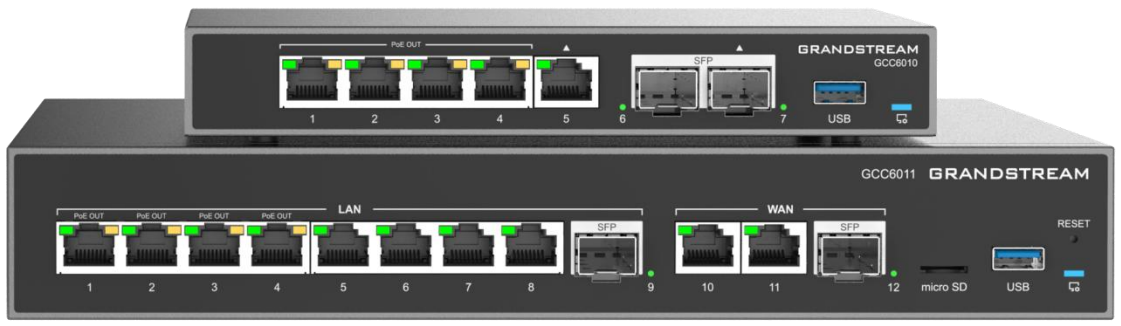
深圳市潮流网络技术有限公司

CC6010|GCC6011|GCC601W

企业级超融合有线/无线网关

防火墙-用户手册



技术支持

深圳市潮流网络技术有限公司为客户提供全方位的技术支持。您可以与本地代理商或服务提供商联系，也可以与公司总部直接联系。

地址：深圳市南山区科技园北区酷派大厦C座14楼

邮编：518057

网址：http://www.grandstream.cn

客服电话：0755-26014600

客服传真：0755-26014601

技术支持热线：4008755751

技术支持论坛：http://forums.grandstream.com/forums

网上问题提交系统：http://www.grandstream.com/support/submit-a-ticket

商标注明

注意

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

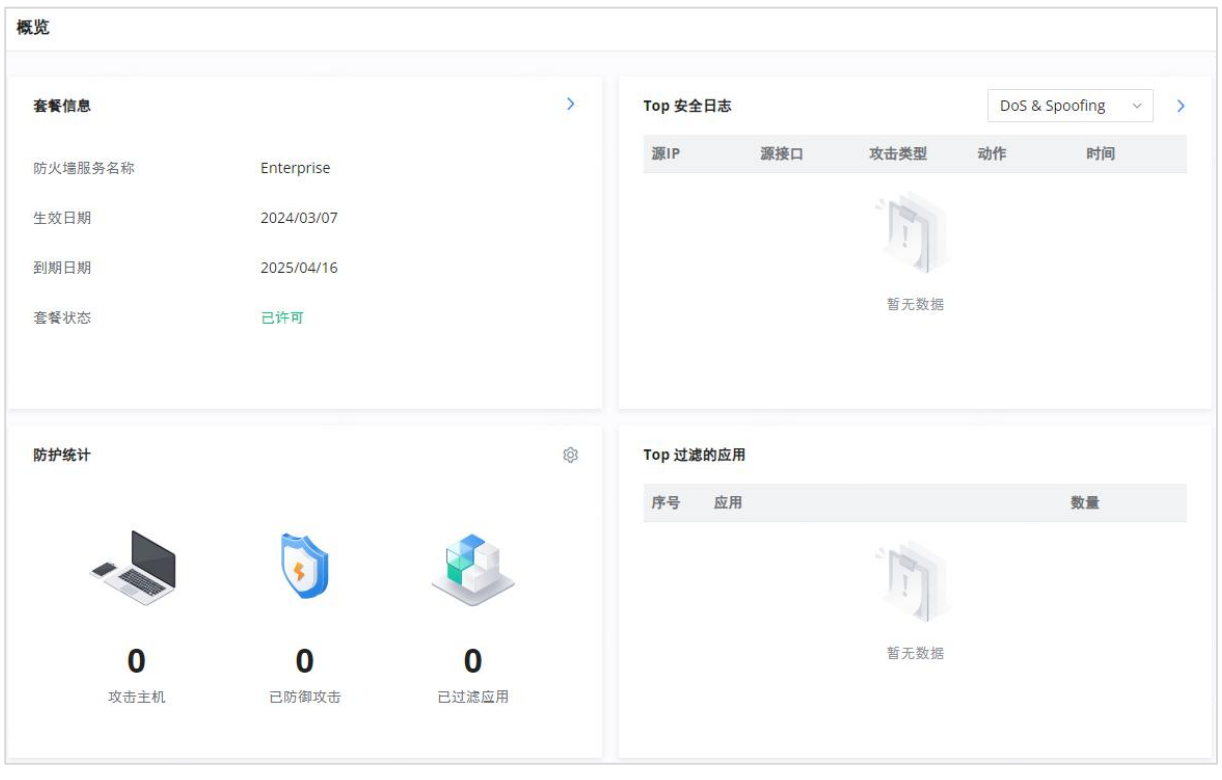
目录

在本指南中，我们将介绍GCC601X(W)防火墙模块的配置参数。

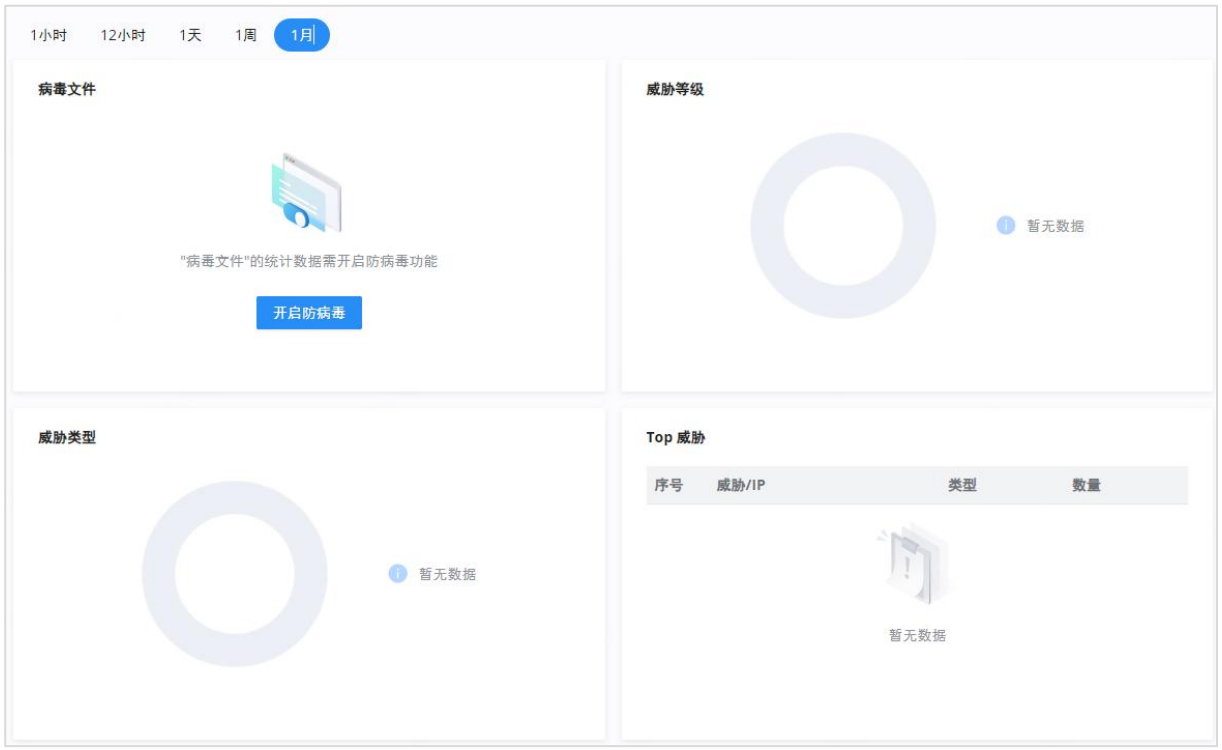
概览

概览页面为用户提供了对GCC防火墙模块以及安全威胁和统计数据的全局了解，概览页面包含：

- 防火墙服务：显示防火墙服务的状态，包括生效日期和过期日期。
- Top安全日志：显示每个类别的Top日志，用户可以从下拉列表中选择类别，也可以单击箭头图标重定向到安全日志页面以获取更多详细信息。
- 防护统计：显示各种防护统计信息，可以通过单击设置图标清除所有统计信息。
- Top 过滤的应用：显示已过滤的Top应用程序（带计数）。
- 病毒文件：显示扫描的文件和发现的病毒文件，要启用/禁用反恶意软件，用户可以单击设置图标。
- 威胁等级：用颜色代码显示从严重到次要的威胁等级。
- 威胁类型：显示具有颜色代码和重复次数的威胁类型，用户可以将鼠标光标悬停在色环上以显示名称和次数的出现。
- Top威胁：显示具有类型和数量的Top威胁。



概览第1部分



概览第2部分

用户可以单击Top安全日志下的箭头图标以重定向到安全日志部分，或者将鼠标悬停在防护统计信息下的 图标上以清除统计信息，或者在病毒文件下禁用反恶意软件。

在“威胁等级”和“威胁类型”下，用户可以将鼠标悬停在图形上以显示更多详细信息。

防火墙策略

规则策略

规则策略允许定义GCC设备将如何处理入站流量，按WAN、VLAN和VPN进行。

规则策略页面

规则策略-编辑

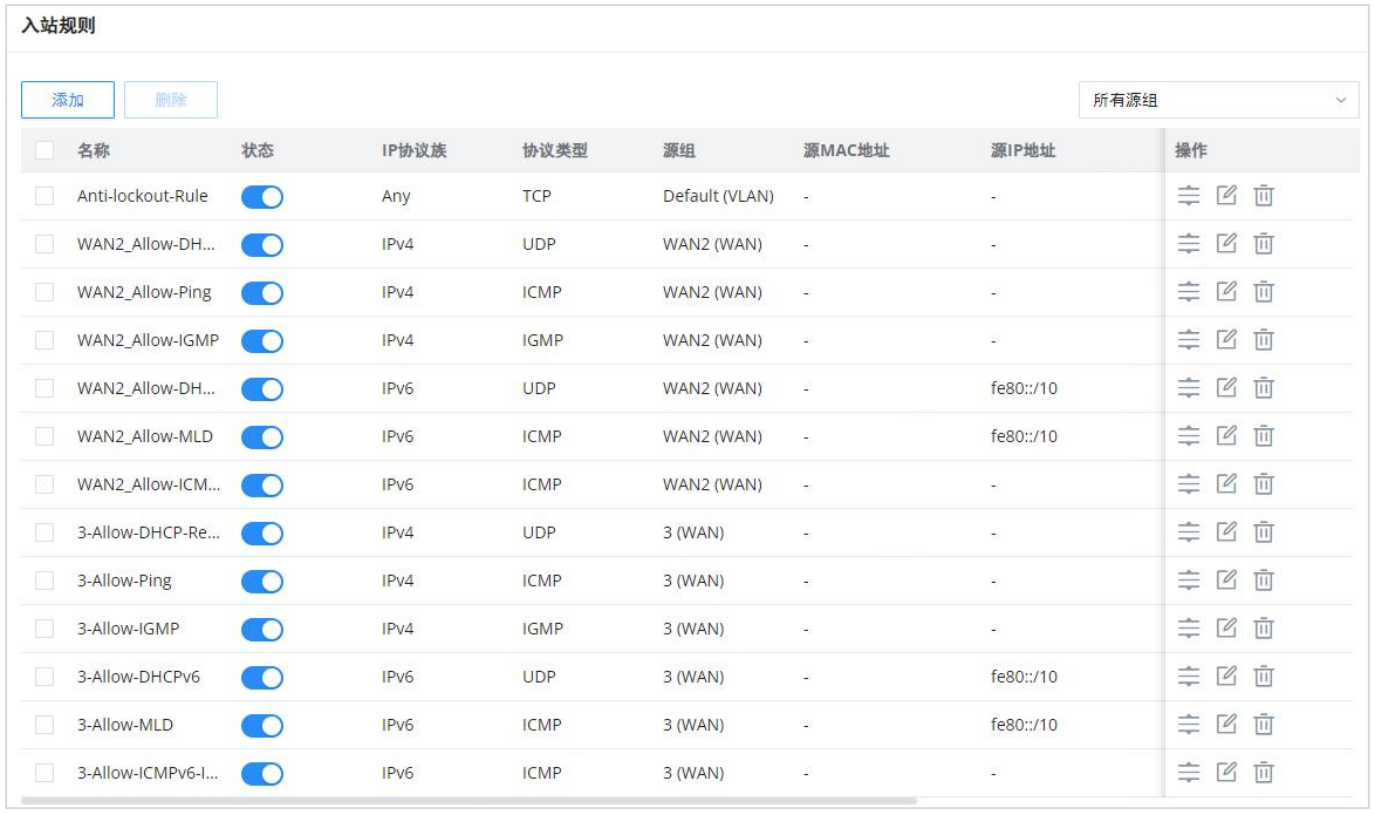
可用的选项有“接受”、“拒绝”和“丢弃”。

- IP伪装：启用IP伪装。这将屏蔽内部主机的IP地址。
- MSS Clamping：启用此选项将允许在TCP会话协商期间协商MSS（最大段大小）
- 记录丢弃/拒绝流量：启用此选项将生成已丢弃或拒绝的所有流量的日志。
- 丢弃/拒绝流量日志限制：指定每秒、分钟、小时或天的日志数。范围为1~99999999，如果为空，则没有限制。

入站规则

GCC601X(W)允许过滤到网络组或端口WAN的传入流量，并应用以下规则：

- 接受：允许流量通过。
- 拒绝：将向远程端发送一个答复，说明数据包被拒绝。
- 丢弃：数据包将被丢弃，而不会通知远端。



防火墙策略-入站规则

入站规则-添加/编辑

名称	输入入站规则的名称。
状态	打开/关闭入站规则的状态。
IP协议族	选择IP协议族。 • 任何 • IPv4 • IPv6
协议类型	选择协议类型。 • UDP • TCP • UDP/TCP • ICMP • IGMP • 所有

源组	如果设置为“全部”，则规则将优先于其他特定规则进行匹配。
源MAC地址	指定源MAC地址。
源IP地址	指定源IP地址。
源端口	要输入多个端口/端口范围，请使用逗号（，）分隔它们，例如：4,5-10。
目的IP地址	支持输入IP地址/掩码长度，例如192.168.122.0/24
目标端口	要输入多个端口/端口范围，请使用逗号（，）分隔它们，例如：4,5-10。
策略	如果设置为“接受”，则允许外部设备访问路由器；如果设置为“拒绝”，则拒绝外部设备的访问，并返回结果；若设置为“丢弃”，则直接丢弃外部设备的访问请求。

流量规则-入站规则

转发规则

GCC601X(W)允许不同组和接口（WAN/VLAN/VPN）之间通信。

要添加转发规则，请导航到**防火墙模块→ 防火墙策略→ 转发规则**，然后单击“**添加**”按钮可添加新的转发规则，或单击“**编辑**”图标可编辑规则。

添加转发规则

添加转发规则

高级NAT

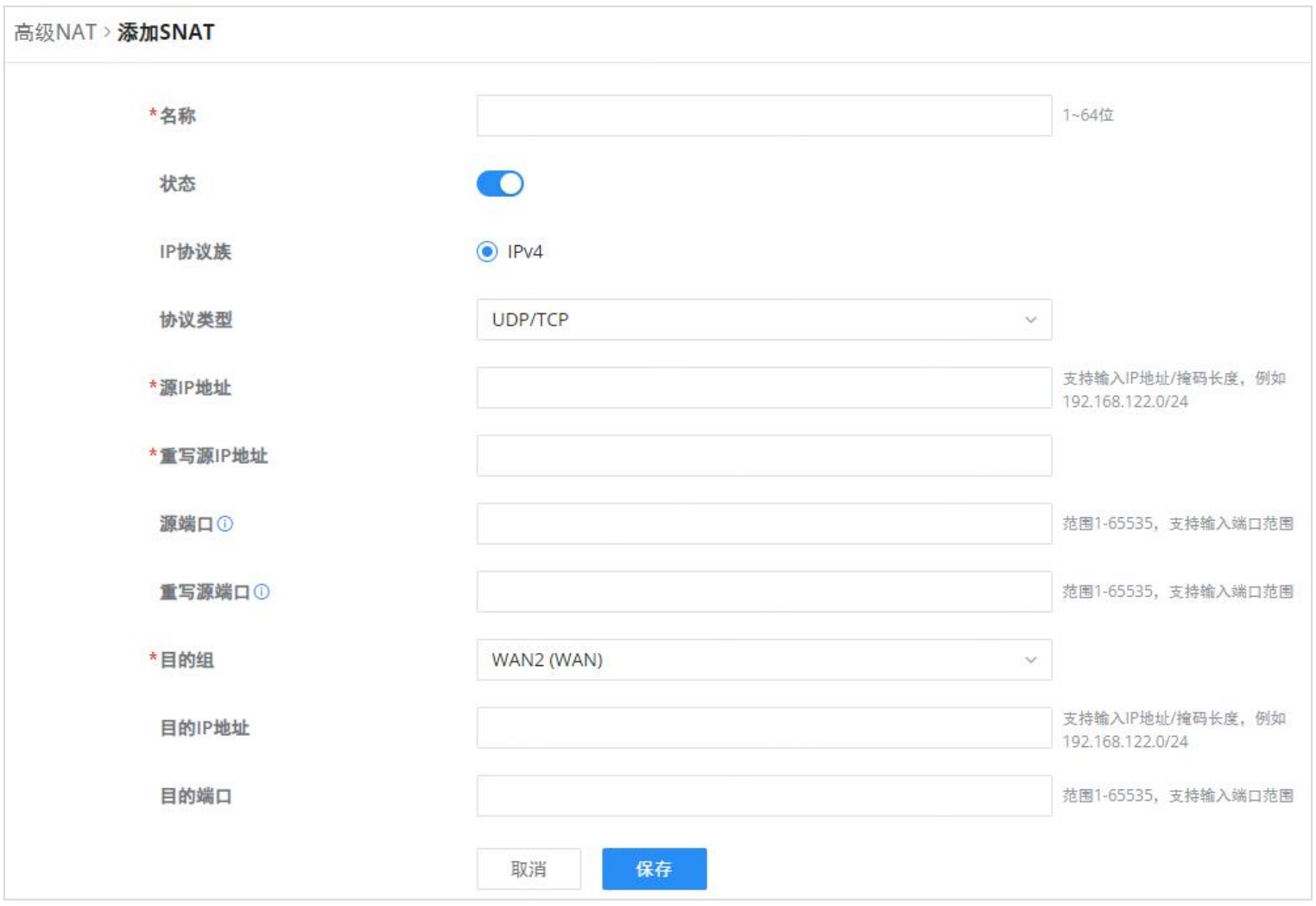
NAT或网络地址转换是私有或内部地址到公共IP地址的转换或映射，反之亦然，GCC601X(W)同时支持这两者。

- SNAT:源NAT指客户端的IP地址（私有或内部地址）到公共地址的映射。
- DNAT:目的地NAT是SNAT的反向过程，数据包将被重定向到特定的内部地址。

“防火墙高级NAT”页面提供设置源和目标NAT配置的功能。导航到**防火墙模块→ 防火墙策略→ 高级NAT。**

SNAT

要添加SNAT，请单击“添加”按钮添加新的SNAT，或单击“编辑”图标编辑以前创建的SNAT。请参阅下图和下表：



添加SNAT

创建或编辑SNAT条目时，请参阅下表：

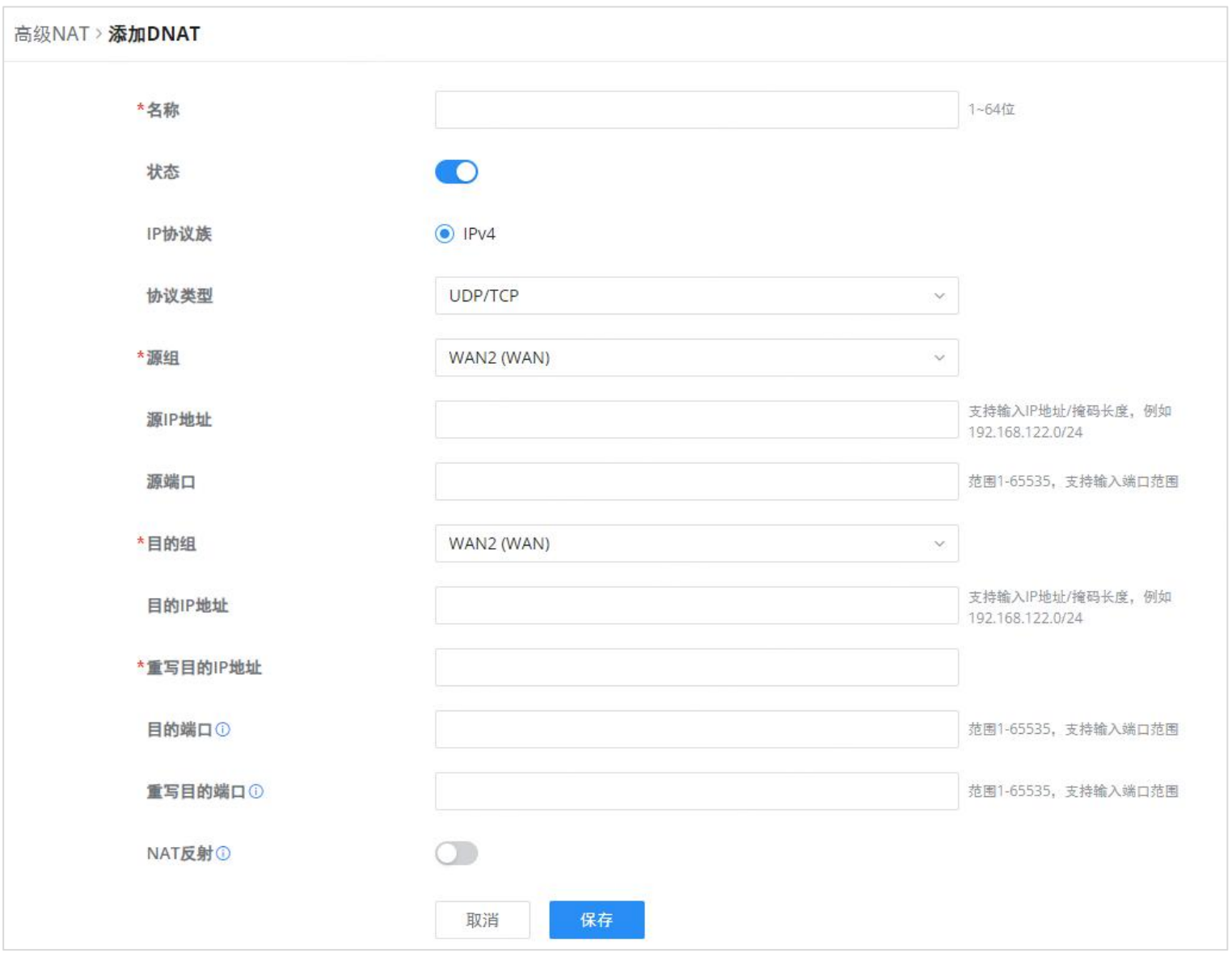
名称	指定SNAT条目的名称
IP协议族	选择IP版本，有两个选项可用：IPv4或Any。
协议类型	从下拉列表中选择一个协议或全部，可用选项为：UDP/TCP、UDP、TCP和全部。
源IP地址	设置源IP地址。
重写源IP地址	设置“重写IP”。源组中数据包的源IP地址将为已更新为此配置的IP。
源端口	设置源端口
重写源端口	设置“重写”源端口。
目的组	为目标组选择WAN接口或VLAN。

目的IP地址	设置目标IP地址。
目的端口	设置目的端口

SNAT页面

DNAT

要添加DNAT，请单击“添加”按钮添加新的DNAT，或单击“编辑”图标编辑以前创建的DNAT。请参阅下图和下表：



高级NAT - DNAT

创建或编辑DNAT条目时，请参阅下表：

名称	指定DNAT条目的名称
IP协议族	选择IP版本，有三个选项可用：IPv4、IPv6或任意。
协议类型	从下拉列表中选择一个协议或全部，可用选项为：UDP、TCP、TCP/UCP和全部。
源组	为“源组”选择WAN接口或LAN组，或选择“全部”。
源IP地址	设置源IP地址。
源端口	设置源端口。
目的组	选择WAN接口或LAN组作为“目标组”，或选择“全部”。 目的地组和源组是不同的，以避免冲突。

目的IP地址	设置目标IP地址。
重写目的IP地址	设置“重写目标IP地址”。
目的端口	设置目标端口。
重写目标端口	设置重写目标端口
NAT反射	单击“on”以启用NAT反射
NAT反射源	选择“内部”或“外部”NAT反射。

高级NAT - DNAT

全局配置

- Flush连接重置

启用此选项并更改防火墙配置后，以前的防火墙规则允许的现有连接将被终止。

如果新的防火墙规则不允许以前建立的连接，则该连接将被终止，无法重新连接。

禁用此选项后，即使新规则不允许建立此连接，也允许现有连接继续进行，直到它们超时为止。

Flush连接重置

安全防御

DoS防御

基本设置

拒绝服务攻击是一种通过向目标机器发送大量请求来使系统过载甚至崩溃或关闭，从而使合法用户无法使用网络资源的攻击。

DoS防御 - 基本设置

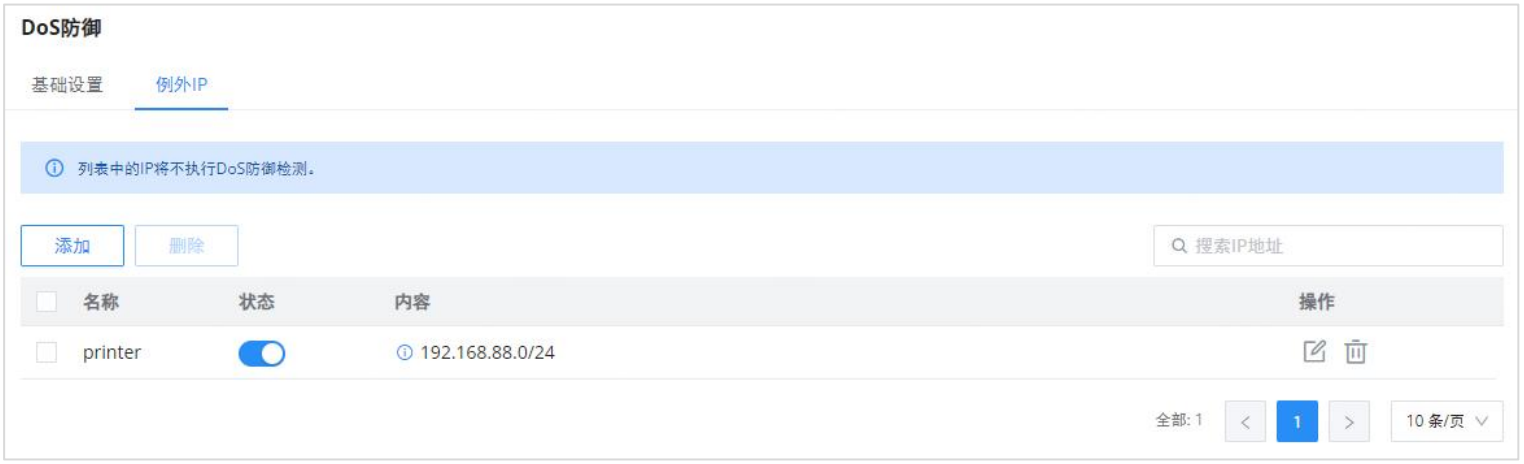
DoS防御	打开/关闭DoS防御
动作	选择操作： 监控：生成报警，但未被阻止。 阻止：监视和阻止攻击。
洪水攻击防御	
TCP SYN洪水攻击防御	启用此选项后，设备将对SYN Flood Attack采取反措施。 ● TCP SYN Flood数据包阈值（数据包/秒）：如果来自Internet的TCP SYN数据包的阈值超过了定义的值，则在指定的超时时间内将丢弃后续的TCP同步数据包。 ● TCP SYN Flood Timeout（sec）：如果在指定的超时时间内，每秒接收的TCP SYN数据包数超过阈值，则攻击防御将立即启动。
UDP Flood攻击防御	启用此选项后，设备将对UDP Flood攻击采取反措施。 ● UDP Flood数据包阈值（数据包/s）：如果来自Internet的UDP数据包的阈值超过了定义的值，则后续UDP数据包将在指定的超时期内丢弃。 ● UTCP SYN Flood Timeout（sec）：如果在超时时间内，每秒接收的UDP数据包的平均数量达到阈值，则攻击防御将立即启动。
	启用此选项后，设备将对ICMP Flood攻击采取反措施。 ● ICMP Flood数据包阈值（数据包/s）：如果来自Internet的ICMP数据包的阈值超

ICMP Flood攻击防御	过了定义的值，则将在指定的超时期内丢弃后续ICMP数据包。 ● ICMP Flood超时（秒）：如果在超时期内每秒接收的ICMP数据包的平均数量达到阈值，则攻击防御将立即启动。
ACK洪水攻击防御	启用此选项后，设备将对ACK Flood Attack采取反措施。 ● ACK Flood数据包阈值（数据包/s）：如果来自 如果Internet超过了定义的值，则在指定的超时时间内将丢弃后续的ACK数据包。 ● ACK Flood Timeout（sec）：如果在超时时间内，平均每秒接收的ACK数据包数达到阈值，则攻击防御将立即启动。
异常数据包攻击防御	
端口扫描检测	● 端口扫描数据包阈值（数据包/秒）：如果端口数据包达到阈值，端口扫描检测将立即开始。
阻止IP选项	启用此选项后，设备将忽略任何带有“选项”字段的IP数据包。
阻止TCP标志扫描	启用此选项后，设备将忽略任何意外的数据包 TCP标志中的信息。
阻止Land攻击	启用此选项后，设备将阻止任何可能具有被欺骗并修改为将源地址和目标地址设置为路由器的地址。如果禁用此选项，可能会导致路由器陷入对自身的响应循环。
阻止Smurf	启用此选项后，设备将丢弃任何ICMP回显请求。
阻止死亡Ping	启用此选项后，设备将丢弃任何异常或损坏的ping数据包。
阻止Trace Route	启用此选项后，设备将不允许从WAN端启动traceroute请求。
阻止ICMP片段	启用此选项后，设备将丢弃分段的ICMP数据包。
屏蔽SYN分片	启用此选项后，设备将丢弃分段的SYN数据包。
阻止未分配的协议编号	如果启用，设备将拒绝接收IP协议号大于133的IP数据包。
阻止Fraggle攻击	如果启用，设备将丢弃从WAN端发起的任何UDP广播数据包。

DoS防御

例外IP

用户可以添加要从DoS防御扫描中排除的IP地址或IP范围。添加IP地址或IP范围到列表，单击“**添加**”按钮，如下所示：



DoS防御 - 例外IP

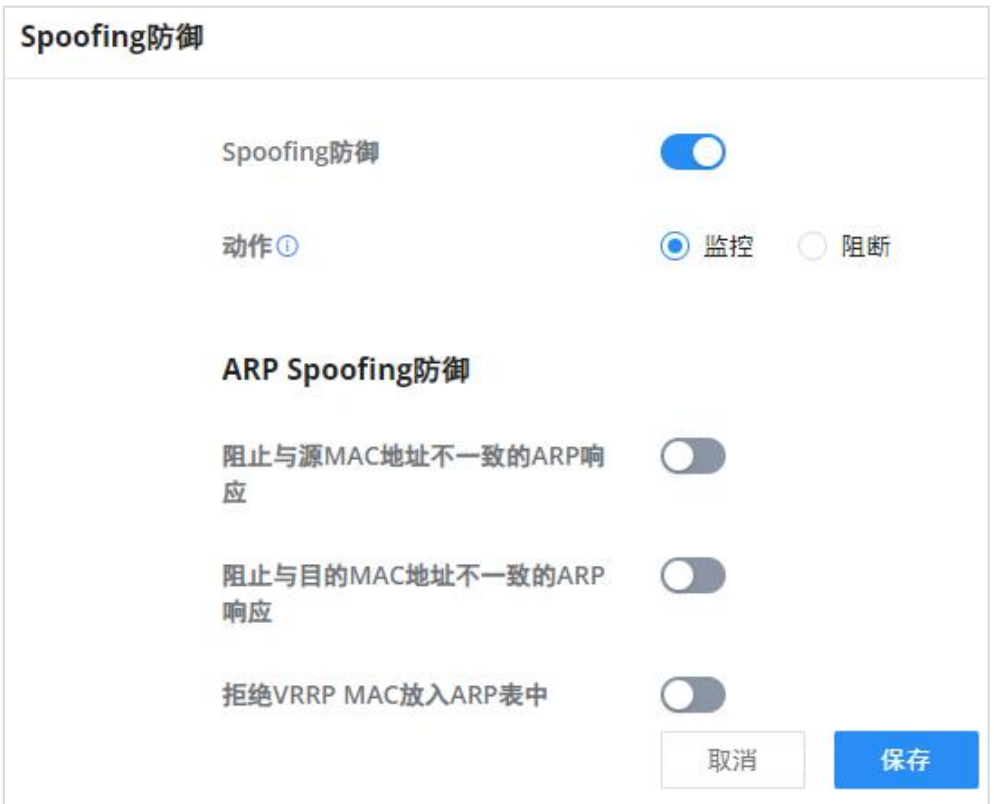
指定一个名称，然后在指定IP地址或IP范围后将状态切换为“开启”。

DoS防御 - 添加例外IP

Spoofing防御

Spoofing防御部分提供了几种应对各种欺骗技术的措施。为了保护您的网络免受欺骗，请启用以下措施以消除您的流量被拦截和欺骗的风险。

GCC601X(W)设备提供了对抗ARP信息的措施。



Spoofing防御

ARP Spoofing防御

- 阻止源MAC地址不一致的ARP响应：GCC设备将验证特定数据包的目标MAC地址，当设备收到响应时，它将验证源MAC地址，并确保它们匹配。否则，GCC设备将不转发数据包。

- 阻止与目标MAC地址不一致的ARP响应：收到响应时，GCC601X(W)将验证源MAC地址。设备将验证目标MAC地址，并确保它们匹配。否则，设备将不会转发数据包。

- 拒绝VRRP MAC放入ARP表：GCC601X(W)将拒绝，包括ARP表中生成的任何虚拟MAC地址。

反恶意软件

在本节中，用户可以启用反恶意软件并更新其签名库信息。

配置

要启用反恶意软件，请导航到**防火墙模块→ 反恶意软件→ 配置反恶意软件**：打开/关闭以用/禁用反恶意软件。

注意

若要过滤HTTPs URL，请启用"SSL代理"。

- 数据包检查深度：根据配置检查每个流量的数据包内容。深度越深，检测率越高，CPU消耗也越高。有三个级别的深度低，中等和高。

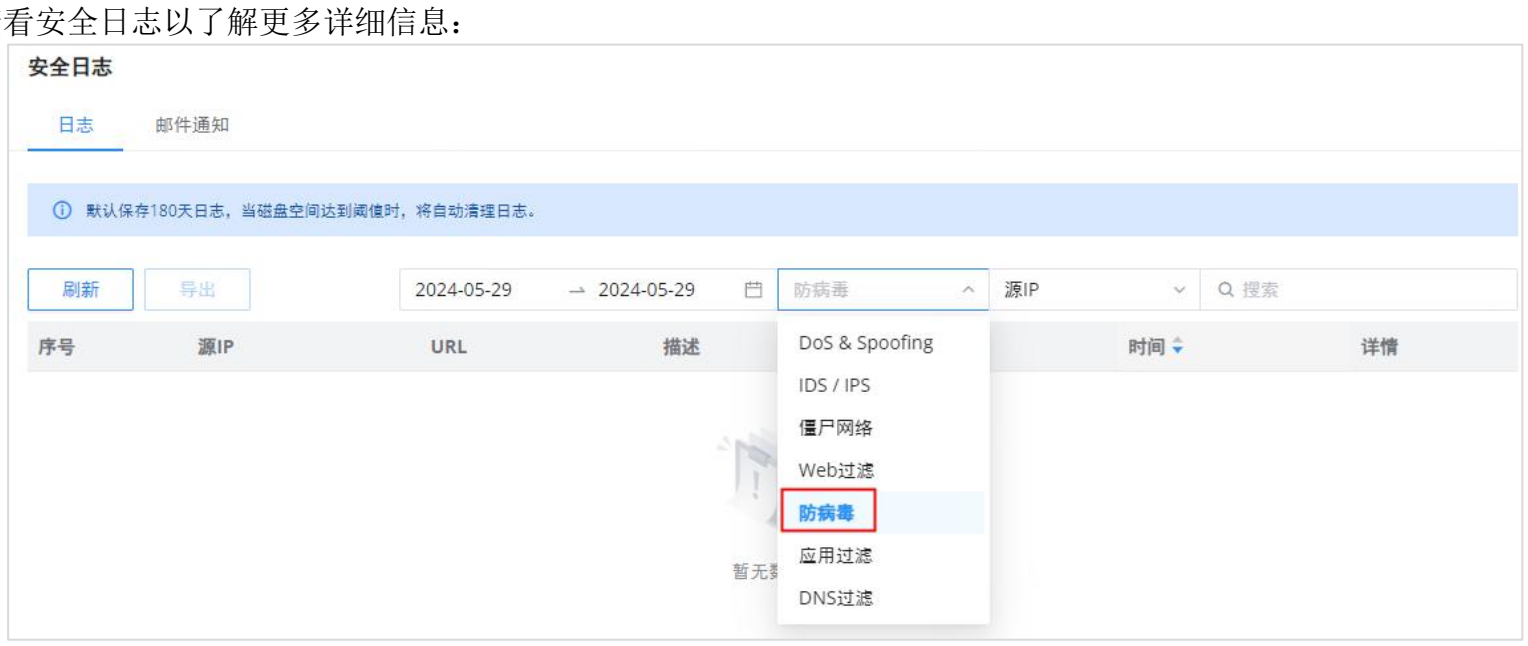
- 扫描压缩文件：支持扫描压缩文件。

反恶意软件配置

在概览页面上，用户可以查看统计信息并进行概览。

概览页 - 反恶意软件统计信息

还可以查看安全日志以了解更多详细信息：



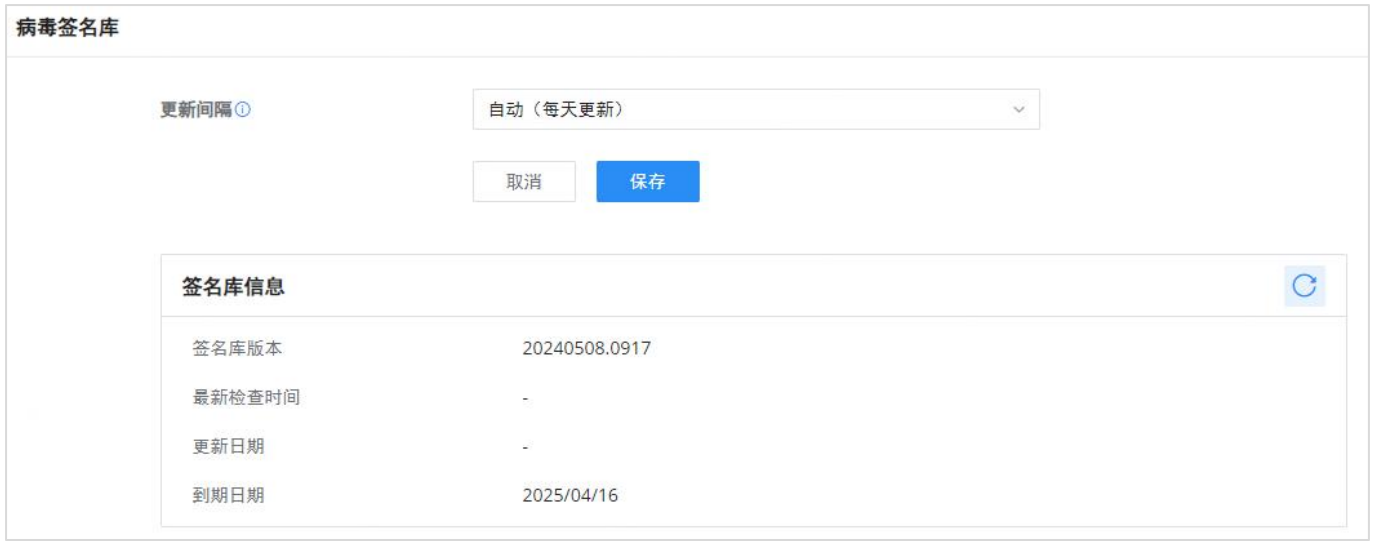
安全日志-反恶意软件

病毒签名库

在该页面上，用户可以手动更新反恶意软件签名库信息，每天更新或创建时间表，请参阅下图：

注意

默认情况下，设备在每天随机时间点（00:00-6:00）更新。


病毒签名库
更新间隔
自动（每天更新）
取消
保存
签名库信息
签名库版本
20240508.0917
最新检查时间
-
更新日期
-
到期日期
2025/04/16

病毒签名库

入侵防御

入侵防御系统（IPS）和入侵检测系统（IDS）是监控网络流量以防可疑活动和未经授权的访问尝试的安全机制。IDS通过分析网络数据包和日志来识别潜在的安全威胁，而IPS则通过实时阻止或减少恶意流量来主动预防这些威胁。IPS和IDS共同提供了一种分层的网络安全方法，有助于抵御网络攻击和保护敏感信息。僵尸网络是一个受恶意软件感染并由恶意行为者控制的受损计算机网络，通常用于进行大规模网络攻击或非法活动。

IDS/IPS

基本设置-IDS/IPS

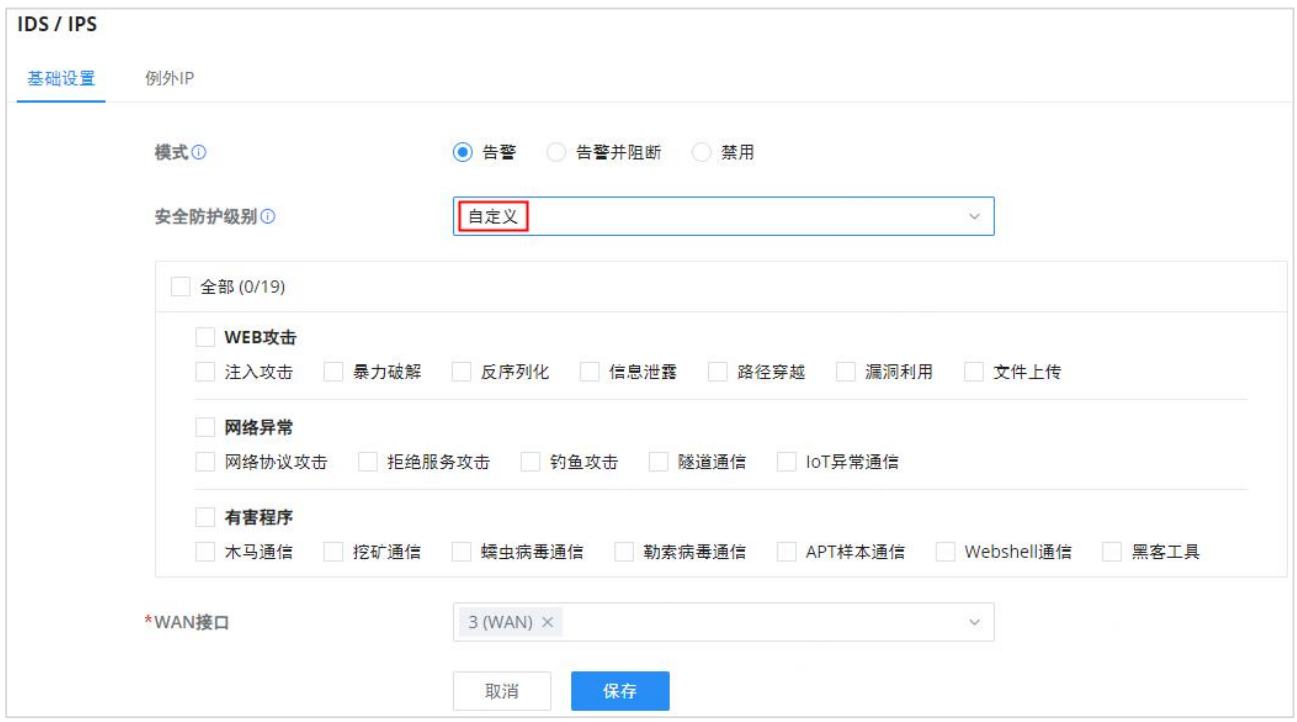
在此选项卡上，用户可以选择IDS/IPS模式、安全保护级别。

IDS/IPS模式

- 告警：检测流量，只通知用户，不阻塞流量，相当于IDS（入侵检测系统）。
- 禁用：无通知或预防，IDS/IPS在这种情况下被禁用。
- 安全防护级别：选择保护级别（低、中、高、极高和自定义）。用户可以自定义保护类型。保护级别越高，保护规则就越多，“自定义”将允许用户选择IDS/IPS将检测的内容。

IDS/IPS - 基本设置

请参考下图：



IDS/IPS - 安全保护级别设置为自定义

要检查通知和所采取的操作，请在安全日志下，从下拉列表中选择IDS/IPS，如下所示：

安全日志 - IDS/IPS

例外IP

IDS/IPS不会检测到此列表上的IP地址。要将IP地址添加到列表中，请单击“**添加**”按钮，如下所示：

IDS/IPS - 例外IP

输入名称，然后启用状态，然后选择IP地址的类型（源或目标）。添加IP地址点击“+”图标，要删除IP地址，点击“**-**”图标，如下所示：

IDS/IPS - 添加例外IP

僵尸网络

基本设置-僵尸网络

在此页面上，用户可以配置监控出站僵尸网络 IP和僵尸网络域名的基本设置，有三个选项：

- 监控：报警已生成，但未被阻止。
- 阻断：监视和阻止访问僵尸网络的出站IP地址/域名。
- 不检测：不检测到出站僵尸网络的IP地址/域名。

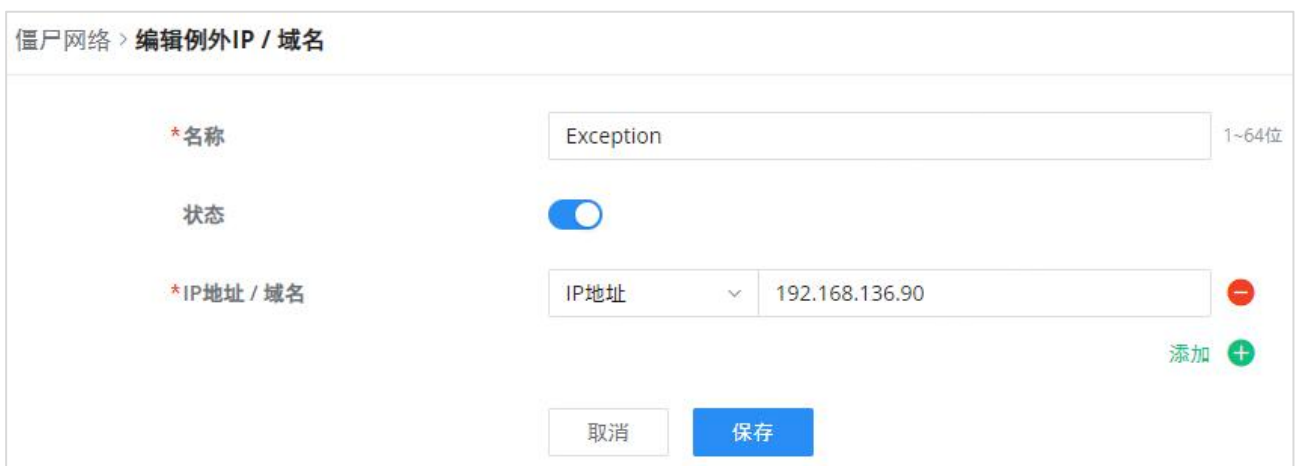
僵尸网络 - 基本设置

例外IP/域名

此列表中的IP地址将不会检测到僵尸网络。要将IP地址添加到列表中，请单击“**添加**”按钮，如下所示：

输入名称，然后启用状态。要添加IP地址/域名，请单击“+”图标并删除IP地址/域名点击“ - ”图标，如下所示：

僵尸网络 - IP/域名异常

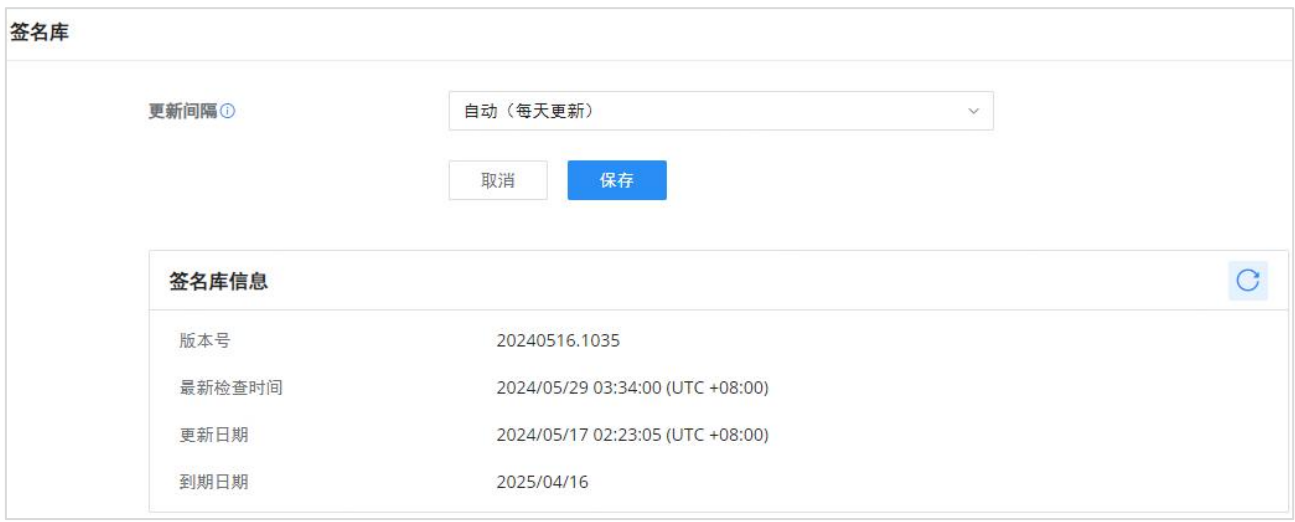


僵尸网络 - IP/域名异常

签名库-入侵防御

用户可以手动更新IDS/IPS和僵尸网络签名库信息，每天更新或创建时间表，请参阅下图：

> **注意**
>
> 默认情况下，设备在每天随机时间点（00:00-6:00）更新。



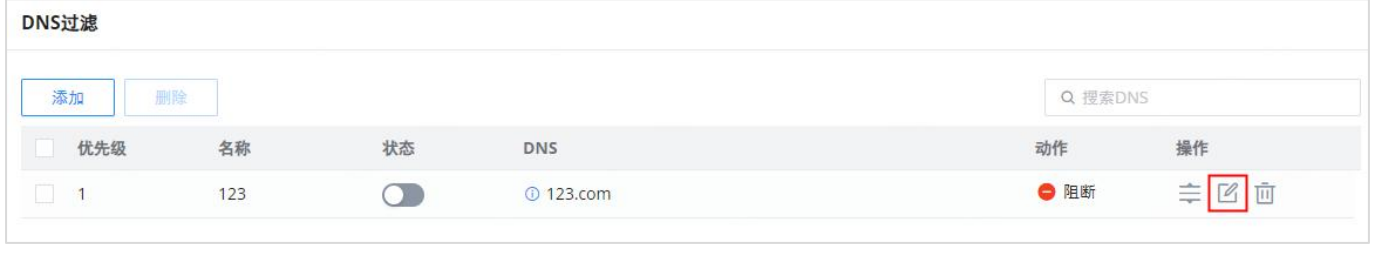
IDS/IPS和僵尸网络——签名库

内容控制

内容控制功能使用户能够根据DNS、URL、关键字和应用程序过滤（允许或阻止）流量。

DNS过滤

要根据DNS过滤流量，**请导航至防火墙模块→内容控制→DNS过滤**。单击“添加”按钮添加新的DNS过滤，如下所示：



DNS过滤页

然后，输入DNS过滤器的名称，启用状态，并选择操作（允许或阻止）。对于过滤的DNS，有两个选项：

- 简单匹配：域名支持多级域名匹配。
- 通配符：可以输入关键字和通配符*，通配符*只能添加在输入的关键字之前或之后。

比如：*.imag ， news*，*news*.在中间的*当普通字符处理。

添加DNS过滤器

要检查过滤的DNS，用户可以在概览页或安全日志下找到它，如下所示：

DNS过滤——安全日志

Web过滤

基本设置—Web过滤

用户可以启用/禁用全局web过滤，然后用户可以启用或禁用web URL过滤，URL类别过滤和关键字过滤。

若需过滤HTTPs网址，请启用“SSL代理”。

网页过滤——基本设置

URL过滤

URL过滤使用户能够使用简单匹配（域名或IP地址）或通配符（例如*example*）来过滤URL地址。

要创建URL过滤，请导航到**防火墙模块→内容过滤→网页过滤页面→URL过滤**页面，然后点击“添加”按钮，如下所示：

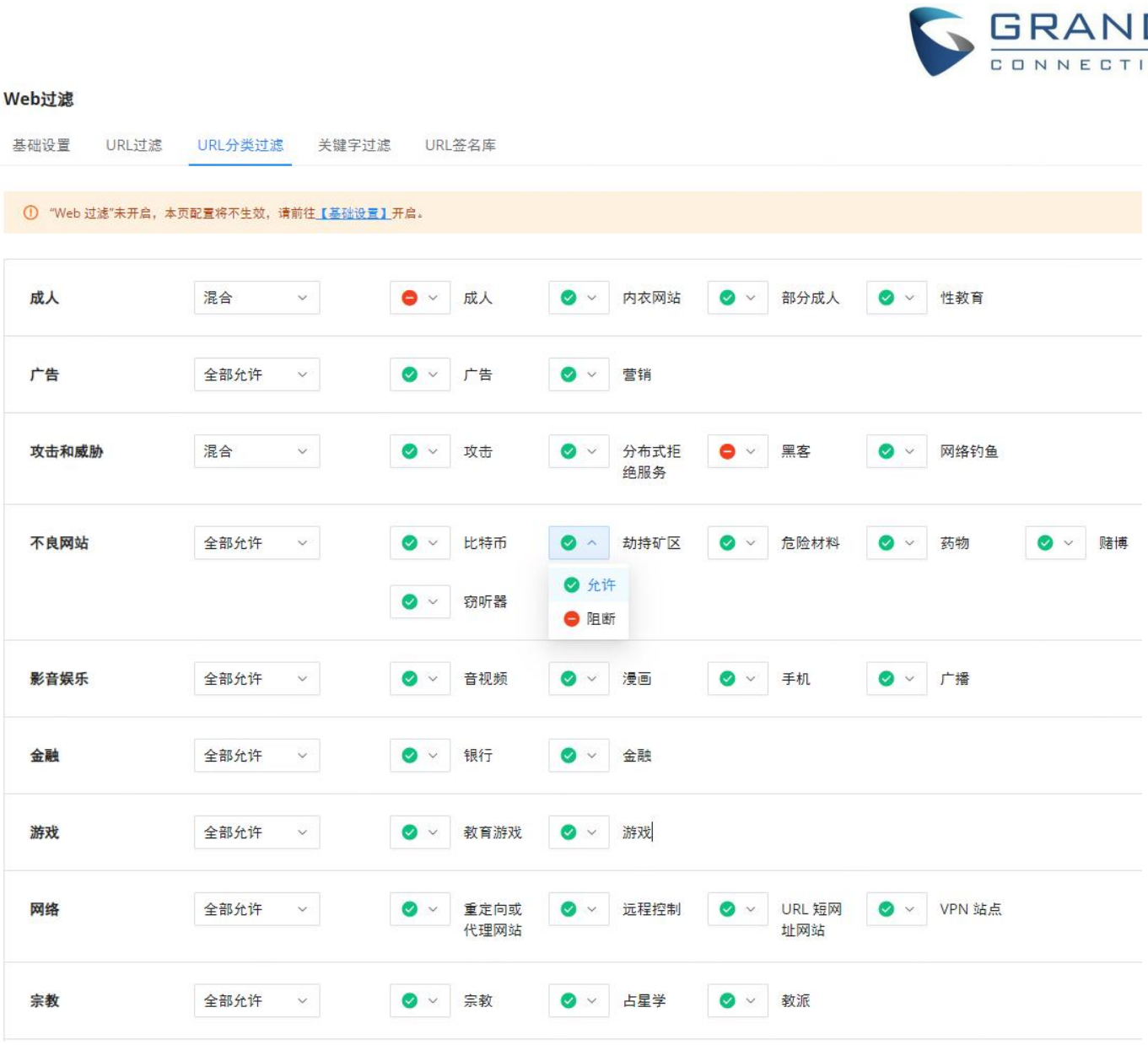
网页过滤-URL过滤

指定一个名称，然后打开状态，选择操作（允许、阻止），最后使用简单的域名、IP地址（简单匹配）或通配符指定URL。请参阅下图：

URL分类过滤

用户不仅可以选择按特定域/IP地址或通配符过滤，还可以按分类过滤，例如攻击和威胁、成人等。

要阻止或允许整个类别，请单击该行的第一个选项，然后选择全部允许或全部阻止。也可以按子类别阻止/允许，如下所示：



网页过滤-URL过滤

关键字过滤

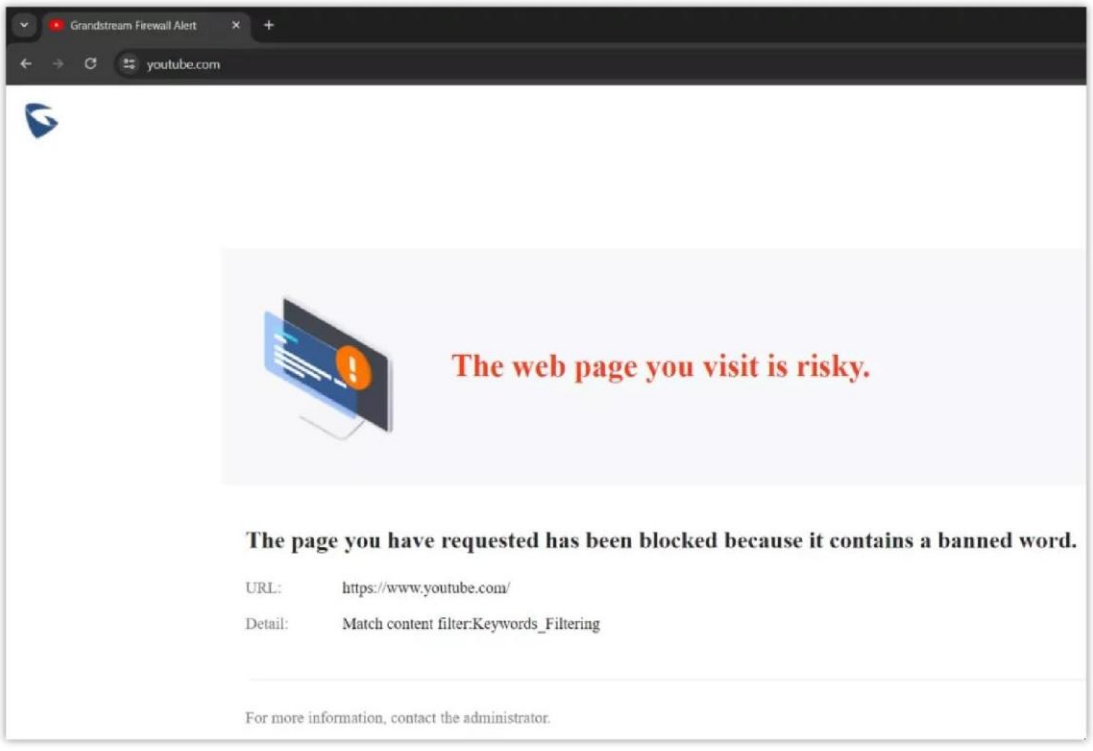
关键字过滤使用户能够使用正则表达式或通配符（例如*example*）进行过滤。

要创建关键字过滤，**请导航到防火墙模块→内容过滤→网页过滤页面→关键字过滤**选项卡，然后单击“添加”按钮，如下所示：

网页过滤——关键字过滤

指定一个名称，然后打开状态，选择操作（允许、阻止），最后使用正则表达式或通配符指定过滤的内容。请参阅下图：

当关键字过滤打开且操作设置为阻止时。例如，如果用户尝试在浏览器上访问“YouTube”，将提示他们防火墙警报，如下所示：



浏览器上的关键字过滤示例

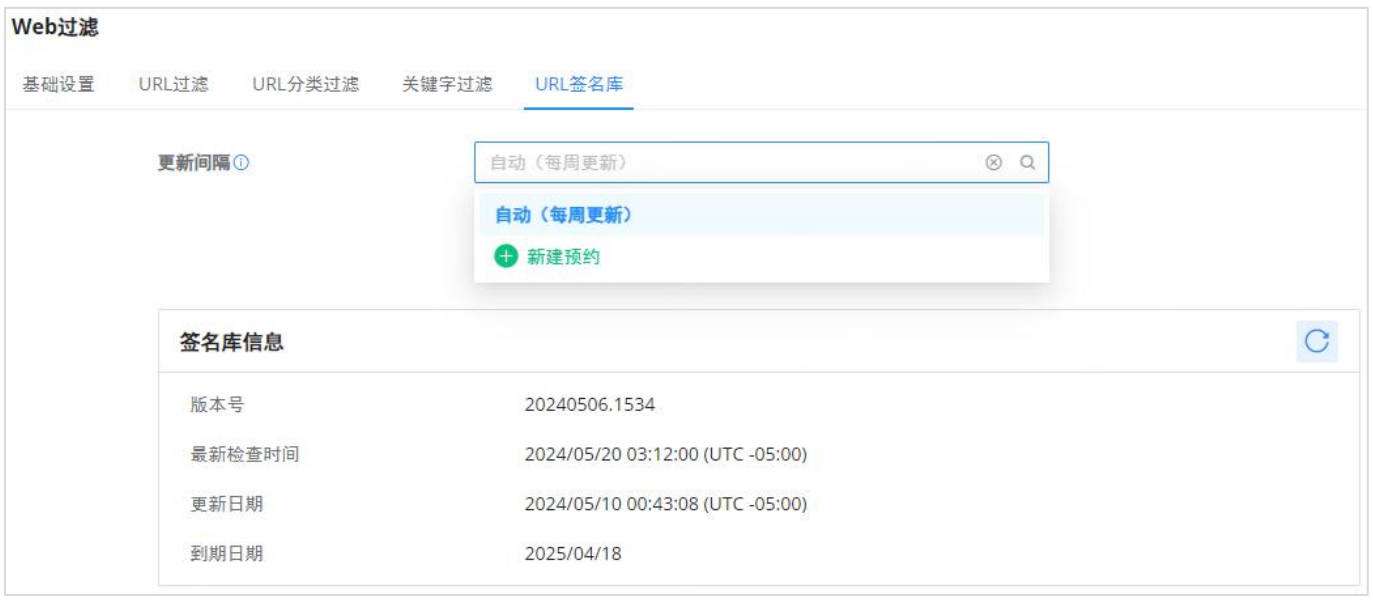
有关警报的更多详**细信息，用**户可以导航到防火墙模块→安全日志。

GCC安全日志上的关键字过滤示例

URL签名库

用户可以手动更新网页过滤签名库信息，每天更新，或创建一个时间表，请参考下图：

> **注：**
>
> 默认情况下，设备会在每天随机的时间点（00:00-6:00）更新。



网页过滤-URL签名库

应用程序过滤

基本设置—应用程序过滤

在页面上，用户可以启用/禁用全局应用程序过滤，然后用户可以按应用程序类别启用或禁用。

导航到**防火墙模块→内容控制→应用程序过滤**，并在基本设置选项卡上启用应用程序全局过滤，也有可能启用人工智能识别，以实现更好的分类。

> **注：**
>
> 当启用AI识别时，将使用AI深度学习算法来优化应用分类的准确性和可靠性，这可能会消耗更多的CPU和内存资源。

应用程序过滤——基本设置

应用程序过滤规则

在“应用程序过滤规则”选项卡上，用户可以按应用程序类别允许/阻止，如下所示：

应用程序过滤——应用程序过滤规则

要查看应用程序类别包括的内容，请单击文本，将显示应用程序列表。请参阅下图：

应用程序过滤——类别

应用程序过滤的结果将显示在安全日志下。

GCC安全日志上的应用程序过滤示例

有关更多详细信息，请单击日志中的感叹号图标。

覆盖过滤规则

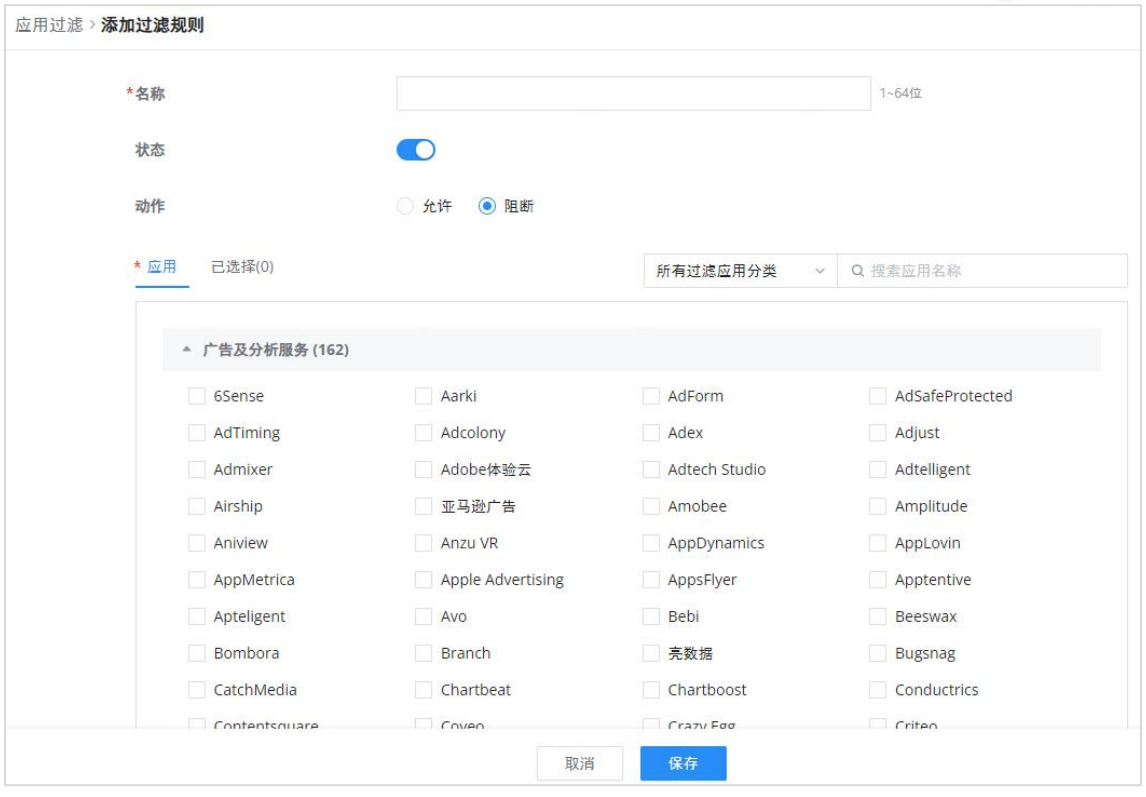
如果选择了应用类别，用户仍可以选择使用覆盖过滤规则功能覆盖一般规则（应用类别）。

例如，如果浏览器应用程序类别设置为阻止，可以添加一个覆盖过滤规则来允许Opera Mini，这样除了Opera Mini之外，整个浏览器应用程序类别都会被阻止。

要创建覆盖过滤规则，请单击“添加”按钮，如下所示：

应用程序过滤——覆盖过滤规则

然后指定一个名称并打开状态，将操作设置为允许或阻止，最后从列表中选择将被允许或阻止的应用程序。请参阅下图：



添加/编辑过滤规则

签名库—应用程序过滤

用户可以手动更新应用程序过滤签名库信息，每天更新或创建时间表，请参考下图：

> **注：**
>
> 默认情况下，设备会在每周随机的时间点（00:00-6:00）更新。

应用程序过滤——签名库

SSL代理

SSL代理是一种服务器，使用SSL加密来保护客户端和服务器之间的数据传输。它运行透明，加密和解密数据而不被检测到。它能确保敏感信息在互联网上的安全传递。

启用SSL代理后，GCC601X(W)将充当连接客户端的SSL代理服务器。

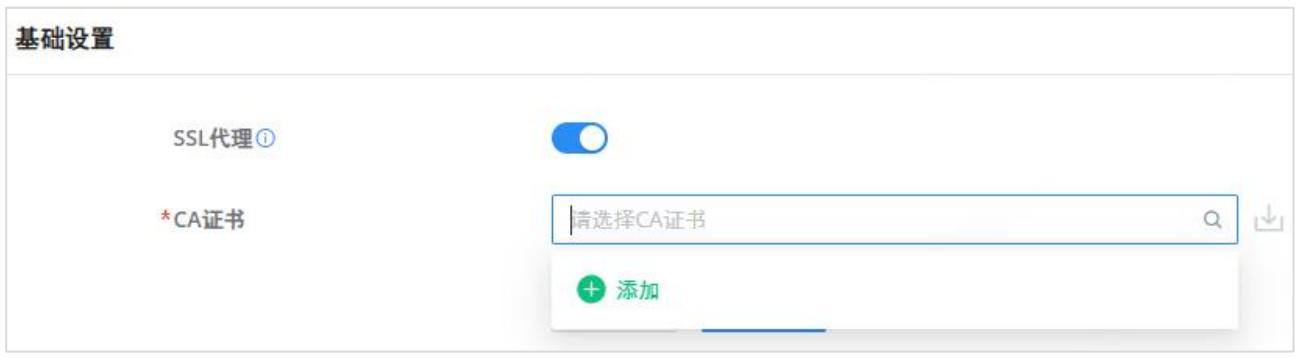
基本设置-SSL代理

打开SSL代理、网页过滤或反恶意软件等功能有助于检测网站上的某些类型的攻击，如SQL注入和跨站点脚本（XSS）攻击。这些攻击试图损害或窃取网站信息。

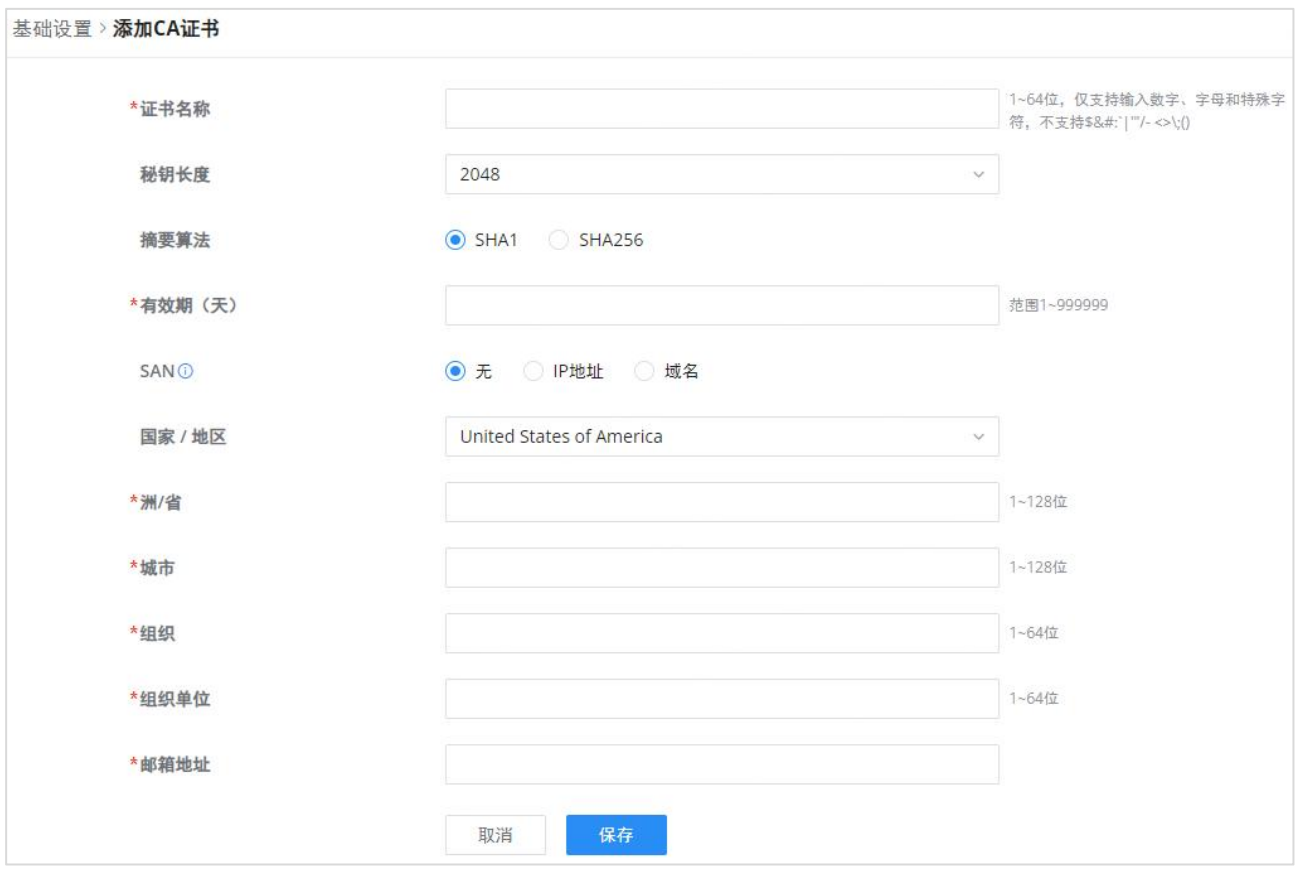
当这些功能处于活动状态时，它们会在安全日志下生成警报日志。

但是，当这些功能打开时，用户在浏览网页时可能会看到有关证书的警告。发生这种情况是因为浏览器无法识别正在使用的证书。为了避免这些警告，用户可以在浏览器中安装证书。如果证书不可信，某些应用程序在访问Internet时可能无法正常工作。

对于HTTPS过滤，用户可以通过导航到防火墙模块→SSL代理→基本设置来启用SSL代理，然后在从下拉列表中选择CA证书或单击“添加”按钮创建新的CA证书后打开SSL代理。请参阅下表：



启用/禁用SSL代理



SSL代理——添加CA证书

证书名称	输入CA的证书名称。 注意：它可以是标识此证书的任何名称。例如：“CAT”。
密钥长度	选择用于生成CA证书的密钥长度。 以下值可用：

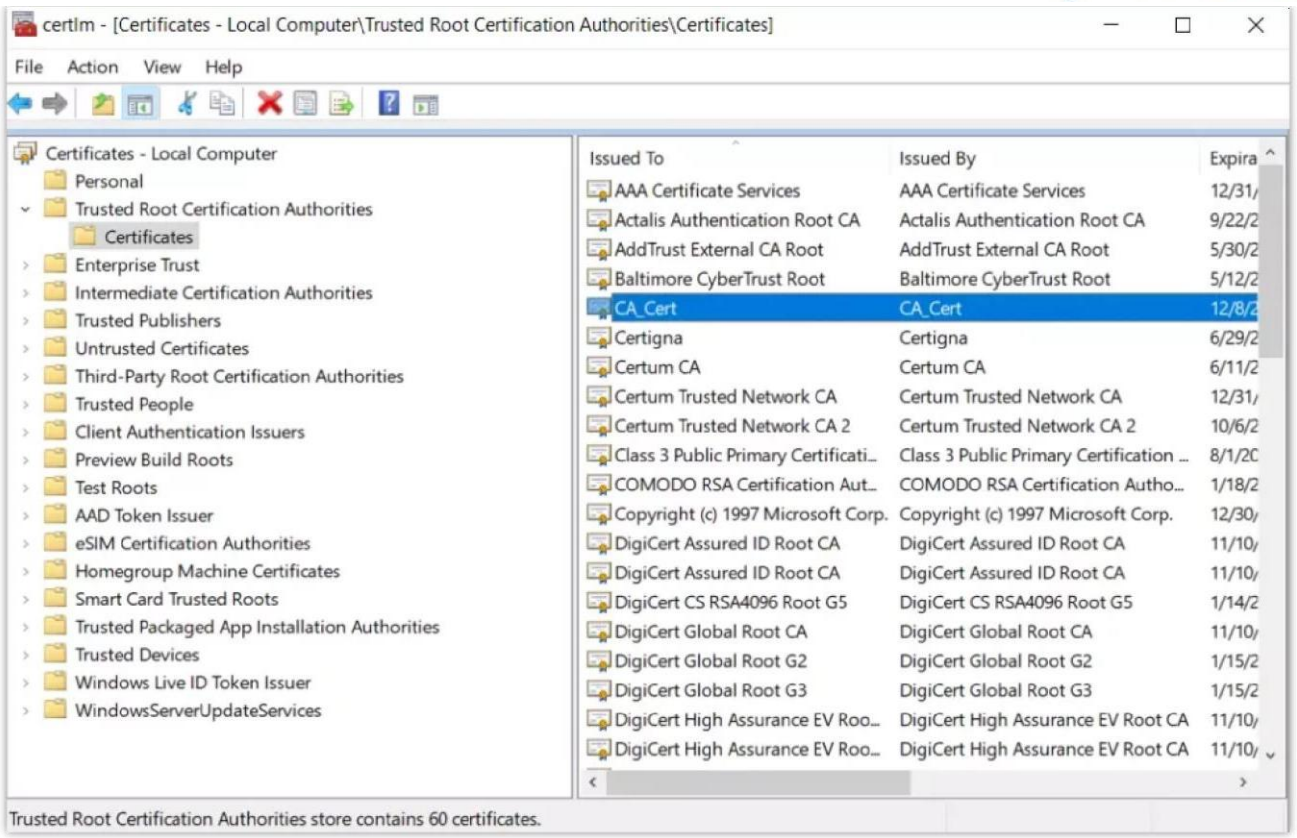
	● 1024：1024位密钥不再足以抵御攻击。 ● 2048：2048位密钥是一个很好的最小值。（推荐）。 ● 4096：几乎所有RSA系统都接受4096位密钥。使用4096位密钥将显著增加生成时间、TLS握手延迟和TLS操作的CPU使用率。
摘要算法	选择摘要算法： ● SHA1：这种摘要算法基于任意长度的输入提供160位指纹输出。 ● SHA256：这种摘要算法生成一个几乎唯一的、固定大小的256位散列。 注意：哈希是一个单向函数，它不能被解密回来。
有效期（天）	以天为单位输入CA证书的有效日期。 有效范围为1~999999.
SAN	输入SAN的地址、IP或域名（主题备用名称）。
国家/地区	从下拉列表中选择一个国家代码。 例如：“中国”。
州/省	输入州名或省名。 例如：“浙江”。
城市	输入城市名称。 例如：“杭州”。
组织	输入组织名称。 例如：“GS”。
组织单位	此字段是提出请求的部门或组织单位的名称。 例如：“GS销售”。
邮箱地址	输入电子邮件地址。 例如：“EMEAregion@grandstream.com”

SSL代理—添加CA证书

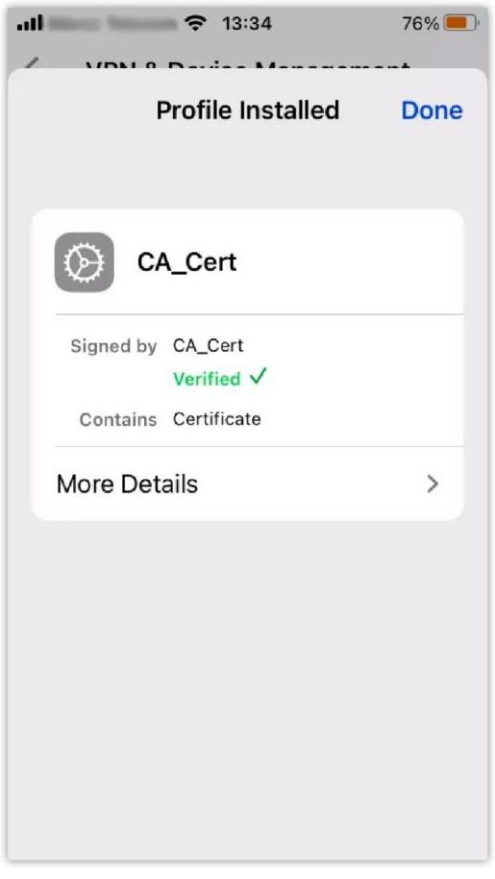
要使SSL代理生效，用户可以通过单击下载图标手动下载CA证书，如下所示：

SSL代理—下载CA证书

然后，可以将CA证书添加到受信任证书下的预期设备中。



SSL代理—向Windows添加CA证书

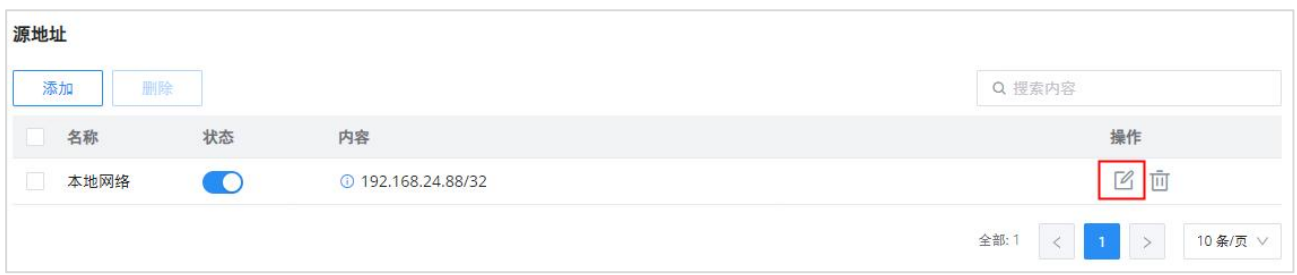


SSL代理—向电话添加CA证书

源地址

当没有指定源地址时，所有传出连接都会通过SSL代理自动路由。

但是，在手动添加新的源地址时，只有特别包含的地址才会通过SSL进行代理，从而确保基于用户定义的标准进行选择性加密。



SSL代理—源地址

SSL代理—添加/编辑源地址

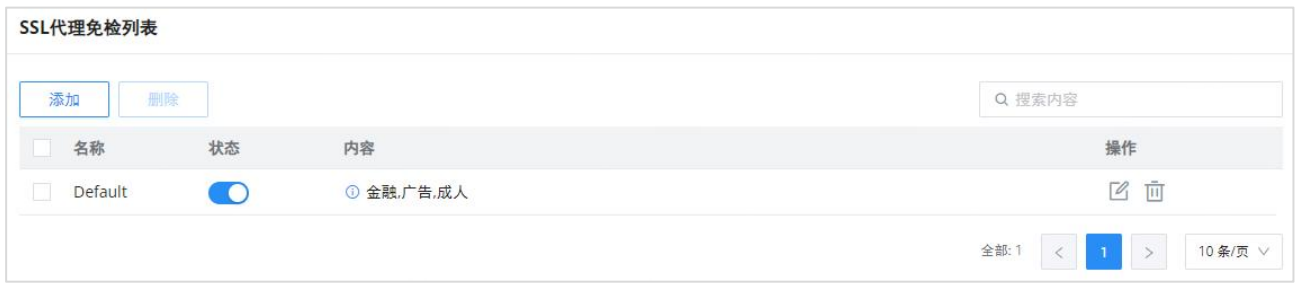
SSL代理免检列表

SSL代理涉及拦截和检查客户端和服务器之间的SSL/TLS加密流量，这通常是出于公司网络中的安全和监控目的。

但是，在某些情况下，SSL代理对于特定的网站或域可能不理想或不实用。

免检列表允许用户指定他们的IP地址、域、IP范围和web类别，以便从SSL代理中豁免。

单击“添加”按钮添加SSL豁免，如下所示：



SSL代理免检列表

在“内容”选项下，用户可以点击“+图标”按钮添加内容，点击“-”按钮删除内容图标”如下所示：

添加/编辑SSL免检地址

安全日志

日志

安全日志将列出许多详细信息，如源IP、源接口、攻击类型、操作和时间。

点击“刷新”按钮刷新列表。点击“导出”按钮将列表下载到本地机器。用户还可以选择通过以下方式过滤日志：

1. 时间

2. 攻击类型

日志条目排序依据：

1. 源IP
2. 源接口
3. 攻击类型
4. 动作

安全日志

注：

默认情况下，日志保留180天。当磁盘空间达到95%阈值时，将自动清除安全日志。

如需了解更多详细信息，请单击“详情”列下的“感叹号图标”。

当用户点击“导出”按钮时，一个Excel文件将被下载到他们的本地机器上。请参阅下图：

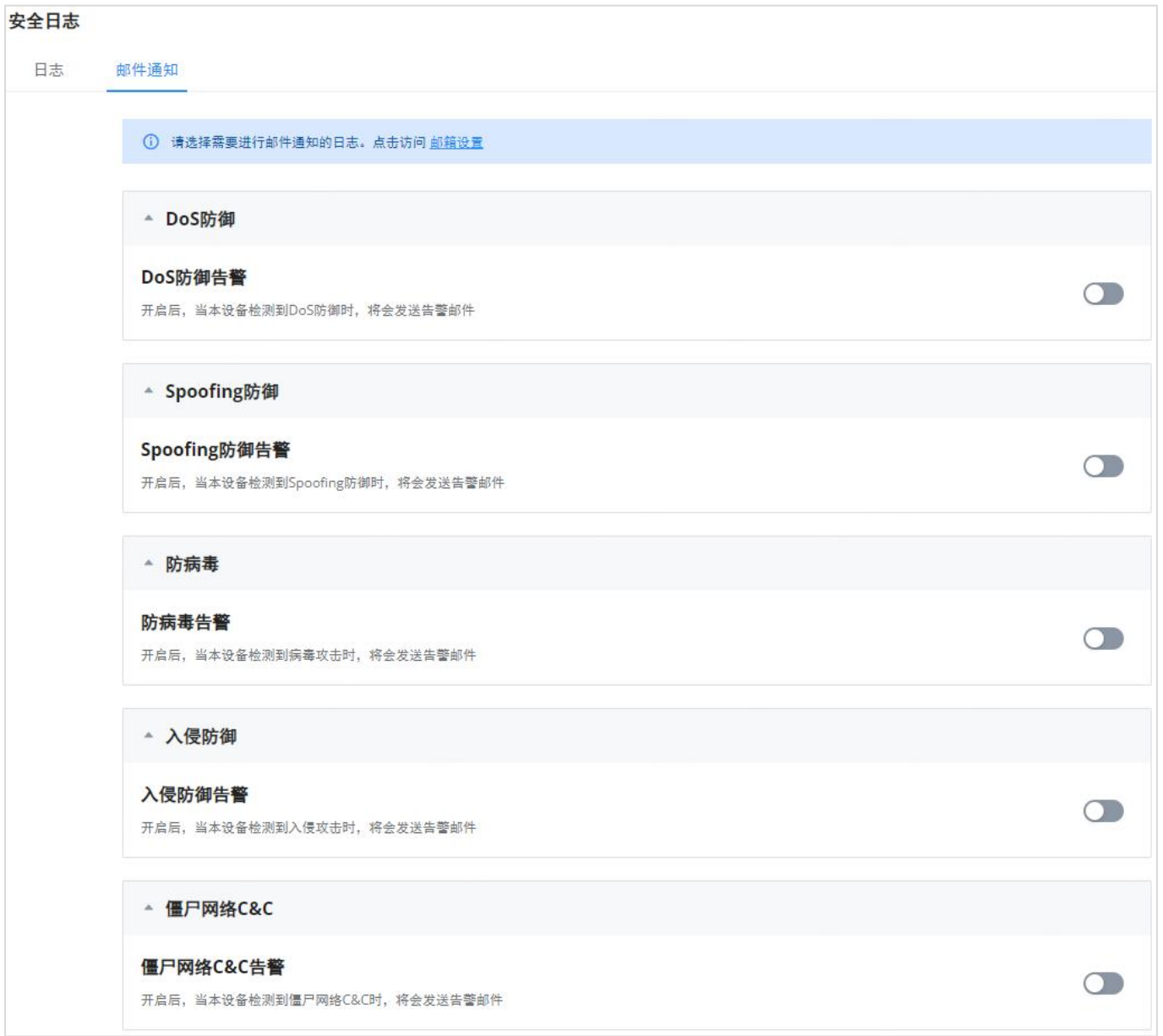
	A	B	C	D	E	F
1	Time	Source IP	Source Interface	Attack Type	Filter Quantity	Action
2	####	192.168.5.128	NET5	Port Scan	35	block
3	####	192.168.5.222	NET5	Port Scan	7	block
4	####	192.168.5.222	NET5	Port Scan	23	block
5	####	192.168.5.222	NET5	Port Scan	2	block
6	####	192.168.5.222	NET5	Port Scan	21	block
7	####	192.168.5.222	NET5	Port Scan	23	block
8	####	192.168.5.222	NET5	Port Scan	12	block
9	####	192.168.5.222	NET5	Port Scan	24	block
10	####	192.168.5.222	NET5	Port Scan	22	block
11	####	192.168.5.222	NET5	Port Scan	23	block
12	####	192.168.5.222	NET5	Port Scan	15	block
13	####	192.168.5.222	NET5	Port Scan	11	block
14	####	192.168.5.222	NET5	Port Scan	25	block
15	####	192.168.5.222	NET5	Port Scan	11	block
16	####	192.168.5.222	NET5	Port Scan	23	block
17	####	192.168.5.222	NET5	Port Scan	25	block
18	####	192.168.5.222	NET5	Port Scan	23	block
19	####	192.168.5.222	NET5	Port Scan	11	block
20	####	192.168.5.222	NET5	Port Scan	23	block
21	####	192.168.5.222	NET5	Port Scan	23	block
22	####	192.168.5.1	NET5	ARP Spoofing (Source MAC)	1	block
23	####	192.168.5.222	NET5	Port Scan	11	block
24	####	192.168.5.1	NET5	ARP Spoofing (Source MAC)	1	block
25	####	192.168.5.222	NET5	Port Scan	23	block
26	####	192.168.5.222	NET5	Port Scan	24	block
27	####	192.168.5.70	NET5	Port Scan	224	block
28	####	192.168.5.70	NET5	Port Scan	277	block

安全日志导出（Excel文件）

邮件通知

用户可以选择使用电子邮件地址通知哪些安全威胁。从列表中选择您希望收到的通知。

> **注：**
>
> 必须首先配置电子邮件设置，单击“电子邮件设置”启用和配置电子邮件通知。



电子邮件通知