interface feth0 switchport mode access
network interface feth0 switchport trunk native-vlan 1
network interface feth0 switchport access-vlan 1
network interface feth0 switchport trunk allowed-vlan 1-1000
network interface feth0 mss-adjust 1460
network interface feth0 no shutdown
```

network interface <*string*> **ipv6 clean**

命令描述：

清除某接口所有的 IPv6 地址。

参数说明：

network interface	必选项，指定待清除地址的接口。
string	字符串类型，表示接口名称，可为物理接口或虚接口。
ipv6 clean	必选项，清除指定接口上所有的 IPv6 地址。

以下为清空指定接口 IPv6 地址的示例：

清空 feth2 接口上所有的 IPv6 地址。

```
TopsecOS# network interface feth2 ipv6 clean
```

network interface <*string*> **shutdown**

命令描述：

关闭指定接口。

参数说明：

network interface	必选项，指定待关闭的接口。
string	字符串类型，表示接口名称，可为物理接口或虚接口。
shutdown	必选项，禁用接口。

以下为关闭指定接口的示例：

```
TopsecOS# network interface feth2 ipv6 clean
```

network interface <*string*> **switchport**

命令描述：

设置某物理接口的工作模式为交换模式，NGFW 物理接口默认工作在路由模式下，更改工作模式使其工作在交换模式时，接口上的所有 IP 地址将被删除。

可使用 **network interface** <*string*> **no switchport** <cr>命令取消设置某物理接口的工作模式为交换模式。

参数说明：

network interface	必选项，指定设置某个接口工作在交换模式下。
string	字符串类型，表示物理接口的名称，可为物理接口或虚接

	口。
switchport	必选项，设置当前接口工作在交换模式下。

以下为设置某物理接口工作在交换模式下的示例：

设置接口 feth2 的工作模式为交换模式。

```
TopsecOS# network interface feth2 switchport
```

network interface <*string*> **switchport mode** <access|trunk>

命令描述：

设置交换接口的工作模式。

参数说明：

network interface	必选项，指定设置某个交换接口的工作模式。
string	字符串类型，表示物理接口名称。
switchport mode	必选项，设置当前交换接口的工作模式。
access|trunk	access 模式：该交换接口只属于一个 VLAN。 trunk 模式：该交换接口可以同时属于多个 VLAN。

以下为设置交换接口工作模式的示例：

设置 feth0 接口为 trunk 接口。

```
TopsecOS# network interface feth0 switchport
TopsecOS# network interface feth0 switchport mode trunk
```

network interface <*string1*> **switchport trunk allowed-vlan** <*string2*>

命令描述：

设置 trunk 接口的属性。即该 trunk 端口属于哪些 VLAN。

参数说明：

network interface	必选项，指定设置 Trunk 属性的接口。
string1	字符串类型，表示交换接口的名称。
switchport trunk	必选项，设置该交换接口属于 trunk 接口时的属性。
allowed-vlan	必选项，设置端口所属 VLAN 范围。
string	字符串类型，表示 VLAN 范围，格式为 N1，N2，……，N3-N4（N 表示数值，且 N3 <=N4）。例如：1-10 表示 VLAN1，VLAN2，……，VLAN10；1，10 表示 VLAN1 和 VLAN10；1，10，11-12，表示 VLAN1，VLAN10，VLAN11 和 VLAN12。

network interface <*string*> **switchport trunk native-vlan** <*number*>

命令描述：

设置该 Trunk 接口的本地 VLAN。

参数说明：

network interface	必选项，指定设置本地 VLAN 的 Trunk 接口。
string	字符串类型，表示接口名称。
switchport trunk	必选项，设置该 trunk 接口时的属性。
native-vlan	必选项，trunk 端口的缺省 VLAN ID。由于 Trunk 端口属于多个 VLAN，所以需要设置缺省 VLAN ID，用于当该交换接口接收到没有标记的报文时，该 Trunk 端口将此报文发往缺省 VLAN ID 标识的 VLAN。
number	数值类型，指定 VLAN ID 值。

以下为设置 trunk 口属性的示例：

设定 feth0 接口为 trunk 接口，且只允许 vlan1 和 vlan5 通过。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk allowed-vlan** *1,5*

设定 feth0 接口为 trunk 接口，且只允许 vlan1、vlan2、vlan3、……、vlan10 通过。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk allowed-vlan** *1-10*

设定 feth0 接口为 trunk 接口，并将本地 vlan 设置为 vlan5。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport mode** trunk

TopsecOS# **network interface** *feth0* **switchport trunk native-vlan** *5*

network interface <*string*> **switchport access-vlan** <*number*>

命令描述：

设置 access 接口所属的 VLAN。

参数说明：

network interface	必选项，指定设置所属 VLAN 的 access 接口。
string	字符串类型，表示交换接口的名称。
switchport access-vlan	必选项，设置该交换接口为 access 接口时所属的 VLAN ID 号码。
number	数值类型，表示 VLAN 的 ID。

以下为指定接口所属的 VLAN 的示例：

设置 feth0 接口为 access 接口，且将其添加到 vlan2。

```
TopsecOS# network interface feth0 switchport
TopsecOS# network interface feth0 mode access
TopsecOS# network interface feth0 switchport access-vlan 2
```

network interface <*string*> **show** [configuration]

命令描述：

查看设备接口配置信息。

参数说明：

network interface	必选项，设备接口。
string	字符串类型，表示接口的名称。如果不指定该参数，将查看所有接口的配置信息。
show	查看接口配置。
configuration	接口的功能配置信息。

以下为查看接口配置的示例：

```
TopsecOS# network interface show
feth0       Link encap:Ethernet    HWaddr 00:13:32:05:01:40
              Link status: established, Autoneg enable
              Full-duplex, 100Mb/s
              inet addr:192.168.16.2    Bcast:192.168.16.255    Mask:255.255.255.0
```

```
        inet6 addr:fe80::213:32ff:fe05:140/64    Scope:Link
        UP BROADCAST RUNNING MULTICAST    MTU:1500
        Rx packets:730764 Tx packets:100935 Dropped:0
        RX bytes:204385211 (194.9 Mb)    TX bytes:53400476 (50.9 Mb)
        Vsysid:0    Vrid:0    Ifindex:102
        Commtype:routing    Management Port

feth1       Link encap:Ethernet    HWaddr 00:13:32:05:01:41
        Link status:not established, Autoneg enable
        Unknown-duplex, unknown speed
        UP BROADCAST MULTICAST    MTU:1500
        Rx packets:0 Tx packets:0 Dropped:0
        RX bytes:0 (0.0 b)    TX bytes:0 (0.0 b)
        Vsysid:0    Vrid:0    Ifindex:103
        Commtype:switching    Management Port
feth10      Link encap:Ethernet    HWaddr 00:10:f3:2f:f0:ba
        Link status:not established, Autoneg enable
        Unknown-duplex, unknown speed
        UP BROADCAST MULTICAST    MTU:1500
        Rx packets:0 Tx packets:0 Dropped:0
        RX bytes:0 (0.0 b)    TX bytes:0 (0.0 b)
        Vsysid:0    Vrid:0    Ifindex:112
        Commtype:switching
……
```

以下为查看接口功能配置的示例：

```
TopsecOS# network interface feth1 show configuration
network interface feth1 vsid 0
network interface feth1 mtu 1500
```

```
network interface feth1 speed auto
network interface feth1 duplex auto
network interface feth1 switchport mode access
network interface feth1 switchport trunk native-vlan 2
network interface feth1 switchport access-vlan 2
network interface feth1 switchport trunk allowed-vlan 2
network interface feth1 switchport
network interface feth1 vlan-vpn disable
network interface feth1 mss-adjust off
network interface feth1 gratuitous-arp-interval 0
network interface feth1 ha-virtual-mac-address enable
network interface feth1 tgid 0
network interface feth1 no shutdown
```

6.2.3 配置接口基本属性

设置物理接口的基本属性，包括接口的工作速率、协商模式、MSS 值、MTU 值、VSID、MAC 地址和描述信息。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **物理接口**，或者选择 **网络管理** > **接口** > **VLAN**。

步骤 2 点击某接口对应的操作图标“”，在弹出的对话框中，点击“高级信息”。

步骤 3 在界面中配置接口的 MTU 和 MSS。

在设置接口的基本属性时，各项参数的具体说明如下表所示。

参数	说明
MTU	物理接口设置为路由模式或交换模式、VLAN 虚接口时，需要设置该项。必选项，设置指定接口的 MTU。单位：字节；取值范围：68-1500；默认值：1500。
MSS	物理接口设置为路由模式或交换模式、VLAN 虚接口时，需要设置该项。

参数	说明
	设置指定接口的 MSS 值。可选项：自适应、关闭和自定义。设置为自定义时的取值范围：200-1460。
双工模式	物理接口设置为 SLAVE 模式或虚拟线模式时，可以设置该项。 设置物理接口的双工模式。可选项：自适应、半双工、全双工。默认值：自适应。
速率	物理接口设置为 SLAVE 模式或虚拟线模式时，可以设置该项。 设置物理接口的速率。可选项：自适应、10Mb/s、100Mb/s、1000Mb/s、10000Mb/s。默认值：自适应。

CLI 方式配置

步骤	配置命令	配置说明
1	**network interface** <*string*> **speed** <10|100|1000|10000|auto>	配置物理接口的工作速率。
2	**network interface** <*string*> **duplex** <half|full|auto>	设置物理接口的协商模式。
3	**network interface** <*string*> **mtu** <*number*>	设置物理接口的 MTU。
4	**network interface** <*string*> **mss-adjust** <auto|off|*number*>	设置物理接口的 MSS 值。
5	**network interface** <*string*> **vsid** <*number*>	设置物理接口的 VSID。
6	**network interface** <*string*> **mac-address** <*macaddress*>	设置物理接口的 MAC 地址。
7	**network interface** <*string1*> **description** <*string2*>	设置物理接口的描述信息。

network interface <*string1*> **description** <*string2*>

命令描述：

设置接口的描述信息。

使用 **network interface** <*string1*> **no description** <*string2*>命令可以删除该描述信息。

参数说明：

network interface	必选项，指定配置描述信息的网络接口。
string1	字符串类型，表示接口名称。
description	必选项，设置该接口的描述信息。
string2	字符串类型。

以下为添加描述信息的示例：

给 feth0 添加“guanlikou”的描述信息。

```
TopsecOS# network interface feth0 description guanlikou
```

network interface <*string*> **duplex** <half|full|auto>

命令描述：

设置物理接口的工作模式。

参数说明：

network interface	必选项，指定设置工作模式的物理接口。
string	字符串类型，表示接口名称。
duplex	必选项，设置指定接口的工作模式，默认为自动协商模式。
half|full|auto	半工|全工|自动

以下为设置接口工作模式的示例：

设置接口 feth0 的工作模式为全工。

```
TopsecOS# network interface feth0 duplex full
```

network interface <*string*> **mac-address** <*macaddress*>

命令描述：

设置物理接口的 MAC 地址。

参数说明：

network interface	必选项，指定设置 MAC 地址的物理接口。
string	字符串类型，表示接口名称，可为物理接口和虚接口。
mac-address	必选项，设置指定接口的 MAC 地址。
macaddress	MAC 地址字符串，格式为 aa:bb:cc:dd:ee:ff。

以下为设置接口 MAC 地址的示例：

设置接口 feth3 的 MAC 地址为 f2:ab:12:6c:56:bb。

```
TopsecOS# network interface feth3 mac-address f2:ab:12:6c:56:bb
TopsecOS# network interface feth3 show
feth3       Link encap:Ethernet    HWaddr f2:ab:12:6c:56:bb
              Link status: established, Autoneg enable
```

```
Unknown-duplex, unknown speed
UP BROADCAST RUNNING MULTICAST  MTU:1500
Rx packets:0 Tx packets:0 Dropped:0
RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
Vsysid:0  Vrid:0  Ifindex:29
Commtype:routing
```

network interface <*string*> **restore** <mac>

命令描述：

恢复接口的 MAC 地址为默认配置。

参数说明：

network interface	必选项，指定恢复 MAC 地址为默认配置的接口。
string	字符串类型，表示接口名称，可为物理接口或虚接口。
restore	必选项，恢复指定接口的 MAC 地址为默认配置。
mac	MAC 地址。

以下为恢复接口 MAC 地址为默认配置的示例：

恢复接口 feth3 的 MAC 地址为默认配置。

```
TopsecOS# network interface feth3 restore mac
```

network interface <*string*> **mss-adjust** <auto|off|*number*>

命令描述：

对某物理接口的 MSS 值进行自动调整，即根据接口的 mtu 值对该接口的 MSS 值进行调整，调整的数值是接口的 MTU–60，留部分空间给可能的 IP 选项。

参数说明：

network interface	必选项，指定设置 MSS 调整功能的接口。
string	字符串类型，表示接口名称。
auto|off|*number*	自动调整|关闭自动调整|设置 MSS 数值，其中 *number* 取值范围：200-1460。

以下为开启接口 MSS 调整功能的示例：

开启接口 feth0 的 MSS 调整功能。

TopsecOS# **network interface** *feth0* **mss-adjust** off

network interface <*string*> **mtu** <*number*>

命令描述：

设置物理接口的 MTU。

参数说明：

network interface	必选项，指定设置 MTU 的物理接口。
string	字符串类型，表示接口名称。
mtu	必选项，设置指定接口的 mtu。
number	数值类型，单位：字节；取值范围：68-1500；默认值：1500。

以下为设置接口 MTU 的示例：

设置接口 feth0 的 MTU 为 1460。

TopsecOS# **network interface** *feth0* **mtu** *1460*

network interface <*string*> **speed** <10|100|1000|10000|auto>

命令描述：

设置物理接口的工作速率。

参数说明：

network interface	必选项，指定设置工作速率的物理接口。
string	字符串类型，表示接口名称。
speed	必选项，设置指定接口的工作速率大小，接口默认为自动获取工作速度。
10|100|1000|10000|auto	10Mbps|100Mbps|1000Mbps|10000Mbps|自动

以下为设置接口速率的示例：

设置接口 feth0 的工作速率为 1000Mbps。

TopsecOS# **network interface** *feth0* **speed** 1000

6.2.4 配置 MAC 子接口

子接口是在工作于路由模式下的物理接口上配置的逻辑接口，子接口与其关联的物理接口在数据链路层和网络层相对独立，通过在物理接口上配置子接口可实现多个网络互连互通。

在配置 MAC 子接口之前，需要先进行如下步骤：

- 配置子接口对应物理接口的工作模式为路由模式，关于接口属性的配置具体请参见 6.2.3 配置接口基本属性。

WEBUI 方式配置

子接口提供了在一个物理接口上支持多个网络互连的功能，为用户提供了很高的灵活性。工作在路由模式下的 NGFW 的每个物理接口均可支持多达 32 个子接口。

步骤 1 选择 **网络管理** > **接口** > **MAC 子接口**。

步骤 2 添加子接口。

1）点击界面左上角的『添加』，弹出“新增子接口”窗口。

在添加子接口时，各项参数的具体说明如下表所示。

参数	说明
接口	选择要在其下添加子接口的物理接口，该接口必须为路由接口。
添加单个子接口	添加单个子接口的 ID 号，取值范围：0-31。添加后，子接口的名称为“以太网接口名+mv+子接口 ID”，如 feth0mv02，表示以太网接口 feth0 的 ID 号为 2 的子接口。
添加子接口范围	一次性在某个物理接口下添加多个名称连续的子接口。取值范围：0-31。如在 feth0 接口下输入范围“2-10”，则一次性添加 feth0mv02、feth0mv03、feth0mv04……feth0mv10。

2）点击【确定】按钮完成子接口的添加。添加完成后，子接口默认处于“停用”状态。

步骤 3 设置子接口属性。

1）在已添加的子接口对应的编辑图标“”，弹出“编辑子接口”窗口。

在设置子接口属性时，各项参数的具体说明如下表所示。

参数	说明
描述	输入对子接口的简要描述。

参数	说明
状态	设置该子接口是否可用；默认接口为“启用”状态，表示可以使用该子接口；如勾选“停用”，则表示该子接口将不会工作，该子接口状态将会显示为“停用”。 说明： 当物理接口为“停用”状态时，不允许启用属于它的子接口。
IPv4 地址/掩码	输入子接口的 IPv4 地址及其子网掩码。 说明： 1）可以为子接口设置多个 IPv4 地址。 2）不同的物理接口和子接口不能配置相同的 IPv4 地址，也不能配置同一子网内的不同的 IPv4 地址。
非同步地址	如果在网络中配置了高可用性功能，则设置心跳口 IP 时必须要选择“非同步地址”，否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。热备组中的备设备的管理 IP 必须选择“非同步地址”，否则无法对备设备进行管理。关于双机热备的配置具体请参见 4.7 高可用性。
添加	如果“地址/掩码”设置正确，点击【添加】按钮，则新添加接口的 IPv4 地址会显示在列表中。
删除	点击 IPv4 地址对应的删除图标，可以删除添加的 IPv4 地址。
IPv6 地址	输入子接口的 IPv6 地址。 说明： 1）可以为子接口设置多个 IPv6 地址。 2）不支持不同的子接口配置相同的 IPv6 地址或 IPv6 地址在同一子网内。
添加	如果“IPv6 地址”设置正确，点击【添加】按钮，则新添加接口的 IPv6 地址会显示在列表中。
删除	点击 IPv6 地址对应的删除图标，可以删除添加的 IPv6 地址。

2）点击【确定】按钮，完成子接口属性的设定。

CLI 方式配置

步骤	配置命令	配置说明
1	**network interface** <*string*> **macvif add id** <*number*>	在物理接口上添加一个子接口。
2	**network interface** <*string1*> **macvif add range** <*string2*>	在物理接口上一次性添加多个 ID 连续的子接口。
3	**network interface** <*string*> **macvif show**	查看子接口配置信息。
4	**network interface** <*string*> **macvif clean**	清除子接口配置信息。

network interface <*string*> **macvif add id** <*number*>

命令描述：

在物理接口上添加一个子接口。每个物理接口都可支持多达 32 个子接口，其中子接口的名称由以太网接口名+mv+子接口 ID 组成，如果在路由接口 feth1 上添加 ID 为 2 的子接口，则该子接口的名称为 feth1mv02。

使用 **network interface** <*string*> **macvif delete id** <*number*>命令删除添加的子接口。

参数说明：

network interface	必选项，指定在某个物理接口上添加子接口。
string	字符串类型，表示接口名称，该接口需工作在路由模式下。
macvif add	必选项，添加单个子接口。
id	必选项，设置子接口 ID。
number	数值类型。取值范围：0-31。

以下为在物理接口下添加单个子接口的示例：

在物理接口 feth2 上添加名称为 feth2mv01 的子接口。

```
TopsecOS# network interface feth2 macvif add id 1
```

network interface <*string1*> **macvif add range** <*string2*>

命令描述：

在物理接口上一次性添加多个 ID 连续的子接口。

使用 **network interface** <*string1*> **macvif delete range** <*string2*>命令删除添加的多个子接口。

参数说明：

network interface	必选项，指定在某个物理接口上添加子接口。
string1	字符串类型，表示接口名称，该接口需工作在路由模式下。
macvif add	必选项，添加子接口。
range	必选项，设置所添加子接口的 ID 范围。
string2	字符串类型，格式：N1-N2（N 为数值类型，且 N1 <=N2），N 的取值范围：0-31，如 5-20。

以下为在物理接口下一次添子接口的示例：

在物理接口 feth2 上添加名称为 feth2mv10、feth2mv11……feth2mv20 的子接口。

TopsecOS# **network interface** *feth2* **macvif add range** *10-20*

network interface <*string*> **macvif clean** <cr>

命令描述：

清空某物理接口上的所有子接口。

参数说明：

network interface	必选项，指定清空某物理接口上的子接口。
string	字符串类型，表示物理接口名称。
macvif clean	必选项，清空指定物理接口上的所有子接口。

以下为清空物理接口上的子接口的示例：

清空 feth2 接口上所有的子接口。

TopsecOS# **network interface** *feth2* **macvif clean**

network interface <*string*> **macvif show** <cr>

命令描述：

查看某物理接口上的所有子接口。

参数说明：

network interface	必选项，指定在某个物理接口上查看子接口。
string	字符串类型，表示接口名称。
macvif show	必选项，查看子接口。

以下为查看相应物理接口下子接口的示例：

在物理接口 feth2 上查看已添加的子接口。

TopsecOS# **network interface** *feth2* **macvif add id** *1*			
TopsecOS# **network interface** *feth2* **macvif add range** *10-20*			
TopsecOS# **network interface** *feth2* **macvif show**			
feth2mv01	feth2mv10	feth2mv11	feth2mv12
feth2mv13	feth2mv14	feth2mv15	feth2mv16
feth2mv17	feth2mv18	feth2mv19	feth2mv20

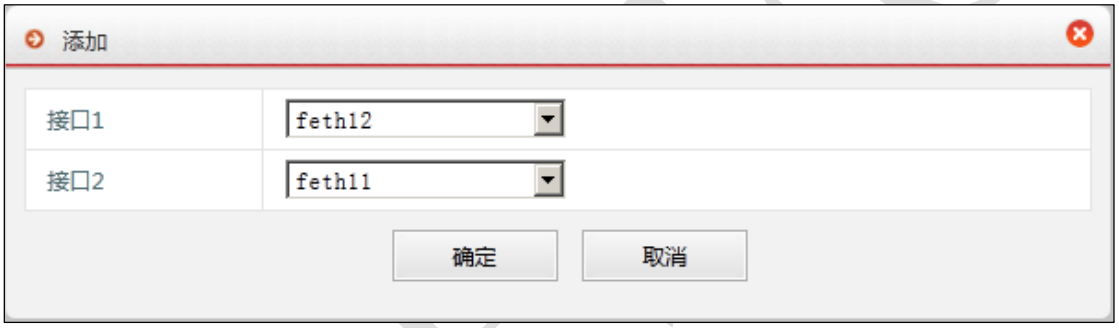
6.2.5 虚拟线

接口工作虚拟线模式/管理员只需在 NGFW 设定一个物理接口组 AB 作为一条虚拟线，如数据包从虚拟线接口组 AB 中的 A 口进入 NGFW 后，除了目的地址为 NGFW 的数据包外，均强制从虚拟线接口组 AB 中的 B 口进行转发，即不经过二层交换以及三层路由的检查过程就将报文直接发送出去。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **虚拟线**。

步骤 2 点击『添加』，在弹出的“新增”对话框中，通过下拉列表选择虚拟线路两端的物理接口。



步骤 3 设置好虚拟线路两端的物理接口后，点击【确定】按钮完成虚拟线路的添加。

步骤 4 设置虚拟线路两端的物理接口属性。

点击某接口对应的操作图标“”，可以设置虚拟线接口的 MTU、MSS、接口速率和双工模式属性。物理接口关于属性参数的解释具体请参见 6.2.3 配置接口基本属性。加入虚拟线的端口其属性显示为“虚拟线”，如下图所示。

物理接口

	名称	描述	接口模式	地址/掩码	MTU	状态	链路状态	双工模式	速率	操作
1	feth0		路由	IPv4:192.168.16.2/255.255.255.0	1500	启用		Full-duplex	100Mb/s	
2	feth1		交换		1500	启用		-	-	
3	feth2		交换		1500	启用		-	-	
4	feth3		交换		1500	启用		-	-	
5	feth10		交换		1500	启用		-	-	
6	feth11		虚拟线		1500	启用		-	-	
7	feth12		虚拟线		1500	启用		-	-	
8	feth13		路由		1500	启用		-	-	
9	feth14		交换		1500	启用		-	-	
10	feth15		交换		1500	启用		-	-	
11	feth16		交换		1500	启用		-	-	
12	feth17		交换		1500	启用		-	-	

CLI 方式配置

步骤	配置命令	配置说明
1	**network virtual-line add dev1** <*string1*> **dev2** <*string2*>	添加一条虚拟线。
2	**network virtual-line show** <cr>	查看所有虚拟线路。
3	**network virtual-line delete id** <*number*>	删除某条虚拟线。
4	**network virtual-line clean** <cr>	清空所有的虚拟线配置。

network virtual-line add dev1 <*string1*> **dev2** <*string2*>

命令描述：

添加一条虚拟线。

参数说明：

network virtual-line add	添加虚拟线。
dev1	必选项，设置虚拟线路左端的物理接口名。
string1	字符串类型，表示物理接口名称。
dev2	必选项，设置虚拟线路右端的物理接口名。
string2	字符串类型，表示物理接口名称。

以下为添加虚拟线的示例：

将 feth0 和 feth1 加入到一条虚拟线中。

```
TopsecOS# network virtual-line add dev1 feth0 dev2 feth1
TopsecOS# network virtual-line show
ID 8006 dev1:feth0          dev2:feth1
```

network virtual-line clean <cr>

命令描述：

清空所有虚拟线路。

以下为清空所有虚拟线的示例：

```
TopsecOS# network virtual-line clean
```

network virtual-line delete id <*number*>

命令描述：

删除某条虚拟线路。

参数说明：

network virtual-line delete	删除某条虚拟线路。
id	必选项，设置虚拟线路的 ID 号。
number	数值类型。

以下为删除虚拟线的示例：

将 feth0 和 feth1 组成的虚拟线删除。

```
TopsecOS# network virtual-line show
ID 8006 dev1:feth0          dev2:feth1
TopsecOS# network virtual-line delete id 8006
```

network virtual-line show <cr>

命令描述：

查看所有虚拟线路。

以下为查看所有虚拟线的示例：

```
TopsecOS# network virtual-line show
ID 8006 dev1:feth0          dev2:feth1
```

6.2.6 接口联动

接口联动主要用于防火墙工作在双机热备、负载均衡或者连接保护模式时，在短时间内根据单一接口的状态调整组内所有接口的状态，保证转发设备出接口和入接口状态的一致性，以防止在设备链路出现故障时，出现丢包情况。例如：当连接保护模式下的设备 A 负责转发数据的出口 down 掉时，属于同联动组的入口状态也同步

down，则入口所连设备将会判断入口 down 了，就可以及时将数据通过其它的设备 B 进行传输。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口**> **接口联动**。

步骤 2 添加联动组。

接口联动功能处于“  ”状态时，不能修改接口联动组的配置，必须停止联动组后，才可进行配置。

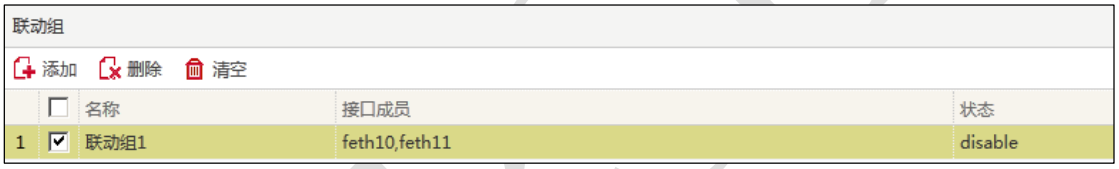
1）点击『添加』，进入“添加”对话框，如下图所示。

在添加接口联动组时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项。输入接口联动组的名称。 最多不能超过 31 个字节。
接口	选择接口联动组中的接口成员。 “选择成员”下的文本框中列出了设备当前所有的物理接口，选择该文本框中的接口后，点击【→】按钮将其添加到联动组中；“已经选择”下的文本框中列出了联动组中当前包括的接口，选中该文本框中的接口后，点击【×】按钮将其从联动组中删除掉。 说明： 1）联动组的接口成员可以是防火墙的物理接口或链路聚合口，不支持子接口和 VLAN； 2）同一个物理接口不能同时属于不同的联动组，并且每个联动组的成员数不能低于两个，不能高于八个； 3）已经加入到链路聚合中的接口不能再加入到接口联动组中。

2）点击【确定】按钮完成接口联动组的创建，点击【取消】按钮撤销本次操作。

刚创建成功的接口联动组处于“未运行”状态，如下图所示。



步骤 3 启动接口联动功能。

点击状态右侧的“  ”按钮，启动接口联动功能。此时，接口联动组处于“  ”状态。

此后，当该联动组内的一个物理接口 down 后，该组内所有的物理接口都同步 down 掉。

CLI 方式配置

步骤	配置命令	配置说明
1	**network suitstate add name** <*string1*> **member** <*string2*>	添加接口联动组。
2	**network suitstate clean** <cr>	删除所有接口联动组。
3	**network suitstate enable** <cr>	应用接口联动组。
4	**network suitstate show** <configuration|status>	查看接口联动组配置或者状态信息。

network suitstate add name <*string1*> **member** <*string2*>

命令描述：

添加接口联动组。

可使用 **suitstate delete name** <*string*>命令删除接口联动组。

参数说明：

add	添加接口联动组。
name	必选项，设置接口联动组名称。
string1	字符串类型，表示接口联动组名称。
member	必选项，设置接口联动组成员。
string2	字符串类型，表示物理接口名称，至少有 2 个接口，如 feth0 形式，多个接口用空格隔开。

使用说明：

接口联动组的成员只能是物理接口。

以下是添加接口联动组的示例：

添加接口联动组“feth1-2”，设置参与联动的物理接口为 feth1 和 feth2。

TopsecOS# **network suitstate add name** *feth1-2* **member** ‘*feth1 feth2’*

network suitstate clean <cr>

命令描述：

删除所有接口联动组。

以下是删除所有接口联动组的示例：

TopsecOS# **network suitstate clean**

network suitstate enable <cr>

命令描述：

启用接口联功能。

使用 **suitstate disable** <cr>命令禁用接口联功能。

network suitstate show <configuration|status>

命令描述：

显示接口联动的配置或状态。

参数说明：

show	必选项，显示接口联动的配置或状态。
configuration|status	显示接口联动的配置|显示接口联动的状态

以下是查看接口联动的当前状态的示例：

```
TopsecOS# network suitstate show status
```

6.3 VLAN

6.3.1 简介

VLAN

VLAN（Virtual Local Area Network，虚拟局域网）是一种从逻辑上将局域网划分的技术。一个 VLAN 即一个广播域。在二层网络中，同一 VLAN 互连互通，不同 VLAN 间相互隔离。要实现 VLAN 间的通信，需通过三层路由技术。

VLAN 划分不受物理位置限制，同一 VLAN 中的主机可以连接在同一交换机，也可连接在不同的交换机上。如下图所示，PC 1 和 PC 3，虽然都连接了 Switch A，但是分别划分到了 VLAN 1 和 VLAN 2 中，所以 PC 1 和 PC 3 不能直接通信。

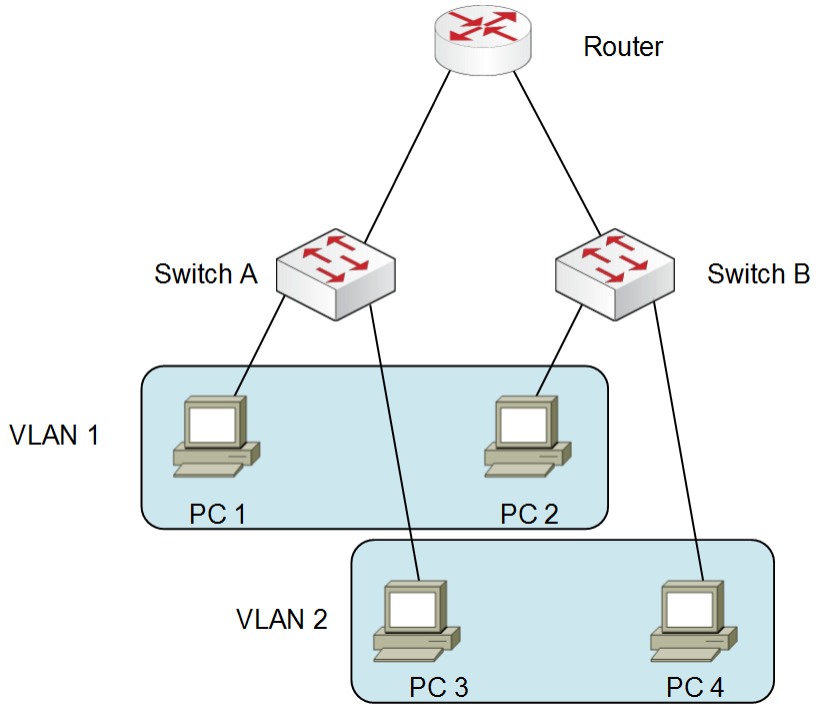


图 6-4 VLAN 示意图

VLAN 虚接口是 VLAN 内所有设备对外通信的出口，详细说明请参见 6.1 网络规划，其命名方式为“vlan.”加上四位 VLAN 的 ID 组成，如“vlan.0009”。

QinQ

QinQ（也称 Stacked VLAN 或 Double VLAN）技术是对 IEEE 802.1Q（即 VLAN）的扩展，是 IEEE 在 802.1ad 标准中定义的。

QinQ 是一种简单的二层 VPN 隧道（VLAN-VPN）技术，QinQ 报文共有 2 层的 VLAN 通过 Tag，包括用户网络（私网）的内层 VLAN Tag 和运营商网络（公网）的外层 VLAN Tag。在运营商网络接入端为私网报文封装外层 VLAN Tag，报文携带两层 VLAN Tag 穿越公网。在公网中，报文只根据外层 VLAN Tag 进行传输，用户的私网 VLAN Tag 则作为报文中的数据部分来进行传输。

通过该技术最多可以提供 4094×4094 个 VLAN，用户可以规划私网 VLAN ID，可以缓解日益紧缺的公网 VLAN ID（4094 个）资源，不会导致和公网 VLAN ID 冲突。QinQ 技术为小型城域网或企业网提供一种较为简单的二层 VPN 解决方案。

NGFW 支持在交换模式的接口上启用 QinQ 功能。QinQ 功能的基本原理如下图所示，当开启交换接口的 QinQ 功能后，接口接收到报文时，无论报文是否带有 VLAN

Tag，NGFW 都会为该报文打上本端口缺省 VLAN 的 VLAN Tag。这样，如果接收到的是已经带有 VLAN Tag 的报文，该报文就成为双 Tag 的报文；如果接收到的是不带 VLAN Tag 的报文，该报文就成为带有端口缺省 VLAN Tag 的报文。

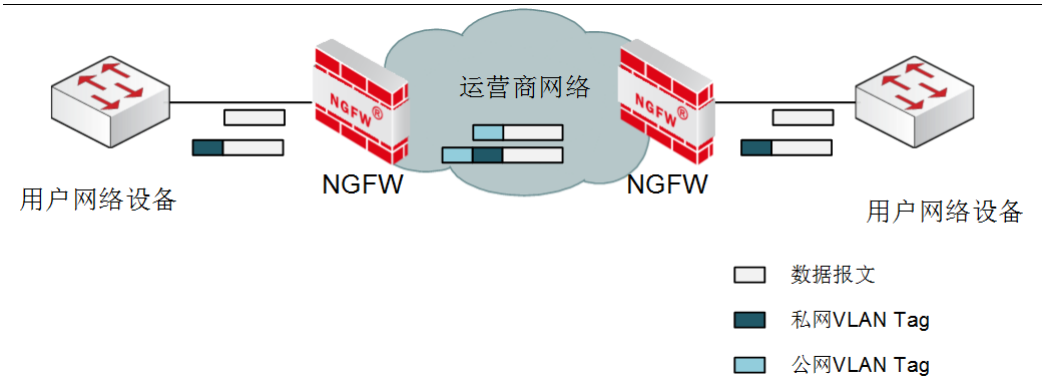


图 6-5 QinQ 基本原理示意图

6.3.2 配置接口 VLAN

NGFW 可用的 VLAN 数量为 4094 个，为解除城域网中可用 VLAN 数量的限制瓶颈，NGFW 支持在交换模式的接口上启用 QinQ 功能以扩充 VLAN 数量。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **VLAN**。

步骤 2 添加 VLAN。

1）点击『添加』，弹出“新增 VLAN”窗口。

在添加 VLAN 时，各项参数的具体说明如下表所示。

参数	说明
添加单个 VLAN	添加单个 VLAN 的 ID 号，取值范围：1-4094。 说明： 1）添加后，VLAN 的名称为“vlan. ID 号”，如 vlan.0001。 2）新添加的 VLAN 默认属于虚拟路由域 VR0。
添加 VLAN 范围	一次性添加多个名称连续的 VLAN。ID 号取值范围：1-4094。 说明： 1）起始 VLAN ID 和终止 VLAN ID 中设置的数值既可以相同也可以不同，但起始 VLAN ID 一定不能大于终止 VLAN ID。数值不同时，表示添加的是一段 ID 连续的 VLAN；数值相同时，表示添加的是某一个 VLAN。 2）一次性添加多个名称连续的 VLAN 时，单次最多添加 500 个。

2）设置完成后，点击【确定】按钮完成 VLAN 的添加，点击【取消】按钮撤销本次操作。如果添加 VLAN 成功，则新添加的 VLAN 会显示在界面中。

步骤 3 设置 VLAN 虚接口属性。

添加 VLAN 后，需要给 VLAN 虚接口配置接口 IP 地址和子网掩码等属性。

1）点击待配置 VLAN 虚接口对应的“操作”一列下的编辑图标“  ”，弹出“VLAN 配置”窗口。

在设置 VLAN 虚接口时，各项参数的具体说明如下表所示。

参数	说明
描述	输入对该接口的简要描述。
状态	默认接口为“启用”，表示可以使用该 VLAN；如果选择“停用”，则该 VLAN 将不会工作，该 VLAN 所在的区域将无法和其他接口进行通讯。
IPv4 地址/掩码	输入 VLAN 虚接口的 IPv4 地址及其子网掩码。 说明： NGFW 不同的 VLAN 虚接口之间、及与路由接口之间不能配置相同的 IPv4 地址或 Ipv4 地址不能在同一子网内。
非同步地址	如果在网络中配置了高可用性功能，则设置心跳口 IP 时必须要选择“非同步地址”，否则接口的 IP 地址信息会在主/从设备同步运行状态时被对方覆盖。热备组中的备设备的管理 IP 必须选择“非同步地址”，否则无法对备设备进行管理。关于双机热备的配置具体请参见 4.7 高可用性。
添加	点击【添加】按钮，如果设置正确，则新添加接口的 IP 地址会显示在列表中。
IPv6 地址	输入 VLAN 虚接口的 IPv6 地址。 说明： 1）可以为 VLAN 虚接口设置多个 IPv6 地址。 2）不同的 VLAN 虚接口不能配置相同的 IPv6 地址或 IPv6 地址不能在同一子网内。
添加	如果“IPv6 地址”设置正确，点击【添加】按钮，则新添加接口的 IPv6 地址会显示在列表中。
删除	点击 IPv6 地址对应的删除图标，可以删除添加的 IPv6 地址。

2）参数设置完成后，点击【确定】按钮完成 VLAN 虚接口的属性设置，点击【取消】按钮撤销该操作。

CLI 方式配置

步骤	配置命令	配置说明
1	**network interface** <*string*> **switchport** <cr>	设置接口为交换模式。
2	**network vlan add id** <*number*>	添加 VLAN。
	network vlan add range <*string*>	添加多个 VLAN。
3	**network vlan clean** <cr>	（可选）清除所有 VLAN。
4	**network interface** <*string*> **vlan-vpn** <enable|disable>	开启接口的 QinQ 功能。
5	**network interface** <*string1*> **vlan-vpn tpid** <*string2*>	设置 QinQ 功能使用的协议类型。

network vlan add id <*number*>

命令描述：

添加一个 VLAN。

使用 **network vlan delete id** <*number*>命令删除一个 VLAN。

参数说明：

network vlan add	添加一个 VLAN。
id	必选项，设置 VLAN 号。
number	数值类型，取值范围：1-4094。

以下为添加一个 VLAN 的示例：

添加 VLAN10。

```
TopsecOS# network vlan add id 10
```

network vlan add range <*string*>

命令描述：

一次添加一个或多个连续 VLAN。

使用 **network vlan delete range** <*string*>命令删除一个或者多个 VLAN。

参数说明：

network vlan add	添加一个或多个 VLAN。
range	必选项，设置 VLAN 号。
string	字符串类型，格式：A-B 或 A，A 和 B 为数值，取值范围：1-4094。 说明：如果添加一个 VLAN，可输入一个数值，也可输入 A-A；如果添加多个 VLAN，输入 A-B，且 A 需小于 B。

以下为添加多个连续 VLAN 的示例：

添加 VLAN10、VLAN11、VLAN12……VLAN100。

```
TopsecOS# network vlan add range10-100
```

network vlan clean <cr>

命令描述：

清除所有 VLAN。

以下为清除所有 VLAN 的示例：

```
TopsecOS# network vlan clean
TopsecOS# network vlan show
Number of existing VLANS          :0
VLAN      status        ports
------------------------------------------------------------------------------------------
```

network vlan show <cr>

命令描述：

显示所有 VLAN。

以下为显示所有 VLAN 的示例：

```
TopsecOS# network vlan add id 11
TopsecOS# network vlan add id 20
TopsecOS# network vlan add range 15-18
TopsecOS# network vlan show
Number of existing VLANS          :6
VLAN      status        ports
------------------------------------------------------------------------------------------
11        active
```

15	active
16	active
17	active
18	active
20	active

6.3.3 配置 QinQ

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **物理接口**。

步骤 2 点击某接口对应的操作图标“”，在弹出的“接口属性配置”对话框中配置接口属性。

步骤 3 设置接口为交换模式。在“基本属性”页签下，配置接口模式为“交换”。

步骤 4 配置 QinQ 功能。

在设置 QinQ 功能时，各项参数的具体说明如下表所示。

参数	说明
VLAN VPN 使能	默认接口为“停用”，表示关闭 QinQ 功能；如果选择“启用”，则表示已开启 QinQ 功能。
VLAN VPN 封装协议号	设置 QinQ 功能使用的协议类型，数值类型，十六进制形式，默认为 0x8100。 为了实现不同厂商的设备互通，接口 QinQ 外层 VLAN Tag 的协议类型应该配置为和该接口连接的设备能够识别的协议类型。 VLAN VPN 封装协议号一般只在网络侧接口配置，用于指定运营商采用的协议类型。

CLI 方式配置

network interface <*string*> **vlan-vpn** <enable|disable>

命令描述：

开启交换接口的 VLAN-VPN 功能。

参数说明：

network interface	必选项，指定设置 VLAN-VPN 功能的物理接口。
string	字符串类型，表示接口名称。
vlan-vpn	必选项，设置是否开启指定交换接口的 VLAN-VPN 功能。
enable|disable	开启|关闭

使用说明：

交换接口工作在 access 模式和 trunk 模式均支持 VLAN-VPN 功能。工作在 access 模式时，接口接收到数据报文时，NGFW 为该报文打上该 access 接口所属 VLAN 相应的 VLAN Tag；工作在 Trunk 模式时，接口接收到数据报文时，NGFW 为该报文打上该 Trunk 接口本地 VLAN 相应的 VLAN Tag，NGFW 的 Trunk 接口默认本地 VLAN 为 VLAN 1。

以下为开启接口 VLAN-VPN 功能的示例：

开启接口 feth0 的 VLAN-VPN 功能，并将该接口的本地 VLAN 修改为 VLAN5。

```
TopsecOS# network interface feth0 switchport
TopsecOS# network interface feth0 switchport trunk native-vlan 5
TopsecOS# network interface feth0 vlan-vpn enable
```

network interface <*string1*> **vlan-vpn tpid** <*string2*>

命令描述：

设置 VLAN-VPN 的协议类型。VLAN-VPN 的协议类型由报文外层 VLAN Tag 中的 TPID 字段来标识，不同厂商的设备只有具有相同的 TPID 值才能实现互通。NGFW 支持 TPID 调整功能，可以与 TPID 为 Ox8100 和 Ox9100 的厂商的设备实现互通。

参数说明：

network interface	必选项，指定设置 VLAN-VPN 功能的物理接口。
string1	字符串类型，表示接口名称。
vlan-vpn tpid	必选项，设置 NGFW 对经过 VLAN-VPN 接口的数据包进行封装的 TPID 字段值。
string2	字符串类型，16 进制，默认值：8100，即 Ox8100。

以下为设置 VLAN-VPN 协议类型的示例：

开启接口 feth0 的 VLAN-VPN 功能，设置该接口的本地 VLAN 为 VLAN5，调整 VLAN-VPN 协议类型值为 Ox9100。

TopsecOS# **network interface** *feth0* **switchport**

TopsecOS# **network interface** *feth0* **switchport trunk native-vlan** *5*

TopsecOS# **network interface** *feth0* **vlan-vpn** enable

TopsecOS# **network interface** *feth0* **vlan-vpn tpid** *9100*

6.4 链路聚合

6.4.1 简介

链路聚合功能，是将多个物理接口聚合成一个逻辑上的聚合组。在聚合组中，被捆绑在一起的物理接口称为成员接口，聚合所形成的逻辑接口称为聚合接口。物理接口加入聚合组后，工作模式为 SLAVE 模式。

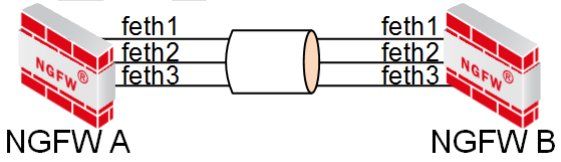


图 6-6 链路聚合示意图

链路聚合有如下优点：

- 聚合接口性能接近各个物理接口的性能总和，大大提高端口间的通信速度。
- 配置链路聚合功能时，无需重新布线，直接使用现有网络中的设备，减少网络维护工作。
- 聚合组内部的物理链路共同完成数据收发任务并相互备份，只要还存在能正常工作的链路，整个聚合组就不会失效，从而提高链路的可靠性。
- 聚合组内的成员接口可随时加入或者离开聚合组，管理员可根据实际需求灵活配置。

NGFW 支持手工方式链路聚合，手工链路聚合需要手工将物理接口加入到到聚合组中，所有的物理接口均处于转发状态，聚合组通过预先设置的负载均衡算法分担链路流量到聚合组中的不同链路，实现链路的负载均衡。

NGFW 通过采用不同的负载分担算法选择报文的发送接口，保证具有相同属性的报文能够从同一接口发送，可以灵活地实现对聚合组内业务流量的负载分担。

用户既可以指定系统按照报文中携带的端口号、IP 地址、MAC 地址等信息之一或其组合来选择所采用的负载分担模式。NGFW 支持的负载分担算法包括：

- src-mac：根据源 MAC 地址均衡，表示对发送的报文的源 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- dst-mac：根据目的 MAC 地址均衡，表示对发送的报文的目的 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-dst-mac：根据源和目的 MAC 地址组合均衡，表示对发送的报文的源和目的 MAC 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-ip：根据源 IP 地址均衡，表示对发送的报文的源 IP 地址进行哈希计算根据计算结果选择数据转发接口。
- dst-ip：根据目的 IP 地址均衡，表示对发送的报文的目的 IP 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-dst-ip：根据源和目的 IP 地址组合均衡，表示对发送的报文的源和目的 IP 地址进行哈希计算，根据计算结果选择数据转发接口。
- src-port：根据源 TCP/UDP 端口地址均衡，表示对发送的报文的源端口进行哈希计算，根据计算结果选择数据转发接口。
- dst-port：根据目的 TCP/UDP 端口地址均衡，表示对发送的报文的目的端口进行哈希计算，根据计算结果选择数据转发接口。
- src-dst-port：根据源和目的 TCP/UDP 端口地址均衡，表示对发送的报文的源和目的端口进行哈希计算，根据计算结果选择数据转发接口。
- quinary：根据五元组均衡，表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算，根据计算结果选择数据转发接口。
- per-packet：根据发送端口轮询均衡，表示发送数据时进行轮询，依次使用从第一个到最后一个可用的成员接口。

NGFW 支持 8 个聚合组，每个聚合组最多支持 8 个成员接口。

6.4.2 配置链路聚合

说明

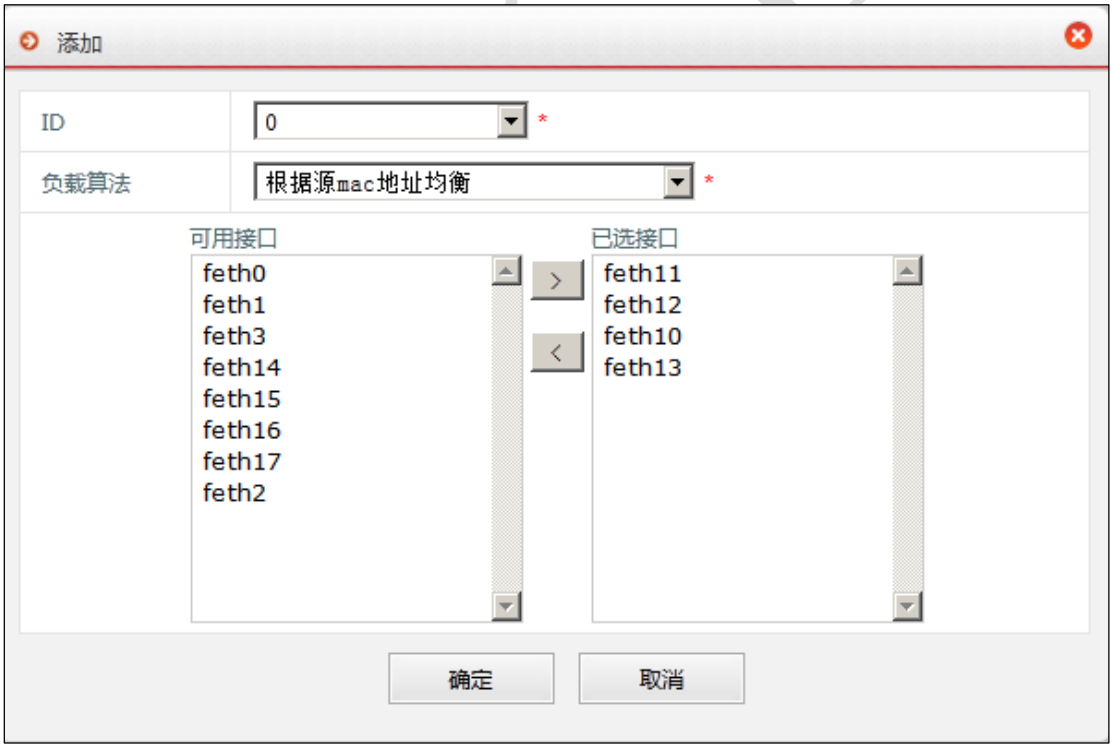
- ✧ 在 NGFW 上，只有路由工作模式的物理接口可以加入到聚合接口中，不支持 VLAN 虚接口或子接口等其他逻辑接口加入聚合接口中。
- ✧ 一个物理接口只能属于一个聚合接口。
- ✧ 聚合接口内的物理接口必须具备相同的属性，如相同的速度、单双工模式等。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **接口** > **聚合接口**。

步骤 2 添加新的聚合接口。

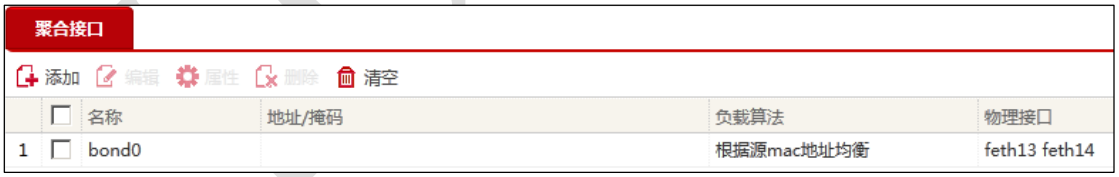
1）点击『添加』，添加新的聚合接口，如下图所示。



在添加聚合接口时，各项参数的具体说明如下表所示。

参数	说明
ID	必选项，选择聚合接口的 ID 号，可选项：0、1、2、3、4、5、6、7，聚合接口命名为 bond＋ID 号，例如此处设定为 0，则新添加的 bond 端口为 bond0。
负载算法	必选项，设置负载均衡算法，根据计算结果，选择聚合组内不同的物理接口转发流量。可选项： 1）根据源 mac 地址均衡：对发送报文的源 MAC 地址进行哈希计算。 2）根据目的 mac 地址均衡：对发送报文的目的 MAC 地址进行哈希计算。 3）根据源和目的 mac 地址组合均衡：表示对发送报文的源和目的 MAC 地址进行哈希计算。 4）根据源 IP 地址均衡：对发送报文的源 IP 地址进行哈希计算。 5）根据目的 IP 地址均衡：对发送报文的目的 IP 地址进行哈希计算。 6）根据源和目的 IP 地址组合均衡：对发送报文的源和目的 IP 地址进行哈希计算。 7）根据源 TCP/UDP 端口均衡：对发送报文的源端口进行哈希计算。 8）根据目的 TCP/UDP 端口均衡：对发送报文的目的端口进行哈希计算。 9）根据源和目的 TCP/UDP 端口组合均衡：对发送报文的源和目的端口进行哈希计算。 10）根据五元组均衡：对发送报文的源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算。 11）根据发送端口的轮流均衡：发送报文时进行轮询，依次使用从第一个到最后一个可用的成员接口。
物理接口	选择将哪些物理接口加入到该聚合接口中。

2）参数设置完成后，点击【确定】按钮完成聚合链路添加，新添加的逻辑端口将显示在界面中，如下图所示。



步骤 3 设置聚合接口属性。

点击某聚合接口对应的『属性』，可以设置聚合接口属性。关于属性参数的解释具体请参见 6.2.3 配置接口基本属性。不同的是，不能设置聚合接口的 MAC 地址、接口速率等参数。加入链路聚合的端口其属性显示为“SLAVE”，如下图所示。

物理接口

	名称	描述	接口模式	地址/掩码	MTU	状态	链路状态	双工模式	速率	操作
1	feth0		路由	IPv4:192.168.16.2/255.255.255	1500	启用		Full-duplex	100Mb/s	
2	feth1		交换		1500	启用		-	-	
3	feth2		交换		1500	启用		-	-	
4	feth3		交换		1500	启用		-	-	
5	feth10		交换		1500	启用		-	-	
6	feth11		虚拟线		1500	启用		-	-	
7	feth12		虚拟线		1500	启用		-	-	
8	feth13		SLAVE		1500	启用		-	-	
9	feth14		SLAVE		1500	启用		-	-	
10	feth15		交换		1500	启用		-	-	
11	feth16		交换		1500	启用		-	-	
12	feth17		交换		1500	启用		-	-	

当物理接口加入聚合接口（即成为聚合接口的 SLAVE 接口）后，不能对它再进行 IP 层以上的配置，即禁止设置 SLAVE 设备的 IP 地址、MAC 地址、MTU 值、mss-adjust 值、子接口，禁止设置 SLAVE 设备为交换口。只能启用/禁用接口，配置接口 Speed、配置 MTU 值。

CLI 方式配置

步骤	配置命令	配置说明
1	**network bond add id** <*number*> **load-balance** <per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip| src-dst-ip|src-port|dst-port|src-dst-port|quinary>	增加一个聚合接口，同时指定负载均衡算法。
2	**network bond leave id** <*number*> **dev** <*string*>	将物理接口从聚合接口删除。
3	**network bond modify id** <*number*> **load-balance** <per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip| src-dst-ip|src-port|dst-port|src-dst-port|quinary>	修改一个聚合接口的属性。
4	**network bond join id** <*number*> **dev** <*string*>	将物理接口加入到聚合接口。
5	**network bond clean** <cr>	清空所有聚合接口。

network bond add id <*number*> **load-balance** <per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary>

命令描述：

增加一个聚合接口，同时指定负载均衡算法。

使用 **network bond delete id** <*number*>命令删除聚合接口。

参数说明：

add	增加一个聚合接口。
id	必选项，指定接口 ID 号。
number	数值类型，取值范围：0-7。
load-balance	必选项，指定负载均衡算法，将流量分配给聚合链路内不同的物理接口。
per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip|src-dst-ip|src-port|dst-port|src-dst-port|quinary	可选项： 1）src-mac：对发送的报文的源 MAC 地址进行哈希计算。 2）dst-mac：对发送的报文的目的 MAC 地址进行哈希计算。 3）src-dst-mac：对发送的报文的源和目的 MAC 地址进行哈希计算。 4）src-ip：对发送的报文的源 IP 地址进行哈希计算。 5）dst-ip：对发送的报文的目的 IP 地址进行哈希计算。 6）src-dst-ip：对发送的报文的源和目的 IP 地址进行哈希计算。 7）src-port：对发送的报文的源端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 8）dst-port：对发送的报文的目的端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 9）src-dst-port：对发送的报文的源和目的端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 10）quinary：根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算。 11）per-packet：发送数据时进行轮询，依次使用从第一个到最后一个可用的 slave 接口。

使用说明：

1）一个物理接口只能属于一个聚合接口。

2）支持在聚合接口上做 GRE（但是反过来不行，GRE 是虚接口，不可以把 GRE 接口加入端口聚合）。

3）当物理接口加入 bond 成为 slave 接口后，不能对它再进行 IP 层以上的配置，即禁止设置 slave 设备的 ip 地址、MAC 地址、MTU 值、mss-adjust 值、子接口，禁止设置 slave 设备为交换口。只能启用/禁用接口，配置接口 speed、配置 MTU 值。

以下是添加聚合接口的示例：

添加 ID 号为 1 的聚合接口，采用轮询算法进行负载均衡。

```
TopsecOS# network bond add id 1 load_blance per-packet
```

network bond clean <cr>

命令描述：

清空所有聚合接口。

network bond join id <*number*> **dev** <*string*>

命令描述：

将物理接口加入到聚合接口。

参数说明：

join	把物理接口加入到聚合接口。
id	必选项，指定接口 ID 号。
number	数值类型，取值范围：0-3。
dev	必选项，指定物理接口。
string	字符串类型，表示接口名。

使用说明：

加入到聚合接口的物理接口必须满足如下条件：

1）不是交换模式

2）还没有加入其他 bond

3）没有子接口

4）在静态 arp 表里没有对应项

以下是将物理接口加到聚合接口的示例：

将接口 eth0 加入到 ID 号为 1 的聚合接口。

```
TopsecOS# network bond join id 1 dev eth0
```

network bond leave id <*number*> **dev** <*string*>

命令描述：

将物理接口从聚合接口删除。

参数说明：

leave	把物理接口从聚合接口删除。
id	必选项，指定接口 ID 号。
number	数值类型，取值范围：0-3。
dev	必选项，指定物理接口。

string	字符串类型，表示接口名。

以下是将物理接口从聚合接口删除的示例：

将接口 eth0 从 ID 号为 1 的聚合接口删除。

```
TopsecOS# network bond leave id 1 dev eth0
```

network bond modify id <*number*> **load-balance** <per-packet|src-mac|dst-mac|src-dst-mac|src-ip|dst-ip| src-dst-ip|src-port|dst-port|src-dst-port|quinary>

命令描述：

修改一个聚合接口的属性。

参数说明：

modify	修改一个聚合接口的属性。
id	必选项，指定接口 ID 号。
number	数值类型，取值范围：0-3。
load-balance	必选项，指定负载均衡算法，将流量分配给聚合链路内不同的物理接口。
per-packet|src-mac|dst-mac| src-dst-mac|src-ip|dst-ip| src-dst-ip|src-port|dst-port| src-dst-port|quinary	可选项： 1）Src-mac：表示对发送的报文的源 MAC 地址进行哈希计算。 2）dst-mac：表示对发送的报文的目的 MAC 地址进行哈希计算。 3）src-dst-mac：表示对发送的报文的源和目的 MAC 地址进行哈希计算。 4）Src-ip：表示对发送的报文的源 IP 地址进行哈希计算。 5）dst-ip：表示对发送的报文的目的 IP 地址进行哈希计算。 6）src-dst-ip：表示对发送的报文的源和目的 IP 地址进行哈希计算。 7）Src-port：表示对发送的报文的源端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 8）dst-port：表示对发送的报文的目的端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 9）src-dst-port：表示对发送的报文的源和目的端口进行哈希计算决定分配给聚合接口内哪个 slave 接口。 10）Quinary：表示根据源地址、目的地址、源端口、目的端口和 IP 协议类型进行哈希计算。 11）Per-packet：表示发送数据时进行轮询，依次使用从第一个到最后一个可用的 slave 接口。

以下是修改指定聚合接口属性的示例：

修改 ID 号为 1 的聚合接口的负载均衡算法为 dst-ip，对发送的报文的目的 IP 地址进行哈希计算决定将数据分配给聚合接口内哪个成员接口。

TopsecOS# **network bond modify id** *1* **load_blance** dst-ip

network bond show <cr>

命令描述：

显示聚合接口配置。

6.5 路由

路由指利用网络层协议将数据包从源主机通过寻址方案最终转发到目标主机的过程，最终实现不同网段间网络节点的互联互通。NGFW 工作在路由模式下时，转发数据报文的关键是路由表，表中每条路由项都指明分组到某子网或某主机应通过 NGFW 的哪个接口发送出去。

NGFW 支持的路由类型包括：直连路由、静态路由和策略路由，其中，策略路由优先级高于静态路由。

- 直连路由：指路由接口所连接子网的路由，随路由接口的启用自动生成。
- 静态路由：基于数据报文的目的地址选路。由管理员手工添加，具有简单、稳定、安全、不随网络的变化而自动更新特征，网络故障或网络结构发生变化时，需由管理员手工修改，因此，静态路由适用于网络结构较简单的网络。
- 策略路由：可基于数据报文的源地址、源端口、目的地址、目的端口和协议选路。由管理员手工添加，具有不随网络的变化动态更新、可精细控制路由选路行为等特征。

数据报文经过 NGFW 路由模块时，路由的查找原则如下：

1）如果入接口或 VR 绑定了策略路由，报文将匹配该入接口或相应 VR 绑定的所有策略路由项，有匹配项，则根据策略路由网关和出接口转发数据报文。

2）如果入接口没有绑定策略路由或者策略匹配失败时，则查找静态路由，有匹配项，则根据静态路由网关和出接口转发数据报文。

3）静态路由匹配失败时，则根据缺省路由处理数据报文。

说明

✧ 报文成功匹配路由表中多条路由条目后，遵循以下标准：（a）最小度量值路由优先；（b）度量值相同，最大权重值路由优先；（c）度量值和权重值均相同，通过此多条链路负载分担流量。

6.5.1 静态路由

天融信 NGFW 支持 IPv4 静态路由和 IPv6 静态路由，静态路由需由管理员手工添加，不随网络结构的变化而发生任何变化。其表项的各字段包括：目的地址、掩码、网关、度量值、出接口、标记。

数据报文匹配静态路由时，如果数据报文满足路由表项的目的地址和掩码匹配条件，NGFW 则根据该路由表项的网关和出接口确定从哪个接口转发报文；如果数据报文同时匹配多条静态路由，NGFW 通过负载分担方式处理报文。

IPv4 静态路由用于实现 IPv4 网络互连互通，IPv6 静态路由用于实现 IPv6 网络互连互通，其主要区别是地址格式不同，配置 IPv4 静态路由时使用 IPv4 地址，配置 IPv6 静态路由时使用 IPv6 地址。静态路由表项各字段说明如下：

- 目的地址（必选）：标识 IP 数据包的目的地址或目的网络。
- 网络前缀（必选）：与目标地址一起标识目的主机所在网段。将目的地址与掩码进行“逻辑与”运算后可得到目的主机所在网段的网络号。
- 网关（必选）：一般指 IP 数据包经过 NGFW 后下一跳路由设备的 IP 地址。
- 度量值（具有默认值）：标识路由至目的地址的开销，路由度量值只在同一路由协议内起作用，不同路由协议的路由的度量值没有可比性。度量值表明路由表项的优先级，度量值越小路由优先级越高。对于去往同一目的地的多条路由，如果此多条路由优先级不同，可实现路由备份，优先级最高的路由为主路由，优先级次高的路由为备份路由；如果此多条路由优先级相同，此多条路由为等价路由，可实现流量的负载均衡。
- 出接口（可选）：指定目的地址为非 NGFW 的 IP 数据包经哪个接口转发出去。

- 标记（系统根据路由自动标记）：表明路由表项的路由类别及其所处状态，S：静态路由；C：直连路由；L：回环路由；H：主机路由；I：指定出接口；G：指定网关；U：路由处于启用状态。

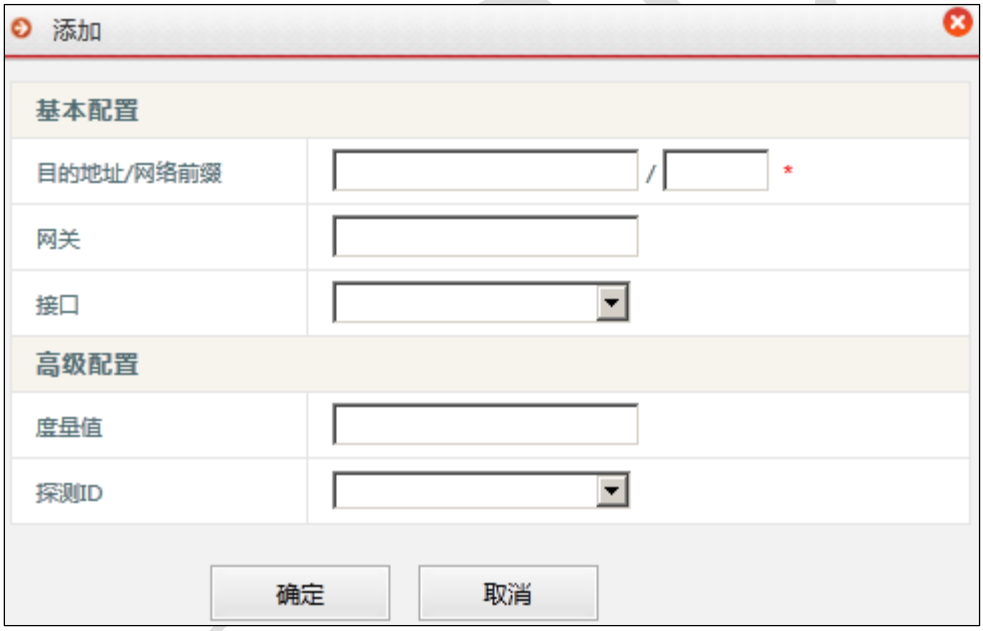
WEBUI 方式配置

在配置静态路由之前，需要先进行如下步骤：

- 配置路由接口 IP 地址。关于接口的配置具体请参见 6.2 接口。
- 确定 NGFW 路由表中的直连路由。
- 确定所添加的静态路由的目标地址。
- 明确数据通信是双向过程，确保通过 NGFW 的数据包具备来和回路由。

步骤 1 选择 **网络配置** > **路由** > **路由**。

步骤 2 点击『添加』，如下图所示。



在添加静态路由时，各项参数的具体说明如下表所示。

参数	说明
目的地址/网络前缀	必选项。用来标识 IPv4/IPv6 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。 说明： 1）IPv4 目标地址格式：x.x.x.x/(0-32)；IPv6 目标地址格式：x:x:x:x:x:x:x:x/(0-128)。

参数	说明
	2）IPv4 目的地址设置为 0.0.0.0/0，IPv6 目的地址设置为::/0 时，配置的为缺省路由，当数据包查找路由表没有匹配项后，NGFW 根据缺省路由进行数据包的转发。
网关	必选项。指定路由的网关地址，通常为下一跳路由器的入口 IP 地址。 说明： 对于点对点网络，配置路由时可以不指定网关而只指定出接口；但对于以太网多路访问链路中，必须指定网关，否则 NGFW 通过 ARP 协议获取下一跳网络设备的 MAC 地址时，无法获取到下一跳设备相应接口的 MAC 地址，导致数据包在发送前封装失败。NGFW 网络通信接口目前只支持以太网接口，因此网关为必选参数。
接口	指定数据报文从 NGFW 的哪个接口进行转发。可以选择物理接口或 VLAN 虚接口。
度量值	设置路由的优先级，值越小，优先级越高。 说明： 同一目的地存在多条路由时，优先级高的路由将成为当前的最优路由。
探测 ID	选择已经设置的探测链路的 ID 号，用于探测路由是否可达。如果不选择，则不进行探测。

步骤 3 参数设置完成后，点击【确定】按钮完成路由的添加。

CLI 方式配置

network route add [**family** <ipv4|ipv6>] **dst** <*string1*> **gw** <*gwaddress*> [**dev** <*string2*>] [**metric** <*number1*>] [**vr_id** <*number2*>] [**id** <*number3*>]

命令描述：

添加一条静态路由。配置静态路由时，必须指定目的地址和网关。

对于同一目的地存在多条静态路由时，度量值 metric 最小路由将优先级最高，度量值相同时，可实现到达同一目的流量的负载分担。

参数说明：

network route add	添加一条静态路由。
family	添加 IPv6 静态路由时，该参数为必选参数。用于设置静态路由的类型，默认为 IPv4 静态路由。
ipv4|ipv6	IPv4 静态路由|IPv6 静态路由
dst	必选项，设定目标地址/掩码。
string1	字符串类型，添加 IPv4 静态路由时，格式为 A.B.C.D/(0-32)；添加 IPv6 静态路由时，格式为 X:X:X:X:X:X:X:X/(0-128)，其中 X 为一个 4 位十六进制整数。
gw	必选项，设定路由的下一跳。

gwaddress	网关地址字符串，对于 IPv4 静态路由，格式为 A.B.C.D；对于 IPv6 静态路由，格式为 X:X:X:X:X:X:X:X，其中 X 为一个四位十六进制整数。
dev	可选项，设定路由出接口，可为物理接口或虚接口。
string2	字符串类型，表示出接口，如 feth0。
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。
number1	数值类型。
vr_id	可选项，指定添加路由到哪个 VR，如果不指定 VR，默认将路由添加到 VR0。
number3	数值类型，指 VR 的 ID。
id	可选项，指定路由的 id 号，建议不要指定。
number2	数值类型，取值范围：100-13000，不能与已有策略 ID 相冲突。

以下为添加静态路由的示例：

添加一条目的地址为 202.103.96.0/24、网关为 192.168.90.1、出接口为 feth2 的 IPv4 静态路由。

TopsecOS# **network route add dst** *202.103.96.0/24* **gw** *192.168.90.1* **dev** *feth2*

TopsecOS# **network route show family** ipv4

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

ID	Destination	Gateway	Flags	Metric	Vr	Iface
100	202.103.96.0/24	192.168.90.1	GSi	0	0	feth2

添加一条目的地址为 2fbb:aabb::/64、网关为 3faa::aaaa 的 IPv6 静态路由。

TopsecOS# **network route add family** ipv6 **dst** *2fbb:aabb::/64* **gw** *3faa::aaaa*

TopsecOS# **network route show family** ipv6

Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface

ID	Destination	Next Hop	Flags	Metric	Vr	Iface
101	2fbb:aabb::/64	2faa::aaaa	GS	1024	0	*

network route show family <ipv4|ipv6> [**vr_id** <*number*>]

命令描述：

查看静态路由。

参数说明：

network route show	查看静态路由。
family	必选项，设置查看静态路由的类型。
ipv4|ipv6	IPv4 静态路由|IPv6 静态路由
vr_id	可选项，设置查看哪个 VR 的静态路由。
number	数值类型，指 VR 的 ID。

以下为查看静态路由的示例：

查看所有静态路由。

```
TopsecOS# network interface show
Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface
========================IPv4================================
ID      Destination          Gateway          Flags   Metric   Vr    Iface
100     202.103.96.0/24      192.168.90.1     GSi     0        0     feth0
======================IPv6==================================
ID      Destination          Next Hop         Flags   Metric   Vr    Iface
101     2fbb:aabb::/64       2faa::aaaa       GS      1024     0     *
```

查看 IPv4 静态路由。

```
TopsecOS# network interface show family ipv4
Flags: U-Up, G-Gateway, H-Host, S-Static, L-Local, C-Connected, i-Interface
ID      Destination          Gateway          Flags   Metric   Vr    Iface
100     202.103.96.0/24      192.168.90.1     GSi     0        0     feth0
```

network route clean [**family** <ipv4|ipv6>] [**vr_id** <*number*>]

命令描述：

清除静态路由。

参数说明：

network route clean	清除静态路由。
family	可选项，设置清除静态路由的类型。
ipv4|ipv6	IPv4 静态路由|IPv6 静态路由
vr_id	可选项，设置清除哪个 VR 的静态路由。
number	数值类型，指 VR 的 ID。

以下为清除静态路由的示例：

清除所有 IPv6 静态路由。

```
TopsecOS# network route clean family ipv6
```

6.5.2 策略路由

策略路由可针对具体的应用流量进行选路，不仅能够根据目的地址和目的端口，而且能够根据 IP 地址、端口和协议类型条件来确定报文的转发路径，可使不同类型的流量分别走不同的链路，达到保证类应用走优质链路，非保证类应用走另外链路的目的。此外，策略路由还可根据其度量值和权重值属性实现多链路的负载均衡和链路备份。

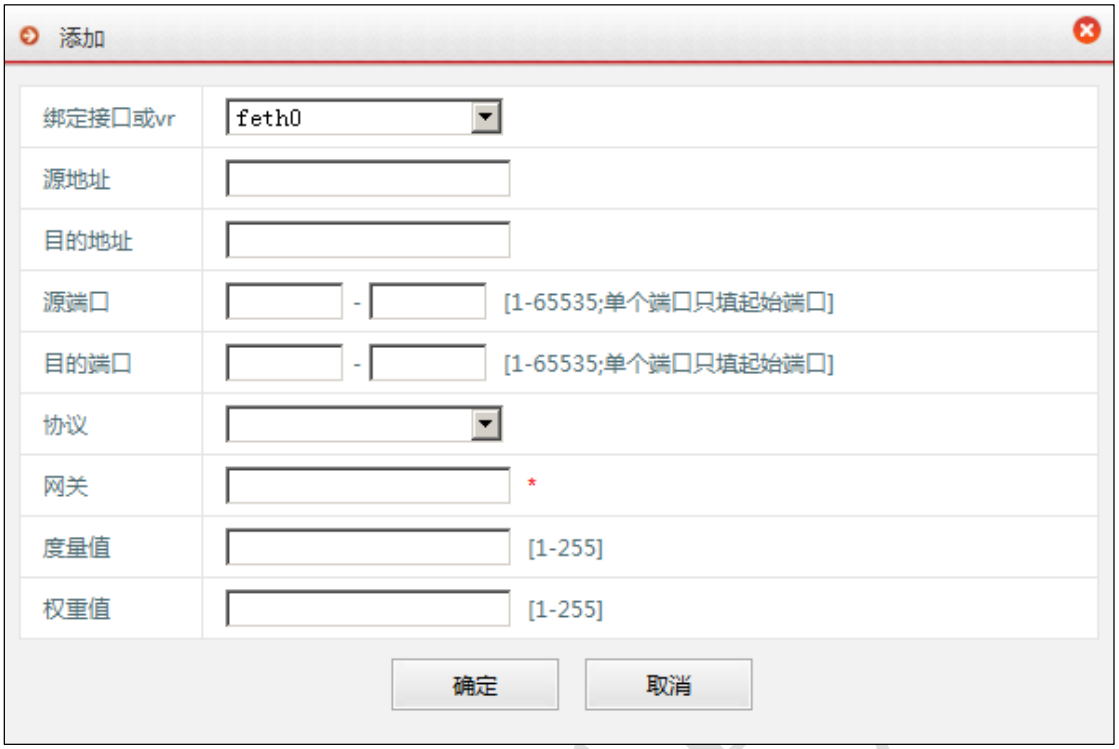
NGFW 的策略路由可与入接口和 VR 绑定，数据报文匹配策略路由时，首先匹配其进入 NGFW 时的入接口所绑定的策略路由，如果无匹配项，则再匹配处理该数据报文的 VR 所绑定的策略路由。

本节介绍策略路由的相关配置：包括策略路由的添加、删除、清空操作，以及通过移动来改变策略路由中路由条目的默认排列顺序。

WEBUI 方式配置

步骤 1 选择 **网络配置** > **路由** > **策略路由**。

步骤 2 点击『添加』，如下图所示。



在添加策略路由时，各项参数的具体说明如下表所示。

参数	说明
绑定接口或 vr	绑定策略路由的入接口或 vr。
源地址	用来标识 IP 包的源地址或源网络。注意填写源地址转换前的 IP 及掩码，也就是真实的子网地址。
目的地址	用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。
源端口	标识数据包的源端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
目的端口	标识数据包的目的端口的范围，如果为单个端口，则只填写起始端口即可。默认是所有端口。
协议	通过下拉框选择数据包使用的协议。
网关	指定数据报文从 NGFW 的哪个接口转发出去。
度量值	接口跃点数。度量值的大小定义了路由的优先级，度量值越小，优先级越高。
权重值	设置该策略路由的权重值。 说明： 如果策略路由表中存在多个度量值相同的下一跳，则根据权重值分配各链路负载网络流量的百分比。

步骤 3 点击【确定】按钮完成策略路由的创建。

CLI 方式配置

network route-policy add-entry bind <vr|interface> **name** <*string1*> **gw** <*gwaddress*> [**src** <*string2*>] [**sport** <*number1*>] [**sport2** <*number2*>] [**dst** <*string3*>] [**dport** <*number3*>] [**dport2** <*number4*>] [**protocol** <*string4*>] [**dev** <*string5*>] [**metric** <*number5*>] [**weight** <*number6*>]

命令描述：

添加一条策略路由。

参数说明：

network route-policy add-entry	添加一条策略路由。
bind	必选项，将策略路由与 VR 或接口绑定。
vr|interface	虚拟路由域|接口
name	必选项，指定策略路由绑定的 VR 或接口名称。
string1	字符串类型。
src	可选项，设定源地址/掩码。
string2	格式为 A.B.C.D/(0-32)的字符串，表示源地址/掩码。
sport	可选项，标识数据包的源端口的起始端口，如果为单个端口，则只填写起始端口即可。
number1	数值类型。
sport2	可选项，标识数据包的源端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number2	数值类型，应大于等于 sport 设定的端口号。
dst	可选项，用来标识 IP 包的目的地址或目的网络。需要填写目的地址转换后的真实地址。
string3	表示目标地址/掩码。
dport	可选项，标识数据包的目的端口的起始端口，如果为单个端口，则只填写起始端口即可。
number3	数值类型，取值范围：0-65535。
dport2	可选项，标识数据包的目的端口的结束端口，如果为单个端口，可以不必填写该项，也可以填写与起始端口相同的端口号。
number4	数值类型，取值范围：0-65535。应大于等于 dport 设定的端口号。
protocol	可选项，设置数据包使用的协议。
string4	为 0-255 的数值或 TCP、UCP、ICMP 等协议名称。
gw	必选项，设定网关地址。
gwaddress	表示网关 IP 地址。
dev	必选项，指定转发接口。包括物理接口、虚接口和子接口。
string5	字符串类型。如 feth0。
metric	可选项，指定路由度量值，metric 值越小，路由优先级越高。默认为 1。

number5	数值类型。
weight	可选项，设置该策略路由的权重值。
number6	数值类型。

以下是添加一条策略路由的示例：

对于源地址为 192.168.90.0/24，目的地址为 192.168.83.0/24，且从 NGFW 的 feth0 进入的数据报文，网关为 192.168.16.1。

TopsecOS#**network route-policy add-entry bind** interface **name** *feth0* **gw** *192.168.16.1* **src** *192.168.90.0/24* **dst** *192.168.83.0/24*

network route-policy clean-entry bind <vr|interface> **name** <*string*> **id** <*number*>

命令描述：

删除一条策略路由。

参数说明：

route-policy clean -entry	删除一条策略路由条目。
bind	必选项，设置策略路由与 VR 还是接口绑定。
vr|interface	虚拟路由域|接口
name	必选项，设置虚拟路由域或接口名称。
string	字符串类型。
id	必选项，设置需要删除的策略路由条目的 ID。
number	数值类型。

以下是删除策略路由的示例：

删除一条与接口 feth0 绑定且 ID 为 2 的策略路由。

TopsecOS#**network route-policy clean-entry bind** interface **name** *feth0* **id** *2*

network route-policy move bind <vr|interface> **name** <*string*> **id** <*number1*> **to** <before|after> **id** <*number2*>

命令描述：

移动策略路由条目。

参数说明：

route-policy move	移动策略路由条目。
bind	必选项，设置策略路由绑定 VR 还是接口。

vr|interface	虚拟路由域|接口
name	必选项，指定策略路由所绑定 VR 或接口的名称。
string	字符串类型。
id	必选项，指定待移动的策略路由条目的 ID 号。
number1	数值类型。
to	必选项，指定策略路由移动方式。
before|after	移动到基准策略路由条目之前|之后
id	必选项，指定基准策略路由条目的 ID 号。
number2	数值类型。

以下是移动策略路由的示例：

移动 ID 为 101 且绑定接口 feth0 策略路由移动到 ID 为 103 的策略路由之后。

TopsecOS#**network route-policy move bind** interface **name** *feth0* **id** *101* **to** after **id***103*

network route-policy show bind <vr|interface> **name** <*string*>

命令描述：

显示绑定某接口或 VR 的策略路由。

参数说明：

route-policy show	显示策略路由。
bind	必选项，设置策略路由绑定 VR 还是接口。
vr|interface	虚拟路由域|接口
name	必选项，指定策略路由所绑定 VR 或接口的名称。
string	字符串类型。

以下是显示与某接口或 VR 绑定的策略路由的示例：

显示与接口 feth0 绑定的策略路由。

TopsecOS#**network route-policy show bind** interface **name** *feth0*

network route-policy list <cr>

命令描述：

显示所有策略路由。

以下是显示所有策略路由的示例：

TopsecOS#**network route-policy list**

network route-policy clear <cr>

命令描述：

删除所有策略路由。

以下是删除所有策略路由的示例：

TopsecOS#**network route-policy clear**

6.6 邻居

6.6.1 简介

ARP

以太网设备在发送数据包前需封装第二层报头（包含 MAC 地址）和第三层报头（包含 IP 地址），但是 IP 地址和 MAC 地址相互独立，在发送报文时仅知道设备的 IP 地址，此时需要 ARP（Address Resolution Protocol，地址解析协议）协议根据已知的 IP 地址解析出二层的 MAC 地址。

当主机在以太网中发送数据包时，根据目的地址与主机是否处于同一个网段可进行不同的处理。

1）如果目的地址与主机处于同一个子网，根据主机 ARP 表中是否存在目的地址的 ARP 表项，可进行如下处理。

- PC A 在 ARP 表中查找到 PC D 表项，直接利用其中的 MAC 地址对 IP 报文进行数据帧封装，发送给 PC D。
- PC A 在 ARP 表中未查找到 PC D 表项，ARP 工作过程如图 6-7 所示。
  - PC A 以广播方式发送一个 ARP 请求报文。该报文的源 IP 地址和源 MAC 地址为 PC A 的 IP 地址和 MAC 地址，目的 IP 地址为 PC D 的 IP 地址、目的 MAC 地址为全 0。

- 处于同一广播域内的所有设备均可接收到该 ARP 请求报文，并将自己的 IP 地址与报文中的目的 IP 地址比较，若不同则丢弃报文，不做任何应答。
- PC D 在发现请求报文中 IP 地址与自身的 IP 地址相同，于是将 ARP 请求报文中的源 IP 地址和源 MAC 地址的映射关系存入自己的 ARP 表中，发送 ARP 响应报文给 PC A。ARP 响应报文以单播方式发送，其中包含 PC D 的 MAC 地址。
- PC A 收到 ARP 响应报文后，在 ARP 表中加入 PC D 的 MAC 地址用于后续的报文转发，并将 IP 报文进行数据帧封装，发送给 PC D。

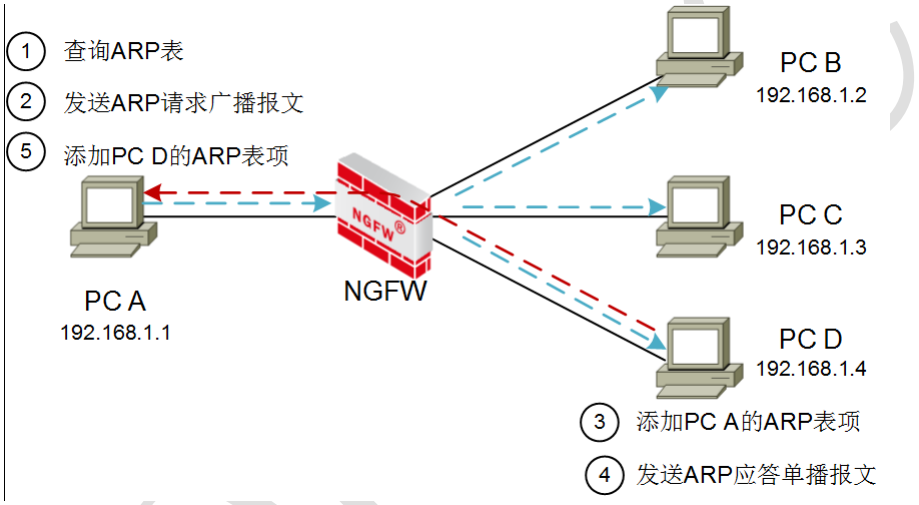


图 6-7 ARP 工作过程示意图

2）如果目的地址与主机处于不同子网，PC A 会广播 ARP 请求报文，此时网关进行应答，发送 ARP 响应报文给 PC A，将自己的 MAC 地址写入 PC A 的该 ARP 表项。网关收到报文后，再经过 1）中处于同一子网的处理步骤，将报文转发给 PC B。

ARP 表用于存储 IP 地址到 MAC 地址的映射，包括动态 ARP 表项和静态 ARP 表项两种。其中，动态 ARP 表项由设备动态学习，通过 ARP 协议动态更新，超过 ARP 表项老化时间后将被自动删除；静态 ARP 表项由管理员手工添加，则不存在老化问题，而且能够有效地防止 ARP 欺骗。

Neighbor

IPv6 协议扩大了地址空间，使得网络节点只需要知道链路层地址及本地网络的子网前缀，就能够通过无状态或全状态自动配置得到唯一的 IPv6 地址而成为网络的一部

分。同时，IPv6 还支持网络节点的移动性。这些功能都是通过邻居发现协议（NDP，Neighbor Discovery Protocol）来实现的，同一个子网内所有主机与路由器之间的交互也都是通过邻居发现协议来实现的。

邻居发现协议是 IPv6 协议的关键组成部分，采用路由器请求（RS，Router Solicitation）、路由器通告（RA，Router Advertisement）、邻居请求（NS，Neighbor Solicitation）、邻居通告（NA，Neighbor Advertisement）和重定向 5 种类型的 IPv6 控制信息报文（ICMPv6，Internet Control Management Protocol Version 6），实现了在 IPv4 中的地址解析协议（ARP）、控制报文协议（ICMP）中的路由器发现协议和重定向协议的所有功能，并具有邻居不可达检测机制。

- 路由器请求报文：主机启动后，向路由设备发出路由器请求，路由设备则会以路由器通告报文响应。
- 路由器通告报文：路由设备周期性的发布路由器通告报文，或者响应主机的路由器请求，其中包括前缀和一些标志位的信息。
- 邻居请求报文：IPv6 节点发送邻居请求报文，请求邻居的链路层地址，检查邻居是否可达，也可以验证邻居的地址是否是唯一的。
- 邻居通告报文：邻居通告报文是 IPv6 节点对邻居请求报文的响应，或者 IPv6 节点在链路层变化时也可以主动发送邻居通告报文。
- 重定向报文（Redirect）报文：路由设备通过发送重定向报文，通知链路上报文的发送节点，网络中存在更优的转发数据报文的路由设备。节点接收到重定向报文后，修改本地路由表项，选择最优路径转发。

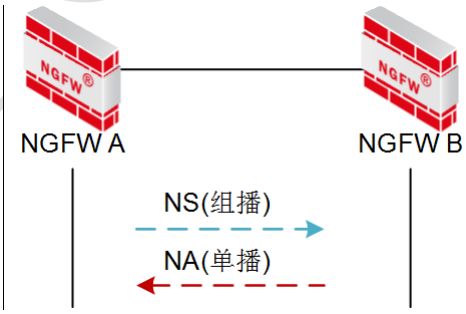


图 6-8 邻居地址解析过程示意图

如上图所示，以 NGFW A 为例，NGFW A 要获取 NGFW B 的 MAC 地址，说明邻居地址解析过程，实现过程如下。

1）NGFW A 通过组播方式发送 NS 消息。其中 NS 消息的源地址是 NGFW A 的 IPv6 地址，目的地址是被请求节点 NGFW B 的组播地址，NS 消息中还包含了 NGFW A 的 MAC 地址。

2）NGFW B 收到 NS 消息后，判断报文的目的地址是否为自己的 IPv6 地址对应的被请求设备组播地址。如果是，则 NGFW B 可以学习到 NGFW A 的 MAC 地址，并以单播方式发送 NA 消息，其中包含了自身的 MAC 地址。

3）NGFW A 收到 NGFW B 发送的 NA 消息，获得 NGFW B 的 MAC 地址。

邻居发现协议由邻居表实现，邻居表是一组有关邻居信息的表项。邻居表项可以自动生成，也可以由管理员手动添加。邻居表项自动生成的为动态邻居表，由 NGFW 动态学习而生成，可根据通过 NGFW 的数据流量自动更新；邻居表项由管理员手动添加的为静态邻居表，不会随网络的变化而自动更新。

邻居表记录的主机 IP 地址与 MAC 地址对应关系主要用来完成 IPv4 中的地址解析协议（ARP）功能。当 NGFW 发送数据报文时，会查看邻居表，如果目的 IP 地址已经在邻居表中，则根据邻居表中该 IP 地址对应的 MAC 地址封装数据报文；否则，NGFW 需发送组播报文以获取目的主机的 MAC 地址来封装数据报文。

Neighbor 表记录了主机 IPv6 地址和 MAC 地址的映射关系，包括动态 Neighbor 表和静态 Neighbor 表。动态 Neighbor 表由 NGFW 动态学习而生成的；静态 Neighbor 表由管理员手工添加，不会随网络的变化自动更新。

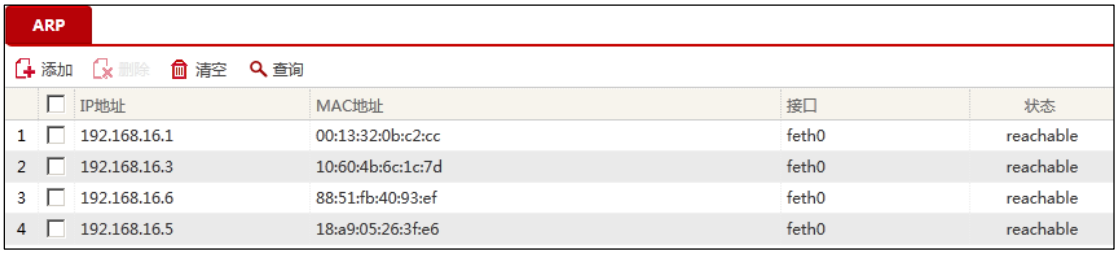
6.6.2 配置 ARP

在配置 ARP 之前，需要先进行如下步骤：

- 配置添加 ARP 表项的接口的工作模式为路由模式，关于接口属性的配置具体请参见 6.2.3 配置接口基本属性。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **邻居** > **ARP**。



步骤 2 点击『添加』，弹出“添加”窗口。

在添加 ARP 表项时，各项参数的具体说明如下表所示。

参数	说明
接口	设置源地址所在区域所对应的路由接口或 VLAN 虚接口名称。
IP 地址	输入 IPv4 地址格式字符串。
MAC 地址	输入 IPv4 地址对应的 MAC 地址。

步骤 3 查询邻居表项。

点击『查询』，在弹出的对话框中，输入需要查询的邻居表项对应的接口、IP 地址或者 MAC 地址后，点击【确定】按钮，可以筛选出相应的邻居表项。

CLI 方式配置

步骤	配置命令	配置说明
1	**network arp add ip** <*string1*> **mac-address** <*string2*> **dev** <*string3*>	添加一条静态 ARP 表项。
2	**etwork arp reachable_time** < *number* >	设置 ARP 可达时间。
3	**network arp del ip** <*string1*> **dev** <*string2*>	删除一条 ARP 表项。
4	**network arp clean** [**dev** <*string*>] [**vr_id** <*number*>]	清除所有的 ARP 表项。

network arp add ip <*string1*> **mac-address** <*string2*> **dev** <*string3*>

命令描述：

添加一条静态 ARP 表项。

可通过 **network arp delete ip** <*string1*> **dev** <*string2*>命令删除一条静态 ARP 表项。

参数说明：

network arp add	添加一个静态 ARP 表项。
ip	必选项，设置 IPv4 地址。
string1	字符串类型，IPv4 地址格式为 A.B.C.D。
mac-address	必选项，设置 MAC 地址。
string2	字符串类型，格式为 AA:BB:CC:DD:EE:FF。
dev	必选项，设置出接口。
string3	字符串类型，表示接口名称，可为物理接口或虚接口。

以下为添加一条静态 ARP 表项的示例：

添加一条主机地址为 192.168.99.100、MAC 地址为 18:a9:05:26:aa:8c、出接口为 feth0 的 ARP 表项。

TopsecOS# **network arp add ip** *192.168.99.100* **mac-address** *18:a9:05:26:aa:8c* **dev** *feth0*

network arp clean [**dev** <*string*>] [**vr_id** <*number*>]

命令描述：

清空静态 ARP 表。

参数说明：

network arp clean	清空静态 ARP 表。
dev	可选项，清空与相应接口相关的所有静态 ARP 表项。
string	字符串类型，表示接口名称。
vr_id	可选项，清空与相应 VR 相关的所有静态 ARP 表项。
number	数值类型，表示 VR 的 ID。

以下为清空静态 ARP 表的示例：

TopsecOS# **network arp clean**

network arp reachable_time < *number* >

命令描述：

设置可达时间。

参数说明：

network arp reachable_time	设置可达时间。
number	数值类型，最小时间为 300 秒，单位是秒。

以下为设置可达时间的示例：

设置可达时间为 350s。

```
TopsecOS# network arp reachable_time 350
```

network arp show [**vr_id** <*number*>]

命令描述：

查看静态 ARP 表详细信息。

参数说明：

network arp show	查看静态 ARP 表的详细信息。
vr_id	可选项，设置查看属于哪个 VR 的静态 ARP 表。
number	数值类型，表示 VR 的 ID 号。

以下为查看 ARP 表的示例：

```
TopsecOS# network arp show
```

6.6.3 配置 Neighbour

WEBUI 方式配置

步骤 1 选择 **网络管理** > **邻居** > **NEIGH**。

步骤 2 添加邻居表项。

1）点击『添加』，弹出“添加”窗口。

在添加邻居表项时，各项参数的具体说明如下表所示。

参数	说明
接口	选择待添加邻居表项的接口。
IPv6 地址	输入接口的 IPv6 地址。
MAC 地址	输入匹配的 MAC 地址。

2）参数设置完成后点击【确定】按钮即可完成邻居表项的添加；点击【取消】按钮撤销该操作。

步骤 3 查询邻居表项。

点击『查询』，输入需要查询的邻居表项对应的接口、IP 地址或者 MAC 地址后，点击【确定】按钮，可以筛选出相应的邻居表项。

CLI 方式配置

步骤	配置命令	配置说明
1	**network neighbour add ip** <*string1*> **mac-address** <*string2*> **dev** <*string3*>	添加一条静态邻居表项。
2	**network neighbour reachable_time** < *number* >	设置邻居可达时间。
3	**network neighbour delete ip** <*string1*> **dev** <*string2*>	删除一条 ARP 表项。
4	**network neighbour clean** [**dev** <*string*>] [**vr_id** <*number*>]	清除所有的 ARP 表项。

network neighbour add ip <*string1*> **mac-address** <*string2*> **dev** <*string3*>

命令描述：

添加一条静态邻居表项。

使用 **network neighbour delete ip** <*string1*> **dev** <*string2*>命令删除一条静态邻居表项。

参数说明：

network neighbour add ip	必选项，设置 IPv6 地址。
string1	字符串类型，IPv6 地址格式为 X:X:X:X:X:X:X:X，其中 X 为一个 4 位十六进制整数。
mac-address	必选项，设置 MAC 地址。
string2	字符串类型，格式为 AA:BB:CC:DD:EE:FF。
dev	必选项，设置出接口。
string3	字符串类型，表示接口名称，可为物理接口或虚接口。

以下为添加静态邻居表的示例：

添加一条主机地址为 fe80::252a:b38d:93c7:91f0、MAC 地址为 18:a9:05:26:3f:e6、出接口为 feth0 的邻居表项。

```
TopsecOS# network neighbour add ip fe80::252a:b38d:93c7:91f0 mac-address
18:a9:05:26:3f:e6 dev feth0
```

network neighbour clean [**dev** <*string*>] [**vr_id** <*number*>]

命令描述：

清空静态邻居表。

参数说明：

network neighbour clean	清空静态邻居表。
dev	可选项，清空与相应接口相关的所有静态邻居表项。
string	字符串类型，输入接口名称。
vr_id	可选项，清空与相应 VR 相关的所有静态邻居表项。
number	数值类型，输入 VR 的 ID。

以下为清空静态邻居表的示例：

TopsecOS# **network neighbour clean**

network neighbour reachable_time <*number*>

命令描述：

设置邻居的可达时间。

参数说明：

network neighbour reachable_time	设置邻居的可达时间。
number	数值类型，单位：秒；取值范围：300-86400。

以下为设置邻居可达时间的示例：

设置邻居可达时间为 350s。

TopsecOS# **network neighbour reachable_time** *350*

network neighbour show [**vr_id** <*number*>] [**dev** <*string1*>] [**type** <static|dynamic>] [**ip** <*string2*>] [**mac-address** <*string3*>]

命令描述：

查看静态邻居表详细信息。

参数说明：

network neighbour show	查看静态邻居表的详细信息。
vr_id	可选项，设置查看属于哪个 VR 的静态邻居表。
number	数值类型，表示 VR 的 ID 号。
dev	可选项，设置接口。
string1	字符串类型。
type	可选项，设置类型。
static|dynamic	静态|动态
ip	可选项，设置 IP 地址。
string2	字符串类型。
mac-address	可选项，设置 MAC 地址。
string3	字符串类型。

以下为查看静态邻居表的示例：

```
TopsecOS# network neighbour show
```

6.7 MAC

6.7.1 简介

当接口工作在交换模式时，根据 MAC 地址表来对报文进行转发。MAC 地址表的表项包含 MAC 地址、VLAN、转发的物理接口号。设备在转发报文时，将首先查询 MAC 地址表项中是否包含与目的 MAC 地址匹配的表项。如果有匹配的表项，则将报文通过相应的端口进行转发。如果没有相应的匹配项，则采取广播方式向除接收端口外的所有接口转发该数据帧。

当 NGFW 进行报文转发时，根据 MAC 地址表中是否包含报文的目的地址，可进行如下处理。

- 如果 MAC 地址表中存在目的 MAC 地址表项，则按照 MAC 地址表进行单播转发。

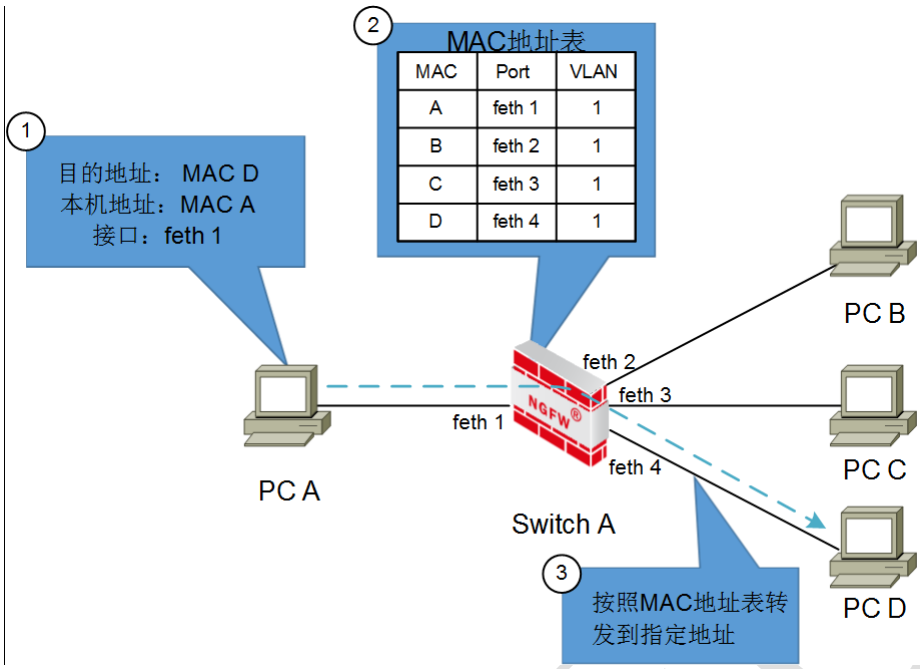


图 6-9 MAC 地址单播示意图

- 如果 MAC 地址表中不存在目的 MAC 地址表项，或者报文的目的地址为广播地址，则在该广播域中进行广播转发。如果在广播域中存在目的 MAC 地址，目的设备响应广播包，NGFW 将目的地址加入到 MAC 地址表中；如果广播域中没有设备响应，则再有报文的目的地址为该 MAC 地址时，依然进行广播。

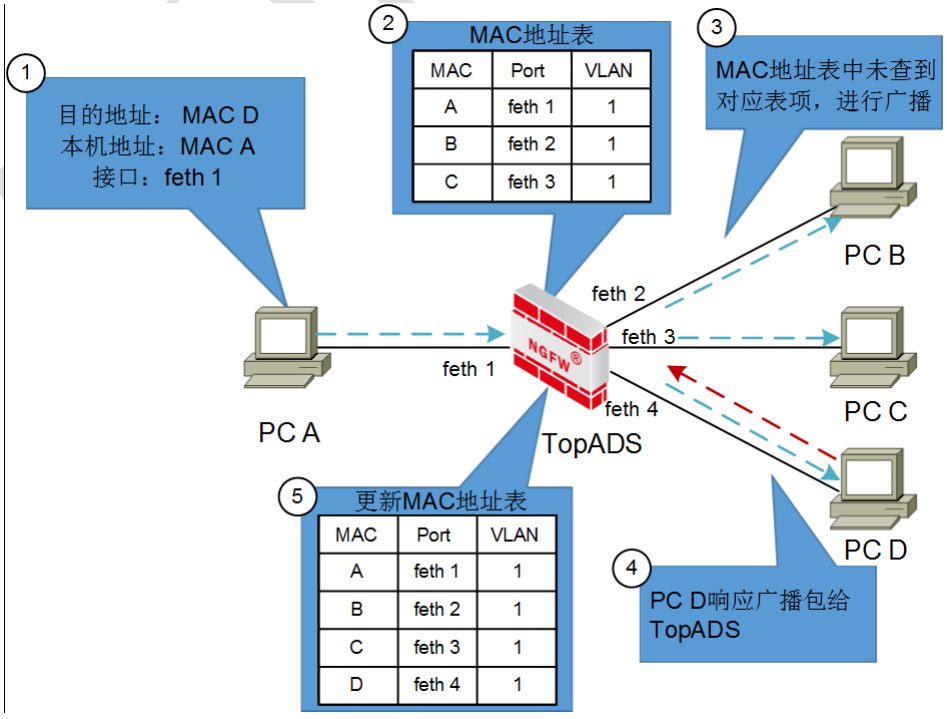


图 6-10 MAC 地址广播示意图

MAC 地址表中的表项包括静态表项和动态表项两种：

- 静态表项

静态表项由管理员配置，不会随着时间而老化。

- 动态表项

动态 MAC 表项由设备自动生成并更新，无需管理员配置。交换接口接收到数据帧时，分析收到数据帧中的源 MAC 地址，如果 MAC 地址表中包含该 MAC 地址对应的表项则更新表项；如果 MAC 地址表中没有该表项，则建立该地址同端口的映射，并将其写入 MAC 地址表中，生成新的动态 MAC 表项。

NGFW 支持添加和删除静态表项，查看动态表项。

6.7.2 配置 MAC 地址

在配置 MAC 地址之前，需要先进行如下步骤：

- 配置接口的工作模式为交换模式和允许通过的 VLAN，关于接口属性的配置具体请参见 6.2 接口。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **MAC**。

步骤 2 添加静态项。

1）点击『添加』，弹出“添加”对话框。

在添加静态项时，各项参数的具体说明如下表所示。

参数	说明
VLAN	选择通过哪个 VLAN 虚拟接口进行转发。 说明： 当“选择端口”处设定的交换接口工作在“access”模式时，必须选择其所属的 VLAN 的 ID 号；当“选择端口”处设定的交换接口工作在“Trunk”模式时，可以选择 VLAN 范围中的一个 ID 号。
接口	选择转发的物理接口。只能选择工作在交换模式的物理接口名。
物理地址	输入匹配的 MAC 地址。

2）设置完成后，点击【确定】按钮完成静态 MAC 的添加，点击【取消】按钮撤销该操作。

步骤 3 查询 MAC 地址。

在界面中输入 VLAN ID 和 MAC 地址，点击『查询』，界面将显示符合查询条件的结果。

CLI 方式配置

步骤	配置命令	配置说明
1	**network mac add** <static> **address** <*macaddress*> **vlan** <*number*> **interface** <*string*>	添加一条静态 MAC 表项。
2	**network mac delete** <static> **address** <*macaddress*> **vlan** <*number*> **interface** <*string*>	删除一条 MAC 表项。
3	**network mac clean** <static|dynamic>	清除所有的 MAC 表项。

network mac add <static> **address** <*macaddress*> **vlan** <*number*> **interface** <*string*>

命令描述：

添加一条静态 MAC 表项。

使用 **network mac delete** <static> **address** <*macaddress*> **vlan** <*number*> **interface** <*string*>命令删除一条静态 MAC 表项。

参数说明：

network mac add static	添加一条静态 MAC 表项。
address	必选项，设置 MAC 表项的 MAC 地址。
macaddress	MAC 地址字符串，格式为 AA:BB:CC:DD:EE:FF。
vlan	必选项，设置 MAC 表项的 VLAN。
number	数值类型，表示 VLAN 号。
interface	必选项，设置 MAC 表项的接口。
string	字符串类型，表示接口名称，如 feth3。

以下为添加静态 MAC 表项的示例：

添加一条 MAC 地址为 a9:0f:ac:dd:56:f9、VLAN 为 10、出接口为 feth3 的 MAC 表项。

```
TopsecOS# network interface feth3 switchport
TopsecOS# network vlan add id 10
TopsecOS# network interface feth3 switchport access-vlan 10
```

```
TopsecOS# network mac add static address a9:0f:ac:dd:56:f9 vlan 10 interface
feth3
```

network mac clean <static|dynamic>

命令描述：

清空 MAC 表。

参数说明：

network mac clean	清空 MAC 表。
static|dynamic	清空静态 MAC 表项|清空动态 MAC 表项

以下为清空静态 MAC 表项的示例：

```
TopsecOS# network mac clean static
```

network mac show [**address** <*macaddress*>] [**type** <static|dynamic>] [**vcom** <*number1*>] [**vlan** <*number2*>] [**interface** <*string*>]

命令描述：

查看 MAC 表。

参数说明：

network mac show	查看 MAC 表。
address	可选项，指定只查看相应 MAC 地址的 MAC 表项。
macaddress	MAC 地址字符串，格式为 AA:BB:CC:DD:EE:FF。
type	可选项，指定查看 MAC 表项的类别，默认全部显示。
static|dynamic	静态 MAC 表|动态 MAC 表
vcom	可选项，指定查看 MAC 表项所属的 VR。
number1	数值类型，取值范围 0-255。
vlan	可选项，指定只查看相应 VLAN 的 MAC 表项。
number2	数值类型，表示 VLAN 号。
interface	可选项，指定只查看相应接口的 MAC 表项。
string	字符串类型，表示接口名称，如 feth3。

以下为查看动态 MAC 表项的示例：

```
TopsecOS# network mac show type dynamic
Total:10240     Static:2     Link:4
vcom          mac             vlan       dev                flags
```

```
--------------------------------------------------------------------------------
0       4e:b2:bc:3b:a7:bc   1       feth1           dynamic
0       1e:a6:6e:19:2a:c1   1       feth0           dynamic
2 matched mac entries.
```

6.8 DHCP

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议），目的是为网络中的主机自动进行 IP 地址分配及其他网络相关设置。通过 DHCP，网络主机登录网络时可自动获取 IP 地址、网关、DNS 等相关网络配置，避免了繁琐的手工配置，可自动适应网络的变化，极大简化网络管理员的工作。

针对网络中主机自动获取 IP 地址的需求，NGFW 提供比较全面的 DHCP 服务功能，能够很好地结合到客户网络环境中，在网络中可作为 DHCP 客户端、DHCP 服务器和 DHCP 中继。

- DHCP 服务器：负责集中管理和维护 IP 配置信息，处理客户机的 DHCP 请求并提供 IP 地址的动态分配和租期管理，并且可为相应主机绑定固定的 IP 地址，同时还可以向客户机提供其他的 IP 配置信息，如网关、DNS、WINS 等网络配置参数。
- DHCP 客户端：IP 地址需通过 DHCP 服务器自动分配。NGFW 登录网络时，自动发送 DHCP 请求报文获取 IP 地址，使用分配的 IP 及其他信息接入网络。
- DHCP 中继：客户端向服务器发送的 DHCP 请求报文和确认报文均为广播包，DHCP 服务器与客户端部署于不同广播域时，则需要客户端的网关支持 DHCP 报文的转发（DHCP 中继）。通过 DHCP 中继，将 DHCP 广播报文转换为单播报文发送给 DHCP 服务器，达到客户端获取服务器分配 IP 地址的目的。

注意

✧ 如果需要使用 NGFW 的 DHCP 中继功能，需要开放运行 DHCP 服务所在接口所属区域的 DHCP 服务，关于 DHCP 服务的开放具体请参见 7.5 本机服务。使用 NGFW 的 DHCP 服务器和客户端功能是，无需开启 DHCP 服务。

NGFW 通过 8 种报文类型实现 DHCP 各种服务，如获取 IP 地址、释放 IP 地址、续租 IP 地址等服务，具体说明如下：

DHCP Discover	Client 向 Server 发送获取 IP 地址的第一个请求报文，用于发现 DHCP 服务器。
DHCP Offer	Server 对 DHCP Discover 报文的响应，表明其可以提供地址自动分配服务。
DHCP Request	Client 对 DHCP Offer 报文的响应，通知所有可提供服务的 DHCP 服务器，其接收哪台 DHCP 服务器提供 IP 地址分配服务。
DHCP Decline	当 Client 发现 Server 分配给它的 IP 地址无法使用，如 IP 地址发生冲突时，将发出此报文让 Server 禁止使用这次分配的 IP 地址。
DHCP Ack	Server 对 DHCP request 报文的响应，Client 收到此报文后才真正获得了 IP 地址和相关配置信息。
DHCP Nack	此报文是 Server 对 Client 的 DHCP Request 报文的拒绝响应，Client 收到此报文后，会重新开始发送 DHCP Discover 包请求获取 IP 地址过程。
DHCP Release	此报文用于 Client 主动释放 IP 地址，当 Server 收到此报文后收回为客户端分配的该 IP 地址。
DHCP Inform	Client 已经获取 ip，Client 发送此报文用于获取其他网络配置信息，如 DNS、网关等配置信息。

DHCP 客户端首次获取 IP 地址报文交换过程

➢ DHCP 客户端与 DHCP 服务器处于同一广播域，DHCP 报文交互过程。

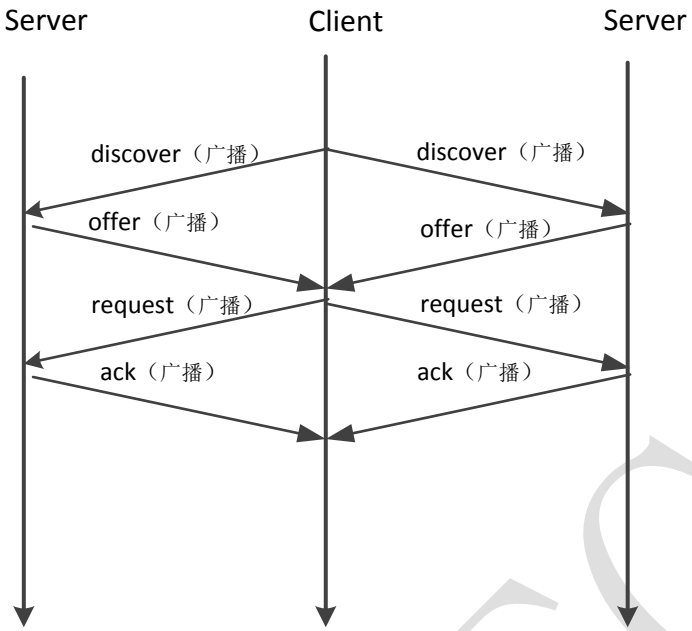


图 6-11 DHCP 报文交换过程图

- Client 发现 Server 阶段

DHCP 客户端第一次登录网络的时，向网络发出一个 DHCP Discover 广播包。

- Server 表明其可用性阶段

DHCP 服务器接收到客户端发出的 DHCP Discover 广播包后，从地址池中选择最前面的空置 IP 地址，封装于 DHCP Offer 广播包中向网络发送。根据服务器端的设定，DHCP Offer 封包会包含租约期限的信息。

- Client 选择由哪个 Server 提供服务阶段

DHCP 客户端收到广播域内多个 DHCP 服务器的响应时，只挑选其中一个 DHCP Offer 而已（通常是最先抵达的那个），然后向网络发送一个 DHCP Request 广播包，告诉广播域内所有 DHCP 服务器它将接受哪一台服务器提供的 IP 地址。

同时，DHCP 客户端发送一个免费 ARP 封包，查询网络上面有没有其它机器使用该 IP 地址，如果发现该 IP 已经被占用，客户端则会送出一个 DHCP Decline 封包给 DHCP 服务器，拒绝接受其 DHCP Offer，并重新发送 DHCP Discover 信息。

- 确认服务阶段

1）DHCP 服务器接收到客户端的 DHCP Request 之后，会向客户端发出一个 DHCP Ack 响应，以确认 IP 租约的正式生效。

2）DHCP 客户端接收到 DHCP Ack 报文后，获取的 IP 地址可用，结束一个完整的 DHCP 工作过程。

➢ DHCP 客户端与 DHCP 服务器处于不同广播域，DHCP 报文交互过程。

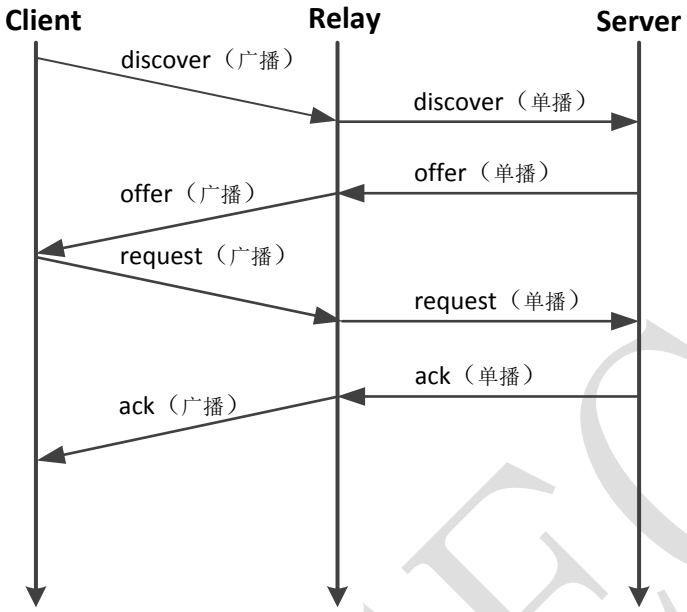


图 6-12 DHCP 报文交换过程图

■ Client 发现 Server 阶段

1）DHCP 客户端第一次登录网络的时，向网络发出一个 DHCP Discover 广播包。

2）DHCP 中继接收到客户端发出的 DHCP Discover 广播包后，将广播包的源地址修改为自身的 IP 地址，目的地址修改为 DHCP 服务器的 IP 地址，发送给 DHCP 服务器。

■ Server 表明其可用性阶段

1）DHCP 服务器接收到中继发送的 DHCP Discover 单播报文后，从地址池中选择最前面的空置 IP 地址，封装于 DHCP Offer 单播包中发送给 DHCP 中继。根据服务器端的设定，DHCP Offer 封包会包含租约期限的信息。

2）DHCP 中继接收到服务器发送的 DHCP Offer 单播包后，将源地址修改为自身的 IP 地址，目的地址修改为 255.255.255.255，向其网络广播。

■ Client 选择由哪个 Server 提供服务阶段

1）DHCP 客户端收到中继广播的不同 DHCP 服务器响应包时，只挑选其中一个 DHCP Offer 而已（通常是最先抵达的那个），然后向网络发送一个 DHCP Request 广播封包，申明它将接受哪一台服务器提供的 IP 地址。

同时，客户端发送一个免费 ARP 封包，查询网络上面有没有其它机器使用该 IP 地址，如果发现该 IP 已经被占用，客户端则会送出一个 DHCP Decline 封包给 DHCP 中继，拒绝接受其转发的相应 DHCP Offer，并重新发送 DHCP Discover 信息；DHCP 中继则将该 DHCP Decline 封包转发给 DHCP 服务器）。

2）DHCP 中继接收到该 DHCP Request 广播封包后，将报文的源地址修改为自身的 IP 地址，目的地址修改为 DHCP 服务器的 IP 地址，转发给 DHCP 服务器。

- 确认服务阶段

1）DHCP 服务器接收到中继转发的 DHCP Request 之后，会向中继发送一个 DHCP Ack 响应。

2）DHCP 中继接收到该 DHCP 服务器的 DHCP Ack 响应包后，将源 IP 地址修改为自身的 IP 地址，目的地址修改为 255.255.255.255，向其网络广播。

3）DHCP 客户端接收到中继转发的 DHCP Ack 响应包后，确认 IP 租约的正式生效，结束一个完整的 DHCP 工作过程。

说明

- ✧ 如果客户端租约 IP 地址过期，重新申请 IP 地址时，DHCP 服务器会尽量让客户端使用原来的 IP 地址，如果该 IP 地址空闲，服务器直接响应 DHCP Ack 确认；如果该地址已经失效或已经被其它机器使用了，服务器则会响应一个 DHCP Nack 封包给客户端，要求客户端重新发送 DHCP Discover 申请 IP 地址。

6.8.1 DHCP 服务器

NGFW 作为 DHCP 服务器时，可为运行 DHCP 客户端服务的主机分配网络配置参数，如 IP 地址、默认网关、DNS 及 WINS 服务器等。NGFW 可以指定某个物理接口、VLAN 虚接口和聚合端口运行 DHCP 服务器，为该接口所在子网的主机动态分配 IP 地址，此时该接口必须工作在路由模式下。

此外，管理员可以在租约期内保留一个特定的 IP 地址供某台 DHCP 客户端主机（由 MAC 地址来标识）使用。

NGFW 作为 DHCP 服务器时，其部署于网络中的拓扑结构如下图所示。

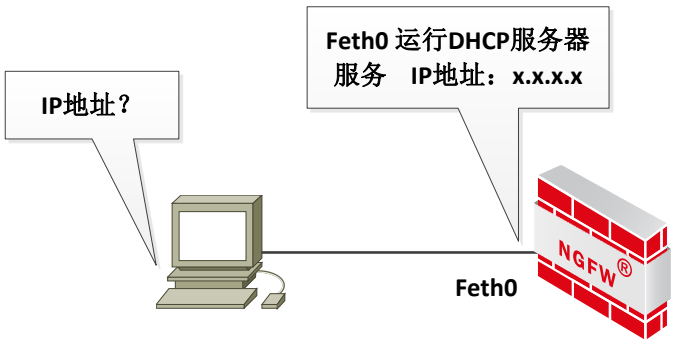


图 6-13 NGFW 运行 DHCP 服务器服务示意图

下面介绍如何启用 NGFW 的 DHCP 服务器功能。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **DHCP**。

步骤 2 添加地址池。

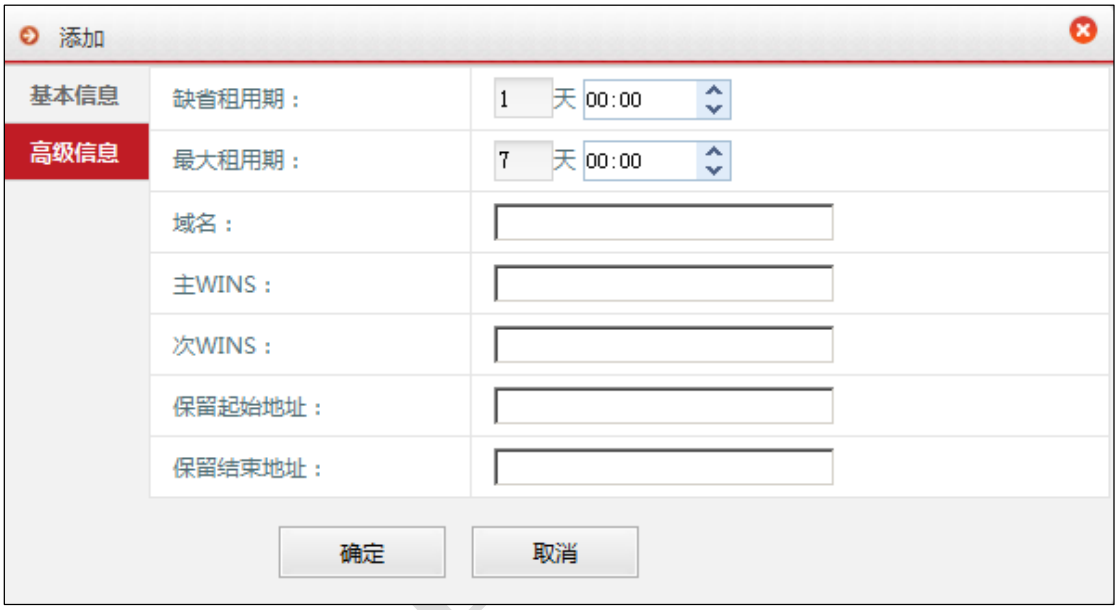
1）点击【地址池】按钮，然后在地址池区域点击『添加』，如下图所示。

在添加 DHCP 地址池基本信息时，各项参数的具体说明如下表所示。

参数	说明
子网/掩码	必选项，设置为哪个子网创建 DHCP 作用域。
分配起始地址/分配结束地址	必选项，输入 DHCP 服务器可以为客户端分配地址的范围。应当与“子网”设定的 IP 在同一个网段，并且不能包含已经分配的 IP 地址。

参数	说明
网关地址	如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定其网关地址。
主 DNS/次 DNS	如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定主/次 DNS 服务器地址。
虚拟路由 ID	设置该 DHCP 地址池所属虚拟路由域。

激活“高级信息”页签，如下图所示。



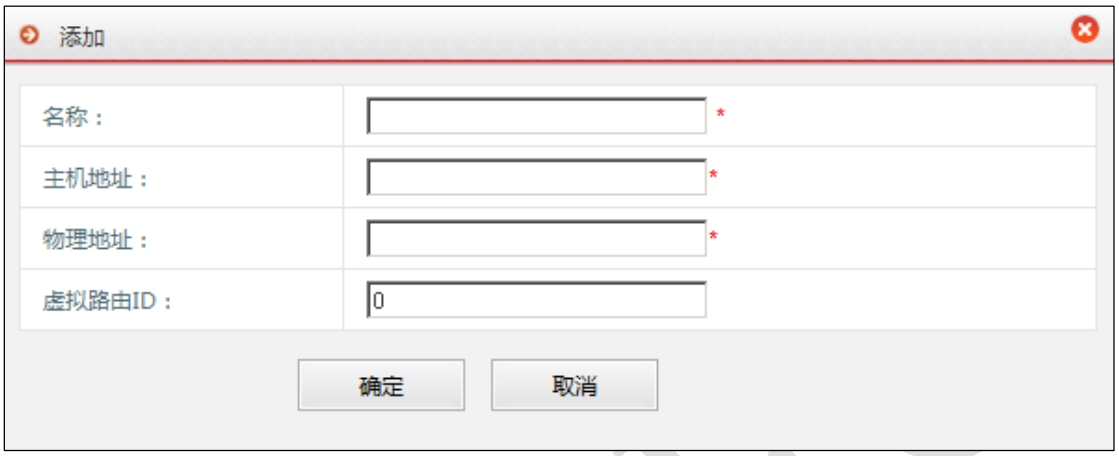
在添加 DHCP 地址池高级信息时，各项参数的具体说明如下表所示。

参数	说明
缺省租用期	DHCP 服务器向 DHCP 客户端租借地址的期限。到期后如果客户端要继续使用该地址则必须续订。默认值：1 天。 说明： 缺省租用期一定不能高于最大租用期。
最大租用期	服务器端为客户保留地址的最长期限。这个宽限期在出现以下情况时保护客户端租约：客户端和服务器处于不同的时区、个别计算机的时钟没有同步、在租约过期时客户端从网络上断开。默认值：7 天。 说明： 缺省租用期一定不能高于最大租用期。
域名	为网络上的客户计算机用来进行 DNS 名称解析时使用的父域。
主 WINS/次 WINS	如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IP 地址的同时按照该设置设定主/次 WINS 服务器地址。
保留起始/结束地址	“分配起始地址/分配结束地址”中预留的地址。DHCP 服务器不会分配给 DHCP 客户端预留 IP 地址。

2）点击【确定】按钮完成 DHCP 地址池的创建。

步骤 3 （可选）设置地址绑定。

1）点击【地址绑定】按钮，然后在地址绑定区域点击『添加』，如下图所示。



在添加 DHCP 地址绑定规则时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，添加该地址绑定规则的名称。
主机地址	必选项，设置需要绑定的 IP 地址，绑定的 IP 地址必须为地址池中可分配地址范围内。
物理地址	必选项，设置主机的 MAC 地址，16 进制字母大小写输入均可。
虚拟路由 ID	添加该地址绑定规则到哪个虚拟路由域。

2）设置完成后，点击【确定】按钮完成地址绑定规则的添加。

步骤 4 设置运行 DHCP 服务器的接口。

在页面左上方“接口配置”处将提供 DHCP 服务的物理接口、VLAN 虚接口名以及聚合端口添加到“已选择接口”中。

步骤 5 启动 DHCP 服务器进程。

点击【开始】按钮即可在该接口启动 DHCP 服务。

说明

- ✧ 配置 NGFW 作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。

步骤 6 查看 DHCP 地址分配情况。

点击【已分配地址】按钮，即可查看 NGFW 作为 DHCP 服务器为客户端**动态分配**的 IP 地址情况。

CLI 方式配置

network dhcp server add_host name <*string*> **macaddr** <*macaddress*> **ipaddr** <*ipaddress*> [**vcom** <*number*>]

命令描述：

添加地址绑定规则，用于 DHCP 服务器为指定 MAC 地址对应的主机分配指定的 IPv4 地址。

参数说明：

network dhcp server add _host	DHCP 服务器给指定 MAC 分配绑定的 IPv4 地址。
name	必选项，设定地址绑定规则名称。
string	字符串类型，可为 1~31 个英文、数字、“-”、“_”等字符的组合。
macaddr	必选项，指定 MAC 地址。
macaddress	MAC 地址字符串，格式为 AA:BB:CC:DD:EE:FF。
ipaddr	必选项，指定要绑定的 IPv4 地址。
ipaddress	IPv4 地址字符串，格式为 A.B.C.D。
vcom	设置地址绑定规则所属虚拟路由域。
number	数值类型。

使用说明：

如果管理员把某主机的 MAC 地址与某 IPv4 地址绑定，则 DHCP 服务器将分配给此主机固定的 IPv4。

以下为给指定 MAC 对应的主机分配指定 IPv4 地址的示例：

给 MAC 地址为 00:50:04:c3:b0:31 的主机分配 IPv4 地址 10.10.10.25。

```
TopsecOS# network dhcp server add_host name binding1 macaddr
00:50:04:c3:b0:31 ipaddr 10.10.10.25
```

network dhcp server del_host name <*string*> [**vcom** <*number*>]

命令描述：

删除地址绑定对象。

参数说明：

network dhcp server del_host	删除地址绑定对象。
name	必选项，地址绑定对象名称。
string	字符串类型，表示已经设定的地址绑定对象名。
vcom	设置地址绑定规则所属虚拟路由域。
number	数值类型。

以下为删除地址绑定策略的示例：

删除地址绑定对象 bind1。

```
TopsecOS# network dhcp server del_host name binding1
```

network dhcp server add_subnet subnet <*ipaddress1*> **submask** <*ipaddress2*> **sub_start** <*ipaddress3*> **sub_end** <*ipaddress4*> [**gateway** <*ipaddress5*>] [**domain** <*string1*>] [**pri_dns** <*ipaddress6*>] [**sec_dns** <*ipaddress7*>] **pri_wins** <*ipaddress8*>] [**sec_wins** <*ipaddress9*>] [**def-lease-day** <*number1*>] [**def-lease-hour** <*number2*>] [**def-lease-min** <*number3*>] [**max-lease-day** <*number4*>] [**max-lease-hour** <*number5*>] [**max-lease-min** <*number6*>] [**reserve_start** <*ipaddress10*>] [**reserve_end** <*ipaddress11*>] [**vcom** <*number7*>]

命令描述：

添加一个 DHCP 服务器地址池，即可用来分配动态 IPv4 的地址范围。

参数说明：

network dhcp server add_subnet	添加一个 DHCP 服务器地址池。
subnet	必选项，设置为哪个子网创建 DHCP 作用域。
ipaddress1	IPv4 地址字符串，格式为 A.B.C.D。
submask	必选项，设置子网掩码。
ipaddress2	子网掩码字符串。
sub_start	必选项，设置地址池起始地址。
ipaddress3	IPv4 地址字符串。应小于 **sub_end** 设定的地址。
sub_end	必选项，设置地址池结束地址。
ipaddress4	IPv4 地址字符串。应大于 **sub_start** 设定的地址。
gateway	可选项，设置网关地址，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IPv4 地址的同时按照该设置设定其网关地址。默认为空。
ipaddress5	IPv4 地址字符串，格式为 A.B.C.D。

domain	可选项，为网络上的客户计算机用来进行 DNS 名称解析时使用的父域。
string1	字符串类型。
pri_dns	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IPv4 地址的同时按照该设置设定主 DNS 服务器地址。默认为空。
ipaddress6	IPv4 地址字符串，格式为 A.B.C.D。
sec_dns	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IPv4 地址的同时按照该设置设定次 DNS 服务器地址。默认为空。
ipaddress7	IPv4 地址字符串。
pri_wins	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IPv4 地址的同时按照该设置设定主 WINS 服务器地址。默认为空。
ipaddress8	IPv4 地址字符串，格式为 A.B.C.D。
sec_wins	可选项，如果 DHCP 服务器设定了网关地址，则客户端主机在获取 IPv4 地址的同时按照该设置设定次 WINS 服务器地址。默认为空。
ipaddress9	IPv4 地址字符串。
def-lease-day	可选项，设置缺省租用期的天数。最大值为 7 天，如果该项设置为 7，则不能设置缺省租用小时数及分钟数。
number1	数值类型，单位：天；取值范围：0-7；默认值：1。
def-lease-hour	可选项，设置缺省租用期的小时数。默认为 0 小时。
number2	数值类型，单位：小时；取值范围：0-23；默认值：0。
def-lease-min	可选项，设置缺省租用期的分钟数。
number3	数值类型，单位：分钟；取值范围：0-59；默认值：0。
max-lease-day	可选项，设置最大租用期的天数。
number4	数值类型，单位：天；取值范围：0-3650；默认值：7。
max-lease-hour	可选项，设置最大租用期的小时数。
number5	数值类型，单位：小时；取值范围：0-23；默认值：0。
max-lease-min	可选项，设置最大租用期的分钟数。
number6	数值类型，单位：分钟；取值范围：0-59；默认值：0。
reserve_start	可选项，设置预留起始地址。
ipaddress10	IP 地址字符串。
reserve_end	可选项，设置预留起始地址。
ipaddress11	IP 地址字符串。
vcom	可选项，设置地址池所属虚拟路由域。
number7	数值类型。

使用说明：

1）配置 NGFW 作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。

2）缺省租用期表示 DHCP 服务器向 DHCP 客户端租借地址的期限。到期后如果客户端要继续使用该地址则必须续订。默认为 1 天。

以下为添加 DHCP 地址池的示例：

添加 10.1.1.0/24 地址池，地址分配范围为 10.1.1.22-10.1.1.45。

```
TopsecOS# network dhcp server add_subnet subnet 10.1.1.0 submask
255.255.255.0 sub_start 10.1.1.22 sub_end 10.1.1.45
```

network dhcp server del_subnet subnet <*ipaddress*> [**vcom** <*number*>]

命令描述：

删除地址池。

参数说明：

network dhcp server del_subnet	删除地址池。
subnet	必选项，地址池所在子网。
ipaddress	IPv4 地址字符串，格式为 A.B.C.D，输入已经设定的地址池所在子网 IPv4。
vcom	可选项，设置地址池所属虚拟路由域。
number	数值类型。

以下为删除 DHCP 地址池的示例：

删除 10.1.1.0/24 地址池。

```
TopsecOS# network dhcp server del_subnet subnet 10.1.1.0.
```

network dhcp server start on <*string*>

命令描述：

在 NGFW 某接口启动 DHCP 服务器。启动 DHCP 服务器服务后，管理员不能配置 DHCP 服务器的地址绑定规则和地址池。

参数说明：

network dhcp server start	在 NGFW 某接口启动 DHCP 服务器。
on	必选项，指定接口名。
string	字符串类型，表示物理接口或虚接口。

使用说明：

配置 NGFW 作为 DHCP 服务器，需要首先配置地址池，才能在相应接口运行 DHCP 服务器。

以下为启动 DHCP 服务器的示例：

在 NGFW 的 feth0 口启动 DHCP 服务器。

```
TopsecOS# network dhcp server start on feth0
```

network dhcp server stop <cr>

命令描述：

在 NGFW 上停止 DHCP 服务器。只有在停止 DHCP 服务器服务后，管理员才可以配置 DHCP 服务器的地址绑定规则和地址池。

以下为停止 DHCP 服务器的示例：

```
TopsecOS# network dhcp server stop
```

6.8.2 DHCP 客户端

NGFW 多个路由接口可同时运行 DHCP Client 服务，从 DHCP 服务器端自动获取 IP 地址。对于工作在路由模式下的物理接口和聚合端口，可直接在该接口上运行 DHCP Client 服务；对于工作在交换模式下的物理接口，可在该交换接口所属 VLAN 上运行 DHCP 客户端服务。NGFW 的接口运行 DHCP Client 服务的典型应用有如下两种情况：

- NGFW 接口与 DHCP 服务器通过二层网络相连

例如：NGFW 的接口 feth1 工作在路由模式且启动了 DHCP Client 服务，feth2 口工作在交换模式且属于 Vlan2，Vlan2 上也启动了 DHCP Client 服务。因 NGFW 的 feth1 和 Vlan2 不能获取同一子网的 IP 地址，为使 feth1 和 Vlan2 口均能正确获取 IP 地址，故 feth1 和 Vlan2 需连接不同的 DHCP 服务器，如下图所示。

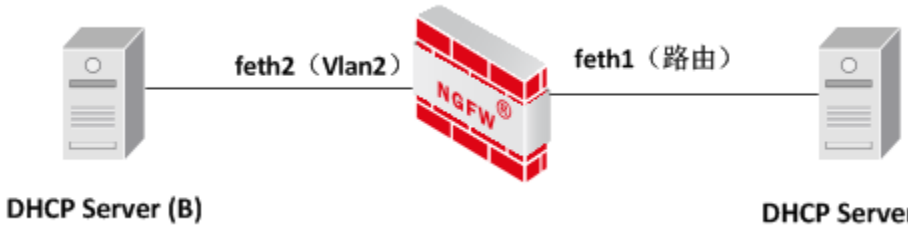


图 6-14 NGFW 接口运行 DHCP Client 服务示意图

注意

- ✧ NGFW 接口启动 DHCP Client 服务时，接口连接的 DHCP 服务器不能与别的物理接口或 VLAN 虚接口处于同一个网段，否则即使 DHCP Client 服务运行成功，也不能正确获取 IP 地址。

- ➢ NGFW 接口与 DHCP 服务器跨三层网络

例如：NGFW 的接口 feth2 工作在路由模式且启动了 DHCP Client 服务，feth1 通过路由设备与 DHCP 服务器相连。为使接口 feth2 自动获取 IP 地址，可在接口 feth1 上运行 DHCP Delay 服务，将接口 feth2 获取 IP 地址的广播报文转化为单播报文发送给 DHCP 服务器，从而使接口 feth2 获取 IP 地址，如下图所示。

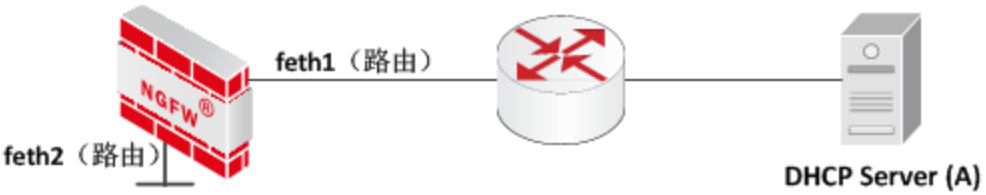


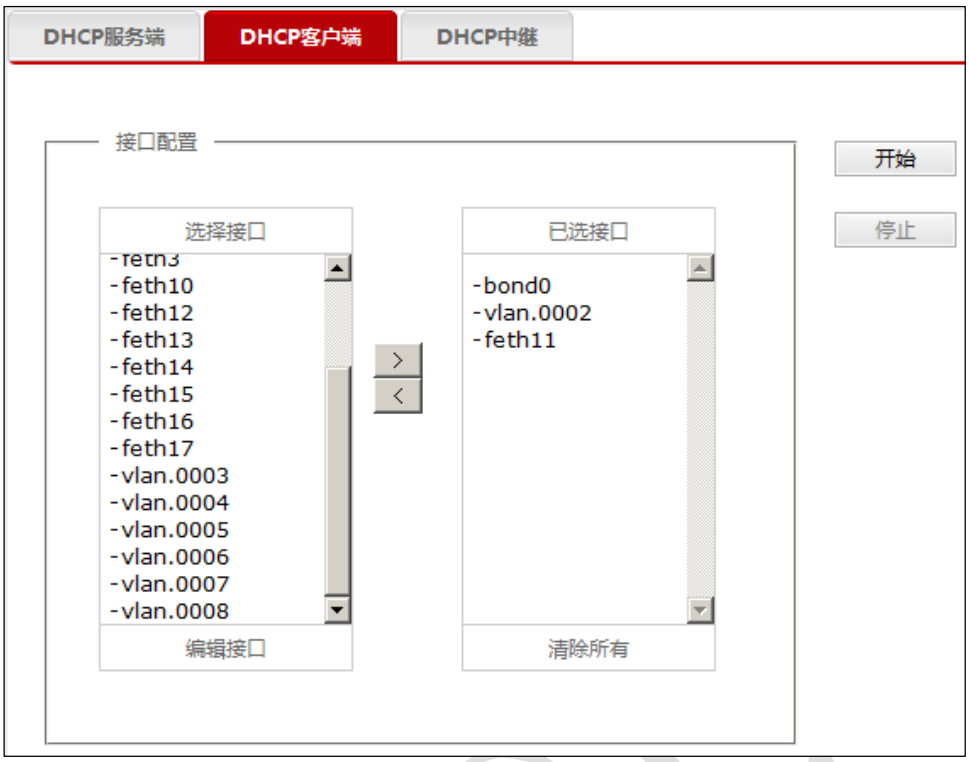
图 6-15 NGFW 接口运行 DHCP Client 服务示意图

下面介绍如何启动 NGFW 的 DHCP Client 服务。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **DHCP**，激活“DHCP 客户端”页签。

步骤 2 设置需自动获取 IP 地址的接口，可以是工作在路由模式下的物理接口、聚合端口，以及 Vlan 虚接口。DHCP 客户端服务可以同时运行在多个接口上，如下图所示。



步骤 3 点击【开始】按钮后，相应接口将从 DHCP 服务器自动获取 IP 地址，点击【停止】按钮后，接口将停止获取 IP 配地址，如果已获取 IP 地址，则释放 IP 地址。

CLI 方式配置

network dhcp client start on <*string*>

命令描述：

在 NGFW 接口启动 DHCP 客户端服务。

参数说明：

network dhcp client start	启动 DHCP 客户端服务。
on	必选项，指定接口名。
string	字符串类型，表示启动 DHCP 客户端服务的接口，可以是物理接口或虚接口。如 feth0、vlan.0001，多个接口间需要使用逗号“,”进行分隔。

使用说明：

1）如果 NGFW 的接口为交换模式，必须在相应虚接口启动 DHCP 客户端服务，否则会提示错误；

2）NGFW 可以对多个接口同时启用 DHCP CLIENT 的服务。

以下为启动 DHCP 客户端服务的示例：

将 NGFW 的接口 feth0 作为 DHCP 客户端。

```
TopsecOS# network dhcp client start on feth0
```

同时在接口 feth0 和 VLAN 虚接口 vlan.0001 上启动 DHCP 客户端服务。

```
TopsecOS# network dhcp client start on feth0,vlan.0001
```

network dhcp client stop <cr>

命令描述：

停止 NGFW 所有接口上启用的 DHCP 客户端服务。

以下为停止 NGFW 所有接口上 DHCP 客户端服务的示例：

```
TopsecOS# network dhcp client stop
```

6.8.3 DHCP 中继

DHCP 客户端和 DHCP 服务器不在同一个子网内（广播域）时，DHCP 客户端与其他子网连接点必须部署 DHCP 中继，接收客户端接收 DHCP 广播请求报文，并将该广播报文转换为单播报文转发给指定 DHCP 服务器，当收到 DHCP 服务器的响应报文，再将该响应报文转发给发起请求的 DHCP 客户端主机。

NGFW 作为 DHCP 中继时，其部署于网络中的拓扑结构如下图所示。

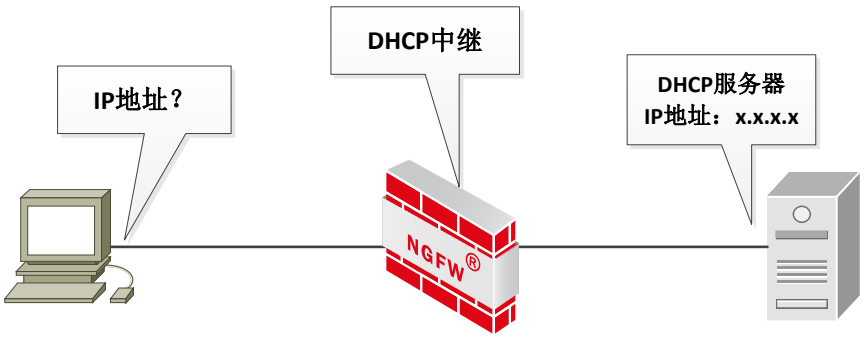


图 6-16 NGFW 运行 DHCP 中继服务示意图

NGFW 作为 DHCP 中继，可帮助客户机从其他网段的 DHCP 服务器获取 IP 地址及其他配置参数，如默认网关、DNS 等等。下面介绍如何启用 NGFW 的 DHCP 中继功能。

WEBUI 方式配置

在启用 NGFW 的 DHCP 中继功能之前，需要先进行如下步骤：

- 在相应的接口开放 DHCP 服务，关于相应接口 DHCP 服务的开放具体请参见 7.5 本机服务。

步骤 1 选择 **网络管理** > **DHCP**，激活“DHCP 中继”页签。

步骤 2 在“接口配置”处选择与 DHCP 客户端相连的 NGFW 接口，同时还要选择与 DHCP Server 相连的 NGFW 接口。

步骤 3 设置 DHCP 服务器地址，如下图所示。

说明

- ✧ 防火墙启用 DHCP 中继功能时，只支持为一个 DHCP 服务器转发 DHCP 请求包和响应包，因此，必须配置两个接口运行 DHCP 中继服务，一个为连接 DHCP 客户端的接口，另一个为连接 DHCP 服务器的接口。
- ✧ 如果 DHCP 服务器的默认网关不是 NGFW 的接口（虚接口）地址，必须在该服务器上添加一条静态路由，目的地址为 DHCP 服务器作用域的网段，网关地址为 NGFW 与 DHCP 服务器连接的接口地址，否则客户机无法正确获取 IP。

步骤 4 点击【开始】按钮，启动中继服务。

CLI 方式配置

network dhcp relay start on <*string*> **dhcp_server** <*ipaddress*>

命令描述：

在 NGFW 接口启动 DHCP 中继服务。

参数说明：

network dhcp relay start	启动 DHCP 中继服务。
on	必选项，指定接口名。
string	字符串类型，需为 NGFW 通往 DHCP 客户端和 NGFW 通往 DHCP 服务器的两个接口，接口可以是物理接口或逻辑接口，如 feth0、vlan.0001。 说明： 接口间需要使用逗号“,”进行分隔，格式如：feth0,feth1。
dhcp_server	必选项，指定网络上的 DHCP 服务器地址。
ipaddress	指定服务器的 IPv4 地址值。

使用说明：

1）如果 NGFW 的接口为交换模式，必须在相应虚接口启动 DHCP 中继服务，否则会提示错误。

2）中继服务需要同时开放服务器和客户机所属区域的 DHCP 服务。

3）中继服务需要同时选中与服务器和客户机物理连接的接口（或虚接口）。

4）如果 DHCP 服务器的默认网关不是 NGFW 的接口（虚接口）地址，必须在该服务器上添加一条静态路由（目的地址为 DHCP 作用域的网段、网关为 NGFW 与服务器端连接的接口），否则客户机无法正确获取 IPv4 地址。

以下为启动 DHCP 中继的示例：

已知 DHCP 服务器的 IP 地址为 192.168.92.234，DHCP 客户端与服务器处于不同网段，NGFW 通往 DHCP 客户端和服务器的接口分别为 feth0 和 feth1。将 NGFW 设置为 DHCP 客户端和服务器的命令如下。

TopsecOS# **network dhcp relay start on** *feth0,feth1* **dhcp_server** *192.168.92.234*

dhcp relay stop <cr>

命令描述：

停止 DHCP 中继服务。

以下为停止 DHCP 中继服务的示例：

TopsecOS# **network dhcp relay stop**

6.9 IPSec VPN

VPN（Virtual Private Network，虚拟私有网）是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建虚拟专用网络，“虚拟”指这种网络是一种逻辑上的网络。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。

NGFW 支持标准的 IKE 和 IPSec 协议，可以与天融信的 IPSec VPN 以及其他支持 IKE 标准协议的 VPN 网关设备协商并建立标准的 IPSec VPN 隧道。此外，NGFW 还支持对通过 VPN 隧道内的网络流量进行访问控制、流量带宽控制及 NAT 处理，甚至还可对通过 VPN 隧道的流量进行病毒查杀。

IPSec VPN 特点

IPSec（IP Security）协议作为网络层隧道协议，是由 IETF 制定的一系列协议，它为 IP 数据报提供了高质量、可互操作、基于密码学的安全性。特定的通信方之间在 IP 层通过加密与数据源验证等方式，来保证数据报文在网络上传输时的私有性、完整性、真实性和防重放。IPSec VPN 可实现功能包括：

- 保证数据机密性（Confidentiality）：在传输数据包之前通过加密算法将数据包加密，只有真正的接收者才对该数据包进行解密，进而查看其内容，以保证数据的机密性。
- 保证数据完整性（Data integrity）：在目的地通过验证算法验证数据包，以保证该数据包在传输过程中有任何数据被篡改或丢失都能被检测出来。
- 保证数据真实性（Data authentication）：在 IPSec 通信之前，通信双方先认证对方身份的合法性，身份验证通过之后才能通信，验证数据源，以保证数据来自真实的发送者。
- 防重放（Anti-replay）：防止恶意用户通过重复发送捕获到的数据包所进行的攻击，即接收方会拒绝旧的或重复的数据包。

IPSec VPN 基本概念

IPSec VPN 是采用 IPSec（IP Security）协议实现可基于公网基础设施安全传输数据的一种隧道技术，IPSec 协议并非为一个单独的协议，而是由 Internet 工程任务组（IETF）制定的一组安全协议套件，为确保网络层数据通信的安全机制，其体系机构包括：安全联盟、安全协议、密钥管理、操作模式、验证算法、加密算法和安全策略等。

1．安全联盟

安全联盟 SA（Security Association，安全联盟）是通信对等体间对某些要素的约定，包括：安全协议（AH、ESP 或者两者结合使用）、协议的操作模式（传输模式和隧道模式）、加密算法、验证算法、特定流中保护数据的共享密钥以及密钥的生存周期等。

安全联盟是单向的，在两个对等体之间的双向通信，最少需要两个安全联盟来分别对两个方向的数据流进行安全保护。同时，如果希望同时使用 AH 和 ESP 来保护对等体间的数据流，则分别需要两个 SA，一个用于 AH，另一个用于 ESP。

安全联盟由一个三元组来唯一标识，这个三元组包括 SPI（Security Parameter Index，安全参数索引）、目的 IP 地址、安全协议号（AH 为 51，ESP 为 50），其中，SPI 是为唯一标识 SA 而生成的一个 32 比特的数值，它在 AH 和 ESP 头中传输。

2．安全联盟的协商方式

建立安全联盟的协商方式包括两种：一种是手工方式（manual），一种是 IKE 自动协商（isakmp）方式。前者配置比较复杂，创建安全联盟所需的全部信息都必须手工配置，而且 IPSec 的一些高级特性（例如定时更新密钥）不被支持，但优点是可以不依赖 IKE 而单独实现 IPSec 功能。而后者则相对比较简单，只需要配置好 IKE 协商安全策略的信息，由 IKE 自动协商来创建和维护安全联盟。

当与之进行通信的对等体设备数量较少时，或是在小型静态环境中，手工配置安全联盟是可行的。对于中、大型的动态网络环境中，推荐使用 IKE 协商建立安全联盟。

3．操作模式与安全协议

IPSec VPN 有两种操作模式：传输模式和隧道模式。IPSec 提供了两个安全协议用以保护网络通信：AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷），对于 AH 和 ESP，均支持 IPSec VPN 的两种操作模式。

数据包需经过 IPSec VPN 隧道传输时，NGFW 在发送数据包之前需对数据包进行封装，在传输模式下，AH 或 ESP 被插入到 IP 报头之后但在所有传输层协议之前，或所有其他 IPSec 协议之前；在隧道模式下，AH 或 ESP 插在原始 IP 报头之前，另外生成一个新头放到 AH 或 ESP 之前。

1）AH 协议

AH 是报文头验证协议，为基于 IP 的传输层协议，主要提供数据源验证、数据完整性校验和防报文重放功能，可对整个 IP 数据包进行完整性验证（将数据包在传输过程中可能会发生变化的字段置 0），但并不加密所保护的数据包。报头结构如下图所示。

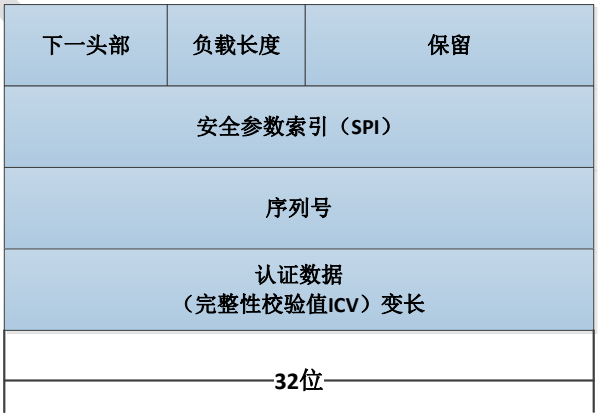


图 6-17 AH 协议报头结构

- 下一头部：标识 AH 报头后面的负载类型。传输模式下，为 TCP、UDP 或 ESP 协议的编号，隧道模式下，为 IP 或 ESP 协议的编号。
- 安全参数索引（SPI）：与目的 IP 地址和安全协议一起唯一标识 IPSec SA，接收端设备通过 SPI 查找安全联盟，以解密 IPSec 协议保护的数据。
- 序列号（32 位）：唯一标识数据包，用于防重放攻击。
- 认证数据：包含数据完整性校验值 ICV，用于接收方进行完整性校验时对比，以确认数据在传输过程中是否被篡改或丢失。

NGFW 通过 AH 协议封装数据报文时，如下图所示。

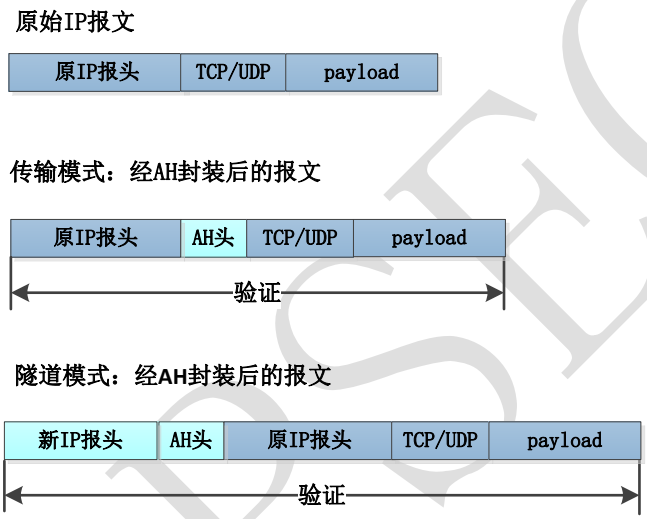


图 6-18 AH 安全协议封装报文格式

2）ESP 协议

ESP 是封装安全载荷协议，除了提供 AH 协议的所有功能外（但其数据完整性校验只针对 ESP 报头与 ESP 报尾之间数据），还可对 IP 数据包中 ESP 报头之后与 ESP 报尾之间的数据进行加密。其报头结构如下图所示。

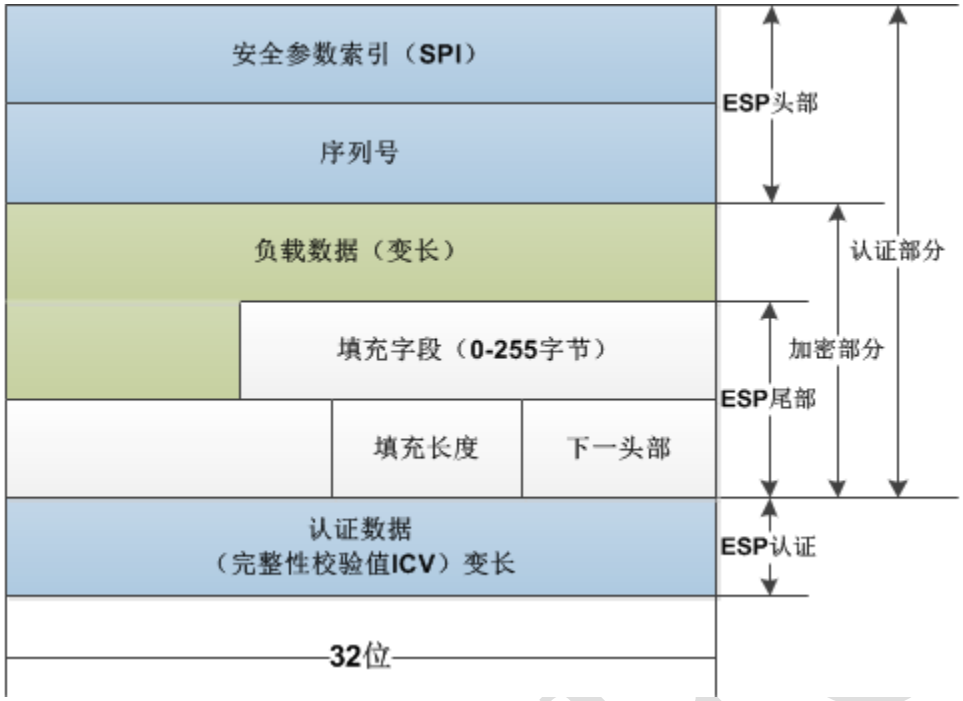


图 6-19 ESP 协议报头结构

- 安全参数索引（SPI）：与目的 IP 地址和安全协议一起唯一标识 IPSec SA。
- 序列号（32 位）：唯一标识数据包，用于防重放攻击。
- 下一头部：标识 ESP 报头后面的负载类型，传输模式下，为 TCP 或 UDP 协议的编号，隧道模式下，为 IP 协议的编号。
- 认证数据：包含数据完整性校验值 ICV，用于接收方进行完整性校验时对比，以确认数据在传输过程中是否被篡改或丢失。

NGFW 通过 ESP 协议封装数据报文时，如下图所示。

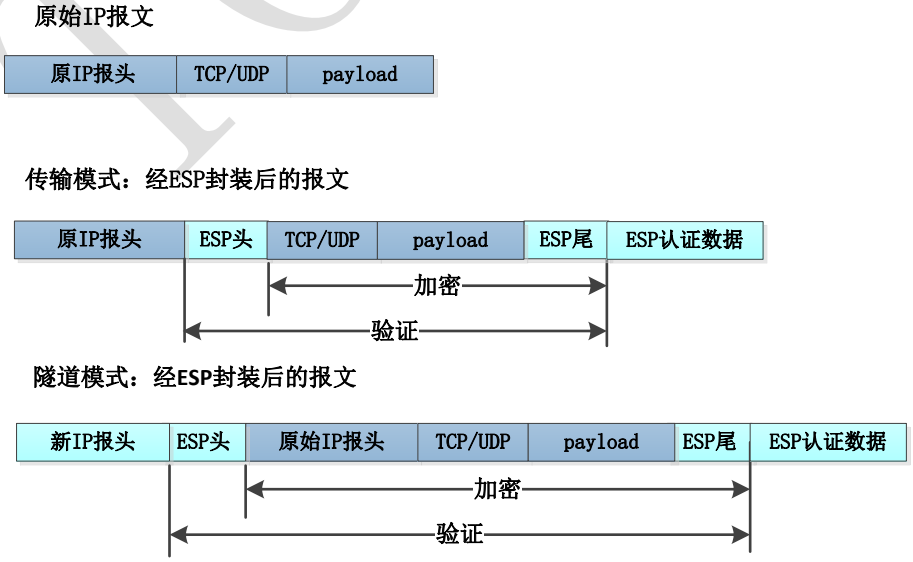


图 6-20 ESP 安全协议封装报文格式

3）AH 协议+ESP 协议

IPSec VPN 同时采用 AH 和 ESP 协议时，NGFW 处理数据报文时既根据 AH 协议对数据报文进行处理，也根据 ESP 协议对数据报文进行处理。AH 和 ESP 协议封装报文格式如下图所示。

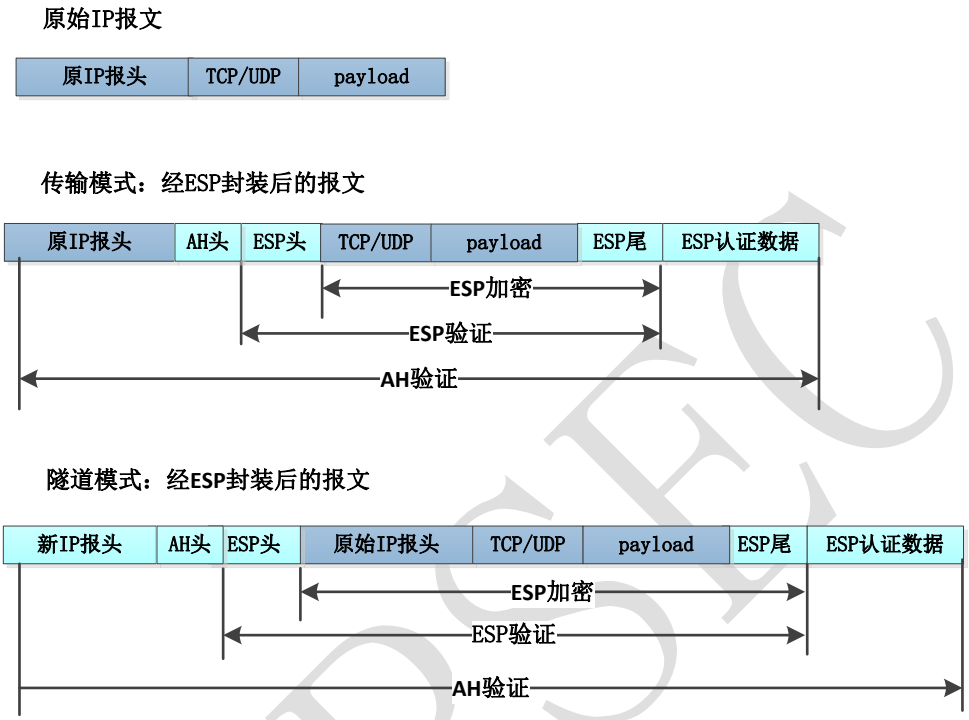


图 6-21 （AH+ESP）协议封装报文格式

从安全性来讲，隧道模式优于传输模式，原始 IP 报头前新增的 IP 报头可以使用 IPSec 对等体的 IP 地址来隐藏客户机的真实 IP 地址、协议类型，且原始 IP 报文的所有内容可被验证及加密。从性能来讲，隧道模式比传输模式占用更多带宽，因为它有一个额外的 IP 头。因此，到底使用哪种模式需要在安全性和性能间进行权衡。

因 AH 协议不提供加密功能，ESP 协议不对数据包的报头进行验证，在安全性要求较高的应用场景中，建议结合 AH 协议和 ESP 协议处理数据报文。

4．验证算法与加密算法

1）验证算法

AH 和 ESP 都能够对 IP 报文的完整性进行验证，以判别报文在传输过程中是否被篡改。验证算法的实现主要是通过杂凑函数，杂凑函数是一种能够接受任意长的消息输入，并产生固定长度输出的算法，该输出称为消息摘要。IPSec 对等体计算摘要，如

果两个摘要是相同的，则表示报文是完整未经篡改的；否则，表明报文在传输过程中已发送改变。一般来说 IPSec 使用两种验证算法：

- MD5：MD5 通过输入任意长度的消息，产生 128bit 的消息摘要。
- SHA-1：SHA-1 通过输入长度小于 2 的 64 次方比特的消息，产生 160bit 的消息摘要。

SHA-1 的摘要长于 MD5，因而是更安全的。

2）加密算法

ESP 能够对 IP 报文内容进行加密保护，防止报文内容在传输过程中被窥探。加密算法实现主要通过对称密钥系统，它使用相同的密钥对数据进行加密和解密。一般来说 IPSec 使用两种加密算法：

- DES：使用 56bit 的密钥对一个 64bit 的明文块进行加密。
- 3DES：使用三个 56bit 的 DES 密钥（共 168bit 密钥）对明文进行加密。

无疑，3DES 具有更高的安全性，但其加密数据的速度要比 DES 慢得多。

5．IKE

IKE 协议用于自动协商 AH 和 ESP 所使用的密码算法，并将算法所需的必备密钥放到恰当位置。为简化 IPSec 的使用和管理，IPSec 可以通过 IKE（Internet Key Exchange，因特网密钥交换协议）进行自动协商交换密钥、建立和维护安全联盟的服务。

说明

- IPSec 所使用的策略和算法等也可以手工协商，所以 IKE 协商属于可选配置。

IKE 协商过程

IPSec 的安全联盟可以通过手工配置的方式建立，但是当网络中节点增多时，手工配置将非常困难，而且难以保证安全性。这时就要使用 IKE（Internet Key Exchange，因特网密钥交换）自动地进行安全联盟建立与密钥交换的过程。

IKE 协议是建立在由 Internet 安全联盟和密钥管理协议 ISAKMP（Internet Security Association and Key Management Protocol）定义的框架上。它能够为 IPSec 提供了自动协商交换密钥、建立安全联盟的服务，以简化 IPSec 的使用和管理。

IKE 具有一套自保护机制，可以在不安全的网络上安全地分发密钥、验证身份、建立 IPSec 安全联盟。

IKE 使用了两个阶段为 IPSec 进行密钥协商并建立安全联盟：

第一阶段：通信各方彼此间建立了一个已通过身份验证和安全保护的通道，此阶段的交换建立了一个 ISAKMP 安全联盟，即 ISAKMP SA（也可称 IKE SA）。下图左边为第一阶段 IKE 主模式协商过程。

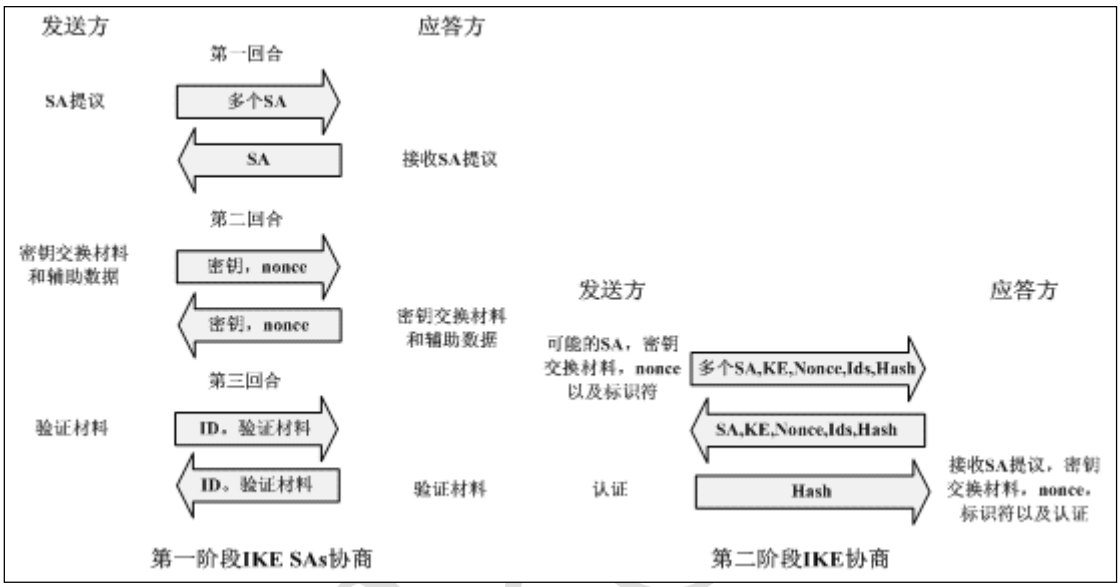


图 6-22 基于 IKE 自动协商过程

第二阶段：用在第一阶段建立的安全通道为 IPSec 协商安全服务，即为 IPSec 协商具体的安全联盟，建立 IPSec SA，IPSec SA 用于最终的 IP 数据安全传送。上图右边描述了第二阶段 IKE 协商基本过程。

6.9.1 静态隧道

IPSec VPN 静态隧道通过 IKE（Internet Key Exchange，因特网密钥交换）自动地进行安全联盟建立与密钥交换而自动建立。本节介绍如何配置静态隧道。

WEBUI 方式配置

要使 NGFW 能与其他网关设备成功建立 IPSec VPN 隧道，NGFW 需线执行如下步骤：

- 开放物理接口所属区域的 IPSecVPN 服务，请参见 7.5 本机服务。

- 如果静态隧道采用证书认证方式，则需要在 NGFW 上导入对端设备的证书，请参见 5.4.2 对端证书。

步骤 1 选择 **网络管理** > **IPSec VPN** > **静态隧道**。

步骤 2 点击『添加』。

步骤 3 配置 IPSec VPN 第一阶段协商参数。

1）配置第一阶段协商参数的基本信息，如下图所示。

在配置 IPSec VPN 第一阶段协商的基本信息时，各项参数的具体说明如下表所示。

参数	说明
隧道名	必选项。添加的静态隧道的名称。 隧道名称最多不能超过 40 个字符，并且不能包含除“-”或“_”之外的特殊字符。
协议类型	设置静态隧道所使用的协议类型。 可选项：国际、国密。 说明： 国际协议表示国际上统一使用的 IPSEC VPN 隧道协议标准规范簇。

参数	说明
	国密协议表示我国国家密码管理局制定的 IPSEC VPN 技术规范。
认证方式	进行隧道协商时的身份认证方式，目前支持“预共享密钥”和“数字证书”两种认证方式。 说明： 1）“预共享密钥”认证方式是指隧道两端的网关通过口令密码来确认对方身份，因此隧道两端必须配置相同的预共享密钥；“数字证书”认证方式是指隧道两端的网关通过网关证书来确认对方身份。 2）协议类型选择“国际”时，支持两种认证方式。协议类型选择“国密”时，只支持数字证书的认证方式。
证书位置	选择本机证书的类型。 可选项：主证书、从证书。 说明： 当且仅当认证方式选择“数字证书”时该参数可选择。 主证书类型为 RSA 证书类型，从证书类型为 ECC 证书类型。
预共享密钥	必选项。指隧道两端用于确认对方身份的口令密码。 说明： 当认证方式为“预共享密钥”时，必须配置该参数值。
本地标识	指用于本地 VPN 网关搜索共享密钥文件的索引，必须与隧道对端的“对方标识”保持一致。 填写格式：@XXX 或 XXX@XXX（XXX 为字母或数字）。
对方标识	指用于对方 VPN 网关搜索共享密钥文件的索引。 1）当认证方式为“预共享密钥”时，需要手动输入对方标识，填写格式为：@XXX 或 XXX@XXX（XXX 为字母或数字），且必须与隧道对端的“本地标识”保持一致。 2）当认证方式为“数字证书”，既可以手工输入对端网关证书中的“subject”字段值；也可以通过点击“浏览”设定数字证书的存储路径，然后点击“获取标识”来得到对方的标识信息。
本地地址	设置 NGFW 连接公网的接口 IP 地址，该接口用于与隧道对端设备进行通信。 说明： 建立 IPv4 静态隧道时，本参数设置为 IPv4 地址，格式：x.x.x.x；建立 IPv6 静态隧道时，本参数设置为 IPv6 地址，格式：x:x:x:x:x:x:x:x。
对方地址	设置隧道对端设备连接公网的接口 IP 地址，该接口用于与隧道对端设备进行通信。 说明： 建立 IPv4 静态隧道时，本参数设置为 IPv4 地址，格式：x.x.x.x；建立 IPv6 静态隧道时，本参数设置为 IPv6 地址，格式：x:x:x:x:x:x:x:x。
IKE 协商模式	指在 IKE 协商时采用的协商模式。 可选项：主模式、野蛮模式。 说明： 1）当协议类型为“国密”时，协商模式只能选择“主模式”。

参数	说明
	2）主模式交换的消息为 6 个，占用更多的资源和时间。但它对身份信息的交换进行了加密，安全性比野蛮模式高。 3）野蛮模式交换的消息为 3 个，占用资源少，协商速度快。它相对于主模式来说更灵活，能支持协商发起端为动态 IP 地址的情况。但它以明文的方式传输身份信息，安全性不及主模式。
主动发起隧道协商	选择是否主动发起隧道协商。 可选项：打开、关闭。选择“打开”，则该隧道本端主动发起协商；选择“关闭”，则隧道本端不主动发起协商。 说明： 只要有一端设备配置了主动发起协商，隧道就可以自动进行协商；如果隧道两端设备均不主动发起协商，则可以通过点击“协商”图标手动发起协商。

2）配置第一阶段协商参数的高级信息，如下图所示。

在配置 IPSec VPN 第一阶段协商参数的高级信息时，各项参数的具体说明如下表所示。

参数	说明
描述	隧道的相关信息。
SA 协商重试次数	IKE 协商不成功时的最大重试次数，超过该次数不再发起协商。 取值范围：1-100；默认值：3。
ISAKMP-SA 存活时间	IKE 安全联盟（SA）的生存时间，超过该时间则需要重新协商新的 SA。 单位：秒；取值范围：1-86400 秒；默认值：86400 秒。
ISAKMP-SA 的安全政策属性	在进行 IKE 安全协商时需要指定 ISAKMP-SA 安全政策属性。 当协议类型为“国际”时，加密算法包括：3DES、AES、DES、SM4；校验算法包括：MD5、SHA1、SM3；DH 交换值包括：DH1（modp768）、DH2（modp1024）、DH5（modp1536）。 当协议类型为“国密”时，加密算法只包括 SM4，校验算法包括：SHA1、SM3。 说明： 可以添加多个 ISAKMP-SA 安全政策属性。

步骤 4 配置第二阶段协商参数。

1）配置第二阶段协商参数的基本信息，如下图所示。

在设置第二阶段协商参数的基本配置时，各项参数的具体说明如下表所示。

参数	说明
本地子网/掩码	指静态隧道保护的本地子网地址/掩码。
对方子网/掩码	指静态隧道保护的对端网关的子网地址/掩码。
ESP 的算法提议列表	进行信息加密传输时，需要指定 ESP 算法提议列表，包括加密算法和校验算法。 说明： 当协议类型为“国密”时，加密算法只支持“SM4”，校验算法支持“SHA1”、“SM3”。
IPSEC-SA 的安全政策属性	定义对 IP 数据包提供何种保护，保护方式有：隧道模式、ESP、AH。 说明： 可以设置多个 IPSEC-SA 的安全政策属性。

2）配置第二阶段协商参数的高级信息，如下图所示。

在设置第二阶段协商参数的高级信息时，各项参数的具体说明如下表所示。

参数	说明
IPSEC-SA 存活时间	IPSEC 安全联盟的生存时间。

参数	说明
	单位：秒；取值范围：1-86400 秒；默认值：28800 秒。
启用 DPD	选择是否启用对端失效检测功能（Dead peer detection），该功能用于检测 VPN 另一端网关是否失效。 可选项：启用、不启用；默认值：启用。
DPD 间隔	进行 DPD 查询的时间间隔，即经过该段时间间隔没有收到对端网关的 IPSec 报文，就进行一次 DPD 请求。 单位：秒；取值范围：1-3600；默认值：30。
DPD 超时时间	等待对端网关 DPD 应答报文的超时时间，即：发送 DPD 请求报文后，如果超过此处设定的超时时间仍然没有收到对端网关正确的 DPD 应答报文，就表示对端网关不在线。 单位：秒；取值范围：1-28800；默认值：300。

步骤 5 （可选）点击【恢复默认】按钮，配置的参数恢复系统出厂配置。

步骤 6 点击【确定】按钮完成 IPSec VPN 静态隧道的添加。

CLI 方式配置

vpn tunnel add name <*string1*> [**gmneg** <on|off>] **authmode** <psk|rsasig> {**presharekey** <*string2*> **localid** <*string3*> **peerid** <*string4*>} |{**localcert_id** <primary|secondary> **peerid** <*string4*>} **localhost** <*string5*> **peerhost** <*string6*> **negomode** <main|aggressive|ikev2> **localsubnet** <*ipaddress1*> **localsubmask** <*netmask1*> **peersubnet** <*ipaddress2*> **peersubmask** <*netmask2*> [**auto_negotiate** <on|off>] [**description** <*string7*>] [**sa_keying_tries** <*number1*>] [**ike_life_seconds** <*number2*>] [**ike_policy** <*string8*>] [**alg_esp** <*string9*>] [**ipsecpolicy** <*string10*>] [**ipsec_ life_seconds** <*number3*>] [**dpd_switch** <on|off>] [**dpd_delay** <*number4*>] [**dpd_timeout** <*number5*>] [**dpd_action** <clear|hold|restart>] [**use-xauth** <on|off>] [**use-modecfg** <on|off>] [**as-xs-xc** <xs|xc>] [**xc-username** <*string11*>] [**xc-password** <*string12*>] [**as-ms-mc** <ms|mc>] [**use-modecfg-pull** <on|off>] [**sa_rekey_margin** <*number6*>] [**sa_rekey_fuzz** <*number7*>] [**keep_alive** <*number8*>] [**keeplive-flag** <on|off>] [**keeplive-name** <*string13*>] [**enable** <on|off>] [**line-type** <single >]

命令描述：

添加一条 IPSec VPN 静态隧道。

参数说明：

vpn tunnel add	添加一条静态隧道。

name	必选项，静态隧道的名称。
string1	字符串类型。
gmneg	可选项，是否是国密协商协议。
on|off	是|否，“是”表示静态隧道使用的协议类型为国密；“否”表示静态隧道使用的协议类型为国际，默认为 off（国际）。 说明： 协商协议为国密时，NGFW 只能通过证书与对端认证；协商协议为国际时，NGFW 可通过证书或预共享密钥方式与对端认证。
authmode	选择进行隧道协商时的身份认证方式。
psk|rsasig	“psk”指预共享密钥认证方式；“rsasig”指证书认证方式。
presharekey	认证方式为预共享密钥认证时，该参数必选。指静态隧道两端用于确认对方身份的口令密码。
string2	字符串类型。 当使用隧道两端通过预共享密钥认证时，必须填写该参数值。
localid	认证方式为预共享密钥认证时，该参数必选。用于本地 VPN 网关搜索共享密钥文件的索引，必须与隧道对端的“**peerid**”保持一致。
string3	字符串类型。填写格式为@XXX 或 XXX@XXX，XXX 为字母或数字。 说明： 只有当认证方式为“psk”时，才能配置。
peerid	必选项。用于对方 VPN 网关搜索共享密钥文件的索引。
string4	字符串类型。 当认证方式为“psk”时，需要手动输入对方标识，填写格式为@XXX 或 XXX@XXX，XXX 为字母或数字，且必须与隧道对端的“**localid**”保持一致。
localcert_id	只有当认证方式为“数字证书”时，该项参数可选。指定本地证书路径。
primary|secondary	主证书|从证书。默认为主证书。
peerid	必选项。用于对方 VPN 网关搜索共享密钥文件的索引。
string4	字符串类型。 说明： 当认证方式为“rsasig”，需要手工输入对端网关证书中的“subject”字段值。
localhost	必选项，设置本地接口地址。 说明： 建立 IPv4 静态隧道，格式：A.B.C.D；建立 IPv6 静态隧道，格式：x:x:x:x:x:x:x:x。
string3	IP 地址字符串。
peerhost	输入对端网关的地址/域名，或者输入中心网关的名称。
string5	IP 地址或域名字符串。 说明：

	建立 IPv4 静态隧道，格式：A.B.C.D；建立 IPv6 静态隧道，格式：x:x:x:x:x:x:x:x。
negomode	在第一阶段协商（即 IKE 协商）时采用的协商模式。
main|aggressive|ikev2	“main”指主模式；“aggressive”指野蛮模式。 默认为 main（主模式）。“ikev2”指 IKE 的第二版协议。 说明： 主模式与野蛮模式是 IKE 协议第一阶段协商的两种模式，而 IKEV2 是 IKE 的第二版协议。
localsubnet	指定静态隧道保护的本地子网地址。
ipaddress1	标准网络地址字符串。
localsubmask	指定静态隧道保护的本地子网掩码。
netmask1	标准子网掩码字符串。
peersubnet	指定静态隧道保护的对端网关的子网地址。
ipaddress2	标准子网字符串。
peersubmask	指定静态隧道保护的对端网关的子网掩码。
netmask2	标准子网掩码字符串。
auto_negotiate	选择是否主动发起隧道协商。
on|off	“on”指自动协商；“off”指不自动协商。 缺省值：on（自动协商）。设置为“on”，则该隧道本端主动发起协商；设置为“off”，则隧道本端不主动发起协商。 说明： 1）单线路情况下，只要有一端设备配置了主动发起协商，隧道就可以自动进行协商；如果隧道两端设备均不主动发起协商，则可以通过命令“**#tunnel initiate name** <*string*> ”手动发起协商。 2）多线路情况下，必须由分支网关主动发起隧道协商。
description	隧道的相关描述信息。
string7	字符串类型。
sa_keying_tries	IPSEC SA 协商重试次数。
number1	数值类型。 取值范围：1-100；默认值：3。
ike_life_seconds	ISAKMP-SA 存活时间。
number2	数值类型。 单位：s；取值范围：1-86400；默认值：86400。
ike_policy	在进行 IKE 安全协商时需要指定 ISAKMP-SA 安全政策属性。加密算法包括：3DES、AES、DES、SM1、SM4；校验算法包括：MD5、SHA1、SM3；DH 交换值包括：DH1（modp768）、DH2（modp1024）、DH5（modp1536）。 说明： 当协议类型为“国密”时，加密算法只包括 SM1、SM4，校验算法包括：SHA1、SM3。
string8	字符串类型。 可以输入多个，多个安全政策属性之间用“,”分

	隔。
alg_esp	进行信息加密传输时，需要指定 ESP 算法提议列表，包括加密算法和校验算法，默认的加密算法为 3DES-MD5。
string9	字符串类型。 例如：3des-md5 或 3des-sha1。
ipsecpolicy	定义对 IP 数据包提供何种保护，保护方式有：完美向前加密、隧道模式、压缩、ESP、AH。
string10	字符串类型。 为 pfs、tunnel、compress、encrypt、authenticate 中的一个或多个，选取多个时中间用“,”隔开，例如：pfs,tunnel。
ipsec_life_seconds	IPSEC-SA 存活时间。
number3	数值类型。 单位：s；取值范围：1-86400；默认值：28800。
dpd_switch	选择是否启用 DPD 功能，用于探测对端网关是否在线。
on|off	启用|不启用
dpd_delay	进行 DPD 查询的时间间隔，即：隔了多久没有收到对端网关的 IPSec 报文，就进行一次 DPD 请求。
number4	数值类型。 单位：s；取值范围：1-3600；默认值：30。
dpd_timeout	等待对端网关 DPD 应答报文的超时时间，即：发送 DPD 请求报文后，如果超过此处设定的超时时间仍然没有收到对端网关正确的 DPD 应答报文，就表示对端网关不在线。
number5	数值类型。 单位：s；取值范围：1-28800；默认值：300。
dpd_action	DPD 探测失败后，网关采取的措施。
clear|hold|restart	清除隧道|保持隧道当前状态|重建隧道，默认值：clear（清除隧道）。 说明： WEBUI 中的 DPD 失败隧道操作只能配置 clear，但是通过命令行进行配置后，网关将执行命令行中的配置。
use-xauth	是否启用 XAUTH“扩展认证”功能。 说明： 如果启用了扩展认证，则本地保护子网与对端保护子网必须设置为单个 IP 地址。
on|off	启用|不启用
use-modecfg	是否启用“扩展认证/模式配置”功能。 说明： 如果启用了扩展认证，则本地保护子网与对端保护子网必须设置为单个 IP 地址。
on|off	启用|不启用 说明： 启用“**use-modecfg**”功能后，参数“**as-xs-xc**”和“**as-ms-mc**”必须配置相同值，否则无法认证成功。

as-xs-xc	启用“**use-xauth**”或者“**use-modecfg**”功能后，选择 IPSec VPN 网关是作为认证服务端还是认证客户端。作为服务端，需要等待客户端进行认证；作为客户端，需要向服务器端主动认证。
xs|xc	服务端|客户端 说明： 启用“**use-modecfg**”功能后，参数“**as-xs-xc**”和“**as-ms-mc**”必须配置相同值，否则无法认证成功。
xc-username	作为 XAUTH 客户端时，向服务端进行认证的用户名。
string11	字符串类型。
xc-password	作为 XAUTH 客户端时，向服务端进行认证的密码。
string12	字符串类型。
as-ms-mc	启用“**use-modecfg**”功能后，选择 IPSec VPN 网关是作为认证服务端还是认证客户端。
ms|mc	服务端|客户端 说明： 启用“**use-modecfg**”功能后，参数“**as-xs-xc**”和“**as-ms-mc**”必须配置相同值，否则无法认证成功。
use-modecfg-pull	选择是否启用模式配置的 PULL 模式。
on|off	启用|不启用
sa_rekey_margin	ISAKMP-SA 周期重叠时间。 为了防止因为前一个 IKE SA 结束时新的 IKE SA 没有协商成功而造成通信中断，该参数与“**sa_rekey_fuzz**”共同作用，计算出新的 IKE SA 提前进行协商的时间点。
number6	数值类型。 单位：s；取值范围：1-540；默认值：540。
sa_rekey_fuzz	ISAKMP-SA 模糊比。 该参数与“**sa_rekey_margin**”共同作用，计算新的 IKE SA 提前进行协商的时间点。
number7	数值类型。取值范围：1-100；默认值：3。
keep_live	KEEP-ALIVE 间隔。 说明： 此参数只是为了兼容 3.3.005 以前版本而保留，在新版本中不再起作用，故无需配置。
number8	数值类型。 单位：s；取值范围：1-40；默认值：20。
keeplive-flag	是否启用天融信私有隧道保活。 一般情况下，IPSec VPN 网关通过 DPD 来实现静态隧道的保活，但是由于有些特殊的网络环境会导致 DPD 失效，隧道无法保活，因此需要使用天融信私有的保活方法来实现。
on|off	启用|关闭 说明： 为了避免不必要的开销，建议用户在 DPD 能有效工作的网络环境下只启用 DPD 保活，关闭天融信

	私有隧道保活。
keeplive-name	输入隧道保活对象的名称。
string13	字符串类型。必须是网关中已经配置完成的隧道保活对象的名称。
enable	是否启用该静态隧道。
on|off	启用|不启用
line-type	选择本地网关与对端网关建立静态隧道时应用的线路类型。
single	指单线路。 说明： 单线路是指建立隧道的两台网关都只有一条外网连接线路，网关之间只需要配置并协商一条静态隧道，两端保护子网之间的流量完全通过该隧道进行发送。

以下是添加静态隧道的示例：

添加一条协议类型为国密的静态隧道。隧道本地地址为 192.168.16.2，对端地址为 172.16.16.3，对端设备证书 subject 字段为 cn=css，保护的流量为子网 50.0.0.0/8 通往子网 60.0.0.0/8 的流量。

TopsecOS# **vpn tunnel add name** *tu001* **gmneg** on **authmode** rsasig **localcert_id** primary **peerid** *cn=sss* **localhost** *192.168.16.2* **peerhost** *172.16.16.3* **negomode** main **localsubnet** *50.0.0.0* **localsubmask** *255.0.0.0* **peersubnet** *60.0.0.0* **peersubmask** *255.0.0.0*

添加一条协议类型为国际且认证方式为预共享密钥认证的静态隧道。隧道本地地址为 192.168.16.2，对端地址为 172.16.99.100，预共享密钥为 111111，保护的流量为子网 70.0.0.0/8 通往子网 80.0.0.0/8 的流量。

TopsecOS# **vpn tunnel add name** *tu002* **authmode** psk **presharekey** *111111* **localid** *@aaa* **peerid** *@bbb* **localhost** *192.168.16.2* **peerhost** *172.16.99.100* **negomode** main **localsubnet** *70.0.0.0* **localsubmask** *255.0.0.0* **peersubnet** *80.0.0.0* **peersubmask** *255.0.0.0*

vpn tunnel delete name <*string*>

命令描述：

删除一条静态隧道。

参数说明：

vpn tunnel delete	删除一条 IPSec VPN 静态隧道。
name	根据名字删除。
string	字符串类型。必须是网关中已经配置完成的静态隧道名称。 说明： 除了“查看”之外，建议用户不要对从 TP 服务器下载到网关的静态隧道进行任何其他操作。

以下是删除静态隧道 tu001 的示例：

```
TopsecOS#vpn tunnel delete name tu001
```

vpn tunnel show [**name** <*string*>]

命令描述：

显示静态隧道信息。

参数说明：

vpn tunnel show	查看静态隧道信息。
name	可选项，根据名字查看静态隧道的详细配置信息。
string	字符串类型。必须是已经配置完成的静态隧道名称或从 TP 系统成功下载到网关的静态隧道名称。

使用说明：

不指定任何参数时显示所有静态隧道信息。

以下是显示所有静态隧道信息的示例：

```
TopsecOS#vpn tunnel show
name      localhost      localclient      peerhost      peerclient      state      enable
tu        1.1.1.1        10.0.0.0/8       1.1.1.2       20.0.0.0/8      ready      yes
tu002     192.168.16.2   70.0.0.0/8       172.16.99.100 80.0.0.0/8      negotiateing yes
```

vpn tunnel enable name <*string*>

命令描述：

启用某条静态隧道，使其配置生效。

参数说明：

vpn tunnel enable	启用某条静态隧道，使其配置生效。
name	必选项，设置静态隧道的名称。
string	字符串类型。必须是网关中配置完成的静态隧道名称。 说明： 除了“查看”之外，建议用户不要对从 TP 服务器下载到网关的静态隧道进行任何其他操作。

以下是启用静态隧道 tu002 的示例：

```
TopsecOS#vpn tunnel enable name tu002
```

vpn tunnel disable name <*string*>

命令描述：

禁用某条静态隧道，使其配置失效。

参数说明：

vpn tunnel disable	禁用某条静态隧道，使其配置失效。
name	必选项，指定静态隧道的名称。
string	字符串类型。必须是网关中配置完成的静态隧道名称。 说明： 除了“查看”之外，建议用户不要对从 TP 服务器下载到网关的静态隧道进行任何其他操作。

以下是禁用静态隧道 tu002 的示例：

```
TopsecOS#vpn tunnel disable name tu002
```

vpn tunnel initiate name <*string*>

命令描述：

手动使处于“ready”状态的静态隧道主动发起协商。

参数说明：

vpn tunnel initiate	手动使处于“ready”状态的隧道主动发起协商。
name	必选项，指定静态隧道的名称。
string	字符串类型。必须是网关中配置完成的静态隧道名称。 说明： 除了“查看”之外，建议用户不要对从 TP 服务器下载到网关的静态隧道进行任何其他操作。

以下是手动使静态隧道 tu 主动发起协商的示例：

```
TopsecOS#vpn tunnel initiate name tu
```

vpn tunnel terminate name <*string*>

命令描述：

拆除一条静态隧道，使该隧道状态变为“stop”。

参数说明：

vpn tunnel terminate	拆除一条静态隧道，使该隧道状态变为“stop”。
name	必选项，指定静态隧道的名称。
string	字符串类型。必须是网关中配置完成的静态隧道名称。 说明： 除了“查看”之外，建议用户不要对从 TP 服务器下载到网关的静态隧道进行任何其他操作。

使用说明：

隧道激活启动后，可以通过隧道中止命令拆除隧道。

以下是拆除静态隧道 tu 的示例：

```
TopsecOS#vpn tunnel terminate name tu
```

vpn tunnel clean <cr>

命令描述：

清除静态隧道。

以下是清空静态隧道的示例：

```
TopsecOS#vpn tunnel clean
```

6.9.2 手工隧道

IPSec 的基础是安全联盟（SA），它是两个通信实体经协商建立起来的一种协定。SA 可以采用前面所述的密钥交换的动态方式产生，也可以通过用户手工配置的方式建立。手工隧道就是通过手工设置 IPSec SA 而建立的静态隧道。

手工隧道的优点：

1）没有 IKE 协商的过程，开销小，也更简单。

2）不需要启用 DPD 来实现手工隧道的保活。

手工隧道的缺点：

1）网络管理员要为每条隧道做详细的配置，且需要两端所在网络的管理员协作才能完成。

2）加密密钥容易泄露，安全性不高。

管理员可以根据具体的需求来确定静态隧道的建立方式。

WEBUI 方式配置

要使 NGFW 能与其他网关设备成功建立 IPSec VPN 隧道，NGFW 需先执行如下步骤：

- 开放用于物理接口所属区域的 IPSecVPN 服务，请参见 7.5 本机服务。

步骤 1 选择 **网络管理** > **IPSec VPN** > **手工隧道**。

步骤 2 点击『添加』，如下图所示。

在设置手工隧道时，各项参数的具体说明如下表所示。

参数	说明
隧道名称	必选项，设置手工隧道的名称。 隧道名称最多不能超过 40 个字符，并且不能包含除“-”或“_”之外的特殊字符。
本端地址	必选项。指手工隧道本端的 IP 地址。
入 SPI	必选项。进入端的安全参数索引（Security Parameter Index，SPI），用来标识 IP 报文所对应的安全关联。它由一个 32 位二进制数字组成。取值范围：4096-65535，建议从 40961 开始取值，因为 4096-40960 范围内的值通常会在自动建立隧道时被引用。
对方地址	必选项。指手工隧道对端的 IP 地址。

参数	说明
出 SPI	必选项。出端的安全参数索引（Security Parameter Index，SPI），用来标识 IP 报文所对应的安全关联。它由一个 32 位二进制数字组成。取值范围：4096-65535，建议从 40961 开始取值，因为 4096-40960 范围内的值通常会在自动建立隧道时被引用。
原始加密密钥	必选项。用于加密的原始密钥，需要手工隧道两端填写一致，且它的填写格式受参数“由原始密钥派生加密密钥”的影响。 1）如果勾选了“由原始密钥派生加密密钥”，则“加密密钥”可填写长度在 128 位以内的字符串，可包括大小写英文字母及数字。 2）如果没有勾选“由原始密钥派生加密密钥”，则“加密密钥”必须填写十六进制数，长度与参数“加密算法”中所选算法的长度保持一致。
加密算法	用于生成加密密钥的算法，需要与手工隧道对端的填写一致。 可选项：DES、3DES、AES128、AES192、AES256、NULL。
由原始密钥派生加密密钥	设置是否根据上面所选择的加密算法使用原始加密密钥生成加密密钥。
原始认证密钥	必选项。用于认证的密钥，需要与手工隧道对端的填写一致，且它的格式受参数“由原始密钥派生认证密钥”的影响。 1）如果勾选“由原始密钥派生认证密钥”，则“认证密钥”可填写长度在 128 位以内的字符串，包括大小写英文字母及数字。 2）如果没有勾选“由原始密钥派生认证密钥”没有被选中，则“认证密钥”必须填写十六进制数，长度与参数“校验算法”中所选算法的长度保持一致。
认证算法	用于生成认证密钥的算法，需要手工隧道两端填写一致。 可选项：MD5，SHA-1。
由原始密钥派生认证密钥	设置是否根据上面所选择的校验算法使用原始认证密钥生成认证密钥。
本地子网/掩码	必选项。指手工隧道保护的本地子网 IP 地址/掩码。 说明： 建立 IPv4 手工隧道，格式：x.x.x.x/(0-32)；建立 IPv6 手工隧道，格式 x:x:x:x:x:x:x:x/(0-128)。
对方子网/掩码	必选项。指手工隧道保护的对端网关的子网 IP 地址/掩码。 说明： 建立 IPv4 手工隧道，格式：x.x.x.x/(0-32)；建立 IPv6 手工隧道，格式 x:x:x:x:x:x:x:x/(0-128)。
IPSEC-SA 的安全政策属性	选择 IP 数据包的保护方式，可选项：隧道模式、压缩、ESP、AH。 说明： 1）“ESP”和“AH”至少选中一项。默认是选中“ESP”。 2）如果选中“AH”，则参数“NAT 穿越”不可再选。
NAT 穿越	设置是否支持 NAT 穿越。如果采用 AH 封装，则该选项不可填写。

步骤 3 （可选）点击【恢复默认】按钮，配置的参数恢复系统出厂配置。

步骤 4 点击【确定】按钮完成 IPSec VPN 手工隧道的添加。

CLI 方式配置

vpn manual-tunnel add name <*string1*> [**ipsecmode** <tunnel|trans>] **localhost** <*string2*> [**encalg** <*string3*>] **enckey** <*string4*> [**authalg** <md5|sha1>] **authkey** <*string5*> [**compalg** <deflate>] **sport** <*number1*> **dport** <*number2*> **inspi** <*number3*> **outspi** <*number4*> **localsubnet** <*ipaddress1*> **localsubmask** <*netmask1*> [**mkauthkey** <on|off>] [**mkenckey** <on|off>] [**natt** <on|off>] **peerhost** <*string6*> **peersubnet** <*ipaddress2*> **peersubmask** <*netmask2*> [**proto_ah** <on|off>] [**proto_comp** <on|off>] [**proto_esp** <on|off>] [**action** <on|off>]

命令描述：

添加手工隧道。

参数说明：

vpn manual-tunnel add	添加手工隧道。
name	必选项，设置手工隧道名称。
string1	字符串类型，最多不能超过 48 字节。不能包含除“-”或“_”之外的特殊字符。
ipsecmode	可选项，设置 VPN 模式。
tunnel|trans	隧道模式或传输模式，默认值：tunnel。
localhost	必选项，设置本端的 IP 地址。
string2	IP 地址字符串。
encalg	可选项，设置隧道采用的加密算法，需要隧道两端一致。
string3	可选项：AES128、AES192、AES256、3DES、DES、NULL；默认值：3DES。
enckey	必选项，原始加密密钥，需要隧道两端一致。
string4	16 进制数，长度因算法而异。
authalg	可选项，设置隧道所采用的认证算法，需要隧道两端一致。
md5|sha1	md5 或 sha1，默认值：md5。
authkey	必选项，原始认证密钥，需要隧道两端一致。
string5	16 进制数，长度因算法而异。
compalg	可选项，设置压缩算法。
deflate	目前只支持 deflate 算法，默认值：deflate。

sport	必选项，设置源端口，也即本地端口。该参数是支持 NAT 穿越功能时配置的端口。
number1	符合端口规范，一般设为 4500。
dport	必选项，设置目的端口，也即对端端口。该参数是支持 NAT 穿越功能时配置的端口。
number2	符合端口规范，一般设为 4500。
inspi	必选项，设置入方向上的 SA 的 spi 值。 安全参数指针（Security Parameter Index，SPI）用来标识 IP 报文所对应的安全关联（SA）。
number3	32 位的整数。取值范围：4096-65535，建议从 40961 开始取值，因为 4096-40960 范围内的值通常会在自动建立隧道时被引用。
outspi	必选项，设置出方向上的 SA 的 spi 值。 安全参数指针（Security Parameter Index，SPI）用来标识 IP 报文所对应的安全关联（SA）。
number4	32 位的整数。取值范围：4096-65535，建议从 40961 开始取值，因为 4096-40960 范围内的值通常会在自动建立隧道时被引用。
localsubnet	必选项，设置本地保护的内部子网。
ipaddress1	子网 IP 地址。
localsubmask	必选项，设置本地保护的内部子网掩码。
netmask1	子网掩码。
mkauthkey	可选项，设置是否采用由原始认证密钥生成认证密钥。
on|off	on 表示要采用，off 表示不采用，默认值：on。
mkenckey	可选项，设置是否采用由原始加密密钥生成原始密钥。
on|off	on 表示要采用，off 表示不采用，默认值：on。
natt	可选项，设置是否支持 NAT 穿越。
on|off	on 表示支持，off 表示不支持，默认值：off。
peerhost	必选项，设置对端地址。
string6	IP 地址或域名。
peersubnet	必选项，设置对方保护的内部子网。
ipaddress2	子网地址。
peersubmask	必选项，设置对方保护的内部子网掩码。
netmask2	子网掩码。
proto_ah	可选项，设置是否采用 AH 封装。
on|off	on 表示要采用，off 表示不采用，默认值：off。 说明： 如果选择采用，则不可支持 NAT 穿越。

proto_comp	可选项，设置是否采用压缩。
on|off	on 表示要采用，off 表示不采用，默认值：off。
proto_esp	可选项，设置是否采用 ESP 封装。
on|off	on 表示要采用，off 表示不采用，默认值：on。
action	可选项，设置是否启用该隧道。
on|off	on 表示启用，off 表示不启用，默认值：on。

以下是添加手工隧道的示例：

添加一条名为 abc 的手工隧道，选择隧道模式，本端地址为 192.168.83.237，保护子网为 10.10.10.0，对端地址为 192.168.87.134，保护子网为 20.20.20.0，采用 3DES 加密算法，MD5 的认证算法，原始加密密钥为 123abc，原始认证密钥为 456abc，采用 ESP 封装。

TopsecOS#**vpn manual-tunnel add name** *abc* **localoutlink** *0* **ipsecmode** *tunnel* **localhost** *192.168.83.237* **inspi** *40961* **localsubnet** *10.10.10.0* **localsubmask** *255.255.255.0* **peerhost** *192.168.87.134* **outspi** *40961* **peersubnet** *20.20.20.0* **peersubmask** *255.255.255.0* **proto_esp** *on* **encalg** *3des* **enckey** *123abc* **mkenckey** *on* **authalg** *md5* **authkey** *456abc* **mkauthkey** *on* **proto_ah** *on* **proto_comp** *off* **metric** *100*

TopsecOS#**vpn manual-tunnel showall**

name localhost localclient peerhost peerclient interface enable

abc 192.168.83.237 10.10.10.0/255.255.255.0 192.168.87.134 20.20.20.0/255.255.255.0 ipsec0 yes

vpn manual-tunnel clean <cr>

命令描述：

清空手工隧道。

vpn manual-tunnel show name <*string*>

命令描述：

显示某条手工隧道的状态及配置。

参数说明：

vpn manual-tunnel show	显示某条手工隧道的状态及配置。
name	指定隧道名称。
string	字符串类型，最多不能超过 48 字节。不能包含除“-”或“_”之外的特殊字符。

vpn manual-tunnel start name <*string*>

命令描述：

启用某条手工隧道。

参数说明：

vpn manual-tunnel start	启用隧道。
name	隧道名称。
string	字符串类型，最多不能超过 48 字节。不能包含除“-”或“_”之外的特殊字符。

vpn manual-tunnel stop name <*string*>

命令描述：

禁用某条手工隧道。

参数说明：

vpn manual-tunnel stop	禁用隧道命令。
name	必选项，指定隧道名称。
string	字符串类型，最多不能超过 48 字节。不能包含除“-”或“_”之外的特殊字符。

6.10GRE

GRE（Generic Routing Encapsulation，通用路由封装）协议是网络层协议，采用了 Tunnel（隧道）技术，通过对某些网络层协议（如 IP 和 IPX）的数据报文进行封装，使这些被封装的数据报文能够在另一个网络层协议（如 IP）中传输。

Tunnel 是一个虚拟的点对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通道使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

GRE 隧道传输的报文具有三个报头，包括：

1）原 IP 报头（源/目的 IP 地址为数据报文通信真正的源/目的 IP 地址）；

2）GRE 报头；

3）新 IP 报头（源/目的 IP 地址为 GRE 隧道两端通往公网的接口地址）。

在公网中，数据包的载荷、原 IP 报头、GRE 报头均作为新 IP 报头的载荷在网络中传输，直至数据包到达隧道的目的端，真正的数据报文才被解析出来。以 IP 网络主机通过 GRE 隧道通信为例，GRE 封装及解封装过程如下图所示。

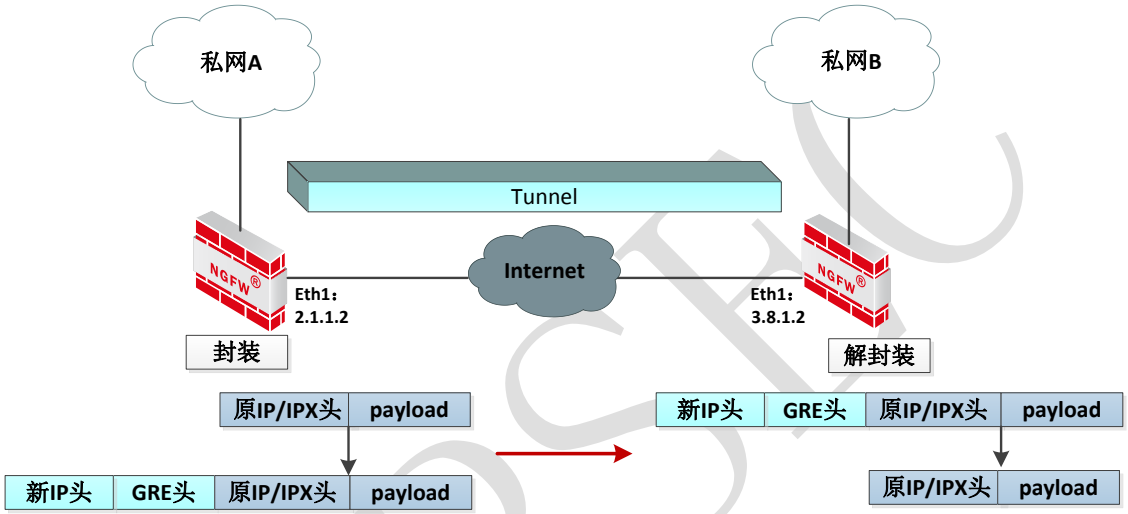


图 6-23 GRE 隧道封装/解封装示意图

➢ GRE 封装过程

1）本端设备接收到 IP 数据报文，如果数据报文经过各安全功能模块均允许放行，且查找路由表时该数据报文的出接口为 GRE 虚接口，则将该数据报文交由 GRE 虚接口。

2）GRE 虚接口接收到该数据报文后，为其封装 GRE 报头，然后在 GRE 报头基础上封装新的 IP 报头，此新 IP 报头的源 IP 地址为该 GRE 隧道源接口 IP 地址，目的 IP 地址为该 GRE 隧道目的接口 IP 地址。

3）根据新 IP 报头中的目的 IP 地址查找路由表，从隧道源接口将该被 GRE 协议封装的数据报文转发出去。

➢ 解 GRE 封装过程

1）对端设备接收到该被封装的数据报文后，根据目的地址发现该数据报文的接收者为自己，且该数据报文为 GRE 报文，则将该数据报文交由 GRE 协议处理。

2）GRE 协议进行关键字验证、校验和检测以及序列号检测后，去掉新 IP 头及 GRE 头部，然后交由 IP 协议处理。

3）IP 协议根据解除 GRE 封装的报文查找路由表，从相应接口将该报文转发到真正接收者。

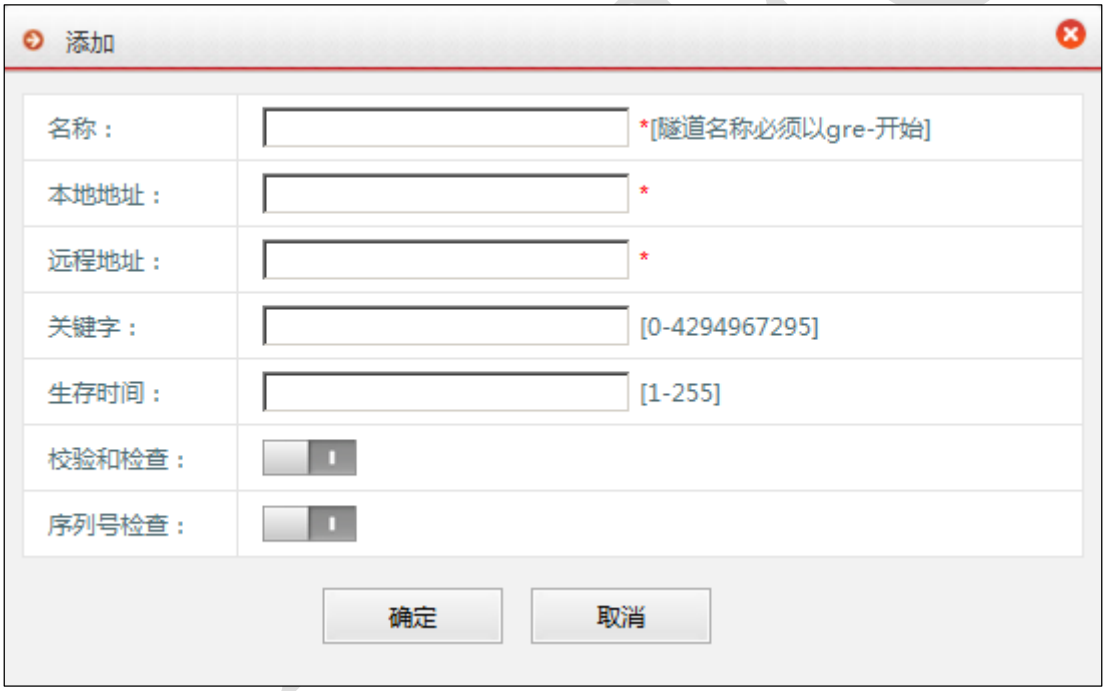
下面介绍在 NGFW 上设置 GRE 隧道。配置 GRE 隧道的要点包括：1）配置 GRE 隧道的源 IP 地址和目的 IP 地址；2）配置需通过 GRE 隧道传输的数据包的路由。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **GRE**。

步骤 2 添加 GRE 隧道。

1）点击『添加』，如下图所示。



在设置 GRE 隧道时，各项参数的具体说明如下表所示。

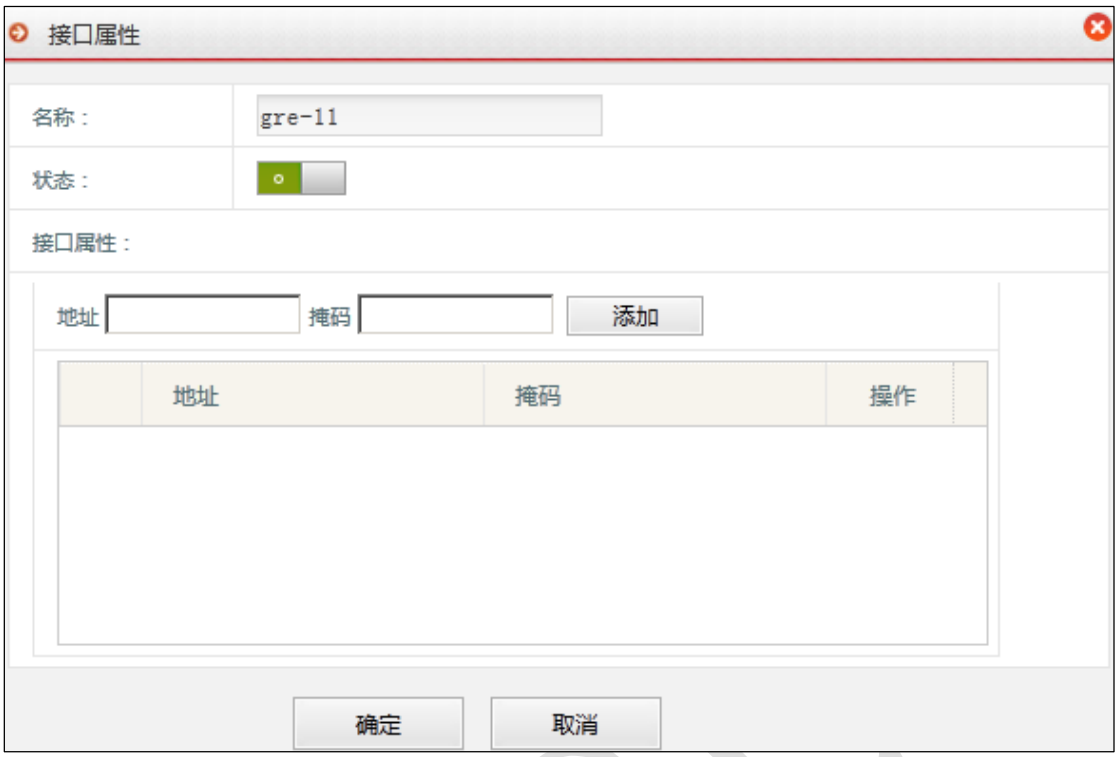
参数	说明
名称	必选项。设置隧道名称，必须以“gre-”开头。建议使用 gre-加 0 到 1023 之间的数字来为 GRE 隧道命名，例如 gre-0。
本地地址	必选项，指定 GRE 隧道的源 IP 地址，需设置隧道本地与公网相连物理的接口 IP 地址。 说明：

参数	说明
	GRE 隧道本端的“本地地址”需与对端的“远程地址”一致，否则，隧道将不能建立。
远程地址	必选项，指定 GRE 隧道的目的 IP 地址，需设置隧道对端与公网相连物理接口的 IP 地址。 说明： GRE 隧道本端的“远程地址”需与对端的“本地地址”一致，否则，隧道将不能建立。
关键字	标识隧道关键字，作为验证隧道有效性的依据。隧道两端配置的“隧道关键字”必须一致，否则无法通过验证。 取值范围：0-4294967295。
生存时间	可选项，设置 GRE 隧道本端设备与对端设备经过的最大路由器数目。 取值范围：1-255。
校验和检查	可选项，设置是否开启校验和检查。如果开启校验和检查功能，则发送方将对 GRE 头及报文负载计算校验和，接收方对接收到的报文计算校验和并与报文中的校验和进行比较，一致则对报文进一步处理，否则丢弃。  ：开启；  ：关闭。默认值：  。 说明： 如果只有隧道一端配置了使用校验和，将不对报文进行校验和检验；只有隧道两端都配置了开启“校验和检查”功能，才对报文进行校验和检验。
序列号检查	可选项，设置是否开启序列号检查。开启后，收发双方将进行序列号同步，只有对同步的报文才进行进一步处理，否则将报文丢弃。  ：开启；  ：关闭。默认为  。 说明： 只有在通道两端同时开启或关闭序列号同步机制时，通道才能建立。

2）点击【确定】按钮完成 GRE 隧道的创建。

步骤 3 （可选）配置 GRE 虚接口。

1）添加 GRE 隧道后，会自动在 NGFW 上添加同名的虚拟 GRE 接口。点击某 GRE 隧道的接口属性图标“  ”，即可配置该 GRE 虚接口的 IP 地址，如下图所示。



设置 GRE 虚接口时，各项参数的具体说明如下表所示。

参数	说明
状态	设置 GRE 虚接口的状态。默认为“打开”状态；如选择“关闭”，则该虚接口将不会工作。
接口地址	配置 GRE 虚接口的 IP 地址/掩码。

2）点击【确定】按钮完成 GRE 虚接口的创建。

步骤 4 配置 GRE 路由。

如果管理员配置了出接口为 GRE 虚接口的路由，匹配该路由的数据报文则需通过 GRE 隧道，关于路由的添加具体请参见 6.5 路由。

例如新添加 gre-0 隧道，如果管理员要求去往目的网段 192.168.95.0/24 的通信需由 gre-0 隧道处理，添加路由如下图所示。

CLI 方式配置

network tunnel add name <*string1*> **local** <*string2*> **remote** <*string3*> [**key** <*number1*>] [**csum** <on|off>] [**seq** <on|off>] [**ttl** <*number2*>] [**interface** <*string4*>]

命令描述：

增加 GRE 通道策略对象。

参数说明：

network tunnel add	增加 GRE 通道策略对象。
name	必选项，设置通道名称。
string1	字符串类型，隧道名称必须以“gre-”作为开头。
local	必选项，设置通道本地端封装地址。
string2	字符串类型，表示 IP 地址。
remote	必选项，设置通道目的端封装地址。
string3	字符串类型，表示 IP 地址。
key	可选项，设置标识通道的关键字。
number1	数值类型，取值范围：0-4294967295。
csum	可选项，设置是否开启校验和检查。
on|off	是|否
seq	可选项，设置是否开启序列号检查。
on|off	是|否
ttl	可选项，设置通道 TTL。
number2	数值类型，取值范围：1-255。
interface	可选项，设置与 GRE 通道绑定的接口。
string4	字符串类型，表示接口名称。 说明： 接口需配置 GRE 隧道的本地地址对应的接口。

以下是增加 GRE 通道策略对象的示例：

增加 GRE 通道，使去往 20.20.20.0/24 网段的通信数据由该 GRE 隧道传输。

TopsecOS# **network tunnel add name** *gre-test* **local** *192.168.6.24*

remote*192.168.7.23* **key** *111111* **csum** on **seq** on **ttl** *111*

TopsecOS**#network route add dst** *20.20.20.0/24* **dev** *gre-test*

network tunnel clean <cr>

命令描述：

清空 GRE 通道策略对象。

network tunnel show [**name** <*string*>]

命令描述：

显示 GRE 通道策略对象。

参数说明：

tunnel show	显示 GRE 表中的相关记录。
name	可选项，指定 GRE 策略名称。
string	字符串类型。

以下是显示 GRE 通道策略对象的示例：

显示名称为 gre-test 的策略。

```
TopsecOS# network tunnel show name gre-test
```

6.11智能 DNS

智能 DNS 可智能分析出请求域名解析的用户所属运营商及区域，为用户解析与其处于同一运营商的域名对应的 IP 地址，或距离用户较近服务器的 IP 地址，以提升用户访问网络资源的速度，从而为用户提供最佳网络体验。智能 DNS 可实现功能包括：

- 避免用户跨运营商访问。智能 DNS 可智能的判断通过域名访问某 Internet 资源的访问者所属网络，然后为访问者解析该域名对应的 IP 地址为域名对应的所有 IP 地址中，与用户处于同一运营商的 IP 地址。如访问者是电信用户，智能 DNS 解析服务器会把域名对应的电信 IP 地址解析给访问者。
- 保证用户就近访问机制。提供相同服务的多个服务器部署于不同地方时，DNS 服务器可根据用户与服务器的距离为用户解析与其距离较近服务器的 IP 地址。如企业在国外和国内都放置了服务器，智能 DNS 可以让国外的网络用户访问国外的服务器，国内的用户访问国内的服务器，从而使国内外的用户都能迅速的访问服务器资源。
- 服务器负载均衡。多台服务器同时对外提供相同服务时，智能 DNS 可将来自各地的访问流量比较平均的分配到每台服务器上，实现服务器负载均衡。

例如，topsec.com.cn 域名注册商部署了智能 DNS 服务器，外网用户通过域名访问 www.topsec.com.cn 时，域名解析详细过程如下图所示。

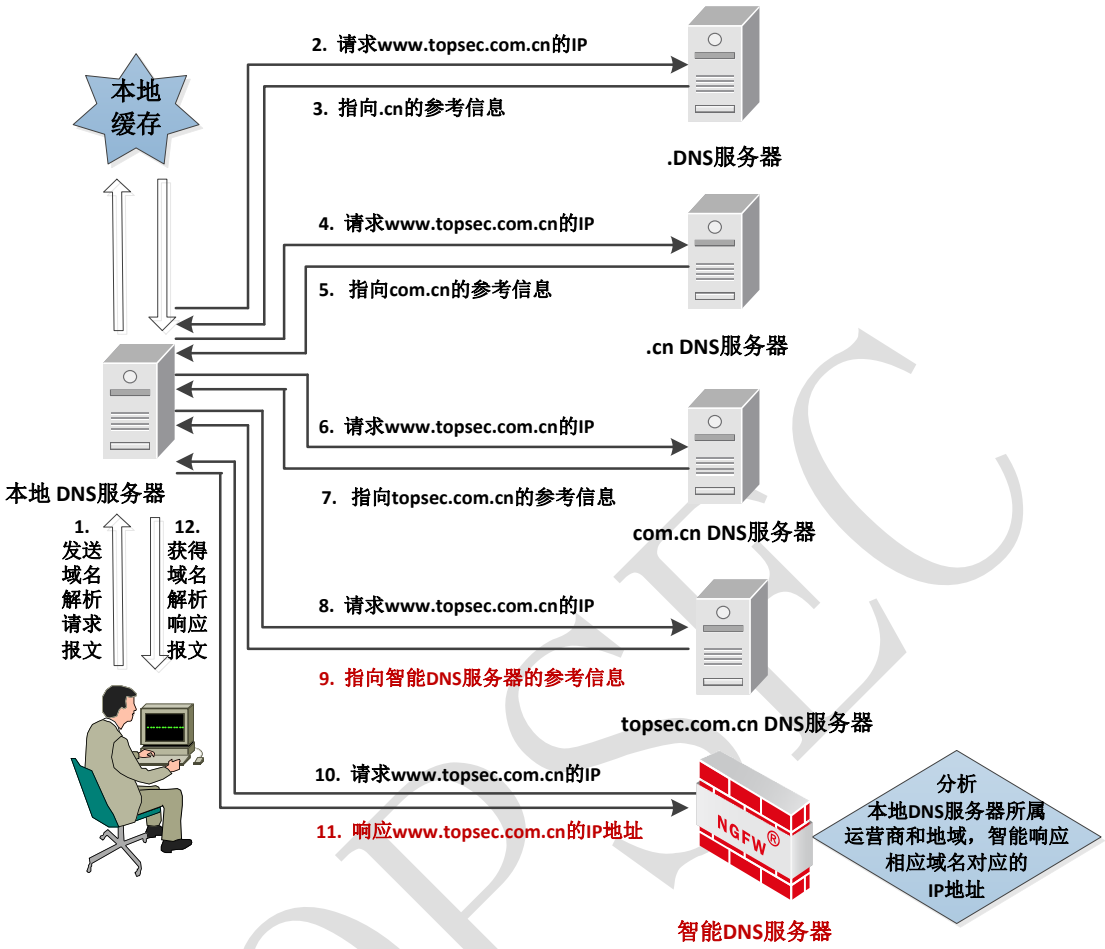


图 6-24 智能 DNS 服务器域名解析示意图

用户通过其本地 DNS 服务器进行域名解析的步骤和常规大体一致（关于常规域名解析流程具体请参见 4.1.7 本地域名解析），不同点为上图中的步骤 9-10，具体如下：

1）用户的本地 DNS 服务器查询到 topsec.com.cn 的 DNS 服务器的时候，topsec.com.cn 的 DNS 服务器返回给本地 DNS 服务器指向智能 DNS 服务器的地址，这样，本地 DNS 服务器就会转向智能 DNS 服务器去查询 www.topsec.com.cn 的 IP 地址。

2）用户的本地 DNS 服务器最后向智能 DNS 服务器发起 www.topsec.com.cn 的域名解析请求报文后，智能 DNS 服务器则通过分析本地 DNS 服务器的 IP，确定其所属运营商和区域，将与本地域名服务器属于同一个运营商或距离区域较近的域名对应的 IP 地址返回给本地 DNS 服务器。

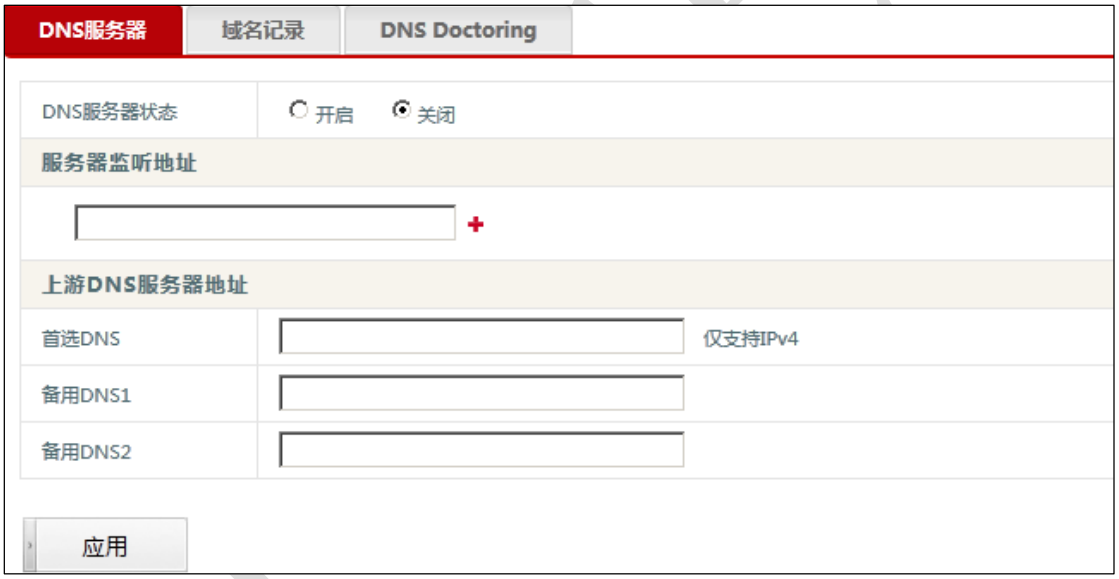
6.11.1 DNS 服务器

NGFW 同时支持本地 DNS 服务器和智能 DNS 服务器功能。内网用户通过域名访问网络资源时，NGFW 可作为用户的本地 DNS 服务器和智能 DNS 服务器进行域名解析；外网用户通过域名访问内网资源时，NGFW 可作为智能 DNS 服务器分析外网用户所处运营商及地域，为用户响应与其处于同一运营商的域名对应的 IP 地址，或响应与用户距离较近服务器对应的 IP 地址。

下面介绍如何启动 NGFW 的 DNS 服务器功能，以及 NGFW 作为本地 DNS 服务器时，配置上游 DNS 服务器信息。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **智能 DNS**，如下图所示。



步骤 2 配置 DNS 服务器。

在配置 DNS 服务器时，各项参数的具体说明如下表所示。

参数	说明
DNS 服务器状态	是否开启 NGFW 的 DNS 服务器功能。
服务器监听地址	设置 NGFW 监听 DNS 请求接口的 IP 地址，点击“✚”图标可添加多个监听接口。 说明： 启动 NGFW 的 DNS 服务器功能，必须开启监听接口所属区域的 DNS 服务，关于服务的开放具体请参见 7.5 本机服务。

参数	说明
上游 DNS 服务器地址	NGFW 作为普通 DNS 服务器时，该参数必选。配置上游 DNS 服务器的 IP 地址。 说明： 1）NGFW 接收到 DNS 请求时，如果 NGFW 本地缓存表中无对应 IP 地址与域名的映射项，则向 DNS 服务器发起域名解析请求，由 DNS 服务器为其解析域名对应的 IP 地址。 2）NGFW 支持主/备上游 DNS 服务器，向首选 DNS 服务器进行域名解析失败后，则通过备用上游 DNS 服务器进行域名解析。

步骤 3 点击【应用】按钮完成 DNS 服务器的配置。

CLI 方式配置

dns switch <on|off>

命令描述：

设置是否开启 DNS 服务器开关。DNS 服务器处于关闭状态时，才可配置 DNS 服务器的参数。

参数说明：

dns switch	设定 DNS 服务器开关。
on|off	开|关，默认 DNS 服务器处于关闭状态。

以下是开启 NGFW 的 DNS 服务器功能的示例：

```
TopsecOS#dns switch on
```

dns local add ipaddr <*ipaddress*>

命令描述：

设置 DNS 服务器接口的 IP 地址。

参数说明：

dns local add	设定 DNS 服务器监听接口的 IP 地址。
ipaddr	设置接口 IP 地址。
ipaddress	IP 地址字符串。

以下是设置 DNS 服务器监听接口的示例：

```
TopsecOS#dns local add ipaddr 192.168.90.79
```

TopsecOS**#dns local add ipaddr** *192.168.99.100*

dns local show <cr>

命令描述：

查看 DNS 服务器监听接口的 IP 地址。

以下是查看 DNS 服务器监听接口的 IP 地址的示例：

TopsecOS**#dns local show**
ID 8004 dns local add ipaddr 192.168.90.79
ID 8005 dns local add ipaddr 192.168.99.100

dns local clean <cr>

命令描述：

清除 DNS 服务器监听接口。

以下是查看 DNS 服务器监听接口的 IP 地址的示例：

TopsecOS**#dns local clean**

dns upstream-svr add ipaddr <*ipaddress*>

命令描述：

配置上游 DNS 服务器。

参数说明：

dns upstream-svr add	添加上游 DNS 服务器。
ipaddr	设置上游 DNS 服务器的 IP 地址。
ipaddress	IP 地址字符串。

以下是添加上游 DNS 服务器的示例：

TopsecOS**#dns upstream-svr add ipaddr** *202.103.96.100*
TopsecOS**#dns upstream-svr add ipaddr** *202. 96.0.133*

dns upstream-svr show <cr>

命令描述：

显示上游 DNS 服务器。

以下是显示上游 DNS 服务器的示例：

```
TopsecOS#dns upstream-svr show
ID 8009 dns upstream-svr add ipaddr 202.100.160.68
ID 8010 dns upstream-svr add ipaddr 202.96.0.133
```

dns upstream-svr clean <cr>

命令描述：

清除上游 DNS 服务器。

以下是清除上游 DNS 服务器的示例：

```
TopsecOS#dns upstream-svr clean
```

dns show <configuration|status>

命令描述：

显示 DNS 服务器信息。

参数说明：

dns show	显示 DNS 服务器信息。
configuration|status	配置信息|状态信息，默认显示配置信息。

以下是显示 DNS 服务器信息的示例：

显示 DNS 服务器状态信息。

```
TopsecOS# dns show status
DNS_Server is running
```

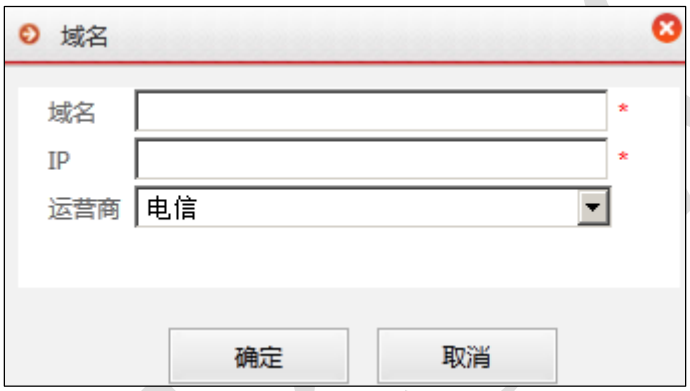
6.11.2 域名记录

域名记录用于 DNS 服务器响应域名解析请求报文。NGFW 目前支持的域名记录为 A 记录，即指域名（或主机名）与其对应 IP 地址的映射关系，内容包括域名、域名对应的 IP 地址、IP 地址所属运营商或所属区域。下面介绍如何添加域名记录。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **智能 DNS**，激活“域名记录”页签。

步骤 2 点击『添加』，如下图所示。



在配置域名与 IP 地址的映射关系时，各项参数的具体说明如下表所示。

参数	说明
域名	必选项，设置域名。
IP	必选项，设置域名对应的 IP 地址，格式：X.X.X.X。
运营商	设置 IP 地址所属运营商，可选项：空白、电信、移动、联通、教育、国外和其他。

说明

- ✧ 为某域名添加其 N 个对应 IP 地址的域名记录时，只需添加 N 个域名相同而 IP 地址不同的域名记录即可。

步骤 3 参数配置完成后，点击【确定】按钮完成域名记录的添加。

CLI 方式配置

dns domain add name <*string*> **desc** <*ipaddress*> **type** <a> [**isp** <ctc|cmc|cuc|edu|oth|otc>] [**ttl** <*number*>]

命令描述：

添加域名记录。

参数说明：

dns domain add	添加一个域名记录
name	必选项，设置域名。
string	字符串类型。
desc	必选项，设置域名对应的 IP 地址。
ipaddress	IP 地址字符串。
type	必选项，设置域名记录的类型。
a	表示 A 记录，A 记录用来指定域名（或主机名）对应的 IP 地址。
isp	可选项，设置域名对应 IP 地址所属运营商。
ctc|cmc|cuc|edu|oth|otc	电信|移动|联通|教育|其他|国外
ttl	可选项，设置全球各地 DNS 服务器获取到该域名记录后，该域名记录在其缓存表中的生存时间。
number	数值类型。

以下是添加域名记录的示例：

添加一条域名为 www.xxxx.com.cn，IP 地址为 2.2.2.2 的域名记录。

TopsecOS#**dns domain add name** *www.xxxx.com.cn* **desc** *2.2.2.2* **type** a

dns domain delete id <*number*>

命令描述：

删除指定 DNS 域名记录。

参数说明：

dns domain delete	删除 DNS 域名记录。
id	设置 DNS 域名的 ID。
number	数值类型。

以下是删除 DNS 域名信息的示例：

TopsecOS**#dns domain show**

ID 8003 dns domain add name www.security.com. type a desc 202.96.100.100 ttl 200

TopsecOS**#dns domain delete id** *8003*

dns domain clean <cr>

命令描述：

清除所有的域名记录。

以下是清除所有域名记录的示例：

```
TopsecOS#dns domain clean
```

6.11.3 DNS Doctoring

DNS Doctoring 记录了域名对应的内网 IP 地址和外网 IP 地址，既便于内网用户通过域名访问内网资源服务器，还可实现外网用户使用公网 IP 地址访问内网资源服务器时进行地址转换。

内网用户使用域名访问内部资源服务器时，NGFW 直接响应该域名对应的内网地址供用户访问资源服务器。外网用户访问 NGFW 所防护网络的内网资源服务器时，NGFW 可将服务器对外的公网 IP 地址转换为内网服务器真实 IP 地址，实现外网用户对内网资源服务器的访问。

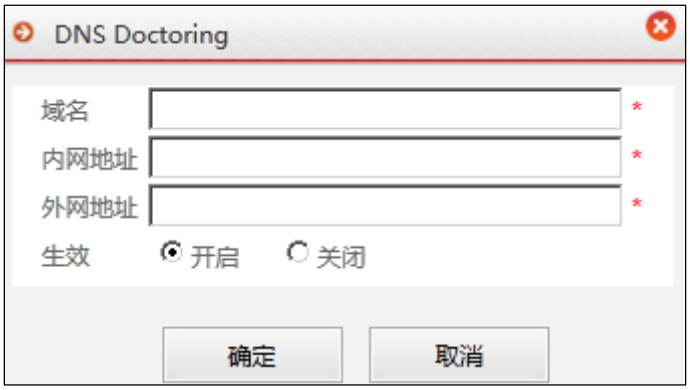
此外，当内网中有多台服务器对外提供相同服务时，通过配置多条 DNS Doctoring（同一域名对应不同的内网服务器真实 IP 地址），可实现内网资源服务器的负载均衡。

下面介绍如何配置 DNS Doctoring。

WEBUI 方式配置

步骤 1 选择 **网络管理** > **智能 DNS**，激活“DNS Doctoring”页签。

步骤 2 点击『添加』，如下图所示。



在配置 DNS Doctoring 时，各项参数的具体说明如下表所示。

参数	说明
域名	必选项，设置域名。
外网地址	必选项，配置该域名对应的公网 IP 地址。
内网地址	必选项，配置该域名对应的私网 IP 地址。
生效	设置 DNS Doctoring 是否生效。选择“开启”表示生效，选择“关闭”表示不生效。

说明

✧ N 个内网资源服务器使用一个域名对外提供服务时，只需添加 N 个域名相同而内网 IP 地址不同的 DNS Doctoring，即可轻易实现服务器的负载均衡。

步骤 3 参数配置完成后，点击【确定】按钮完成 DNS Doctoring 的添加。

CLI 方式配置

dns doctoring add name <*string*> **inside** <*ipaddress1*> **outside** <*ipaddress2*> [**enable** <yes|no>]

命令描述：

添加 DNS Doctoring。

参数说明：

dns doctoring add	添加 DNS Doctoring。
name	必选项，设置域名。
string	字符串类型。
inside	必选项，设置域名对应的内网 IP 地址。
ipaddress1	IP 地址字符串。
outside	必选项，设置域名对应的外网 IP 地址。

ipaddress2	IP 地址字符串。
enable	可选项，是否启用该 DNS Doctoring。
yes|no	是|否

以下是添加 DNS Doctoring 的示例：

配置域名 www.xxxx.com.cn 对应的私有 IP 为地址 10.0.0.2，公有 IP 地址为 2.2.2.3。

TopsecOS#**dns doctoring add name** *www.xxxx.com.cn* **inside** *10.0.0.2* **outside** *2.2.2.3* **enable** yes

dns doctoring show <cr>

命令描述：

显示 DNS Doctoring。

以下是显示 DNS Doctoring 的示例：

TopsecOS# **dns doctoring show**

ID 10994 dns doctoring add name www.sohu1.com inside 10.0.0.3 outside 2.2.2.2 enable yes

ID 10995 dns doctoring add name www.sohu1.com inside 10.0.0.10 outside 3.3.3.3 enable yes

ID 11487 dns doctoring add name www.xxxx.com inside 192.168.99.10 outside 200.20.20.20 enable yes

dns doctoring clean <cr>

命令描述：

清除 DNS Doctoring。

以下是清除 DNS Doctoring 的示例：

TopsecOS# **dns doctoring clean**

7 安全策略

安全策略是网络安全设备的基本功能，控制安全域间或不同地址段间的流量转发。安全策略则通过策略规则决定从一个（多个）安全域到另一个（多个）安全域/从一个地址段到另一个地址段的哪些流量该被允许，哪些流量该被拒绝。

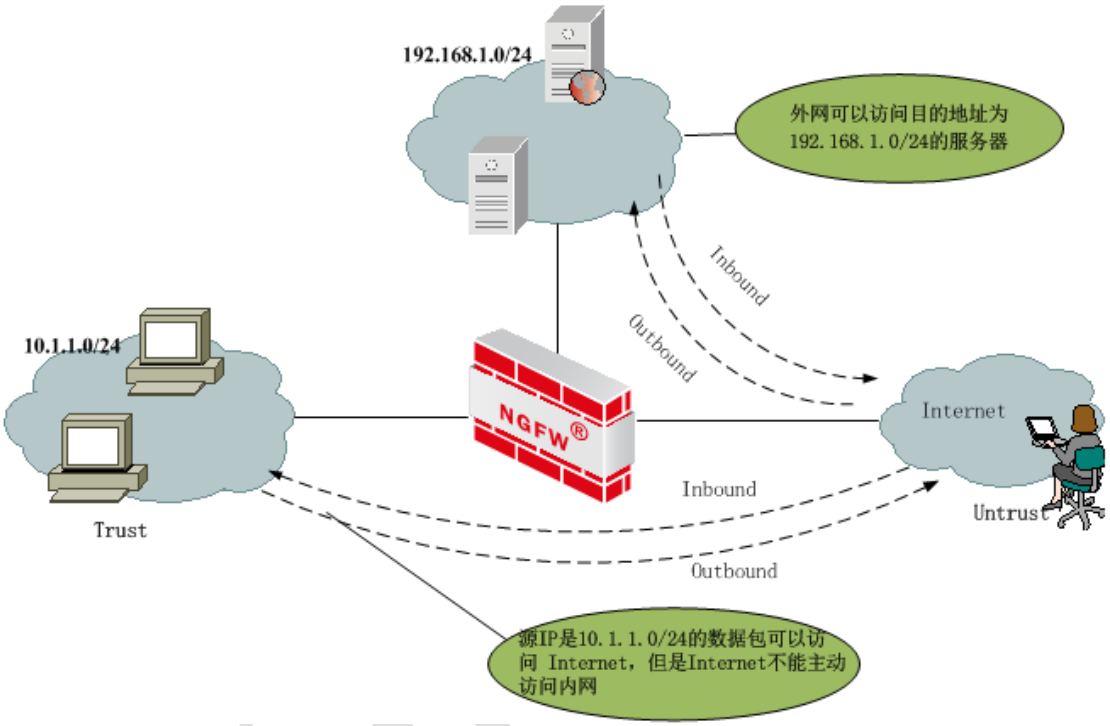


图 7-1 安全策略的规则示意图

NGFW 的基本作用是保护特定网络免受“不信任”的网络的攻击，但是同时还必须允许两个网络之间可以进行合法的通信。安全策略的作用就是对通过 NGFW 的数据流进行检验，符合安全策略的合法数据流才能通过 NGFW。

随着技术的发展，安全策略大致分为几个阶段：

- 基于访问控制规则的包过滤
  - 通过在域间引用访问控制规则实现包过滤
  - 匹配条件：报文头的五元组和时间段
  - 动作：拒绝和允许报文通过
- 融合 UTM 的安全策略（包过滤+UTM）
  - 在包过滤基础上增加 UTM 处理，包括 IPS/AV/URL 过滤等

- 动作为“允许”的报文继续进行 UTM 处理，通过 UTM 检测的报文才真正允许通过
- 功能叠加，应用没有添加到策略的匹配条件中

➢ 一体化安全策略（五元组+应用+用户）

- 真正的一体化策略，可一次识别流量的应用类型、携带的内容等数据，供内容安全功能使用
- 增加应用、用户两个匹配条件，解决了基于端口、IP 识别流量不准确的问题
- 应用、内容、威胁感知能力增强

NGFW 实现了基于五元组、用户和应用的一体化安全策略，并结合内容、安全引擎等多个维度的识别将模糊的网络环境映射为实际的业务环境，从而细粒度的管理与控制通过设备的各种数据报文中隐藏的攻击等，实现精准的访问控制和安全检测。

通过 NGFW 提供的安全策略模块，管理员可以将访问控制规则与资源对象相关联，从而实现对指定对象（包括区域、地址、时间、服务、应用、服务器和均衡组）细粒度的访问控制。通过安全策略模块中的地址转换策略，管理员可以控制内外网之间的访问，如限制外网用户对内网服务器的直接访问等。通过流量控制策略，管理员可以对通过设备的流量进行管理和控制，合理分配带宽资源。通过本机服务，管理员可以根据设备本身提供的管理服务或者信息服务，配置对本机端口的访问控制规则。同时，安全策略模块还提供了入侵防御、DDOS 防御、URL 过滤、内容过滤、文件过滤和病毒过滤的安全引擎策略，为网络提供了全面、高效的安全保护。

NGFW 将数据报文的属性与安全策略的条件进行匹配，若所有条件都匹配，则此流量成功匹配安全策略，若其中有一个条件不匹配则未匹配安全策略。

同一域内应用多条安全策略时，优先级高的安全策略优先匹配数据报文。若数据报文匹配到了一条策略就不再继续匹配剩下的策略，若没有匹配到任何策略就按系统默认规则进行处理。

说明

- ✧ 一般情况下，每对安全区域之间的通信都会受到阻止，直至至少添加一个规则后，才允许在两个区域之间进行通信。
- ✧ 对于同一条数据流只有首包匹配安全策略并建立会话，后续包都匹配会话转发。即在访

问发起的方向上应用安全策略。

本章内容主要包括：

- 对象：主要介绍如何添加防火墙的对象资源，用于在配置安全策略时进行引用。
- 访问控制：主要介绍如何配置防火墙的访问控制策略，并应用已配置好的入侵防御、URL 过滤、内容过滤、文件过滤和病毒过滤规则。
- 地址转换：主要介绍 NAT 转换规则应用场景及其在防火墙。
- 流量控制：主要介绍如何在防火墙上配置访流量控制策略及实现原理。
- 本机服务：主要介绍如何根据需求配置防火墙的本机服务功能开启或者关闭。
- ALG：主要介绍如何配置防火墙应用协议的的 ALG 功能开启或者关闭。
- 入侵防御：主要介绍如何配置防火墙的入侵防御规则。
- DDoS 防御：主要介绍如何配置防火墙的 DDoS 防御功能。
- URL 过滤：主要介绍如何配置防火墙的 URL 过滤功能。
- 内容过滤：主要介绍如何配置防火墙的内容过滤功能。
- 文件过滤：主要介绍如何配置防火墙的文件过滤功能。
- 病毒过滤：主要介绍如何配置防火墙的病毒过滤功能。

7.1 对象

对象，是具备某些公共特征的一些实例的集合，是安全策略的重要组成部分。安全策略中的条件和访问控制行为等都是通过对象定义的，安全策略可以看成是基于对象（组）的规则。

某一对象资源可以被其他对象所引用，合理地构建和管理对象资源能够大大简化管理员对 NGFW 的管理工作，当某个对象发生变化时，管理员只需要修改对象本身即可，而无需逐一地修改所有引用该资源的策略或规则。

在 NGFW 中，管理员可以定义的资源对象的类型包括：

- 区域对象：通过与接口绑定，定义区域的访问权限。

- 地址对象：包括主机对象、地址范围对象、子网对象、MAC 地址对象和地址组。
- 时间对象：包括循环时间对象、单次时间对象和时间组。
- 服务对象：包括 NGFW 预定义的服务对象、管理员自定义的服务对象和服务组。
- 应用对象：包括 NGFW 预定义的应用对象、管理员自定义的应用对象和应用组。
- 服务器：定义服务器对象及其权重。
- 均衡组：定义服务器组及其负载均衡方式。

说明

- 对象名称不允许出现的特殊字符：空格、'、"、\、;、"、$、&、@、%、|、~、 <、>、#、+、!、=、^、?、`。
- NGFW 支持对对象进行重命名操作。
- 对对象进行修改时，如果对象被访问控制规则引用，则修改对象后进行保存时，系统会进行策略冲突检查，如果对对象的修改导致和已有策略冲突，则将拒绝相应修改。

7.1.1 区域

区域，设置接口所属的安全域，是一个或多个接口的集合，以供内容安全、流量控制等模块调用。NGFW 通过区域划分网络、标识报文的传输路径，当报文在不同的区域之间进行传输时，触发安全策略的检查。

NGFW 支持区域对象的设置，管理员可以根据实际情况，将网络划分为不同的安全区域，并根据其不同的安全需求，定义相应的规则进行区域边界防护。如果不存在可匹配的访问控制规则，NGFW 将根据目的接口所在区域的权限处理该报文。关于访问控制规则的设置具体请参见 7.2.2 配置访问控制规则。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **区域**。

步骤 2 点击『添加』，弹出“区域”窗口。

在设置区域对象时，各项参数的具体说明如下表所示。

参数	说明
区域名称	必选项，设置区域对象名称。
描述	设置必要的说明信息。最多可输入 256 个字节。
接口	必选项，选择与该区域绑定的接口属性，可同时选择一个或多个接口属性。 说明： 1）接口属性的设置请参见 6.2 接口； 2）如果接口属性较多，可以在“成员”右侧的文本框中输入关键字，点击“🔍”图标后，接口属性成员列表中与该关键字匹配的成员将被筛选出来。

步骤 3 点击【确定】按钮完成区域对象的添加。

CLI 方式配置

define area add name <*string1*> **interface** <*string2*> [**comment** <*string3*>]

命令描述

添加一个区域对象。

参数说明

define area add	添加一个区域对象。
name	必选项，设置区域对象名称。
string1	字符串类型，表示区域名称。
interface	必选项，指定接口。
string2	字符串类型，表示设备接口。
comment	可选项，设置对区域对象的具体说明。
string3	字符串类型。

使用说明：

所谓**区域**，就是一段具有相似安全属性的网络空间，对于 NGFW 来说，访问控制规则引用区域来做访问控制。

以下是添加区域对象的示例：

添加一个与接口 feth0 绑定的区域 area_feth0。

```
TopsecOS# define area add name area_feth0 interface feth0 comment
comment_content
```

define area delete name <*string*>

命令描述

删除一个区域对象。如果该区域被规则引用，则无法删除。

参数说明

define area delete	删除一个区域对象。
name	必选项，指定要删除的区域对象名称。
string	字符串类型，表示区域对象名称。

使用说明：

如果所删除的区域属于某个虚系统（带有虚系统号），删除时就必须在命令行中指定相应的虚系统号。

以下是删除指定区域对象的示例：

```
TopsecOS# define area delete name area_feth 0
```

define area show [**name** <*string*>]

命令描述

显示 NGFW 系统中的区域对象。

参数说明

define area show	显示区域对象。
name	可选项，指定要显示的区域对象名称。
string	字符串类型，表示区域名称。

以下是显示 NGFW 系统中所有区域对象的示例：

```
TopsecOS# define area show
ID 10065 define area add name area_feth0 interface 'feth0 ' refered 5
ID 10066 define area add name 23 interface 'feth0 ' comment ' ' refered 2
ID 10067 define area add name 3453525 interface 'feth3 ' comment ' ' refered 0
```

7.1.2 地址

地址是 IPv4 地址或 IPv6 地址的集合，地址组是地址的集合。在 NGFW 系统中，地址是 NGFW 多个功能模块配置的重要组成元素，比如访问控制规则、地址转换规则以及会话数限制等，它包含一个或若干个 IPv4 或 IPv6 地址，只需定义一次即可被各种策略规则多次引用。

按照网络地址的表达方式，可以将四种类型的地址加入到地址中：

- 主机地址：可以唯一标识网络中的主机。
- 连续的 IP 地址范围：若干个主机 IP 的集合，这些 IP 地址是连续的。
- 子网地址：若干个主机 IP 的集合，它与连续的 IP 地址范围的区别在于：不是通过起始 IP 和终止 IP 来指定地址范围，而是通过 IP 地址和网络掩码来共同确定。如子网地址“192.168.1.0/24”，表示 IP 范围为“192.168.1.1-192.168.1.255”。
- MAC 地址：（Media Access Control）地址也叫硬件地址，是收录在网卡里的识别网络节点的标识，具有全球唯一性。MAC 地址采用十六进制数表示，共六个字节（48 位）。

说明

✧ 地址（地址组）的成员可以是 IPv4 地址、IPv6 地址，也可以同时将 IPv4 地址和 IPv6 地址加入地址（地址组）。

当地址包含的成员越来越多时，地址的管理变得很复杂，如一个地址的不同子集有可能被不同的策略引用，如果每个策略都要配置一个地址，地址的数目会越来越多。因此，NGFW 支持地址组功能，地址组是一个集合，成员可以是主机地址、连续的 IP 地址范围、网段地址和已经定义好的地址或地址组。与地址相比，地址组增强了资源对象管理的层次性，提高了地址管理的灵活度。

7.1.2.1 地址对象

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **地址**，激活“地址”页签。

步骤 2 点击『添加』，弹出“地址属性”窗口，如下图所示。

➢ 添加主机地址对象

添加主机地址对象的界面如上图所示。

在添加主机地址对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置主机对象的名称。
主机地址	必选项，地址类型选择“主机”，在文本框中输入该主机对象的 IP 地址。 说明： 主机地址支持 IPv6 版本，格式为：xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。

➢ 添加地址范围对象

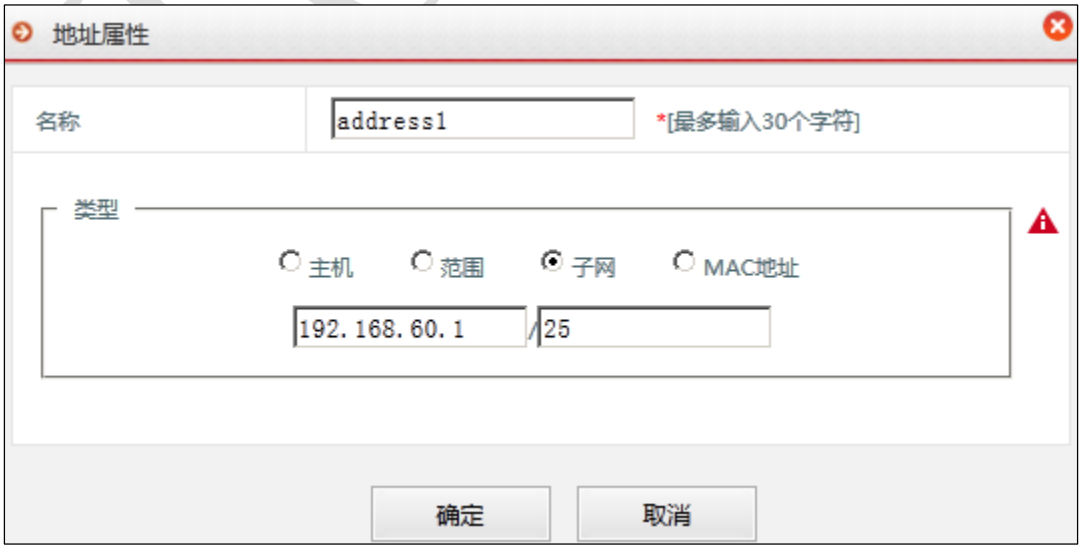
添加地址范围对象的界面如下图所示。

在添加地址范围对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置地址范围对象的名称。
地址范围	必选项，地址类型选择“范围”，在文本框中输入地址范围的起始 IP 地址和终止 IP 地址。 说明： 地址范围的起始 IP 和终止 IP 地址支持 IPv6 版本，格式为：xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。

➢ 添加子网地址对象

添加子网地址对象的界面如下图所示。

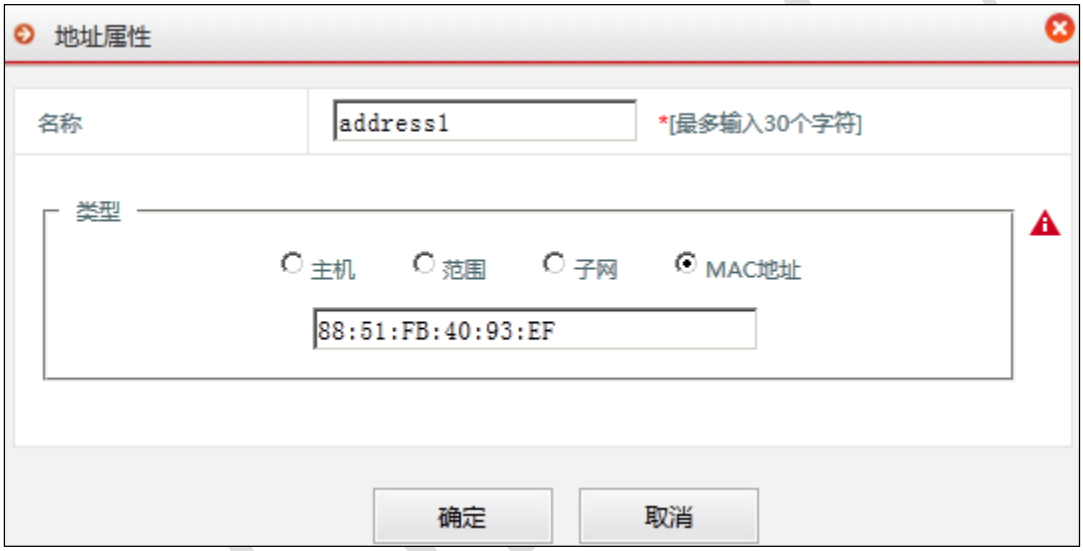


在添加子网地址对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置子网地址对象的名称。
子网地址	必选项，地址类型选择“子网”，在文本框中输入子网对象的 IP 地址和子网掩码地址。 说明： 子网地址支持 IPv6 版本，格式为： xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx。

- 添加 MAC 地址对象

添加 MAC 地址对象的界面如下图所示。



在添加 MAC 地址对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置 MAC 地址对象的名称，用于在 NGFW 中唯一标识该 MAC 地址对象。 名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。
MAC 地址	必选项，地址类型选择“子网”，在文本框中输入设备的 MAC 地址。

步骤 3 点击【确定】按钮完成地址对象的添加。

CLI 方式配置

- 主机地址对象

define host add name <*string1*> **ipaddr** <*string2*>

命令描述

添加一个主机地址对象。

参数说明

define host add	添加一个主机对象。
name	必选项，设置要添加的主机对象的名称。
string1	字符串类型，表示主机对象名称。
ipaddr	可选项，设置主机对象的 IP 地址。
string2	字符串类型，表示 IP 地址，格式为：192.168.1.6，可以为一个或多个 IP 地址，多个时用单引号括起来，之间用空格分隔’192.168.83.1 192.168.1.6’。

以下是添加主机对象的示例：

添加一个主机 host1，并设定其 IP 地址为 192.168.1.8。

TopsecOS# **define host add name** *host1* **ipaddr** *192.168.1.8*

define host show [**name** <*string*>]

命令描述

查看所有主机地址对象。

参数说明

define host show	查看所有主机对象。
name	可选项，指定要查看的主机对象的名称。
string	数值类型，表示主机名称。

以下是查看主机对象的示例：

TopsecOS# **define host show**

ID 10063 define host add name 123 ipaddr '1.1.1.1' refered 1

ID 10064 define host add name add ipaddr '127.0.0.1' refered 0

ID 10185 define host add name host1 ipaddr '127.0.0.1' refered 0

define host delete [**id** <*number*>] [**name** <*string*>]

命令描述

删除一个主机对象。如果该对象被规则引用，则无法删除。

参数说明

define host delete	删除一个主机对象。
id	可选项，指定要删除的主机对象对应的 ID 号。
number	数值类型，表示主机对象的 ID 号。
name	可选项，指定要删除的主机对象的名称。
string	字符串类型，表示主机对象名称。

使用说明：

在删除主机对象时，既可根据主机对象的名称来删除，又可以通过主机地址对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除**未被策略引用的**主机地址对象。

以下是删除主机对象的示例：

删除主机对象 host1。

```
TopsecOS# define host delete name host1
```

- 地址范围对象

define range add name <*string1*> **ip1** <*string2*> **ip2** <*string3*>

命令描述

添加一个地址范围对象。

参数说明

define range add	添加地址范围对象。
name	必选项，设置地址范围对象的名称。
string1	字符串类型，表示地址范围对象的名称。
ip1	必选项，设置地址范围的起始 IP 地址。
sting2	字符串类型，表示 IP 地址，格式为 x.x.x.x 或 x:x:x:x:x:x:x:x，比如 192.168.1.254 或 2014::3。
ip2	必选项，设置地址范围的结束 IP 地址。
string3	字符串类型，表示 IP 地址，格式为 x.x.x.x 或 x:x:x:x:x:x:x:x，比如 192.168.1.254 或 2014::3。

使用说明：

ip1 的参数值应不大于 ip2 的参数值，否则就会出现错误提示。

在 NGFW 的缺省配置已经有一个范围对象 any：0.0.0.0-255.255.255.255

同一时刻，应该是地址范围内所有地址各自的连接数不能大于该并发连接数。

以下是添加地址范围对象的示例：

添加地址范围对象 range1，其地址范围为：172.16.1.10-172.16.1.80。

TopsecOS# **define range add name** *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.80*

define range modify name <*string1*> [**ip1** <*string2*>] [**ip2** <*string3*>]

命令描述

修改一个地址范围资源对象。

参数说明

define range modify	修改一个地址范围资源对象。
name	必选项。指定待修改的地址范围对象。
string1	字符串类型，表示地址范围对象名称，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
ip1	可选项。设置地址范围的起始 IPv4 或 IPv6 地址。
string2	字符串类型，表示 IPv4 或 IPv6 地址。
ip2	可选项。设置地址范围的结束 IPv4 或 IPv6 地址。
string3	字符串类型，表示 IPv4 或 IPv6 地址。

以下是修改一个地址范围资源对象的示例：

修改 range1 对象的 IPv4 地址范围为：172.16.1.10-172.16.1.90。

TopsecOS# **define range modify name** *range1* **ip1** *172.16.1.10* **ip2** *172.16.1.90*

define range delete [**name** <*string*>] [**id** <*number*>]

命令描述

根据名称或 ID 号删除未被引用的地址范围资源对象。

参数说明

define range delete	根据名称或 ID 号删除未被引用的地址范围资源对象。
name	可选项，设置待删除的地址范围资源对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
id	可选项，设置待删除的地址范围资源对象的 ID 号。
number	数值类型。

使用说明：

在删除地址范围对象时，既可根据地址范围对象的名称来删除，又可以通过地址范围对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

以下是根据名称删除地址范围资源对象的示例：

删除地址范围对象 range1。

TopsecOS# **define range delete name** *range1*

define range show [**name** <*string*>]

命令描述

显示地址范围资源对象。

参数说明

define range show	显示地址范围资源对象。
name	可选项，按名字显示某个地址范围资源对象。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

以下是显示地址范围资源对象的示例：

TopsecOS# **define range show** ID 8011 define range add name r1 ip1 172.16.1.10 ip2 172.16.1.80 refered 0 ID 8012 define range add name r2 ip1 1111::2 ip2 2222::2 refered 0 TopsecOS# **define range show name** *r2* ID 8012 define range add name r2 ip1 1111::2 ip2 2222::2 refered 0

define range clean <cr>

命令描述

清空地址范围资源对象。

以下是清空地址范围资源对象的示例：

```
TopsecOS# define range clean
```

- 子网地址对象

define subnet add name <*string1*> **ipaddr** <*string2*> [**mask** <*netmask*>]

命令描述

添加一个子网地址对象。

参数说明

define subnet add	添加一个子网地址对象。
name	必选项。设置待添加的子网地址对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
ipaddr	必选项。设置子网 IPv4 或 IPv6 地址。
string2	字符串类型。IPv4 子网地址格式为 x.x.x.x/x，例如 192.168.0.1/24。 IPv6 中子网用前缀表示，格式为 xxxx::xxxx/x，例如 2014::1/64。
mask	可选项，设置子网掩码，用来判断任意两个 IP 地址是否属于同一子网络。
netmask	字符串类型，表示 IPv4 子网掩码，例如 255.255.255.0。如果采用 IPv6 地址，不需输入该参数。

以下是添加一个子网地址对象的示例：

添加子网对象 subnet1，其子网地址为：192.168.10.1，掩码为：255.255.255.0。

```
TopsecOS# define subnet add name subnet1 ipaddr 192.168.10.1 mask
255.255.255.0
```

define subnet delete [**name** <*string*>] [**id** <*number*>]

命令描述

根据名称或 ID 号删除未被引用的子网地址对象。

参数说明

define subnet delete	根据名称或 ID 号删除未被引用的子网地址对象。
name	可选项，设置待删除的子网地址对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

id	可选项，设置待删除的子网对象对应的 ID 号。
number	数值类型。

使用说明：

在删除子网对象时，既可根据子网对象的名称来删除，又可以通过子网对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

以下是根据名称删除子网资源对象的示例：

删除子网对象 subnet1。

```
TopsecOS# define subnet delete name subnet1
```

define subnet show [**name** <*string*>]

命令描述

显示所有的子网资源对象。

参数说明

define subnet show	显示所有的子网资源对象。
name	可选项，按名字显示某个子网资源对象。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

以下是显示所有的子网资源对象的示例：

```
TopsecOS# define subnet show
ID 8008 define subnet add name subnet1 ipaddr 192.168.20.0/24    refered 0
ID 8009 define subnet add name subnet2 ipaddr 2200::1/64 refered 0
ID 8010 define subnet add name subnet3 ipaddr 192.168.0.1/24    refered 0

TopsecOS# define subnet show name subnet2
ID 8009 define subnet add name subnet2 ipaddr 2200::1/64 refered 0
```

define subnet clean <cr>

命令描述

清空所有未被引用的子网资源对象。

- MAC 地址对象

define mac add name <*string1*> **macaddr** <*string2*>

命令描述

添加 mac 地址资源对象。

参数说明

define mac add	添加 mac 地址资源对象。
name	必选项。设置 mac 地址资源对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
macaddr	必选项，设置待添加的 mac 地址 资源对象的 mac 地址。
string2	字符串类型，格式为 aa:bb:cc:dd:ee:ff。

以下是添加 mac 地址资源对象的示例：

TopsecOS# **define mac add name** *address1* **macaddr** *11:22:33:44:55:66*

define mac modify name <*string1*> [**macaddr** <*string2*>]

命令描述

修改 mac 地址资源对象。

参数说明

define mac modify	修改 mac 地址资源对象。
name	必选项。设置待修改的 mac 地址资源对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
macaddr	可选项，设置修改后的 mac 地址。
string2	字符串类型，格式为 aa:bb:cc:dd:ee:ff。

以下是修改 mac 地址资源对象的示例：

将 mac 地址资源对象 address1 的地址修改为 00:08:2E:1A:06:80。

TopsecOS# **define mac modify name** *address1* **macaddr** *00:08:2E:1A:06:80*

define mac delete [**name** <*string*>] [**id** <*number*>]

命令描述

删除 mac 地址资源对象。

参数说明

define mac delete	删除 mac 地址资源对象。
name	可选项。设置待删除的 mac 地址资源对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
id	可选项，设置待删除的 mac 地址资源对象的 ID 号。
number	数值类型，表示 ID 号。

以下是删除 mac 地址资源对象的示例：

TopsecOS# **define mac delete name** *address1*

define mac show <cr>

命令描述

显示 mac 地址资源对象。

以下是显示 mac 地址资源对象的示例：

TopsecOS# **define mac show**

ID 8002 define mac add name address1 macaddr 11:22:33:44:55:66 refered 0

define mac clean <cr>

命令描述

清空 mac 地址资源对象。

7.1.2.2 地址组对象

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **地址**，激活“地址组”页签。

步骤 2 点击『添加』，弹出“地址属性”窗口。

在添加地址组对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置地址组对象名称。
地址组成员	必选项，选择地址对象，可同时选择一个或多个地址对象。

步骤 3 点击【确定】按钮完成地址组对象的添加。

CLI 方式配置

步骤	配置命令	配置说明
1	**define host add name** <*string1*> **ipaddr** <*string2*>	配置地址对象
2	**define group_address add name** <*string1*> [**member** <*string2*>]	配置地址组对象

define group_address add name <*string1*> [**member** <*string2*>]

命令描述

添加一个地址组对象。

参数说明

define group_address add	添加地址组对象。
name	必选项，设置地址组对象的名称。
string1	字符串类型，表示地址组对象的名称。
member	可选项，设置地址组对象中的成员。
string2	字符串类型，表示地址对象，可以是已经定义的主机对象、子网对象或地址范围对象。

使用说明：

在定义地址组之前，可以先定义地址对象，关于地址对象的定义请参考相关章节。

以下是添加地址组对象的示例：

添加地址组对象 groupaddr1，其成员为已定义的主机对象 host1。

TopsecOS# **define host add name** *host1* **ipaddr** *192.168.16.3*

TopsecOS# **define group_address add name** *groupaddr1* **member** *host1*

define group_address show <cr>

命令描述

查看所有地址组对象。

以下是查看所有地址组对象的示例：

```
TopsecOS# define group_address show
ID 10181 define group_address add name ad12    refered 0
ID 10183 define group_address add name ad34    refered 0
```

define group_address delete [**id** <*number*>] [**name** <*string*>]

命令描述

删除一个地址组对象。如果该对象被规则引用，则无法删除。

参数说明

define group_address delete	删除一个地址组。
id	可选项，指定要删除的地址组对象对应的 ID 号。
number	数值类型，表示地址组对象的 ID 号。
name	可选项，指定要删除的地址组的名称。
string	字符串类型，表示地址组名称。

使用说明：

在删除地址组对象时，既可根据地址组对象的名称来删除，又可以通过地址组对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除所有**未被引用的**地址组对象。

以下是删除指定地址组对象的示例：

删除地址组 groupaddr1。

```
TopsecOS# define group_addrees delete name groupaddr1
```

define group_address clean <cr>

命令描述

删除所有未被引用的地址组对象。

以下是清除 NGFW 系统上的所有未被引用的地址组对象的示例：

```
TopsecOS# define group_address clean
```

7.1.3 时间

NGFW 可以定义一些时间对象，即定义一些时间段的组合，基于时间对数据包进行细粒度的访问控制、流量控制，使其选择设置好的时间段定义，以设定这些规则生效或失效的时间。比如，管理员可以针对工作时间和非工作时间设置不同的访问控制规则。NGFW 支持的时间分为循环时间对象、单次时间对象和时间组。

循环时间是指以日、周、月为单位的循环时间段，设备将在这个指定的时间段循环执行某项规则；单次时间是指任意某一特定时段，设备将在指定的时间范围启动某项规则，且只会被执行一次；时间组是循环时间或者单次时间的逻辑组合。

7.1.3.1 循环时间对象

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **时间**，激活“循环时间”页签。

步骤 2 点击『添加』，弹出“循环时间对象”窗口。

在添加循环时间对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置循环时间对象名称，用于在 NGFW 中唯一标识该循环时间对象。 名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
生效时间	必选项，循环时间段可以分为每日、每周、每月。 1）选择每日时，设置每天的起始时间和结束时间； 2）选择每周时，设置每周的生效日以及当天的起始时间和结束时间； 3）选择每月时，设置每月的生效起始日及其起始时间、结束日及其结束时间。

步骤 3 点击【确定】按钮完成循环时间对象的添加。

7.1.3.2 单次时间对象

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **时间**，激活“单次时间”页签。

步骤 2 点击『添加』，弹出“单次时间对象”窗口。

在添加单次时间对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，输入单次时间对象名称，用于在 NGFW 中唯一标识该单次时间对象。 名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
开始时间	必选项，设置从具体某天的某个时刻开始算起。 说明： 点击文本框后面的“”，弹出日期选择工具，选择开始日期及相应的具体时间，时间输入格式为 24 小时制。
结束时间	必选项，设置到具体某天的某个时刻为止。 说明： 点击文本框后面的“”，弹出日期选择工具，选择结束日期及相应的具体时间，时间输入格式为 24 小时制。

步骤 3 点击【确定】按钮完成单次时间对象的添加。

CLI 方式配置

define schedule add name <*string1*> **cyctype** *year* **sdate** <*string2*> **edate** <*string3*> [**stime** <*string4*>] [**etime** <*string5*>] [**time_unit** <*string6*>]

命令描述

添加年时间对象。对于包含年的时间对象，它代表的是具体的某一个时间点，因此需要精确到秒，使用 stime 和 etime 参数。

参数说明

define schedule add	添加时间对象。
name	必选项。指定待添加的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的

	任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
year	单次按年循环。year 用于单次时间对象。
sdate	可选项。设置待添加的时间对象的开始日期。
string2	字符串类型，格式为“年-月-日”，YY-MM-DD。例如：2010-10-01。
edate	可选项。设置待添加的时间对象的结束日期。
string3	字符串类型，格式为“年-月-日”，YY-MM-DD。例如：2010-10-30。
stime	可选项，设置待添加的时间对象的开始时间。
string4	字符串类型，格式为“小时:分钟:秒”，HH:MM:SS。例如：00:00:00。默认为“00:00:00”。
etime	可选项，设置待添加的时间对象的结束时间。
string5	字符串类型，格式为“小时:分钟:秒”，HH:MM:SS。例如：23:59:59。默认为“23:59:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string6	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是添加年时间对象的示例：

添加一个 2010 年 10 月 1 号上午 10：30 到 2010 年 10 月 31 号上午 10：59：59 的时间对象。

TopsecOS# **define schedule add name** *test* **sdate** *2010-10-01* **edate** *2010-10-31* **time_unit** *1* **cyctype** *year* **stime** *10:30:00* **etime** *10:59:59*

TopsecOS# **define schedule show**

ID 8001 define schedule add name test cyctype yearcyc sdate 2010-10-01 stime 10:30:00 edate 2010-10-31 etime 10:59:59 refered 0

define schedule add name <*string1*> **cyctype** *monthcyc* [**month** <*string2*>] [**start** <*string3*>] [**stop** <*string4*>] [**time_unit** <*string5*>]

命令描述

添加月时间对象。对于按月循环的时间对象，不需要精确到秒，使用 start 和 stop 参数。

参数说明

define schedule add	添加时间对象。
name	必选项。设置待添加的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的

	任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
monthcyc	按月循环。monthcyc 用于多次时间对象。
month	可选项。添加按月循环的时间对象时表示一个月的某一天。
string2	字符串类型。默认为不限制。例如：“20”代表每月 20 号，“1-20”代表每月 1 到 20 号。
start	可选项，设置待添加的时间对象的开始时间。
string3	字符串类型，格式为“小时:分钟”，HH:MM。例如：00:00。默认为“00:00”。
stop	可选项，设置待添加的时间对象的结束时间。
string4	字符串类型，格式为“小时:分钟”，HH:MM。例如：23:59。默认为“23:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string5	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是添加月时间对象的示例：

添加一个每月 20 号 10：00 到 10：30 的时间对象。

TopsecOS# **define schedule add name** *test1* **month** *20* **start** *10:00* **stop** *10:30* **cyctype** *monthcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8001 define schedule add name test1 cyctype monthcyc month 20 start 10:00 stop 10:30 refered 0

define schedule add name <*string1*> **cyctype** *weekcyc* [**week** <*string2*>] [**start** <*string3*>] [**stop** <*string4*>] [**time_unit** <*string5*>]

命令描述

添加周时间对象。对于按周循环的时间对象，不需要精确到秒，使用 start 和 stop 参数。

参数说明

define schedule add	添加时间对象。
name	必选项。设置待添加的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
weekcyc	按周循环。weekcyc 用于多次时间对象。
week	可选项，添加按周循环的时间对象时表示一周的某

	一天。
string2	字符串类型。默认为不限制。例如：“5”代表周五。“1234”代表周一周二周三周四。
start	可选项，设置待添加的时间对象的开始时间。
string3	字符串类型，格式为“小时:分钟”，HH:MM。例如：00:00。默认为“00:00”。
stop	可选项，设置待添加的时间对象的结束时间。
string4	字符串类型，格式为“小时:分钟”，HH:MM。例如：23:59。默认为“23:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string5	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是添加时间对象的示例：

添加一个每周五 10：00 到 10：30 的时间对象。

TopsecOS# **define schedule add name** *test2* **week** *5* **start** *10:00* **stop** *10:30* **cyctype** *weekcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8001 define schedule add name test2 cyctype weekcyc week '5' start 10:00 stop 10:30 refered 0

define schedule modify name <*string1*> **cyctype** *year* **sdate** <*string2*> **edate** <*string3*> [**stime** <*string4*>] [**etime** <*string5*>] [**time_unit** <*string6*>]

命令描述

修改年时间对象。对于包含年的时间对象，它代表的是具体的某一个时间点，因此需要精确到秒，使用 stime 和 etime 参数。

参数说明

define schedule modify	修改时间对象。
name	必选项。设置待修改的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
year	单次按年循环。year 用于单次时间对象。
sdate	可选项，设置待修改的时间对象的开始日期。
string2	字符串类型，格式为“年-月-日”，YY-MM-DD。例如：2010-10-01。
edate	可选项，设置待修改的时间对象的结束日期。
string3	字符串类型，格式为“年-月-日”，YY-MM-DD。例

	如：2010-10-30。
stime	可选项，设置待修改的时间对象的开始时间。
string4	字符串类型，格式为“小时:分钟:秒”，HH:MM:SS。例如：00:00:00。默认为“00:00:00”。
etime	可选项，设置待修改的时间对象的结束时间。
string5	字符串类型，格式为“小时:分钟:秒”，HH:MM:SS。例如：23:59:59。默认为“23:59:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string6	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是修改年时间对象的示例：

修改一个 2010 年 10 月 1 号上午 10：30 到 2010 年 10 月 31 号上午 10：59：59 的时间对象 test 为 2014 年 10 月 1 号上午 11：00 到 2014 年 12 月 31 号 14：00。

TopsecOS# **define schedule add name** *test* **sdate** *2010-10-01* **edate** *2010-10-31* **time_unit** *1* **cyctype** *year* **stime** *10:30:00* **etime** *10:59:59*

TopsecOS# **define schedule show**

ID 8000 define schedule add name test cyctype yearcyc sdate 2010-10-01 stime 10:30:00 edate 2010-10-31 etime 10:59:59 refered 0

TopsecOS# **define schedule add name** *test* **sdate** *2014-10-01* **edate** *2014-12-31* **time_unit** *1* **cyctype** *year* **stime** *11:00:00* **etime** *10:59:59*

TopsecOS# **define schedule show**

ID 8000 define schedule add name test cyctype year sdate 2014-10-01 stime 11:00:00 edate 2014-12-31 etime 10:59:59 refered 0

define schedule modify name <*string1*> **cyctype** *monthcyc* **month** <*string2*> [**start** <*string3*>] [**stop** <*string4*>] [**time_unit** <*string5*>]

命令描述

修改月时间对象。对于按月循环的时间对象，不需要精确到秒，使用 start 和 stop 参数。

参数说明

define schedule modify	修改时间对象。

name	必选项。设置待修改的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
monthcyc	按月循环。monthcyc 用于多次时间对象。
month	可选项，修改按月循环的时间对象时表示一个月的某一天。
string2	字符串类型。默认为不限制。例如：“20”代表每月 20 号，“1-20”代表每月 1 到 20 号。
start	可选项，设置待修改的时间对象的开始时间。
string3	字符串类型，格式为“小时:分钟”，HH:MM。例如：00:00。默认为“00:00”。
stop	可选项，设置待修改的时间对象的结束时间。
string4	字符串类型，格式为“小时:分钟”，HH:MM。例如：23:59。默认为“23:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string5	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是修改月时间对象的示例：

修改一个每月 20 号 10：00 到 10：30 的时间对象 test1 为每月 10 号 14：00-14：59。

TopsecOS# **define schedule add name** *test1* **month** *20* **start** *10:00* **stop** *10:30* **cyctype** *monthcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8001 define schedule add name test1 cyctype monthcyc month 20 start 10:00 stop 10:30 refered 0

TopsecOS# **define schedule modify name** *test1* **month** *20* **start** *10:00* **stop** *10:30* **cyctype** *monthcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8001 define schedule add name test1 cyctype monthcyc month 10 start 14:00 stop 14:59 refered 0

define schedule modify name <*string1*> **cyctype** *weekcyc* [**week** <*string2*>] [**start** <*string3*>] [**stop** <*string4*>] [**time_unit** <*string5*>]

命令描述

修改周时间对象。对于按周循环的时间对象，不需要精确到秒，使用 start 和 stop 参数。

参数说明

define schedule modify	修改时间对象。
name	必选项。指定待修改的时间对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
cyctype	必选项。设置循环类型，默认为“按周循环”。
weekcyc	按周循环。weekcyc 用于多次时间对象。
week	可选项，修改按周循环的时间对象时表示一周的某一天。
string2	字符串类型。默认为不限制。例如：“5”代表周五。“1234”代表周一周二周三周四。
start	可选项，设置待修改的时间对象的开始时间。
string3	字符串类型，格式为“小时:分钟”，HH:MM。例如：00:00。默认为“00:00”。
stop	可选项，设置待修改的时间对象的结束时间。
string4	字符串类型，格式为“小时-分钟”，HH:MM。例如：23:59。默认为“23:59”。
time_unit	可选项，设置单位时间，以半小时为单位。如果小于 15 分钟按 0 小时算；如果大于等于 15 分钟按 0.5 小时算。
string5	字符串类型。1 或 30 分钟，默认为 1 分钟。

以下是修改时间对象的示例：

修改一个每周五 10：00 到 10：30 的时间对象 test2 为每周六 14：00-15：00。

TopsecOS# **define schedule add name** *test2* **week** *5* **start** *10:00* **stop** *10:30* **cyctype** *weekcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8002 define schedule add name test2 cyctype weekcyc week '5' start 10:00 stop 10:30 refered 0

TopsecOS# **define schedule modify name** *test2* **week** *5* **start** *10:00* **stop** *10:30* **cyctype** *weekcyc* **time_unit** *1*

TopsecOS# **define schedule show**

ID 8002 define schedule add name test2 cyctype weekcyc week '6' start 14:00 stop 15:00 refered 0

define schedule delete [**name** <*string*>] [**id** <*number*>]

命令描述

按名称或 ID 号删除未被引用的时间对象。

参数说明

define schedule delete	按名称或 ID 号删除未被引用的时间对象。
name	可选项，设置待删除的时间对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
id	可选项，设置待删除的时间对象的 ID 号。
number	数值类型。

以下是按名称删除时间对象的示例：

```
TopsecOS# define schedule delete name test
```

define schedule show [**type** <cycle|single>] [**name** <*string*>]

命令描述

显示时间对象。

参数说明

define schedule show	显示时间对象。
type	可选项，设置时间对象的类型。
cycle	显示所有循环类型的时间对象。
single	显示所有单次类型的时间对象。
name	可选项，按名字显示某个时间对象。
string	字符串类型，表示时间对象的名字。不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

以下是显示时间对象的示例：

显示所有循环类型的时间对象。

```
TopsecOS# define schedule show type cycle
ID 8001 define schedule add name sch1 cyctype weekcyc week '1234567' start 12:00
stop 14:00 refered 0
```

define schedule clean [**type** <cycle|single>]

命令描述

清空时间对象。可选择清空循环或单次时间对象。

参数说明

define schedule clean	清空时间对象。
type	可选项，设置时间对象的类型。
cycle	清空所有循环类型的时间对象。
single	清空所有单次类型的时间对象。

以下是清空时间循环对象的示例：

```
TopsecOS# define schedule clean type cycle
```

7.1.3.3 时间组对象

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **时间**，激活“时间组”页签。

步骤 2 点击『添加』，弹出“添加时间组”窗口。

在添加时间组对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置时间组对象名称，用于在 NGFW 中唯一标识该时间组对象。名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
时间成员	必选项，选择时间对象，时间组中可以同时包括循环时间对象和单次时间对象。

步骤 3 点击【确定】按钮完成时间组对象的添加。

CLI 方式配置

步骤	配置说明
1	配置时间对象，具体请参见 7.1.3.1 循环时间对象、7.1.3.2 单次时间对象。
2	配置时间组对象

define group_schedule add name <*string1*> [**member** <*string2*>]

命令描述

添加时间组对象。

参数说明

define group_schedule add	添加一个时间组对象。
name	必选项，设置时间组对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
member	可选项，设置成员对象名称。成员对象必须是服务对象、地址对象或时间对象。
string2	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

以下是添加时间组对象的示例：

TopsecOS# **define schedule add name** *test* **cyctype** weekcyc **start** *10:30* **stop** *22:10*

TopsecOS# **define group_schedule add name** *g1* **member** *test*

TopsecOS# **define group_schedule show**

ID 8003 define group_schedule add name g1 member 'test' refered 0

define group_schedule modify name <*string1*> [**member** <*string2*>]

命令描述

修改时间组对象。

参数说明

define group_schedule modify	修改时间组对象。
name	必选项。设置时间组对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
member	可选项，设置成员对象名称。成员对象必须是服务对象、地址对象或时间对象。
string2	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

以下是修改时间组对象的示例：

为时间组对象 TIME 添加成员对象 time1。

TopsecOS# **define schedule add name** *time1* **cyctype** weekcyc **start** *10:30* **stop** *22:10*

```
TopsecOS# define group_schedule add name TIME
TopsecOS# define group_schedule modify name TIME member time1
```

define group_ schedule delete [**name** <*string*>] [**id** <*number*>]

命令描述

根据名称或 ID 号删除未被引用的时间组对象。

参数说明

define group_ schedule delete	根据名称或 ID 号删除未被引用的时间组对象。
name	可选项，设置时间组对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
id	可选项，设置时间组对象的 ID 号。
number	数值类型。

以下是根据名称删除时间组对象的示例：

删除名称为 g1 的时间组对象。

```
TopsecOS# define group_schedule delete name g1
```

define group_ schedule show <cr>

命令描述

显示时间组对象。

以下是显示时间组对象的示例：

```
TopsecOS# define group_schedule show
ID 8003 define group_schedule add name g1 member 'test' refered 0
```

define group_ schedule clean <cr>

命令描述

清空时间组对象。

以下是清空时间组对象的示例：

```
TopsecOS# define group_schedule clean
```

7.1.4 服务

服务是具有协议标准的信息流，通过协议类型、协议端口号等特征来确定应用协议类型，是一个或若干个服务的集合。服务组是各种服务的集合。

7.1.4.1 服务对象

服务对象是 NGFW 多个功能模块配置的重要组成元素，比如访问控制规则、地址转换规则、流量控制策略等，便于 NGFW 管理员根据不同的服务指定策略规则。服务对象由协议类型和协议端口号组成，分为以下三类：

- 预定义服务：系统预定义的一些常用服务；
- 自定义服务：根据自身业务的需要自定义的服务和端口号；
- 服务组：系统服务和自定义服务的逻辑集合。

WEBUI 方式配置

- 预定义服务

为方便对用户网络中不同服务的访问控制，系统预先定义了 194 条常见服务供用户在设置访问控制规则时使用。对于这些预定义的服务，用户不可以进行修改和删除，只能通过在左侧导航树中选择 **安全策略** > **对象** > **服务**，激活“预定义服务”页签来进行查看。

- 自定义服务

为实现对网络中某种服务进行访问控制，但在系统没有预先定义该服务，用户可以根据需要自行定义服务，然后设置 ACL 规则对自定义服务进行控制。

步骤 1 选择 **安全策略** > **对象** > **服务**，激活“自定义服务”页签。

步骤 2 点击『添加』，弹出“添加服务对象”窗口。

在设置自定义服务对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置自定义服务对象名，用于在 NGFW 中唯一标识自定义服务对象。 名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
描述	输入自定义服务对象的描述信息。
类型	必选项，表示自定义服务使用的协议类型，可选项：TCP、UDP、ICMP 和其他 IP 协议。
端口	当“类型”选择 TCP、UDP、ICMP 时显示该选项。用于输入自定义服务对象占用的单个端口或端口范围，前后两个文本框分别表示起始和终止端口号。如果是单个端口则只填写起始端口。 说明： 当协议类型为 TCP 或 UDP 时，可输入的数值取值范围：0-65535；当协议类型为 ICMP 时，可输入的数值取值范围：0-18。
协议号	当协议类型为“其他 IP 协议”时，界面显示该项。端口可输入的数值取值范围：1-255。

点击【确定】按钮完成自定义服务对象的添加。

CLI 方式配置

define service add name <*string1*> **protocol** <*number1*> [**port1** <*number2*>] [**port2** <*number3*>] [**comment** <*string2*>]

命令描述

添加一个服务对象。

参数说明

define service add	添加一个服务对象。
name	必选项，设置服务对象名称。
string1	字符串类型，表示自定义服务对象的名称，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
protocol	必选项，设置 3 层或 4 层协议号。
number1	数值类型，表示协议码。
port1	可选项，设置服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口。如果为 ICMP 协议，则表示类型范围。取值范围：0-18。
number2	数值类型，表示起始端口号或 ICMP 协议类型。
port2	可选项，设置服务的结束端口。
number3	数值类型，表示结束端口号。
comment	可选项，设置备注内容。
string2	字符串类型，表示备注内容。

使用说明：

服务分为系统提供的缺省服务和用户自定义服务，对于缺省服务用户无法进行添加、删除、修改等操作。

以下是添加服务对象的示例：

添加服务对象 http8080，设置协议号为 6、端口号为 8080。

```
TopsecOS# define service add name http8080 protocol 6 port1 8080
```

define service modify name <*string1*> [**protocol** <*number1*>] [**port1** <*number2*>] [**port2** <*number3*>] [**comment** <*string2*>]

命令描述

修改一个自定义服务对象。

参数说明

define service modify	修改服务对象。
name	必选项。指定要修改的服务对象的名称。
string1	字符串类型，表示自定义服务对象的名称，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
protocol	可选项，重新设置 3 层或 4 层协议号。
number1	数值类型，表示协议码。
port1	可选项，修改服务的起始端口，只有一个端口时只须设置起始端口，不用设置结束端口。如果为 ICMP 协议，则表示类型范围。取值范围：0-18。
number2	数值类型，表示起始端口号或 ICMP 协议类型。
port2	可选项，修改服务的结束端口。
number3	数值类型，表示结束端口号。
comment	可选项，修改备注内容。
string2	字符串类型，表示备注内容。

以下是修改服务对象的示例：

将服务对象 http8080 的端口号改为 8000。

```
TopsecOS# define service add name http8080 protocol 6 port1 8080
TopsecOS# define service modify name http8080 port1 8000
```

define service delete id <*number*>| **name** <*string*>

命令描述

删除一个自定义服务对象。

参数说明

define service delete	删除服务对象。
id	可选项，指定要删除的服务对象对应的 ID 号。
number	数值类型，表示服务对象的 ID 号。
name	可选项，指定要删除的服务对象的名称。
string	字符串类型，表示服务对象名称，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。

使用说明：

在删除服务对象时，既可根据服务对象的名称来删除，又可以通过服务对象的 id 来删除，也可以同时指定 id 和 name，但是当两者不一致时以名称为准。

当不指定任何参数时，删除未被策略引用的服务对象。

以下是删除服务对象的示例：

删除服务对象 http8000。

```
TopsecOS# define service delete name http8000
```

define service clean <cr>

命令描述

清空所有未被引用的自定义服务对象。

define service show [**name** <*string*>] [**type** <custom|default>]

命令描述

查看所有服务对象信息。

参数说明

define service show	查看所有服务对象信息。
name	可选项，按名称显示某个服务对象的信息。
string	字符串类型，表示服务对象名称，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
type	可选项，按类型查看服务对象信息。
custom|default	自定义服务对象|预定义服务对象

以下是查看所有服务对象的示例：

```
TopsecOS# define service show
ID 8001 define service add name http8080 protocol 6 port1 8080 refered 0
```

7.1.4.2 服务组对象

管理员可以灵活地将几个系统预定义或自定义服务组合在一个服务组中。在设置策略规则时引用服务组，即可以实现对该服务组中的所有服务对象进行控制管理。

NGFW 服务组有以下特征：

- 服务对象中的每一条服务都可以被一个或多个服务组引用；
- 每个服务组中既可以包含预定义服务，也可以包含用户自定义服务。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **服务**，激活“服务组”页签。

步骤 2 点击『添加』，弹出“添加服务组”窗口。

在添加服务组时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置服务组对象名，用于在 NGFW 中唯一标识该服务组对象。名称中不能包含如下特殊字符：%、\、’、 <、>、’、&、“。最多输入 30 个字符。
服务组成员	必选项。选择服务组成员。服务组中可以同时包括系统定义服务对象和用户自定义服务对象。

步骤 3 点击【确定】按钮完成服务组对象的添加。

CLI 方式配置

步骤	配置说明
1	配置自定义服务对象（可选），具体请参见 7.1.4.1 服务对象
2	配置服务组对象

define group_service add name <*string1*> **member** <*string2*>

命令描述

添加服务组对象。定义服务组对象之前，需先定义服务对象。

参数说明

define group_ service add	添加服务组对象。
name	必选项。设置服务组对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
member	可选项，设置成员对象名称。此处的服务可以是用户自定义的服务，也可以是系统的默认服务。
string2	字符串类型，表示服务名称。

以下是添加服务组对象的示例：

添加服务组对象 goupservice1，并将服务 http8080 作为成员加入该服务组。

TopsecOS# **define group_service add name** *groupservice1* **member** *http8080*

define group_service modify name <*string1*> **member** <*string2*>

命令描述

修改服务组对象。

参数说明

define group_ service modify	修改服务组对象。
name	必选项。设置服务组对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
member	可选项，设置成员对象名称。此处的服务可以是用户自定义的服务，也可以是系统的默认服务。
string2	字符串类型，表示服务名称。

以下是修改服务组对象的示例：

修改服务组对象 groupservice1，并将服务 http8080 作为成员加入该服务组。

TopsecOS# **define group_service modify name** *groupservice1* **member** *http8080*

define group_service delete [**name** <*string*>] [**id** <*number*>]

命令描述

删除服务组对象。

参数说明

define group_ service delete	删除服务组对象。
name	可选项，设置服务组对象名称。
string	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
id	可选项，设置待删除服务组对象的 ID 号。
number	数值类型。

以下是删除服务组对象的示例：

删除服务组对象 groupservice2。

```
TopsecOS# define group_service delete name groupservice2
```

define group_service show <cr>

命令描述

显示服务组对象。

以下是显示服务组对象的示例：

```
TopsecOS# define group_service show
ID 8015 define group_service add name g1 member 'http8080' refered 0
```

define group_service clean <cr>

命令描述

清空服务组对象。

7.1.5 应用

应用对象，作为访问控制规则中的过滤条件之一，使 NGFW 能够针对各种应用进行数据报文的监控，比如禁止视频、禁止 WEB 下载、允许 WEB 浏览等。

应用对象还可以应用到流量控制中，实现基于应用的精细流量控制。关于流量控制的设置具体请参见 7.4 流量控制。

NGFW 可以对各种类型的应用层的流量进行检测和控制：既支持传统的应用层协议，也支持各种新的应用类型，如财经软件类应用、即时通讯类应用、网上银行类应

用、网络游戏类应用、语音电话类应用、P2P 下载类应用、网络视频类应用、其他流量应用等。同时，NGFW 还支持通过自定义应用来扩展新的应用类型。

应用类型一共分为 23 个大类（称为“父类”），每个大类中又分为若干个小的分类（称为“子类”），点击父类协议左侧的箭头“▷”，可以查看子类协议的详细信息。

7.1.5.1 预定义应用

为方便对网络中不同应用的访问控制，系统预先定义了 23 种类型的常见应用供管理员在设置访问控制规则时使用。对于这些预定义的应用，管理员不可以进行修改和删除。

WEBUI 方式配置

选择 **安全策略** > **对象** > **应用**，激活“预定义”页签，查看系统预定义应用，如下图所示。

CLI 方式配置

ai obj cat show id <*number*>

命令描述

根据应用大类 ID 获取该大类的信息。

参数说明

ai obj cat show id	必选项，根据应用大类 ID 获取该大类的信息。
number	数值类型，表示大类 ID 号。

以下是根据应用大类 ID 获取该大类的信息的示例：

显示 ID 号为 1 的应用类别对象。

```
TopsecOS# ai obj cat show id 1
ID 8000 name: C-1    id: 1    flag: 0x0 appcount: 0 protocount: 0 enCatName:
P2P_Download         cnCatName: P2P 下载  custom:0 valid:0 customson:0
```

ai obj cat search <allvalid|preall|prevalid|custom|customson>

命令描述

搜索应用大类信息。

参数说明

ai obj cat search	搜索应用大类信息。
allvalid|preall|prevalid|custom|customson	枚举类型。 allvalid：所有有效的，策略引用界面使用。 preall：所有预定义的，调试使用。 prevalid：所有预定义，且是有效的，预定义界面使用。 custom：自定义的，保存使用。 customson：子自定义，即其下存在自定义应用或协议，并且该预定义大类是有效的，自定义列表使用。

以下是搜索应用大类信息的示例：

```
TopsecOS# ai obj cat search allvalid
ID 8000 name: C-1    id: 1    flag: 0x4 appcount: 0 protocount: 4 enCatName:
P2P_Download              cnCatName: P2P 下载  custom:0 valid:0 customson:1
ID 8001 name: C-2    id: 2    flag: 0x0 appcount: 0 protocount: 0 enCatName:
P2P_Audio                 cnCatName: P2P 音频  custom:0 valid:0 customson:0
ID 8002 name: C-3    id: 3    flag: 0x0 appcount: 0 protocount: 0 enCatName:
P2P_Video                 cnCatName: P2P 视频  custom:0 valid:0 customson:0
ID 8003 name: C-4    id: 4    flag: 0x4 appcount: 0 protocount: 1 enCatName: IM
cnCatName:  即时通讯  custom:0 valid:0 customson:1
```

```
ID 8004 name: C-5    id: 5    flag: 0x0 appcount: 0 protocount: 0 enCatName: VoIP
cnCatName:  语音电话  custom:0 valid:0 customson:0
ID 8005 name: C-6    id: 6    flag: 0x0 appcount: 0 protocount: 0 enCatName:
Online_Bank                  cnCatName:  网上银行  custom:0 valid:0 customson:0
ID 8006 name: C-7    id: 7    flag: 0x0 appcount: 0 protocount: 0 enCatName:
Electronic_Commerce       cnCatName:  电子商务  custom:0 valid:0 customson:0
ID 8007 name: C-8    id: 8    flag: 0x0 appcount: 0 protocount: 0 enCatName:
Finance_SoftWare          cnCatName:  财经软件  custom:0 valid:0 customson:0
ID 8008 name: C-9    id: 9    flag: 0x0 appcount: 0 protocount: 0 enCatName: Games
cnCatName:  网络游戏  custom:0 valid:0 customson:0
```

ai obj app show id <*number*>

命令描述

显示指定 ID 的应用对象。

参数说明

ai obj app show id	根据应用 ID 获取该应用信息。
number	数值类型，表示应用 ID 号。

以下是显示应用对象的示例：

显示 ID 号为 1 的应用对象信息。

```
TopsecOS# ai obj app show id 1
ID 8023 name: A-1      id: 1      catid: 8      flag: 0x0 protocount: 0 enAppName:
DaZhiHui          cnAppName:  大智慧                    shared
```

ai obj app search type <allvalid|preall|prevalid|custom|customson> [**catid** <*number*>]

命令描述

搜索应用信息，当输入 catid 时，将搜索到指定大类下的信息；若不输入 catid，或大类 id 为 0 时，则搜索指定类型应用信息。

参数说明

ai obj app search	搜索应用信息。

type	
allvalid|preall|prevalid|custom|customson	枚举类型。 allvalid：所有有效的，策略引用界面使用。 preall：所有预定义的，调试使用。 prevalid：所有预定义，且是有效的，预定义界面使用。 custom：自定义的，保存使用。 customson：子自定义，即其下存在自定义应用或协议，并且该预定义大类是有效的，自定义列表使用。
catid	可选项，设置应用对象所属的大类 ID 号。
number	数值类型。

以下是搜索应用信息的示例：

显示类型为 allvalid 的应用对象。

```
TopsecOS# ai obj app search type allvalid
ID 8023 name: A-1      id: 1      catid: 8      flag: 0x0 protocount: 0 enAppName:
DaZhiHui              cnAppName: 大智慧                    shared
ID 8024 name: A-2      id: 2      catid: 13     flag: 0x0 protocount: 0 enAppName:
ND_119                cnAppName: 119 网盘                  shared
ID 8025 name: A-3      id: 3      catid: 13     flag: 0x0 protocount: 0 enAppName:
ND_163                cnAppName: 163 网盘                  shared
ID 8026 name: A-4      id: 4      catid: 6      flag: 0x0 protocount: 0 enAppName:
China_Citic_Bank      cnAppName: 中信银行                  shared
ID 8027 name: A-5      id: 5      catid: 6      flag: 0x0 protocount: 0 enAppName:
China_GuangFa_Bank    cnAppName: 广发银行                  shared
ID 8028 name: A-6      id: 6      catid: 1      flag: 0x0 protocount: 0 enAppName:
BT                    cnAppName: BT                        shared
ID 8029 name: A-7      id: 7      catid: 2      flag: 0x0 protocount: 0 enAppName:
KuWo                  cnAppName: 酷我音乐盒                shared
ID 8030 name: A-8      id: 8      catid: 1      flag: 0x0 protocount: 0 enAppName:
eDonkey               cnAppName: 电驴                      shared
ID 8031 name: A-9      id: 9      catid: 6      flag: 0x0 protocount: 0 enAppName:
PingAn_Bank           cnAppName: 平安银行                  shared
```

```
ID 8032 name: A-10      id: 10      catid: 6      flag: 0x0 protocount: 0 enAppName:
ICBC                    cnAppName:  工商银行                shared
ID 8033 name: A-11      id: 11      catid: 6      flag: 0x0 protocount: 0 enAppName:
SPD_Bank                cnAppName:  浦发银行                shared
```

ai obj proto show id <*number*>

命令描述

根据协议 ID 获取该协议信息。

参数说明

ai obj proto show id	根据协议 ID 获取该协议信息。
number	数值类型。

以下是根据协议 ID 获取该协议信息的示例：

显示 ID 号为 1 的应用协议对象信息。

```
TopsecOS# ai obj proto show id 1
ID 8689 name: P-1       id: 1       flag: 0x0 enProName: DaZhiHuiHangQing
 cnProName:  大智慧行情              CatId: 8    AppId: 1        shared
```

ai obj proto search type <allvalid|preall|prevalid|custom|customson> [**appid** <*number*>]

命令描述

搜索协议信息，当输入 **appid** 时，将搜索到指定应用下的协议信息；若不输入 **appid**，或 **appid** 为 0 时，则搜索指定类型应用下的协议信息。

参数说明

ai obj proto search type	搜索协议信息
allvalid|preall|prevalid|custom|customson	枚举类型。 allvalid：所有有效的，策略引用界面使用。 preall：所有预定义的，调试使用。 prevalid：所有预定义，且是有效的，预定义界面使用。 custom：自定义的，保存使用。 customson：子自定义，即其下存在自定义应用或协议，并且该预定义大类是有效的，自定义列表使用。
appid	可选项，设置应用 ID。
number	数值类型。

以下是搜索协议信息的示例：

显示 ID 号为“2”、协议类型为“allvalid”的应用协议对象信息。

```
TopsecOS# ai obj proto search appid 2 type allvalid
ID 8690 name: P-2       id: 2       flag: 0x0 enProName: ND_119_Login
 cnProName: 119 网盘登录                CatId: 13 AppId: 2        shared
ID 8691 name: P-3       id: 3       flag: 0x0 enProName: ND_119_Upload
 cnProName: 119 网盘上传                CatId: 13 AppId: 2        shared
ID 8692 name: P-4       id: 4       flag: 0x0 enProName: ND_119_Download
 cnProName: 119 网盘下载                CatId: 13 AppId: 2        shared
```

ai obj show objname <*string*>

命令描述

根据对象名称获取该对象对应的大类应用协议信息。

参数说明

ai obj show objname	必选项，根据对象名称获取该对象对应的大类应用协议信息。
string	字符串类型，表示对象名称。

以下是查询对象名称为 A-1 的示例：

```
TopsecOS# ai obj show objname A-1
ID 8023 name: A-1       id: 1       catid: 8       flag: 0x0 protocount: 0 enAppName:
DaZhiHui                          cnAppName: 大智慧                          shared
```

7.1.5.2 自定义应用对象

除了系统自带的应用，NGFW 允许管理员根据特定的需要自行定义应用协议。设置好的自定义应用协议会自动添加到系统规则库中，供管理员在安全策略中设置访问控制规则时引用。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **应用**，激活“自定义”页签。

步骤 2 点击『添加』，弹出“选择”窗口，设置自定义应用。

在配置自定义应用时，各项参数的具体说明如下表所示。

参数	说明
所属大类	必选项，设置自定义应用所属的大类名称。可以选择系统预定义的应用大类名称，也可以新建应用的大类名称。
所属应用	必选项，设置自定义应用所属大类下的应用名称。可以选择系统预定义的应用大类的应用名称，也可以新建应用名称。
协议名称	必选项，设置自定义应用协议的名称。
配置规则	配置该应用匹配的特征规则。关于规则的配置具体请参见 配置规则。

配置规则

在配置自定义规则窗口的规则配置页面中，点击『添加』，弹出“规则”窗口。

在设置规则信息时，各项参数的具体说明如下表所示。

参数	说明
IP 层	设置规则应用的 IP 层，可选项：IPV4、IPV6、Any。
传输层	设置规则应用的传输层，可选项：TCP、UDP、Any。
基于 HTTP	开启该功能后，表示该应用是基于 HTTP 的。
特征规则	设置不同类型的规则特征。可选项：特征字、端口、IP、包长。 说明： 1）包长的格式为特定长度值、长度起始值-长度结束值。 2）端口的格式为（src/dst/any）:指定端口、（src/dst/any）:（端口起始值-端口结束值）。如 src:1025、src:1025-1026。 3）特征字的格式为（str/hex）:距报文首部偏移:特征串内容。如 str:0:user。 4）IP 的格式为（src/dst/any）:地址:子网掩码。如 src:13.10.10.2:24。

步骤 3 点击【确定】按钮完成应用规则的添加。

CLI 方式配置

应用识别引擎的配置和规则管理：可进行大类、应用、协议、规则的添加、修改、删除以及显示。

ai custom cat mod id <*number*> **name** <*string*>

命令描述

修改一个自定义大类。

参数说明

ai custom cat mod	修改自定义大类。
id	必选项，指定大类 ID。
number	数值类型，表示大类 ID。
name	必选项，指定大类名称。
string	字符串类型，表示大类名称。

以下是修改一个自定义大类名称的示例：

TopsecOS# ai custom cat mod id *32* **name** *cat1*

ai custom cat del id <*number*>

命令描述

删除一个自定义大类。

参数说明

ai custom cat del	删除自定义大类。
id	必选项，指定大类 ID。
number	数值类型，表示大类 ID。

以下是删除一个自定义大类的示例：

TopsecOS# ai custom cat del id *32*

ai custom cat show <cr>

命令描述

显示所有自定义大类。

以下是显示所有自定义大类的示例：

TopsecOS# **ai custom cat show**

ID: 8805 ai custom cat add id 32 name cuscat

ai custom app mod id <*number*> **name** <*string*>

命令描述

修改一个自定义应用。

参数说明

ai custom app mod	修改自定义应用。
id	必选项，指定应用 ID。
number	数值类型，表示应用 ID。
name	必选项，指定应用名称。
string	字符串类型，表示应用名称。

以下是修改一个自定义应用的名称的示例：

TopsecOS# ai custom app mod id *8193* **name** *app1*

ai custom app del id <*number*>

命令描述

删除一个自定义应用。

参数说明

ai custom app del	删除自定义应用。
id	必选项，指定应用 ID。
number	数值类型，表示应用 ID。

以下是删除一个自定义应用的示例：

TopsecOS# **ai custom app del id** *8193*

ai custom app show <cr>

命令描述

显示所有自定义应用。

以下是显示所有自定义应用的示例：

TopsecOS# **ai custom app show**

ID 8806 ai custom app add id 8193 name cusapp catid 32

ai custom proto add protoid <*number1*> **protoname** <*string1*> **catid** <*number2*> **catname** <*string2*> **appid** <*number3*> **appname** <*string3*>

命令描述

添加一个自定义协议。

参数说明

ai custom proto add	添加自定义协议。
protoid	必选项，设置协议 ID。
number1	数值类型，表示协议 ID。
protoname	必选项，设置协议名称。
string1	字符串类型，表示协议名称。
catid	必选项，设置大类 ID。
number2	数值类型。表示大类 ID。
catname	必选项，设置大类名称。
string2	字符串类型，表示大类名称。
appid	必选项，设置应用 ID。
number3	数值类型，表示应用 ID。
appname	必选项，设置应用名称。
string3	字符串类型，表示应用名称。

使用说明

当大类 id 和应用 id 不为 0 时（已经存在），那么在输入命令时不需要输入大类和应用的名称；当大类 id 和应用 id 为 0 时（必须同时为 0），必须输入大类和应用名称。

以下是添加一条自定义协议的示例：

TopsecOS# **ai custom proto add protoid** *0* **protoname** *cuspro* **catid** *0* **catname** *cuscat* **appid** *0* **appname** *cusapp*

ai custom proto mod id <*number*> **name** <*string*>

命令描述

修改一个自定义协议。

参数说明

ai custom proto mod	修改自定义协议。
id	必选项，指定协议 ID。
number	数值类型，表示协议 ID。
name	必选项，指定协议名称。
string	字符串类型，表示协议名称。

以下是修改一条自定义协议的示例：

TopsecOS# ai custom proto mod id *8193* **name** *pro1*

ai custom proto del id <*number*>

命令描述

删除一个自定义协议。

参数说明

ai custom proto del	删除自定义协议。
id	必选项，指定协议 ID。
number	数值类型，表示协议 ID。

以下是删除一条自定义协议的示例：

TopsecOS# **ai custom proto del id** *8193*

ai custom proto show <cr>

命令描述

显示所有自定义协议。

以下是显示所有自定义协议的示例：

TopsecOS# **ai custom proto show**

ID 8807 ai custom proto add id 8193 name pro1 catid 32 appid 8193

ai custom rule add protoid <*number*> **l3** <ipv4|ipv6|any> **l4** <tcp|udp|any> **http** <yes|no> **signature** <*string1*> **ip** <*string2*> **port** <*string3*> **paylen** <*string4*>

命令描述

添加一个自定义规则。

参数说明

ai custom rule add	添加自定义规则。
protoid	必选项，设置协议 ID。
number	数值类型，表示协议 ID，协议 ID 必须已经建立的。
l3	必选项，设置三层协议。
ipv4|ipv6|any	三层协议名称。
l4	必选项，设置四层协议。
tcp|udp|any	四层协议名称。
http	必选项，设置是否开启 http 协议识别功能。
yes|no	打开|关闭
signature	必选项，设置特征字。
string1	字符串类型。
ip	必选项，设置 Ip 地址。
string2	点分十进制 Ip 地址字符串类型。

port	必选项，设置端口。
string3	端口字符串类型，可以是一个也可以是一个范围。
paylen	必选项，设置包长。
string4	数值类型，表示包的长度。

使用说明

当 **http** 为 yes 时，支持报文全包扫描，**signature** 中偏移量加特征的长度小于 1460 即可，如果偏移量为-1 则特征为任意位置。Offset 取值范围[-1，0-1460]。

例如：signature str:-1:abcd，报文中任意位置取 abcd 字符串。

当 **http** 为 no 时，支持首尾 64 字节扫描，**signature** 中偏移量加特征的长度小于 64，为首 64 字节特征，如果要取尾 64 字节的特征，则偏移量输入-1（任意位置）。

Offset 取值范围[-1，0-64]。

例如：signature str:60:abcd，报文第 60 个字节处取四个字节为 abcd。

signature 中（特征）str:-1:abcd，最多有 8 个，并且以逗号分隔；而且特征的类型为 hex（十六进制）时，去特征时必须按偶数个十六进制字符来获取。

例如 signature str:-1:abc,hex:-1:1234。

以下是添加一条自定义规则的示例：

TopsecOS# **ai custom rule add protoid** *8193* **http** yes **l3** ipv4 **l4** any **paylen** *11* **port** *src:11* **signature** '*str:23:22222,hex:12:3456*' **ip** *dst:2.2.2.2:24*

ai custom rule mod ruleid <*number1*> **protoid** <*number2*> **l3** <ipv4|ipv6|any> **l4** <tcp|udp|any> **http** <yes|no> **signature** <*string1*> **ip** <*string2*> **port** <*string3*> **paylen** <*string4*>

命令描述

修改一个自定义规则。

参数说明

ai custom rule mod	修改自定义规则。
ruleid	必选项，指定规则 ID。
number1	数值类型，表示规则 ID。
protoid	必选项，设置协议 ID。
number2	数值类型，表示协议 ID，协议 ID 必须已经建立的。
l3	必选项，设置三层协议。
ipv4|ipv6|any	三层协议名称。
l4	必选项，设置四层协议。

tcp|udp|any	四层协议名称。
http	必选项，设置是否开启 http 协议识别功能。
yes|no	打开|关闭
signature	必选项，设置特征字。
string1	字符串类型。
ip	必选项，设置 Ip 地址。
string2	点分十进制 Ip 地址字符串类型。
port	必选项，设置端口。
string3	端口字符串类型，可以是一个也可以是一个范围。
paylen	必选项，设置包长。
string4	数值类型，表示包的长度。

使用说明：

1）当 http 为 yes 时，支持报文全包扫描，Signature 中偏移量加特征的长度小于 1460 即可，如果偏移量为-1 则特征为任意位置。Offset 取值范围[-1,0-1460]。

例如：signature str:-1:abcd,报文中任意位置取 abcd 字符串。

2）当 http 为 no 时，支持首尾 64 字节扫描，Signature 中偏移量加特征的长度小于 64，为首 64 字节特征，如果要取尾 64 字节的特征，则偏移量输入-1（任意位置）。Offset 取值范围[-1,0-64]。

例如：signature str:60:abcd，报文第 60 个字节处取四个字节为 abcd。

3）signature 中（特征）str:-1:abcd，最多有 8 个，并且以逗号分隔；而且特征的类型为 hex（十六进制）时，去特征时必须按偶数个十六进制字符来获取。

例如 signature str:-1:abc,hex:-1:1234。

4）当 **l3** 输入 any 时，ip 地址参数不能填写。

以下是修改一条自定义规则的示例：

TopsecOS# **ai custom rule mod ruleid** *1* **protoid** *8193* **http** yes **l3** ipv4 **l4** any **paylen** *11* **port** *src:11* **signature** '*str:23:22222,hex:12:3456*' **ip** *dst:2.2.2.2:24*

ai custom rule del ruleid <*number1*> **protoid** <*number2*>

命令描述

删除一个自定义规则。

参数说明

ai custom rule del	删除自定义规则。
ruleid	必选项，指定规则 ID。

number1	数值类型，表示规则 ID。
protoid	必选项，指定协议 ID。协议 ID 必须大于 8192。
number2	数值类型，表示协议 ID。

以下是删除一条自定义规则的示例：

```
TopsecOS# ai custom rule del ruleid 1 protoid 8193
```

ai custom rule show <cr>

命令描述

显示所有自定义规则。

以下是显示所有自定义规则：

```
TopsecOS# ai custom rule show
ai custom rule add protoid 8193 ruleid 1 l3 any l4 any http yes    paylen 4-4
ai custom rule add protoid 8194 ruleid 1 l3 ipv4 l4 tcp http yes    paylen 3-3
ai custom rule add protoid 8196 ruleid 1 l3 ipv4 l4 tcp http yes    port any:43-43
ai custom rule add protoid 8197 ruleid 1 l3 ipv4 l4 tcp http yes    paylen 14-14
ai custom rule add protoid 8193 l3 ipv4 l4 any http yes signature
'str:23:22222,hex:12:3456' paylen 11-11 ip dst:2.2.2.2:24 port src:11-11
```

ai custom cat clear <cr>

命令描述

清除不属于对象组的所有自定义大类以及包含的应用及协议。

ai custom app clear <cr>

命令描述

清除不属于对象组的所有自定义应用以及包含的协议。

ai custom proto clear <cr>

命令描述

清除不属于对象组的所有自定义协议。

7.1.5.3 应用组对象

管理员可以灵活地将几个系统预定义或自定义应用组合在一个应用组中。在设置访问控制规则时引用应用组，即可以实现对该应用组中的所有应用对象进行访问控制。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **应用**，激活“应用组”页签。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置应用组对象时，各项参数的具体说明如下表所示。

参数	说明
组名	必选项，设置应用组对象名。 说明： 对象名称不能为 all，因为 all 用于对所有对象组的操作。
应用组成员	选择组成员，应用组中可以同时包括系统定义应用和管理员自定义应用。

步骤 3 点击【确定】按钮完成应用组对象的添加。

说明

- ✧ 管理员可以勾选父类应用，设置对父类中的所有子类的控制策略，也可以分别勾选子类协议，设置对各个子类不同的控制策略。

CLI 方式配置

步骤	配置说明
1	配置自定义应用对象（可选），具体请参见 7.1.5.2 自定义应用对象。
2	配置应用组对象

ai obj group add name <*string1*> **app-obj** <*string2*> **pro-obj** <*string3*> **cat-obj** <*string4*>

命令描述

根据对象名称创建应用对象组。

参数说明

ai obj group add	添加应用组对象。
name	必选项，设置应用组对象名称。
string1	字符串类型。
app-obj	必选项，设置应用名称。必须以 A-开头，数字代表对应的应用 ID，多个应用之间以逗号分隔。
string2	字符串类型。
pro-obj	必选项，设置协议名称。必须以 P-开头，数字代表对应的协议 ID，多个协议之间以逗号分隔。
string3	字符串类型。
cat-obj	必选项，设置应用大类名称。必须以 C-开头，数字代表对应的大类 ID，多个大类之间以逗号分隔。
string4	字符串类型。

使用说明

应用组对象名称不能为 all，因为 all 用于对所有对象组的操作。

以下是创建应用组对象的示例：

添加名称为“test2”支持协议“P-1”的应用组对象。

```
TopsecOS# ai obj group add name tese2 pro-obj P-1
```

ai obj group inc name <*string1*> **app-obj** <*string2*> **pro-obj** <*string3*> **cat-obj** <*string4*>

命令描述

向已添加的应用组对象中添加具体的应用、类别或协议对象。

参数说明

ai obj group inc	增加应用对象组成员。
name	必选项，指定应用对象组。
string1	字符串类型，表示应用组对象名称。
app-obj	必选项，设置应用名称。必须以 A-开头，数字代表对应的应用 ID，多个应用之间以逗号分隔。
string2	字符串类型。
pro-obj	必选项，设置协议名称。必须以 P-开头，数字代表对应的协议 ID，多个协议之间以逗号分隔。
string3	字符串类型。
cat-obj	必选项，设置应用大类名称。必须以 C-开头，数字代表对应的大类 ID，多个大类之间以逗号分隔。
string4	字符串类型。

以下为增加应用对象组成员的示例：

```
TopsecOS#ai obj group inc name t1 cat-obj C-1,C-2 app-obj A-100 pro-obj P-10
```

ai obj group show all <cr>

命令描述

显示所有的应用组对象。

以下是显示所有的应用组对象的示例：

```
TopsecOS# ai obj group show all
Total-Count: 4
**********************************************************************
Group-Name:fuwu                                  Cat-Count:1   App-Count:0
Pro-Count:0       Root-Sys:1
Group-Name:tese                                  Cat-Count:0   App-Count:1
Pro-Count:0       Root-Sys:1
Group-Name:tese1                                 Cat-Count:0   App-Count:1
Pro-Count:1       Root-Sys:1
Group-Name:tese2                                 Cat-Count:1   App-Count:1
Pro-Count:1       Root-Sys:1
**********************************************************************
```

ai obj group delete all <cr>

命令描述

删除所有对象组信息。

以下是删除所有对象组的示例：

```
TopsecOS# ai obj group delete all
```

ai obj group delete name <*string*>

命令描述

根据对象组名称删除指定对象组。

参数说明

ai obj group delete name	必选项，根据指定名称删除对象组。
string	字符串类型，表示应用组对象名称。

以下是删除指定应用对象组的示例：

删除名称为 t1 的应用组对象。

```
TopsecOS# ai obj group delete name t1
```

ai obj group show name <*string*>

命令描述

显示指定名称的应用对象组信息。

参数说明

ai obj group show name	必选项，根据指定名称查询对象组信息。
string	字符串类型，表示应用对象组名称。

以下是显示指定名称的应用组对象的示例：

显示名称为 abc 的应用对象组信息。

```
TopsecOS# ai obj group show name abc
**********************************************************************
Root-Sys: 1
Group-Name: abc
Cat-Num: 0
App-Num: 0
Pro-Num: 1
Pro-IDs: 144
**********************************************************************
```

ai obj group search name <*string1*> **type** <cat|app|pro>

命令描述

根据指定名称和对象组类型显示这一类型的所有成员的信息。

参数说明

ai obj group search	显示应用组对象的成员信息。
name	必选项，指定应用组对象名称。
string1	字符串类型。
type	必选项，指定应用组成员所属的基本协议类型。
cat|app|pro	所属大类|所属应用|协议名称

以下是根据对象组名称和对象组类型显示所有类型成员信息的示例：

TopsecOS# **ai obj group add name** *avgroup1* **app-obj** *A-1* **pro-obj** *P-1* **cat-obj** *C-2*

TopsecOS# **ai obj group search name** *avgroup1* **type** cat

ID 8001 name: C-2 id: 2 flag: 0x0 appcount: 0 protocount: 0 enCatName: P2P_Audio cnCatName: P2P 音频 custom:0 valid:0 customson:0

ai obj desc show <cat|app>

命令描述

指定类型显示对象的描述信息。

以下是显示应用类型对象信息的示例：

TopsecOS# ai obj desc show APP

id: 1 enAppName: DaZhiHui cnAppName: 大智慧 desc:大智慧是一款具有行情显示、分析并同时即时接收信息的证券软件。

id: 2 enAppName: ND_119 cnAppName: 119 网盘 desc:119 网络硬盘是一套使用云计算、分布式处理等高新技术，运行在国际互联网络上的数据（文件）储存系统。

id: 4 enAppName: China_Citic_Bank cnAppName: 中信银行 desc:中信银行通过 Internet 向客户提供开户、查询、对帐、行内转帐、跨行转账、信贷、网上证券、投资理财等传统服务项目。

id: 5 enAppName: China_GuangFa_Bank cnAppName: 广发银行 desc:广发银行通过 Internet 向客户提供开户、查询、对帐、行内转帐、跨行转账、信贷、网上证券、投资理财等传统服务项目。

id: 7 enAppName: KuWo cnAppName: 酷我音乐盒 desc:酷我音乐盒是一款融歌曲和 MV 搜索、在线播放、同步歌词为一体的音乐聚合播放器。

id: 8 enAppName: eDonkey cnAppName: 电驴 desc:eDonkey 是一款 P2P 下载软件,用于共享音乐、电影和软件等资源。

id: 9 enAppName: PingAn_Bank cnAppName: 平安银行 desc:平安银行通过 Internet 向客户提供开户、查询、对帐、行内转帐、跨行转账、信贷、网上证券、投资理财等传统服务项目。

7.1.6 服务器

NGFW 的服务器对象主要应用于负载均衡功能。管理员通过配置服务器的地址及相应的权重值，可以实现不同服务器分担不同大小的数据流量，还可以根据用户需求和灵活的负载均衡方式，将服务器对象划分到不同的均衡组中。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **对象** > **服务器**。

步骤 2 点击『添加』，弹出“添加”窗口，设置服务器对象。

在设置服务器对象时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置服务器名称。
地址	必选项，设置服务器对象的真实 IP 地址。支持 IPv4、IPv6。
权重	数值越大，当根据权重选择负载均衡方式时，该服务器承担的流量就越大。通常情况下根据服务器的性能或处理能力来定义权重，取值范围：1-100；默认值：1。

步骤 3 点击【确定】按钮完成服务器的添加。

CLI 方式配置

define server add name <*string1*> **ipaddr** <*string2*> [**weight** <*string3*>]

命令描述

添加一个服务器对象。

参数说明

define server add	添加服务器对象。
name	必选项。设置待添加的服务器对象名称。
string1	字符串类型，不包含“!@#$%^&+=|?\"\\'> <`~”中的任一字符。
ipaddr	必选项。设置服务器的 IP 地址。
string2	字符串类型，表示 IP 地址。支持 IPv4、IPv6。
weight	可选项，设置服务器的权重。
string3	数值类型，表示服务器的权重，取值范围：1-100。

以下是添加服务器对象的示例：

添加服务器对象 server1，地址为 127.1.1.1，权重为 20。

TopsecOS# **define server add name** *server1* **ipaddr** *127.1.1.1* **weight** *20*

define server show <cr>

命令描述

显示所有服务器对象。

以下是显示服务器对象的示例：

TopsecOS# **define server show**

ID 10068 define server add name 11 ipaddr '127.0.0.1' weight 1 refered 1

define server clean <cr>

命令描述

清空所有未被引用的服务器对象。

7.1.7 均衡组

均衡组，即负载均衡组，将多个服务器对象按照不同方式组合进行负载分配，适用于多个服务器对外提供相同的服务，使用同一个公网 IP 地址，共同分担用户访问流

量的场景。同时，每台服务器亦可单独提供服务，当某个主机发生故障时，负载均衡群集也可以不间断的提供服务。

配置均衡组对象后，当不同用户访问同一个服务器时，NGFW 可将用户的请求分送给了不同的服务器进行处理。这样可以分别利用各个服务器的处理能力，达到流量分担的目的，确保服务器的可用性，实现最佳的网络扩展性。因此，NGFW 提供的均衡组对象能够在满足信息化发展需求的同时极大地提升工作效率。

注意

- ✧ 均衡组中的成员必须是服务器对象，并且包含的服务器对象仅仅能够被一个均衡组引用。关于服务器对象的设置具体请参见 7.1.6 服务器。

WEBUI 方式配置

在配置均衡组之前，需要先进行服务器对象的配置，关于服务器对象的设置具体请参见 7.1.6 服务器。

步骤 1 选择 **安全策略** > **对象** > **均衡组**。

步骤 2 点击『添加』，弹出“均衡组”窗口。

在设置均衡组时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置服务器负载均衡组的名称。
状态	开启状态开关即可启用均衡组对象。
可用服务器	选择要加入此均衡组的服务器对象。
负载均衡方式	设置对多个服务器进行负载分配时所依据的原则。 说明： 1）轮流：当负载均衡组中的所有服务器性能基本相同时，可以选择轮流选择的方式，网络请求会轮流分配给负载均衡组中的服务器； 2）根据权重轮流：根据服务器的权重值来分配服务请求流量。根据权重的负载均衡方式可以保证高性能的服务器负担较多的请求，性能差一点的服务器承担相对少一点的请求； 3）最少连接：记录服务器的当前连接数，将新连接分配到当前连接最少的服务器； 4）加权最少连接：在最少连接方式下根据系统定义的权值分配连接； 5）根据源地址作 HASH 查找：相同的源 IP 地址均衡到相同的服务器；

参数	说明
	6）根据目的地址作 HASH 查找：相同的目的 IP 地址映射到相同的服务器上。

点击【确定】按钮完成服务器均衡组的添加。

CLI 方式配置

步骤	配置命令	配置说明
1	**define server add name** <*string1*> **ipaddr** <*string2*> [**weight** <*string3*>]	配置服务器对象
2	**define virtual_server add name** <*string1*> **enable** <yes|no> [**balance** <rr|wrr|lc|wlc|sh|dh>] [**server** <*string2*>]	配置均衡组对象

define virtual_server add name <*string1*> **enable** <yes|no> [**balance** <rr|wrr|lc|wlc|sh|dh>] [**server** <*string2*>]

命令描述

添加均衡组对象。

参数说明

define virtual_server add	添加均衡组对象。
name	必选项，设置均衡组对象名称。
string1	字符串类型。
enable	必选项，设置是否启用负载均衡。
yes|no	是|否
balance	可选项，设置均衡组对象的均衡算法。
rr|wrr|lc|wlc|sh|dh	轮流|根据权重轮流|最少连接|加权最少连接|根据源地址作 HASH 查找|根据目的地址作 HASH 查找
server	可选项，设置可用真实服务器对象。
string2	字符串类型，表示服务器对象名称。

以下是添加均衡组对象的示例：

添加名称为“*group_serve*”均衡方法为“rr”的均衡组对象，并添加可用服务器“server”。

```
TopsecOS# define server add name server1 ipaddr 192.168.16.5
```

TopsecOS# **define virtual_server add name** *group_server* **enable** yes **balance** rr **server** *server*

define virtual_server show <cr>

命令描述

显示均衡组对象。

以下是显示均衡组对象的示例：

TopsecOS# **define virtual_server show**

ID 10466 define virtual_server add name 3432 enable 'yes' balance 'rr' server '1 1 44' refered 0

7.2 访问控制

实现包过滤的核心技术是使用访问控制列表（Access Control Lists，简称 ACL）。ACL 包含一组指令列表，这些指令列表表明哪些数据包可以接收、哪些数据包需要拒绝。指令列表是由多条访问控制规则组成的。

访问控制规则，是一组管理员自定义的策略，这些规则可以描述满足哪些条件的报文可以通过 NGFW，以及满足哪些条件的报文将被 NGFW 禁止。

7.2.1 原理简介

包过滤的处理过程是先获取需要转发数据包的报文头信息，然后和访问控制规则进行比较，根据比较的结果对数据包进行转发或者丢弃。但由于包过滤只能基于 IP 地址、端口号等控制流量是否可以通过防火墙，无法准确识别应用。

随着防火墙的发展，访问控制越来越精确，NGFW 实现了基于应用、用户和内容的多维度精确的访问控制。

在访问策略中，**策略源**定义了报文的来源，策略源可以是地址（主机、范围、子网、MAC 地址）、区域、用户对象。当报文的源地址属于策略源的范围，则被认为满

足策略源约束条件。**策略目的**定义了报文的目的地址范围，可以包括一个或多个主机、子网、或范围，也可以包括多个区域（或 VLAN）。**策略服务**定义了报文采用的网络协议或特定端口号。**策略应用**定义了报文包含的应用程序。**访问控制**定义了 NGFW 对满足策略的报文所采取的处理方式，包括允许（该报文被允许通过）和禁止（丢弃该包）。同时 NGFW 支持用户定义访问策略有效的时段，即**访问时间**，即在哪一天或哪一时段访问策略有效；支持 IPv6 扩展头的访问控制（逐跳扩展头|分段扩展头|目的扩展头|认证扩展头|路由扩展头|ESP 扩展头）。一个报文和某一条访问策略匹配指的是：报文的源地址包含于策略源定义、报文目的地址包含于策略目的，以及报文端口包含于策略服务，如果定义了访问时间，则报文的接收时间也必须满足策略访问时间约束。只有当一个报文**完全**符合策略中所规定的所有条件时，这条策略才匹配该报文。

NGFW 的资源对象建立后就可以创建访问策略。访问策略分为权限为“允许”和“禁止”的规则。访问控制规则的配置包括规则组添加、规则管理等内容。

7.2.2 配置访问控制规则

NGFW 通过访问控制规则的设置对设备各个接口之间的数据转发进行控制。一般情况下，访问控制规则分为两部分：过滤条件和行为，过滤条件由安全域间流量的源安全域/源地址、目的安全域/目的地址、服务类型、时间等构成。策略规则都有其独有的 ID 号，策略规则 ID 会在定义规则时自动生成。NGFW 的所有策略规则有特定的排列顺序，管理员也可以按照自己的需求设置策略规则的排列位置。策略规则的排列位置可以是绝对位置，即处在首位或者处在末位，也可以是相对位置，即位于某个 ID 之前或之后。在流量进入系统时，系统会对流量按照找到的第一条与过滤条件相匹配的策略规则进行处理。同时，对于定义的策略规则，NGFW 提供了对规则的分组管理功能，不同组之间的前后顺序和组内规则的排列顺序共同决定访问控制规则的匹配顺序。

此外，访问控制规则与安全引擎相结合，并引用安全引擎的策略配置信息，能够使安全网关完成细粒度的应用层访问控制。安全引擎针对不同的应用定义不同的操作，将复杂控制信息简单化，从而简化安全网关的配置。NGFW 支持将五类安全引擎引入访问控制规则，分别是入侵防御、URL 过滤、内容过滤、文件过滤、病毒过滤。

每一类安全引擎可以针对具体应用分别配置不同的控制动作。如果策略中定义了某一类安全引擎策略，则检查报文是否包含相应的内容，如果匹配，则按照该策略规定的处理动作处理该报文。访问控制策略规则的匹配流程如下图所示。

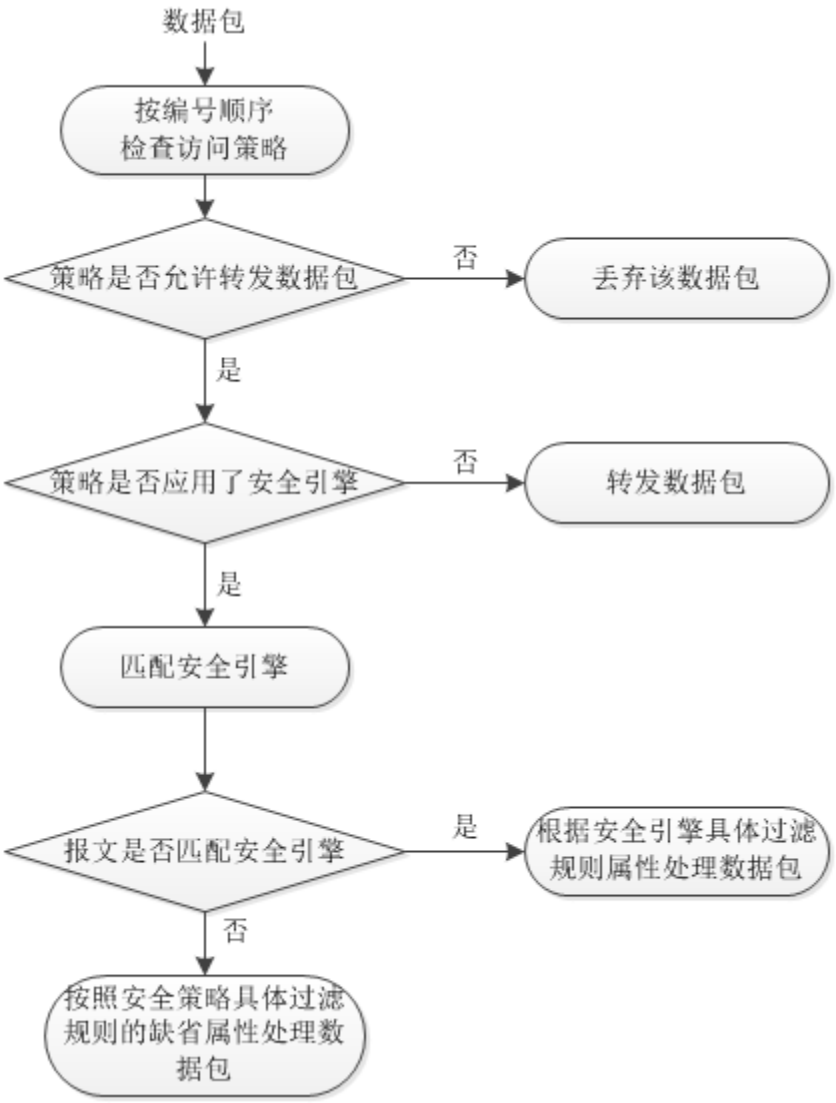


图 7-2 访问控制规则匹配流程图

7.2.2.1 配置访问控制策略

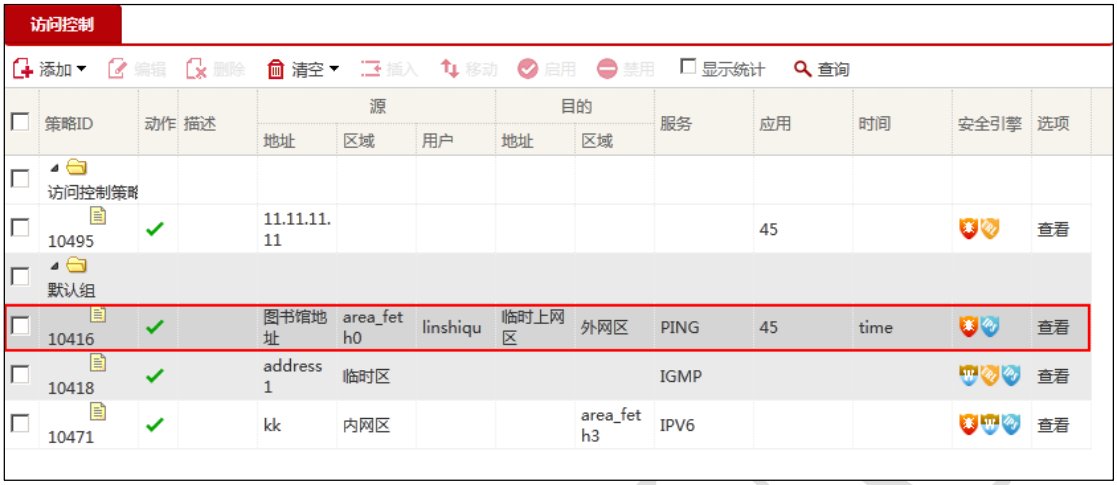
WEBUI 方式配置

在配置访问控制策略之前，需要先进行如下两个步骤：

- 配置对象属性（可选）。关于对象属性的配置具体请参见 7.1 对象。

- 配置安全引擎策略（可选）。关于安全引擎相关策略的配置具体请参见 7.7 入侵防御、7.9URL 过滤、7.10 内容过滤、7.11 文件过滤、7.12 病毒过滤。

步骤 1 选择 **安全策略** > **访问控制**，进入访问控制界面，如下图所示。



界面显示已添加访问控制策略和策略组的基本内容，如策略 ID、地址、区域、服务、应用以及引用的安全引擎策略等。

选中已有访问控制策略，点击『启用』，弹出确定启用当前策略的提示对话框，然后点击【确定】按钮表示该策略被启用；点击『禁用』，弹出确定禁用当前策略的提示对话框，然后点击【确定】按钮表示该策略被禁用，并且该条策略显示深灰色，如上图红框处所示，其余策略均处于启用状态。勾选“显示统计”，界面显示匹配访问控制策略的次数。

步骤 2 添加访问控制策略。

1）点击『添加』，选择“策略”，弹出“添加”窗口。

在设置访问控制规则时，各项参数的具体说明如下表所示。

参数	说明
源	选择对象，设定发起连接的源应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1）区域：选择区域资源限定报文的来源区域。 2）地址：选择已定义的地址资源对象，限定报文的源 IP 地址。 3）用户：选择用户对象或用户组对象。 说明： 1）多个选项设定的条件之间是“与”的关系，数据包的源地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效；

参数	说明
	2）每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可； 3）当没有设置地址对象时，默认表示任意地址； 4）用户组是用户的集合，管理员可以根据用户间的联系将若干用户分为一个用户组。关于用户相关参数的设置具体请参见 5.1 用户管理。
目的	选择对象，设定发起连接的目的应当匹配的条件。可以实现基于哪些条件对报文进行访问控制。当设定多项时，必须同时满足各个条件才匹配该规则。如果不指定，表示任何源地址均匹配该规则。可设定的选项包括： 1）区域：选择区域资源限定报文的目的区域。 2）地址：选择已定义的地址资源对象，限定报文的目的 IP 地址。 说明： 1）多个选项设定的条件之间是“与”的关系，数据包的目的地址在匹配规则的时候必须都要匹配上选择的选项，规则才能生效； 2）每一选项均可选择多个对象，多个对象之间是“或”的关系。只要满足其中一个对象即可； 3）当没有设置地址对象时，默认表示任意地址。
服务	选择服务对象，对数据报文的协议和目的端口号进行限定。如果没有选择任何服务，则系统默认为不对协议和端口号进行限定。
应用	设置匹配该访问控制规则的应用程序。关于应用的介绍和设置具体请参见 7.1.5 应用。 说明： 如果应用程序具有多项功能，则可以选择整个应用程序或个别功能。如果选择整个应用程序，则所有功能均将包含，而且在将来添加功能时会自动更新应用程序定义。
时间	设置该访问控制规则生效的时间段。如果没有选择时间段对象则表示所有时间。
动作	设置对于匹配规则的数据报文采取的操作。可选项：允许、禁止。 当选择“允许”时，表示对于匹配规则的数据报文，允许通过设备。
状态	设置是否启动该访问控制规则。可选项：启用、禁用。
策略组	设置访问控制规则所属的规则组对象。
描述	设置对该访问控制规则的必要描述信息。
长连接	设置是否开启该长连接开关。可选项：开启、关闭；默认值：关闭，即为普通连接。选择“开启”表示该连接永不超时。 说明： 一般来说，网关对通信空闲一定时间的连接将自动断开，以提高安全性和释放通信资源，但某些应用所建立的连接需要长时期保持，即使处于空闲状态。例如 ATM 机器必须和处理中心的服务器一直保持着连接，这个连接必须设置为长连接。
统计	设置是否开启该策略统计开关，可选项：开启、关闭。选择“开启”则可以显示所有策略的匹配情况。

参数	说明
访问控制日志	当数据报文匹配该访问控制规则后，设置是否记录日志。可选项：不记录、记录。
连接日志	设置是否记录设备的会话日志。可选项：记录、不记录。
原始目的地址	为了防止原始目的地址在进行 DNAT 后无法被检测识别，在对数据包的原始目的地址进行访问控制时需要设置该项。
最大活动会话数	设置 NGFW 上的用户或用户访问的应用的最大会话个数。取值范围：0-2147483647。
IPv6 逐跳扩展头	逐跳扩展头位于 IPv6 头之后，包含数据包到达目的地过程中经过的每个节点的检查项。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 逐跳扩展头的数据报文。提高 NGFW 对数据包的处理能力。
IPv6 目的地扩展头	目的地扩展头包含只能由最终目的地节点所处理的选项。目前，只定义了填充选项，将报文头填充为 64 位边界。 开启该项开关后，该条访问控制策略只匹配包含 IPv6 目的地扩展头的数据报文。
IPv6 路由扩展头	路由扩展头指明了数据包在到达目的地过程中将经过的特殊的节点，包含了各节点的地址列表。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 路由扩展头的数据报文。
IPv6 分段扩展头	分段扩展头包括一个分段偏移值、一个“更多段”标志和一个标识字段，用于源节点对长度超出源端和目的端间路径 MTU 的包进行分段。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 分段扩展头的数据报文。
IPv6 认证扩展头	认证扩展头提供了一种机制，对 IPv6 头进行加密的校验。 开启该项开关后，该条访问控制策略只匹配包含 IPv6 认证扩展头的数据报文。
IPv6 ESP 扩展头	ESP 扩展头，即封装安全性净荷扩展头，不进行加密，指明剩余的净荷已经加密，并为已经获得授权的目的节点提供足够的解密信息。 开启该项开关后，该条访问控制规则只匹配包含 IPv6ESP 扩展头的数据报文。
安全引擎	安全引擎包括：入侵防御、URL 过滤、内容过滤、文件过滤、病毒过滤，都可以引用到访问控制策略中。关于安全引擎的配置具体请参见 7.7 入侵防御、7.9URL 过滤、7.10 内容过滤、7.11 文件过滤、7.12 病毒过滤。

说明

- ✧ 数据包的源地址和目的地址在匹配访问控制规则时必须匹配上选择的所有选项，规则才能生效。
- ✧ 默认情况下，管理员可配置 2000 条访问控制策略。

2）点击【确定】按钮完成该条访问控制规则的添加。

步骤 3 点击『查询』，弹出“搜索”窗口，设置资源对象参数和源/目的 IP 地址，点击【确定】按钮即可将匹配的访问控制策略显示在访问控制列表中。

步骤 4 选择访问控制规则，点击『编辑』，可进行策略内容的修改。

步骤 5 选择访问控制规则，点击移动图标“  ”，弹出“移动策略”窗口，设置将当前规则移动到已存在规则之前或之后。

CLI 方式配置

步骤	配置说明
1	配置对象（可选），具体请参见 7.1 对象
2	配置安全引擎策略（可选），具体请参见 7.7 入侵防御、7.9URL 过滤、7.10 内容过滤、7.11 文件过滤、7.12 病毒过滤
3	配置访问控制策略

firewall policy add action <accept|deny> [**srcarea** <*string1*>] [**dstarea** <*string2*>] [**src** <*string3*>] [**dst** <*string4*>] [**dstopts** <setup|notset>] [**service** <*string5*>] [**log** <on|off>] [**enable** <yes|no>] [**schedule** <*string6*>] [**group_name** <*string7*>] [**app** <*string8*>] [**max_active_session** <*string9*>] [**orig_dst** <*string10*>] [**permanent** <yes|no>] [**user** <*string11*>] [**traffic-statistic** <on|off>] [**comment** <*string12*>] [**ah** <setup|notset>] [**esp** <setup|notset>] [**fragment** <setup|notset>] [**hopopts** <setup|notset>] [**routing** <setup|notset>] [**slog** <on|off>] [**profile** <*string13*>]

命令描述

添加一条访问控制规则。当虚系统处于关闭状态时，除了虚系统管理员以外的具备 firewall 模块权限的管理员可以配置该条命令。当虚系统处于开启状态时，只有虚系统管理员可以配置该条命令。

参数说明

firewall policy add	添加一条访问控制规则。
action	必选项，设定访问权限，即允许或禁止匹配该规则的报文通过 NGFW。
accept|deny	允许|禁止
srcarea	可选项，设定源区域。
string1	字符串类型，必须为已定义的区域资源名，可以有一个

	或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
dstarea	可选项，设定目标区域。
string2	字符串类型，为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
src	可选项，源地址对象。
string3	字符串类型，为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dst	可选项，目的地址对象。
string4	字符串类型，为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
service	可选项，设定服务资源。
string5	字符串类型，必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间用空格分隔。名称的大小写必须与系统定义相一致，如’IP’。
log	可选项，设置当数据报文匹配规则时，是否在日志中记录还是进行报警提示，默认不做记录。
on|off	记录日志|不记录日志
enable	可选项，设置是否启用这条规则，默认启用该规则。
yes|no	启用|不启用
schedule	可选项，选择时间资源，必须在 define 模块已经定义。
string6	字符串类型，表示对象名称。
group_name	可选项，设置访问控制规则组。
string7	字符串类型，表示规则组名称。
app	可选项，设置应用对象 ID。
string8	字符串类型。
max_active_session	可选项，设置 NGFW 上的用户或用户访问的应用的最大会话个数。取值范围：0-2147483647。
string9	数值类型。
orig_dst	可选项，设置地址转换前的目标地址对象。
string10	字符串类型，表示对象名称。必须是系统已经定义的地址对象名。
permanent	可选项，设置长连接开关，默认为关闭状态，即为普通连接。一般来说，网关对通信空闲一定时间的连接将自动断开，以提高安全性和释放通信资源，但某些应用所建立的连接需要长时期保持，即使处于空闲状态。例如 ATM 机器必须和处理中心的服务器一直保持着连接，这个连接必须设置为长连接。
yes|no	开|关，分别表示长连接和普通连接。
user	可选项，设置用户/用户组对象名，需要在 user 中定义。
string11	字符串类型，长度必须小于 126 位。
traffic-statistic	可选项，设置策略统计开关，默认为关。
on|off	开|关
comment	可选项，设置访问控制规则描述。
string12	字符串类型，长度必须小于 126 位。
ah	可选项，设置 IPV6 认证扩展头，对 IPv6 头进行加密的

	校验。 开启该项开关后，该条访问控制策略只匹配包含 IPv6 认证扩展头的数据报文。
setup|notset	开启|关闭
dstopts	可选项，设置 IPV6 目的地扩展头。开启该项开关后，该条访问控制策略只匹配包含 IPv6 目的地扩展头的数据报文。
setup|notset	开启|关闭
esp	可选项，设置 IPV6 ESP 扩展头，即封装安全性净荷扩展头，不进行加密，指明剩余的净荷已经加密，并为已经获得授权的目的节点提供足够的解密信息。 开启该项开关后，该条访问控制规则只匹配包含 IPv6ESP 扩展头的数据报文。
setup|notset	开启|关闭
fragment	可选项，设置 IPv6 分段扩展头，包括一个分段偏移值、一个“更多段”标志和一个标识字段，用于源节点对长度超出源端和目的端间路径 MTU 的包进行分段。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 分段扩展头的数据报文。
setup|notset	开启|关闭
hopopts	可选项，设置 IPV6 逐跳扩展头。逐跳扩展头位于 IPv6 头之后，包含数据包到达目的地过程中经过的每个节点的检查项。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 逐跳扩展头的数据报文。提高 NGFW 对数据包的处理能力。
setup|notset	开启|关闭
routing	可选项，设置 IPV6 路由扩展头，指明数据包在到达目的地过程中将经过的特殊的节点，包含了各节点的地址列表。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 路由扩展头的数据报文。
setup|notset	开启|关闭
slog	可选项，设置是否记录设备的会话日志。
on|off	记录|不记录
profile	可选项，设置引入到访问控制规则中的内容安全策略对象，包括内容过滤、IPS、AV、URL、DLP 等应用层检测内容。
string13	字符串类型。

以下是添加访问控制规则的示例：

在虚系统关闭的情况下，添加一条拒绝 area_feth0 源区域数据包访问的访问控制策略，并记录日志。

TopsecOS# **define area add name** *area_feth0* **interface** *feth0* **comment**

comment_content

TopsecOS# **firewall policy add action** *deny* **srcarea** *area_feth0* **log** *on* **enable** *yes*

firewall policy modify action <accept|deny> **id** <*number*> [**srcarea** <*string1*>] [**dstarea** <*string2*>] [**src** <*string3*>] [**dst** <*string4*>] [**dstopts** <setup|notset>] [**service** <*string5*>] [**log** <on|off>] [**enable** <yes|no>] [**schedule** <*string6*>] [**group_name** <*string7*>] [**app** <*string8*>] [**max_active_session** <*string9*>] [**orig_dst** <*string10*>] [**permanent** <yes|no>] [**user** <*string11*>] [**traffic-statistic** <on|off>] [**comment** <*string12*>] [**ah** <setup|notset>] [**esp** <setup|notset>] [**fragment** <setup|notset>] [**hopopts** <setup|notset>] [**routing** <setup|notset>] [**slog** <on|off>] [**profile** <*string13*>]

命令描述

修改访问控制规则。当虚系统处于关闭状态时，除了虚系统管理员以外的具备 firewall 模块权限的管理员可以配置该条命令。当虚系统处于开启状态时，只有虚系统管理员可以配置该条命令。

参数说明

firewall policy modify	修改一条访问控制规则。
action	必选项，指定访问权限，即允许或禁止匹配该规则的报文通过 NGFW。
accept|deny	允许|禁止
id	必选项，指定已设定的访问控制规则 ID。
number	数值类型。
srcarea	可选项，设定源区域。
string1	字符串类型，必须为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
dstarea	可选项，设定目标区域。
string2	字符串类型，为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
src	可选项，源地址对象。
string3	字符串类型，为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dst	可选项，目的地址对象。
string4	字符串类型，为已定义的地址对象名，可以用主机、子网或地址范围。也可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
service	可选项，设定服务对象。
string5	字符串类型，必须是系统缺省服务或自定义服务的名称，可以输入多个，格式为’IP ICMP’，用单引号，中间

	用空格分隔。名称的大小写必须与系统定义相一致，如'IP'。
log	可选项，设置当数据报文匹配规则时，是否在日志中记录还是进行报警提示，默认不做记录。
on|off	记录日志|不记录日志
enable	可选项，是否启用这条规则，默认启用该规则。
yes|no	启用|不启用
schedule	可选项，选择时间资源，必须在 define 模块已经定义。
string6	字符串类型，对象名称。
group_name	可选项，策略组对象名。
string7	字符串类型，表示对象名称。
app	可选项，应用对象 ID。
string8	字符串类型。
max_active_session	可选项，最大活动会话数。
string9	字符串类型。
orig_dst	可选项，指定地址转换前的目标地址对象。
string10	字符串类型，表示对象名称。必须是系统已经定义的地址对象名。
permanent	可选项，长连接开关，默认为关闭状态，即为普通连接。一般来说，网关对通信空闲一定时间的连接将自动断开，以提高安全性和释放通信资源，但某些应用所建立的连接需要长时期保持，即使处于空闲状态。例如 ATM 机器必须和处理中心的服务器一直保持着连接，这个连接必须设置为长连接。
yes|no	开|关，分别表示长连接和普通连接。
user	可选项，用户/用户组对象名，需要在 user 中定义。
string11	字符串类型，长度必须小于 126 位。
traffic-statistic	可选项，策略统计开关，默认为关。
on|off	开|关
comment	可选项，输入规则描述。
string12	字符串类型，长度必须小于 126 位。
ah	可选项，设置 IPV6 认证扩展头，对 IPv6 头进行加密的校验。 开启该项开关后，该条访问控制策略只匹配包含 IPv6 认证扩展头的数据报文。
setup|notset	开启|关闭
dstopts	可选项，设置 IPV6 目的地扩展头。开启该项开关后，该条访问控制策略只匹配包含 IPv6 目的地扩展头的数据报文。
setup|notset	开启|关闭
esp	可选项，设置 IPV6 ESP 扩展头，即封装安全性净荷扩展头，不进行加密，指明剩余的净荷已经加密，并为已经获得授权的目的节点提供足够的解密信息。 开启该项开关后，该条访问控制规则只匹配包含 IPv6ESP 扩展头的数据报文。
setup|notset	开启|关闭
fragment	可选项，设置 IPv6 分段扩展头，包括一个分段偏移值、一个“更多段”标志和一个标识字段，用于源节点对长度超出源端和目的端间路径 MTU 的包进行分段。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 分

	段扩展头的数据报文。
setup|notset	开启|关闭
hopopts	可选项，设置 IPV6 逐跳扩展头。逐跳扩展头位于 IPv6 头之后，包含数据包到达目的地过程中经过的每个节点的检查项。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 逐跳扩展头的数据报文。提高 NGFW 对数据包的处理能力。
setup|notset	开启|关闭
routing	可选项，设置 IPV6 路由扩展头，指明数据包在到达目的地过程中将经过的特殊的节点，包含了各节点的地址列表。 开启该项开关后，该条访问控制规则只匹配包含 IPv6 路由扩展头的数据报文。
setup|notset	开启|关闭
slog	可选项，设置是否记录设备的会话日志。
on|off	记录|不记录
profile	可选项，设置引入到访问控制规则中的内容安全策略对象，包括内容过滤、IPS、AV、URL、DLP 等应用层检测内容。
string13	字符串类型。

以下是修改访问控制规则的示例：

允许匹配 IP 号为 11156 的访问控制策略的源区域 area_feth0 的数据报文通过，并记录日志。

TopsecOS# **define area add name** *area_feth0* **access** *on* **interface** *feth0* **comment** *comment_content*

TopsecOS# **firewall policy modify id** *11156* **action** *accept* **srcarea** *area_feth0* **log** *on* **enable** *yes*

firewall policy delete id <*number*>

命令描述

删除一条访问控制规则。

参数说明

firewall policy delete	删除一条访问控制规则。
id	必选项，指定访问控制规则 ID。
number	字符串类型，必须是已定义的规则 ID 值。

以下是删除一条访问控制规则的示例：

```
TopsecOS# firewall policy delete id 8503
```

firewall policy move <*number1*> [**before** <*number2*>| **after** <*number3*>]

命令描述

移动一条访问控制规则的位置。

参数说明

firewall policy move	必选项，移动一条访问控制规则的位置。
number1	数值类型，表示待移动的规则的 ID 号。
before	可选项，设置将规则移动到指定规则之前。
number2	数值类型，表示参照物规则的 ID 号。
after	可选项，设置将规则移动到指定规则之后。
number3	数值类型，表示参照物规则的 ID 号。

以下是移动访问控制规则的示例：

移动一条访问控制规则 8503 到规则 8490 之前。

```
TopsecOS# firewall policy move 8503 before 8490
```

firewall policy show [**src** <*string1*>] [**srcarea** <*string2*>] [**srcip** <*string3*>] [**dst** <*string4*>] [**dstarea** <*string5*>] [**dstip** <*string6*>] [**group-name** <*string7*>] [**name** <*string8*>] [**orig_dst** <*string9*>]

命令描述

查看访问控制规则。

参数说明

firewall policy show	查看访问控制规则。
src	可选项，指定源地址对象。
string1	字符串类型，表示已定义的地址对象名。可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
srcarea	可选项，设定源区域。
string2	字符串类型，必须为已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
srcip	可选项，指定源 IP 的名称。
string3	字符串类型，表示 IP 地址。
dst	可选项，指定目的地址对象。
string4	字符串类型，表示已定义的地址对象名，可以输入多个，格式为’aa ll’，用单引号，中间用空格分隔。
dstarea	可选项，设定目标区域。

string5	字符串类型，表示已定义的区域资源名，可以有一个或多个，需用单引号’‘括起来，多个区域名之间用空格分隔即可，例如'area_feth0 area_feth1'。
dstip	可选项，指定目的 IP 地址。
string6	字符串类型，表示已定义 VLAN 号。
group-name	可选项，指定策略组。不指定时表示默认组。
string7	字符串类型，表示策略组对象名。
name	可选项，设置访问控制规则的名称，未引用任何对象时为“none”。
string8	字符串类型，表示已定义的访问控制规则对象名称。
orig_dst	可选项，设置地址转换前的目的地址对象名称。
string9	字符串类型。

以下是查看访问控制规则的示例：

查看所有访问控制规则。

```
TopsecOS# firewall policy show
ID 11151 firewall policy add action accept slog on group_name '3' app 'fuwu' enable
ID 11156 firewall policy add action accept log on srcarea 'area_feth0' enable
```

查看源区域为 area_feth0 的访问控制规则。

```
TopsecOS# firewall policy show srcarea area_feth0
ID 11156 firewall policy add action accept log on srcarea 'area_feth0' enable
```

firewall policy clean <cr>

命令描述

清空所有或某个虚系统的访问控制规则。

以下是清空访问控制规则的示例：

```
TopsecOS# firewall policy clean
```

firewall policy total [**status** <enable|disable>]

命令描述

根据策略状态统计访问控制规则的数量。

参数说明

firewall policy total	根据策略状态统计访问控制规则的数量。
status	可选项，设置访问控制策略状态。
enable|disable	启用|未启用

以下是根据策略状态统计访问控制规则的数量的示例：

TopsecOS# **firewall policy total**

total:2

firewall policy dump <on|off>

命令描述

设置访问控制策略的显示开关。

参数说明

firewall policy dump	必选项，设置访问控制策略的显示开关。
on|off	打开|关闭

以下是设置访问控制策略的显示开关的示例：

TopsecOS# **firewall policy dump** on

7.2.2.2 配置访问控制策略组

WEBUI 方式配置

步骤 1 选择 **安全策略** > **访问控制**，进入访问控制界面。

步骤 2 点击『添加』，选择“策略组”，弹出“添加策略组”窗口，设置访问控制规则组名称后，点击【确定】按钮完成规则组的添加。

步骤 3 选择访问控制策略组，点击插入图标“”，弹出“插入组”窗口，设置规则组名称，然后点击【确定】按钮完成访问控制规则组的添加；点击移动图标“”，弹出“移动组”窗口，设置将当前规则组移动到已存在规则组之前或之后。

CLI 方式配置

firewall group_policy add name <*string*> [**before** <*number*>]

命令描述

添加一条访问控制规则组。

参数说明

firewall group_policy add	添加一条访问控制规则组。
name	必选项，设置规则组名称。
string	字符串类型。
before	可选项，设置在某规则组之前插入一条规则组。
number	数值类型，表示已经添加的 ACL 规则组的 ID 号。

以下是添加访问控制规则组的示例：

在 ACL 规则组 8108 前插入规则组 subnat83 中。

```
TopsecOS# firewall group_policy add name subnat83 before 8108
```

firewall group_policy clean <cr>

命令描述

清空访问控制规则组。

以下是清空访问控制规则组的示例：

```
TopsecOS# firewall group_policy clean
```

firewall group_policy delete [**id** <*number1*>| **name** <*string*>]

命令描述

根据 ID 或名称删除某访问控制规则组。

参数说明

firewall group_policy delete	根据 ID 或名称删除某访问控制规则组。
id	可选项，指定规则组 ID 号。
number	数值类型。
name	可选项，设置规则组名称。

string	字符串类型。

以下是根据 ID 或名称删除某访问控制规则组的示例：

删除规则组 subnat83。

```
TopsecOS# firewall group_policy delete name subnat83
```

firewall group_policy rename oldname <*string1*> **newname** <*string2*>

命令描述

重命名访问控制规则组。

参数说明

firewall group_policy rename	重命名访问控制规则组。
oldname	必选项，设置规则组旧的名称。
string1	字符串类型。
newname	必选项，设置规则组新的名称。
string2	字符串类型。

firewall group_policy show <cr>

命令描述

查看访问控制规则组。

以下是查看访问控制规则组的示例：

```
TopsecOS# firewall group_policy show
ID 10070 firewall group_policy add name 33
ID 10071 firewall group_policy add name dfg
ID 10072 firewall group_policy add name df
ID 10073 firewall group_policy add name 234
ID 10186 firewall group_policy add name dre
```

firewall group_policy move <*string1*> **before** <*string2*>

firewall group_policy move <*string1*> **after** <*string3*>

命令描述

移动访问控制规则组。

参数说明

firewall group_policy move	必选项，移动访问控制规则组。
string1	字符串类型，表示待移动的规则组的名称。
before	必选项，移动到指定的规则组之前。
string2	字符串类型，表示参照物规则组的名称。
after	必选项，移动到指定规则组之后。
string3	字符串类型，表示参照物规则组的名称。

以下是移动访问控制规则组的示例：

将名为“test10”的规则组移动到名为“test2”的规则组之前。

```
TopsecOS# firewall group_policy move test10 before test2
```

7.3 地址转换

网络地址转换（Network Address Translation，简称 NAT）是将 IPv4 报文头中的 IPv4 地址转换为另一个 IPv4 地址的技术，这种技术被普遍应用于公网用户访问受保护私有网络中的资源服务器，以及有多台主机但只能通过少量公有 IPv4 地址访问因特网的私有网络中。

NAT 技术可隐藏私有网络中主机真实的 IPv4 地址，增强内部网络的安全性，虽破坏了主机端到端的连接，降低数据通信效率，但随着移动用户急剧新增以及互联网规模的不断扩大，NAT 技术无疑是解决 IPv4 地址短缺的成功案例。

NAT 分类

根据应用场景不同，NGFW 提供以下几种地址转换方式：

转换方式	转换内容	特点
源地址转换（SNAT）	源 IP 地址	1）通过配置 SNAT 地址池，实现特定数据报文经过 NGFW 后，数据报文的源 IP 地址转换为 SNAT 地址池中某个 IP 地址。 2）该地址转换方式为一对一转换。用户共享 SNAT 地址池中 IP 地址，SNAT 地址池中的 IP 地址全部被使用情况下，后续用户将不能通过 NGFW 的 SNAT

转换方式	转换内容	特点
		技术进行地址转换，即 SNAT 地址池中地址个数为允许同时通过防火墙通信的最大用户数。
	源 IP 地址+源端口	1）通过配置 SNAT 地址池，实现特定数据报文经过 NGFW 后，数据报文的源 IP 地址转换为 SNAT 地址池中某个 IP 地址，并转换源端口号。 2）该转换方式为多对一转换。多个用户可同时使用同一个 IP 地址访问网络资源，NGFW 根据端口号区分不同的用户。
目的地址转换（DNAT）	目的 IP 地址	通过配置 DNAT 地址池，实现特定数据报文经过 NGFW 后，数据报文的目的 IP 地址转换为 DNAT 地址池中某个 IP 地址。
	目的 IP 地址+目的端口	通过配置 DNAT 地址池和转换后的目的端口号，实现特定数据报文经过 NGFW 后，数据报文的目的 IP 地址转换为 DNAT 地址池中某个 IP 地址，目的端口号转换为特定的端口号。
双向地址转换（双向 NAT）	源 IP 地址+目的 IP 地址（+源/目的端口）	通过配置 SNAT 和 DNAT 地址池，实现特定数据报文经过 NGFW 后，将数据报文的源 IP 地址转换为 SNAT 地址池中某个 IP 地址，目的 IP 地址转换为 DNAT 地址池中某个 IP 地址。 说明： 双向 NAT 为 SNAT 和 DNAT 的结合，其功能特性也为 SNAT 和 DNAT 的结合。
不作转换（NoNAT）	不转换	不转换数据包的 IP 地址和端口。主要在已定义的 SNAT、DNAT、双向 NAT 基础上，定义无需执行地址转换的特例。 说明： 数据报文匹配 NAT 规则时，首先匹配 NoNAT 规则，如果满足 NoNAT 规则的条件，则不进行地址转换。

NAT 处理数据流程

管理员定义的所有 NAT 规则都按顺序存储在一张规则表中，每次检测时都按照规则的排列顺序逐一与数据包匹配，一旦存在一条满足条件的地址转换规则，NGFW 将停止检索，并按该满足条件的规则处理数据包。

此外，NAT 对路由、访问控制、QoS 和 IPSec VPN 等功能模块均有影响。管理员在配置 NGFW 时，需从整体上掌握 NGFW 根据各功能模块处理数据报文的流程，使数据包经过 NAT 模块后不影响其他安全引擎的检测。

例如，如果对某主机发送的数据包配置了 NAT 策略，在为该主机配置访问控制策略时，访问控制策略的目的 IP 地址需为 DNAT 之后的地址，而并非主机的真实目的 IP 地址。NAT 处理数据流程如下图所示。

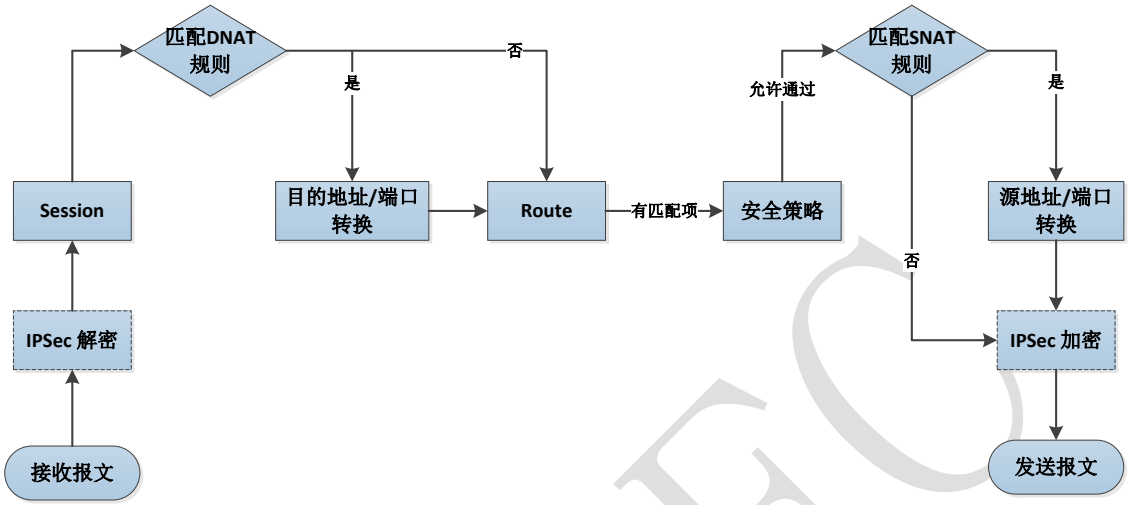


图 7-3 NAT 数据处理流程示意图

NGFW 的 NAT 模块处理数据报文流程简述如下：

1）NGFW 接收数据报文后，首先按顺序查找 DNAT 规则，如果报文满足 DNAT 匹配条件，则转换报文的目的 IP 地址/端口后查找路由表，并在地址转换连接表中记录转换信息，转步骤 2）；否则，不执行地址转换，直接转步骤 2）。

2）如果数据包查找到有满足条件的路由表项，记录路由查找结果，进入安全策略匹配流程，转步骤 3）；否则，将报文直接丢弃。

3）如果安全策略允许数据报文通过，则按顺序查找 SNAT 规则，转步骤 4）；否则，将报文直接丢弃。

4）如果报文满足 SNAT 匹配条件，则转换报文的源 IP 地址/端口；否则，不进行源地址转换，直接转步骤 5）。

5）如果数据报文在匹配安全策略阶段满足 IPSec VPN 网段匹配条件，进行 IPSec 加密后，再将数据报文根据路由查找结果从相应出接口转发出去；否则，直接根据路由查找结果转发出去。

注意

- ✧ 限制条件精细的 NAT 规则应当置于条件宽松的规则之前，以提高数据报文匹配 NAT 规则的精确度。

7.3.1 配置 SNAT

SNAT（Source Network Address Translation，源地址转换），转换数据报文的源 IP 地址，可隐藏主机真实的 IP 地址。主要应用于使用私网 IP 地址的内网用户访问 Internet，在此网络应用环境下，私网用户数据包经过 NGFW 时，NGFW 通过将数据包的私有源 IP 地址转换为公有 IP 地址，不仅可隐藏内网主机真实 IP 地址，还使响应报文在公网中有路由，实现使用私有 IP 地址的内网主机成功访问 Internet 的目的。

SNAT 分类

根据实际应用场景不同，NGFW 支持三种 SNAT 技术，包括：不带端口转换为地址池中地址、带端口转换为地址池中地址、转换为出接口所使用的地址。管理员可根据如下特征为特定的场景选择不同的 SNAT 方式，具体如下：

类型	说明
不带端口转换为地址池中地址	适用于需同时访问 Internet 的用户小于或等于其所申请的公网 IP 地址个数的网络。 说明： 1）属于一对一转换，一个用户使用一个 IP 地址，如果该 SNAT 规则中的“源地址转换为”地址池中地址已被全部分配，后续满足该 SNAT 匹配条件的用户将不能获取 IP 地址，直到地址池中有释放的 IP 地址； 2）隐藏局域网主机真实 IP 地址。
带端口转换为地址池中地址	适用于需同时访问 Internet 的用户大于其所申请的公网 IP 地址个数的网络。 说明： 1）属于多对一转换，多个用户可复用同一个 IP 地址，NGFW 通过源端口号区分不同用户； 2）隐藏局域网主机真实 IP 地址和端口号。
转换为出接口所使用的地址	适用于公网 IP 地址为动态获取的局域网。注意：此种网络环境中，需配置 NAT 的“源 IP 地址+端口”转换方式，其中“源地址转换为”参数需设置为绑定接口的安全域，因此在配置该类型 SNAT 前，需将物理接口与安全区域绑定，关于物理接口与安全区域的绑定具体请参见 7.1.1 区域。 说明： 1）属于多对一转换，所有用户复用 NGFW 出接口 IP 地址，NGFW 通过源端口号区分不同用户；

类型	说明
	2）隐藏局域网主机真实 IP 地址和端口号。

应用场景举例

NGFW 部署于局域网与公网的边界，局域网申请了固定公网 IP 地址“1.1.1.10-1.1.1.17”供内网用户访问公网，其中 A 部门用户的私有 IP 地址段为 10.0.0.10-10.0.0.15，访问 Internet 时一人单独使用一个 IP 地址；B 部门用户 IP 地址处于 10.0.1.0/24 子网内，访问 Internet 时共用剩下的两个公网 IP 地址。其网络拓扑结构如下图所示。

实现方案：混合采用 SNAT 的“带端口转换为地址池中地址”和“不带端口转换为地址池中地址”方式，支持内网用户访问 Internet。为使内网用户能根据需求访问公网服务器时，其 SNAT 配置方法如下图中的“NAT 规则”所示。

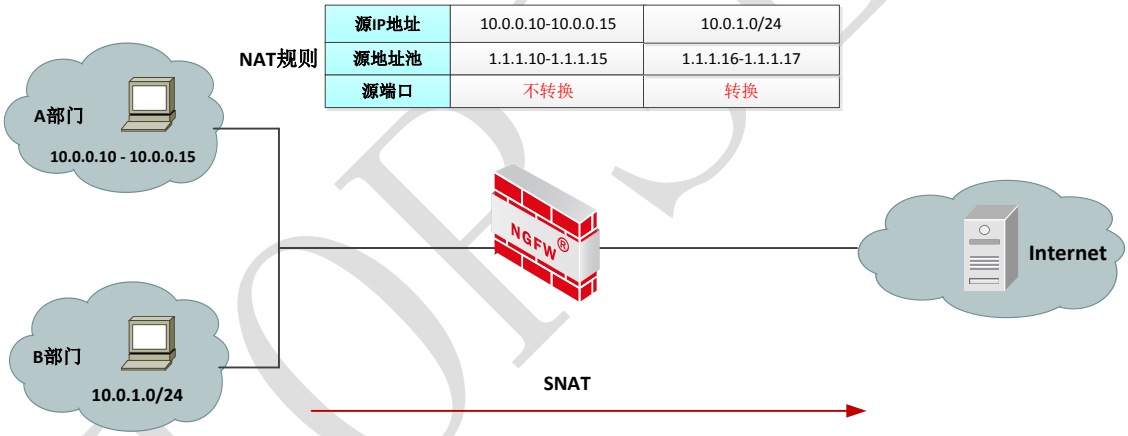


图 7-4 SNAT 应用示意图

➢ A 部门主机（10.0.0.10）访问 Internet 时，NGFW 处理数据流程如下：

1）NGFW 接收到主机（10.0.0.10）发往公网服务器的数据包后，按顺序匹配 NAT 规则表，发现有匹配数据报文的“源端口不做转换”方式 SNAT 规则，停止检索。

2）根据成功匹配的 SNAT 规则，从源地址地址池中选择一个未被使用的 IP 地址替换数据报文的源 IP 地址，并创建会话，然后将数据报文发送出去。

3）NGFW 接收到公网服务器的响应报文后，根据步骤 2）创建的会话表，将报文的目的地址替换为主机（10.0.0.10）真实的 IP 地址，然后将报文发送给主机（10.0.0.10）。

➢ B 部门主机（10.0.1.2）访问 Internet 时，NGFW 处理数据流程如下：

1）NGFW 接收到主机（10.0.1.2）发往公网服务器的数据包后，按顺序匹配 NAT 规则表，发现有匹配数据报文的“源端口做转换”方式 SNAT 规则，停止检索。

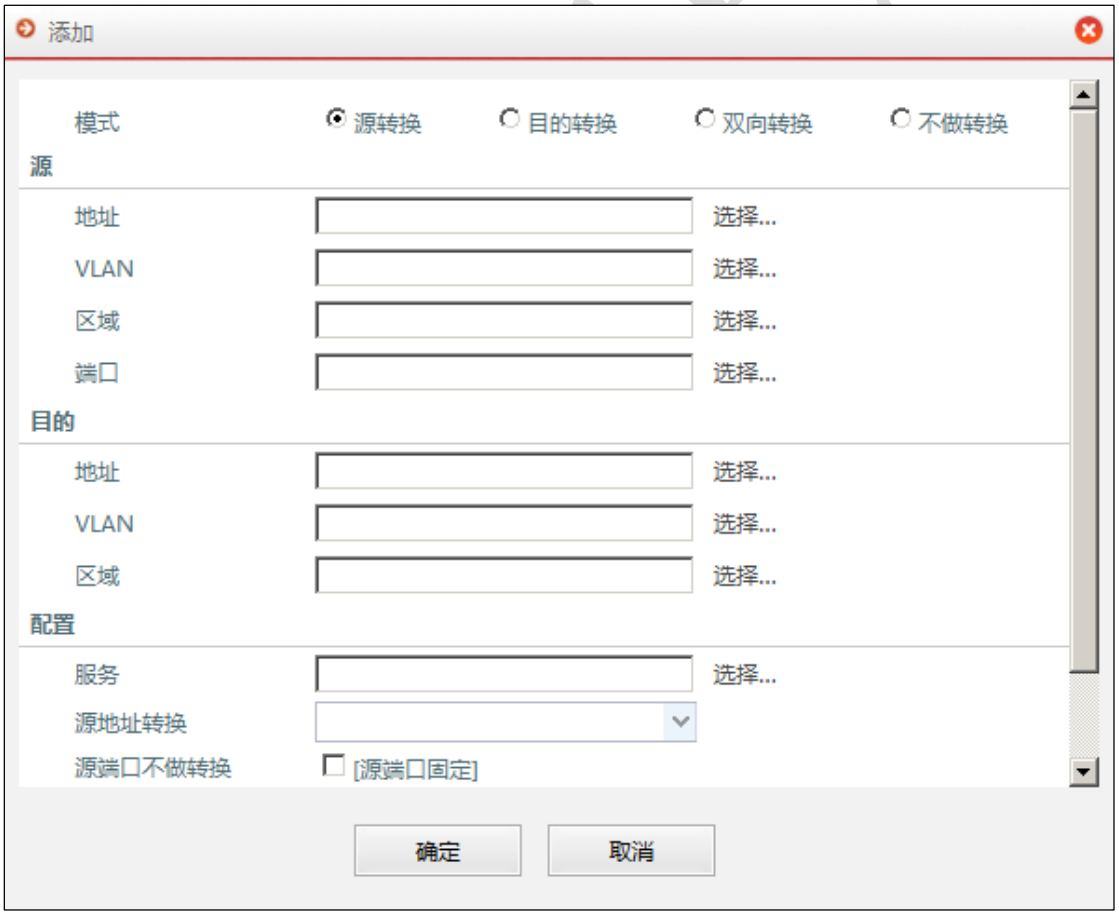
2）根据成功匹配的 NAT 规则，从源地址池中选择一个 IP 地址替换数据报文的源 IP 地址，并转换源端口号，然后创建会话，将数据报文发送出去。

3）NGFW 接收到公网服务器的响应报文后，根据步骤 2）创建的会话表，将报文的目的地址替换为主机（10.0.1.2）真实的 IP 地址，端口替换为主机原始的端口号，然后将报文发送给主机（10.0.1.2）。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **地址转换**。

步骤 2 点击『添加』，弹出添加 NAT 规则窗口，如下图所示。



在添加 SNAT 规则时，各项参数的具体说明如下表所示。

参数	说明
源地址	配置数据报文的源地址应满足的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象，关于地址对象的定义具体请参见 7.1.2 地址。
源 VLAN	配置数据报文的源 VLAN 应满足的条件。
源区域	配置数据报文的源区域应满足的条件。
源端口	配置数据报文的源端口应满足的条件。
目的地址	配置数据报文的目的地址应当匹配的条件。 1）点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象。
目的 VLAN	配置数据报文的目的 VLAN 应满足的条件。
目的区域	配置数据报文的目的区域应当匹配的条件。
服务	选择匹配的服务对象，可以选择一个或多个。
源地址转换	必选项。设置 SNAT 源转换的地址池，可为主机地址、地址范围对象或区域对象。 说明： 1）选择主机地址对象时，表示将源地址固定映射为某一 IP 地址； 2）选择地址范围对象时，将源地址动态映射为某一网段或某一地址范围内的地址； 3）选择区域对象时，将源地址转换为具有该区域的物理接口的地址（默认映射为端口的主地址）。因此要求区域对象必须与物理接口绑定，关于区域与接口的绑定具体请参见 7.1.1 区域。
源端口不做转换	系统默认情况下，在源地址转换同时也会转换源端口。如果勾选该选项，表示数据包在经过 NGFW 系统时将固定源端口而不对源端口进行随机转换。
策略开关	启动后该 NAT 规则才会生效。默认为启用状态。
Sticky NAT 开关	地址粘性开关。启动后，相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同。

说明

- ✧ 如果在某一条 NAT 规则中设置了多个条件，则数据包必须同时满足这些条件才认为成功匹配该规则，才根据规则相应的动作转换数据包的 IP 地址或端口。

步骤 3 点击【确定】按钮完成 SNAT 规则的配置。

CLI 方式配置

步骤	配置说明
1	配置地址、VLAN、服务等对象。
2	可选。物理接口绑定区域，只有添加地址转换为 NGFW 出接口 IP 地址的 SNAT，才需配置该项。
3	配置 SNAT 规则。

nat policy add [**enable** <yes|no>] [**vr_id** <*string1*>] [**orig_src** <*string2*>] [**orig_sport** <*string3*>] [**srcarea** <*string4*>] [**srcvlan** <*string5*>] [**orig_dst** <*string6*>] [**orig_service** <*string7*>] [**dstarea** <*string8*>] [**dstvlan** <*string9*>] **trans_src** <*string11*> [**pat** <yes|no>] [**sticky** <yes|no>]

命令描述：

增加一条 SNAT 策略。

参数说明：

nat policy add	增加地址转换策略。
enable	可选项，设定地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示暂时禁用这条地址转换策略。默认值为“yes”。
vr_id	可选项，设定该地址转换策略所属的虚拟路由域。
string1	数值类型，表示 VR。
orig_src	可选项，设定所匹配报文的源地址对象。
string2	字符串类型，表示所匹配报文的源地址对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	可选项，设定所匹配报文的源端口对象。
string3	字符串类型，表示所匹配报文的源端口对象名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
srcarea	可选项，设定所匹配报文的源区域。
string4	字符串类型，表示所匹配报文的源区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称。 2）可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
srcvlan	可选项，设定所匹配报文的源 VLAN。
string5	字符串类型，表示所匹配报文的源 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称。 2）可以输入一个或多个 VLAN 的名称，输入多个时用

	单引号括起来，并用空格隔开，如’vlan.0001 vlan.0002’。
orig_dst	可选项，设定所匹配报文的目的地址对象。
string6	字符串类型，表示所匹配报文的目的对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_service	可选项，设定所匹配报文的服务资源。
string7	字符串类型，表示所匹配报文的服务资源名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
dstarea	可选项，设定所匹配报文的目标区域。
string8	字符串类型，表示所匹配报文的目的区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。 2）添加目的地址转换策略时，不能设定该参数值。
dstvlan	可选项，设定所匹配报文的目的 VLAN。
string9	字符串类型，表示所匹配报文的目的 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’ vlan.0001 vlan.0002’。 2）添加目的地址转换策略时，不能设定该参数值。
trans_src	必选项，设定转换后的源地址对象。
string11	字符串类型，表示转换后的源对象名称。 说明： 1）该参数值必须是已经定义的地址对象或属性名称。 2）只能输入一个对象。 3）添加源地址转换策略时，该参数值必须设置。
pat	可选项，设定源端口转换开关。
yes|no	yes 表示对源端口进行端口转换；no 表示不对源端口进行端口转换。默认值为“yes”。
sticky	可选项，设定是否开启地址转换策略的粘连开关。
yes|no	是|否

使用说明：

1）系统默认情况下，在源地址转换同时也会转换源端口。

2）未做接口与区域绑定的区域对象不能作为地址转换策略的转换后地址。

以下为添加 SNAT 策略的示例：

增加并启用一条源地址转换策略，使内网中的主机 A 通过 NGFW 访问公网时，使用公网地址“201.10.10.1”。1）主机 A 的 IP 地址为“10.10.10.22”（地址对象名称为“10.22”）；2）主机 A 转换后的公网地址为“201.10.10.1”（地址对象名称为“internet01”）；3）NGFW 的 feth0 连接内网，feth1 连接公网（区域对象名称分别为“area_feth0”和“area_feth1”）。

```
TopsecOS# define host add name 10.22 ipaddr 10.10.10.22
TopsecOS# define host add name internet01 ipaddr 201.10.10.1
TopsecOS# define area add name area_feth0 interface feth0
TopsecOS# define area add name area_feth1 interface feth1
TopsecOS# nat policy add enable yes srcarea area_feth0 orig_src 10.22 dstarea
area_feth1 trans_src internet01
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01 vr_id 0 hit-session 0
```

nat policy show <cr>

命令描述：

查看所有 NAT 策略。

以下为查看所有 NAT 策略的示例：

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01 vr_id 0 hit-session 0
ID 8012 nat policy add orig_dst 'nat_address1 ' orig_service 'http8080 'trans_dst
web_server1 vr_id 0 hit-session 0
ID 8017 nat policy add orig_src '10.22 ' orig_dst '83.234 ' orig_service 'http80
'trans_src nat_address2 trans_dst nat_address3 trans_service http8080 vr_id 0 hit-
session 0
```

nat policy move <*number1*> **after** <*number2*>

命令描述：

将 NAT 策略移动至某基准 NAT 策略之后。

参数说明：

nat policy move	向后移动 NAT 策略。
number1	数值类型，表示待移动 NAT 策略的 ID。
after	必选项。将待移动 NAT 策略移动的基准 NAT 策略之后。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之后。

TopsecOS# **nat policy move** *8017* **after** *8062*

nat policy move <*number1*> **before** <*number2*>

命令描述：

将 NAT 策略移动至某基准 NAT 策略之前。

参数说明：

nat policy move	向前移动一条 NAT 策略。
number1	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
before	必选项。将待移动 NAT 策略移动的基准 NAT 策略之前。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之前。

TopsecOS# **nat policy move** *8017* **before** *8062*

nat policy del nat_id <*number*>

命令描述：

删除一条 NAT 策略。

参数说明：

nat policy del	删除一条 NAT 策略。

nat_id	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
number	数值类型，表示 NAT 策略的 ID。

以下为删除一条 NAT 策略的示例：

删除 ID 为 8008 的 NAT 策略。

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01    vr_id 0 hit-session 0
TopsecOS# nat policy del nat_id 8008
```

nat policy clean [**vr_id** <*number*>]

命令描述：

清除 NAT 策略。

参数说明：

nat policy clean	清除 NAT 策略。
vr_id	必选项，清除属于相应 VR 的 NAT 策略。
number	数值类型，表示 VR 的 ID。

以下为清除 NAT 策略的示例：

```
TopsecOS# nat policy clean
```

7.3.2 配置 DNAT

DNAT（Destination Network Address Translation，目的地址转换），转换数据报文的目的 IP 地址。主要应用于公网用户访问使用私网 IP 地址的局域网资源，在此网络应用环境下，公网用户的数据报文通过局域网边界的 NGFW 时，NGFW 将数据包的目的 IP 地址转换为内网资源服务器真实的 IP 地址，实现公网用户成功访问内网资源的目的。

DNAT 分类

为适应不同的应用场景，NGFW 通过 DNAT 技术可实现的功能主要包括：1）静态映射；2）服务器负载均衡。具体如下：

参数	说明
静态映射	属于一对一映射，根据映射关系，转换报文的目的 IP 地址为特定 IP 地址。 如内网服务器通过公网 IP 地址对外提供服务，当用户通过服务器公网 IP 地址访问服务器时，NGFW 可根据静态映射技术将用户数据包中的目的 IP 地址转换为服务器真实的 IP 地址，实现用户访问内网资源服务器。 说明： 配置静态映射 DNAT 规则时，“目的地址”需配置为服务器对外提供服务的公网 IP 地址，“目的地址转换为”需设置内网服务器真实的 IP 地址。
服务器负载均衡	IP 地址为地址池中的某个 IP 地址。 用户访问内网资源服务器时，NGFW 通过结合服务器均衡组，将用户数据包中目的地址根据均衡组的负载均衡算法转换为均衡组中某个服务器的真实 IP 地址。 说明： 配置服务器负载均衡 DNAT 规则时，“目的地址”需配置为均衡组服务器对外提供服务的 IP 地址，“目的地址转换为”需配置特定均衡组，关于均衡组的配置具体请参见 7.1.7 均衡组。

应用场景举例

NGFW 部署于局域网和公网的边界，私网中有多台服务器通过公网 IP 地址对外提供相同服务，其网络拓扑结构如下图所示。需求：多台服务器能以负载分担的方式处理外网用户的请求。

实现方案：配置服务器均衡组对象并结合 DNAT 规则，其中，服务器均衡组对象为多台服务器真实 IP 地址（均衡组对象），DNAT 规则的“目的地址”配置为服务器组对外提供服务的公网 IP 地址，“目的地址转换为”引用服务器均衡组，其 DNAT 规则配置方法如下图“NAT 规则”所示。

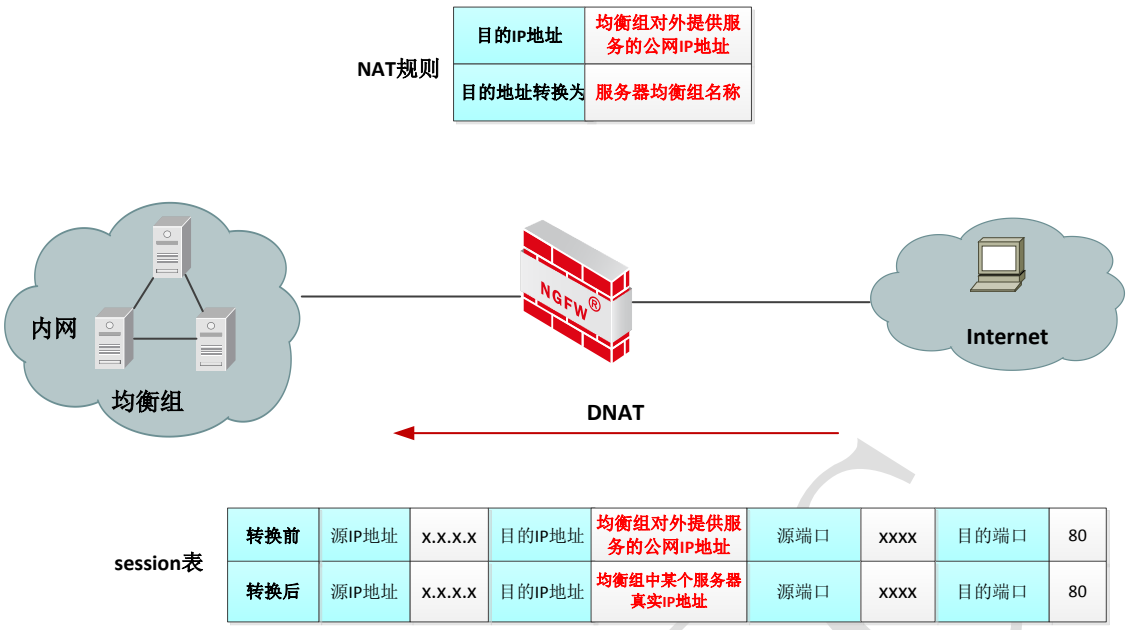


图 7-5 DNAT 应用示意图

用户访问以负载均衡方式提供服务的服务器时，NGFW 处理数据流程如下：

1）NGFW 接收到用户访问均衡组的数据包后，按顺序匹配 NAT 规则表，发现有匹配数据报文的 DNAT 规则，停止检索。

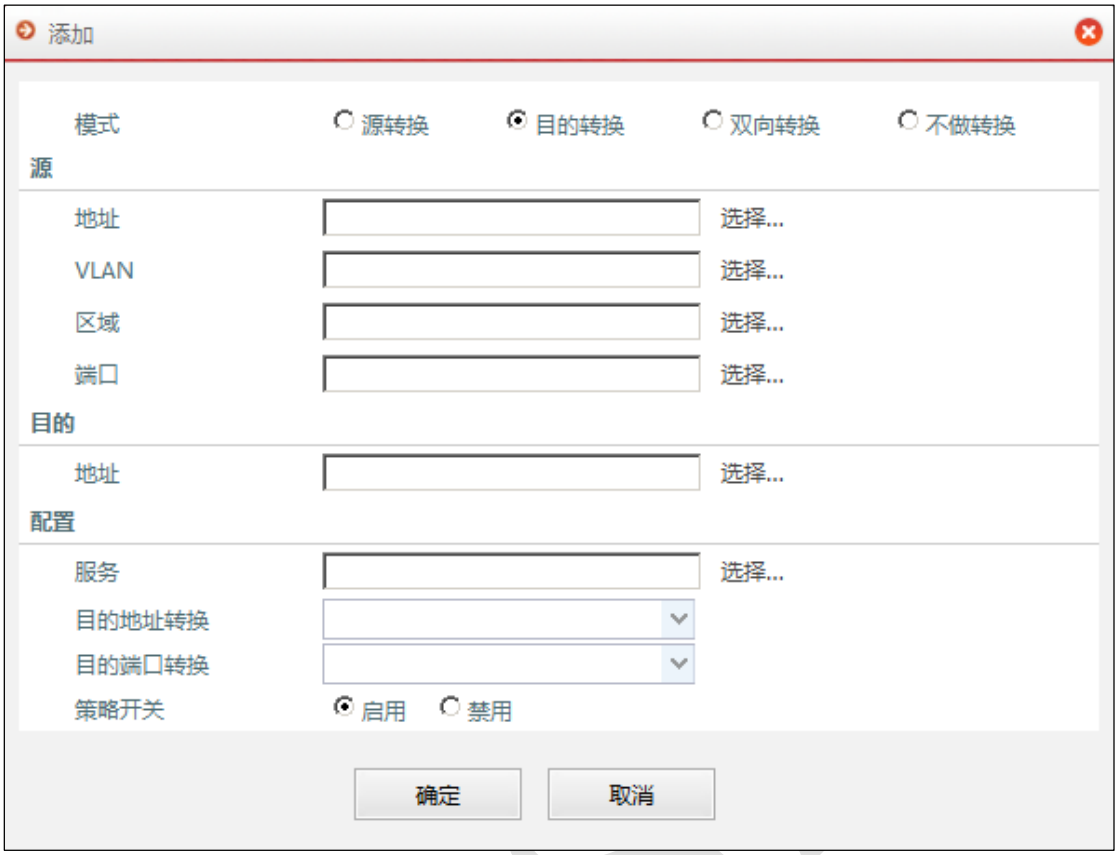
2）根据成功匹配的 DNAT 规则，并依据均衡组的负载均衡算法，选择均衡组中某个服务器的真实 IP 地址替换用户请求包的目的 IP 地址，并创建会话，然后将用户请求报文转发至真实服务器。

3）NGFW 接收到服务器的响应报文后，根据步骤 2）创建的会话表，将报文的源地址替换为转换前 IP 地址，然后将报文发送给用户。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **地址转换**。

步骤 2 点击『添加』，弹出添加 NAT 规则窗口，然后选择 NAT 模式为“目的转换”，如下图所示。



在添加 DNAT 规则时，各项参数的具体说明如下表所示。

参数	说明
源地址	配置数据报文的源地址应满足的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象，关于地址对象的定义具体请参见 7.1.2 地址。
源 VLAN	配置数据报文的源 VLAN 应满足的条件。
源区域	配置数据报文的源区域应满足的条件。
源端口	配置数据报文的源端口应满足的条件。
目的地址	配置数据报文的目的地址应当匹配的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象。
服务	选择匹配的服务对象，可以选择一个或多个。
目的地址转换	可选。配置 DNAT 规则的地址池，可以为主机地址、范围地址对象或子网地址对象。 说明： “目的地址转换”和“目的端口转换”参数必须至少设置一项。
目的端口转换	可选。设置转换后的服务端口，可以选择系统预定义的服务或用户自定义的服务。

参数	说明
	说明： “目的地址转换”和“目的端口转换”参数必须至少设置一项。
策略开关	启动后该 NAT 规则才会生效。默认为启用状态。

说明

✧ 如果在某一条 NAT 规则中设置了多个条件，则数据包必须同时满足这些条件才认为成功匹配该规则，才根据规则相应的动作转换数据包的 IP 地址或端口。

步骤 3 点击【确定】按钮完成 DNAT 规则的配置。

CLI 方式配置

nat policy add [**enable** <yes|no>] [**vr_id** <*string1*>] [**orig_src** <*string2*>] [**orig_sport** <*string3*>] [**srcarea** <*string4*>] [**srcvlan** <*string5*>] [**orig_dst** <*string6*>] [**orig_service** <*string7*>] **trans_dst** <*string8*> **trans_service** <*string9*>

命令描述：

增加一条 DNAT 策略。

参数说明：

nat policy add	增加目的地址转换策略。
enable	可选项，设定地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示暂时禁用这条地址转换策略。默认值为“yes”。
vr_id	可选项，设定该地址转换策略所属的虚拟路由域。
string1	数值类型，表示 VR。
orig_src	可选项，设定所匹配报文的源地址对象。
string2	字符串类型，表示所匹配报文的源地址对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	可选项，设定所匹配报文的源端口对象。
string3	字符串类型，表示所匹配报文的源端口对象名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格

	分隔。
srcarea	可选项，设定所匹配报文的源区域。
string4	字符串类型，表示所匹配报文的源区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称。 2）可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
srcvlan	可选项，设定所匹配报文的源 VLAN。
string5	字符串类型，表示所匹配报文的源 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称。 2）可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’vlan.0001 vlan.0002’。
orig_dst	可选项，设定所匹配报文的目的地址对象。
string6	字符串类型，表示所匹配报文的目的对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_service	可选项，设定所匹配报文的服务资源。
string7	字符串类型，表示所匹配报文的服务资源名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
trans_dst	可选项，设定转换后的目的地址对象。必须保证该参数和 **trans_service 参数至少设置一项。**
string8	字符串类型，表示转换后的目的对象名称。 说明： 1）该参数值必须是已经定义的主机地址对象或均衡组对象名称。 2）只能输入一个对象名。 3）添加目的地址转换策略时，该参数值必须设置。
trans_service	可选项，设定转换后的服务资源。必须保证该参数和 **trans_dst 参数至少设置一项。**
string9	字符串类型，表示转换后的服务资源的名称。 说明： 该参数值必须是 define 模块已经定义的名称。

以下是增加一条目的地址转换策略的示例：

公网用户通过 NGFW 访问内网 WEB 服务器时，为了隐藏服务器在内网中的真实地址 172.168.1.2（地址对象名称为“web_server1”），使用公网地址 202.99.27.201（地址对象名称为“nat_address1”）作为用户的访问地址。

```
TopsecOS# define host add name web_server1 ipaddr 172.168.1.2
TopsecOS# define host add name nat_address1 ipaddr 202.99.27.201
TopsecOS# define service add name http80 protocol 6 port1 80
TopsecOS#nat policy add enable yes orig_dst nat_address1 orig_service http80
trans_dst web_server1
TopsecOS# nat policy show
ID 8012 nat policy add orig_dst 'nat_address1 ' orig_service 'http80' trans_dst
web_server1 vr_id 0 hit-session 0
```

nat policy show <cr>

命令描述：

查看所有 NAT 策略。

以下为查看所有 NAT 策略的示例：

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01 vr_id 0 hit-session 0
ID 8012 nat policy add orig_dst 'nat_address1 ' orig_service 'http8080 'trans_dst
web_server1 vr_id 0 hit-session 0
ID 8017 nat policy add orig_src '10.22 ' orig_dst '83.234 ' orig_service 'http80
'trans_src nat_address2 trans_dst nat_address3 trans_service http8080 vr_id 0 hit-
session 0
```

nat policy move <*number1*> **after** <*number2*>

命令描述：

移动 NAT 策略。

参数说明：

nat policy move	移动 NAT 策略。
number1	数值类型，表示待移动 NAT 策略的 ID。
after	必选项。将待移动 NAT 策略移动的基准 NAT 策略之后。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之后。

```
TopsecOS# nat policy move 8017 after 8062
```

nat policy move <*number1*> **before** <*number2*>

命令描述：

移动一条 NAT 策略。

参数说明：

nat policy move	移动一条 NAT 策略。
number1	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
before	必选项。将待移动 NAT 策略移动的基准 NAT 策略之前。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之前。

```
TopsecOS# nat policy move 8017 before 8062
```

nat policy del nat_id <*number*>

命令描述：

删除一条 NAT 策略。

参数说明：

nat policy del	删除一条 NAT 策略。
nat_id	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
number	数值类型，表示 NAT 策略的 ID。

以下为删除一条 NAT 策略的示例：

删除 ID 为 8008 的 NAT 策略。

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01    vr_id 0 hit-session 0
```

TopsecOS# **nat policy del nat_id** *8008*

nat policy clean [**vr_id** <*number*>]

命令描述：

清除 NAT 策略。

参数说明：

nat policy clean	清除 NAT 策略。
vr_id	必选项，清除属于相应 VR 的 NAT 策略。
number	数值类型，表示 VR 的 ID。

以下为清除 NAT 策略的示例：

TopsecOS# **nat policy clean**

7.3.3 配置双向 NAT

双向 NAT，转换数据报文的源 IP 地址和目的 IP 地址。双向 NAT 典型应用场景主要包括：1）VPN 隧道两端的私有网络中使用相同的私网 IP 地址时，通过 NAT 技术解决隧道两端使用相同 IP 地址主机间通信地址冲突问题；2）局域网内不同区域使用相同 IP 地址的主机间的互访；3）局域网内网用户通过域名（公网 IP 地址）访问内网资源服务器。

应用场景举例

企业 WEB 服务器（IP：192.168.92.10）通过公网 IP 地址 200.1.1.5 对外提供 WEB 服务，其网络拓扑如下图所示。需求：与 WEB 服务器处于同网段的内网用户可以通过域名（公网 IP 地址）访问 WEB 服务器。

实现方案分析：内网用户使用公网地址访问 WEB 服务器时，数据包的源 IP 为内网用户地址，目的地址为服务器公网地址。如果 NGFW 仅配置目的 NAT，则服务器收到数据包的源 IP 为用户主机地址，目的地址为自身地址。当 WEB 服务器响应用户主机请求时，发出的数据包不会经过 NGFW，导致响应数据包丢失，因此需在 NGFW 上设置双向地址转换规则。配置双向 NAT 规则方法如下图“NAT 规则”所示。

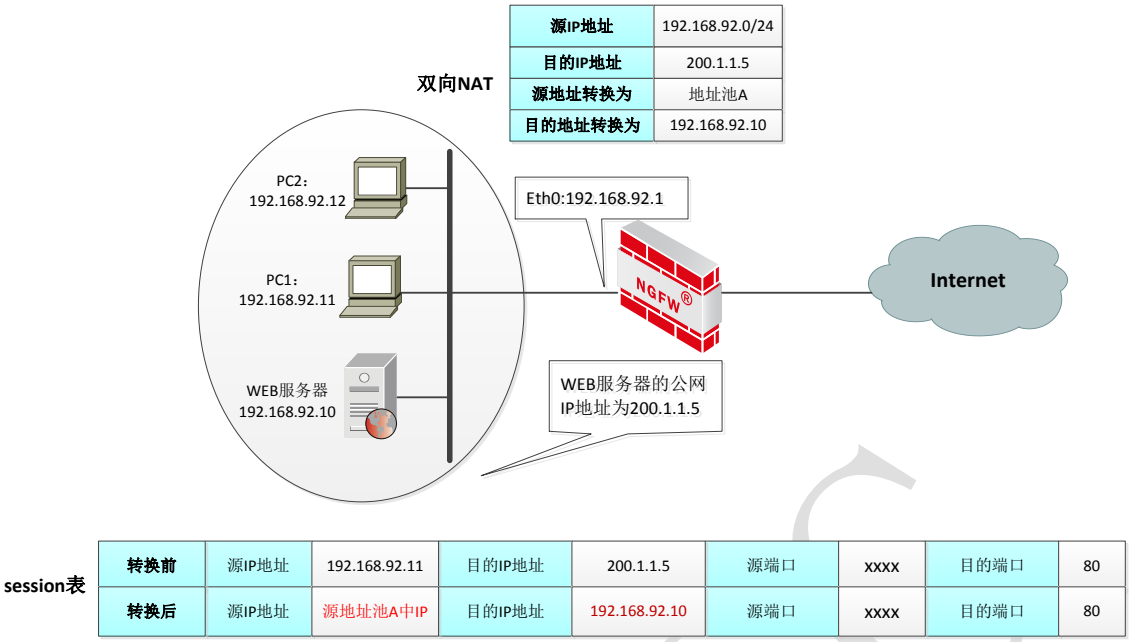


图 7-6 双向地址转换示意图

内网用户通过公网 IP 地址访问 WEB 服务器时，NGFW 处理数据流程如下：

1）NGFW 接收到用户访问 WEB 服务器的数据包后，按顺序匹配 NAT 规则表，发现有匹配数据报文的双向 NAT 规则，停止检索。

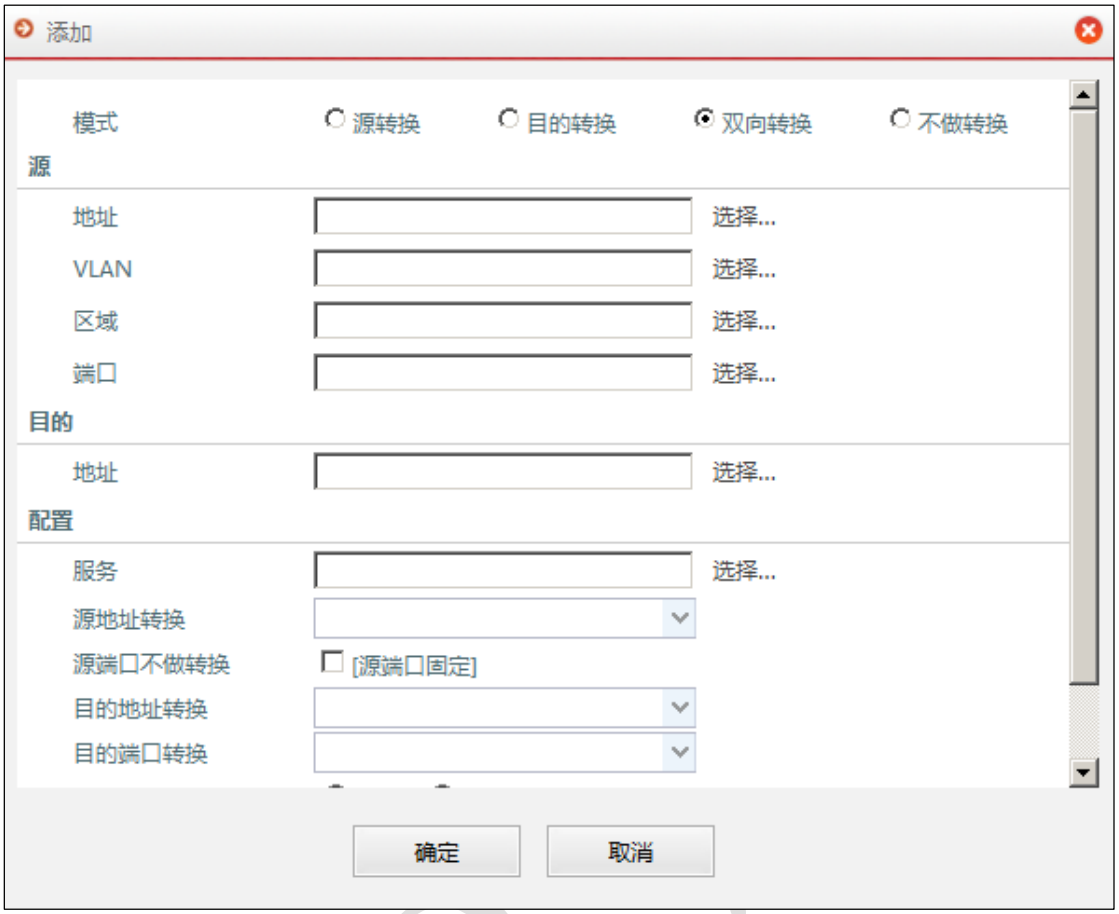
2）根据成功匹配的 DNAT 规则，目的地址转换为 192.168.92.10，源地址转换为双向 NAT 的源地址池中的地址，并创建会话，然后将用户请求报文转发至 WEB 服务器。

3）NGFW 接收到服务器的响应报文后，根据步骤 2）创建的会话表，将报文的源地址用户真正 IP 地址，然后将报文发送给用户。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **地址转换**。

步骤 2 点击『添加』，弹出添加 NAT 规则窗口，然后选择 NAT 模式为“双向转换”，如下图所示。



在添加双向 NAT 规则时，各项参数的具体说明如下表所示。

参数	说明
源地址	配置数据报文的源地址应满足的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象，关于地址对象的定义具体请参见 7.1.2 地址。
源 VLAN	配置数据报文的源 VLAN 应满足的条件。
源区域	配置数据报文的源区域应满足的条件。
源端口	配置数据报文的源端口应满足的条件。
目的地址	配置数据报文的目的地址应当匹配的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的资源对象。
服务	选择匹配的服务对象，可以选择一个或多个。
源地址转换	可项项。选择转换后的主机地址、地址范围对象或区域对象。 说明： 1）选择主机地址对象时，表示将源地址固定映射为某一合法 IP 地址； 2）选择地址范围对象时，将源地址动态映射为某一网段或某一地址范围的地址； 3）选择区域对象时，将源地址转换为具有该区域的物理接口的地址（默认映射为端口的主地址）。因此要求区域对象必须与物理接口绑定。

参数	说明
源端口不做转换	系统默认情况下，在源地址转换同时也会转换源端口。如果勾选该选项，表示数据包在经过 NGFW 系统时将固定源端口而不对源端口进行随机转换。
目的地址转换	可选项。选择转换后的目的地址，可以选择具体的主机地址，或者选择已设定的地址对象等。 说明： “目的地址转换”和“目的端口转换”参数必须至少设置一项。
目的端口转换	可选项。设置转换后的服务端口，可以选择系统预定义的服务或用户自定义的服务。 说明： “目的地址转换”和“目的端口转换”参数必须至少设置一项。
策略开关	启动后该 NAT 规则才会生效。默认为启用状态。
Sticky NAT 开关	地址粘性开关。启动后，相同源 IP 的数据包经过地址转换后为其转换的源 IP 地址相同。

说明

✧ 如果在某一条 NAT 规则中设置了多个条件，则数据包必须同时满足这些条件才认为成功匹配该规则，才根据规则相应的动作转换数据包的 IP 地址或端口。

步骤 3 点击【确定】按钮完成 DNAT 规则的配置。

CLI 方式配置

nat policy add [**enable** <yes|no>] [**vr_id** <*string1*>] [**orig_src** <*string2*>] [**orig_sport** <*string3*>] [**srcarea** <*string4*>] [**srcvlan** <*string5*>] [**orig_dst** <*string6*>] [**orig_service** <*string7*>] **trans_src** <*string8*> [**pat** <yes|no>] **trans_dst** <*string9*> [**trans_service** <*string10*>] [**sticky** <yes|no>]

命令描述：

增加一条双向 NAT 策略。

参数说明：

nat policy add	增加双向地址转换策略。
enable	可选项，设定地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示暂时禁用这条地址转换策略。默认值为“yes”。
vr_id	可选项，设定该地址转换策略所属的虚拟路由域。
string1	数值类型，表示 VR。
orig_src	可选项，设定所匹配报文的源地址对象。

string2	字符串类型，表示所匹配报文的源地址对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	可选项，设定所匹配报文的源端口对象。
string3	字符串类型，表示所匹配报文的源端口对象名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
srcarea	可选项，设定所匹配报文的源区域。
string4	字符串类型，表示所匹配报文的源区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称。 2）可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
srcvlan	可选项，设定所匹配报文的源 VLAN。
string5	字符串类型，表示所匹配报文的源 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称。 2）可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’vlan.0001 vlan.0002’。
orig_dst	可选项，设定所匹配报文的目的地址对象。
string6	字符串类型，表示所匹配报文的目的对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_service	可选项，设定所匹配报文的服务资源。
string7	字符串类型，表示所匹配报文的服务资源名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
trans_src	必选项，设定转换后的源地址对象。
string8	字符串类型，表示转换后的源对象名称。 说明： 1）该参数值必须是已经定义的地址对象或属性名称。 2）只能输入一个对象。 3）添加源地址转换策略时，该参数值必须设置。
pat	可选项，设定源端口转换开关。
yes|no	yes 表示对源端口进行端口转换；no 表示不对源端口进行端口转换。默认值为“yes”。
trans_dst	可选项，设定转换后的目的地址对象。必须保证该参

	数与 trans_service 参数至少设置一项。
string9	字符串类型，表示转换后的目的对象名称。 说明： 1）该参数值必须是已经定义的主机地址对象或均衡组对象名称。 2）只能输入一个对象名。 3）添加目的地址转换策略时，该参数值必须设置。
trans_service	可选项，设定转换后的服务资源。必须保证该参数与 trans_dst 参数至少设置一项。
string10	字符串类型，表示转换后的服务资源的名称。 说明： 该参数值必须是 define 模块已经定义的名称。
sticky	可选项，设定是否开启地址转换策略的快速开关。
yes|no	是|否

以下是增加一条双向地址转换策略的示例：

增加一条使内网用户 A 可通过 NGFW 访问内网 WEB 服务器的 NAT 规则。1）用户 A 的 IP 地址为“192.168.89.220/24”（地址对象名称为“89.220”），转换后地址为“10.10.10.20”（地址对象名称为“nat_address2”）；2）WEB 服务器的 IP 地址为“192.168.83.234/24”（地址对象名称为“83.234”），转换后地址为“10.10.10.23”（地址对象名称为“nat_address3”）；3）WEB 服务器通过自定义的 8080 端口提供 WEB 服务（自定义服务资源名称为“HTTP8080”）。

TopsecOS# **define host add name** *89.220* **ipaddr** *192.168.89.220*

TopsecOS# **define host add name** *nat_address2* **ipaddr** *10.10.10.20*

TopsecOS# **define host add name** *83.234* **ipaddr** *192.168.83.234*

TopsecOS# **define host add name** *nat_address3* **ipaddr** *10.10.10.23*

TopsecOS# define **service add name** *http80* **protocol** *6* **port1** *80*

TopsecOS# **define service add name** *http8080* **protocol** *6* **port1** *8080*

TopsecOS#**nat policy add enable** yes **orig_src** *89.220* **orig_dst** *83.234* **orig_service** *http80* **trans_src** *nat_address2* **trans_dst** *nat_address3* **trans_service** *http8080*

TopsecOS# **nat policy show**

ID 8017 nat policy add orig_src '89.220 ' orig_dst '83.234 ' orig_service 'http80'trans_src nat_address2 trans_dst nat_address3 trans_service http8080 vr_id 0 hit-session 0

nat policy show <cr>

命令描述：

查看所有 NAT 策略。

以下为查看所有 NAT 策略的示例：

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01 vr_id 0 hit-session 0
ID 8012 nat policy add orig_dst 'nat_address1 ' orig_service 'http8080 'trans_dst
web_server1 vr_id 0 hit-session 0
ID 8017 nat policy add orig_src '10.22 ' orig_dst '83.234 ' orig_service 'http80
'trans_src nat_address2 trans_dst nat_address3 trans_service http8080 vr_id 0 hit-
session 0
```

nat policy move <*number1*> **after** <*number2*>

命令描述：

移动 NAT 策略。

参数说明：

nat policy move	移动 NAT 策略。
number1	数值类型，表示待移动 NAT 策略的 ID。
after	必选项。将待移动 NAT 策略移动的基准 NAT 策略之后。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之后。

```
TopsecOS# nat policy move 8017 after 8062
```

nat policy move <*number1*> **before** <*number2*>

命令描述：

移动一条 NAT 策略。

参数说明：

nat policy move	移动一条 NAT 策略。
number1	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
before	必选项。将待移动 NAT 策略移动的基准 NAT 策略之前。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之前。

TopsecOS# **nat policy move** *8017* **before** *8062*

nat policy del nat_id <*number*>

命令描述：

删除一条 NAT 策略。

参数说明：

nat policy del	删除一条 NAT 策略。
nat_id	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
number	数值类型，表示 NAT 策略的 ID。

以下为删除一条 NAT 策略的示例：

删除 ID 为 8008 的 NAT 策略。

TopsecOS# **nat policy show**

ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '

trans_src internet01 vr_id 0 hit-session 0

TopsecOS# **nat policy del nat_id** *8008*

nat policy clean [**vr_id** <*number*>]

命令描述：

清除 NAT 策略。

参数说明：

nat policy clean	清除 NAT 策略。
vr_id	必选项，清除属于相应 VR 的 NAT 策略。
number	数值类型，表示 VR 的 ID。

以下为清除 NAT 策略的示例：

```
TopsecOS# nat policy clean
```

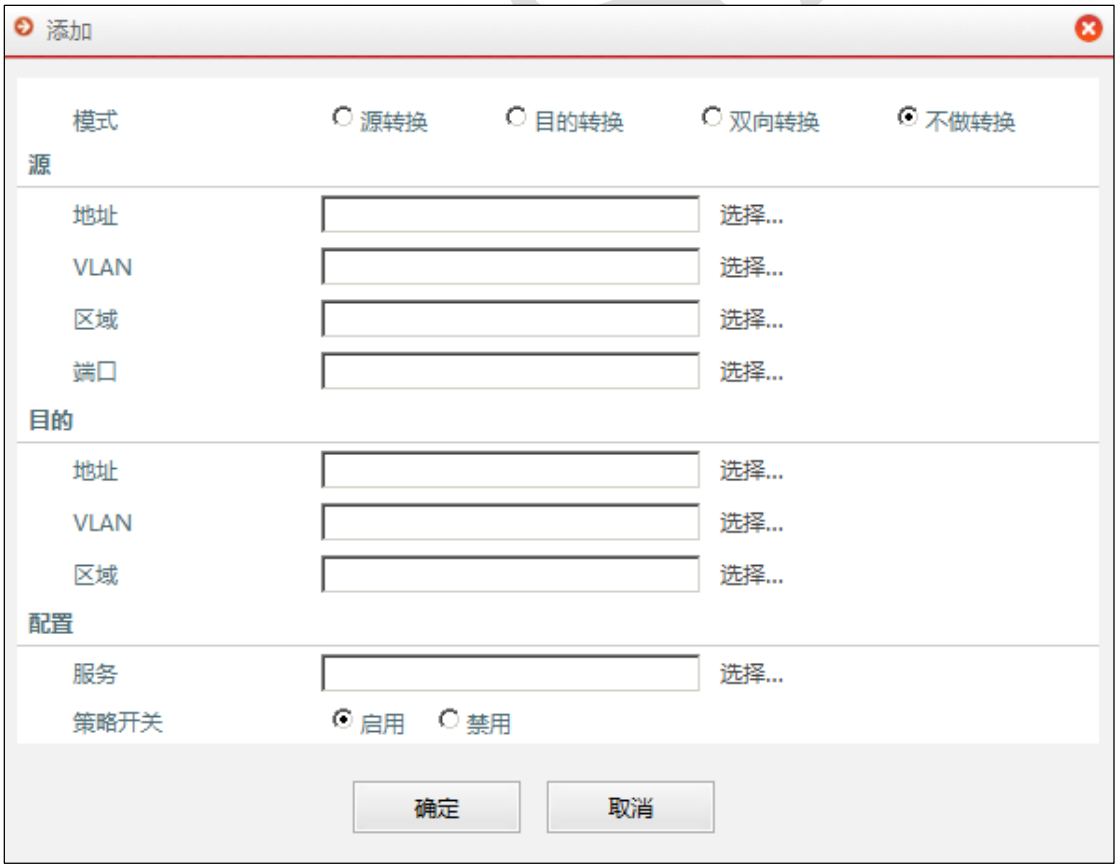
7.3.4 配置 NoNAT

NoNAT 不做地址转换，用于在已定义 SNAT、DNAT 和双向 NAT 的基础上，配置无需执行地址转换的特例。下面介绍如何配置 NoNAT 规则。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **地址转换**。

步骤 2 点击『添加』，弹出添加 NAT 规则窗口，然后选择 NAT 模式为“不作转换”，如下图所示。



在添加 NoNAT 规则时，各项参数的具体说明如下表所示。

参数	说明
源地址	配置数据报文的源地址应满足的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象，关于地址对象的定义具体请参见 7.1.2 地址。
源 VLAN	配置数据报文的源 VLAN 应满足的条件。
源区域	配置数据报文的源区域应满足的条件。
源端口	配置数据报文的源端口应满足的条件。
目的地址	配置数据报文的目的地址应当匹配的条件。 点击『选择』，弹出选择对象窗口，管理员可以选择已经定义的地址对象。
目的 VLAN	配置数据报文的目的 VLAN 应满足的条件。
目的区域	配置数据报文的目的区域应当匹配的条件。
服务	选择匹配的服务对象，可以选择一个或多个。
策略开关	启动后该 NAT 规则才会生效。默认为启用状态。

说明

- ✧ 如果在某一条 NAT 规则中设置了多个条件，则数据包必须同时满足这些条件才认为成功匹配该规则，才根据规则相应的动作转换数据包的 IP 地址或端口。

步骤 3 点击【确定】按钮完成 NoNAT 规则的配置。

CLI 方式配置

nat policy add [**enable** <yes|no>] [**vr_id** <*string1*>] [**orig_src** <*string2*>] [**orig_sport** <*string3*>] [**srcarea** <*string4*>] [**srcvlan** <*string5*>] [**orig_dst** <*string6*>] [**orig_service** <*string7*>] [**dstarea** <*string8*>] [**dstvlan** <*string9*>]

命令描述：

增加一条 NoNAT 策略。

参数说明：

nat policy add	增加一条不做地址转换策略。
enable	可选项，设定地址转换策略开关。
yes|no	yes 表示启用这条地址转换策略；no 表示暂时禁用这条地址转换策略。默认值为“yes”。
vr_id	可选项，设定该地址转换策略所属的虚拟路由域。
string1	数值类型，表示 VR。
orig_src	可选项，设定所匹配报文的源地址对象。
string2	字符串类型，表示所匹配报文的源地址对象名称。

	说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_sport	可选项，设定所匹配报文的源端口对象。
string3	字符串类型，表示所匹配报文的源端口对象名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
srcarea	可选项，设定所匹配报文的源区域。
string4	字符串类型，表示所匹配报文的源区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称。 2）可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。
srcvlan	可选项，设定所匹配报文的源 VLAN。
string5	字符串类型，表示所匹配报文的源 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称。 2）可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’vlan.0001 vlan.0002’。
orig_dst	可选项，设定所匹配报文的目的地址对象。
string6	字符串类型，表示所匹配报文的目的对象名称。 说明： 1）该参数值必须是已经定义的地址对象名称。 2）可以同时输入多个地址对象，输入格式为’test1 test2’。地址对象用单引号括起来，并且中间用空格分隔。
orig_service	可选项，设定所匹配报文的服务资源。
string7	字符串类型，表示所匹配报文的服务资源名称。 说明： 1）该参数值必须是已经定义的服务资源名称。 2）可以同时输入多个服务资源，输入格式为’server1 server2’。服务资源用单引号括起来，并且中间用空格分隔。
dstarea	可选项，设定所匹配报文的目标区域。
string8	字符串类型，表示所匹配报文的目的区域资源名称。 说明： 1）该参数值必须是已经定义的区域资源名称，可以输入一个或多个区域资源的名称，输入多个时用单引号括起来，并用空格隔开，如’area1 area2’。 2）添加目的地址转换策略时，不能设定该参数值。
dstvlan	可选项，设定所匹配报文的目的 VLAN。
string9	字符串类型，表示所匹配报文的目的 VLAN 名称。 说明： 1）该参数值必须是已经定义的 VLAN 名称，可以输入一个或多个 VLAN 的名称，输入多个时用单引号括起来，并用空格隔开，如’ vlan.0001 vlan.0002’。 2）添加目的地址转换策略时，不能设定该参数值。

以下是增加一条不做地址转换策略的示例：

增加并启用一条不做地址转换策略的特例。主机 A 访问公网不做地址转换，1）主机 A 的 IP 地址为“11.11.1.22”（地址对象名称为“22”）；2）NGFW 的 feth0 连接内网，feth1 连接公网（区域对象名称分别为“area_feth0”和“area_feth1”）。

```
TopsecOS# define host add name 22 ipaddr 11.11.1.22
TopsecOS# define area add name area_feth0 interface feth0
TopsecOS# define area add name area_feth1 interface feth1
TopsecOS# nat policy add enable yes srcarea area_feth0 orig_src 22 dstarea
area_feth1
```

nat policy show <cr>

命令描述：

查看所有 NAT 策略。

以下为查看所有 NAT 策略的示例：

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01 vr_id 0 hit-session 0
ID 8012 nat policy add orig_dst 'nat_address1 ' orig_service 'http8080 'trans_dst
web_server1 vr_id 0 hit-session 0
ID 8017 nat policy add orig_src '10.22 ' orig_dst '83.234 ' orig_service 'http80
'trans_src nat_address2 trans_dst nat_address3 trans_service http8080 vr_id 0 hit-
session 0
```

nat policy move <*number1*> **after** <*number2*>

命令描述：

移动 NAT 策略。

参数说明：

nat policy move	移动 NAT 策略。
number1	数值类型，表示待移动 NAT 策略的 ID。
after	必选项。将待移动 NAT 策略移动的基准 NAT 策略之后。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之后。

```
TopsecOS# nat policy move 8017 after 8062
```

nat policy move <*number1*> **before** <*number2*>

命令描述：

移动一条 NAT 策略。

参数说明：

nat policy move	移动一条 NAT 策略。
number1	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
before	必选项。将待移动 NAT 策略移动的基准 NAT 策略之前。
number2	数值类型，表示基准 NAT 策略的 ID。

以下为移动一条 NAT 策略的示例：

将 ID 为 8017 的 NAT 策略移动到 ID 为 8062 的 NAT 策略之前。

```
TopsecOS# nat policy move 8017 before 8062
```

nat policy del nat_id <*number*>

命令描述：

删除一条 NAT 策略。

参数说明：

nat policy del	删除一条 NAT 策略。
nat_id	必选项，设置 NAT 策略的 ID。TopsecOS# **nat policy show** <cr>命令可查看所有 NAT 策略的 ID。
number	数值类型，表示 NAT 策略的 ID。

以下为删除一条 NAT 策略的示例：

删除 ID 为 8008 的 NAT 策略。

```
TopsecOS# nat policy show
ID 8008 nat policy add srcarea 'area_feth0 ' dstarea 'area_feth1 ' orig_src '10.22 '
trans_src internet01    vr_id 0 hit-session 0
TopsecOS# nat policy del nat_id 8008
```

nat policy clean [**vr_id** <*number*>]

命令描述：

清除 NAT 策略。

参数说明：

nat policy clean	清除 NAT 策略。
vr_id	必选项，清除属于相应 VR 的 NAT 策略。
number	数值类型，表示 VR 的 ID。

以下为清除 NAT 策略的示例：

```
TopsecOS# nat policy clean
```

7.4 流量控制

7.4.1 简介

流量控制是指 NGFW 基于应用、用户、源安全区域、目的安全区域、源地址、目的地址、服务、时间段和通道优先级信息，对通过的流量进行管理和控制。在 NGFW 上部署流量控制，可以帮助网络管理员合理分配带宽资源，从而提升网络运营质量。

虚拟链路

虚拟链路是区域到区域之间通信的一条链路，关于区域的配置具体请参见 7.1.1 区域，虚拟链路通过接口对来划分。虚拟链路的设置在 NGFW 设备全局有效。

虚拟链路可以将运营商网络的通信和内部局域网的通信区分开来，分别作不同的流量管理。虚拟链路上可以配置区域间总的流量管理策略，比如区域间上行或者下行带宽，流量管理策略根据配置的带宽大小进行细分的策略，保证带宽的利用率等。

虚拟通道

虚拟通道是在虚拟链路的基础上对流量的进一步细化管理，可以基于网络连接的应用、用户、源 IP 地址、目的 IP 地址、协议、服务、时间段，对数据流设置细粒度的带宽管理策略。虚拟通道上还可以配置虚拟子通道对流量进行进一步的细化管理。

在虚拟通道及其虚拟子通道上，可以设置通道的限制带宽，保证带宽，每 IP 限速，每用户限速、优先级等功能。虚拟通道 ID 在 NGFW 设备全局有效。

- 保证带宽：保证网络中关键业务所需的带宽，当网络拥堵时，确保关键业务不受影响。
- 限制带宽：限制虚拟通道带宽，通道总的流量不得超过限制带宽。
- 优先级：虚拟通道可以设置高、中和低三个优先级，当通道拥塞时，设备将根据队列优先级的高低顺序进行调度。只有高优先级队列中的报文全部调度完毕后，才调度低优先级队列。如果多个通道的优先级相同，则按照通道由上到下顺序进行调度，通道顺序可进行调整。

白名单

虚拟通道上支持白名单功能，当匹配虚拟通道白名单指定的 IP 地址和应用时，可不进行流量策略匹配，直接进行转发。

处理流程

如下图所示，流量进入 NGFW 后的流量控制功能实现过程示意图。

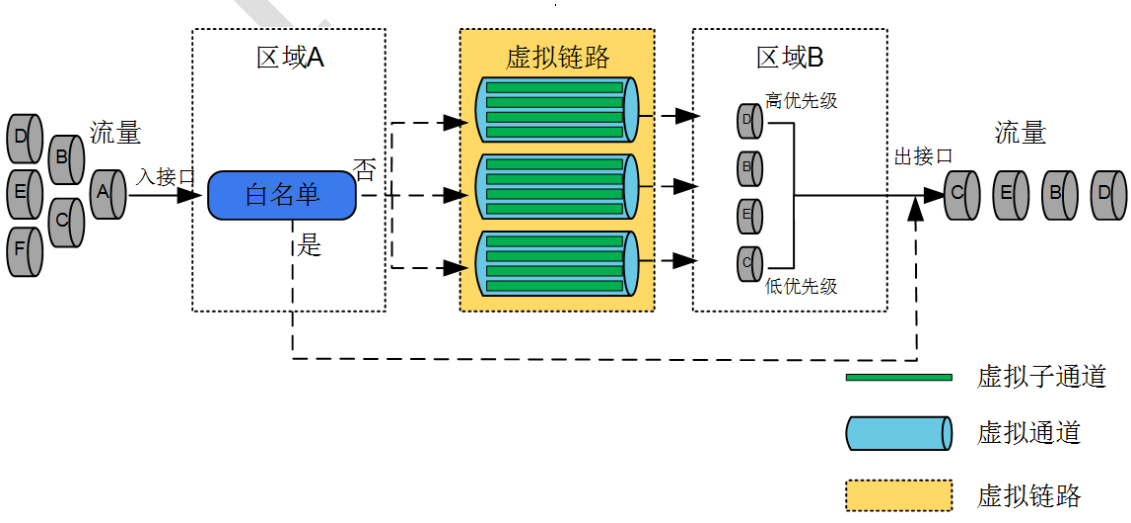


图 7-7 流量控制实现过程示意图

实现处理流程如下：

1）流量从入接口进入时，如果匹配白名单策略，将不进行流量控制策略匹配操作，直接从出接口转发；如果不匹配白名单策略，则进行虚拟链路进行流量策略匹配。

2）流量匹配虚拟链路策略，经过虚拟链路的分流后，进入相应的虚拟通道和虚拟子通道进行处理。虚拟通道和虚拟子通道的处理包括：

- 丢弃超过预先定义的最大带宽的流量。
- 标记流量的优先级，作为后续队列调度的依据。

3）流量从出接口发送时，受接口带宽的限制。如果流量大于接口带宽，将根据标记的优先级对流量进行队列调度，保证高优先级的报文被优先发送。

7.4.2 配置流量策略

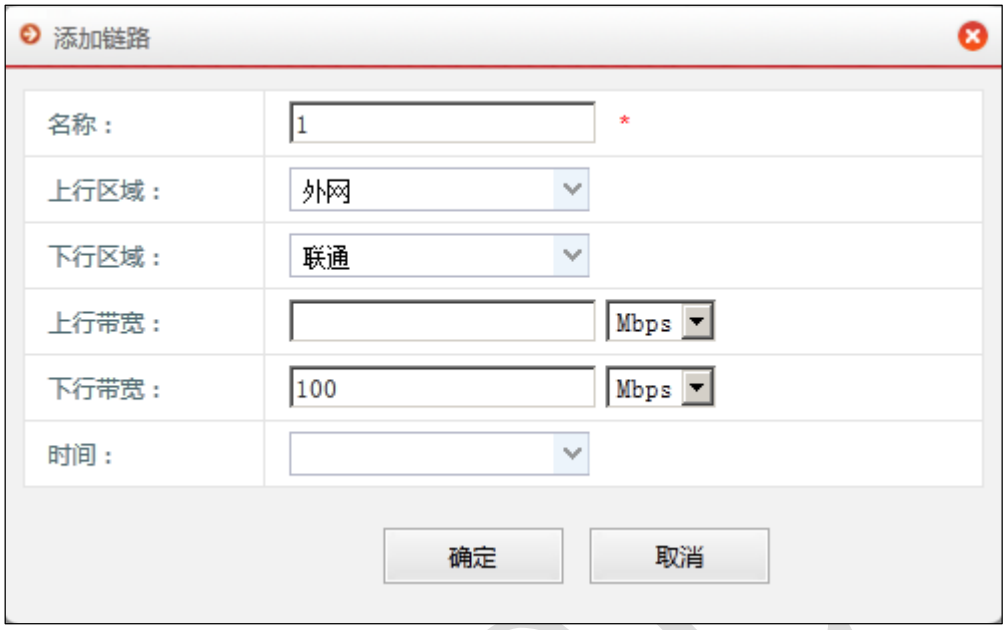
WEBUI 方式配置

步骤 1 选择 **安全策略** > **流量控制** > **流量策略**。

步骤 2 配置虚拟链路。

在两个区域之间可以设置多条的虚拟链路，便于不同时间段调用不同的流量控制策略。

1）点击页面下方的链路信息页签中的『添加』，在弹出的“添加链路”对话框中，配置虚拟链路信息。



在设置虚拟链路时，各项参数的具体说明如下表所示。

参数	说明
名称	设置虚拟链路的名称。
上行区域	设置虚拟链路对应的上行区域。点击下拉列表选择已设置好的区域，或者点击『添加』，新建区域，关于区域的配置具体请参见 7.1.1 区域。
下行区域	设置虚拟链路对应的下行区域。点击下拉列表选择已设置好的区域，或者点击『添加』，新建区域，关于区域的配置具体请参见 7.1.1 区域。
上行带宽	设置虚拟链路的上行带宽，取值范围：1-20000，单位：Mbps。
下行带宽	设置虚拟链路的下行带宽，取值范围：1-20000，单位：Mbps。
时间	设置虚拟链路带宽限制的应用时间。点击下拉列表选择已设置好的时间对象，或者点击『添加』，新建时间对象，关于时间对象的配置具体请参见 7.1.3 时间。

2）配置完成后，点击【确定】按钮，完成虚拟链路的创建。

步骤 3 配置虚拟通道。

1）设置虚拟通道基本信息。点击页面上方的『添加』，选择通道，在弹出的“添加”对话框的“基本信息”页签中，配置虚拟通道基本信息。

在设置虚拟通道基本信息时，各项参数的具体说明如下表所示。

参数	说明
名称	设置虚拟通道的名称。
所属链路	点击下拉列表选择虚拟通道所属的虚拟链路。
通道类型	设置虚拟通道的类型。可选项：保证带宽和限制带宽。 1）限制带宽：只限制虚拟通道的最大带宽。 2）保证带宽：可限制虚拟通道的最大带宽，还可保证通道的最低可用带宽。
上行	设置虚拟通道上行链路的最大带宽和保证带宽，单位是 Mbps。 1）最大带宽：可选项，取值范围：1-1000，如果不设置该选项，最大带宽默认取值为 1000，即 1Gbps； 2）保证带宽：必选项，在通道类型配置为保证带宽时，该选项可配置。 说明： 1）保证带宽的取值不能大于最大带宽。 2）在同一虚拟链路下可配置多个虚拟通道，通道上行最大带宽总和不能超过虚拟链路的上行带宽。
下行	设置虚拟通道下行链路的最大带宽和保证带宽，单位是 Mbps。

参数	说明
	1）最大带宽：可选项，取值范围：1-1000，如果不设置该选项，最大带宽默认取值为 1000，即 1Gbps； 2）保证带宽：必选项，在通道类型配置为保证带宽时，该选项可配置。 说明： 1）保证带宽的取值不能大于最大带宽。 2）在同一虚拟链路下可配置多个虚拟通道，通道下行最大带宽总和不能超过虚拟链路的下行带宽。
限制 IP/用户	在虚拟通道内的流量进行细化管理，可以限制每个 IP 或者每个用户的上行带宽和下行带宽。可选项：不限制、每 IP 和每用户。 1）不限制：不对通道内的 IP 或者用户流量进行限速。 2）每 IP：基于 IP 地址的流量进行限速，设置每个 IP 地址的上行带宽和下行带宽，上行带宽不能超过虚拟通道的上行带宽，下行带宽不能超过虚拟通道的下行带宽。 3）每用户：基于用户的流量进行限速，设置每个用户的上行带宽和下行带宽，上行带宽不能超过虚拟通道的上行带宽，下行带宽不能超过虚拟通道的下行带宽。

2）设置虚拟通道高级信息。在“添加”对话框中，点击“高级信息”页签，配置虚拟通道高级信息。

在设置虚拟通道高级信息时，各项参数的具体说明如下表所示。

参数	说明
地址	设置流量控制生效地址范围。点击『选择』，选择已设置好的地址范围，或者点击『添加』，新建地址范围，关于地址对象的配置具体请参见 7.1.2 地址。
用户	设置流量控制生效用户范围。点击『选择』，选择已设置好的用户范围，或者点击『添加』，新建用户，关于用户对象的配置具体请参见 5.1 用户管理。
服务	设置流量控制生效服务范围。点击『选择』，选择已设置好的服务范围，或者点击『添加』，新建服务，关于服务对象的配置具体请参见 7.1.4 服务。
应用	设置流量控制生效应用范围。在下拉框中点击『添加』，新建应用对象，关于应用对象的配置具体请参见 7.1.5 应用。
时间	设置流量控制生效时间范围。点击『选择』选择已设置好的时间范围，或者点击『添加』，新建时间，关于时间对象的配置具体请参见 7.1.3 时间。
优先级	设置虚拟通道的优先级，可选项：高、中和低。 在同一虚拟链路中有多个虚拟通道，如果流量大于保证带宽、小于最大带宽，这部分流量将会与其它虚拟通道中同类型的流量竞争带宽资源。优先级越高，就会更优先获得剩余的带宽资源。
生效	设置虚拟通道的流量控制策略是否生效。可选项：启用和禁用。

3）配置完成后，点击【确定】按钮，完成虚拟通道的高级信息配置。

步骤 4 配置虚拟子通道。

点击页面上方的『添加』，选择“子通道”，在弹出的“添加”对话框中，配置虚拟子通道信息。

虚拟子通道的配置过程类似于虚拟通道，虚拟通道的基础信息页签中的“所属通道”选项可点击下拉列表选择虚拟子通道所属的虚拟通道。其余配置过程可参见上述虚拟通道的配置步骤。

虚拟子通道下还可设置子通道，共可设置 5 层虚拟通道。NGFW 支持的虚拟通道（包括子通道）个数为 100 个。

CLI 方式配置

步骤	配置命令	配置说明
1	**qos vlink add name** <*string1*> **downarea** <*string2*> **downrate** <*number1*> **uparea** <*string3*> **uprate** <*number2*> **schedule** <*string4*>	创建虚拟链路。
2	**qos chunnel add name** <*string1*> **parent** <*string2*> **qos_type** <ensure|limit> **downceil** <*number1*> **downrate** <*number2*> **upceil** <*number3*> **uprate** <*number4*> [**node_limit** <ip|user>] **downnrate** <*number5*> **upnrate** <*number6*> **ipaddr** <*ipaddress*> **user** <*string3*> **service** <*string4*> **app** <*string5*> **schedule** <*string6*> **qos_pri** <high|normal|low> **enable** <yes|no>	创建虚拟通道。
3	**qos chunnel move name** <*string1*> <**before** <*string2*>|**after** <*string3*>>	（可选）移动虚拟通道。
4	**qos vlink show** <cr>	查看所有虚拟链路信息。
5	**qos chunnel show** <cr>	查看所有虚拟通道信息。

qos chunnel add name <*string1*> **parent** <*string2*> **qos_type** <ensure|limit> **downceil** <*number1*> **downrate** <*number2*> **upceil** <*number3*> **uprate** <*number4*> [**node_limit** <ip|user>] **downnrate** <*number5*> **upnrate** <*number6*> **ipaddr** <*ipaddress*> **user** < *string3*> **service** <*string4*> **app** <*string5*> **schedule** <*string6*> **qos_pri** <high|normal|low> **enable** <yes|no>

命令描述：

添加虚拟通道或者虚拟子通道。

可使用 **qos chunnel del name** <*string1*>删除虚拟通道或者虚拟子通道。

参数说明：

qos chunnel add	必选项，添加虚拟通道。
name	虚拟通道名称。
string1	字符串类型，表示虚拟通道名称。
parent	虚拟通道的父策略，如果添加的虚拟通道，其父策略应为虚拟链路，如果添加的是虚拟子通道，父策略应为虚拟通道。
string2	字符串类型，表示虚拟通道的父策略名称。
qos_type	虚拟通道的通道类型。
ensure|limit	保证带宽|限制带宽。
node_limit	每用户或者每 IP 的限速规则。如果不选择该参数表示不设置每用户或者每 IP 的限速规则。
ip|user	每 IP|每用户
downceil	虚拟通道或者虚拟子通道的下行最大带宽。
number1	数值类型，取值范围：1-20000，单位：Mbps。 不得超过其继承的父策略下行最大带宽。
downrate	设置虚拟通道类型为保证带宽时，设置虚拟通道或者虚拟子通道的下行保证带宽。
number2	数值类型，取值范围：1-20000，单位：Mbps。 不得超过其继承的父策略下行保证带宽。
upceil	虚拟通道或者虚拟子通道的上行最大带宽。
number3	数值类型，取值范围：1-20000，单位：Mbps。 不得超过其继承的父策略上行最大带宽。
uprate	设置虚拟通道类型为保证带宽时，设置虚拟通道或者虚拟子通道的上行保证带宽。
number4	数值类型，取值范围：1-20000，单位：Mbps。 不得超过其继承的父策略上行保证带宽。
downnrate	设置每用户或者每 IP 的限速规则后，设置每用户或者每 IP 的下行限制带宽。
number5	数值类型，取值范围：1-20000，单位：Mbps。 不得超过通道或者子通道的下行最大带宽。
upnrate	设置每用户或者每 IP 的限速规则后，设置每用户或者每 IP 的上行限制带宽。
number6	数值类型，取值范围：1-20000，单位：Mbps。 不得超过通道或者子通道的上行最大带宽。
ipaddr	流量控制生效 IP 地址范围。
ipaddress	IPv4 地址字符串，IPv4 地址格式为 A.B.C.D。
user	流量控制生效用户范围。
string3	字符串类型，表示用户对象名称。
service	流量控制生效服务范围。
string4	字符串类型，表示服务对象名称。
app	流量控制生效应用范围。
string5	字符串类型，表示应用对象名称。
schedule	流量控制生效时间。
string6	字符串类型，表示时间对象名称。
qos_pri	虚拟通道的优先级。在同一虚拟链路中有多个虚拟通道，如果流量大于保证带宽、小于最大带宽，这部分流量将会与其它虚拟通道中同类型的流量竞争带宽资源。优先级越高，就会更优先获得剩余的带宽资源。
high|normal|low	高|中|低。

enable	设置虚拟通道的流量控制策略是否生效。
yes|no	生效|不生效。

以下为添加虚拟通道的示例：

TopsecOS# **qos chunnel add name** *chunnel1* **parent** *vlink1* **qos_type** limit **downceil** 300 **downrate** 10 **upceil** 200 **uprate** 10 **qos_pri** high **enable** yes

qos chunnel move name <*string1*> <**before** <*string2*>|**after** <*string3*>>

命令描述：

移动虚拟通道。

参数说明：

qos chunnel **move**	必选项，移动虚拟通道。
name	虚拟通道名称。
string1	字符串类型，表示待移动的虚拟通道的名称。
before	可选项，移动到指定的虚拟通道之前。
string2	字符串类型，表示参照物虚拟通道的名称。
after	可选项，移动到指定虚拟通道之后。
string3	字符串类型，表示参照物虚拟通道的名称。

以下是移动虚拟通道的示例：

将名为“test10”的虚拟通道移动到名为“test20”的虚拟通道之前。

TopsecOS# **qos chunnel move name** *test10* **before** *test20*

qos chunnel show <cr>

命令描述：

显示所有的虚拟通道信息。

以下为显示虚拟通道的示例：

显示虚拟通道信息。

TopsecOS# **qos chunnel show**

ID 10205 qos chunnel add name abc parent 5 qos_type ensure uprate 200Mbps upceil 1Gbps downrate 50Mbps downceil 1Gbps qos_pri normal up_qos_id: 250066 down_qos_id: 260066 match: 0

```
ID 10207 qos chunnel add name 1234 parent abc qos_type ensure uprate 2Mbps upceil
100Mbps downrate 10Mbps downceil 50Mbps qos_pri normal up_qos_id: 250067
down_qos_id: 260067 match: 0
```

qos level show name <*string1*>

命令描述：

查看虚拟通道子通道配置信息。

以下为查看流量控制白名单的示例：

```
TopsecOS# qos level show name
ID 10856 qos chunnel add name 12345 parent 1234 qos_type limit upceil 10Mbps
downceil 100Mbps qos_pri normal up_qos_id: 250068 down_qos_id: 260068 match:
0
```

qos node show chunnel_name <*string1*> [**detail**]

命令描述：

查看虚拟通道中每 IP 或者每用户的流量统计信息。

参数说明：

qos node show	必选项，查看虚拟通道中每 IP 或者每用户的流量统计信息。
chunnel_name	虚拟通道名称。
string1	字符串类型，表示虚拟通道名称。
detail	流量的详细统计信息。

qos vlink add name <*string1*> **downarea** <*string2*> [**downrate** <*number1*>] **uparea** <*string3*> [**uprate** <*number2*>] [**schedule** <*string4*>]

命令描述：

添加虚拟链路。

可使用 **qos vlink del name** <*string1*>删除虚拟链路。

参数说明：

qos vlink add	添加虚拟链路。
name	必选项，设置虚拟链路名称。
string1	字符串类型，表示虚拟链路名称。
downarea	必选项，设置虚拟链路的下行区域名称。
string2	字符串类型，表示虚拟链路下行区域名称。
downrate	可选项，设置虚拟链路下行带宽。
number1	数值类型，取值范围：1-20000，单位：Mbps。
uparea	必选项，设置虚拟链路的上行区域名称。
string3	字符串类型，表示虚拟链路上行区域名称。
uprate	可选项，设置虚拟链路上行带宽。
number2	数值类型，取值范围：1-20000，单位：Mbps。
schedule	可选项，设置流量控制生效时间。
string4	字符串类型，表示时间对象名称。

以下为添加虚拟链路的示例：

TopsecOS# qos vlink add name *vlink1* **downarea** *area1* **downrate** *1000* **uparea** <*string3*> **uprate** *area1* **schedule** *everythu*

qos vlink show <cr>

命令描述：

查看虚拟链路配置信息。

以下为显示虚拟通道的示例：

查看虚拟链路配置信息。

TopsecOS# **qos vlink show**

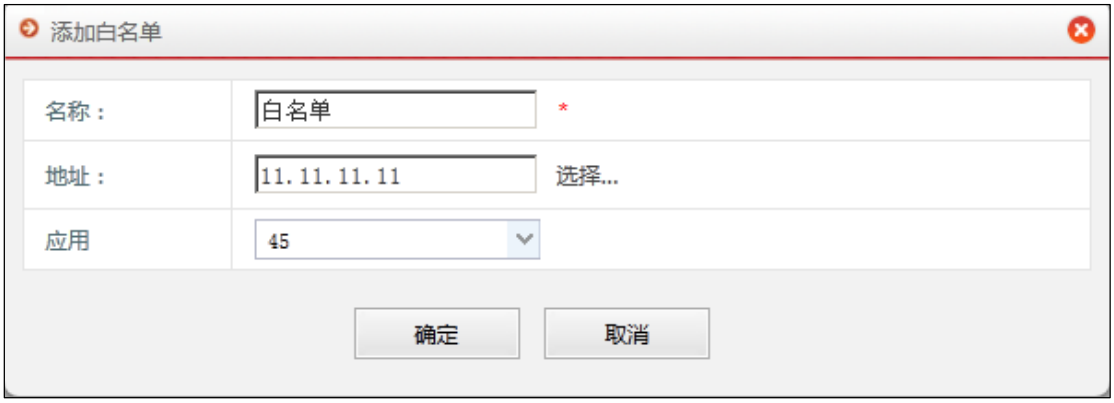
ID 10173 qos vlink add name 5 downarea 23 uparea area_feth0 uprate 1Gbps downrate 1Gbps freeid 64000

7.4.3 配置白名单

WEBUI 方式配置

白名单功能可配置指定 IP 地址和应用不进行流量策略匹配，直接进行转发。

步骤 1 选择 **安全策略** > **流量控制** > **白名单**。



步骤 2 点击『添加』，在弹出的“添加白名单”对话框中，配置白名单信息。

在设置白名单时，各项参数的具体说明如下表所示。

参数	说明
名称	设置白名单的名称。
地址	设置白名单的生效地址范围。点击下拉列表选择已设置好的时间对象，或者点击『选择』，新建地址对象，关于地址对象的配置请参见 7.1.2 地址。
应用	设置白名单的生效应用范围。点击下拉列表选择已设置好的时间对象，或者点击『添加』，新建应用对象，关于应用对象的配置请参见 7.1.5 应用。

步骤 3 配置完成后，点击【确定】按钮，完成白名单的创建。

CLI 方式配置

步骤	配置命令	配置说明
1	**qos excep_policy add name** <*string1*> **ip** <*ipaddress*> **app** <*string2*>	添加流量控制白名单。
2	**qos excep_policy show** <cr>	显示流量控制白名单信息。

qos excep_policy add name <*string1*> [**ip** <*ipaddress*>] [**app** <*string2*>]

命令描述：

添加流量控制白名单。

可使用 **qos excep_policy del name** <*string1*>删除流量控制白名单。

参数说明：

qos excep_policy add	添加白名单。
name	必选项，设置白名单名称。

string1	字符串类型，表示白名单名称。
ip	可选项，设置流量控制白名单生效 IP 地址范围。
ipaddress	字符串类型，表示地址对象名称。
app	可选项，设置流量控制白名单生效应用范围。
string2	字符串类型，表示应用对象名称。

以下为添加流量控制白名单的示例：

TopsecOS# **qos excep_policy add name** *excep1* **ip** *ip-name* **app** *appname*

qos excep_policy show <cr>

命令描述：

查看流量控制白名单配置信息。

以下为查看流量控制白名单的示例：

TopsecOS# **qos excep_policy show**

qos excep_policy add name 1233 ip '123 add' app 'fuwu'

7.5 本机服务

本机服务就是设备本身提供的管理服务或者信息服务，如 WEBUI、Telnet、SSH、DHCP 等。

通过本机服务模块，管理员可对区域对象或地址对象添加支持的本机服务，并通过配置对本机端口的访问控制规则，允许设备在相应的物理接口接收用户的连接请求。如果设备要接收管理员发出的管理或监控的连接请求，设备上相应的系统服务进程还必须处于“启动”状态，否则无法接收用户的连接请求。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **本机服务**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置本机服务时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置 NGFW 支持规则控制的服务类型。可选项：snmp、ssh、ping、telnet、ntp、dhcp、webui、dns、ipsecvpn。 1）snmp：允许设备与 snmp 管理主机进行通信。 2）ssh：接收 SSH 协议远程管理请求；允许管理员通过 SSH 方式对设备进行配置和管理。 3）ping：允许管理员可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址，还支持 NGFW PING 其他网络设备的 IPv6 接口，以及支持其他网络设备 PING 防火墙的 IPv6 接口。 4）telnet：接收 Telnet 协议远程管理请求。 5）ntp：用于计算机时间同步化的一种协议，能够使计算机对其服务器或时钟源做同步化，提供高精准度的时间校正。NGFW 作为 NTP 服务器为其他网络设备提供 NTP 服务； 6）dhcp：允许设备作为 DHCP/DHCPv6 服务器、DHCP/DHCPv6 客户端或 DHCP/DHCPv6 中继使用。 7）webui：开放该服务用于允许管理员通过 WEBUI 对设备进行配置和管理。 8）dns 服务：允许设备作为 DNS 服务器进行域名解析。 9）ipsecvpn：允许设备与 VPN 设备建立 IPSec VPN 隧道进行通信。 说明： 开放用户通过 IPv4 或 IPv6 地址采用 WEBUI、SSH、Telnet 方式管理 NGFW 的服务均使用该参数，只是控制可管理 NGFW 的主机对象不同，对于 IPv4 主机，控制地址为 IPv4 地址对象；对于 IPv6 主机，控制地址为 IPv6 地址对象。
区域	必选项，设置本机服务支持的区域对象。 说明： “区域”和“地址”不能全部为空。
地址	必选项，设置本机服务支持的地址对象。 说明： 1）“区域”和“地址”不能全部为空。 2）当本机服务为“dhcp”时，该参数不可配置。

点击【确定】按钮完成本机服务的添加。

CLI 方式配置

步骤	配置命令	配置说明
1	**define area add name** <*string1*> **interface** <*string2*> [**comment** <*string3*>]	配置区域及其属性

2	**pf service add name** <telnet|webui|ssh|ping|ntp|dhcp|snmp|dns> **area** <*string1*> **addressname** <*string2*>	配置本机服务

pf service add name <telnet|webui|ssh|ping|ntp|dhcp|snmp|dns|ipsecvpn > **area** <*string1*>

addressname <*string2*>

pf service add name dhcp **area** <*string*>

命令描述

添加本机服务。

参数说明

pf service add	添加本机服务。
name	必选项，设置服务名称。
telnet|webui|ssh|ping|ntp|dhcp|snmp|dns|ipsecvpn	1）telnet：接收 Telnet 协议远程管理请求。 2）webui：当 NGFW 不包含 SSL VPN 模块时，开放该服务用于允许管理员通过 WEBUI 的 443 端口对设备进行配置和管理。 当 NGFW 包含 SSL VPN 模块时，要实现管理员通过 WEBUI 对设备进行管理无需开放该服务，只需开放 SSLVPNMGR 服务。要实现普通管理员通过 443 端口访问设备时只需开放 SSLVPN 服务。 3）ssh：接收 SSH 协议远程管理请求；允许管理员通过 SSH 方式对设备进行配置和管理。 4）ping：允许管理员可以 PING 到设备的物理接口地址、VLAN 虚接口和子接口的地址。 5）ntp（Network Time Protocol）：用于计算机时间同步化的一种协议，能够使计算机对其服务器或时钟源做同步化，提供高精准度的时间校正。NGFW 作为 NTP 服务器为其他网络设备提供 NTP 服务。 6）dhcp：允许设备作为 DHCP/DHCPv6 服务器、DHCP/DHCPv6 客户端或 DHCP/DHCPv6 中继使用。 7）dns：允许设备作为 DNS 服务器进行域名解析。 8）snmp：允许设备与 snmp 管理主机进行通信。 9）ipsecvpn：允许设备与 VPN 设备建立 IPSec VPN 隧道进行通信。
area	必选项，设置本机服务支持的区域对象。 说明： 区域参数和地址参数不能全部为空。
string1	字符串类型。
addressname	必选项，设置本机服务支持的地址对象。
string2	字符串类型。

以下是添加本机服务的示例：

添加名称为 telnet 的本机服务，支持的区域对象为 area_feth0。

```
TopsecOS# define area add name area_feth0 interface feth0
TopsecOS# pf service add name telnet area area_feth0
```

pf service modify name <telnet|webui|ssh|ping|ntp|dhcp|snmp|dns> **id** <*number*> [**area** <*string1*>] [**addressname** <*string2*>]

命令描述

修改本机服务访问控制规则。

pf service show <cr>

命令描述

查看所有本机服务访问控制规则。

以下是查看所有本机服务访问控制规则的示例：

```
TopsecOS# pf service show
ID 10294 pf service add name ssh area area_feth0
ID 10296 pf service add name webui area area_feth0
ID 10297 pf service add name ping area area_feth0
ID 10458 pf service add name telnet area area_feth0
ID 10589 pf service add name ssh area area_feth0 addressname 123
```

pf switch <on|off|status>

命令描述

设置本机服务访问控制开关。

参数说明

pf switch	必选项，设置本机服务访问控制开关。
on|off|status	打开|关闭|显示状态

以下是显示本机服务访问控制开关状态的示例：

```
TopsecOS# pf switch status
```

pf switch is on

7.6 ALG

对于多连接协议，其子连接通信的地址和端口由父连接协商获得，且自动协商的子连接的通信地址和端口存在于父连接数据报文的应用层中。NGFW 支持 ALG 功能，可以对父连接的应用层信息进行解析，获取子连接信息，实现对多连接协议的父连接和子连接均进行控制。

如 FTP 协议，FTP 子连接（数据连接）通信的地址和端口是通过 FTP 父连接（控制连接）协商获得，FTP 父连接需由安全策略引擎处理时，其子连接也需要由相应的安全策略处理。NGFW 为确保 FTP 子连接能通过 NGFW，处理流程为：

1）解析 FTP 的父连接的应用层，获取到 FTP 子连接通信的目的地址和目的端口，并通过 FTP 父连接 IP 报头获取 FTP 子连接相应的源地址等信息；

2）根据获取的 FTP 协议子连接的源地址、目的地址和端口等信息创建一个期待连接，并将该期待连接添加到期待连接表中；

3）在期待连接中记录标记和期待连接通过安全引擎时所需要用到的地址端口；

4）FTP 协议子连接到来时，NGFW 会根据子连接的源地址、目的地址和目的端口查询期待连接表，如果子连接匹配期待连接，则根据期待连接处理子连接。

说明

- ✧ NGFW 处理多连接协议时，根据对父连接进行解析而自动生成相应的子连接规则，因此，在配置多连接协议的安全策略时，只需考虑父连接如何配置即可。

除 FTP 协议外，NGFW 还为 TFTP、SQLNET 和 PPTP 协议提供 ALG 功能，下面介绍如何开启 FTP、TFTP、SQLNET 和 PPTP 协议的 ALG 功能。

WebUI 方式配置

步骤 1 选择 **安全策略** > **ALG**。

步骤 2 勾选 FTP、TFTP、SQLNET、PPTP 对应的选择框，即可启用相应协议的 ALG 功能。

步骤 3 配置完成后，点击【应用】按钮，完成 ALG 功能配置。

步骤 4 （可选）点击【重置】按钮，可以恢复 ALG 功能为出厂配置。

CLI 方式配置

alg config set protocol [ftp|tftp|sqlnet|pptp] **enable** <yes|no>

命令描述

设置应用协议的 ALG 功能开关。

参数说明

alg config set protocol	设置应用协议的 ALG 功能开关。
ftp|tftp|sqlnet|pptp	FTP 协议|TFTP 协议|SQLNET 协议|PPTP 协议 如果不选择该参数，则表示开启所有应用协议的 ALG 功能。
enable	设置开启功能开关。
yes|no	是|否

以下是开启所有应用协议的的 ALG 的示例：

```
TopsecOS# alg config set protocol enable yes
```

alg config show <cr>

命令描述

查看应用协议的 ALG 功能开关状态。

以下是查看应用协议服务的的 ALG 的示例：

```
TopsecOS# alg config show
alg config set protocol ftp enable yes
alg config set protocol tftp enable yes
alg config set protocol sqlnet enable yes
alg config set protocol pptp enable yes
```

alg config reset <cr>

命令描述：

恢复 ALG 功能为出厂配置，此时将开启 FTP、TFTP、SQLNET 和 PPTP 应用协议的 ALG 功能。

以下是恢复 ALG 功能为出厂配置的示例：

```
TopsecOS# alg config reset
```

7.7 入侵防御

7.7.1 简介

入侵防御系统（IPS，Intrusion Prevention System）能够实时监控网络攻击，检测入侵，并根据配置对网络攻击进行告警、拦截等操作，保护网络安全。入侵防御是一种主动积极的入侵防范阻止系统。检测到攻击企图时会自动将攻击包丢掉，有效地实现了主动防御功能。

入侵防御既能发现又能及时阻止入侵行为，通过检测发现网络入侵后，能根据防御规则自动丢弃入侵报文，从而从根本上避免攻击行为。入侵防御主要有如下优势。

- 实时主动防御：设备一般采用直路透明方式部署在网络中，在检测到入侵时，能实时阻止入侵行为、拦截攻击性流量，提高网络的安全性，避免造成损失。

- 内外兼防：同时对经过设备的出入方向流量进行监控，同时防御来自网络内部和外部的攻击。
- 深层防护：传统的防御仅可对 TCP/IP 协议的三层和四层进行检查，不能监测应用的内容，传统防火墙的包过滤功能不会针对每个字节进行检查，因而也无法发现攻击活动。而 IPS 可以做到逐一字节地检查数据包，能够从数据流中检测出二层到七层的攻击，还可以对网络数据进行流重组，并根据攻击类型和防御策略对网络中流量进行放行或者拦截，对网络进行深层防护。
- 支持规则升级：网络中随时会出现各种各样的攻击，高质量的入侵特征库可以有效提高攻击防御效果，IPS 还支持升级入侵特征库，以保持入侵防御的持续有效性和最高水平的安全性。

NGFW 的入侵防御功能是基于模式匹配和异常检测技术对网络数据进行在线数据解析和攻击检测的网络安全解决方案。它通过对数据包进行规则匹配，对异常的数据包进行主动防御，从而保护网络的安全。

实现原理

入侵防御的实现原理如下：

1）IPS 引擎检测

NGFW 会首先进行 IP 分片报文重组以及 TCP 流重组，确保了应用层数据的连续性，有效检测出逃避入侵防御检测的攻击行为。

NGFW 能根据报文内容识别多种常见应用层协议。识别出报文的协议后，NGFW 可根据具体协议分析方案进行更精细的分析，并深入提取报文特征。

2）特征匹配

NGFW 将解析后的报文特征与防御规则集进行匹配，如果符合攻击检测规则集中的规则，则按照规则集中定义的动作进行响应处理。

3）响应处理

完成特征匹配检测后，NGFW 根据管理员配置的防御动作对匹配到防御规则的报文进行处理。

防御规则集

入侵防御规则集用来描述网络中存在的攻击行为的特征，NGFW 通过将数据流和入侵防御规则进行比较来检测和防范攻击。如果某个数据流匹配了某个防御规则时，设备会按照该防御规则的动作来处理数据流。每个防御规则都有缺省的动作，为阻断或者告警。

- 阻断：指丢弃符合防御规则的报文，并记录日志。
- 告警：指对符合防御规则的报文放行，但记录日志。

天融信入侵防御攻击检测规则库包含了所有的系统攻击检测规则，管理员可以根据具体的需求选择系统攻击检测规则，并为其选择相应的处理方式以配置攻击检测规则集。NGFW 已经预定义了入侵防御规则集，并且可以获取新的入侵防御版本来更新规则库，提高防御性能。

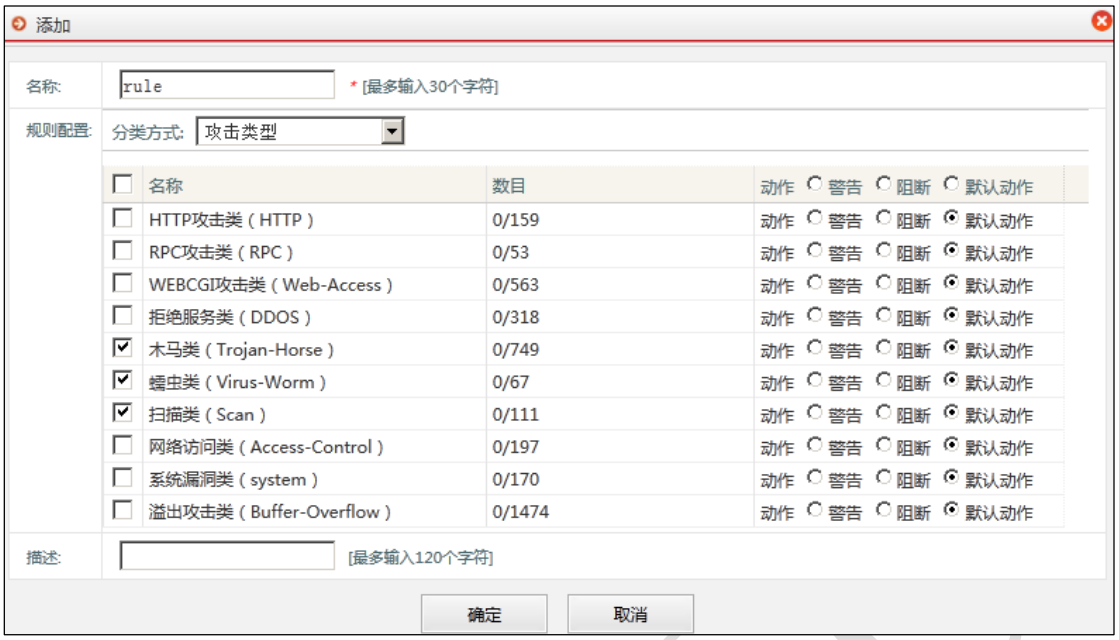
7.7.2 配置攻击检测规则集

WEBUI 方式配置

步骤 1 选择 **安全策略** > **入侵防御**。

步骤 2 添加攻击检测规则。

1）点击『添加』，弹出“添加”对话框，在对话框中添加攻击检测规则集。



在设置攻击检测规则集时，各项参数的具体说明如下表所示。

参数	说明
名称	设置攻击检测规则集名称。
规则配置	设置攻击检测规则集。 1）在分类方式下拉列表中选择攻击分类。可选项：攻击类型、精选、风险等级、流行程度和操作系统。 2）勾选分类方式名称前的复选框，选择细化的攻击防御类型，并在动作处的单选按钮选择对攻击类型的防御动作，可选项：警告、阻断和默认动作。 3）在搜索栏内输入关键字，然后点击【搜索】按钮可以在规则库中查询相关的规则。
描述	设置攻击检测规则集的描述信息。

2）设置完成后，点击【确定】按钮，完成攻击检测规则集添加。

步骤 3 修改攻击检测规则。

1）点击需要修改的攻击检测规则集对应的编辑图标“”，弹出“编辑”对话框。

2）在对话框中，勾选攻击检测规则，并可点击攻击检测规则对应的『编辑』，弹出规则对话框。

3）在规则对话框中，可修改细化的攻击检测规则。

步骤 4 复制攻击检测规则，在模板的基础上配置攻击检测规则集。

1）点击需要复制的攻击检测规则集对应的『克隆』，弹出“克隆”对话框。

2）在弹出的对话框中填写新的攻击检测规则集名称。

说明

✧ 动作操作释义如下：警告，系统对匹配到规则的报文放行且记录日志；阻断，系统对匹配到规则的报文丢弃且记录日志；记录报文，系统对匹配到规则的报文记录其详细内容。

CLI 方式配置

步骤	命令	说明
1	**ips eventset add name** <*string1*> **classby** <atk|sift|os|pop|risk> **content** <*string2*> [**msg** <*string3*>]	添加攻击检测规则集。
2	**ips eventset add-rule name** <*string1*> **rules** <*string2*>	向攻击检测规则集中添加攻击检测规则。
3	**ips eventset clean** <cr>	清空所有未被引用的规则集。
4	**ips eventset clone from** <*string1*>**to** <*string2*>	复制已有攻击检测规则集。
5	**ips eventset modify name** <*string1*> **classby** <atk|sift|os|pop|risk> **content** <*string2*> [**msg** <*string3*>]	修改攻击检测规则集。
6	**ips eventset modify-rule name** <*string1*> **rules** <*string2*>	修改攻击检测规则集中的攻击检测规则。
7	**ips eventset show-class name** <*string1*> **classby** <atk|sift|os|pop|risk>	查看规则集配置信息。
8	**ips rules update filename** <*string1*>	配置规则库升级。

ips eventset add name <*string1*> **classby** <atk|sift|os|pop|risk> **content** <*string2*> [**msg**

<*string3*>]

命令描述：

添加攻击检测规则集。

使用 **eventset delete name** <*string1*>命令删除规则集。

参数说明：

ips eventset add	添加攻击检测规则集。
name	必选项，设置规则集的名称。
string1	字符串类型，表示规则集名称。
classby	必选项，攻击检测规则分类。
atk|sift|os|pop|risk	攻击类型|精选|操作系统|流行程度|风险等级
content	必选项，设置攻击检测规则集内容。
string2	字符串类型，攻击检测规则集内容。
msg	可选项，设置规则集的描述信息。
string3	字符串类型，规则集的描述信息。

以下为添加攻击检测规则集的示例：

添加规则集 IPS_rules。

TopsecOS# **ips eventset add name** *IPS_rules* **classby** atk **content** HTTP 攻击类（HTTP）

ips eventset add-rule name <*string1*> **rules** <*string2*>

命令描述：

向攻击检测规则集中添加攻击检测规则。

使用 **ips eventset delete-rule name rules rules** <*string*>命令删除规则集中的规则。

参数说明：

ips eventset add-rule	向攻击检测规则集中添加攻击检测规则。
name	必选项，设置攻击检测规则的名称。
string1	字符串类型，表示攻击检测规则名称。
rules	必选项，设置攻击检测规则集名称。
string2	字符串类型，攻击检测规则编号及其动作。形式为“tid：动作”，其中 tid 可通过 **ips eventset show-rule class-name** <*string2*> **classby** <**atk|sift|os|pop|risk**> [**eventname** <*string1*>]命令查看；动作取值为 0 或 1，0 表示告警，1 表示阻断。支持多输入形式，多个输入直接用逗号分隔，如“tid：动作,tid：动作”

以下为向攻击检测规则集中添加攻击检测规则的示例：

向规则集 IPS_rules 中添加攻击检测规则 rule。

```
TopsecOS#ips eventset add-rule name rule rules 10986:0
```

ips eventset clean <cr>

命令描述：

清空所有未被引用的规则集。

ips eventset clone from <*string1*> **to** <*string2*>

命令描述：

复制已有攻击检测规则集。

参数说明：

ips eventset eventset addevent	向规则集中添加规则。
string1	字符串类型，指定源规则集的名称。
string2	字符串类型，由源规则集复制得到的新规则集的名称。

ips eventset modify name <*string1*> **classby** <atk|sift|os|pop|risk> **content** <*string2*> [**msg** <*string3*>]

命令描述：

修改攻击检测规则集。

参数说明：

ips eventset modify	修改规则集。
name	必选项，指定需要修改的规则集名称。
string1	字符串类型，表示规则集名称。
classby	必选项，设置攻击检测规则分类。
atk|sift|os|pop|risk	攻击类型|精选|操作系统|流行程度|风险等级
content	必选项，设置攻击检测规则集内容。
string2	字符串类型，攻击检测规则集内容。
msg	可选项，设置规则集的描述信息。
string2	字符串类型，规则集的描述信息。

ips eventset modify-rule name <*string1*> **rules** <*string2*>

命令描述：

修改攻击检测规则集中的攻击检测规则。

参数说明：

ips eventset modify-rule	修改攻击检测规则集中的攻击检测规则。
name	必选项，设置攻击检测规则的名称。
string1	字符串类型，表示攻击检测规则名称。
rules	必选项，设置攻击检测规则集名称。
string2	字符串类型，表示攻击检测规则集名称。

以下为修改攻击检测规则集中的攻击检测规则的示例：

修改规则集 IPS_rules 中的攻击检测规则 rule。

TopsecOS#**ips eventset add-rule name** *rule* **rules** *IPS_rules*

ips eventset show <cr>

命令描述：

查看所有的规则集的状态信息。

以下为查看所有的规则集状态信息的示例：

TopsecOS# **ips eventset show**

name 精选规则(默认动作) classby sift refered no total 340 high 104 medium 80 low 156 alert 225 deny 115

name risk-low classby risk refered no total 3227 high 0 medium 0 low 3227 alert 3227 deny 0

name attack-http classby atk refered yes total 159 high 46 medium 8 low 105 alert 159 deny 0

name rule classby atk refered no total 1040 high 130 medium 73 low 837 alert 111 deny 929

ips eventset show-class name <*string1*>**classby** <atk|sift|os|pop|risk>

命令描述：

查看规则集配置信息。

参数说明：

ips eventset show-class	查看规则集配置信息。
name	可选项，设置要查看的规则集的名称。
string1	字符串类型，表示规则集名称。
classby	可选项，选择分类方式。
attack	分类方式。
atk|sift|os|pop|risk	攻击类型|精选|操作系统|流行程度|风险等级

以下为查看规则集配置信息的示例：

TopsecOS# **ips eventset show-class name rule classby atk**

name HTTP 攻击类（HTTP） rule 159 of 159 action default

name RPC 攻击类（RPC） rule 0 of 53 action default

name WEBCGI 攻击类（Web-Access） rule 563 of 563 action deny

name 拒绝服务类（DDOS） rule 318 of 318 action deny

name 木马类（Trojan-Horse） rule 0 of 749 action default

name 蠕虫类（Virus-Worm） rule 0 of 67 action default

name 扫描类（Scan） rule 0 of 111 action default

name 网络访问类（Access-Control） rule 0 of 197 action default

name 系统漏洞类（system） rule 0 of 170 action default

name 溢出攻击类（Buffer-Overflow） rule 0 of 1474 action default

ips eventset show-rule class-name < *string1*> **classby** <atk|sift|os|pop|risk> [**eventname** < *string2*>]

命令描述：

查看规则集中的防护规则。

参数说明：

ips eventset show-rule	查看规则集中的防护规则。
class-name	必选项，设置要查看的规则集分组的名称。
string1	字符串类型，表示规则集名称。
classby	必选项，选择分类方式。
atk|sift|os|pop|risk	攻击类型|精选|操作系统|流行程度|风险等级
eventname	可选项，设置要查看的防护规则名称。
string2	字符串类型，表示防护规则名称。

以下为查看规则集中的防护规则的示例：

TopsecOS# **ips eventset show-rule eventset-name** *rule* **classby** atk **class-name** *HTTP 攻击类（HTTP）*

tid 11444 msg IIS webexplt 远程拒绝服务攻击 cve CVE-2001-024 action alert enable yes

tid 11676 msg IIS isapi 文件遍历攻击 cve CAN-1999-045 action alert enable yes

tid 11677 msg IIS showcode.asp 脚本源代码泄露攻击 cve CAN-1999-073 action deny enable yes

tid 11678 msg IIS4.0 远程拒绝服务攻击 cve CVE-1999-087 action alert enable yes

tid 11679 msg IIS trans 源代码泄露攻击 cve CVE-2000-077 action alert enable yes

tid 11680 msg IIS ism.dll 缓存溢出攻击 cve CAN-1999-153 action deny enable yes

tid 11681 msg IIS CGI 参数解码变种攻击 1 cve CVE-2001-033 action deny enable yes

tid 11682 msg IIS 源代码泄露变种攻击 1 cve CVE-2000-063 action deny enable yes

tid 11683 msg IIS CGI 参数解码攻击 cve CVE-2001-033 action deny enable yes

tid 11684 msg IIS CGI 参数解码变种攻击 2 cve CVE-2001-033 action deny enable yes

tid 11685 msg IIS isapi 拒绝服务攻击 cve CVE-2001-050 action deny enable yes

tid 11686 msg IIS isapi 拒绝服务变种攻击 1 cve CVE-2001-050 action deny enable yes

tid 11687 msg IIS 目录遍历攻击 cve CVE-2001-098 action deny enable yes

……

ips rules update filename <*string*>

命令描述：

配置规则库升级。

参数说明：

ips rules update	配置规则库升级。
filename	必选项，设置规则文件名称。
string	字符串类型，表示规则文件名称。

7.7.3 配置入侵防御引擎

CLI 方式配置

步骤	命令	说明
1	**ips engine inspect-mode** <intellective|deeply>	设置智能检测。
2	**ips engine http_inspect_depth client** <*number1*> **server** <*number2*>	设置 HTTP 检测深度。
3	**ips engine mode** set <ngtos|stream5>	设置流重组模式。
4	**ips engine reassemble dir** <none|client|server|both> **level** <*number*>	设置流重组参数。
5	**ips engine session-packets tcp** <*number1*> **udp** <*number2*>	设置智能检测式下，检测同一个连接中的前多少个数据包。
6	**ips engine show** <cr>	查看 IPS 引擎配置信息。

ips engine http_inspect_depth client <*number1*> **server** <*number2*>

命令描述：

设置 HTTP 检测深度。

参数说明：

ips engine http_inspect_depth	设置设置 HTTP 检测深度。
client	必选项，设置 HTTP 客户端检测深度。
number1	数值类型，表示 HTTP 客户端检测深度。
server	必选项，设置 HTTP 服务器检测深度。
number2	数值类型，HTTP 服务器检测深度。

ips engine inspect-mode <intellect|deeply>

命令描述：

设置检测模式。

参数说明：

ips engine inspect-mode	必选项，设置检测模式。
intellect	智能检测：根据协议和方向，智能选择检测的报文，如 http 协议只检测数据包头，不检测数据文件及返回的报文。
deeply	深度检测：不管协议和方向，每个报文都检测。

ips engine mode set <ngtos|stream5>

命令描述：

设置流重组模式。

参数说明：

ips engine stream-mode	必选项，设置流重组模式。
ngtos|stream5	ngtos 引擎|stream5 引擎

ips engine reassemble dir <none|client|server|both> [**level** <0|1|2|3|4>]

命令描述：

设置流重组参数。

参数说明：

ips engine reassemble	设置流重组参数。
dir	必选项，设置流重组方向。
none|client|server|both	none 表示两个方向都不进行流重组； client 表示从客户端方向进行流重组； server 表示从服务器端方向进行流重组； both 表示从两个方向进行流重组。
level	可选项，设置流重组深度。
0|1|2|3|4	取值范围：0-4。

ips engine session-packets tcp <*number1*> **udp** <*number2*>

命令描述：

设置智能检测式下，检测同一个连接中的前多少个数据包。

参数说明：

ips engine session-packets	必选项，设置智能检测模式下，检测同一个连接中的前多少个数据包。
tcp	TCP 报文。
number1	数值类型，表示检测 TCP 包个数，默认检测前 256 个。
udp	UDP 报文。
number2	数值类型，表示检测 UDP 包个数，默认检测前 256 个。

ips engine show <cr>

命令描述：

显示 IPS 引擎设置参数。

以下为显示 IPS 引擎参数的示例：

```
TopsecOS# ips engine show
ips engine reassemble dir client level 1
ips engine inspect_mode intellect
ips engine precedence_mode application 10
ips engine http_inspect_depth client 300 server 300
ips engine session_packets tcp 256 udp 256
ips engine firewalllink off
ips engine mode set stream5
```

7.8 DDoS 防御

7.8.1 简介

DDoS 攻击

网络中存在多种防不胜防的攻击，如果攻击者向攻击目标发送大量的虚假请求，被攻击者不断应答这些无用信息，而合法的用户却无法得到相应的服务，即发生拒绝服务。造成 DoS（Denial of Service，拒绝服务）的攻击行为被称为 DoS 攻击。

DDoS（Distributed Denial of Service，分布式拒绝服务）攻击，是在 DoS 攻击基础上产生的一种攻击，通过可利用的僵尸主机（攻击者入侵过或者可间接利用的主机）向目标对象发送大量请求，造成目标对象的网络带宽拥塞、资源耗尽而不能提供正常的服务。

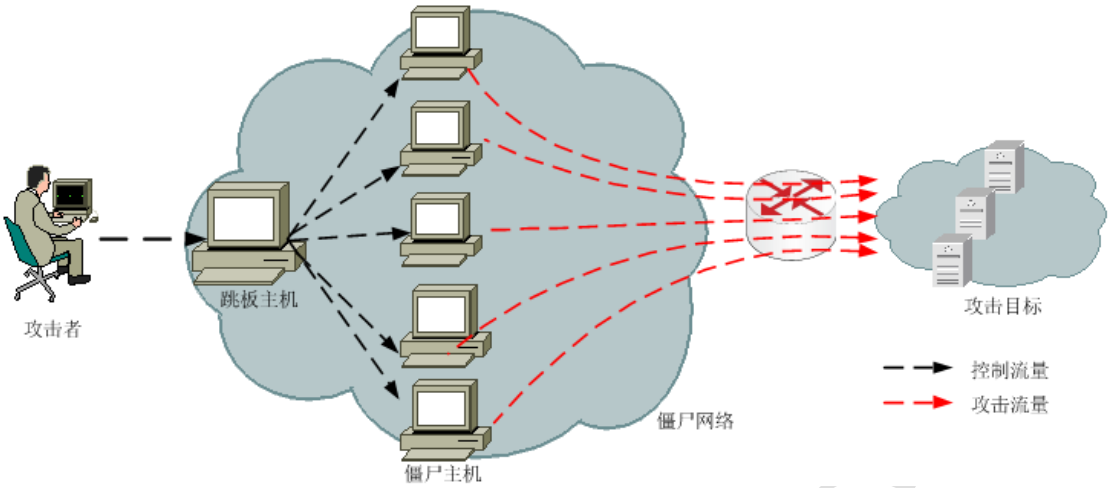


图 7-8 DDoS 攻击示意图

如上图所示，攻击者通过各种手段取得网络上大量在线主机的控制权限，这些被控制的主机称为僵尸主机，攻击者和僵尸主机构成的网络称为僵尸网络。当被攻击目标确定后，攻击者控制僵尸主机向目标发送大量的攻击报文，导致被攻击目标的网络链路拥塞、系统资源耗尽。

针对当前不断泛滥、防范难度很强的 DDoS 攻击，天融信在 NGFW 中集成开发了 DDoS 防御模块，能够有效检测并抵御多种类型的 DDoS 攻击行为及传统的单包攻击，并能采取相应的防御策略保护指定的防护对象免受各种类型的攻击。

- 统计型攻击是指制造大量无用数据，造成通往目的主机的网络拥塞，甚至资源耗尽使目的主机无法正常和外界通信，包括 SYN Flood、UDP Flood、ICMP Flood、Ping Sweep、Port Scan。
- 异常包攻击是指通过向目标系统发送有缺陷的报文，使得目标系统在处理这样的报文时发生错误，或者造成系统崩溃，影响目标系统的正常运行。常见攻击有：Land、Smurf、WinNuke、TCPSScan、IP Option 等。
- DNS 攻击是一种应用层攻击，包含异常包攻击和统计型攻击，包括 DNS 异常包、DNSFlood 等。
- DHCP 攻击是一种应用层攻击，包含异常包攻击和统计型攻击，包括 DHCP 异常包、DHCP Flood 等。

DDoS 防御阈值

为了防御网络中的 DDoS 攻击，需要为各种攻击流量配置防御阈值，该阈值可以看做是网络中正常流量的上限，如果网络中的流量超出设置的阈值，则可判断流量发生异常，可能受到攻击，将会触发 DDoS 防御模块。因此 DDoS 防御阈值设置是否合理将直接影响攻击防御的效果。

不同网络中的流量也有所区别，如果阈值设置过低，那么在没有发生攻击时，系统就启动 DDoS 防御模块，影响设备性能，可能造成网络正常流量被丢弃；如果防范阈值设置过高，那么即使发生了攻击，网络也无法感知，不能及时启动 DDoS 防御模块。因此管理员在配置 DDoS 防御功能前需要了解网络正常流量，根据网络中的实际流量设置不同的阈值。NGFW 支持多种不同的阈值设定。

- 服务器阈值：服务器能处理的每秒访问数的阈值。当对目的服务器的访问量达到该服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视。
- 服务器高压阈值：服务器最多能处理的每秒访问数的阈值。当对目的服务器的访问量达到高压阈值时，该服务器确认为受到攻击，DDOS 防御模块按照策略进行主动防御。
- 单机阈值：允许客户端发起请求数的阈值。根据源地址和目的地址进行统计，当统计值超过该单机阈值时，被认为是攻击，并按照相应的规则处理该包。

NGFW 如果同时设定了服务器阈值和单机阈值，网络中的流量可能只触发一个阈值条件，此时根据不同的阈值优先级，采取不同的防御策略。

- 服务器优先：表示 DDoS 防御基于服务器阈值进行防御。当目的被保护地址的访问量低于服务器阈值时，不开启单机阈值防御，不进行防御动作；当目的被保护地址的访问量高于服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视；当目的被保护地址的访问量到达服务器高压阈值时，DDoS 防御模块按照策略进行主动防御。
- 单机优先：表示无论流量是否触发服务器阈值，DDoS 防御都基于单机阈值进行防御，相当于服务器阈值设为 0。

DDoS 攻击防御

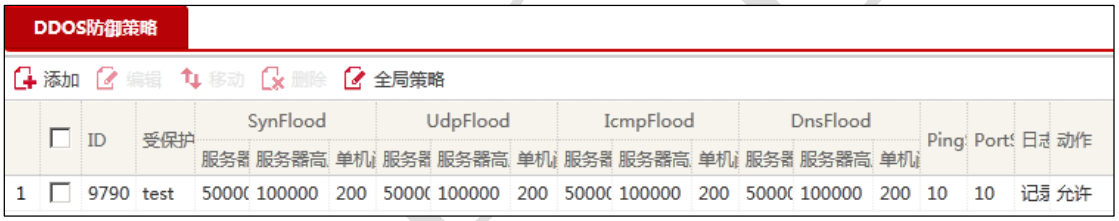
NGFW 的 DDoS 防御模块根据网络中不同的攻击，进行不同的防御。对于统计型攻击分为两类：

- 对于网络中的异常包，可根据防御策略进行放行或者阻断防御。
- 对于 SYN Flood、UDP Flood、ICMP Food、DNS Flood、DHCP Flood、PingSweep、PortScan 统计型攻击，则根据设备设置的 3 个阈值：服务器阈值、服务器高压阈值、单机阈值进行防御。在一定时间内，当攻击包目的地址（服务器地址）达到服务器阈值时，开始对源地址计数。当同一目的地址，对应的源地址达到单机阈值时，认为攻击。当服务器阈值超过服务器高压阈值时也认为发生 DDoS 攻击。

7.8.2 配置 DDoS

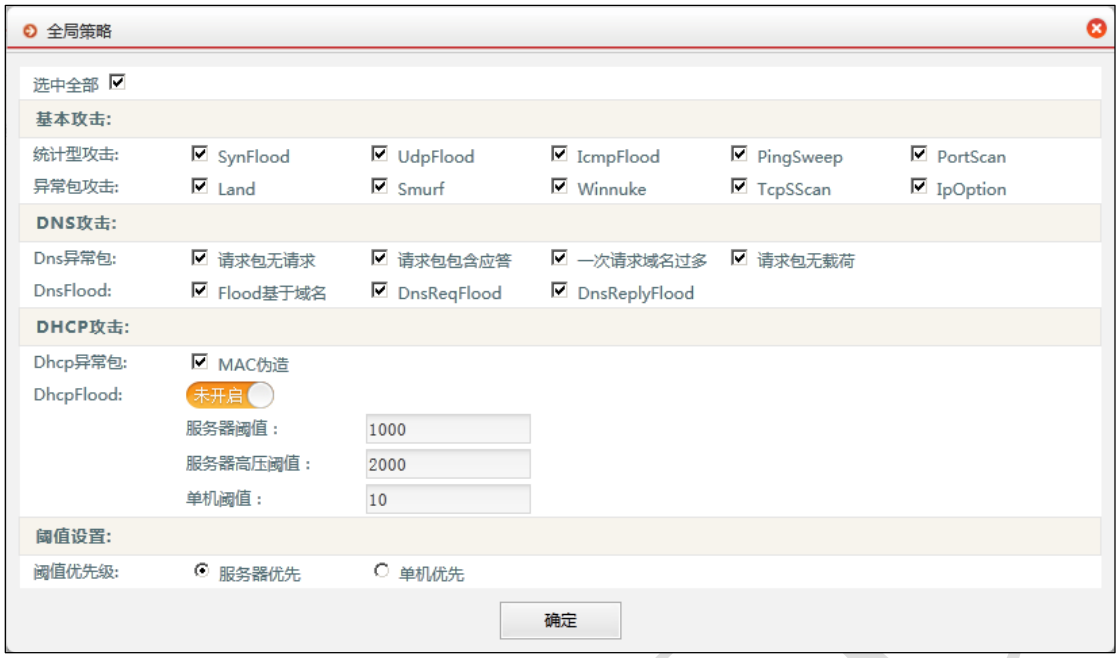
WEBUI 方式配置

步骤 1 选择 **安全策略** > **DDOS 防御**，进入“DDOS 防御策略”界面。



步骤 2 设置全局防御策略。

1）点击『全局策略』，弹出“全局策略”对话框，在对话框中设置 DDoS 全局防御策略。



在设置防御类型时，各项参数的具体说明如下表所示。

参数	说明
选中全部	选择所有防御类型参数。
统计型攻击	点击攻击类型前的复选框，选择需要防御的统计型攻击，可选择多项。 1）SYN Flood 是当前比较流行的拒绝服务攻击的方式之一。SYN Flood 利用了 TCP 协议的固有缺陷，通过发送大量伪造的 TCP 连接请求，使被攻击方充满 SYN 半连接，从而耗尽被攻击方的资源而无法响应正常请求。 2）UDP Flood 是当前比较流行的拒绝服务攻击的方式之一。攻击者通过发送大量的含有 UDP 数据报的 IP 封包，以至于受害者再也无法处理有效的连接时，就发生了 UDP 泛滥。 3）ICMP Flood 通过向被攻击者发送大量的 ICMP 回应请求，消耗被攻击者的资源来进行响应，直至被攻击者再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。 4）Ping Sweep（Ping 扫射），也叫做 ICMP 扫射，是一个发送 ICMP 回应请求（“pings”）给一个 IP 地址范围的攻击，目的在于寻找能够被探查到的攻击主机。 5）Port Scan（端口扫描），通过向一个特定主机地址的不同端口（包括 TCP 端口和 UDP 端口）发送 IP 数据包，以确定该主机开启的服务。
异常包攻击	点击攻击类型前的复选框，选择需要防御的异常包攻击，可选择多项。 1）Land：一种拒绝服务攻击。它使用伪造的 SYN 包，包的源地址和目标地址都被设置成被攻击方的地址，这样被攻击方会给自己发送 SYN-ACK 消息并发回 ACK 消息，创建一个空连接，每一个这样的连接都将保持到超时为止，这样过多的空连接会耗尽被攻击方的资源，导致拒绝服务。

参数	说明
	2）Smurf：是一种拒绝服务攻击，简单的来说，它可以通过大规模的发送以被攻击方的 IP 地址为源地址，以一个具有大量主机的网络广播地址为目的地址的 ICMP 请求包，这样大量的 ICMP 回复包将会耗尽被攻击方的资源，导致拒绝服务的发生。 3）WinNuke：主要是攻击目标端口，被攻击的目标端口一般是是 139、138、137、113、53 等，WinNuke 现已发展到不仅可以攻击单个 IP，还可以连续攻击一个 IP 地址段，造成属于此地址段的主机发生死机或蓝屏等异常情况。 4）TCPSScan：攻击者通过检测 TCP 服务预留的 1024 个端口，比如即时消息服务等，获知哪些端口是打开的。打开的端口暗示着安全漏洞，这些漏洞可以被恶意的黑客利用。 5）IPOption：攻击者通过检查 IP 包中的选项域，使用这个规则选项搜索 IP 包头的特定选项，例如源路由来指定路由，利用可信用户对服务器进行攻击。特别是基于 UDP 协议，由于是面向非连接的，更容易被利用来攻击。
DNS 异常包	点击攻击类型前的复选框，选择需要防御的 DNS 异常包攻击，可选择多项。 1）请求包无请求：客户端向 Dns 服务器发送请求包请求域名时发生异常，包中没有请求。 2）请求包包含应答：客户端向 Dns 服务器发送请求包请求域名时发生异常，包中含有应答。 3）一次请求域名过多：客户端向 Dns 服务器发送请求包请求域名时发生异常，包中的请求域名个数超过限定的最大值。 4）请求包无载荷：客户端向 Dns 服务器发送请求包请求域名时发生异常，包中数据部分值为 0。
DnsFlood	点击攻击类型前的复选框，选择需要防御的 DNS 统计包攻击，可选择多项。 1）Flood 基于域名：该参数仅在勾选“DnsReqFlood”、“DnsReplyFlood”中的一个或者两个时有效。 （a）当在勾选“DnsReqFlood”后勾选该参数，表示客户端向 Dns 服务器发送一个或多个请求包请求域名时域名过多，造成洪水攻击。 （b）当在勾选“DnsReplyFlood”后勾选该参数，表示 Dns 服务器向客户端发送请求回应时域名过多，造成洪水攻击。 2）DnsReqFlood：大量的 Dns 请求攻击，超出 Dns 服务器的负荷承载能力，使得正常的请求得不到处理。 3）DnsReplyFlood：大量的 Dns 应答攻击，超出 Dns 服务器的负荷承载能力，使得正常的请求得不到处理。
Dhcp 异常包	点击攻击类型前的复选框，选择需要防御的 DHCP 异常包攻击。 MAC 伪造：通过大量伪造的 MAC 地址向 DHCP 服务器请求获得 IP，超出 DHCP 服务器的负荷承载能力，使得 DHCP 服务器无法处理正常的请求。

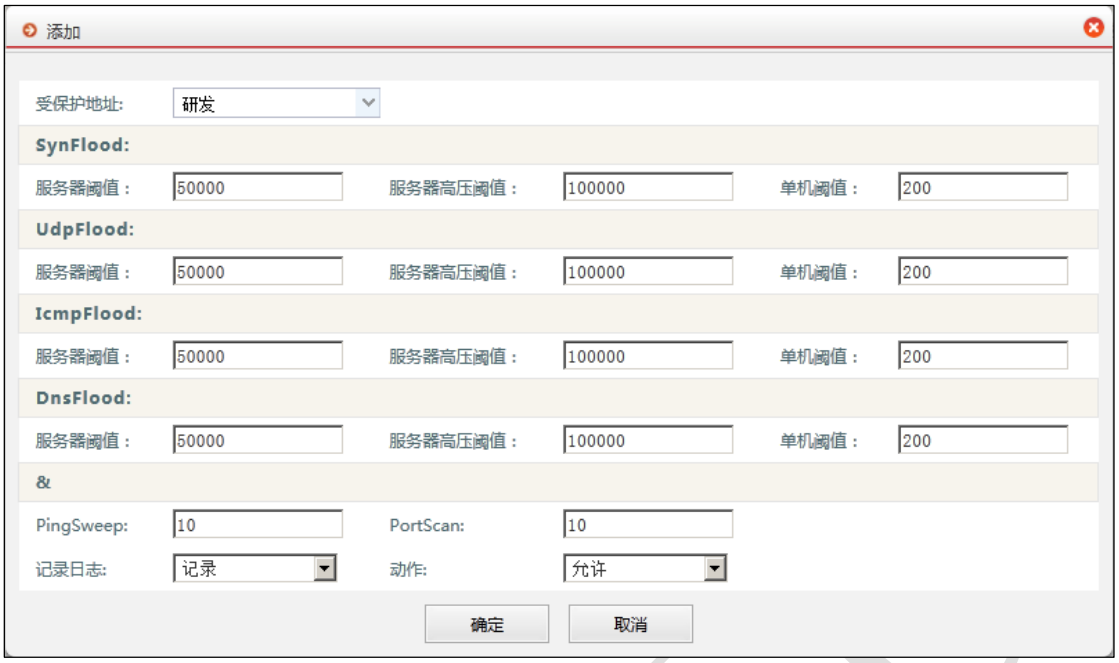
参数	说明
DHCP flood 开关	是否开启对 DHCP flood 的服务器和客户端请求数的阈值设置。默认为“  ”，表示，未开启 DHCP 统计型攻击防御；如果点击该按钮将显示“  ”，则表示已开启 DHCP 统计型攻击防御。
服务器阈值	DHCP flood 开关为开启时，可设置服务器能处理的每秒访问数的阈值。当对目的服务器的访问量达到该服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视。单位：次/秒；默认值：1000。
服务器高压阈值	DHCP flood 开关为开启时，可设置服务器最多能处理的每秒访问数的阈值。当对目的服务器的访问量达到高压阈值时，该服务器确认为受到攻击，DDOS 防御模块按照策略进行主动防御。单位：次/秒；默认值：2000。
单机阈值	DHCP flood 开关为开启时，可设置允许客户端发起请求数的阈值。在单机保护状态下，根据源地址和目的地址进行统计，当统计值超过该单机阈值时，被认为是攻击，并按照相应的规则处理该包。单位：次/秒；默认值：10。
阈值优先级	设置 DDoS 防御基于服务器阈值或单机阈值。 服务器优先：表示 DDoS 防御基于服务器阈值进行防御，目的服务器的访问量达到服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视；访问量到达服务器高压阈值时，DDoS 防御模块按照策略进行主动防御。 单机优先：表示 DDoS 防御基于客户端的阈值进行防御，直接进入单机保护模式，相当于服务器阈值设为 0。

2）设置完成后，点击【确定】按钮，完成设置。

步骤 3 添加受保护对象的防御规则。

设置天融信入侵防御系统可以抵御的攻击类型后，对于统计型攻击，还需确定需要保护的对象，即天融信入侵防御系统保护的对象。

1）点击『添加』，在弹出的“添加”对话框中，设置攻击防御规则。



在设置受保护对象时，各项参数的具体说明如下表所示。

参数	说明
受保护地址	选择受保护的对象。 关于受保护对象的设置具体请参见 7.1.2 地址，可以是主机地址，也可以是子网或地址范围。
服务器阈值（SynFlood、UdpFlood、IcmpFlood、DnsFlood）	分别设置服务器能处理不同流量的每秒访问数的阈值。当对目的服务器的访问量达到该服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视。单位：次/秒；默认值：50000；取值范围：1-1000000。
服务器高压阈值（SynFlood、UdpFlood、IcmpFlood、DnsFlood）	分别设置服务器最多能处理不同流量的每秒访问数的阈值。当对目的服务器的访问量达到高压阈值时，该服务器确认为受到攻击，DDOS 防御模块按照策略进行主动防御。单位：次/秒；默认值：100000；取值范围：1-1000000。
单机阈值（SynFlood、UdpFlood、IcmpFlood、DnsFlood）	分别设置允许客户端发起不同流量请求数的阈值。在单机保护状态下，根据源地址和目的地址进行统计，当统计值超过该单机阈值时，被认为是攻击，并按照相应的规则处理该包。单位：次/秒；默认值：200；取值范围：1-1000000。
PingSweep	Ping 扫射，是指在一定时间（1HZ）内，对于同一个源地址来说，目的地址出现的个数（非次数）。若个数高于设定阈值，则认定其是攻击。 如：该参数设置为 10 表示当一个源 IP 地址在规定的时间间隔（单位：秒；默认值：0.01）内将 10 个 ICMP 封包发送给不同的主机时，TopIDP 即判定进行了一次地址扫描。取值范围：1-65535。
PortScan	端口扫描，是指对于同一个目的地址和源地址来说，端口扫描中不同的端口个数。

参数	说明
	如：该参数设置为 10，表示当一个源 IP 地址在规定的时间间隔内（单位：秒；默认值：0.01）将含有 TCP SYN 片段的 IP 封包发送给位于相同目标 IP 地址的 10 个不同端口时，TopIDP 即判定进行了一次端口扫描。取值范围：1-65535。
记录日志	是否记录日志。可选项：记录、不记录。
动作	设置当超过设定的阈值时，对数据包的控制行为是放行或阻断。可选项：允许、阻断

2）点击【确定】按钮，完成受保护对象配置。

CLI 方式配置

步骤	命令	说明
1	**ddos rule add protect_name** <*string*> [**dnsflood** <*number1*>] [**dnsflood_high** <*number2*>] [**dnshost** <*number3*>] [**icmpflood** <*number4*>] [**icmpflood_high** <*number5*>] [**icmphost** <*number6*>] [**udpflood** <*number7*>] [**udpflood_high** <*number8*>] [**udphost** <*number9*>] [**synflood** <*number10*>] [**synflood_high** <*number11*>] [**synhost** <*number12*>] [**pingsweep** <*number13*>] [**portscan** <*number14*>] [**action** <pass|block>] [**log** <yes|no>]	添加 DDoS 防御规则。
2	**ddos rule modify ruleid** <*string*> [**apptype dnsflood | stattype** <synflood|udpflood|icmpflood|portscan|pingsweep> **threshold** <*number1*> **threshold_high** <*number2*> **threshold_host** <*number3*>] **action** <pass|block> **log** <yes|no>	修改 DDoS 防御规则。
3	**ddos rule move id** <*string1*> <**before** *string2*|**after** *string3*>	移动 DDoS 防御规则。
4	**ddos type add abntype** <land|smurf|winnuke|tcp_sscan|ip_option>	添加 DDoS 防御的异常包类型。
5	**ddos type add apptype dns** <dnsnoreq|repinreq|overreq|nopayload|dnsreqflood|dnsreplyflood|domain>	添加 DDoS 防御的应用层 DNS 报文类型。
6	**ddos type add apptype dhcp** <**dhcpmac**|**dhcpflood threshold** <*number1*> **threshold_high** <*number2*> **threshold_host** <*number3*>>	添加 DDoS 防御的应用层 DHCP 报文类型。
7	**ddos type add globalset host-priority** <cr>	设置 DDoS 防御为单机优先，基于单机阈值防御。
8	**ddos type add stattype** <synflood|udpflood|icmpflood|portscan|pingsweep>	添加 DDoS 防御的统计型攻击类型。
9	**ddos rule clean** <cr>	清空 DDoS 防御规则信息。
10	**ddos rule show** <cr>	显示 DDoS 防护规则配置信息。

11	**ddos config clean** <cr>	清空 DDoS 配置信息，恢复为出厂设置。
12	**ddos config show** <cr>	查看 DDoS 配置信息。
13	**ddos stat clean** <cr>	清空 DDoS 的所有统计信息。
14	**ddos stat show** <cr>	显示 DDoS 的所有统计信息。

ddos config clean <cr>

命令描述：

清空 DDoS 配置信息，恢复为出厂设置。

ddos config show <cr>

命令描述：

查看 DDoS 配置信息。

以下为查看 DDoS 配置的示例：

```
TopsecOS# ddos config show
ddos type add abntype land
ddos type add abntype smurf
ddos type add abntype winnuke
ddos type add abntype tcp_sscan
ddos type add abntype ip_option
ddos type add stattype synflood
ddos type add stattype udpflood
ddos type add stattype icmpflood
ddos type add stattype portscan
ddos type add stattype pingsweep
ddos type add apptype dns dnsnoreq
ddos type add apptype dns repinreq
ddos type add apptype dns overreq
```

```
ddos type add apptype dns nopayload
ddos type add apptype dns dnsreqflood
ddos type add apptype dns dnsreplyflood
ddos type add apptype dns domain
ddos type add apptype dhcp dhcpmac
ID 9415 ddos rule add protect_name 123 synflood 50000 synflood_high 100000
synhost 200 udpflood 50000 udpflood_high 100000 udphost 200 icmpflood 50000
icmpflood_high 100000 icmphost 200 dnsflood 50000 dnsflood_high 100000 dnshost
200 pingsweep 10 portscan 10 log yes action pass
```

ddos stat clean <cr>

命令描述：

清空 DDoS 的所有统计信息。

ddos stat show <cr>

命令描述：

显示 DDoS 的所有统计信息。

以下为显示 DDoS 的统计信息的示例：

```
TopsecOS# ddos stat show
match          hits          alert          drop          receive
0              0             0              0             36595
Detect results:
-------------------------------------------------------------------------------------
ipoption                0
tcpscan                 0
winnuke                 0
smurf                   0
land                    0
```

portscan	0
synflood	0
udpflood	0
icmpflood	0
pingsweep	0
dnsflood	0
dnsabn	0
dhcpflood	0
dhcpmac	0
hits	0

ddos rule clean <cr>

命令描述：

清空 DDoS 防御规则信息。

ddos rule add protect_name <*string*> [**dnsflood** <*number1*>] [**dnsflood_high** <*number2*>] [**dnshost** <*number3*>] [**icmpflood** <*number4*>] [**icmpflood_high** <*number5*>] [**icmphost** <*number6*>] [**udpflood** <*number7*>] [**udpflood_high** <*number8*>] [**udphost** <*number9*>] [**synflood** <*number10*>] [**synflood_high** <*number11*>] [**synhost** <*number12*>] [**pingsweep** <*number13*>] [**portscan** <*number14*>] [**action** <pass|block>] [**log** <yes|no>]

命令描述：

添加 DDoS 防御规则。

可使用 **ddos rule delete id** <*string*>删除 DDoS 防御规则。

参数说明：

ddos rule add	必选项，添加 DDoS 防御规则。
protect_name	DDoS 防御规则名称。
string1	字符串类型，表示 DDoS 防御规则名称。
dnsflood	统计型 DNS 攻击防御的服务器阈值。
number1	数值类型，单位：次/秒；默认值：50000；取值范围：1-1000000。
dnsflood_high	统计型 DNS 攻击防御的服务器高压阈值。
number2	数值类型，单位：次/秒；默认值：100000；取值范围：1-1000000。

dnshost	统计型 DNS 攻击防御的主机阈值。
number3	数值类型，单位：次/秒；默认值：200；取值范围：1-10000。
icmpflood	统计型 ICMP Flood 攻击防御的服务器阈值。
number4	数值类型，单位：次/秒；默认值：50000；取值范围：1-1000000。
icmpflood_high	统计型 ICMP Flood 攻击防御的服务器高压阈值。
number5	数值类型，单位：次/秒；默认值：100000；取值范围：1-1000000。
icmphost	统计型 ICMP Flood 攻击防御的主机阈值。
number6	数值类型，单位：次/秒；默认值：200；取值范围：1-10000。
udpflood	统计型 UDP Flood 攻击防御的服务器阈值。
number7	数值类型，单位：次/秒；默认值：50000；取值范围：1-1000000。
udpflood_high	统计型 UDP Flood 攻击防御的服务器高压阈值。
number8	数值类型，单位：次/秒；默认值：100000；取值范围：1-1000000。
udphost	统计型 UDP Flood 攻击防御的主机阈值。
number9	数值类型，单位：次/秒；默认值：200；取值范围：1-10000。
synflood	统计型 SYN Flood 攻击防御的服务器阈值。
number10	数值类型，单位：次/秒；默认值：50000；取值范围：1-1000000。
synflood_high	统计型 SYN Flood 攻击防御的服务器高压阈值。
number11	数值类型，单位：次/秒；默认值：100000；取值范围：1-1000000。
synhost	统计型 SYN Flood 攻击防御的主机阈值。
number12	数值类型，单位：次/秒；默认值：200；取值范围：1-10000。
pingsweep	Ping 扫射攻击防御阈值。
number13	数值类型，单位：次/秒；默认值：10；取值范围：1-65535。
portscan	端口扫描攻击防御阈值。
number14	数值类型，单位：次/秒；默认值：10；取值范围：1-65535。
action	DDoS 防御动作。
pass|block	通过|阻断。
log	DDoS 防御规则生效信息记录到日志功能是否开启。
yes|no	开启|关闭。

以下为添加 DDoS 防御规则的示例：

TopsecOS# **ddos rule add protect_name** *ddos-rule* **dnsflood** 1000 **action** block **log** yes

ddos rule modify ruleid <*string*> [**apptype dnsflood | stattype**

<synflood|udpflood|icmpflood|portscan|pingsweep> **threshold** <*number1*> **threshold_high** <*number2*> **threshold_host** <*number3*>] **action** <**pass|block**> **log** <yes|no>

命令描述：

修改 DDoS 防御规则。

参数说明：

ddos rule modify	必选项，修改 DDoS 防御规则。
ruleid	DDoS 防御规则号。
string	DDoS 防御规则号，系统自动生成，可通过 **ddos rule show** 命令查看。
apptype dnsflood	应用型 DDoS 攻击，DNS Flood 攻击。
stattype	统计型 DDoS 攻击。
synflood|udpflood|icmpflood|portscan|pingsweep	SYN Flood 攻击|UDP Flood 攻击|ICMP Flood 攻击|端口扫描攻击|PING 扫射攻击
threshold	DDoS 防御的服务器阈值。
number1	数值类型，单位：次/秒；默认值：50000；取值范围：1-1000000。
threshold_high	DDoS 防御的服务器高压阈值。
number2	数值类型，单位：次/秒；默认值：100000；取值范围：1-1000000。
threshold_host	DDoS 防御的主机阈值。
number3	数值类型，单位：次/秒；默认值：200；取值范围：1-10000。
action	DDoS 防御动作。
pass|block	通过|阻断。
log	DDoS 防御规则生效信息记录到日志功能是否开启。
yes|no	开启|关闭。

以下为修改 DDoS 防御规则的示例：

TopsecOS# **ddos rule modify ruleid** *10231* **action** block **log** yes

ddos rule move id <*string1*> <**before** *string2*|**after** *string3*>

命令描述：

移动 DDoS 防御规则。

参数说明：

ddos rule move	必选项，移动 DDoS 防御规则。
id	DDoS 防御规则号。
string1	字符串类型，表示待移动的 DDoS 防御规则号。
before	可选项，移动到指定的 DDoS 防御规则之前。
string2	字符串类型，表示参照物 DDoS 防御规则号。
after	可选项，移动到指定 DDoS 防御规则之后。

string3	字符串类型，表示参照物 DDoS 防御规则号。

以下是移动 DDoS 防御规则的示例：

将规则号“10210”的 DDoS 防御规则移动到规则号为“10010”的 DDoS 防御规则之前。

```
TopsecOS# ddos rule move id10210 before 10010
```

ddos rule show <cr>

命令描述：

显示 DDoS 防护规则配置信息。

以下为显示 DDoS 防护规则的示例：

```
TopsecOS# ddos rule show
ID 9415 ddos rule protect_name 123 synflood 50000 synflood_high 100000 synhost
200 udpflood 50000 udpflood_high 100000 udphost 200
 icmpflood 50000 icmpflood_high 100000 icmphost 200 dnsflood 50000
dnsflood_high 100000 dnshost 200 ipsweep 10 portscan 10 log yes
 action pass
```

ddos type add abntype <land|smurf|winnuke|tcp_sscan|ip_option>

命令描述：

添加 DDoS 防御的异常包类型。

可使用 **ddos type delete abntype** <land|smurf|winnuke|tcp_sscan|ip_option>删除防御的异常包类型。

参数说明：

ddos type add	必选项，添加 DDoS 的防御策略。
abntype	异常包类型。
land|smurf|winnuke|tcp_sscan|ip_option	1）Land：一种拒绝服务攻击。它使用伪造的 SYN 包，包的源地址和目标地址都被设置成被攻击方的地址，这样被攻击方会给自己发送 SYN-ACK 消息并发回 ACK 消息，创建一个空连接，每一个这样的连接都将保持到超时为止，这样过多的空连接会耗尽被攻击方的资源，导致拒绝服务。

	2）Smurf：是一种拒绝服务攻击，简单的来说，它可以通过大规模的发送以被攻击方的 IP 地址为源地址，以一个具有大量主机的网络广播地址为目的地址的 ICMP 请求包，这样大量的 ICMP 回复包将会耗尽被攻击方的资源，导致拒绝服务的发生。 3）WinNuke：主要是攻击目标端口，被攻击的目标端口一般是是 139、138、137、113、53 等，WinNuke 现已发展到不仅可以攻击单个 IP，还可以连续攻击一个 IP 地址段，造成属于此地址段的主机发生死机或蓝屏等异常情况。 4）TCPSScan：攻击者通过检测 TCP 服务预留的 1024 个端口，比如即时消息服务等，获知哪些端口是打开的。打开的端口暗示着安全漏洞，这些漏洞可以被恶意的黑客利用。 5）IPOption：攻击者通过检查 IP 包中的选项域，使用这个规则选项搜索 IP 包头的特定选项，例如源路由来指定路由，利用可信用户对服务器进行攻击。特别是基于 UDP 协议，由于是面向非连接的，更容易被利用来攻击。

以下为添加 DDoS 防御规则的示例：

```
TopsecOS# ddos type add abntype land
```

ddos type add apptype dns

<dnsnoreq|repinreq|overreq|nopayload|dnsreqflood|dnsreplyflood|domain>

命令描述：

添加 DDoS 防御的应用层 DNS 报文类型。

可使用 **ddos type delete apptype dns**

<dnsnoreq|repinreq|overreq|nopayload|dnsreqflood|dnsreplyflood|domain>禁用 DDoS 的 DNS 防御策略。

参数说明：

ddos type add	必选项，添加 DDoS 的防御策略。
apptype	应用层防御。
dns	DNS 应用层防御。
dnsnoreq|repinreq|overreq|nopayload|dnsreqflood|dnsreplyflood|domain	dnsnoreq：DNS 请求包中没有请求信息攻击 repinreq：DNS 请求包中包含应答信息攻击 overreq：DNS 一个请求包中包含过多域名攻击 nopayload：DNS 请求包中没有有效信息攻击 dnsreqflood：DNS 请求 Flood 攻击 dnsreplyflood：DNS 应答 Flood 攻击 domain：DNS 基于同一域名的 Flood 攻击

以下为添加 DDoS 应用层防御策略的示例：

```
TopsecOS# ddos type add apptype dns domain
```

ddos type add apptype dhcp <**dhcpmac|dhcpflood threshold** <*number1*> **threshold_high** <*number2*> **threshold_host** <*number3*>>

命令描述：

添加 DDoS 防御的应用层 DHCP 报文类型。

可使用 **ddos type delete apptype dhcp** <dhcpmac|dhcpflood>禁用 DDoS 防御的 DHCP 报文类型。

参数说明：

ddos type add	必选项，添加 DDoS 的异常包策略。
apptype	应用层防御。
dhcp	DHCP 应用层防御。
dhcpmac	MAC 伪造，通过大量伪造的 MAC 地址向 DHCP 服务器请求获得 IP，超出 DHCP 服务器的负荷承载能力，使得 DHCP 服务器无法处理正常的请求。
dhcpflood	DHCP flood 的服务器和客户端请求数的阈值。
threshold	服务器阈值，服务器能处理的每秒访问数的阈值。当对目的服务器的访问量达到该服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视。
number1	数值类型，单位：次/秒，取值范围：1-1000000。
threshold_high	服务器高压阈值，服务器最多能处理的每秒访问数的阈值。当对目的服务器的访问量达到高压阈值时，该服务器确认为受到攻击，DDOS 防御模块按照策略进行主动防御。
number2	数值类型，单位：次/秒，取值范围：1-1000000。
threshold_host	单机阈值，允许客户端发起请求数的阈值。在单机保护状态下，根据源地址和目的地址进行统计，当统计值超过该单机阈值时，被认为是攻击，并按照相应的规则处理该包。
number2	数值类型，单位：次/秒，取值范围：1-10000。

以下为添加 DDoS 防御规则的示例：

```
TopsecOS# ddos type add apptype dhcpmac threshold 5000 threshold_high 20000
threshold_host 500
```

ddos type add globalset host-priority <cr>

命令描述：

设置 DDoS 防御为单机优先，基于单机阈值防御。表示 DDoS 防御基于客户端的阈值进行防御，直接进入单机保护模式，相当于服务器阈值设为 0。

可使用 **ddos type delete globalset host-priority** 设置 DDoS 防御为服务器优先，基于服务器阈值阈值进行防御。表示 DDoS 防御基于服务器阈值进行防御，目的服务器的访问量达到服务器阈值时，该服务器可能受到攻击，DDOS 防御模块开始监视；访问量到达服务器高压阈值时，DDoS 防御模块按照策略进行主动防御。

以下为添加 DDoS 防御规则的示例：

```
TopsecOS# ddos type add globalset host-priority
```

ddos type add stattype <synflood|udpflood|icmpflood|portscan|pingsweep>

命令描述：

添加 DDoS 防御的统计型攻击类型。

可使用 **ddos type delete stattype** <synflood|udpflood|icmpflood|portscan|pingsweep> 禁用 DDoS 防御的统计型攻击类型。

参数说明：

ddos type add	必选项，添加 DDoS 的防御策略。
stattype	统计型攻击。
synflood|udpflood|icmpflood|portscan|pingsweep	1）SYN Flood 是当前比较流行的拒绝服务攻击的方式之一。SYN Flood 利用了 TCP 协议的固有缺陷，通过发送大量伪造的 TCP 连接请求，使被攻击方充满 SYN 半连接，从而耗尽被攻击方的资源而无法响应正常请求。 2）UDP Flood 是当前比较流行的拒绝服务攻击的方式之一。攻击者通过发送大量的含有 UDP 数据报的 IP 封包，以至于受害者再也无法处理有效的连接时，就发生了 UDP 泛滥。 3）ICMP Flood 通过向被攻击者发送大量的 ICMP 回应请求，消耗被攻击者的资源来进行响应，直至被攻击者再也无法处理有效的网络信息流时，就发生了 ICMP 泛滥。 4）Ping Sweep（Ping 扫射），也叫做 ICMP 扫射，是一个发送 ICMP 回应请求（“pings”）给一个 IP 地址范围的攻击，目的在于寻找能够被探查到的攻击主机。 5）Port Scan（端口扫描），通过向一个特定主机地址

	的不同端口（包括 TCP 端口和 UDP 端口）发送 IP 数据包，以确定该主机开启的服务。

以下为添加 DDoS 防御规则的示例：

```
TopsecOS# ddos type add stattype synflood
```

7.9 URL 过滤

URL 过滤主要用于控制用户访问的网页 URL，根据过滤规则对访问敏感 URL 的行为进行控制。

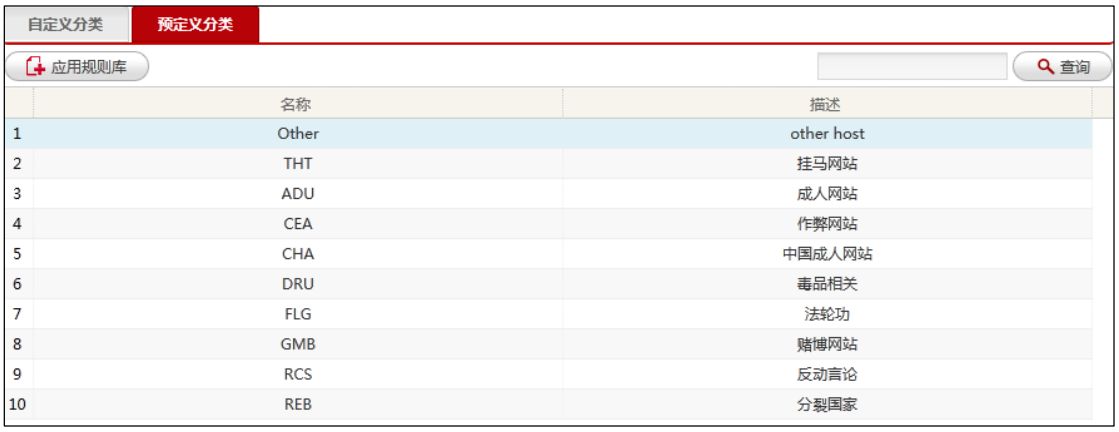
7.9.1 URL 分类

URL 分类库可以根据网页的内容定义出不同的 URL 类型，帮助设备识别各类网站，以实现对各种类型的网站进行访问权限控制和流量控制。NGFW 的 URL 分类库包含系统内置的 URL 组和自定义的 URL 组，系统内置的 URL 分类由 NGFW 定期在服务器上进行更新，自定义的 URL 分类是在内置 URL 分类不满足特定需求时，管理员可以通过已知的 URL 设置 URL 分类。

通过自定义 URL 类别功能，管理员可以创建 URL 列表，可以在任意 URL 过滤配置文件中选择这些 URL。每个自定义 URL 类别均可以独立控制，并且在每个 URL 过滤配置文件中具有与其关联的操作，比如允许、阻断或警报。

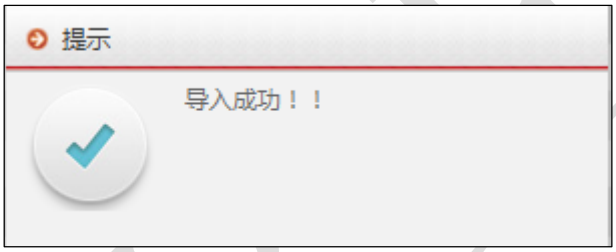
WEBUI 方式配置

步骤 1 选择 **安全策略** > **URL 过滤** > **URL 分类**，激活“预定义分类”页签，进入预定义 URL 分类界面，如下图所示。



	名称	描述
1	Other	other host
2	THT	挂马网站
3	ADU	成人网站
4	CEA	作弊网站
5	CHA	中国成人网站
6	DRU	毒品相关
7	FLG	法轮功
8	GMB	赌博网站
9	RCS	反动言论
10	REB	分裂国家

步骤 2 点击【应用规则库】按钮，将导入到防火墙设备上的 URL 应用规则库进行加载，加载成功后，弹出提示对话窗，如下图所示。关于 URL 应用规则库的导入操作具体请参见 4.2.5 规则库升级。



步骤 3 选择 **安全策略** > **URL 过滤** > **URL 分类**，激活“自定义分类”页签。

步骤 4 点击『添加』，弹出“添加”窗口。

在自定义 URL 分类时，各项参数的具体说明如下表所示。

参数	说明
类别名称	必选项，设置标识自定义 URL 类别的名称。不超过 31 个字符，名称区分大小写，仅可使用字母、数字、空格、连字符和下划线。 说明： 配置 URL 过滤策略时，该自定义 URL 类别名称将出现分类列表中。
描述	设置对自定义 URL 类别的具体说明。最多 255 个字符。
规则	设置具体的分类规则，格式如：www.baidu.com、*baidu.com、www.baidu*。*号表示任意前缀或者后缀内容。

步骤 5 点击【确定】按钮完成 URL 分类的自定义。

CLI 方式配置

步骤	配置命令	配置说明
1	**url-filter user-defined-category add name** <*string1*> [**description** <*string2*>]	配置 URL 分类基本信息
2	**url-filter user-defined-category set name** <*string1*> **add-rule** <*string2*>	配置 URL 分类具体规则

url-filter user-defined-category add name <*string1*> [**description** <*string2*>]

命令描述

添加 URL 过滤的用户自定义分类。

参数说明

url-filter user-defined-category add	添加 URL 过滤的用户自定义分类。
name	必选项，设置自定义 URL 分类的名称。
string1	字符串类型，表示名称。
description	可选项，设置对自定义 URL 类别的具体说明。
string2	字符串类型。

以下是添加 URL 分类的示例：

添加名称为 urlcategory1 的 URL 分类。

```
TopsecOS# url-filter user-defined-category add name urlcategory1
```

url-filter user-defined-category set name <*string1*> **add-rule** <*string2*>

命令描述

设置 URL 过滤自定义分类的规则。

参数说明

url-filter user-defined-category set	设置 URL 过滤的用户自定义分类。
name	必选项，指定自定义分类的名称。
string1	字符串类型。
add-rule	必选项，设置 URL 过滤具体规则信息。
string2	字符串类型。

以下是设置 URL 分类具体规则的示例：

设置名称为 urltest 的 URL 分类的具体规则为 www.baidu.com。

```
TopsecOS# url-filter user-defined-category add name urltest
```

```
TopsecOS# url-filter user-defined-category set name urltest add-rule
www.baidu.com
```

url-filter user-defined-category show [**name** <*string*>]

命令描述

显示 URL 分类规则的具体信息。

以下是显示 URL 分类规则的示例：

```
TopsecOS# url-filter user-defined-category show
ID (UCAT-NAME) (UCAT_DESC)
-----------------------------------------
10471 (哈哈) ( )
10719 (urltest) (df)
10722 (category1) ()
```

显示名称为 urltest 的 URL 分类规则信息。

```
TopsecOS# url-filter user-defined-category show name urltest
-----------------------------------------
user-define cat id :11029
user-define cat name: urltest
user-define cat desc:
user-define cat rules:
        (11238) www.baidu.com
        (11415) www.baidu.con
        (11416) *sina.com
```

7.9.2 URL 策略

URL 分类是定义 URL 过滤策略的基础，管理员根据系统内置 URL 分类或者自定义 URL 分类，并在 URL 策略中引用，以允许或阻止访问特定网站和网站类别，或是在访问指定网站时生成警报。

WEBUI 方式配置

在配置 URL 策略之前，需要先进行 URL 类别的配置，关于 URL 类别的设置具体请参见 7.9.1URL 分类。

步骤 1 选择 **安全策略** > **URL 过滤** > **URL 策略**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置 URL 过滤策略时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置 URL 过滤规则的名称。
描述	设置对 URL 过滤规则的具体描述。
黑名单	设置要过滤的敏感 URL 地址，将其加入黑名单。 说明： 1）参数值是字符串（包括 IP 地址和域名），不支持正则表达式，但支持通配符“*”； 2）最多不能超过 1024 个字符。
白名单	设置加入白名单的 URL 地址，防止被过滤。
分类列表	设置对匹配指定 URL 类别条件的数据报文的执行动作。 可选项：allow、block、alert。 “allow”表示允许访问该 URL；“block”表示禁止访问该 URL； “alert”表示允许用户访问该网站，但向 URL 日志添加警告。

步骤 3 点击【确定】按钮完成 URL 过滤策略的添加。

CLI 方式配置

url-filter policy add name <*string1*> [**description** <*string2*>]

命令描述

添加 URL 过滤策略。

参数说明

url-filter policy add	添加 URL 过滤策略。
name	必选项，设置 URL 过滤策略名称。
string1	字符串类型。
description	可选项，设置对 URL 过滤策略的具体说明。
string2	字符串类型。

以下是添加 URL 过滤策略的示例：

添加名称为 urlfiltertest 的 URL 过滤策略。

```
TopsecOS# url-filter policy add name urlfiltertest
```

url-filter policy set name <*string1*> **description** <*string2*>

命令描述

设置 URL 过滤策略的描述信息。

url-filter policy set name <*string1*> **blacklist-add** <*string2*>

命令描述

设置 URL 过滤策略的黑名单。

参数说明

url-filter policy set	设置 URL 过滤策略的黑名单。
name	必选项，指定 URL 过滤策略。
string1	字符串类型，表示 URL 过滤策略名称。
blacklist-add	必选项，添加黑名单。
string2	字符串类型。

以下是设置 URL 过滤策略黑名单的示例：

在名称为 p11 的 URL 过滤策略中添加黑名单 127.1.1.2。

```
TopsecOS# url-filter policy set name p11 blacklist-add 127.1.1.2
```

url-filter policy set name <*string1*> **blacklist-del** <*string2*>

命令描述

删除指定 URL 过滤策略中的黑名单。

url-filter policy set name <*string1*> **whitelist-add** <*string2*>

命令描述

添加 URL 过滤策略的白名单。

url-filter policy set name <*string1*> **whitelist-del** <*string2*>

命令描述

删除指定 URL 过滤策略中的白名单。

url-filter policy set name <*string1*> **user-defined-category** <*string2*> **action** <allow|alert|block>

命令描述

设置 URL 过滤策略中自定义分类的执行动作。

参数说明

url-filter policy set	设置 URL 过滤策略中自定义分类的执行动作。
name	必选项，指定 URL 过滤策略。
string1	字符串类型，表示 URL 过滤策略名称。
user-defined-category	必选项，指定自定义分类。
string2	字符串类型，表示 URL 分类名称。
action	必选项，设置对 URL 分类的执行动作。
allow|alert|block	允许|警告|阻断

以下是设置 URL 过滤策略中自定义分类的执行动作的示例：

TopsecOS# **url-filter policy add name** *p11*

TopsecOS# **url-filter user-defined-category add name** *urltest*

TopsecOS# **url-filter policy set name** *p11* **user-defined-category** *urltest* **action** allow

url-filter url search rule <*string*>

命令描述

查询 URL 过滤策略中 URL 所属分类。

参数说明

url-filter url search	查询 URL 过滤策略中 URL 所属分类。
rule	必选项，设置待查询的 URL 地址。
string	字符串类型。

以下是查询 URL 过滤策略中 URL 所属分类的示例：

```
TopsecOS# url-filter url search rule www.baidu.com
user-defined-cat name: urltest (rule: www.baidu.com)
```

url-filter rules commit <cr>

命令描述

URL 过滤策略规则提交编译。

使用说明

任何对于 URL 过滤规则的操作，包括黑白名单、用户自定义分类等的添加、删除、修改，执行该编译命令后才可生效。

7.10 内容过滤

公司员工办公时使用外网的频率越来越高，例如通过 Internet 搜索资料、收发邮件等，在使用过程中可能产生如下问题：

1）不经意的上传公司内部文件可能导致泄漏公司机密信息；

2）浏览、发布、传输违规信息，对公司造成不好的影响甚至带来法律风险；

3）搜索与工作无关的内容而导致工作效率下降。

基于此，NGFW 提供了内容过滤功能，可以防止机密信息的泄露及违规信息的传输，既能保证员工正常访问 Internet，又可以对员工接收和发送的信息内容进行过滤。

内容过滤是一种基于关键字对通过防火墙的应用的内容进行过滤的安全机制，对应用协议中包含的关键字进行过滤，针对基于不同协议的应用，设备过滤的内容不同，具体说明如下表所示。

应用	过滤内容
基于 HTTP 协议的应用	1）上传方向 （a）用户发布微博、帖子的内容； （b）用户搜索输入的内容； （c）用户提交信息的内容（比如网络注册用户时提交的申请）； （d）上传文件的名称。 2）下载方向 （a）用户浏览网页的内容；

应用	过滤内容
	（b）使用 HTTP 协议下载文件的名称。
基于 SMTP 协议的应用	发送的邮件的标题、正文和附件名称，并支持发送者和接收者信息的过滤。
基于 POP3 协议的应用	接收的邮件的标题、正文和附件名称，并支持发送者和接收者信息的过滤。

当通过设备的数据报文匹配一条访问控制策略，策略的动作为允许且引用了内容过滤策略时，该数据报文需要进行内容过滤检测。具体处理流程为：

1）设备对数据报文的内容进行检测，识别出报文的内容属性。

如果是应用内容则识别出应用的类型、应用内容传输的方向；如果是文件内容则识别出承载文件的应用类型、文件类型和传输方向。

2）设备将数据报文的内容属性与内容过滤策略的条件进行匹配。

如果所有条件都匹配，则此内容成功匹配该策略；如果其中有一个条件不匹配，则继续执行下一条策略。以此类推，如果所有内容过滤策略都不匹配，则设备允许此条报文通过。

3）如果数据报文的内容成功匹配一条内容过滤策略，则设备对报文内容进行关键字检测，检测内容中是否存在内容过滤策略定义的关键字。

如果识别出关键字，则设备会执行响应动作；否则，设备允许该报文通过。

管理员在 NGFW 中配置内容过滤功能后可实现如下效果：

- 降低公司机密泄露的风险。
  - 对内网用户上传的文件内容进行过滤，阻止内网用户上传包含公司机密信息的文件。
  - 对内网用户发送的邮件内容进行过滤，阻止内网用户发送包含公司机密信息的邮件。
  - 对内网用户发布的帖子等内容进行过滤，阻止内网用户发布包含公司机密信息的内容。
  - 对外网用户从内网服务器下载的文件内容进行过滤，防止黑客窃取包含公司机密信息的文件。
- 降低因员工浏览、发布或传播违规信息给公司带来的法律风险。

- 对内网用户上传和下载的文件内容进行过滤，阻止内网用户上传和下载包含违规信息的文件。
- 对内网用户接收和发送的邮件内容进行过滤，阻止内网用户收发包含违规信息的邮件。
- 对内网用户搜索、浏览网页、发布的内容进行过滤，阻止内网用户搜索、浏览、发布包含违规信息的内容。
- 对外网用户上传到内网服务器的文件内容进行过滤，防止外网用户将违规信息发送到公司服务器。

➢ 阻止员工浏览和搜索与工作无关的内容。

- 对内网用户搜索、浏览网页的内容进行过滤，阻止内网用户搜索、浏览与工作无关的网页。

7.10.1 关键字组

关键字组用于设置关键字，并把关键字分组，这些关键字组是定义内容过滤策略的基础，用于内容过滤中限制某些内容的搜索和上传。

关键字是内容过滤时 NGFW 需要识别的内容，如果在文件或应用中识别出关键字，NGFW 会对相应文件或应用做出响应。关键字通常为机密信息（如公司商业机密）、违规信息（如敏感、暴力或违反公司规则的信息），分为文本和正则表达式两种方式：

1）文本方式是使用文本的方式表示需要识别的关键字。

2）正则表达式方式是使用正则表达式的方式表示需要识别的关键字。一个正则表达式可以表示多个关键字。比如“abc.de”中的“.”可以匹配任意单个字符。正则表达式的具体说明如下表所示。

字符	说明
.	匹配任意单个字符。 说明： 正则表达式不能以“.”结尾。
()	标记一个子表达式的开始和结束位置。
*	匹配前面的字符或表达式零次或多次。比如 It*可以匹配 It、Itt 等。
+	匹配前面的字符或表达式一次或多次。

字符	说明
|	等同于或。比如 l|good 可以匹配 l 或 good。(l|g)ood 匹配 lood 或 good。
[]	匹配所有包含的任意一个字符。
-	用于创建范围表达式。比如[a-d]可以匹配 a 和 d 之间的任意一个字符。包含 a 和 d。
{n}	n 是一个小于等于 20 的非负整数。匹配前面的字符 n 次。比如 e{2}不能匹配 let 中的 e，可以匹配 eerie 中的两个 e。
\	要对上述任一特殊字符执行字面匹配，必须通过在这些字符前面加上“\”，对这些字符进行转义。比如“\(”、“\.”。
\d	匹配一个数字字符，等价于[0-9]。
\w	匹配数字、字母和下划线。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **内容过滤** > **关键字组**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置关键字组时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置关键字组的名称。当配置内容策略时，名称会出现在“关键字组”的参数选择列表中。
描述	必选项，设置对关键组的具体描述。合理填写描述信息有助于管理员正确理解关键字组的功能，方便选择、查找和维护。
协议	设置关键字组应用的协议类型。可选项：http、smtp、pop3。
方向	协议类型为“http”时，设置对满足关键字组的数据报文进行上传还是下载。 可选项：up、down。
领域	协议类型为“smtp”、“pop3”时，设置邮件协议字段。可选项：from、to、subject、content、attach。
关键字	设置内容过滤的敏感内容。 说明： 参数值是支持通配符*（表示多个字符）和？（表示任意一个字符）的字符串，最多不能超过 255 个字符。而且，通配符*和?只可以出现关键字中间，关键字首尾不可以配置通配符*和?。否则系统会提示错误信息。

步骤 3 点击【确定】按钮完成关键字组的添加。

CLI 方式配置

data-filter group add name <*string1*> **description** <*string2*> **protocol** http **direction** <up|down>

命令描述

添加基于 HTTP 协议的关键字组。

参数说明

data-filter group add	添加基于 HTTP 协议的关键字组。
name	必选项，设置关键字组名称。
string1	字符串类型。
description	必选项，设置对关键字组的具体说明。
string2	字符串类型。
direction	必选项，设置对满足关键字组的数据报文的执行动作。
up|down	上传|下载

以下是添加关键字组的示例：

添加名称为“datatest”描述信息为“基于 http 协议的关键字组”协议为“http”传输方向为“up”的关键字组。

TopsecOS# **data-filter group add name** *datatest* **description** *基于 http 协议的关键字组* **protocol** http **direction** up

data-filter group add name <*string1*> **description** <*string2*> **protocol** <smtp|pop3> **field** <from|to|subject|content|attach>

命令描述

添加关键字组。

参数说明

data-filter group add	添加关键字组。
name	必选项，设置关键字组名称。
string1	字符串类型。
description	必选项，设置对关键字组的具体说明。
string2	字符串类型。
protocol	必选项，设置关键字组支持的协议类型。
smtp|pop3	简单邮件传输协议|邮局协议
field	必选项，设置邮件协议字段。
from|to|subject|content|attach	发件人|收件人|主题|内容|附件

以下是添加关键字组的示例：

添加名称为“data1”描述信息为“*添加邮件型关键字组*”协议为“smtp”邮件协议字段为“from”的关键字组。

TopsecOS# **data-filter group add name** *data1* **description** *添加邮件型关键字组* **protocol** smtp **field** from

data-filter group set name <*string1*> **protocol** http **direction** <up|down>

命令描述

设置基于 HTTP 协议的关键字信息。

data-filter group set name <*string1*> **protocol** <smtp|pop3> **field** <from|to|subject|content|attach>

命令描述

设置基于 smtp 或 pop3 协议的内容过滤的关键字信息。

data-filter group set name <*string1*> **do** <add|delete> **keywords** <*string2*>

命令描述

增加或删除关键字组。

参数说明

data-filter group set	添加内容过滤的关键字组。
name	必选项，指定内容过滤关键字组。
string1	字符串类型，表示关键字组名称。
do	必选项，设置执行动作。
add|delete	增加|删除
keywords	必选项，设置增加或删除的规则。
string2	字符串类型。

以下是添加关键字组的示例：

在关键字组 data11 中添加关键字 sina。

TopsecOS# **data-filter group add name** *data11* **description** *guanjianzi* **protocol** http **direction** up

TopsecOS# **data-filter group set name** *data11* **do** add **keywords** *sina*

data-filter group show [**name** <*string*>]

命令描述

显示内容过滤的关键字组信息。

以下是显示关键字组信息的示例：

```
TopsecOS# data-filter group show
ID (GROUP-NAME) (GROUP-DESC)
-----------------------------------------
10561 (12314134) (325315315)
10715 (111) (miaoshu111)
10716 (222) (d)
10717 (333) (d)
```

7.10.2 内容过滤策略

内容过滤策略决定了对哪些应用或文件类型进行过滤，定义内容过滤策略时需要引用关键字组，NGFW 即可对通过设备传输的不同协议的内容进行过滤。当数据报文匹配关键字组中的具体关键字时，按照关键字的权限进行处理，否则系统将按照与关键字权限相反的权限对数据进行处理。

通过配置内容过滤策略，并且在访问控制规则中引用该策略，NGFW 可以实现对应用层的流量的检测和控制。关于访问控制规则的设置具体请参见 7.2.2 配置访问控制规则。NGFW 不仅支持对传统的应用层协议进行配置及深度内容检测，而且支持各种通过自定义应用来扩展新的应用类型。

WEBUI 方式配置

在配置内容策略之前，需要先进行关键字组的配置，关于关键字组的设置具体请参见 7.10.1 关键字组。

步骤 1 选择 **安全策略** > **内容过滤** > **内容策略**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置内容过滤规则时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置内容过滤规则的名称。名称必须是唯一的，当配置安全策略时，名称会出现在“内容过滤”的参数选择列表中。
描述	设置内容过滤策略的具体说明信息。合理填写描述信息有助于管理员正确理解内容过滤策略的功能。
关键字组	配置关键字组的执行动作，可选项：allow、block、alert。 “allow”表示允许，当识别出关键字后，允许内容传输。 “block”表示阻断，当识别出关键字后，阻断内容传输并记录日志。在用户看来则是无法显示网页、上传或下载文件失败、邮件发送或接收失败。 “alert”表示告警，当识别出关键字后，记录日志但不阻断内容传输。 关于关键字组的设置具体请参见 7.10.1 关键字组。

步骤 3 点击【确定】按钮完成内容过滤规则的添加。

CLI 方式配置

步骤	配置说明
1	配置关键字组，具体请参见 7.10.1 关键字组
2	配置内容过滤策略及其属性

data-filter policy add name <*string1*> [**description** <*string2*>]

命令描述

添加内容过滤策略。

参数说明

data-filter policy add	添加内容过滤策略。
name	必选项，设置内容过滤策略名称。
string1	字符串类型。
description	可选项，设置对内容过滤策略的具体说明。
string2	字符串类型。

以下是添加内容过滤策略的示例：

添加名称为 data-filter1 的内容过滤策略。

```
TopsecOS# data-filter policy add name data-filter1
```

data-filter policy set name <*string1*> **group** <*string2*> **action** <allow|alert|block>

命令描述

设置内容过滤策略。

参数说明

data-filter policy set	设置内容过滤策略。
name	必选项，指定内容过滤策略。
string1	字符串类型，表示内容过滤策略名称。
group	必选项，指定内容过滤策略包含的关键字组。
string2	字符串类型，表示关键字组名称。
action	必选项，设置关键字组的执行动作。
allow|alert|block	允许|警告|阻断

以下是设置内容过滤策略的示例：

设置内容过滤策略 data-filter1 中关键字组 data1 的执行动作为 allow。

```
TopsecOS# data-filter group add name data1 description 添加邮件型关键字组
protocol smtp field from
TopsecOS# data-filter policy add name data-filter1
TopsecOS# data-filter policy set name data-filter1 group data1 action allow
```

data-filter policy show [**name** <*string*>]

命令描述

显示内容过滤策略。

以下是显示内容过滤策略的示例：

```
TopsecOS# data-filter policy show
ID (POLICY-NAME) (POLICY_DESC)
----------------------------------------
10563 (wer-3) ()
10564 (wer-3-4) ()
10565 (wer-3-5) ()
```

10566 (wer-3-1) ()
10567 (wer-3-2) ()
10568 (wer-3-1-1) ()
10569 (wer-3-5-1) ()
10718 (p1) ()

data-filter rules commit <cr>

命令描述

内容过滤策略的关键字组提交编辑。

7.11文件过滤

随着社会和网络技术的不断发展，病毒常感染或附着在一些文件或用户信息中，且病毒的反检测和渗透防火墙的能力越来越强，文件安全已经成为公司和个人越来越关注的问题。NGFW 提供了文件过滤功能，通过阻断特定类型的文件传输，可以降低内部网络执行恶意代码和感染病毒的风险，还可以防止员工将公司机密文件泄露到互联网。

文件过滤是一种根据文件类型对通过防火墙的文件进行过滤的安全机制。机密信息和病毒往往存在于特定的文件类型中，比如机密信息一般保存在文档文件中，病毒信息一般附着在可执行文件中，而管理员在 NGFW 上部署文件过滤模块后可实现以下功能：

- 降低机密信息泄露的风险。

机密信息一般保存在文档中，而文档可以被压缩成压缩文件。员工上传包含机密的文档到外网或者黑客从内网服务器窃取机密文档，都会导致公司机密或用户信息的泄露。因此，阻止内网用户上传文档文件和压缩文件到外网，以及外网用户从内网服务器下载文档文件和压缩文件，可以降低机密信息泄露的风险。

- 降低病毒文件进入公司内部网络的风险。

病毒常常包含在可执行文件中，阻止内网用户从外网下载可执行文件或阻断外网用户上传可执行文件到内网服务器，可以降低病毒进入内网的风险。

- 阻止占用带宽和影响员工工作效率的文件传输。

公司员工下载大量与工作无关的视频或图片文件，占用公司网络带宽，降低工作效率。因此，阻止内网用户从外网下载视频、图片和压缩文件，可以保证正常业务的带宽和员工的工作效率。

如果管理员想进一步降低机密信息泄露的风险，可以将文件过滤与内容过滤功能结合使用，关于内容过滤的设置具体请参见 7.10 内容过滤。如果管理员想进一步降低内网感染病毒的风险，可以将文件过滤与病毒过滤功能结合使用，关于病毒过滤的设置具体请参见 7.12 病毒过滤。

WEBUI 方式配置

步骤 1 选择 **安全策略** > **文件过滤**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置文件过滤规则时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置文件过滤策略的名称。当配置安全策略时，名称会出现在“文件过滤”的参数选择列表中。
描述	设置对文件过滤规则的具体描述。合理填写描述信息有助于管理员正确理解文件过滤策略的功能，方便选择、查找和维护。
规则	设置文件过滤规则信息。 1）名称：指定文件过滤具体规则的名称。 2）协议：文件是承载在应用协议上进行传输的，可选项：any、HTTP、SMTP、FTP_Data、POP3。 3）文件类型：指定想要允许、阻断或告警的文件类型，该文件类型是设备能够识别的文件真正的类型，如 office、java-class、rtf 等。 4）方向：指定文件传输方向，可选项：上传、下载、双向。其中，“上传”表示用户将文件从源地址发送到目的地址，“下载”表示用户将文件从目的地址接收到源地址。 5）动作：设置当文件匹配全部条件时设备执行的响应，可选项：允许、阻断、告警。其中“阻断”表示阻断文件传输并记录日志，“告警”表示允许文件传输并记录日志。

步骤 3 点击【确定】按钮完成文件过滤规则的添加。

CLI 方式配置

步骤	配置命令	配置说明
1	**file-block rule add name** <*string1*> [**app** <*string2*>] [**file-type** <*string3*>] [**direction** <both|download|upload>] [**action** <allow|alert|block>]	显示文件过滤规则支持的应用、协议
2	**file-block profile add name** <*string1*> [**comment** <*string2*>] [**rule** <*string3*>]	配置文件过滤具体规则

file-block rule add name <*string1*> [**app** <*string2*>] [**file-type** <*string3*>] [**direction** <both|download|upload>] [**action** <allow|alert|block>]

命令描述

添加文件过滤策略的规则信息。

参数说明

file-block rule add	添加文件过滤策略的规则信息。
name	必选项，设置规则名称。
string1	字符串类型，表示规则名称。
app	可选项，设置文件过滤规则支持的协议。
string2	字符串类型，可选项：any|P-10|P-119|P-128|P-130；默认值：any。对应的协议名称为：any、HTTP、SMTP、FTP_DATA、POP3。
file-type	可选项，设置过滤的文件类型。
string3	字符串类型。
direction	可选项，设置文件传输的方向。
both|download|upload	双向|下载|上传
action	可选项，设置当文件匹配全部条件时设备执行的响应动作。
allow|alert|block	允许|阻断|告警

以下是添加文件过滤具体规则的示例：

添加名称为 ruletest 对传输方向为 download 的文件执行动作 allow 的文件过滤策略规则。

```
TopsecOS# file-block rule support-app show
app                 protocol-name
any                 any
P-10                HTTP
P-119               SMTP
P-128               FTP_Data
```

P-130 POP3

TopsecOS# **file-block rule add name** *ruletest* **app** *P-10* f**ile-type** *any* **direction** download **action** allow

file-block rule show [**name** <*string1*>] [**profile-name** <*string2*>]

命令描述

显示文件过滤具体规则。

参数说明

file-block rule show	显示文件过滤具体规则。
name	可选项，指定文件过滤具体规则的名称。
string1	字符串类型。
profile-name	可选项，指定文件名称。
string2	字符串类型。

以下是显示文件过滤规则信息的示例：

TopsecOS# **file-block rule show**

ID 10057 file-block rule add name er4t file-type 'any' app 'P-10 ' direction both action block

ID 10059 file-block rule add name er4t-1 file-type 'any' app 'P-10 ' direction both action block

ID 10181 file-block rule add name rule2 file-type 'any' app 'any' direction both action allow

file-block rule clone name <*string*>

命令描述

克隆文件过滤策略的具体规则。

file-block rule rename name <*string1*> **new-name** <*string2*>

命令描述

重命名文件过滤具体规则。

file-block rule delete name <*string*>

命令描述

删除指定名称的文件过滤规则。

file-block rule delete profile-name <*string*>

命令描述

删除指定名称的文件过滤策略。

file-block rule support-file-type show <cr>

命令描述

显示文件过滤规则支持的文件类型。

以下是显示文件过滤规则支持的文件类型的示例：

```
TopsecOS# file-block rule support-file-type show
support file type :
any
ms-executable
linux-elf
java-class
ms-office-2003-wps
ms-office-2007
mdb
accdb
rtf
hlp
chm
mht
reg
pdf
eps
```

```
fm
rar
zip
7z
arj
bz2
gzip
```

file-block rule support-app show <cr>

命令描述

显示文件过滤规则支持的应用对象。

以下是显示文件过滤规则支持的应用对象的示例：

```
TopsecOS# file-block rule support-app show
app             protocol-name
any             any
P-10            HTTP
P-119           SMTP
P-128           FTP_Data
P-130           POP3
```

file-block profile add name <*string1*> [**comment** <*string2*>] [**rule** <*string3*>]

命令描述

添加文件过滤策略。

参数说明

file-block profile add	添加文件过滤策略。
name	必选项，设置文件过滤策略的名称。
string1	字符串类型。
comment	可选项，设置文件过滤规则的具体说明。
string2	字符串类型。
rule	可选项，设置文件过滤策略包含的过滤规则。

string3	字符串类型，表示已添加的过滤规则名称。

以下是添加文件过滤策略的示例：

添加名称为“*profiletest*”，规则为“*ruletest*”的文件过滤策略。

```
TopsecOS# file-block rule add name ruletest
TopsecOS# file-block profile add name profiletest rule ruletest
```

file-block profile show [**name** <*string*>]

命令描述

显示文件过滤策略信息。

以下是显示文件过滤策略信息的示例：

```
TopsecOS# file-block profile show
ID 10058 file-block profile add name weg rule 'er4t '
ID 10060 file-block profile add name weg-1 rule 'er4t-1 '
```

7.12病毒过滤

病毒是一种恶意代码，可感染或附着在应用程序或文件中，一般通过邮件或文件共享等协议进行传播，消耗主机资源、控制主机权限并占用网络带宽，还可能对主机硬件造成破坏，从而威胁用户主机和网络的安全。病毒一旦进入网络内部，就会很快地在网络环境中传播，造成整个网络的阻塞，甚至瘫痪。网络病毒已被公认为网络安全的最主要威胁之一。为了解决这一问题，NGFW 提出了病毒过滤功能，防止病毒文件通过网关设备进入受保护网络。

病毒过滤是对应用层数据的过滤，能够对通过 HTTP、FTP 传输的文件，以及使用 SMTP、POP3 协议传送的邮件正文、附件进行准确识别，并对识别出病毒的文件按照预定义的响应措施做出相应处理，使病毒文件在进入受保护网络之前即被干预处理，并可根据文件扩展名选择过滤的附件类型。同时，病毒过滤功能支持管理员定制，管

理员可以根据企业网络的具体使用情况来配置各种协议的病毒过滤策略。NGFW 的病毒过滤功能支持的协议主要有 HTTP、FTP、POP3 和 SMTP。

在系统的访问控制规则中，管理员可以指定是否对满足这条规则的网络数据进行病毒过滤。当系统的某条规则允许来自某个地址段访问病毒过滤支持的协议服务的数据流通过，并且启动了病毒过滤引擎时，就会截取该数据流，并按照该协议过滤策略调用杀毒引擎对传输的网络文件进行病毒过滤。关于访问控制规则的设置具体请参见7.2.2 配置访问控制规则。

病毒过滤的处理流程分为三步：检测入口，病毒检测和响应处理，具体说明如下表所示。

步骤	说明
检测入口	判断目标：文件是否需要做病毒检测。 判断条件：传输文件的应用类型；传输文件的协议类型和文件传输方向。
病毒检测	判断目标：文件中是否包含病毒。 判断条件：文件扫描结果；病毒特征库。
响应处理	判断目标：如何处理病毒文件。 判断条件：防病毒例外中定义的病毒；协议中定义的响应动作。

具体流程如下图所示。

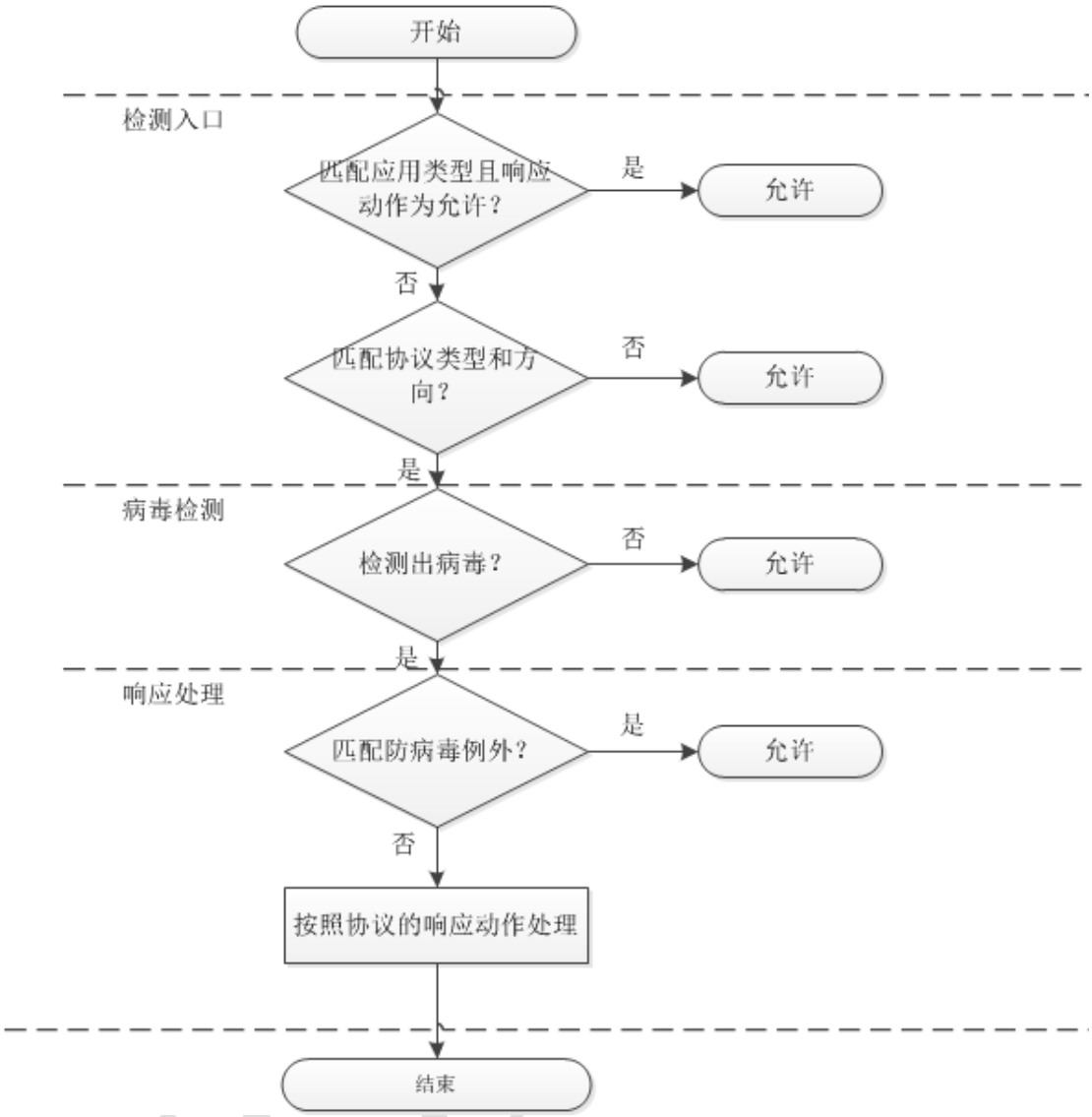


图 7-9 病毒过滤流程

WEBUI 方式配置

步骤 1 选择 **安全策略** > **病毒过滤**。

步骤 2 点击『添加』，弹出“添加”窗口。

在设置病毒过滤规则时，各项参数的具体说明如下表所示。

参数	说明
名称	必选项，设置病毒过滤规则的名称。
描述	设置病毒过滤规则的具体说明。描述信息可以方便管理员区分不同的病毒过滤规则的功能。

参数	说明
http	超文本传输协议。设置基于 HTTP 协议的病毒过滤规则的执行方向和动作。方向可选项：双向、上传、下载，动作可选项：允许、阻断、警告。 说明： 1）双向、上传和下载指文件的传输方向，是 NGFW 判断文件是否需要做病毒过滤检测的重要依据。其中，“上传”指文件从客户端向服务器发送，“下载”指文件从服务器向客户端发送。 2）响应动作“允许”表示放行文件，“阻断”表示断开协议连接，记录日志，“警告”表示放行文件，记录日志。
smtp	简单邮件传输协议。设置基于 SMTP 协议的病毒过滤规则的执行方向和动作。文件传输方向可选项：上传，响应动作可选项：允许、阻断、警告。
pop3	邮局协议的第 3 个版本。设置基于 POP3 协议的病毒过滤规则的执行方向和动作。文件传输方向可选项：下载，响应动作可选项：允许、警告。
ftp	文件传输协议。设置基于 FTP 协议的病毒过滤规则的执行方向和动作。文件传输方向可选项：双向、上传、下载，响应动作可选项：允许、阻断、警告。
防病毒例外	如果管理员认为某个病毒为误报时，可以将该病毒 ID 添加到“防病毒例外”中，使这条病毒规则失效。当后续再检测到包含此病毒的文件通过时，系统将放行该文件。 NGFW 提供的“防病毒例外”机制具有白名单的作用，使管理员可以对某些重要文件做特殊处理，即忽略系统的检测结果而直接放行，从而避免了由于系统误报等原因造成的文件传输失败等情况发生，提高了病毒过滤功能的使用灵活性。 说明： 防病毒例外威胁 ID 不能超过 8 个字符。威胁 ID 从日志中获取。

注意

- ✧ 由于协议的连接请求均由客户端发起，为了使连接可以成功建立，管理员在配置安全策略时需要确保将客户端所在安全区域设置为源、服务器所在安全区域设置为目的。

步骤 3 点击【确定】按钮完成病毒过滤规则的添加。

CLI 方式配置

av profile add name <*string1*> [**comment** <*string2*>]

命令描述

添加病毒过滤策略。

参数说明

av profile add	添加病毒过滤策略。
name	必选项，设置病毒过滤策略名称。
string1	字符串类型，表示策略名称。
comment	可选项，设置对病毒过滤策略的具体说明。
string2	字符串类型。

以下是添加病毒过滤策略的示例：

添加名称为 avtest 的病毒过滤策略。

```
TopsecOS# av profile add name avtest
```

av profile set name <*string1*> **protocol** ftp [**action** <allow|alert|block>] [**direction** <both|upload|download>]

av profile set name <*string1*> **protocol** http [**action** <allow|alert|block>] [**direction** <both|upload|download>] [**exception-app** <*string2*>]

av profile set name <*string1*> **protocol** smtp [**action** <allow|alert|block>] [**direction** <upload>]

av profile set name <*string1*> **protocol** pop3 [**action** <allow|alert>] [**direction** <download>]

命令描述

配置病毒过滤策略。

参数说明

av profile set	配置病毒过滤策略。
name	必选项，指定病毒过滤策略。
string1	字符串类型，表示病毒过滤策略名称。
protocol	必选项，设置病毒检测协议。
http|ftp|smtp|pop3	超文本传输协议|文件传输协议|简单邮件传输协议|邮局协议
action	必选项，设置对匹配病毒过滤规则的报文的执行动作。 说明： 不同病毒过滤检测协议对匹配策略的报文的执行动作不同。
allow|alert|block	允许|警告|阻断
direction	可选项，设置病毒过滤规则的检测方向。
both|download|upload	双向|下载|上传
exception-app	可选项，设置病毒过滤策略信任的应用程序，格式：应用名|操作，如：P-77|allow。

string2	字符串类型。

以下是配置病毒过滤策略的示例：

设置病毒过滤策略 avtest 的协议类型为 ftp，执行动作为 block，文件传输方向为 upload。

```
TopsecOS# av profile add name avtest
TopsecOS# av profile set name avtest protocol ftp action block direction upload
```

av profile set exception-av <*string*>

命令描述

配置病毒过滤策略可确定的病毒信息。

参数说明

av profile set	配置病毒过滤策略信息。
exception-av	必选项，设置可确定的病毒信息。
string	字符串类型。格式：123|worm/kido.aap。

av profile show [**name** <*string*>]

命令描述

显示反病毒配置文件。

以下是显示反病毒配置文件的示例：

```
TopsecOS# av profile show
ID 10293 av profile add name avdefault
        http direction both action block
        ftp direction both action block
        smtp direction upload action alert
        pop3 direction download action alert
ID 10062 av profile add name dfgfage
        http direction both action allow
        ftp direction both action allow
        smtp direction upload action allow
```

```
pop3 direction download action allow
```

av profile rename name <*string1*> **new-name** <*string2*>

命令描述

重命名病毒过滤策略。

av profile clone name <*string*>

命令描述

克隆病毒过滤策略。

av scan-filter set enable <yes|no>

命令描述

设置病毒过滤开关，默认为关闭。

av scan-filter show <cr>

命令描述

显示病毒过滤策略信息。

以下是显示病毒过滤策略信息的示例：

```
TopsecOS# av scan-filter show
av scan-filter set enable yes
```

av statistic show <cr>

命令描述

显示病毒过滤策略统计信息。

以下是显示病毒过滤策略统计信息的示例：

```
TopsecOS# av statistic show
protocol            total
```

FTP	0
HTTP	0
MAIL	0

av statistic clean <cr>

命令描述

清除病毒过滤策略统计信息。

8 显示与监控

8.1 显示（首页）

NGFW 能够实时显示系统的运行情况，精准的检测网络中的流量信息，用户可以根据流量统计分析网络中的潜在风险，并根据监控结果实时修改设备的配置信息。首页以丰富清晰的图像化界面进行生动展现，为管理员提供可靠的网络监管平台。管理员只需通过查看 NGFW 的首页即可轻松快捷掌控防护区域中是否存在安全威胁，了解通往防护对象的流量，结合 NGFW 的日志报表功能可快速追踪攻击来源，保障网络安全。

NGFW 提供优质、丰富、精准、清晰的监控平台同时还提供管理员对监控面板的定制化需求，为管理员提供个性的体验服务。管理员可根据其所关心的信息加载相应的监控窗口至首页中，并可根据管理习惯设计界面风格和监控窗口所处的具体位置，构建特色的界面布局，方便管理员快速掌控有效数据进而分析网络运行情况。本章介绍管理员如何设计首页的布局以及如何查看各监控窗口信息。

8.1.1 设计首页界面布局

在首页界面有多个状态窗口，用户可根据需求进行自定义设置：设置状态窗口是否显示在界面上、调整其显示位置。

WEBUI 方式配置

步骤 1 选择 **首页**，进入首页界面，如下图所示。

步骤 2 设置监控面板显示的监控窗口。

点击界面下方的“ 导入模块 ”，在弹出的界面中，勾选模块名称即可加载对应该名称的监控窗口到监控面板中。如果勾选“全选”可将 NGFW 支持的所有监控窗口显示在监控面板中；点击“ 恢复默认窗口 ”，监控面板将显示 NGFW 默认的监控窗口，如下图所示。

步骤 3 设置窗口排列列数。

点击页面左下角的“”，监控窗口在监控面板中按一列显示；点击“”，监控窗口将按两列显示；点击“”，监控窗口将按三列显示。界面默认按照三列显示。

步骤 4 改变窗口位置。

将管理主机的鼠标移动到监控窗口标题栏，待鼠标变为“”后，长按鼠标左键并将其拖动至具体的位置，确定位置后，放开鼠标，即可改变该监控窗口的显示位置，如下图所示。

步骤 5 关闭窗口。

点击窗口右上角的“”按钮，即可关闭相应的窗口。

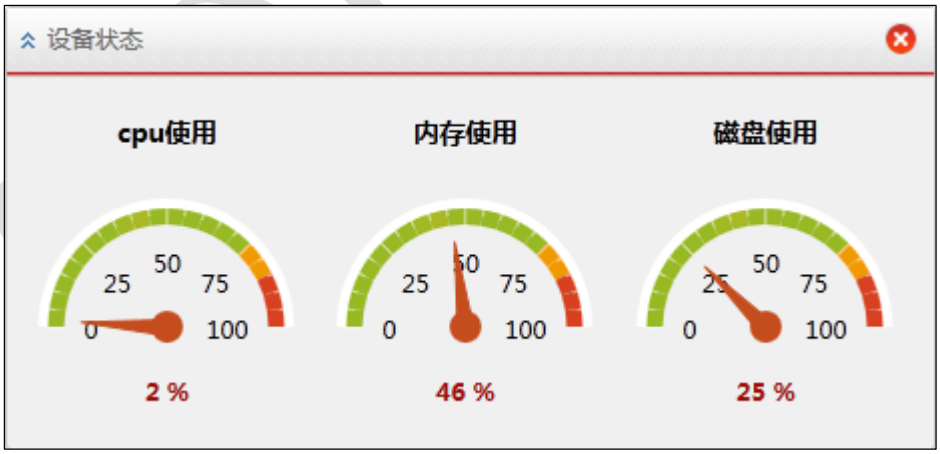
8.1.2 查看首页信息

- 系统信息

系统信息窗口显示 NGFW 的名称、型号、序列号、软件版本、许可证版本号、系统名称、终端超时时间、系统时间、系统运行时间，如下图所示。

➢ 设备状态

设备状态窗口显示 NGFW 的 CPU、内存和磁盘的使用情况，如下图所示。界面每 5 秒自动更新一次设备状态。



➢ 接口信息

接口信息窗口显示 NGFW 所有物理接口信息，包括接口名称、链路状态、接口模式、MTU、状态、速率、发送包数、发送字节、接收包数、接收字节、丢弃包数。

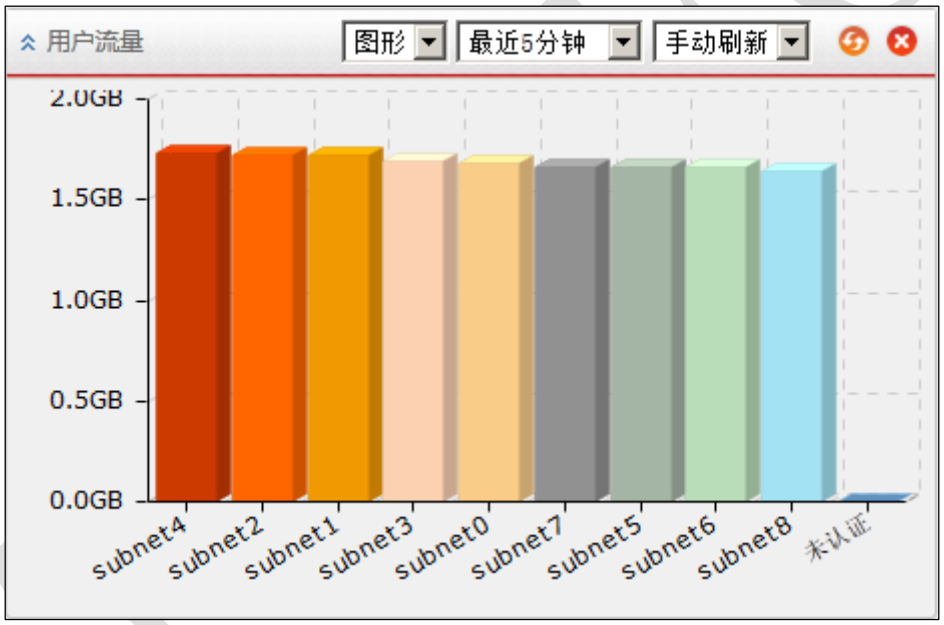
接口信息窗口支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示接口信息；视图模式以图标形式显示接口状态，将管理主机的鼠标移动至接口图标上可显示接口的详细信息。界面每 5 秒自动更新一次设备状态。

➢ 用户流量

用户流量窗口实时显示不同用户的流量信息，包括用户名、所属组、上行流量、下行流量和会话数，支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示用户流量；视图模式以二维图形式显示用户流量，横轴表示用户，纵轴表示流量大小，将管理主机的鼠标移动至流量曲线图上可显示用户流量的详细信息。

可根据需求点击下拉列表选择需要统计的用户流量时间间隔，可选项为最近 5 分钟、最近 30 分钟、最近一小时、最近一天、最近一周、最近一月、前一天、前一周和前一月；选择窗口的刷新周期，可选项为 5 秒、10 秒、30 秒和手动更新。

用户名	所属组	上行流量	下行流量	总流量	会话数
subnet2	net1a	50.86MB	1.71GB	1.76GB	0
subnet0	net1a	49.21MB	1.70GB	1.74GB	1
subnet1	net1a	50.19MB	1.69GB	1.74GB	1
subnet3	net1a	50.94MB	1.68GB	1.73GB	0
subnet4	net1a	51.26MB	1.65GB	1.70GB	0
subnet7	net1b	49.25MB	1.64GB	1.69GB	0
subnet5	net1a	52.21MB	1.63GB	1.68GB	10
subnet8	net1b	49.45MB	1.63GB	1.67GB	0
subnet6	net1b	50.75MB	1.61GB	1.66GB	2
未认证	未知	4.08MB	0B	4.08MB	2

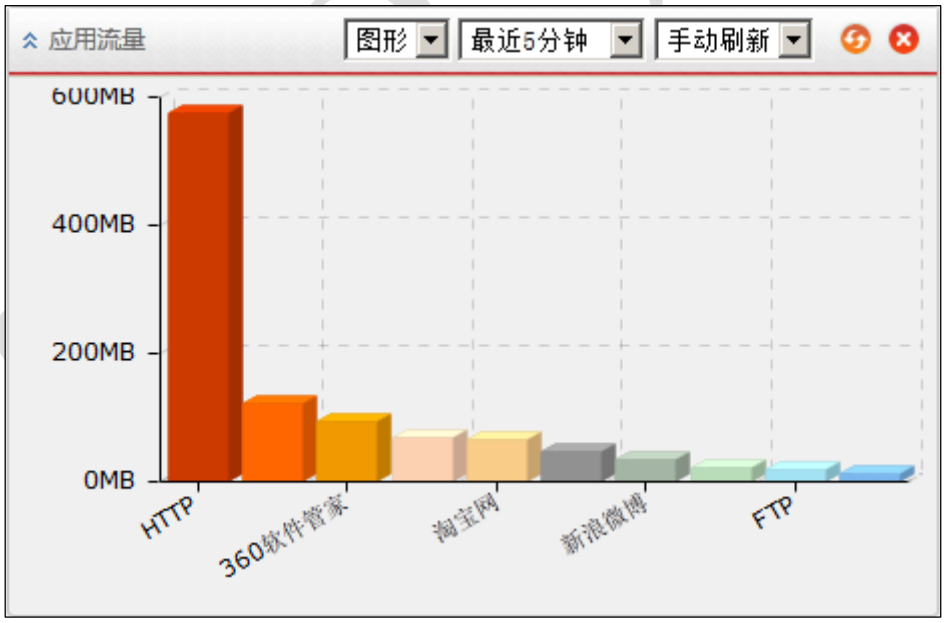


➢ 应用流量

应用流量窗口实时显示不同应用的流量信息，包括应用名称、用户名、所属组、上行流量、下行流量和会话数，支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示应用流量；视图模式以二维图形式显示应用流量，横轴表示应用，纵轴表示流量大小（单位 KB），将管理主机的鼠标移动至流量曲线图上可显示应用流量的详细信息。

可根据需求点击下拉列表选择需要统计的应用流量时间间隔，可选项为最近 5 分钟、最近 30 分钟、最近一小时、最近一天、最近一周、最近一月、前一天、前一周和前一月；选择窗口的刷新周期，可选项为 5 秒、10 秒、30 秒和手动更新。

应用名称	用户名	所属组	上行流量	下行流量	总流量	会话数
HTTP	un_125	未知	60.50MB	521.75MB	582.25MB	0
HTTP下载	un_123	未知	1.40MB	95.23MB	96.63MB	0
360软件管家	un_60	未知	28.33MB	64.16MB	92.49MB	0
POP3	未认证	未知	43.52KB	77.70MB	77.74MB	0
淘宝网	un_123	未知	3.02MB	58.54MB	61.56MB	2
HTTPS	un_125	未知	20.47MB	22.17MB	42.64MB	0
Itunes	un_16	未知	22.45KB	34.59MB	34.61MB	0
新浪微博	un_123	未知	1.80MB	23.18MB	24.97MB	1
京东商城	un_30	未知	3.97MB	18.95MB	22.92MB	0
搜狗拼音更新	un_7	未知	56.01KB	15.77MB	15.82MB	0

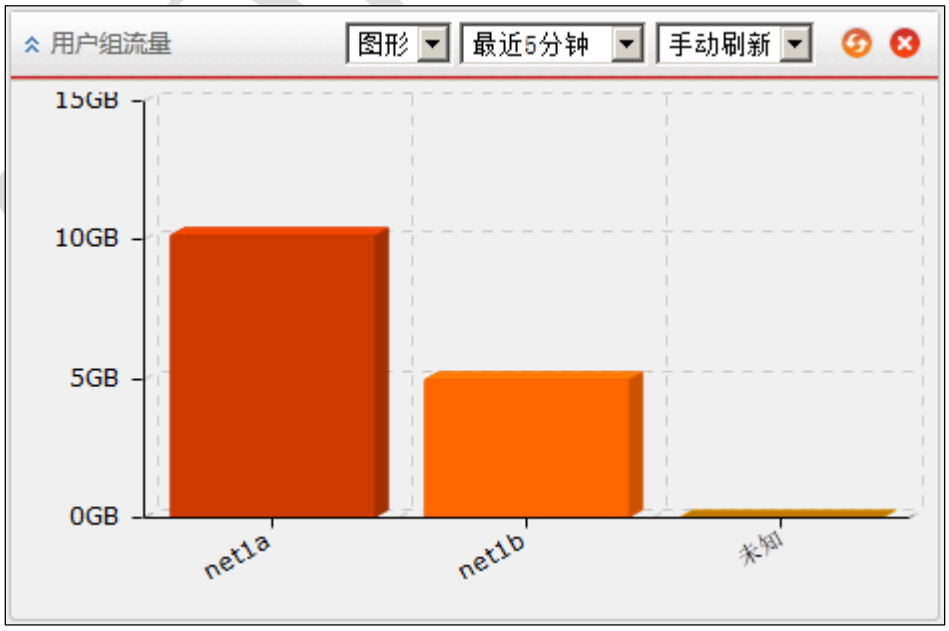


➢ 用户组流量

用户组流量窗口实时显示不同用户组的流量信息，包括用户名、所属组、上行流量、下行流量和会话数，支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示用户组流量；视图模式以二维图形式显示用户组流量，横轴表示用户

组，纵轴表示流量大小（单位 KB），将管理主机的鼠标移动至流量曲线图上可显示用户组流量的详细信息。

可根据需求点击下拉列表选择需要统计的用户组流量时间间隔，可选项为最近 5 分钟、最近 30 分钟、最近一小时、最近一天、最近一周、最近一月、前一天、前一周和前一月；选择窗口的刷新周期，可选项为 5 秒、10 秒、30 秒和手动更新。

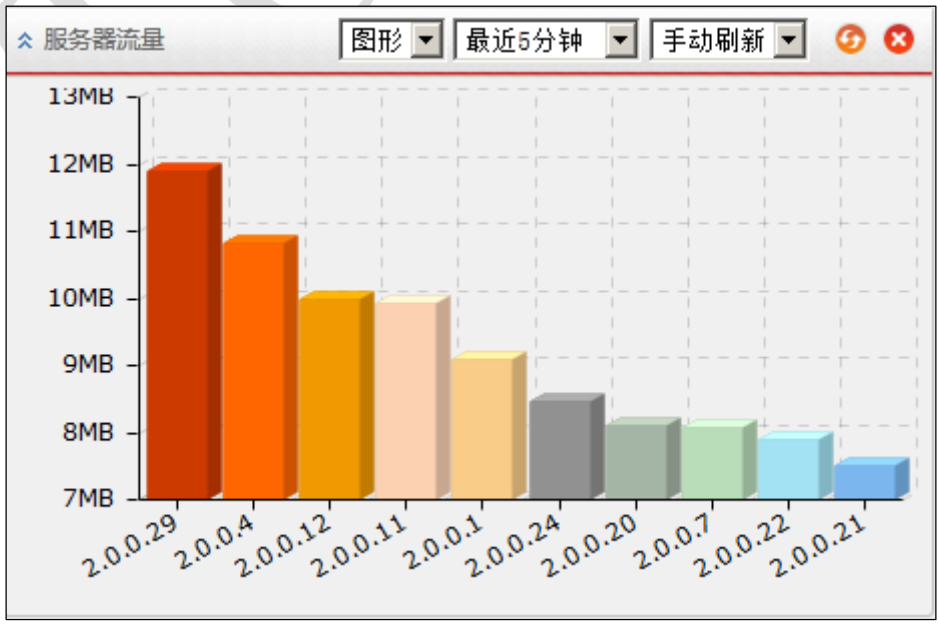


- 服务器流量

服务器流量窗口实时显示不同服务器的流量信息，包括 serverip、VSERVER ID、上行流量、下行流量和会话数，支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示服务器流量；视图模式以二维图形式显示服务器流量，横轴表示服务器，纵轴表示流量大小（单位 B），将管理主机的鼠标移动至流量曲线图上可显示服务器流量的详细信息。

可根据需求点击下拉列表选择需要统计的服务器流量时间间隔，可选项为最近 5 分钟、最近 30 分钟、最近一小时、最近一天、最近一周、最近一月、前一天、前一周和前一月；选择窗口的刷新周期，可选项为 5 秒、10 秒、30 秒和手动更新。

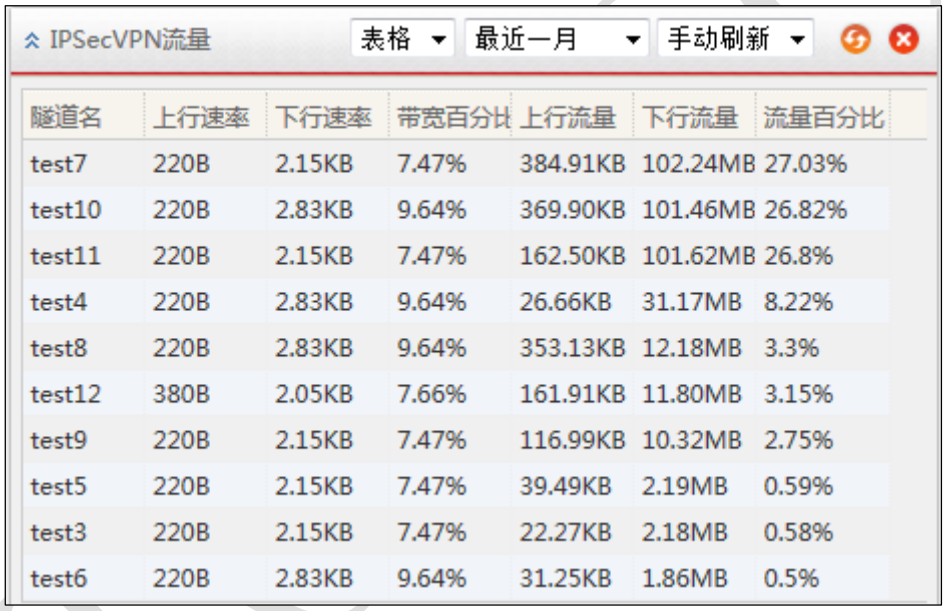
serverip	VSERVER I	上行流量	下行流量	总流量	会话数
2.0.0.29	0	12.52MB	187.93KB	12.70MB	0
2.0.0.4	0	10.74MB	204.15KB	10.94MB	0
2.0.0.12	0	10.70MB	184.95KB	10.89MB	1
2.0.0.11	0	10.06MB	195.49KB	10.25MB	0
2.0.0.27	0	9.04MB	191.84KB	9.22MB	0
2.0.0.24	0	8.52MB	231.73KB	8.74MB	1
2.0.0.1	0	8.54MB	198.78KB	8.73MB	0
2.0.0.22	0	8.35MB	198.22KB	8.54MB	0
2.0.0.8	0	7.98MB	197.59KB	8.17MB	1
2.0.0.7	0	7.93MB	194.92KB	8.12MB	1



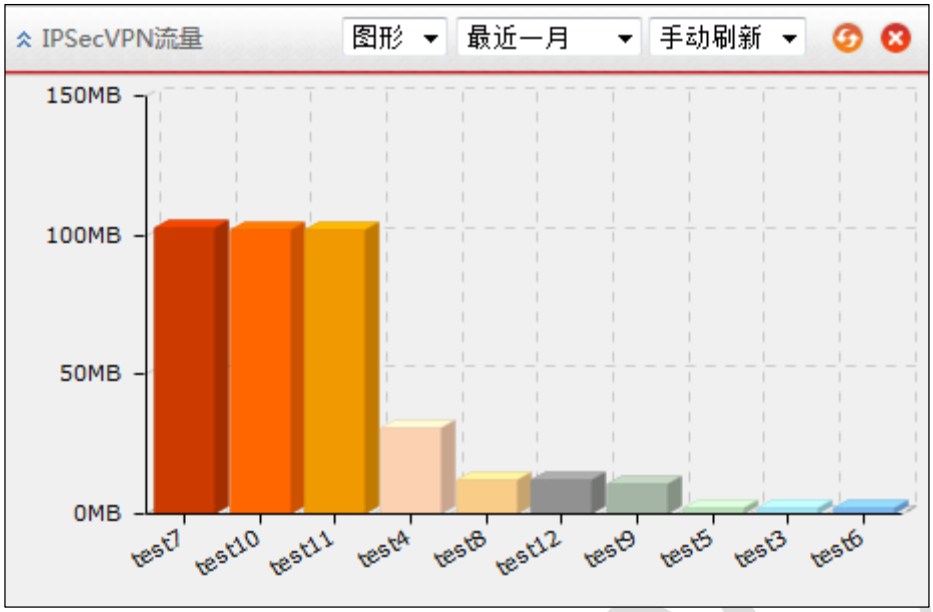
➢ IPSec VPN 流量

IPSec VPN 流量窗口实时显示不同用户的流量信息，包括隧道名、上行速率、下行速率、带宽百分比、上行流量、下行流量和流量百分比。支持表格和视图两种显示模式，如下图所示。表格模式以列表的形式显示 IPSec VPN 流量；视图模式以二维图形式显示 IPSec VPN 流量，横轴表示 VPN 隧道名，纵轴表示流量大小，将管理主机的鼠标移动至流量曲线图上可显示 IPSec VPN 流量的详细信息。

可根据需求点击下拉列表选择需要统计的 IPSec VPN 流量时间间隔，可选项为最近 5 分钟、最近 30 分钟、最近一小时、最近一天、最近一周、最近一月、前一天、前一周和前一月；选择窗口的刷新周期，可选项为 5 秒、10 秒、30 秒和手动更新。

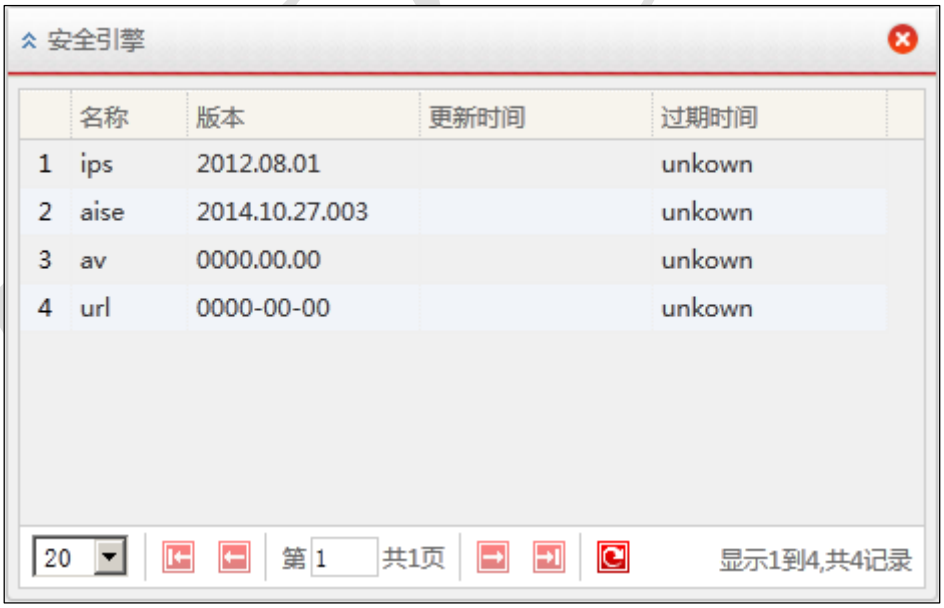


隧道名	上行速率	下行速率	带宽百分比	上行流量	下行流量	流量百分比
test7	220B	2.15KB	7.47%	384.91KB	102.24MB	27.03%
test10	220B	2.83KB	9.64%	369.90KB	101.46MB	26.82%
test11	220B	2.15KB	7.47%	162.50KB	101.62MB	26.8%
test4	220B	2.83KB	9.64%	26.66KB	31.17MB	8.22%
test8	220B	2.83KB	9.64%	353.13KB	12.18MB	3.3%
test12	380B	2.05KB	7.66%	161.91KB	11.80MB	3.15%
test9	220B	2.15KB	7.47%	116.99KB	10.32MB	2.75%
test5	220B	2.15KB	7.47%	39.49KB	2.19MB	0.59%
test3	220B	2.15KB	7.47%	22.27KB	2.18MB	0.58%
test6	220B	2.83KB	9.64%	31.25KB	1.86MB	0.5%



➢ 安全引擎

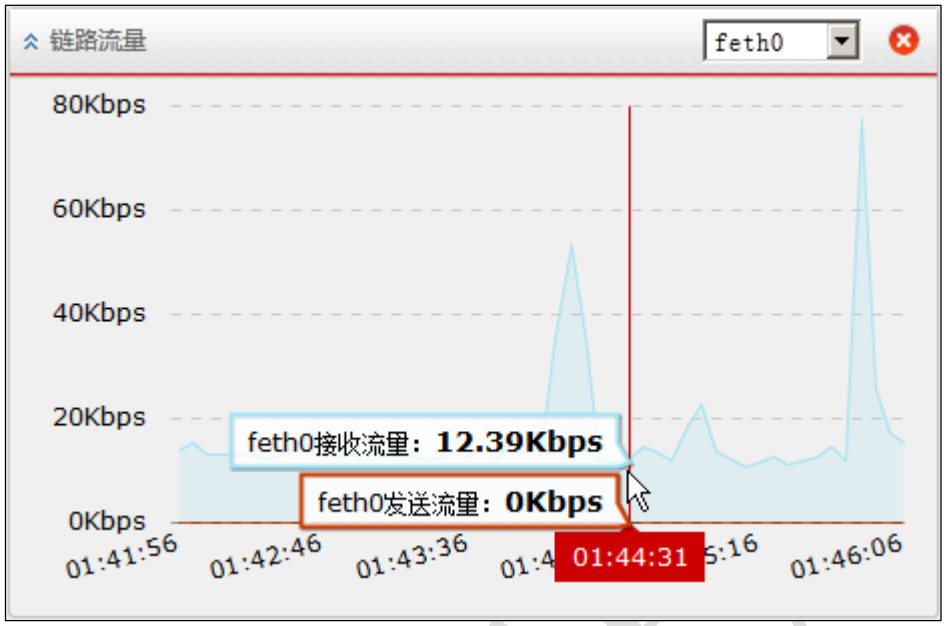
安全引擎窗口显示安全防御规则库的版本、更新时间和过期时间信息，如下图所示。ips 为入侵防御规则库；aise 为应用识别规则库；av 为病毒防御规则库；url 为 URL 过滤规则库。



➢ 链路流量

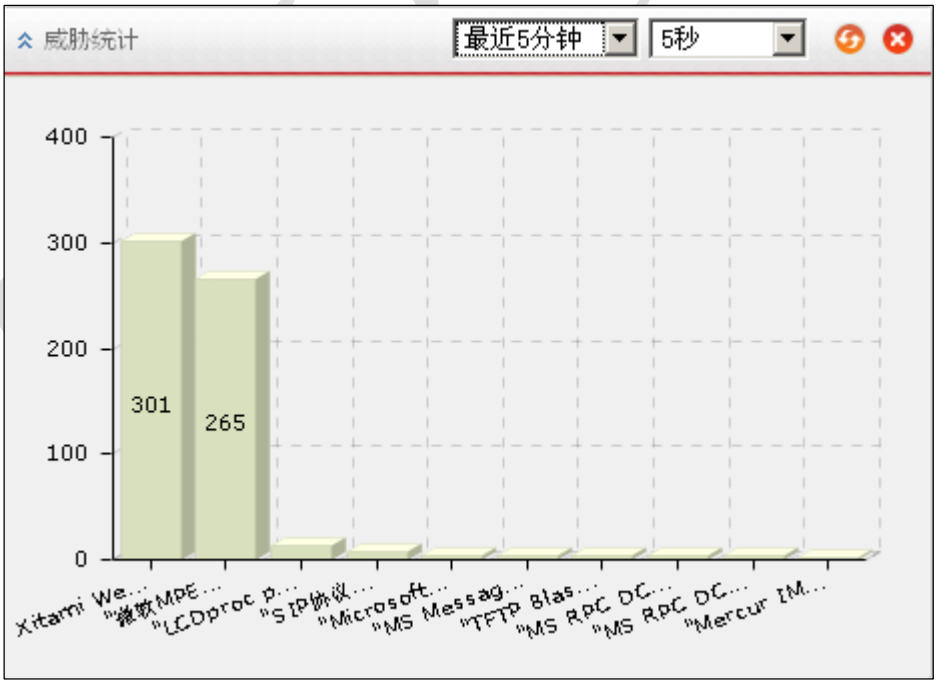
链路流量窗口以二维图的形式实时显示当天通过物理接口的流量，横轴表示时间，纵轴表示流量大小（单位 Kbps）。将管理主机鼠标移动至链路曲线图的任意时间点，将显示相应时间点物理接口上行和下行流量大小，如下图所示。

点击下拉列表，可以选择需要查看的接口流量。重新选择接口后，防火墙将重新统计接口的流量信息。



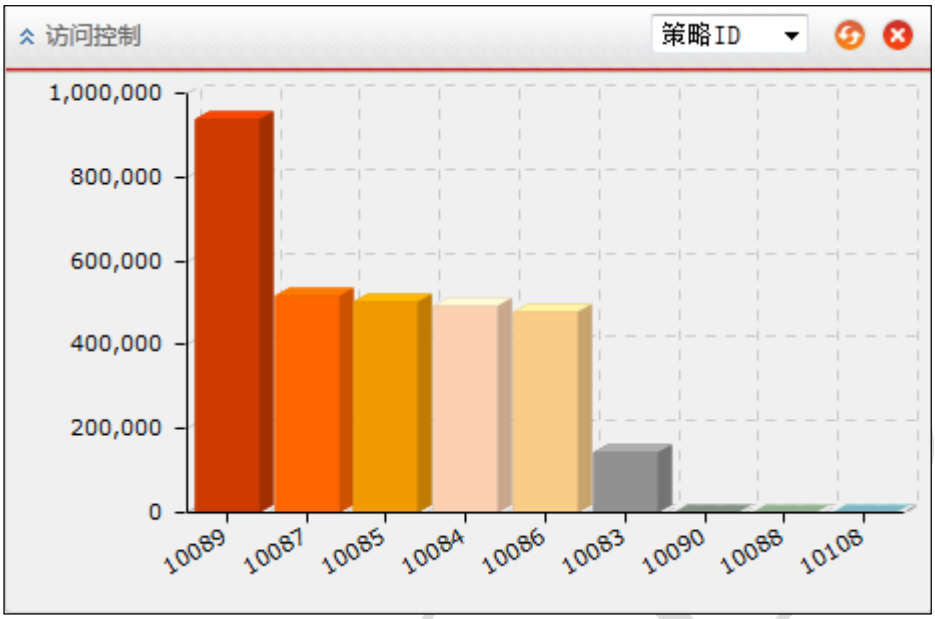
➢ 威胁统计

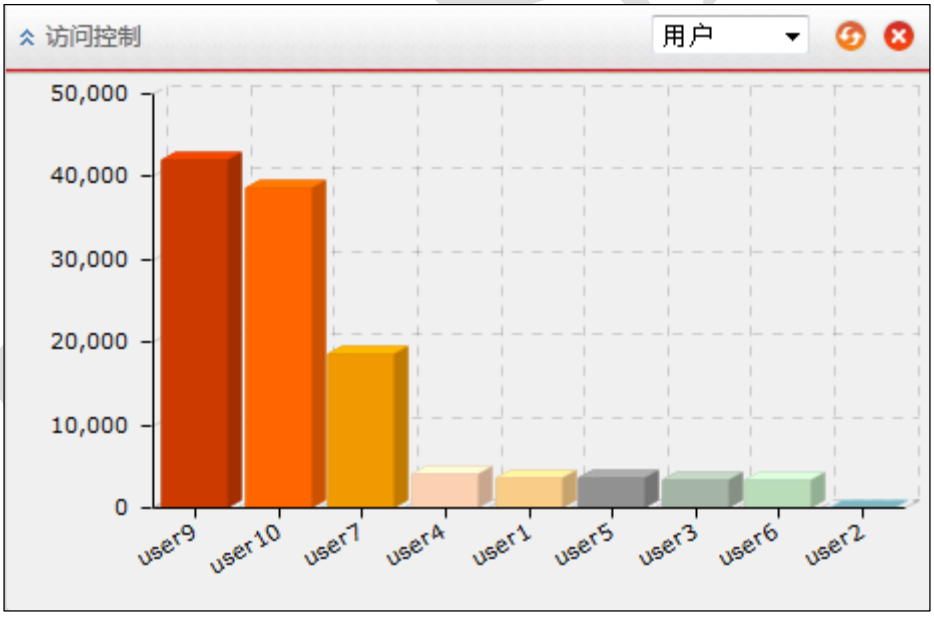
威胁统计窗口以图表的形式实时显示威胁的统计信息，如下图所示。

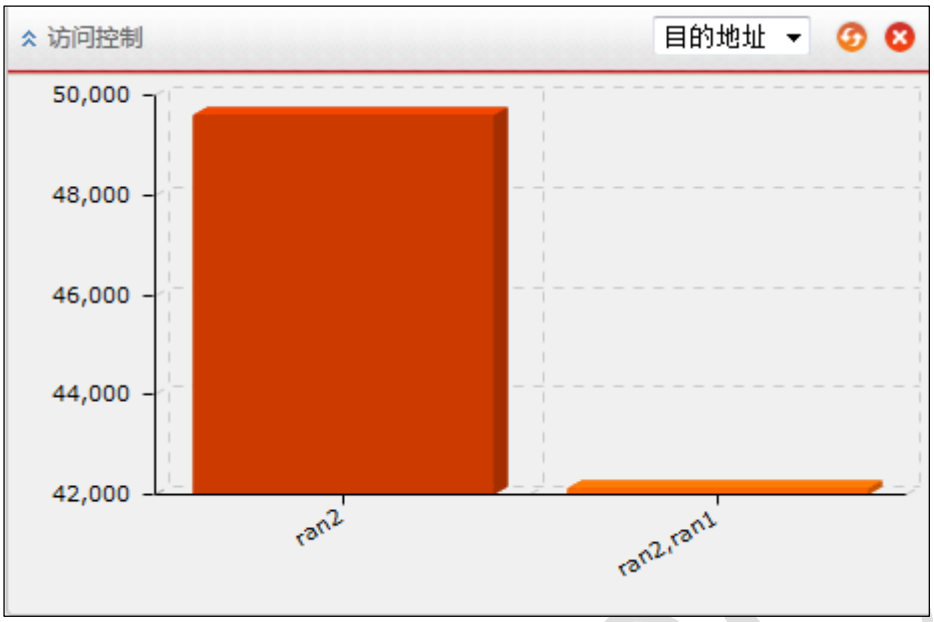


➢ 访问控制

访问控制窗口可显示被不同访问控制策略拒绝次数的统计信息。横轴表示需要显示的访问控制策略，可通过下拉列表更改，可选项策略 ID、用户和目的地址；纵轴表示被访问控制策略阻断连接的次数。





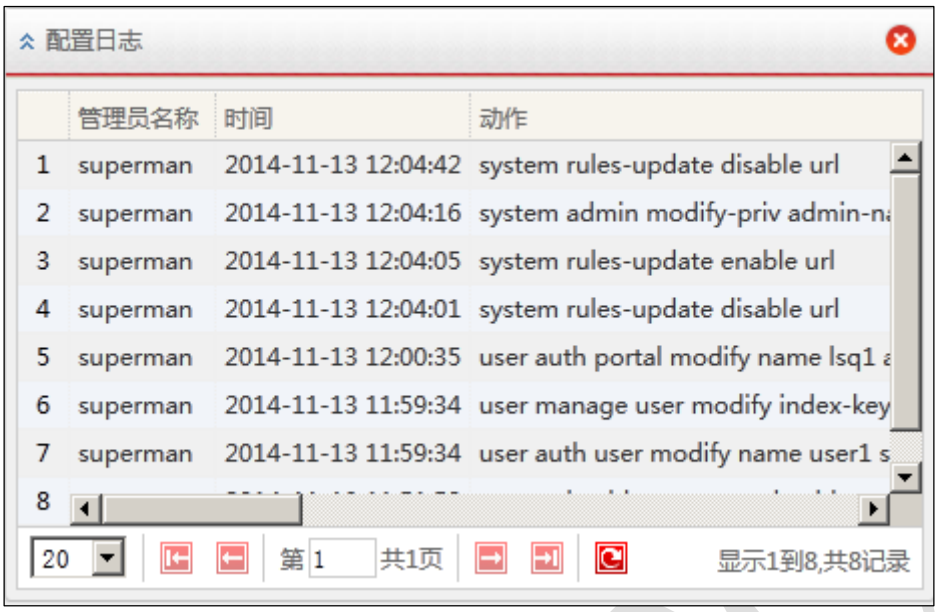


➢ 管理员登录日志

管理员登录日志窗口显示管理员登录设备的信息，包括管理员名称、时间、登录方式、登录 IP、动作。可以通过窗口下方的工具栏，可以修改每页可现实的日志数、翻页查看日志等。

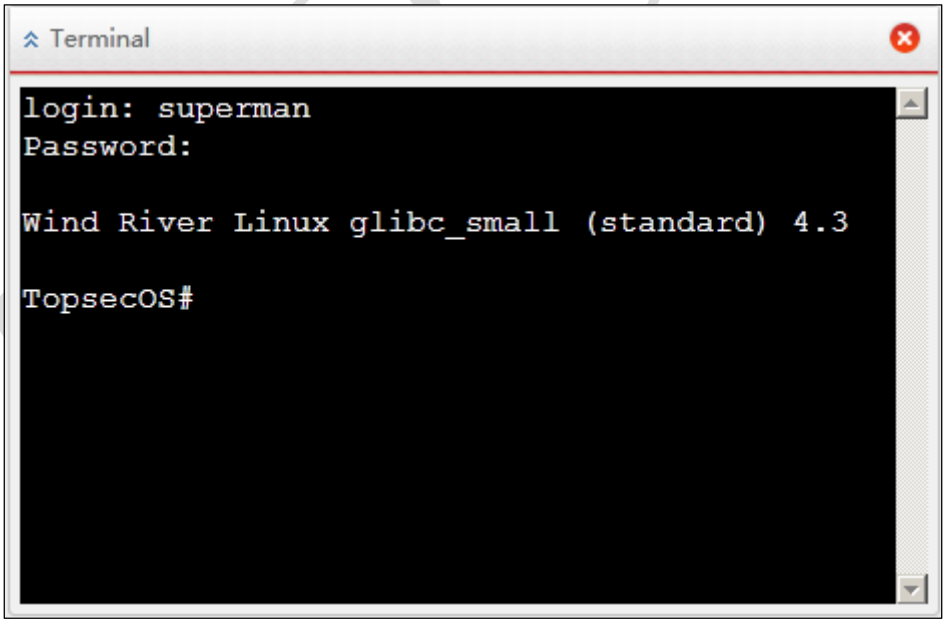
➢ 配置日志

配置日志窗口可以显示管理员对设备进行的操作历史信息记录。可以通过窗口下方的工具栏，可以修改每页可显示的日志数、翻页查看日志等。



➢ 控制台

控制台窗口显示 NGFW 的 CLI 界面，管理员可通过控制台窗口使用命令行管理 NGFW。点击【Connect】按钮即可进入 CLI 的管理界面，输入管理员用户名与密码后，即可登录 NGFW 设备，如下图所示。



8.2 监控

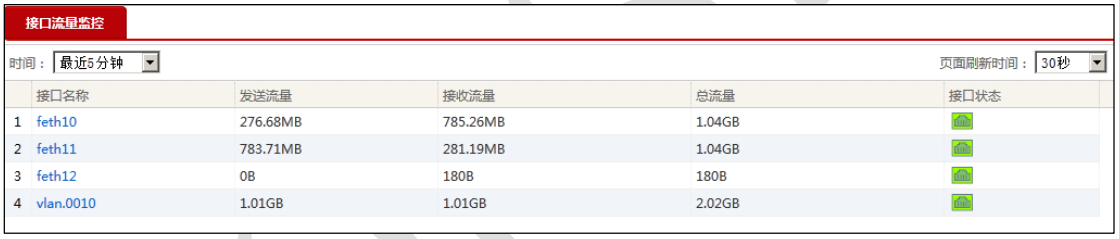
管理员通过监控面板可以快速地查看设备的流量统计信息和了解设备当前的运行情况。可以根据接口、应用、用户、用户组、服务器、IPSec VPN 查看设备的流量统计信息，查看设备受到的威胁信息，查看设备的 IPv4 和 IPv6 连接信息，查看在线的用户信息。

8.2.1 接口流量

NGFW 支持根据物理接口对通过设备的数据报文流量进行统计。接口流量界面显示 NGFW 接口流量信息，并可查看接口的状态。

WEBUI 方式配置

步骤 1 选择 **监控** > **接口流量**。



页面中显示了各个接口接收、发送以及发送和接口总流量的统计情况。

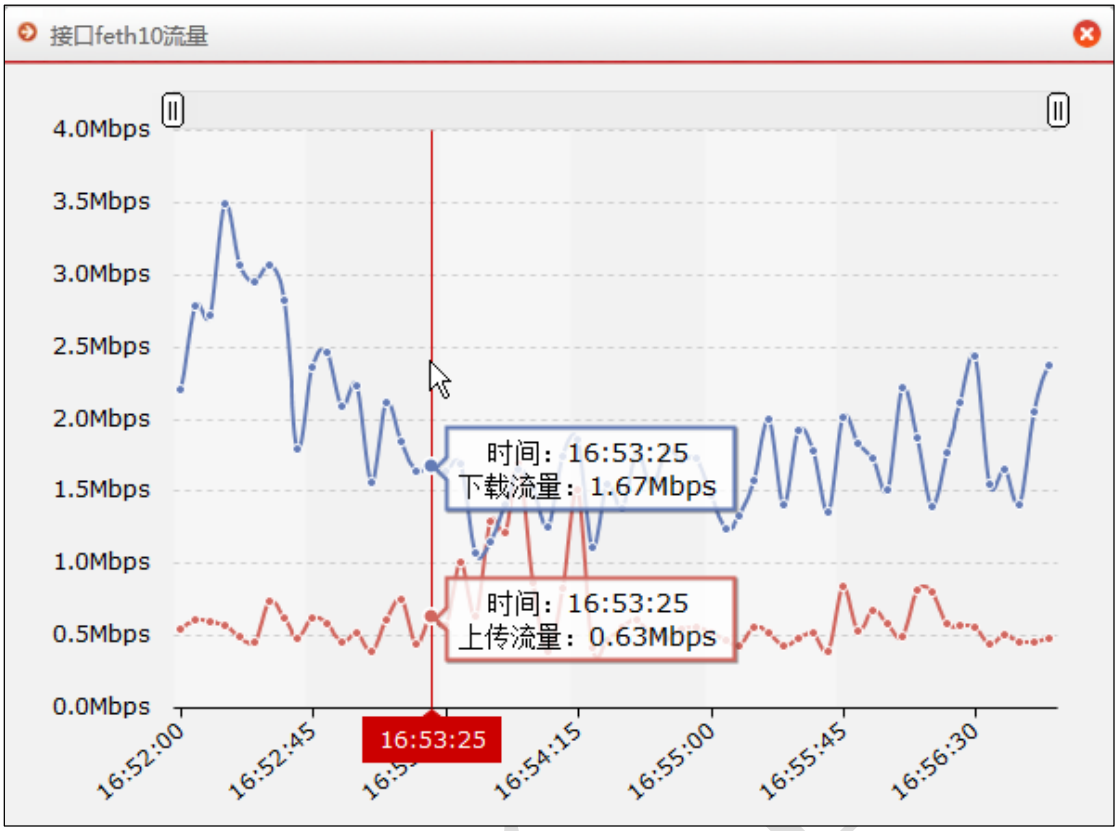
步骤 2 设置统计周期。

管理员可根据需求设置流量的统计周期。通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。

步骤 3 设置页面刷新周期。

管理员可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 点击物理接口名称，弹出接口流量统计对话框，显示该接口的详细流量信息，如下图所示。



对话框以二维图形式显示接口的统计信息，横轴表示统计的时间，纵轴表示接口的流量。将管理主机的鼠标移动至流量曲线图上可显示接口流量的详细信息。

拖动对话框上方的两个滑块“ ”，可调整窗口的时间轴，放大查看流量信息，此时可通过点击对话框中出现的『show all』恢复到查看所有时间的接口流量统计信息。

8.2.2 应用流量

NGFW 支持根据应用对通过设备的数据报文流量进行统计。WEBUI 中显示前 100 个流量最多的应用统计信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **应用流量**。

应用流量监控TOP100

应用类型：请选择　时间：最近5分钟　应用　　页面刷新时间：30秒

	应用名称	上行流量	下行流量	总流量	活动会话数	流量构成(Top5用户)
1	HTTP	51.93MB	369.53MB	421.47MB	8	un_67,un_123,未认证,un_30,un_70
2	HTTP下载	594.20KB	67.64MB	68.22MB	7	un_123,un_30,un_79,un_16,un_67
3	京东商城	5.91MB	47.11MB	53.02MB	23	un_2,un_67,un_123,un_125,un_79
4	HTTPS	29.91MB	22.38MB	52.29MB	4	un_3,未认证,un_15,un_123,un_59
5	QQ文件传输	31.71MB	18.96MB	50.67MB	1	un_60,un_7,un_79,un_14,un_16
6	Windows更新	430.02KB	35.69MB	36.11MB	1	un_123,un_13,un_16,un_15,un_70
7	淘宝网	3.08MB	31.15MB	34.23MB	28	un_123,un_62,un_5,un_8,un_67
8	POP3	5.30MB	20.89MB	26.19MB	1	未认证,un_123,un_7,un_60,un_62
9	360软件管家	10.76MB	14.44MB	25.21MB	4	un_123,un_62,un_70,un_67,un_15
10	百度音乐	81.90KB	17.75MB	17.83MB	1	un_58,un_72,un_8,un_15,un_16
11	360云盘客户端	16.51MB	470.88KB	16.97MB	13	un_60
12	SMTP	16.36MB	67.36KB	16.42MB	2	未认证,un_66,un_123
13	163邮箱	387.76KB	14.61MB	14.99MB	0	un_125,un_123,un_70,un_59,un_79
14	QQ	3.60MB	8.59MB	12.19MB	1	un_123,un_70,un_79,un_30,un_62
15	Others	2.99MB	3.46MB	6.45MB	1	un_7,un_13,未认证,un_96,un_19
16	WebEx	1.99MB	2.74MB	4.73MB	4	un_123,un_13
17	未知	2.63MB	1.16MB	3.79MB	0	un_62,un_123,un_79,un_67,un_30
18	QQ远程协助	2.49MB	1.14MB	3.64MB	1	un_8,un_7
19	DNS	708.01KB	2.18MB	2.88MB	0	un_123,un_67,un_79,un_30,un_70
20	HTTP代理	117.59KB	1.89MB	2.00MB	12	un_123,un_67,un_72

页面中显示了各个应用的协议名称、上行流量、下行流量、活动会话数以及流量构成（根据流量大小显示流量前 5 名的用户信息）。

步骤 2 设置显示的应用类型和流量统计周期。

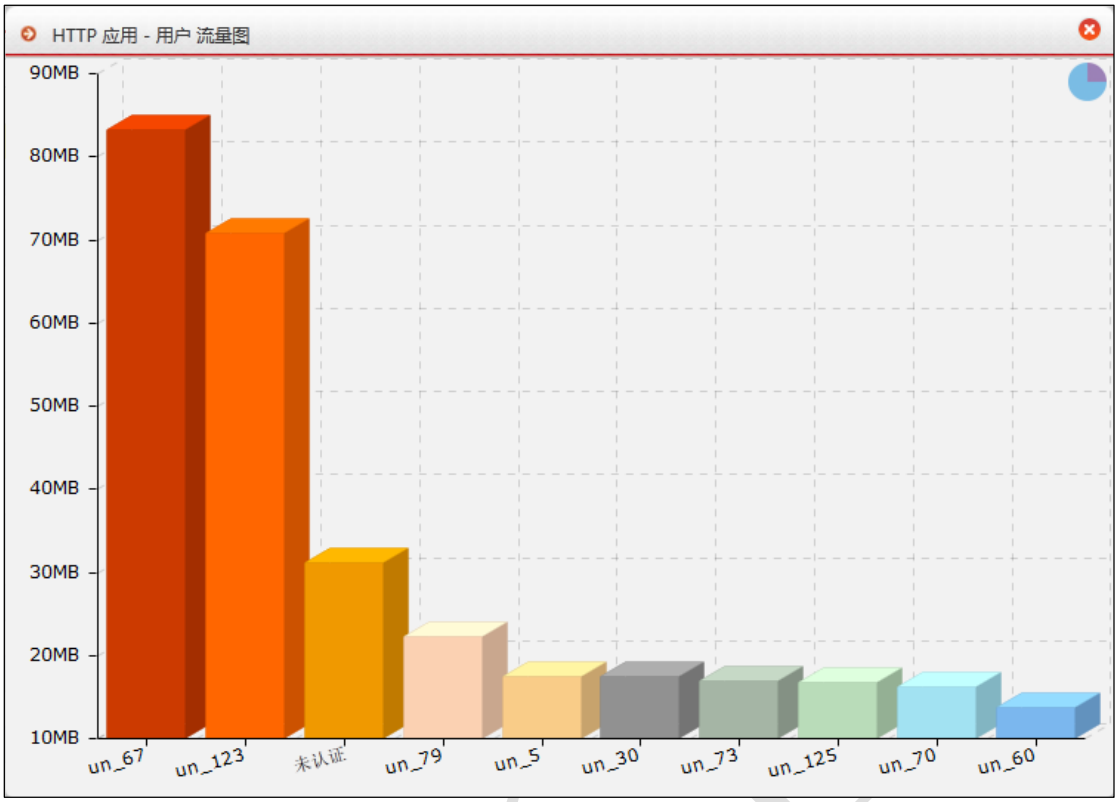
通过页面左上角的应用类型下拉列表选择需要显示的应用统计类型；通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。设置完统计类型和统计周期后，点击【应用】按钮完成配置。

步骤 3 设置页面刷新周期。

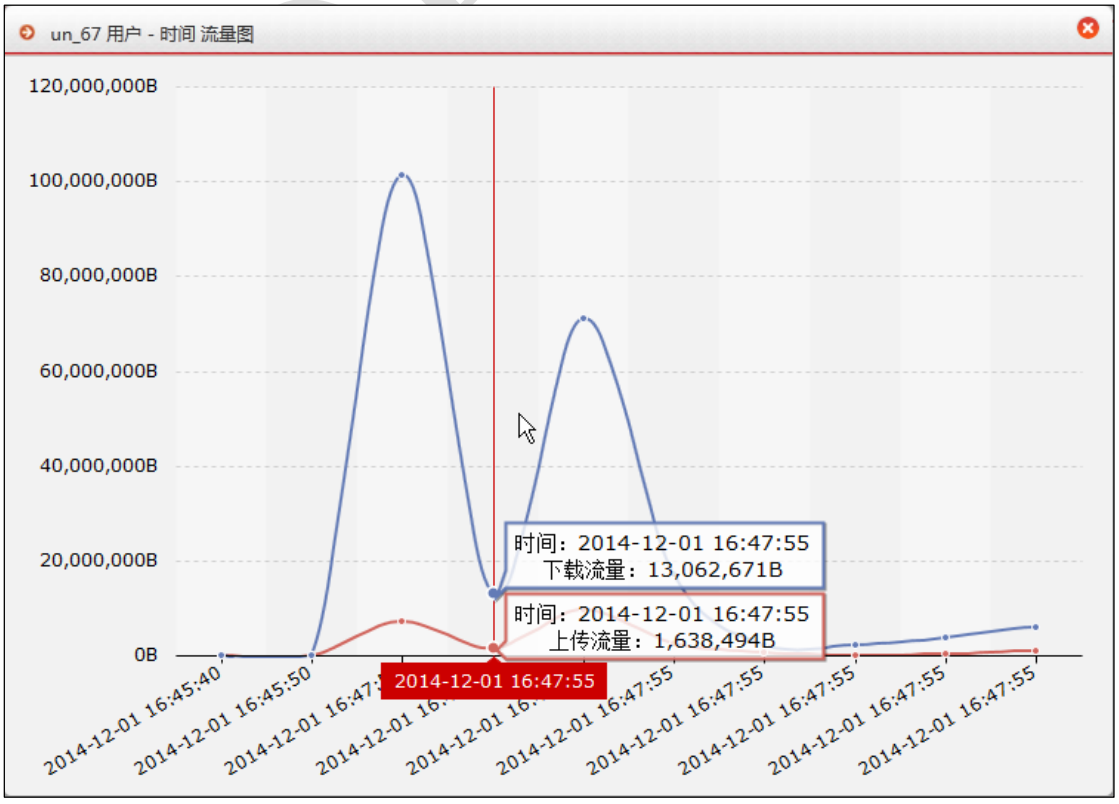
管理员可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 查看应用的流量构成信息。

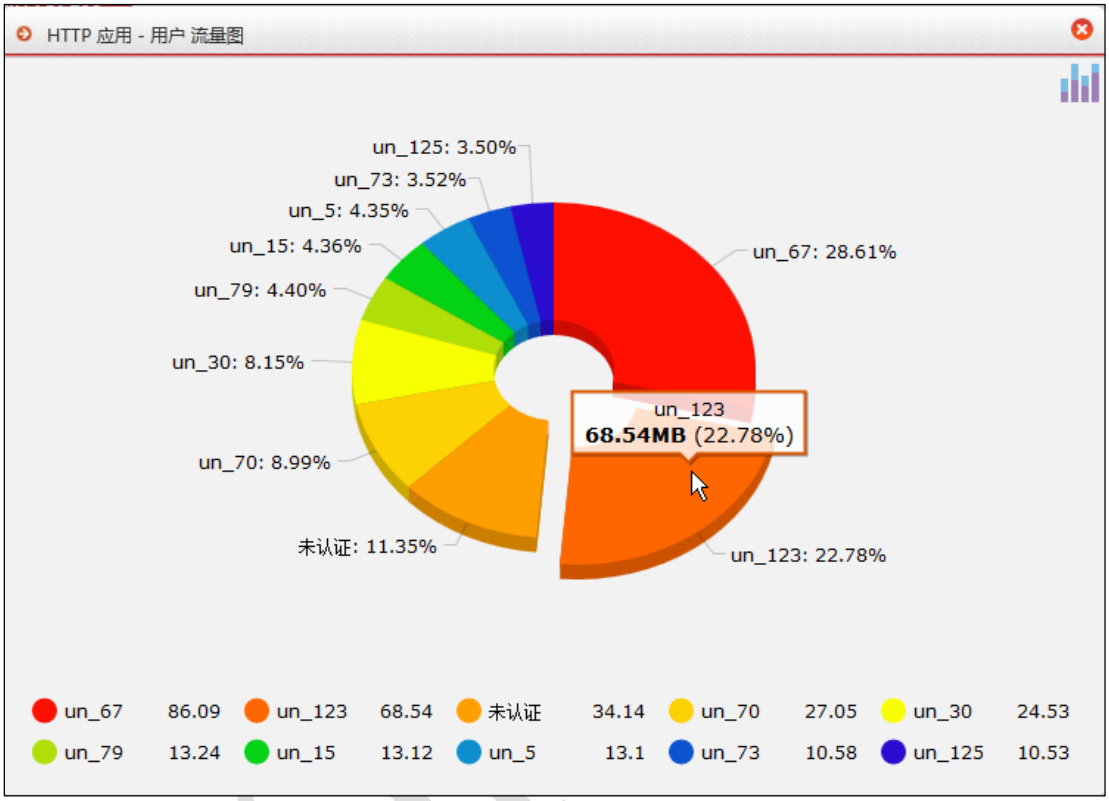
点击应用名称，弹出应用流量统计对话框，显示该应用的详细流量信息的柱状图，如下图所示。



点击柱状图的统计项，可弹出该用户的流量历史统计信息，此时将鼠标移动至曲线图区域，将显示具体的上传流量及下载流量信息，如下图所示。



点击右上角的“  ”图标，可切换为饼状图显示流量统计信息。此时右上角的图标变为“  ”，点击该图标可切换回柱状图显示流量统计信息。将管理主机的鼠标移动至饼状图上可显示接口流量的详细信息，如下图所示。

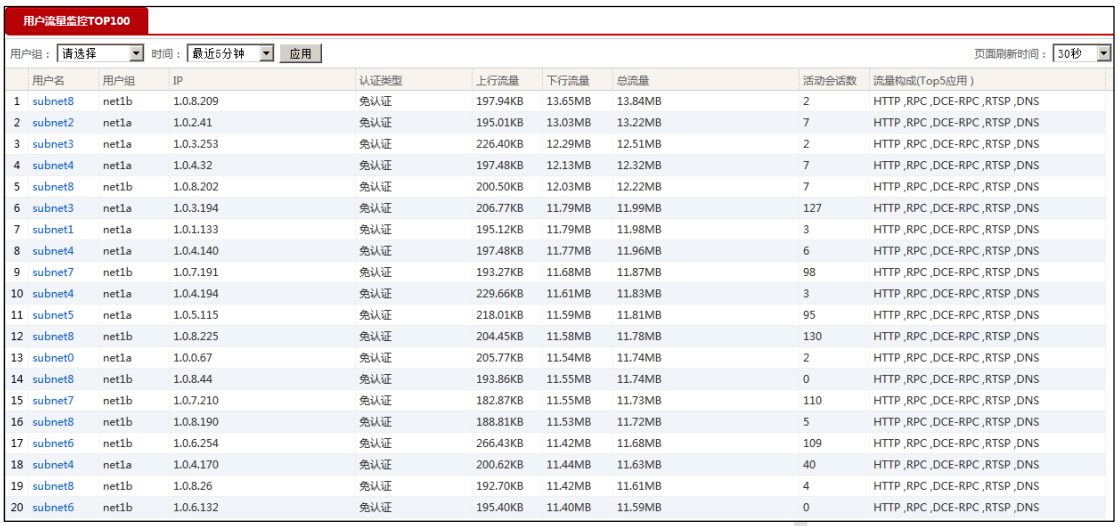


8.2.3 用户流量

NGFW 支持根据用户对通过设备的数据报文流量进行统计。WEBUI 中显示前 100 个流量最多的用户统计信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **用户流量**。


用户流量监控TOP100

用户组：请选择 时间：最近5分钟 应用 页面刷新时间：30秒

	用户名	用户组	IP	认证类型	上行流量	下行流量	总流量	活动会话数	流量构成(Top5应用)
1	subnet8	net1b	1.0.8.209	免认证	197.94KB	13.65MB	13.84MB	2	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
2	subnet2	net1a	1.0.2.41	免认证	195.01KB	13.03MB	13.22MB	7	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
3	subnet3	net1a	1.0.3.253	免认证	226.40KB	12.29MB	12.51MB	2	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
4	subnet4	net1a	1.0.4.32	免认证	197.48KB	12.13MB	12.32MB	7	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
5	subnet8	net1b	1.0.8.202	免认证	200.50KB	12.03MB	12.22MB	7	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
6	subnet3	net1a	1.0.3.194	免认证	206.77KB	11.79MB	11.99MB	127	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
7	subnet1	net1a	1.0.1.133	免认证	195.12KB	11.79MB	11.98MB	3	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
8	subnet4	net1a	1.0.4.140	免认证	197.48KB	11.77MB	11.96MB	6	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
9	subnet7	net1b	1.0.7.191	免认证	193.27KB	11.68MB	11.87MB	98	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
10	subnet4	net1a	1.0.4.194	免认证	229.66KB	11.61MB	11.83MB	3	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
11	subnet5	net1a	1.0.5.115	免认证	218.01KB	11.59MB	11.81MB	95	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
12	subnet8	net1b	1.0.8.225	免认证	204.45KB	11.58MB	11.78MB	130	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
13	subnet0	net1a	1.0.0.67	免认证	205.77KB	11.54MB	11.74MB	2	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
14	subnet8	net1b	1.0.8.44	免认证	193.86KB	11.55MB	11.74MB	0	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
15	subnet7	net1b	1.0.7.210	免认证	182.87KB	11.55MB	11.73MB	110	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
16	subnet8	net1b	1.0.8.190	免认证	188.81KB	11.53MB	11.72MB	5	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
17	subnet6	net1b	1.0.6.254	免认证	266.43KB	11.42MB	11.68MB	109	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
18	subnet4	net1a	1.0.4.170	免认证	200.62KB	11.44MB	11.63MB	40	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
19	subnet8	net1b	1.0.8.26	免认证	192.70KB	11.42MB	11.61MB	4	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS
20	subnet6	net1b	1.0.6.132	免认证	195.40KB	11.40MB	11.59MB	0	HTTP ,RPC ,DCE-RPC ,RTSP ,DNS

页面中显示了各个用户的用户组、IP、认证类型、上行流量、下行流量、活动会话数以及流量构成（根据流量大小显示流量前 5 名的应用信息）。

步骤 2 设置显示的用户和流量统计周期。

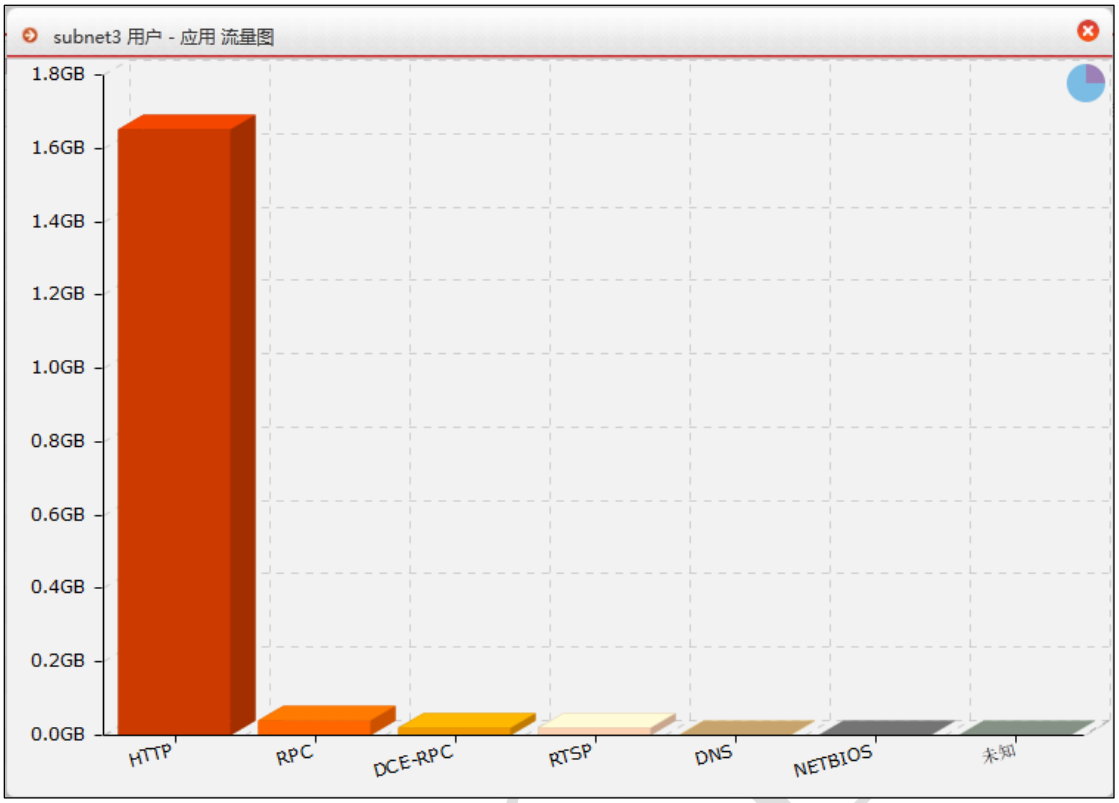
通过页面左上角的用户组下拉列表选择需要显示的用户；通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。设置完统计类型和统计周期后，点击【应用】按钮完成配置。

步骤 3 设置页面刷新周期。

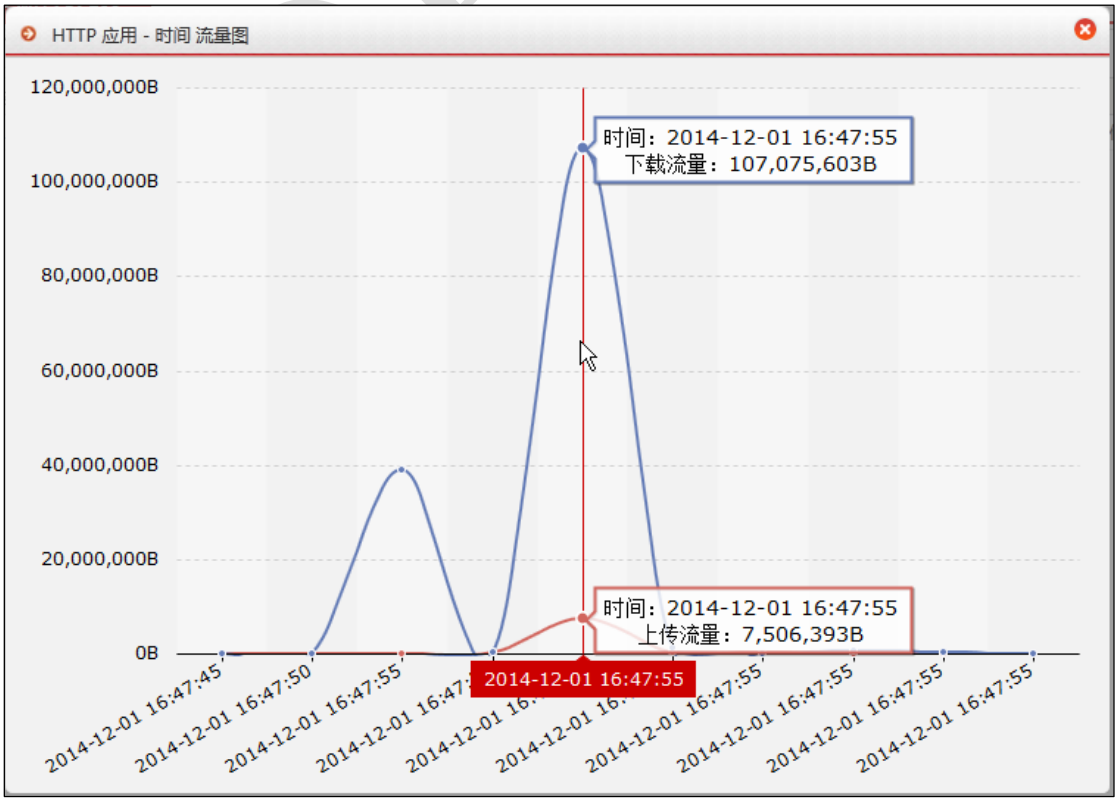
管理员可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 查看用户的流量构成信息。

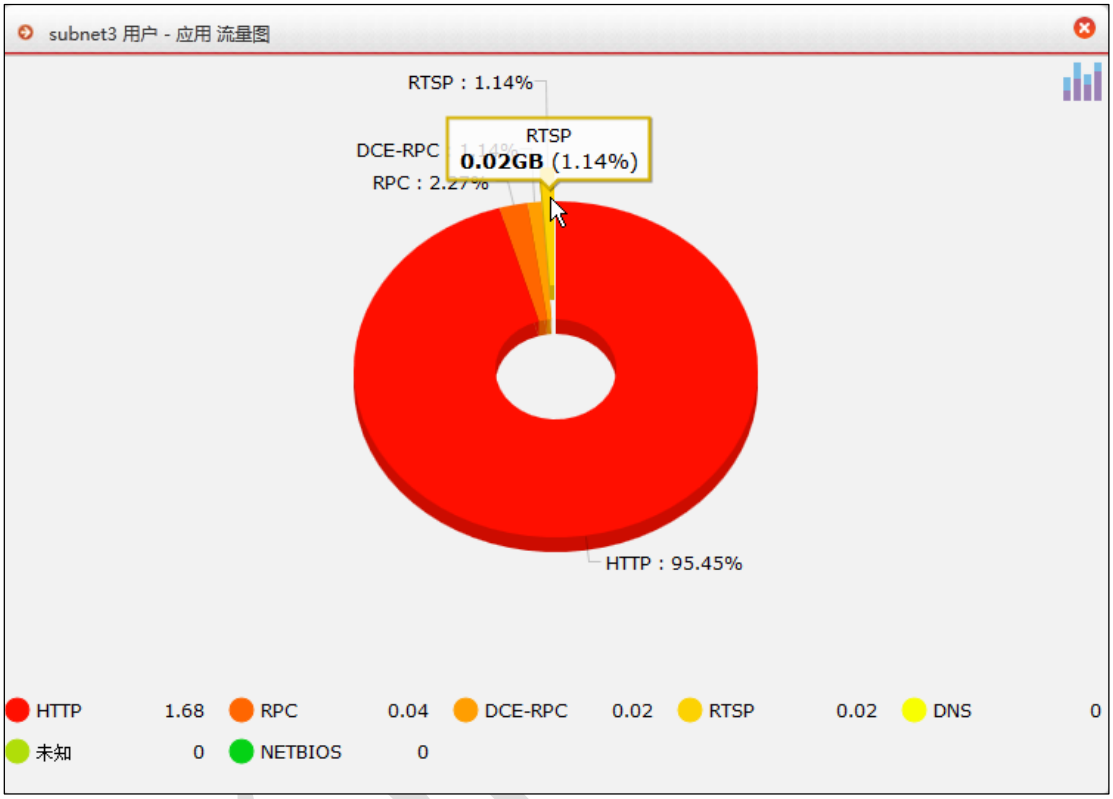
点击用户名称，弹出用户流量统计对话框，显示该用户的详细流量信息柱状图，如下图所示。



点击柱状图的统计项，可弹出该应用的流量历史统计信息，此时将鼠标移动至曲线图区域，将显示具体的上传流量及下载流量信息，如下图所示。



点击右上角的“  ”图标，可切换为饼状图显示流量统计信息。此时右上角的图标变为“  ”，点击该图标可切换回柱状图显示流量统计信息。将管理主机的鼠标移动至饼状图上可显示接口流量的详细信息，如下图所示。

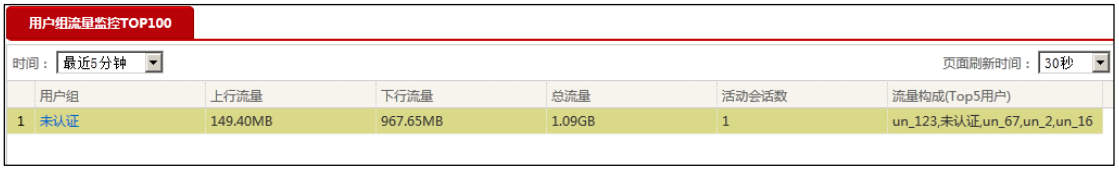


8.2.4 用户组流量

NGFW 支持根据用户组对通过设备的数据报文流量进行统计。WEBUI 中显示前 100 个流量最多的用户组统计信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **用户组流量**。



页面中显示了各个用户组的用户组织、上行流量、下行流量、活动会话数以及流量构成（根据流量大小显示流量前 5 名的用户的流量组成信息）。

步骤 2 设置流量的统计周期。

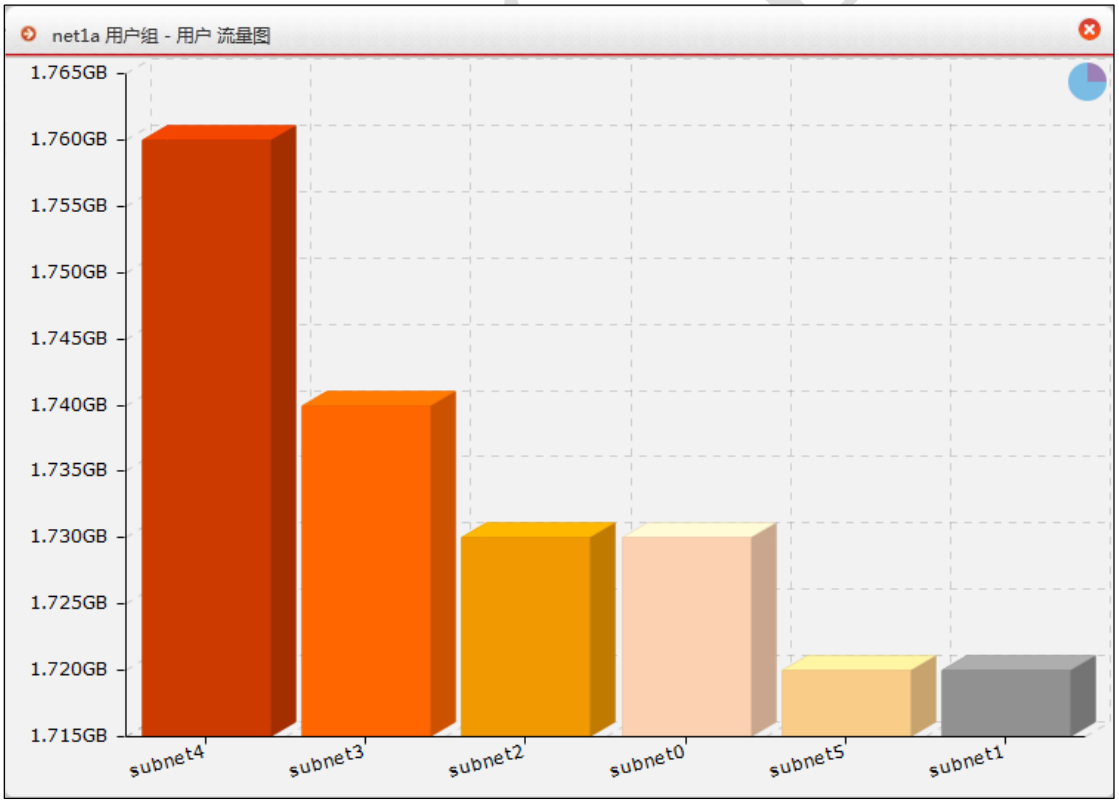
通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。

步骤 3 设置页面刷新周期。

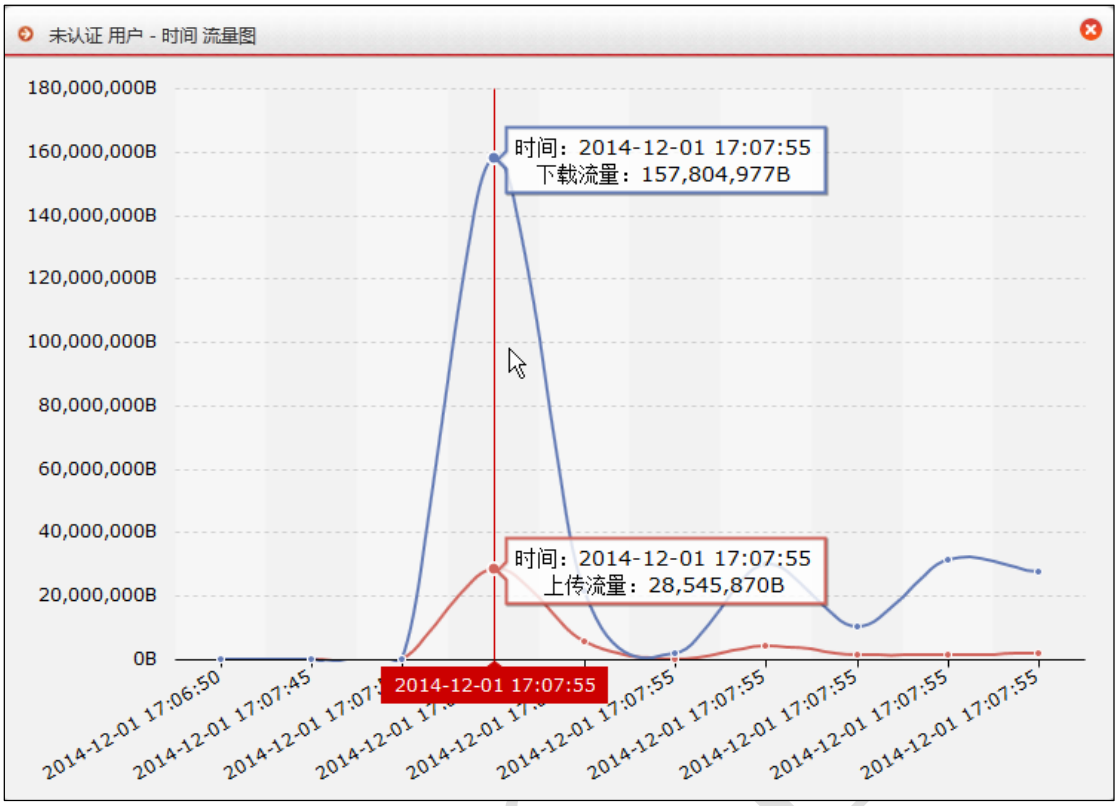
用户组可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 查看用户组的流量构成信息。

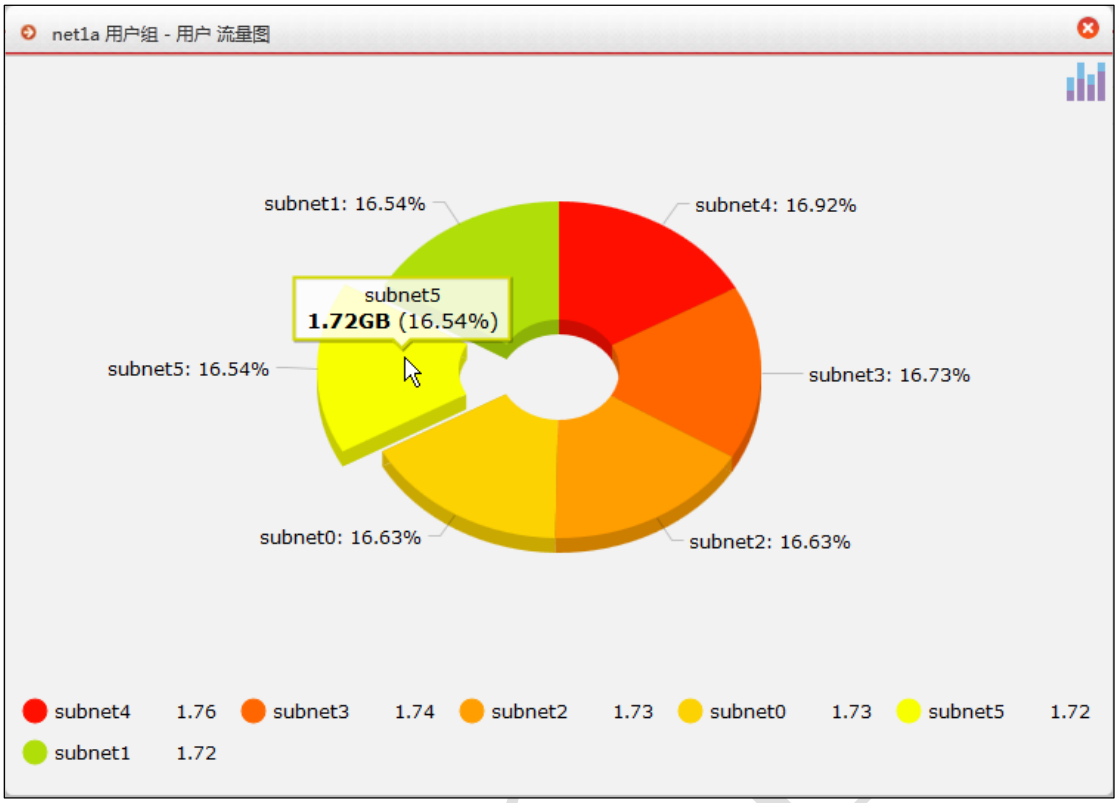
点击用户组名称，弹出用户组流量统计对话框，显示该用户组的详细流量信息柱状图，如下图所示。



点击柱状图的统计项，可弹出该用户的流量历史统计信息，此时将鼠标移动至曲线图区域，将显示具体的上传流量及下载流量信息，如下图所示。



点击右上角的“”图标，可切换为饼状图显示流量统计信息。此时右上角的图标变为“”，点击该图标可切换回柱状图显示流量统计信息，如下图所示。将管理主机的鼠标移动至饼状图上可显示接口流量的详细信息。

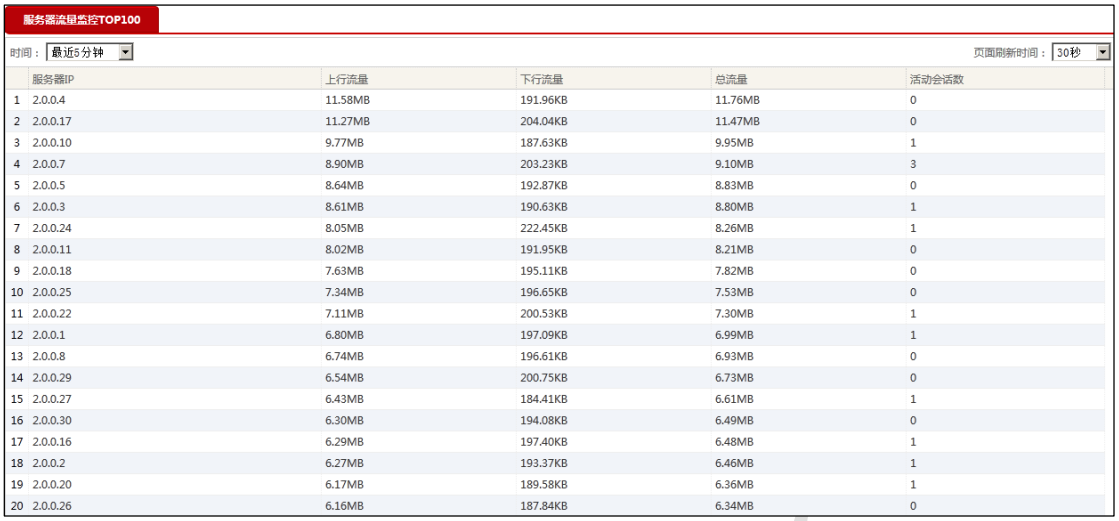


8.2.5 服务器流量

NGFW 支持根据服务器对通过设备的数据报文流量进行统计。WEBUI 中显示前 100 个流量最多的服务器统计信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **服务器流量**。


服务器流量监控TOP100

时间：最近5分钟　　页面刷新时间：30秒

	服务器IP	上行流量	下行流量	总流量	活动会话数
1	2.0.0.4	11.58MB	191.96KB	11.76MB	0
2	2.0.0.17	11.27MB	204.04KB	11.47MB	0
3	2.0.0.10	9.77MB	187.63KB	9.95MB	1
4	2.0.0.7	8.90MB	203.23KB	9.10MB	3
5	2.0.0.5	8.64MB	192.87KB	8.83MB	0
6	2.0.0.3	8.61MB	190.63KB	8.80MB	1
7	2.0.0.24	8.05MB	222.45KB	8.26MB	1
8	2.0.0.11	8.02MB	191.95KB	8.21MB	0
9	2.0.0.18	7.63MB	195.11KB	7.82MB	0
10	2.0.0.25	7.34MB	196.65KB	7.53MB	0
11	2.0.0.22	7.11MB	200.53KB	7.30MB	1
12	2.0.0.1	6.80MB	197.09KB	6.99MB	1
13	2.0.0.8	6.74MB	196.61KB	6.93MB	0
14	2.0.0.29	6.54MB	200.75KB	6.73MB	0
15	2.0.0.27	6.43MB	184.41KB	6.61MB	1
16	2.0.0.30	6.30MB	194.08KB	6.49MB	0
17	2.0.0.16	6.29MB	197.40KB	6.48MB	1
18	2.0.0.2	6.27MB	193.37KB	6.46MB	1
19	2.0.0.20	6.17MB	189.58KB	6.36MB	1
20	2.0.0.26	6.16MB	187.84KB	6.34MB	0

页面中显示了各个服务器的服务器 IP、上行流量、下行流量以及活动会话数。

步骤 2 设置流量的统计周期。

通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。

步骤 3 设置页面刷新周期。

服务器可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

8.2.6 IPSec 流量

NGFW 支持根据 IPSec VPN 对通过设备的数据报文流量进行统计。WEBUI 中显示前 100 个流量最多的 IPSec VPN 统计信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **IPSec 流量**。


IPSecVPN流量监控TOP100

时间： 最近一月　　页面刷新时间： 30秒

	隧道名	上行速率	下行速率	带宽百分比	上行流量	下行流量	流量百分比
1	test1	200B	1.95KB	6.79%	12.70KB	168.18KB	0.05%
2	test10	220B	2.83KB	9.64%	369.90KB	101.46MB	26.82%
3	test11	220B	2.15KB	7.47%	162.50KB	101.62MB	26.8%
4	test12	380B	2.05KB	7.66%	161.91KB	11.80MB	3.15%
5	test13	0B	0B	0%	0B	0B	0%
6	test2	220B	2.83KB	9.64%	12.70KB	887.41KB	0.23%
7	test3	220B	2.15KB	7.47%	22.27KB	2.18MB	0.58%
8	test4	220B	2.83KB	9.64%	26.66KB	31.17MB	8.22%
9	test5	220B	2.15KB	7.47%	39.49KB	2.19MB	0.59%
10	test6	220B	2.83KB	9.64%	31.25KB	1.86MB	0.5%
11	test7	220B	2.15KB	7.47%	384.91KB	102.24MB	27.03%
12	test8	220B	2.83KB	9.64%	353.13KB	12.18MB	3.3%
13	test9	220B	2.15KB	7.47%	116.99KB	10.32MB	2.75%

页面中显示了各个 IPSec VPN 的隧道名、上行速率、下行速率、带宽百分比、上行流量、下行流量以及流量百分比。

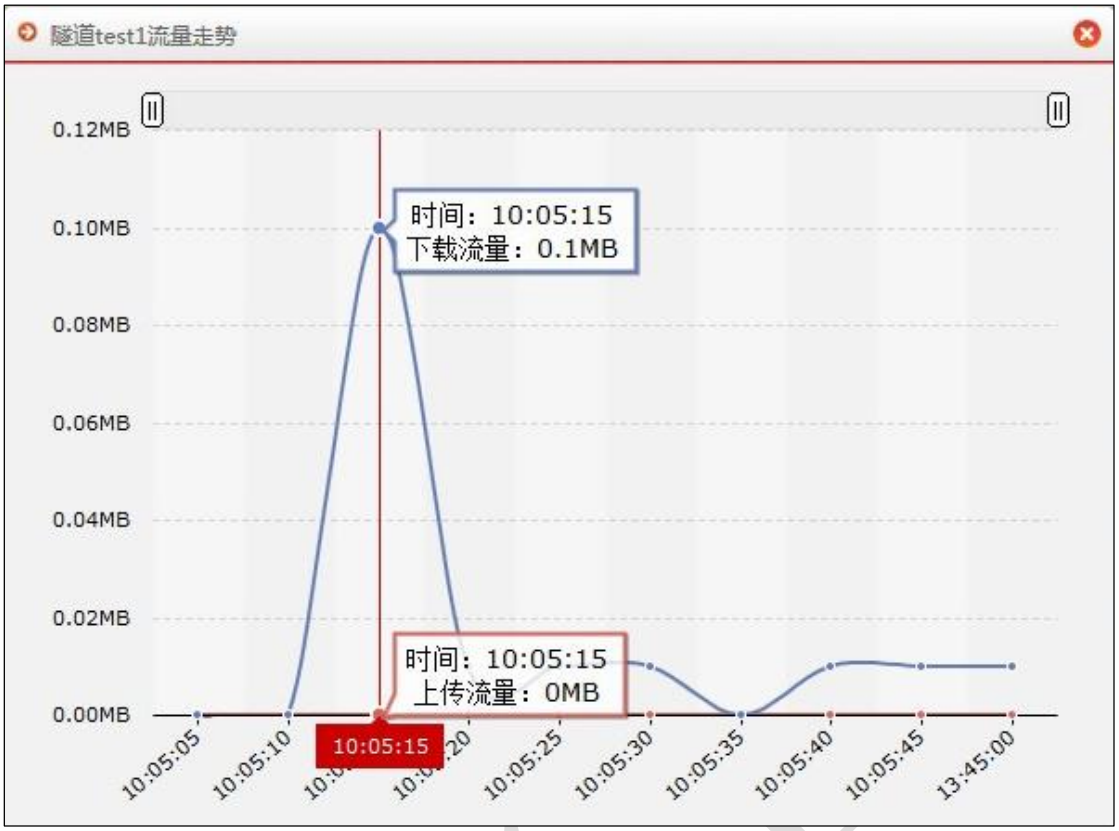
步骤 2 设置流量的统计周期。

通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。

步骤 3 设置页面刷新周期。

IPSec VPN 可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 点击 IPSec VPN 名称，弹出 IPSec VPN 流量统计对话框，显示该 IPSec VPN 的详细流量信息，如下图所示。

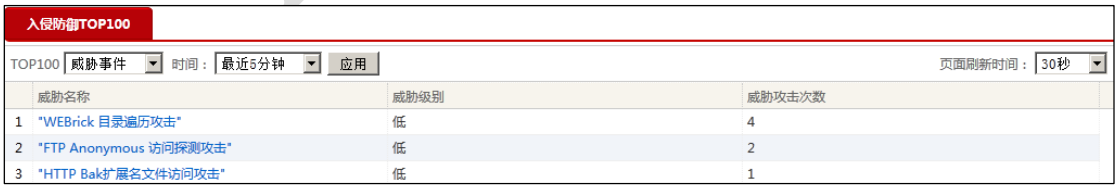


8.2.7 威胁统计

威胁统计包含 NGFW 受到的安全攻击的防御统计信息，包括病毒防御、入侵防御和文件防御。界面查看过程类似，以下仅以入侵防御为例说明。

WEBUI 方式配置

步骤 1 选择 **监控** > **威胁统计** > **入侵防御**。



页面中显示了 NGFW 受到的威胁名称，威胁级别和威胁攻击次数。

步骤 2 设置显示的攻击统计方法和流量统计周期。

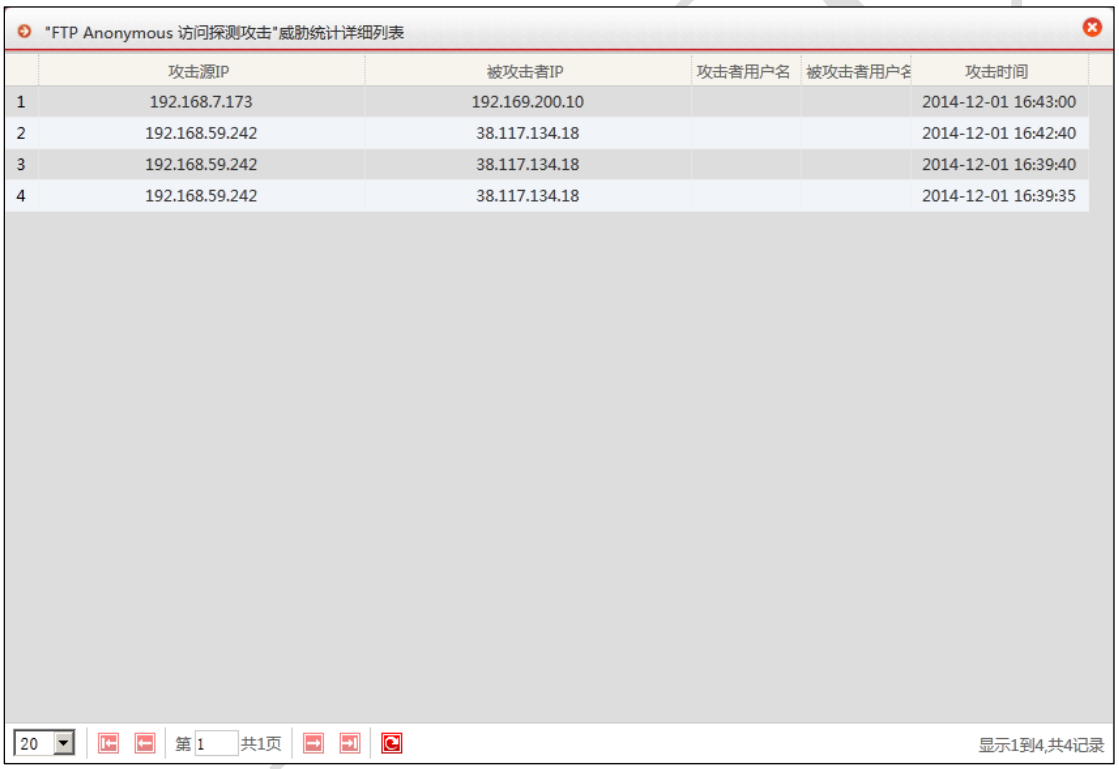
通过页面左上角的 TOP100 下拉列表选择需攻击统计方法，可选项有威胁事件、攻击来源和受攻击主机；通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。设置完统计类型和统计周期后，点击【应用】按钮完成配置。

步骤 3 设置页面刷新周期。

可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 查看威胁的详细信息。

双击威胁名称可弹出该威胁的详细信息，如下图所示。



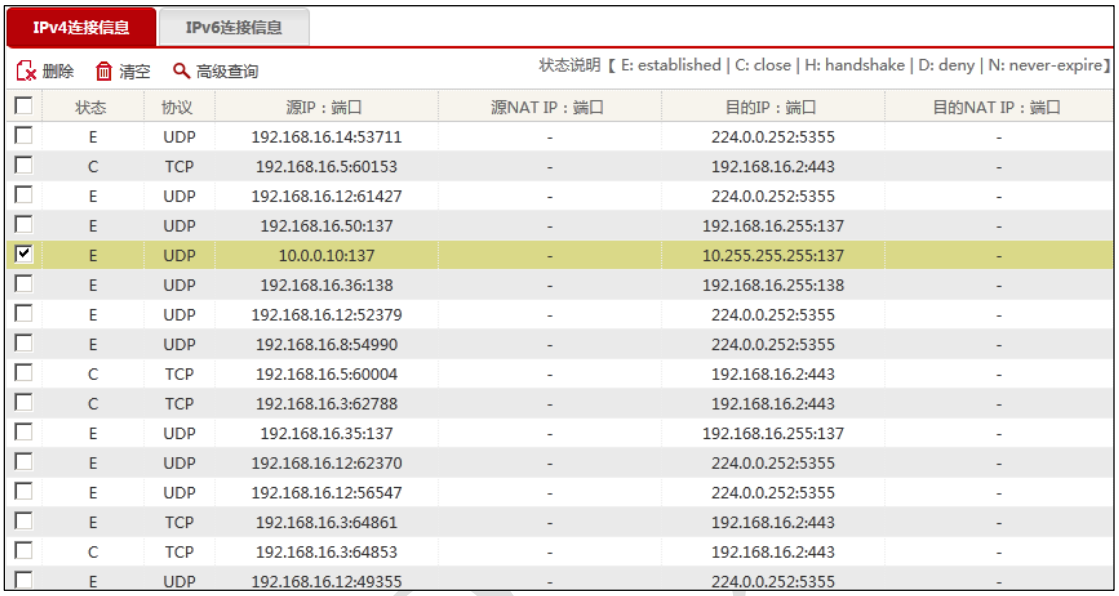
8.2.8 连接信息

NGFW 会记录与其建立连接的所有 IPv4/IPv6 连接的基本信息，包括状态、协议、源/目的 IP 地址和源/目的端口。管理员可通过查看 NGFW 的连接表了解 NGFW 目前的

工作状态。NGFW 将 IPv4 和 IPv6 连接信息分开显示，操作方式类似，下面以 IPv4 连接信息为例介绍。

WEBUI 方式配置

步骤 1 选择 **监控** > **连接信息**，激活“IPv4 连接信息”页签。

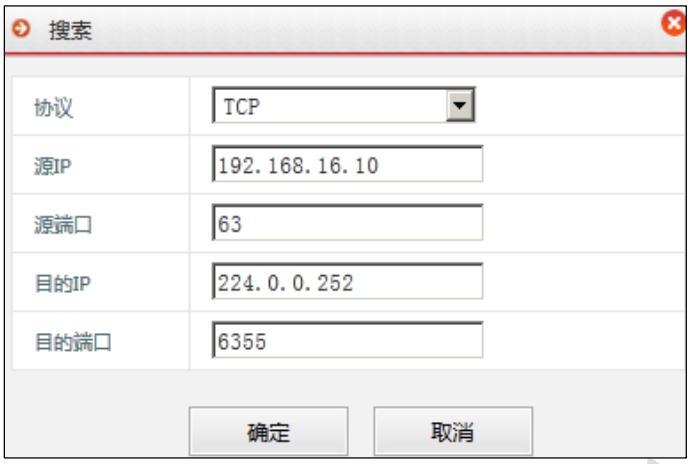


在查看 IPv4 连接信息时，每一条连接信息包括的内容说明如下表所示。

参数	说明
状态	显示连接的状态。
协议	显示连接所使用的通信协议。
源 IP：端口	显示连接的源 IP 地址及端口号。
目的 IP：端口	显示连接的目的 IP 地址及端口号。

步骤 2 按条件查找连接信息。

点击『高级查询』，在弹出的“搜索”对话框中设置查询参数，然后符合所有查询参数的连接信息将被筛选出来。



在查询 IPv4 连接信息时，搜索参数的说明如下表所示。

参数	说明
协议	设置需要查询的连接所使用的通信协议。
源 IP	设置需要查询的连接的源 IP 地址。
源端口	设置需要查询的连接的源端口号。
目的 IP	设置需要查询的连接的目的 IP 地址。
目的端口	设置需要查询的连接的目的端口号。

说明

- ✧ 当输入多个查询参数时，同时满足所有的查询条件的连接信息才会显示在列表中。
- ✧ 如果不设置某个查询参数表示该参数不做限制。

8.2.9 在线用户

在线用户界面显示了当前连接到 NGFW 的用户详细信息。

WEBUI 方式配置

步骤 1 选择 **监控** > **在线用户**。

页面中显示了各个用户的用户名称、IP 地址、服务器名称、客户端类型、在线时间信息。

步骤 2 设置统计周期。

管理员可根据需求设置流量的统计周期。通过页面左上角的时间下拉列表选择统计周期，可选的流量统计间隔为：最近 5 分钟、最近 30 分钟、最近 1 小时、最近 1 天、最近 1 周、最近 1 月、前一天、前一周、前一月和自定义。

步骤 3 设置页面刷新周期。

管理员可根据需求设置 WEB 界面中的刷新间隔。通过页面右上角的时间下拉列表选择页面刷新周期，页面的刷新时间可设置为 30 秒、1 分钟、5 分钟和 10 分钟。

步骤 4 强制在线用户退出登录。

管理员可点击用户对应的『强制下线』，强制该在线管理员退出登录状态。

8.2.10 相关命令

用户可通过命令行设置统计功能。

network session <**on**|**off**>

命令描述：

设置是否允许设备建立连接。

参数说明：

network session	设置是否允许设备建立连接。默认允许。
on|off	是|否

network session delete all <cr>

命令描述：

删除所有的连接信息。

network session delete [**protocol** <*string1*>] [**saddr** <*string2*>] [**sport** <*number1*>] [**daddr** <*string3*>] [**dport** <*number2*>] [**family** <ipv4|ipv6>] [**flags** <on|off>] [**from** <*numbe3*>] [**num** <*number4*>]

命令描述：

删除连接信息。

参数说明：

delete	删除连接信息。
protocol	必选项，指定协议类型。
string1	字符串类型。
saddr	必选项，指定源 IP 地址。
string2	字符串类型，表示 IP 地址。
sport	必选项，指定源端口。
number1	数值类型，表示端口号。
daddr	必选项，指定目的地址。
string3	字符串类型，表示 IP 地址。
dport	必选项，指定目的端口。
number2	数值类型，表示端口号。
family	必选项，协议。
ipv4|ipv6	IPv4 协议族|IPv6 协议族
flag	必选项，是否显示内部标志，默认不显示。
on|off	显示|不显示
from	必选项，是否显示内部标志，默认不显示。
number3	数值类型，起始显示数，默认从第一个连接开始显示。
num	必选项，需要显示的连接数。
number4	数值类型，取值范围：1-256，默认值：20。

network session ipv6 <on|off>

命令描述：

设置是否处理 IPv6 报文。

参数说明：

network session ipv6	设置是否处理 IPv6 报文。
on|off	是|否

network session search [**daddr** <*string1*>] [**dpo**rt <*number1*>] [**flags** <on|off>] [**from** <*number2*>] [**num** <*number3*>] [**proto** <ipv4|ipv6>] [**protocol** <*number4*|tcp|udp|icmp>] [**saddr** <*string2*>] [**sport** <*number5*>]

命令描述：

查看 IP 连接信息。

参数说明：

search	查看 IP 连接信息。
daddr	可选项，根据连接中的目的 IP 地址查看。
string1	字符串类型，表示 IP 地址。
dport	可选项，根据目的端口查看。
number1	数值类型，取值范围：1-65535。

flags	可选项，设置是否显示内部标志，默认不显示。
on|off	是|否
from	可选项，从第几个连接开始显示，默认从第一个连接开始显示。
number2	数值类型。
num	可选项，设置需要显示的连接数目。
number3	数值类型，最大值：8000；默认值：20。
proto	可选项，选择协议类型。
ipv4|ipv6	IPV4|IPV6，不做设置则默认为 IPV4。
protocol	可选项，设置协议类型。
number4	数值类型，取值范围：1-255。
tcp|udp|icmp	选择协议类型。
saddr	可选项，设置源 IP 地址。
string2	字符串类型，表示 IP 地址。
sport	可选项，设置源端口。
number5	数值类型，取值范围：1-65535。

network session show configuration <cr>

命令描述：

查看连接配置信息。

参数说明：

show	查看连接配置信息。
configuration	连接配置信息。

以下是查看连接配置信息的示例：

```
TopsecOS# network session show configuration
network session timeout deny 10
network session timeout close 20
network session timeout other 20
network session timeout handshake 100
network session timeout udp 60
network session timeout established 1800
network session timeout never-expire 86400
network session on
network session tcp-reset off
network session session-integrity on
network session only-syn-create on
```

```
network session packet-checksum on
network session syn-reset off
network session timer delete 128
network session timer jiffies 5
network session reclaim all
network session defrag on
network session ipv6 on
network session never-expire-percent 10
```

network session show all <cr>

命令描述：

查看所有连接信息。

以下是查看所有连接信息的示例：

```
TopsecOS# network session show all
match nums =              53    return count      53.

ts=0x5f001039e400    ts_id=899024 vsys_id=0 confirmed=1 normal=0 dead=0
deny=0
ts_flag=24000    se_flag=0 se_mask=4640 data_mask=440
expire_queue=4(SESSION_EXPIRE_DGRAM_BIDIR) is_vr2vr=0
stat=udp_established
qos_id[0]=0 qos_id[1]=0    pro_name=unknown duration= 23
cpu=    0 request: defvsys-VR0 ipv4_udp 192.168.16.5[58293] --> 224.0.0.252[5355]
pkts=2 bytes=44
cpu=255 reply    : defvsys-VR0 ipv4_udp 224.0.0.252[5355] -->
192.168.16.5[58293] pkts=0 bytes=0

ts=0x5f001039e900    ts_id=899029 vsys_id=0 confirmed=1 normal=0 dead=0
deny=0
```

```
ts_flag=24000    se_flag=0 se_mask=4640 data_mask=440
expire_queue=4(SESSION_EXPIRE_DGRAM_BIDIR) is_vr2vr=0
stat=udp_established
qos_id[0]=0 qos_id[1]=0    pro_name=unknown duration= 21
cpu=    0 request: defvsys-VR0 ipv4_udp 192.168.16.5[61359] --> 224.0.0.252[5355]
pkts=2 bytes=44
cpu=255 reply    : defvsys-VR0 ipv4_udp 224.0.0.252[5355] -->
192.168.16.5[61359] pkts=0 bytes=0
……
```

network session show information <cr>

命令描述：

查看连接的基本信息。

以下是查看连接的基本信息的示例：

```
TopsecOS# network session show information
session hash lines=1048576, total sessions=900000.
Created 24423, deleted 24390, freed 24390, currently 33, rate            1.00 .
================cpu session info=========================
cpu          created          deleted       freed
 0         0G 0M 23K 871          0G 0M 23K 822          0G 0M 23K 822
 1         0G 0M 0K 0             0G 0M 0K 16            0G 0M 0K 16
========================vsys 0 session info====================
vsys_id cpu_id     quota_set       currents          frees     cur_quota
        0         0         900000         33       335         899616
        0         1         900000          0        16         899616
      sum        --         900000         33       351         899616
```

network session stat show <cr>

命令描述：

查看连接的统计信息。

以下是查看连接的统计信息的示例：

```
TopsecOS# network session stat show
================session HA stat info ======================
cpu_id   create   create_send    delete    delete_send    rebuild    rebuild_send
0            0            0            0            0            0            0
1            0            0            0            0            0            0
================session stat info ======================
nr_created     = 24495
nr_set_expires     = 24495
nr_deleted     = 24470
nr_freed     = 24470
----------create ---------------------------------
nr_has_linked     = 0
----------delete---------------------------------------
nr_delete_tos_syn_reset     = 0
nr_delete_reclaim_session     = 0
nr_delete_do_expire_session     = 23828
nr_delete_by_handshake     = 0
nr_delete_by_command     = 16
nr_delete_by_outer     = 626
----------reclaim-----------------------------------
nr_vsys_force_reclaim_times          = 0
nr_vsys_force_reclaim_nums     = 0
----------ha sync info-------------------------------
----------ha pipe info-------------------------------
nr_ha_create_send    = 0
nr_ha_deleted_send = 0
```

```
nr_ha_rebuild_send = 0
nr_ha_send_error      = 0
nr_ha_send_no_mem_error       = 0
nr_ha_create_rcv      = 0
nr_ha_delete_rcv    = 0
nr_ha_rebuild_rcv    = 0
total_sessions= 900000 cur_left_sessions = 900000
```

network session timeout deny <*number*|default>

命令描述：

设置 deny 连接的超时时间。

参数说明：

network session timeout deny	设置 deny 连接的超时时间。
number	数值类型，单位：秒；取值范围：1-10，默认值：1，单位：秒。
default	设定为默认超时值。

以下为设置 deny 连接超时时间的示例：

设置长连接的超时时间为 3 秒。

```
TopsecOS#network timeout deny 3
```

network session timeout syn_proxy <[**quota** <*number1*> **burst** <*number2*>]| default>

命令描述：

SYN 代理参数设置。

参数说明：

timeout	连接设置。
syn_proxy	指定 SYN 代理超时参数。
quota	可选项，设定配额，即平均每秒 SYN 代理数目。
number1	数值类型，单位：个/秒；取值范围：1-20，默认值：2000。
burst	可选项，设定限额值，即最大每秒 SYN 代理数目。
number2	数值类型，单位：个/秒；取值范围：1-20；默认值：5000。
default	设定为默认值，即配额为 2000 个/秒，限额为 5000 个/秒。

以下是 SYN 代理参数设置的示例：

设定 SYN 代理参数值为默认值。

```
TopsecOS# network session    timeout syn_proxy default
```

设定 SYN 代理参数值配额 50。限额 70。

```
TopsecOS# network session    timeout syn_proxy quota 50 burst 70
```

network session timer delete <*number*>

命令描述：

设置连接 timer 删除个数。

参数说明：

network session timer delete	设置连接 timer 删除个数。
number	数值类型，取值范围：32-1024，默认值：128。

network session expire clear <cr>

命令描述：

清除连接超时队列信息。

network session expire show <cr>

命令描述：

显示连接超时队列信息。

以下是查看连接超时队列信息的示例：

```
TopsecOS# network session expire show
==============vsys session expire queue currents info==============
vsys_id      DENY     CLOSE   OTHER   HANDSHAKE       UDP     ESTAB
NEVER SYN_PROXY      HA
     0       0        0       0       0       11      4       0       0       0
   sum       0        0       0       0       11      4       0       0       0
```

**********cpu = 0 **********

-------vsys_id = 0----expire queue SESSION_EXPIRE_DENY----------

total_add = 5197

currents = 0

remove = 0

deleted = 5197

total_timers = 3028983

timer_del = 5197

total_reclaims = 0

reclaim_del = 0

-------vsys_id = 0----expire queue SESSION_EXPIRE_CLOSE----------

total_add = 2029

currents = 0

remove = 0

deleted = 2029

total_timers = 759053

timer_del = 2029

total_reclaims = 0

reclaim_del = 0

-------vsys_id = 0----expire queue SESSION_EXPIRE_OTHER----------

total_add = 3

currents = 0

remove = 0

deleted = 3

total_timers = 6760

timer_del = 3

total_reclaims = 0

reclaim_del = 0

-------vsys_id = 0----expire queue SESSION_EXPIRE_HANDSHAKE----------

total_add = 2070

currents = 0

remove = 2039

deleted = 31

total_timers = 90

timer_del = 31

total_reclaims = 0

reclaim_del = 0

-------vsys_id = 0----expire queue SESSION_EXPIRE_DGRAM_BIDIR----------

total_add = 22975

currents = 11

remove = 5197

deleted = 17767

total_timers = 6172224

timer_del = 17767

total_reclaims = 0

reclaim_del = 0

-------vsys_id = 0----expire queue SESSION_EXPIRE_ESTAB----------

total_add = 2039

currents = 4

remove = 2029

deleted = 6

total_timers = 1916549

timer_del = 6

total_reclaims = 0

reclaim_del = 0

**********cpu = 1 **********

==========total expire info ==========

total_add = 34313

currents = 15

```
remove = 9265
deleted = 25033
total_timers = 11883659
timer_del = 25033
total_reclaims = 0
reclaim_del = 0
```

stat switch reset <cr>

命令描述：

重置统计功能开关。该命令将清除统计信息，请谨慎操作。

stat switch server <on|off>

命令描述：

设置服务器的流量统计开关。

参数说明：

stat switch server	设置服务器的流量统计开关。
on|off	开启|关闭

以下是设置服务器的流量统计开关的示例：

```
TopsecOS# stat switch session on
```

stat switch session <on|off>

命令描述：

设置会话流量的统计开关。

参数说明：

stat switch session	设置会话流量的统计开关。
on|off	开启|关闭

以下是设置会话流量的统计开关的示例：

```
TopsecOS# stat switch session on
```

stat switch show <cr>

命令描述：

查看统计开关状态。

以下是查看统计开关状的示例：

```
TopsecOS# stat switch show
session flow statistics switch is off
user_app flow statistics switch is off
server flow statistics switch is off
qos channel flow statistics switch is off
vpn tunnel flow statistics switch is off
threat flow statistics switch is off
```

stat switch user_app <on|off>

命令描述：

设置用户及应用流量的统计开关。

参数说明：

stat switch user_app	设置用户及应用流量的统计开关。
on|off	开启|关闭

以下是设置用户及应用流量的统计开关示例：

```
TopsecOS# stat switch user_app on
```

stat switch threat <on|off>

命令描述：

设置威胁的统计开关。

参数说明：

stat switch threat	设置威胁的统计开关。
on|off	开启|关闭

以下是设置威胁的统统计开关示例：

```
TopsecOS# stat switch threat on
```

stat switch vpn_tunnel <on|off>

命令描述：

设置 VPN 隧道的统计开关。

参数说明：

stat switch vpn_tunnel	设置 VPN 隧道的统计开关。
on|off	开启|关闭

以下是设置 VPN 隧道的统计开关示例：

```
TopsecOS# stat switch vpn_tunnel on
```

9 FAQ

Q1：NGFW 双机切换时，为什么主备墙同时在日志中报 IP 冲突现象？

A：NGFW 在主备模式下工作墙与备份墙通过心跳接口将 VRRP 信息发送至对端，在默认配置下工作墙发送间隔为 1 秒，基于上述 VRRP 工作原理，当接口出现 DOWN 时 NGFW 将做出如下动作：

1）工作状态 NGFW 检测到本地接口状态 DOWN 时，会通过 VRRP 报文发送到备份状态 NGFW，备份状态 NGFW 收到该报文后同时也向对端发送一个 VRRP 报文信息告知工作墙自己的本地接口是否正常，如果备份墙接口全部正常则双机切换。

2）备份状态 NGFW 切换为工作状态后会向网络中发送 ARP 报文，广播自己的 VRRP 热备组的虚 IP 地址和 MAC 地址。与此同时原工作状态 NGFW 会将本地热备组内接口 IP 置为无效。

3）基于双机切换过程主备两台 NGFW 会存在一个极短的双主时间点，因为此时原工作状态 NGFW 热备组内接口 IP 还没有来得及设置为无效，新工作墙 VRID 组内的接口 IP 就已经生效，于是就出现短暂的 IP 地址冲突的现象。

解决方法：

通过 HA 切换原理的分析和模拟环境的测试，丢包数量很小，基本不会对业务造成影响。

Q2：NGFW 可以通过 DHCP 获取地址吗？

A：可以。但如果获取到网关时会在路由表内生成一条默认路由，该默认路由无法修改 metric 和权重值。

Q3：为什么修改了 SNMP 配置不生效？

A：如果 SNMP 服务已经启动，修改 SNMP 的相关配置是不能生效的，必须手动点击停用，再点击启用才能将新配置加载生效。

Q4：更改已建立 TCP 连接超时时间有什么影响？

A：如果已建立 TCP 超时时间过小，客户端和服务器无数据交互时，会导致连接拆除过快，如推送数据包的间隔大于已建立 TCP 超时时间，后续推送的数据包无法转发。

如果已建立 TCP 超时时间过大，客户端和服务器无数据交互时，会导致连接拆除过慢，导致连接表不断累加。

Q5：NGFW 最大的日志记录条目数为多少？

A：NGFW 最大日志的记录条数为 2048 条，当日志数目达到 2048 条之后，系统会删除最早的日志，将新的日志记录并显示出来。

声明：

1．本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不另行通知。

2．本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。

3．本安装手册中的安装方法、步骤为天融信建议使用，并非唯一和必须的安装途径，请客户参考使用。

4．本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。

5．本手册中提到的信息为正常公开的信息，若因本安装手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。