TREND MICRO

下一代应用安全网关 1.5

全程护航 迈向云端

管理员指南

Network Security

趋势科技 （中国）有限公司保留对本文档以及此处所述产品进行更改而不通知的权利。在安装并使用本软件之前，请阅读自述文件、发布说明和最新版本的适用用户文档，这些文档可以通过趋势科技的以下 Web 站点获得：

http://downloadcenter.trendmicro.com/?regs=CH

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可能是其各自所有者的商标或注册商标。

版权所有 © 2012 趋势科技 （中国）有限公司/Trend Micro Incorporated。保留所有权利。

文档编号：CTCM15544/120816

发布日期：2012 年 8 月

文档版本号：1.5

产品名称和版本号：下一代应用安全网关 1.5

趋势科技下一代应用安全网关的用户文档旨在介绍软件的主要功能以及针对您的生产环境的安装说明。在安装或使用该软件之前，请详细阅读该指南。

有关如何使用软件中特定功能的详细信息，可在联机帮助文件和趋势科技 Web 站点上的知识库中获得。

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

前言

下一代应用安全网关文档 xvi

适用读者 xvii

文档约定 xvii

关于趋势科技 xviii

第 1 章：介绍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

主要功能 1-2

- 安全防护 1-2
- 操作控制 1-3
- 可见性和监控 1-3
- 网络连接 1-4

摘要实时监控简介 1-4

- 关于小组件 1-5
- 定制小组件 1-6
  - 添加新小组件 1-8
  - 删除小组件 1-8
- 关于新选项卡 1-8
  - 添加新选项卡 1-8
  - 修改选项卡设置 1-9
  - 删除选项卡 1-9

第 2 章：更新

产品维护 2-2
续订维护协议 2-2
更改下一代应用安全网关系统密码 2-3
关于 ActiveUpdate 2-3
关于从 Web 控制台更新 2-3
用于更新的代理服务器设置 2-4
可更新的程序组件 2-4
防恶意软件病毒码文件 2-5
防恶意软件协议特征码文件 2-5
入侵防御特征码文件 2-5
Web 信誉技术 2-6
URL 数据库 2-6
电子邮件信誉数据库 2-7
病毒码文件的增量更新 2-7
组件版本信息 2-7
手动更新 2-7
从下一代应用安全网关 Web 控制台手动更新 2-8
预设更新 2-8
预设特征码更新 2-9
维护更新 2-9
验证更新是否成功 2-10
更新通知 2-10
还原更新 2-10

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
关于 VLAN 3-3
添加 VLAN 子接口 3-3

部署设置 3-4
配置部署模式设置 3-4
配置内部地址设置 3-5

网桥 3-5
更改网桥设置 3-5
配置高级网桥设置 3-6
移除网桥设置 3-7

路由网络通信概述 3-7

关于静态路由管理 3-7
添加静态路由 3-8
启用/禁用静态路由 3-8
修改静态路由 3-9
删除静态路由 3-9

关于动态路由管理 3-9
关于路由信息协议 (RIP) 3-10
关于全局 RIP 设置 3-11
启用 RIP 全局设置 3-11
配置高级 RIP 设置 3-11
关于网络 RIP 设置 3-12
添加新 RIP 网络 3-12
删除 RIP 网络 3-13
关于重新分发 RIP 设置 3-13
配置重新分发选项 3-13
开放最短路径优先协议 (OSPF) 3-14

全局 OSPF 3-14
路由器 ID 3-14
启用全局 OSPF 设置 3-15
启用 OSPF 分发缺省路由选项 3-15
关于区域 OSPF 3-15
添加新 OSPF 区域 3-16
修改 OSPF 区域 3-17
删除 OSPF 区域 3-17
关于 OSPF 接口 3-18
修改 OSPF 接口 3-18
重新分发 OSPF 路由 3-19
重新分发 OSPF 路由 3-19
路由表 3-20
查看路由表 3-20

网络地址转换 (NAT) 3-21
NAT 规则 3-23
添加 NAT 规则 3-23
修改 NAT 规则 3-24
更改 NAT 规则优先级 3-24
删除 NAT 规则 3-24

服务 3-25
DNS 转发配置 3-25
DNS 转发设置 3-25
配置 DNS 转发设置 3-26
DHCP 的接口配置 3-26
DHCP 高级设置：静态映射和租用时间 3-26
查看 DHCP 服务设置 3-27
修改 DHCP 服务设置 3-27
动态域名系统服务 3-28
配置 DDNS 客户端 3-29
DDNS 状态 3-29

虚拟专用网络 3-30
用户 VPN 3-31
点对点隧道协议 (PPTP) VPN 3-31
启用 PPTP VPN 3-31
配置常规 PPTP VPN 设置 3-32
查看 PPTP VPN 在线用户 3-32
查看 PPTP VPN 日志以排除故障 3-32
高级设置：启用调试模式和加密级别 3-32
PPTP VPN 疑难解答 3-33
安全套接层虚拟专用网络 3-34
启用 SSL VPN 3-34
配置常规 SSL VPN 服务器设置 3-35
为 SSL VPN 配置本地网络 3-36
为 SSL VPN 配置虚拟 IP 地址池 3-36
为 SSL VPN 配置高级设置 3-36
查看 SSL VPN 客户端 3-38
查看 SSL VPN 日志 3-38
安装 SSL VPN 客户端 3-38
SSL VPN 疑难解答 3-40
用户 VPN：用户管理 3-40
添加 VPN 用户帐户 3-41
修改 VPN 用户帐户 3-41
删除 VPN 用户帐户 3-42

站到站 VPN 3-42
IPSec 连接 3-42
添加新 IPSec 连接 3-43
站到站 VPN 策略 3-45
添加 VPN 站到站策略 3-45
高级 IPSec 配置 3-47
状态 3-47
疑难解答 3-48
IPSec 示例 1：分支机构配置示例 3-48
IPsec 示例 2：NAT 设备的后端配置 3-50

第 4 章：策略和对象

关于策略 4-2
防火墙策略如何工作 4-2
使用 “规则”页面 4-3
添加策略规则 4-3
启用/禁用策略规则 4-6

关于策略对象 4-6
关于地址和地址对象 4-6
地址对象参数 4-7
配置地址对象 4-8
查看地址对象 4-8
删除地址对象 4-8
关于区域和区域对象 4-9
配置区域对象 4-9
查看区域 4-10
删除区域对象 4-10
关于服务和服务对象 4-10
服务对象参数 4-11
添加定制服务对象 4-11
查看定制服务对象 4-12
删除定制服务对象 4-12
关于应用程序和应用程序对象 4-12
添加新应用程序组对象 4-13
查看应用程序组对象 4-13
删除应用程序组对象 4-13
关于时间表和时间表对象 4-14
添加时间表对象 4-14
编辑时间表对象 4-14
移除时间表对象 4-14

关于安全配置 4-15
重置安全配置 4-15

防火墙 4-15
防恶意软件安全配置 4-16
关于文件扩展名验证 4-16
选择要扫描的文件扩展名/类型 4-16
网络入侵防护 4-17
入侵防御安全配置 4-18
修改入侵防御策略 4-19
Web 信誉服务安全配置 4-20
配置 Web 信誉服务安全配置 4-21
配置 Web 信誉服务通知 4-21
URL 过滤安全配置 4-21
URL 过滤类别组 4-22
URL 过滤类别 4-23
配置 URL 过滤安全配置 4-29
修改 URL 过滤安全配置 4-31
删除 URL 过滤安全配置 4-31
配置 URL 过滤通知 4-31
电子邮件扫描 4-32
反垃圾邮件检测 4-32
电子邮件信誉技术 4-32
反垃圾邮件安全配置 4-33
启用和禁用反垃圾邮件安全配置 4-33
修改反垃圾邮件安全配置 4-33
关于 URL 黑/白名单 4-34
将 URL 添加到允许或阻止列表 4-34
启用/禁用白名单或黑名单 4-35
用户识别策略 4-35
添加或编辑用户 ID 策略 4-36
关于网页认证 4-36
配置网页认证设置 4-37

第 5 章：报告

实时监控摘要报表 5-2
安全状态 5-26
通信状态 5-26
系统信息 5-27

报告 5-27
关于即时报表 5-27
生成即时报表 5-27
预设报告 5-28
报告模板 5-28
创建预设报告模板 5-28
创建预设报告 5-29
删除预设报告 5-29
查看保存的报告 5-29
删除保存的预设报告 5-30
报告设置 5-30
配置报告设置 5-30
清除保存的预设报告 5-31

报告类型 5-31
安全事件报告 5-31
前 N 个违例用户报告 5-32
前 N 个网络通信报告 5-32

第 6 章：日志

日志简介 6-2

日志设置 6-2
配置全局日志设置 6-2

日志查询 6-3
查询日志 6-3
查询安全日志 6-4
查询流量日志 6-5

查询 VPN 日志 6-5
查询系统事件日志 6-5
查询审计日志 6-6

日志类型 6-6
安全日志 6-6
流量日志 6-7
VPN 日志 6-8
系统事件日志 6-8
审计日志 6-9

第 7 章：管理

概述 7-2

系统设置 7-2
常规系统设置 7-2
时间和日期设置 7-2
配置时间和日期设置 7-2
控制台设置 7-3
配置 Web 控制台超时 7-3
代理服务器设置 7-3
配置代理服务器设置 7-4
体验改善 7-4

下一代应用安全网关管理 7-4
管理服务 7-4
启用管理服务 （Ping、 SSH 和 SNMP） 7-4
Web 命令行 7-5

通知简介 7-6
系统通知和警报 7-6
配置安全信息汇总通知 7-6
配置硬件监控异常通知 7-7
配置系统资源警告通知 7-8
配置预设更新通知 7-9
停止通知 7-9

通知的 SMTP 设置 7-10
配置通知的 SMTP 设置 7-10
关于 LDAP 用户识别 7-10
LDAP 用户识别方法 7-11
LDAP 集成 7-11
LDAP 认证方法 7-11
基本 LDAP 认证 7-12
高级 LDAP 认证 7-12
配置基本和高级 LDAP 认证设置 7-13
关于 LDAP 全局设置 7-13
配置 LDAP 全局设置 7-14
帐户管理 7-14
添加新帐户 7-14
显示用户列表 7-15
修改用户描述或密码 7-15
删除用户帐户 7-15
产品使用授权 7-16
使用授权过期警告 7-16
获取注册码 7-16
注册下一代应用安全网关 7-17
获取并输入激活码 7-17
更新使用授权 7-18
续订维护协议 7-18
维护 7-18
系统维护 7-19
配置备份与恢复 7-19
诊断 7-19
网络数据包捕获 7-20
使用网络数据包捕获 7-22
通信跟踪 7-23
诊断文件 7-23

支持 7-23
关于下一代应用安全网关 7-24
云安全智能防护网络：基于云的服务 7-24
DNS 最佳实践建议 7-25

第 8 章：测试和配置下一代应用安全网关

EICAR 测试文件 8-2
测试 Web 信誉 8-3
测试应用程序控制 8-4
测试 URL 过滤 8-4

附录 A：联系人信息和基于 Web 的资源

联系技术支持 A-2
知识库 A-2
将可疑代码发送给趋势科技 A-3
TrendLabs A-4
安全信息中心 A-4
TrendEdge A-6

前言

欢迎阅读*趋势科技™ 下一代应用安全网关 1.5 管理员指南*。本指南提供了有关下一代应用安全网关的下一代防火墙配置选项的详细信息。主题包括如何更新软件以使您的最新风险防护保持最新、如何配置和使用策略以支持您的安全目标、如何配置扫描、如何配置 URL 过滤以及如何使用日志和报告。

本前言讨论以下主题：

- 第 P-xvi 页的*下一代应用安全网关文档*
- 第 P-xvii 页的*适用读者*
- 第 P-xvii 页的*文档约定*
- 第 P-xviii 页的*关于趋势科技*

下一代应用安全网关文档

除了 《趋势科技™ 下一代应用安全网关管理员指南》，下一代应用安全网关的文档集还包括以下内容：

- **安装指南** — （仅虚拟设备）本指南通过介绍下一代应用安全网关、帮助进行安装规划、实施与配置以及描述升级后的主要配置任务，帮助您 “启动并运行”。该指南还说明了如何利用无害测试病毒测试安装过程、如何排除故障以及如何获得支持。
- **部署指南** — （仅硬件设备）本指南在部署模式和配置方面为下一代应用安全网关设备用户提供帮助。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支持。
- **快速入门指南** — （仅硬件设备）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** — 联机帮助的目的在于提供主要产品任务的操作指导、使用建议以及特定于文本框的信息（例如有效的参数范围和最佳值）。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** — 该文件包含联机文档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、已知问题以及版本历史的描述。

  您可从以下站点下载电子格式的 《安装指南》、《管理员指南》以及自述文件的最新版本：

  http://downloadcenter.trendmicro.com/?regs=CH

- **知识库** — 知识库是包含问题解决和疑难解答信息的联机数据库。提供有关已知产品问题的最新信息。要访问知识库，请打开：

  http://cn.trendmicro.com/cn/support/techsupport/index.html

- **TrendEdge** — 面向趋势科技员工、合作伙伴和其他相关方的程序，提供不支持的革新技术、工具和趋势科技产品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。

  http://trendedge.trendmicro.com

适用读者

本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，读者已深入了解网络架构方面的知识，包括：

- 网络基础
- 在 VMware ESX 上进行安装时的 VMware ESX 管理经验和在 Hyper-V 上进行安装时的 Microsoft Hyper-V 经验

本文档假定读者没有任何防病毒或 Web 安全技术的知识。

文档约定

为帮助您轻松查找并理解信息，下一代应用安全网关文档将使用以下约定。

表 P-1. 文档约定

约定	描述
全部大写	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、选项和防毒墙群件版任务
斜体	对其他文档的引用
等宽体	示例、示例命令行、程序代码、 Web URL、文件名和程序输出
注意：	配置注意事项

关于趋势科技

趋势科技 （中国）有限公司是网络防病毒和 Internet 内容安全软件和服务的全球领导者。趋势科技成立于 1988 年，引领了从台式机防毒到网络服务器和 Internet 网关防毒的迁移，并在此过程中以其卓越的前瞻和技术革新获得赞誉。

如今，趋势科技通过提供集中控制的基于服务器的病毒防护和内容过滤产品与服务，致力于为客户提供全面的安全战略来管理风险对信息的影响。通过保护流经 Internet 网关、电子邮件服务器和文件服务器的信息，趋势科技帮助全球性公司和服务提供商自一个中心点将病毒和其他恶意代码阻止于台式机之外。

有关详细信息，或要下载趋势科技产品的评估副本，请访问我们的获奖 Web 站点：

http://www.trendmicro.com.cn

第 1 章

介绍下一代应用安全网关下一代防火墙

本章包括以下内容：

- 第 1-2 页的 ***下一代应用安全网关概述***
- 第 1-2 页的 ***主要功能***
- 第 1-4 页的 ***摘要实时监控简介***

下一代应用安全网关概述

下一代应用安全网关解决方案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。它通过一个管理门户规范了众多安全组件的外观，并能够跟踪用户活动、运行报告以及执行必要的管理功能。此外，它还可对内容进行智能扫描并利用多个安全组件对客户进行保护，以缩短客户等待时间并改善用户体验。

主要功能

下面的列表描述了下一代应用安全网关解决方案的关键组成部分。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

- **防火墙** — 下一代应用安全网关提供了易于每日部署和管理的现代防火墙功能。
- **入侵防御** — 入侵防御 (IPS) 可在许多活动威胁、漏洞、后门程序和其他攻击通过设备时识别并阻止它们。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。
- **Web 防护** — 下一代应用安全网关通过基于云的 Web 信誉技术使管理员能够设置针对恶意 Web 站点的防护级别。
- **防病毒** — 下一代应用安全网关可以高速扫描应用程序内容，并利用多个安全组件保护客户，不仅缩短了延迟，同时还改善了用户体验。
- **反垃圾邮件** — 下一代应用安全网关利用基于云的电子邮件信誉服务 (ERS) 集成来根据电子邮件发件人的信誉检测垃圾电子邮件。
- **ActiveUpdate** — 下一代应用安全网关使用 ActiveUpdate （趋势科技的一个实用程序，可以实现对病毒码文件、协议特征码文件和入侵防御特征码文件的按需更新和实时更新）。

操作控制

- **应用程序控制** — 应用程序控制功能可自动发现流行的 Internet 应用程序，并可使管理员利用策略来控制对应用程序的访问。
- **URL 过滤** — URL 过滤模块提供了创建和配置 URL 过滤安全配置的步骤。URL 过滤及 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。
- **LDAP 集成** — 下一代应用安全网关支持包含 Active Directory 和 OpenLDAP 的轻量级目录访问协议 (LDAP)。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。事件日志和报告使用 LDAP 用户名和组来识别用户。

可见性和监控

- **摘要实时监控** — 下一代应用安全网关采用小组件框架用于实时监控实施，允许管理员选择哪些小组件显示系统、网络安全警报、安全应用程序和网络通信的状态。
- **应用程序带宽监控** — 利用应用程序控制和 LDAP 集成，下一代应用安全网关可以记录和监控网络上带宽使用最高的用户。管理员可以通过确定带宽使用最高的用户通知管理者有关网络带宽滥用情况，还可以查看这些用户使用的可能加重网络负荷的应用程序。
- **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)、硬件监控、 URL 过滤和应用程序控制等违例。
- **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。您可以使用此下一代应用安全网关程序事件信息来优化程序设置，并对组织的安全策略进行微调。
- **日志** — 安装并配置下一代应用安全网关之后，将根据您为每种风险类型选择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

- **网络配置** — 下一代应用安全网关允许您查看和编辑自动检测到的网络接口。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 的配置，下一代应用安全网关通过 IP 地址和网络掩码提供动态主机配置协议 (DHCP) 配置以及静态路由配置。以太网点对点协议 (PPPoE) 是 L3 端口的另一种选择。
- **网桥** — 下一代应用安全网关解决方案可以桥接两个下一代应用安全网关接口。该网桥透明地在桥接接口之间传递网络通信。下一代应用安全网关支持生成树协议 (STP)，确保任何桥接以太网局域网的无环回逻辑拓扑结构。
- **路由** — 下一代应用安全网关支持配置静态和动态路由，并且提供路由管理功能，例如：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** — 通过下一代应用安全网关，您可以使用网络地址转换 (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** — 下一代应用安全网关服务支持允许配置域名服务器 (DNS) 转发、动态主机配置协议 (DHCP) 服务器和动态 DNS (DDNS) 设置。
- **用户 VPN** — 下一代应用安全网关支持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)，并提供远程访问用户管理功能。
- **站到站 VPN** — 下一代应用安全网关使用 Internet 密钥交换 (IKE) 协议和 IP 安全 (IPsec) 协议创建加密的 L3 隧道。

摘要实时监控简介

缺省选项卡将显示以下三种类别的状态小组件：

- 安全
- 系统
- 网络通信

注意： 有关支持的小组件的更多信息，请参阅第 5-2 页的*实时监控摘要报表*。



图 1-1. 下一代应用安全网关摘要实时监控

关于小组件

可以在实时监控选项卡中添加或移除小组件。每个小组件都包含对其用途的描述。* 表示缺省显示的小组件：

- “安全状态”选项卡：
  - 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
- “通信状态”选项卡
  - 会话摘要*
  - 用户排名*
  - 最常使用的应用程序*
  - 带宽摘要*
  - 最常访问的站点
  - 最常访问的 URL 类别
- 系统信息
  - 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

定制小组件

小组件可以手动进行更新；并且在某些情况下，可以对其进行配置以显示更多或更少的信息或对信息进行过滤。

管理员可以定制一些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。

定制小组件：

1. 转到**实时监控**。
2. 确定要定制的小组件。
3. 单击小组件左上角的时间链接，选择要显示的时间段。
4. （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。

5. 将鼠标放在所显示的数据上并单击可放大详细信息。
6. 对于某些小组件，可以单击小组件底部的图例，以过滤所显示的信息。
7. 有关其他定制的信息，请参阅*图 1-2* 和*表 1-1*。另请参阅第 5-2 页的*实时监控摘要报表*。

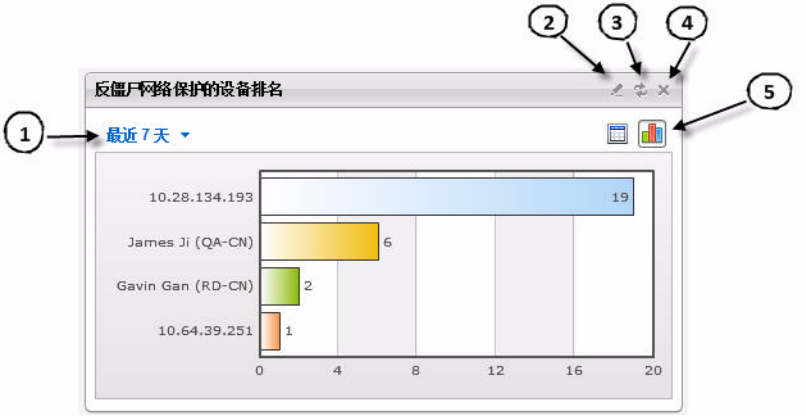


图 1-2. 小组件选项

表 1-1. 小组件选项

标注	描述
1	更改数据显示的时间段 （最近 1 小时、最近 1 天、最近 7 天以及最近 30 天）。
2	编辑显示的信息。某些小组件还允许配置显示的数据量。另外还有一些小组件允许对显示的数据进行过滤。
3	手动刷新。
4	从实时监控移除小组件。
5	选择显示样式 （条形图、饼图或表格格式）。

添加新小组件

添加预定义小组件：

1. 单击实时监控右上角的**添加小组件**图标 ( )。
   此时将显示 “添加小组件”选择页面。
2. 从所显示的预定义小组件设计列表中进行选择。您可以同时选择多个小组件。

   注意： 您还可以按类别 （安全状态、系统信息或通信状态）对小组件进行排序。请单击窗口左侧的类别。

3. 单击**添加**。

您可以删除已添加的小组件或将其拖放到小组件容器中的不同位置，并且仍然可以修改小组件配置。

删除小组件

删除小组件：

单击小组件左上角的 “X”可关闭该小组件。

关于新选项卡

要定制下一代应用安全网关实时监控，管理员可以添加其他选项卡、根据需要命名新选项卡以及添加相应的小组件。同时，还可以修改和删除已添加的选项卡。不能删除缺省选项卡，但可以进行修改。

添加新选项卡

向摘要实时监控中添加新选项卡：

1. 转到**实时监控**。
2. 单击最后一个已命名选项卡右侧的**加号 (+)**。
3. 为新选项卡的**标题**键入一个名称。
4. 选中适当的布局样式单选按钮。

5. 选择自动调整，可以是**打开**或**关闭**。如果选择 “打开”，则所有小组件的高度都将相同。
6. 单击**保存**。

修改选项卡设置

修改摘要实时监控中的选项卡设置：

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**
   - **自动调整**
5. 单击**保存**。

删除选项卡

只能删除已添加的选项卡。不能删除缺省选项卡 （安全状态、通信状态和系统信息）。

删除摘要实时监控中的选项卡：

1. 转到**摘要实时监控**。
2. 单击已添加的选项卡名称旁边的取消按钮 **X**。
3. 单击**确定**确认删除。

第 2 章

更新

由于新的恶意程序和攻击性 Web 站点层出不穷，因此必须持续更新软件以确保具有最新的特征码文件和系统更新 （如趋势科技™ 下一代应用安全网关（下一代应用安全网关） Web 控制台的 “管理 > 更新” 页面中所列）。

本章包括以下内容：

- 第 2-2 页的*产品维护*
- 第 2-3 页的*更改下一代应用安全网关系统密码*
- 第 2-3 页的*关于 ActiveUpdate*
- 第 2-4 页的*用于更新的代理服务器设置*
- 第 2-4 页的*可更新的程序组件*
- 第 2-7 页的*手动更新*
- 第 2-8 页的*预设更新*
- 第 2-9 页的*维护更新*

产品维护

趋势科技可能会不定期地发布一些针对报告的已知问题的 Patch 或适用于您的产品的升级。要了解是否已发布 Patch，请访问以下 URL：

http://downloadcenter.trendmicro.com/?regs=CH

单击下一代应用安全网关链接可以进入下一代应用安全网关的 “更新中心” 页面。单击名为 “搜索此产品的最新 hotfix” 链接，并输入以下搜索条件：

- **类别**：Internet 网关
- **产品**：下一代应用安全网关
- **版本**：当前产品版本

Patch 都注有日期。如果发现尚未应用的 Patch，请打开自述文档，确定该 Patch 是否适合您。如果适合，请遵照自述文件中的升级说明进行操作。

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，但不会再提供安全特征码与程序更新。为避免发生这种情况，请尽快续订 “维护协议”。

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”（用于将防护延长一年）将通过邮件发给贵公司 “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

要查看您的注册资料，请输入在您首次向趋势科技注册您的产品 （作为新客户）时创建的登录 ID 和密码，然后单击**登录**。

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。

更改下一代应用安全网关系统密码：

1. 转到主控制台登录页面。
2. 以管理员身份登录。
3. 单击窗口顶部的**更改密码**。
4. 键入旧密码、新密码以及确认密码。
5. 单击**应用**。

关于 ActiveUpdate

下一代应用安全网关使用趋势科技的 ActiveUpdate 实用程序，可以实现对病毒码文件、扫描引擎以及间谍软件或灰色软件特征码文件的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，也不需要您重新启动计算机。可以按照您配置的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
- 每日
- 每周
- 按需 （手动）

注意： 趋势科技建议您每日更新特征码文件。

用于更新的代理服务器设置

如果您使用代理服务器来访问 Internet，则在尝试更新组件之前，您必须先在下一代应用安全网关 Web 控制台中输入代理服务器信息。输入的任何代理服务器信息将用于执行以下操作：

- 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

配置代理服务器以更新组件和使用授权：

1. 打开下一代应用安全网关 Web 控制台，并单击**管理 > 系统设置 > 代理服务器设置**选项卡。
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，并在所提供的文本框中输入用户 ID 和密码。

   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。如果下一代应用安全网关与其他代理服务器一起部署，则 ActiveUpdate 代理服务器的下一跳地址代理服务器设置应该为位于接口同一侧的同一台服务器。

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：

这些特征码文件包括防恶意软件病毒、防恶意软件协议和入侵防御。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。

每当服务器上提供了新的病毒码文件时，使用 ActiveUpdate 功能 （有关详细信息，请参阅第 2-3 页的*关于 ActiveUpdate*）的所有趋势科技杀毒专家都可以检测到该情况，并可以预设为每小时、每天、每周 （如此等等）自动轮询服务器来获取最新文件。

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。

注意： “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。

入侵防御特征码文件

下一代应用安全网关使用入侵防御特征码文件阻止入侵防御漏洞。如果特征码之间的比较结果表明网络连接存在漏洞，下一代应用安全网关将根据配置采取相应的处理措施。

Web 信誉技术

下一代应用安全网关使用 Web 信誉技术，使管理员可以设置对恶意 Web 站点的防护级别。

在用户访问潜在危险的 Web 站点 （尤其是称为网络钓鱼或域名欺诈的站点，或者潜藏强制下载的站点）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。

URL 数据库

URL 数据库与其余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检索关于该 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。

将针对请求的通过下一代应用安全网关的 URL 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性级别来阻止 URL 访问 （请参阅第 4-21 页的*配置 Web 信誉服务安全配置*）。

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。

如果您认为某个 URL 的信誉分类有误或想要了解某个 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

要了解您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。

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。

从下一代应用安全网关 Web 控制台手动更新

下一代应用安全网关提供了手动更新特征码文件或预设更新的选项。当特征码文件已损坏，您需要重新从更新服务器下载组件时，手动更新功能非常有用。

如果下一代应用安全网关已在使用组件的最新版本，并且没有任何可用更新，则不会更新任何组件。

更新特征码文件：

1. 转到**管理 > 更新**。
2. 单击**特征码更新**或**系统更新**选项卡。
   - 对于特征码更新，选择要更新的部分或全部组件，然后单击**立即更新**。

     如果下一代应用安全网关上的特征码文件的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比远程下载服务器上的文件旧，则会下载较新的特征码文件。
   - 对于系统更新，请转到：

     http://downloadcenter.trendmicro.com/?regs=CH，单击产品名称，浏览到已下载的更新，然后单击**上传**。

预设更新

下一代应用安全网关可以对以下特征码文件执行预设更新：

- 防恶意软件病毒码
- 防恶意软件协议特征码
- 入侵防御特征码

不能为系统更新预设更新。

预设特征码更新

预设自动特征码文件更新：

1. 单击**管理 > 更新 > 特征码更新。**
2. 对于可更新的每种类型的组件，选择更新时间间隔。

   提供的选项包括：

   - 每小时：每隔 15、 30 或 60 分钟更新一次
   - 每天：选择每天的更新时间 （缺省）
   - 每周：从下拉菜单中选择日期和时间
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” 窗口 > “特征码信息” 小组件，验证特征码文件的当前版本。如果您的网络配置包含缓存服务器，则趋势科技建议您在更新特征码文件之后清空缓存并重新启动缓存服务器。这样会强制扫描所有 URL 请求，确保更好的网络防护。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。

维护更新

下一代应用安全网关以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：

- 第 2-10 页的*验证更新是否成功*
- 第 2-10 页的*更新通知*
- 第 2-10 页的*还原更新*

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**窗口在 “特征码信息”小组件中显示正在使用的组件的版本。要验证上次更新的时间和日期，请转到**管理 > 更新 > 特征码更新**选项卡以验证手动更新或预设更新是否已成功完成。

更新通知

下一代应用安全网关可以发出通知，主动通知管理员关于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，请参阅第 7-9 页的*配置预设更新通知*。

还原更新

下一代应用安全网关会检查程序目录并用最新的特征码文件来扫描入站/出站的网络通信。

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，可以还原到以前的特征码文件。

还原到以前的特征码文件：

1. 单击**管理 > 更新 > 特征码更新**选项卡。
2. 选择要还原的组件，然后单击**还原**。
3. 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。（您可能需要添加此小组件。缺省情况下，不会显示该小组件。有关添加小组件的详细信息，请参阅：第 1-8 页的*添加新小组件*。）

第 3 章

处理和识别网络通信

本章包括以下内容：

- 第 3-2 页的*网络通信概述*
- 第 3-2 页的*接口*
- 第 3-4 页的*部署设置*
- 第 3-5 页的*网桥*
- 第 3-7 页的*路由网络通信概述*
- 第 3-7 页的*关于静态路由管理*
- 第 3-9 页的*关于动态路由管理*
- 第 3-21 页的*网络地址转换 (NAT)*
- 第 3-25 页的*服务*
- 第 3-30 页的*虚拟专用网络*
- 第 3-42 页的*站到站 VPN*

网络通信概述

本节描述了如何配置下一代应用安全网关以在网络中操作。基本网络设置包括配置下一代应用安全网关接口。更高级的配置包括路由器、网桥、 VLAN、网络地址转换 (NAT)、广域网 (WAN)、服务以及下一代应用安全网关网络的虚拟专用网络 (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 的配置，下一代应用安全网关通过 IP 地址和网络掩码提供动态主机配置协议 (DHCP) 配置以及静态路由配置。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。

编辑网络接口：

1. 转到下一代应用安全网关 Web 控制台中的**网络 > 接口**以查看所有下一代应用安全网关网络接口。
2. 单击要更改的接口对应的带下划线的蓝色链接。
3. 根据需要，更改以下设置：名称、类型、模式、 IPv4/IPv6 地址、网络掩码、启用/禁用、用户名和密码。
4. 进行更改后单击**应用**。
5. 在**网络 > 接口**的接口列表中验证更新。

关于 VLAN

一个虚拟局域网 (VLAN) 由一组 PC、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。例如，财务部门的工作站和服务器可能分散在一个办公地点或一个城市中，并可连接到很多网段，但仍属于同一个 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

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，因为 0 和 4095 已保留。每个 L3 VLAN 子接口还必须配置有其自己的 IP 地址和网络掩码。

VLAN 通过子接口连接到用于接收标记了 VLAN 的数据包的物理接口。

添加 VLAN 子接口：

1. 转到下一代应用安全网关 Web 控制台中的**网络 > 接口**以查看所有下一代应用安全网关网络接口。
2. 在 “操作” 列中单击 VLAN 添加配置图标 ( )。
3. 输入下列信息：
   - **名称** — 此为 VLAN 子接口的名称。
   - **类型** — 自动显示为 L2 VLAN 或 L3 VLAN，具体取决于父接口。
   - **模式** — 从下拉列表中选择寻址模式类型为 DHCP 或静态。
   - **VLAN ID** — 输入与此 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**。

部署设置

下一代应用安全网关提供两种部署模式：监控模式和接入模式。它还支持用于添加内部地址的位置。

关于监控模式

监控模式提供了一种用于访问计算机网络上的数据流的方法。通过在监控模式下进行部署，您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 （某些）接口专门用作 “监控模式”接口并将该 （这些）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。

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传递的网络通信。

关于内部地址

在 “内部地址”选项卡中配置的设置决定了内部网络的 IP 地址范围。缺省情况下，它包括所有内部 IP 地址范围。您可以根据内部网络对其进行配置。（支持单个 IP 地址， "-" 作为范围标记；IP 地址/网络掩码，如 192.168.1.1/24。）

配置部署模式设置

配置脱机模式设置：

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：
   - **接入模式**
   - **监控模式**

4. 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 (-) 将它移回原位。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。
5. 单击**应用**。

配置内部地址设置

以下设置可确定内部网络的 IP 地址范围。缺省情况下，它包括所有内部 IP 地址范围。您可以根据内部网络对其进行配置。（支持单个 IP 地址， "-" 作为范围标记；IP 地址/网络掩码，如 192.168.1.1/24。）

配置内部地址设置：

1. 转到**网络 > 部署**。
2. 单击**内部地址**选项卡。
3. 输入网络的 IP 地址、 IP 地址范围，或 IP 地址和网络掩码。
4. 单击**添加**。

网桥

下一代应用安全网关解决方案可以桥接两个下一代应用安全网关接口。只支持一个网桥，其中包含两个 L2 或 L3 端口。通过此网桥，可以在桥接的接口之间透明地传递网络通信。

下一代应用安全网关支持生成树协议 (STP)，该协议可确保对于任何桥接的以太网局域网具有无环回逻辑拓扑结构。

更改网桥设置

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。

  此时将显示警告消息，通知用户某些操作可能导致 Web 控制台访问问题，例如，未为网桥配置 IP 地址。

注意： 如果系统中还存在其他 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。用户必须访问 CLI 以修复此状况。

配置或修改网桥设置：

1. 转到下一代应用安全网关 Web 控制台中的**网络 > 网桥**来配置或更改所有下一代应用安全网关桥接接口。
2. 从下拉列表中选择要桥接的可用接口。
3. 单击**应用**。

配置高级网桥设置

如果系统中还存在其他 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。

配置高级网桥设置：

1. 转到下一代应用安全网关 Web 控制台中的**网络 > 网桥 > 高级部分**来配置或更改所有下一代应用安全网关高级网桥接口设置。
2. 在“网桥配置”下，键入 IPv4 地址和网络掩码和/或 IPv6 地址/网络掩码。
3. 根据需要将管理设置设为阻止或允许特定基于管理的服务或网络通信。选择以下一种或多种设置以配置如何远程访问下一代应用安全网关：
   - Web 控制台
   - Ping
   - SSH
   - SNMP
4. 单击**应用**。

移除网桥设置

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。如果系统中还存在其他 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。如果有多个 VLAN 依赖于该接口，它们也会被移除。

移除网桥设置：

1. 转到下一代应用安全网关 Web 控制台中的**网络 > 网桥**来移除下一代应用安全网关桥接接口。
2. 单击**移除网桥**以删除网桥设置。
3. 单击**应用**。

路由网络通信概述

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。您需要了解一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”中配置静态和动态路由。下一代应用安全网关将提供路由管理功能，如：静态和动态路由，包括路由信息协议 (RIP)、适用于 IPv6 的 RIP、开放最短路径优先协议 (OSPF) 以及适用于 IPv6 的 OSPF。所有功能都可以使用下一代应用安全网关进行配置。

不管您管理小型网络还是大型网络，本节都将帮助您了解下一代应用安全网关单元如何执行路由功能。

关于静态路由管理

您可以选择静态路由，以手动控制网络通信从一台连接到网络的计算机移动到另一台的方式。

您可以通过定义希望下一代应用安全网关单元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。

“网络”>“路由”>“静态”下的“静态路由”列表显示下一代应用安全网关单元为了路由数据包而与数据包头进行比较的信息。您可以手动添加新条目。

将静态路由添加到“静态路由”列表时，下一代应用安全网关单元会执行检查以确定在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。如果未找到匹配路由，下一代应用安全网关单元会将该路由添加到路由表中。

如果要配置 IPv6 静态路由，请在“协议”下拉列表中选择“IPv6”。

添加静态路由

添加静态路由：

1. 转到 Web 控制台中的**网络 > 路由 > 静态**。
2. 单击**新增**链接。
3. 输入网络 IP 地址/位掩码或类域间路由 (CIDR) 表示法。位掩码是网络掩码的十进制等效值。例如， 255.255.255.0 = /24
4. 输入下一个跃点 IP 地址或接口。
5. 选中**启用**复选框。
6. 单击**应用**。

启用/禁用静态路由

启用/禁用静态路由：

1. 转到**网络 > 路由 > 静态**。
2. 在静态路由列表中，单击要启用的路由对应的**启用**复选框。
3. 取消选中**启用**复选框以禁用静态路由。

修改静态路由

修改静态路由：

1. 转到**网络 > 路由 > 静态**。
2. 单击要更改的静态路由的 IP 地址。
3. 更改 “网络 IP 地址/位掩码”和 “下一个跃点”值。
4. 单击**应用**。

删除静态路由

删除静态路由：

1. 转到**网络 > 路由 > 静态**。
2. 单击 “删除”图标。
3. 单击**删除**以确认删除。

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根据指定的规则动态更新路由表。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施支持 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，该协议可以帮助防止形成路由循环，但同时也限制了所支持网络的大小。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会以多播形式从其启用了 RIP 的每个接口发送 RIP 更新请求。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。当路由表中存在某个路由时，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，而跃点计数 16 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两个指向相同目标的路由时，会将具有最低跃点计数的路由添加到路由表中。

同样，在接口中启用 RIP 时，下一代应用安全网关会定期将 RIP 响应发送到相邻路由器。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。

配置 RIP 设置时，您必须指定运行 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 操作所需的所有附加设置。

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中调整 RIP 操作所需的其他任何设置。

转到 “网络” > “路由” > “RIP” > “全局”以查看全局 RIP 设置。

用户可以配置以下设置：

- 启用/禁用 RIP
- 分发缺省路由 — 允许再次分发缺省路由
- 设置计时器 — 配置更新计时器、超时计时器和垃圾计时器

启用 RIP 全局设置

启用并设置 RIP 全局设置：

1. 转到**网络 > 路由 > RIP**。
2. 选择 **IPv4** 或 **IPv6**，具体取决于您的网络设置。
3. 单击**全局**。
4. 选中**启用**复选框。
5. 单击**应用**。

配置高级 RIP 设置

设置 RIP 全局高级计时器设置：

1. 转到**网络 > 路由 > RIP**。
2. 单击**全局**。
3. 单击**高级设置**。
4. 选中**分发缺省路由**复选框，以启用缺省路由的分发。（此选项只有在应用更改后才启用。）

5. 需要设置下列计时器：
   - **更新计时器** — 输入下一代应用安全网关在两次发送 RIP 更新之间等待的时间 （以秒为单位）。缺省值：30 秒
   - **超时计时器** — 输入在没有接收到任何路由更新的情况下路由可以连接的最长时间 （以秒为单位）。此时间为下一代应用安全网关在没有收到相应更新的情况下将某个可访问路由保留在路由表中的最长时间。如果在超时时间过期前下一代应用安全网关收到了该路由的更新，则计时器会重新启动。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
   - **垃圾计时器** — 输入下一代应用安全网关将某个路由公布为无法访问的时间 （以秒为单位）。达到该时间值后，会将该路由从路由表中删除。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
6. 单击**应用**。

关于网络 RIP 设置

将 IP 地址和网络掩码的网络设置应用于已连接运行 RIP 的下一代应用安全网关的主要网络。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

添加新 RIP 网络：

1. 转到 Web 控制台中的**网络 > 路由 > RIP > 网络**。
2. 单击**新增**。
3. 为新 RIP 网络输入 IP 地址/位掩码。
4. 单击**应用**。
5. 验证**网络 > 路由 > RIP > 网络**下的列表中是否显示新 RIP 网络。

删除 RIP 网络

删除 RIP 网络：

1. 转到 Web 控制台中的**网络 > 路由 > RIP > 网络**。
2. 单击要删除的 RIP 网络的**操作**列中的删除图标。
3. 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以重新分发关于不是通过 RIP 识别的路由的 RIP 更新。下一代应用安全网关可以使用 RIP 重新分发从直接连接的网络、内核、静态路由和 OSPF 中识别的路由。

配置重新分发选项

配置重新分发选项：

1. 转到 Web 控制台中的**网络 > 路由 > RIP > 重新分发**。
2. 单击**重新分发**链接将其展开。
3. 选中相应的重新分发选项：
   - **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
   - **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**。

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。

分层技术用于限制需要公布的路由以及相关联的 LSA 的数目。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。

全局 OSPF

通过 OSPF 的全局设置，管理员可以启用 OSPF、输入路由 ID 以及启用缺省路由分配。

路由器 ID

输入唯一的路由器 ID 以在 OSPF 路由器中识别出下一代应用安全网关。按照惯例，路由器 ID 为分配给任意下一代应用安全网关接口的数值最高的 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

启用全局 OSPF 设置：

1. 转到 Web 控制台中的**网络 > 路由 > OSPF > 全局**。
2. 选中**启用 OSPF** 复选框。
3. 输入**路由器 ID**。
4. 单击**应用**。

启用 OSPF 分发缺省路由选项

启用全局 OSPF 分发缺省路由选项：

1. 转到 Web 控制台中的**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。

要添加新的 OSPF 区域，管理员需要配置以下内容：

- **区域 ID** — 区域的唯一标识符。
- **区域类型** — 区域类型选项包括：
    - **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** — 与无链接状态公告 (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输入以下信息：
    - **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。

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

添加新 OSPF 区域

添加新的 OSPF 区域：

1. 转到 Web 控制台中的**网络 > 路由 > OSPF > 区域**。
2. 配置下列内容：
    - 键入**区域 ID** — 区域的唯一标识符。
    - 选择**区域类型**：
        - **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** — 与无链接状态公告 (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。

3. 单击“添加网络”并输入一个新的有效的 IP 地址/位掩码。
4. 如果需要，请展开“虚拟链路设置”并添加一个路由器 ID。
5. 单击**应用**。
6. 确认在**网络 > 路由 > OSPF > 区域**下的列表中显示新区域。

修改 OSPF 区域

修改 OSPF 区域：

1. 转到**网络 > 路由 > OSPF > 区域**。
2. 单击某个现有 OSPF 区域的区域 ID。
3. 修改“区域名称”、“区域类型”、“网络设置”和/或“虚拟链路设置”的设置。
4. 单击**应用**。
5. 确认在**网络 > 路由 > OSPF > 区域**下的列表中显示新区域更改。

删除 OSPF 区域

删除 OSPF 区域：

1. 转到**网络 > 路由 > OSPF > 区域**。
2. 单击要删除的 OSPF 区域对应的删除图标。
3. 在确认操作中单击“删除”。
4. 确认 OSPF 区域已从**网络 > 路由 > OSPF > 区域**下的列表中移除。

关于 OSPF 接口

OSPF 接口定义包含下一代应用安全网关启用 OSPF 的接口的特定操作参数。定义中包含接口的名称 （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，定义一个区域 0.0.0.0， OSPF 网络定义为 10.0.0.0/16。然后将 vlan1 定义为 10.0.1.1/24， vlan2 定义为 10.0.2.1/24， vlan3 定义为 10.0.3.1/24。这三个 VLAN 都可以在区域 0.0.0.0 内运行 OSPF。要启用所有接口，应创建一个 OSPF 网络 0.0.0.0/0。

当多个 IP 地址分配给同一下一代应用安全网关接口时，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。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相兼容；再为同一接口配置第二个 OSPF 接口定义，确保其与另一个相邻路由器的设置相兼容。

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

修改 OSPF 接口：

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，更改下列一项或多项：
   - **接口名称** — 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** — 为该接口输入 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。
- **被动**选项 — 如果不希望 OSPF 接口发送或接收 OSPF 数据包，则选中此复选框。

4. 单击**应用**。
5. 在**网络 > 路由 > OSPF > 接口**的列表中验证更改。

重新分发 OSPF 路由

管理员可以决定是否分发内核、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：

1. 转到**网络 > 路由 > OSPF > 重新分发**。
2. 选中下面一个或多个选项：
   - **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
   - **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 RIP** — 选择此选项以重新分发从直接连接的 RIP 网络中识别的路由

3. 单击**应用**。

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。您可以通过定义其他静态路由向路由表添加路由信息。该表可能包含几个指向相同目标的不同路由 — 这些路由中指定的下一个跃点路由器的 IP 地址或与这些路由关联的下一代应用安全网关接口可能不同。

下一代应用安全网关通过评估路由表中的信息，为数据包选择 “最佳”路由。到目标的最佳路由通常与下一代应用安全网关单元和最近的下一个跃点路由器之间的最短距离相关联。某些情况下，如果最佳路由不可用，则可能选择下一个最佳路由。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

路由表使用代码指示路由类型。

代码：K — 内核路由， C — 已连接， S — 静态， R — RIPng， O — OSPFv3

查看路由表：

1. 转到**网络 > 路由 > 路由表**。
2. 选择相应的协议：**IPv4** 或 **IPv6**。

网络地址转换 (NAT)

如果在下一代应用安全网关中定义了第 3 层接口，则可以使用网络地址转换 (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 （请参阅*图 3-1*）将私有源地址范围 （从 10.0.0.1 到 10.0.0.100）转换为单一的公共 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，因此无法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 （或在同一子集中），则本地路由器需要静态路由以将返回网络通信导向下一代应用安全网关。



图 3-1. 示例 NAT 规则

下一代应用安全网关提供源 NAT 和目标 NAT 模式选项。

对于源 NAT：

- **源 NAT** — 源 NAT (SNAT) 更改数据包的 IP 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。如果选择 SNAT，您必须进行配置。
  - **出接口** — 从下拉列表中选择 “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** — 从以下选项中选择：
  - **使用出接口 IP** — 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。
  - **使用单个 IP** — 指定的 IP 地址将用于进行转换。
  - **使用 IP 范围** — 指定的 IP 地址范围将用于进行转换。
  - **使用子网** — 指定的子网将用于进行转换。
- **SNAT 的高级选项**允许用户指定更多详细信息或匹配条件，包括：
  - **协议：**任何、 TCP 或 UDP。“任何”指所有协议。
  - **源 IP 地址范围：**由管理员指定。
  - **源端口范围：**由管理员指定。
  - **目标 IP 地址范围：**由管理员指定。
  - **目标端口范围：**由管理员指定。

对于目标 NAT：

- **目标 NAT** — 目标 NAT (DNAT) 更改数据包的 IP 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。如果您选择 DNAT，您同样必须进行配置：
  - **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** — 从以下选项中选择：
    - **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 地址）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”复选框以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。

- **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：
  - **源 IP 地址范围：**由管理员指定。
  - **源端口范围：**由管理员指定。

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。与安全策略类似，将 NAT 策略规则依次与传入网络通信相比较，并应用匹配网络通信的第一个规则。

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。可能还需要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私有地址。

添加 NAT 规则

添加 NAT 规则：

1. 转到**网络 > NAT > 新增**。
2. 选择源或目标 **NAT 类型**：
   - 对于源 NAT，请选择出接口和源 IP 转换。请参阅第 3-21 页的***网络地址转换 (NAT)***。
   - 对于目标 NAT，请选择入接口和目标 IP 转换。请参阅第 3-21 页的***网络地址转换 (NAT)***。
3. 单击**高级 (匹配条件)** 指定更多详细信息或匹配条件 （如果需要）。
4. 单击**应用**。
5. 在**网络 > NAT** 验证添加到列表中的新规则。

修改 NAT 规则

修改 NAT 规则：

1. 转到**网络 > NAT**。
2. 在 “协议”列中单击要更改的 NAT 规则的名称。
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

更改 NAT 规则优先级：

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. 使用 NAT 规则列表上方的运算符 （置顶、上移、下移、置底）重新排序。
4. 单击**更新优先级**以保存更改。

删除 NAT 规则

删除 NAT 规则：

1. 转到**网络 > NAT**。
2. 单击要删除的 NAT 规则所在那一行的删除图标。
3. 单击**删除**以确认删除。
4. 确认在**网络 > NAT** 中不再列出此 NAT 规则。

服务

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

DNS 转发配置

多个下一代应用安全网关功能使用域名服务器 (DNS)，包括警报电子邮件和 URL 过滤。可以指定下一代应用安全网关连接到的 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，至少必须有一个下一代应用安全网关接口使用 DHCP （或 PPPoE）寻址模式。请参阅 ***DHCP 的接口配置***。

下一代应用安全网关可以在接口中提供 DNS 转发。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，以及指定名称服务器以使用本地 DNS 或定制的 DNS。

DNS 转发设置

下一代应用安全网关中的 DNS 转发设置选项包括：

- **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/路由器模式中操作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** — 输入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）。

配置 DNS 转发设置

配置 DNS 设置：

1. 转到**网络 > 服务 > DNS 转发**。
2. 从下列选项中选择：
   - **不使用 DNS 转发** — 不需要其他信息。
   - **使用系统 DNS 设置** — 以 IPv4 或 IPv6 格式显示主和 （可选）辅助 IP 地址。
   - **使用指定的 DNS 服务器** — 以 IPv4 或 IPv6 格式输入 DNS 服务器的特定 IP 地址。
3. 单击**应用**。

DHCP 的接口配置

下一代应用安全网关支持网络接口的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。

如果将接口配置为使用 DHCP，则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

通过*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。您可以输入天数、小时数或分钟数。例如，如果仅输入小时数，则租用时间将限制在该小时数以内。

查看 DHCP 服务设置

查看 DHCP 服务设置：

1. 转到**网络 > 服务 > DHCP**。
2. 查看与任何 DHCP 服务关联的参数：
   - **名称** — DHCP 服务的名称，例如 eth0、 eth1 等等。
   - **IP 地址/子网** — 从 DHCP 服务器租用的 IP 地址/位掩码。
   - **启用/禁用** — 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 地址的范围。
   - **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

修改 DHCP 服务设置：

1. 转到**网络 > 服务 > DHCP**。
2. 单击要修改的 DHCP 服务的名称。
3. 修改与 DHCP 服务关联的参数：
   - **IP 地址/位掩码** — 从 DHCP 服务器租用的 IP 地址/位掩码。
   - **启用/禁用** — 单击图标以在启用 （绿色/开启）和禁用 （红色/关闭）的 DHCP 服务之间进行切换。
   - **首选 DNS** — 输入首选 DNS 服务器的 IP 地址。
   - **网关** — 输入 DHCP 服务器定义的网关的 IP 地址。
   - **IP 地址范围开始和结束** — 输入 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：
   - **租用时间** — 调整租用的 IP 地址和网络掩码不再有效时的时间和日期。
   - **静态映射** — 选中复选框以启用该选项并单击**添加静态映射**。
     - 添加 **Mac 地址**、 **IP 地址**，然后选择**取消**或**提交**操作。

5. 单击**应用**。
6. 在**网络 > 服务 > DHCP** 中验证这些设置已更改。

动态域名系统服务

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。使用 DDNS 客户端，下一代应用安全网关可以就主机名到 IP 地址的更改与 DDNS 服务提供商进行通信。

有了下一代应用安全网关的动态 DNS 支持，管理员可以在 DDNS 服务供应商的 Web 站点中注册域，然后将信息 （如帐户、密码和域）配置为通过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计算机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。

支持以下四个 DDNS 服务提供程序：

- 适用于全球用户的 Dyn DNS 和 FreeDNS
- 主要适用于中国用户的 Oray 和 DNSPod

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。

注意： 不支持 IPv6。

配置 DDNS 客户端

管理员必须根据其选择的服务供应商，配置某些基本设置。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。

配置 DDNS 客户端：

1. 转到**网络 > 服务 > 动态 DNS > 常规**选项卡。
2. 在 “动态 DNS”对话框中，执行下列操作：
   - 选中**启用动态 DNS** 复选框。
   - 选择一个**供应商**。
   - 键入您的**用户名**、**密码**和**域** （例如 company.com）。“密码”文本框可以显示纯文本或模糊文本。单击**隐藏密码**或**显示密码**以进行更改。
   - （适用于 DNSPod）键入您的**主机记录** （例如 www、 @ 或 *）。
   - （仅适用于 Oray）选择您的**服务级别** （免费版、专业版、企业版或旗舰版）。所有非免费的服务都是 HTTPS 连接所需的付费服务。
   - 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接口获取公共 IP 地址。
3. 如果选择了 “专业版”服务类型，则选中 “启用 HTTPS 连接”。
4. 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

虚拟专用网络技术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。

下一代应用安全网关是一个集成软件解决方案，在各种开放平台和安全设备中提供与企业网络、远程和移动用户、分支机构以及业务合作伙伴的连接。通常情况下的下一代应用安全网关部署允许在移动用户的便携式计算机中连接企业网络 （从 Internet）和远程访问软件。其他远程站点由附加下一代应用安全网关提供保护，通过严格的安全策略管理所有组件之间的通信。

下一代应用安全网关通过 VPN 访问支持 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 VPN 为远程用户扩展了 VPN 功能，使用户可以使用拨号连接 （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递敏感信息。用户通过安全网关服务器的内部数据库或通过外部 RADIUS 服务器进行管理。

点对点隧道协议 (PPTP) VPN

下一代应用安全网关支持点对点隧道协议 (PPTP) 以在两个 VPN 对等体之间传递 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。作为替代选项，也可以配置下一代应用安全网关以将 PPTP 数据包转发到下一代应用安全网关之后的网络中的 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。

当您打算使用下一代应用安全网关作为 PPTP 网关时，可以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。您需要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。

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。

管理员必须选择本地服务或远程认证拨号用户服务 (RADIUS) 进行认证。与 LDAP 设置和 SMTP 服务器设置一样，管理员还需要配置一个可以使用的 RADIUS 服务器。（SSL VPN 也需要 RADIUS 服务器。）

启用 PPTP VPN

启用 PPTP VPN：

1. 转到**网络 > 用户 VPN > PPTP VPN**。
2. 选中**启用 PPTP** 复选框。

配置常规 PPTP VPN 设置

配置全局 PPTP VPN：

1. 转到**网络 > 用户 VPN > PPTP VPN > 常规**。
2. 从 “认证”下拉列表中选择认证服务 （**本地**或 **RADIUS**）。
3. 选择 IP 地址的分配方式：**IP 地址池**或 **DHCP 服务器**。
   - *对于 IP 地址池*，请输入 IP 地址和位掩码。输入通过 PPTP 获取远程访问权限的客户端的 IP 地址 （示例：192.168.0.0）。
   - *对于 DHCP 服务器*，请输入 DHCP 服务器的 IP 地址/位掩码 （示例：10.10.1.1./24），并从下拉列表中选择有效的接口 （eth1 至 eth3）。
4. 配置高级设置 （如果需要）。请参阅第 3-32 页的***高级设置：启用调试模式和加密级别***。
5. 单击**应用**。

查看 PPTP VPN 在线用户

查看 PPTP VPN 在线用户：

转到**网络 > 用户 VPN > PPTP VPN > 在线用户**。

查看 PPTP VPN 日志以排除故障

查看 PPTP VPN 日志：

转到**网络 > 用户 VPN > PPTP VPN > 疑难解答**。

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。

启用调试模式并更改加密强度：

1. 转到**网络 > 用户 VPN > PPTP VPN > 常规**。
2. 单击**高级设置**链接。
   - 指定**加密**强度：
     - 40 位 （弱）
     - 128 位 （强）
3. 选中**启用调试模式**复选框以在 PPTP 日志中显示更多调试信息。
4. 单击**应用**。

PPTP VPN 疑难解答

如果您在设置 PPTP VPN 时遇到问题，可能会收到以下错误之一：

错误消息：`VPN 错误 800 – 无法建立 VPN 连接。`

- **说明：**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。
- **推荐的处理措施：**
  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 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。

  2) 要允许 PPTP 网络通信，请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 转发至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。

错误消息：`VPN 错误 734 – PPP 链接控制协议已终止。`

- **说明：**PPTP 客户端与下一代应用安全网关服务器之间的协议不匹配。
- **推荐的处理措施：**出于安全考虑，下一代应用安全网关服务器仅支持 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。

错误消息：VPN 错误 691 – 拒绝访问，因为用户名和/或密码在该域上无效。

- **说明：**用户名和/或密码无效。
- **推荐的处理措施：**输入正确的用户名和/或密码，或者请求管理员重置密码。

错误消息：VPN 错误 649 – 该帐户无权拨入。

- **说明：**该帐户无权拨入。
- **推荐的处理措施：**在 RADIUS 服务器配置中为该帐户添加拨入权限。

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。

如果用户对其计算机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/路由器模式中运行的下一代应用安全网关支持 SSL VPN 功能。

启用 SSL VPN

启用 SSL VPN：

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 客户端都使用覆盖主机名选项。

配置常规 SSL VPN 服务器设置：

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
2. 从下拉列表中选择将用于 SSL VPN 的协议 （**TCP** 或 **UDP**）。
3. 键入 SSL **端口**号。
4. 如果设备的主机名无法在客户端计算机上解析，请为**覆盖主机**键入设备 IP 地址。
5. 选择认证服务器：本地或 RADIUS。
   a. 对于 RADIUS，还需要添加：
      - RADIUS 服务器 IP 地址/位掩码
      - 端口号
      - 共享密码

      注意： 共享密码是在通信过程开始之前已分配给通信双方的预共享的密钥。

      - 选择**显示密码**以显示共享密码值。选择**隐藏密码**以仅显示星号来代表共享密码值字符。
6. 单击**应用**或继续进行下列操作：
   - 第 3-36 页的*为 SSL VPN 配置本地网络*
   - 第 3-36 页的*为 SSL VPN 配置虚拟 IP 地址池*
   - 第 3-36 页的*为 SSL VPN 配置高级设置*

为 SSL VPN 配置本地网络

为 SSL VPN 配置本地网络：

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. 为该本地网络输入 IP 地址/位掩码。
5. 单击**确定**。
6. 确认已在**网络 > 用户 VPN > SSL VPN > 常规 > 本地网络**下的列表中添加本地网络。

为 SSL VPN 配置虚拟 IP 地址池

为 SSL VPN 配置虚拟 IP 地址池：

1. 转到**网络 > 用户 VPN > SSL VPN > 常规**。
2. 单击**虚拟 IP 池设置**。
3. 输入 **IP 地址范围**。例如：10.252.1.1 - 10.252.1.254
4. 从下拉列表中选择**位掩码**值。
5. 单击**应用**。

为 SSL VPN 配置高级设置

为 SSL VPN 配置高级设置：

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**：

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。

- **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。
- **3DES** — 三重 DES，即，使用三个密钥对纯文本加密三次。
- **BF-CDC** — Blowfish 的未获得专利但使用密钥的 64 位块对称密码分组链接 (CBC) 算法。

4. 选择 “认证算法”：
   - **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. 选中**启用压缩流量**复选框以允许对 SSL VPN 流量进行透明压缩和解压缩。
8. 选中 “启用调试模式”复选框以在 SSL VPN 日志中显示更多调试信息。
9. 单击**应用**。

查看 SSL VPN 客户端

必须启用 SSL VPN 才能执行此过程。

查看 SSL VPN 客户端：

转到**网络 > 用户 VPN > SSL VPN > 客户端**。

查看 SSL VPN 日志

查看 SSL VPN 日志：

转到**网络 > 用户 VPN > SSL VPN > 疑难解答**。

安装 SSL VPN 客户端

对于 Windows 用户， SSL VPN 客户端安装软件包可以从 https://<下一代应用安全网关服务器 IP 地址>/vpnclient.html 下载。

对于 Linux 或 Mac 用户，最新的安装软件包可以从 **http://openvpn.net** 下载，而 SSL VPN 配置文件可以从 https://<下一代应用安全网关服务器 IP 地址>/vpnclient.html 获取。

在 Windows 上执行全新安装：

1. 使用浏览器访问 `https://<下一代应用安全网关服务器 IP 地址>/vpnclient.html`。
2. 单击**带有配置文件的安装包**以下载 **`sslvpnclient.zip`** 文件。
3. 将 `sslvpnclient.zip` 文件解压缩到本地文件夹，然后浏览到解压缩文件夹以安装 SSL VPN 客户端：
   - 对于 Windows 7（或更高版本）和 Vista 用户，右键单击 **`install.bat`** 文件并选择**以管理员身份运行**。
   - 对于所有其他 Windows 用户，双击 **`install.bat`** 文件。
4. 成功完成安装后，从 Windows “开始”菜单访问 SSL VPN 客户端：
   - 对于 Windows 7（或更高版本）和 Vista 用户，右键单击 **OpenVPN GUI** 图标并选择**以管理员身份运行**选项。
   - 对于其他 Windows 用户，单击 **OpenVPN GUI** 图标。

为已安装 SSL VPN 客户端的 Windows 用户执行安装：

1. 使用浏览器访问
   `https://<下一代应用安全网关服务器 IP 地址>/vpnclient.html`。
2. 单击适用于 Windows 操作系统的**配置软件包**以下载 **`sslvpnconfig.zip`** 文件。
3. 将 `sslvpnconfig.zip` 文件解压缩到本地文件夹，然后浏览到解压缩文件夹以安装 SSL VPN 配置文件：
   - 对于 Windows 7（或更高版本）和 Vista 用户，右键单击 **`install.bat`** 文件并选择**以管理员身份运行**选项。
   - 对于其他 Windows 用户，仅需双击 **`install.bat`** 文件。
4. 成功完成安装后，从 Windows “开始”菜单访问 SSL VPN 客户端：
   - 对于 Windows 7（或更高版本）和 Vista 用户，右键单击 **OpenVPN GUI** 图标并选择**以管理员身份运行**选项。
   - 对于其他 Windows 用户，单击 **OpenVPN GUI** 图标。

在 Linux 或 MAC 操作系统上安装 SSL VPN 客户端：

1. 使用浏览器访问
   `https://<下一代应用安全网关服务器 IP 地址>/vpnclient.html`。
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** 安全配置夹。

   客户端计算机将拨入下一代应用安全网关。有关问题，请查看第 3-40 页的 ***SSL VPN 疑难解答***。

SSL VPN 疑难解答

如果在设置 SSL VPN 时遇到问题，以下是一些常规疑难解答指南：

- 验证客户端是否可以成功 ping 下一代应用安全网关服务器。
- 验证客户端是否可以访问配置了 SSL VPN 的 TCP 或 UDP 端口。
- 验证客户端配置文件 `openvpn.ovpn` 与 `https://[下一代应用安全网关服务器 ip]/vpnclient.html` 文件是否具有相同配置。

您可能会收到以下错误之一：

错误消息： `TCP：无法连接到 X.X.X.X:8445， 5 秒后将重试：拒绝连接`

- **说明：**SSL VPN 客户端无法访问下一代应用安全网关服务器。
- **推荐的处理措施：**

  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 客户端与下一代应用安全网关服务器之间执行 Ping 操作。确认在 SSL VPN 客户端与下一代应用安全网关服务器之间具有网络连接。

  2) 要允许 SSL VPN 网络通信，请配置网络防火墙以向下一代应用安全网关服务器开放配置了 SSL VPN 的 TCP 或 UDP 端口。

错误消息： `收到 SIGTERM[软件,认证失败]，进程退出`

- **说明：**用户名和/或密码无效。
- **推荐的处理措施：**输入正确的用户名和/或密码，或者请求管理员重置密码。

用户 VPN：用户管理

远程认证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。总的来说，认证是尝试验证通信 （例如登录请求）发送者的 （数字）身份的过程。发送者可能是使用计算机的某个人、计算机本身或某个计算机程序。由于计算机系统仅应由经过授权的人使用，因此必须有适当的措施来检测和排除所有未经授权的访问。

下一代应用安全网关通过定义授权用户的列表 （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：

- 属于某个允许访问的用户组
- 在系统要求时，输入正确的用户名和密码以证明其身份

添加 VPN 用户帐户

添加 VPN 用户帐户：

1. 转到**网络 > 用户 VPN > 用户管理**。
2. 单击**新增**链接。
3. 为新用户输入下列信息：
   - 用户名
   - 密码
   - 密码确认
   - 描述
4. 单击**应用**。
5. 验证用户已添加到**网络 > 用户 VPN > 用户管理**下的用户列表中。

修改 VPN 用户帐户

修改 VPN 用户帐户：

1. 转到**网络 > 用户 VPN > 用户管理**。
2. 单击要修改的用户帐户的名称。
3. 更改下列任何信息：
   - 用户名
   - 密码
   - 密码确认
   - 描述
4. 单击**应用**。
5. 验证用户帐户更改已添加到**网络 > 用户 VPN > 用户管理**下的列表中。

删除 VPN 用户帐户

删除用户 VPN 用户帐户：

1. 转到**网络 > 用户 VPN > 用户管理**。
2. 单击要删除的用户帐户的名称所在那一行的删除图标。
3. 单击**删除**以确认删除用户帐户。
4. 验证**网络 > 用户 VPN > 用户管理**下的列表中不再显示此用户帐户。

站到站 VPN

虚拟专用网络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 内核在该数据包进入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 进入计算机。
- 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 隧道接口进入 IP 堆栈。

添加新 IPSec 连接

使用 “IPSec 连接”页面设置参数以在下一代应用安全网关之间建立 IPSec VPN 隧道。

注意： 开始前，请确保以太网接口和路由器已正确配置。

添加 IPSec 连接：

1. 转到**网络 > 站到站 VPN > 连接**。
2. 单击**添加新连接**。

   将显示 “添加/编辑 IPSec 连接”对话框。

3. 输入以下参数：
   - **名称** — 键入一个名称以标识 IPSec 隧道。
   - **启用** — 选中该复选框可启用隧道。
   - **网关类型** — 为 IPSec 隧道选择**发起**（主动）或**响应**（被动）角色。
   - **接口名称** — 从下拉列表中选择接口名称（eth0、eth1 等）。
   - **策略名称** — 从下拉列表中选择策略名称，选择缺省策略或特定策略，该策略将应用于 IPSec 隧道。

     注意： 在**网络 > 站到站 VPN > 策略**中配置非缺省 IPsec 策略。

   - **认证类型** — 从下拉菜单中选择**预共享密钥**或 **RSA 密钥**。
     - **对于预共享密钥** — 输入密钥并确认。

       如果选择了“预共享密钥”，请键入下一代应用安全网关用于对远程对等体或拨号客户端进行自身认证的预共享密钥。必须为远程对等体或客户端定义相同的值。该密钥必须至少包含 6 位可打印字符，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。
     - **对于 RSA 密钥** — 输入公共密钥。

       如果选择了“RSA 密钥”，请选择下一代应用安全网关用于对远程对等体进行自身认证的服务器证书的名称。
     - **VPN ID** — 如果 IPSec 网关在 NAT 设备后面，请输入本地 IP 地址。
4. 为本地网络（在**添加本地网络**下）或远程网络（在**添加远程网络**下）添加 IP 地址和网络掩码。
5. 单击**确定**。
6. 验证在**网络 > 站到站 VPN > 连接**中是否列出新的 IPsec 连接。

站到站 VPN 策略

作为站到站 VPN 策略的一部分，您可以配置两个 VPN 对等体来自动生成唯一的 Internet 密钥交换 (IKE) 密钥。 IPSec 策略：

- 在 NAT/路由或透明模式下可用。
- 需要防火墙策略中包含指定 VPN 隧道的 IPSec 操作。一个策略可控制两个方向的连接。

添加 VPN 站到站策略

添加 VPN 站到站策略：

1. 转到**网络 > 站到站 VPN > 策略**。
2. 单击**添加新 IPSec 策略**。
3. 键入新 IPSec 策略的名称。
4. 从下拉列表中选择 **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。

   - **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 256 位密钥的 128 位块密码分组链接 (CBC) 算法。
5. 从下拉列表中选择 **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 (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. 从下拉列表中选择 **IPSec 加密**值。
   - **无加密** — 不使用加密算法
   - **3DES**
   - **AES 128**
   - **AES 192**
   - **AES 256**
9. 从下拉列表中选择 **IPSec 认证算法**值。
   - **MD5**
   - **SHA1**
10. 从下拉列表 (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 高级配置选项包括：

- **启用对等体失效检测** — 对等体失效检测通过 ICMP ping 标识非活动的或不可用的 IKE Peer，可帮助恢复某一对等体不可用时丢失的资源。选中此复选框可在空闲连接上重建 VPN 隧道，并根据需要清除无效的 IKE Peer。您也使用此选项在隧道上升或下降时接收通知，或在隧道内未生成任何网络通信时将隧道连接保持打开状态。

  （例如，在一个动态 DNS 对等体通过定期变化的 IP 地址进行连接的情况下，当 IP 地址变化时，网络通信可能会被挂起）。
- **IKE 调试** — 选中以下 IKE 调试选项框。
  - 控制流
  - 发出报文
  - 接收报文
  - 原始内容
  - 算法信息
- **NAT 穿透** — 如果在本地下一代应用安全网关与 VPN 对等体或客户端之间存在 NAT 设备，则选中此复选框。本地下一代应用安全网关与 VPN 对等体或客户端必须具有相同的 NAT 穿透设置 （两者都选中或两者都清除）以进行可靠连接。
- **当前本地公共 RSA 密钥** — 以一种可复制、可输入使用 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。
- **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。

状态

“状态”选项卡显示实时 IPSec 连接状态。

疑难解答

通过**网络 > 站到站 VPN > 疑难解答**显示实时 IPsec 日志。使用 IPSec 日志可查看 IPSec VPN 隧道上的活动。

有关更多 IPSec 配置示例，请参阅：

- 第 3-48 页的 ***IPSec 示例 1：分支机构配置示例***
- 第 3-50 页的 ***IPsec 示例 2：NAT 设备的后端配置***

IPSec 示例 1：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

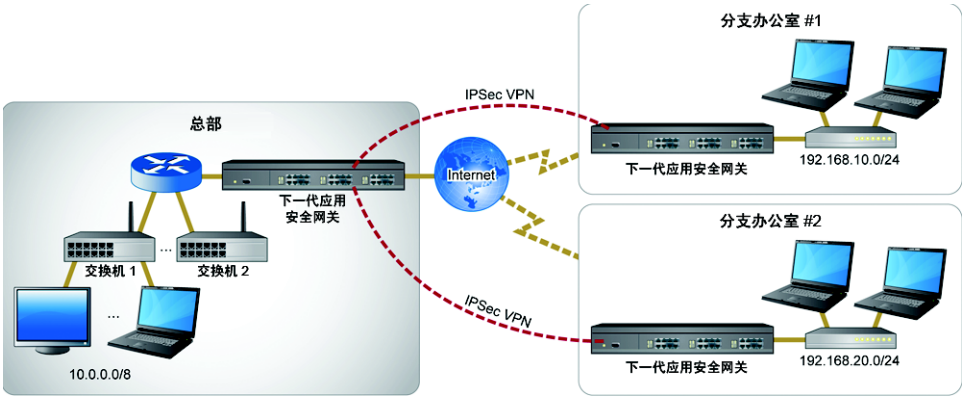


图 3-2. 下一代应用安全网关通过 IPSec VPN 连接两个分支办公室

VPN 连接的配置：

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 & 192.168.20.0/24

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 示例 2：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

下一代应用安全网关-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

下一代应用安全网关-B：

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

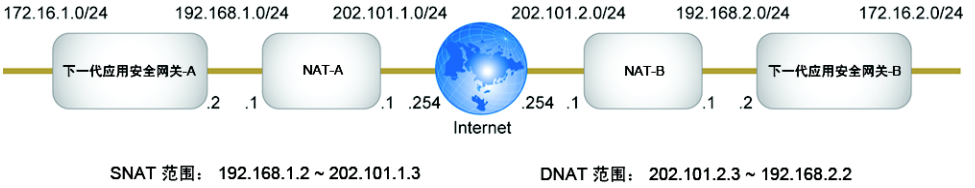


图 3-3. 下一代应用安全网关 VPN 位于 NAT 设备后面

VPN 连接的配置：

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

下一代应用安全网关-右：

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

策略和对象

本章包括以下内容：

- 第 4-2 页的*关于策略*
- 第 4-6 页的*关于策略对象*
- 第 4-15 页的*关于安全配置*
- 第 4-15 页的*防火墙*
- 第 4-32 页的*电子邮件扫描*
- 第 4-34 页的*关于 URL 黑/白名单*
- 第 4-35 页的*用户识别策略*

关于策略

策略可让您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）阻止或允许网络会话的安全策略。

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。

防火墙策略是指下一代应用安全网关单元用于确定是否接受通过该单元的网络通信以及如何处理该网络通信的数据包的指令。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在收到匹配的数据包时要遵循的许多指令。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。

防火墙策略可以与其他下一代应用安全网关功能相集成，以便为以下各项提供一个集中配置和管理策略的体系结构：

- 防病毒、间谍软件和电子邮件策略
- 第 4-17 页的*网络入侵防护*策略
- 第 4-29 页的*配置 URL 过滤安全配置*
- 第 4-15 页的*关于安全配置*。受支持的安全配置包括：
  - 防火墙
  - 防恶意软件
  - 入侵防御
  - Web 信誉服务
  - URL 过滤
  - 反垃圾邮件

使用 “规则” 页面

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，需要先创建某些用于定义策略规则参数的策略对象。有关详细信息，请参阅第 4-6 页的*关于策略对象*。

通过 “策略” > “规则” 中的 “策略” 页面，用户可以：

- 查看现有策略规则的列表
- 通过将鼠标悬停在规则名称上，查看规则的详细信息
- 根据键入内容过滤表
- 访问要编辑的规则
- 添加、复制和删除规则
- 应用和放弃规则

添加策略规则

使用 “规则” 页面可确定根据指定的网络通信属性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。

添加策略规则：

1. 转到**策略 > 规则**。
2. 单击**新增**。
3. 键入**策略名称**。
4. 键入可选的**策略描述**。

5. 单击**来源**选项卡。这些选项指定将对来自源区域、源 IP 地址和源用户的网络通信强制执行该规则。如果需要，可指定以下选项：
   - **源区域** — 使用缺省设置 “任何”（包括所有源区域），或 “选定”（显示先前配置的源区域的列表，供您从中选择）。

注意： 选择 “选定”单选按钮可提供 “添加新区域”选项。有关添加地址对象的详细信息，请参阅第 4-9 页的***配置区域对象***。

   - **源地址** — 使用缺省设置 “任何”（包括所有源地址），或 “选定”（显示先前配置的源地址的列表，供您从中选择）。

注意： 选择 “选定”单选按钮可提供 “添加新地址”选项。有关添加地址对象的详细信息，请参阅第 4-8 页的***配置地址对象***。

   - **源用户** — 使用缺省设置 “任何”（包括所有用户）、某个已知用户、某个未知用户，或 “选定的已知用户”（显示 “搜索”文本框以便搜索用户或组。该选项还会显示先前配置的用户的列表，以供从中选择。）
6. 单击**目标**选项卡。这些选项指定将对在这些目标区域和 IP 地址终止的网络通信强制执行该规则。如果需要，可指定以下选项：
   - **目标区域** — 使用缺省设置 “任何”（包括所有目标区域），或 “选定”（显示先前配置的目标区域的列表，供您从中选择）。如果使用 “选定”选项，则可以添加目标区域。
   - **目标地址** — 使用缺省设置 “任何”（包括所有目标地址），或 “选定”（显示先前配置的目标地址的列表，供您从中选择）。如果使用 “选定”选项，则可以添加目标区域。
7. 单击**服务**选项卡。这些选项指定将对与选定服务匹配的网络通信强制执行该规则。如果需要，可指定以下选项：
   - **服务** — 使用缺省设置 “任何”（包括所有服务），或 “选定”（显示可用服务的列表）。如果使用 “选定”选项，则可以添加服务。

8. 单击**应用程序**选项卡。这些选项指定将对与选定应用程序匹配的网络通信强制执行该规则。如果需要，可指定以下选项：
   - **应用程序** — 使用缺省设置“任何”（包括所有应用程序），或“选定”（显示可用应用程序的列表）。如果使用“选定”选项，则可以添加应用程序。
9. 单击**时间表**选项卡。这些选项指定将对与选定时间表匹配的网络通信强制执行该规则。如果需要，可指定以下选项：
   - **时间表** — 使用缺省设置“任何”（包括所有时间表），或“选定”（显示可用时间表的列表）。如果使用“选定”选项，则可以添加服务。
10. 单击**操作**选项卡。这些选项定义对于与策略匹配的网络通信所采取的处理措施。如果需要，可指定以下选项：
    - **操作** — 使用缺省设置：
      - **在进行检查的情况下允许**：允许访问，并对恶意内容进行扫描。
      - **阻止**：拒绝访问。
      - **在不检查的情况下允许**：允许访问，但不进行扫描。（不推荐）
11. 单击**安全配置**选项卡。这些选项将为该策略分配安全配置。已应用的安全配置显示在“安全配置”列中。如果需要，可指定以下选项：
    - **防恶意软件** — 使用缺省设置**阻止**，或另一个选项**监控**。
    - **反垃圾邮件** — 使用缺省设置**阻止**，或另一个选项**监控**。
    - **入侵防御** — 使用缺省设置：**阻止**，或者其他选项**监控**或**使用安全配置。**（“使用安全配置”是指遵循通过“策略”>“安全配置”>“入侵防御”在入侵防御安全配置中设置的处理措施。）有关详细信息，请参阅第 4-19 页的*修改入侵防御策略*。
    - **URL 过滤** — 使用缺省设置**阻止**，或者其他选项**监控**或**使用安全配置。**（“使用安全配置”是指遵循通过“策略”>“安全配置”>“URL 过滤”在“URL 过滤”安全配置设置中配置的处理措施。）此外，从“安全配置”列中选择适用的安全配置。（安全配置必须先前进行过配置。）有关详细信息，请参阅第 4-29 页的*配置 URL 过滤安全配置*。
    - **Web 信誉服务** — 使用缺省设置**阻止**，或另一个选项**监控**。
12. 单击**确定**。
13. 要启用策略，请参阅第 4-6 页的*启用/禁用策略规则*。

启用/禁用策略规则

除了启用 （或禁用）策略，还可以提供策略。当创建了策略，或策略为更高版本时，可以启用策略。该过程适用于已经创建但并未启用的策略规则。

启用/禁用策略规则：

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. 选中策略规则描述下方的复选框以启用该策略规则。取消选中以禁用该策略规则。
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：

- 地址对象，用于确定策略范围。请参阅第 4-6 页的*关于地址和地址对象*。
- 区域对象，用于将接口和 VLAN 子接口分组到区域中以便简化策略创建。请参阅第 4-9 页的*关于区域和区域对象*。
- 服务对象，用于限制协议 （TCP 或 UDP）和端口号。请参阅第 4-10 页的*关于服务和服务对象*。
- 应用程序对象，用于指定如何处理策略中的特定软件应用程序。请参阅第 4-12 页的*关于应用程序和应用程序对象*。
- 时间表，用于指定策略活动时间。请参阅第 4-14 页的*关于时间表和时间表对象*。

关于地址和地址对象

要为特定源或目标地址定义安全策略，必须首先定义地址和地址范围。

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，必须指定以下信息。

表 4-1. 地址对象参数

参数	描述
名称	输入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。
IP 地址	**IPv4 地址：** 使用以下表示法输入地址或网络： • ip_address/位掩码或 ip_address （其中，位掩码指用于地址的网络部分的有效二进制位数。） • IP 地址范围，如：192.168.1.1-192.168.1.10 例如： “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。 **IPv6 地址：** 输入 IPv6 地址或带有前缀的地址。 例如： “2001:db8:123:1::1”或 “2001:db8:123:1::/64”

配置地址对象

配置地址对象：

1. 转到**策略 > 对象 > 地址**。
2. 单击**新增**。
3. 输入以下内容：
   - 名称
4. 从下拉列表中选择合适的协议版本。
5. 键入 IP 地址。

> **注意：** 在填写 “IP 地址”文本框时，请键入 IP 地址或 CIDR 网络 （如多个以逗号分隔）。例如，以 192.168.0.1、10.0.0.1-10.0.0.4 或 10.0.0.8 的形式输入 IP 地址。

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

必须先创建地址对象，然后才可以查看这些对象。

查看地址对象：

转到**策略 > 对象 > 地址**。

删除地址对象

删除地址对象：

1. 转到**策略 > 对象 > 地址**。
2. 单击要删除的地址所在那一行的复选框。
3. 单击**删除**图标。在 “确认”对话框中单击**确定**。
4. 转到**策略 > 对象 > 地址**以验证已删除的地址对象是否不在列表中。

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。可以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。可以添加、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。

配置区域对象：

1. 转到**策略 > 对象 > 区域**。
2. 单击**添加区域**。
3. 添加下列信息：
   - 名称
   - 描述
4. 从下拉列表中选择接口。可以在**网络 > 接口**中查看可用接口。

   注意： 无法将管理接口添加到区域对象。

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。

查看区域对象：

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。

删除区域对象：

1. 转到**策略 > 对象 > 区域**。
2. 选中要删除的区域对象的名称旁边的复选框。
3. 单击**删除**图标。在 “确认”对话框中单击**确定**。
4. 转到**策略 > 对象 > 区域**以验证已删除的区域对象是否不在列表中。

关于服务和服务对象

为特定应用程序定义安全策略时，可以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 种服务，包括预定义的 DNS、FTP、HTTP、POP3、 SMTP、 SSL 和 TELNET 服务，而且您可以添加定制服务定义。

这些受支持的预定义协议不与任何端口关联。并不是所有协议都会接受下一代应用安全网关安全配置的扫描。可用的处理措施包括 “允许”或 “阻止”。

服务对象参数

要定义服务，请指定以下信息。

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，此名称将出现在服务列表中。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	选择该服务使用的协议或创建定制服务。
目标端口	（对于定制服务）输入服务使用的端口号 （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

添加定制服务对象：

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

注意： “目标端口”参数可以是单一端口 （例如 22）、多个单一端口 （例如 22、 23）、端口范围 （例如 22-80），或者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

查看定制服务：

转到**策略 > 对象 > 服务 > 定制服务**选项卡。

删除定制服务对象

删除定制服务对象：

1. 转到**策略 > 对象 > 服务 > 定制服务**选项卡。
2. 单击要删除的定制服务对象所在那一行的复选框。
3. 单击**移除**图标。在“确认”对话框中单击**确定**。
4. 转到**策略 > 对象 > 服务 > 定制服务**选项卡，以验证已删除的定制服务对象是否已不再列出。

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计算机使用策略。为了避免重大风险，应用程序控制功能提供了一项安全技术，该安全技术可自动发现热门 Internet 应用程序，并使管理员能够使用策略控制这些应用程序。

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）。

通过 “预定义组”选项卡，可以查看分配给每个缺省类别的所有单个应用程序。

在此页面上您可以实现以下任一功能：

- *添加新应用程序组对象*
- *查看应用程序组对象*
- *删除应用程序组对象*

添加新应用程序组对象

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，从而可以对该组应用一个策略。要执行此操作，需要创建一个定制应用程序组，并向该组添加特定的应用程序。可能需要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来阻止每个应用程序，可以将这些应用程序分成一组，以便允许使用一个策略来阻止这些应用程序。

添加应用程序组对象：

1. 转到**策略 > 对象 > 应用程序 > 定制组**选项卡。
2. 单击**新增**。
3. 输入下列信息：
   - 名称
   - 描述
4. 单击要包含在应用程序组中的相应应用程序类别的复选框。
5. 单击要包含在应用程序组中的应用程序类别内的应用程序的复选框。
6. 单击**确定**。
7. 转到**策略 > 对象 > 应用程序 > 定制组**选项卡，并验证新的应用程序组对象是否显示在列表中。

查看应用程序组对象

查看应用程序组对象：

转到**策略 > 对象 > 应用程序 > 定制组**选项卡。

删除应用程序组对象

删除应用程序组对象：

1. 转到**策略 > 对象 > 应用程序 > 定制组**选项卡。
2. 选中要删除的应用程序组所在那一行的复选框。
3. 单击**删除**图标。在 “确认”对话框中单击**确定**。
4. 转到**策略 > 对象 > 应用程序 > 定制组**选项卡。

关于时间表和时间表对象

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，请参阅第 4-15 页的*关于安全配置*。

添加时间表对象

添加时间表对象：

1. 转到**策略 > 对象 > 时间表**。
2. 单击**新增**。
3. 输入名称、开始时间和结束时间。
4. 如有必要，请单击 “添加其他时间表时间”以添加其他时间表对象。
5. 单击**确定**。
6. 验证新的时间表对象是否已添加到**策略 > 对象 > 时间表**的列表中。

编辑时间表对象

编辑时间表对象：

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 “编辑时间表对象”对话框中进行更改。
4. 单击**确定**。

移除时间表对象

从主安全配置页面中移除时间表对象：

1. 转到**策略 > 对象 > 时间表**。
2. 选中要移除的时间表对象名称前的复选框。
3. 单击 “删除”图标。

从 “编辑时间表对象”对话框中移除时间表对象：

如果在 “编辑时间表对象”对话框中时间表对象处于打开状态，请单击 “移除时间表对象”链接。

关于安全配置

每个安全策略包含一个或多个提供其他防护和控制的安全配置的规范。定义安全配置时，可以选择以下处理措施：

- **监控** — 允许应用程序网络通信并记录在安全日志中
- **阻止** — 禁止应用程序网络通信
- （仅针对入侵防御和 URL 过滤）**遵循** — 遵循入侵防御或 URL 过滤安全配置中设置的处理措施

提供的安全配置类型如下：

- *防恶意软件安全配置*
- *入侵防御安全配置*
- *Web 信誉服务安全配置*
- *URL 过滤安全配置*
- *反垃圾邮件安全配置*

重置安全配置

所有安全配置可以重置到先前保存的设置。如果您更改了安全配置，但没有单击**确定**，您可以单击**重置**来恢复先前的安全配置设置。

防火墙

下一代应用安全网关提供了现代防火墙功能，能够轻松地进行日常部署和管理。它能够阻止代价高昂的数据丢失或被盗、工作站受感染以及其他妨害生产力的事件 （例如，扫描程序、恶意代码、拒绝服务攻击和其他威胁）。该保护包含双向基于状态的检查，附有可配置对象的集中式目标策略， IPv4 和 IPv6 支持，用户和组支持以及日志和报告。

防恶意软件安全配置

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，或者仅根据文件扩展名扫描其中的一部分文件。

根据扩展名处理文件：

1. 转到**策略 > 对象 > 防恶意软件**。
2. 利用白名单、黑名单或扫描列表，按以下格式 “exe;rar;mp3” 输入文件扩展名。使用半角分号 (;) 分隔文件扩展名。
   - **白名单文件类型的扩展名：**无需扫描即允许这些文件类型。
   - **黑名单文件类型的扩展名：**文件未经扫描便已阻止。
   - **扫描列表：**这些文件类型在通过下一代应用安全网关服务器之前会先进行扫描。
3. 单击**确定**来保存您的设置。

网络入侵防护

网络入侵防护功能是下一代应用安全网关的基本功能的一部分。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和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，但仍允许管理员创建定制入侵防御规则。

入侵防御安全配置

每个安全策略可指定一个入侵防护安全配置，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。

入侵防护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利用、蠕虫病毒和恶意网络通信的攻击。此外，入侵防护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。

定制的安全配置可用于最大程度减少针对可信的安全区域之间网络通信的漏洞检查，还可以用于最大程度地针对从不可信区域 （如 Internet）接收的网络通信以及发送至高度敏感的目标 （如服务器群）的网络通信进行保护。

可以设置阻止或监控处理措施的类别包括：

- **杂项** — 例如， SIP Foundry sipiXtapi Buffer Overflow
- **文件传输服务** — 例如， NetTerm NetFTPF User Buffer Command 或 3Com 3CDaemon FTP server overflow
- **Web 服务** — 例如， Microsoft Windows Explorer Drag and Drop Remote Code Execution、 Microsoft IIS WebDAV Long Request Buffer Overflow 等
- **通用服务** — Microsoft SSL PCT Buffer Overflow Vulnerability、 Solaris Telnetd User Authentication Bypass Vulnerability 等
- **客户端** — 例如， Microsoft Visual Studio WMI Object Broker Unspecified Code Execution、 Microsoft Internet Explorer XMLHTTP ActiveX Control setRequestHeader Code Execution 等
- **即时通讯** — IBM Lotus Sametime Multiplexer Buffer Overflow、MSN MSNP2P Message Integer Overflow 等
- **邮件服务** — Sendmail Signal Race Vulnerability、 Microsoft Exchange SMTP Service Extended Verb Request Buffer Overflow 等

修改入侵防御策略

修改入侵防御策略：

1. 转到**策略 > 安全配置 > 入侵防御**。
2. 从 “入侵防御规则”列表中，选择要更改的类别或类别中的项目。如果需要，可使用搜索文本框查找特定的入侵防御规则。请参阅*图 4-1*。

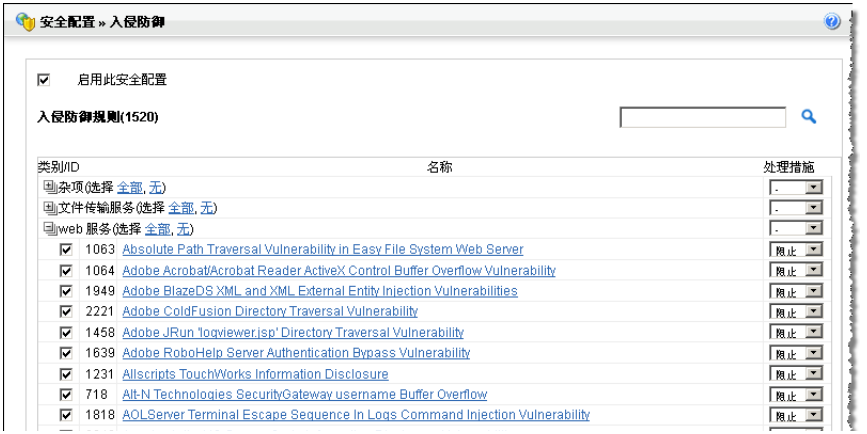


图 4-1. “策略” > “安全配置” > “入侵防御”中的入侵防御安全配置类别和操作

3. 为相应的类别或项目选择处理措施。
   a. 使用运算符来选择类别中的所有项目 （使用 “所有”）或取消选择类别中的所有项目 （使用 “无”）。
   b. 按需要展开或折叠类别。
   c. 单击某个项目的名称可获得更多相关的详细信息 （如描述）。
   d. 在项目级别或类别级别上选择处理措施 （阻止或监控）。
4. 单击**确定**。

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或提前破坏感染链来提供实时防护、节省系统扫描资源和网络带宽。 Web 信誉技术保护终端用户抵御新出现的 Web 威胁。由于 Web 信誉查询会返回 URL 类别信息 （供 URL 过滤功能使用），因此下一代应用安全网关不使用本地储存的 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 信誉以获取信誉分值，然后根据此分值是高于还是低于用户指定的敏感度等级来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），您可以在不同的防护级别 （低、中和高）执行 Web 站点扫描。

通过 Web 信誉 （如果已启用），下一代应用安全网关可提供防网络钓鱼和防域名欺诈防护。

Web 信誉服务 (WRS) 安全配置可应用于任一策略。如果您当前没有使用 Web 信誉服务，则可以安全地禁用任一 Web 信誉服务安全配置。

Web 信誉数据库驻留在远程服务器中。在用户尝试访问某一 URL 时，下一代应用安全网关会从 Web 信誉数据库中检索有关该 URL 的信息，并将其存储在本地缓存中。如果将 Web 信誉数据库存储在远程服务器上，并使用该数据库信息构建本地缓存，则可以降低下一代应用安全网关的开销并提高性能。 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。如果您认为一个 URL 的信誉被错误分类或想要了解一个 URL 的信誉，请使用下面的 URL 通知趋势科技：

http://global.sitesafety.trendmicro.com/

配置 Web 信誉服务安全配置

如果您收到太多误报或想要增强防护，则可以修改 Web 信誉服务安全配置使其更严格或更宽松。

修改 Web 信誉服务安全配置：

1. 转到**策略 > 安全配置 > Web 信誉服务**。
2. 单击相应的单选按钮 （高、中或低），以便根据公司目标设置 URL 阻止敏感度等级：
   - **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。
3. 单击**确定**。

配置 Web 信誉服务通知

下一代应用安全网关具有标准 Web 信誉服务通知。您可以通过编辑 HTML 通知消息，来更改 Web 信誉服务通知的内容。

编辑 Web 信誉服务通知：

1. 转到**策略 > 安全配置 > Web 信誉服务**。
2. 转到 **Web 信誉服务安全配置的用户通知消息**部分。
3. 单击**编辑**，并根据需要对要显示的 HTML 文本进行更改。
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**重置**以恢复为缺省消息。

URL 过滤安全配置

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”选项，您可以根据 URL 的类别（例如，“成人”、“赌博”和 “金融服务”）来设置策略。当用户请求某一 URL 时，下一代应用安全网关将首先查找该 URL 的类别，然后根据您设置的策略来允许、拒绝或监控对该 URL 的访问。也可以定义不会被过滤的已批准的 URL 列表。

URL 过滤类别组

URL 类别分为若干个 URL 过滤组，如*表 4-3* 所示。

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
通信和搜索	为在线通信和搜索提供工具和服务的 Web 站点
常规	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
生活方式	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计算机的 Internet 连接速度的 Web 站点

注意： 要使 URL 过滤能够正常工作，下一代应用安全网关必须能够向趋势科技服务发送 HTTP 请求。如果需要 HTTP 代理服务器，请通过选择**管理 > 系统设置 > 代理服务器设置**选项卡来配置代理服务器设置。

URL 过滤类别

下面的*表 4-4* 列出了各个 URL 过滤类别的定义以及所分配的组。

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
成人	非法/可疑	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）

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
成人	格调低下的内容	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	为以竞购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
商业	求职/职位	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购站点
通信和搜索	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
通信和搜索	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

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
通信和搜索	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
通信和搜索	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
通信和搜索	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
通信和搜索	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
通信和搜索	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
通信和搜索	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站点
通信和搜索	Web 托管	提供顶级域或 Web 托管服务的组织站点
常规	计算机/ Internet	有关计算机、 Internet 或相关技术的站点，包括销售或审查电子设备的站点
常规	教育	学校站点、远程教育站点和其他与教育相关的站点
常规	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
常规	健康	有关健康、瘦身或养生的站点
常规	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
常规	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

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
常规	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
常规	参考	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
常规	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）
常规	未经测试的	尚未分类为任一类别的站点
常规	汽车	与机动交通工具 （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	广告程序	含有显示广告或其他宣传内容的下载项的站点；包括安装浏览器辅助对象 (BHO) 的站点
网络安全	Cookie	向访问的 Web 浏览器发送恶意跟踪 cookie 的站点
网络安全	拨号程序	含有未经用户同意拨号至其他网络或优惠费率电话号码的下载项的站点
网络安全	恶意站点	直接或间接促进恶意软件或源代码传播的站点
网络安全	黑客	为绕过计算机安全系统提供可下载软件的站点
网络安全	恶作剧程序	提供可下载的 “恶作剧”软件 （包括可能会对用户造成扰乱的应用程序）的站点
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	恶意软件释放器	恶意程序使用的站点，包括用于托管升级或存储窃取资料的站点

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
网络安全	密码破解	分发密码破解软件的站点
网络安全	网络钓鱼	模仿合法站点以收集敏感信息（如用户名和密码）的欺诈性站点
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	远程访问程序	为远程监控和控制计算机提供工具的站点
网络安全	垃圾邮件	地址出现在垃圾邮件中的站点
网络安全	间谍软件	从毫无戒心的用户的计算机收集和传输数据的下载站点
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
生活方式	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
生活方式	另类杂志	超市海报和其他附加出版物的在线替代品
生活方式	艺术	有关视觉艺术（如绘画和雕塑）的站点
生活方式	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
生活方式	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
生活方式	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

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
生活方式	儿童	专为儿童设计的站点
生活方式	游戏	有关棋盘游戏、纸牌游戏、主机游戏或计算机游戏的站点；包括销售游戏或相关商品的站点
生活方式	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
生活方式	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
生活方式	笑话	笑话站点
生活方式	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
生活方式	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
生活方式	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
生活方式	宗教	有关民间宗教、宗教习俗或祈祷场所的站点
生活方式	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
生活方式	社交/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
生活方式	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
生活方式	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

表 4-4. URL 过滤类别定义（续）

类别组	类别类型	类别定义
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/移动电话下载内容	为移动设备提供内容（如铃声、游戏或视频）的站点
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

配置 URL 过滤安全配置

配置 URL 过滤安全配置：

1. 转到“策略”>“安全配置”>“URL 过滤”。
2. 单击**添加/编辑安全配置**选项卡。
3. 单击**新增**。
4. 输入 URL 过滤安全配置的“名称”和“描述”（可选）。

5. 执行下列操作之一：
   - 要对一组类别配置处理措施，请单击类别名称旁边的**全部**。
   - 要对某个特定类别配置处理措施，请展开相应的组 （例如 “成人”），然后找到该类别 （例如 “赌博”）。请参阅*图 4-2*。

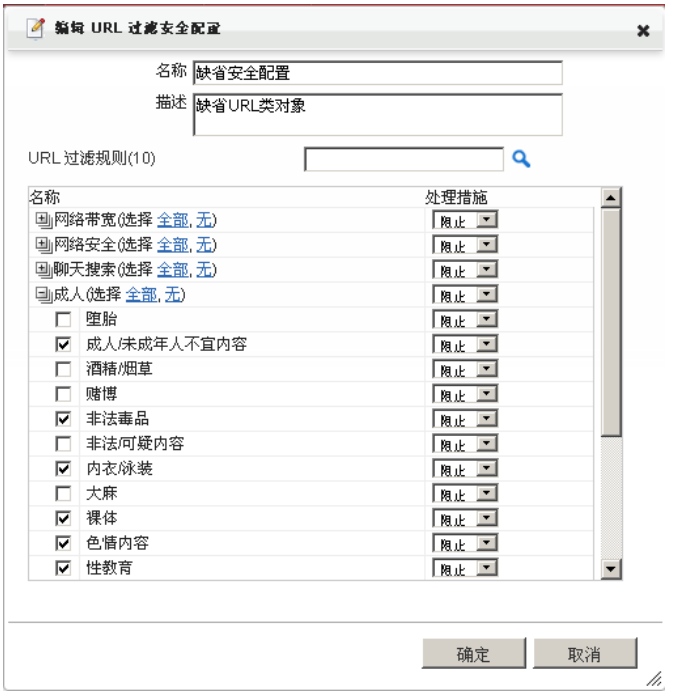


图 4-2. 用于限制赌博 Web 站点的 URL 过滤安全配置

6. 选择要执行的处理措施/行为 （阻止或监控）。
   - **阻止**处理措施不允许访问类别或规则中的 Web 站点。下一代应用安全网关会记录访问尝试。
   - **监控**处理措施允许访问符合指定条件的 Web 站点，但下一代应用安全网关会记录访问情况。

7. 单击**确定**。
8. 验证该规则是否已在**策略 > 规则 > 新增 > 安全配置**中创建。当在 “URL 过滤安全配置”列中访问下拉列表时，会显示新规则。

修改 URL 过滤安全配置

修改 URL 过滤安全配置：

1. 转到**策略 > 安全配置 > URL 过滤**。
2. 单击要修改的 URL 过滤安全配置的**名称**。
3. 在**编辑 URL 过滤**对话框中进行更改。
4. 单击**确定**。

删除 URL 过滤安全配置

删除 URL 过滤安全配置：

1. 转到**策略 > 安全配置 > URL 过滤**。
2. 选中要移除的 URL 过滤策略的**名称**旁边的复选框。
3. 单击**删除**图标。
4. 单击**确定**以确认移除。

配置 URL 过滤通知

下一代应用安全网关具有标准 URL 过滤通知。您可以通过编辑 HTML 通知消息，来更改 URL 过滤通知的内容。

编辑 URL 过滤通知：

1. 转到**策略 > 安全配置 > URL 过滤 > 常规**选项卡。
2. 单击**编辑**，并根据需要对要显示的 HTML 文本进行更改。
3. 单击**预览**以查看所做的更改。
4. 单击**确定**以保存更改，或单击**重置**以恢复为缺省消息。

电子邮件扫描

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。

反垃圾邮件检测

下一代应用安全网关使用电子邮件信誉服务 (ERS) 集成来检测反垃圾邮件。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，可用于基于内容的反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) 技术来为您提供最强的防护。 ER 技术可让您根据源 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。

注意： 为了使电子邮件信誉服务能够正常工作，入站 SMTP 网络通信的所有地址转换都必须在网络通信通过下一代应用安全网关之后进行。如果在入站 SMTP 网络通信到达下一代应用安全网关之前执行 NAT 或 PAT 操作，则下一代应用安全网关会始终将本地地址视为原始 MTA。 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 连接之前对其进行转换。

- 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 ER 将 “标记”此连接，并且下一代应用安全网关将根据您选择的设置执行相应操作。

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。如果您不打算使用反垃圾邮件扫描，则可以安全地禁用此安全配置。

反垃圾邮件使用电子邮件信誉（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 Zombie 和僵尸网络首次出现时将其停止。

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，才能在策略中使用它。

启用反垃圾邮件安全配置：

1. 转到**策略 > 安全配置 > 反垃圾邮件**。
2. 要启用反垃圾邮件安全配置，请选中“启用此安全配置”复选框。
3. 要禁用反垃圾邮件安全配置，请取消选中“启用此安全配置”复选框。
4. 单击“确定”。

修改反垃圾邮件安全配置

可以修改缺省反垃圾邮件安全配置处理措施以使用缺省智能处理措施或指定 SMTP 错误代码。

修改反垃圾邮件安全配置：

1. 转到**策略 > 安全配置 > 反垃圾邮件**。
2. 选择合适的单选按钮：
   - **智能处理措施**（缺省）— 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. 单击**确定**。

关于 URL 黑/白名单

通过 URL 白名单和黑名单，您可以覆盖已定义的 URL 过滤类别和入侵防御、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
- 允许列表的优先级高于阻止列表
- 白名单和黑名单不支持 “https://” 类的 URL

将 URL 添加到允许或阻止列表

将 URL 添加到允许列表或阻止列表：

1. 转到**策略 > 黑/白名单**。
2. 选择**加入白名单**选项卡以添加允许的 URL。

   注意： 预先审批 Web 站点的工作必须慎之又慎。如果不扫描或阻止某个 Web 站点可能会带来安全风险。

3. 选择**加入黑名单**选项卡以阻止要禁止的 URL。
4. 在文本框中输入相应的字符串。
   - 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`**

   注意： 请使用逗号或分号分隔多个条目。

5. 单击**确定**。

启用/禁用白名单或黑名单

启用/禁用白名单或黑名单：

1. 转到**策略 > 黑/白名单**。
2. 单击要启用或禁用的名单的选项卡，即**加入白名单的 URL** 或**加入黑名单的 URL**。
3. 要启用名单，请单击**启用**图标 （不是 “启用日志”图标）直至该图标显示**绿色 （打开）**。
4. 要禁用名单，请单击**启用**图标直至该图标显示**红色 （关闭）**。
5. 单击 “确定”，然后单击 “确定”以进行确认。

用户识别策略

缺省情况下，下一代应用安全网关只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。

用户识别代理是一个安装在网络中的下一代应用安全网关应用程序，可用于获取所需的 IP 地址和网络用户映射信息。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。

管理员可以配置特定的 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从域控制器检索登录日志信息，这样就可以将用户映射到 IP 地址。如果此操作失败，下一代应用安全网关会直接连接到客户端计算机 （即尝试访问网络外部某个位置的计算机）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整个 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” > “用户 ID 设置” > “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，请参阅第 4-36 页的*关于网页认证*。

添加或编辑用户 ID 策略

添加或编辑用户识别策略：

1. 转到**策略 > 用户 ID 设置 > 用户 ID 规则**。
2. 单击**新增**。
3. 在**名称**文本框中键入用户 ID 策略名称。
4. 将名称与**地址对象相关联**。使用过滤选项可以减少与该名称关联的选项。
5. 选中下面一个或多个选项：
   - **网页认证**
   - **透明认证**
6. 单击**保存**。
7. 验证该名称是否显示在**策略 > 用户 ID 规则 > 用户 ID 设置**的用户 ID 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。

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 页面提示用户输入用户名和密码。

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向 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本地缓存，并在使用期限 (TTL) 生命周期内保留在该缓存中。如果认证失败，下一代应用安全网关会通知用户认证不成功。

通过 下一代应用安全网关，管理员可以设计和创建用户在登录时所看到的文本。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 (URL)

配置网页认证设置

网页认证登录页面为管理员提供了一个要求所有用户先输入用户名和密码（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。

配置网页认证设置：

1. 转到**策略 > 用户 ID 设置 > 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。该图像不能超过 700 x 200 像素，且大小不能超过 1 MB。单击**上传**以上传该图像。
3. 添加合适的**公司名称**。
4. （可选）定制**欢迎消息**。
5. （可选）将外部 HTTP 链接添加到公司 Web 站点。
6. 单击**预览**以显示您的消息并进行验证。
7. 关闭显示预览的选项卡。
8. 如果满意，则单击**应用**，否则单击**重置**以恢复为缺省值。

第 5 章

报告

本章包含以下信息：

- 第 5-2 页的***实时监控摘要报表***
- 第 5-27 页的***报告***
- 第 5-31 页的***报告类型***

实时监控摘要报表

下一代应用安全网关使用小组件框架来实现实时监控，以便管理员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下表中的通信状态、系统信息和安全状态小组件。

表 5-1. 实时监控小组件

小组件	刷新时间间隔	描述
通信状态小组件		
会话摘要 （缺省情况下显示）	随显示的时间而不同。 “过去 5 分钟”时间设置每 10 秒钟刷新一次。 所有其他的时间设置每 5 分钟刷新一次。	该小组件显示系统的 TCP/UDP 会话状态。显示的时间段可以显示过去一小时、一天、一周或一个月的信息。 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。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。

表 5-1. 实时监控小组件 （续）

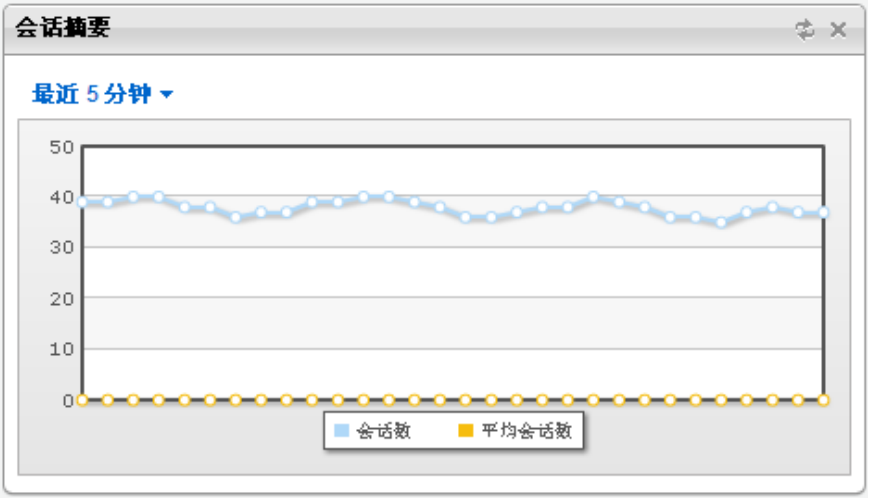
小组件	刷新时间间隔	描述
		
用户排名 （缺省情况下显示）	5 分钟	该小组件显示使用网络的用户排名。显示的时间段可以显示过去一小时、一天、一周或一个月的信息。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。 缺省情况下以表格样式进行显示，但可以切换成以表格格式进行显示。如果您扩大用户数据，则会显示最常使用的应用程序。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件 （续）

小组件	刷新时间间隔	描述
		
最常使用的应用程序 （缺省情况下显示）	5 分钟	该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 2:08 pm，则该数据为 1:08 pm - 2:08 pm 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。要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件 （续）

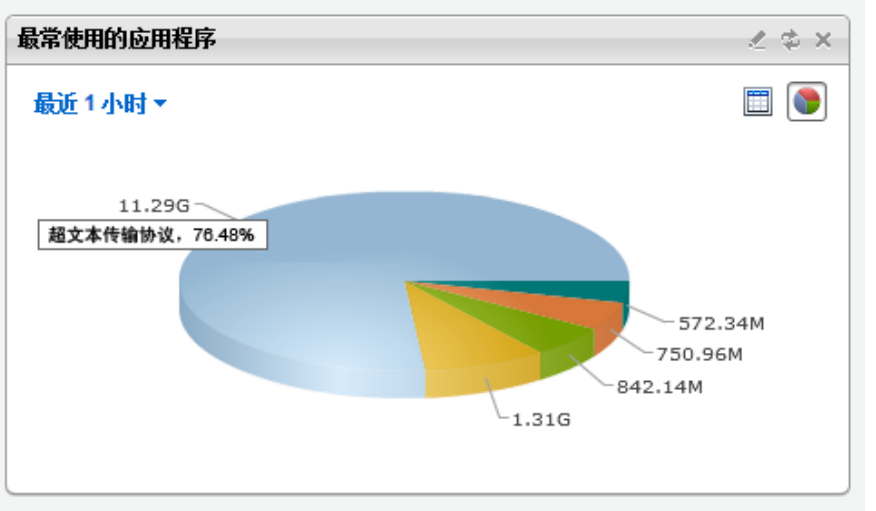
小组件	刷新时间间隔	描述
		
		

表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
带宽摘要 （缺省情况下显示）	随显示的时间而不同。 “过去 5 分钟”时间设置每 10 秒钟刷新一次。 所有其他的时间设置每 5 分钟刷新一次。	该小组件根据 IP 地址显示带宽传入/传出信息。将鼠标放在彩色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。 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。 对于带宽摘要小组件，传入/传出网络通信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” > “部署” > “内部地址”中进行配置。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。



表 5-1. 实时监控小组件（续）

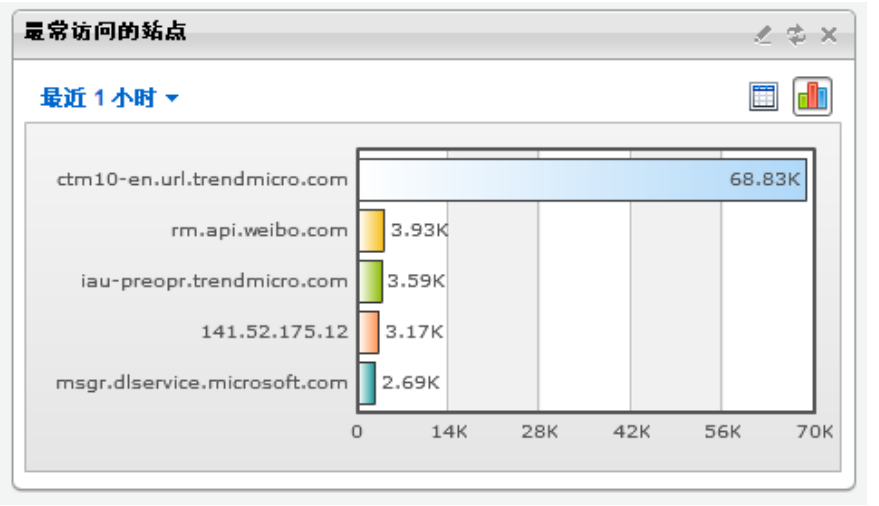
小组件	刷新时间间隔	描述
最常访问的站点	5 分钟	该小组件显示最常访问的域的信息。可配置显示的域的数量。缺省情况下显示前 5 个。同样，可以显示最近一小时、一天、一周或一月的信息。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。 缺省情况下以条形图样式进行显示，但可以转换成以表格格式进行显示。 要配置将显示多少源，请单击“刷新”图标旁边的“编辑”图标，然后在弹出窗口中设置所需的值。
		

表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
最常访问的 URL 类别	5 分钟	该小组件显示与 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。 同样，可以显示最近一小时、一天、一周或一月的信息。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。 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。 要配置将显示多少源，请单击“刷新”图标旁边的“编辑”图标，然后在弹出窗口中设置所需的值。



表 5-1. 实时监控小组件 （续）

小组件	刷新时间间隔	描述
系统信息小组件		
接口信息 （缺省情况下显示）	5 分钟	该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。 单击**编辑**以转至**网络 > 接口**页面，然后对接口进行更改。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。



表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
系统信息 （缺省情况下显示）	5 分钟	该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。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。 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**。



表 5-1.　实时监控小组件 （续）

小组件	刷新时间间隔	描述
系统资源 （缺省情况下显示）	10 秒	系统资源使用信息为接近实时的信息。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。

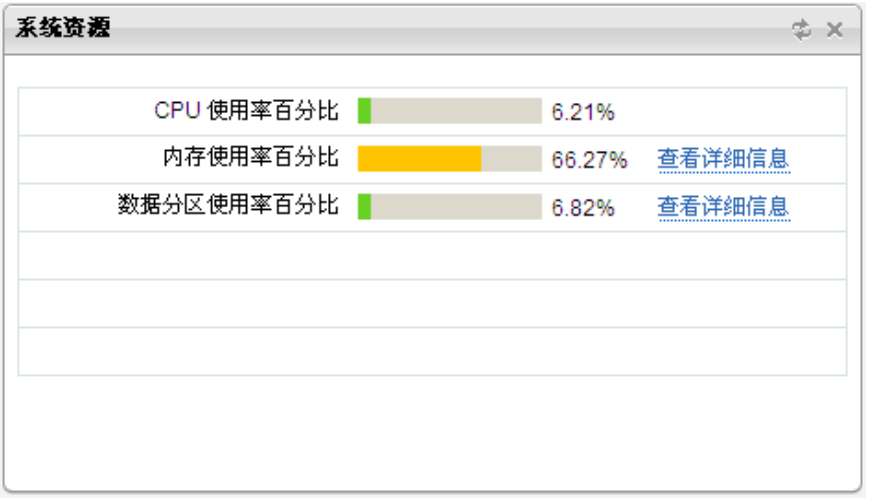


表 5-1. 实时监控小组件 （续）

小组件	刷新时间间隔	描述
网络信息 （缺省情况下显示）	5 分钟	该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。 单击**编辑**图标更改测试域地址。 **注意：** 默认情况下，该测试域是趋势科技域：`ctm10-en.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”，但事实上仍处于连接状态。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。

表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
		
		

表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
特征码信息	5 分钟	该小组件显示系统特征码版本信息。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。
		
硬件监控程序	5 分钟	此小组件显示硬件监控信息。 用户可以通过单击小组件右上角的**刷新**图标来手动刷新数据。 当发生一些特定事件时，系统会生成一封电子邮件发送给系统管理员。可以在以下位置配置系统管理员：管理 > 通知 > SMTP 设置。有关具体的配置参数的更多电子邮件通知，请转至 “管理” > “通知” > “通知事件”选项卡 > “硬件监控”链接。

表 5-1.　实时监控小组件 （续）

小组件	刷新时间间隔	描述
		
安全状态小组件		
安全事件状态 （缺省情况下显示）	5 分钟	该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。同样，可以显示最近一小时、一天、一周或一月的信息。 用户可以通过单击 “编辑” 图标来配置要显示的信息。在弹出窗口中，选中相应的复选框。 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。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件（续）

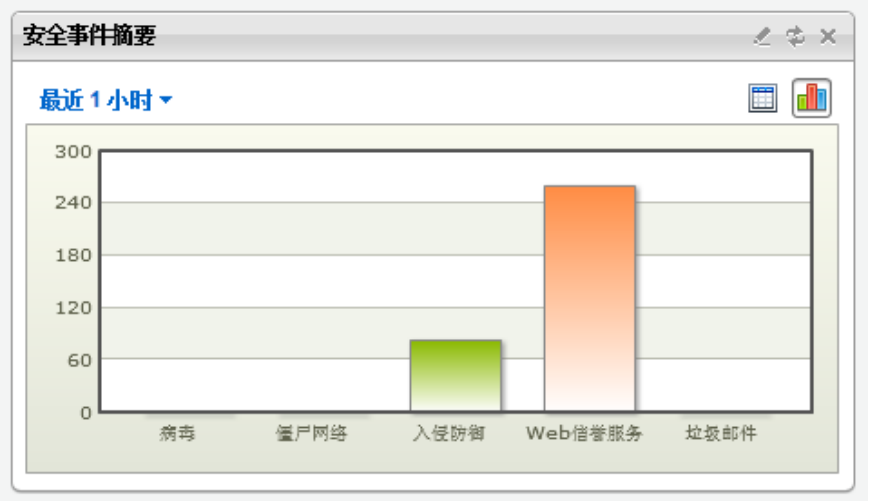
小组件	刷新时间间隔	描述
		

表 5-1. 实时监控小组件 （续）

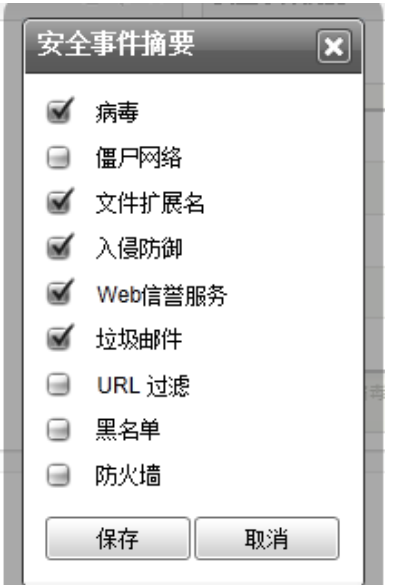
小组件	刷新时间间隔	描述
		
会话事件摘要 （缺省情况下显示）	随显示的时间而不同。 “过去 5 分钟”时间设置每 10 秒钟刷新一次。 所有其他的时间设置每 5 分钟刷新一次。	“会话事件摘要”显示了指定时间段内发生的会话信息，包括允许、阻止或检查的会话数。该时间段可以为过去 5 分钟、1 小时、1 天、7 天或 30 天。小组件自动刷新。 用户可通过单击小组件右上角的**刷新**图标来手动刷新数据。单击图表下方图例中的 “允许”、“阻止”或 “检查”图标会切换显示的信息。

表 5-1. 实时监控小组件 （续）

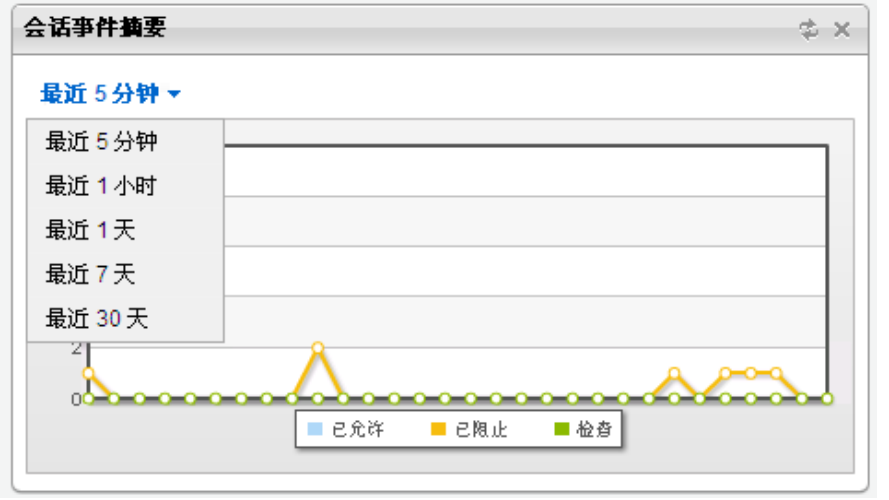
小组件	刷新时间间隔	描述
		
Web 信誉服务保护的设备排名 （缺省情况下显示）	5 分钟	小组件显示与 Web 信誉服务 (WRS) 相关的违例。同样，可以显示最近一小时、一天、一周或一月的信息。 缺省情况下以表格样式进行显示，但可以通过图标转换成以条形图格式进行显示。 如果用户信息可用 （如果已将 IP 地址映射到用户），则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1.　实时监控小组件 （续）

小组件	刷新时间间隔	描述
		
防病毒保护的设备排名 （缺省情况下显示）	5 分钟	该小组件显示与病毒相关的违例信息。同样，可以显示最近一小时、一天、一周或一月的信息。 缺省情况下以表格样式进行显示。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。 要配置将显示多少源，请单击 “刷新”图标旁边的 “编辑”图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件 （续）

小组件	刷新时间间隔	描述
		
设备风险摘要	5 分钟	小组件显示具有安全信息汇总的设备排名。可配置显示的设备数量。缺省情况下显示前 5 个。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 缺省情况下以表格样式进行显示，但单击提供的图标会以条形图样式呈现信息。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。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1.　实时监控小组件 （续）

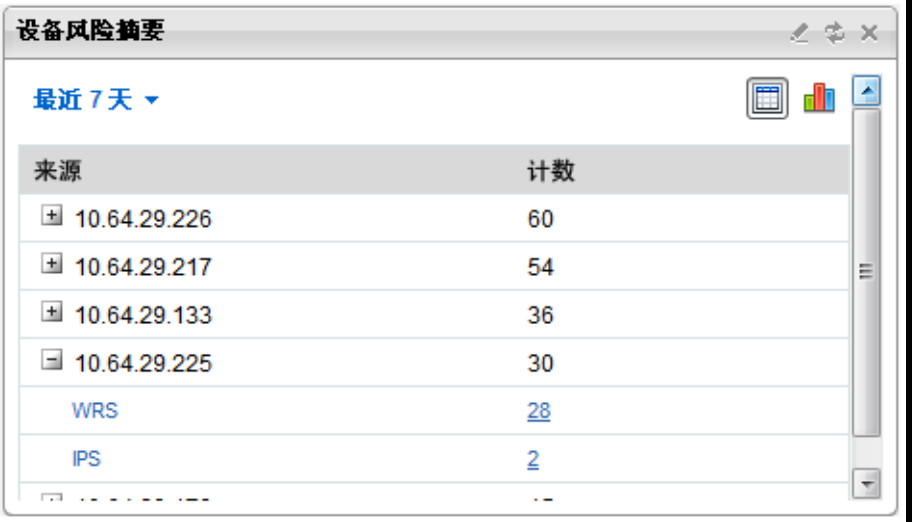
小组件	刷新时间间隔	描述
		
反僵尸网络保护的设备排名	5 分钟	该小组件显示与僵尸网络违例相关的最大在线用户数。可配置显示的设备数量。缺省情况下显示前 5 个。用户可以设置其他数值，如前 10。同样，可以显示最近一小时、一天、一周或一月的信息。 缺省情况下以表格样式进行显示，但单击提供的图标会以条形图样式呈现信息。如果用户信息可用（如果已将 IP 地址映射到用户），则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件（续）

小组件	刷新时间间隔	描述
表格样式  		

表 5-1. 实时监控小组件 （续）

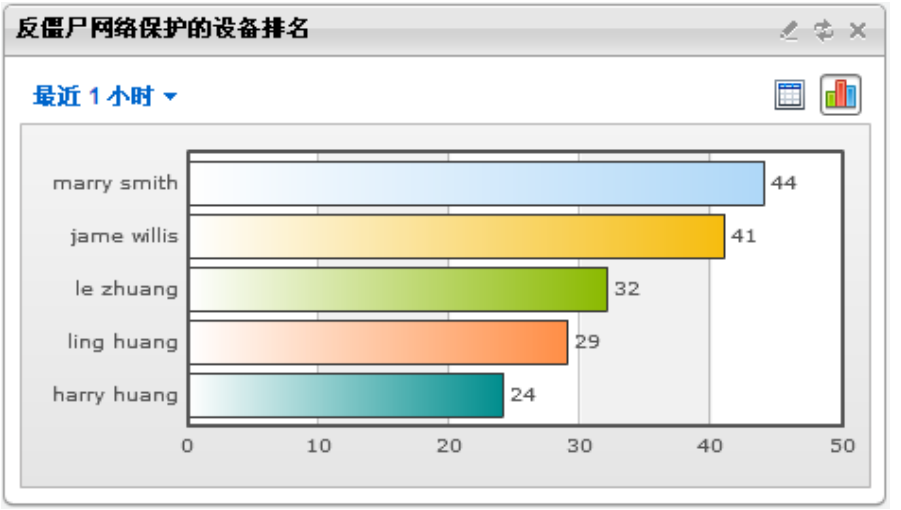
小组件	刷新时间间隔	描述
图表样式  		
入侵防御保护的设备排名	5 分钟	该小组件显示与入侵防御相关的信息。缺省情况下以表格样式进行显示。如果用户信息可用 （如果已将 IP 地址映射到用户），则该小组件会将源列显示为用户。如果 IP 地址未映射，则会显示源 IP 地址。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1. 实时监控小组件 （续）

小组件	刷新时间间隔	描述
		
反垃圾邮件保护的设备排名		该小组件显示与垃圾邮件相关的违例。 同样，可以显示最近一小时、一天、一周或一月的信息。 缺省情况下以表格样式进行显示。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。 要配置将显示多少源，请单击 “刷新” 图标旁边的 “编辑” 图标，然后在弹出窗口中设置所需的值。

表 5-1.　实时监控小组件 （续）

小组件	刷新时间间隔	描述
		

注意： 下一代应用安全网关不支持小组件定制。有关添加小组件的更多信息，请参阅第 1-8 页的*添加新小组件*。

安全状态

安全状态小组件按以下类别显示过去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、垃圾邮件和加入黑名单的 URL。将鼠标放在每个类别的条形图上，便可提供确切的违例计数。

安全状态小组件包括：

- 安全事件摘要 （缺省）
- 会话事件摘要 （缺省）
- Web 信誉服务保护的设备排名 （缺省）
- 防病毒保护的设备排名 （缺省）
- 设备风险摘要
- 反僵尸网络保护的设备排名
- 入侵防御保护的设备排名
- 反垃圾邮件保护的设备排名

通信状态

应用程序通信状态页面包含五个小组件：

- 带宽摘要 （缺省）
- 会话摘要 （缺省）
- 用户排名 （缺省）
- 最常使用的应用程序 （缺省）
- 最常访问的站点
- 最常访问的 URL 类别

系统信息

系统信息类别包含五个小组件：

- 系统信息 （缺省）
- 系统资源 （缺省）
- 网络信息 （缺省）
- 接口信息 （缺省）
- 特征码信息
- 硬件监控

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。您可以使用此下一代应用安全网关程序事件信息来优化程序设置，并对组织的安全策略进行微调。

下一代应用安全网关让您可以针对访问 Internet 的客户端生成预设报告或即时报表。报告生成后，即可打印。

关于即时报表

下一代应用安全网关允许您按需 （近乎实时）生成有关安全事件、违例用户和用户网络通信的报告。

生成即时报表

配置并生成即时报表：

1. 单击**日志和报告 > 报告 > 即时报表**。
2. 选择以下选项之一：
   - **时间周期：**今天、最近 7 天或最近 30 天
   - **定制范围：**选择开始、结束日期和时间

3. 在**报告类型**下，从**安全事件**、**用户违例排名**（以及要包括的编号）和**网络通信排名**（以及要包括的编号）中选择要包括的报告。
4. 单击**生成报告**。
5. 如果需要，可打印生成的报告。

预设报告

您可以配置下一代应用安全网关使其可以按每日、每周、每月定期生成预设报告。报告基于存储在数据库中的日志数据。

报告模板

使用报告模板创建可以按预设间隔定期生成的报告。报告模板中定义的参数确定将在生成的报告中显示的数据的范围和数量。预设一个报告后，您可以将该报告添加到日、周或月报表中保存的报告。

创建预设报告模板

创建预设报告模板：

1. 转到**日志和报告 > 报告 > 报告模板**。
2. 单击**添加**。
3. 键入报告**名称**。
4. 选择要包含在模板中的报告。
5. 单击**应用**。
6. 验证新报告显示在**日志和报告 > 报告 > 报告模板**的报告列表中。

创建预设报告

预设报告可以每天、每周或每月运行一次。

创建预设报告：

1. 转到“日志和报告”>“报告”。
2. 选择**日报表**、**周报表**或**月报表**。
3. 单击**预设报告**选项卡。
4. 单击“添加”。
5. 为报告命名。
6. 配置开始时间。
7. 选择要使用的模板。（有关更多信息，请参阅第 5-28 页的***创建预设报告模板***。）
8. 单击“确定”。
9. 验证新报告在**日志和报告 > 报告 > 日、周或月报表**中存在。

删除预设报告

删除预设报告：

1. 转到**日志和报告 > 报告**。
2. 转到日、周或月报表。
3. 选中要删除的报告名称对应的复选框。
4. 单击**删除**图标。
5. 单击**删除**来确认并删除预设报告。
6. 验证预设报告在**日志和报告 > 报告 > 日、周或月报表 > 预设报告**选项卡中不再存在。

查看保存的报告

查看保存的报告：

1. 转到**日志和报告 > 报告**。
2. 选择**每日**、**每周**或**每月**报告。
3. 单击**保存的报告**选项卡。

删除保存的预设报告

在“日志和报告”>“报告”>“报告设置”中配置保存预设报告的天数。

删除现有保存的预设报告：

1. 转到**日志和报告 > 报告**。
2. 转到日、周或月报表。
3. 单击**保存的报告**选项卡。
4. 选中要删除的已保存报告的复选框。
5. 单击**删除**图标。
6. 单击**删除**来确认并删除保存的报告。
7. 验证新保存的报告在**日志和报告 > 报告 > 日、周或月报表 > 保存的报告**选项卡中不再存在。

报告设置

可以为每日、每周和每月的预设报告配置清除报告前保存的报告数量。同时，所有预设报告均有清除选项。

配置报告设置

配置报告设置：

1. 转到**日志和报告 > 报告 > 报告设置**。
2. 为以下预设报告设置保存的天数：
   - 日报表 （缺省值为 60 天）
   - 周报表 （缺省值为 20 周）
   - 月报表 （缺省值为 4 个月）
3. 单击**应用**。

清除保存的预设报告

清除全部或部分保存的预设报告：

1. 转到**日志和报告 > 报告 > 报告设置**。
2. 将要清除的报告类型 （每日、每周、每月或全部）的值设为 0。
3. 执行下列操作之一：
   - 单击**清除**立即清除报告。在确认窗口中，单击**确定**。
   - 单击**应用**根据设置在缺省时间 （凌晨 3 点）清除报告。
4. 转到**日志和报告 > 报告 > 日、周或月报表 > 保存的报告**。
5. 验证保存的预设报告是否已清除。

报告类型

下一代应用安全网关有三种可用的报告类型：

- *安全事件报告*
- *前 N 个违例用户报告*
- *前 N 个网络通信报告*

安全事件报告

安全事件报告包括：

- 安全摘要
- 违例 （按 URL 类别）
- 违例 （按防恶意软件）
- 违例 （按垃圾邮件）
- 违例 （按入侵防御）
- 违例 （按 Web 信誉服务）

前 N 个违例用户报告

下一代应用安全网关允许您指定在不同报告中显示的记录数量。例如，您可以配置“最多违例 （按用户）” Web 安全报告中要列出的用户数量。所有报告的缺省记录数量为 10 个，报告记录允许的最大数量为 99 个。

前 N 个违例用户报告 （按计数）包括：

- 最多违例 （按用户）
- 最多防火墙违例 （按用户）
- 最多 URL 过滤违例 （按用户）
- 最多防恶意软件违例 （按用户）
- 最多入侵防御违例 （按用户）
- 最多 Web 信誉服务违例 （按用户）

前 N 个网络通信报告

下一代应用安全网关允许您指定在不同报告中显示的记录数量。例如，您可以配置“按用户的最多带宽” Web 网络通信报告中要列出的用户数量。所有报告的缺省记录数量为 10 个，报告记录允许的最大数量为 99 个。

前 N 个网络通信报告 （按计数）包括：

- 带宽 （按应用程序）
- URL 类别
- 带宽 （按用户）
- URL 类别 （按用户）

第 6 章

日志

本章包含以下信息：

- 第 6-2 页的*日志简介*
- 第 6-2 页的*日志设置*
- 第 6-3 页的*日志查询*
- 第 6-6 页的*日志类型*

日志简介

安装并配置下一代应用安全网关之后，将根据您为每种风险类型选择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。

提供的日志包括：

- 第 6-6 页的*安全日志*
- 第 6-7 页的*流量日志*
- 第 6-8 页的*VPN 日志*
- 第 6-8 页的*系统事件日志*
- 第 6-9 页的*审计日志*

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。

日志设置

转到 “日志和报告” > “日志设置” 以配置适用于所有日志的全局设置。其中包括：

- 日志选项：选择要记录的安全配置，并启用网络通信统计日志记录
- 日志管理：x 天后清除日志
- 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

配置全局日志设置：

1. 转到**日志和报告 > 日志设置**。
2. 在 “日志选项” 下，选中要记录的安全类型的复选框。

注意： 启用安全日志可获得有关网络通信活动或用于疑难解答的其他信息。禁用日志可能会提高性能。

3. 选中 “启用网络通信统计”复选框可启用网络通信统计日志记录。

注意： 打开流量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长时间保存。

4. 如果需要，更改日志清除之前的保留天数值。

注意： 将清除值设为少于 62 天可能会阻止生成月报表。将值设为超过 62 天可能会导致累积数据过大以致影响性能。

5. 如果需要，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。
6. 输入将系统日志转发到的服务器 IP 地址和端口号。
7. 单击**应用**。

日志查询

下一代应用安全网关提供的日志会记录配置更改、系统事件、安全威胁和网络通信流。除了流量日志外，缺省情况下，下一代应用安全网关还会在本地保存所有日志。对于系统日志，您可以启用日志转发。

查询日志

以下过程说明了查询日志的一般流程。有关每种日志类型的具体信息，请参阅：

- 第 6-4 页的*查询安全日志*
- 第 6-5 页的*查询流量日志*
- 第 6-5 页的*查询 VPN 日志*
- 第 6-5 页的*查询系统事件日志*
- 第 6-6 页的*查询审计日志*

查询日志：

1. 转到**日志和报告 > 日志查询**。
2. 选择以下要查询的日志之一：
   - 安全日志
   - 流量日志
   - VPN 日志
   - 系统事件日志
   - 审计日志
3. 选择用于过滤日志的**时间周期**或**定制范围**。
4. 为需要查询的特定日志选择所需参数。
5. 单击**查询**、**打印**或**导出为 CSV 格式**。

查询安全日志

查询安全日志：

1. 转到**日志和报告 > 日志查询**。
2. 单击**安全日志**。
3. 选择用于过滤日志的**时间周期**或**定制范围**。
4. 输入以下参数：
   - **源地址：**作为违例源的 IP 地址。
   - **目标地址：**作为违例目标的 IP 地址。
   - **源用户：**用户名或组名。
   - **操作：**选择**全部**或者**允许**、**阻止**或**监控**来跟踪特定处理措施。
   - **策略：**选择**全部**或某个特定策略名称来跟踪该策略。
   - **应用程序：**选择**全部**或某个特定应用程序名称来跟踪该应用程序。
   - **安全配置：**选择**全部**或防火墙、入侵防御、防恶意软件、 Web 信誉服务、 URL 过滤、防垃圾邮件或黑名单来跟踪特定的安全配置。
5. 单击**查询**、**打印**或**导出为 CSV 格式**。

查询流量日志

查询流量日志：

1. 转到**日志和报告 > 日志查询**。
2. 单击**安全日志**。
3. 选择用于过滤日志的**时间周期**或**定制范围**。
4. 输入以下参数：
   - **源地址**：作为网络通信源的 IP 地址。
   - **目标地址**：作为网络通信目标的 IP 地址。
   - **源用户**：用户名或组名。
   - **应用程序**：选择**全部**或某个特定应用程序名称来跟踪该应用程序。
5. 单击**查询**、**打印**或**导出为 CSV 格式**。

查询 VPN 日志

查询 VPN 日志：

1. 转到**日志和报告 > 日志查询**。
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. 键入 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**。

查询系统事件日志

开始该过程前，请先验证**日志和报告 > 日志设置**上已启用系统事件日志记录（系统日志）。

查询系统事件日志：

1. 转到**日志和报告 > 日志查询**。
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**。

查询审计日志

查询审计日志：

1. 转到**日志和报告 > 日志查询**。
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**选择管理员**部分右侧的 “可用管理员用户” 标题下，单击要审计的一个或多个用户对应的加号 (+)。选定的用户名将移到 “选定管理员用户” 标题下方的左侧。
5. 单击**查询**、**打印**或**导出为 CSV 格式**。

日志类型

下一代应用安全网关提供以下类型的日志：

- 第 6-6 页的*安全日志*
- 第 6-7 页的*流量日志*
- 第 6-8 页的*VPN 日志*
- 第 6-8 页的*系统事件日志*
- 第 6-9 页的*审计日志*

安全日志

日志信息包括：

- 时间戳
- 源 IP 地址
- 目标 IP 地址
- 目标端口
- 用户 ID

- 应用程序 ID
- 规则名称
- 操作
- 安全类型 （入侵防御/URL/Web 信誉服务/ERS/NCIE/防火墙）
- 查看、打印生成的日志或将其导出为 CSV 格式的能力

违例详细信息基于安全类型：

- **入侵防御**：基于入侵防御规则
- **Web 信誉服务**：基于 URL
- **URL 过滤**：基于 URL 和类别
- **ERS**：基于源发件人/垃圾邮件发件人的 IP 地址
- **防恶意软件**：基于病毒名称
- **防火墙**：基于应用程序或按照条件阻止

流量日志

流量日志包括以下信息：

- 日志时间
- 开始时间
- 结束时间
- 源
- 目标
- 应用程序
- 操作
- 详细信息

VPN 日志

用于远程访问模式的 VPN 日志包括以下信息：

- 日期、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

系统事件日志

系统事件日志包括：

- 所有下一代应用安全网关服务开始/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

UI 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

审计日志

审计日志包含以下信息：

- 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

第 7 章

管理

本章包括以下内容：

- 第 7-2 页的*概述*
- 第 7-2 页的*系统设置*
- 第 7-4 页的 *下一代应用安全网关管理*
- 第 7-6 页的*通知简介*
- 第 7-10 页的*关于 LDAP 用户识别*
- 第 7-14 页的*帐户管理*
- 第 7-16 页的*产品使用授权*
- 第 7-18 页的*维护*
- 第 7-19 页的*诊断*
- 第 7-23 页的*支持*
- 第 7-24 页的*关于下一代应用安全网关*
- 第 7-24 页的*云安全智能防护网络：基于云的服务*

概述

通过 “管理”菜单，您可以访问全局系统设置、添加和编辑管理员帐户、为管理员定义安全配置以及配置中央管理。此外，还可以定义常规管理设置，例如，超时以及对支持和使用授权信息的访问。

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

通过 “系统设置”下的 “常规”选项卡，您可以配置下一代应用安全网关主机名以及 IPv4 和 IPv6 格式的主 DNS 服务器 IP 地址和辅助 DNS 服务器 IP 地址。

时间和日期设置

通过 “时间和日期设置”选项卡，可以对以下项进行配置：

- **系统时间设置：**将系统时间设置为与 NTP 服务器同步或手动设置时间。
- **时区设置：**选择下一代应用安全网关防火墙的时区。

配置时间和日期设置

配置时间和日期设置：

1. 转到**管理 > 系统设置 > 时间和日期设置**选项卡。
2. 在 “系统时间设置”部分，您可以手动设置时间，也可以将时间与 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输入当前时间，格式如下：yyyy-mm-dd hh:hh:ss。例如：2012-01-16 13:03:28

3. 在 “时区设置”部分，可以从提供的下拉列表中选择距离您最近的大洲和城市以设置相应的时区。
4. 单击**应用**。

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。建议使用该会话超时，以防止某人从已登录下一代应用安全网关却无人参与的 PC 中使用 Web 控制台。
- **语言：**提供多种语言 （英语、简体中文和日语）以从下拉列表中选择。
- **证书：**允许您浏览并选择 SSL 证书，以便在 SSL-VPN 登录时进行验证或访问网页认证时使用。

配置 Web 控制台超时

更改下一代应用安全网关 Web 控制台会话超时值：

1. 转到**管理 > 系统设置 > 控制台设置**选项卡。
2. 根据需要，更改会话超时分钟数。
3. 从下拉列表中选择所需的语言。
4. 添加证书设置。
5. 单击**应用**。

代理服务器设置

您可以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

配置下一代应用安全网关代理服务器设置：

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. 输入 HTTP 代理服务器 IP 地址和端口号。
4. 输入服务器要求的用户名和密码。
5. 单击**应用**。

体验改善

如果您希望为趋势科技贡献系统配置信息来帮助改善该产品，请选中**加入该计划**复选框。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。

下一代应用安全网关管理

通过下一代应用安全网关管理，管理员可以配置是否能够访问特定服务 （如 SSH、 SNMP）。通过它，还可以访问下一代应用安全网关 CLI。

管理服务

可以将下一代应用安全网关管理接口配置为允许或阻止来自位于下一代应用安全网关设备之后的设备的特定类型的基于管理的服务 （或网络通信）。使用此页面可配置如何远程访问设备。

启用管理服务 （Ping、 SSH 和 SNMP）

启用管理服务可允许远程访问。通过启用 SNMP 支持 （如步骤 3 所示），用户可以使用 SNMP 管理器获取有关支持的对象的信息。

启用管理服务：

1. 转到**管理 > 管理 > 管理服务**选项卡。
2. 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。
3. 要配置 SNMP，请选中 “SNMP 设置”选项卡上的 “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。

---

4. 键入下列 SNMP 值：
   - **联系人：**键入联系人的电子邮件地址。
   - **位置：**联系人的位置，例如 “China office, IT room”。
   - **团体名称：**键入所需的团体字符串以将陷阱发送到指定目标 （缺省：public）。

注意： 设备的联系信息和位置信息均可以在 SNMP 管理器中查看。仅当输入的团体字符串是有效的 v2 团体字符串， SNMP 管理器才可以管理设备。

---

5. 验证已选中相应的复选框。
6. 单击**应用**。

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。

通知简介

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
- 更新提醒

此外，还包括一个 SMTP 设置选项卡，因为这些设置与通知有关，例如，SMTP 服务器的名称以及电子邮件的发件人和收件人。

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。

您可以配置以下通知：

- 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时间表更新

配置安全信息汇总通知

配置安全信息汇总通知：

1. 转到**管理 > 通知**。
2. 单击**趋势科技下一代应用安全网关安全信息汇总**。
3. 选中**启用**复选框以启用通知。

4. 输入下列信息：
   - **通知一次的时间间隔：**根据您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：**键入发送通知的电子邮件地址。
   - **电子邮件收件人：**键入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

配置硬件监控异常通知：

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. 输入下列信息：
   - **电子邮件发件人：**键入发送通知的电子邮件地址。
   - **电子邮件收件人：**键入将接收通知的电子邮件地址。
   - **通知一次的时间间隔：**根据您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：
     - CPU 温度
     - 环境温度
     - 主板温度
     - 风扇速度
     - CMOS 电池
     - 机箱入侵

- **阈值使用率：**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：
  - CPU 温度：80°C
  - 环境温度：40°C
  - 主板温度：40°C
  - 风扇速度：550 转/分
  - CMOS 电池：2.64v
  - 机箱入侵：0 事故

5. 单击**应用**。

配置系统资源警告通知

配置系统资源警告的通知：

1. 转到**管理 > 通知**。
2. 单击**趋势科技下一代应用安全网关系统资源警告**。
3. 选中**启用**复选框以启用通知。
4. 输入下列信息：
   - **电子邮件发件人：**键入发送通知的电子邮件地址。
   - **电子邮件收件人：**键入将接收通知的电子邮件地址。
   - **通知一次的时间间隔：**根据您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：
     - CPU 使用率百分比
     - 数据分区使用率百分比
     - 内存使用率百分比
     - 交换内存使用率百分比

- **阈值使用率**：对于每个选定的事件，选择将触发通知的阈值的百分比。缺省百分比为：
  - 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%
  - 交换内存使用率百分比 — 50%

5. 单击**应用**。

配置预设更新通知

配置预设更新的通知：

1. 转到**管理 > 通知**。
2. 单击**趋势科技下一代应用安全网关预设更新**。
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. 键入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

停止先前配置的通知：

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消息，必须指定电子邮件设置。定义电子邮件设置后，可以启用电子邮件通知，如第 7-6 页的*系统通知和警报*中所示。

配置通知的 SMTP 设置

您无法删除在系统设置、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。

配置通知的 SMTP 设置：

1. 转到**管理 > 通知 > SMTP 设置**选项卡。
2. 键入以下项的值：
   - **SMTP 服务器名称和端口号：**输入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：**输入“发件人”电子邮件地址，如“security_notification@company.com”。
   - **电子邮件收件人：**输入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. 如果您没有测试连接，则必须单击**应用**以保存新的设置。

关于 LDAP 用户识别

需要配置下一代应用安全网关识别客户端的方法以定义 HTTP 病毒扫描、URL 过滤和应用程序控制策略的作用范围。您对于用户识别方法的选择还会决定，在日志文件和报告中如何针对受影响的系统跟踪安全性事件。

下一代应用安全网关提供的用户识别方法根据 IP 地址识别客户端，然后应用相应的策略。

LDAP 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。

缺省情况下，所有的 IP 地址都不会自动用于用户识别。管理员必须定义哪一源 IP 地址或 IP 地址范围需要用于用户识别。如果源 IP 地址不在定义的范围内，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”以便用户或组策略起作用。）

对于指定的 IP 地址或 IP 地址范围，管理员可以定义的用户识别方法包括：

- 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

LDAP 集成

下一代应用安全网关支持最通用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 认证方法

LDAP 设置让管理员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

下一代应用安全网关提供 LDAP 认证的基本和高级方法来简化用户的 LDAP 配置。

基本 LDAP 认证

下一代应用安全网关为最广泛使用的 LDAP 服务提供简便的 LDAP 配置：MS Active Directory (AD)。如果管理员使用 AD，则他们可在 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。

有了该信息后，下一代应用安全网关使用 AD 自动发现工具来获得必要的信息，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 服务器的地址，自动发现工具为域确定所有的域控制器，且下一代应用安全网关选择和使用两个最快的服务器。

高级 LDAP 认证

下一代应用安全网关为熟悉 LDAP 的用户提供高级的认证模式配置。

下一代应用安全网关支持以下 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只支持先前提到的这些服务器的 “故障切换”。如果主服务器的认证失败，则下一代应用安全网关将尝试认证辅助服务器。

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针对 MS Active Directory 和 OpenLDAP 支持以下 LDAP 认证方法：

- 简单
- Kerberos

对于基本和高级模式，管理员 cab 单击 “测试连接” 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。

配置基本和高级 LDAP 认证设置

配置 LDAP 认证设置：

1. 登录下一代应用安全网关系统。
2. 转到**管理 > 系统设置**以确保 DNS 已正确配置。
3. 转到**管理 > LDAP 设置 > LDAP 服务器**选项卡。
4. 选择**基本**选项。
5. 键入**域名**、**用户名**和**密码**。
6. 如果需要，请单击**高级**选项并按需要更改。有关详细信息，请参阅第 7-12 页的*高级 LDAP 认证*。
7. 单击**测试连接**。
8. 单击**应用**。

关于 LDAP 全局设置

管理员也可以定义 CommonLDAP 的某些全局设置，如：

- **LDAP 认证缓存 TTL：**下一代应用安全网关支持两种类型：
  - **固定 TTL （初次命中）：**缺省 TTL 为 2 小时
  - **最后的活动 TTL （上一次命中）：**无缺省值
- **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 LDAP 全局设置

配置 LDAP 认证缓存 TTL 和同步时间间隔：

1. 转到**管理 > LDAP 设置 > 缓存和同步**选项卡。
2. 选择**固定**或**最后活动**选项。
3. 设置选定的 TTL 的时间。（固定 TTL 的缺省值是 2 小时。最后的活动 TTL 没有缺省值。）
4. 设置 **LDAP 同步时间间隔**。（缺省值为 24 小时）
5. 单击**刷新**对 LDAP 服务器执行手动刷新。
6. 单击**应用**来保存新的设置。

帐户管理

多个用户能够以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。如果需要遵守某些政府机构标准，则该功能可能至关重要。

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。

添加新帐户

所有用户拥有相同权限。

添加用户：

1. 转到**管理 > 帐户 > 新增**。
2. 输入用户名、密码、密码确认以及用户的可选描述。
3. 单击**确定**。

显示用户列表

显示当前用户列表：

转到**管理 > 帐户**。

修改用户描述或密码

要更改用户名，最好将用户完全删除，然后添加一个新用户。

修改用户描述或密码：

1. 转到**管理 > 帐户**。
2. 单击要修改的用户名。
3. 要更改密码，请单击**重置**，随后键入新密码并确认密码。
4. 要编辑描述，请在描述文本框中编辑文本。
5. 单击**应用**。

删除用户帐户

删除用户帐户或密码：

1. 转到**管理 > 帐户**。
2. 单击用户名所在行的“删除”图标。
3. 单击**删除**确认要删除该帐户。

产品使用授权

通过产品使用授权功能，可以注册下一代应用安全网关以及进行使用授权。完全激活下一代应用安全网关需要两个步骤。首先，您必须注册趋势科技的下一代应用安全网关。注册后，将提供有效的下一代应用安全网关激活码 (AC) 来对该产品进行使用授权。

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。

要激活下一代应用安全网关，首先需要注册码，可以在产品注册过程中要求得到该注册码。通过该注册码，您可以获得一个激活码。随后可以利用下一代应用安全网关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/

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 （购买产品后即可获得）

注册并激活下一代应用安全网关副本将授予您以下权利：

- 更新下一代应用安全网关病毒码文件和扫描引擎
- 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

注册下一代应用安全网关：

1. 在**管理 > 使用授权**中单击产品的 “趋势科技产品注册中心”链接。
2. 单击**激活您的使用授权**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**：输入您的登录 ID 和密码。
4. 在**我的产品**窗口中，单击**添加产品**并键入**注册码**。
5. 要编辑贵公司的资料，请单击**查看/编辑公司资料**。
6. 下一窗口将显示您的激活码。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人员或您的经销商。在**管理 > 产品使用授权**中单击**在线检查状态**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。

获取并输入激活码

完全版到期后，下一代应用安全网关安全更新将被禁用；评测周期到期后，安全更新与扫描功能都将被禁用。在 “产品使用授权”窗口中，可以在线获取激活码、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，需要激活码。可以通过几种方法执行此操作。

- 如果从趋势科技 Web 站点下载下一代应用安全网关，您会自动收到一个评测用的激活码。
- 可以使用注册码在线获得激活码。

激活码包含 31 个字符，格式如下：

```
xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx
```

在线获取和输入激活码：

1. 打开下一代应用安全网关控制台，然后单击**管理 > 使用授权**。
2. 通过注册下一代应用安全网关，获取激活码 （单击页面顶部的链接进行注册，然后遵照屏显提示完成操作）。
3. 单击**激活您的使用授权**链接或**输入新激活码**按钮。
4. 当系统提示时，在 “激活码”文本框中键入激活码，然后单击**下一步**。
5. 单击**完成**即已完成使用授权激活。

更新使用授权

要通过 Web 获取最新的使用授权，请转到**管理 > 使用授权**，然后单击**在线检查状态**。

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”。

- 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”（延长一年时间的防护）将通过邮件发给贵公司 “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：

  https://olr.trendmicro.com/registration/apac/zh-cn/

维护

通过 “维护”页面，可以关闭和重新启动下一代应用安全网关，并能备份和恢复配置。

系统维护

下一代应用安全网关提供的系统维护功能包括：

- **系统关闭：**停止服务、关闭计算机和关闭电源
- **系统重新启动：**停止服务并重新启动计算机
- **恢复出厂设置：**恢复设备的原始硬件设置
- **消息：**允许向日志添加有关关闭、重新启动和恢复事件的消息

关闭、重新启动或恢复下一代应用安全网关的设置：

1. 转到**管理 > 维护 > 系统维护**选项卡。
2. 选择相应选项：
   - 关闭
   - 重新启动
   - 恢复出厂设置
3. （可选）输入日志中与事件对应的消息 （最多 100 个字符）。
4. 单击**继续**。

配置备份与恢复

通过 “管理” > “维护” 上的 “备份/恢复” 选项卡，管理员可以执行以下操作：

- 为现有配置设置创建备份文件
- 从备份文件恢复配置设置

诊断

通过下一代应用安全网关的 “诊断” 部分，您可以执行以下操作：

- 运行网络数据包捕获，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

网络数据包捕获

“网络数据包捕获”向导位于 “管理” > “诊断” > “网络数据包捕获”。使用已捕获的网络数据包，管理员或支持团队可以执行网络通信调试或分析。

使用此功能，管理员可以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在命名约定为“capture-{interface}-{date:time}.pcap”的单个文件中。例如，capture-eth0-2012-02-17.1329518492.75.pcap.tar.gz 将会是 2012 年 2 月 17 日在 eth0 网络接口上执行的数据包捕获的文件名。

在完成网络数据软件包捕获之后，所有数据软件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。管理员可以下载或删除相应压缩文件。

要为您的过滤器确定一些组件，这有助于针对 HTTP 请求或响应运行数据包捕获。请参阅*图 7-1* 中的捕获示例和*表 7-1* 中的说明。

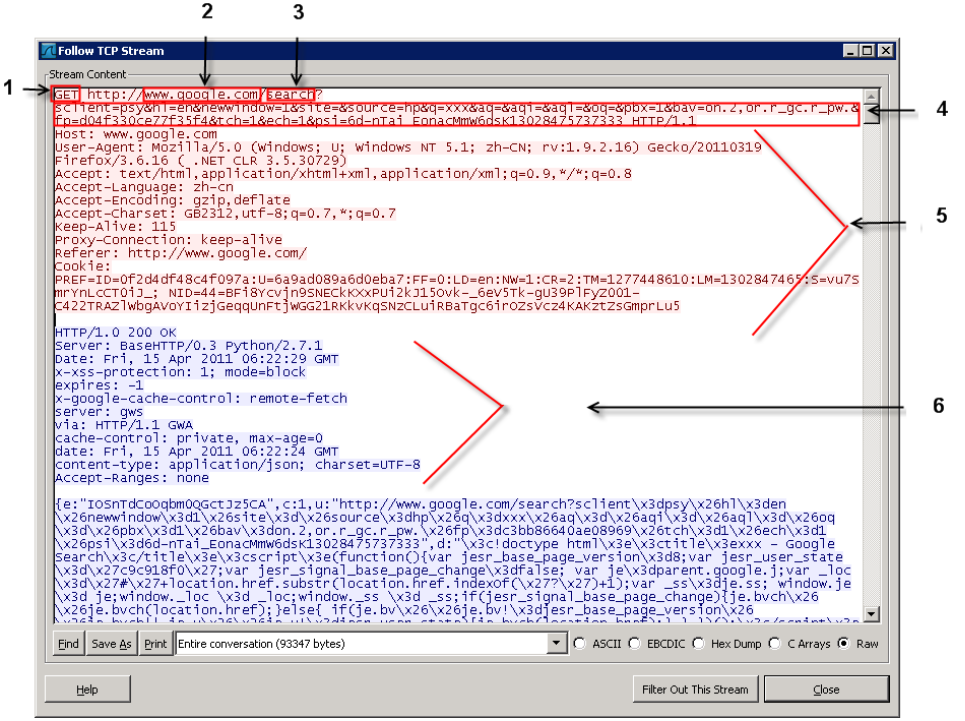


图 7-1. 用于 Google 搜索的数据包捕获

表 7-1. 数据包捕获中显示的组件

编号	组件
1	请求方法
2	URL 主机
3	URL 路径

表 7-1. 数据包捕获中显示的组件 （续）

编号	组件
4	URL 查询
5	请求标头
6	响应标头

使用网络数据包捕获

这一功能允许为选定的接口或单一的接口进行数据包捕获，管理员可以使用此功能分析网络通信。

捕获网络数据包：

1. 转到**管理 > 诊断**页面，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：
   - 指定在其上捕获数据包的 IP 地址
   - 指定在其上捕获数据包的端口
   - （可选，如果使用复选框）**捕获数据包限制** (Mb) （缺省：500Mb)
   - （可选，如果使用复选框）**捕获时间限制** （分钟）（缺省：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 500Mb 时，捕获将停止，除非在步骤 3 中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**操作**列中的**图标**，打开捕获的文件
   - 单击**删除**图标可删除选定的生成文件

通信跟踪

使用通信跟踪可生成会话详细信息，帮助管理员诊断应用程序的任何相关问题。该网络工具将确定数据包在 IP 网络上采用的路由。

跟踪网络通信：

1. 转到**管理 > 诊断 > 通信跟踪**。
2. 输入将从中跟踪网络通信的 **IP 地址**和**端口**。
3. 在 “操作”下拉菜单中，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。单击某一会话可查看该会话的详细信息。

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您的设备出现的问题。

生成诊断文件：

1. 转到**管理 > 诊断 > 诊断文件**。
2. 单击**生成诊断文件**。

支持

下一代应用安全网关 Web 控制台 “支持”页面提供了指向以下项的链接：

- **文档**：访问可搜索的联机帮助可查找有关下一代应用安全网关特定区域的信息和说明。
- **威胁百科全书**：威胁百科全书中提供了全面的安全信息。
- **知识库**：趋势科技 Web 站点上维护的趋势科技知识库提供了针对产品问题的最新解答。

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

下一代应用安全网关的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：

- **Web 信誉服务 (WRS)** 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。
  - 域信誉
  - 页面信誉
  - 电子邮件信誉
  - 文件信誉
- **URL 过滤服务**将其 URL 数据库存储在云中，用于快速更新和保护趋势科技的全局用户群，而无需在下一代应用安全网关服务器上下载和更新 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。
- **反馈循环**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。在客户内部部署的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。

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。为保证最快的响应和最少的延时，必须使用主和辅助 DNS 服务器来配置下一代应用安全网关设备。

DNS 服务器必须能够支持下一代应用安全网关做出的 DNS 请求数量。通常，在下一代应用安全网关建立本地 DNS 缓存前，将为每个被访问的 URL 进行两次 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。

该 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，以减少延迟。

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 服务器具有节流机制，会限制每秒进行的 DNS 请求的数量，并影响下一代应用安全网关的 Web 信誉服务 (WRS) 性能。

尽可能靠近下一代应用安全网关单元放置 DNS 服务器，以减少设备之间不必要的网络跃点，从而改善网络响应时间并提高性能。

在 HTTP 端口 80 上进行 Web 信誉服务和 URL 过滤请求。不要在您的防火墙上阻止这些端口的下一代应用安全网关管理 IP 地址。

第 8 章

测试和配置下一代应用安全网关

打开下一代应用安全网关控制台后，使用以下步骤验证程序是否正常运行。以下要点列出了本章中描述的测试：

- 第 8-2 页的 ***EICAR 测试文件***
- 第 8-3 页的***测试 Web 信誉***
- 第 8-4 页的***测试应用程序控制***
- 第 8-4 页的***测试 URL 过滤***

EICAR 测试文件

欧洲计算机防病毒研究所 (EICAR) 开发了一种测试病毒，可用于测试您的防病毒设备。此脚本是一个惰性文本文件。二进制特征码包含在多数防病毒产品供应商的病毒码文件中。它本质上不是病毒，并且不包含任何程序代码。

警告！ 请勿使用真实病毒来测试您的网络安全。

可以从以下 URL 之一下载 EICAR 测试病毒：

- **http://www.eicar.org/download/eicar.com.txt**

另外，通过将以下内容键入或复制到一个文本文件并将该文件命名为 `eicar.com`，也可以自行创建 EICAR 测试病毒：

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

注意： 测试之前，请清空本地浏览器缓存。如果本地浏览器缓存包含测试病毒的副本，则尝试下载文件时可能会从缓存而非从 Internet 获取该文件，且下一代应用安全网关不会检测该文件。

测试病毒扫描：

1. 登录下一代应用安全网关 Web 控制台。
2. 单击**策略 > 规则 > 新增**。
3. 键入**策略名称**和**描述**。
4. 选中**启用**和**启用日志**复选框。
5. 单击**操作**选项卡。将处理措施设置为**在进行检查的情况下允许**。单击**确定**。
6. 对于相同的策略，单击**安全配置**选项卡，将**防恶意软件安全配置**设置为**缺省安全配置**，并将 **Web 信誉服务安全配置**设置为**缺省安全配置**。
7. 单击 **URL 过滤安全配置 > 新增**。

8. 通过以下步骤，添加一个新的 URL 过滤安全配置：
   - 键入**名称**和**描述**。
   - 在 URL 过滤类别中，单击**成人**。
   - 在成人 URL 过滤规则中，单击**全部**以选择所有规则。
   - 单击**确定**。
9. 在**安全配置**选项卡中，选择新添加的 URL 过滤安全配置。
10. 单击**确定**，然后单击页面顶部的**应用**。
11. 使用测试客户端访问以下 Web 站点并下载测试病毒：
    http://www.eicar.org/download/eicar.com.txt
12. 使用测试客户端计算机访问以下 Web 站点两次：
    http://wrs21.winshipway.com
13. 使用测试客户端计算机访问以下 Web 站点两次：
    ca06-3.winshipway.com
14. 等待 30 秒，然后转到**日志和报告 > 日志查询 > 安全日志**。
15. 转到**策略 > 规则**。
16. 删除添加的策略，单击**确定**，然后单击**应用**。

测试 Web 信誉

测试下一代应用安全网关的 Web 信誉功能：

1. 打开一个 Web 浏览器，在地址文本框键入以下文本：
   `http://wr21.winshipway.com`
2. 清空本地浏览器缓存，然后重新访问相同的 URL。
   如果测试成功，您会收到一条下一代应用安全网关安全事件消息，说明：“由于其 Web 信誉分数的原因， IT 策略阻止了对以下 Web 站点的访问。”

测试应用程序控制

通过以下步骤可以修改下一代应用安全网关安全策略，以阻止最终用户访问 Google Web 站点。

测试应用程序控制：

1. 打开下一代应用安全网关控制台，然后转到**策略 > 规则**。
2. 单击**新增**链接以添加新的策略。
3. 键入**名称**。如有需要，请添加可选的**描述**。
4. 单击**应用程序**选项卡。
5. 单击**选定的**单选按钮。
6. 单击**新增**图标。
7. 键入**名称**。如有需要，请添加可选的**描述**。
8. 在应用程序类别列表中展开 **Web** 类别。
9. 选中 **"google"** 复选框，然后单击**确定**。
10. 选中您刚刚创建的应用程序名称复选框。
11. 单击**操作**选项卡。
12. 在 “操作”下拉菜单中，选择**阻止**。单击**确定**。
13. 单击**应用**。
14. 打开浏览器，尝试访问 **http://www.google.com**。
    如果测试成功，您的浏览器不会显示 Google Web 站点。

测试 URL 过滤

趋势科技推荐使用缺省设置测试 URL 过滤。

测试 URL 过滤：

1. 打开下一代应用安全网关控制台，然后转到**策略 > 规则**。
2. 单击**新增**链接以添加新的策略规则。
3. 键入**名称**。如有需要，请键入可选的**描述**。

4. 单击**操作**选项卡。
5. 在 “操作”下拉菜单中，选择**在进行检查的情况下允许**。
6. 单击**安全配置**选项卡。
7. 在 “URL 过滤安全配置”下拉菜单中，选择**新增...**。
8. 单击**新增**图标，然后为新的 URL 过滤规则键入**名称**。
9. 在 URL 过滤类别列表中，展开**通信和搜索**类别。
10. 单击**全部**以选择 “通信和搜索”类别中的所有项。
11. 单击**确定**。
12. 选择您刚刚在 “安全配置”选项卡中的 “URL 过滤安全配置”下拉菜单中创建的 URL 过滤规则。
13. 在 “URL 过滤操作/行为”列下拉菜单中，选择**使用安全配置**。单击**确定**。
14. 在 “规则”页面中，选中**新 URL 过滤规则**复选框，然后单击页面顶部的**应用**链接。
15. 打开浏览器，尝试访问 **http://www.google.com**。
16. 清空浏览器 URL 缓存，重新尝试访问 **http://www.google.com**。

    如果测试成功，浏览器会显示安全事件通知。浏览器不会显示 Google Web 站点。

附录 A

联系人信息和基于 Web 的资源

此附录提供了可优化下一代应用安全网关（下一代应用安全网关）性能并进一步协助您解决任何技术支持问题的信息。

本附录中的主题包括：

- 第 A-2 页的*联系技术支持*
- 第 A-2 页的*知识库*
- 第 A-3 页的*将可疑代码发送给趋势科技*
- 第 A-4 页的*TrendLabs*
- 第 A-4 页的*安全信息中心*
- 第 A-6 页的*TrendEdge*

联系技术支持

在中国，您可以通过电话、传真或电子邮件与趋势科技销售代表取得联系。我们的 Web 站点和电子邮件地址如下：

http://cn.trendmicro.com/cn/home/
http://cn.trendmicro.com/cn/support/techsupport/index.html
service@trendmicro.com.cn

常用的中国电话与传真号码如下：

电话：021-6384 8899

传真：021-6384 1899

趋势科技中国办事处：

上海市淮海中路 398 号世纪巴士大厦 8 楼

要获取您所在地区/国家的趋势科技联系信息，请访问
http://www.trendmicro.com

知识库

趋势科技知识库是全天候在线的资源，其中包括了成千上万趋势科技产品的自助技术支持步骤。例如，若您收到错误消息并想找出处理办法，请使用知识库。每天都有新解决方案添加至知识库。

还可以在知识库中找到产品常见问题解答、热门提示、预防病毒的建议及支持和销售的区域联系信息。

http://cn.trendmicro.com/cn/support/techsupport/index.html

如果您无法找到特定问题的答案，知识库还提供一项额外服务，使您可以通过电子邮件提交问题。通常会在 24 小时内给您答复。

将可疑代码发送给趋势科技

请将可疑文件压缩加密后，以电子邮件附件的形式，发送到 **service@trendmicro.com.cn**。

压缩格式不拘， WinZIP 或 WinRAR 皆可，但请务必使用压缩程序的加密功能来加密，密码请设为小写 virus。

系统会提示您在电子邮件中提供以下信息：

- **电子邮件**：您想要用于接收防病毒团队回复邮件的电子邮件地址。将 "virus" 放在主题行中。
- **产品**：您当前使用的产品。如果您使用多个趋势科技产品，请选择对您提交的问题产生影响最大的产品或最常使用的产品。
- **受感染的座席数**：您组织中受感染的用户人数。
- **密码保护的文件**：趋势科技建议您将该可疑文件创建为受密码保护的 zip 文件并添加到附件，使用 "virus" 作为密码。
- **描述**：请针对您遭遇的病毒症状输入简短的描述。我们的病毒工程师团队将在 48 小时内 “解剖” 文件以识别并特征化其中可能包含的任何风险，然后将干净的文件返回给您。

注意： 提交的问题将迅速得到解决并且不受趋势科技病毒响应服务等级合约书中规定的策略及限制的约束。

将问题发送到以下地址：

`virus_doctor@trendmicro.com.cn`

在美国，您也可以拨打以下免费咨询电话：

(877) TRENDAV 或 877-873-6328

TrendLabs

TrendLabs 是趋势科技防病毒研究的全局基础架构和为用户提供最新安全信息的产品支持中心。

TrendLabs 的“病毒医生”监视全世界潜在的安全风险，以确保趋势科技产品能抵御最新出现的风险，从而保持其安全性。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。

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。专业服务中心和快速回复团队位于东京、马尼拉、台北、慕尼黑、巴黎和加利福尼亚的森林湖市。

安全信息中心

在 Internet 上的趋势科技安全信息 Web 站点有免费的完整安全信息：

http://www.trendmicro.com/vinfo/zh-cn/virusencyclo/default.asp

访问安全信息站点以：

- 阅读每周病毒报告，其中包括了本周预期触发的风险列表，并描述了本周全球 10 大最流行的风险

查看全球 10 大不同类别风险的**十大恶意软件列表**。

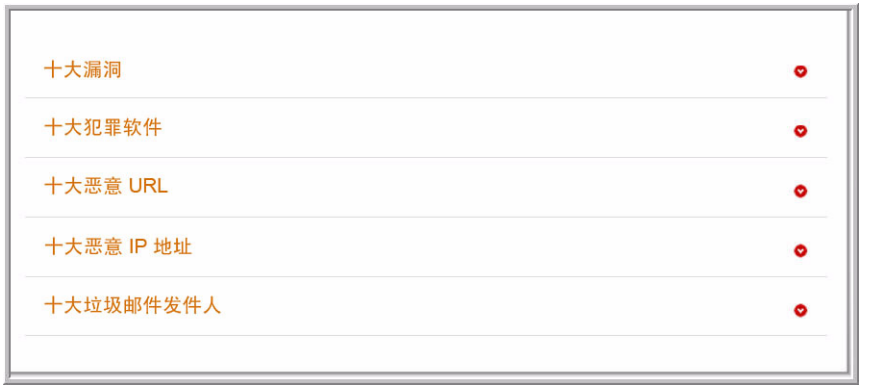


图 A-1. 十大趋势科技恶意软件

- 查阅病毒百科全书，病毒百科全书是对已知风险 （包括风险评估、感染症状、易感染平台、损害例程和如何移除风险的说明以及计算机谣言的相关信息）的综合
- 从欧洲计算机防病毒研究所 (EICAR) 下载测试文件，帮助测试您的安全产品是否已正确配置
- 阅读常规病毒信息，如：
  - 病毒入门书，帮助您了解病毒、特洛伊木马、蠕虫病毒及其他风险之间的不同
  - 趋势科技*安全计算指南*
  - 对风险评估的描述，帮助您了解评估等级为 “非常低”、“低”、“中”或 “高”的风险的破坏力
  - 病毒及其他安全风险术语的词汇表
- 下载综合行业白皮书

查看威胁测量仪或搜索威胁百科全书。

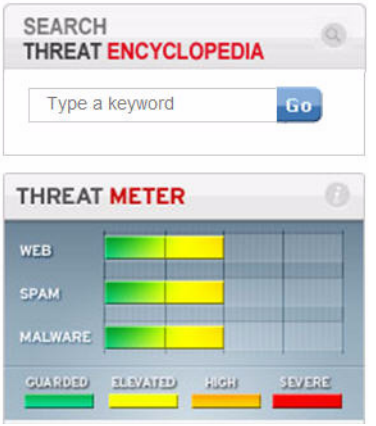


图 A-2. 趋势科技威胁信息

- 免费订购趋势科技病毒警报服务，以及时了解爆发并获取每周病毒报告
- 了解 Web 管理员可用的免费病毒更新工具

打开安全信息：

1. 打开下一代应用安全网关 Web 控制台。
2. 在窗口右上角面板的下拉菜单中单击**安全信息**。此时将打开**安全信息**窗口。

TrendEdge

面向趋势科技员工、合作伙伴和其他相关方的程序，提供不支持的革新技术、工具和趋势科技产品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。

`http://trendedge.trendmicro.com`



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: CTCM15544/120816