

2.5 下一代应用安全网关 管理员指南

下一代防火墙防护



趋势科技（中国）有限公司/Trend Micro Incorporated 保留对本文档以及此处所述产品进行更改而不另行通知的权利。在安装并使用产品之前，请阅读自述文件、发布说明和/或最新版本的适用文档，这些文档可以从趋势科技的以下 Web 站点获得：

<http://docs.trendmicro.com/zh-cn/enterprise/deep-edge.aspx>

趋势科技、趋势科技 t 球徽标、趋势科技杀毒专家、TrendLabs、TrendEdge 和云安全智能防护网络是趋势科技（中国）有限公司/Trend Micro Incorporated 的商标或注册商标。所有其他产品或公司名称均为其各自所有者的商标或注册商标。

© 2014 趋势科技（中国）有限公司/Trend Micro Incorporated.保留所有权利。

文档编号：CTCM26326/140304

发布日期：2014 年 3 月

实施保护的美国专利号：专利正在申请。

本文档介绍产品的主要功能和/或适用于生产环境的安装说明。在安装或使用产品之前，请先阅读本文档。

有关如何使用产品中特定功能的详细信息可能位于趋势科技联机帮助中心和/或趋势科技知识库。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，请通过 service@trendmicro.com.cn 与我们联系。我们始终欢迎您的反馈。

目录

关于本手册

关于本手册	ix
下一代应用安全网关文档	x
适用读者	xi
文档约定	xi
关于趋势科技	xii

第 1 章：下一代应用安全网关下一代防火墙

下一代应用安全网关概述	1-2
新增功能	1-2
主要功能	1-6
安全防护	1-6
操作控制	1-6
可见性和监控	1-7
网络连接	1-8

第 2 章：入门

登录到下一代应用安全网关 Web 控制台	2-2
访问入门窗口	2-2
更改下一代应用安全网关系统密码	2-3
配置概述	2-4
操作摘要	2-5

第 3 章：处理和识别网络通信

网络通信概述	3-2
接口	3-2
编辑网络接口	3-2

监控主机	3-3
接口带宽设置	3-4
关于 VLAN	3-4
地址	3-6
关于地址和地址对象	3-6
地址对象参数	3-6
添加地址对象	3-7
配置地址对象	3-8
查看地址对象	3-8
删除地址对象	3-8
部署设置	3-9
关于部署模式	3-9
网桥接口	3-17
关于桥接接口的重要注意事项	3-17
添加网桥	3-18
删除网桥	3-20
路由网络通信	3-20
关于静态路由	3-21
关于基于策略的路由管理	3-23
关于动态路由管理	3-27
网络地址转换 (NAT)	3-40
NAT 规则	3-40
服务	3-44
关于 DNS 转发	3-44
关于 DHCP	3-46
关于动态 DNS	3-48
虚拟专用网络	3-51
用户 VPN	3-51
安全套接层虚拟专用网络	3-55
移动 VPN	3-71
定制 VPN 门户	3-95
站到站 VPN	3-96
IPsec 连接	3-96
站到站 VPN 策略	3-99

高级 IPsec 配置	3-101
IPSec 状态	3-102
IPsec 问题排查	3-102

第 4 章：策略、对象和安全

关于策略	4-2
防火墙策略如何工作	4-2
关于策略规则	4-2
关于策略对象	4-9
关于地址和地址对象	4-10
关于区域和区域对象	4-10
关于服务和服务对象	4-12
关于应用程序和应用程序对象	4-14
关于 URL 类别对象	4-16
关于时间表和时间表对象	4-27
关于处理措施安全配置	4-30
关于安全设置	4-33
网络入侵防御	4-34
入侵防御安全	4-35
防恶意软件安全措施	4-37
反垃圾邮件安全	4-39
Web 信誉服务安全配置	4-44
关于 HTTPS 检查	4-46
HTTPS 检查的常规设置	4-46
关于数字证书	4-47
关于带宽控制	4-52
添加带宽规则	4-52
启用/禁用带宽规则	4-57
关于黑/白名单	4-58
配置黑/白名单	4-58
启用/禁用黑/白名单	4-59
关于防 DoS	4-60
配置 Flood 保护	4-60
添加地址例外	4-61
修改地址例外	4-62

删除地址例外	4-62
关于认证	4-63
用户识别方法	4-64
添加认证规则	4-64
关于网页认证	4-65
关于用户通知	4-67
配置 Web 信誉服务违例通知	4-67
配置 URL 过滤违例通知	4-68
配置应用程序控制违例通知	4-69
配置防恶意软件违例通知	4-69
配置黑名单违例通知	4-70
配置文件扩展名违例通知	4-71
配置入侵防御安全通知	4-72
证书失败通知	4-72

第 5 章：智能日常监控

实时监控和小组件	5-2
关于选项卡	5-2
关于小组件	5-4
使用小组件	5-8
分析和报告	5-30
日志分析	5-31
日志收藏夹	5-34
报告	5-34
管理报告模板	5-36
日志设置	5-38
配置全局日志设置	5-39
设备日志	5-40
审计日志	5-40
系统事件日志	5-41
VPN 日志	5-41
查询日志	5-42
查询审计日志	5-43
查询系统事件日志	5-43
查询 VPN 日志	5-44

第 6 章：管理

切换语言设置	6-2
系统设置	6-2
常规系统设置	6-2
关于位置和时间设置	6-2
关于控制台设置	6-3
关于代理服务器设置	6-4
体验改善	6-5
设备管理	6-5
管理访问权限	6-5
配置 SNMP 设置	6-6
管理帐户	6-7
Web 命令行	6-9
终端用户管理	6-9
关于常规设置	6-9
LDAP 用户识别	6-11
本地用户和组管理	6-13
关于通知	6-19
系统通知和警报	6-19
通知的 SMTP 设置	6-23
产品使用授权	6-24
更新	6-24
设备日志	6-25
邮件隔离	6-25
查询邮件隔离	6-25
配置邮件隔离设置	6-26
系统维护	6-27
执行系统维护	6-27
配置备份与恢复	6-28
诊断	6-29
数据包捕获	6-29
通信跟踪	6-31
生成诊断文件	6-32

支持	6-32
关于下一代应用安全网关	6-33
云安全智能防护网络：基于云的服务	6-33

第 7 章：保持更新

可更新的程序组件	7-2
防恶意软件病毒码文件	7-2
防恶意软件协议特征码文件	7-2
C&C 联系人信息特征码	7-3
入侵防御特征码和引擎	7-3
病毒扫描引擎和特征码	7-3
IntelliTrap 特征码和例外	7-3
间谍软件特征码	7-3
反垃圾邮件特征码和引擎	7-4
Web 信誉服务	7-4
URL 数据库	7-4
电子邮件信誉数据库	7-5
病毒码文件的增量更新	7-5
组件版本信息	7-5
ActiveUpdate	7-5
关于从 Web 控制台更新	7-6
配置用于更新的代理服务器设置	7-6
选择更新源	7-7
手动更新	7-8
应用系统更新	7-8
更新组件	7-9
验证更新是否成功	7-10
关于更新维护	7-10
预设更新	7-11
预设特征码更新	7-11
更新通知	7-12
配置预设更新通知	7-12

第 8 章：产品维护和使用授权

维护协议	8-2
续订维护协议	8-2
产品使用授权	8-3
使用授权过期警告	8-3
获取注册码	8-3
注册下一代应用安全网关	8-4
获取激活码	8-5
更新使用授权	8-5
续订维护协议	8-5

附录 A：技术支持

资源问题排查	A-2
趋势团体	A-2
使用支持门户	A-2
安全智能团体	A-3
威胁百科全书	A-3
联系趋势科技	A-4
加快支持呼叫	A-4
将可疑内容发送给趋势科技	A-5
文件信誉服务	A-5
电子邮件信誉服务	A-5
Web 信誉服务	A-5
其他资源	A-6
TrendEdge	A-6
已知问题	A-6
TrendLabs	A-6

附录 B：日志详细信息

策略强制日志	B-2
应用程序带宽日志	B-3
网络安全日志	B-4
Internet 访问日志	B-6

VPN 日志	B-7
系统事件日志	B-8
审计日志	B-10
审计日志对象	B-12

索引

索引	IN-1
----------	------

前言

关于本手册

欢迎阅读《趋势科技™ 下一代应用安全网关 2.5 管理员指南》。本指南提供了有关下一代应用安全网关下一代防火墙配置选项的详细信息。主题包括管理更新以使风险防护保持最新、使用策略支持安全目标、配置扫描和 URL 过滤以及了解日志和报告。

本前言讨论以下内容：

- [下一代应用安全网关文档](#) 第 x 页
- [适用读者](#) 第 xi 页
- [文档约定](#) 第 xi 页
- [关于趋势科技](#) 第 xii 页

下一代应用安全网关文档

下一代应用安全网关的文档集包括以下内容：

表 1. 下一代应用安全网关文档集

文档	描述
管理员指南	本指南提供了有关下一代应用安全网关下一代防火墙配置选项的详细信息。主题包括管理更新以使风险防护保持最新、使用策略支持安全目标、配置扫描和 URL 过滤以及了解日志和报告。
部署指南	本指南介绍了下一代应用安全网关设备部署模式和初始策略配置。该指南还说明了升级后配置、如何测试安装、如何排除故障以及如何获得技术支持。
快速入门指南	本指南提供有关解包、设置以及登录新的下一代应用安全网关设备的信息。
联机帮助	联机帮助提供的内容与《管理员指南》相同，可以从下一代应用安全网关 Web 控制台访问联机帮助。
自述文件	该文件包含联机或印刷文档中尚未包括的最新产品信息。主题包括新增功能、安装提示、已知问题以及发布历史的描述。
知识库	知识库是包含解决问题和问题排查信息的联机数据库。提供有关已知产品问题的最新信息。要访问知识库，请转到： http://cn.trendmicro.com/cn/support/techsupport/index.html
TrendEdge	TrendEdge 向趋势科技员工、合作伙伴和其他相关方提供了趋势科技产品所不支持的创新技术、工具和最佳实践的相关信息。TrendEdge 数据库包含涵盖各种主题的大量文档。要访问 TrendEdge，请转到： http://trendedge.trendmicro.com

您可以从以下地址获取该文档的最新电子版本：

<http://docs.trendmicro.com/zh-cn/home.aspx>

适用读者

此下一代应用安全网关文档是针对在企业环境中工作的 IT 经理和系统管理员而编写的。本文档假定，读者拥有深厚的网络架构方面的知识和基本网络知识。

文档约定

本文档使用以下约定：

表 2. 文档约定

约定	描述
大写	首字母缩写词、缩写、特定命令名称以及键盘上的键名
粗体	菜单和菜单命令、命令按钮、选项卡和选项
<i>斜体</i>	对其他文档的引用
等宽体	示例命令行、程序代码、Web URL、文件名和程序输出
导航 > 路径	到达特定窗口的导航路径 例如， 文件 > 保存 是指在界面上依次单击 文件 和 保存
 注意	配置注意事项
 提示	建议或意见
 重要信息	有关所需或缺省配置设置和产品限制的信息
 警告!	关键处理措施和配置选项

关于趋势科技

作为云安全方面的全球领先者，趋势科技开发了 Internet 内容安全和威胁管理解决方案，能够使世界环境适合企业和客户交换数字信息。趋势科技拥有 20 年以上的经验，提供排名第一的客户端、服务器和基于云的解决方案，可更快地阻止威胁并保护物理、虚拟和云环境中的数据。

随着新威胁和漏洞的出现，趋势科技将继续致力于帮助客户保护数据、确保合规性、降低成本并维护业务完整性。有关详细信息，请访问：

<http://www.trendmicro.com.cn>

Trend Micro 和 Trend Micro t 球徽标是趋势科技（中国）有限公司/Trend Micro Incorporated 的商标，并已在某些辖区内注册。所有其他标记是其各自公司的商标或注册商标。

第 1 章

下一代应用安全网关下一代防火墙

本章包括以下内容：

- [下一代应用安全网关概述 第 1-2 页](#)
- [新增功能 第 1-2 页](#)
- [主要功能 第 1-6 页](#)

下一代应用安全网关概述

下一代应用安全网关进一步简化了下一代防火墙的部署、配置和管理，将其提高到了一个新的水平。已开启所有功能的高性能扫描可智能地保护网络、端点和服务器环境免受基于 Web、电子邮件和其他网络的恶意活动（包括病毒、蠕虫病毒、间谍软件、bot、特洛伊木马和网络钓鱼欺诈）。下一代应用安全网关还提供了 VPN 连接，以确保与移动设备、公司站点和远程员工的连接安全。所有高级安全功能可在直观且灵活的基于 Web 的控制台上进行轻松配置、部署和查看。

新增功能

此版本的新增功能包括：

表 1-1. 下一代应用安全网关 2.5 的新增功能

功能	描述
双 ISP 和 WAN 支持	<p>下一代应用安全网关现在可以支持双 WAN 或 ISP 连接。</p> <ul style="list-style-type: none">在路由器模式下，下一代应用安全网关 2.5 使用目标或源 IP 地址、服务类型或多个 ISP 或 WAN 的出接口扩展静态和动态路由以及基于策略的路由。有关详细信息，请参阅关于基于策略的路由管理 第 3-23 页。在网桥模式下，下一代应用安全网关 2.5 支持多个桥接的接口。有关详细信息，请参阅网桥接口 第 3-17 页。
增强了 IPS 性能	<p>下一代应用安全网关入侵防御系统 (IPS) 对所有通信执行深度内容检查，以阻止有害活动。下一代应用安全网关 2.5 现在能够扫描具有超过 7000 条轻松配置的预定义 IPS 规则的通信，方法为设置关于严重性级别、受影响的操作系统、发布日期或通信类别的筛选条件。有关详细信息，请参阅入侵防御安全 第 4-35 页。</p>

功能	描述
粒度应用程序控制	应用程序控制对象现在包括应用程序内的特定行为（例如，仅限制视频电话或上传文件），以设置粒度策略规则。
新建定制 URL 类别对象	下一代应用安全网关 2.5 支持定制的 URL 类别对象。有关详细信息，请参阅 添加定制 URL 类别 第 4-25 页。
僵尸网络服务	<p>僵尸网络服务向下一代应用安全网关提供增强的检测功能，可以阻止高风险源的流量，从而减少高级持久性威胁和针对性攻击所造成的损害。</p> <p>新的 C&C 回调尝试 小组件通过提供关于用户、受威胁主机以及下一代应用安全网关强制实施策略操作的方式的行动情报，来跟踪网络中的高级持久性威胁活动。有关详细信息，请参阅僵尸网络 第 5-29 页。</p>
改进了小组件框架	对小组件框架的多项改进提高了实时监控小组件的性能、可靠性和速度。
增强了配置可视性	<p>新的入门指南可用于简化设置流程。直接从 Web 控制台单击入门可查看帮助内容。</p> 
改善了 NAT 规则	每个下一代应用安全网关 2.5 NAT 规则现在都有一个描述参数，可轻松区分多个 SNAT 和 DNAT 配置。
更可靠的日志分析	下一代应用安全网关 2.5 增强了实时监控、日志查询结果和报告中的日志表示。

表 1-2. 下一代应用安全网关 2.1 的新增功能

功能	描述
带宽控制	<p>点对点下载、视频流和即时消息应用程序会消耗网络带宽并影响生产力。下一代应用安全网关 2.1 支持使用带宽控制通过控制通信、减少不必要的网络通信并允许关键网络通信或服务进行相应的带宽分配来减少网络拥塞。有关详细信息，请参阅关于带宽控制 第 4-52 页。</p> <p>除策略设置以外，新增的“带宽控制”小组件可显示受影响的网络通信。有关详细信息，请参阅“带宽控制”小组件 第 5-18 页。</p>
VPN 增强功能	<p>下一代应用安全网关 2.1 增强了 VPN 兼容性：</p> <ul style="list-style-type: none"> • 连接的全部在线用户现已列于在线用户选项卡中 • PPTP VPN 现在支持更大的地址池 • 地址对象现已列在本地网络下拉列表中 <p>有关详细信息，请参阅虚拟专用网络 第 3-51 页。</p>
移动 VPN 兼容性	<p>下一代应用安全网关 2.1 移动 VPN 支持多个本地域名。有关详细信息，请参阅配置高级移动 VPN 设置 第 3-73 页。</p>
本地用户和组	<p>当组织不使用 Active Directory 或 LDAP 认证时，本地用户和组管理允许进行认证。下一代应用安全网关 2.1 的其他增强功能包括：</p> <ul style="list-style-type: none"> • 只有经过认证的本地用户可以访问外部网络 • 策略规则支持本地用户和组选择 • 本地用户管理的改进功能 • VPN 支持 <p>有关详细信息，请参阅本地用户和组管理 第 6-13 页。</p>

表 1-3. 下一代应用安全网关 2.0 的新增功能

功能	描述
HTTPS 检查	下一代应用安全网关中的 HTTPS 检查功能允许您启用或禁用 HTTPS 检查、配置客户端证书请求以及从检查中排除特定 Web 站点、URL 和 IP 地址。有关详细信息，请参阅 关于 HTTPS 检查 第 4-46 页 。
移动 VPN 支持	作为一种网关设备，下一代应用安全网关可为便携机或台式机以及移动设备提供 VPN 服务。移动 VPN 可对 Apple iOS 的“封闭”环境或 Android 的“开源”环境中的移动设备提供支持。有关详细信息，请参阅 移动 VPN 第 3-71 页 。
防 DoS 功能（以及报告）	下一代应用安全网关可阻止拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击，这些攻击会尝试使用户无法使用计算机或网络资源，目的是暂时或无限期中断或挂起已连接到 Internet 的主机的服务。 典型的攻击包括通过外部通信请求使目标计算机达到饱和状态，以致于计算机无法再响应合法的网络通信，或响应极其缓慢，呈现不可用状态。此类攻击通常会导致服务器超负荷。有关详细信息，请参阅 关于防 DoS 第 4-60 页 。
终端用户通知	下一代应用安全网关针对以下策略的违例提供终端用户通知： Web 信誉服务 (WRS) 、 URL 过滤 、 防恶意软件 、 加入黑名单的 URL 、 文件扩展名检测 、 入侵防御 和 证书失败 （服务器和客户端）。有关详细信息，请参阅 关于用户通知 第 4-67 页 。
电子邮件安全解决方案	下一代应用安全网关会处理并扫描 SMTP 或 POP3 电子邮件，然后清除受感染的电子邮件并进行投递，或者对违例电子邮件执行已在策略中设置的用户选定的处理措施。可以稍后隔离和投递电子邮件。有关详细信息，请参阅 反垃圾邮件安全配置 第 4-40 页 。
SSL VPN 增强功能	下一代应用安全网关支持安全套接层虚拟专用网络 (SSL VPN)，这是一种可以与标准 Web 浏览器一起使用的 VPN 形式。下一代应用安全网关 SSL VPN 解决方案要求安装客户端软件，是包括基于 Web 的电子邮件、企业和政府目录、文件共享、远程备份、远程系统管理以及消费类电子商务在内的应用程序的理想选择。有关详细信息，请参阅 安全套接层虚拟专用网络 第 3-55 页 。

主要功能

下表介绍了下一代应用安全网关解决方案中的关键部分。所有技术组件均设计为方便集成，并经优化以提升性能。通过集成和优化，在开启所有安全功能的同时，仍可以提供优异的产品性能。

安全防护

功能	描述
高级防火墙	轻松部署和管理下一代防火墙功能。高级防火墙会在允许良好的应用程序网络通信通过的同时阻止攻击。
IPS/IDS	当许多活动威胁、漏洞利用、后门程序和其他攻击（包括 DoS 和 DDoS 攻击）通过设备时，可以识别并进行阻止。通过对防火墙所允许的网络通信进一步检查以确保其不包含有害威胁，入侵防御系统和入侵检测系统 (IPS/IDS) 可以增强防火墙安全策略。
Web 防护	使用趋势科技 Web 信誉技术控制针对恶意 Web 站点的防护级别。
防病毒	通过高速扫描应用程序内容，利用多个安全组件和病毒防护保护客户，不仅缩短了延迟，同时还改善了用户体验。
反垃圾邮件	利用趋势科技电子邮件信誉服务 (ERS) 和集成的高速反垃圾邮件引擎来根据邮件发件人的信誉和电子邮件内容检测、阻止或隔离垃圾电子邮件。
ActiveUpdate	实现从云安全智能防护网络对本地病毒、协议、间谍软件、入侵防御、IntelliTrap 和反垃圾邮件特征码文件的按需更新或实时更新。

操作控制

功能	描述
应用程序控制	自动发现热门 Internet 应用程序，并使用策略控制对这些应用程序的访问。

功能	描述
URL 过滤	为不同的安全配置创建和配置唯一的 URL 过滤步骤。URL 过滤以及 Web 信誉服务都是多层次、多威胁防护解决方案的一部分。
LDAP 集成	与轻量级目录访问协议 (LDAP) (包括 Active Directory 和 OpenLDAP) 集成, 以创建特定于用户或组的策略。事件日志和报告使用 LDAP 用户名和组来识别用户。

可见性和监控

功能	描述
摘要实时监控	定制要选择的实时监控, 使用小组件深化并显示安全和网络通信信息。
应用程序带宽监控	利用应用程序控制和 LDAP 集成, 记录和监控网络中带宽使用最高的用户。通过确定带宽使用最高的用户以及所使用的会加重网络负荷的应用程序来通知管理者相关滥用情况。
系统通知和警报	<p>发送以下项目的安全相关事件的电子邮件通知 (警报):</p> <ul style="list-style-type: none"> • 防火墙 • Web 信誉服务 (WRS) • 恶意软件 • 入侵防御 (IPS) • 硬件监控异常 • URL 过滤 • 应用程序控制违例 <p>通知可直接发送给终端用户, 允许用户在不影响 IT 管理员的情况下采取纠正措施。</p>
报告	生成有关检测到的恶意软件和恶意代码、阻止的文件以及访问的 URL 的报告, 用于优化程序设置, 并对安全策略进行调整。

功能	描述
日志	根据针对每种风险类型指定的设置，检测安全风险并采取相应操作。这些事件将记录在日志中。

网络连接

功能	描述
网络配置	查看和编辑检测到的网络接口，或修改物理 L2 和 L3 端口的配置。L3 端口支持以下配置： <ul style="list-style-type: none"> • 动态主机配置协议 (DHCP) • 按 IP 地址和网络掩码进行静态路由的配置 • 以太网点对点协议 (PPPoE)
桥接	将两个接口透明地桥接到一起，并过滤网络通信以保护端点和服务器，从而使对现有网络环境的影响最小。跨树协议 (STP) 可确保所有桥接的以太网局域网实现无环回逻辑拓扑结构。
路由	配置静态和动态路由，包括路由信息协议 (RIP) 以及开放最短路径优先协议 (OSPF)。
NAT	配置网络地址转换 (NAT) 策略来指定源或目标 IP 地址和端口是否在公共和私有地址和端口之间转换。
服务	配置下列服务： <ul style="list-style-type: none"> • 域名服务器 (DNS) 转发 • 动态主机配置协议 (DHCP) 服务器 • 动态 DNS (DDNS) 设置
用户 VPN	配置使用点对点隧道协议 (PPTP) 的虚拟专用网络 (VPN) 和安全套接层虚拟专用网络 (SSL VPN)。
站到站 VPN	使用 Internet 密钥交换 (IKE) 协议和 IP 安全 (IPSec) 协议创建加密的 L3 隧道。

功能	描述
移动 VPN	允许 iPhone 和 Android 移动设备用户通过利用内置 IPsec VPN 客户端轻松并安全地重新连接到公司环境。移动设备上不需要安装任何代理。

第 2 章

入门

“入门”介绍了首次使用下一代应用安全网关时如何开始。请务必先阅读《下一代应用安全网关部署指南》，然后再阅读《下一代应用安全网关管理员指南》继续操作。如果您要从先前的下一代应用安全网关版本升级，或更新现有配置的组件，请参阅[保持更新 第 7-1 页](#)。

主题包括：

- [登录到下一代应用安全网关 Web 控制台 第 2-2 页](#)
- [访问入门窗口 第 2-2 页](#)
- [更改下一代应用安全网关系统密码 第 2-3 页](#)
- [配置概述 第 2-4 页](#)
- [操作摘要 第 2-5 页](#)

登录到下一代应用安全网关 Web 控制台

登录到下一代应用安全网关以设置部署模式。

过程

1. 使用地址 `https://<appliance_IP_address>:8443`。

指定在安装过程中提供的 IP 地址。



重要信息

记住要在 `https://` 中包含 “s”

2. 指定管理员凭证。

缺省凭证：

用户名: `admin`

密码: `adminDeepEdge`

3. 按 ENTER 键，或单击**登录**。
-

访问入门窗口

新的入门窗口使安装过程更加直观明白。有关部署下一代应用安全网关的详细信息，请参阅《下一代应用安全网关部署指南》。

过程

1. 登录到 Web 控制台。

请参阅 [登录到下一代应用安全网关 Web 控制台 第 2-2 页](#)。

2. 直接从 Web 控制台单击**入门**可查看帮助内容。



此时将显示入门窗口。

更改下一代应用安全网关系统密码

安装下一代应用安全网关后或者系统安全可能已受到威胁时，应更改下一代应用安全网关系统密码。

过程

1. 登录到下一代应用安全网关 Web 控制台。
请参阅 [登录到下一代应用安全网关 Web 控制台 第 2-2 页](#)。
2. 单击窗口顶部的**更改密码**。



此时将显示**更改密码**窗口。

3. 指定旧密码和新密码。

4. 单击应用。

配置概述

下表介绍了开始使用下一代应用安全网关需要、建议和可选的设置。查看配置概述后，请参阅[操作摘要 第 2-5 页](#)开始配置您的下一代应用安全网关设备。

表 2-1. 所需配置

配置	参考资料
配置 DNS	常规系统设置 第 6-2 页
激活使用授权	产品使用授权 第 8-3 页
设置缺省网关	添加静态路由 第 3-21 页.

表 2-2. 建议的配置

配置	参考资料
更改 Web 控制台密码	更改下一代应用安全网关系统密码 第 2-3 页
设置位置和时间	配置时间和日期设置 第 6-3 页
启用体验改善	体验改善 第 6-5 页
配置反垃圾邮件和白名单	关于黑/白名单 第 4-58 页

表 2-3. 可选配置

配置	参考资料
切换语言设置	切换语言设置 第 6-2 页
配置代理服务器设置	配置代理服务器设置 第 6-4 页
为内部地址添加地址对象	关于地址和地址对象 第 3-6 页
配置带宽设置	关于带宽控制 第 4-52 页

配置	参考资料
端点用户	终端用户管理 第 6-9 页

操作摘要

以下步骤介绍了首次使用下一代应用安全网关所需的基本配置。有关部署下一代应用安全网关的详细信息，请参阅《下一代应用安全网关部署指南》。

过程

1. 设置缺省路由。
请参阅 [添加静态路由 第 3-21 页](#)。
2. 配置系统设置。
 - 有关主机名和 DNS 设置，请参阅[常规系统设置 第 6-2 页](#)。
 - 有关位置和时间设置，请参阅[配置时间和日期设置 第 6-3 页](#)。
3. 选择部署模式并配置设置。
 - 有关网桥模式，请参阅[网桥接口 第 3-17 页](#)。
 - 有关路由器模式，请参阅[路由网络通信 第 3-20 页](#)。



注意

有关部署模式和所需设置的其他要求，请阅读《下一代应用安全网关部署指南》的“部署模式配置”一章。

4. 可选：设置管理接口 IP 地址。
请参阅 [编辑网络接口 第 3-2 页](#)。
5. 可选：配置代理服务器设置。
请参阅 [配置代理服务器设置 第 6-4 页](#)。

6. 配置策略和安全。

请参阅 [策略、对象和安全](#) 第 4-1 页。



注意

有关建议的策略配置，包括 DMZ 网络中的配置，请阅读《下一代应用安全网关部署指南》中的“安全策略配置”一章。

7. 配置带宽控制。

请参阅 [关于带宽控制](#) 第 4-52 页。

8. 配置 VPN 访问。

请参阅[虚拟专用网络](#) 第 3-51 页

9. 配置用户认证。

请参阅 [关于认证](#) 第 4-63 页。

第 3 章

处理和识别网络通信

本章包括以下内容：

- [网络通信概述](#) 第 3-2 页
- [接口](#) 第 3-2 页
- [部署设置](#) 第 3-9 页
- [网桥接口](#) 第 3-17 页
- [路由网络通信](#) 第 3-20 页
- [关于静态路由](#) 第 3-21 页
- [关于动态路由管理](#) 第 3-27 页
- [网络地址转换 \(NAT\)](#) 第 3-40 页
- [服务](#) 第 3-44 页
- [虚拟专用网络](#) 第 3-51 页
- [站到站 VPN](#) 第 3-96 页

网络通信概述

本部分介绍了如何将下一代应用安全网关配置为在网络中运行。基本网络设置包括配置下一代应用安全网关接口。更高级的配置包括下一代应用安全网关网络的路由器、网桥、VLAN、网络地址转换 (NAT)、广域网 (WAN)、服务以及虚拟专用网络 (VPN) 设置。

接口

安装完成后，可以在 Web 控制台的**网络 > 接口**下查看并编辑自动检测到的下一代应用安全网关网络接口。下一代应用安全网关支持修改物理 L2 和 L3 端口的配置。对于 L3 配置，下一代应用安全网关可提供动态主机配置协议 (DHCP) 配置以及按 IP 地址和网络掩码进行静态路由的配置。以太网点对点协议 (PPPoE) 是 L3 端口的另一种选择。

编辑网络接口

下一代应用安全网关会自动检测 L2 和 L3 接口。

过程

1. 转到**网络 > 接口**以查看所有下一代应用安全网关网络接口。
2. 在**名称**列中单击一个接口。
3. 根据需要，更改以下基本设置：
 - **名称**
 - **类型**: L2、L3
 - **模式**: 静态、DHCP、PPPoE
 - **IPv4 地址**
 - **IPv4 网络掩码**

- **管理访问权限：** Web 控制台、Ping、SSH 和 SNMP



有关控制管理访问权限的信息，请参见[管理访问权限 第 6-5 页](#)。

4. 在**监控设置**下，配置监控主机。
请参阅 [监控主机 第 3-3 页](#)。
5. 在**带宽设置**下，指定允许的最大上行和下行带宽。
请参阅 [接口带宽设置 第 3-4 页](#)。
6. 单击**应用**。
7. 在**网络 > 接口**下的接口列表中验证更新。

监控主机

下一代应用安全网关通过对每个出接口的相应监控 IP 地址或主机名执行 ping 操作检查 WAN 是否运行。如果监控主机无法连接，则会禁用任何与该接口相关联的静态路由或基于策略的路由。如果网络通信与其他路由匹配，则网络通信会路由至其他静态路由或基于策略的路由。如果网络通信与其他路由不匹配，则会通过缺省网关路由网络通信或放弃网络通信。

要配置监控主机，请参阅[编辑网络接口 第 3-2 页](#)。

有关缺省网关的信息，请参阅[添加静态路由 第 3-21 页](#)。

要配置基于策略的路由，请参阅[添加基于策略的路由 第 3-25 页](#)。

有关自动故障转移的信息，请参阅[多个 ISP/WAN 环境自动进行故障转移 第 3-25 页](#)。

接口带宽设置

配置接口带宽设置，以设置下行和上行流量的最大阈值。带宽控制策略不能超过接口带宽阈值。缺省情况下，下一代应用安全网关不会限制带宽。可为每个接口配置不同的阈值。

接口带宽设置分配不正确时可能会发生网络拥塞。趋势科技建议将接口带宽设置为接口允许的最大阈值，然后设置带宽控制策略，以决定哪个网络通信具有更高优先级。有关带宽控制策略的详细信息，请参阅[关于带宽控制 第 4-52 页](#)。

要配置接口带宽设置，请参阅[编辑网络接口 第 3-2 页](#)。

关于 VLAN

一个虚拟局域网 (VLAN) 由一组端点、服务器和其他网络设备组成，这些设备可以彼此进行通信，就像在同一个 LAN 网段中一样，而不管其位置如何。即使端点和服务器分散在一个地理位置中并连接到多个网段，它们仍属于同一个 VLAN。

VLAN 将以逻辑方式而不是物理方式隔离各个设备。每个 VLAN 都视为一个广播域。VLAN 1 中的设备可以与 VLAN 1 中的其他设备连接，但不能与其他 VLAN 中的设备连接。一个 VLAN 中各个设备之间的通信是独立于物理网络的。

一个 VLAN 通过在该 VLAN 中的设备发送和接收的所有数据包中添加 802.1Q VLAN 标记来隔离这些设备。VLAN 标记是由 4 个字节组成的帧扩展，它包含 VLAN 标识符以及其他信息。

添加 VLAN 子接口




重要信息

每个 VLAN 子接口的 VLAN ID 必须与 IEEE 802.1Q 兼容的路由器添加的 VLAN ID 相匹配。VLAN ID 可以是 1 到 4094 之间的任意数字（0 和 4095 已保留）。为每个 L3 VLAN 子接口配置唯一的 IP 地址和网络掩码。

将 VLAN 子接口添加到用于接收标记了 VLAN 的数据包的物理接口。

过程

1. 要查看所有下一代应用安全网关网络接口，请转到**网络 > 接口**
2. 在**操作**列中单击 VLAN 添加配置图标 .
3. 指定下列信息：

选项	说明
名称	命名 VLAN 子接口。
类型	自动显示为 L2 VLAN 或 L3 VLAN，具体取决于父接口。
模式	对于 L3 接口，请使用 模式 下拉列表来设置子接口是使用动态地址，还是使用静态地址。
VLAN ID	指定与此 VLAN 子接口接收的数据包的 VLAN ID 相匹配的 VLAN ID。您无法更改现有 VLAN 子接口的 VLAN ID。VLAN ID 可以是 1 到 4094 之间的任意数字，并且必须与 IEEE 802.1Q 兼容的路由器或连接到 VLAN 子接口的交换机添加的 VLAN ID 相匹配。

4. 单击**应用**。

地址

地址可确定内部网络 IP 地址范围。缺省情况下，下一代应用安全网关允许所有内部 IP 地址范围。根据内部网络要求配置设置。下一代应用安全网关支持单个 IP 地址，"." 作为范围标记和 IP 地址/网络掩码 (192.168.1.1/24)。

关于地址和地址对象

地址对象影响策略和网络设置。地址对象可确定内部网络中允许的 IP 地址范围。缺省情况下，下一代应用安全网关包括所有内部 IP 地址范围。要为特定源或目标地址设置安全策略，首先请在网络设置中定义地址和地址范围。


转到**网络 > 地址**。

地址对象参数

使用以下信息来定义配置地址对象参数可简化安全策略的创建。
要创建地址对象，请指定以下信息。

表 3-1. 地址对象参数

参数	描述
名称	指定描述要定义的地址的名称。定义安全策略时，此名称将出现在地址列表中。此名称区分大小写，且必须是唯一的。仅使用字母、数字、空格、连字符和下划线。
协议	指定是使用 IPv4 地址还是 IPv6 地址。

参数	描述
IP 地址	<p>IPv4 地址:</p> <p>使用以下表示法指定地址或网络:</p> <ul style="list-style-type: none"> • ip_address • ip_address/bitmask <hr/> <p> 注意</p> <p>位掩码指用于地址的网络部分的有效二进制位数。</p> <hr/> <ul style="list-style-type: none"> • IP 地址范围, 如: 192.168.1.1-192.168.1.10 <p>例如:</p> <p>192.168.80.150/32 表示一个地址, 而 192.168.80.0/24 表示从 192.168.80.0 到 192.168.80.255 的所有地址</p> <p>IPv6 地址</p> <p>指定 IPv6 地址或带有前缀的 IPv6 地址。例如: 2001:db8:123:1::1 或 2001:db8:123:1::/64</p>

添加地址对象

过程

1. 转到**网络 > 地址**。
2. 单击**添加**。
3. 指定网络的 IP 地址、IP 地址范围, 或 IP 地址和网络掩码。
4. 单击**应用**。

配置地址对象

过程

1. 转到**策略 > 对象 > 地址**。
 2. 单击**新增**。
 3. 为地址对象指定名称。
 4. 从下拉列表框中选择合适的协议版本。
 5. 指定 IP 地址或 CIDR 网络（单个或多个以逗号分隔）。
例如：192.168.0.1 或 10.0.0.1-10.0.0.4 或 10.0.0.8
 6. 单击**确定**。
 7. 验证新的地址对象是否显示在**策略 > 对象 > 地址**的列表中。
-

查看地址对象


过程

- 转到**网络 > 地址**。
-

删除地址对象

过程

1. 转到**网络 > 地址**。

2. 选中要删除的对象所在行对应的复选框。
3. 单击**删除**图标 。
4. 在确认对话框中单击**删除**。
5. 验证删除的地址对象是否在**网络 > 地址**列表中。

部署设置

下一代应用安全网关提供了两种部署模式：监控模式和接入模式。下一代应用安全网关还支持添加内部地址。

关于部署模式

本节概述了下一代应用安全网关的工作模式，以及如何为每个模式配置下一代应用安全网关。

根据网络基础架构和要求，下一代应用安全网关会在两种不同的接入模式下运行。使用路由器模式和网桥模式进行网络通信检查，并基于策略采取适当的处理措施。它们支持相同的网络安全功能。使用监控模式可评估在路由器模式或网桥模式下部署时安全策略可能会有哪些效果。

表 3-2. 部署模式

模式	目的
网桥	下一代应用安全网关设备对于网络不可见。它的所有接口都位于相同的子网中。您只需配置管理 IP 地址便可进行配置更改。通常，您应通过现有防火墙或路由器在专用网络中使用网桥模式。有关详细信息，请参阅 网桥模式概述 第 3-10 页 。

模式	目的
路由	下一代应用安全网关设备对于网络可见。它的所有接口都位于不同的子网中。连接到网络的每个接口都必须配置有对该网络有效的 IP 地址。通常，如果将下一代应用安全网关设备部署为专用网络和公共网络之间的网关，则应使用路由器模式。有关详细信息，请参阅 路由器模式概述 第 3-12 页 。
监控	监控模式设计为在生产网络中评估下一代应用安全网关，而不会阻止任何网络通信或使下一代应用安全网关成为网络流中的一个故障点。在监控模式下，下一代应用安全网关仅将策略应用于镜像的网络通信以生成日志和报告，但不会对网络通信强制实施任何阻止处理措施。有关详细信息，请参阅 监控模式概述 第 3-14 页 。

关于接入模式

接入模式允许下一代应用安全网关主动检查通过网络的网络通信。

网桥模式概述

在网桥模式下，下一代应用安全网关在网络上不可见，它充当网络设备（交换机、路由器或防火墙）之间的第 2 层网桥，并透明地扫描两个方向的网络通信。网桥模式是将下一代应用安全网关部署到现有网络拓扑中的最简单方式，该模式不需要对客户端、路由器或交换机进行修改。下一代应用安全网关充当

“嵌入式串接装置 (BITW)” 并扫描恶意软件。图 3-1：网桥模式下的下一代应用安全网关 第 3-11 页说明了网桥模式下的下一代应用安全网关。

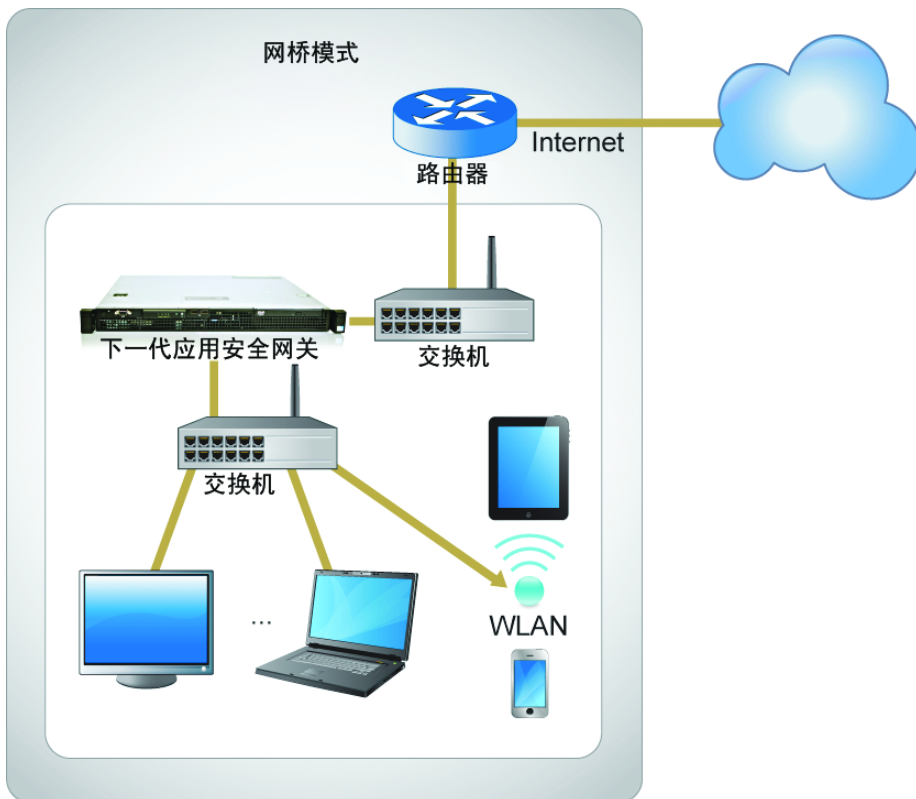


图 3-1. 网桥模式下的下一代应用安全网关

与使用网桥相似，所有下一代应用安全网关接口必须位于同一子网上。配置网桥模式需要两个网卡：一个供内部使用，一个供外部使用。您还可以在网桥上配置 IP 地址以管理下一代应用安全网关以用于预设特征码更新，并利用云中的趋势科技云安全智能防护网络™的实时安全信息功能。

当下一代应用安全网关通过现有防火墙或路由器在专用网络中运行时配置网桥模式，这样下一代应用安全网关便可透明地执行所有扫描功能。

有关配置网桥模式的详细信息，请参阅[网桥接口 第 3-17 页](#)。

路由器模式概述

在路由器模式下，下一代应用安全网关在网络上可见，并充当具有网络通信流扫描功能的第 3 层路由设备。在路由器模式下部署需要配置两个网络接口：一个供内部使用，一个供外部使用。所有接口都位于不同的子网上，这使您能够使单个 IP 地址可用于公用 Internet。下一代应用安全网关可以在将数据包发送到目标网络和接收数据包并充当路由器的角色之前，执行网络地址转换。

下一代应用安全网关还提供以太网上的点对点协议 (PPPoE) 功能以支持通过非对称数字用户线路 (ADSL) 拨号到 ISP。查看下图了解典型部署。[图 3-2: 路由](#)

器模式下的下一代应用安全网关 第 3-13 页说明了路由器模式下的下一代应用安全网关：

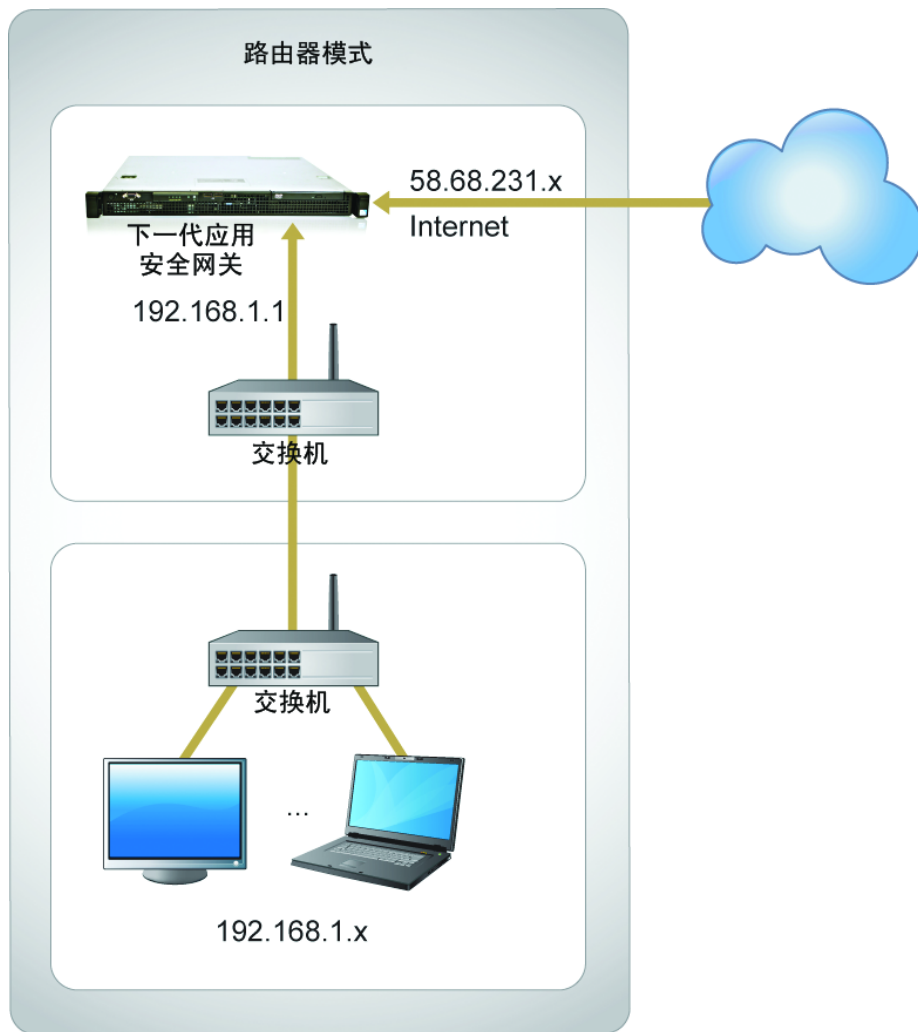


图 3-2. 路由器模式下的下一代应用安全网关

当下一代应用安全网关用作专用网络和公用网络之间的网关时，配置路由器模式。在此配置中，您必须创建 NAT 模式防火墙策略来控制内部网络、专用网络与外部网络、公用网络（通常为 Internet）之间的网络通信流。

关于监控模式

监控模式提供了一种用于访问网络上的数据流的方法。通过在监控模式下进行部署，下一代应用安全网关可以被动监控通过交换机 SPAN 或镜像端口的网络通信。

SPAN 或镜像端口允许复制交换机上其他端口中的网络通信。通过将防火墙中的某个接口专门用作“监控模式”接口并将该接口连接至交换机 SPAN 端口，交换机 SPAN 端口可为防火墙提供镜像网络通信。这使得应用程序在网络内可见，而无需进入网络通信流中。



注意

在监控模式下进行部署时，防火墙无法采取阻止网络通信等处理措施。

监控模式概述

监控模式设计为在生产网络中评估下一代应用安全网关，而不会阻止任何网络通信或使下一代应用安全网关成为网络流中的一个故障点。在监控模式下，下一代应用安全网关对于网络不可见。在网络交换机上建立正确的监控设置，以将网络通信镜像到与下一代应用安全网关连接的端口。下一代应用安全网关会将策略应用于镜像的网络通信，但仅记录与违例相关的信息。在此模式下，策

略永远不会阻止网络通信。图 3-3：监控模式下的下一代应用安全网关 第 3-15 页说明了监控模式下的下一代应用安全网关：

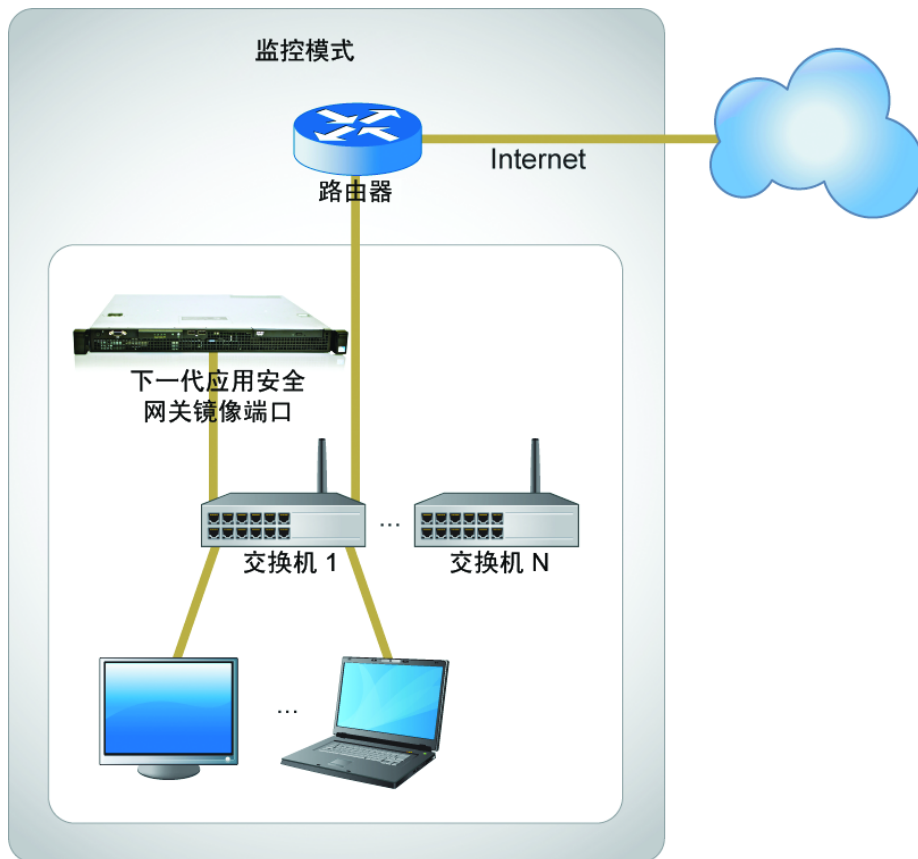


图 3-3. 监控模式下的下一代应用安全网关

在监控模式下，网络通信不会直接通过下一代应用安全网关。下一代应用安全网关在由网络交换机（在逻辑上）辅助的网络外部独立运行，这些交换机将指定的网络通信镜像到下一代应用安全网关侦听的接口。下一代应用安全网关监控网络通信的状态并向下一代应用安全网关用户提供该信息。

为了看到离开和进入网络的所有 Internet 网络通信的副本，趋势科技建议在核心 Internet 交换机处部署下一代应用安全网关。下一代应用安全网关至少需要两个网络接口才能在监控模式下正常运行。除了下一代应用安全网关用于侦听网络通信的接口之外，还应该存在另一个连接，以供下一代应用安全网关访问 Internet 并连接到 ActiveUpdate 和 Web 信誉服务查询服务器，以及下一代应用安全网关提供的其他云防护源。

监控模式通常在以下情况下使用：

- 网络已经部署相关设备（防火墙、IDPS），但看不到整体网络状态。在这种情况下，下一代应用安全网关提供可见性，而不会明显更改网络拓扑。
- 在部署下一代应用安全网关接入之前，监控模式可以帮助评估下一代应用安全网关设备。在了解了下一代应用安全网关提供的安全益处之后，您可以从监控模式更改为网桥模式或路由器模式，以进行真正的接入保护。

配置部署模式设置

过程

1. 转到**网络 > 部署**。
2. 单击**部署模式**选项卡。
3. 选择相应模式的单选按钮：

选项	说明
接入模式	有关详细信息，请参阅 关于接入模式 第 3-10 页 。
监控模式	有关详细信息，请参阅 关于监控模式 第 3-14 页 。

- a. 对于监控模式，单击要在脱机模式中使用的接口的名称右侧的 (+)。它将移动到表的左侧列中。如果需要，请单击 (-) 将其移回原位。使用**全部添加**链接将所有接口移动到左侧，以便在监控模式中使用所有接口。
4. 单击**应用**。

网桥接口

网桥使用相同协议连接两个接口，从而在桥接的接口之间透明地传递网络通信。在网桥模式下，下一代应用安全网关在网络上不可见，它充当网络设备（交换机、路由器或防火墙）之间的第 2 层网桥，并透明地扫描两个方向的网络通信。



注意

要从趋势科技接收安全更新，请确保管理接口可以访问 Internet。

下一代应用安全网关支持双链接以配置连接到设备的多个 WAN/ISP。下一代应用安全网关有两个进站链接和两个出站链接。添加多个网桥以支持多个 ISP 或 WAN。在 L3 路由器管理网络通信时，两个 ISP 之间的下一代应用安全网关是透明的。

下一代应用安全网关支持跨树协议 (STP)，此协议可确保所有桥接的以太网局域网实现无环回逻辑拓扑结构。

关于桥接接口的重要注意事项

选择两个不同的接口以形成一个网桥。尽管所有的 L2 和 L3 接口都可以选择，但不同的组合会产生不同的行为：

- 如果接口 1 和接口 2 都是 L2 接口，这两个接口会添加到网桥中。
- 网桥的 IP 地址和网络掩码是可选的。
- 在创建网桥时使用的任何 L3 接口都将降级为 L2 接口类型。
- 如果 L3 接口被 NAT、DHCP 和动态 DNS 等服务引用，则只有在移除该引用关系之后才可以将该接口添加到网桥中。



注意

如果还存在其他已配置的 L3 接口具有 Web 控制台的访问权限，则网桥的 IP 地址和网络掩码是可选的。否则，Web 控制台访问可能无法访问下一代应用安全网关。用户必须访问 CLI 以修复此状况。

添加网桥

有关网桥模式的概述，请参阅[网桥模式概述 第 3-10 页](#)。

过程

1. 转到**网络 > 部署**，并确认选中了**接入模式**单选按钮。
2. 转到**网络 > 网桥**。
3. 单击**新增**。

将显示**添加/编辑网桥**窗口。

4. 指定网桥名称。
 5. 从**接口 1**和**接口 2**下拉列表框中，选择要桥接的接口。
-



注意

这些桥接接口应该与网络的可信端和不可信端相对应，以便数据可以在 Internet 与内部系统之间传递。

6. 根据网络环境，在**网桥绑定 IP 配置**下指定以下参数：
 - IPv4 地址
 - IPv4 网络掩码
 - IPv6 地址/网络掩码
 - 管理访问权限：Web 控制台、Ping、SSH 和 SNMP

**注意**

有关控制管理访问权限的信息，请参见[管理访问权限 第 6-5 页](#)。

**注意**

如果还存在其他 L3 接口具有 Web 控制台的访问权限，则网桥 IP 地址和网络掩码是可选的。

7. 要确保桥接网络的无环回逻辑拓扑结构，请选中**启用生成树协议**。
8. 要确保连接设备了解高可用性网络的链接状态，请选中**启用链接损耗转发**。
有关链接损耗转发的信息，请参阅[链接丢失转发 第 3-19 页](#)。
9. 单击**应用**。

链接丢失转发

链接丢失转发可在一个接口故障时禁用两个桥接的接口，以确保高可用性。信号链接的所有故障都会通过，并可通过连接的设备进行查看。禁用链接丢失转发后，其中一个桥接的接口发生故障不会禁用其他接口，因此连接的设备不知道链接已丢失。

桥接的接口信号链接恢复后，下一代应用安全网关监控并启用该接口。

配置管理服务

配置管理服务可允许远程访问下一代应用安全网关。已配置 IP 地址的所有网桥都将显示在**管理设置**下的表中。如果未配置网桥，则接口将不会显示。有关管理接口设置的详细信息，请参阅[设备管理 第 6-5 页](#)。

过程

1. 转到**管理 > 设备管理**。
2. 在**管理设置**下，找到网桥接口，并选择以下一个或多个选项：


- Web 控制台
- Ping
- SSH
- SNMP

3. 单击**应用**。

删除网桥

移除网桥会移除该网桥的 ACL 设置。该网桥的 IP 地址设置也会被删除。如果还存在其他 L3 接口具有 Web 控制台的访问权限，则网桥的 IP 地址和网络掩码是可选的。如果没有，这可能会导致失去对下一代应用安全网关 Web 控制台的访问权限。用户可以访问 CLI 修复此状况。

过程

1. 转到**网络 > 网桥**。
 2. 选中网桥旁的复选框。
 3. 单击 **删除**。
 4. 在显示确认消息时，单击**删除**。
-

路由网络通信

下一代应用安全网关在网络中可作为安全设备使用，数据包必须经过它。必须了解某些基本路由概念才能相应地配置下一代应用安全网关单元。

下一代应用安全网关支持在**网络 > 路由**中配置静态、动态和基于策略的路由。下一代应用安全网关支持将这些动态协议用于 IPv4 和 IPv6：

- 路由信息协议 (RIP)

- 开放最短路径优先协议 (OSPF)

下一代应用安全网关选择路由并基于指定规则动态更新其路由表。基于给定的一组规则，该单元可以确定将数据包发送到目标位置的最佳路由或路径。有关路由网络通信的详细信息，请参阅[路由器模式概述 第 3-12 页](#)

关于静态路由

静态路由可控制网络通信如何在连接到网络的端点之间移动。定义一个静态路由，为下一代应用安全网关提供将数据包转发到某个特定目标所需的信息。通过定义希望下一代应用安全网关设备截获的数据包的目标 IP 地址和网络掩码并指定这些数据包的网关 IP 地址，来配置静态路由。网关地址指定网络通信将路由到的下一跳地址路由器。

您可以指定数据包将通过哪个接口离开以及要将数据包路由到哪个设备。**网络 > 路由 > 静态路由**下的“静态路由”列表显示了下一代应用安全网关设备与数据包头进行比较以路由数据包的信息。

添加静态路由

添加新的静态路由时，下一代应用安全网关会检查下一代应用安全网关路由表中是否已存在匹配的路由和目标。如果未找到任何匹配项，下一代应用安全网关会将该路由添加到路由表中。

要配置 IPv6 静态路由，请在“协议”下拉列表框中选择 **IPv6**。

过程

1. 转到**网络 > 路由 > 静态路由**。

2. 单击**新增**添加缺省路由。

将显示**添加/编辑静态路由**窗口。

3. 选择**启用静态路由**。

4. 在**网络**中，指定网络地址。

以下任一选项均有效：

- **IP 地址**
- **缺省网关**（例如：0.0.0.0/0）



注意

如果已配置多个缺省网关，则通过这些网关以循环方式路由传出网络通信。

- **位掩码**





注意

位掩码是网络掩码的十进制等效值。

- **类域间路由 (CIDR) 表示法**（例如：255.255.255.0/24）
5. 在**下一跳地址**中，指定下一跳 IP 地址。
 6. 单击**应用**。
-


启用/禁用静态路由

过程

1. 转到**网络 > 路由 > 静态路由**。
 2. 在静态路由列表中，请执行以下操作之一：
 - 选择**启用**图标 () 以启用静态路由。
 - 取消选择**启用**图标 () 以禁用静态路由。
-

修改静态路由

过程


1. 转到**网络 > 路由 > 静态路由**。
2. 执行下列操作之一：
 - 在**路由 ID**列中，单击路由名称。
 - 在**处理措施**列中，单击编辑图标 。

将显示**添加/编辑静态路由**窗口。

3. 更改“网络”和“下一跳地址”值。
 4. 单击**应用**。
-

删除静态路由

过程

1. 转到**网络 > 路由 > 静态路由**。
 2. 在**处理措施**列中，单击删除图标 。
 3. 单击**删除**以确认删除。
-

关于基于策略的路由管理

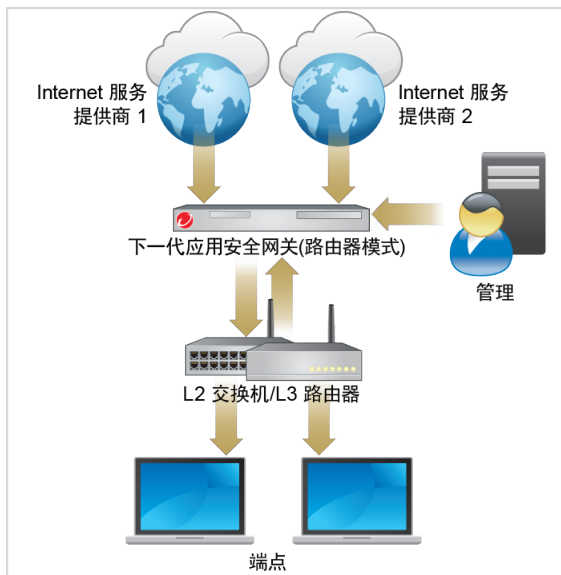
在当今的高性能网络中，组织希望根据自己定义的策略灵活执行数据包转发和路由，而不是按照传统路由协议中的方式。静态和动态路由专注于要路由的网络通信目标，而基于策略的路由提供了一个可以标记数据包的机制，以便某些类型的网络通信接收不同的路由。基于目标的路由技术很难更改特定网络通信

的路由行为。基于策略的路由（也称为“智能路由”）允许您基于多个不同的标准（包括源接口、源或目标地址或服务类型）而不是目标网络来确定路由行为。

例如，公司的不同位置之间有两条链接，其中一条是高带宽、低延迟、较昂贵的链接，另一条是低带宽、高延迟、较便宜的链接。使用传统路由协议时，根据链接的带宽和/或延迟特征（使用 EIGRP 或 OSPF）获得的度量节省，带宽较高的链接将占用通过其发送的大部分（如果不是全部的话）网络通信。基于策略的路由可通过高带宽/低延迟链接路由由优先级较高的网络通信，而通过低带宽/高延迟链接发送所有其他网络通信。

使用基于策略的路由，下一代应用安全网关可路由多个 ISP 和 WAN 的网络通信。下图显示了如何使用 L2 交换机为两个 ISP 配置下一代应用安全网关。

图 3-4. 基于策略的路由示例



如果一个接口的监控 IP 地址不可用，则会禁用与该接口相关联的所有基于策略的路由。通过缺省网关路由与基于策略的路由规则匹配的所有网络通信。要

配置监控 IP 地址，请转到[监控主机 第 3-3 页](#)。如果已配置多个缺省网关，则通过这些网关以循环方式路由传出网络通信。

多个 ISP/WAN 环境自动进行故障转移

下一代应用安全网关支持在 ISP 或 WAN 连接失败时在多个 WAN/ISP 链接之间自动进行故障转移。下一代应用安全网关每十 (10) 秒检查一次连接。如果下一代应用安全网关无法检测到连接，则下一代应用安全网关会继续每两 (2) 秒检查一次。在连接尝试连续失败四 (4) 次后，将启动自动故障转移。如果稍后建立连接，则链接将自动恢复。

发生故障转移时，请执行以下操作：

- 查看系统事件日志
- 查看路由表，以验证实际网络通信路由



注意

有关监控主机的详细信息，请参阅[监控主机 第 3-3 页](#)。

添加基于策略的路由

网络通信与任何基于策略的路由规则均不匹配时，会将缺省网关（静态路由到 0.0.0.0/0）应用到所有网络通信。要配置缺省网关，请转到[添加静态路由 第 3-21 页](#)。



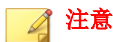
提示

趋势科技建议至少配置一个缺省网关。

过程

1. 转到[网络 > 路由 > 基于策略的路由](#)。
2. 单击**新增**。
3. （可选）启用规则。

4. 指定包含 1 到 32 个字符的策略名称，由字母、数字和下划线组成。
5. 键入可选的**描述**。
6. 在**源地址**下，选择以下参数之一：
 - **任何**：包括所有源地址。（缺省）
 - **选择地址**：显示之前配置的可用的源地址列表或添加新的 IP 地址。



注意

要添加新地址对象，请参阅[配置地址对象 第 3-8 页](#)。

7. 从下拉框中选择合适的源接口。
8. 在**目标地址**下，选择以下参数之一：
 - **任何**：包括所有目标地址
 - **选定的地址**：显示先前配置的目标地址的可选列表，以供使用。如果需要，使用此选项添加地址对象。



注意

要添加目标地址，请参阅[配置地址对象 第 3-8 页](#)。

9. 在**服务类型**下，选择以下参数之一：
 - **任何**：包括所有服务
 - **选定**：仅包括选定的服务
10. 选择出接口。
11. 对于具有静态 IP 地址的接口，指定下一跳地址。
12. （可选）启用网络伪装。



注意

如果内部 IP 地址必须转换为出接口的 IP 地址，启用网络伪装。

13. 单击**确定**。

关于动态路由管理

本部分说明如何配置动态协议以通过大型或复杂网络路由网络通信。通过动态路由协议，下一代应用安全网关可以自动与相邻路由器共享路由信息，并了解它们公布的路由和网络。下一代应用安全网关支持以下动态路由协议：

- 路由信息协议 (RIP) 和 RIP for IPv6
- 开放最短路径优先协议 (OSPF) 和 OSPF for IPv6

下一代应用安全网关选择路由并基于指定规则动态更新其路由表。基于给定的一组规则，下一代应用安全网关可以确定将数据包发送到目标位置的最佳路由或路径。也可以定义规则以禁止对相邻路由器公布路由并在公布之前更改下一代应用安全网关路由信息。

关于路由信息协议 (RIP)

路由信息协议 (RIP) 是一种距离矢量路由协议。RIP 的下一代应用安全网关实现支持 RIP 版本 2（请参阅 RFC 2453）和 RIPng（请参阅 RFC 2080）。

RIP 是为小型 IP 网络设计的，根据跃点计数来确定路由；最佳路由的跃点数最少。RIP 基于 UDP，使用端口 520 进行路由更新。通过将路由限制为最多 15 个跃点，该协议可帮助防止路由循环，但同时也限制了支持的网络大小。如果需要 15 个以上的跃点，则不会路由网络通信。另外，与 OSPF 和其他路由协议相比，RIP 可能需要更长的时间来聚合。

启用 RIP 后，下一代应用安全网关多播将从每个启用了 RIP 的接口请求 RIP 更新。相邻路由器使用路由表中的信息响应。仅当来自相邻路由器的路由尚未记录在路由表中时，下一代应用安全网关才会将这些路由添加到自己的路由表中。当路由已存在于路由表中时，下一代应用安全网关会将公布的路由与记录的路由进行比较，并根据路由表选择最短路由。

RIP 使用跃点计数作为选择最佳路由的度量。跃点计数 1 表示直接连接到单元的网络，跃点计数 16 则表示下一代应用安全网关无法访问的网络。数据包为

到达目标所经过的每个网络通常计为一个跃点。当下一代应用安全网关比较指向同一目标的两个路由时，会将跃点计数最小的路由添加至路由表。

同样，如果接口上启用了 RIP，下一代应用安全网关会定期向相邻路由器发送 RIP 响应。更新依照您为公布下一代应用安全网关路由表中的路由指定的规则，提供有关这些路由的信息。可以指定下一代应用安全网关发送更新的频率、在不更新的情况下路由可以在路由表中保留多久，以及（对于未定期更新的路由）在单元将路由公布为无法到达之后多久会从路由表中移除该路由。

在配置 RIP 设置时，请务必指定正在运行 RIP 的网络，还必须指定在连接到启用了 RIP 的网络的下一代应用安全网关接口上调整 RIP 操作所需的任何附加设置。

关于全局 RIP 设置

配置全局 RIP 设置时，必须指定运行 RIP 的网络，并指定在连接到启用 RIP 的网络的下一代应用安全网关接口上调整 RIP 操作所需的所有附加设置。

启用 RIP 全局设置

过程

1. 转到**网络 > 路由 > RIP**。
 2. 打开**全局**选项卡。
 3. 选中**启用 RIP 服务**复选框。
 4. 单击**应用**。
-

配置 RIP IP 设置

过程

1. 转到**网络 > 路由 > RIP**
2. 在选项卡的右上角，选择**协议**。

- IPv4
- IPv6

3. 单击**应用**。

配置高级 RIP 设置

过程

1. 转到**网络 > 路由 > RIP > 全局**。
2. 展开**高级设置**。
3. 选择**分发缺省路由**以启用缺省路由的分发。



注意

分发缺省路由只有在应用更改后才启用。

4. 根据需要设置计时器。
请参阅 [高级 RIP 计时器描述](#) 第 3-29 页。
5. 单击**应用**。

高级 RIP 计时器描述

表 3-3. 高级 RIP 计时器设置

计时器	描述
超时	下一代应用安全网关在两次发送 RIP 更新之间等待的时间（秒）。缺省值：30 秒
垃圾	在未接收到任何路由更新的情况下路由可以连接的最长时间（秒）。这是在没有接收到任何路由更新的情况下下一代应用安全网关可以将可连接路由保存在路由表中的最长时间。如果在超时期限过期之前下一代应用安全网关接收到路由更新，则计时器将重新启动。超时期限应该至少是为“升级计时器”设置的升级时段的三倍。缺省值：180 秒

计时器	描述
垃圾	下一代应用安全网关在从路由表中删除某个路由之前公布该路由无法连接的时间（秒）。该值确定了一个无法连接的路由可在路由表中保存的期限。缺省值：120 秒

关于网络 RIP 设置

IP 地址和网络掩码的网络设置适用于通过下一代应用安全网关进行连接并运行 RIP 的主要网络。将网络添加到“网络”列表时，会在 RIP 更新中公布属于该网络的下一代应用安全网关接口。可以在 IP 地址与 RIP 网络地址空间匹配的所有下一代应用安全网关接口中启用 RIP。

添加新 RIP 网络

过程


1. 转到**网络 > 路由 > RIP**。
2. 打开**网络**选项卡。
3. 单击**新增**。
4. 为新 RIP 网络指定 IP 地址/网络掩码。
5. 单击**应用**。
6. 验证新 RIP 网络是否显示在**网络 > 路由 > RIP > 网络**下的列表中。

修改 RIP 网络

当前任务的上下文


过程

1. 转到**网络 > 路由 > RIP**。
2. 打开**网络**选项卡。

3. 在**处理措施**列中，单击要修改的 RIP 网络的编辑图标 .
4. 单击**确定**进行确认。

删除 RIP 网络

过程

1. 转到**网络 > 路由 > RIP**。
2. 打开**网络**选项卡。
3. 在**处理措施**列中，单击要删除的 RIP 网络的删除图标 .
4. 单击**确定**进行确认。

关于重新分发 RIP 设置

选择一个或多个选项来重新分发有关不是通过 RIP 了解的路由的 RIP 更新。下一代应用安全网关可以使用 RIP 重新分发通过直接连接的网络、内核、静态路由和 OSPF 了解的路由。

配置重新分发选项

过程

1. 转到**网络 > 路由 > RIP**。
2. 打开**重新分发**选项卡。
3. 选择相应的重新分发选项：

选项	说明
重新分发内核路由	选择此选项以重新分发安装在内核路由表中的路由

选项	说明
重新分发直连路由	选择此选项以重新分发从直接连接的网络中识别的路由
重新分发静态路由	选择此选项以重新分发从静态路由中识别的路由
重新分发 OSPF 路由	选择此选项以重新分发通过 OSPF 识别的路由

4. 单击应用。

关于开放最短路径优先协议 (OSPF)

开放最短路径优先协议 (OSPF) 是一个链接状态路由协议，经常用于大型异构网络，以便在相同自治系统 (AS) 中的路由器之间共享路由信息。下一代应用安全网关支持 OSPF 版本 2（请参阅 RFC 2328）和 OSPF 版本 3（请参阅 RFC 2740）。

OSPF 的主要优点是，只要在邻居更改状态时才公布路由，而不是按一定的时间间隔公布路由，因此降低了路由开销。

OSPF 可通过从其他路由器获取信息并以链接状态公告 (LSA) 的方式向其他路由器公布路由来动态地确定路由。路由器将维护有关它与目标之间的链接的信息，并以较高的效率做出路由决策。每个路由器接口都分配有一个成本，在对所有遇到的出站路由器接口和接收 LSA 的接口进行成本累加计算后，成本最低的路由将确定为最佳路由。

下一代应用安全网关使用分层技术限制需要公布的路由以及相关联的 LSA 的数目。



注意

由于 OSPF 会动态处理大量路由信息，因此与 RIP 相比，它需要更多的处理器和内存资源。

关于全局 OSPF

通过 OSPF 的全局设置，您可以启用 OSPF、指定路由 ID 以及启用缺省路由分配。

路由器 ID

指定唯一的路由器 ID，以向其他 OSPF 路由器标识下一代应用安全网关。按照惯例，路由器 ID 是分配给任一下一代应用安全网关接口的数值最大的 IP 地址。

如果在接口上配置 OSPF 时更改路由器 ID，所有到 OSPF 相邻路由器的连接都会暂时断开。随后会自动重新建立连接。

启用全局 OSPF 设置

过程

1. 转到**网络 > 路由 > OSPF > 全局**。
 2. 选中**启用 OSPF 服务**复选框。
 3. 指定**路由器 ID**。
 4. 单击**应用**。
-

启用 OSPF 分发缺省路由

过程

1. 转到**网络 > 路由 > OSPF > 全局**。
 2. 选中**分发缺省路由**复选框。
 3. 单击**应用**。
-

关于区域 OSPF

区域 OSPF 信息是指在下一代应用安全网关中构成 **OSPF** 的区域。**OSPF** 数据包的头包含一个区域 ID，它有助于确定数据包的来源。

在**网络 > 路由 > OSPF > 区域**中访问 OSPF 区域的列表。

要添加新的 **OSPF** 区域，需要配置以下内容：

- **区域 ID** — 区域的唯一标识符。
- **区域类型** — 区域类型选项包括：

表 3-4. 区域类型

区域类型	描述
正常	常规 OSPF 区域，此类区域包含多个路由器，每个路由器至少包含一个已启用 OSPF 的接口，该接口将连接到该区域。
存根	要访问 OSPF 主干，存根区域中的路由器必须将数据包发送到一个区域边界路由器。通向非 OSPF 域的路由不会公布到存根区域中的路由器。区域边界路由器会将一个缺省路由公布到存根区域，这样可以确保任何无法与特定路由匹配的 OSPF 数据包都与该缺省路由匹配。任何连接到存根区域的路由器均被视为存根区域的一部分。
NSSA	在次末节区域 (NSSA) 中，从该区域通向非 OSPF 域的路由可由 OSPF 识别。但该区域本身仍被视为存根区域。
存根，无摘要	与无链接状态广告 (LSA) 或外部目标信息的存根区域相同。
NSSA，无摘要	与无链接状态公告 (LSA) 或外部目标信息的 NSSA 相同。
区域网络	定义在区域 ID 上运行 OSPF 的接口
(可选) 区域虚拟链路	配置虚拟链路设置以维护或增强主干区域连接。必须为区域边界路由器定义该设置，并且必须在主干区域 (0.0.0.0) 内定义。请为主干区域要包含的每个虚拟链路指定 IP 地址/位掩码。IP 地址/位掩码用于描述虚拟链路另一端上的路由器（邻居）的路由器 ID。


添加新 OSPF 区域

过程

1. 转到**网络 > 路由 > OSPF > 区域**。
 2. 指定**区域 ID**。
 3. 对于**区域类型**，请指定以下选项：
 - 正常
 - 存根
 - NSSA
 - 存根，无摘要
 - NSSA，无摘要
 4. 要添加网络，请展开**网络设置**并指定有效的 IP 地址/网络掩码。
 5. 如果需要，请展开**虚拟链接设置**并添加路由器 IP 地址。
 6. 单击**应用**。
 7. 验证新区域是否显示在**网络 > 路由 > OSPF > 区域**下的列表中。
-

修改 OSPF 区域

过程


1. 转到**网络 > 路由 > OSPF > 区域**。
2. 执行下列操作之一：
 - 在**区域 ID** 列中，单击 IP 地址。
 - 在**处理措施**列中，单击编辑图标 。

将显示**添加/编辑 OSPF 区域**窗口。

3. 修改 OSPF 区域设置。
4. 单击**应用**。
5. 验证在**网络 > 路由 > OSPF > 区域**下的列表中显示新区域更改。

删除 OSPF 区域

过程

1. 转到**网络 > 路由 > OSPF > 区域**。
2. 在**处理措施**列中，单击删除图标 。
3. 要进行确认，请单击**删除**。
4. 验证 OSPF 区域是否已从**网络 > 路由 > OSPF > 区域**下的列表中移除。

关于 OSPF 接口

OSPF 接口定义包含启用了 OSPF 的下一代应用安全网关接口的特定操作参数。定义中包括接口名称（例如，external 或 VLAN_1）、优先级以及用于发送和接收 OSPF Hello 和停顿时间间隔数据包的计时器设置。

可以在 IP 地址与启用 OSPF 的网络空间匹配的所有下一代应用安全网关接口中启用 OSPF。例如，定义区域 0.0.0.0，并将 OSPF 网络定义为 10.0.0.0/16。然后将 vlan1 定义为 10.0.1.1/24，将 vlan2 定义为 10.0.2.1/24，将 vlan3 定义为 10.0.3.1/24。所有这三个 VLAN 均可在区域 0.0.0.0 中运行 OSPF。要启用所有接口，请创建一个 OSPF 网络 0.0.0.0/0

如果向同一个下一代应用安全网关接口分配了多个 IP 地址，则可以为该接口配置不同的 OSPF 参数。例如，同一个下一代应用安全网关接口可以通过不同的子网连接到两个邻居。您可以配置一个包含一组 Hello 和停顿时间间隔参数的 OSPF 接口定义，使其与一个相邻路由器的设置兼容；再为同一个接口配置另一个 OSPF 接口定义，确保其与另一个相邻路由器的设置兼容。

要查看下一代应用安全网关接口的 OSPF 操作参数，请转到**网络 > 路由 > OSPF > 接口**。

修改 OSPF 接口

过程

1. 转到**网络 > 路由 > OSPF > 接口**。
2. 单击要更改的 OSPF 接口的名称。
3. 根据需要，更改以下一个或多个选项：

选项	说明
“被动”选项	选中此复选框以限制 OSPF 接口发送或接收 OSPF 数据包。
接口	选择要与该 OSPF 接口定义关联的下一代应用安全网关接口的名称（例如，port1、external 或 VLAN_1）。下一代应用安全网关单元可以使物理、VLAN、虚拟 IPSec 或 GRE 接口连接到启用了 OSPF 的网络。
优先级	为该接口指定 OSPF 优先级 (0-255)。它是根据 OSPF 协议将路由器选为指定路由器 (DR) 还是备份指定路由器 (BDR) 的优先级。当值为零时，不会将路由器选为 DR 或 BDR。
呼叫时间间隔	（可选）将“呼叫时间间隔”设置为与所有 OSPF 邻居的“呼叫时间间隔”设置相兼容。此设置定义了下一代应用安全网关在通过该接口发送呼叫数据包之间所等待的时间段（以秒为单位）。
停顿时间间隔	（可选）将“停顿时间间隔”设置为与所有 OSPF 邻居的“停顿时间间隔”设置相兼容。此设置定义了下一代应用安全网关等待通过该接口从 OSPF 邻居接收呼叫数据包的时间段（以秒为单位）。如果下一代应用安全网关没有在指定时间内收到呼叫数据包，则下一代应用安全网关将声明邻居不可访问。按照惯例， 停顿时间间隔 值通常比“呼叫时间间隔”值大四倍。

4. 单击**应用**。

5. 在**网络 > 路由 > OSPF > 接口**下的列表中验证更改。

关于重新分发 OSPF 路由

分发内核、已连接、静态或 RIP 的路由信息。

选择一个或多个选项（内核、已连接、静态和/或 RIP）以重新分发关于不是通过 OSPF 识别的路由的 OSPF 链接状态公布。下一代应用安全网关可以使用 OSPF 重新分发从直接连接的网络、静态路由和 RIP 中识别的路由。

重新分发 OSPF 路由

重新分发不是通过 OSPF 识别的链接状态公布。

过程

1. 转到**网络 > 路由 > OSPF > 重新分发**。
2. 选中下面一个或多个选项：

选项	说明
重新分发内核路由	重新分发安装在内核路由表中的路由。
重新分发直连路由	重新分发从直接连接的网络中识别的路由。
重新分发静态路由	重新分发从静态路由中识别的路由。
重新分发 RIP 路由	重新分发从直接 RIP 网络中识别的路由。

3. 单击**应用**。

关于路由表

在出厂缺省配置中，下一代应用安全网关路由表包含单一静态缺省路由。可以通过定义其他静态路由向路由表添加路由信息。路由表可能包含指向同一目标的几个不同路由，但这些路由中指定的下一跳地址路由器的 IP 地址或者与这些路由关联的下一代应用安全网关接口可能会不同。

下一代应用安全网关会评估路由表中的信息，并选择指向目标的最佳路由，通常为下一代应用安全网关与最近的下一跳地址路由器之间的最短距离。某些情况下，如果最佳路由不可用，将选择较长的路由。下一代应用安全网关在单元转发表（该表为单元路由表的子集）中安装最佳可用路由。数据包将根据转发表中的信息进行转发。

查看路由表

过程

1. 转到**网络 > 路由 > 路由表**。
2. 在选项卡的右上角，选择**协议**。
 - IPv4
 - IPv6

路由表指示灯

下表介绍了路由表指示灯。

代码	定义
K	内核路由
C	已连接
S	静态
R	RIPng
O	OSPFv3

网络地址转换 (NAT)

使用网络地址转换 (NAT) 策略可指定源或目标 IP 地址和端口是否在第 3 层接口上的公共和私有地址与端口之间转换。例如，对于从内部（可信）区域发送至公共（不可信）区域的网络通信，可以将私有源地址转换为公共地址。

以下 NAT 策略规则可将一系列私有源地址（10.0.0.1 到 10.0.0.100）转换为单个公共 IP 地址（200.10.2.100）和唯一的源端口号（动态源转换）。该规则仅适用于在内部（可信）区域中的第 3 层接口上接收的并发送至公共（不可信）区域中的接口的网络通信。由于私有地址处于隐藏状态，因此可从公共网络发起网络会话。如果公共地址不是下一代应用安全网关接口地址（或者不在同一子网中），则本地路由器需要一个静态路由将返回网络通信定向到下一代应用安全网关。



图 3-5. 示例 NAT 规则

NAT 规则

NAT 地址转换规则基于源和目标地址以及源和目标端口。类似于安全策略，NAT 策略规则会依次与传入网络通信进行比较，并应用第一个与网络通信相匹配的规则。

根据需要，将静态路由添加到本地路由器以便将所有公共地址的网络通信路由至下一代应用安全网关。还可以将静态路由添加到下一代应用安全网关中的接收接口，以便将网络通信路由回至私有地址。

添加源 NAT 规则

源 NAT (SNAT) 更改数据包的 IP 标头中的源地址。主要目的是将私有 (RFC 1918) 地址/端口更改为公共地址/端口，以便数据包离开网络。下表介绍了使用 SNAT 时所需的配置。

过程

1. 转到**网络 > NAT > 新增**。
2. 根据 NAT 类型配置 NAT 设置，然后单击**应用**。

选项	说明
NAT 类型	接收 IP 数据包时，请选择 源 NAT 以指定设置。
出接口	从下拉框列表中选择 任何 或任何 L3 接口来用作出站网络通信的接口，其中出站网络通信指源自网络内部的网络通信。
源 IP 转换	<p>从下列选项中选择：</p> <ul style="list-style-type: none"> • 出接口 IP 地址 — 出接口 IP 地址用于进行转换。如果不使用出接口 IP 地址，用户必须显式指定具有以下三个选项之一的接口。 • 单个 IP 地址 — 指定的 IP 地址将用于进行转换。 • IP 地址范围 — 指定的 IP 地址范围将用于进行转换。 • 子网 — 指定的子网将用于进行转换。
描述	指定一个关于 NAT 规则使用或配置的可识别的特征。
SNAT 的高级选项	<p>允许用户指定更多详细信息或匹配条件，包括：</p> <ul style="list-style-type: none"> • 协议 - 任何、TCP 或 UDP。“任何”指所有协议。 • 源 IP 地址范围 - 由网络指定。 • 源端口范围 - 由管理员指定。 • 目标 IP 地址范围 - 由管理员指定。

选项	说明
	<ul style="list-style-type: none"> 目标端口范围 - 由管理员指定。

- 验证新规则是否已添加到**网络 > NAT** 下的列表中。

添加目标 NAT 规则

目标 NAT (DNAT) 更改数据包的 IP 标头中的目标地址。目标 NAT 的主要目的是利用公共地址/端口的目标将传入数据包重定向到网络内的私有 IP 地址/端口。下表介绍了使用 DNAT 时所需的配置。

过程

- 转到**网络 > NAT > 新增**。
- 根据 NAT 类型配置 NAT 设置，然后单击**应用**。

NAT 类型	转发 IP 数据包时，请选择 目标 NAT 以指定设置。
入接口	从下拉列表中选择 任何 或任何 L3 接口来用作网络通信的接口，其中网络通信源自网络路由器的外部并继续向网络内的目标传输。
目标 IP 转换	<p>从下列选项中选择：</p> <ul style="list-style-type: none"> 使用入接口 IP — 指定的入接口 IP 地址范围将用于进行转换。如果不使用入接口 IP 地址，用户必须显式指定具有以下选项（使用虚拟 IP）的接口。 使用虚拟 IP 地址 — 当用户指定外部 IP 地址范围时，转换的 IP 地址范围会根据该 IP 地址的开头自动生成。该映射是一对一关系的映射。 端口转发 — 选中“端口转发”复选框将与端口转发构成静态一对一 NAT 映射。外部 IP 地址始终转换成相同的映射 IP 地址，外部端口号始终转换为相同的映射端口号。从“任何”、“TCP”或“UDP”中选择一种作为协议。（“任何”指所有协议。）当用户指定“外部服务端口”范围时，“映射至端口”会根据开始端口自动生成。该映射是一对一关系的映射。

描述	指定一个关于 NAT 规则使用或配置容易识别的特征。
DNAT 的高级选项	允许用户指定更多详细信息或匹配条件，包括： <ul style="list-style-type: none">• 源 IP 范围：由管理员指定。• 源端口范围：由管理员指定。

3. 验证新规则是否已添加到**网络 > NAT** 下的列表中。

修改 NAT 规则

过程

1. 转到**网络 > NAT**。
2. 在**优先级**列中，单击要更改的 NAT 规则的数量。
3. 根据需要编辑参数。
4. 单击**应用**。
5. 在**网络 > NAT** 中验证更改。

更改 NAT 规则优先级


过程

1. 转到**网络 > NAT**。
2. 选中要赋予其更高优先级的 NAT 规则的复选框。
3. 要重新排序，请使用 NAT 规则列表上方的运算符（置顶、上移、下移、置底）。

4. 单击**更新优先级**以保存更改。
-

删除 NAT 规则

过程

1. 转到**网络 > NAT**。
 2. 选择要删除的 NAT 规则所在行。
 3. 单击  **删除**。
将显示**删除**确认消息。
 4. 要进行确认，请单击**删除**。
 5. 验证**网络 > NAT**中是否不再列出 NAT 规则。
-

服务

下一代应用安全网关服务支持允许域名服务器 (DNS) 转发、动态主机配置协议 (DHCP) 服务器和动态 DNS (DDNS) 配置设置。

关于 DNS 转发

下一代应用安全网关的某些功能（包括警报电子邮件和 URL 过滤）需要使用 DNS。指定下一代应用安全网关所连接的 DNS 服务器的 IP 地址。DNS 服务器 IP 地址通常由您的 ISP 提供。

可以将下一代应用安全网关配置为自动获取 DNS 服务器地址。要自动获取这些地址，至少需要有一个下一代应用安全网关接口使用 DHCP（或 PPPoE）寻址模式。有关配置详细信息，请参阅[关于 DHCP 第 3-46 页](#)。

下一代应用安全网关可以在其接口上提供 DNS 转发功能。所连接网络上的主机使用该接口 IP 地址作为其 DNS 服务器。发送到接口的 DNS 请求将转发至已配置或下一代应用安全网关自动获取的 DNS 服务器地址。

用户可以在下一代应用安全网关中启用和禁用 DNS 转发，或指定名称服务器以使用本地 DNS 或定制的 DNS。

配置 DNS 转发设置

过程

1. 转到**网络 > 服务 > DNS 转发**。
2. 选择 DNS 转发设置。
有关选项详细信息，请参阅 [DNS 转发设置 第 3-45 页](#)。
3. 单击**应用**。

DNS 转发设置

下一代应用安全网关的 DNS 转发设置包括：

设置	描述
禁用 DNS 转发	不提供 DNS 转发功能。
使用系统 DNS 设置	此选项仅适用于在 NAT/路由模式下运行的下一代应用安全网关单元。请使用指定的主 DNS 服务器和辅助 DNS 服务器地址将收到的 DNS 请求转发到所配置的 DNS 服务器。
使用指定的 DNS 服务器	指定要在客户端上使用的主和辅助域名服务 (DNS) 服务器的 IP 地址（采用 IPv4 或 IPv6 格式）。

关于 DHCP

下一代应用安全网关对于网络接口支持多个动态主机配置协议 (DHCP) 服务。它可支持多个池，并且一个 DHCP 池支持一个物理池。请指定 IPv4 或 IPv6 DHCP 服务，并在**网络 > 服务 > DHCP** 中配置 IPv4 或 IPv6 DHCP 设置。

对于配置为使用 DHCP 的接口，下一代应用安全网关会自动响应 DHCP 请求。该接口将配置有 IP 地址池以及 DHCP 服务器提供的任何 DNS 服务器地址和缺省网关地址。

DHCP 高级设置：静态映射和租用时间

设置	描述
静态映射	可以使用手动绑定的方式分配静态 IP 地址。
租用时间	表示对 DHCP 租用时间间隔的任何限制。指定天数、小时数或分钟数。例如，如果仅指定小时数，则租用时间将限制在该小时数以内。

查看 DHCP 服务设置

过程


1. 转到**网络 > 服务 > DHCP**。
2. 在表中，查看与任何 DHCP 服务关联的参数：

选项	说明
名称	DHCP 服务的名称，例如 eth0、eth1 等等。
IP 地址/网络掩码	从 DHCP 服务器租用的 IP 地址/位掩码。

选项	说明
启用	此图标指示服务的状态：启用（绿色/开启）或禁用（红色/关闭）。
IP 池	适用于 DHCP 服务的 IP 地址范围。
选项	DNS 服务器 IP 地址、网关 IP 地址和租用时间。
操作	单击图标以编辑 DHCP 服务设置。

修改 DHCP 服务设置

过程

1. 转到**网络 > 服务 > DHCP**。
2. 执行下列操作之一：
 - 在**名称**列中，单击要修改的 DHCP 服务器的名称。
 - 在**处理措施**列中，单击要修改的 DHCP 服务所在行的编辑图标 。
3. 修改与 DHCP 服务关联的参数：

选项	说明
启用	选择该选项可启用服务。
IP 地址/网络掩码	从 DHCP 服务器租用的 IP 地址/位掩码。
首选 DNS	指定首选 DNS 服务器的 IP 地址。
网关	指定 DHCP 服务器定义的网关的 IP 地址。
IP 地址范围开始和结束	指定 IP 地址的范围以创建应用了 DHCP 配置的 IP 池。

4. 如果需要，请更改**高级设置**：
 - 在**租用时间**中，调整租用的 IP 地址和网络掩码不再有效时的时间和日期。

- 在**静态映射**部分下，指定要添加到服务的 MAC 地址和 IP 地址。
5. 单击**应用**。
 6. 在**网络 > 服务 > DHCP** 中验证已更改的设置。
-

关于动态 DNS

动态域名系统 (DDNS) 是指实时更新 Internet DNS 名称服务器，以保持现有的 DNS 配置（主机名、地址以及其他信息）处于最新状态。通常，如果由于公司使用 PPPoE 或 DHCP 来获取 Internet 访问而频繁更改公共主机名到 IP 地址的映射，则会用到该系统。通过 DDNS 服务，可以自动在 Internet 上传播新主机名到 IP 地址的映射。DDNS 服务提供商作为中介来管理此进程。下一代应用安全网关设计为在尝试访问企业时外部客户端将连接到的第一个面向 Internet 的设备，它需要确保对于尝试在企业端访问的每个主机名/域，所有 Internet 用户都将其网络通信路由到此设备。借助 DDNS 客户端，下一代应用安全网关可以将主机名到 IP 地址的更改传送到 DDNS 服务提供商。

通过下一代应用安全网关的动态 DNS 支持，可在 DDNS 服务供应商的 Web 站点上注册其域，然后配置相应的信息（如帐户、密码和域），以便由下一代应用安全网关进行维护。DDNS 提供商将静态主机名分配给用户；只要为该用户分配新 IP 地址，就会通过在该地址的端点或网络设备中运行的软件（执行 RFC 2136 或其他协议）将此信息传递给 DDNS 提供商；提供商将主机名和地址之间的关联分发给 Internet 的 DNS 服务器，以便它们可以解析 DNS 查询。下一代应用安全网关 DDNS 客户端监控公共 IP 地址更改并自动同步 IP 地址-域映射。



系统会记录部分异常事件（例如，服务供应商返回意外状态）。同时还会记录所有更新事件。

受支持的 DDNS 服务提供商

支持以下四个 DDNS 服务提供程序：

提供商	用户范围
Dyn DNS	全局
Free DNS	
Oray	中国
DNSPod	

**注意**

不支持 IPv6。

配置 DDNS 客户端

根据服务供应商配置基本设置。所需信息因服务不同而异。基本上，每个服务都需要域名、帐户和密码信息。

一些供应商（例如 Oray 和 Dyn DNS）提供 HTTPS 连接作为选项。其他供应商（例如 FreeDNS）不公开 HTTPS 接口，而 DNSPod 要求强制性 HTTPS 连接。

过程

1. 转到**网络 > 服务 > 动态 DNS > 常规**。
2. 在“动态 DNS”对话框中，执行下列操作：
 - a. 选中**启用动态 DNS**复选框。
 - b. 选择**供应商**。
 - c. 键入**用户名、密码和域**。
 - d. 选择 WAN 接口：

自动：

（缺省）下一代应用安全网关将根据 RFC 1597 自动发现具有非私有 IP 地址的接口

其他:	下一代应用安全网关将始终尝试从该接口获取公共 IP 地址。
------------	-------------------------------

3. 仅对于 Oray，选择**服务级别**。所有非免费版的服务都是 HTTPS 连接所需的付费服务。
 - 免费版
 - 专业版
 - 企业版
 - 旗舰版
 4. 如果在**服务级别**中选择了**专业版**，则选择**启用 HTTPS**。
 5. 单击**应用**。
-

DDNS 状态

网络 > 服务 > 动态 DNS > 状态选项卡显示当前 DDNS 运行状态，包括当前接口（自动发现的或指定的）、WAN IP 地址和状态消息。

可能的状态消息包括：

- 成功
- 错误:认证失败
- 错误:帐户尚未激活
- 错误:域信息无效或未注册
- 错误:Internet 访问不可用或无法连接到服务供应商
- 错误:使用了一些仅为付费用户提供的功能（例如 HTTPS 连接服务），相关设置已重置
- 错误:从服务供应商收到服务不可用的消息
- 错误:未检测到可用的 WAN IP

- 错误:指定的接口上没有合适的 IP
- 错误:服务接口可能已更改, 请联系趋势科技进行更新
- 错误:认证不成功的次数太多, 已暂时禁用此帐户
- 错误:子域信息无效或未注册
- 错误:不允许以循环方式更新主机。
- 错误:未知错误, 请检查您的 Internet 访问。
- 未启用

虚拟专用网络

虚拟专用网络 (VPN) 技术通常用于确保员工在外办公时可以通过相应的安全措施远程访问其公司网络。概括而言, 认证是尝试验证 (数字) 身份以访问网络资源和登录 VPN 网络的过程。VPN 可利用现有基础架构 (Internet) 来安全地构建和增强现有连接。VPN 技术基于标准的 Internet 安全协议, 因此它的实现能够确保特殊类型的网络节点 (即安全网关) 之间的链接是安全的。站到站 VPN 可确保网关之间的链接安全。用户 VPN 可确保网关与远程访问客户端之间的链接安全。

典型的下一代应用安全网关部署允许用户使用 VPN 远程连接公司网络资源。其他远程站点可由下一代应用安全网关进行保护, 并通过严格的安全策略来管理所有网络资源和远程端点之间的通信。

下一代应用安全网关支持 IPV4 到 IPV4 的访问。

用户 VPN

每当用户从远程位置访问组织时, 都必须保证同时满足安全连接的常规要求和远程客户端的特殊需求。用户虚拟专用网络 (VPN) 将 VPN 功能扩展到了远程用户, 使用户能够使用拨号连接 (包括宽带连接) 和 LAN (以及无线 LAN) 连接, 通过 VPN 隧道安全地向网络和服务器传输敏感信息。

有关配置 LDAP 或本地用户帐户的 VPN 访问权限的详细信息，请参阅[终端用户管理 第 6-9 页](#)。

点对点隧道协议 (PPTP) VPN

本节说明了如何指定 PPTP 在线用户的 IP 地址范围，或者如何配置要在隧道设置中使用的 PPTP 客户端 IP 地址。下一代应用安全网关支持点对点隧道协议 (PPTP)，以便在两个 VPN 对端之间通过隧道传输 PPTP 网络通信。Windows 或 Linux PPTP 在线用户可以与配置为 PPTP 服务器的下一代应用安全网关建立 PPTP 隧道。此外，也可以对下一代应用安全网关进行配置，以便将 PPTP 数据包转发到网络上位于下一代应用安全网关后端的 PPTP 服务器。PPTP VPN 仅适用于 NAT/Route 模式。目前 PPTP 会话的最大数目是 254。

当使用下一代应用安全网关作为 PPTP 网关时，可从本地地址范围中选择 PPTP 客户端 IP 或使用在 PPTP 用户组中定义的服务器。选择使用哪种方法检索 IP 地址，如果使用用户组服务器，请提供 IP 地址和用户组。

必须在**管理 > 终端用户管理 > 常规设置**选项卡上选择本地用户或 LDAP 进行认证。

启用 PPTP VPN

过程

1. 转到**网络 > 用户 VPN > PPTP VPN**。
 2. 选中**启用 PPTP VPN** 复选框。
 3. 单击**应用**。
-

配置常规 PPTP VPN 设置



注意

如果已将 LDAP 配置为认证 PPTP VPN 用户，则下一代应用安全网关只能支持未加密的密码 (PAP) 认证协议。

过程

1. 转到**网络 > 用户 VPN > PPTP VPN > 常规**。
2. 选择 IP 地址的分配方式：

选项	说明
IP 地址池	指定通过 PPTP 获取远程访问权限的在线用户的 IP 地址 (192.168.0.0)。
DHCP 服务器	指定 DHCP 服务器的 IP 地址/位掩码 (示例：10.10.1.1./24)，并从下拉列表框中选择有效的接口 (eth1 至 eth3)。

3. 如果需要，配置**高级设置**。
请参阅 [高级设置：启用调试模式和加密级别](#) 第 3-53 页。
4. 单击**应用**。

高级设置：启用调试模式和加密级别

下一代应用安全网关 PPTP VPN 使用 Microsoft 点对点加密 (MPPE)。MPPE 是通过点对点协议 (PPP) 和虚拟专用网络 (VPN) 链接来加密数据的协议。它使用 RSA RC4 加密算法。MPPE 支持 40 位和 128 位会话密钥，这些密钥经常更改以提高安全性。

过程

1. 转到**网络 > 用户 VPN > PPTP VPN > 常规**。

2. 单击**高级设置**链接。
 3. 指定**加密强度**:
 - 40 位（弱）
 - 128 位（强）
 4. 要在 PPTP 日志中显示其他调试信息，请选中**启用调试模式**复选框。
 5. 单击**应用**。
-

查看 PPTP VPN 在线用户

在线用户 选项卡可显示当前通过 VPN 连接的所有在线用户。同时显示用户名、会话开始的时间、在线用户公共 IP 地址和虚拟 IP 地址。连接的在线用户的总数将显示在表的上方。

过程

1. 转到**网络 > 用户 VPN > PPTP VPN**。
 2. 单击**在线用户**选项卡。
-

查看 PPTP VPN 日志以排除故障

过程

1. 转到**网络 > 用户 VPN > PPTP VPN**。
 2. 单击**问题排查**选项卡。
-

PPTP VPN 问题排查

如果在设置 PPTP VPN 时遇到问题，可能会收到以下错误。

表 3-5. 了解 PPTP VPN 错误消息

错误消息	说明	推荐的处理措施
VPN 错误 800 — 无法建立 VPN 连接。	来自 VPN 客户端的 PPTP 数据包无法到达下一代应用安全网关服务器。	<ol style="list-style-type: none"> - Ping 下一代应用安全网关服务器，假定允许（也就是说，不会阻止）在 PPTP 客户端和下一代应用安全网关服务器之间执行 ping 操作。确认在 PPTP 客户端和下一代应用安全网关服务器之间具有网络连接。 - 要允许 PPTP 网络通信，配置网络防火墙以打开 TCP 端口 1723 并将通用路由封装 (GRE) 网络通信的 IP 协议 47 转发到下一代应用安全网关服务器。一些防火墙将 IP 协议 47 视为 VPN 或 PPTP 直通。
VPN 错误 734 — PPP 链接控制协议已终止。	PPTP 客户端和下一代应用安全网关服务器之间的协议不匹配。	出于安全考虑，下一代应用安全网关服务器只支持 MS-CHAP 版本 2 和点对点加密。请确保 PPTP 客户端支持这两种协议。
VPN 错误 691 - 拒绝访问，因为用户名和/或密码在该域上无效	用户名和/或密码无效。	输入正确的用户名和/或密码，或者请求系统管理员重置密码。

安全套接层虚拟专用网络

安全套接层虚拟专用网络 (SSL VPN) 是可以与标准 Web 浏览器一起使用的一种 VPN 形式。下一代应用安全网关 SSL VPN 解决方案要求安装客户端软件，它是包括基于 Web 的电子邮件、企业和政府目录、文件共享、远程备份、远程系统管理以及消费类电子商务在内的应用程序的理想选择。

如果用户对其端点拥有完全管理权限且使用各种应用程序，通过隧道模式，远程客户端可访问本地内部网络，就如直接连接到网络中一样。

本部分提供有关可在基于 Web 的管理器上进行配置的 SSL VPN 功能的信息。只有在 NAT/路由器模式下运行的下一代应用安全网关设备支持 SSL VPN 功能。

启用 SSL VPN

过程

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
 2. 选中**启用 SSL VPN** 复选框。
-

配置常规 SSL VPN 服务器设置

必须启用 SSL VPN 才能执行此过程。要配置常规 SSL VPN 设置，请选择接口、协议 (TCP/UDP)、端口以及与 VPN 服务器关联的认证方法。访问公司网络时，所有 SSL VPN 在线用户都使用覆盖主机名选项。

过程

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
2. 使用**协议**下拉列表选择协议或 SSL VPN。
 - TCP
 - UDP
3. 在**端口**中，指定 SSL 端口号。
4. 如果设备的主机名无法在客户端端点中解析，请为**覆盖主机**指定端点 IP 地址。
5. 配置**本地网络**。

请参阅 [为 SSL VPN 配置本地网络](#) 第 3-57 页。

6. 配置**虚拟 IP 池**设置。

请参阅 [为 SSL VPN 配置虚拟 IP 地址池](#) 第 3-57 页。

7. 配置**高级**设置。

请参阅 [为 SSL VPN 配置高级设置](#) 第 3-58 页。

8. 单击**应用**。

为 SSL VPN 配置本地网络

过程

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
 2. 单击**本地网络**。
 3. 单击**新增**。
 4. 为本地网络指定 IP 地址/位掩码。
 5. 单击**确定**。
 6. 验证已在**网络 > 用户 VPN > SSL VPN > 常规 > 本地网络**下添加本地网络。
-

为 SSL VPN 配置虚拟 IP 地址池

过程

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
2. 单击**虚拟 IP 池**设置。
3. 指定**网络池**（缺省：10.252.1.0）。
4. 从下拉列表框中选择位掩码值。

5. 单击**应用**。

为 SSL VPN 配置高级设置

过程

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
2. 单击**高级设置**。
3. 选择**加密算法**：

选项	说明
AES 128 CBC	使用 128 位密钥的 128 位块密码分组链接 (CBC) 算法。
AES 192 CBC	使用 192 位密钥的 192 位块密码分组链接 (CBC) 算法。
AES 256 CBC	使用 256 位密钥的 256 位块密码分组链接 (CBC) 算法。
DES-EDE3-CBC	三重 DES，即，使用三个密钥对纯文本加密三次。
BF-CBC	Blowfish 的使用密钥的 64 位块对称密码分组链接 (CBC) 算法。



注意

数字加密标准 (DES) 是使用 56 位密钥的 64 位块算法。高级加密标准 (AES) 是支持 128 到 256 位长度的密钥和可变长度数据块的私有密钥算法。

4. 选择**认证算法**：

选项	说明
MD5	由 RSA Data Security 开发的消息摘要（版本 5）哈希算法（单向哈希函数），设计用于数字签名应用程序，其中大型文件在使用私有密钥/公共密钥算法加密前必须以安全方式进行压缩。
SHA1	安全哈希算法 1，可生成 160 位消息摘要。大消息摘要可抵御强力冲突攻击和逆推攻击。

5. 选择**密钥长度**：

- 1024 位
 - 2048 位
6. 设置**密钥生命周期**选项（以小时为单位，在 1 到 24 之间）。允许的最大值为 24 小时。
 7. 指定**本地 DNS** 设置。
 8. 添加或移除**本地域名**:
 - 使用 >> 选项添加新的本地域
 - 使用 << 选项移除现有的本地域
 9. 选中**启用压缩流量**以允许对 SSL VPN 流量进行透明压缩和解压缩。
 10. 选中**启用调试模式**以在 SSL VPN 日志中显示更多调试信息。
 11. 选中**启用多用户同时登录**以允许多个客户端使用一个帐户。
 12. 选中**启用网络伪装**以自动添加 NAT 规则。
 13. 单击**应用**。
-

查看 SSL VPN 在线用户

在线用户 选项卡可显示当前通过 VPN 连接的所有在线用户。同时显示用户名、会话开始的时间、在线用户公共 IP 地址和虚拟 IP 地址。连接的在线用户的总数将显示在表的上方。

过程

1. 转到**网络 > 用户 VPN > SSL VPN**。
 2. 选择**在线用户**选项卡
-

查看 SSL VPN 日志

过程

1. 转到**网络 > 用户 VPN > SSL VPN**。
 2. 选择**问题排查**选项卡。
-

客户端安装

下一代应用安全网关支持多个 SSL VPN 客户端安装类型。

对于 Windows 用户，在使用 SSL VPN 门户登录以下链接时，将自动安装 SSL VPN 客户端安装软件包：

`https://<appliance_server_IP_address>/`

对于 Linux 或 Mac 用户，请从 <http://openvpn.net> 下载最新安装软件包。从 `https://<appliance_server_IP_address>/` 获取 SSL VPN 配置文件。

SSL VPN Windows 客户端所支持的浏览器

操作系统	浏览器
Windows XP	<ul style="list-style-type: none">• Internet Explorer 7, 8, 9• Firefox 21+ (安装了 JRE)• Chrome 27+ (安装了 JRE)
Windows 7	<ul style="list-style-type: none">• Internet Explorer 8, 9, 10• Firefox 21+ (安装了 JRE)• Chrome 27+ (安装了 JRE)

在 Linux 或 MAC 操作系统上安装 SSL VPN 客户端

过程

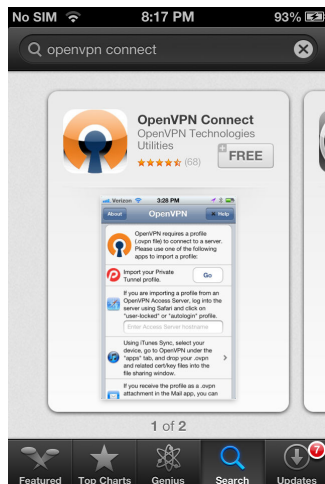
1. 通过浏览器访问 `https://<appliance_server_IP_address>/`。
2. 单击适用于 Linux 和 Mac 操作系统的**配置软件包**以下载 `sslvpnlinuxconfig.tgz` 文件。
3. 将 `sslvpnlinuxconfig.tgz` 文件解压缩到本地文件夹，然后将 `ca.crt` 和 `openvpn.ovpn` 文件复制到 **OpenVPN** 配置文件夹。

客户端计算机将拨号至下一代应用安全网关。有关问题，请查看 [SSL 和 VPN 问题排查 第 3-69 页](#)。

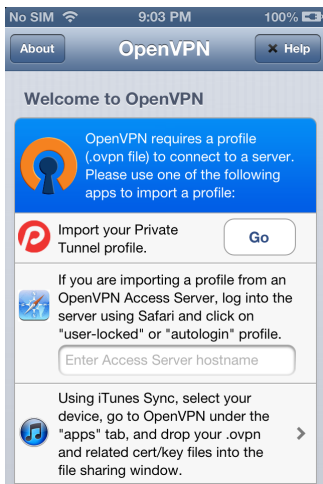
在 iOS 上安装 SSL VPN 客户端

过程

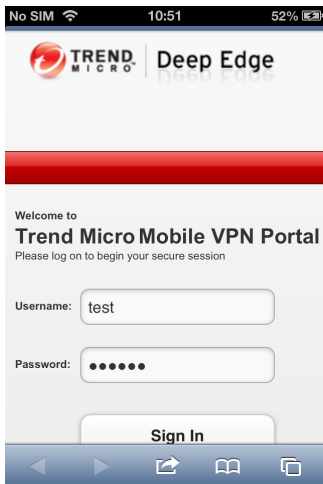
1. 从 App Store 安装 **OpenVPN Connect**。



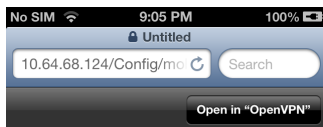
2. 打开 **OpenVPN Connect** 应用程序。



3. 通过 Safari 访问下一代应用安全网关 VPN 门户 (https://appliance_server_IP_address/), 然后进行登录。



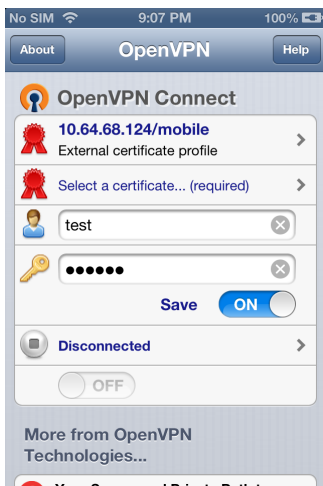
- 从 `https://<appliance_server_IP_address>/Config/mobile.ovpn` 下载 OVPN 文件。



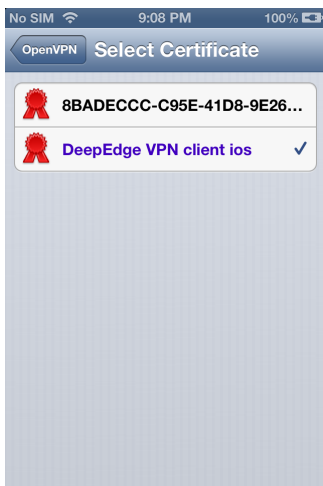
- 点击在“OpenVPN”中处于打开状态，通过 OpenVPN Connect 加载配置文件。



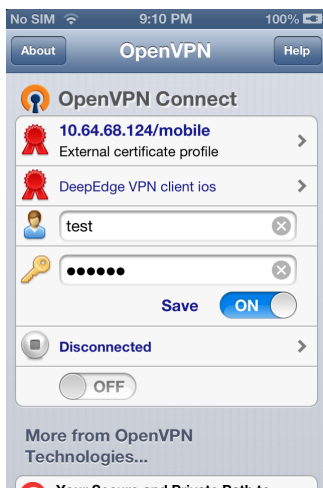
6. 点击“+”配置安全配置。



7. 点击**选择证书…（必需）**，再点击下一代应用安全网关 VPN 客户端 iOS 选择证书。



8. 点击 OpenVPN 返回到主菜单。



9. 指定帐户用户名和密码，然后切换已断开连接下的关闭按钮以访问下一代应用安全网关 SSLVPN 服务器。

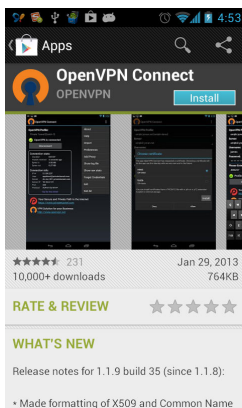


此时将建立 SSLVPN 隧道，用户将可以通过安全 VPN 隧道访问内部资源。

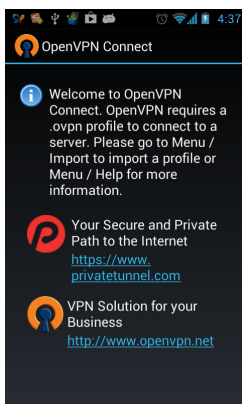
在 Android 操作系统（4.0 以上版本）上安装 SSL VPN 客户端

过程

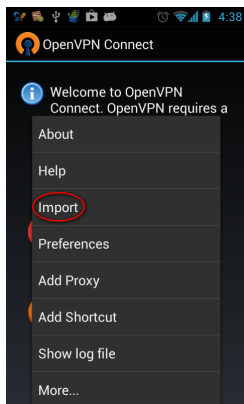
1. 从 https://<appliance_server_IP_address>/Config/mobile.ovpn 下载 SSLVPN 移动配置文件，然后将配置文件复制到 Android 设备的 SD 卡。
2. 从 Google Play 安装 **OpenVPN Connect**。



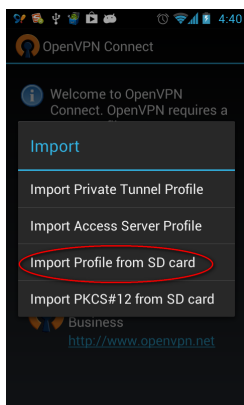
3. 打开 **OpenVPN Connect** 应用程序。



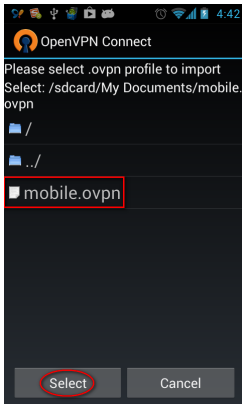
- 按操作溢出按钮，然后选择导入。



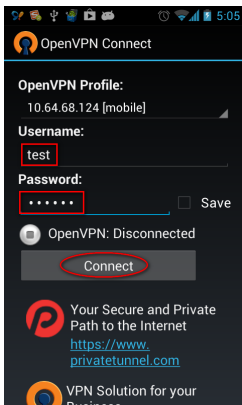
- 选择从 SD 卡导入安全配置。



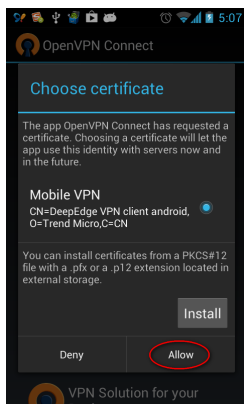
- 选择 `mobile.ovpn`，然后点击选择。



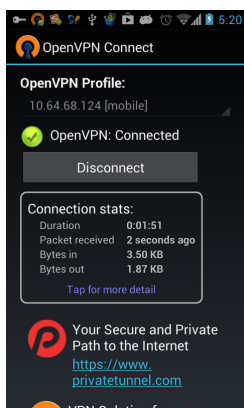
7. 指定用户名和密码，然后点击**连接**。



8. 点击**允许**。



将显示 **OpenVPN Connect** 窗口。



此时将建立 SSLVPN 隧道，用户将可以通过安全 VPN 隧道访问内部资源。

SSL 和 VPN 问题排查

如果在设置 SSL VPN 时遇到问题，以下列表介绍了一些常规问题排查指南：

过程

- 验证客户端是否可以成功地对下一代应用安全网关服务器执行 ping 操作。
- 验证客户端是否可以访问配置了 SSL VPN 的 TCP 或 UDP 端口。
- 验证 Windows 客户端配置文件 `openvpn.ovpn` 与 `https://<appliance_server_IP_address>/Config/openvpn.ovpn` 文件是否具有相同配置。
- 验证移动客户端配置文件 `mobile.ovpn` 与 `https://<appliance_server_IP_address>/Config/mobile.ovpn` 是否具有相同配置。

了解 SSL VPN 错误消息

错误消息	说明	推荐的处理措施
TCP:无法连接到 X.X.X.X:8445, 5 秒后将重试: 拒绝连接	SSL VPN 客户端无法到达下一代应用安全网关服务器。	<ol style="list-style-type: none"> 1. Ping 下一代应用安全网关服务器，假定允许（也就是说，不会阻止）在 SSL VPN 客户端和下一代应用安全网关服务器之间执行 ping 操作。确认您具有 SSL VPN 客户端和下一代应用安全网关服务器之间的网络连接。 2. 要允许 SSL VPN 网络通信，配置网络防火墙以打开下一代应用安全网关服务器的配置了 SSL VPN 的 TCP 或 UDP 端口。
收到 SIGTERM[soft,auth-failure], 进程退出	用户名和/或密码无效。	指定正确的用户名和/或密码，或者请求管理员重置密码。

移动 VPN

作为一种网关设备，下一代应用安全网关可为便携机或台式机以及移动设备提供 VPN 服务。移动 VPN 可对 Apple iOS 的“封闭”环境或 Android 的“开源”环境中的移动设备提供支持。

下一代应用安全网关可通过利用内置 IPsec VPN 客户端对 iOS 和 Android 设备提供 VPN 支持。移动设备上不需要安装任何代理。

下一代应用安全网关支持创建策略安全配置，以便支持 iOS 的“按需 VPN”。此支持提供了将 iOS 策略安全配置推送到 iOS 设备的功能。这使得 iOS 设备能够在公司资源被访问时自动触发并建立 VPN 连接。



注意

Android 设备不支持按需 VPN。

移动 VPN 支持以下功能：

- 通过公司 LDAP 服务器进行用户认证
- 在公司环境中集成 DHCP 服务器，以将 IP 地址发送到远程客户端
- 当只有公司网络通信通过 VPN 隧道路由，非公司网络通信通过提供商的网络路由时，会出现“拆分隧道”。
- 当公司资源通过 VPN 隧道发送到驻留在公司环境中的 DNS 服务器时，会出现“拆分 DNS”。对非公司资源进行的查找会发送到提供商的 DNS 服务器。
- 单个用户使用多个设备
- 撤销对任何设备的 VPN 访问权限。可通过从公司 LDAP 服务器或本地用户数据库中移除用户凭证，来撤销用户的 VPN 访问权限
- 用于创建和管理策略以及监控与 VPN 连接相关的所有活动的管理界面，其中包括：
 - 每个用户的活动 VPN 连接
 - 为这些连接分配的 IP 地址

移动 VPN、SSL VPN 和 PPTP VPN 可接受在**管理 > 终端用户管理 > 本地用户**中添加的本地 VPN 用户。

配置移动 VPN 常规设置

缺省情况下，禁用 IPSec 远程访问 VPN 连接。确保配置所需的设置来启用它。以下任务中的选项定义：

- 要使用的接口
- 要使用的用户认证方法
- 要使用的网络池和本地网络
- 按需 VPN（适用于 iOS）配置

过程

1. 转到**网络 > 用户 VPN > 移动 VPN > 常规**选项卡。
2. 选中**启用移动 VPN**复选框。
3. 从**接口**下拉列表框中选择一个接口，以用于移动 VPN 客户端连接。
4. 为虚拟 IP 地址池网段指定 IP 地址和网络掩码，以用于连接客户端。
5. 指定**本地网络**的 IP 地址。
6. 对于 Apple 设备，配置**按需 VPN (适用于 iOS)**设置。
 - a. 选中**按需 VPN**复选框，以允许基于证书的 VPN 配置，此配置可在访问某些域时自动触发 VPN 连接。



注意

启用“按需 VPN (适用于 iOS)”可将此信息添加到安全配置文件。

- b. 指定**域或主机**信息。
- c. 选择以下建立连接的条件：

- 始终建立
- 从不建立
- 需要时建立

7. 单击**应用**。

查看移动 VPN 在线用户

在线用户 选项卡可显示当前通过 VPN 连接的所有在线用户。同时显示用户名、会话开始的时间、在线用户公共 IP 地址和虚拟 IP 地址。连接的在线用户的总数将显示在表的上方。

过程

1. 转到**网络 > 用户 VPN > 移动 VPN**。
 2. 单击**在线用户**选项卡。
-

配置高级移动 VPN 设置

高级选项卡提供了一些高级功能的设置，如拆分 DNS 和拆分隧道。

过程

1. 转到**网络 > 用户 VPN > 移动 VPN**。
2. 单击**高级**选项卡。
3. 选中**对端断线检测**，以允许系统检测断开（脱机）的远程系统。
4. 选择相应的 IKE 调试级别：
 - **控制流**
 - **发出报文**

- 接收报文
 - 原始内容
 - 算法信息
5. 选中**启用网络伪装**以自动添加 NAT 规则。
 6. 选中**启用拆分隧道**以拆分**常规**选项卡上指定的本地网络。

只有公司网络通信会通过 VPN 隧道进行路由，而非公司网络通信会通过提供商的网络进行路由。有关设置本地网络的详细信息，请参阅[配置移动 VPN 常规设置 第 3-72 页](#)。
 7. 选中**启用拆分 DNS**以通过 VPN 隧道将公司资源发送到公司环境中的 DNS 服务器。



注意

非公司查找会发送到提供商的 DNS 服务器。

- a. 在 **DNS 服务器** 中，指定公司环境中的 DNS 服务器的 DNS 服务器 IP 地址。
- b. 在 **本地域** 中，指定与 DNS 服务器对应的所有相关的本地域。



注意

如果未指定本地域，则移动 VPN 在线用户无法解析 FQDN。

8. 单击**应用**。
-

移动 VPN 问题排查

问题排查选项卡可显示用于调试的 IPSec 守护程序的实时日志。

过程

1. 转到**网络 > 用户 VPN > 移动 VPN > 问题排查**选项卡。

2. 查看实时的日志内容。
-

移动设备 VPN 配置

虚拟专用网络 (VPN) 通常在组织内使用，以允许您通过公共网络安全地传递私人信息。例如，您必须配置 VPN，以便在 iOS 设备上访问工作电子邮件帐户。VPN 通过 Wi-Fi 和手机数据网络连接工作。下一代应用安全网关使用 IPsec 连接解决方案，不需要在移动设备上安装任何代理。

移动 VPN 可建立经过认证的加密隧道，使移动用户能够通过公共网络安全访问驻留在公司网络中的应用程序和网络资源。下一代应用安全网关同时为 Apple iOS 和 Android 设备提供移动 VPN 应用程序。

访问 Apple 设备的移动 VPN

过程

1. 转到 https://<appliance__IP_address>，以使用 Safari 访问下一代应用安全网关 VPN 门户。

将显示**欢迎使用趋势科技移动 VPN 门户**页面。



图 3-6. 移动 VPN 登录

2. 指定有效的用户名和密码，然后按 **VPN 登录**。
将显示[从此处下载安全配置文件链接](#)。



图 3-7. 移动 VPN 安全配置下载

3. 按此处链接可安装 VPN 安全配置。
4. 按安装按钮。



图 3-8. 安装安全配置

5. 在未签名的安全配置警告中按现在安装。



图 3-9. 确认未签名的安全配置



图 3-10. 移动 VPN 安全配置摘要

- 按**完成**并返回到**登录**页面。
- 按**注销**链接可进行注销。



图 3-11. 已注销确认

更改苹果设备的移动 VPN 设置

更改移动 VPN 设置以从 iOS 设备访问公司内部资源。



注意

如果从下一代应用安全网关 Web 控制台启用“按需 VPN”，则当移动用户访问预定义的域或主机时，将自动建立移动 VPN 隧道。

过程

1. 登录移动 VPN 门户。有关详细信息，请参阅：[访问 Apple 设备的移动 VPN 第 3-75 页](#)

2. 转到**设置 > VPN**。



图 3-12. 更改移动 VPN 设置

3. 按**移动 VPN 趋势科技**以继续。



4. 键入有效的帐户和密码凭证，然后按**保存**返回到上一屏幕。
5. 交换机 打开。
将建立 VPN 连接。



图 3-13. 移动 VPN 连接状态显示

访问 Android 设备的移动 VPN

过程

1. 将浏览器指向以下网址访问下一代应用安全网关 VPN 门户：[https://<appliance_IP address>](https://<appliance_IP_address>).

将显示安全警告。



图 3-14. 访问移动 VPN 门户

2. 确认警告，然后单击**继续**。

将显示**欢迎使用趋势科技移动 VPN 门户**页面。



图 3-15. 趋势科技移动 VPN 登录

3. 指定有效的用户名和密码，然后按 **VPN 登录**。



图 3-16. 设置选项

4. 单击[此处](#)链接可下载证书。

将显示[提取证书](#)窗口。



图 3-17. 证书下载

5. 键入 `111111` 可提取证书。然后点击**确定**。



图 3-18. 添加证书名称

- 指定缺省的证书名称或将其重命名，然后按**确定**。
将下载证书文件。
- 返回到**设置选项**窗口。

后续步骤

点击**注销**可进行注销，或点击**此处**可以添加 VPN 连接。有关详细信息，请参阅 [为 Android 设备添加移动 VPN 连接 第 3-90 页](#)

为 Android 设备添加移动 VPN 连接

必须先添加移动 VPN 连接，Android 设备才可以建立 VPN 隧道并访问公司内部资源。



注意

与 Apple 设备不同的是，Android 设备不支持按需 VPN。

过程

1. 登录移动 VPN 门户。有关详细信息，请参阅[访问 Android 设备的移动 VPN 第 3-84 页](#)
2. 要添加新连接，请在**设置选项**窗口的 **2. 添加 VPN 连接**选项下点击[此处](#)。



图 3-19. 配置新 VPN 连接

3. 请按照以下步骤添加 VPN 连接：
 - a. 转到**设置 > 更多 > VPN > 添加 VPN 网络**。
 - b. 添加下列信息：

名称	指定名称。
类型	键入 IPSEC Xauth RSA
服务器地址	指定 VPN 网关服务器 IP 地址或 FQDN

IPSec 用户证书	选择之前安装的证书。有关详细信息，请参阅： 访问 Android 设备的移动 VPN 第 3-84 页
IPSec CA 证书	选择之前安装的证书。
IPsec 服务器证书	保留空白。

- 查看如何添加 VPN 连接之后注销。
- 登录并转到**设置 > 更多 > VPN > 添加 VPN 网络**。



图 3-20. 编辑 VPN 安全配置

- 按**保存**。
将显示新的安全配置。



图 3-21. 新的移动 VPN 安全配置

7. 按下要连接到下一代应用安全网关的新建 VPN 安全配置。



图 3-22. 连接到新的移动 VPN 安全配置

8. 键入有效的用户名和密码，然后按**连接**。



图 3-23. 已连接状态

定制 VPN 门户

可定制 VPN 门户登录页面以包含公司徽标、公司名称和欢迎消息

过程

1. 转到**网络 > 用户 VPN > 门户定制**。
2. 单击**浏览**查找徽标文件。



注意

使用 .PNG 或 .GIF 文件格式。不超过 700 x 60 像素，或者大小不能超过 1MB。

3. 单击**上传**以上传该文件。
4. 在**公司名称**文本框中键入一个值。
5. 在**欢迎消息**文本框中更新欢迎消息。
6. 单击**应用**。

站到站 VPN

虚拟专用网络 (VPN) 是采用加密隧道来交换受安全保护的数据的网络。下一代应用安全网关使用 Internet 密钥交换 (IKE) 和 IP 安全 (IPsec) 协议来创建加密的隧道。IKE 创建 VPN 隧道，此隧道可用于传输 IPSec 编码的数据。

可将 IKE 视为构建隧道的过程，而将 IPSec 数据包视为运输加密数据通过隧道的卡车。

下一代应用安全网关单元实施封装安全有效载荷 (ESP) 协议。加密数据包看起来与其他可通过任何 IP 网络的普通数据包一样。

IKE 基于预共享密钥或 X.509 数字证书自动运行。您也可以选择指定手动密钥。接口模式（仅 NAT/路由器模式中支持）为 VPN 隧道的本地端创建一个虚拟接口。

IPsec 连接

在安全网关上运行的动态路由协议守护程序，可以与在 **IPSec** 隧道/连接的另一端上运行的相邻路由守护程序交换路由信息。

IPsec（或 VPN）隧道是安全网关上与现有 VPN 连接相关联的虚拟接口，IP 路由将使用该接口作为直接与 VPN 对等网关连接的点对点接口。

出站数据包采用以下路由过程：

- 目标地址为 X 的 IP 数据包根据路由表进行匹配
- 路由表指示 IP 地址 X 应通过点对点链接（即，与对等网关 Y 相关联的 VPN 隧道接口）进行路由
- VPN 内核在该数据包指定虚拟隧道接口时截获该数据包
- 该数据包使用对等网关 Y 的适当 IPsec 认证类型参数进行加密，新的数据包收到对等网关 Y 的 IP 地址作为目标 IP。
- 该数据包根据新的目标 IP 以及 Y 地址的相应路由表条目重新路由到物理接口

入站数据包采用以下路由过程：

- IPsec 数据包从网关 Y 指定计算机
- VPN 内核在物理接口上截获该数据包
- VPN 内核识别原始 VPN 对等网关
- VPN 内核拆封该数据包，并提取原始 IP 数据包
- VPN 内核检测到对等 VPN 网关存在 VPN 隧道接口，并将该数据包从物理接口重新路由到相关联的 VPN 隧道接口
- 该数据包通过 VPN 隧道接口指定 IP 堆栈

添加新 IPsec 连接

使用**站到站 VPN** 在下一代应用安全网关之间建立 IPsec VPN 隧道。



注意

请确保以太网接口和路由器已正确配置。


过程

1. 转到**网络 > 站到站 VPN > 连接**。

2. 单击**新增**。

将显示**添加/编辑 IPsec 连接**对话框。

3. 指定 IPsec 连接参数。

启用 IPsec 连接	选择该复选框可启用隧道。
名称	键入一个名称以标识 IPsec 隧道。
网关类型	为 IPsec 隧道选择 发起 （主动）或 响应 （被动）角色。
网关	指定网关 IP 地址。
接口名称	从下拉列表框中选择接口名称（eth0、eth1）。
策略名称	<p>从下拉列表框中选择策略名称，选择缺省策略或特定策略，该策略将应用于 IPsec 隧道。</p> <hr/> <p> 注意 在网络 > 站到站 VPN > 策略中配置非缺省 IPsec 策略。</p> <hr/>
认证类型	从下拉列表框中选择 预共享密钥 或 RSA 密钥 。
对于预共享密钥	<p>指定密钥并确认。</p> <p>如果选择了预共享密钥，请指定下一代应用安全网关用于对远程对端或拨号客户端验证自己身份的预共享密钥。确保为远程对端或客户端定义相同的值。该密钥必须至少包含六个可打印字符，且应该只有网络管理员知道该密钥。为获得可抵御当前已知攻击的最佳防护，密钥至少应包含 16 个随机选择的字母数字字符。</p>
对于 RSA 密钥	<p>指定公共密钥。</p> <p>如果选择了RSA 密钥，请选择下一代应用安全网关用于向远程对端验证自己身份的服务器证书的名称。</p>
VPN ID	如果 IPsec 网关位于 NAT 设备之后，请输入本地 IP 地址。
添加本地网络	选择本地网络，或添加新的地址对象。
添加远程网络	选择远程网络，或添加新的地址对象。

4. 单击**应用**。
5. 验证新 IPsec 连接是否在**网络 > 站到站 VPN > 连接**中。

站到站 VPN 策略

下一代应用安全网关使您能够配置用于 VPN 策略的 IKE 加密和认证算法。

添加 VPN 站到站策略

过程

1. 转到**网络 > 站到站 VPN > 策略**。
2. 单击**新增**。
3. 为新 IPsec 策略指定名称。
4. 从下拉列表框中选择 **IKE 加密算法**：



注意

数字加密标准 (DES) 是使用 56 位密钥的 64 位块算法。高级加密标准 (AES) 是支持 128 到 256 位长度的密钥和可变长度数据块的私有密钥算法。

选项	说明
3DES	三重 DES，即，使用三个密钥对纯文本加密三次。
AES 128	使用 128 位密钥的 128 位块密码分组链接 (CBC) 算法。
AES 192	使用 128 位密钥的 192 位块密码分组链接 (CBC) 算法。
AES 256	使用 128 位密钥的 256 位块密码分组链接 (CBC) 算法。

5. 从下拉列表框中选择 **IKE 认证算法**值。

- **MD5** — 由 RSA Data Security 开发的消息摘要（版本 5）哈希算法（单向哈希函数），设计用于数字签名应用程序，其中大型文件在使用私有密钥/公共密钥算法加密前必须以安全方式进行压缩。
 - **SHA1** — 安全哈希算法 1，可生成 160 位消息摘要。大消息摘要可抵御强力冲突攻击和逆推攻击。
6. 从下拉列表框 (1-24) 中选择 **IKE SA 生命周期** 值（以小时为单位，最大值为 24）。该值指定了协商密钥的有效期。
7. 从下拉列表框中选择安全网关支持的 **IKE DH 组** 值。
- **Group2:MODP** — 1024 位（缺省值）
 - **Group5:MODP** — 1536 位
 - **Group14: MODP** — 2048 位
- 上述涉及 Diffie-Hellman 密钥计算（也称作指数密钥协议）的几个组基于 IKE 和 IPSec 安全协会 (SA) 的安全网关所支持的 Diffie-Hellman (DH) 数学组。
8. 从下拉列表框中选择 **IPSec 加密算法** 值。
- **无加密** — 不使用加密算法。
 - **3DES**
 - **AES 128**
 - **AES 192**
 - **AES 256**
9. 从下拉列表框中选择 **IPSec 认证算法** 值。
- **MD5**
 - **SHA1**
10. 从下拉列表框 (1-24) 中选择 **IPSec 生命周期** 值（以小时为单位，最大值为 24）。
11. 从下拉列表框中选择 **IPSec PFS 组** 值。

- 无
- Group2:MODP
- Group5:MODP
- Group14:MODP

12. 单击**应用**。

13. 验证新策略是否已列在**网络 > 站到站 VPN > 策略**中。

高级 IPsec 配置

网络 > 站到站 VPN > 高级选项中的站到站 VPN 的高级配置选项包括：

配置	描述
启用对端断线检测	对端断线检测通过 ICMP ping 识别非活动或不可用的 IKE 对端，可帮助恢复在对端不可用时丢失的资源。选择 启用对端断线检测 可在空闲连接上重建 VPN 隧道，并根据需要清除断线的 IKE 对端。使用此选项可在隧道打开或关闭时接收通知，或者在隧道内未生成任何网络通信时使隧道连接保持打开状态。例如，在动态 DNS 对端通过定期更改的 IP 地址进行连接的情况下，当 IP 地址发生更改时，网络通信可能会挂起。
IKE 调试	选中以下 IKE 调试选项的复选框： <ul style="list-style-type: none"> • 控制—用于显示 IKE 决策制定 • 发出报文—用于显示输出消息的结构 • 接收报文—用于显示输入消息的结构 • 原始内容—用于显示消息的原始内容字节数 • 算法信息—用于显示消息的加密状态和解密状态
当前本地公共 RSA 密钥	以一种可复制、可指定到使用 IPSec RSA 认证的远程设备的格式来显示本地 RSA 密钥的当前公共部分。

配置	描述
重新生成本地 RSA 密钥	重新生成具有不同密钥长度的本地 RSA 密钥，并覆盖当前安装的 RSA 密钥。

IPSec 状态

要查看实时 IPSec 连接状态，请转到**网络 > 站到站 VPN > 状态**选项卡。

IPsec 问题排查

通过**网络 > 站到站 VPN > 问题排查**显示实时 IPSec 日志。使用 IPSec 日志可查看 IPSec VPN 隧道上的活动。

IPsec 问题排查：分支机构配置示例

在第一个示例中，两个分支办公室连接到同一个总部办公室。

总部:	公共 IP 1.1.1.1，在接口 eth0 上。本地网络为 10.0.0.0/8
分支办公室 1:	公共 IP 2.2.2.1，在接口 eth0 上。本地网络为 192.168.10.0/8
分支办公室 2:	公共 IP 3.3.3.1，在接口 eth0 上。本地网络为 192.168.20.0/8

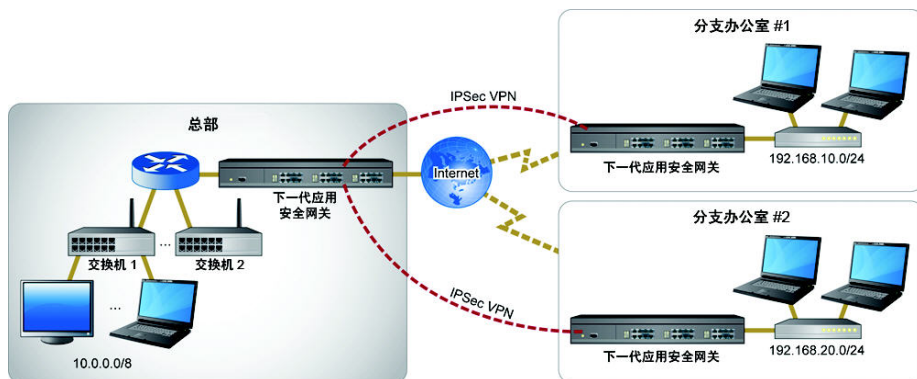


图 3-24. 下一代应用安全网关通过 IPSec VPN 连接两个分支办公室

表 3-6. VPN 连接配置

位置	配置
总部	名称: HQ 启用: 是 网关类型: 响应 接口名称: Eth0 策略名称: 缺省 认证类型: 预共享密钥 密钥: ***** 本地网络: 10.0.0.0/24 远程网络: 192.168.10.0/24 和 192.168.20.0/24

位置	配置
分支办公室 1	名称: toHQ1 启用: 是 网关类型: 发起 网关: 1.1.1.1 接口名称: Eth0 策略名称: 缺省 认证类型: 预共享密钥 密钥: ***** 本地网络: 192.168.10.0/24 远程网络: 10.0.0.0/24
分支办公室 2	名称: toHQ1 启用: 是 网关类型: 发起 网关: 1.1.1.1 接口名称: Eth0 策略名称: 缺省 认证类型: 预共享密钥 密钥: ***** 本地网络: 192.168.10.0/24 远程网络: 10.0.0.0/24

IPsec 问题排查: NAT 设备的后端配置

在第二个示例中, 下一代应用安全网关位于 NAT 设备后面。

NAT-A:	公共 IP 202.101.1.1, NAT 将 192.168.1.2 转换为 202.101.1.3
DeepEdge-A:	内部 IP 192.168.1.2, 在接口 eth0 上。本地网络为 172.16.1.0/24
NAT-B:	公共 IP 202.101.2.1, NAT 将 202.101.2.3 转换为 192.168.2.2

DeepEdge-B:	内部 IP 192.168.2.2，在接口 eth0 上。本地网络为 172.16.2.0/24
--------------------	--

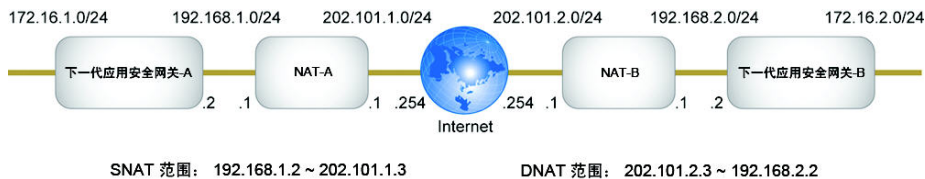


图 3-25. 下一代应用安全网关 VPN 位于 NAT 设备后面

表 3-7. VPN 连接配置

位置	配置
下一代应用安全网关-A	名称: toB 启用: 是 网关类型: 发起 网关: 202.101.2.3 接口名称: Eth0 策略名称: 缺省 认证类型: 预共享密钥 密钥: ***** 本地网络: 172.16.1.0/24 远程网络: 172.16.2.0/24 VPN ID: 192.168.1.2

位置	配置
下一代应用安全网关-B	名称: toA 启用: 是 网关类型: 响应 接口名称: Eth0 策略名称: 缺省 认证类型: 预共享密钥 密钥: ***** 本地网络: 172.16.1.0/24 远程网络: 172.16.2.0/24

第 4 章

策略、对象和安全

下一代应用安全网关使用策略、策略对象和安全设置来提供方便日常部署和管理的现代防火墙功能。下一代应用安全网关可阻止代价高昂的事件（如扫描程序、恶意代码、拒绝服务攻击和其他威胁），这些事件会导致数据丢失或被盗、端点受感染以及其他妨害生产力的意外事件。提供的保护包括双向状态检查、附有可配置对象的集中式目标策略、IPv4 和 IPv6 支持、用户和组支持、日志以及报告。

本章包括以下内容：

- [关于策略 第 4-2 页](#)
- [关于策略对象 第 4-9 页](#)
- [关于安全设置 第 4-33 页](#)
- [关于 HTTPS 检查 第 4-46 页](#)
- [关于带宽控制 第 4-52 页](#)
- [关于黑/白名单 第 4-58 页](#)
- [关于防 DoS 第 4-60 页](#)
- [关于认证 第 4-63 页](#)
- [关于用户通知 第 4-67 页](#)

关于策略

策略可通过执行规则和自动采取处理措施来控制防火墙操作。根据应用程序、源和目标区域和地址、源用户以及（可选）服务（端口和协议）配置安全策略以阻止或允许网络会话。

防火墙策略如何工作

防火墙策略用于控制在下一代应用安全网关接口、区域和 VLAN 子接口之间进行传输并尝试通过下一代应用安全网关单元的所有网络通信。

防火墙策略是下一代应用安全网关单元用于决定连接接受和处理企图通过的网络通信的数据包的指导信息。防火墙接收连接数据包时，会分析该数据包的源地址、目标地址和服务（根据端口号），并尝试找到与该数据包匹配的防火墙策略。

防火墙策略可以包含下一代应用安全网关接收匹配的数据包时要遵循的许多指导信息。有些指导信息是必需的（例如，删除还是接受并处理数据包），而有些指导信息（例如，登录和认证）是可选的。

策略指导信息可以包含防护安全配置，该安全配置可以指定应用层检查和其他特定于协议的防护和日志记录。

防火墙策略与其他下一代应用安全网关功能相集成，针对以下内容提供了一个集中式策略配置和管理体系结构：

- 防病毒、间谍软件和电子邮件策略
- 网络入侵防御策略（请参阅[网络入侵防御 第 4-34 页](#)）
- URL 类别对象（请参阅[关于 URL 类别对象 第 4-16 页](#)）

关于策略规则

根据需要，安全策略可以是通用的，也可以是特定的。策略规则依次与传入网络通信进行比较，因为会应用第一个与网络通信相匹配的规则，所以特定规则

必须位于通用规则之前。例如，如果与网络通信相关的所有其他设置均相同，则针对单个应用程序的规则必须位于适用于所有应用程序的规则之前。如果网络通信与所有规则都不匹配，则网络通信将被阻止。

要创建策略规则，需要先创建一些用于定义策略规则参数的策略对象。有关详细信息，请参阅[关于策略规则 第 4-2 页](#)。

通过**策略 > 规则**下的**策略**页面，用户可以：

- 查看现有规则的列表
- 添加、复制和删除规则
- 启用或禁用规则

添加策略规则

策略规则可根据指定的网络通信属性确定是允许还是阻止网络会话。创建新规则后，通过使用选项卡指定相应的信息来配置规则。

过程

1. 转到**策略 > 规则**。
2. 单击**新增**。
3. （可选）启用规则。
4. 指定包含 1 到 32 个字符的策略名称，由字母、数字和下划线组成。
5. 键入可选的**描述**。
6. 也可以选择**启用 Internet 访问日志**。



重要信息

要捕获流量日志，请启用**分析和报告 > 日志设置**下的 Internet 访问日志和过滤条件。有关详细信息，请参阅[日志设置 第 5-38 页](#)。

7. 配置源地址和用户规则。

请参阅 [配置源和用户策略规则](#) 第 4-4 页。

8. 配置目标地址规则。

请参阅 [配置目标策略规则](#) 第 4-5 页。

9. 配置通信类型规则。

请参阅 [配置通信类型策略规则](#) 第 4-6 页。

10. 配置时段和带宽规则。

请参阅 [配置时段和处理措施安全配置策略规则](#) 第 4-8 页。

11. 单击**确定**。

配置源和用户策略规则

开始之前

在**策略 > 规则 > 新增**添加新的策略。有关详细信息，请参阅[添加策略规则](#) 第 4-3 页。

使用**源和用户**选项卡定义对来自指定的源 IP 地址、源用户和组和/或源区域的通信强制实施的规则。

过程

1. 单击**源和用户**选项卡。
 2. 在**源地址**下，选择以下参数之一：
 - **任何**：包括所有源地址。（缺省）
 - **选择地址**：显示之前配置的可用的源地址列表或添加新的 IP 地址。
-



要添加新地址对象，请参阅[配置地址对象](#) 第 3-8 页。

3. 从**用户和组**下的以下选项中选择

选项	说明
任何人	规则会影响所有已知和未知的用户。
已知用户	规则通过网页认证影响认证的用户，或通过透明认证影响识别的用户。有关用户识别的详细信息，请参阅 关于认证 第 4-63 页 。
未知用户	规则会影响透明认证无法识别的用户。有关用户识别的详细信息，请参阅 关于认证 第 4-63 页 。
选定的用户	规则影响指定的用户和组（本地用户或 LDAP）。有关用户管理的详细信息，请参阅 终端用户管理 第 6-9 页 。

4. 选中**启用源区域规则**以启用源区域。
- **任何：**包括所有源区域。
 - **选定的区域：**提供了**新增**区域选项。有关添加区域的详细信息，请参阅[配置区域对象 第 4-10 页](#)

后续步骤

继续配置以下内容：

- 要配置目标地址，请参阅[配置目标策略规则 第 4-5 页](#)
- 要配置通信类型，请参阅[配置通信类型策略规则 第 4-6 页](#)
- 要配置时间表和处理措施，请参阅[配置时段和处理措施安全配置策略规则 第 4-8 页](#)

配置目标策略规则

开始之前

- 在**策略 > 规则 > 新增**添加新的策略。有关详细信息，请参阅[添加策略规则 第 4-3 页](#)。
- （可选）按照[配置源和用户策略规则 第 4-4 页](#)中所示配置源和用户。

使用**目标**选项卡为在指定 IP 地址和目标区域结束的网络通信定义规则。

过程

1. 单击**目标**选项卡。
2. 在**目标地址**下，选择以下参数之一：
 - **任何**：包括所有目标地址
 - **选定的地址**：显示先前配置的目标地址的可选列表，以供使用。如果需要，使用此选项添加地址对象。



注意

要添加目标地址，请参阅[配置地址对象 第 3-8 页](#)

3. 选中**启用目标区域规则**复选框以启用目标区域。
 - **任何**：包括所有源区域。
 - **选定的区域**：提供了**新增**区域选项。有关添加区域的详细信息，请参阅[配置区域对象 第 4-10 页](#)

后续步骤

继续配置以下内容：

- 要配置通信类型，请参阅[配置通信类型策略规则 第 4-6 页](#)
- 要配置时间表和处理措施，请参阅[配置时段和处理措施安全配置策略规则 第 4-8 页](#)

配置通信类型策略规则

开始之前

- 在**策略 > 规则 > 新增**添加新的策略。有关详细信息，请参阅[添加策略规则 第 4-3 页](#)。
- （可选）配置源地址和用户，如[配置源和用户策略规则 第 4-4 页](#)中所示
- （可选）配置目标地址，如[配置目标策略规则 第 4-5 页](#)中所示。

使用**通信类型**选项卡为与任何指定应用程序、URL 类别或服务匹配的网络通信定义规则。

过程

1. 单击**通信类型**选项卡。
2. 在**应用程序**和 **URL 类别**下，选择以下参数之一：
 - **任何**：包括所有应用程序组和 URL 类别（缺省）
 - **选定**：仅包括选定的应用程序类别和 URL 类别



注意

有关添加新的应用程序、URL 类别组或定制 URL 类别的详细信息，请参阅：

- [添加新应用程序对象 第 4-14 页](#)
- [添加新 URL 类别对象 第 4-23 页](#)
- [添加定制 URL 类别 第 4-25 页](#)

-
3. 选中**启用服务规则**以对特定服务强制实施规则。
 - **任何**：包括所有服务
 - **选定**：仅包括选定的服务

有关添加服务对象的详细信息，请参阅[添加定制服务对象 第 4-13 页](#)

后续步骤

继续配置时间表和处理措施，如[配置时段和处理措施安全配置策略规则 第 4-8 页](#)中所示。

配置时段和处理措施安全配置策略规则

开始之前

- 在**策略 > 规则 > 新增**添加新的策略。有关详细信息，请参阅[添加策略规则 第 4-3 页](#)。
- 配置源地址和用户，如[配置源和用户策略规则 第 4-4 页](#)中所示
- 配置目标地址，如[配置目标策略规则 第 4-5 页](#)中所示。
- 配置通信类型，如[配置目标策略规则 第 4-5 页](#)中所示。

使用**时段和处理措施安全配置**选项卡为规则定义在通信匹配策略时的时间表和处理措施。

过程

1. 单击**时段和处理措施安全配置**选项卡。
2. 从**时间表**下拉列表中选择以下选项之一：

选项	说明
始终	包括所有时间表。（缺省）
时间表名称	显示可用的时间表对象的名称。
新增	访问 添加/编辑 时间表对象创建对话框。



注意

有关时间表对象的详细信息，请参阅[关于时间表和时间表对象 第 4-27 页](#)。

3. 从下拉列表中选择**处理措施**。



注意

有关处理措施安全配置的信息，请参阅[关于处理措施安全配置 第 4-30 页](#)。

4. 单击**确定**。

启用/禁用策略规则

可在提供策略时将其禁用。此过程适用于已创建但并未启用的策略规则。

过程

1. 转到**策略 > 规则**。
2. 单击要启用或禁用的策略规则的名称
3. 执行下列操作之一：
 - 选中此复选框以启用策略
 - 取消选中此复选框以禁用策略
4. 单击**确定**。

关于策略对象

策略对象是使您能够构造、预设和搜索策略的元素。支持以下元素类型：

表 4-1. 策略对象

对象	描述
地址对象	确定策略的范围。请参阅 关于地址和地址对象 第 3-6 页 。
区域对象	将接口和 VLAN 子接口分组到区域中以便简化策略创建。请参阅 关于区域和区域对象 第 4-10 页 。
服务对象	限制协议（TCP 或 UDP）和端口号。请参阅 关于服务和服务对象 第 4-12 页 。
应用程序对象	指定如何处理策略中的软件应用程序。请参阅 关于应用程序和应用程序对象 第 4-14 页 。
URL 类别对象	限制访问特定 Web 站点和 Web 站点类别。请参阅 关于 URL 类别对象 第 4-16 页 。

对象	描述
时间表对象	指定策略活动时间。请参阅 关于时间表和时间表对象 第 4-27 页 。
处理措施安全配置对象	控制针对特定安全策略识别的网络通信类型而采取的处理措施。请参阅 关于处理措施安全配置 第 4-30 页 。

关于地址和地址对象

地址对象影响策略和网络设置。地址对象可确定内部网络中允许的 IP 地址范围。缺省情况下，下一代应用安全网关包括所有内部 IP 地址范围。要为特定源或目标地址设置安全策略，首先请在网络设置中定义地址和地址范围。

转到**网络 > 地址**。

关于区域和区域对象

将接口和 VLAN 子接口分组到区域中可简化策略创建，更快创建策略和防火墙规则。可配置连接到区域和从区域连接的策略，但无法为区域内接口之间的连接配置策略。可添加、重命名或编辑区域，以及从区域列表中删除区域。添加区域时，选择要添加到区域的接口和 VLAN 子接口的名称。

应从物理网络适配器配置区域。

配置区域对象

添加区域对象可以使策略创建变得更快、更简单。为了使防火墙接口能够处理网络通信，必须将其分配到安全区域。当定义安全策略并配置接口时，区域名称会显示在区域列表中。

过程

1. 转到**策略 > 对象 > 区域**。

2. 单击**新增**。
 3. 指定下列参数：
 - **对象名称**
 - **描述**
 4. 在**接口**中，单击 + 以从右侧窗格中添加任何适用的接口。
 5. 单击**确定**。
 6. 验证新的区域是否显示在**策略 > 对象 > 区域**的列表中。
-

查看区域

必须先配置区域对象，然后这些区域对象才显示在区域列表中。


过程

- 转到**策略 > 对象 > 区域**。
-

删除区域对象

无法删除已分配给策略的区域对象。

过程

1. 转到**策略 > 对象 > 区域**。
 2. 选中要删除的对象所在行对应的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

对象即被移除。

关于服务和服务对象

为特定应用程序定义安全策略时，选择一个或多个服务来限制应用程序可使用的端口号。缺省服务为所有，允许所有 TCP 和 UDP 端口。

下一代应用安全网关提供超过 100 种预定义服务（DNS、FTP、HTTP、POP3、SMTP、SSL 和 TELNET）。如果需要，也可以添加定制服务定义。

提供了以下功能：

- [添加定制服务对象 第 4-13 页](#)
- [查看定制服务对象 第 4-13 页](#)
- [删除定制服务对象 第 4-14 页](#)

服务对象参数

使用下表中的参数来定义服务。

表 4-2. 服务对象参数

参数	描述
服务对象名称	定义安全策略时，此名称将显示在服务列表中。此名称区分大小写，且必须是唯一的。仅使用字母、数字、空格、连字符和下划线。
协议	选择该服务使用的任何协议或创建定制服务。
目标端口	对于定制服务，指定服务使用的端口号（0 到 65535）或端口号范围（端口 1 - 端口 2）。多个端口或范围之间必须用逗号隔开。

添加定制服务对象

过程

1. 转到**策略 > 对象 > 服务 > 定制服务**。
2. 单击**新增**。
3. 指定下列信息：
 - **对象名称**
 - **协议**
 - **目标端口**
 - **描述**



注意

目标端口可以是单一端口 (22)、多个单一端口 (22、23)、端口范围 (22-80) 或这些选项的任意组合。最多允许使用 15 个端口段。

4. 单击**确定**。
 5. 验证新的服务对象是否已在**策略 > 对象 > 服务 > 定制服务**中列出。
-


查看定制服务对象

过程

- 转到**策略 > 对象 > 服务 > 定制服务**。
-

删除定制服务对象

过程

1. 转到**策略 > 对象 > 服务 > 定制服务**。
2. 选中要删除的对象所在行对应的复选框。
3. 单击**删除**图标 。
4. 在确认对话框中单击**删除**。

对象即被移除。

关于应用程序和应用程序对象

近几年，基于 Internet 的应用程序日益流行，其使用量甚至已经超过了用于访问 Web 站点的浏览器。即使有公司使用策略的明文规定，许多公司也无力限制和监管这些应用程序的使用。最新的研究结果表明，75% 到 80% 的公司用户无视公司的端点使用策略。为了避免重大风险，下一代应用安全网关应用程序控制会自动发现热门 Internet 应用程序，并允许您设置限制应用程序访问的策略。

通过下一代应用安全网关，可以查看并控制在任何端口上运行的将近 1000 种应用程序类型，其中包括使用定制客户端的应用程序（例如，Skype、BitTorrent、P2P）或在浏览器中使用 Web 2.0 技术的应用程序（例如，社交网络、webmail 和流媒体站点）。可灵活控制应用程序，也可以允许应用程序，但对应用程序内的活动（如上传文件、观看视频或玩特定游戏）进行粒度控制。

添加新应用程序对象

可以添加一个新应用程序组，以便将不同应用程序类别中的多个应用程序合并为一个组。向该组添加特定的应用程序，从而可以对所有已添加的应用程序应用策略。例如，对一系列禁止的应用程序（包括 iTunes™、MSN Messenger®、

Netflix™ 和 Facebook™) 进行分组。缺省情况下, 这些应用程序属于不同的应用程序类别。

要避免创建多个策略阻止特定的应用程序, 可以对这些应用程序进行分组, 以允许一个策略来阻止这些应用程序。

过程

1. 转到**策略 > 对象 > 应用程序**。
2. 单击**新增**。
3. 指定新应用程序对象的名称和描述。
4. 展开要包括在应用程序组中的相应应用程序类别。
5. 选择要包含在应用程序组中的应用程序类别内的任何应用程序的复选框。
6. 单击**确定**。

新应用程序对象将添加到列表中。


查看/编辑应用程序对象

过程

1. 转到**策略 > 对象 > 应用程序**。
 2. 单击相应应用程序对象的名称。
 3. 查看应用程序对象和/或修改选择。
 4. 单击**确定**。
-

删除应用程序对象

过程

1. 转到**策略 > 对象 > 应用程序**。
 2. 选中要删除的对象所在行对应的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

对象即被移除。

关于 URL 类别对象

URL 过滤安全配置用于限制访问特定 Web 站点和 Web 站点类别。每个安全策略可以指定一个 URL 过滤安全配置，该 URL 过滤安全配置可阻止访问特定 Web 站点和 Web 站点类别或当指定的 Web 站点被访问时生成警报。Web 类别由趋势科技进行了预定义。

URL 过滤模块提供了用于创建和配置在 URL 过滤策略中使用的安全配置的步骤。URL 过滤以及 Web 信誉都是下一代应用安全网关提供的多层次、多威胁防护解决方案的一部分。

通过下一代应用安全网关中的“URL 过滤”功能，根据 URL 的类别（例如，“成人”、“赌博”和“金融服务”）来设置策略。用户请求 URL 时，下一代应用安全网关首先在类别中查找该 URL，然后根据配置的策略允许或拒绝其访问该 URL。也可以定义不会被过滤的白名单列表。

URL 过滤类别组

下表显示了 URL 过滤组和类别。

表 4-3. URL 类别的分组定义

类别组	描述
成人	通常认为对儿童不宜的 Web 站点
商业	与商业、就业或贸易相关的 Web 站点
聊天搜索	为在线通信和搜索提供工具和服务的 Web 站点。
一般	不属于或未分类为其他类别的 Web 站点。
网络安全	潜在有害的 Web 站点，包括那些已知分发恶意软件的 Web 站点
生活	与宗教、政治或性取向以及休闲娱乐有关的 Web 站点
网络带宽	提供的服务可能会严重影响端点的 Internet 连接速度的 Web 站点

URL 过滤类别

下表列出了各个 URL 过滤类别以及分组的定义。

表 4-4. URL 过滤类别定义

类别组	类别类型	类别定义
成人	堕胎	宣传、鼓励或讨论堕胎的站点，包括涉及有关堕胎的道德或政治观点的站点
成人	成人/未成年人不宜内容	具有通常认为对未成年人不宜的粗俗或低级趣味内容的站点；包括提供色情内容或性服务广告的站点，但不包括具有色情图片的站点
成人	酒精/烟草	宣传、销售或提供有关酒精或烟草产品信息的站点
成人	赌博	宣传或提供有关赌博信息的站点，包括在线赌博站点。
成人	非法毒品	散布、宣扬、供应、销售或阐述如何使用违法或非法麻醉品的站点

类别组	类别类型	类别定义
成人	非法/可疑内容	宣传和讨论如何实施非暴力犯罪（包括盗窃、欺诈、知识产权窃取和剽窃）的站点；包括销售剽窃物品或赃物的站点
成人	内衣/泳装	销售泳装或内衣且具有模特展示的站点
成人	大麻	讨论种植、使用或制备大麻，或者销售相关制品的站点
成人	裸体	展示通常视为艺术而非庸俗或淫秽内容的全裸或半裸图片的站点
成人	色情内容	含有能唤起性欲的性暴露图片的站点，包括提供性服务的站点
成人	性教育	讨论生殖、性倾向、节育、性病、安全性行为或应对性创伤的站点（提供或未提供明确的图片）
成人	粗俗的内容	含有无故令人讨厌和恐惧的内容的站点；包括展示以极端形式整形或自残以及虐待动物的站点
成人	暴力/仇恨/种族歧视	宣扬仇恨和暴力的站点；包括支持对某一社会群体的偏见、极端暴力和危险活动、肢体残毁和刺伤或制造破坏性装置的站点
成人	武器	与武器（包括其配件和使用）有关的站点；与军事机构有关的站点或将武器作为体育或娱乐设施讨论的站点除外
商业	拍卖	为以竞拍方式销售或购买商品提供平台的站点，包括正在拍卖的商业站点
商业	经纪/贸易	有关股票或债券投资的站点，包括在线交易站点；包括有关车险的站点
商业	商业/经济	与商业和经济（包括创业与营销）有关的站点；包括不属于其他类别的公司站点
商业	金融服务	提供金融服务相关信息或提供基本金融服务的站点，包括金融行业的企业所拥有的站点

类别组	类别类型	类别定义
商业	职位搜索/职业	有关搜索工作职位或就业服务的站点
商业	房地产	与房地产有关的站点，包括协助销售、租赁、购买或出租房屋的站点
商业	购物	销售商品或支持销售不属于其他类别的商品的站点；但不包括在线拍卖或竞拍站点
聊天搜索	博客/Web 通信	涉及各种主题或者其他类别未涵盖的主题的博客站点或论坛；提供多种类型的 Web 通信方式（例如，电子邮件或即时通讯）的站点
聊天搜索	聊天/即时通讯	提供基于 Web 的服务或基于文本的即时通讯或聊天的可下载软件的站点
聊天搜索	电子邮件	提供电子邮件服务的站点，包括公司为基于 Web 的电子邮件所使用的门户
聊天搜索	Internet 基础架构	内容服务器、镜像服务器或用于收集、处理和显示数据及数据分析的站点，包括基于 Web 的分析工具和网络监控程序
聊天搜索	Internet 电话	为 Voice Over Internet 协议 (VoIP) 呼叫提供 Web 服务或可下载软件的站点
聊天搜索	新闻组	可以访问 Usenet 或者提供其他新闻组、论坛或电子公告牌服务的站点
聊天搜索	搜索引擎/门户	为 Web 提供目录、索引或其他检索系统的搜索引擎站点或门户
聊天搜索	社交网络	旨在表达和交流个人思想，并将志趣相投的人联系起来的人联系起来的站点
聊天搜索	Web 托管	提供顶级域或 Web 托管服务的组织站点
一般	计算机/Internet	有关端点、Internet 或相关技术的站点，包括销售或审查电子设备的站点
一般	教育	学校站点、远程教育站点和其他与教育相关的站点

类别组	类别类型	类别定义
一般	政府/法律	有关政府（包括法律或政策）的站点；但不包括政府军事或医疗站点
一般	健康	有关健康、瘦身或养生的站点
一般	军事	有关军事机构或武装力量的站点；但不包括讨论或销售武器或军事装备的站点
一般	新闻/媒体	与新闻、时事、当今问题或天气有关的站点；包括主题不属于其他类别的在线杂志
一般	政治	讨论政党、利益集团或参与公共政策问题的类似组织或者由这些组织资助的站点；包括讨论阴谋活动或与政府有关的不同观点的非仇恨站点
一般	参考资料	一般及专业参考站点，包括地图、百科全书、字典、天气、操作方法和换算站点
一般	翻译器/缓存页	可用于规避代理服务器和 Web 过滤系统的在线页面翻译器或缓存 Web 页面（由搜索引擎使用）
一般	未经测试的	尚未分类为任一类别的站点
一般	汽车	与机动车辆（包括定制、采购零部件和实际车辆）或维修服务有关的站点；与军用车辆有关的站点除外
网络安全	为 AdSense 而制作的站点 (MFA)	使用废弃或复制的内容污染包含冗余和不需要的结果的搜索引擎的站点
网络安全	潜在的恶意软件	含有潜在有害下载项的站点
网络安全	代理规避	与绕过代理服务器或 Web 过滤系统有关的站点，包括为此目的提供工具的站点
网络安全	Web 广告	专门显示广告的站点，包括用于显示横幅或弹出广告的站点

类别组	类别类型	类别定义
生活	激进团体	散布公共政策变更、公共舆论、社会实践、经济活动或经济关系的站点，包括由服务机构、慈善机构、专业机构或劳工组织控制的站点
生活	另类杂志	超市海报和其他附加出版物的在线替代品
生活	艺术	有关视觉艺术（如绘画和雕塑）的站点
生活	迷信/灵异	有关其他宗教、信仰和宗教习俗的站点，包括被认为是迷信或灵异的站点
生活	文化机构	由力图保护文化遗产的组织（如图书馆和博物馆）控制的站点；也包括男童子军、女童子军、国际扶轮社和其他类似组织所拥有的站点
生活	娱乐	宣传或提供有关电影、音乐、非新闻广播和电视、书籍、笑话或杂志的信息的站点
生活	适合儿童	专为儿童设计的站点
生活	游戏	有关棋盘游戏、纸牌游戏、主机游戏或端点游戏的站点；包括销售游戏或相关商品的站点
生活	男同性恋/女同性恋	有关男同性恋、女同性恋、变性或双性恋的站点
生活	枪支俱乐部/狩猎	有关枪支俱乐部或其他类似团体的站点；包括有关狩猎、作战游戏或彩弹射击游戏装备的站点
生活	笑话	笑话站点。
生活	个人站点	由个人维护的关于其自身情况或兴趣的站点；但不包括社交网络站点、博客站点中的个人页面或其他类似服务
生活	交友/约会	帮助访问者建立关系的站点，包括提供单身人士列表、做媒或约会服务的站点

类别组	类别类型	类别定义
生活	消遣娱乐/爱好	与休闲活动和爱好（例如，收藏、园艺、户外活动、传统的非视频游戏以及工艺）有关的站点；包括与宠物、娱乐设施或休闲组织有关的站点
生活	宗教	有关民间宗教、宗教习俗或祈祷场所的站点
生活	餐馆/饮食	罗列、评论、讨论、宣扬或促销食品、饮食、餐饮服务、烹饪或食谱的站点
生活	社会/生活方式	提供与生活或日常事务有关的信息的站点；与娱乐、兴趣爱好、性或运动有关的站点除外，但包括与化妆品或时装有关的站点
生活	运动	与体育或其他竞技活动有关的站点；包括粉丝站点或销售体育商品的站点
生活	旅游	有关旅游或旅游目的地的站点；包括旅游预定和规划站点
网络带宽	Internet 广播和电视	主要提供流媒体广播或电视节目的站点；但不包括提供其他类型的流媒体内容的站点
网络带宽	上网付费	对查看某些 Web 站点、电子邮件或广告的用户以及单击链接或响应调查的用户给予补偿的站点
网络带宽	点对点	提供与在点对点 (P2P) 网络中共享和传输文件所用软件相关的信息的站点
网络带宽	专用网络存储/文件下载服务器	提供个人在线存储空间、备份或托管空间的站点，包括提供加密或其他安全服务的站点
网络带宽	照片搜索	主要托管图片的站点，用户可以共享、组织、存储或搜索照片或其他图片
网络带宽	铃声/移动电话下载	为移动设备提供内容（如铃声、游戏或视频）的站点

类别组	类别类型	类别定义
网络带宽	软件下载	专门提供免费、试用或付费软件下载的站点
网络带宽	流媒体/MP3	提供不含广播或电视节目的视频或音频流的站点；提供音乐或视频下载（如 MP3 或 AVI 文件）的站点

添加新 URL 类别对象

过程

1. 转到**策略 > 对象 > URL 类别**。
2. 单击**新增**。
将显示**添加/编辑 URL 类别组**窗口。
3. 为新的 URL 类别组指定名称和可选描述。
4. 展开要包括的相应的类别。
5. 选中要包含的内容对应的复选框。

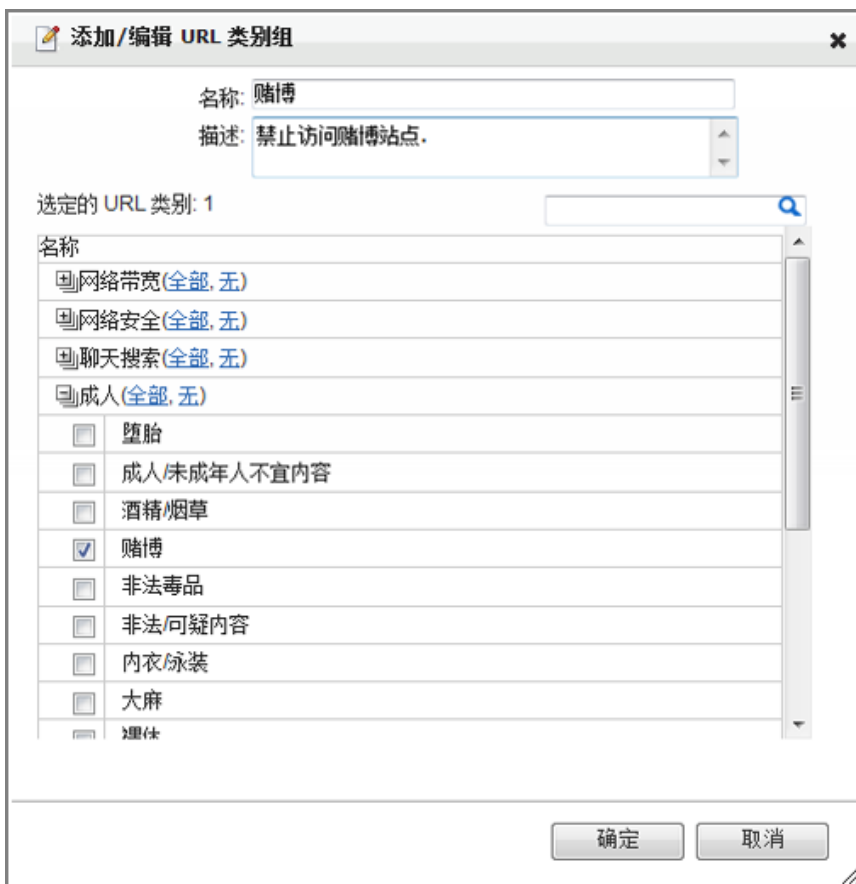


图 4-1. 用于限制赌博 Web 站点的 URL 类别组

6. 单击**确定**。

已将新的 URL 类别组添加到列表中。


修改 URL 过滤类别对象

过程

1. 转到**策略 > 对象 > URL 类别**。
 2. 单击要修改的 URL 类别对象的名称。
 3. 在**编辑 URL 类别组**对话框中进行更改。
 4. 单击**确定**。
-

删除 URL 类别对象

过程

1. 转到**策略 > 对象 > URL 类别**。
 2. 选中要删除的对象所在行对应的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

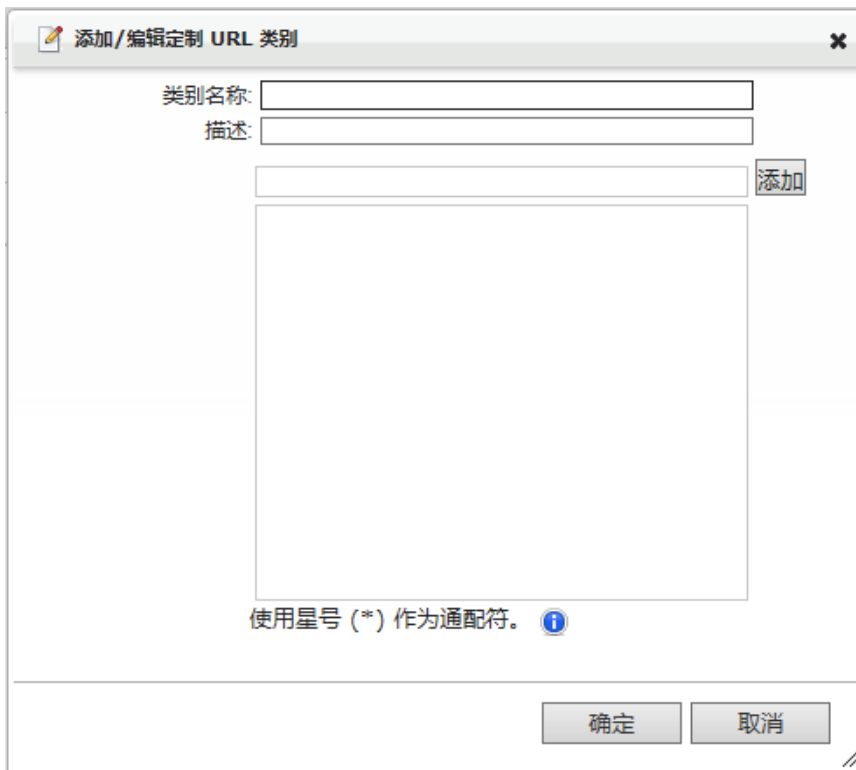
对象即被移除。

添加定制 URL 类别

过程

1. 转到**策略 > 对象 > URL 类别**。
2. 打开**定制 URL 类别**选项卡。
3. 单击**新增**。

将显示**添加/编辑定制 URL 类别**窗口。



4. 指定定制 URL 类别名称。
5. 指定 URL 类别描述。
6. 指定一个 URL，然后单击**添加**。

 **注意**

在 URL 的开头或结尾插入通配符 (*) 以与 0 或更多字符匹配。示例：
.example.com、www.example.com/。

7. 单击**确定**。
-

关于时间表和对象

缺省情况下，每个安全策略适用于所有日期和时间。要将安全策略限制在特定时间内，可以定义时间表，然后将这些时间表应用到相应策略。时间表对象可能包含多个固定的日期和时间范围。

要为安全策略应用时间表，请参阅[关于安全设置 第 4-33 页](#)。

添加时间表对象

过程

1. 转到**策略 > 对象 > 时间表**。
2. 单击**新增**。

将显示**添加/编辑时间表对象**窗口。

添加/编辑时间表对象

名称:

描述:

	周日	周一	周二	周三	周四	周五	周六
↑ 08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
↓ 18:00							

3. 指定**名称**。
 4. 指定**描述**。
 5. 单击并拖动以选择适用的时间段。
 6. 单击**确定**。
 7. 验证新的时间表对象是否已添加到**策略 > 对象 > 时间表**下的列表中。
-


编辑时间表对象

过程

1. 转到**策略 > 对象 > 时间表**。
 2. 单击要更改的时间表对象的名称。
 3. 根据需要在**添加/编辑时间表对象**对话框中进行更改。
 4. 单击**确定**。
-

删除时间表对象

过程

1. 转到**策略 > 对象 > 时间表**。
 2. 选中要删除的对象所在行对应的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

对象即被移除。

关于处理措施安全配置

处理措施安全配置中包含了针对特定安全策略识别的网络通信类型而采取的处理措施的详细信息。缺省情况下，每个安全策略允许采取一个处理措施。要为安全策略指定处理措施，可以使用为特定网络通信提供的缺省处理措施安全配置，或定义特定网络通信的处理措施安全配置，并将其应用到相应策略。

要查看处理措施安全配置，请转到**策略 > 对象 > 处理措施安全配置**。

预定义的处理措施安全配置

要查看预定义的处理措施安全配置，请转到**策略 > 对象 > 处理措施安全配置 > 预定义安全配置**。

下一代应用安全网关缺省处理措施安全配置包括：

表 4-5. 预定义的处理措施安全配置

操作	描述
深度扫描	深度扫描 预定义的处理措施安全配置执行以下操作： <ul style="list-style-type: none">对网络通信中的恶意内容进行扫描，以阻止病毒、特洛伊木马、蠕虫病毒和僵尸网络启用 Web 信誉扫描，以阻止信誉分数较低的站点启用入侵防御，以阻止恶意行为
常规扫描	常规扫描 预定义的处理措施安全配置执行以下操作： <ul style="list-style-type: none">对网络通信中的恶意内容进行扫描，以阻止病毒、特洛伊木马、蠕虫病毒和僵尸网络启用 Web 信誉扫描，以阻止信誉分数较低的站点启用入侵防御，以记录恶意行为

操作	描述
恶意软件扫描	<p>恶意软件扫描 预定义的处理措施安全配置执行以下操作：</p> <ul style="list-style-type: none"> 对网络通信中的恶意内容进行扫描，以记录任何病毒、特洛伊木马、蠕虫病毒或僵尸网络活动 启用 Web 信誉扫描，以阻止信誉分数较低的站点 启用入侵防御扫描，以记录恶意行为
扫描以供记录	<p>扫描以供记录 预定义的处理措施安全配置执行以下操作：</p> <ul style="list-style-type: none"> 对网络通信中的恶意内容进行扫描，以记录任何病毒、特洛伊木马、蠕虫病毒或僵尸网络活动 启用 Web 信誉扫描，以记录访问的信誉分数较低的站点 启用入侵防御扫描，以记录恶意行为
邮件扫描	<p>邮件扫描 预定义的处理措施安全配置执行以下操作：</p> <ul style="list-style-type: none"> 启用防恶意软件扫描，以阻止包含恶意内容的电子邮件 启用反垃圾邮件扫描，以标记包含垃圾邮件的电子邮件 <p>要配置邮件标记设置，请转到 策略 > 安全设置 > 反垃圾邮件，然后指定 其他设置。有关详细信息，请参阅 配置反垃圾邮件设置 第 4-40 页。</p>

查看预定义的处理措施安全配置

过程

1. 转到 **策略 > 对象 > 处理措施安全配置 > 预定义安全配置**。
2. 单击安全功能（**入侵防御**、**防恶意软件**、**反垃圾邮件**或 **Web 信誉服务**）的名称以查看设置。



注意

无法修改预定义安全配置。

3. 取消显示的设置以查看其他安全功能的附加设置。
-

添加处理措施安全配置对象

如果组织需要将特定网络通信所采取的处理措施视为与所提供的缺省处理措施不同，则添加处理措施对象。

过程

1. 转到**策略 > 对象 > 处理措施安全配置 > 定制安全配置**。
 2. 单击**新增**。
 3. 指定名称和（可选）描述。
 4. 选中要配置的安全功能的复选框：入侵防御、防恶意软件、反垃圾邮件和/或 Web 信誉服务。
 5. 根据需要从相应的下拉列表框中设置处理措施：
 - 对于**入侵防御、Web 信誉服务**或**防恶意软件**，请选择：
 - **阻止**：阻止网络通信
 - **监控**：允许网络通信通过，但将其记录在安全日志中
 - 对于**反垃圾邮件**，请选择：
 - **标记**：允许递交主题行中包含标记的电子邮件，如 [垃圾邮件]
 - **隔离**：不允许递交电子邮件，但会将其保存到一个安全位置。
 - **阻止**：不允许递交电子邮件内容。
 - **监控**：允许递交电子邮件，并将其记录在安全日志中。
 6. 单击**确定**。
-

编辑处理措施安全配置对象

可以编辑现有处理措施安全配置，以满足企业需求。无法修改预定义的处理措施安全配置。


过程

1. 转到**策略 > 对象 > 处理措施安全配置 > 定制安全配置**。
 2. 单击要更改的处理措施安全配置的名称。
 3. 根据需要更改名称、描述或处理措施设置。
 4. 单击**确定**。
-

删除处理措施安全配置对象

如有必要，可以删除现有处理措施安全配置。无法删除预定义的处理措施安全配置。

过程

1. 转到**策略 > 对象 > 处理措施安全配置 > 定制安全配置**。
 2. 选中要删除的对象所在行对应的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

对象即被移除。

关于安全设置

定义安全配置时，可选择以下处理措施：

入侵防御 (IPS)

集成了高性能深度包检查体系结构和动态更新的特征数据库以提供完善的网络防护，从而抵御应用程序漏洞、蠕虫病毒和恶意网络通信的攻击。有关详细信息，请参阅[入侵防御安全 第 4-35 页](#)。

防恶意软件

缺省的全局防恶意软件安全配置。由所有策略使用，以提供恶意软件防护并使网络免遭其他威胁。包括病毒、间谍软件、特洛伊木马、蠕虫病毒和僵尸网络。如果启用了“全局防恶意软件”安全配置，则将执行网络连接扫描以确保内容不包含恶意软件。有关详细信息，请参阅[防恶意软件安全措施 第 4-37 页](#)。

反垃圾邮件

反垃圾邮件使用电子邮件信誉评价（一个云安全智能防护网络组件，可使用世界最大且最可信的信誉数据库之一以及动态信誉评价数据库来验证传入电子邮件的 IP 地址）识别新的垃圾邮件和网络钓鱼来源，从而在 Zombie 和僵尸网络首次出现时将其停止。有关详细信息，请参阅[反垃圾邮件安全 第 4-39 页](#)。

Web 信誉服务 (WRS)

用户访问有潜在危险的 Web 站点（尤其是称为网络钓鱼或域名欺诈的站点）之前，Web 信誉服务 (WRS) 会先审查 URL。利用 Web 信誉服务，设备可通过阻止感染链或提前将其破坏来提供实时防护、节约系统扫描资源并节省网络带宽。有关详细信息，请参阅[Web 信誉服务安全配置 第 4-44 页](#)。

网络入侵防御

网络入侵防御功能是下一代应用安全网关基本功能的一部分。当威胁、漏洞利用、后门程序和其他攻击通过设备时，入侵防御 (IPS) 可以识别并进行阻止。通过对防火墙规则策略所允许的网络通信进一步检查以确保其不包含有害威胁，入侵防御可以增强防火墙安全策略。

用于检测威胁的特征码将在官方更新或 Patch 可用之前发布 — 在此关键期保护业务。下一代应用安全网关入侵防御是一个深度数据包检查系统，它可以检查网络通信数据包内部，并移除某些包含恶意内容的数据包，这些内容会与一个含有数百个特征码的可部署规则列表进行比较。该特征码的签名列表每隔几分

钟进行一次实时更新，并且不断适应和发展以在威胁出现或传播时立即进行防护，从而使您免受威胁。

入侵防御针对常见的攻击类型提供支持，如下所示：

- DoS/DDoS 攻击
- 协议攻击
- 操作系统攻击
- 应用程序攻击
- 不正常的网络通信/无效的标头攻击
- 恶意软件和混合攻击
- TCP 分段和 IP 碎片攻击
- 端口扫描

入侵防御解决方案具有常用应用程序的预定义策略模板和使入侵防御功能易于使用的协议。趋势科技虽然提供了预定义的规则，但仍允许您创建定制入侵防御规则。

入侵防御安全

每个安全策略可指定一个入侵防御安全配置，该文件可确定防御缓存溢出、非法执行代码以及其他企图利用系统漏洞的防护级别。缺省安全配置可保护客户端和服务器免受所有已知的严重性级别为严重、高和中等的威胁。

入侵防御集成了高性能深度包检查体系结构和动态更新的特征数据库以提供完善的网络防护，从而抵御应用程序漏洞、蠕虫病毒和恶意网络通信的攻击。此外，入侵防御还提供了对即时通讯程序 (IM) 和点对点 (P2P) 应用程序的访问控制。

可使用定制的安全配置最大程度地减少针对可信安全区域之间网络通信的漏洞检查，并最大程度地针对从不可信区域 (Internet) 接收的网络通信以及发送至高度敏感的目标（服务器群）的网络通信进行保护。

在下一代应用安全网关中，您可以定义过滤规则条件，然后选择适用于网络通信的 IPS 规则。

阻止或监控处理措施的类别：

- **其他** — SIP Foundry sipiXtapi 缓存溢出
- **文件传输服务器** — NetTerm NetFTPF 用户缓存命令或 3Com 3CDaemon FTP 服务器溢出
- **Web 服务器** — Microsoft Windows Explorer 拖放远程代码执行、Microsoft IIS WebDAV 长请求缓存溢出等
- **通用服务** — Microsoft SSL PCT Buffer Overflow Vulnerability、Solaris Telnetd User Authentication Bypass Vulnerability 等
- **客户端** — Microsoft Visual Studio WMI 对象代理未指定代码执行、Microsoft Internet Explorer XMLHTTP ActiveX Control setRequestHeader 代码执行等
- **即时通讯** — IBM Lotus Sametime Multiplexer Buffer Overflow、MSN MSNP2P Message Integer Overflow 等
- **邮件服务器** — Sendmail Signal Race 漏洞、Microsoft Exchange SMTP Service Extended Verb 请求缓存溢出等

修改入侵防御规则

过程

1. 转到**策略 > 安全设置 > 入侵防御**。
2. 选中**启用入侵防御安全措施**复选框。
3. 在**入侵防御过滤条件**下，选择要过滤的最低入侵防御严重性级别。将对严重性级别等于或大于选定严重性级别的所有网络通信进行过滤。

选项	说明
1 - 信息	基于端口的网络通信（例如：HTTP、SMTP）。

选项	说明
2 - 低	与策略相关的签名（例如：IM、P2P、游戏）
3 - 中	隧道和扫描活动。
4 - 高	大多数与入侵相关的签名。
5 - 关键	严重性级别与“高”相同，但对服务器和用户产生非常严重的影响（例如：CVE-2008-4250、Conficker）。

4. 选择威胁的发布日期。
5. 选择受影响的操作系统。
6. 选择入侵防御类别。
7. 单击**应用过滤**来设置过滤条件。
与**过滤规则**下的表中填充的指定条件匹配的所有预定义入侵防御过滤规则。
8. 在**入侵防御规则**下，将自动选择所有匹配的条件。要移除入侵防御规则，请取消选中规则 ID 旁边的复选框。
9. 单击**确定**。
更改已保存。

防恶意软件安全措施

防恶意软件安全配置可以抵御蠕虫和病毒。您可以为此安全配置启用或禁用日志记录，但不能删除此安全配置。此安全配置可以供所有策略使用，以防御恶意软件并阻止其他威胁侵袭您的网络。如果在策略中启用了“全局防恶意软件”安全配置，则网络连接扫描将确保内容不包含恶意软件。

每个安全策略都可以指定是否使用全局防恶意软件安全配置。该安全配置可确定在哪些应用程序中检查恶意软件，以及检测到恶意软件时采取的处理措施。缺省安全配置将检查所有列出的协议解码器中是否有恶意软件，然后根据检测到的恶意软件类型，采取由策略确定的处理措施（阻止或监控）。

关于文件扩展名验证

当今的大多数防病毒解决方案提供了两种用于确定要扫描哪些文件来检查潜在风险的方法。即，扫描所有文件（最安全的方法），或者仅扫描具有特定文件扩展名、被认为最容易受感染的那些文件。

选择要扫描的文件扩展名/类型

下一代应用安全网关可以扫描通过它的所有文件，或根据文件扩展名仅扫描其中的一部分文件。

过程

1. 转到**策略 > 安全设置 > 防恶意软件**。
 2. 利用黑/白名单或扫描列表，按以下格式 `exe;rar;mp3` 指定文件扩展名。使用半角分号 (;) 分隔文件扩展名。
 - **允许的文件扩展名** — 无需扫描即允许这些文件类型。
 - **阻止的文件扩展名** — 文件未经扫描便已阻止。
 - **扫描列表** — 先扫描这些文件类型，然后下一代应用安全网关服务器再成功放行。
 3. 如果需要，请在**扫描优化**下指定扫描时要跳过的文件大小。
 4. 如果需要，请选择扫描时要跳过的 HTTP MIME 类型。
 5. 如果需要，配置在对电子邮件采取某个处理措施时要置于该邮件主题行中的标记。缺省为 **[已清除病毒]**。
 6. 单击**确定**保存设置。
 7. 选中**启用防恶意软件安全措施**复选框。
-

反垃圾邮件安全

本节说明了如何为 SMTP 电子邮件配置下一代应用安全网关反垃圾邮件过滤安全配置。下一代应用安全网关可通过检测和识别来自已知或可疑垃圾邮件服务器的垃圾邮件来管理未经请求的商业电子邮件。

关于垃圾邮件检测

下一代应用安全网关使用电子邮件信誉服务 (ERS) 集成来检测垃圾邮件。趋势科技还提供了一个单独的名为托管电子邮件安全的软件即服务 (SaaS) 安全组件，可用于基于内容的垃圾邮件过滤和数据泄漏过滤以及电子邮件加密功能。

电子邮件信誉技术

下一代应用安全网关使用电子邮件信誉 (ER) 技术以最大限度进行防护。ER 技术可让下一代应用安全网关根据源邮件传输代理 (MTA) 的信誉结果判定垃圾邮件。启用 ER 后，IP 数据库会检查所有入站 SMTP 网络通信，查看源 IP 地址是没有感染病毒还是已被作为已知的垃圾邮件站点列入黑名单。



为了使电子邮件信誉服务正常工作，入站 SMTP 网络通信上的所有地址转换必须在网络通信通过下一代应用安全网关之后进行。如果 NAT 或 PAT 在入站 SMTP 网络通信到达下一代应用安全网关之前出现，则下一代应用安全网关会始终将源 MTA 视为本地地址。ERS 仅阻止疑似 MTA 公共 IP 地址的连接，而不阻止私有地址或本地地址的连接。因此，使用电子邮件信誉服务的客户不应在下一代应用安全网关扫描入站 SMTP 连接前转换这些连接。

- ERS 标准服务（原“实时黑名单”或“RBL+”）是一个用于跟踪大约二十亿个 IP 地址信誉的数据库。始终与垃圾邮件投递关联的 IP 地址已添加到数据库并且很少被移除。
- ERS 高级服务（原“RBL + 和快速 IP 查找”或“QIL 组合”）是基于查询的 DNS 服务，与 ERS 标准服务相似。该服务的核心是标准信誉数据库以及动态信誉实时数据库。该服务会在垃圾邮件源发送数百万封邮件的过程中将其阻止。

如果在其中任何一个数据库中发现 IP 地址，则 ERS 将“标记”此连接，并且下一代应用安全网关将根据您选择的配置执行相应操作。

反垃圾邮件安全配置

反垃圾邮件安全配置是全局性的，不能创建或删除，只能启用或禁用。将反垃圾邮件安全配置作为安全配置应用时，所有策略将共享相同的反垃圾邮件设置，但可以修改安全处理措施类型。不使用反垃圾邮件扫描时，可以安全地禁用反垃圾邮件安全配置。

反垃圾邮件使用电子邮件信誉服务 (ERS) 技术（一个云安全智能防护网络组件，可使用世界最大且最可信的信誉数据库之一以及动态信誉数据库来验证传入电子邮件的 IP 地址）识别新的垃圾邮件和网络钓鱼来源，从而在 Zombie 和僵尸网络首次出现时将其停止。有关详细信息，请参阅[电子邮件信誉技术 第 4-39 页](#)。

启用和禁用反垃圾邮件安全配置

必须先启用反垃圾邮件安全配置，然后才可在策略中使用它。

过程

1. 转到**策略 > 安全设置 > 反垃圾邮件**。
 2. 执行下列操作之一：
 - 要启用反垃圾邮件安全配置，请选中**启用电子邮件信誉**复选框。
 - 要禁用反垃圾邮件安全配置，请取消选中**启用电子邮件信誉**复选框。
 3. 单击**确定**。
-

配置反垃圾邮件设置

配置下一代应用安全网关反垃圾邮件设置以：

- 使用电子邮件信誉服务，根据源 MTA 的信誉确定垃圾邮件。启用 ERS 后，IP 数据库会检查所有进站 SMTP 和 POP3 网络通信，查看源 IP 地址是未感染病毒还是已被作为已知的垃圾邮件站点列入黑名单。
- 对垃圾邮件采取缺省智能处理措施或为组织定制处理措施设置
- 创建允许和阻止的发件人列表
- 设置垃圾邮件的敏感度级别或捕获率
- 定义垃圾邮件主题行中使用的标记

过程

1. 转到**策略 > 安全设置 > 反垃圾邮件 > 反垃圾邮件**选项卡。

2. 选择**启用电子邮件信誉**以启用 ERS。

请参阅[电子邮件信誉技术 第 4-39 页](#)

3. 选择要对检测到的垃圾邮件采取的处理措施：

- a. 使**缺省智能处理措施**单选按钮处于选中状态，以使下列处理措施生效：
 - 永久拒绝 RBL+ 匹配项的连接 (550)
 - 临时拒绝 Zombic 匹配项的连接 (450)



注意

当使用缺省智能处理措施时，MTA 会拒绝垃圾邮件并显示一条简短的消息。

- a. 单击**对所有匹配项采取定制处理措施**单选按钮以设置垃圾邮件所需的处理措施，如：
 - SMTP 错误代码：设置介于 400 到 599 之间的代码。缺省错误代码为 450
 - SMTP 错误字符串：“服务不可用”为缺省字符串。
4. 在**允许的发件人**下，指定电子邮件地址，然后单击**添加**以允许发件人。

5. 在**阻止的发件人**下，指定电子邮件地址，然后单击**添加**以阻止发件人。
6. 设置**反垃圾邮件捕获率 (敏感度级别)**。
 - **高**：捕获较多垃圾邮件。如果有太多的垃圾邮件传递到客户端，请选择高捕获率。
 - **中**：标准设置（缺省）
 - **低**：捕获较少垃圾邮件。如果下一代应用安全网关将过多的合法电子邮件标记为垃圾邮件，请选择低捕获率。

**注意**

如果需要，可稍后调整反垃圾邮件捕获率。如果阈值太低，将出现垃圾邮件高发率。如果阈值太高，将出现高误报（合法邮件被识别为垃圾邮件）率。

7. 在**其他设置**下，更改用于将检测到的电子邮件识别为垃圾邮件的主题行标记。缺省为 [SPAM]。
8. 单击**确定**保存更改。

修改反垃圾邮件设置

可以修改缺省反垃圾邮件安全配置处理措施，以便使用缺省智能处理措施或指定 SMTP 错误代码，在黑/白名单中添加或删除条目，更改捕获率设置或垃圾邮件主题行中使用的标记。

过程

1. 转到**策略 > 安全设置 > 反垃圾邮件**。
2. 要更改邮件内容扫描处理措施，请选择相应的单选按钮：
 - **缺省智能处理措施** — 永久拒绝 RBL+ 匹配项的连接（SMTP 错误代码 550）以及临时拒绝 Zombie 匹配项的连接（SMTP 错误代码 450）。RBL+ 匹配项是更高等级的确信，发件人为已知的垃圾邮件制造者。当趋势科技认为先前良好的发件人由于僵尸网络感染而转变为恶意发件人时，则为 Zombie 匹配项。为此，发送临时拒绝连接的代码 (450)。

- **对所有匹配项采取定制处理措施** — 如果选择此按钮，请指定违反该安全配置时要查看的 SMTP 错误代码和消息。
3. 在允许和阻止用户列表中添加或移除条目。要删除某个条目，请选择它，然后单击**移除**。
 - 选择某个条目，然后单击**移除**以将其删除。
 - 单击**全部移除**以移除列表中的所有条目。
 4. 更改**反垃圾邮件捕获率 (敏感度级别)**。
 - **高**
 - **中：**（缺省）
 - **低**

**注意**

配置反垃圾邮件设置后，可以调整反垃圾邮件捕获率。如果阈值太低，将出现垃圾邮件高发率。如果阈值太高，将出现高误报（合法邮件被识别为垃圾邮件）率。

5. 在**其他设置**下，更改用于将检测到的电子邮件识别为垃圾邮件的主题行标记。缺省为 **SPAM**。
 6. 单击**确定**。
-

配置反垃圾邮件内容设置

反垃圾邮件内容设置使用各种条件来过滤邮件。

- 大小
- 标题内容
- 正文内容
- 附件内容

过程

1. 转到**策略 > 安全设置 > 反垃圾邮件 > 内容过滤**选项卡。
2. 在**过滤邮件标题**下，指定关键字或正则表达式，以过滤电子邮件标题。



注意

当配置标题、脚注和附件的过滤字符串时，可以使用关键字和正则表达式的任意组合来定义关键字表达式。指定一个反斜杠 \ 再紧跟以下字符：

`. \ | () { } [] ^ $ * + 或 ?`

关键字和正则表达式以逗号分隔。

3. 在**过滤邮件正文**下，指定关键字或正则表达式，以过滤电子邮件正文。
 4. 在**过滤邮件附件名称**下，指定关键字或正则表达式，以过滤电子邮件附件文件名。
 5. 单击**确定**应用更改。
-

Web 信誉服务安全配置

用户访问有潜在危险的 Web 站点（尤其是称为网络钓鱼或域名欺诈的站点）之前，Web 信誉服务 (WRS) 会先审查 URL。利用 Web 信誉服务，下一代应用安全网关可通过阻止感染链或提前将其破坏来提供实时防护、节约系统扫描资源并节省网络带宽。Web 信誉技术保护终端用户抵御新出现的 Web 威胁。因为 Web 信誉查询会返回 URL 类别信息（用于 URL 过滤），所以下一代应用安全网关不使用本地存储的 URL 数据库。

Web 信誉技术也为 URL 分配信誉分值。对于访问的每个 URL，下一代应用安全网关会查询 Web 信誉的信誉分值，然后根据此分值相对用户指定敏感度级别的高低采取必要的处理措施。利用趋势科技 Web 信誉技术（云安全智能防护网络的一部分），下一代应用安全网关可以在不同的防护级别（低、中和高）执行 Web 站点扫描。

下一代应用安全网关通过 Web 信誉（如果已启用）提供防网络钓鱼及防域名欺诈防护。

Web 信誉服务安全配置可应用于任一策略。可以安全地禁用不在使用中的任何 Web 信誉服务安全配置。

Web 信誉数据库驻留在远程服务器中。当用户尝试访问某个 URL 时，下一代应用安全网关会从 Web 信誉数据库检索关于该 URL 的信息，并将其存储在本地缓存中。将 Web 信誉数据库存储在远程服务器并使用该数据库信息构建本地缓存便可降低下一代应用安全网关中的开销并提高性能。

Web 信誉数据库会使用有关 Web 页面的最新安全信息进行更新。如果 URL 的信誉似乎已被错误分类或要发现 URL 的信誉，请访问：<http://global.sitesafety.trendmicro.com/>

配置 Web 信誉服务安全配置

如果存在太多误报或想要增强防护，请修改 Web 信誉服务安全配置使其更严格或更宽松。

过程

1. 转到**策略 > 安全设置 > Web 信誉服务**。
 2. 选中**启用 Web 信誉服务安全措施**复选框。
 3. 单击相应的单选按钮（**高**、**中**或**低**），以便根据公司目标设置 URL 阻止敏感度级别：
 - **高** — 阻止较多的 Web 站点，但存在阻止非恶意 Web 站点的风险。
 - **中** — 平衡“高”与“低”设置（缺省）之间的风险。
 - **低** — 阻止较少的 Web 站点，但存在不阻止潜在恶意 Web 站点的风险。
 4. 单击**确定**。
-

关于 HTTPS 检查

安全套接层 (SSL) 和传输层安全性 (TLS) 是当今在网络通信中广泛采用和部署的加密协议。将加密并签名 SSL/TLS 间的网络通信以确保安全性，对 HTTPS 也将执行同样的操作。因为加密的 HTTP 连接和未加密的 HTTP 连接可能存在同样的风险，所以下一代应用安全网关将扫描所有网络通信中的潜在风险和威胁。

下一代应用安全网关可以启用或禁用 HTTPS 检查并从检查中排除特定的 Web 站点、URL 类别或 IP 地址。在识别网络通信后，下一代应用安全网关将基于指定的策略设置确定相应的网络通信处理措施。要扫描 HTTPS 网络通信，下一代应用安全网关将识别 SSL 握手第一个数据包处的 SSL 连接，从会话中获取客户端 IP 地址信息（如果可用），然后从握手记录中获取服务器主机名。如果此信息和下一代应用安全网关例外列表中的任何允许的 URL 类别、Web 站点或 IP 地址相匹配，则将不会解密连接。

有关 HTTPS 检查的信息将显示在相应的日志和报告中。HTTPS 检查通知也可用于通知最终用户其操作在 Web 上被阻止的原因。

HTTPS 检查的常规设置

加密的 HTTP 连接与未加密的 HTTP 连接可能存在相同的风险。这些连接也需要进行检查，以查找潜在风险和威胁。下一代应用安全网关可以启用或禁用 HTTPS 检查，并从 HTTPS 检查中排除特定 Web 站点、URL 类别或 IP 地址

添加 HTTPS 例外

下一代应用安全网关可通过解密和检查所有加密的网络通信来关闭 HTTPS 安全漏洞。您可以允许客户端访问指定 URL 类别或源 IP 地址的所有 HTTPS 网络通信，方法是将这些类别和地址添加到 HTTPS 检查例外列表中。解密后，会按已应用 URL 过滤和扫描规则的 HTTP 网络通信的相同方式处理数据。解密数据在下一代应用安全网关服务器的内存中仍处于完全安全状态。在离开下一代应用安全网关服务器之前，会对数据进行加密，以使其可以安全通过客户端的浏览器。

对于网络通信过滤，下一代应用安全网关首先会根据主机名从本地特征码或本地缓存中查询 URL 类别。如果本地特征码或本地缓存中没有这种类别，则不会解密此连接。要确定是否要对网络通信进行解密，另一个线程会同时发出趋势科技 URL 过滤引擎 (TMUFE) 查询并将结果放到本地缓存中。当将来某个用户访问同一站点时，下一代应用安全网关会将解密策略与在本地缓存中查询的类别进行匹配。

过程

1. 转到**策略 > HTTPS 检查 > 常规设置**。
2. 选择**启用 HTTPS 通信检查**。
3. 在“URL 类别例外”下，搜索或指定要允许的特定 URL 类别。有关可用 URL 类别的完整描述，请参阅[关于 URL 类别对象 第 4-16 页](#)。
4. 在**服务器主机名例外**下，单击**允许或阻止主机**以更新黑/白名单。
将显示**黑/白名单** 窗口。有关管理允许的和黑名单的详细信息，请参阅[关于黑/白名单 第 4-58 页](#)。
5. 在**源地址例外**下，单击**新增**以指定所有客户端可以使用 HTTPS 连接进行访问的 IP 地址。
将显示**添加/编辑**窗口。
6. 指定名称、协议和所有要允许的 IP 地址，然后单击**确定**。
此时会将新源添加到列表中。
7. 选择下一代应用安全网关不会检查的新源地址。
8. 单击**确定**。
现在，将不会检查指定 URL 类别、服务器或源地址的所有 HTTPS 网络通信。

关于数字证书

缺省情况下，下一代应用安全网关充当私有 CA，并动态生成发送到客户端浏览器以完成 HTTPS 连接安全通道的数字证书。但是，缺省 CA 不是由 Internet

上的知名（可信）CA 签名。每次用户访问 HTTPS Web 站点时，客户端浏览器始终会显示证书警告。尽管用户可以安全地忽略证书警告，但趋势科技还是建议您对下一代应用安全网关使用已签名的 CA。



注意

下一代应用安全网关支持采用 X509 和 PKCS12 格式的证书。

导入证书颁发机构

导入组织的证书颁发机构，以保护网络与下一代应用安全网关之间的通信。

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书颁发机构**选项卡。
 2. 执行下列操作之一：
 - 对于公共证书，单击**公共证书**文本框旁边的**浏览**，然后选择要导入的相应证书。
 - 对于私有密钥，单击**私有密钥**文本框旁边的**浏览**，然后选择要导入的相应证书。如果私有密钥使用密码进行加密，请在**密码**文本框中键入该密码。如果私有密钥未使用密码进行加密，请将**密码**文本框保留为空。
 3. 单击**导入证书**。
-

导出证书颁发机构

下一代应用安全网关将仅导出公共证书。

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书颁发机构**选项卡。
2. 单击**导出证书**。

此时将会显示**打开 default.cer** 弹出窗口。

3. 单击**确定**可保存证书。

数字证书管理

下一代应用安全网关要确定某个 Web 服务器的签名是否可信，必须将签名所基于的根证书颁发机构 (CA) 证书添加到下一代应用安全网关证书存储中。生成数字签名的数字证书类型有 3 种：

- 包含用于验证实际 Web 服务器签名的公共密钥的“最终”或“签名”证书
- 包含用于验证签名证书或链中其他中间证书的公共密钥的一个或多个“中间”CA 证书
- 包含用于验证链中第一个中间 CA 证书（或者极少情况下直接验证签名证书）的公共密钥的“根”CA 证书。

如果下一代应用安全网关在 SSL 握手或签名处理期间遇到未知证书，它会将证书保存在“不可信”列表中。所有类型的证书均通过此种方式收集（签名证书、中间证书和根证书）。如果之后需要，通过此种方式收集的 CA 证书可被下一代应用安全网关“信任”，从而允许依赖于该 CA 证书的那些 Web 服务器的签名被处理为“有效”。中间 CA 证书和最终证书可能已激活，但这仅在根证书也激活的情况下起作用。

要管理下一代应用安全网关证书存储中的证书，请执行以下操作：

- **新增** — 在系统中添加一个新的证书。
- **删除** — 将选定的证书从证书存储中移除。
- **信任证书的真实性** — 使 CA 证书可信。
- **不信任证书的真实性** — 将证书保存在下一代应用安全网关证书存储中，但不信任在证书路径中使用该证书的其他证书。

查看证书详细信息

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书管理**选项卡。
 2. 单击下一代应用安全网关证书存储中列出的任意证书。
将显示**证书详细信息**窗口。
 3. 查看详细信息，然后单击**返回**以返回到证书存储。
-

添加新证书

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书管理**选项卡。
 2. 单击**新增**。
将显示**添加新证书**窗口。
 3. 单击**浏览**以选择证书，然后单击**打开**。
 4. 单击**添加**。
 5. 在确认窗口中，单击**确定**。
新证书将添加到下一代应用安全网关的证书存储中。
-

更改证书状态

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书管理**选项卡。

2. 通过使用搜索栏或滚动条找到要修改的证书来将其选中。


**注意**

无法将证书更新为与当前设置的状态相同。

3. 执行下列操作之一：
 - 将 CA 更改为可信：
 - a. 单击**信任证书的真实性**。
将显示**信任证书的真实性**窗口。
 - b. 单击**信任**。
 - 将 CA 更改为不可信：
 - a. 单击**不信任证书的真实性**。
将显示**不信任证书的真实性**窗口。
 - b. 单击**不信任**。
 4. 在状态更改确认窗口中，单击**确定**。
将更改下一代应用安全网关证书存储中所有选定证书的状态。
-

删除证书

过程

1. 转到**策略 > HTTPS 检查 > 数字证书 > 证书管理**选项卡。
 2. 选择要删除的任意证书。
 3. 单击**删除**图标 .
 4. 在确认对话框中单击**删除**。
-

该证书随即从下一代应用安全网关的证书存储中删除。

关于带宽控制

点对点下载、视频流和即时消息应用程序会消耗网络带宽并影响生产力。带宽控制通过控制通信、减少不需要的网络通信并为重要的网络通信或服务分配相应的带宽来减少网络拥塞。带宽控制使所有用户可以公平地访问资源，并确保更好地访问对组织较为重要的资源。与策略规则类似，带宽控制可以根据源 IP 地址或目标 IP 地址、网络通信类型或服务以及每天的时间来限制网络通信。

根据需要，带宽控制规则可以是通用的，也可以是特定的。带宽控制规则依次与传入网络通信进行比较，因为会应用第一个与网络通信相匹配的规则，所以特定规则必须位于通用规则之前。例如，如果与网络通信相关的所有其他设置均相同，则针对单个应用程序的规则必须位于适用于所有应用程序的规则之前。如果网络通信与所有规则都不匹配，则网络通信将使用剩余的带宽。

要创建带宽控制规则，需要先创建一些用于定义策略规则参数的策略对象。有关详细信息，请参阅[关于策略规则 第 4.2 页](#)。

通过[策略 > 带宽控制](#)上的**带宽控制**页面，用户可以：

- 查看现有规则的列表
- 添加、复制规则以及确定规则的优先级
- 启用或禁用规则



注意

带宽控制策略不能超过接口带宽设置。

添加带宽规则

使用**带宽**页面可根据指定的网络通信属性确定网络会话的带宽分配。创建新规则后，通过使用选项卡指定相应的信息来配置规则。

过程

1. 转到**策略 > 带宽控制**。
 2. 单击**新增**。
 3. （可选）禁用规则。
 4. 指定包含 1 到 32 个字符的策略名称，由字母、数字和下划线组成。
 5. 键入可选的**描述**。
 6. 配置源地址和用户规则。
请参阅 [配置源和用户规则 第 4-53 页](#)。
 7. 配置目标地址规则。
请参阅 [配置目标规则 第 4-54 页](#)。
 8. 配置通信类型规则。
请参阅 [配置通信类型规则 第 4-55 页](#)。
 9. 配置时段和带宽规则。
请参阅 [配置时段和带宽规则 第 4-56 页](#)。
 10. 单击**确定**。
-

配置源和用户规则

开始之前

在**策略 > 带宽规则 > 新增**中添加新的带宽控制策略，如[添加带宽规则 第 4-52 页](#)中所示。

使用**源和用户**选项卡定义对来自指定的源 IP 地址、源用户和组和/或源区域的通信强制实施的规则。

过程

1. 单击**源和用户**选项卡。
2. 在**源地址**下，选择以下参数之一：
 - **任何**：包括所有源地址。（缺省）
 - **选择地址**：显示之前配置的可用的源地址列表或添加新的 IP 地址。



注意

要添加新地址对象，请参阅[配置地址对象 第 3-8 页](#)。

3. 从**用户和组**下的以下选项中选择

选项	说明
任何人	规则会影响所有已知和未知的用户。
已知用户	规则通过网页认证影响认证的用户，或通过透明认证影响识别的用户。有关用户识别的详细信息，请参阅 关于认证 第 4-63 页 。
未知用户	规则会影响透明认证无法识别的用户。有关用户识别的详细信息，请参阅 关于认证 第 4-63 页 。
选定的用户	规则影响指定的用户和组（本地用户或 LDAP）。有关用户管理的详细信息，请参阅 终端用户管理 第 6-9 页 。

后续步骤

继续配置目标规则，如[配置目标规则 第 4-54 页](#)中所示。

配置目标规则

开始之前

- 在**策略 > 带宽规则 > 新增**中添加新的带宽控制策略，如[添加带宽规则 第 4-52 页](#)中所示。
- 如果需要，请按照[配置源和用户规则 第 4-53 页](#)中所示配置源和用户。

使用**目标**选项卡为在指定 IP 地址和目标区域结束的网络通信定义规则。

过程

1. 单击**目标**选项卡。
2. 在**目标地址**下，选择以下参数之一：
 - **任何**：包括所有目标地址
 - **选定的地址**：显示先前配置的目标地址的可选列表，以供使用。如果需要，使用此选项添加地址对象。



注意

要添加目标地址，请参阅[配置地址对象 第 3-8 页](#)

后续步骤

继续配置通信类型规则，如[配置通信类型规则 第 4-55 页](#)中所示。

配置通信类型规则

开始之前

- 在**策略 > 带宽规则 > 新增**中添加新的带宽控制策略，如[添加带宽规则 第 4-52 页](#)中所示。
- 如果需要，配置源和用户（如[配置源和用户规则 第 4-53 页](#)中所示）及目标（如[配置目标规则 第 4-54 页](#)中所示）。

使用**通信类型**选项卡为与任何指定应用程序、URL 类别或服务匹配的网络通信定义规则。

过程

1. 单击**通信类型**选项卡。
2. 在**应用程序**和**URL 类别**下，选择以下参数之一：

- **任何：**包括所有应用程序组和 URL 类别（缺省）
- **选定：**仅包括选定的应用程序类别和 URL 类别



注意

有关添加新的应用程序、URL 类别组或定制 URL 类别的详细信息，请参阅：

- [添加新应用程序对象 第 4-14 页](#)
- [添加新 URL 类别对象 第 4-23 页](#)
- [添加定制 URL 类别 第 4-25 页](#)

3. 选中**启用服务规则**以对特定服务强制实施规则。

- **任何：**包括所有服务
- **选定：**仅包括选定的服务

有关添加服务对象的详细信息，请参阅[添加定制服务对象 第 4-13 页](#)

后续步骤

继续配置时段和带宽规则，如[配置时段和带宽规则 第 4-56 页](#)中所示。

配置时段和带宽规则


开始之前

- 在**策略 > 带宽规则 > 新增**中添加新的带宽控制策略，如[添加带宽规则 第 4-52 页](#)中所示。
- 如果需要，配置源和用户（如[配置源和用户规则 第 4-53 页](#)中所示）、目标（如[配置目标规则 第 4-54 页](#)中所示）以及通信类型（如[配置通信类型规则 第 4-55 页](#)中所示）。

使用**时段和带宽**选项卡以强制实施基于所选时间表和带宽消耗的规则。

过程

1. 单击**时段和带宽**选项卡。
2. 指定时间表和下行带宽设置。

时间表	<p>从下拉列表中选择时间表。</p> <ul style="list-style-type: none"> • 始终：（缺省）包括所有时间表。 • 时间表名称：显示可用的时间表对象的名称。 • 新增：访问添加/编辑时间表对象创建对话框。 <hr/> <p> 注意 有关创建时间表对象的详细信息，请参阅：添加时间表对象 第 4-27 页。</p>
出接口	从下拉列表中选择合适的接口。
保证的带宽	指定保证的下行带宽。
最大带宽	指定保证的下行带宽。

3. 可选：指定**高级设置**。

保证的带宽	指定保证的上行带宽。
最大带宽	指定保证的上行带宽。
服务优先级	从下拉列表中选择服务优先级。如果发生网络拥塞，相比较带宽控制规则设置为较低服务级别的网络通信，较高服务级别的网络通信具有优先权。

4. 单击**确定**。

启用/禁用带宽规则

可在提供策略时将其禁用。此过程适用于已创建但并未启用的策略规则。

过程

1. 转到**策略 > 带宽控制**。
 2. 单击要启用或禁用的策略规则的名称
 3. 执行下列操作之一：
 - 选中此复选框以启用策略
 - 取消选中此复选框以禁用策略
 4. 单击**确定**。
-

关于黑/白名单

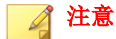
通过黑/白名单，网络通信可以覆盖已定义的 URL 过滤类别、入侵防御、Web 信誉服务和防恶意软件设置。将 URL 添加到列表中时，请谨记以下事项：

- URL 可以使用星号 (*) 作为通配符，该通配符应仅在字符串的开头或结尾键入。
- 白名单的优先级高于黑名单。

配置黑/白名单

过程

1. 转到**策略 > 黑/白名单**。
2. 执行下列操作之一：
 - 选择**允许的 URL** 选项卡以添加允许的 URL。



仔细审核 Web 站点。如果不扫描或阻止某个 Web 站点可能会带来安全风险。

- 选择**黑名单**选项卡以阻止要禁止的 URL。
3. 在文本框中指定相应的字符串：
- 对于 Web 站点，请键入 `www.example.com/*`
 - 对于关键字，请键入 `*keyword_example*`
 - 对于字符串，请键入 `string_example` 或 `123.123.123.123`
-



请使用逗号或分号分隔多个条目。

4. 单击**确定**。
-

启用/禁用黑/白名单

过程

1. 转到**策略 > 黑/白名单**。
 2. 单击要启用或禁用的列表的选项卡，即**白名单** 或**黑名单**。
 3. 执行下列操作之一：
 - 要启用列表，请选中“启用列表”复选框。
 - 要禁用列表，请取消选中“启用列表”复选框。
 4. 单击**确定**以保存更改。
-

关于防 DoS

拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击会试图使用户无法使用计算机或网络资源，它旨在暂时或无限期中断或挂起连接到 Internet 的主机的服务。

典型的攻击包括通过外部通信请求使目标计算机达到饱和状态，以致于计算机无法再响应合法的网络通信，或响应极其缓慢，呈现不可用状态。此类攻击通常会导致服务器超负荷。

三种最常见的攻击方法包括：

TCP SYN Flood

当恶意主机发送一大批 TCP/SYN 数据包（通常使用伪造的发件人地址）时，将发生传输控制协议 (TCP) 同步传输 (SYN) Flood。其中的每个数据包都像连接请求一样进行处理，从而导致服务器发送回 TCP/SYN-ACK 数据包（确认）并等待发送方地址响应中的数据包（响应 ACK 数据包），最终生成大量半开连接。但是，由于发送方地址是伪造的，因此永远不会进行响应。这些半开连接使服务器所能建立的可用连接数达到饱和，从而导致其在攻击结束之前一直无法响应合法的请求。

UDP Flood

用户数据报协议 (UDP) Flood 通过反复发送大量 UDP 数据包而使目标服务器超负荷。

ICMP/Ping Flood

Internet 控制消息协议 (ICMP) Flood 通常通过使用 ping 命令，向受害者发送大量 ping 数据包。此类攻击很容易发动，从而获得对大于其受害者的带宽的访问权限。

配置 Flood 保护

使用用户定义的阈值，下一代应用安全网关限制了会淹没服务器的每秒数据包的数量。这些数据包转发到下一代应用安全网关，并划分为传输控制协议 (TCP) 同步传输 (SYN)、用户数据报协议 (UDP) 和 Internet 控制消息协议 (ICMP) flood 保护类别。

过程

1. 转到**策略 > 防 DoS > Flood 保护**。
 2. 选中相应的框，并在 TCP SYN、UDP 或 ICMP flood 保护的每秒数据包文本框上指定 flood 限制。
 - 根据各种 flood 类型的源或目标地址限制网络通信
 - 指定阈值限制
 3. 单击**确定**。
-

添加地址例外

下一代应用安全网关维护一个将 IP 地址指定到不受限制或不会被过滤的列表的例外源地址列表。

过程

1. 转到**策略 > 防 DoS > 地址例外**选项卡。
2. 单击**新增**。
将显示**添加/编辑地址对象**页面。
3. 指定不限制或不过滤的 IP 地址、IP 地址范围，或地址对象的 IP 地址/网络掩码。
4. 选择要应用到此特定例外列表的数据包类型：

选项	说明
TCP SYN	传输控制协议/同步传输
UDP	用户数据报协议
ICMP	Internet 控制报文协议

5. 单击**确定**。
-


修改地址例外

过程

1. 转到**策略 > 防 DoS > 地址例外**。
 2. 单击要修改的地址。
 3. 根据需要修改地址对象。
 4. 单击**确定**。
-

删除地址例外

过程

1. 转到**策略 > 防 DoS > 地址例外**。
 2. 选中要删除的地址的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

关于认证

缺省情况下，下一代应用安全网关仅允许策略规则明确允许的网络通信。使用用户识别和认证方法识别来自指定 IP 地址的用户。其他策略根据源和目标 IP 地址、安全配置、服务、时间表和/或应用程序类型来强制执行。

用户 ID 代理是安装在网络中的一个下一代应用安全网关应用程序，用于获取 IP 地址和网络用户之间所需的映射信息。用户 ID 代理会自动收集用户到 IP 地址的映射信息，并将此信息提供给防火墙以用于安全策略和日志记录。

配置特定的 IP 地址或 IP 地址范围，以使用特定的认证方法：

- 对于透明认证，下一代应用安全网关会定期在域控制器中检索登录日志信息，这样可以将用户映射到 IP 地址。如果上述方法失败，下一代应用安全网关将直接连接到客户端计算机（即尝试访问网络之外的位置的客户端计算机）以查询当前登录的用户。（这要求 LDAP 设置帐户拥有相应的权限。）
- 对于网页认证，如果 IP 地址尚未获得认证，并且如果当前请求为 HTTP 请求，则用户将被定向到一个 Web 页以提供域帐户登录信息。

对于用户/组信息，下一代应用安全网关会定期将总体 LDAP 用户树同步到本地缓存。后续用户组关系查询将在本地解析。



注意

用户识别映射要求防火墙在使用 NAT 转换 IP 地址之前获取用户的源 IP 地址。如果由于 NAT 或使用代理服务器造成多个用户拥有相同的源地址，则不可能进行准确的用户识别。

用户 ID 策略列表使用**策略 > 对象 > 地址**条目。

可以从**策略 > 认证 > 网页认证**页面访问定制的网页认证登录信息。如果用户 ID 代理无法将用户与 IP 地址关联，则网页认证可以接管和认证用户。有关详细信息，请参阅[关于网页认证 第 4-65 页](#)。

用户识别方法

用户识别将识别出哪一 IP 地址属于哪一用户。这样可允许使用匹配策略的 IP 地址到用户的映射缓存来构建用户识别方法。有关添加规则的详细信息，请参阅[添加认证规则 第 4-64 页](#)。

缺省情况下，所有的 IP 地址都不会自动用于用户识别。请务必定义哪一源 IP 地址或 IP 地址范围必须用于用户识别。如果源 IP 地址不在定义的范围，则此 IP 地址将不能用于用户识别。（在这种情况下，策略源 IP 地址必须设置为“任何”以使用户或组策略起作用。）

对于指定的 IP 地址或 IP 地址范围，定义用户识别的方法包括：

- 透明认证（使用 Windows 客户端查询和域控制器事件日志查询）
- 网页认证

添加认证规则

过程

1. 转到**策略 > 认证 > 端点识别**。

2. 单击**新增**。

3. 选择是否使用**网页认证**。

请参阅[关于网页认证 第 4-65 页](#)。

4. 为策略指定名称。

5. 选择现有地址对象或添加新的地址对象。

有关地址对象的详细信息，请参阅[关于地址和地址对象 第 3-6 页](#)。

6. 单击**确定**。

后续步骤

验证该名称是否显示在**策略 > 认证 > 端点识别**下的认证策略列表中。

关于网页认证

如果用户识别代理无法将用户与 IP 地址关联，网页认证可以接管并使用 Web 表单对用户进行认证。

要接收 Web 表单，用户必须使用 Web 浏览器并且处于连接过程中。成功认证后，用户将自动定向到最初请求的 Web 站点。现在，防火墙可以根据用户信息为通过防火墙的任一应用程序（不仅是使用 Web 浏览器的应用程序）执行策略。



重要信息

要启用网页认证，请参阅[启用网页认证 第 4-66 页](#)。

以下规则适用于网页认证：

- 网页认证规则仅适用于 Web (HTTP) 网络通信。
- Web 页面提示用户指定用户名和密码。

如果由于网络通信不是 HTTP 或没有匹配的规则而无法应用上述网页认证规则，则防火墙会应用基于其 IP 地址的安全策略。

下一代应用安全网关会根据 LDAP 服务器验证用户名和密码。如果认证成功，下一代应用安全网关会将 IP 地址到用户的映射添加到使用期限 (TTL) 生命周期的本地缓存中。如果认证失败，下一代应用安全网关将通知用户认证未成功。

还可以设计和创建用户登录时看到的文本。可定制的消息包括：

- 公司徽标
- 公司名称
- 欢迎消息

- 外部 HTTP 链接

启用网页认证

过程

1. 转到**管理 > 设备管理 > 管理服务**选项卡并在相应接口上选择 **Web 控制台**。
 2. 请确保使用网页认证的客户端可以解析下一代应用安全网关主机名。
-

配置网页认证设置

网页认证登录页面提供了一个要求所有用户先指定用户名和密码（由管理员分配）再访问网络或 Internet 的选项。如果用户 ID 代理无法将用户与 IP 地址相关联，则网页认证将接管并认证用户。

过程

1. 转到**策略 > 认证 > 网页认证**。
 2. 单击**浏览**以浏览到公司徽标的 .PNG 或 .GIF 文件的位置，以便显示网页认证登录页面。
-



注意

该图像不能超过 700 x 200 像素，且大小不能超过 1MB。

3. 单击**上传**以上传该图像。
4. 添加合适的**公司名称**。
5. （可选）定制**欢迎消息**。
6. （可选）将外部 HTTP 链接添加到公司 Web 站点。
7. 单击**预览**以显示消息并进行验证。

8. 关闭显示预览的选项卡。
 9. 如果满意，则单击**应用**，否则单击**重置**以恢复为缺省值。
-

关于用户通知

使用相应页面上的设置向终端用户通知所出现的违例。

要配置终端用户通知，请参见以下内容：

- [配置 Web 信誉服务违例通知](#) 第 4-67 页
- [配置 URL 过滤违例通知](#) 第 4-68 页
- [配置应用程序控制违例通知](#) 第 4-69 页
- [配置防恶意软件违例通知](#) 第 4-69 页
- [配置黑名单违例通知](#) 第 4-70 页
- [配置文件扩展名违例通知](#) 第 4-71 页
- [配置入侵防御安全通知](#) 第 4-72 页
- [配置服务器证书失败通知](#) 第 4-73 页
- [配置客户端证书失败通知](#) 第 4-74 页

配置 Web 信誉服务违例通知

下一代应用安全网关具有缺省的 Web 信誉服务违例通知。使用此过程编辑和预览 Web 信誉服务违例的终端用户通知中使用的 HTML 消息。

过程

1. 转到**策略 > 用户通知 > Web 信誉服务违例**。
2. 单击显示的邮件并按需要更改。



注意

要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %W:显示终端用户访问的 URL 的 Web 信誉分数
 - %H:用于显示下一代应用安全网关设备的主机名
 4. 单击**预览**以查看所做的更改。
 5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置 URL 过滤违例通知

下一代应用安全网关具有缺省的 URL 过滤违例通知。使用此过程编辑和预览 URL 过滤违例的终端用户通知中使用的 HTML 消息。

过程

1. 转到**策略 > 用户通知 > URL 过滤违例**。
 2. 单击显示的邮件并按需要更改。
-



注意

要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %C:显示终端用户访问的 URL 类别
 - %H:用于显示下一代应用安全网关设备的主机名
4. 单击**预览**以查看所做的更改。

- 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置应用程序控制违例通知

下一代应用安全网关具有缺省应用程序控制违例通知。使用此过程可编辑和预览在应用程序控制违例的终端用户通知中使用的 HTML 邮件。

过程

- 转到**策略 > 用户通知 > 应用程序控制违例**。
- 单击显示的邮件并按需要更改。



注意

要对 HTML 进行更改，请单击格式栏左上角的 **HTML** 图标。

- 使用以下令牌定制邮件：
 - `%U`:用于显示终端用户访问的 URL
 - `%T`:用于显示终端用户访问的 URL 的应用程序类型
 - `%H`:用于显示下一代应用安全网关设备的主机名
 - 单击**预览**以查看所做的更改。
 - 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置防恶意软件违例通知

下一代应用安全网关具有缺省防恶意软件违例通知。使用此过程可编辑和预览在防恶意软件违例的终端用户通知中使用的 HTML 邮件。

过程

1. 转到**策略 > 用户通知 > 防恶意软件违例**链接。
2. 单击显示的邮件并按需要更改。



要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %V:用于显示终端用户访问的 URL 中的病毒名称
 - %H:用于显示下一代应用安全网关设备的主机名
 4. 单击**预览**以查看所做的更改。
 5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置黑名单违例通知

黑名单违例通知具有缺省终端用户通知。使用此过程编辑和预览黑名单违例的终端用户通知中使用的消息。

过程

1. 转到**策略 > 用户通知 > 黑名单违例**链接。
2. 单击显示的邮件并按需要更改。



要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：

- %U:用于显示终端用户访问的 URL
 - %H:用于显示下一代应用安全网关设备的主机名
4. 单击**预览**以查看所做的更改。
 5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置文件扩展名违例通知

下一代应用安全网关具有缺省文件扩展名违例通知。使用此过程可编辑和预览在文件扩展名违例的终端用户通知中使用的 HTML 邮件。

过程

1. 转到**策略 > 用户通知 > 文件扩展名违例**链接。
2. 单击显示的邮件并按需要更改。



注意

要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %M:用于显示终端用户访问的 URL 中相匹配的文件扩展名
 - %H:用于显示下一代应用安全网关设备的主机名
 4. 单击**预览**以查看所做的更改。
 5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。
-

配置入侵防御安全通知

下一代应用安全网关具有缺省入侵防御安全通知。使用此过程可编辑和预览在入侵防御安全的终端用户通知中使用的 HTML 邮件。

过程

1. 转到**策略 > 用户通知 > 入侵防御安全**链接。
2. 单击显示的邮件并按需要更改。



要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %V:用于显示违例的入侵防御规则 ID
 - %H:用于显示下一代应用安全网关设备的主机名
4. 单击**预览**以查看所做的更改。
5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。

证书失败通知

当下一代应用安全网关检测到尝试访问违反具有阻止处理措施的 HTTPS 检查策略的 URL 时，将在请求客户端浏览器中显示警告窗口，指示此 URL 已被阻止。对于 HTTPS 解密，有 3 种通知类型：HTTPS 扫描、HTTPS 证书失败和客户端证书阻止。HTTPS 扫描通知和正常 HTTP 网络通信通知相同。有关详细信息，请参阅[关于用户通知 第 4-67 页](#)。

配置服务器证书失败通知

下一代应用安全网关具有缺省的服务器证书失败通知。使用此过程编辑和预览服务器证书失败的终端用户通知中使用的 HTML 消息。

当用户因证书未通过验证测试而被拒绝访问某个网站时，将看到此 HTML 警告消息。用户可以选择执行下列操作之一：

- 审查证书。
- 继续访问该网站（不推荐）。

过程

1. 转到**策略 > 用户通知 > 服务器证书失败**。
2. 单击显示的邮件并按需要更改。



注意

要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：
 - %U:用于显示终端用户访问的 URL
 - %H:显示下一代应用安全网关的主机名
4. 单击**预览**以查看所做的更改。
将显示 **HTTPS 证书失败**预览。

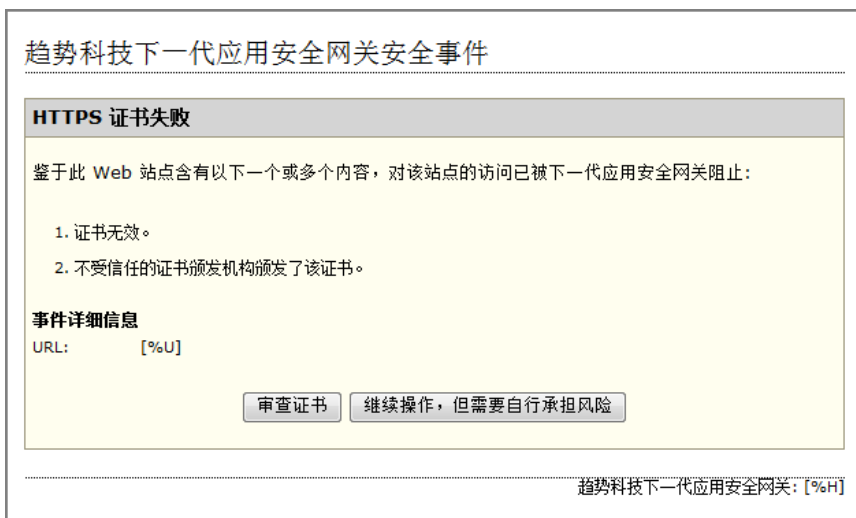


图 4-2. HTTPS 证书失败通知

5. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。

配置客户端证书失败通知

下一代应用安全网关具有缺省的客户端证书失败通知。使用此过程编辑和预览客户端证书失败的终端用户通知中使用的 HTML 消息。

过程

1. 转到**策略 > 用户通知 > 客户端证书失败**链接。
2. 单击显示的邮件并按需要更改。



注意

要在 HTML 中进行更改，请单击邮件工具栏上的第一个图标。

3. 使用以下令牌定制邮件：

- %U:用于显示终端用户访问的 URL
 - %H:显示下一代应用安全网关的主机名
4. 单击**预览**以查看所做的更改。
将显示**客户端证书失败**预览。

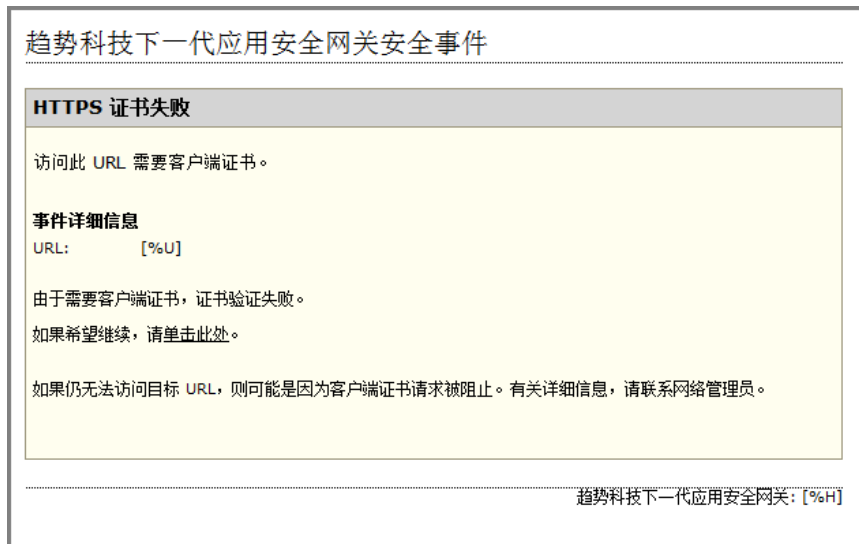


图 4-3. 客户端证书失败通知

5. 关闭预览返回到配置屏幕。
6. 单击**确定**以保存更改，或单击**取消**以恢复为缺省消息。

第 5 章

智能日常监控

下一代应用安全网关可智能监控网络以及如何强制执行策略。在配置网络设置以处理和标识通过网络的网络通信后，将拥有各种监控功能来主动了解最新出现的安全威胁。

主题包括：

- [实时监控和小组件 第 5-2 页](#)
- [分析和报告 第 5-30 页](#)
- [日志设置 第 5-38 页](#)
- [设备日志 第 5-40 页](#)

实时监控和小组件

实时监控和小组件会通知您下一代应用安全网关监控或控制的所有网络活动的相关信息。下一代应用安全网关会收集大量关于您的网络通信的日志数据。您可以通过实时监控小组件中日志的图形表示获取可操作的情报，从而快速了解影响网络的威胁以及下一代应用安全网关如何保护您的客户端免受侵害，而非通过筛选大量日志数据。

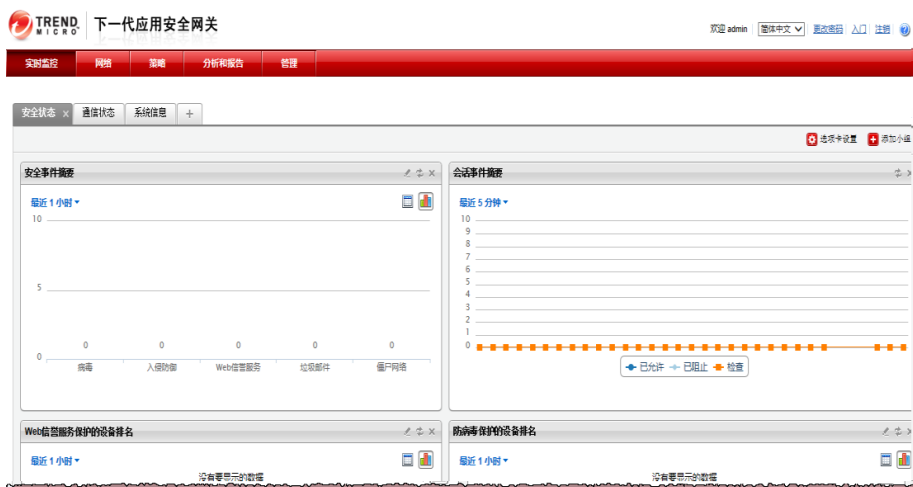


图 5-1. 下一代应用安全网关实时监控



注意

有关小组件的详细信息，请参阅[使用小组件](#) 第 5-8 页。

关于选项卡


要定制下一代应用安全网关实时监控，您可以添加其他选项卡，根据需要为新选项卡命名，并添加相应的小组件。可以修改和删除所添加的选项卡。不能删除缺省选项卡，但可以进行修改。

缺省选项卡将显示以下三种类别的状态小组件：

- 安全状态
- 系统信息
- 网络通信

添加新选项卡

过程

1. 转到**实时监控**。
 2. 单击最后一个已命名选项卡右侧的 。
 - 此时将显示**新建选项卡**窗口。
 3. 为新选项卡的**标题**指定名称。
 4. 选择相应布局样式的单选按钮。
 5. 选择**自动调整 打开**可使选项卡上的所有小组件的高度一致。
 6. 单击**保存**。
-

新选项卡将添加到现有选项卡的右侧。

修改选项卡设置

过程

1. 转到**实时监控**。
2. 单击要修改的选项卡。
3. 单击**选项卡设置**链接。

4. 根据需要更改以下项：
 - 标题
 - 布局
 5. 单击**保存**。
-

删除选项卡

只可能删除添加的选项卡。只有添加的选项卡才能删除。缺省选项卡（安全状态、流量状态和系统状态）不可删除。

过程

1. 转到**实时监控**。
 2. 单击添加的选项卡名称旁边的 **X**。
 3. 单击**确定**确认删除。
-

关于小组件

可以在实时监控选项卡中添加或移除可定制的小组件。每个小组件都包含对其用途的描述。

表 5-1. 下一代应用安全网关小组件

选项卡	小组件
安全状态	<ul style="list-style-type: none"> • 安全事件摘要* • 会话事件摘要* • 反僵尸网络保护的 设备排名 • 防病毒保护的 设备排名* • 设备风险摘要 • Web 信誉服务保护的 设备排名* • 入侵防御保护的 设备排名 • 反垃圾邮件保护的 设备排名 • 僵尸网络
通信状态	<ul style="list-style-type: none"> • 会话摘要* • 用户排名* • 最常使用的应用程序* • 带宽摘要* • 带宽控制 • 最常访问的 站点 • 最常访问的 URL 类别
系统信息	<ul style="list-style-type: none"> • 接口信息* • 网络信息* • 系统信息* • 系统资源* • 特征码信息 • 硬件监控

* 表示缺省显示的小组件。

定制小组件

可以手动更新和配置/过滤小组件，以显示所需信息。

可以定制小组件，以显示特定时间段的信息。对于某些小组件，该信息可通过图形或表格的形式显示。

过程

1. 转到**实时监控**。
 2. 选择要定制的小组件。
 - a. 单击小组件左上角的时间链接，选择要显示的时间段。
 - b. （对于适用的小组件）单击小组件右上角的图表或列表图标，选择显示信息的样式。
 - c. 将鼠标放在所显示的数据上并单击可放大详细信息。
 3. 对于某些小组件，单击小组件底部的图例，以过滤所显示的信息。
 4. 有关其他定制的信息，请参阅下图和下表。另请参阅[使用小组件 第 5-8 页](#)
-

小组件选项



图 5-2. 小组件选项

标注	描述
1	更改显示数据的时间段。
2	根据小组件的用途过滤信息。
3	手动刷新显示的信息。
4	从实时监控删除小组件。
5	更改显示数据的图形格式：条形图、饼图或表格。

添加新小组件

过程

- 单击实时监控右上角的**添加小组件**图标 (➕)。

将显示**添加小组件**选择窗口。
- 从所显示的预定义小组件设计列表中选择一个或多个小组件。



要按类别对小组件进行排序，请单击窗口左侧的类别。

3. 单击**添加**。

可以删除添加的小组件或将其拖放到小组件容器内的不同位置，并且仍可以修改小组件的配置。

删除小组件

过程

1. 单击小组件左上角的 **X**。
-

使用小组件

下一代应用安全网关使用小组件框架来实现实时监控，以便可以选择要显示的小组件。下一代应用安全网关摘要实时监控支持流量状态、系统信息和安全状态小组件。



下一代应用安全网关不支持小组件定制。有关添加小组件的详细信息，请参阅[添加新小组件](#) 第 5-7 页。

关于系统信息小组件

系统信息类别包含以下小组件：

- “接口信息” 小组件 第 5-9 页
- “系统信息” 小组件 第 5-10 页


- “系统资源” 小组件 第 5-11 页
- “网络信息” 小组件 第 5-11 页
- “特征码信息” 小组件 第 5-13 页
- “硬件监控” 小组件 第 5-13 页

“接口信息” 小组件

接口信息小组件显示系统的接口信息。接口的当前状态为接近实时状态。



要更改接口，请单击**编辑**以转到**网络 > 接口**窗口。

要手动刷新数据，请单击小组件右上角的  图标。

“系统信息” 小组件

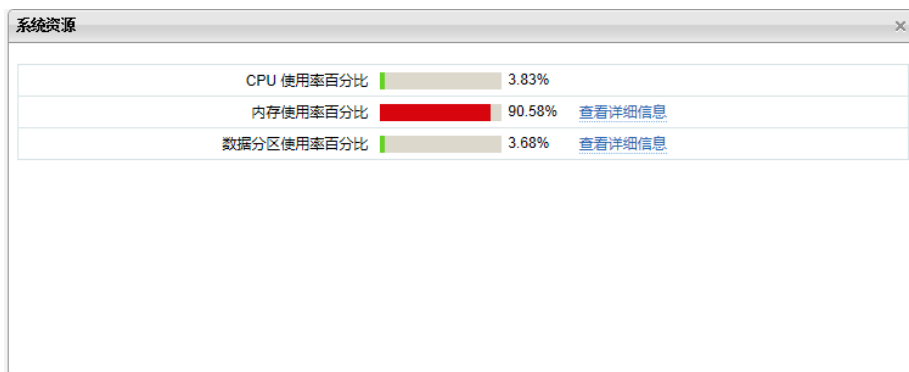
系统信息小组件显示与系统相关的信息。系统信息为接近实时的信息。

系统信息	
产品名称	下一代应用安全网关
版本	2.5.0.1110
当前管理员	admin
系统时间	2014-03-12 23:15:06 [更改]
正常运行时间	1天 4小时 16分钟
使用授权状态	✔ 已激活 [更改]
部署模式	接入模式 [更改]

- 根据系统时间信息单击**更改**，以转到**管理 > 系统设置**页面，然后更新系统时间
- 根据使用授权状态单击**更改**，以转到**管理 > 使用授权**
- 根据部署模式单击**更改**，以转到**网络 > 部署**

“系统资源” 小组件

系统资源小组件显示接近实时的 CPU、内存和数据分区使用信息。




“网络信息” 小组件

网络信息小组件显示与网络相关的信息，例如与网络相关的系统设置。




单击**更改**以转至**管理 > 系统设置**页面，然后更新名称或 IP 地址信息。

要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。指定测试域 IP 地址。

**注意**

默认情况下，该测试域是趋势科技域：de20-sc.url.trendmicro.com

如果此测试域不可用，在**系统资源**小组件中显示的“Internet 连接”状态会显示“已断开连接”，但实际上仍处于连接状态。


要手动刷新数据，请单击小组件右上角的  图标。

“特征码信息”小组件

特征码信息小组件可显示每个组件的最新特征码。单击任何组件旁边的**查看**可转至**特征码更新**窗口。有关更新组件的详细信息，请参阅[可更新的程序组件第 7-2 页](#)。



组件名称	版本	操作
防恶意软件病毒码	1.11411.00	[查看]
入侵防御特征码	1.11002.00	[查看]
入侵防御引擎	1.0.13	[查看]
病毒扫描引擎	9.750.1005	[查看]
病毒扫描引擎_64	9.750.1005	[查看]
病毒码	10.644.60	[查看]
IntelliTrap 例外特征码	0.961.00	[查看]
IntelliTrap 特征码	0.173.00	[查看]
间谍软件特征码	1.362.00	[查看]
垃圾邮件引擎	7.5.1017	[查看]

要手动刷新数据，请单击小组件右上角的  图标。


“硬件监控”小组件

硬件监控小组件可显示下一代应用安全网关设备硬件的温度和性能。



CPU 温度(°C)	NA
环境温度(°C)	NA
主板温度(°C)	NA
CPU 风扇速度(RPM)	NA
RAM风扇速度(RPM)	NA
主风扇速度(RPM)	NA

当发生特定事件时，下一代应用安全网关会通过发送电子邮件通知系统管理员。在以下位置配置系统管理员：**管理 > 通知 > SMTP 设置**。有关配置其他通知的详细信息，请转到**管理 > 通知 > 通知事件 > 硬件监控**。

要手动刷新数据，请单击小组件右上角的  图标。

关于流量状态小组件

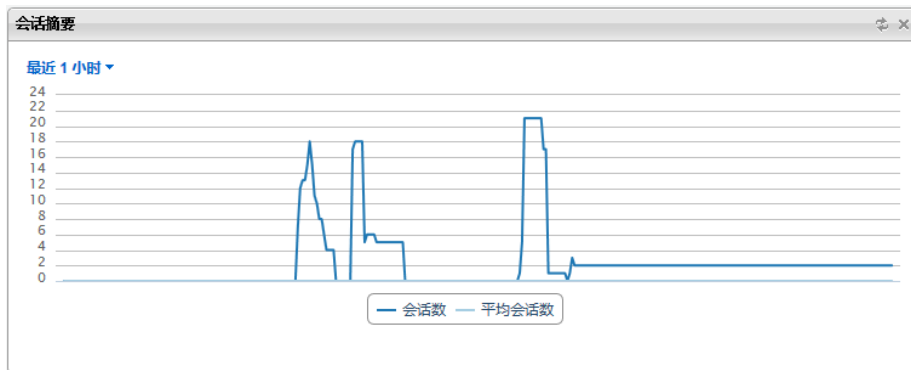
流量状态类别包含以下小组件：

- “会话摘要”小组件 第 5-14 页
- “用户排名”小组件 第 5-15 页
- “最常使用的应用程序”小组件 第 5-17 页
- “带宽摘要”小组件 第 5-18 页
- “带宽控制”小组件 第 5-18 页
- “最常访问的站点”小组件 第 5-20 页
- “最常访问的 URL 类别”小组件 第 5-21 页

“会话摘要”小组件

会话摘要小组件显示系统的 TCP/UDP 会话状态。

单击小组件底部图例中的项目可过滤显示的信息。将鼠标悬停在折线图的点上可获得更多详细信息。




要手动刷新数据，请单击小组件右上角的 🔄 图标。刷新率随显示的时间而不同。**最近 5 分钟**时间设置每 10 秒钟刷新一次。其他时间设置每分钟刷新一次。

“用户排名”小组件


用户排名小组件显示网络上最活跃的用户。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。

缺省情况下以条形图进行显示，但可以转换成以表格格式进行显示。要显示最常使用的应用程序，请扩大用户数据。

要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。

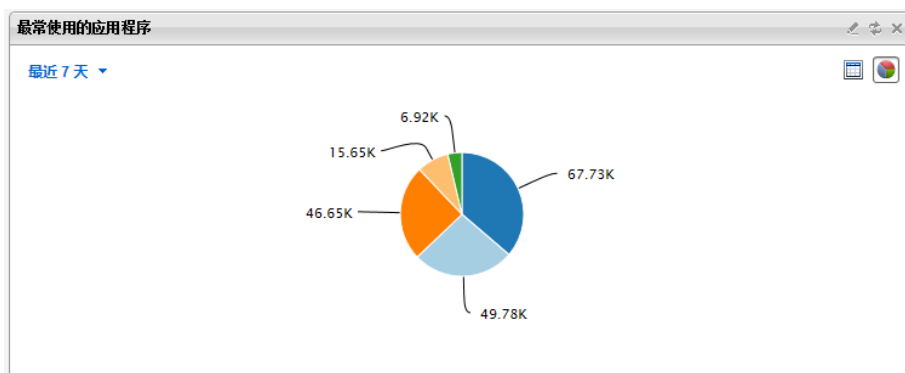


来源	带宽 (字节)	连接
 192.168.4.10	1.91M	113
HTTP	1.89M	44
DNS	11.42K	50
POP3	6.08K	12
Unknown	1.11K	7
 172.16.26.252	1.87K	4


要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

“最常使用的应用程序” 小组件


最常使用的应用程序小组件显示通过下一代应用安全网关的最常使用的应用程序（可配置成按带宽或按连接进行计数）。可配置显示的设备数量。缺省情况下显示前 5 个。



数据为最后一小时的数据。（例如：如果当前时间为下午 2:08，则该数据只能为下午 2:00 - 2:08 的数据。）

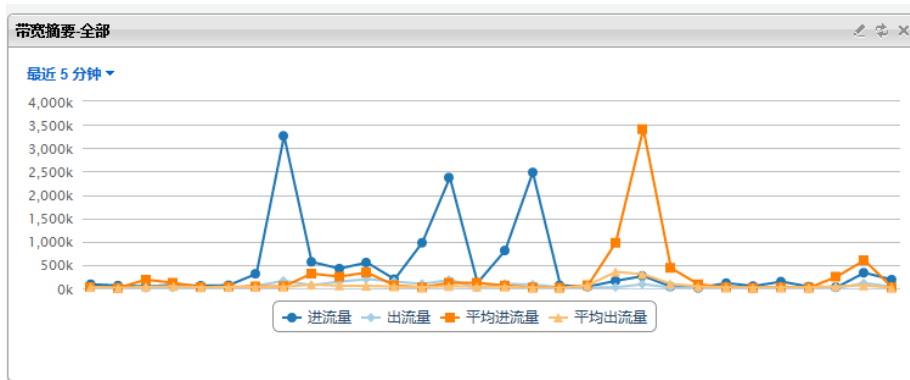
用户可设置显示的应用程序的数量。根据该信息，应用程序可按带宽或连接进行排序。要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。




要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。


“带宽摘要”小组件

该**带宽摘要**小组件根据 IP 地址显示带宽传入/传出信息。将鼠标放在折线的点上可显示特定接口的详细信息。数据为实时数据，但小组件本身也会累积数据。



传入/传出流量计数基于数据包的源地址。如果源地址为内部地址，则显示为“传出”，否则显示为“传入”。内部地址在**网络 > 地址组 > 缺省 Internal 地址**中进行配置。平均值计算基于与前一天相同的时间段。例如，如果当前值为 10:05，则使用前 7 天相同时间内的值计算相应的平均值。

一次可显示一个接口的流量。小部件的标题表示当前在小组件中显示的接口流量。要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。

要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

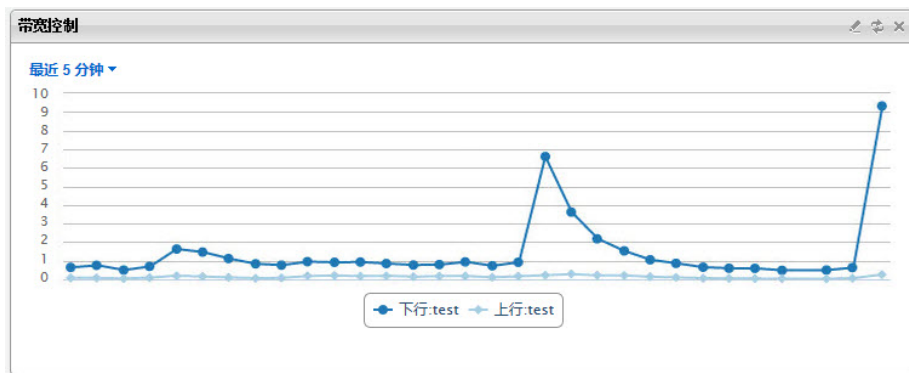
“带宽控制”小组件


带宽控制小组件显示选定时间段内所选带宽控制策略的上行和下行带宽。

**注意**

带宽控制小组件要求设置带宽控制策略。有关带宽控制策略的详细信息，请参阅[关于带宽控制 第 4-52 页](#)。

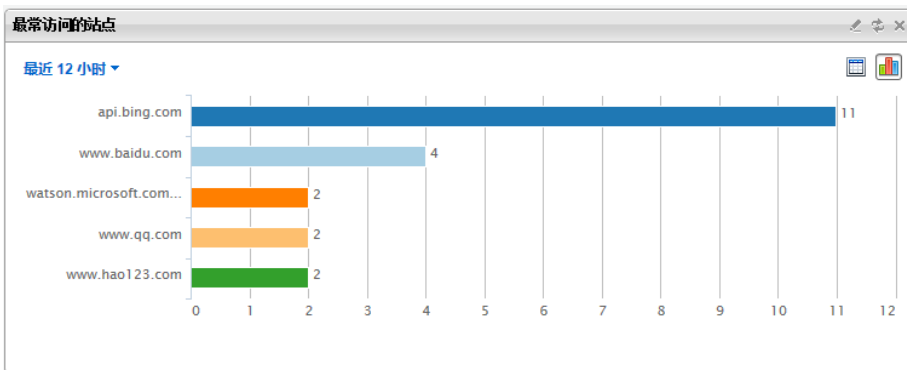
单击小组件底部图例中的项目可过滤显示的信息。将鼠标悬停在折线图的点上可获得更多详细信息。




要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。


“最常访问的站点”小组件

最常访问的站点小组件显示网络中最常访问的域。可配置显示的域的数量。缺省情况下显示前 5 个。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



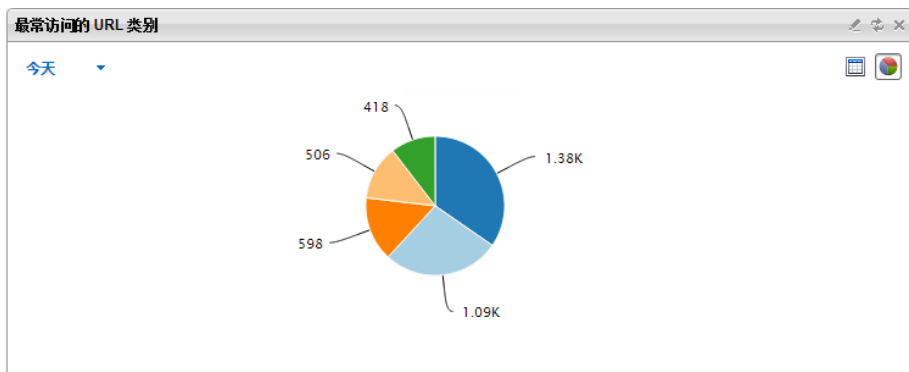
缺省情况下以条形图样式进行显示，但可以转换成以表格格式进行显示。


要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。


要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

“最常访问的 URL 类别” 小组件

最常访问的 URL 类别小组件显示与 URL 类别相关的违例。同样，可以显示最近一小时、一天、一周或一月的信息。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



缺省情况下以条形图样式进行显示，但可以转换成以表格格式进行显示。要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。

要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

关于安全状态小组件

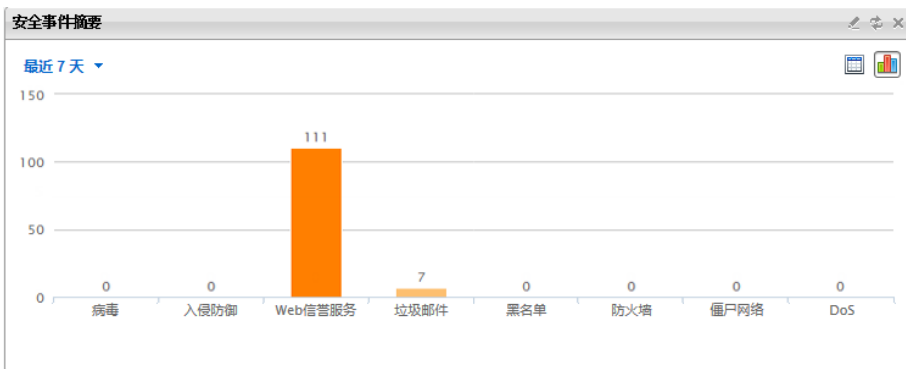
安全状态类别按以下类别显示最近一小时中威胁触发的次数：防火墙、病毒、入侵防御、Web 信誉服务、URL 过滤、垃圾邮件和黑名单。安全状态类别包含以下小组件：


- “安全事件摘要” 小组件 第 5-22 页
- “会话事件摘要” 小组件 第 5-24 页
- “Web 信誉服务保护的设备排名” 小组件 第 5-25 页
- 防病毒保护的设备排名 第 5-26 页

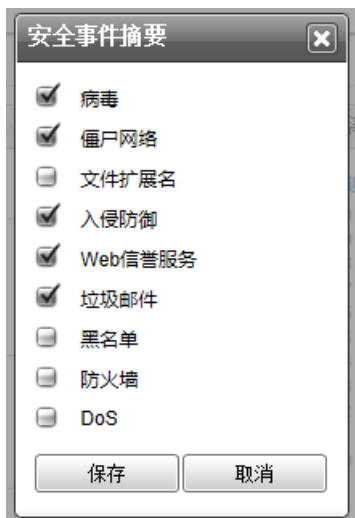
- “设备风险摘要” 小组件 第 5-26 页
- “入侵防御保护的设备排名” 小组件 第 5-28 页
- “反垃圾邮件保护的设备排名” 小组件 第 5-29 页
- 僵尸网络 第 5-29 页


“安全事件摘要” 小组件

安全事件摘要小组件通过条形图显示针对病毒、僵尸网络、入侵防御、Web 信誉服务和垃圾邮件所发现的违例。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



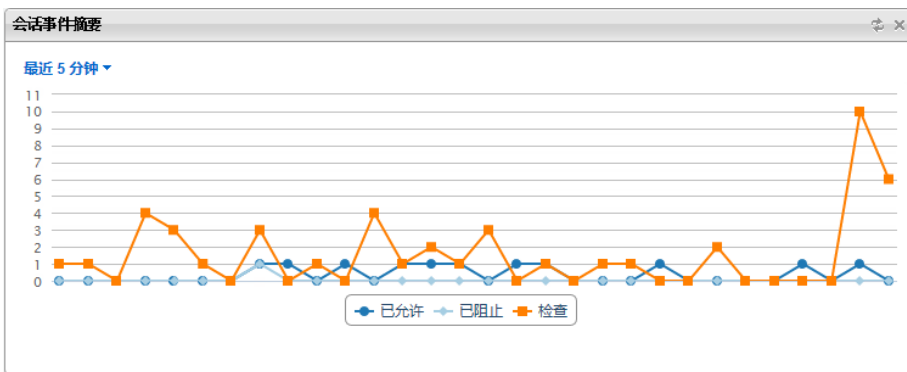
要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。缺省情况下以条形图样式进行显示，但可以转换成以表格格式进行显示。




要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

“会话事件摘要”小组件

会话事件摘要小组件显示了指定时间段内发生的会话事件，包括允许、阻止或检查的会话数。小组件自动刷新。



要更改显示的信息，请单击图例中的**允许**、**阻止**或**检查**图标。

要手动刷新数据，请单击小组件右上角的  图标。刷新率随显示的时间而不同。**最近 5 分钟**时间设置每 10 秒钟刷新一次。其他时间设置每分钟刷新一次。

“Web 信誉服务保护的设备排名” 小组件

Web 信誉服务保护的**设备排名**小组件显示与 Web 信誉服务 (WRS) 相关的违例。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



缺省情况下以条形图样式进行显示。单击位于图表右上角的表图标 (📄) 以表格格式显示信息。如果用户信息可用 (如果已将 IP 地址映射到用户)，则该小组件会将**源**列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。

如果用户信息可用 (如果已将 IP 地址映射到用户)，则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。

要配置显示的数据源，请单击小组件右上角的 🛠️ 图标，然后在显示的窗口中设置参数。

要手动刷新数据，请单击小组件右上角的 🔄 图标。小组件每分钟自动刷新一次数据。

防病毒保护的设备排名

防病毒保护的设备排名小组件显示与病毒相关的违例信息。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



缺省情况下以条形图样式进行显示。单击位于图表右上角的表图标 (📄) 以表格格式显示信息。如果用户信息可用（如果已将 IP 地址映射到用户），则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。

要配置显示的数据源，请单击小组件右上角的 📄 图标，然后在显示的窗口中设置参数。

要手动刷新数据，请单击小组件右上角的 🔄 图标。小组件每分钟自动刷新一次数据。

“设备风险摘要”小组件

设备风险摘要小组件显示具有安全信息汇总的设备排名。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。根据违例数量，该小组件从下列小组件中合并数据点：

- 入侵防御保护的设备排名
- 防病毒保护的设备排名
- 反僵尸网络保护的设备排名
- Web 信誉服务保护的设备排名
- 僵尸网络



缺省情况下以条形图样式进行显示。单击位于图表右上角的表图标 (📄) 以表格格式显示信息。如果用户信息可用 (如果已将 IP 地址映射到用户)，则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。


可配置显示的设备数量。缺省情况下显示前 5 个。要配置显示的数据源，请单击小组件右上角的 📄 图标，然后在显示的窗口中设置参数。


要手动刷新数据，请单击小组件右上角的 🔄 图标。小组件每分钟自动刷新一次数据。


“入侵防御保护的设备排名”小组件

入侵防御保护的**设备排名**小组件显示与入侵防御相关的信息。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



缺省情况下以条形图样式进行显示。单击位于图表右上角的表图标 () 以表格格式显示信息。如果用户信息可用（如果已将 IP 地址映射到用户），则该小组件会将**源**列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。

要配置显示的数据源，请单击小组件右上角的  图标，然后在显示的窗口中设置参数。

要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

“反垃圾邮件保护的设备排名”小组件

反垃圾邮件保护的**设备排名**小组件显示与垃圾邮件相关的违例。时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。



缺省情况下以条形图样式进行显示。单击位于图表右上角的表图标 (📄) 以表格格式显示信息。如果用户信息可用 (如果已将 IP 地址映射到用户)，则该小组件会将**源**列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。

要配置显示的数据源，请单击小组件右上角的 📄 图标，然后在显示的窗口中设置参数。

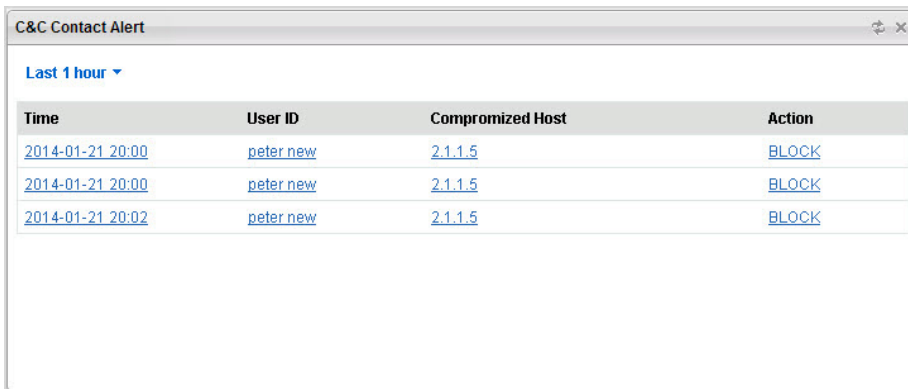
要手动刷新数据，请单击小组件右上角的 🔄 图标。小组件每分钟自动刷新一次数据。

僵尸网络

如果运行一个恶意软件，该恶意软件可能会立即发起与命令和控制 (C&C) 服务器的通信，等待进一步的指示，或潜伏在某个系统上数小时，试图保持隐藏状态。该软件访问 C&C 服务器时，通常会发生两种情况之一。首选，该软件可

自动下载和安装其他恶意软件。这种恶意软件类型称为“下载软件”。第二，该软件可以重新与 C&C 服务器通信。届时，监控 C&C 服务器的人员（攻击者）将通知新连接并发起某类操作。这种软件类型称为“远程访问特洛伊木马” (RAT)，能让攻击者检查系统、提取文件、下载要在受威胁系统上运行的新文件，打开系统的视频摄像头和麦克风，屏幕截图、捕获击键及运行命令 shell。


僵尸网络小组件可显示受威胁主机连接 C&C 服务器的所有尝试。当下一代应用安全网关检测到 C&C 回调尝试时，会根据策略操作配置控制通信。



The screenshot shows a window titled "C&C Contact Alert" with a refresh icon and a close button. Below the title bar, there is a dropdown menu set to "Last 1 hour". The main content is a table with four columns: Time, User ID, Compromized Host, and Action. The table contains three rows of data, all with the same values: Time: 2014-01-21 20:00, User ID: peter.new, Compromized Host: 2.1.1.5, and Action: BLOCK.

Time	User ID	Compromized Host	Action
2014-01-21 20:00	peter.new	2.1.1.5	BLOCK
2014-01-21 20:00	peter.new	2.1.1.5	BLOCK
2014-01-21 20:02	peter.new	2.1.1.5	BLOCK

时间段显示今天、最近 1 小时、最近 12 小时、最近 24 小时以及最近 7 天的相关信息。

要手动刷新数据，请单击小组件右上角的  图标。小组件每分钟自动刷新一次数据。

分析和报告

下一代应用安全网关可以生成有关检测到的病毒和恶意代码、阻止的文件和访问的 URL 的报告。您可以使用此有关下一代应用安全网关事件的信息来优化网络路由设置，并对安全策略进行微调。

日志分析

查看并分析关于带宽消耗的日志，策略如何控制网络通信，用户访问的站点，以及扫描引擎是否能使用户免受恶意软件、网络威胁和其他潜在危害的侵害。



注意

要查看详细的日志信息和示例，请参阅[日志详细信息](#) 第 B-1 页。

应用程序带宽日志

跨网络的 IP 地址、用户和应用程序查看并分析带宽消耗。查看日志后，调整已分配的上行和下行带宽来控制通信、阻止不需要的通信并将相应的带宽分配给关键通信和服务。

策略强制日志

查看并分析策略是如何控制网络通信的。查看日志后，调整策略规则可允许或过滤某些通信以及对配置错误的策略进行故障排除。

Internet 访问日志

查看并分析特定用户访问的 Web 站点和域。查看日志后，添加定制 URL 类别过滤某些类型的通信，并根据需要允许或阻止这些类别以外的特定 URL。

网络安全日志

查看并分析扫描引擎是如何防止用户免受恶意软件、网络威胁和其他潜在危害的侵害的。查看日志后，启用或禁用安全功能，并调整处理措施、时间表或用户策略从而更好地保护网络。

日志分析界面

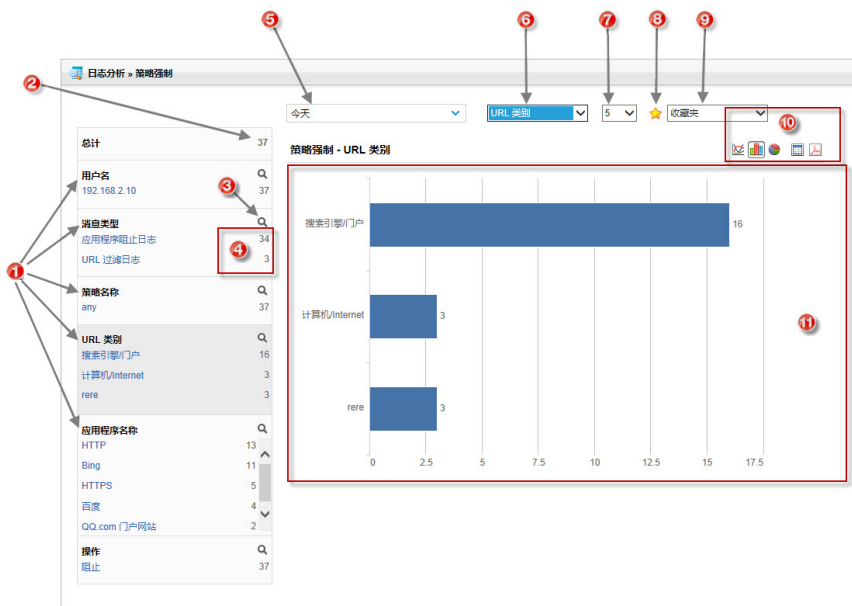



表 5-2. 日志分析界面描述


标注	描述
1	单击任意实体可显示其收集的日志。
2	查看策略违例或检测的总数。
3	单击  , 然后指定一条术语来搜索唯一的日志条目。

标注	描述
4	查看每个项目的计数。每个日志窗口都表示不同的日志数据。 <ul style="list-style-type: none"> • 应用程序带宽: 流量大小 • 策略强制: 策略违例 • Internet 访问: 访问 • 网络安全: 威胁
5	选择日志显示的时间范围。
6	为日志显示方式选择过滤选项。
7	选择显示最相关的日志。例如，选择 策略强制 中的前 10 个策略违例。
8	添加一个新收藏夹，将报告的日志结果收藏为书签。
9	从已保存收藏中选择以查看和分析更新日志。
10	控制图形布局。包括以下选项：条形图、折线图、饼图、表格和 PDF。
11	分析选定图形中显示的指定过滤器的日志结果。

日志分析菜单选项

下表介绍了过滤和控制**日志分析**图形的可用菜单选项。将其用于了解位于**分析和报告 > 日志分析**中的下拉菜单。

表 5-3. 日志分析菜单选项描述

菜单选项	示例	描述
用户名	Joe 用户	消耗流量或受恶意软件影响的用户。  注意 如果没有用户名信息， 用户名 会显示为客户端的 IP 地址。

菜单选项	示例	描述
客户端 IP	123.123.123.123	上行或下行流量的源或目标 IP 地址。 始终是源 IP 地址
应用程序名称	Google Picassa, Groupon	策略规则所控制的应用程序的名称。
策略名称	全局 URL 过滤	下一代应用安全网关管理员所指定的策略名称。
URL 类别	成人/未成年人不宜内容	一些基于要允许、过滤或阻止的托管内容类型的 Web 站点。
消息类型	HTTP 检查日志, APT 检测	基于 VSAPI、TMASE 或其他扫描引擎的其他安全信息汇总。要查看可用选项, 请转至 策略 > 安全设置 (IPS、防恶意软件、反垃圾邮件、WRS)。
操作	阻止, 监控	接收符合策略规则条件的数据包后, 策略执行的操作。
域	www.google.com	源或目标 IP 地址的主机名。
恶意软件名称	HTTP_REQUEST_GET_PRORAT_URI	威胁网络的恶意软件的名称。

日志收藏夹

添加日志收藏夹可创建定制日志分析书签, 以供将来参考。使用收藏夹将此信息包括在定制报告中。转到**分析和报告 > 日志收藏夹**以搜索或删除日志收藏夹。

报告

趋势科技下一代应用安全网关可以生成有关检测到的病毒和恶意代码、阻止的文件以及访问的 URL 的报告, 管理员可以使用此趋势科技下一代应用安全网关程序事件信息来优化程序设置, 并对安全策略进行微调。

趋势科技下一代应用安全网关可以生成预设报表或即时报表。

报告类别

趋势科技下一代应用安全网关有五种可用的报告类别：

- 带宽
- 策略强制
- Internet 访问
- 网络安全
- 定制报告

关于即时报表

报告基于日志数据。将下一代应用安全网关配置为在以下任一时间序列生成即时报表：

- 按需（接近实时）
- 一次
- 每日
- 每周
- 每月

生成即时报表

目的：生成即时报表。

位置：“分析和报告” > “报告”

过程

1. 选择要运行的首选“按需”报告模板。
 2. 单击**立即运行**。
-

关于预设报告

按一次性、每日、每周或每月定期生成预设报告。报告基于从注册设备上传的日志数据。

关于定制报告

使用定制报告可保存“收藏夹日志方面”，这样在创建报告模板时，即可在其中添加相关的“定制报告”类型。

关于报告模板

使用报告模板可按预设的时间间隔定期生成报告。报告模板中定义参数确定将在生成的报告中显示的数据的范围和数量。

关于报告模板设置

配置报告模板设置：数据范围、频率、要保存的报告数量及其他设置。

管理报告模板

目的：通过添加、编辑、复制或删除现有的报告模板来管理报告模板。

位置：“分析和报告” > “报告”

过程

- 打开要更改的任何所需报告模板，或者单击相应的按钮来复制、删除或添加报告模板。
-

添加/编辑报告模板

目的：通过定义报告模板名称和其他设置来添加/编辑报告模板。

位置：“分析和报告” > “报告”

过程

1. 单击**添加**或选择要更改的项目，然后单击**编辑**。
2. 指定报告模板名称和报告的简短描述。
3. 启用或禁用报告功能。
4. 指示所需的报告设置，包括日期范围和频率。

如果将**生成报告**设置为“按需”，则不会预设报告模板。在所有其他情况下，将会预设报告模板。

5. 要在报告生成时发送电子邮件通知，请启用**通过电子邮件发送报告**，然后指定报告收件人的电子邮件地址，以及此电子邮件模板的主题和内容。

使用逗号分隔多个条目。



重要信息

确保在**管理 > 通知 > SMTP 设置**中配置 SMTP 服务器和端口信息。

6. 指示要包括其报告的用户，是所有用户、特定用户或组，还是特定 IP 地址或范围。
7. 通过选择相应类型、格式或选项来定义单个报告模板。如果存在日志收藏夹，也可将定制报告选为额外报告类型。

8. 单击**保存**。
-

删除报告模板

目的：删除多个报告模板。

位置：“分析和报告” > “报告”

过程

1. 选择所需的报告模板。
 2. 单击**删除**。
-

复制报告模板

目的：复制多个报告模板。

位置：“分析和报告” > “报告”

过程

1. 选择所需的报告模板。
 2. 单击**复制**。
 3. 单击**确定**进行确认。
-

日志设置

转到**分析和报告** > **日志设置**以配置适用于所有日志的全局设置，包括：

日志选项

选择要记录的安全配置，并启用 Internet 访问统计日志记录。

日志管理

在指定天数后或在日志大小增加到特定阈值时清除日志。

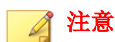
系统日志服务器

启用系统日志和系统日志转发。

配置全局日志设置

过程

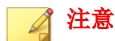
1. 转到**分析和报告 > 日志设置**。
2. 在**日志选项**下，设置以下参数：
 - a. 选择要记录的安全类型。



注意

启用安全日志可获得有关网络通信活动或用于问题排查的其他信息。禁用安全日志可能会提高性能。

- b. 选中**启用 Internet 访问日志**以启用网络通信统计日志记录。



注意

要捕获日志数据，还要在策略规则中启用 Internet 访问日志记录。有关详细信息，请参阅[添加策略规则 第 4-3 页](#)。

打开 Internet 访问日志比仅打开安全日志消耗更多存储。使用系统日志服务器从框中卸载日志以使日志保留较长时间

3. 根据需要，在**日志管理**下，设置以下限制：

选项	说明
将日志存储限制为 [x] GB	缺省值：2 GB
自动删除 [x] 天之前的日志	缺省值：62 天

4. 如果需要，更改日志删除之前的保留天数的清除值。



注意

将值设置为少于 62 天可能会阻止生成每月报告。将值设置为超过 62 天可能会导致累积数据过大以致影响性能。当日志超出大小限制时，将自动移除较旧的日志。

5. 如果需要，在**系统日志服务器**下，选中**启用系统日志并将所有日志转发给系统日志服务器**复选框。
 - a. 指定 IP 地址和端口号以转发系统日志。
 6. 单击**应用**。
-

设备日志

下一代应用安全网关将根据影响每种风险类型的策略设置检测安全风险并采取相应操作。这些事件将记录在日志中。不同日志类型之间的日志查询参数略有不同。

设备日志包括审计管理员登录到设备的时间、系统事件和 VPN 连接。

审计日志

审计日志包括以下信息：

- 所有网络更改/设置事件
- 所有管理员更改设置事件（包括更改人、更改规则、保存规则、提交规则）
- VPN 用户 — 添加/删除/编辑或更改密码
- AU 更新/还原的手动操作
- 日志查询显示用户、日期和操作
- 缺省时间周期为当天

- 当前系统日期的时间范围，显示范围内的当天
- 列出所有具有管理角色的用户 日志结果可按时间或用户排序
- 查看、打印生成的日志或将其导出为 CSV 格式的能力

系统事件日志

系统事件日志包括以下信息：

- 所有下一代应用安全网关服务启动/停止/重新启动
- 所有系统重新启动/重新引导
- 与 AU 相关的事件
- 管理通知事件

用户界面包括：

- 缺省时间周期为当天
- 时间范围会加载当前系统日期，并显示包括当天的范围
- 日志结果可按时间排序
- 查看、打印生成的日志或将其导出为 CSV 格式的能力

查询结果包括：

- 日期、时间
- 源（服务、系统、AU）
- 描述

VPN 日志

用于远程访问模式的 VPN 日志包括以下信息：

- 日志时间
- 开始时间
- 结束时间
- VPN 协议
- VPN 用户
- 事件（拨入、拨出）
- VPN 查询输入：时间范围、用户名或空白
- 查询结果：日期、时间、用户、事件
- VPN 和 PPPOE 调试日志保留 15 天
- 列出最近 15 天的信息，并从 UI 下载日志文件
- 查看、打印生成的日志或将其导出为 CSV 格式的能力

查询日志

以下过程说明了查询日志的一般流程。

过程

1. 转到**管理 > 设备日志**。
2. 选择以下要查询的日志之一：
 - 审计日志
 - VPN 日志
 - 系统事件日志
3. 选择用于过滤日志的**时间周期或定制范围**。
4. 指定日志查询参数。

5. 单击**查询、打印或导出为 CSV 格式**。
-

查询审计日志

过程

1. 转到**管理 > 设备日志**。
 2. 单击**审计日志**。
 3. 选择用于过滤日志的**时间周期或定制范围**。
 4. 在表的右侧，单击要审计的一个或多个帐户旁边的 **+** 图标。
该帐户将移动到**选定帐户**下的左侧。
 5. 要添加所有帐户，请单击右上角的**全部添加**。
 6. 单击**查询、打印或导出为 CSV 格式**。
-

查询系统事件日志

过程

1. 转到**管理 > 设备日志**。
 2. 单击**系统事件日志**。
 3. 选择用于过滤日志的**时间周期或定制范围**。
 4. 单击**查询、打印或导出为 CSV 格式**。
-

查询 VPN 日志

过程

1. 转到**管理 > 设备日志**。
 2. 单击 **VPN 日志**。
 3. 选择用于过滤日志的**时间周期**或**定制范围**。
 4. 指定 VPN 用户的用户名或 IP 地址。
 5. 单击**查询**、**打印**或**导出为 CSV 格式**。
-

第 6 章

管理

本章包括以下内容：

- [系统设置](#) 第 6-2 页
- [设备管理](#) 第 6-5 页
- [关于通知](#) 第 6-19 页
- [LDAP 用户识别](#) 第 6-11 页
- [管理帐户](#) 第 6-7 页
- [产品使用授权](#) 第 8-3 页
- [系统维护](#) 第 6-27 页
- [诊断](#) 第 6-29 页
- [关于下一代应用安全网关](#) 第 6-33 页
- [云安全智能防护网络：基于云的服务](#) 第 6-33 页

切换语言设置

下一代应用安全网关提供了英语和简体中文语言支持。

过程

1. 展开下一代应用安全网关 Web 控制台右上角的下拉列表框。
2. 选择相应语言。

系统设置

使用**系统设置**页面指定下一代应用安全网关设备的全局设置，如主机名以及时间和日期设置。其他高级设置包括会话超时和代理服务器设置。

常规系统设置

转到**管理 > 系统设置 > 常规**以配置下一代应用安全网关主机名以及 IPv4 或 IPv6 格式的主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。

关于位置和时间设置

使用**位置和时间**选项卡配置：

表 6-1. 位置和时间设置

设置	描述
时间设置	将系统时间设置为与 NTP 服务器同步或手动设置时间。
位置设置	选择下一代应用安全网关防火墙所处的位置和城市。

配置时间和日期设置

过程

1. 转到**管理 > 系统设置 > 位置和时间**选项卡。
2. 在**时间设置**部分，手动设置时间或将时间设置为与 NTP 服务器同步：
 - 要与 NTP 服务器同步，请选中**启用 NTP 服务器**复选框并添加 NTP 服务器 IP 地址。
 - 要手动设置时间，请选中**手动设置时间**复选框，并在时间值文本框中指定当前时间，格式如下：yyyy-mm-dd hh:mm:ss.例如：
2012-01-16 13:03:28
3. 在**位置设置**部分中，可选择距离下一代应用安全网关设备最近的位置和城市以设置相应的时区。



注意

趋势科技保持特定于位置的安全服务。下一代应用安全网关使用趋势科技 ActiveUpdate 服务更新到最新特征码和 Web 信誉技术以过滤 URL。例如，中国地区使用中国用户特定的 ActiveUpdate 和 Web 信誉服务。中国以外的地区使用其他地区的 ActiveUpdate 和 Web 信誉。

4. 单击**应用**。

关于控制台设置

下一代应用安全网关 Web 控制台设置包括以下选项：

- **会话超时**：如果 5 分钟内未进行任何活动，则断开管理会话的连接。建议使用此会话超时，以防止有人从已登录下一代应用安全网关却无人看管的 PC 使用 Web 控制台。
- **证书**：浏览并选择 Web 控制台的 SSL 证书。

配置 Web 控制台超时

过程

1. 转到**管理 > 系统设置 > 控制台设置**选项卡。
 2. 根据需要，在**空闲超时**部分中，设置会话超时。
 3. 在**证书设置**部分，添加证书设置。
 - SSL 证书
 - SSL 密码
 4. 单击**应用**。
-

关于代理服务器设置

将下一代应用安全网关配置为使用 HTTP 代理服务器进行产品更新、使用授权更新以及 Web 信誉查询。

配置代理服务器设置

过程

1. 转到**管理 > 系统设置 > 代理服务器设置**选项卡。
 2. 选中**使用 HTTP 代理服务器**复选框。
 3. 指定 HTTP 代理服务器 IP 地址和端口号。
 4. 如果需要，指定服务器要求的用户名和密码。
 5. 单击**应用**。
-

体验改善

选中**加入体验改善**复选框，以为趋势科技™贡献系统配置信息来帮助改善该产品。未曾向趋势科技发送过任何设备名称或 IP 信息。趋势科技获得的信息仅限于正在使用哪些功能。而趋势科技无法了解这些功能的配置方法。

设备管理

配置是否能够访问特定服务（SSH、SNMP）。通过设备管理，还可以访问下一代应用安全网关 CLI。

管理访问权限

将下一代应用安全网关管理接口配置为允许或阻止来自下一代应用安全网关设备之后的设备的特定类型的管理服务（或网络通信）。有三个位置可控制下一代应用安全网关设备的管理访问权限：

- 在**管理 > 设备管理 > 管理处**修改设备管理设置
- 在**网络 > 接口**处修改网络接口设置
- 在**网络 > 网桥**处修改网桥设置

启用管理服务（Web 控制台、Ping、SSH 和 SNMP）

启用管理服务可允许远程访问。通过启用 SNMP 支持，用户可以使用 SNMP 管理器获取有关支持的对象的信息。

过程

1. 转到**管理 > 设备管理 > 管理访问权限**。
2. 在表下面的文本框中，指定允许访问该设备的所有地址。

**注意**

此设置确定了可远程访问该设备的 IP 地址范围。支持单个 IP 地址，“-”符号可用作范围标记。使用 192.168.1.1/24 作为 IP 地址和网络掩码的格式。如果未指定任何格式，则允许所有 IP 地址进行访问。

3. 要为接口启用 **Web 控制台**、**Ping**、**SSH** 或 **SNMP** 服务，请选中相应的复选框。
4. 单击**应用**。

配置 SNMP 设置

过程

1. 转到**管理 > 设备管理 > SNMP 设置**。
2. 选中**启用 SNMP** 复选框。

**注意**

如果启用 SNMP 管理，用户可以使用 SNMP 管理器管理设备。

3. 指定 SNMP 设置。

选项	说明
电子邮件地址	指定联系人的电子邮件地址。
位置	联系人的位置，如“China office, IT room”。
团体名称	指定从下一代应用安全网关检索信息所需的团体字符串（缺省：public）。

**注意**

设备联系人的电子邮件地址和位置信息均可以在 SNMP 管理器中查看。仅当指定的团体字符串是有效的 v2 团体字符串时，SNMP 管理器才可以管理设备。

管理帐户

多个用户可以利用管理用户的身份访问下一代应用安全网关。这些用户可以对配置进行更改，这些更改将记录在审计日志中。访问权限还使您可以审计在下一代应用安全网关中进行的更改。如果必须遵守某些政府机构或公司信息安全标准，则具有其他管理帐户可能至关重要。

用户对系统具有不受限的完全访问权限。他们可以读取和修改可通过控制台访问的任何设置，包括创建、删除和修改用户帐户。

显示帐户列表

过程

- 转到**管理 > 设备管理 > 管理帐户**。

添加新帐户

所有用户拥有相同权限。

过程

1. 转到**管理 > 设备管理 > 管理帐户**。
2. 单击**新增**。
3. 指定用户名、密码、密码确认以及用户的可选描述。

4. 单击**添加**。
-

修改用户描述或密码


要更改帐户，请将管理员完全删除，然后添加具有相同凭证的新用户。

过程

1. 转到**管理 > 设备管理 > 管理帐户**。
 2. 单击要修改的帐户的名称。
 3. （可选）请执行以下操作：
 - 要更改密码，请单击**重置密码**，随后键入新密码并确认密码。
 - 要编辑描述，请在描述文本框中编辑文本。
 4. 单击**应用**。
-

删除管理帐户

过程

1. 转到**管理 > 设备管理 > 管理帐户**。
 2. 单击**删除**图标 。
 3. 在确认对话框中单击**删除**。
-

Web 命令行

Web 命令行选项卡提供对下一代应用安全网关命令行接口 (CLI) 的访问以便进行高级配置。强烈建议在您使用此 CLI 时与趋势科技支持部门代表配合工作以免出现配置错误。

终端用户管理

下一代应用安全网关通过定义授权用户列表（称为“用户组”）来控制对网络资源的访问。要使用特定资源（如网络或 VPN 隧道），用户必须：

- 属于其中一个允许访问的用户组
- 当系统要求时，指定正确的用户名和密码以证明其身份

关于常规设置

定义终端用户认证的全局设置，其中包括：


- 通过本地用户帐户或 LDAP 进行的用户认证。
- 下一代应用安全网关支持以下两种类型的 LDAP 认证缓存使用期限 (TTL) 选项：
 - 固定 TTL（初次命中）— 缓存用户上一次认证的时间。缺省值：2 小时
 - 最后的活动 TTL（最后一次命中）— 缓存用户最后一次与下一代应用安全网关交互的时间。缺省值：2 小时
- LDAP 同步时间间隔（1-48 小时）— 下一代应用安全网关定期对源自 LDAP 服务器的用户组映射进行自动同步。（缺省值为 24 小时）

配置常规设置

使用常规设置配置 CommonLDAP 的全局设置。

过程

1. 转到**管理 > 终端用户管理**
2. 打开 **LDAP 服务器**选项卡。
3. 在**用户类型**下，选择以下选项之一：

选项	说明
本地用户	用户使用在下一代应用安全网关中配置的凭证登录。有关详细信息，请参阅 本地用户和组管理 第 6-13 页 。  注意 选择 本地用户 以自动认证 VPN 用户。
LDAP	用户使用 LDAP 认证登录。有关详细信息，请参阅 LDAP 用户识别 第 6-11 页 。

4. 在**认证缓存**下，选择以下选项之一：
 - 固定 TTL (小时)
 - 最后的活动 TTL (小时)请参阅 [关于常规设置 第 6-9 页](#)。
5. 单击**应用**。

配置同步设置

过程

1. 转到**管理 > 终端用户管理 > 常规设置**

2. 打开**同步**选项卡。
 3. 使用**频率 (小时)** 设置 LDAP 同步时间间隔。
 4. 单击**刷新**对 LDAP 服务器执行手动刷新。
-

LDAP 用户识别

配置下一代应用安全网关如何识别客户端以定义 HTTP 病毒扫描、URL 过滤和应用程序控制策略的作用范围。所选择的用户识别方法还会确定在日志文件和报告中如何针对受影响的系统跟踪安全事件。

下一代应用安全网关提供的用户识别方法根据 IP 地址来识别客户端，然后应用相应的策略。

关于 LDAP 集成

下一代应用安全网关支持以下最常见的轻量级目录访问协议 (LDAP) 供应商：Microsoft 和 Linux。使用 LDAP 服务器，可通过下一代应用安全网关方便地创建特定于用户或组的策略。事件日志、报告和通知将使用您的 LDAP 层次结构来识别用户。

LDAP 认证

使用 LDAP 设置指定与下一代应用安全网关集成的 LDAP 服务器。下一代应用安全网关使用指定的 LDAP 服务器执行以下操作：

- 验证要在网页认证中识别的用户。
- 使用域控制器代理查询 DC 事件日志
- 对于管理员帐户，使用 Windows Management Instrumentation (WMI) 客户端查询
- 对于用户/组策略，使用策略设置和策略匹配

为了简化用户的 LDAP 配置，下一代应用安全网关提供了基本和高级 LDAP 认证方法。

配置 LDAP 认证设置

过程

1. 转到**管理 > 系统设置**以确保 DNS 已正确配置。
2. 转到**管理 > 终端用户管理 > LDAP 设置**。
3. 单击 **LDAP 服务器**选项卡。
4. 选择以下选项之一：

选项	说明
基本	指定 域名、用户名和密码 。有关详细信息，请参阅 基本 LDAP 认证第 6-12 页 。
高级	指定认证服务器，添加 LDAP 服务器并选择认证方法。有关详细信息，请参阅 高级 LDAP 认证第 6-13 页 。

5. 单击**测试 LDAP 服务器连接**。
6. 单击**应用**。

基本 LDAP 认证

下一代应用安全网关可以为使用最广泛的 LDAP 服务 MS Active Directory (AD) 提供简单 LDAP 配置。如果使用 AD，则可在 Web 控制台中输入以下基本信息来配置用户识别方法：域名、用户名和密码。

借助此信息，下一代应用安全网关可使用 AD 自动发现工具来获取必要的信息，其中包括：

- LDAP 服务器地址
- 基准域名
- 认证信息（Kerberos 范围/域/KDC）

这些信息将填充**高级 LDAP 认证**文本框。如果管理员确定自动发现的结果不正确或不起作用，则管理员可以切换到“高级模式”并修改设置。

对于 LDAP 服务器地址，自动发现工具可确定域中的所有域控制器，下一代应用安全网关将选择并使用速度最快的两台服务器。

高级 LDAP 认证

下一代应用安全网关为熟悉 LDAP 的用户提供了一种高级认证模式配置。

下一代应用安全网关支持下列 LDAP 服务器类型：

- MS Active Directory
- OpenLDAP

对于服务器关系，下一代应用安全网关仅支持对上述服务器进行“故障转移”。如果向主服务器认证失败，则下一代应用安全网关会尝试向辅助服务器进行认证。



注意

下一代应用安全网关只支持同一域内的多个 LDAP 服务器以进行故障切换。下一代应用安全网关不支持不同 LDAP 服务器的多个域。

对于 LDAP 认证方法，下一代应用安全网关支持针对 MS Active Directory 和 OpenLDAP 使用以下 LDAP 认证方法：

- 简单
- Kerberos

对于基本和高级模式，单击**测试 LDAP 服务器连接**按钮，以验证对配置的 LDAP 服务器进行认证的能力并报告结果。

本地用户和组管理

本地用户和组管理是当组织不使用 Active Directory 或 LDAP 认证时允许进行认证的机制（以及关联用户识别策略规则）。有关 LDAP 认证的详细信息，请参阅 [LDAP 用户识别 第 6-11 页](#)。

有关用户认证策略的详细信息，请参阅[关于认证 第 4-63 页](#)。

有关配置用户认证的网页认证的详细信息，请参阅[关于网页认证 第 4-65 页](#)。

配置本地用户帐户认证

过程

1. 创建本地用户帐户。

请参阅 [添加本地用户 第 6-15 页](#)。

2. 配置地址对象。

请参阅[配置地址对象 第 3-8 页](#)

3. 设置用户识别策略规则。

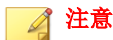
请参阅[添加认证规则 第 4-64 页](#)

4. 在属于内部网络的接口上启用下一代应用安全网关 Web 控制台。

请参阅 [启用管理服务（Web 控制台、Ping、SSH 和 SNMP） 第 6-5 页](#)。

5. 配置 DNS 设置。

请参阅 [常规系统设置 第 6-2 页](#)。



DNS 服务器必须存在于内部网络中，以供本地用户进行认证。

本地用户

创建本地用户帐户后，请转到[用户 VPN 第 3-51 页](#)以配置用户 VPN 规则。

添加本地用户

过程

1. 转到**管理 > 终端用户管理 > 本地用户**。
2. 单击**新增**。
3. 要允许用户登录，请选择**启用用户**。
4. 指定以下详细信息：
 - 用户名
 - 别名
 - 电子邮件地址
 - 密码
 - 描述



注意

需要每个用户设置一个高安全强度密码。本地用户帐户还可通过外部接口的 Web 服务用于 VPN。

5. 指定组成员资格。
请参阅[本地组 第 6-17 页](#)
 6. 单击**确定**。
-

将添加本地用户。

编辑本地用户

过程


1. 转到**管理 > 终端用户管理 > 本地用户**。

2. 在**用户名**列中，单击要编辑的本地用户帐户的用户名。
 3. 进行相应更改。
 4. 单击**确定**。
-

将编辑本地用户。

删除本地用户

过程

1. 转到**管理 > 终端用户管理 > 本地用户**。
 2. 选中本地用户帐户旁的复选框。
 3. 单击**删除**图标 。
 4. 在确认对话框中单击**删除**。
-

将删除本地用户。

从文件导入本地用户

下一代应用安全网关本地用户导入接受采用以下格式的逗号分隔值 (CSV) 文件：

用户名、别名、电子邮件、组、描述、启用、密码



注意

需要每个用户设置一个高安全强度密码。本地用户帐户还可通过外部接口的 Web 服务用于 VPN。

以换行符隔开每个新本地用户。

过程

1. 转到**网络 > 用户管理 > 本地用户**选项卡。
2. 单击**导入**。
将显示**导入用户**窗口。
3. 可以选择是否清除所有现有用户和组。
4. 单击**浏览**并选择格式正确的 CSV 文件。

CSV 文件中的所有帐户都导入为本地用户。

将本地用户导出到文件

过程

1. 转到**网络 > 用户管理 > 本地用户**选项卡。
2. 单击**导出**。

所有本地用户帐户都将以逗号分隔值 (CSV) 文件格式自动下载到浏览器指定的位置。

本地组

添加本地组

要添加或编辑本地组，请添加新的本地用户帐户或打开现有的本地用户帐户。

过程

1. 转到**管理 > 终端用户管理 > 本地用户**。
2. 单击现有的本地用户帐户，或单击**新增**。

3. 在**组**部分中，选中要删除的组旁边的复选框。
 4. 指定或更改组详细信息。
 5. 单击**应用**。
-

已添加本地组。

编辑本地组

要添加或编辑本地组，请添加新的本地用户帐户或打开现有的本地用户帐户。

过程


1. 转到**管理 > 终端用户管理 > 本地用户**。
 2. 单击现有的本地用户帐户，或单击**新增**。
 3. 在**组**部分中，单击要编辑的组名。
将显示**编辑组属性**窗口。
 4. 指定或更改组详细信息。
 5. 单击**应用**。
-

将编辑本地组。

删除本地组

过程

1. 转到**管理 > 终端用户管理 > 本地用户**。
2. 单击现有的本地用户帐户，或单击**新增**。
3. 在**组**部分中，单击要编辑的组名。
将显示**编辑组属性**窗口。

4. 单击**删除**图标 。
5. 在确认对话框中单击**删除**。

将删除本地组。

关于通知

通过“通知”部分，用户可以为下列事件配置通知：

- 安全信息汇总
- 硬件监控异常
- 系统资源警告
- 预设更新

使用 **SMTP 设置** 选项卡配置 SMTP 通知（SMTP 服务器名称、发件人、收件人）。有关配置 SMTP 通知的详细信息，请参阅[通知的 SMTP 设置 第 6-23 页](#)。

系统通知和警报

下一代应用安全网关支持以下项目的安全相关事件的电子邮件系统通知（警报）：防火墙、Web 信誉服务 (WRS)、恶意软件、入侵防御 (IPS)、URL 过滤和应用程序控制等违例。还可以发送电子邮件通知来警告发生硬件故障，如 CPU 温度升高、风扇速度加快或任何机箱入侵。

配置以下通知：

- 趋势科技下一代应用安全网关安全信息汇总
- 趋势科技下一代应用安全网关硬件监控异常
- 趋势科技下一代应用安全网关系统资源警告

- 趋势科技下一代应用安全网关预设更新

配置安全信息汇总通知

过程

1. 转到**管理 > 通知**。
 2. 单击**安全信息汇总**。
 3. 选中**启用**复选框以启用通知。
 4. 指定下列信息：
 - **通知一次的时间间隔**：根据接收通知的频率可以选择**1小时**、**6小时**、**12小时**或**24小时**。
 - **电子邮件发件人**：指定发送通知的电子邮件地址。
 - **电子邮件收件人**：指定将接收通知的电子邮件地址。
 5. 单击**应用**。
-

配置硬件监控异常通知

过程

1. 转到**管理 > 通知**。
2. 单击**硬件监控异常**。
3. 选中**启用**复选框以启用通知。
4. 指定下列信息：

选项	说明
电子邮件发件人	指定发送通知的电子邮件地址。
电子邮件收件人	指定将接收通知的电子邮件地址。
通知一次的时间间隔	根据接收通知的频率可以选择 30 分钟 、 1 小时 、 4 小时 或 12 小时 。
安全事件	选择一个或多个会触发通知的事件： <ul style="list-style-type: none"> • CPU 温度 • 环境温度 • 主板温度 • 风扇速度
阈值	对于每个选定的事件，选择将触发通知的阈值的百分比。 缺省值为： <ul style="list-style-type: none"> • CPU 温度：80°C • 环境温度：40°C • 主板温度：40°C • 风扇速度：550 转/分

5. 单击**应用**。

配置系统资源警告通知

过程

1. 转到**管理 > 通知**。
2. 在**通知事件**选项卡中，单击**系统资源警告**。

3. 选中**启用系统资源通知**以启用通知。
4. 指定下列信息：

选项	说明
发件人	指定发送通知的电子邮件地址。
收件人	指定将接收通知的电子邮件地址。
频率	选择接收通知的频率。
资源使用率百分比	选择一个或多个会触发通知的资源： <ul style="list-style-type: none"> • CPU • 数据分区 • 内存
阈值	对于每个选定的资源，选择将触发通知的阈值的百分比。缺省百分比为： <ul style="list-style-type: none"> • CPU 使用率百分比 — 90% • 数据分区使用率百分比 — 90% • 内存使用率百分比 — 90%

5. 单击**应用**。

配置预设更新通知

过程

1. 转到**管理 > 通知**。
2. 单击**预设更新**。
3. 选中**启用**复选框以启用通知。
4. 选中以下一项或两项的相应复选框，以指定发送通知电子邮件的时间：

- 系统更新成功时发送通知
 - 系统更新失败时发送通知
5. 指定发送通知的电子邮件地址和接收通知的电子邮件地址。
多个地址之间使用半角逗号隔开。
 6. 单击**应用**。
-

停止通知

过程

1. 转到**管理 > 通知**。
 2. 单击要停止的通知名称。
 3. 取消选中**启用**复选框以禁用通知。
 4. 单击**应用**。
-

通知的 SMTP 设置

要生成有关安全信息汇总、系统资源警告或预设更新日志条目的电子邮件，请务必指定电子邮件设置。在定义电子邮件设置后，可以启用电子邮件通知，如[系统通知和警报](#) 第 6-19 页中所示。

配置通知的 SMTP 设置

无法删除在任何系统设置、配置日志设置或日志记录安全配置中使用的电子邮件设置。

过程

1. 转到**管理 > 通知 > SMTP 设置**。
 2. 指定下列参数：
 - **SMTP 服务器名称和端口号**：指定用于发送电子邮件的简单邮件传输协议 (SMTP) 服务器的 IP 地址或主机名和端口号。
 - **电子邮件发件人**：指定“发件人”电子邮件地址，如“security_notification@company.com”。
 - **电子邮件收件人**：指定收件人的电子邮件地址。
 3. 单击**测试 SMTP 服务器连接**。

您将接收到两条确认信息。一条信息将显示连接已成功。另一条信息将显示设置已成功应用。
 4. 如果未测试连接，请单击**应用**保存新的设置。
-

产品使用授权

通过产品使用授权功能，组织可以注册下一代应用安全网关并为其授予使用许可。完全激活下一代应用安全网关需要两个步骤。首先，向趋势科技注册下一代应用安全网关。注册后，将提供一个有效的下一代应用安全网关激活码 (AC) 以授予产品许可。

有关更新和维护产品使用授权的详细信息，请参阅[保持更新 第 7-1 页](#)。

更新

新的恶意程序和攻击性 Web 站点层出不穷。下一代应用安全网关提供了多个保持最新的方法。在下一代应用安全网关 Web 控制台中，转到**管理 > 更新**以查看有关最新特征码文件和系统更新的更新，从而保护下一代应用安全网关。

有关更新下一代应用安全网关产品组件的详细信息，请参阅[保持更新 第 7-1 页](#)。

设备日志

下一代应用安全网关将根据影响每种风险类型的策略设置检测安全风险并采取相应操作。这些事件将记录在日志中。不同日志类型之间的日志查询参数略有不同。可以配置日志启用、日志保留期限和系统日志转发等日志设置。

设备日志包括当管理员登录到下一代应用安全网关后对系统事件和 VPN 连接的审计。有关分析设备日志的详细信息，请参阅[设备日志 第 5-40 页](#)。

邮件隔离

隔离查询可用于邮件导出、删除和重新发送。当邮件与某个策略匹配且处理措施为“隔离”时，下一代应用安全网关会将邮件移到隔离区域。为避免对性能产生负面影响，必须设置合适的约束，以减少隔离邮件存储。提供了手动清除功能。

查询邮件隔离

如果为垃圾邮件选择了**隔离**处理措施，这些邮件将移动到隔离区域。可以查询所有隔离的邮件。

过程

1. 转到[管理 > 邮件隔离 > 查询](#)。
2. 根据需要，设置以下搜索过滤器：
 - [时间周期或定制范围](#)
 - [协议](#)

- 状态
 - 隔离原因
 - 发件人、收件人或主题
3. 单击**查询**。
 4. 在返回的结果中，单击**详细信息**列中的图标，以获取有关隔离区中特定邮件的详细信息。
 5. 执行下列操作之一：
 - 重新发送电子邮件（如果需要）。



注意

如果未配置重新发送 SMTP 服务器，则电子邮件在隔离时将重新发送到原始 IP 地址。有关配置 SMTP 重新发送服务器的信息，请参阅[配置邮件隔离设置](#) 第 6-26 页。

- 删除电子邮件（如果不需要）。
 - 将电子邮件导出到相应用户（如果下行邮件服务器不可用）。
-

配置邮件隔离设置

指定隔离存储大小和清除频率。也可以启用和配置 SMTP 邮件服务器的重新发送设置。

过程

1. 转到**管理 > 邮件隔离 > 设置**。
2. 指定隔离区域的大小（以 GB 为单位）。（缺省值：2GB）
3. 指定保留隔离邮件的天数。（缺省值：10 天）

**注意**

可以按大小或日期清除隔离区域。

4. 启用用于重新发送电子邮件的 SMTP 服务器（如果需要）。
 5. 指定 SMTP 服务器 IP 地址、端口和认证凭证。
 6. 单击**应用**。
-

系统维护

使用**维护**页面可关闭和重新启动下一代应用安全网关，以及备份和恢复配置。有关维护的更多详细信息，请参阅[产品维护和使用授权](#) 第 8-1 页。

执行系统维护

下一代应用安全网关可提供系统维护功能。

**警告!**

应用系统维护操作会断开所有用户的连接。

过程

1. 转到**管理 > 维护 > 系统维护**选项卡。
2. 选择相应选项：
 - **关闭** — 停止服务、关闭设备并关闭电源。
 - **重新启动** — 停止服务并重新启动设备。
 - **恢复到出厂设置** — 恢复设备的原始硬件设置。
3. 在**消息**下，（可选）指定日志中与事件对应的消息（最多 100 个字符）。

4. 单击**应用**。

配置备份与恢复

使用**管理 > 维护**页面上的**备份/恢复**选项卡来执行以下操作：

- 为现有配置设置创建备份文件
- 从备份文件恢复配置设置

备份当前配置

应用 Patch 后，即可恢复下一代应用安全网关配置备份。

过程

1. 在 Web 控制台上，转到**管理 > 维护 > 备份/恢复**。
 2. 在**备份配置**下，单击**创建备份**。
将下载备份文件。
-

当前下一代应用安全网关配置现已保存。

恢复先前的配置

先前的下一代应用安全网关配置可以在系统故障或升级之后恢复。

过程

1. 在 Web 控制台上，转到**管理 > 维护 > 备份/恢复**。
2. 在**恢复配置**部分中，单击**浏览**。
将显示**打开**对话框。

3. 导航到存储备份文件的文件夹并选择该文件，然后单击**打开**。
4. 单击**恢复**。

将恢复下一代应用安全网关配置备份。您现在可以准备执行进一步的配置更改或开始使用下一代应用安全网关。

诊断

使用下一代应用安全网关的诊断工具来执行以下操作：

- 运行数据包捕获，以调试和分析网络通信。
- 确定数据包在 IP 网络中所采用的路由
- 为趋势科技技术支持部门创建情况诊断文件。

数据包捕获

“数据包捕获”向导位于**管理 > 诊断 > 数据包捕获**。使用已捕获的数据包执行网络通信调试或分析。

选择在单一或多个网络接口上同时捕获网络数据包。捕获开始后，将显示已用时间。当管理员单击**停止捕获**或当配置的时间或大小满足条件时，捕获操作将停止。

每个接口的数据包捕获将会保存为命名约定为“capture-`{interface}`-`{date:time}`.pcap”的单个文件。例如，capture-eth0-2013-07-02.1329518492.75.pcap.tar.gz 将会是 2013 年 7 月 2 日在 eth0 网络接口上执行的数据包捕获的文件名。

在完成数据包捕获之后，所有数据包捕获文件将保存在一个名为“capture-`{date}`.tgz”的压缩软件包文件中。该文件将显示在可下载列表中。可以下载或删除相应压缩文件。

要为过滤器确定一些组件，请针对 HTTP 请求或响应运行数据包捕获。请参阅图 6-1：用于 Google 搜索的数据包捕获 第 6-30 页中的捕获示例和表 6-2：数据包捕获中显示的组件 第 6-30 页中的说明。

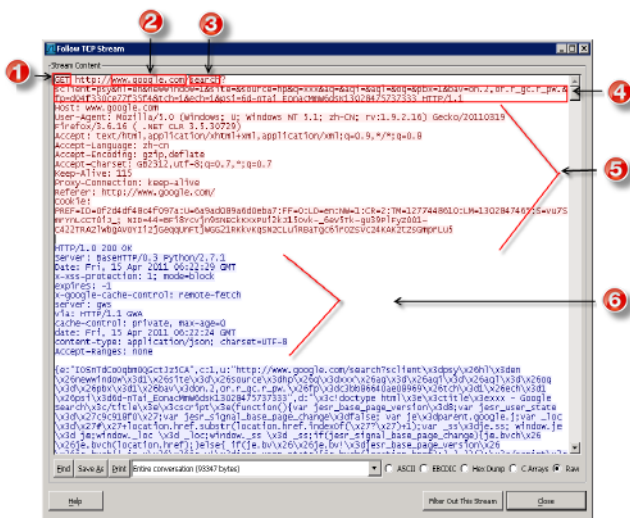


图 6-1. 用于 Google 搜索的数据包捕获

表 6-2. 数据包捕获中显示的组件

标注	组件
1	请求方法
2	URL 主机
3	URL 路径
4	URL 查询
5	请求标头
6	响应标头

捕获网络数据包

捕获数据包来分析选定接口或单个接口的网络通信。

过程

1. 转到**管理 > 诊断**，然后单击**数据包捕获**。
2. 从**接口**列选择相应的接口。
3. 填写下列文本框：
 - 指定用于捕获数据包的 IP 地址
 - 指定用于捕获数据包的端口
 - **大小限制 (MB)**（缺省值：500MB）
 - **超时 (分钟)**（缺省值：30 分钟）

4. 单击**开始捕获**。

将显示已用时间。当达到文件大小上限 500 MB 时，捕获将停止，除非为**捕获数据包限制 (MB)** 选项配置了较小的文件大小。

5. 如有必要，请单击**停止捕获**以在达到文件大小上限前停止数据包捕获。
 6. 捕获完成后，选中捕获文件的复选框，然后选择一项处理措施：
 - 单击**处理措施**列中的图标，然后打开捕获文件。
 - 单击**删除**图标可删除选定的生成文件。
-

通信跟踪

使用通信跟踪生成会话详细信息，以帮助诊断应用程序存在的任何问题。该网络工具将确定数据包在 IP 网络上采用的路由。

过程

1. 转到**管理 > 诊断 > 通信跟踪**。
 2. 指定将从中跟踪网络通信的 **IP 地址**和**端口**。
 3. 从**操作**下拉列表框中选择要跟踪的操作：**全部**、**允许**或**阻止**。
 4. 单击**启动**。
 5. 单击**停止**可停止跟踪。
 6. 可在**捕获的会话**部分查看结果。单击某个会话可查看该会话的详细信息。
-

生成诊断文件

趋势科技情况诊断工具 (CDT) 可以利用诊断文件创建一个文件，以帮助趋势科技技术支持部门诊断设备出现的问题。

过程

1. 转到**管理 > 诊断 > 诊断文件**。
 2. 单击**生成诊断文件**。
-

支持

要从 Web 控制台获取支持信息，请转到**管理 > 支持**。有关问题排查、维护和
支持的其他信息，请参阅[技术支持 第 A-1 页](#)。

关于下一代应用安全网关

管理 > 关于页面提供了产品版本和许可协议信息。

云安全智能防护网络：基于云的服务

云安全智能防护网络 (SPN) 是行业内最高等级的基于云的恶意软件防护服务。云安全智能防护网络包含以下恶意软件检测组件：

表 6-3. SPN 服务

服务	描述
Web 信誉服务 (WRS)	<p>由若干个相关联的服务组成，这些服务能够主动检测并阻止已知的恶意 Web 站点、域、文件和对象以及电子邮件相关项，包括防域名欺诈和防网络钓鱼检测功能。</p> <ul style="list-style-type: none"> • 域信誉 • 页面信誉 • 电子邮件信誉 • 文件信誉
URL 过滤服务	<p>可在云中存储 URL 数据库，以便于快速更新，并可保护趋势科技的全球用户群，而无需从下一代应用安全网关服务器下载和更新 URL 数据库文件。这样，就可以为每个客户提供最新的 URL 信息，并能够加快主动保护的速度，以缩短发现恶意站点与将该站点添加到 URL 数据库来保护所有客户之间的时间差。</p>
反馈循环	<p>可提供所有趋势科技产品的实时信息，以更新基于云的 SPN 组件和 URL 过滤数据库。在客户设备上检测到的恶意软件可以实时反馈到云体系结构，并用于对信息进行微调。这样就加快了主动保护趋势科技全球客户群的速度，并且误报率低。</p>

DNS 最佳实践建议

云安全智能防护网络 (SPN) 使用基于云的服务，并依靠 DNS 查询进行查找。为确保快速响应并减少延迟，必须为下一代应用安全网关设备配置主和辅助 DNS 服务器。

该 DNS 服务器必须能够支持下一代应用安全网关所发出的 DNS 请求量。通常，在下一代应用安全网关构建其本地 DNS 缓存之前，会为所访问的每个 URL 生成两个 DNS 请求。请确保安装 DNS 服务器的服务器具有足够的资源和性能来处理额外的 DNS 请求量。

要减少延迟，每个 DNS 服务器应配有一个快速网卡，并安装在一个快速网络交换机上。

与 ISP 在公司网络外部提供的 DNS 服务器相比，趋势科技建议使用现场 DNS 服务器。通常，ISP DNS 服务器的延迟率很高，并且不支持单一 IP 地址发出的大量 DNS 查询。许多 ISP DNS 服务器都具有一定的限制机制，用于限制每秒发出的 DNS 请求数，因此可能会影响下一代应用安全网关的 Web 信誉服务 (WRS) 性能。

要缩短网络响应时间并提高性能，请尝试将 DNS 服务器放在尽可能靠近下一代应用安全网关单元的位置上，以消除设备间不必要的网络跃点。

Web 信誉服务和 URL 过滤请求将通过 HTTP 端口 80 发出。请不要在防火墙上阻止这些端口上的下一代应用安全网关管理 IP 地址。

第 7 章

保持更新

新的恶意程序和攻击性 Web 站点层出不穷。下一代应用安全网关提供了多个保持最新的方法。在下一代应用安全网关 Web 控制台中，转到**管理 > 更新**以查看有关最新特征码文件和系统更新的更新，从而保护下一代应用安全网关。

本章包括以下内容：

- [可更新的程序组件 第 7-2 页](#)
- [ActiveUpdate 第 7-5 页](#)
- [手动更新 第 7-8 页](#)
- [预设更新 第 7-11 页](#)

可更新的程序组件

为了确保能够以最新防护抵御最新风险，可以更新以下几个特征码文件组件：

这些文件包含已知安全风险的二进制“特征”或特征码。当已知风险通过 Internet 网关时，下一代应用安全网关使用二进制“特征”或特征码来检测已知风险。新的病毒码文件通常每周发布数次，而协议和入侵防御特征码文件的更新频率则较低。

防恶意软件病毒码文件

趋势科技扫描引擎使用一种外部数据文件（称为病毒码文件）来保持与最新的病毒和其他 Internet 风险（例如，特洛伊木马、群发邮件程序、蠕虫和混合式攻击）同步。新的病毒码文件每周会创建和发布数次，并在发现危害极大的风险时随时创建和发布。

每当服务器上发布新的病毒码文件时，使用 ActiveUpdate 功能（有关详细信息，请参阅 [ActiveUpdate 第 7-5 页](#)）的所有趋势科技防病毒程序都可以检测到该情况，并且可以预设为按每小时、每天、每周等时间间隔自动轮询服务器以获取最新文件。

如果在同一目录中有多个病毒码文件，则只使用编号最高的病毒码文件。趋势科技会定期发布新的病毒码文件（通常每周数次），并建议您在**管理 > 更新 > 特征码更新**窗口上配置每小时自动更新。所有与趋势科技签有有效维护合同的客户均可进行更新。



“安装”新的特征码文件时，不需要删除旧的特征码文件或执行任何特殊步骤。

防恶意软件协议特征码文件

网络内容检查引擎 (NCIE) 使用防恶意软件特征码文件执行网络扫描。

C&C 联系人信息特征码

命令与控制 (C&C) 联系人信息特征码为下一代应用安全网关提供增强的删除和警报功能，以减少持续的高级威胁和针对性攻击造成的破坏。

入侵防御特征码和引擎

下一代应用安全网关使用入侵防御特征码文件和引擎阻止入侵防御漏洞。如果特征码之间的比较结果表明网络连接存在漏洞，则下一代应用安全网关将根据配置采取相应的处理措施。

病毒扫描引擎和特征码

病毒扫描引擎会分析每个文件的二进制特征码，并将其与特征码文件中的二进制信息进行比较。如果有匹配项，则确定为恶意文件。

IntelliTrap 特征码和例外

IntelliTrap 检测会使用带有 IntelliTrap 特征码（对于潜在的恶意文件）和 IntelliTrap 例外特征码（作为白名单）的趋势科技病毒扫描引擎中的扫描选项。下一代应用安全网关会使用可供检测恶意压缩文件（如压缩文件中的 bot）的 IntelliTrap 选项和特征码。病毒写入程序通常会尝试通过使用不同的文件压缩方案来规避病毒过滤。IntelliTrap 对压缩文件进行启发式评估，以帮助降低 bot 或任何其他恶意压缩文件可能对网络造成的风险。

间谍软件特征码

随着秘密收集机密信息的新隐藏程序（灰色软件）的编写、公开发布和发现，趋势科技会收集其泄密签名并将信息整合到间谍软件/灰色软件特征码文件中。

反垃圾邮件特征码和引擎

垃圾邮件特征码可帮助下一代应用安全网关确定邮件和附件中的最新垃圾邮件。反垃圾邮件引擎可检测邮件和附件中的垃圾邮件。

Web 信誉服务

利用全球最大的域信誉数据库之一，趋势科技 Web 信誉技术可根据 Web 站点年限、历史位置变更以及通过恶意软件行为（例如，旨在诱使用户提供个人信息的网络钓鱼欺诈）分析发现的可疑活动指示等因素分配信誉分数，来跟踪 Web 域的可信度。为提高准确性并减少误报，趋势科技 Web 信誉服务为站点内的特定网页或链接分配信誉分数，而不是对整个站点进行分类或阻止，因为通常只有合法站点的某些部分被非法侵入，且信誉可随时间动态变化。

URL 数据库

URL 数据库与其他趋势科技™云安全智能防护网络™服务器均驻留在云中。当用户尝试访问某个 URL 时，下一代应用安全网关会从该数据库中检索有关此 URL 的信息，并将其存储在本地缓存中。将 URL 数据库存储在云中并使用此数据库信息构建本地缓存，可降低下一代应用安全网关的开销并提高性能。

针对通过下一代应用安全网关的所请求 URL，将检索以下信息：

- Web 分类，可以与 URL 过滤策略一起使用以控制对 Web 站点的访问。
- Web 信誉分值，用于根据指定的敏感度级别来阻止 URL 访问（请参阅[配置 Web 信誉服务安全配置 第 4-45 页](#)）。

URL 数据库会使用最新的 Web 页面分类和信誉进行实时更新，以提供有关终端用户可能尝试访问的任何 URL 的最新信息。

如果认为某个 URL 的信誉分类有误或者您想要了解某个 URL 的信誉，请使用下面的链接通知趋势科技：

<http://SiteSafety.trendmicro.com>

电子邮件信誉数据库

趋势科技在中央数据库中维护着一个属于已知垃圾邮件发件人的 IP 地址列表。电子邮件信誉通过阻止存储在该数据库中的 IP 地址来过滤垃圾邮件。

缺省情况下，下一代应用安全网关中的反垃圾邮件安全配置会使用电子邮件信誉（一个云安全智能防护网络™ 组件，可使用世界最大且最可信的信誉数据库之一以及动态信誉数据库来验证传入电子邮件的 IP 地址）识别新的垃圾邮件和网络钓鱼来源，从而在僵尸程序和僵尸网络首次出现时就将其停止。

病毒码文件的增量更新

ActiveUpdate 支持对最新特征码文件进行增量更新。ActiveUpdate 可以只下载新增的文件部分，并将其附加到现有文件，而不是每次都下载整个文件。这种高效的更新方法可以显著减少在贵组织环境内更新防病毒软件或部署特征码文件所需的带宽。

组件版本信息

要了解正在运行哪个特征码文件或应用程序 build，可以在主菜单中单击**实时监控**。正在使用的应用程序版本将显示在**系统信息**小组件中。**特征码信息**小组件显示了特征码版本。（如果上述小组件均未显示，可单击**添加小组件**，然后将所需的小组件添加到实时监控中。）

组件版本信息也可以通过**管理 > 更新 > 特征码更新**获得。

ActiveUpdate

下一代应用安全网关使用 ActiveUpdate，它是一种趋势科技实用程序，可对病毒码文件以及扫描引擎、间谍软件或灰色软件特征码文件启用按需更新或后台更新。ActiveUpdate 是许多趋势科技产品的一项通用服务。ActiveUpdate 可以连接到趋势科技的 Internet 更新服务器，以下载最新的特征码文件和引擎。

ActiveUpdate 不会中断网络服务，也不需要重新启动端点。可以按照预设时间间隔定期进行更新，也可以根据需要手动进行更新。

关于从 Web 控制台更新

下一代应用安全网关会直接轮询 ActiveUpdate 服务器。更新后的组件将按照您所定义的时间表部署到下一代应用安全网关，如下所示：

- 每小时
- 每周
- 每日
- 按需（手动）



注意

趋势科技建议您每日更新特征码文件。

配置用于更新的代理服务器设置

如果使用代理服务器访问 Internet，请使用下一代应用安全网关 Web 控制台指定代理服务器信息，然后才能尝试更新组件。指定的代理服务器信息用于执行以下操作：

- 从趋势科技的更新服务器更新组件
- 产品注册和使用授权
- Web 信誉查询

过程

1. 在下一代应用安全网关 Web 控制台中，转到**管理 > 系统设置 > 代理服务器设置**。

2. 选择**使用 HTTP 代理服务器 (进行系统更新、使用授权更新及其他操作。)**，以指定代理服务器或端口。
3. 如果代理服务器要求认证，请选中该复选框并指定用户 ID 和密码。

**注意**

如果代理服务器不要求认证，请将这些文本框保留为空。

4. 单击**应用**。

**注意**

在网桥模式下，下一代应用安全网关具有一个内部接口和一个外部接口。要确保更新能够正常运行，ActiveUpdate 代理服务器与服务器设置必须在同一端配置。如果使用其他代理服务器部署下一代应用安全网关，则 ActiveUpdate 代理服务器和服务器的下一跳地址代理服务器设置应为该接口的同一端上的同一台服务器。

选择更新源

过程

1. 转到**管理 > 更新**。
 2. 单击**组件**选项卡。
 3. 在**源**下，选择更新源。
 - **趋势科技 ActiveUpdate 服务器**
选择此选项可自动从 ActiveUpdate 接收更新。
 - **其他 Internet 源**
选择此选项可指定自己的更新源的 URL。
 4. 单击**应用**。
-

手动更新

下一代应用安全网关的有效性取决于是否使用了最新的特征码文件。基于特征的病毒扫描的工作方式是：将所扫描文件的二进制特征码与特征码文件中的已知风险的二进制特征码进行比较。趋势科技会经常发布新版本的病毒码和间谍软件特征码，以应对最新发现的风险。同样，当发现新的网络钓鱼 URL 时，也会发布新版本的网络钓鱼特征码。

应用系统更新

下载产品 Patch 并（可选）备份当前配置后，请将更新应用到下一代应用安全网关。

当特征码文件已损坏且必须再次从更新服务器下载时，手动更新功能也非常有用。

过程

1. 下载 Patch。

请参阅 [下载产品 Patch 第 7-9 页](#)。

2. 在 Web 控制台中，转至**管理 > 更新 > 系统更新**。
3. 在**选择要安装的更新包**下，单击**浏览**。

将显示**打开**对话框。

4. 导航到包含已下载文件的文件夹并选择该文件，然后单击**打开**。
5. 单击**上传**。

可以准备恢复之前保存的配置或开始新的配置。

后续步骤

遵循窗口上的 Patch 说明以应用该 Patch。

下载产品 Patch

此过程允许您选择所需的产品 Patch 并将其下载到下一代应用安全网关。

过程

1. 转到 <http://downloadcenter.trendmicro.com/?regs=CH> 并选择下一代应用安全网关。
 2. 打开**产品 Patch** 选项卡。
 3. 选择适用的产品 Patch 并单击**下载软件包**图标。
 4. 将文件保存到要更新的下一代应用安全网关设备可以访问的位置。
-

更新组件

如果下一代应用安全网关已在使用最新版本的组件，则不会更新任何组件。

过程

1. 转到**管理 > 更新**。
2. 单击**特征码更新**选项卡。
3. 选择要更新的部分或全部特征码，然后单击**立即更新**

可用性列显示特征码是否有可用的新版本。

如果下一代应用安全网关上的特征码文件版本高于或等于远程下载服务器上的对应版本，则会显示一个消息框。如果下一代应用安全网关上的特征码文件早于远程下载服务器上的文件，则会下载较新的特征码文件。

验证更新是否成功

下一代应用安全网关 Web 控制台的**实时监控**窗口将在“特征码信息”小组件中显示正在使用的组件版本。

过程

1. 转到**管理 > 更新 > 特征码更新**
 2. 验证手动更新或预设更新是否已成功完成。
-

关于更新维护

下一代应用安全网关可通过两种方式帮助维护更新。它可以让您了解上次更新的时间，并提供有关未来更新的通知，同时还可以使您还原到先前的软件和组件版本。

有关详细信息，请参阅：

- [验证更新是否成功](#) 第 7-10 页
- [更新通知](#) 第 7-12 页
- [还原更新](#) 第 7-10 页

还原更新

下一代应用安全网关会检查程序目录并使用最新的特征码文件扫描入站/出站网络通信。有时，新的特征码文件可能会将未受感染的文件误检为病毒感染文件（称为“误报”）。如果需要，恢复到以前的特征码文件。

过程

1. 转到**管理 > 更新 > 特征码更新**
2. 选择要还原的组件，然后单击**还原**。

- 单击**确定**确认还原。

此时会显示一个进度条，用于指示还原进度，然后会显示一个消息窗口，用于显示还原的结果。还原后，可以在“特征码信息”小组件中的“实时监控”窗口上找到当前版本。



注意

缺省情况下，不会显示**特征码信息**小组件。有关添加小组件的详细信息，请参阅：[添加新小组件 第 5-7 页](#)。

预设更新

下一代应用安全网关可预设更新可更新的程序组件 [第 7-2 页](#) 中列出的任何产品组件。



注意

不能为系统更新预设更新。

预设特征码更新

过程

- 转到**管理 > 更新 > 特征码更新**。
- 对于每种组件类型，选择更新时间间隔。

选项	说明
每小时	预设更新在每小时的 00、15、30 或 45 分运行一次。
每日	预设更新在每天的特定时间运行一次。（缺省）

选项	说明
每周	预设更新在每周的特定日期和时间运行一次。

3. 单击**应用**。



注意

使用下一代应用安全网关 Web 控制台中的**实时监控 > 特征码信息**可验证特征码文件的当前版本。如果网络配置包含缓存服务器，则趋势科技建议在更新特征码文件之后清空缓存并重新启动缓存服务器，以强制扫描所有 URL 请求，确保获得更好的网络防护。有关如何清空缓存和重新启动该服务器的信息，请参阅缓存服务器文档。

更新通知

下一代应用安全网关可以发出通知，主动通知您有关特征码或引擎更新状态的信息。有关配置与更新相关的通知的更多信息，请参阅[配置预设更新通知](#) 第 6-22 页。

配置预设更新通知

过程

1. 转到**管理 > 通知**。
2. 单击**预设更新**。
3. 选中**启用**复选框以启用通知。
4. 选中以下一项或两项的相应复选框，以指定发送通知电子邮件的时间：
 - 系统更新成功时发送通知
 - 系统更新失败时发送通知

5. 指定发送通知的电子邮件地址和接收通知的电子邮件地址。
多个地址之间使用半角逗号隔开。
 6. 单击**应用**。
-

第 8 章

产品维护和使用授权

趋势科技软件的使用授权通常只包括自购买之日起为期一 (1) 年的产品更新、病毒码文件更新以及基础技术支持（“维护”）的权利。第一年之后，必须每年以趋势科技当时的维护费用续订维护。本章介绍如何管理维护协议和产品使用授权。

主题包括：

- [维护协议 第 8-2 页](#)
- [产品使用授权 第 8-3 页](#)

维护协议

“维护协议”是贵组织与趋势科技之间的合同，其中包括在支付相关费用后获得技术支持和产品更新权利的相关规定。在购买趋势科技产品时，产品随附的《许可协议》规定了该产品“维护协议”的条款。

趋势科技软件的使用授权通常只包括自购买之日起为期一 (1) 年的产品更新、病毒码文件更新以及基础技术支持（“维护”）的权利。第一年之后，必须每年以趋势科技当时的维护费用续订维护。

维护协议到期后，虽然仍可进行扫描，但将无法更新产品，即使采用手动方式也不行。并且也无权从趋势科技获得技术支持。

通常在维护协议到期前九十 (90) 天，将提示您产品即将到期。可通过从您的经销商、趋势科技销售代表或在以下趋势科技联机注册 URL 上购买续订维护来续订“维护协议”：

<https://olr.trendmicro.com/registration>

续订维护协议

趋势科技或授权经销商为所有注册用户提供为期一 (1) 年的技术支持、病毒码下载和程序更新服务，在此之后必须购买续订维护。

维护协议到期后，仍然能够扫描，但病毒码与程序更新将停止。为避免发生这种情况，请尽快续订“维护协议”。

过程

1. 要续订维护协议，请执行以下操作之一：

- 要购买续订维护，请联系您购买产品的同一家供应商。维护协议（用于将防护再延长一年）将通过邮件发送给贵公司注册资料中所列的主要公司联系人。
- 要查看或修改贵公司的注册资料，请登录以下趋势科技在线注册 Web 站点上的帐户：<https://olr.trendmicro.com/registration/apac/zh-cn/>

- 要查看注册资料，请指定在首次向趋势科技注册产品（作为新客户）时创建的登录 ID 和密码，然后单击**登录**。
-

产品使用授权

通过产品使用授权功能，组织可以注册下一代应用安全网关并为其授予使用许可。完全激活下一代应用安全网关需要两个步骤。首先，向趋势科技注册下一代应用安全网关。注册后，将提供一个有效的下一代应用安全网关激活码以授予产品许可。

趋势科技软件的使用授权通常只包括自购买之日起为期一 (1) 年的产品更新、特征码文件更新以及基础技术支持（“维护”）的权利。

要激活下一代应用安全网关，请在产品注册过程中获取注册码。通过该注册码，您可以获得一个激活码。稍后使用下一代应用安全网关 Web 控制台激活下一代应用安全网关。

使用授权过期警告

通常在“维护协议”到期前九十 (90) 天，开始向您发送电子邮件通知，提醒产品即将到期。通过从经销商、趋势科技销售代表或在以下趋势科技联机注册网站上购买续订维护来更新“维护协议”：<https://olr.trendmicro.com/registration>

获取注册码

可从以下位置获取注册码：

- 趋势科技企业解决方案 DVD
- 使用授权证书（在购买产品后即可获取）

注册并激活下一代应用安全网关将授予以下权利：

- 更新下一代应用安全网关特征码文件与扫描引擎

- 技术支持
- 轻松查看使用授权过期更新、注册和使用授权信息以及续订提醒
- 轻松续订使用授权并更新客户安全配置

注册码包含 18 个字符，格式如下：

XX-XXXX-XXXX-XXXX-XXXX

注册下一代应用安全网关

过程

1. 在**管理 > 使用授权**中单击产品的“趋势科技产品注册服务器”链接。
2. 单击**激活使用授权**链接。
3. 在“激活向导”窗口中，单击**在线注册**链接。
 - **新用户**：单击**未注册**下的**继续**按钮，然后创建一个新帐户并单击**提交**。
 - **老用户**：指定您的登录 ID 和密码。
4. 在**我的产品**窗口中，单击**添加产品**并指定注册码。
5. 要编辑贵公司的资料，请单击**查看/编辑公司资料**。
下一窗口将显示激活码。
6. 要在注册的电子邮件地址中收到激活码的副本，请单击**立即发送**。



注意

有关维护续订的信息，请联系趋势科技的销售代表或经销商。在**管理 > 使用授权**中单击**检查状态**以在“产品使用授权”窗口上针对维护过期日期进行手动更新。

获取激活码

完全版到期后，下一代应用安全网关安全更新将被禁用；评测期到期后，安全更新与扫描功能都将被禁用。使用**产品使用授权**窗口在线获取激活码、查看续订指导信息并检查产品的状态。

要激活下一代应用安全网关，请执行以下操作之一来获取激活码：

- 会在从趋势科技 Web 站点下载下一代应用安全网关后自动接收到一个评估激活码。
- 使用注册码在线获取激活码。

激活码包含 31 个字符，格式如下：

XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX

更新使用授权

过程

1. 要获取最新的使用授权，请转到**管理 > 使用授权**。
 2. 单击**检查状态**。
 3. 有关续订指导的更多信息，请参阅 https://olr.trendmicro.com/registration/apac/zh-cn/instruction_renew.aspx
-

续订维护协议

趋势科技或授权经销商为所有注册用户为为期一 (1) 年的技术支持、病毒码下载和程序更新服务，在此之后必须购买续订维护。

维护协议到期后，仍然能够扫描，但病毒码与程序更新将停止。为避免发生这种情况，请尽快续订“维护协议”。

过程

1. 要续订维护协议，请执行以下操作之一：
 - 要购买续订维护，请联系您购买产品的同一家供应商。维护协议（用于将防护再延长一年）将通过邮件发送给贵公司注册资料中所列的主要公司联系人。
 - 要查看或修改贵公司的注册资料，请登录以下趋势科技在线注册 Web 站点上的帐户：<https://olr.trendmicro.com/registration/apac/zh-cn/>
 2. 要查看注册资料，请指定在首次向趋势科技注册产品（作为新客户）时创建的登录 ID 和密码，然后单击**登录**。
-

附录 A

技术支持

本附录介绍如何在线查找解决方案、使用支持门户及联系趋势科技。

- [资源问题排查 第 A-2 页](#)
- [联系趋势科技 第 A-4 页](#)
- [将可疑内容发送给趋势科技 第 A-5 页](#)
- [其他资源 第 A-6 页](#)

资源问题排查

在联系技术支持之前，请先考虑访问以下趋势科技在线资源。

趋势团体

要同其他用户、发烧友和安全专家寻求帮助、共享经验、询问问题及讨论安全事项，请转至：

<http://www.iqushi.com/>

使用支持门户

趋势科技支持门户是全天候的在线资源，其中包括了有关常见和不常见问题的最新信息。

过程

1. 转至 <http://cn.trendmicro.com/cn/support/techsupport/index.html>。
2. 从相应的下拉列表中选择产品或服务，然后指定任何其他相关的信息。
将显示**技术支持**产品页面。
3. 使用**搜索支持**框搜索可用的解决方案。
4. 如果找不到任何解决方案，请从左侧导航单击**提交支持案例**并添加任何相关详细信息，或在以下位置提交支持案例：

<http://esupport.trendmicro.com/zh-cn/srf/cnbizmain.aspx>

趋势科技支持工程师会调查此案例并在 24 小时之内进行答复。

安全智能团体

趋势科技网络安全专家是一支安全智能精英团队，善于威胁检测和分析、云和虚拟安全以及数据加密。

转至 <http://www.trendmicro.com/us/security-intelligence/index.html> 了解以下内容：

- 趋势科技博客、Twitter、Facebook、YouTube 和其他社交媒体
- 威胁报告、学术论文和焦点文章
- 全球安全人士提供的解决方案、播客和新闻稿
- 免费工具、应用程序和小组件。

威胁百科全书

现在，大部分恶意软件由“混合性威胁”组成，即两个或更多技术结合，以绕过端点安全协议。趋势科技使用可创建定制防御策略的产品来应对这种复杂的恶意软件。威胁百科全书提供了各种混合性威胁名称和症状的全面列表，其中包括已知恶意软件、垃圾邮件、恶意 URL 和已知漏洞。

转至 <http://www.trendmicro.com/vinfo/zh-cn/virusencyclo/default.asp> 了解以下内容：

- 当前处于活动状态或未受控制的恶意软件和恶意移动代码
- 形成完整 Web 攻击历史的相关威胁信息页面
- 关于目标攻击和安全威胁的 Internet 威胁公告
- Web 攻击和在线趋势信息
- 每周恶意软件报告。

联系趋势科技

在中国，您可以通过电话或电子邮件与趋势科技销售代表取得联系。

地址	上海市淮海中路 398 号世纪巴士大厦 8 楼
销售咨询热线	800-820-8876
销售咨询邮箱	business@trendmicro.com.cn
公司网站链接	http://cn.trendmicro.com/cn/home/

- 全球支持中心：
http://cn.trendmicro.com/cn/about/contact_us/index.html
- 趋势科技产品文档：
<http://docs.trendmicro.com/zh-cn/home.aspx>

加快支持呼叫

要改进问题的解决，必须提供以下信息：

- 重现问题的步骤
- 设备或网络信息
- 计算机品牌、型号和连接到端点的任何其他硬件
- 内存量和可用的硬盘空间
- 操作系统和服务包版本
- 端点客户端版本
- 序列号或激活码
- 安装环境的详细说明

- 接收到的任何错误消息的确切文本。

将可疑内容发送给趋势科技

有多个选项可用于将可疑内容发送给趋势科技以供进一步分析。

文件信誉服务

收集系统信息并将可疑文件内容提交给趋势科技：

<http://esupport.trendmicro.com/solution/zh-CN/1095943.aspx>

记录案例编号以供跟踪。

电子邮件信誉服务

查询特定 IP 地址的信誉，并指定要列入全球白名单的邮件传输代理：

<https://ers.trendmicro.com/>

Web 信誉服务

查询怀疑为钓鱼网站或其他所谓的“恶意站点”（Internet 威胁的蓄意来源，例如间谍软件和恶意软件）的 URL 的安全评估和内容类型：

<http://global.sitesafety.trendmicro.com/>

如果分配的评估不正确，请向趋势科技发送重新分类请求。

其他资源

除解决方案和支持外，我们还在线提供了许多其他有用的资源以供您了解最新信息、知晓创新举措并掌握最新的安全趋势。

TrendEdge

查找关于趋势科技产品和服务不支持的创新技术、工具和最佳实践的信息。TrendEdge 数据库包含涵盖面向趋势科技合作伙伴、员工和其他相关方的各种主题的大量文档。

有关添加到 TrendEdge 中的最新信息，请访问：

<http://trendedge.trendmicro.com/>

已知问题

已知问题是可能临时需要变通方法的产品或软件中的功能。已知问题通常记录在自述文档的第 7 部分。您也可以在趋势科技下载专区找到趋势科技产品的自述文件以及最新的产品手册副本：

<http://downloadcenter.trendmicro.com/?regs=CH>

可以在技术支持知识库中找到已知问题：

<http://cn.trendmicro.com/cn/support/techsupport/index.html>

趋势科技建议您时时查看自述文件，来了解可能会影响安装或性能的已知问题以及特定版本中的新功能的描述、系统要求和其他技巧等信息。

TrendLabs

TrendLabsSM 是一个全球性的研究、开发和操作中心网络，致力于全天候威胁监控、攻击防御和及时无缝的解决方案交付。作为趋势科技服务基础架构的主

干，TrendLabs 由上百个工程师及有资历支持人员的团队组成，提供广泛的产品和技术支持服务。

TrendLabs 监控全球范围内的威胁情况以提供有效的安全措施，旨在检测、抢占和消除攻击。每天这些努力成果的最高点都通过频繁的病毒码文件更新及扫描引擎改进与客户共享。

有关 TrendLabs 的详细信息，请访问：

<http://cloudsecurity.trendmicro.com/us/technology-innovation/experts/index.html#trendlabs>

附录 B

日志详细信息

本附录提供了有关下一代应用安全网关日志数据内容的详细信息。

本附录介绍以下内容：

- [策略强制日志 第 B-2 页](#)
- [应用程序带宽日志 第 B-3 页](#)
- [网络安全日志 第 B-4 页](#)
- [Internet 访问日志 第 B-6 页](#)
- [VPN 日志 第 B-7 页](#)
- [系统事件日志 第 B-8 页](#)
- [审计日志 第 B-10 页](#)

策略强制日志

日志项	描述	示例
时间	记录的日期和时间	2014-02-11 22:51:00
用户名	用户帐户（如果下一代应用安全网关配置为 LDAP 或本地用户认证）。否则，将为客户端 IP 地址	Lily Jerry
消息类型	防火墙/URL 过滤/黑名单/应用程序阻止	应用程序阻止日志
组名称	认证的用户的组名称（缺省为空）	英语俱乐部
URL	由客户端访问的 URL（如果适用）	u034024.778669.com/
客户端 IP	来源	192.168.1.101
服务器 IP	目标	192.168.1.119 10.64.1.55
域	由客户端访问的域（如果适用）	www.google.com
URL 类别	由下一代应用安全网关识别的 URL 类别名称	购物 间谍软件
应用程序名称	由下一代应用安全网关识别的应用程序名称	DNS HTTP 新浪微博
操作	阻止/监控	阻止
Web 信誉服务分数	由 Web 信誉服务查询的 URL 分数（如果适用）。范围介于 0 和 100 之间。值越高，信誉越好。	49
源端口	端口号	42074 39199

日志项	描述	示例
目标端口	端口号	53 80
入侵防御规则	入侵防御规则名称（如果由入侵防御扫描触发）	--
ERS 类别	1 = 被 ERS 阻止；0 = 其他情况	0
邮件发件人	邮件通信的邮件发件人。缺省为空。	--
邮件收件人	邮件通信的邮件收件人。缺省为空。	--
邮件主题	邮件通信的邮件主题。缺省为空。	--
传输协议	TCP/UDP/ICMP/ICMPv6	TCP
应用程序属性名称	粒度应用程序名称	新浪微博发布消息
策略名称	网络通信控制的安全策略名称	缺省安全配置 已知用户

应用程序带宽日志

日志项	描述	示例
时间	记录的日期和时间	2014-02-11 22:51:00
用户名	用户帐户（如果下一代应用安全网关配置为 LDAP 或本地用户认证）。否则，将为客户端 IP 地址	Lily Jerry
应用程序名称	由下一代应用安全网关识别的应用程序名称	DNS HTTP 新浪微博
客户端 IP	来源	192.168.1.101

日志项	描述	示例
策略名称	网络通信控制的安全策略名称	缺省安全配置 已知用户
进字节	进站字节	552
出字节	出站字节	910

网络安全日志

由“消息类型”识别的 11 种安全日志对下一代应用安全网关网络安全日志进行分类。下表介绍了安全日志中各项的详细信息。

日志项	描述	示例
时间	记录的日期和时间	2014-02-11 22:51:00
消息类型	防恶意软件/反垃圾邮件/防 DoS/WRS/IPS/ Botnet/僵尸网络/阻止的文件扩展名/HTTP 证书错误/客户端证书错误	防恶意软件
用户名	用户帐户（如果下一代应用安全网关配置为 LDAP 或本地用户认证）。否则，将为客户端 IP 地址	Lily Jerry
组名称	认证的用户的组名称（缺省为空）	英语俱乐部
URL	由客户端访问的 URL（如果适用）	u034024.778669.com/
客户端 IP	来源	192.168.1.101
服务器 IP	目标	192.168.1.119 10.64.1.55
域	由客户端访问的域（如果适用）	www.google.com
URL 类别	由下一代应用安全网关识别的 URL 类别名称	购物 间谍软件

日志项	描述	示例
文件名	由客户端下载的文件名（如果适用）	eicar.zip
恶意软件名称	被防恶意软件扫描阻止的病毒名称	Eicar
操作	阻止/监控	阻止
策略名称	网络通信控制的安全策略名称	缺省安全配置 已知用户
Web 信誉服务分数	由 Web 信誉服务查询的 URL 分数（如果适用）。范围介于 0 和 100 之间。值越高，信誉越好。	49
源端口	端口号	42074 39199
目标端口	端口号	53 80
入侵防御规则	入侵防御规则名称（如果由入侵防御扫描触发）	--
ERS 类别	1 = 被 ERS 阻止；0 = 其他情况	0
邮件发件人	邮件通信的邮件发件人。缺省为空。	--
邮件收件人	邮件通信的邮件收件人。缺省为空。	--
邮件主题	邮件通信的邮件主题。缺省为空。	--
传输协议	TCP/UDP/ICMP/ICMPv6	TCP
应用程序名称	由下一代应用安全网关识别的应用程序名称	DNS HTTP 新浪微博
应用程序属性名称	粒度应用程序名称	新浪微博发布消息

Internet 访问日志

下一代应用安全网关会记录遍历网络的每个会话。通过 Internet 访问日志，可以更清楚地了解网络通信并获得有关网络通信的详细信息。下表包含详细信息。

日志项	描述	示例
时间	记录的日期和时间	2014-02-11 22:51:00
用户名	用户帐户（如果下一代应用安全网关配置为 LDAP 或本地用户认证）。否则，将为客户端 IP 地址	Lily Jerry
消息类型	访问日志	访问日志
URL	由客户端访问的 URL（如果适用）	u034024.778669.com/
客户端 IP	来源	192.168.1.101
服务器 IP	目标	192.168.1.119 10.64.1.55
域	由客户端访问的域（如果适用）	www.google.com
文件名	由客户端下载的文件名（如果适用）	eicar.zip
应用程序名称	由下一代应用安全网关识别的应用程序名称	DNS HTTP 新浪微博
应用程序属性名称	粒度应用程序名称	新浪微博发布消息
URL 类别	由下一代应用安全网关识别的 URL 类别名称	购物 间谍软件
会话开始时间	网络通信的开始时间	2014-02-11 15:50:53
会话结束时间	网络通信的结束时间	2014-02-11 15:53:28

日志项	描述	示例
源接口	源网络接口	eth0
目标接口	目标网络接口	eth1
源端口	端口号	42074 39199
目标端口	端口号	53 80
传输协议	TCP/UDP/ICMP/ICMPv6	TCP
策略名称	网络通信控制的安全策略名称	缺省安全配置 已知用户
入侵防御规则	入侵防御规则名称（如果由入侵防御扫描触发）	--
恶意软件名称	被防恶意软件扫描阻止的病毒名称	Eicar
Web 信誉服务分数	由 Web 信誉服务查询的 URL 分数（如果适用）。范围介于 0 和 100 之间。值越高，信誉越好。	49
ERS 类别	1 = 被 ERS 阻止；0 = 其他情况	0
邮件发件人	邮件通信的邮件发件人。缺省为空。	--
邮件收件人	邮件通信的邮件收件人。缺省为空。	--
邮件主题	邮件通信的邮件主题。缺省为空。	--
操作	缺省为空。如果已指定，允许/阻止/监控	允许

VPN 日志

建立或断开 VPN 连接后，下一代应用安全网关将生成 VPN 日志，其中包括有关时间、用户名和 IP 地址的详细信息。PPTP VPN 和 SSL VPN 都会生成 VPN 日志。

日志项	描述
日志时间	日志日期和时间
类型	SSL VPN 或 PPTP VPN
IP 地址	VPN 服务 IP 地址
用户	VPN 用户帐户
事件	有以下四种类型的事件： <ul style="list-style-type: none"> • VPN 服务启动 • VPN 服务关闭 • VPN 客户端连接（还会显示客户端 IP 地址。） • VPN 客户端断开连接（还会显示已传输/已接收的字节数。）

表 B-1. VPN 日志示例

日志时间	类型	IP 地址	用户	事件
2013-01-25 13:43:59	SSL VPN	222.94.7.186	vpn01	SSL VPN client(192.168.150.6) disconnect,bytes_received: 684436,bytes_sent:31375
2013-01-25 13:43:59	SSL VPN	192.168.150.1	tun0	SSL VPN 服务关闭
2013-01-25 13:40:15	SSL VPN	222.94.7.186	vpn01	SSL VPN 客户端 (192.168.150.6) 连接
2013-01-25 09:55:36	SSL VPN	192.168.150.1	tun0	SSL VPN 服务启动

系统事件日志

发生重要事件时，下一代应用安全网关将生成事件。事件可能与系统资源太低或安全更新不成功相关。

日志项	描述
日志时间	日志日期和时间
类型/服务	与此事件相关的下一代应用安全网关服务。主要包括以下服务： zebra、ripngd、ospf、rip、bgp、openvpn、pptp、sshd、ipsec、hostapd、dnsmasq、dhcp、pppoe、snmp、httpd、postgres、memcached、postfix、imss、imssManager、dpid、vtmservice、sysmon
描述	有以下两种类型的事件： 1. 服务已启动/已停止 2. 系统资源状态（内存、CPU、磁盘空间）

表 B-2. 系统事件日志示例：重要服务启动/停止事件

事件时间	服务	事件内容
2013-01-25 13:44:03	openvpn	服务已启动
2013-01-25 13:43:59	openvpn	服务已停止
2013-01-25 11:14:41	dpid	服务已启动
2013-01-25 11:14:40	dpid	服务已停止
2013-01-25 09:56:54	imssd	服务已启动
2013-01-25 09:56:54	imssd	服务已停止
2013-01-25 09:55:39	vtmservice	服务已启动
2013-01-26 19:51:39	OS	系统已启动
2013-01-26 19:52:49	OS	系统已停止

表 B-3. 系统事件日志示例：系统资源状态事件

事件时间	类型/服务	事件内容
2013-01-25 13:42:43	sysmon	内存使用率百分比 (91.13%) 将在 5 分钟内超过 90%。 (事件每小时仅发送一次。)
2013-01-25 12:38:29	sysmon	内存使用率百分比 (92.69%) 将在 5 分钟内超过 90%。 (事件每小时仅发送一次。)

审计日志

管理员登录下一代应用安全网关并进行更改后，将创建审计事件。审计日志还包括有关认证尝试不成功或访问权限无效的事件。

日志项	描述
日志时间	日志日期和时间
IP 地址	客户端 IP 地址
管理员用户	登录帐户名称（如果适用）。缺省为空。
描述	此事件的内容。有以下两种类型的审计日志： <ol style="list-style-type: none"> 有关访问下一代应用安全网关本身（如 AdminUI 或 SSH 登录）但认证失败或该访问无效的记录 有关下一代应用安全网关管理的记录

表 B-4. 审计日志示例：访问和认证记录

日志时间	IP 地址	管理员用户	描述
2013-01-27 21:51:03	10.64.44.133	admin	从 WebUI 登录帐户成功

日志时间	IP 地址	管理员用户	描述
2013-01-22 21:53:55	10.64.44.133	admin	使用 ssh 登录成功
2013-01-22 19:45:02	10.64.44.133	admin	从 WebUI 登录帐户失败：用户名或密码无效。
2013-01-22 20:51:12	localhost	admin	使用 ssh 登录成功
2013-01-22 16:25:21	localhost	admin	使用 ssh 登录成功：用户名或密码无效
2013-01-22 19:47:02	10.64.68.149	未知	丢弃的请求：未经允许尝试执行 Ping 操作。
2013-01-22 19:48:32	10.64.68.149	未知	丢弃的请求：未经允许尝试连接 HTTPS。
2013-01-22 19:49:02	10.64.68.149	未知	丢弃的请求：未经允许尝试连接 SSH。
2013-01-22 19:50:12	10.64.68.149	未知	丢弃的请求：未经允许发出 SNMP 请求。
2013-01-28 16:40:33	10.64.68.149	未知	未经允许尝试从 eth0 执行 Ping 操作
2013-01-28 16:40:06	10.64.68.149	未知	未经允许尝试从 eth0 与 ssh 连接
2013-01-28 16:39:50	10.64.68.149	未知	未经允许尝试从 eth0 与 HTTPS 连接
2013-01-28 16:39:50	10.64.68.149	未知	未经允许尝试使用 SNMP 从 eth0 进行访问

表 B-5. 审计日志示例：管理设置日志

日志时间	IP 地址	管理员用户	描述
2013-01-25 01:28:13	10.64.44.133	admin	从 WebUI 进行 NormalUpdate AuSetting 成功。

日志时间	IP 地址	管理员用户	描述
2013-01-23 00:34:55	10.64.44.133	admin	从 WebUI 进行 ForceUpdate AuSetting 成功。
2013-01-22 23:36:00	10.64.44.133	admin	从 WebUI 激活 PrSetting 成功。
2013-01-22 22:13:31	10.64.44.133	admin	从 WebUI 设置 LogSetting 成功。
2013-01-22 22:03:15	10.64.44.133	admin	从 WebUI 应用策略成功。
2013-01-22 22:02:37	10.64.44.133	admin	从 WebUI 设置 SecurityPolicy 测试成功。
2013-01-22 21:56:57	10.64.44.133	admin	从 WebUI 设置网桥 br0 成功。
2013-01-22 21:55:03	10.64.44.133	admin	从 WebUI 应用策略成功。
2013-01-22 19:45:02	10.64.44.133	admin	从 WebUI 应用策略成功。
2013-01-22 19:43:40	10.64.44.133	admin	从 WebUI 设置 SecurityPolicy 测试成功。
2013-01-22 19:43:24	10.64.44.133	admin	从 WebUI 添加 SecurityPolicy 测试成功。

审计日志对象

下表提供了审计日志中**对象**列的描述和菜单路径。

对象名称	描述	菜单路径
SecurityPolicy	安全规则	策略 规则
AddressObj	地址对象	策略 > 对象 地址

对象名称	描述	菜单路径
ZoneObj	区域对象	策略 > 对象 > 区域
ServiceObj	服务对象	策略 > 对象 > 服务
AppldObj	应用程序对象	策略 > 对象 > 应用程序
UrlFilteringObj	URL 类别对象	策略 > 对象 > URL 类别
SchedulerObj	计划程序对象	策略 > 对象 > 时间表
ProfileObj	安全配置对象	策略 > 对象 > 处理措施安全配置
IpsProfile	入侵防御安全配置	策略 > 安全设置 > 入侵防御
AntiMalwareSetting	防恶意软件设置	策略 > 安全设置 > 防恶意软件
ErsObj	电子邮件信誉服务设置	策略 > 安全设置 > 反垃圾邮件
MailSecurity	邮件安全设置	策略 > 安全设置 > 反垃圾邮件
WrsObj	Web 信誉服务设置	策略 > 安全设置 > Web 信誉服务
HttpsCAAuth	HTTPS 证书设置	策略 > HTTPS 检查 > 数字证书
HttpsInspectionSettings	HTTPS 检查设置	策略 > HTTPS 检查 > 常规设置
UrlWhiteBlackList	URL 黑/白名单设置	策略 > 黑/白名单
AntiDosSetting	防 DoS 设置	策略 > 防 DoS
IdPolicy	用户识别策略	策略 > 认证 > 端点识别
EndUserNotifSetting	终端用户通知设置	策略 > 用户通知
NetworkInterface	网络接口设置	网络 > 接口
VlanInterface	VLAN 接口设置	网络 > 接口
PppoeSetting	PPPoE 设置	网络 > 接口

对象名称	描述	菜单路径
WorkModeObj	系统工作模式设置	网络 > 部署
InternalAddress	内部地址设置	网络 > 部署 > 内部地址
网桥	网桥设置	网络 > 网桥
StaticRoute	静态路由设置	网络 > 路由 > 静态路由
StaticRoute6	IPv6 的静态路由设置	网络 > 路由 > 静态路由
RipSetting	RIP 设置	网络 > 路由 > RIP
RipngSetting	RIPng 设置	网络 > 路由 > RIP
OSPF	OSPF 设置	网络 > 路由 > OSPF
Ospf6d	IPv6 的 OSPF 设置	网络 > 路由 > OSPF
RouteTable	路由表	网络 > 路由 > 路由表
RouteTable6	IPv6 的路由表	网络 > 路由 > 路由表
NatRule	NAT 规则设置	网络 > NAT
DnsForward	DNS 转发设置	网络 > 服务 > DNS 转发
DhcpServer	DHCP 服务器设置	网络 > 服务 > DHCP
Dhcp6s	IPv6 的 DHCP 服务器设置	网络 服务 DHCP
DDNSConfig	动态 DNS 设置	网络 > 服务 > 动态 DNS
PptpSetting	PPTP VPN 设置	网络 > 用户 VPN > PPTP VPN
OpenVpnSetting	SSL VPN 设置	网络 > 用户 VPN > SSL VPN
MobileSetting	移动 VPN 设置	网络 > 用户 VPN > 移动 VPN
IpssecSetting	站到站 VPN 设置	网络 > 站到站 VPN
LogSetting	日志设置	分析和报告 > 日志设置

对象名称	描述	菜单路径
MailQrtMgmt	邮件隔离管理设置	管理 > 邮件隔离 > 查询
QareaPurge	隔离邮件清除设置	分析和报告 > 邮件隔离 > 设置
ReportTemplate	报告模板设置	分析和报告 > 报告
SystemSetting	系统设置	管理 > 系统设置
ProxySetting	代理服务器设置	管理 > 系统设置 > 代理服务器设置
证书	Web 控制台证书设置	管理 > 系统设置 > 控制台设置
ExperienceImprovement	体验改善设置	管理 > 系统设置 > 体验改善
ManagementService	管理服务	管理 > 管理
模板	通知事件模板设置	管理 > 通知 > 通知事件
SMTP	SMTP 设置	管理 > 通知 > SMTP 设置
用户 ID	LDAP 设置	管理 > LDAP 设置
用户	管理帐户设置	管理 > 设备管理 > 管理帐户
终端用户	终端用户管理	管理 > 终端用户管理
PrSetting	产品注册设置	管理 > 使用授权
patch	系统 Patch 更新设置	管理 > 更新 > 系统更新
AuSetting	动态更新设置	管理 > 更新 > 特征码更新
SystemMaintenance	系统维护	管理 > 维护
配置	系统配置设置	管理 > 维护 > 备份/恢复
PacketCapture	数据包捕获	管理 > 诊断 > 数据包捕获
TrafficTracing	通信跟踪	管理 > 诊断 > 通信跟踪

对象名称	描述	菜单路径
CDT	诊断文件生成	管理 > 诊断 > 诊断文件
ConnectionTestSetting	网络连接测试设置	实时监控 > 系统信息 > 网络信息
策略	系统策略	N/A
帐户	管理帐户处理措施	N/A
ErrorLang	Web 控制台语言设置	N/A

索引

A

ActiveUpdate, 7-5

C

CA, 4-48, 4-49

D

DCHP 服务, 3-47

DDNS

 Dyn DNS, 3-48

 FreeDNS, 3-48

 IPv6, 3-49

 概述, 3-48

 配置客户端, 3-49

 状态, 3-50

 状态消息, 3-50

DDNS 客户端, 3-49

DHCP

 查看服务, 3-46

 查看设置, 3-46

 高级设置, 3-46

 接口配置, 3-46

 静态映射, 3-46

 修改服务, 3-47

 修改设置, 3-47

 租用时间, 3-46

DNS, 6-34

 配置转发, 3-45

 转发配置, 3-45

 转发设置, 3-45

DNS 服务器, 6-34

DNS 转发配置, 3-44

DoS 攻击

 ICMP/Ping flood, 4-60

 TCP SYN flood, 4-60

 UDP flood, 4-60

Dyn DNS, 3-48

F

FreeDNS, 3-48

H

HTTPS 检查

 关于, 4-46

 设置, 4-46

 添加例外, 4-46

I

ICMP, 4-60

IKE, 3-96, 3-99

IKE 调试, 3-101

IntelliTrap, 7-3

Internet 密钥交换, 3-96

IPsec, 3-102

 NAT 配置示例, 3-104

 RSA 密钥, 3-101

 分支配置示例, 3-102

 高级配置, 3-101

 连接, 3-96

 生成 RSA 密钥, 3-102

 添加连接, 3-97

 问题排查, 3-102

 状态, 3-102

IPv4 或 IPv6, 3-51

IP 地址池

 SSL VPN, 3-57

L

LDAP, 4-65

 高级认证, 6-13

- 基本认证, 6-12
- 集成, 6-11
- 配置, 基本和高级, 6-12
- 认证方法, 6-11
- 设置, 全局, 6-9, 6-10
- 用户识别方法, 4-64
- LDAP 用户识别
 - 关于, 6-11
- N**
- NAT, 3-40, 4-63
 - IPsec 配置, 3-104
 - 更改规则优先级, 3-43
 - 规则, 3-40
 - 删除规则, 3-44
 - 添加规则, 3-41, 3-42
 - 修改规则, 3-43
 - 站到站 VPN 配置, 3-104
- O**
- OSPF, 3-32
 - 接口, 3-36
 - 路由器 ID, 3-33
 - 启用 OSPF 分发路由, 3-33
 - 启用全局设置, 3-33
 - 区域, 3-34
 - 全局, 3-33
 - 删除区域, 3-36
 - 添加区域, 3-35
 - 修改接口, 3-37
 - 修改区域, 3-35
 - 重新分发, 3-38
 - 重新分发链接状态公布, 3-38
- P**
- ping
 - 启用, 6-6

- PPTP VPN, 3-53
 - 查看日志, 3-54
 - 查看在线用户, 3-54
 - 错误消息, 3-55
 - 概述, 3-52
 - 高级设置, 3-53
 - 加密级别, 3-53
 - 启用, 3-52
 - 问题排查, 3-55

- R**
- RIP, 3-27
 - 高级全局设置, 3-29
 - 配置全局设置, 3-28
 - 启用全局设置, 3-28
 - 全局设置, 3-28
 - 删除 RIP 网络, 3-31
 - 网络设置, 3-30
 - 重新分发, 3-31
- RIP:
 - 添加网络, 3-30
- RSA 密钥, 3-101
 - 生成, 3-102

- S**
- shell
 - 关于, 6-9
- SMTP
 - 通知, 6-23
- SNMP
 - 管理, 6-6
 - 启用, 6-6
- SolutionBank. *请参阅* 知识库
- SSH
 - 启用, 6-6
- SSL VPN
 - IP 地址池, 3-57

- 安装客户端, 3-60
 - 查看日志, 3-60
 - 查看在线用户, 3-59
 - 服务器设置, 3-56
 - 概述, 3-55
 - 配置本地网络, 3-57
 - 配置高级设置, 3-58
 - 启用, 3-56
 - 问题排查, 3-69
- SYN, 4-60
- T**
- TCP, 4-60
 - TrendEdge, x
 - TrendLabs, A-6
- U**
- URL
- 技术支持, A-6
 - 知识库, x, A-6
 - 注册, 8-2, 8-5
 - 自述文档, A-6
- URL 过滤, 4-58
 - 通知, 4-68
- URL 过滤通知, 4-68
 - URL 数据库, 7-4
- V**
- VLAN, 3-4
 - 添加子接口, 3-5
- VPN, 3-51, 3-71
 - iOS 和 Android, 3-71
 - SSL, 3-55
 - 用户, 3-51
 - 站到站, 3-96
- VPN 日志
 - 查询, 5-44
 - 关于, 5-41
- VPN 隧道
 - IPsec, 3-96
- VPN 站到站
 - 添加策略, 3-99
- W**
- Web 命令行
 - 关于, 6-9
- Web 信誉, 7-4
 - URL 数据库, 7-4
 - 安全配置, 4-44
- Web 信誉服务
 - 安全配置, 4-44
 - 对安全配置进行配置, 4-45
 - 通知, 4-67
- Web 信誉服务保护的的设备排名
 - 小组件, 5-25
- Web 信誉服务通知, 4-67
- A**
- 安全配置, 4-35, 4-37, 4-40
 - Web 信誉, 4-44
 - Web 信誉服务, 4-44
 - 配置 Web 信誉服务, 4-45
- 安全设置
 - 反垃圾邮件, 4-39
 - 关于, 4-33
- 安全事件摘要
 - 小组件, 5-22
- 安全套接层 VPN, 3-55
 - 安全信息汇总
 - 配置警报, 6-20
- 安全状态
 - 小组件, 5-21
- 安装:
 - SSL VPN 客户端, 3-60

按需 VPN, 3-71

B

白名单

URL, 4-58

报告, 5-30

参数, 5-36

定制, 5-36

关于, 5-34

类型, 5-35

模板, 5-36

设置, 5-36

实时监控摘要, 5-8

手动, 5-35

手动, 生成, 5-35

预设, 关于, 5-36

报告类型, 5-30

备份, 6-28

系统, 6-28

本地用户, 6-14

本地用户识别

关于, 6-13

本地组, 6-17

编辑

处理措施安全配置, 4-33

时间表对象, 4-29

编辑接口, 3-2

病毒码, 7-3

病毒扫描引擎, 7-3

部署

监控模式, 3-14, 3-16

接入模式, 3-10, 3-16

静态路由, 3-21

配置, 3-16

设置, 3-9

网桥, 3-17

部署模式

监控模式, 3-9, 3-14

路由器模式, 3-9, 3-12

网桥模式, 3-9, 3-10

部署指南, x

C

参数, 3-6

报告, 5-36

地址对象, 3-6

服务对象, 4-12

日志设置, 全局, 5-39

网页认证, 4-66

策略, 4-67

策略如何工作, 4-1, 4-2

带宽控制, 4-52

地址, 3-6, 4-10

地址对象, 3-6, 4-10

对象, 4-9

规则页面, 4-2, 4-52

启用规则, 4-9, 4-57

添加 VPN 站到站, 3-99

添加带宽规则, 4-52

添加规则, 4-3

修改入侵防御, 4-36

用户 ID, 添加, 4-64

用户识别, 4-63

策略对象, 4-9

查看

DCHP 服务, 3-46

DHCP 设置, 3-46

PPTP VPN 日志, 3-54

PPTP VPN 在线用户, 3-54

SSL VPN 日志, 3-60

SSL VPN 在线用户, 3-59

处理措施安全配置, 4-30, 4-31

地址对象, 3-8

服务对象, 4-13

- 路由表, 3-39
- 区域对象, 4-11
- 移动 VPN 在线用户, 3-73
- 应用程序对象, 4-15
- 用户列表, 6-7
- 查询
 - VPN 日志, 5-44
 - 审计日志, 5-43
 - 系统事件日志, 5-43
- 查询日志, 5-42
- 产品
 - 版本, 6-33
 - 管理, 6-1
 - 管理, 关于, 6-5
 - 使用授权, 6-33
- 产品 Patch
 - 备份当前配置, 6-28
 - 恢复先前的配置, 6-28
 - 下载 Patch, 7-9
 - 应用 Patch, 7-8
- 产品概述, 1-2
- 产品使用授权, 6-24, 8-3
- 常规系统设置, 6-2
- 程序组件
 - 更新, 7-2
- 处理措施:
 - 安全, 4-30
- 处理措施安全配置, 4-30
 - 编辑, 4-33
 - 查看, 4-30, 4-31
 - 删除, 4-33
 - 添加, 4-32
- 传输控制协议, 4-60
- 错误消息
 - PPTP VPN, 3-55
 - SSL VPN, 3-69
- D**
- 带宽控制
 - 策略设置, 4-52
 - 网络设置, 3-4
 - 小组件, 5-18
- 带宽摘要
 - 小组件, 5-18
- 代理服务器, 6-4
- 代理服务器设置, 6-4, 7-6
 - 配置, 6-4
- 代码
 - 路由表, 3-39
- 到期
 - 警告, 8-3
 - 使用授权, 8-3
- 地址对象, 3-6, 4-10
 - 查看, 3-8
 - 配置, 3-8
 - 删除, 3-8
- 点对点隧道 VPN, 3-52
 - 概述, 3-52
- 电子邮件信誉
 - 数据库, 7-5
- 电子邮件信誉服务, 4-39
- 电子邮件信誉技术, 4-39
- 调试
 - IPsec, 3-101
- 调试模式
 - 启用 PPTP VPN, 3-53
- 定制
 - 报告, 5-36
 - 小组件, 5-8
- 动态域名系统服务, 3-48
- 动态源转换, 3-40
- 对端断线检测, 3-101
- 对象

- 策略, 4-9
- 地址, 3-6, 4-10
- 地址参数, 3-6
- 服务对象, 4-12
- 区域, 4-10
- 时间表对象, 4-27
- 应用程序对象, 4-14

E

- 恶意软件
 - 通知, 4-69
- 恶意软件通知, 4-69

F

- 反垃圾邮件
 - 安全设置, 4-39
 - 反垃圾邮件安全配置, 4-40
- 反垃圾邮件安全配置
 - 禁用, 4-40
 - 配置, 4-40
 - 内容设置, 4-43
 - 启用, 4-40
 - 修改, 4-42
- 反垃圾邮件保护的设备排名
 - 小组件, 5-29
- 反垃圾邮件协议特征码文件, 7-4
- 防 DoS
 - flood 保护
 - 配置, 4-60
 - 关于, 4-60
 - 例外
 - 删除, 4-62
 - 添加, 4-61
 - 修改, 4-62
- 防病毒保护的设备排名
 - 小组件, 5-26
- 防病毒特征码文件, 7-2

- 防恶意软件, 7-2
 - 防恶意软件安全配置, 4-37
 - 文件扩展名, 4-38
- 防恶意软件特征码文件, 7-2
- 防恶意软件协议特征码文件
 - 特征码文件
 - 防恶意软件协议, 7-2, 7-3
- 封装安全有效载荷
 - ESP, 3-96
- 服务, 3-44
 - DNS 转发配置, 3-44
 - DNS 转发设置, 3-45
 - 管理, 6-5
 - 管理, 启用, 6-5
- 服务对象, 4-12
 - 参数, 4-12
 - 查看, 4-13
 - 删除, 4-14
 - 添加, 4-13
- 服务器证书失败
 - 通知, 4-73
- 服务器证书失败通知, 4-73

G

- 概述
 - DDNS, 3-48
 - DDNS 状态, 3-50
 - DNS 接口配置, 3-46
 - NAT, 3-40
 - OSPF 接口, 3-36
 - SSL VPN, 3-55
 - VLAN, 3-4
 - VPN, 3-51
 - 动态路由管理, 3-27
 - 动态域名系统服务, 3-48
 - 服务, 3-44
 - 高级 IPsec 配置, 3-101

- 接口, 3-2
- 开放最短路径优先协议 (OSPF), 3-32
- 路由表, 3-38
- 路由信息协议 (RIP), 3-27
- 全局 OSPF, 3-33
- 网络通信, 3-2
- 用户的远程访问, 6-9
- 用户管理, 6-9
- 远程访问, 3-51
- 站到站 VPN, 3-96
- 重新分发 OSPF 路由, 3-38
- 重新分发 RIP 设置, 3-31
- 高级
 - IPsec 配置, 3-101
- 高级设置
 - PPoP VPN, 3-53
 - SSL VPN, 3-58
- 更改
 - NAT 规则, 3-43
- 更改网桥设置, 3-18
- 更新, 7-3
 - Web 控制台, 7-6
 - 程序组件, 7-2
 - 代理服务器设置, 7-6
 - 反垃圾邮件协议, 7-4
 - 防病毒, 7-2
 - 防恶意软件, 7-2
 - 防恶意软件协议, 7-2, 7-3
 - 还原, 7-10
 - 缓存服务器, 7-12
 - 建议, 7-6
 - 手动, 7-8
 - 通知, 7-12
 - 维护, 7-10
 - 验证是否成功, 7-10
 - 预设, 7-6, 7-11
 - 增量, 7-5
 - 组件版本, 7-5
- 更新使用授权, 8-5
- 关于
 - HTTPS 检查, 4-46
 - LDAP 用户识别, 6-11
 - 安全设置, 4-33
 - 本地用户识别, 6-13
 - 产品使用授权, 6-24, 8-3
 - 防 DoS, 4-60
 - 数字证书, 4-47
- 关于产品, 6-33
- 管理, 6-1
 - SNMP, 6-6
 - 服务, 6-5
 - 服务, 启用, 6-5
 - 概述, 6-1
 - 关于, 6-5, 6-33
 - 启用
 - 管理服务, 6-5
 - 设备
 - 帐户, 6-7
 - 时间和日期设置, 6-2
 - 系统设置, 6-2
 - 系统设置, 常规, 6-2
 - 语言设置, 6-2
 - 支持, 6-32
- 管理员
 - 帐户, 删除, 6-8
- 管理员指南, x
- 规则
 - NAT, 3-40
 - 更改 NAT 优先级, 3-43
 - 删除 NAT, 3-44
 - 添加 NA, 3-41, 3-42
 - 修改 NAT, 3-43

规则页面

策略, 4-2, 4-52

H

黑/白名单, 4-58

启用/禁用, 4-59

添加, 4-58

黑名单

URL, 4-58

通知, 4-70

黑名单通知, 4-70

还原更新, 7-10

缓存服务器, 7-12

恢复, 6-28

系统, 6-28

会话事件摘要

小组件, 5-24

会话摘要

小组件, 5-14

J

基于云的服务, 6-33

激活码, 8-5

集成

LDAP, 6-11

即时报表, 5-35

生成, 5-35

技术支持, A-1

加密

SSL, 4-46

TLS, 4-46

加密级别

PPTP VPN, 3-53

监控模式, 3-14

间谍软件, 7-3

特征码, 7-3

检测

对端断线, 3-101

简介

通知, 6-19

接口, 3-2

OSPF, 3-36, 3-37

编辑, 3-2

接口信息

小组件, 5-9

接入模式, 3-10

网桥, 3-17

警报:

通知, 6-19

警告

系统资源, 通知, 6-21

静态路由

启用, 3-22

删除, 3-23

添加, 3-21

修改, 3-23

静态映射, 3-46

拒绝服务攻击, 4-60

K

开放最短路径优先协议, 3-32

客户端

SSL VPN, 安装, 3-60

客户端证书失败

通知, 4-74

客户端证书失败通知, 4-74

控制台超时, 6-3

控制台设置, 6-3

控制台, 6-4

配置, 6-4

控制台证书, 6-3

快速入门指南, x

L

垃圾邮件检测, 4-39

联机帮助, x

连接

 IPsec, 3-96

路由

 动态路由管理, 3-27

 静态路由管理, 3-21

 设置, 3-20

路由表

 查看, 3-39

 概述, 3-38

 指示灯, 3-39

路由信息协议, 3-27

M

密码

 用户, 修改, 6-8

模板

 报告, 5-36

模式

 监控, 3-14

 接入, 3-10

 路由, 3-20

 网桥, 3-17, 3-18, 3-20

P

配置

 DDNS 客户端, 3-49

 DNS 转发, 3-44

 LDAP, 基本和高级, 6-12

 SMTP 通知, 6-23

 SSL VPN IP 地址池, 3-57

 SSL VPN 本地网络, 3-57

 SSL VPN 高级设置, 3-58

 URL 过滤通知, 4-68

 Web 信誉服务通知, 4-67

 安全信息汇总的警报, 6-20

 部署, 3-16

 代理服务器设置, 6-4

 地址对象, 3-8

 恶意软件通知, 4-69

 服务器证书失败通知, 4-73, 4-74

 黑名单通知, 4-70

 控制台设置, 6-4

 路由, 3-20

 区域对象, 4-10

 入侵防御安全通知, 4-72

 时间和日期设置, 6-3

 网桥, 3-18, 3-20

 网页认证, 4-66

 文件扩展名通知, 4-71

 系统设置, 6-3

 系统资源警告, 6-21

 应用程序控制通知, 4-69

 用户通知, 4-67

 预设更新的通知, 6-22, 7-12

配置:

 PPTP VPN 常规设置, 3-53

配置常规设置, 3-53

Q

启用

 ping, 6-6

 PPTP VPN, 3-52, 3-53

 RIP 全局设置, 3-28

 SNMP, 6-6

 SSH, 6-6

 SSL VPN, 3-56

 策略规则, 4-9, 4-57

 调试模式, 3-53

 高级 RIP 全局设置, 3-29

 规则, 4-9, 4-57

 静态路由, 3-22

区域

对象, 4-10

区域 OSPF, 3-34

区域对象, 4-10

查看, 4-11

配置, 4-10

删除, 4-11

全局日志设置, 5-39

R

认证

LDAP, 高级, 6-13

LDAP, 基本, 6-12

LDAP, 配置, 6-12

网页认证, 4-65

用户, 4-65

认证方法

LDAP, 6-11

日期

设置, 6-2

日志

VPN, 关于, 5-41

查看 PPTP VPN, 3-54

查看 SSL VPN, 3-60

查询, 5-42

查询 VPN 日志, 5-44

查询审计日志, 5-43

查询系统事件日志, 5-43

关于, 5-40, 6-25

简介, 5-40, 6-25

设置, 5-38

设置, 全局, 5-39

审计, 关于, 5-40

系统事件, 关于, 5-41

入门

摘要, 2-5

入侵防御

安全配置, 4-35

策略, 4-36

点对点, 4-35

关于, 4-34

即时消息, 4-35

类别, 4-35

类别和处理措施, 4-36

入侵防御, 4-34

入侵防御安全

通知, 4-72

入侵防御安全通知, 4-72

入侵防御保护的设备排名

小组件, 5-28

入侵防御特征码文件, 7-3

S

扫描

按文件扩展名, 4-38

删除

NAT 规则, 3-44

OSPF 区域, 3-36

处理措施安全配置, 4-33

地址对象, 3-8

服务对象, 4-14

管理帐户, 6-8

静态路由, 3-23

区域对象, 4-11

选项卡, 5-4

应用程序对象, 4-16

设备

管理, 帐户, 6-7

设备风险摘要

小组件, 5-26

设置, 6-4

DNS 转发设置, 3-45

LDAP, 全局, 6-9, 6-10

PPTP VPN 常规, 3-53

- RIP 重新分发, 3-31
- SMTP 通知, 6-23
- SSL VPN 服务器, 3-56
- 报告, 5-36
- 部署, 3-9
- 控制台, 关于, 6-3
- 日志, 5-38
- 日志, 全局, 5-39
- 网络 RIP, 3-30
- 终端用户同步, 6-10
- 深度数据包检查, 4-35
- 审计日志
 - 查询, 5-43
 - 关于, 5-40
- 生成
 - 即时报表, 5-35
- 时间
 - 设置, 6-2
- 时间表对象, 4-27
 - 编辑, 4-29
 - 添加, 4-27
 - 移除, 4-29
- 时间和日期
 - 设置, 6-2
- 实时监控
 - 小组件, 5-8
- 使用授权, 6-24, 8-3
 - 到期, 8-3
 - 更新, 8-5
 - 激活码, 8-5
 - 注册, 8-4
 - 注册码, 8-3
- 示例
 - IPsec NAT 配置, 3-104
 - IPsec 分支配置, 3-102
 - 站到站 VPN, 3-102, 3-104

- 手动更新, 7-8
- 数据包捕获, 6-29
 - 组件, 6-31
- 数字证书
 - 查看, 4-50
 - 更改状态, 4-50
 - 关于, 4-47
 - 管理, 4-49
 - 删除, 4-51
 - 新增, 4-50
 - 证书颁发机构
 - 导出, 4-48
 - 导入, 4-48

T

- 特征码文件, 7-2
 - 病毒, 7-2
 - 反垃圾邮件协议, 7-4
 - 服务器上多个, 7-2
 - 入侵防御, 7-3
 - 增量更新, 7-5
- 特征码信息, 7-5
 - 小组件, 5-13
- 体验改善
 - 加入, 6-5
- 添加
 - IPsec 连接, 3-97
 - NAT 规则, 3-41, 3-42
 - OSPF 区域, 3-35
 - VLAN 子接口, 3-5
 - VPN 站到站策略, 3-99
 - 策略规则, 4-3, 4-52
 - 处理措施安全配置, 4-32
 - 带宽规则, 4-52
 - 服务对象, 4-13
 - 规则, 4-3
 - 静态路由, 3-21

- 时间表对象, 4-27
- 选项卡, 5-3
- 应用程序对象, 4-14
- 用户 ID 策略, 4-64
- 帐户, 6-7
- 通信跟踪, 6-31
- 通信状态
 - 小组件, 5-14
- 通知
 - SMTP, 6-23
 - SMTP, 配置, 6-23
 - URL 过滤, 4-68
 - Web 信誉服务, 4-67
 - 恶意软件, 4-69
 - 更新, 7-12
 - 黑名单, 4-70
 - 简介, 6-19
 - 警报, 6-19
 - 配置安全信息汇总, 6-20
 - 入侵防御安全, 4-72
 - 停止, 6-23
 - 通知, 6-23
 - 文件扩展名, 4-71
 - 应用程序控制, 4-69
 - 用户策略, 4-67
 - 预设更新, 配置, 6-22, 7-12
 - 证书失败, 4-72
 - 服务器, 4-73
 - 客户端, 4-74
- 同步传输 (SYN), 4-60
- 团体, A-2
- W**
- 网络
 - 带宽控制, 3-4
 - 为 SSL VPN 配置, 3-57
 - 网络 RIP 设置, 3-30
 - 删除, 3-31
 - 添加, 3-30
 - 网络地址转换, 3-40
 - 网络功能, 1-8
 - NAT, 1-8
 - 服务, 1-8
 - 路由, 1-8
 - 网桥, 1-8
 - 移动虚拟专用网络, 1-9
 - 用户虚拟专用网络, 1-8
 - 站到站虚拟专用网络, 1-8
 - 网络配置
 - 接口, 1-8
 - 网络入侵防御, 4-34
 - 网络通信:路由, 3-20
 - 网络通信概述, 3-2
 - 网络信息
 - 小组件, 5-11
 - 网桥
 - 接口, 3-17
 - 设置, 3-18, 3-20
 - 网页认证, 4-63
 - 关于, 4-65
 - 配置, 4-66
 - 设置, 4-66
 - 维护, A-1
 - 备份, 6-28
 - 关闭, 6-27
 - 关于, 6-27
 - 恢复, 6-28
 - 维护
 - 重新启动, 6-27
 - 系统, 6-27
 - 维护更新, 7-10
 - 维护协议
 - 到期, 8-2

- 定义, 8-2
- 续订, 8-2, 8-5
- 文档集, x
- 文件扩展名
 - 扫描类型, 4-38
 - 通知, 4-71
- 文件扩展名通知, 4-71
- 文件扩展名验证, 4-38
- 问题排查, 3-102
 - PPTP VPN, 3-55
 - SSL VPN, 3-69
 - 数据包捕获, 6-29
 - 站到站 VPN, 3-102
 - 诊断, 6-29
- 误报, 7-10
- X**
- 系统
 - 备份, 6-28
 - 恢复, 6-28
- 系统警报
 - 通知, 6-19
- 系统设置
 - 常规, 6-2
 - 代理服务器, 6-4
 - 关于, 6-2
 - 配置, 6-3
- 系统事件日志
 - 查询, 5-43
 - 关于, 5-41
- 系统维护, 6-27
 - 关于, 6-27
- 系统信息
 - 小组件, 5-8, 5-10
- 系统资源
 - 小组件, 5-11
- 系统资源警告, 6-21
- 下一代防火墙, 1-2
- 下载
 - 产品 Patch, 7-9
- 显示
 - 用户列表, 6-7
- 小组件, 5-30
 - Web 信誉服务保护的 设备排名, 5-25
 - 安全事件摘要, 5-22
 - 安全状态, 5-21
 - 带宽控制, 5-18
 - 带宽摘要, 5-18
 - 定制, 5-6, 5-8
 - 反垃圾邮件保护的 设备排名, 5-29
 - 防病毒保护的 设备排名, 5-26
 - 关于, 5-4
 - 会话事件摘要, 5-24
 - 会话摘要, 5-14
 - 接口信息, 5-9
 - 描述, 5-8
 - 入侵防御保护的 设备排名, 5-28
 - 删除, 5-8
 - 设备风险摘要, 5-26
 - 实时监控, 5-8
 - 特征码信息, 5-13, 7-5
 - 添加, 5-7
 - 通信状态, 5-14
 - 网络信息, 5-11
 - 系统信息, 5-8, 5-10
 - 系统资源, 5-11
 - 硬件监控, 5-13
 - 用户排名, 5-15
 - 最常访问的 URL 类别, 5-21
 - 最常访问的 站点, 5-20
 - 最常使用的 应用程序, 5-17
- 修改
 - DHCP 设置, 3-47

- NAT 规则, 3-43
- OSPF 接口, 3-37
- OSPF 区域, 3-35
- 静态路由, 3-23
- 密码, 用户, 6-8
- 选项卡, 5-3
- 虚拟专用网络, 3-51
- 选项卡
 - 关于, 5-2
 - 删除, 5-4
 - 添加, 5-3
 - 修改, 5-3
 - 摘要实时监控, 5-2
- 选择
 - 文件扩展名扫描, 4-38

Y

- 验证
 - 文件扩展名, 4-38
- 验证是否更新, 7-10
- 移除
 - 时间表对象, 4-29
- 移除网桥设置, 3-20
- 移动 VPN
 - 查看在线用户, 3-73
- 已知问题
 - 自述文件, A-6
- 应用程序
 - 组对象, 4-14 - 4-16
- 应用程序对象, 4-14
 - 查看, 4-15
 - 删除, 4-16
 - 添加, 4-14
- 应用程序控制
 - 通知, 4-69
- 应用程序控制通知, 4-69
- 硬件监控

- 小组件, 5-13
- 用户
 - VPN, 3-51
 - 列表, 6-7
 - 密码, 修改, 6-8
- 用户 ID 策略
 - 添加, 4-64
- 用户管理, 6-9
 - 常规设置, 6-10
 - 远程访问, 6-9
- 用户排名
 - 小组件, 5-15
- 用户认证, 4-65
- 用户识别
 - LDAP, 6-11
 - LDAP, 高级, 6-13
 - LDAP, 基本, 6-12
 - 本地, 6-13
 - 策略, 4-63
 - 方法, LDAP, 4-64
- 用户数据报协议, 4-60
- 用户通知, 4-67
- 语言更改, 6-2
- 预设报告, 5-36
- 预设更新, 7-11
 - 配置通知, 6-22, 7-12
- 远程访问, 3-51
 - 用户管理, 6-9
- 云安全智能防护, 7-4
 - Web 信誉服务, 7-4
- 云安全智能防护网络, 6-33, 6-34

Z

- 在线
 - 团体, A-2
- 在线用户
 - 查看 PPTP VPN, 3-54

- 查看 SSL VPN, 3-59
- 查看移动 VPN, 3-73
- 增量更新, 7-5
- 摘要实时监控, 5-2
 - 删除选项卡, 5-4
 - 添加选项卡, 5-3
 - 修改选项卡, 5-3
 - 选项卡, 5-2
- 站到站 VPN, 3-96
 - IKE, 3-96
 - IPsec, 3-96
 - 配置示例, 3-102, 3-104
 - 问题排查, 3-102
- 帐户
 - 管理员, 删除, 6-8
 - 添加, 6-7
- 诊断
 - 跟踪通信, 6-31
 - 关于, 6-29
 - 数据包捕获, 6-29
 - 通信跟踪, 6-31
 - 网络数据包捕获, 6-29
 - 文件, 6-32
 - 问题排查
 - 通信跟踪, 6-31
 - 诊断:
 - 关于, 6-29
 - 诊断文件
 - 生成, 6-32
 - 证书颁发机构
 - 导出, 4-48
 - 导入, 4-48
 - 管理, 4-49
 - 证书失败通知, 4-72
 - 支持, 6-32
 - TrendLabs, A-6
 - 更快地解决问题, A-4
 - 知识库, A-2
- 知识库, A-6
 - URL, x
- 终端用户
 - 设置, 全局, 6-10
- 重新分发
 - RIP, 3-31
 - RIP 设置, 3-31
- 重新分发 OSPF 路由, 3-38
- 主要功能, 1-6
 - ActiveUpdate, 1-6
 - LDAP 集成, 1-7
 - URL 过滤, 1-7
 - Web 信誉, 1-6
 - 安全防护, 1-6
 - 报告, 1-7
 - 病毒扫描, 1-6
 - 反垃圾邮件, 1-6
 - 日志, 1-8
 - 网络入侵防御, 1-6
 - 系统通知和警报, 1-7
 - 应用程序带宽监控, 1-7
 - 应用程序控制, 1-6
 - 摘要实时监控, 1-7
- 注册
 - URL, 8-2, 8-5
 - 安全配置, 8-2, 8-5
 - 密钥, 8-2, 8-5
- 注册产品, 8-4
- 注册码, 8-3
- 状态
 - IPsec, 3-102
- 自述文件, x, A-6
- 租用时间, 3-46
- 组件

- 更新, 7-2
- 组件版本, 7-5
- 最常访问的 URL 类别
 - 小组件, 5-21
- 最常访问的站点
 - 小组件, 5-20
- 最常使用的应用程序
 - 小组件, 5-17
- 最佳实务
 - DNS 服务器, 6-34
 - 建议, 6-34



趋势科技·中国 趋势科技（中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

电话：021-6384 8899 传真：021-6384 1899 邮箱：service@trendmicro.com.cn

www.trendmicro.com

Item Code: CTCM26326/140304