ISR G2安全概述

思科第二代集成多业务路由器的网络安全特性详细概述
本白皮书将详细概述思科® 1900、2900 和 3900 系列集成多业务路由器的网络安全特性。

下一代分支机构安全性

思科 1900、2900 和 3900 系列集成多业务路由器是 思科解决方案和产品组合 中的不可缺少的重要组件，它提供了嵌入式安全性和 VPN 功能，可允许组织在广域网的范围内识别、防止和及时应对远程分支机构的网络安全威胁。
作为网络安全保护中的重要设备，路由器的核心安全元素包括：

- **安全连接：**这些特性提供高度安全且可伸缩的网络连接，并且能整合多种类型的流量。典型的例子包括 IP 安全 (IPsec) VPN、分组加密传输 VPN、动态多点 VPN (DMVPN)、增强型简易 VPN 和安全套接字层 (SSL) VPN。
- **集成威胁控制：**这些特性将使用网络服务阻止和应对网络攻击和威胁。典型的例子包括思科 IOS® 防火墙、思科 IOS 入侵防御系统 (IPS)、内容过滤、NetFlow 和灵活数据包匹配（Flexible Packet Matching，FPM）。
- **身份确认：**这些特性允许网络使用认证、授权和结算（AAA）以及公钥基础设施（PKI）来智能地保护网络端点。
- **思科网络基础保护：**这些特性将保护网络基础设施不受攻击和漏洞的威胁，从网络的层面上说尤为如此。典型的例子包括 AutoSecure、控制面板监管和保护、基于源的远程触发黑洞 (RTBH) 过滤和单播反向路径转发 (URPF)。

安全连接

IP 网络的典型特性是充斥着不计其数的合法和非法应用，它们在话音、视频和实时数据方面等对性能敏感的方面展开激烈的竞争。举例来说，话音流量对延时非常敏感——话音数据包通常较小，而当它们排列在较大的非关键数据包后面时，您可以从嘀嗒声中立即判断出是否出现了级降。视频流量需要占用很高的带宽，并且对于偏差非常敏感；通常，在延时过程中缓冲视频数据是不切实际的做法，因此视频在传输过程中经常地抛弃一些数据包，以便于恢复到稳定的数据流；如果数据包丢失的情况过于频繁地出现，则最终会导致数据流不稳定并影响观众的心情。
这些企业话音和视频应用需要采用复杂的服务质量 (QoS) 和 IP 组播机构来维持话音和视频的质量。实现站点间和远程访问 VPN 的前提是能够在加密、廉价、无处不在的公共 Internet 网络上传输这种流量组合，并且主连接和备用连接均采用这种方式。在 VPN 上扩展话音和视频应用会引入 IPsec 与 QoS 或 IP Multicast 集成方面的需求。Voice over IP [VoIP] 和 IPTV 已经成为了主流，而思科 TelePresence™ 系统仍然在不断发展壮大。随着这些话音和视频电话应用的广泛普及，分支机构对 VPN 和安全特性、可伸缩性和特性集成的需求也会不断增加。
思科 1900、2900 和 3900 系列集成多业务路由器为通过话音、视频和实时数据集成提供了一个可伸缩的 VPN：

- **QoS：**加密前的低延时阵列队列（Low-Latency Queuing，LLQ）是确保 VPN 上的话音质量的一个关键因素。嵌入式处理器提供了 LLQ 以及加密后的接口级 QoS。
- **IP 组播：**安全组播（Secure Multicast）是一项基本技术，它通过结合密钥协议、群组释域（Group Domain of Interpretation，GDOI）和 IPsec 加密，为用户提供了一种保护 IP 组播流量的有效途径。它允许路由器对非通道（即“本地的”）IP 组播数据包执行加密，从而避免了单独配置各个通道需要，并能提高效率。封装 IP 组播数据包甚至允许 IP 组播路由（比如说协议无关组播 [PIM]）处理经过加密的数据包。本地 IP 组播封装还可以避免单播通道中经常出现的数据包过度复制的情况。安全组播非常适合用于对通过卫星链接传送的 IP 数据包执行加密，对音频会议执行加密，保护实时内容复制以及 DMVPN 等。

标准 IPsec VPN

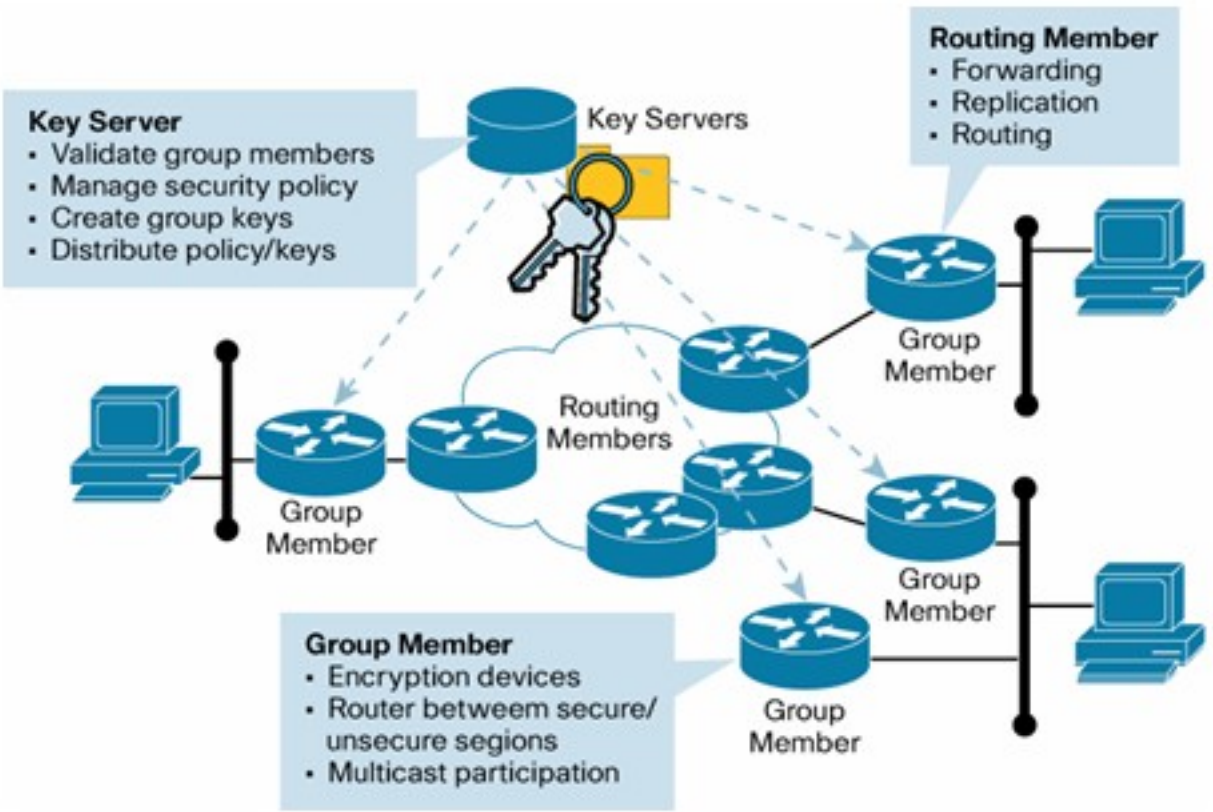
作为一种网络连接形式，VPN 始终保持着良好迅速的发展势态。并且，随着 VPN 应用的不断普及，企业对其性能、可伸缩性和特性的需求也在日益增长，而对于快节奏的企业分支机构环境来说尤为如此。一般而言，解决这些苛刻的网络需求的完美方案是通过单一设备来处理远程访问和站点间 VPN，同时提供多种安全服务。思科 1900、2900 和 3900 系列集成多业务路由器嵌入了对 IPsec 高级加密标准 (AES)、数据加密标准 (DES)、三重 DES (3DES) 加密和 VPN 流程的加速。
下面列出了其主要特性：

- DES、3DES 和 AES（128、192 和 256）加密程式的加速
- 支持通过 Rivest、Shamir、Aldeman (RSA) 程式签名和 Diffie-Hellman 实现认证
- 使用安全散列程式 1 (SHA-1) 或消息摘要程式 5 (MD5) 散列程式确保数据的完整性

有关思科 IOS 软件标准 IPsec 的更多信息，请访问：
http://www.cisco.com/go/ipsec
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/12_4t/sec_secure_connectivity_12_4t_book.html

分组加密传输 VPN

随着分组加密传输 VPN 的引入，思科提供了一种创新、可伸缩的 VPN，并且避免了通道的使用。它支持根据路由协议决策将加密 IP 单播和组播数据包直接路由到远程站点，或者在故障路径之间来回路由，从而提供了更好的可用性。它支持组织依赖已有第 3 层路由信息，因此能解决组播复制低效问题并改善网络性能。分布式分支机构网络可以实现更好的扩展，同时持续提供对于话音和视频质量至关重要的网络智能特性，比如说 QoS、路由和组播。
分组加密传输 VPN 提供了一种全新的基于标准的 IPsec 安全模型，并在其中应用了“受信”分组成员的概念。受信的分组成员路由器所使用的公共安全方法独立于任何对到对 IPsec 通道关系。该模型通过一台密钥服务器向所有注册和认证的分组成员路由器分发密钥和策略（图 1）。
图 1. 分组安全功能



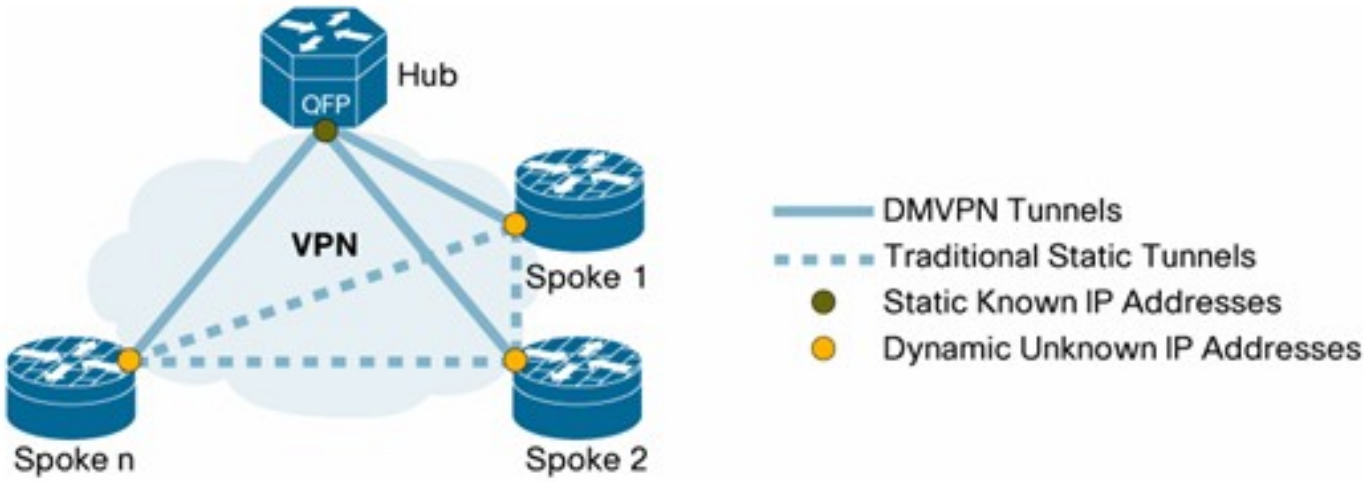
分组加密传输 VPN 可以为各种应用带来收益。特别需要注意的是，分组加密传输 VPN：

- 提供数据安全和传输认证，通过对所有广域网流量加密来满足内部及外部的安全遵从性需求
- 支持高度扩展的网络结构，通过分组加密密钥消除复杂的端到端（peer-to-peer）密钥管理
- 维持网络智能，比如说多协议标签交换 (MPLS) 网络中的全网状连接、自然路由路径和 QoS
- 通过集中密钥服务器实现简易的成员授权控制
- 在站点间提供全天候、直接通信，避免使用中央集线器，以便将延时和偏差保持在较低水平
- 使用核心网络实现组播流量复制，避免各对等站点多次执行数据包复制，从而减小客户预置设

备 (CPE) 和提供商边缘加密设备的流量负载。
有关思科 GET VPN 的更多信息，请访问：
http://www.cisco.com/go/getvpn
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_encrypt_trns_vpn.html

动态多点 VPN

思科路由器提供了 DMVPN 功能。思科 DMVPN 可以帮助随需应变且可伸缩的全网状 VPN 减少延时、节省带宽并简化 VPN 部署（图 2）。DMVPN 特性建立在思科 IPsec 和专业路由技术的基础之上，它允许动态地配置通用路由封装 (GRE) 通道、IPsec 加密、下行解析协议 (NHRP)、开放最短路径优先协议 (OSPF) 和增强内部网关路由协议 (EIGRP)。
图 2. DMVPN



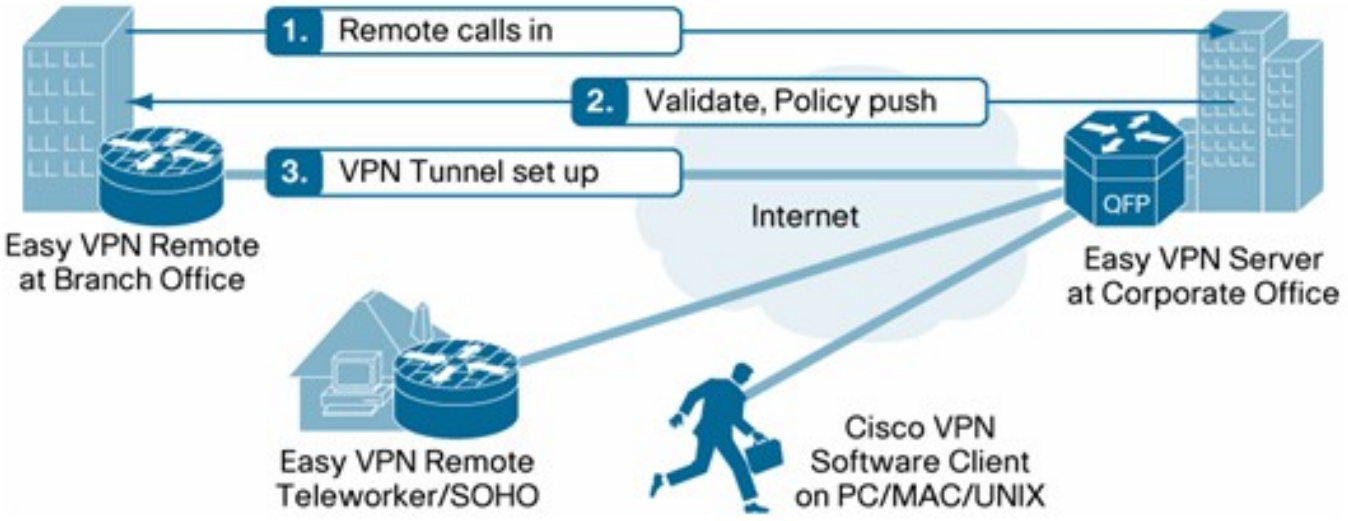
DMVPN 的真正强大之处体现在企业总部内部：VPN 通道的动态配置与 QoS 和 IP 组播等技术相结合，不仅可以优化延时敏感应用的性能，还可以减轻管理负担。举例来说，话音和视频应用在 IP 传输网络上可以获得与广域风链路方案相同的性能 —— 同时确保安全性和效率。
DMVPN 已广泛应用于结合企业分支机构、远程工作人员和外联网连接。其主要获益包括：

- 通过简单的星形拓扑配置实现全网状连接
- 在建立 IPsec 通道时使用自动 IPsec 触发
- 支持通过零接触配置来添加辐（spoke）
- 支持动态寻址的辐

有关思科 DMVPN 的更多信息，请访问：
http://www.cisco.com/go/dmvpn
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_DMVPN.html

简易 VPN 增强型简易 VPN

针对简单、高度扩展、远程访问需求，思科提供了简易 VPN 解决方案。该解决方案使用“策略推送”技术简化配置，同时维持丰富的特性和策略控制。总部指定的简易 VPN 服务器用于将安全策略推送到远程 VPN 设备，从而确保在建立连接之前已经指定了最新的策略（图 3）。
图 3. 简易 VPN 通道设置 [[edits: setup (one word);;



简易 VPN 提供了以下获益：

- 简易 VPN 使用相同的中央站点路由器为硬件（接入路由器）CPE 和软件远程接入客户端提供支持。您可以在PC、Mac 和 UNIX 系统上安装思科 VPN 客户端软件，以便为基于路由器的 VPN 增加远程接入连接，而无需任何额外的成本。由于硬件 CPE 和软件客户端只采用了一种技术（简易 VPN），因此设置、监控和 AAA 服务的简化和统一帮助降低了总体拥有成本 (TCO)。
- 简易 VPN 支持对 CPE 和各用户执行本地（基于路由器）以及集中化的 RADIUS 和 AAA 认证。
- 简易 VPN 支持数字证书，从而能改善预共享密钥的安全性。
- 该技术可以通过中央站点的多台简易 VPN 集中器实现负载均衡。策略推送功能可以将备用集中器信息发送给 CPE，这样您就可以直接扩展解决方案，而无需重新配置 CPE 。
- 该技术可以实现简易 VPN 服务器的虚拟化，允许服务提供商使用单一平台向多个客户提供 VPN 服务。
- 简易 VPN 实现了全功能集成，包括动态 QoS 策略分配、防火墙和 IPS、通道分离以及用于性能监控的思科 IP 服务水平协议 (SLA) 和 NetFlow。
- Cisco Configuration Professional 支持通过向导迅速部署集成了 AAA、防火墙以及远程简易 VPN 客户端实时图形监控的简易 VPN。
- 所有 VPN 产品线都支持简易 VPN：包括思科 IOS 软件和思科自适应安全程式 (ASA) 设备。

集成增强型简易 VPN 特性与虚拟通道接口 (VTI) 时，您可以直接使用简易 VPN 来配置虚拟接口，从而实现简易部署和高级网络集成。获益包括：

- 数据转发器以及远程分支机构的配置需求得到极大简化。
- 您可以使用 VTI 来配置 IP 服务（或者从 AAA 服务器下载服务）。并且，在连接时，VTI 实例会动态克隆自这些模板。不需要手动为各远程站点创建大量类似的配置命令。
- VTI 提供了一些特定于用户（per-user）的属性，比如说 QoS，可以轻松地为每个用户配置策略，这使管理员可以主动提供所需的应用性能，并保持用户的生产力和积极性。
- VTI 支持使用它自己的参数集来配置各分支机构 VPN，因此可以根据特定于站点的需求来灵活地定制配置和安全。

有关思科简易 VPN 的更多信息，请访问：
http://www.cisco.com/go/easyvpn
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_rem.html
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_easy_vpn_srvr.html

思科 IOS SSL VPN

思科 IOS SSL VPN 是一个基于路由器的解决方案，它提供了 SSL VPN 远程接入连接，并在一个聚

合的数据、话音和无线平台中集成了安全性和行业领先的路由特性。借助 SSL VPN，各公司可以安全、明晰地将它们的业务网络扩展到任何支持 Internet 的位置。思科 IOS SSL VPN 支持在没有客户端的情况下访问各种应用，比如说基于 HTML 的内联网内容、电子邮件、网络文件共享、Citrix 和思科 SSL VPN 客户端，因此可以远程访问几乎任何应用。作为思科 IOS SSL VPN 的一部分，思科安全桌面（Cisco Secure Desktop）甚至为非公司设备提供了数据失窃保护。Cisco Configuration Professional 可以简化思科 IOS SSL VPN 简化，并能对 SSL VPN 会话执行实时监控和管理。
有关思科 IOS SSL VPN 的更多信息，请访问：
http://www.cisco.com/go/iossslvpn
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn.html

虚拟通道接口

VPN 作为一款主流的安全广域网连接解决方案已经得到了越来越广泛的认可。它们将替代或扩充已有的使用租用线程、帧中继或 ATM 的专用网络，以更加经济高效和灵活的方式连接远程分支机构和中央站点。这种新形势要求 VPN 设备提供更高的性能和网络可用性，并且支持局域网和广域网接口。
您可以使用全新的思科 IPsec VTI 工具为站点间设备配置基于 IPsec 的 VPN。它提供了一个可路由的接口来终止 IPsec 通道，因此可以简化配置。思科 IPsec VTI 通道为共享广域网提供了一条指定路径，并将流量封装在全新的数据包头部中，以确保将数据传递给特定的目标位置。这是一个专用网络，因为流量只能在端点进入通道。此外，IPsec 提供了真正的机密性（以及加密），并且可以携带加密流量。
借助思科 IPsec VTI，您的企业可以充分利用经济高效的 VPN，并能继续向数据网络添加话音和视频，而不需要在质量和可靠性之间做出权衡。该技术为站点间 VPN 提供了高度安全的连接，从而支持在 IP 网络上聚合话音、视频和数据。
有关思科 IPsec VTI 的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_virt_tunnl.html

多重虚拟路由转发 (Multi-VRF) 和 MPLS 安全级连

Multi-VRF CE（或称作 VRF-Lite）支持在同一物理路由器中配置和维护多个路由和转发表实例。与以太网 VLAN 技术和 WAN VPN 技术（如帧中继）相结合，该技术可以使用一个物理网络来提供多个逻辑服务，从而将隐私和安全性扩展到客户所有角落。
借助 Multi-VRF CE，一台思科路由器可以支持 IP 地址重叠的多家公司，同时维持数据、路由和物理接口之间的隔离性。
有关 Multi-VRF CE 的更多信息，请访问：
http://www.cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html.

IPsec 高可用性

思科 VPN 支持各种用于部署冗余和负载均衡的特性。对于小规模的数据转发器 IPsec 部署，您可以使用热备份路由器协议 (HSRP) 和反向路由器注入 (RRI) 来提供冗余；则对于较大规模的部署来说，您可以使用思科服务器负载均衡 (SLB) 来提供冗余和负载均衡：

- **IPsec 故障转移**：通过 IPsec 故障转移，在遇到计划内或计划外故障时，您可以使用备用 IPsec 服务器继续处理和转发 IPsec 数据包。备用 IPsec 服务器会自动接替活动路由器的任务，而不会在活动路由器连接意外断开时丢失与其对等设备之间的安全连接。此过程是明晰的，并且不需要调整或重新配置任何远程对等设备。IPsec 状态化故障转移主要用于与状态化切换 (SSO) 及 HSRP 结合使用。HSRP 为 IP 网络提供了网络冗余，可确保用户流量能立即明晰地从网络边缘设备或接入环路（access circuit）中的故障恢复过来。IPsec 状态化故障转移将为 IPsec 通道、支持 GRE 的 IPsec 以及思科 IOS 简易 VPN 流量提供保护。
- **HSRP 和 RRI**：RRI 可以处理动态和静态加密映射，从而简化了具备高可用性和负载均衡需求的 VPN 的设计。它将为各远程网络或数据转发器设备上的主机创建相应的路由器，以便于支持动态路由传播。HSRP 和 IPsec 可以通过动态重新路由最大限度提高服务的可用性。对于无法

在主用路由器出现故障时切换到其他路由器的交换机来说，HSRP 提供了持续的网络访问。这时将使用 HSRP 虚拟 IP 地址作为 VPN 通道端点来为 IPsec 的无状态故障转移提供持续可用性。

- **SLB**：您可以指定虚拟服务器作为网络服务器集群（服务器群）中的物理服务器。当某客户端发起到虚拟服务器的连接时，思科 IOS 软件会根据所配置的负载均衡程式选择一台物理服务器进行连接。当物理服务器出现故障时，SLB 会重新将所有传入的新 IPsec 会话动态路由到其他服务器，以便于提供冗余功能。

有关 IPsec 高可用性的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_vpn_ha_enhance.html.

集成威胁控制

思科集成威胁控制通过简化的策略控制和主动系统联保提供了全面的网络保护功能。这些安全功能包括思科 IOS 防火墙、思科 IOS IPS、思科 IOS 内容过滤、NetFlow、基于网络的应用识别 (NBAR) 和灵活数据包匹配 (FPM)。这些特性将共同完成以下工作：

- 保护网络、服务器、端点和信息
- 管理网络访问、隔离被感染系统、阻止入侵以及保护重要企业资产
- 阻止恶意流量，比如说蠕虫、病毒和恶意软件，避免它们对您的企业造成不利影响。

思科 IOS 防火墙

思科 IOS 防火墙是内置在思科 IOS 软件中的状态化防火墙。正是得益于此防火墙的坚固的安全特性，思科 1900、2900 和 3900 系列集成多业务路由器成为了理想的安全和路由解决方案，专用于保护网络中的广域网入口点。

思科 IOS 防火墙的主要特性包括：

- **基于区域的策略**：此特性支持将物理和虚拟接口划分到不同的区域（zone）中，以便于简化逻辑网络拓扑。创建了这些区域之后，企业可以根据区域来应用防火墙策略，而不是在各接口上单独配置策略。除非在各区域对之间明确指定各方向的区域对策略，否则不会转发数据包。策略需要使用思科策略语言（即 Modular QoS CLI [MQC]）编写，并且将为各区域应建立相应的状态化检测和会议参数。举例来说，Internet 与非管制区（DMZ）之间的边界需要明确指定策略以允许 HTTP 和域名系统（DNS）经过。
- **高级应用检测和控制 (AIC)**：此特性使用检测引擎确保协议一致性，并禁止恶意或未授权行为，比如说使用端口 80 作为通道，或滥用电子邮件连接（简单邮件传输协议 [SMTP]、扩展 SMTP [ESMTP]、Point Of Presence 3 [POP3] 和 Internet 邮件访问协议 [IMAP]）。
- **通过防火墙实现安全统一通信**：思科 IOS 防火墙可以明晰地支持话音流量，包括在应用层面上与媒体协议呼叫流程和相关开放通道保持一致。它支持各种话音协议，比如说 H.323v2、v3 和 v4；瘦客户端控制协议 (SCCP)；会议发起协议 (SIP)，并能为各统一通信组件提供万无一失的保障，比如说思科统一通信管理器（Cisco Unified Communications Manager）、思科统一边界元素（Cisco Unified Border Element）及其端点。
- **VRF 感应的防火墙**：各种级连水平的 VRF 部署中的可用服务都内置了防火墙。
- **防火墙高可用性**：状态化防火墙故障转移有助于在两个设备之间实现基于 HSRP 的“活动-备用”故障转移，从而避免活动会话中断。
- **明晰的防火墙**：此特性提供第 2 层隔离，允许轻松地将防火墙添加到已有网络中，而不需要对 IP 子网重新编号。
- **IPv6 防火墙**：IPv6 防火墙允许思科 IOS 防火墙在 IPv6 和 IPv4 混合环境中工作。
- **粒度化安全策略**：此特性支持为各用户、接口和子接口指定安全策略。
- **集成身份服务**：集成身份服务可以为各用户提供认证和授权。
- **基于策略的防火墙管理**：Cisco Security Manager 和 Cisco Configuration Professional 提供了

直观的、基于策略的管理思科 IOS 防火墙的途径。

有关思科 IOS 防火墙的更多信息，请访问：
http://www.cisco.com/go/iosfw
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/12_4t/sec_data_plane_12_4t_book.html

思科 IOS IPS

一些思科路由器提供了 IPS 功能。思科 IOS IPS 是一种基于深度数据包检测的嵌入式解决方案，它可以帮助思科 IOS 软件有效地缓解网络攻击造成的威胁。与各种思科入侵防御系统 (IPS) 设备和模块相同，思科 IOS IPS 也使用状态化数据扫描技术以及攻击和漏洞签名机制。
现在，这个 IPS 解决方案已经集成到了已有接入路由器中，因此可以在网络边缘建立多层防线，同时将开销降至最低。
思科 IOS IPS 的主要特性包括：

- **嵌入式功能**：除了检测之外，此特性还可以帮助路由器立即对安全威胁做出响应，并为网络提供保护。路由器可以根据需要抛弃流量、发送警报、本地避让或者重置连接，以便于尽早阻止攻击流量并尽快从网络中清除它们。您可以根据各个签名来配置这些操作。
- **签名事件操作处理器 (SEAP)**：独特的、基于风险评级的签名事件操作处理器可以实现更加准确有效的 IPS 事件监控——它可以过滤或分离风险评级（Risk Rating）较低/高的事件，从而显著简化 IPS 策略的管理。
- **现成可用的签名文件**：对于希望获取最大入侵保护的用户来说，此特性可以为他们提供一个易于使用的签名文件，并且其中包含“可能性最大的”蠕虫和攻击签名。匹配这些“可能性评级较高的”蠕虫和攻击签名的流量将被抛弃。Cisco Configuration Professional 提供了一个直接的用户界面，用于配置这些签名，包括从 Cisco.com 上传新签名，而不需要更改软件镜像，以及为这些签名适当配置路由器。
- **可定制签名**：通过此特性，您可以修改已有签名或创建一个签名来应对最新发现的威胁（您可以单独启用各签名操作）。
- **明晰的 IPS**：此特性可为第 2 层连接提供第 2 层 IPS，允许轻松地向已有网络添加 IPS，而不需要对 IP 子网重新编号
- **VRF 感应的 IPS**：各种级连水平的 VRF 部署中的可用服务都内置了 IPS。
- **大签名数据库**：可供选择的签名数量在不断增加；目前，思科 IPS 传感器平台支持超过 1200 种签名。
- **一致的管理**：您可以采用与思科入侵检测系统 (IDS) 传感设备相同的方式来加载和启用所选 IPS 签名。有关思科 IOS IPS 的更多信息，请访问：
  http://www.cisco.com/go/iosips

思科 IOS 内容过滤

思科 IOS 内容过滤可以帮助您的组织保护自身不受已知和新出现的 Internet 威胁的影响，改善员工生产力以及依照法规执行企业策略。它可以监控和管理所有 Internet 活动，具体方式包括阻止或限制对特定网站的访问，阻止包含恶意软件、广告软件、间谍软件和钓鱼软件的恶意站点，以及帮助您的组织通过简单的部署更好地管理网络资源。
思科 IOS 内容过滤的主要特性包括：

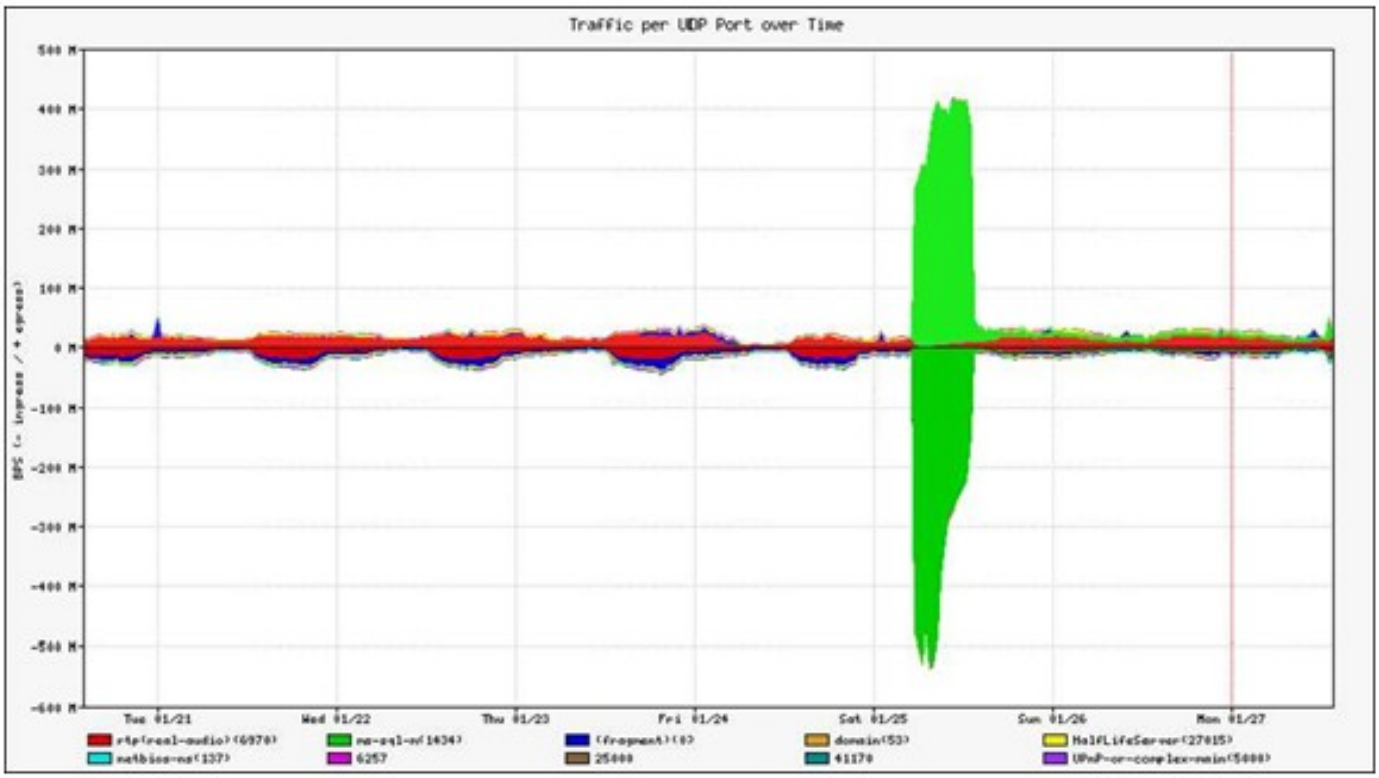
- **基于订阅的服务**：易于续订的、为期 1 年、2 年或 3 年的订阅服务与路由器平台相关；而不需要单独的用户许可。此订阅将允许您访问 Trend Micro 的数据库，并将为路由器设定内容过滤策略。
- **安全评级**：思科 IOS 内容过滤可以有效应对包括零日攻击在内的各种基于 Web 的威胁。它将根据 Trend Micro 的 TrendLabs 提供的分析来评定网站的安全风险，并且可以帮助防止钓鱼软件和间谍软件将机密信息发送给黑客和电子罪犯。TrendLabs 将根据过去的行为以及当前是否公开了恶意软件、广告软件、钓鱼软件、间谍软件和黑客攻击来评定特定 URL 的安全级别。

- **基于类别的 URL 分类**：基于内容的 URL 分类机制可以帮助限制对不良网站的访问（比如说关于赌博或军火的网站）。可用的类别达到 70 种以上，包括基于声誉的阻截机制（比如说间谍软件和键盘记录）。
- **关键字阻截**：思科 IOS 内容过滤可以根据 URL 中出现的关键字来阻截网站。
- **黑名单和白名单支持**：思科 IOS 内容过滤支持 100 个黑名单 URL 和 1000 个白名单 URL。举例来说，您可以向白名单添加受信任的网站。
- **管理设置**：思科 IOS 内容过滤易于使用和部署。可以通过基于 Web 的路由器管理工具 Cisco Configuration Professional 来对它进行管理。
- **缓存**：缓存特许将在路由器本地存储 URL 类别及其策略（允许或拒绝），从而能确保缩短访问 Internet 时的响应时间。管理员可以配置缓存在路由器上存在的时间。

有关思科 IOS 内容过滤的更多信息，请访问：
http://www.cisco.com/go/ioscontentfiltering.

NetFlow

NetFlow 是行业中用于检测网络异常的主要技术。它提供了遥感勘测数据来分析 IP 流量——举例来说，谁在与谁通信，采用何种协议和端口，持续多长时间，传输速度如何。
分布式拒绝服务 (DDoS) 攻击会造成网络使用率突然达到峰值。与传统的利用所收集的历史配置信息和基线的流量模式相比，NetFlow 可以更加迅速地将这些攻击识别为异常网络“事件”。
通过分析详细的 NetFlow 流数据，管理员还可以对攻击类型（即攻击的源和目标）、攻击持续时间以及攻击中所使用的数据包的大小进行分类。分析工具包括思科安全合作伙伴提供的产品以及思科安全监控、分析和响应系统 (MARS)。（参见 图 4）。
图 4. 使用 NetFlow 和 Arbor 网络实现基于异常的 DDoS 检测示例



有关思科 IOS NetFlow 的更多信息，请访问： http://www.cisco.com/go/netflow。
有关思科安全 MARS 的更多信息，请访问： http://www.cisco.com/go/mars。

基于网络的应用识别

NBAR 是思科 IOS 软件中的一个分类引擎，它使用深度和状态化数据包检测功能来识别各种应用，包括基于 Web 的应用和其他使用动态 TCP/用户数据报协议 (UDP) 端口分配的难以分类的协议。在安全级连中使用时，NBAR 可以根据有效负载的签名来检测蠕虫。当 NBAR 识别某个应用并对其

分类时，网络可以调用该特定应用的服务。通过使用 QoS 特性提供有保障的带宽、带宽限制、流量整形（traffic shaping）和数据包渲染，该技术还有助于确保网络带宽得到了有效使用。
Cisco Configuration Professional 可以通过一个易于使用的向导来启用 NBAR，此外还提供了一个关于应用流量的图形视图。
有关 Cisco NBAR 的更多信息，请访问：http://www.cisco.com/go/nbar。

灵活数据包匹配（Flexible Packet Matching）

FPM 可以检测数据包的攻击特征，并采取适应的措施（记入日志、抛弃或者通过 ICMP 发送“目标无法到达”消息）。它提供了灵活的从第 2 层到第 7 层的无状态分类机制。您可以根据任何协议以及流量协议栈的任何字段来指定分类标准。根据分类结果，您可以采取适当操作，比如说抛弃或者记录分类流量。
有关 FPM 的更多信息，请访问：
http://www.cisco.com/go/fpm
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_flex_pack_match.html

信任和身份

PKI 客户端（x.509 数字证书）

借助公钥基础设施 (PKI)，客户可以通过一种可伸缩、安全的机制在安全数据网络中分发、管理和撤销加密及身份信息。思科 IOS 软件支持嵌入式 PKI 客户端功能，它可以与思科 IOS 认证服务器及第三方认证机构交互。
路由器将生成一个 Rivest、Shamir 和 Adelman (RSA) 密钥对（一个私钥和一个公钥），并为它建立合法身份。 认证中心（Certificate Authority，CA）服务器将验证路由器并发布数字证书，授予进入 PKI 的权限。使用证书中的信息，PKI 中的各路由器可以验证其他对等设备的身份，并与包含在证书中的公钥建立一个加密会话。
PKI 客户端支持的特性包括：

- **认证服务器**：支持外部（如 Verisign）或内部（如 Microsoft）证书服务器；对于较小规模的部署，可以使用思科 IOS 软件证书服务器
- **证书认证和登记**：支持 SCEP、手动和 TFTP 方法
- **自动登记和续订**：允许路由器自动请求数字证书并在过期之前续订证书；证书回滚（rollover）用于在续订 CA 的证书后实现无缝过渡
- **安全设备设置**：允许使用 PKI 和IPsec VPN 安全地部署使用工厂默认配置的路由器，而不需要大量最终用户配置；远程办公室或远程工作位置的的理想方案
- **PKI – AAA 集成**：允许路由器在后端使用 AAA 服务器来提供认证；根据认证字段提供粒度化控制
- **基于认证的访问控制**：提供类似于 PKI – AAA 集成的功能，此外还可以使用开箱即用的 ACL 来根据认证字段接受或拒绝认证
- **HTTPS 管理和 SSL VPN 特性**：支持永久自签名证书
- **证书撤销检查**：支持证书撤销列表 (CRL) 和在线证书状态协议 (OCSP)
- **多层 CA 结构**：允许路由器在多个层次使用 CA TrustPoints；可用于设置分支机构路由器处理部门 CA 或其他附属部门的认证服务器
- **PKI 凭证（RSA 密钥）库**：在 NVRAM 中为私钥提供保护，可以选择对密钥进行加密；同时支持 USB 令牌
- **其他受支持的高级 PKI 功能**：在任何用户尝试恢复密码时擦除 RSA 密钥；多密钥对；以 PEM 格式导入密钥对和证书；以及 4096 位公钥和私钥

有关思科 IOS 软件 PKI 客户端的更多信息，请访问：
http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/

guide/sec_pki_feat_rmap_ps6441_TSD_Products_Configuration_Guide_Chapter.html
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_white_paper0900aecd8046cbc4.html
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/ps6807/prod_white_paper0900aecd805249e3_ns855_Networking_Solutions_White_Paper.html

思科 IOS 认证服务器

思科 IOS 认证服务器嵌入在思科 IOS 软件中，允许路由器充当网络上的认证中心。通常，随着 VPN 安装的不断增加，企业会难以生成和管理加密信息。思科 IOS 认证服务器在支持 IPsec VPN 的相同硬件中建立了一个简单、可伸缩、易于管理的认证中心，从而解决了这些挑战。思科 IOS 认证服务器提供了一种重要的替代方案，可以实现简单的对称密钥部署。
所支持的特性包括：

- 简单证书登记协议 (SCEP)
- 生成 RSA 密钥对
- 数据库文件存储
- 自动存档 CA 证书及密钥
- 在当前证书过期时自动回位（rollover）CA 证书和密钥
- 证书撤销列表 (CRL)
- 附属机构和注册中心模式

有关思科 IOS 软件认证服务器的更多信息，请访问：
http://www.cisco.com/en/US/products/ps6664/products_ios_protocol_option_home.html
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_mng_cert_serv_external_docbase_0900e4b1805afd65_4container_external_docbase_0900e4b1807b4277.html

基于 802.1x 的标准身份服务

标准 802.1x 应用要求用户提供有效的访问凭证，因此未授权用户要访问受保护的信息资源将变得更加困难。通过部署 802.1x 应用，网络管理员还可以有效避免用户部署不安全的无线接入点，从而解决了 WLAN 设备简易部署中的一个最令人担忧的问题。
有关 802.1 的更多信息，请访问：
http://www.cisco.com/en/US/products/ps6662/products_ios_protocol_option_home.html
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_ieee802_pba.html
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_ieee_loc_auth_sv.html
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_vpn_ac_802_1x.html

AAA

思科 IOS 软件 AAA 网络安全服务提供了为路由器或接入服务器建立访问控制的框架。AAA 旨在帮助管理员使用适用于特定服务或接口的方法列表为各用户或各服务（举例来说，针对 IP、Internetwork Packet Exchange [IPX] 或虚拟专用拨号网络 [VPDN]）动态配置认证和授权的类型。
有关思科 IOS 软件 AAA 的更多信息，请访问：
http://www.cisco.com/en/US/products/ps6663/products_ios_protocol_option_home.html
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/12_4T/sec_securing_user_services_12.4t_book.html

思科 IOS 网络基础保护

网络基础设施设备的持续可用性对于企业总部的重要性是无以复加的。如果某个网络路由器或交换机的安全受到威胁，则恶意攻击者将获得对整个网络的访问权。无论针对攻击采用何种技术性的防御措施，都有必要防患于未然。
以下技术突显了提供可靠的 网络基础保护 是多么的重要，包括思科 IOS 软件设备在遇到 DDoS 攻击时采取的自我防御措施，以及通过安全管理访问来最大限度降低管理和控制接口遇到的哄骗攻击的几率。

AutoSecure

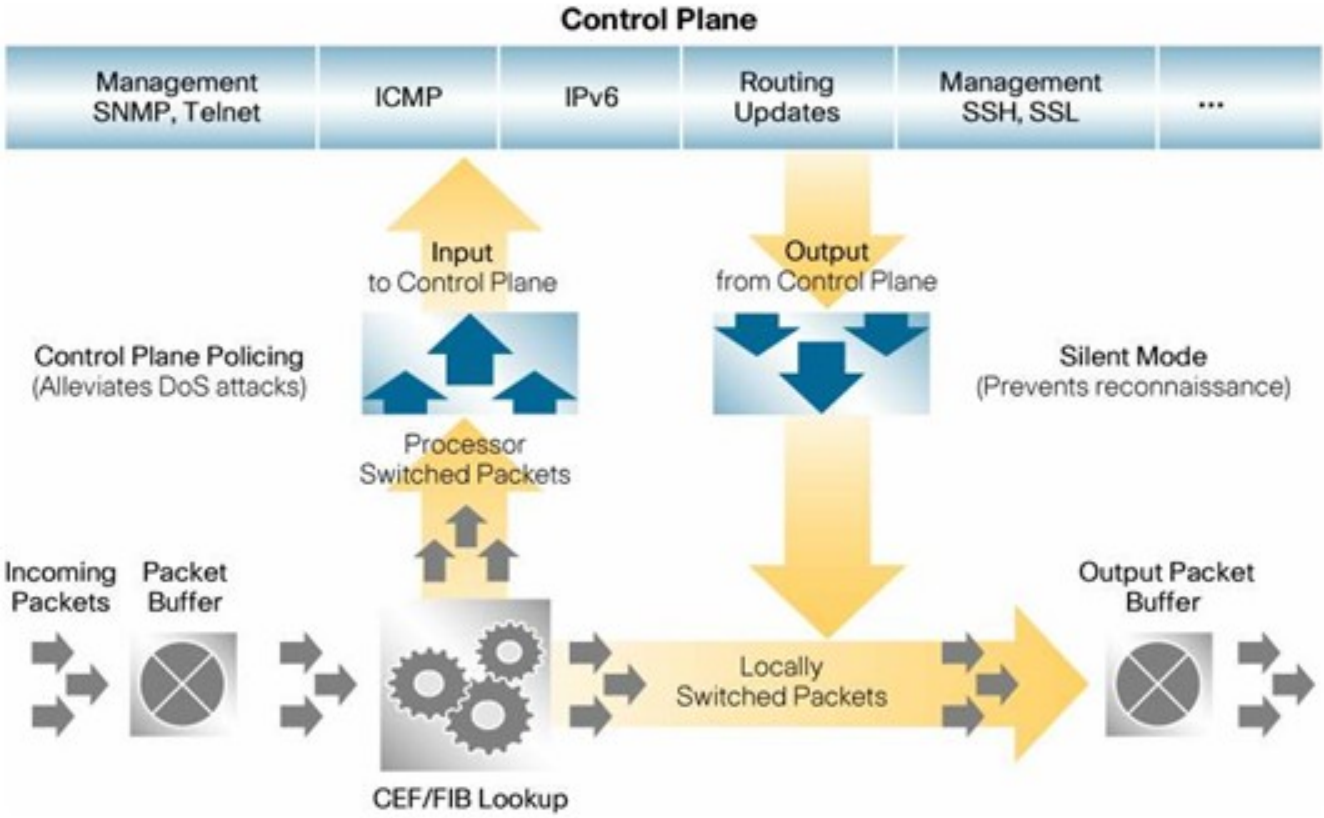
安全配置要求掌握各设置参数对安全的影响。在配置这些参数的过程中，任何错误和疏忽都可能造成易受攻击的漏洞，从而危及网络的安全性，并影响网络信息的可用性、完整性和隐私性。许多网络管理员都无法全面理解各思科 IOS 软件特性与安全性之间的隐含关系。
Cisco AutoSecure 整合了一种直观、“一触式的”设备锁定流程，从而满足了企业和服务提供商网络的重要安全需求。它可以帮助管理员快速实现安全策略和过程，而不需要具备关于思科 IOS 软件特性或命令行接口 (CLI) 的手动执行的丰富知识，从而简化了安全流程。此特性提供了一条 CLI 命令，可以即时配置路由器的安全状态，禁用不重要的系统进程和服务，从而排除潜在的安全威胁。
您可以将思科 AutoSecure 部署为它支持的两种部署之一，这取决于特定的客户部署场景：

- **交互模式**：允许您选择启用和禁用服务以及其他安全特性
- **非交互模式**：使用建议的思科默认设置自动执行 AutoSecure 命令

有关 AutoSecure 的更多信息，请访问：
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper09186a00801dbf61.html
http://www.cisco.com/en/US/products/ps6642/products_white_paper09186a0080183b83.shtml
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_autosecure.html

控制面板监管和保护

再安全可靠的软件实现和硬件架构也难免会受到 DoS 攻击的威胁。DoS 攻击是一种恶意行为，其手段是通过伪装特定类型的控制数据包，向控制面板处理器发起洪水攻击，从而造成网络基础设施故障。分布式 DoS (DDoS) 攻击由于可以采用几百个攻击源，因此它所发送的垃圾 IP 流量也将翻倍，有时甚至可以达到几 GB 每秒。这些 IP 数据流中的数据包将发送给思科路由器处理器的控制面板进行处理。由于路由器处理器接收到的欺骗数据包的数量非常之多，因此控制面板不得不花费过多时间来处理和抛弃 DoS 流量。
为了应对这些以及类似的针对系统核心（即处理器）的威胁，控制面板监管（Control Plane Policing）可以使用可编程的监管功能来限制（或监管）路由器控制面板接收到的流量。通过与思科 IOS QoS 分类机制相结合，您可以配置此监管机制识别特定的流量类型并完全限制它们，或者限制超过指定标值水平的流量（图 5）。
控制面板保护（Control Plane Protection）对这种监管功能进行了扩展，它支持离散性更高的监管。有关控制面板监管和保护的更多信息，请访问：
http://www.cisco.com/en/US/products/ps6642/prod_white_papers_list.html.
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122s/122snwft/release/122s18/gtrtlimt.htm.
图 5. 控制面板监管：数据包缓冲；传入数据包；思科快速转发（Cisco Express Forwarding）和转发信息库（Forwarding
Information Base，FIB）查询；输出数据包缓冲；静默模式



CPU 和内存标值通知

CPU 和内存是缓解网络设备的潜在可用性影响的重要资源。简单网络管理协议 (SNMP) MIB 目前支持监控应用查询特定资源的可用性。由于这些资源具有动态特性，因此调度轮询这些变量经常会造成最大限度提高网络可用性所需的操作出现延时。
借助内存标值通知（Memory Thresholding Notification），您可以管理各种资源分组所占用的内存量。您可以以字节为单元指定最大内存空间，或者指定总处理器资源的百分比。当某资源分组接近其指定内存标值时，您将接收到相应通知。
您可以使用 CPU 标值通知（CPU Thresholding Notification）来配置 CPU 使用率标值，当 CPU 使用率超过这个值时便会发出通知。思科 IOS 软件两种 CPU使用率标值：

- 上限标值（Rising threshold）：当 CPU 资源百分比超过指定值一段时间后触发 CPU 标值通知
- 下限标值（Falling threshold）：当 CPU 资源百分比低于指定值一段时间后触发 CPU 标值通知

有关 CPU 和内存标值通知的更多信息，请访问：
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_cput.htm
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_memnt.html

路由保护

- MD5 邻居认证：MD5 邻居认证可确保路由器只从受信任的邻居节点接收路由信息。每个路由更新都将使用 MD5 程式进行加密，并且所生成的签名（摘要）将作为路由更新消息的一部分发送。这样，路由器便可以验证各邻居的身份以及其路由更新的完整性。
- BGP TTL 安全检查：TTL 安全检查可以防止基于路由的 DoS 攻击以及未授权的对等互联和会话重置攻击（发起这些攻击的系统并未直接连接到与被攻击路由器相同的子网）。
- TTL 安全检查允许配置在两台 eBGP 对等设备之间交换的数据包的最小 TTL 值。启用此功能后，两台对等路由器在相互传输流量时会将 TTL 设定为 255。此外，仅当其他 eBGP 对等设备所使用的 TTL 大于或等于为对等会话配置的 TTL 标值时，路由器才会建立一个对等会话。如果接收到的数据包的 TTL 值小于预定值，则它们将被静默抛弃。

- 建议为所有路由器都启用这些特性，特别是需要与外部对等设备连接的路由器。有关这些特性的更多信息，请访问：http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Baseline_Security/sec_chap3.html

ACL 保护

- ACL 将保护路由器不受恶意流量攻击。它们可以明确指定允许合法流量（比如说授权设备发起的路由和管理流量）发送给边缘路由器目标地址。
- IP 选项选择性抛弃（Options Selective Drop）：在大多数思科路由器上，软件会对带 IP 选项的数据包执行过滤和交换操作，以便于处理选项并重写 IP 头部。这将造成潜在的安全威胁，因为包含 IP 选项的数据包有时会对设备的性能造成不利影响。ACL IP 选项选择性抛弃允许思科路由器过滤掉包含 IP 选项的数据包，通过抛弃这些数据包并忽略处理 IP 选项来缓解对性能的负面影响。

有关 ACL IP 选项选择性抛弃的更多信息，请访问：http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120s/120s23/sel_drop.htm.

安全访问模式（静默模式）

侦察是黑客发起系统攻击之前的一项必要准备工作；也就是获取关于网络的信息。黑客的侦察手段是监听系统消息，比如说数据包传输的状态（包括设备的 IP 地址等信息）。
安全访问模式（也称作静默模式）是一个全新的思科 IOS 软件特性，旨在限制黑客可收集到的关于网络的信息。它可以阻止路由器生成说明性数据包（informational packet）。举例来说，它可以阻止通常由路由器生成的 Internet 控制消息协议（ICMP）消息和 SNMP 陷阱（trap）。与控制面板监管相类似，安全访问模式将使用熟悉的 MQC 界面。
有关安全访问模式的更多信息，请访问：https://www.cisco.com/en/US/products/ps6540/prod_bulletin09186a00801d7229.html#wp1002091

原始 IP 流量导出

要对网络流量执行详尽的安全分析，许多网络管理员都需要借助工具来实现，比如说协议分析程序或缓解服务器。但是，目前只能通过直接插入（inline insertion）的方式来将这些工具连接到路由器，而这在操作上是非常困难的。
原始 IP 流量导出（Raw IP Traffic Export）是一个轻量级的思科 IOS 软件特性，用于将到达到离开网络设备的 IP 数据包导出到外部设备。它使用指定的局域网接口来导出所捕获的 IP 数据包。其目标是将原始 IP 数据包以未修改的格式导出到指定设备（比如说数据包分析程序或 IDS 设备）。
原始 IP 流量导出的特性包括：

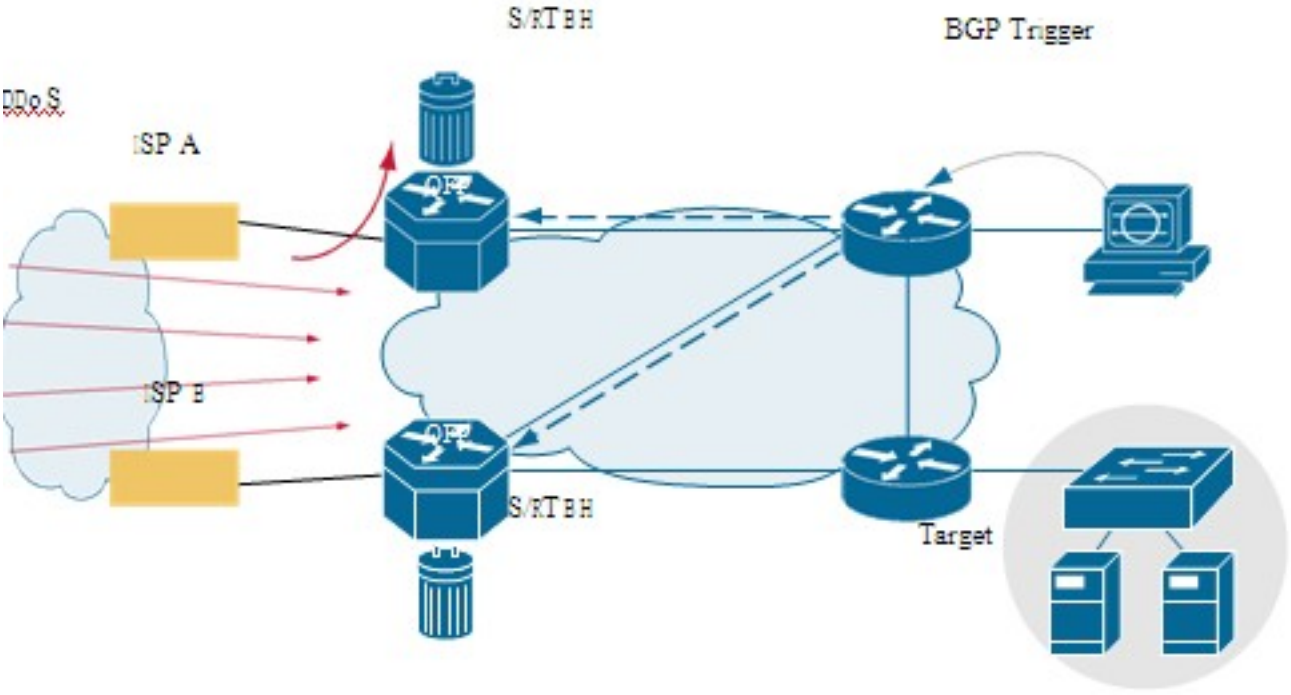
- 通过过滤功能（使用 ACL），可以只导出感兴趣的流量
- 采样选项可以减少流量输出量
- 使用与目标主机相关的 MAC、802.1q 或者交换机间链路（Inter-Switch Link，ISL）地址（而不是 IP 地址）来指定执行导出的以太网端口。
- 当特性激活或禁用时设置 syslog 信息

有关原始 IP 流量导出的更多信息，请访问：http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rawip.html。

基于源的远程触发黑洞过滤

如果您的组织设法查明了攻击的来源（比如说，通过分析 NetFlow 数据），那么可以采用 ACL 这样的围堵机制。检测到攻击流量并对其进行分类之后，您可以为必要的路由器创建并部署适当的 ACL。由于这种手动流程有时非常耗时且复杂，因此许多客户都可以使用边界网络协议（Border Gateway Protocol，BGP）来迅速有效地向所有路由器传递抛弃信息。这项技术的专业名称是远程触发黑洞（Remotely Triggered Blackhole，RTBH），它可以将受害者 IP 地址的下行设定为无效

（null）接口。发送给受害者的流量将在网络入口处被抛弃。
另一种方案是抛弃来自特定源的流量。此方法类似于之前介绍过的一种抛弃机制，即通过预先部署的单播反向路径转发（URPF）来抛弃源“无效”的数据包。无效的路由器。发送 BGP 时将使用相同的基于目标的抛弃机制，并且此更新会将源的下行设置为 null0。现在，接口在启用了 URPF 之后将抛弃来自这个源的所有流量。虽然具备可伸缩性，但 BGP 触发的抛弃机制会限制应对攻击时的离散水平；如前所述，它们会抛弃来自黑洞源或发往黑洞目标的所有流量。在许多情况下，这种方式可以有效阻截大多数攻击，并且可以缓解间接损失（参见图 6）。
有关基于源的 RTBH 过滤的更多信息，请访问：
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6642/prod_white_paper0900aecd80313fac.pdf。
图 6. 使用基于源的 RTBH 过滤功能实时阻截 DDoS 攻击



单播反向路径转发

URPF 可以帮助限制企业网络中的恶意流量。它的工作原理是支持路由器验证所转发数据包中的源地址的可访问性（reachability）。此功能可以限制伪造地址进入网络。如果源 IP 地址无效，则数据包将被抛弃。思科 1900、2900 和 3900 系列集成多业务路由器支持严格格式和宽松模式。
当管理员在严格模式下使用 URPF 时，接收数据包的接口必须是路由器用于转发返回数据包的接口。当接口接收到合法流量时，如果路由器未选择发送返回流量，则严格模式下的 URPF 配置可以抛弃这些合法流量。当网络中出现不对称的路由路径时，则会出现抛弃合法流量的情况。
当管理员在宽松模式下使用 URPF 时，则源地址必须出现在路由表中。管理员可以使用 allow-default 选项来更改此行为，这将允许在源验证过程中使用默认路由器。此外，如果数据包所包含的源地址的返回路由目标指向 null0 接口，则该数据包将被抛弃。在 URPF 宽松模式下，您可以指定一个访问列表来允许或拒绝特定的源地址。
有关 URPF 的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_cfg_unicast_rpf.html
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_urpf_mib.html

数字镜像签名

数据镜像签名（Digital Image Signing）通过附加数字签名提供了一种验证软件镜像身份的途径。它使用 SHA-512 程式计算软件镜像的唯一 64 位散列值。然后，使用一个 RSA 2048 位私钥对该散列值进行加密，并将生成的数字签名附加到软件镜像。
在加载软件镜像的过程中，路由器使用公钥对嵌入在镜像中的散列进行解密，然后验证镜像的身份

是否真实无误。如果发现镜像经过修改，则会弹出镜像，以保护设备。
有关数据镜像签名的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_ips5_sig_fs_ue.html
。

思科 IOS 软件登录增强

为了控制对网络设备的访问，思科 IOS 软件要求用户在登录到设备时输入用户名和密码。遗憾的是，黑客可以通过字典攻击来破解密码。在这种攻击中，黑客编写暴力破解工具来尝试用户名和密码的各种组合，从而获取对设备的访问权。
思科 IOS 软件登录增强（Cisco IOS Software Login Enhancements）为用户登录提供了一种全新的基于时间的维度。网络管理员可以使用此特性来指定重试的间隔时间，从而缓解字典攻击的威胁。用户必须在指定的时间内成功登录设备，否则其帐户将被锁定。
有关思科 IOS 软件登录增强的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_login.html。

基于角色的 CLI 访问

基于角色的 CLI 访问（Role-Based CLI Access）允许网络管理员定义“视图”（即一组操作命令和配置功能）来限制用户对思科 IOS 软件的访问。视图可以限制用户访问思科 IOS 软件 CLI 和配置信息，并且可以定义允许执行的命令以及配置信息的可见性。基于角色的 CLI 访问的应用包括网络管理员为特定功能提供安全个人访问。此外，服务提供商可以使用此特性为最终客户提供受限访问，以便于帮助客户诊断网络。
有关基于角色的 CLI 访问的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_role_base_cli.html。

SSHv2

安全壳 (SSH) 协议第 2 版提供了全新的、更加强大的认证和加密功能。通过加密连接处理各种类型的流量时，系统为您提供了更加丰富的选择，包括文件复制和电子邮件协议。网络安全也因为更加丰富的认证功能得到了增强，包括数字证书和更多双因素认证选项。
有关 SSH 的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_secure_shell_ps6441_TSD_Products_Configuration_Guide_Chapter.html

SNMPv3

SNMPv3 是一种基于交互标准的网络管理协议，它通过对网络上的数据包进行认证和加密提供对设备的安全访问SNMPv3 所提供的安全特性包括：

- 消息完整性：确保数据包在传输过程中未被修改
- 认证：验证消息来自有效源
- 加密：对数据包内容进行加密，防止未授权源看到它

SNMPv3 同时提供了安全模型和安全水平。安全模型是为用户以及用户所在用户组建立的一种认证策略。安全水平是安全模型中准许的安全性水平。安全模型与安全水平相结合可以确定采用哪种安全机制来处理 SNMP 数据包。共有三种安全模型可用：SNMPv1、SNMPv2c 和 SNMPv3。
有关 SNMPv3 的更多信息，请访问：
http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/snmpv3ae.html
http://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ipsec_snmp_supp.html
http://www.cisco.com/en/US/docs/ios/12_0t/12_0t3/feature/guide/Snmp3.html

结束语

思科安全路由器提供了多种安全技术来为远程办公室、远程工作人员和移动用户提供保护。其中包

括各种站点间和远程访问 VPN 技术，它们提供了隐私和数据完整性、边界安全性、入侵防御和零日保护功能、信任和身份保护功能以及一些基本的安全特性。仅就其本身而言，这些技术所带来的价值足以超过购买路由器所花费的成本。此外，思科安全路由器在部署和管理上便捷性可以将总体拥有成本控制在较低水平，从而使解决方案能够随时间不断积累价值。