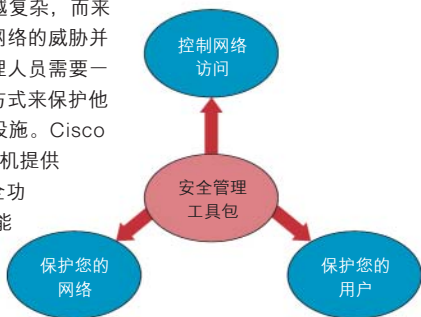


简介

网络攻击正在变得越来越复杂，而来自于网络内部的攻击对网络的威胁并不亚于外部的。安全管理人员需要一种可扩展的、可管理的方式来保护他们的网络和用户的基础设施。Cisco Catalyst 6500 系列交换机提供了业界功能最丰富的安全功能。其中的一些主要性能让 Catalyst 6500 在各个安全领域独树一帜，下面将详细加以介绍。

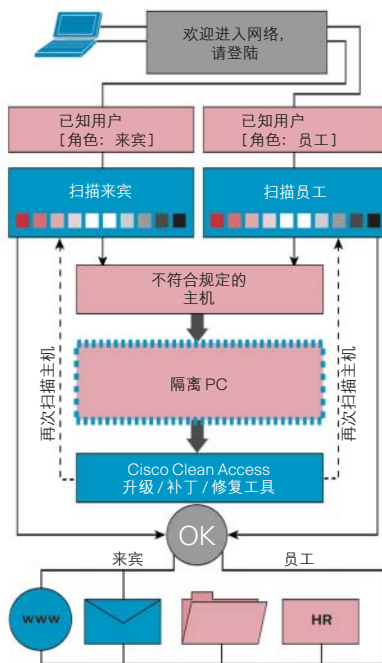


控制网络访问

网络安全管理人员最关心的是保护传输中的网络资源和用户信息。为此，第一步要做的是在网络的入口防范未经授权的访问。



- 802.1x 是一种第二层身份验证机制。除了标准的 802.1x 功能集——端点验证、VLAN 分配、语音 VLAN ID 支持等，Catalyst 6500 还支持多种独有的改进功能，例如：
 - 802.1x 与 ACL/QoS 结合——如果用户不断地从一个网络地点转移到另一处，这项功能简化了对 ACL、QoS 和其他基于端口的策略的管理——它们随着用户自动移动。
 - 802.1x 与 HA 结合——如果某个交换管理引擎发生故障，冗余交换管理引擎会接替它的工作，而且数百个已经通过身份验证的 802.1x 客户端将不需要再次进行验证。
- 您可能拥有一个功能强大的 802.1x 身份验证系统。但是怎样对那些客户端不支持 802.1x 的用户进行身份验证呢？
 - Web 身份验证——让用户可以通过一个基于 Web 的验证进程访问网络。例如，宾馆中的旅客的笔记本电脑可能不支持 802.1x。这项功能可以让不支持 802.1x 的客户端访问网络。
 - MAC 身份验证——对于性能有限的主机（例如打印机和扫描仪），交换机可以利用设备的 MAC 地址进行代理验证。



- 网络准入控制 (NAC)——无论接入设备是集线器、交换机还是路由器，您是否都需要在网络中建立一种统一的访问控制机制？NAC 是思科联合多家安全厂商共同推出的、覆盖整个网络的安全架构。该网络将根据设备的安全状况为其提供适当的访问权限——例如，是否安装了最新的安全补丁、DAT 文件、病毒检查等。
 - NAC 可以为不同的部署场合提供支持：
 - 直接连接到交换机端口的设备
 - 通过共享设备（例如集线器）直接连接到交换机端口的设备
 - 在一个 IP 网络上，通过路由器连接到交换机端口的设备
 - 如果终端设备不能响应交换机的扫描请求，NAC 将会为评估无响应设备的安装状况提供另一种替代机制。
 - 基于策略的 ACL——频繁地在端口之间移动的主机，或者频繁地更改端口上的安全策略，都可能会在硬件上触发复杂的 ACL 合并。PBACL 对这种动态网络进行了专门的优化，可以在执行安全策略方面提供独一无二的灵活性。
- 防火墙服务模块——通过向 Cisco Catalyst 6500 机箱添加一个防火墙服务模块，可以监督和控制访问网络的用户。集成化方法可以消除独立设备所带来的成本和复杂性。

保护您的用户

您能否及时发现您的网络中发生的“中间人攻击”？您可能会对其一无所知。因为这种攻击，信息可能会在传输中被窃取，而身份证明可能会在相关各方都毫不知情的情况下被盗用。

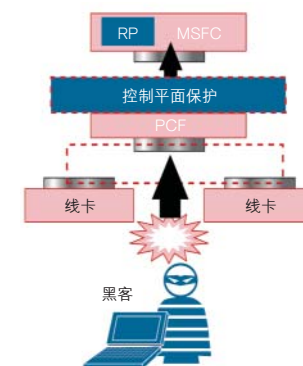
为了防范“中间人攻击”，Cisco Catalyst 6500 系列提供了一个名为思科集成化安全工具包 (CIST)，其中包含三种功能。



- DHCP 监听——建立一个列表，将每个客户端的 IP 地址与 MAC 地址一一对应起来。下面两种特性可利用该表防范 MITM 攻击。
- 动态 ARP 检测——查询 DHCP 监听表，防止黑客篡改交换机的 ARP 表。
- IP 源保护——查询 DHCP 监听表，防止黑客使用虚假的 IP 地址。

- 专用 VLAN——在用户对有人窃听他们的流量非常敏感的环境中，PVLAN 可以提供将用户彼此隔离的功能。它可以为数据中心、配线间和城域以太网提供增强的 L2 安全。PVLAN 由 Cisco Catalyst 6500 系列首次推出。一些即将增加的功能包括：

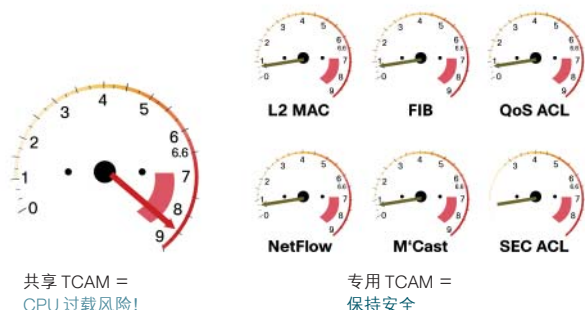
- 混合中继——在数据中心，主机往往需要访问多台服务器。这项功能允许多台服务器借助一条统一的中继线路连接到交换机，从而提高端口的使用率。
- 专用主机——在城域以太网中，这项功能将允许在中继端口上进行 DSLAM 汇聚。
- 数据加密——为了保护传输中的用户信息，可以选择下列加密方式：
 - SSHv2 和 3DES 加密结合。所有 Cisco Catalyst 6500 系列软件镜像都支持这项功能。
 - 硬件加速加密。可以选择 IPsec VPN 服务模块或者 SSL VPN 服务模块。



保护您的网络

在遭受“拒绝服务”攻击时，交换机本身就是攻击目标。怎样防止您的网络遭受这样的攻击？

- **控制平面监管** —— 不要失去对您的交换机的控制权！控制平面速率限制器和监管器是基于硬件的，可限制发往 CPU 的流量速率，从而最大限度地降低拒绝服务攻击力。
- **专用于 ACL 的 TCAM** —— 低端交换机可能会使用共享 TCAM 空间，从而导致 ACL 溢出。ACL 溢出会触发基于软件的转发和对性能造成严重的影响。
 - Cisco Catalyst 6500 系列提供了广泛的 ACL 支持，有 32K 专用 TCAM 空间，从而最大限度地减小发生 ACL 溢出的可能性。
 - 防止基于软件的转发和保持安全。

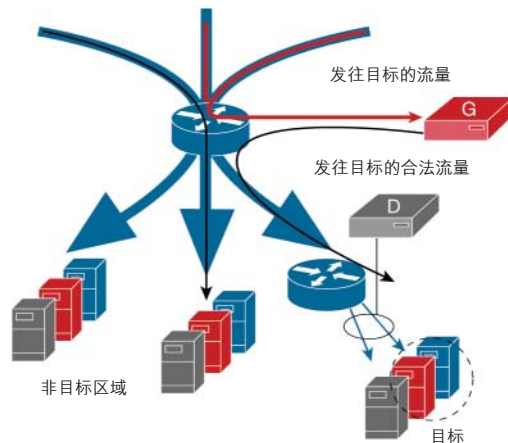


- **基于硬件的 MAC 学习** —— 对于通过软件学习 MAC 地址的低端交换机，黑客可以凭借生成数千个虚假 MAC 地址占据 CPU 资源。Cisco Catalyst 6500 系列通过硬件学习 MAC 地址，因而可以避免这种 DoS 攻击。
- **多路径 uRPF** —— 典型的 DoS 攻击从地址伪装开始。多路径单播 RPF 可以通过对分组进行反向路径转发检查，防止源地址伪装 —— 即使在多个路径指向同一个来源时也是如此。
- **基于用户的速率限制** —— 为了防止某个用户独占网络资源，通过硬件动态学习流量和对每个数据流进行速率限制。
- **广播抑制** —— 黑客可以利用流量阻塞网络，让其处于无法使用的状态。Cisco Catalyst 6500 系列提供了一组泛洪控制工具 —— 流量风暴控制、未知单播泛洪阻塞和单播泛洪防范 —— 以防止网络遭受此类 DoS 攻击。
- **IDS/AD 服务模块** —— 入侵检测和异常流量检测服务模块可集成到 Catalyst 6500 中，提供独一无二的安全性和业界领先的吞吐量。

服务模块

利用新一代的集成化服务模块，Cisco Catalyst 6500 平台为网络带来了新的安全功能和更高价值，同时不会增加网络的复杂度和成本。

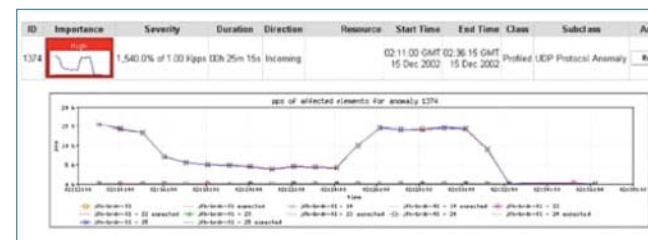
- **防火墙服务模块 (FWSM)** —— 提供业界最快的防火墙数据速率：5Gbps 吞吐率，每秒 10 万个连接，以及 100 万个并发连接。基于 Cisco PIX® 技术。
- **异常检测 / 保护模块 (ADSM/AGSM)** —— 进行先进的流量行为分析，检测并自动消除最大范围的 DDoS 攻击。



- **入侵检测系统模块 (IDS)** —— 完全集成的入侵检测功能可在交换机的背板进行流量监控。提供实时的安全威胁检测、智能威胁分析和简便的管理。
- **网络分析模块 (NAM)** —— 为实时流量分析提供应用级的可见度。信息能用于监控 VoIP 质量、抑制非生产性网络流量和优化 WAN 带宽。
- **IPSec VPN 服务模块 (IVSM)** —— 提供 IPSec VPN 服务，而不需要重叠设备或者网络调整。提供 2.5Gbps 的 AES 加密流量；支持 8000 个有效隧道并每秒可激活隧道 60 次。
- **WebVPN 或者 SSL VPN 服务模块 (SSLSM)** —— 利用 SSL 来提高性能和由 Web 激活的应用的安全性。同时支持 8000 个用户和最多 32000 个并发连接。

安全管理

- **CVDM** —— 您如何管理如此繁多的安全功能？Catalyst 6500 为配置这些功能和服务模块提供了基于 CLI 的传统配置工具和基于 GUI 的 CiscoView 设备管理器。
- **集成化 NetFlow** —— 精明的攻击者一直在调整他们的攻击方法。要击败这些攻击者，最重要的任务是在攻击传染到整个网络之前迅速地发现攻击。Catalyst 6500 提供了集成化 NetFlow 用来发现硬件中的异常行为流量。Catalyst 6500 所独有的这项功能让安全管理人员轻松地跟踪某个异常流量模式的来源，进而制止攻击。



- **PSIRT 补丁** —— 利用 Cisco IOS® 软件模块化，Catalyst 6500 可以提供 PSIRT 运行时补丁安装功能。这意味着：
 - 在安装安全升级补丁时不需要中断正常运行
 - 小型补丁 vs. 镜像升级：最大限度地减少新的安全漏洞
 - 缩短在安装完安全升级之后需要的审核时间
- **AutoSecure** —— 安全管理人员过去需要花费大量的时间确保网络中的所有交换机都采用了统一的安全策略。这项功能自动地在交换机上设置一个标准的安全策略，进而迅速地让整个网络进入安全状态。
- **NAM** —— 利用网络分析服务模块来监控、优化和管理流量，特别是 WAN 边缘的流量。

如需了解更多信息，请访问：<http://www.in.cisco.com/dsw/switching/>。