硬化Cisco IOS设备的Cisco指南

目录

管理平面
控制层面
数据层面

简介

本文包含信息帮助您巩固您的Cisco IOS系统设备，强化您的网络整体安全。本文档围绕网络设备的功能所属的三个平面来组织内容，提供每项所包含功能的概述和对相关文档的引用。

网络的三架功能飞机-管理层面、控制层面和数据层面-中的每一架提供需要保护的另外功能。

- 管理层面-管理层面管理发送到Cisco IOS设备和由应用程序和协议做成例如安全壳SSH和简单网络管理协议(SNMP)的流量。
- 控制层面-网络设备的控制层面处理是至高无上的维护网络基础设施的功能的流量。控制层面由网络设备之间的应用程序和协议组成，其中包括边界网关协议 (BGP) 以及增强型内部网关路由协议 (EIGRP) 和开放最短路径优先 (OSPF) 等内部网关协议 (IGP)。
- 数据层面-数据层面通过网络设备转递数据。数据层面不包括发送到本地 Cisco IOS 设备的数据流。

通常，本文档对安全功能的介绍将提供足够详细的信息，以便于您配置该功能。但是，在未能提供详细信息的情况下，我们会对该功能进行说明，以便于您评估是否需要对该功能引起额外的关注。本文档将在可能和适当的地方提供一些在实施后将有助于保护网络安全的建议。

贡献用Shashank辛哈， Cisco TAC工程师。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

确保运行安全

确保网络运行安全是一个非常重要的主题。虽然本文档的大部分内容主要用于说明如何确保 Cisco IOS 设备的配置安全，但仅仅通过配置并不能完全确保网络安全。网络上使用的运行过程与底层设备的配置一样，在很大程度上影响着网络的安全。

这些主题中包含一些建议您实施的操作建议。这些主题主要着眼于网络运行的特定重要方面，因此并不全面。

监视 Cisco 安全建议及响应

Cisco 产品安全事件响应小组 (PSIRT) 针对 Cisco 产品中与安全相关的问题，创建并维护通常称为《PSIRT 建议》的出版物。可使用“Cisco 安全响应”这一方法来传达严重程度较低的问题。在 http://www.cisco.com/go/psirt 上可以找到安全建议及响应。

在 Cisco 安全漏洞策略中可以找到有关这些通信手段的其他信息。

为维护网络安全，您需要了解已发布的 Cisco 安全建议和响应。您首先需要了解有关漏洞的知识，然后才能评估漏洞可能对网络造成的威胁。要完成此评估过程，请参阅安全漏洞通告风险分类以获取相应的帮助。

利用身份验证、授权和记账

验证、授权和统计(AAA)框架是重要巩固网络设备。AAA 框架提供针对管理会话的身份验证功能，还可以将用户限制为只能执行特定的、管理员定义的命令，并记录所有用户输入的全部命令。请参阅本文的认证、授权和记帐部分关于如何有效利用AAA的更多信息。

集中处理日志收集和监视

为了获取关于存在的知识，涌现，并且有历史的事件与安全事件涉及，您的组织必须有事件日志和相关性的一个统一的策略。此策略必须利用来自所有网络设备的日志记录，并使用预封装的可自定义关联功能。

实施集中式日志记录后，您必须开发一个用于进行日志分析和事件跟踪的结构化方法。基于您组织的需要，此方法的范围可以介于对日志数据的简单复查和基于规则的高级分析之间。

有关如何在 Cisco IOS 网络设备上实施日志记录的详细信息，请参阅本文档的日志记录最佳实践部分。

尽可能使用安全协议

许多协议用于传送敏感的网络管理数据。您必须尽可能使用安全协议。一种安全协议选择包括使用 SSH（而不使用 Telnet），以便对身份验证数据和管理信息进行加密。此外，在复制配置数据时，您必须使用安全的文件传输协议。例如，使用安全复制协议 (SCP) 代替 FTP 或 TFTP。

请参阅本文的安全交互管理会话部分关于Cisco IOS设备的更多信息安全管理。

使用 NetFlow 获得数据流可见性

使用 NetFlow 可以监视网络中的数据流。尽管最初用于将数据流信息导出到网络管理应用程序中，但 NetFlow 也可用于在路由器上显示数据流信息。使用此功能可以实时查看经过网络的数据流。不论数据流信息是否导出到远程收集器，建议您针对 NetFlow 配置网络设备，以便可以在需要时反应性地使用 NetFlow。

关于此功能的更多信息是可用的在本文的流量识别和Traceback部分和在http://www.cisco.com/go/netflow（仅限注册用户）。

配置管理

配置管理是用于建议、审查、批准并部署配置更改的过程。在有关 Cisco IOS 设备配置的上下文中，配置管理的另外两个方面至关重要：配置存档和安全。

您可以使用配置存档来回滚对网络设备所做的更改。在有关安全的上下文中，配置存档还可用于确定已做出的安全更改，以及发生这些更改的时间。与 AAA 日志数据相结合，此信息可在对网络设备进行安全审计时提供帮助。

Cisco IOS 设备的配置包含许多敏感的详细信息。用户名、口令和访问控制列表的内容都属于此类型的信息。需要保护用于将 Cisco IOS 设备配置存档的存储库。以不安全的方式访问这些信息可能会破坏整个网络的安全。

管理平面

管理平面包含用于实现网络管理目标的功能。这包括使用SSH的交互管理会话，以及统计信息采集与SNMP或Netflow。考虑网络设备的安全时，保护管理平面非常重要。如果安全事件能够破坏管理平面的功能，您可能将无法恢复网络或使网络变得稳定。

本文档的这些部分详细说明了 Cisco IOS 软件中提供的有助于强化管理平面的安全功能和配置。

一般管理平面强化

管理平面用于访问、配置和管理设备，并用于监视该设备的运行情况及部署该设备的网络。管理平面是接收和发送用于运行这些功能的数据流的平面。因为控制层面的操作直接地影响管理层面的操作，您必须巩固设备的管理层面和控制层面。以下为管理平面使用的协议列表：

- 简单网络管理协议 (SNMP)
- Telnet
- Secure Shell 协议 (SSH)
- 文件传输协议
- 简单文件传输协议 (TFTP)
- 安全复制协议 (SCP)
- TACACS+
- RADIUS
- Netflow
- 网络时间协议 (NTP)
- Syslog

发生安全事件时，必须采取相应的步骤确保管理和控制层面可以继续运行。如果其中一个平面被顺利地攻陷，则可能会危及所有平面的安全。

密码管理

口令控制对资源或设备的访问。这通过定义用于对请求进行身份验证的口令或加密口令来实现。收到针对资源或设备的访问请求时，将对该请求进行质询，以便验证口令和身份，然后再根据质询结果授予、拒绝授予或限制访问权限。作为一项安全最佳实践，口令必须使用 TACACS+ 或 RADIUS 身份验证服务器进行管理。然而，请注意在TACACS+的失败或RADIUS服务情形下，特许访问的一本地配置的口令还是必要。设备的配置中也可能存在其他口令信息，如 NTP 密钥、SNMP 社区字符串或路由协议密钥。

enable secret 命令用于设置授予对 Cisco IOS 系统的特权管理访问权限的口令。必须使用 enable secret 命令，而不是更旧的 enable password 命令。enable password 命令使用的是一种加密强度较低的加密算法。

如果没有设置 enable secret，但为控制台 tty 线路配置了口令，则可以使用控制台口令（甚至是从远程虚拟 tty (vty) 会话中）获得特权访问权限。此操作几乎肯定是不必要的，这也是另一个确保配置 enable secret 的原因。

service password-encryption 全局配置命令指示 Cisco IOS 软件对口令、质询握手身份验证协议 (CHAP) 加密口令和保存在其配置文件中的类似数据进行加密。此类加密用于防止他人在无意中看到口令，例如他们越过管理员查看屏幕时。然而， service password-encryption命令使用的算法是关于密码器的简单Vigen。此算法甚至无法阻止稍微有些老练的攻击者对配置文件进行深入的

分析，因此不能用于上述目的。任何包含加密口令的 Cisco IOS 配置文件，都必须和这些口令的明文列表一样受到严密的保护。

虽然 enable secret 命令并不使用这一加密强度较低的加密算法，但 enable password 全局配置命令以及 password 行配置命令均使用该加密算法。必须去除这种类型的口令，并需要使用 enable secret 命令或增强的口令安全功能。

enable secret 命令和“增强的口令安全”功能将消息摘要 5 (MD5) 用于口令散列。此算法曾受到相当多的公开检验，并被认为是不可逆的。但是，此算法容易受到字典攻击。在字典攻击中，攻击者尝试字典或其他一组候选口令中的每一个词，希望找到匹配项。因此，必须安全地存储配置文件，并仅与受信任的个人共享该文件。

增强的口令安全

在 Cisco IOS 软件版本 12.2(8)T 中引入的“增强的口令安全”功能允许管理员为 username 命令配置 MD5 口令散列。在此功能之前，有以下两种类型的口令：类型0，是明文密码和类型7，使用从Vigen的算法关于密码器。“增强的口令安全”功能不能与要求明文口令可检索的协议（如 CHAP）一起使用。

要使用 MD5 散列功能加密用户口令，请发出 username secret 全局配置命令。

```
!

username <name> secret <password>

!
```

有关此功能的详细信息，请参阅增强的口令安全。

登录密码重试锁定

登录密码重试次数中断功能，已添加在Cisco IOS软件版本12.3(14)T，允许您在不成功登录尝试以后配置的号码锁定本地用户帐户。一旦用户被锁定，在您将其帐户取消锁定之前，其帐户将保持锁定状态。使用此功能无法锁定配置有权限级别 15 的授权用户。因此，必须将具有权限级别 15 的用户数量保持到最少。

请注意，如果达到该失败登录尝试次数，即使授权用户也可能会将自己锁定在设备之外。此外，恶意用户也可能会使用有效用户名重复进行身份验证尝试，从而创造出拒绝服务 (DoS) 条件。

本示例说明如何启用“登录口令重试锁定”功能：

```
!

aaa new-model
aaa local authentication attempts max-fail <max-attempts>
aaa authentication login default local

!

username <name> secret <password>

!
```

此功能也适用于 CHAP 和口令身份验证协议 (PAP) 等身份验证方法。

No Service Password-Recovery

在 Cisco IOS 软件版本 12.3(14)T 及更高版本中，“禁用口令恢复”功能禁止任何具有控制台访问权限的用户以不安全的方式访问设备配置和清除口令。此功能还可用于阻止恶意用户更改配置注册值和访问 NVRAM。

```
!

no service password-recovery

!
```

Cisco IOS软件提供取决于在对ROM监控模式的一密码恢复流程(ROMMON)的访问在系统启动期间，使用Break键。在ROMMON中，设备软件可以重新加载为了提示包括新密码的新的系统配置。

当前的口令恢复过程允许任何具有控制台访问权限的用户访问设备及其网络。No service password-recovery功能不防止Break键顺序的完成和输入ROMMON在系统启动期间。

如果在某设备上启用 no service password-recovery，则建议保存该设备配置的脱机副本，并实施配置存档解决方案。启用此功能后，如果需要恢复 Cisco IOS 设备的口令，整个配置将被删除。

关于此功能的更多信息参考的安全ROMMON配置示例。

禁用未使用的服务

作为一项安全最佳实践，必须禁用任何不必要的服务。使用用户数据报协议(UDP)的特别是那些，用于合法目的偶尔地使用这些不需要的服务，但是可以使用为了发起由信息包过滤否则防止的DoS和其他攻击。

必须禁用 TCP 和 UDP 小型服务。这些服务包括：

- echo（端口号 7）
- discard（端口号 9）
- daytime（端口号 13）
- chargen（端口号 19）

虽然可以通过反欺骗访问列表来避免对这些小型服务的滥用或降低其危险性，但是，仍然必须在网络中的任何可访问的设备上禁用这些服务。默认情况下，Cisco IOS 软件版本 12.0 及更高版本中已禁用这些小型服务。在更低版本的软件中，可以发出 no service tcp-small-servers 和 no service udp-small-servers 全局配置命令来禁用它们。

下面是在未被使用时必须禁用的其他服务的列表：

- 请发出 no ip finger 全局配置命令以禁用 Finger 服务。默认情况下，高于 12.1(5) 及 12.1(5)T 版本的 Cisco IOS 软件版本禁用此服务。
- 请发出 no ip bootp server 全局配置命令以禁用 Bootstrap 协议 (BOOTP)。
- 在 Cisco IOS 软件版本 12.2(8)T 及更高版本中，请在全局配置模式下发出 ip dhcp bootp ignore 命令以禁用 BOOTP。这样可以使动态主机配置协议 (DHCP) 服务停留在启用状态。
- 如果不需要 DHCP 中继服务，则可以禁用 DHCP 服务。请在全局配置模式下发出 no service dhcp 命令。
- 请在接口配置模式下发出 no mop enabled 命令以禁用维护操作协议 (MOP) 服务。
- 请发出 no ip domain-lookup 全局配置命令以禁用域名系统 (DNS) 解析服务。
- 请在全局配置模式下发出 no service pad 命令以禁用用于 X.25 网络的分组拆/装器 (PAD) 服务。
- HTTP服务器可以用no ip http server命令禁用在全局配置模式，并且安全HTTP (HTTPS)服务器可以用没有IP HTTP安全服务器全局配置命令禁用。
- 除非 Cisco IOS 设备在启动期间从网络中检索配置，否则必须使用 no service config 全局配置命令。这防止Cisco IOS设备尝试寻找在网络的一个配置文件与TFTP。
- Cisco 发现协议 (CDP) 是一种网络协议，使用该协议可以发现其他用于邻居邻接和网络拓扑的、启用了 CDP 的设备。CDP 可以由网络管理系统 (NMS) 使用，也可以在故障排除期间使用。必须对所有连接到不受信任的网络的接口禁用 CDP。使用 no cdp enable 接口命令可完成此操作。或者，也可以使用 no cdp run 全局配置命令全局禁用 CDP。请注意，恶意用户可能会将 CDP 用于侦察和网络映射。
- 链路层发现协议 (LLDP) 是一种在 802.1AB 中定义的 IEEE 协议。LLDP 与 CDP 类似。但是，该协议允许在其他不支持 CDP 的设备之间进行互操作。必须以处理 CDP 的同一方式对 LLDP 进行处理，对所有连接到不受信任的网络的接口禁用 LLDP。为了完成此操作，请发出 no lldp transmit 和 no lldp receive 接口配置命令。请发出 no lldp run 全局配置命令以全局禁用 LLDP。恶意用户也可能将 LLDP 用于侦察和网络映射。

EXEC 超时

要设置 EXEC 命令解释程序在终止会话之前等待用户输入的时间间隔，请发出 exec-timeout 行配置命令。必须使用 exec-timeout 命令注销 vty 或 tty 线路上处于空闲状态的会话。默认情况下，会话将在处于非活动状态 10 分钟之后断开连接。

```
!

line con 0
exec-timeout <minutes> [seconds]
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

TCP 会话的 Keepalive

service tcp-keepalives-in和service tcp-keepalives-out全局配置命令使设备发送TCP会话的TCP Keepalive。必须使用此配置在设备的入站连接和设备的出站连接上启用 TCP keepalive。这样可以确保在连接远程端上的设备仍然处于可访问状态，并且半开放的连接或孤立的连接会从本地 Cisco IOS 设备上删除。

```
!

service tcp-keepalives-in
service tcp-keepalives-out
!
```

管理接口使用

设备的管理平面可以通过物理或逻辑管理接口以带内或带外方式访问。理想情况下，应为每台网络设备同时提供带内和带外管理访问，以便可以在网络中断期间访问管理平面。

逻辑环回接口是用于对设备进行带内访问的最常用接口之一。环回接口始终处于接通状态，而物理接口可以更改状态，并且该接口可能无法进行访问。建议为每台设备添加一个环回接口作为管理接口，并将其专门用于管理平面。这使得管理员可以在整个网络中应用管理平面策略。在设备上配置环回接口后，管理平面协议（如 SSH、SNMP 和 syslog）可以使用该接口发送和接收数据流。

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
```

内存阈值通知

使用 Cisco IOS 软件版本 12.3(4)T 中添加的“内存阈值通知”功能可以缓解设备上内存不足的状况。此功能使用两个方法为了完成此：“内存阈值通知”和“内存保留”。

“内存阈值通知”会生成日志消息以指出设备上的可用内存量已降低至低于配置的阈值。本配置示例说明如何使用 memory free low-watermark 全局配置命令启用此功能。这使设备能够在可用内存量降低至低于指定的阈值时生成通知，并在可用内存量上升到高于指定的阈值 5% 时再次生成通知。

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

使用“内存保留”是为了有足够的内存可用于重要通知。本配置示例说明如何启用此功能。该功能可确保即使设备的内存耗尽，管理进程仍然能够继续运行。

```
!
memory reserve critical <value>!
```

有关此功能的详细信息，请参阅内存阈值通知。

CPU 阈值通知

使用 Cisco IOS 软件版本 12.3(4)T 中引入的“CPU 阈值通知”功能可以检测到设备上的 CPU 负载何时超过配置的阈值，并在发生这种情况时收到相应的通知。负载超过阈值时，设备会生成并发送 SNMP 陷阱消息。Cisco IOS 软件支持两种 CPU 使用率阈值设置方法：“上升阈值”和“下降阈值”。

本示例配置说明如何启用触发 CPU 阈值通知消息的上升阈值和下降阈值：

```
!

snmp-server enable traps cpu threshold
!

snmp-server host <host-address> <community-string> cpu
!

process cpu threshold type <type> rising <percentage> interval <seconds>
    [falling <percentage> interval <seconds>]
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

有关此功能的详细信息，请参阅 CPU 阈值通知。

保留内存以用于控制台访问

在 Cisco IOS 软件版本 12.4(15)T 及更高版本中，可以使用“保留内存以用于控制台访问”功能保留足够的内存，从而确保能够对 Cisco IOS 设备进行控制台访问以实现管理和故障排除目的。当设备在内存不足的情况下运行时，此功能特别有用。您可以发出 memory reserve console 全局配置命令启用此功能。本示例将 Cisco IOS 设备配置为保留 4096 千字节的内存以用于此目的。

```
!
memory reserve console 4096
!
```

有关此功能的详细信息，请参阅保留内存以用于控制台访问。

内存泄漏探测器

使用 Cisco IOS 软件版本 12.3(8)T1 中引入的“内存泄漏探测器”功能可以检测到设备上的内存泄漏。“内存泄漏探测器”能够发现所有内存池、数据包缓冲区和区块中的泄漏情况。内存泄漏是不能为任何有用用途提供服务的静态或动态内存分配。此功能主要用于检测动态内存分配。您可以使用 show memory debug leaks EXEC 命令检测到是否存在内存泄漏。

缓冲区溢出：检测并修复 Redzone 损坏

在 Cisco IOS 软件版本 12.3(7)T 及更高版本中，可以在设备上启用“缓冲区溢出：检测并修复 Redzone 损坏”功能，以检测并修复内存块溢出并继续运行。

可以使用这些全局配置命令来启用此功能。配置 show memory overflow 命令后，可以使用该命令显示缓冲区溢出检测和修复统计信

息。

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

改进的 Crashinfo 文件收集

“改进的 Crashinfo 文件收集”功能能够自动删除旧的 crashinfo 文件。当设备失败时，此功能，已添加在Cisco IOS软件版本12.3(11)T，允许设备恢复空间为了创建新建的crashinfo文件。使用此功能还可以配置要保存的 crashinfo 文件的数量。

```
!
exception crashinfo maximum files <number-of-files>
!
```

网络时间协议 (NTP)

网络时间协议 (NTP) 并不是一种特别危险的服务，但任何不必要的服务都可能代表攻击矢量。如果使用 NTP，则必须明确配置受信任的时间源并使用适当的验证。为了实现 syslog 目的（例如在对潜在的攻击进行取证调查期间），并且为了在依靠证书进行第 1 阶段验证时成功建立 VPN 连接，需要使用准确而可靠的时间。

- NTP时间区域-当您配置NTP时，时间区域需要配置，以便时间戳可以准确地关联。通常有配置设备的时间区域的两个途径在网络以一全局在线状态。一种方法是使用协调世界时 (UTC)（以前称为格林威治标准时间 (GMT)）配置所有网络设备。另一种方法是使用本地时区配置网络设备。关于此功能的更多信息可以在“时钟时区”找到Cisco产品文档的。

- NTP认证-如果配置NTP认证，提供保证NTP消息被交换在委托NTP对等体之间。

配置示例使用NTP认证：

客户端：

```
(设置) #ntp验证
(设置) #ntp认证密钥5 md5 ciscotime
(设置) #ntp信任键5
(设置) #ntp服务器172.16.1.5密钥5
```

服务器：

```
(设置) #ntp验证
(设置) #ntp认证密钥5 md5 ciscotime
(设置) #ntp信任键5
```

对网络的限制访问与基础设施ACL

基础架构访问控制列表 (iACL) 旨在防止直接与网络设备进行未授权通信，是可以在网络中实施的最为重要的安全控制之一。基础架构 ACL 利用了以下理念：几乎所有网络数据流都流经网络，但并非以网络本身为目标。

iACL被修建并且应用为了指定从需要允许到网络设备的主机或网络的连接。这些类型的连接通常包括 eBGP、SSH 和 SNMP。所需的连接被允许之后，所有其他发送到基础架构的数据流都被明确拒绝。然后，会明确允许所有经过该网络并且不以基础架构设备为目标的中转数据流。

iACL 提供的保护与管理平面和控制层面密切相关。通过对网络基础架构设备使用不重复的编址，可以更轻松地实施 iACL。有关 IP 编址的安全含义的详细信息，请参阅面向安全的 IP 编址方法。

本示例 iACL 配置说明了在开始 iACL 实施过程时必须用作起点的结构：

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit required connections for routing protocols and
!--- network management
!

permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
permit tcp host <trusted-management-stations> any eq 22
permit udp host <trusted-netmgmt-servers> any eq 161
!
!--- Deny all other IP traffic to any network device
!
```

```
deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

一旦创建，该 iACL 必须应用于所有面向非基础架构设备的接口。这包括与其他组织、远程访问段、用户段和数据中心中的段连接的接口。

有关基础架构 ACL 的详细信息，请参阅保护您的核心：基础架构保护访问控制列表。

ICMP 数据包过滤

Internet 控制消息协议 (ICMP) 设计为一种 IP 控制协议。因此，一般而言，该协议传达的消息可能会对 TCP 和 IP 协议产生深远的影响。虽然网络故障排除工具 ping 和 traceroute 使用 ICMP，但网络的正常运行很少需要外部 ICMP 连接。

Cisco IOS软件提供功能为了名义上特别地过滤ICMP消息或键入和编码。本示例 ACL 必须与前几个示例中的访问控制条目 (ACE) 一起使用，允许来自受信任管理工作站和 NMS 服务器的 ping，并阻止所有其他 ICMP 数据包：

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!

permit icmp host <trusted-management-stations> any echo
permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

过滤器IP段

被分段的IP信息包的过滤过程能形成对安全设备的一挑战。这是因为用于过滤 TCP 和 UDP 数据包的第 4 层信息仅存在于初始分段中。Cisco IOS软件使用一个特定方法为了根据配置的访问列表检查??液初始分段。Cisco IOS 软件根据 ACL 来评估这些非初始分段并忽略任何第 4 层过滤信息。这会使非初始分段仅仅在任何已配置 ACE 的第 3 层上进行评估。

在本示例配置中，如果以端口 22 上的 192.168.1.1 为目标的 TCP 数据包在传输过程中被分段，那么，第二个 ACE 将根据数据包中的第 4 层信息，按照预期丢弃该数据包的初始分段。但是，第一个 ACE 将完全根据数据包和 ACE 中的第 3 层信息来允许所有剩余的（非初始）分段。此方案显示在以下配置中：

```
!

ip access-list extended ACL-FRAGMENT-EXAMPLE
permit tcp any host 192.168.1.1 eq 80
deny tcp any host 192.168.1.1 eq 22
!>
```

由于分段处理的非直观性质，ACL 常常会在无意中允许 IP 分段。试图逃避入侵检测系统的检测时，也会经常使用分段功能。正是由于这些原因，IP 分段经常在攻击中被使用，并因此必须在任何已配置 iACL 的顶部明确地进行过滤。本示例 ACL 包括全面的 IP 分段过滤。本示例说明的功能必须与前面几个示例说明的功能结合使用。

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
!--- Deny all other IP traffic to any network device
!
```

```
deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

参考的访问控制列表和IP段关于ACL如何的更多信息处理被分段的IP信息包。

对过滤 IP 选项的 ACL 支持

Cisco IOS 软件版本 12.3(4)T 添加了对使用 ACL 以基于包含在数据包中的 IP 选项过滤 IP 数据包的支持。由于 IP 选项必须作为异常数据包进行处理，因此，这些选项对网络设备提出了一个安全方面的难题。这需要 CPU 付出一定的努力，而经过网络的典型数据包则没有这种需求。数据包中存在 IP 选项，还意味着可能有人会试图利用这些选项破坏网络中的安全控制或更改数据包的中转特征。正是由于这些原因，必须在网络边界过滤具有 IP 选项的数据包。

本示例必须与前面几个示例中的 ACE 一起使用才能完全过滤包含 IP 选项的 IP 数据包：

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets containing IP options
!

deny ip any any option any-options
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

过滤的ACL支持在TTL值

Cisco IOS软件版本12.4(2)T添加ACL支持过滤根据存活时间(TTL)值的IP信息包。当数据包由源流向目标时，IP 数据报的 TTL 值将按每台网络设备递减。虽然 TTL 的初始值因操作系统而异，但当 TTL 值达到零时，数据包必须被丢弃。减少TTL到零，并且的设备丢弃数据包，要求为了生成和发送ICMP超时消息到数据包的来源。

生成和传输这些消息属于异常处理。路由器可执行此功能，当的IP信息包数量就该超时时低，但是，如果由于的数据包数量超时高，这些消息生成和发射能浪费所有联机CPU资源。这提供了一个 DoS 攻击矢量。为此是设备需要被硬化使用IP信息包高速率就该超时的DOS攻击。

建议组织在网络边界使用较小的 TTL 值过滤 IP 数据包。使用不足以穿越网络的 TTL 值完全过滤数据包可以减轻基于 TTL 的攻击造成的威胁。

本示例 ACL 使用小于 6 的 TTL 值过滤数据包。这样做可以在宽度最多为 5 跳的网络上防范 TTL 到期攻击。

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets with TTL values insufficient to traverse the network
!

deny ip any any ttl lt 6
!
!--- Deny all other IP traffic to any network device
!

deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

permit ip any any
!
```

注意：一些协议做合法使用数据包与低值TTL。eBGP 就是这样一个协议。有关尽量避免受到基于 TTL 到期的攻击的详细信息，请参阅识别和防范 TTL 到期攻击。

有关此功能的详细信息，请参阅对按 TTL 值过滤的 ACL 支持。

安全交互管理塞申斯

使用设备的管理会话可以查看和收集有关设备及其运行的信息。如果这些信息泄露给恶意用户，则该设备可能会成为攻击目标，遭到攻陷并被用于执行其他攻击。任何具有对设备的特权访问权限的用户都有能力对该设备进行完全的管理控制。对安全管理会话为了防止信息描述和未经授权的访问是必要的。

管理平面保护

在Cisco IOS软件版本12.4(6)T和以后，功能管理层面保护(MPP)在哪个接口管理数据流允许管理员限制可以由设备接收。这向管理员提供了对设备以及访问设备的方式的更多控制。

此示例显示如何使MPP为了只允许SSH，并且在GigabitEthernet0/1的HTTPS建立接口：

```
!

control-plane host
 management-interface GigabitEthernet 0/1 allow ssh https
!
```

有关 MPP 的详细信息，请参阅管理平面保护。

控制层面保护

控制层面保护 (CPPr) 建立在“控制层面策略”功能的基础之上，用于限制和管制以 IOS 设备的路由处理器为目标的控制层面数据流。在 Cisco IOS 软件版本 12.4(4)T 中引入的 CPPr 将控制层面划分为几个不同的控制层面类别（称为“子接口”）。共有三种控制层面子接口：“主机”、“中转”和“CEF 异常”。此外， CPPr 还包括以下这些额外的控制层面保护功能：

- 波尔特过滤功能-此功能提供去已关闭或非侦听的TCP和UDP端口的管制或丢弃数据包。
- 队列阀值策略功能-此功能限制在控制层面IP Input queue允许数据包的数量指定的协议的。

CPPr允许管理员分类，修正和限制发送到一个设备管理目的有主机子接口的流量。例如，分类为主机子接口类别的数据包包括管理数据流（如 SSH 或 Telnet）和路由协议。

注意：CPPr不支持IPv6和限制到IPv4输入路径。

有关 Cisco CPPr 功能的详细信息，请参阅控制层面保护功能指南 - 12.4T 和了解控制层面保护。

加密管理塞申斯

由于信息在一交互管理会话上可以被透露，必须加密此流量，以便恶意用户不能获得访问到传送的数据。数据流加密允许对设备的一个安全远程访问连接。如果管理会话数据流是通过网络以明文形式发送的，则攻击者就可能获取有关设备和网络的敏感信息。

管理员能设立已加密和巩固对一个设备的远程访问管理连接有SSH或HTTPS (安全的超文体传输协议)功能的。Cisco IOS软件软件支持SSH版本1.0 (SSHv1)， SSH使用安全套接字协议层(SSL)和传输层安全的版本2.0 (SSHv2)和HTTPS (TLS)验证和数据加密。SSHv1和SSHv2不兼容。

Cisco IOS软件也支持安全的复制协议(SCP)，允许已加密和安全连接为了复制设备配置或软件镜像。SCP 依赖于 SSH。本示例配置在 Cisco IOS 设备上启用 SSH：

```
!

ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1
!

line vty 0 4
transport input ssh
!
```

本配置示例启用 SCP 服务：

```
!
```

```
ip scp server enable
!
```

下面是 HTTPS 服务的配置示例：

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

有关 Cisco IOS 软件 SSH 功能的详细信息，请参阅在运行 Cisco IOS 的路由器和交换机上配置Secure Shell和Secure Shell (SSH) 常见问题。

SSHv2

在Cisco IOS软件版本12.3(4)T介绍的SSHv2支持功能允许用户配置SSHv2。(SSHv1支持在Cisco IOS软件更早版本实现。) SSH运行在它上面可靠的传输传送层并且提供强认证和加密功能。为SSH定义的唯一的可靠的传输是TCP。SSH提供方法安全地访问和安全地执行on命令另一个计算机或设备在网络。在SSH被建立隧道的安全的复制协议(SCP)功能允许文件安全转移。

此配置示例启用SSHv2 (当SSHv1禁用)在Cisco IOS设备：

```
!

hostname router

!

ip domain-name example.com

!

crypto key generate rsa modulus 2048

!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1

!

ip ssh version 2

!

line vty 0 4
transport input ssh

!
```

关于使用的参考的Secure Shell版本2支持SSHv2的更多信息。

SSHv2 RSA密钥的增强

Cisco IOS SSHv2支持键盘交互和基于密码的认证方法。RSA主要特点的SSHv2增强也支持客户端和服务器的基于RSA的公共密钥验证。

对于用户认证，基于RSA的用户认证使用一个私有/公共密钥对关联与每个用户验证。用户必须生成在客户端的一个私有/公共密钥对和配置在Cisco IOS SSH服务器的一个公共密钥为了完成验证。

设法设立凭证的SSH用户提供一个已加密签名专用密钥。签名和用户的公共密钥发送到验证的SSH服务器。SSH服务器计算在用户提供的公共密钥的一哈希。哈希用于为了确定服务器是否有配比的一个条目。如果找到匹配，基于RSA的消息验证用公共密钥执行。因此，用户验证或拒绝访问根据已加密签名。

对于服务器验证， Cisco IOS SSH客户端必须为每个服务器分配主机密钥。当客户端设法建立一个SSH会话用服务器时，作为密钥交换交换消息一部分，接收服务器的签名。如果检查标志的严格主机密钥在客户端启用，客户端证实是否有对应于服务器预先配置的主机密钥键输入。如果找到匹配，客户端设法验证与服务器主机密钥的签名。如果服务器顺利地验证，会话建立继续;否则它终止并且显示服务器验证失败消息。

此配置示例启用使用RSA密钥与在Cisco IOS设备的SSHv2 ：

```
!
! Configure a hostname for the device
!
```

```
hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Specify the name of the RSA key pair (in this case, "sshkeys") to use for SSH
!

ip ssh rsa keypair-name sshkeys
!
! Enable the SSH server for local and remote authentication on the router using
! the "crypto key generate" command
! For SSH version 2, the modulus size must be at least 768 bits
!

crypto key generate rsa usage-keys label sshkeys modulus 2048
!
! Configure an ssh timeout (in seconds)
!
! The following enables a timeout of 120 seconds for SSH connections
!

ip ssh time-out 120
!
! Configure a limit of five (5) authentication retries
!

ip ssh authentication-retries 5
!
! Configure SSH version 2
!

ip ssh version 2
!
```

RSA密钥的参考的Secure Shell版本2增强关于使用RSA密钥的更多信息与SSHv2。

此配置示例使Cisco IOS SSH服务器进行基于RSA的用户认证。如果在服务器存储的RSA公共密钥验证与在客户端，或专用密钥对存储的公共用户认证是成功的。

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
!

       username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

参考配置Cisco IOS SSH服务器实行RSA根据用户认证关于使用RSA密钥的更多信息与SSHv2。

此配置示例使Cisco IOS SSH客户端进行基于RSA的服务器验证。

```
!
!
```

```
hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

       server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

参考配置Cisco IOS SSH客户端实行RSA根据服务器验证关于使用RSA密钥的更多信息与SSHv2。

控制台和 AUX 端口

在 Cisco IOS 设备中，控制台和辅助 (AUX) 端口是可用于对本地和远程设备进行访问的异步线路。您一定知道，Cisco IOS 设备上的控制台端口具有特殊权限。特别是这些权限允许管理员执行口令恢复过程。要执行口令恢复，未经身份验证的攻击者需要能够访问控制台端口并能够断电或导致设备崩溃。

任何用于访问设备控制台端口的方法都必须受到保护，保护的方式与对设备进行特权访问时强制执行保护的方式相同。用于确保访问安全的方法必须包括使用 AAA、exec-timeout 以及调制解调器口令（如果有调制解调器连接到控制台）。

如果不需要口令恢复，则管理员可以使用 no service password-recovery 全局配置命令取消执行口令恢复过程的能力；但是，一旦启用 no service password-recovery 命令，管理员将无法再对设备执行口令恢复。

在大多数情况下，必须禁用设备的Aux端口为了防止未经授权的访问。Aux端口可以用这些命令禁用：

```
!

line aux 0
transport input none
transport output none
no exec
exec-timeout 0 1
no password
!
```

控制 vty 和 tty 线路

Cisco IOS 软件中的交互式管理会话使用 tty 或虚拟 tty (vty)。tty 是本地异步线路，终端可以连接到该线路以对设备进行本地访问，或者连接到调制解调器以对设备进行拨号访问。请注意，tty 可用于连接到其他设备的控制台端口。此功能允许将具有 tty 线路的设备用作控制台服务器，在该服务器上可以建立通过网络到已连接到 tty 线路的设备的控制台端口的连接。还必须对用于网络上这些反向连接的 tty 线路进行控制。

vty 线路用于设备所支持的所有其他远程网络连接，而不管协议（如 SSH、SCP 或 Telnet）如何。为了确保能够通过本地或远程管理会话访问设备，必须对 vty 和 tty 线路执行适当的控制。Cisco IOS 设备具有的 vty 线路的数量有限；线路数联机可以用show line exec命令确定。当所有VTY线路是在使用中的时，新建的管理会话不可能建立，创造访问的DoS条件对设备。

对设备的 vty 或 tty 线路实施的最简单形式的访问控制，就是对所有线路都使用身份验证，而不管设备在网络中的位置如何。这对于 vty 线路非常重要，因为它们可以通过网络访问。连接到调制解调器使用对设备的远程访问的tty线路或者连接到其它设备控制台端口的tty线路通过网络也是可访问。VTY和tty访问控制其他表可以用传输输入或access-class配置命令强制执行，与使用CoPP和CPPr功能，或者，如果运用访问列表对接口在设备。

验证可以通过使用AAA被强制执行，是认证接入的推荐的方法对设备，与使用本地用户数据库，或者由直接地在VTY或tty线路配置的

简单密码验证。

必须使用 exec-timeout 命令注销 vty 或 tty 线路上处于空闲状态的会话。必须也用于service tcp-keepalives-in命令为了启用在流入连接的TCP Keepalive对设备。这样可以确保在连接远程端上的设备仍然处于可访问状态，并且半开放的连接或孤立的连接会从本地 IOS 设备上删除。

控制 vty 和 tty 线路的传输

如果使用作为控制台服务器，只应该配置VTY和tty为了接受已加密和巩固远程访问管理连接对设备或通过设备。本部分讨论 tty，因为此类线路可以连接到其他设备上的控制台端口，这使得 tty 可以通过网络进行访问。为了防止信息泄露或禁止对在管理员与设备之间传输的数据进行未授权的访问，应使用 transport input ssh，而不使用 Telnet 和 rlogin 等明文协议。传输输入无配置在tty可以启用，实际上禁用使用反向控制台连接的tty线路。

vty 和 tty 线路都允许管理员连接到其他设备。为了限制管理员能够用于传出连接的传输类型，请使用 transport output line 配置命令。如果不需要传出连接，则应使用 transport output none。但是，如果允许传出连接，则应通过使用 transport output ssh 对连接执行加密的安全远程访问方法。

注意：IPSec能用于已加密和巩固对设备的远程访问连接，如果支持。如果使用 IPSec，这也会给设备添加额外的 CPU 开销。但是，即使使用了 IPSec，也仍然必须执行 SSH 作为传输协议。

警告标志

在一些法律权限，检控和非法监控有恶意的用户可以无法的，除非他们通知他们没有允许使用系统。提供这种通知的一个方法是将此信息放置到用 Cisco IOS 软件 banner login 命令配置的标志消息中。

法律通知要求非常复杂，因管辖区和情况而异，并且应与法律顾问进行讨论。即使在管辖区内，法律观点也可能有所不同。在顾问的配合下，标志能够提供以下部分或全部信息：

- 请注意，本系统仅供已专门授权的个人登录或使用，并可能提供有关谁可以授予使用权限的信息。
- 请注意，对本系统的任何未经授权的使用均属非法行为，并可能受到民事和刑事制裁。
- 请注意，对系统的任何使用可能会被记录或监视，恕不另行通知，并且生成的日志可以用作法庭证据。
- 本地法律需要的特定通知。

从安全角度（而不是法律角度）而言，登录标志不应包含任何有关路由器名称、型号、软件或所有权的特定信息。此信息可能会被恶意用户滥用。

验证、授权和记帐

验证、授权和统计(AAA)框架是关键为了获取对网络设备的交互式访问。AAA框架提供可以被剪裁根据网络的需要的一个高度可配置环境。

TACACS+ 身份验证

TACACS+是Cisco IOS设备能使用管理用户验证一个远程AAA服务器的认证协议。这些管理用户可以通过 SSH、HTTPS、telnet 或 HTTP 访问 IOS 设备。

TACACS+ 身份验证（更常被称为 AAA 验证）使每个网络管理员能够使用单个用户帐户。当您不取决于单个共享密码时，网络的安全改善，并且您的责任被加强。

RADIUS是协议相似在目的与TACACS+;然而，它只加密在间网络被发送的密码。相反， TACACS+加密整个TCP有效载荷，包括两个用户名和密码。因此，当 AAA 服务器支持 TACACS+ 时，应使用 TACACS+，而不使用 RADIUS。有关比较这两种协议的详细信息，请参阅比较 TACACS+ 和 RADIUS。

TACACS+认证在有配置的一个Cisco IOS设备可以启用类似于此示例：

```
!

aaa new-model
aaa authentication login default group tacacs+
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

前一个配置可用作特定于组织的 AAA 身份验证模板的起点。有关 AAA 配置的详细信息，请参阅身份验证、授权和记账。

方法列表是描述认证方法将被查询为了验证用户的一连续的列表。万一最初的方法发生故障，方法列表使您选定将用于验证一个或更多安全协议和因而保证验证的一个备份系统。Cisco IOS软件使用顺利地接受或拒绝用户的第一个列出的方法。在更早的方法发生故障由于服务器前不可用或不正确的配置处，随后的方法只尝试。验证的参考的已命名方法列表关于Named方法列表的配置的更多信

息。

身份验证回退

如果所有已配置的 TACACS+ 服务器都不可用，则 Cisco IOS 设备可以依靠辅助验证协议。如果所有已配置的 TACACS+ 服务器都不可用，典型的配置包括使用 local 或 enable 验证。

设备上的全部验证选项包括 enable、local 和 line。这些选项各有其优点。使用enable secret更喜欢，因为机密切细与比加密算法是固有地的更多安全使用与类型7密码线路或本地认证的一种单程算法。

但是，在支持对本地定义的用户使用加密口令的 Cisco IOS 软件版本上，可能有必要回退到 local 验证。这允许为一个或多个网络管理员创建本地定义的用户。如果 TACACS+ 变得完全不可用，每个管理员可以使用他们的本地用户名和口令。虽然此操作提高网络管理员的责任TACACS+中断的，极大增加管理负担，因为必须维护在所有网络设备的本地用户帐户。

此配置示例构件在上一个TACACS+认证示例为了包括fallback验证到用enable secret命令配置本地的密码：

```
!

enable secret <password>
!

aaa new-model
aaa authentication login default group tacacs+ enable
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

有关将 AAA 与回退验证一起使用的详细信息，请参阅配置验证。

使用类型 7 口令

最初设计为了允许存储的密码的快速解密，类型7密码不是密码存贮一安全表。有许多工具可以轻易解密这些口令。除非 Cisco IOS 设备上使用的功能要求使用类型 7 口令，否则应避免使用此类型的口令。

废除此类型的口令可以通过使用 AAA 验证和使用增强的口令安全功能来帮助实现；后者允许对通过 username global configuration 命令在本地定义的用户使用加密口令。如果不能完全避免使用类型 7 口令，可以将这些口令视为已随机化，而不是已加密。

请参阅本文的一般管理平面硬化的部分关于类型7密码的更多信息删除。

TACACS+ 命令授权

TACACS+ 和 AAA 命令授权提供了允许或拒绝管理用户输入的每条命令的机制。当用户输入 EXEC 命令时，Cisco IOS 会将每条命令发送到已配置的 AAA 服务器。然后，AAA 服务器使用其已配置的策略针对此特定用户允许或拒绝每条命令。

此配置可以添加到前一个 AAA 验证示例中以实施命令授权：

```
!

aaa authorization exec default group tacacs none
aaa authorization commands 0 default group tacacs none
aaa authorization commands 1 default group tacacs none
aaa authorization commands 15 default group tacacs none
!
```

有关命令授权的详细信息，请参阅配置授权。

TACACS+ 命令记账

配置 AAA 命令记账后，它会将有关已输入的每条 EXEC 命令的信息发送到配置的 TACACS+ 服务器。信息发送对TACACS+服务器包括被执行的命令被执行，日期和输入命令用户的用户名。命令核算不支持与RADIUS。

本示例配置对在权限级别 0、1 和 15 输入的 EXEC 命令启用 AAA 命令记账。本配置建立在前面几个包括 TACACS 服务器配置的示例的基础之上。

```
!

aaa accounting exec default start-stop group tacacs
aaa accounting commands 0 default start-stop group tacacs
aaa accounting commands 1 default start-stop group tacacs
aaa accounting commands 15 default start-stop group tacacs
!
```

参考配置核算关于Aaa accounting的配置的更多信息。

冗余 AAA 服务器

环境中利用的 AAA 服务器应具有冗余，并以容错方式进行部署。这有助于确保在 AAA 服务器不可用时可以进行交互式管理访问（如 SSH）。

当您设计或实现一冗余AAA服务器解决方案时，请记住这些考虑事项：

- AAA 服务器在可能的网络故障期间的可用性
- AAA 服务器在地理上的分散放置
- 装载在稳定和故障情况的各自的AAA服务器
- 网络接入服务器与 AAA 服务器之间的网络延迟
- AAA 服务器数据库同步

有关详细信息，请参阅部署访问控制服务器。

加强简单网络管理协议

本部分重点介绍几种可用于保护 IOS 设备内的 SNMP 部署的方法。非常重要的是SNMP适当地获取为了保护此数据传输网络数据和网络设备的机密性、完整性和可用性。SNMP 可为您提供大量有关网络设备运行状况的信息。应该从要有效利用此数据为了进行攻击网络的有恶意的用户保护此信息。

SNMP 社区字符串

社区字符串是一些口令，这些口令应用于 IOS 设备以限制对设备上的 SNMP 数据进行访问（包括只读访问和读写访问）。和所有口令一样，这些社区字符串应经过仔细选择，以确保它们具有保密作用。社区字符串应根据网络安全策略定期进行更改。例如，在网络管理员更换职位或离开公司时，应更改社区字符串。

以下这些配置行用于配置只读社区字符串 READONLY 和读写社区字符串 READWRITE：

```
!

snmp-server community READONLY RO
snmp-server community READWRITE RW
!
```

注意：上一个社区字符串示例是选定的为了清楚地解释使用这些字符串。在生产环境中，选择社区字符串时应非常谨慎，并且社区字符串应包含一系列字母、数字和非字母数字符号。有关选择具有保密作用的口令的详细信息，请参阅关于创建强口令的建议。

有关此功能的详细信息，请参阅 IOS SNMP 命令参考。

SNMP 社区字符串与 ACL

除社区字符串以外，还应当应用 ACL 将 SNMP 访问进一步限制为选定的一组源 IP 地址。本配置将 SNMP 只读访问限制为位于 192.168.100.0/24 地址空间中的终端主机设备，并且将 SNMP 读写访问限制为只能访问位于 192.168.100.1 的终端主机设备。

注意：由这些ACL允许的设备要求适当的社区字符串为了访问请求的SNMP信息。

```
!

access-list 98 permit 192.168.100.0 0.0.0.255
access-list 99 permit 192.168.100.1
!

snmp-server community READONLY RO 98
snmp-server community READWRITE RW 99
!
```

在Cisco IOS网络management命令参考资料的参考的snmp-server community关于此功能的更多信息。

基础架构 ACL

基础设施ACL (iACLs)可以部署为了保证仅终端主机用委托IP地址能发送SNMP流量到IOS设备。iACL 中应包含一个用于拒绝 UDP 端口 161 上的未授权 SNMP 数据包的策略。

有关使用 iACL 的详细信息，请参阅本文档中的使用基础架构 ACL 限制对网络的访问部分。

SNMP 视图

SNMP 视图是可用于允许或拒绝对某些 SNMP MIB 的访问的安全功能。创建视图并使用 snmp-server community community-string view 全局配置命令将其应用于社区字符串后，如果您访问 MIB 数据，您将被限制为只能使用该视图定义的权限进行访问。在适当的时候，建议您使用视图将 SNMP 用户限制为只能访问他们需要的数据。

本配置示例使用社区字符串 LIMITED 将 MIB 访问限制为位于系统组中的 MIB 数据：

```
!

snmp-server view VIEW-SYSTEM-ONLY system include
!

snmp-server community LIMITED view VIEW-SYSTEM-ONLY RO
!
```

有关详细信息，请参阅配置 SNMP 支持。

SNMP 版本 3

SNMP 版本 3 (SNMPv3) 由 RFC3410、RFC3411、RFC3412、RFC3413、RFC3414 和 RFC3415 定义，是一种基于标准的可互操作网络管理协议。因为验证和或者加密在网络的数据包SNMPv3提供安全访问对于设备。那里支持， SNMPv3可以用于为了添加安全另一块层，当您部署SNMP时。SNMPv3 包括三个主要的配置选项：

- 没有验证-此模式不要求任何验证亦不SNMP数据包的任何加密
- 验证-此模式要求SNMP数据包的验证，不用加密
- priv -此模式要求验证和加密(保密性)每SNMP数据包

授权引擎ID必须存在为了使用SNMPv3安全机制-验证或验证和加密-处理SNMP数据包;默认情况下，该引擎 ID 在本地生成。使用 show snmp engineID 命令可以显示引擎 ID，如本示例所示：

```
router#show snmp engineID
  Local SNMP engineID: 80000090300000152BD35496
  Remote Engine ID          IP-addr    Port
```

注意：如果engineID更改，必须重新配置所有SNMP用户帐户。

下一步是配置 SNMPv3 组。此命令配置SNMPv3的一个Cisco IOS设备与SNMP服务器组AUTHGROUP并且启用此组的仅验证有验证关键字的：

```
!
snmp-server group AUTHGROUP v3 auth
!
```

此命令配置SNMPv3的一个Cisco IOS设备与SNMP服务器组PRIVGROUP并且启用验证和加密此组的有priv关键字的：

```
!
snmp-server group PRIVGROUP v3 priv
!
```

此命令使用 MD5 验证口令 authpassword 和 3DES 加密口令 privpassword 配置 SNMPv3 用户 snmpv3user：

```
!

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des
    privpassword
!
```

请注意，根据 RFC 3414 的要求，snmp-server user configuration 命令不会显示在该设备的配置输出中；因此，无法从配置中查看用户口令。要查看已配置的用户，请输入 show snmp user 命令，如本示例所示：

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000090300000152BD35496
storage-type: nonvolatile        active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

有关此功能的详细信息，请参阅配置 SNMP 支持。

管理平面保护

管理层面保护(MPP)功能在Cisco IOS软件方面可以用于为了帮助安全SNMP，因为限制SNMP流量在设备能终止的接口。MPP 功能允许管理员将一个或多个接口指定为管理接口。仅允许管理数据流通过这些管理接口进入设备。启用 MPP 后，除指定的管理接口外，没有任何接口能够接收以设备为目标的网络管理数据流。

注意MPP是CPPr功能的一子集并且要求该的IOS版本支持CPPr。有关 CPPr 的详细信息，请参阅了解控制层面保护。

在本示例中，MPP 用于将 SNMP 和 SSH 访问限制为只能访问 FastEthernet 0/0 接口：

```
!
control-plane host
management-interface FastEthernet0/0 allow ssh snmp
!
```

有关详细信息，请参阅管理平面保护功能指南。

日志记录最佳实践

通过使用事件日志记录，您可以看到 Cisco IOS 设备和该设备部署到的网络的运行状况。Cisco IOS 软件提供几种灵活的日志记录选项，可帮助实现组织的网络管理和可见性目标。

这些部分提供一些基本的日志记录最佳实践，可帮助管理员成功地利用日志记录，同时最大限度地减少日志记录对 Cisco IOS 设备的影响。

将日志发送到中央位置

建议您将日志记录信息发送到远程 syslog 服务器。这使成为可能更加有效关联和审计网络和安全事件在网络设备间。请注意，syslog 消息通过 UDP 以明文形式传输，这种传输方式并不可靠。例如为此，网络能管理数据流应该扩展的所有保护(加密或带外访问)为了包括Syslog流量。

此配置示例配置Cisco IOS设备为了发送记录信息到远程系统日志服务器：

```
!
logging host <ip-address>
!
```

有关日志关联的详细信息，请参阅使用防火墙和 IOS 路由器 Syslog 事件识别突发事件。

集成在12.4(15)T和最初介绍在12.0(26)S，记录日志对在一个先进技术附件(ATA)闪存盘将保存的本地非易失性存储器(ATA磁盘)功能 enable (event)系统日志消息。在路由器重新启动后，在ATA驱动保存的消息仍然存在。

此配置行配置134,217,728个字节(128 MB)日志消息对ATA闪存(disk0)的Syslog目录，指定文件大小16,384个字节：

```
logging buffered
logging persistent url disk0:/syslog size 134217728 filesize 16384
```

在日志消息写入到在ATA磁盘前的一个文件， Cisco IOS软件检查是否有充足的磁盘空间。否则，日志消息最旧的文件(由时间戳)删除和当前文件保存。文件名格式是log_month ：天：年： ：时间。

注意：ATA闪存驱动器限制了磁盘空间和因而需要维护避免覆盖存储的数据。

作为维护程序一部分，此示例显示如何复制日志消息从路由器ATA闪存盘到在FTP服务器192.168.1.129的一张外部磁盘：

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

对本地非易失性存储器(ATA磁盘)的参考的记录日志关于此功能的更多信息。

日志记录级别

Cisco IOS 设备生成的每条日志消息都会被分配一个严重性级别，严重性级别共分八个级别，范围从级别 0（紧急）到级别 7（调试）。除非专门要求，否则建议您避免在级别 7 进行日志记录。在级别 7 进行日志记录会增加设备 CPU 的负载，可能导致设备和网络不稳定。

全局配置命令日志陷阱级别用于为了指定哪些日志消息传送到远程系统日志服务器。指定的 level 指示所发送消息的最低严重性级别。对于缓冲的日志记录，可以使用 logging bufferedlevel 命令。

本配置示例将发送到远程 syslog 服务器和本地日志缓冲区的日志消息限制为严重性级别 6（信息性）到 0（紧急）：

```
!

logging trap 6
logging buffered 6
!
```

有关详细信息，请参阅故障排除、故障管理和日志记录。

请勿记录到控制台或监视会话中

使用Cisco IOS软件，传送日志消息对-的监控会话监控会话是exec命令终端监视器发出-的交互管理会话是可能的和到控制台。然而，这能举起IOS设备的CPU负载并且没有推荐。反而，您建议发送记录信息到本地日志缓冲区，可以用show logging命令查看。

请使用全局配置命令no logging console和no logging monitor为了禁用记录日志对控制台和监控会话。本配置示例说明了这些命令的用法：

```
!

no logging console
no logging monitor
!
```

有关全局配置命令的详细信息，请参阅 Cisco IOS 网络管理命令参考。

使用缓冲的日志记录

Cisco IOS 软件支持使用本地日志缓冲区，以便管理员能够查看本地生成的日志消息。强烈建议使用缓冲的日志记录，而不是记录到控制台或监视会话中。

有两个配置选项与配置缓冲的日志记录有关：日志记录缓冲区的大小和存储在缓冲区中的消息严重性级别。日志记录缓冲区的大小使用全局配置命令 logging buffered size 来配置。在缓冲区包括的最低的严重性用logging buffered严重性命令配置。管理员可以通过 show logging EXEC 命令查看日志记录缓冲区的内容。

此配置示例包括16384个字节操作日志缓冲区的配置，以及严重性6，信息性，表明在级别0 (紧急状态)的消息通过6 (信息性)存储：

```
!

logging buffered 16384 6
!
```

有关缓冲的日志记录的详细信息，请参阅 Cisco IOS 网络管理命令参考。

配置日志记录源接口

为了提供一个增加的级别一致性，当您收集并且检查日志消息时，您建议静态配置记录日志源接口。通过 logging source-interface interface 命令可完成此配置，静态配置日志记录源接口可确保从单个 Cisco IOS 设备发送的所有日志记录消息中都显示同一个 IP 地址。为提高稳定性，建议您使用环回接口作为日志记录源接口。

此配置示例说明使用logging source-interface接口全局配置命令为了指定loopback0接口的IP地址使用所有日志消息：

```
!
logging source-interface Loopback 0
!
```

有关详细信息，请参阅 Cisco IOS 命令参考。

配置日志记录时间戳

配置日志记录时间戳可帮助您关联各个网络设备上的事件。必须实施正确且一致的日志记录时间戳配置，以确保能够关联日志记录数据。应将日志记录时间戳配置为包括精度为毫秒的日期和时间，并包括设备上正在使用的时区。

此示例包括协调世界时 (UTC) 区域内精度为毫秒的日志记录时间戳的配置：

```
!
service timestamps log datetime msec show-timezone
!
```

如果您不希望记录相对于 UTC 的时间，可以配置特定的本地时区，并将该信息配置为显示在生成的日志消息中。本示例说明太平洋标准时间 (PST) 区域的设备配置：

```
!

clock timezone PST -8
service timestamps log datetime msec localtime show-timezone
!
```

Cisco IOS 软件配置管理

Cisco IOS 软件包括几项可用于在 Cisco IOS 设备上启用配置管理的功能。这些功能包括将配置存档、将配置回滚到以前的版本以及创建详细的配置更改日志。

配置替换和配置回滚

在Cisco IOS软件版本12.3(7)T和以后，配置替换，并且配置回退功能允许您归档在设备的Cisco IOS设备配置。存储手工或自动，配置在此存档可以用于为了用配置替换当前运行的配置替换filename命令。这与 copy filename running-config 命令形成对比。configure replace filename 命令替换正在运行的配置，而 copy 命令执行合并操作。

建议您在网络中的所有 Cisco IOS 设备上启用此功能。一旦启用，管理员能造成当前运行的配置被添加到存档用存档设置privileged exec命令。归档的配置可以查看与exec命令的show archive。

本示例说明自动配置存档的配置。本示例指示 Cisco IOS 设备将存档的配置作为名为 archived-config-N 的文件存储在 disk0:文件系统上，维护最多 14 个备份，每天（1440 分钟）存档一次，并且在管理员发出 write memory EXEC 命令时也进行存档。

```
!

archive
path disk0:archived-config
maximum 14
time-period 1440
write-memory
!
```

虽然配置存档功能能存储14个备份配置，您建议考虑空间需求，在您使用最大命令前。

以独占方式进行配置更改访问

添加到 Cisco IOS 软件版本 12.3(14)T 中的“以独占方式进行配置更改访问”功能可确保在给定的时间只有一个管理员能够对 Cisco IOS 设备进行配置更改。此功能有助于消除同时更改相关配置组件所造成的负面影响。此功能配置与全局配置命令配置模式不包括模式并且在两个模式之一中运行：自动模式和手动模式。在自动模式下，当管理员发出 configure terminal EXEC 命令时，配置自动锁定。在手动模式，当输入配置模式时，管理员使用lock命令的configure terminal为了锁定配置。

本示例说明此功能的自动配置锁定的配置：

```
!
configuration mode exclusive auto
!
```

Cisco IOS 软件弹性配置

添加在Cisco IOS软件版本12.3(8)T，能适应配置功能使成为可能安全地存储由Cisco IOS设备当前使用Cisco IOS软件镜像和设备配置的复制。启用此功能后，将无法更改或删除这些备份文件。您建议使此功能为了防止因疏忽所致和有恶意的尝试删除这些文件。

```
!
secure boot-image
secure boot-config!
```

启用此功能后，可能能够恢复已删除的配置或 Cisco IOS 软件映像。此功能的当前运行状态可以显示与exec命令显示安全的引导程序。

数字式地签字的Cisco软件

添加在Cisco的1900， 2900和3900系列路由器Cisco IOS版本15.0(1)M，数字式地签字的Cisco软件功能实现数字式地签字和因而委托的使用Cisco IOS软件，与使用安全不对称的(公共密钥)加密算法。

一数字式地签字的镜像运载一已加密(与专用密钥)哈希本身。在检查，设备解密哈希用有在其关键存储并且计算其镜像的自己的哈希从密钥的对应的公共密钥。如果解密的哈希匹配计算的镜像哈希，镜像未被窜改并且可以是委托。

数字式地签字的Cisco软件密钥由密钥的种类和版本识别。密钥可以是特殊、制作或者反转密钥类型。制作和特殊关键类型有一个相关的关键版本增量按字母顺序，每当密钥取消并且替换。当您使用数字式地签字的Cisco软件功能时， ROMMON和正常Cisco IOS镜像签字与特殊或制作密钥。ROMmon镜像可升级，并且必须签字与密钥和装载的特殊或制作镜像一样。

此命令在设备密钥存储验证镜像c3900-universalk9-mz.SSA完整性在闪存的与密钥：

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```

数字式地签字的Cisco软件功能在思科Catalyst 4500电子系列交换机的Cisco IOS XE版本3.1.0.SG也集成。

关于此功能的更多信息参考的数字式地签字的Cisco软件。

在Cisco IOS版本15.1(1)T及以后，关键更换数字式地签字的Cisco软件的介绍。关键更换和撤销替换并且去除使用从平台的关键存储设备的一张数字式地签字的Cisco软件支票的密钥。在一关键妥协情形下，只特殊和制作密钥可以取消。

a (特殊或制作)镜像的一新的(特殊或制作)密钥进来使用为了取消上一个特殊或制作密钥的a (制作或撤销)镜像。撤销镜像完整性验证与在平台来预存的反转密钥。反转密钥不更改。当您取消制作密钥，在撤销镜像装载后，运载被添加到关键存储的新密钥，并且对应的旧有密钥可以取消，只要ROMmon镜像升级，并且新的制作镜像是引导。当您取消一特殊密钥时，制作镜像装载。此镜像添加新的

特殊密钥，并且能取消旧有特殊密钥。在您upgrade rommon，新的特殊镜像可以是启动后。

此示例描述一特殊密钥的撤销。这些add命令对关键存储的新的特殊密钥从当前制作镜像，复制一个新的ROMmon镜像(C3900_rom-monitor.srec.SSB)到存储区域(usbflash0 ：)，升级ROMMON文件，并且取消旧有特殊密钥：

```
software authenticity key add special
copy tftp://192.168.1.129/C3900_rom-monitor.srec.SSB usbflash0:
upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
software authenticity key revoke special
```

一个新的特殊镜像(c3900-universalk9-mz.SSB)可能然后复制到闪存将装载和镜像的签名验证与新加的特殊密钥(.SSB) ：

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```

Catalyst 4500运行Cisco IOS XE软件的电子系列交换机不支持关键撤销和更换，虽然这些交换机支持数字式地签字的Cisco软件功能。

参考数字式地签字的Cisco软件指南的数字式地签字的Cisco软件密钥撤销和替换部分关于此功能的更多信息。

配置更改通知和日志

使用 Cisco IOS 软件版本 12.3(4)T 中添加的“配置更改通知和日志记录”功能可以记录对 Cisco IOS 设备所做的配置更改。该日志保留在 Cisco IOS 设备上，并且包含做出更改的个人的用户信息、输入的配置命令以及做出更改的时间。此功能用configuration mode命令logging enable配置更改的记录器启用。因为他们防止密码数据记录日志并且增加更改日志的长度，可选命令hidekeys和记录日志大小条目用于为了改进默认配置。

建议您启用此功能，以使 Cisco IOS 设备的配置更改历史记录更加易于了解。另外，当配置更改做时，您建议使用通知Syslog配置命令为了启用系统消息的生成。

```
!

archive
log config
 logging enable
 logging size 200
 hidekeys
 notify syslog
!
```

启用“配置更改通知和日志记录”功能后，可以使用特权 EXEC 命令 show archive log config all 查看配置日志。

控制层面

控制层面功能包括通信在网络设备之间为了移动数据从来源到目的地的协议和进程。其中包括路由协议（如边界网关协议）以及 ICMP 和资源保留协议 (RSVP) 等协议。

管理和数据层面中的事件不会对控制层面造成负面影响，是非常重要的。如果数据层面事件（如 DoS 攻击）影响了控制层面，则整个网络可能会变得不稳定。这些有关 Cisco IOS 软件功能和配置的信息有助于确保控制层面的弹性。

一般控制层面强化

由于控制层面可确保管理和数据层面受到维护并可以正常运行，因此，保护网络设备的控制层面至关重要。如果控制层面在安全事件期间变得不稳定，则您可能无法恢复网络的稳定。

在许多情况下，您能禁用消息特定类型接收和发射在要求处理不需要的数据包的接口的为了最小化相当数量CPU负载。

IP ICMP 重定向

如果在同一个接口上接收并传输数据包，路由器可能会生成 ICMP 重定向消息。在这种情况下，路由器会转发数据包，并将一条 ICMP 重定向消息发送回原始数据包的发送方。这种行为允许发送方避开路由器，并直接将随后的数据包转发到目标（或者更接近目标的路由器）。在正常运行的 IP 网络中，路由器仅向它自己的本地子网中的主机发送重定向消息。换句话说，ICMP 重定向消息从不应超出第 3 层边界。

共有两种类型的 ICMP 重定向消息：主机地址重定向消息和整个子网重定向消息。恶意用户能利用路由器的能力发送ICMP重定向通过连续发送数据包对路由器，强制路由器回应ICMP重定向消息，并且导致在CPU的一个路由器的不利影响和性能。要防止路由器发送 ICMP 重定向消息，请使用 no ip redirects 接口配置命令。

ICMP 不可达

使用接口访问列表进行过滤将导致 ICMP 不可达消息被传输回已过滤数据流的源。这些消息的生成能增加在设备的CPU利用率。在 Cisco IOS 软件中，默认情况下生成 ICMP 不可达消息的速度限制为每 500 毫秒一个数据包。ICMP不可达信息生成可以禁用与interface configuration命令no ip unreachables。ICMP不可得到速率限制可以从与global configuration命令ip icmp速率限制不

可达的间隔在MS的默认更改。

代理 ARP

代理 ARP 是一种技术；采用这种技术，一台设备（通常为路由器）可以应答发往另一台设备的 ARP 请求。通过“伪造”其身份，路由器承担了将数据包路由到真正目标的责任。代理 ARP 可帮助子网上的计算机到达远程子网，而无需配置路由或默认网关。RFC 1027 中定义了代理 ARP。

有几个缺点对代理ARP利用率。它能导致在相当数量的一增加在网段的ARP流量和资源耗尽和中间人攻击。代理 ARP 提供了一种资源耗尽攻击矢量，因为每个被代理的 ARP 请求都会消耗少量内存。如果发送很大数量的ARP请求，攻击者可以能用尽所有可利用的内存。

中间人攻击使在网络的一台主机伪装路由器的MAC地址，导致发送流量的信任的主机对攻击者。代理ARP可以禁用与interface configuration命令no ip proxy-arp。

有关此功能的详细信息，请参阅启用代理 ARP。

限制控制层面流量CPU影响

保护控制层面是至关重要的。由于在缺少数据和管理数据流的情况下，应用程序性能和最终用户体验可能会受到负面影响，因此，控制层面正常运行的能力可确保其他两个平面受到维护并可以正常运行。

了解控制层面流量

为了向 Cisco IOS 设备的控制层面提供适当的保护，必须了解由 CPU 进程交换的数据流的类型。进程交换的数据流通常包括两种不同类型的数据流。第一种类型的数据流以 Cisco IOS 设备为目标，并且必须由 Cisco IOS 设备 CPU 直接处理。这种数据流包括以下类别：

- 接收邻接流量-此流量包含在Cisco express forwarding (CEF)表的一个条目，藉以下一台路由器跳是设备，由期限接收在show ip cef CLI输出中表示。对于需要由 Cisco IOS 设备 CPU 直接处理的任何 IP 地址，这一指示包括接口 IP 地址、多播地址空间和广播地址空间。

由CPU处理的第二种流量类型是数据层面流量-与一个目的地的流量在Cisco IOS设备之外-要求处理由CPU的特殊的。虽然下表并未列出影响 CPU 的全部数据层面数据流，但这些类型的数据流是进程交换的数据流，因此可能影响控制层面的运行：

- 访问控制表记录- ACL记录流量包括生成的归结于匹配的所有数据包(permit或拒绝) ACE日志关键字使用。
- 单播反向路径转发(单播RPF) -单播RPF，使用与ACL一道，能导致进程交换某些数据包。
- Ip options -必须由CPU处理有选项的所有IP信息包包括。
- 分段-必须通过所有IP数据包要求的分段到处理的CPU。
- 存活时间(TTL)终止-有一个TTL值小于或等于一个要求互联网控制消息协议Time exceeded的数据包(ICMP类型11，代码0)消息将发送，导致CPU处理。
- ICMP不可达的-导致ICMP不可达信息由于路由的数据包， MTU或者过滤由CPU处理。
- 要求ARP请求的流量- ARP条目不存在的目的地由CPU要求处理。
- 非IP数据流-所有非IP数据流由CPU处理。

本列表详细介绍了几种方法，用于确定哪些类型的数据流正由 Cisco IOS 设备的 CPU 处理：

- show ip cef 命令提供 CEF 表中包含的每个 IP 前缀的下一跳信息。如前所述，包含 receive 作为“下一跳”的条目被视为接收邻接关系，并指示数据流必须直接发送到 CPU。
- 关于是设备交换的进程数据包的数量的show interface switching命令提供信息。
- show ip traffic 命令提供有关具有以下特征的 IP 数据包的数量的信息：
    - 具有本地目标（即接收邻接关系数据流）
    - 具有选项
    - 需要分段
    - 被发送到广播地址空间
    - 被发送到多播地址空间
- 接收邻接关系数据流可以通过使用 show ip cache flow 命令来识别。任何以 Cisco IOS 设备为目标的数据流都具有 local 目标接口 (DstIf)。

- 可以使用控制层面策略来确定到达 Cisco IOS 设备控制层面的数据流的类型和速率。控制层面策略可以通过使用粒度分类 ACL、日志记录以及使用 show policy-map control-plane 命令来执行。

基础架构 ACL

基础架构 ACL（iACL）用于限制从外部与网络设备进行通信。基础设施ACL在对网络的限制访问广泛地被覆盖用基础设施本文的ACL部分。

您建议实现iACLs为了保护所有网络设备控制层面。

接收 ACL

在分布式平台上，可以选择对用于 12000 (GSR) 的 Cisco IOS 软件版本 12.0(21)S2、用于 7500 的软件版本 12.0(24)S 和用于 10720 的软件版本 12.0(31)S 使用接收 ACL (rACL)。rACL 可在数据流影响路由处理器之前防止设备受到有害数据流的侵害。接收 ACL 设计为仅保护配置有它的设备，而中转数据流不会受到 rACL 的影响。因此，以下示例 ACL 条目中使用的目标 IP 地址仅指的是路由器的物理或虚拟 IP 地址。接收 ACL 也被视为网络安全最佳实践；要使网络非常安全，应考虑长期使用它。

这是为了允许来自 192.168.100.0/24 网络上的受信任主机的 SSH（TCP 端口 22）数据流而写入的接收路径 ACL：

```
!
!--- Permit SSH from trusted hosts allowed to the device.
!

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22
!
!--- Deny SSH from all other sources to the RP.
!

access-list 151 deny tcp any any eq 22
!
!--- Permit all other traffic to the device.
!--- according to security policy and configurations.
!

access-list 151 permit ip any any
!
!--- Apply this access list to the receive path.
!

ip receive access-list 151
!
```

请参阅 GSR：接收访问控制列表以帮助标识合法数据流并允许其进入设备，同时拒绝所有不需要的数据包。

控制层面策略

控制层面策略 (CoPP) 功能还可用于限制以基础架构设备为目标的 IP 数据包。在本示例中，只允许来自受信任主机的 SSH 数据流到达 Cisco IOS 设备 CPU。

注意：降低流量从未知或不信任IP地址可以防止主机用动态分配的IP地址连接到Cisco IOS设备。

```
!

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22
access-list 152 permit tcp any any eq 22
access-list 152 deny ip any any
!

class-map match-all COPP-KNOWN-UNDESIRABLE
match access-group 152
!

policy-map COPP-INPUT-POLICY
class COPP-KNOWN-UNDESIRABLE
 drop
!

control-plane
service-policy input COPP-INPUT-POLICY
!
```

在上一个CoPP示例中，配比的ACL条目有permit操作的未授权信息包导致这些数据包丢弃由策略映射丢弃功能，而匹配拒绝操作的数据包没有影响的是受策略映射丢弃功能的。

CoPP 在 Cisco IOS 软件版本系列 12.0S、12.2SX、12.2S、12.3T、12.4 和 12.4T 中可用。

有关配置和使用 CoPP 功能的详细信息，请参阅部署控制层面策略。

控制层面保护

Cisco IOS 软件版本 12.4(4)T 中引入的控制层面保护 (CPPr) 可用于限制或管制以 Cisco IOS 设备的 CPU 为目标的控制层面数据流。尽管与 CoPP 类似，但 CPPr 能够对数据流进行更细致的限制。CPPr 将整个控制层面划分为三个不同的控制层面类别，这些类别称为子接口。存在“主机”、“中转”和“CEF 异常”数据流类别的子接口。此外，CPPr 还包括以下这些控制层面保护功能：

- 波尔特过滤功能-此功能提供被发送到已关闭或非侦听的TCP或UDP端口的修正和丢弃数据包。
- 队列门限功能-此功能限制在控制面板IP Input queue允许数据包的数量指定的协议的。

有关配置和使用 CPPr 功能的详细信息，请参阅控制层面保护和了解控制层面保护 (CPPr)。

硬件速率限制器

对于特殊的联网方案，Cisco Catalyst 6500 系列 Supervisor 引擎 32 和 Supervisor 引擎 720 支持特定于平台的、基于硬件的速率限制器 (HWRL)。这些硬件速率限制器称为特例速率限制器，因为它们涵盖一组特定的预定义 IPv4、IPv6、单播和多播 DoS 方案。HWRL 可以保护 Cisco IOS 设备，以防其受到各种需要 CPU 处理数据包的攻击。

有几个 HWRL 在默认情况下处于启用状态。有关详细信息，请参阅 PFC3 基于硬件的速率限制器默认设置。

有关 HWRL 的详细信息，请参阅 PFC3 上的基于硬件的速率限制器。

安全BGP

边界网关协议 (BGP) 是 Internet 的路由基础。同样地，与更多比普通的连接要求的所有组织经常使用BGP。BGP由攻击者经常瞄准由于其无所不在和“集并且忘记” BGP配置的本质在更加小的组织的。不过，有许多特定于 BGP 的安全功能可用于提高 BGP 配置的安全性。

下面概括介绍最重要的 BGP 安全功能。在适当的地方提供了一些配置建议。

基于 TTL 的安全保护

每个 IP 数据包都包含一个称为存活时间 (TTL) 的 1 字节字段。IP 数据包每经过一台设备，该值就递减 1。TTL 的起始值因操作系统而异，范围通常介于 64 到 255 之间。当数据包的 TTL 值达到零时，数据包将被丢弃。

叫作两个概括的基于Ttl的安全机制(GTSM)和BGP TTL安全删改(BTSH)，一个基于Ttl的安全保护有效利用TTL值IP信息包为了保证接收的BGP数据包是从一直接地连接的对等体。此功能通常要求对等路由器进行协调；但是，一旦启用，它就可以完全抵御许多针对 BGP 的基于 TCP 的攻击。

BGP的GTSM启用与邻接BGP路由器配置命令的ttl安全选项。本示例说明此功能的配置：

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> ttl-security hops <hop-count>
!
```

收到 BGP 数据包时，将检查其 TTL 值，并且该值必须大于或等于 255 减去指定的 hop-count。

使用 MD5 进行 BGP 对等验证

与MD5的对等点身份验证创建每数据包MD5摘要发送作为BGP会话一部分。具体来说，IP 和 TCP 报头的一些部分、TCP 有效负载和一个机密密钥将用于生成该摘要。

然后，创建的摘要将存储在 TCP 选项 Kind 19 中，该选项是 RFC 2385 专门为了此目的而创建的。接收的BGP扬声器使用同一算法和密钥为了重新生成消息摘要。如果接收到的摘要与经过计算得出的摘要不同，则丢弃数据包。

与MD5的对等点身份验证配置与对邻接BGP路由器配置命令的Password选项。此命令的用法如下所示：

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> password <secret>
!
```

有关使用 MD5 进行 BGP 对等验证的详细信息，请参阅邻居路由器验证。

配置最大前缀

BGP 前缀由路由器存储在内存中。越多前缀路由器必须保持，越多内存BGP必须浪费。在一些配置中，所有互联网前缀的一子集可以存储，例如在有效利用一个仅默认路由或路由供应商的客户网络的配置方面。

为了防止内存耗尽，必须配置基于每个对等体接受的前缀的最大数量。建议为每个 BGP 对等体配置一个限制值。

当您配置此功能用邻接最大前缀BGP路由器配置命令时，一个参数要求：在对等体被关闭之前接受的前缀的最大数量。还可以选择输入一个介于 1 到 100 之间的数字。此数字表示发送日志消息时占最大前缀值的百分比。

```
!

router bgp <asn>
neighbor <ip-address> remote-as <remote-asn>
neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>
!
```

有关对等最大前缀的详细信息，请参阅配置 BGP 最大前缀功能。

过滤器与前缀列表的BGP前缀

网络管理员可以使用前缀列表允许或拒绝通过 BGP 发送或接收的特定前缀。应该尽可能用于前缀列表为了保证网络流量在打算的路径发送。应在入站和出站方向对每个 eBGP 对等体应用前缀列表。

配置的前缀列表限制那些由网络路由策略专门允许的对等体发送或接收的前缀。如果由于接收到大量前缀而导致这样做并不可行，则应配置一个前缀列表以专门阻止已知的应被拒绝的前缀。这些已知的应被拒绝的前缀包括 RFC 3330 为内部或测试目的而保留的未分配 IP 地址空间和网络。应配置出站前缀列表以专门允许组织打算通告的前缀。

本配置示例使用前缀列表限制被获知的通告路由。具体来说，前缀列表 BGP-PL-INBOUND 仅允许一个默认路由入站，前缀 192.168.2.0/24 是唯一被 BGP-PL-OUTBOUND 允许通告的路由。

```
!

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0
ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24
!

router bgp <asn>
neighbor <ip-address> prefix-list BGP-PL-INBOUND in
neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out
!
```

有关 BGP 前缀过滤的全面介绍，请参阅使用外部 BGP 连接到服务提供商。

过滤器与自治系统路径访问列表的BGP前缀

BGP 自治系统 (AS) 路径访问控制列表允许用户基于前缀的 AS 路径属性过滤已接收且已通告的前缀。这可以与前缀列表一道用于为了设立一一套坚固的过滤器。

此配置示例使用AS路径访问列表为了限制入站前缀到远程产生的那些AS和出站前缀对本地自治系统产生的那些。来自所有其他自治系统的前缀均被过滤，不会安装到路由表中。

```
!

ip as-path access-list 1 permit ^65501$
ip as-path access-list 2 permit ^$
!

router bgp <asn>
neighbor <ip-address> remote-as 65501
neighbor <ip-address> filter-list 1 in
neighbor <ip-address> filter-list 2 out
!
```

安全内部网关协议

网络正确转发数据流以及从拓扑更改或故障中恢复的能力取决于准确的拓扑视图。您能经常运行一内部网关路由协议(IGP)按顺序提供此视图。默认情况下，IGP 是动态的，并且能够发现与正在使用的特定 IGP 通信的其他路由器。IGP 还能够发现可在网络链路出现故障时使用的路由器。

这些子部分概括介绍最重要的 IGP 安全功能。在适当的地方，将提供涵盖路由信息协议版本 2 (RIPv2)、增强型内部网关路由协议 (EIGRP) 和开放最短路径优先 (OSPF) 的建议和示例。

使用消息摘要 5 的路由协议验证和验证

如果无法确保十分安全地交换路由信息，攻击者可能会在网络中引入伪造的路由信息。可以通过在路由器之间将口令验证与路由协议一起使用，来提高网络的安全性。但是，由于此验证以明文发送，因此，破坏这种安全控制对于攻击者而言可能十分简单。

通过在验证过程中添加 MD5 散列功能，路由更新将不再包含明文口令，路由更新的整个内容也更加不易被篡改。然而，如果弱密码选择， MD5认证是易受暴力和词典攻击。建议您使用充分随机化的口令。由于 MD5 验证比口令验证更加安全，因此，这些示例特定于 MD5 验证。IPSec 也可用于验证和保护路由协议，但这些示例并未详细说明其用法。

EIGRP 和 RIPv2 在配置过程中利用了“密钥链”。有关配置和使用“密钥链”的详细信息，请参阅 key。

这是使用 MD5 的 EIGRP 路由器验证的示例配置：

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip authentication mode eigrp <as-number> md5
ip authentication key-chain eigrp <as-number> <key-name>
!
```

这是 RIPv2 的 MD5 路由器验证示例配置。RIPv1 不支持验证。

```
!

key chain <key-name>
key <key-identifier>
key-string <password>
!

interface <interface>
ip rip authentication mode md5
ip rip authentication key-chain <key-name>
!
```

这是使用 MD5 的 OSPF 路由器验证示例配置。OSPF 不使用“密钥链”。

```
!

interface <interface>
ip ospf message-digest-key <key-id> md5 <password>
!

router ospf <process-id>
network 10.0.0.0 0.255.255.255 area 0
area 0 authentication message-digest
!
```

有关详细信息，请参阅配置 OSPF。

Passive-interface 命令

可以使用有助于对路由信息的通告进行控制的 passive-interface 命令来防范信息泄漏或 IGP 中引入伪造的信息。建议不要在您无法对其进行管理控制的网络中通告任何信息。

本示例说明此功能的用法：

```
!

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
!
```

路由过滤

为了减少可能性您在网络引入错误路由信息，您必须使用路由过滤。与 passive-interface 路由器配置命令不同，一旦启用路由过滤，路由将在接口上发生，但被通告或处理的信息将受到限制。

EIGRP和RIP，使用情况distribute-list命令与缩小关键字限额什么信息通告，当使用情况在关键字限额时什么更新处理。
distribute-list 命令可用于 OSPF，但它并不能禁止路由器传播已过滤的路由。可以改用 area filter-list 命令。

本 EIGRP 示例使用 distribute-list 命令和前缀列表过滤出站通告：

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!
```

```
router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> out <interface>
!
```

本 EIGRP 示例使用前缀列表过滤入站更新：

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
passive-interface default
no passive-interface <interface>
distribute-list prefix <list-name> in <interface>
!
```

参考配置IP路由协议独立功能关于如何控制广播和处理的更多信息路由更新。

此OSPF示例以OSPF特有的area filter-list命令使用一张前缀列表：

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router ospf <process-id>
area <area-id> filter-list prefix <list-name> in
!
```

路由进程资源消耗

路由器将路由协议存储在内存中，因此资源消耗将随着路由器必须保留的附加前缀数量的增加而增加。为了防止资源耗尽，必须配置路由协议以限制资源消耗。如果使用林克状态数据库超载保护特点，这对OSPF是可能的。

本示例说明 OSPF 链路状态数据库超载保护功能的配置：

```
!

router ospf <process-id>
max-lsa <maximum-number>
!
```

有关 OSPF 链路状态数据库超载保护的详细信息，请参阅限制 OSPF 进程的自生成 LSA 的数量。

获取第一份跳跃冗余协议

第一份跳跃冗余协议(FHRPs)为作为默认网关的设备提供弹性和冗余。这种情况和这些协议在一对第 3 层设备为网段或一组包含服务器或工作站的 VLAN 提供默认网关功能的环境中十分常见。

网关负载均衡协议 (GLBP)、热备用路由器协议 (HSRP) 和虚拟路由器冗余协议 (VRRP) 都属于 FHRP。默认情况下，这些协议与未经鉴定的通信联络。攻击者可能会利用这种类型的通信伪装成 FHRP 通话设备，以承担网络上的默认网关角色。这种接管行为使攻击者能够执行中间人攻击并拦截离开网络的所有用户数据流。

为了防止此种攻击， Cisco IOS软件支持的所有FHRPs包括与MD5或文本字符串的一个验证功能。由于未经验证的 FHRP 所造成的威胁，建议这些协议实例使用 MD5 验证。本配置示例说明如何使用 GLBP、HSRP 和 VRRP MD5 验证：

```
!

interface FastEthernet 1
description *** GLBP Authentication ***
glbp 1 authentication md5 key-string <glbp-secret>
glbp 1 ip 10.1.1.1
!

interface FastEthernet 2
description *** HSRP Authentication ***
standby 1 authentication md5 key-string <hsrp-secret>
standby 1 ip 10.2.2.1
!

interface FastEthernet 3
description *** VRRP Authentication ***
vrrp 1 authentication md5 key-string <vrrp-secret>
vrrp 1 ip 10.3.3.1
```

```
!
```

数据层面

虽然数据层面负责将数据从源移动到目标，但就安全而言，数据层面是三个平面中最不重要的平面。为此是保护管理和控制层面在首选在数据层面是重要的，当您巩固一个网络设备时。

但是，在数据层面本身之内，仍然有许多功能和配置选项有助于保护数据流。以下部分将详细说明这些功能和选项，以便您能够更轻松地保护网络。

一般数据层面强化

在间网络的绝大多数的数据层面通信流如取决于网络的路由配置。但是，使用 IP 网络功能可以修改经过网络的数据包的路径。功能例如Ip options，特别地源路由选项，形成在今天网络的一个安全挑战。

使用中转 ACL 也与数据层面的强化有关。欲知更多信息，请参阅与传输本文的ACL部分的过滤器中转流量。

IP 选项选择性丢弃

IP 选项造成了两个安全问题。包含 IP 选项的数据流必须由 Cisco IOS 设备进行进程交换，这可能导致 CPU 的负载增加。Ip options也包括功能修改流量通过网络采取，潜在允许它推翻安全控制的路径。

由于这些问题，全局配置命令 ip options {drop|ignore} 被添加到 Cisco IOS 软件版本 12.3(4)T、12.0(22)S 和 12.2(25)S 中。以此命令第一个形式， ip options丢弃，包含Ip options由Cisco IOS设备接收的所有IP信息包下降。这样可以防止 IP 选项使 CPU 负载增加，并可以防止这些选项破坏安全控制。

使用此命令的第二种形式（即 ip options ignore）可以将 Cisco IOS 设备配置为忽略接收的数据包中包含的 IP 选项。虽然这样做可以减轻本地设备面临的与 IP 选项有关的威胁，但存在的 IP 选项仍然可能会影响下游设备。正是由于此原因，强烈建议使用此命令的 drop 形式。下面的配置示例中显示了如何使用此命令的 drop 形式：

```
!
ip options drop
!
```

请注意，一些协议（如 RSVP）会合法地使用 IP 选项。这些协议的功能会受到此命令的影响。

一旦启用“IP 选项选择性丢弃”，就可以使用 show ip traffic EXEC 命令确定由于存在 IP 选项而被丢弃的数据包的数量。此信息存在于 forced drop 计数器中。

有关此功能的详细信息，请参阅 ACL IP 选项选择性丢弃。

禁用 IP 源路由

IP 源路由功能同时使用“松散源路由”和“记录路由”选项，或者将“严格源路由”与“记录路由”选项一起使用，以使 IP 数据报的源能够指定数据包采用的网络路径。试图绕开网络中的安全控制来路由数据流时，可能会使用此功能。

如果没有通过“IP 选项选择性丢弃”功能完全禁用 IP 选项，请务必禁用 IP 源路由。默认情况下，所有 Cisco IOS 软件版本中均已启用 IP 源路由，该功能可通过 no ip source-route 全局配置命令禁用。本配置示例说明了此命令的用法：

```
!
no ip source-route
!
```

禁用 ICMP 重定向

ICMP 重定向用于向网络设备通知一条通向 IP 目标的更佳路径。默认情况下，如果 Cisco IOS 软件收到的数据包必须通过接收该数据包的接口进行路由，它就会发送重定向消息。

在某些状况下，攻击者促成Cisco IOS设备传送许多ICMP重定向信息也许是可能的，导致高的CPU负载。为此，建议禁用 ICMP 重定向传输。ICMP重定向禁用与接口配置no ip redirects命令，如配置示例所显示：

```
!

interface FastEthernet 0
no ip redirects
!
```

禁用或限制 IP 定向广播

使用 IP 定向广播可以向远程 IP 子网发送 IP 广播数据包。数据包到达远程网络后，转发 IP 设备会将其作为第 2 层广播发送到子网上的所有工作站。有多种攻击（包括 Smurf 攻击）已将此定向广播功能用于帮助实现放大和反射。

默认情况下，当前版本的 Cisco IOS 软件已禁用此功能；但是，可以通过 ip directed-broadcast 接口配置命令启用该功能。默认情况下，12.0 版本之前的 Cisco IOS 软件版本已启用此功能。

如果网络确实需要定向广播功能，则应当对该功能的使用进行控制。这对使用是可能的访问控制表作为选项对ip directed-broadcast命令。此配置示例限制定向广播到产生在可靠网络的那些UDP数据包， 192.168.1.0/24 ：

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

interface FastEthernet 0
ip directed-broadcast 100
!
```

与传输ACL的过滤器中转流量

控制是可能的什么流量传输与使用的网络传输ACL (tACLs)。这与设法对以网络自身为目标的数据流进行过滤的基础架构 ACL 形成对比。tACLs提供的过滤是有利的，当是理想对过滤数据流对传输网络设备或流量的一个特定组时。

传统上，这种类型的过滤由防火墙执行。但是，在某些情况下，在网络中的 Cisco IOS 设备上执行此过滤功能可能也是有益的，例如，在必须执行过滤但并不存在防火墙的情况下。

中转 ACL 也是一个适合实施静态反欺骗保护的位置。欲知更多信息，请参阅本文的反欺骗保护部分。

请参阅中转访问控制列表：在边界执行过滤了解有关 tACL 的详细信息。

ICMP 数据包过滤

Internet 控制消息协议 (ICMP) 设计为一种 IP 控制协议。因此，一般而言，该协议传达的消息可能会对 TCP 和 IP 协议产生深远的影响。网络故障排除工具 ping 和 Traceroute 以及路径 MTU 发现功能会使用 ICMP；但是，网络的正常运行很少需要外部 ICMP 连接。

Cisco IOS 软件提供按名称或类型和代码专门过滤 ICMP 消息的功能。当阻塞从其他来源时的ICMP数据包此示例ACL允许从可靠网络的ICMP ：

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Permit ICMP packets from trusted networks only
!

permit icmp host <trusted-networks> any
!
!--- Deny all other IP traffic to any network device
!

deny icmp any any
!
```

过滤器IP段

如以前被选派在限制访问对与基础设施本文的ACL部分的网络，被分段的IP信息包过滤能形成对安全设备的一挑战。

由于分段处理的非直观性质，ACL 常常会在无意中允许 IP 分段。试图逃避入侵检测系统的检测时，也会经常使用分段功能。正是由于这些原因，IP 分段经常在攻击中被使用，并应在任何已配置 tACL 的顶部明确地进行过滤。下面的 ACL 包括全面的 IP 分段过滤。本示例中说明的功能必须与前面几个示例所说明的功能结合使用：

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

deny tcp any any fragments
deny udp any any fragments
deny icmp any any fragments
deny ip any any fragments
!
```

参考的访问控制列表和IP段关于ACL处理被分段的IP信息包的更多信息。

对过滤 IP 选项的 ACL 支持

在Cisco IOS软件版本12.3(4)T和以后， Cisco IOS软件软件支持使用ACL过滤在数据包包含根据Ip options的IP信息包。Ip options出现在数据包内的也许指示尝试推翻在网络的安全控制或修改数据包的传输特性。正是由于这些原因，应该在网络边界过滤具有 IP 选项的数据包。

本示例必须与前面几个示例中的内容一起使用才能完全过滤包含 IP 选项的 IP 数据包：

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP packets containing IP options
!

deny ip any any option any-options
!
```

反欺骗保护

伪装许多攻击使用的源IP地址有效或隐瞒攻击的真正的源和妨害准确traceback。Cisco IOS软件提供单播RPF和IP源防护(IPSG)为了阻止依靠源IP地址伪装的攻击。此外，ACL 和空路由也会被经常作为手动的防欺骗方法进行部署。

IP源防护工作最小化伪装在管理控制下由执行的交换机端口、MAC地址和源地址验证的网络的。单播 RPF 提供源网络验证，并且可以减少未受到直接管理控制的网络中发起的欺骗性攻击。可以使用“端口安全”来验证接入层上的 MAC 地址。动态地址解析服务(ARP)检查(戴)缓和使用毒害在本地网段的ARP的攻击向量。

单播 RPF

单播 RPF 使设备能够验证转发的数据包的源地址是否可通过接收该数据包的接口到达。您不能完全依赖单播 RPF，将其作为防止欺骗的唯一保护措施。如果存在通向源 IP 地址的相应返回路由，则欺骗性数据包可能会通过启用单播 RPF 的接口进入网络。单播RPF在单个交换面基础上依靠您启用在每个设备的Cisco快速转发和配置。

单播 RPF 可以采用以下两种模式之一进行配置：松散模式或严格模式。在存在不对称路由的情况下首选松散模式，因为已经知道严格模式会在这些情况下丢弃数据包。在配置 ip verify 接口配置命令期间，关键字 any 用于配置松散模式，而关键字 rx 用于配置严格模式。

本示例说明此功能的配置：

```
!

ip cef
!

interface <interface>
 ip verify unicast source reachable-via <mode>
!
```

有关配置和使用单播 RPF 的详细信息，请参阅了解单播反向路径转发。

IP 源防护

如果您可以控制第 2 层接口，则 IP 源防护是可用于防止欺骗的有效方法。IP 源防护使用来自 DHCP 监听的信息在第 2 层接口上动态配置端口访问控制列表 (PACL)，并拒绝任何来自在 IP 源绑定表中没有关联的 IP 地址的数据流。

IP 源防护可以应用于属于启用了 DHCP 监听的 VLAN 的第 2 层接口。可以使用以下这些命令启用 DHCP 监听：

```
!

ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

启用 DHCP 监听之后，可以使用以下这些命令启用 IPSG：

```
!
interface <interface-id>
  ip verify source
!
```

可以使用 ip verify source port security interface 配置命令来启用端口安全。这需要使用全局配置命令 ip dhcp snooping information option；此外，DHCP 服务器必须支持 DHCP 选项 82。

有关此功能的详细信息，请参阅配置 DHCP 功能和 IP 源防护。

端口安全性

端口安全用于减少接入接口上的 MAC 地址欺骗。端口安全可以使用动态获知的（粘滞）MAC 地址轻松地进行初始配置。一旦端口安全确定了一MAC侵害，能使用四个侵害模式之一。这些模式包括保护模式、限制模式、关闭模式和关闭 VLAN 模式。在实例，当端口一个单一工作站的仅提供访问有使用的标准协议，最大一个可能是满足的。当最大数量设置为 1 时，利用虚拟 MAC 地址的协议（如 HSRP）不会起作用。

```
!

interface <interface>
 switchport
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security maximum <number>
 switchport port-security violation <violation-mode>
!
```

参考配置端口安全关于端口安全confuration的更多信息。

动态 ARP 检查

动态ARP检查(戴)可以用于为了缓和毒害在本地网段的ARP攻击。ARP 下毒攻击是攻击者向本地网段发送伪造 ARP 信息的攻击方法。此信息设计为了破坏ARP缓存其它设备。攻击者经常使用 ARP 下毒以执行中间人攻击。

DAI 拦截并验证不受信任端口上的所有 ARP 数据包的 IP 与 MAC 地址的关系。在DHCP环境，戴使用由DHCP监听的功能生成的数据。在受信任接口上接收但未能通过验证的 ARP 数据包，以及不受信任接口上的无效数据包将被丢弃。在非 DHCP 环境中需要使用 ARP ACL。

可以使用以下这些命令启用 DHCP 监听：

```
!
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

启用 DHCP 监听之后，可以使用以下这些命令启用 DAI：

```
!
ip arp inspection vlan <vlan-range>
!
```

在非 DHCP 环境中，启用 DAI 时需要 ARP ACL。本示例说明使用 ARP ACL 的 DAI 的基本配置：

```
!

arp access-list <acl-name>
permit ip host <sender-ip> mac host <sender-mac>
!

ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

有关此如何配置 DAI 的详细信息，请参阅配置动态 ARP 检查。

反欺骗 ACL

手工配置的ACL能提供静态反欺骗防护使用已知未使用和不信任地址空间的攻击。通常，这些反欺骗 ACL 作为大型 ACL 的组件应用于网络边界上的输入数据流。因为他们能频繁地更改，防欺骗ACL要求正常监听。伪装在于本地网络起源的流量可以最小化，如果应用对有效本地地址限制流量的出站ACL。

本示例说明如何使用 ACL 限制 IP 欺骗。此 ACL 应用于所需接口上的入站数据流。构成此 ACL 的 ACE 并不全面。如果要配置这些类型的 ACL，请寻找具有确定性的最新参考资料。

```
!

ip access-list extended ACL-ANTISPOOF-IN
deny ip 10.0.0.0 0.255.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
!

interface <interface>
ip access-group ACL-ANTISPOOF-IN in
!
```

有关如何配置访问控制列表的详细信息，请参阅配置常用的 IP ACL。

未分配的 Internet 地址的正式列表由 Team Cymru 维护。有关过滤未使用的地址的其他信息可以在 Bogon 参考页上找到。

限制数据层面流量CPU影响

使用路由器和交换机的主要目的，是将数据包和帧通过设备转发到最终目标。这些将经过部署在整个网络中的设备的数据包可能会影响设备 CPU 的运行。应该巩固数据层面，包括流量传输网络设备，保证管理和控制层面的操作。如果中转数据流能够导致设备处理交换机数据流，则设备的控制层面可能会受到影响，从而导致运行中断。

影响 CPU 的功能和数据流类型

尽管并不详尽，但此列表包括需要 CPU 专门进行处理以及由 CPU 进行进程交换的数据层面数据流类型：

- ACL记录- ACL记录流量包括生成的归结于匹配的所有数据包(permit或拒绝) ACE日志关键字使用。
- 单播RPF -与ACL一道使用的单播RPF也许导致进程交换某些数据包。
- Ip options -必须由CPU处理有选项的所有IP信息包包括。
- 分段-必须通过所有IP数据包要求的分段到处理的CPU。
- 存活时间(TTL)终止-有一个TTL值小于或等于1要求互联网控制消息协议Time exceeded的数据包(ICMP类型11，代码0)消息将发送，导致CPU处理。
- ICMP不可达的-导致ICMP不可达信息由于路由， MTU或者过滤的数据包由CPU处理。
- 要求ARP请求的流量- ARP条目不存在的目的地由CPU要求处理。
- 非IP数据流-所有非IP数据流由CPU处理。

有关数据层面强化的详细信息，请参阅本文档的一般数据层面强化部分。

过滤在TTL值

您可以在扩展的 IP 访问列表中使用 Cisco IOS 软件版本 12.4(2)T 中引入的“对按 TTL 值过滤的 ACL 支持”功能来基于 TTL 值过滤数据包。此功能可用于保护接收其 TTL 值为 0 或 1 的中转数据流的设备。基于 TTL 值过滤数据包还可用于确保 TTL 值不会小于网络直径，从而防止下游基础架构设备的控制层面受到 TTL 到期攻击。

请注意，一些应用程序和工具（如 Traceroute）将 TTL 到期数据包用于测试和诊断目的。一些协议（如 IGMP）合法使用 TTL 值 1。

本 ACL 示例创建一个策略，用于过滤 TTL 值小于 6 的 IP 数据包。

```
!
!--- Create ACL policy that filters IP packets with a TTL value
!--- less than 6
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any ttl lt 6
permit ip any any
!
!--- Apply access-list to interface in the ingress direction
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

有关基于 TTL 值过滤数据包的详细信息，请参阅识别和防范 TTL 到期攻击。

有关此功能的详细信息，请参阅对按 TTL 值过滤的 ACL 支持。

在Cisco IOS软件版本12.4(4)T匹配及以后，灵活的数据包中(FPM)在数据包的任意位允许管理员配比。此 FPM 策略丢弃 TTL 值小于 6 的数据包。

```
!

load protocol flash:ip.phdf
!

class-map type access-control match-all FPM-TTL-LT-6-CLASS
match field IP ttl lt 6
!

policy-map type access-control FPM-TTL-LT-6-DROP-POLICY
class  FPM-TTL-LT-6-CLASS
 drop
!
```

```
interface FastEthernet0
service-policy type access-control input FPM-TTL-LT-6-DROP-POLICY
!
```

有关此功能的详细信息，请参阅位于 Cisco IOS 灵活数据包匹配主页上的灵活数据包匹配。

在Ip options出现的过滤器

在Cisco IOS软件版本12.3(4)T和以后，您能使用ACL支持过滤Ip options功能在已命名，扩展IP访问列表为了过滤有现在的Ip options的IP信息包。基于存在的 IP 选项过滤 IP 数据包还可用于避免基础架构设备的控制层面必须在 CPU 级别处理这些数据包。

请注意，“对过滤 IP 选项的 ACL 支持”功能只能与已命名的扩展 ACL 一起使用。应该也注意RSVP、多协议标签交换数据流工程，IGMP版本2和3和使用Ip options数据包的其他协议也许不能正常运行，如果这些协议的数据包丢弃。如果网络正在使用这些协议，则可以使用“对过滤 IP 选项的 ACL 支持”；然而， ACL Ip options有选择性的丢弃功能可能降低此流量，并且这些协议也许不正常运行。如果没有要求Ip options的协议在使用中， ACL Ip options有选择性的丢弃是丢弃这些数据包的首选方法。

本 ACL 示例创建一个用于过滤包含任何 IP 选项的 IP 数据包的策略：

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option any-options
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

本示例 ACL 说明了一个用于过滤具有五个特定 IP 选项的 IP 数据包的策略。包含这些选项的数据包将被拒绝：

- 0 选项列表末尾 (eool)
- 7 记录路由 (record-route)
- 68 时间戳 (timestamp)
- 131 - 松散源路由 (lsr)
- 137 - 严格源路由 (ssr)

```
!

ip access-list extended ACL-TRANSIT-IN
deny ip any any option eool
deny ip any any option record-route
deny ip any any option timestamp
deny ip any any option lsr
deny ip any any option ssr
permit ip any any
!

interface GigabitEthernet 0/0
ip access-group ACL-TRANSIT-IN in
!
```

有关“ACL IP 选项选择性丢弃”的详细信息，请参阅本文档的一般数据层面强化部分。

请参阅中转访问控制列表：在边界执行过滤了解有关过滤中转和边界数据流的详细信息。

在 Cisco IOS 软件中，CoPP 是另一项可用于过滤具有 IP 选项的数据包的功能。在Cisco IOS软件版本12.3(4)T和以后， CoPP允许管理员过滤控制层面数据包通信流。支持 Cisco IOS 软件版本 12.3(4)T 中引入的 CoPP 和“对过滤 IP 选项的 ACL 支持”的设备，可以使用访问列表策略过滤包含 IP 选项的数据包。

此 CoPP 策略会丢弃设备收到的存在任何 IP 选项的中转数据包：

```
!

ip access-list extended ACL-IP-OPTIONS-ANY
permit ip any any option any-options
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS-ANY
!

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
 drop
!

control-plane
```

```
service-policy input COPP-POLICY
!
```

此 CoPP 策略会丢弃设备收到的存在以下这些 IP 选项的中转数据包：

- 0 选项列表末尾 (eool)
- 7 记录路由 (record-route)
- 68 时间戳 (timestamp)
- 131 松散源路由 (lsr)
- 137 严格源路由 (ssr)

```
!

ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
!

policy-map COPP-POLICY
class ACL-IP-OPTIONS-CLASS
 drop
!

control-plane
service-policy input COPP-POLICY
!
```

在前面的 CoPP 策略中，将数据包与 permit 操作进行匹配的访问控制列表条目 (ACE) 导致这些数据包被 policy-map drop 函数丢弃，而与 deny 操作匹配的数据包（未显示）并未受到 policy-map drop 函数的影响。

参考部署控制平面策略关于CoPP功能的更多信息。

控制层面保护

在Cisco IOS软件版本12.4(4)T和以后，控制层面保护(CPPr)可以由Cisco IOS设备的CPU用于为了限制或修正控制层面流量。虽然与 CoPP 类似，但与 CoPP 相比，CPPr 能够使用更细的粒度限制或管制数据流。CPPr 将整个控制层面划分为三个称为子接口的不同控制层面类别：“主机”、“中转”和“CEF 异常”子接口。

此 CPPr 策略丢弃设备收到的 TTL 值小于 6 的中转数据包，以及设备收到的 TTL 值为 0 或 1 的中转或非中转数据包。该 CPPr 策略还丢弃设备收到的具有所选 IP 选项的数据包。

```
!

ip access-list extended ACL-IP-TTL-0/1
permit ip any any ttl eq 0 1
!

class-map ACL-IP-TTL-0/1-CLASS
match access-group name ACL-IP-TTL-0/1
!

ip access-list extended ACL-IP-TTL-LOW
permit ip any any ttl lt 6
!

class-map ACL-IP-TTL-LOW-CLASS
match access-group name ACL-IP-TTL-LOW
!

ip access-list extended ACL-IP-OPTIONS
permit ip any any option eool
permit ip any any option record-route
permit ip any any option timestamp
permit ip any any option lsr
permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
match access-group name ACL-IP-OPTIONS
!

policy-map CPPR-CEF-EXCEPTION-POLICY
```

```
class ACL-IP-TTL-0/1-CLASS
 drop
class ACL-IP-OPTIONS-CLASS
 drop
!

!-- Apply CPPr CEF-Exception policy CPPR-CEF-EXCEPTION-POLICY to
!-- the CEF-Exception CPPr sub-interface of the device

!

control-plane cef-exception
service-policy input CPPR-CEF-EXCEPTION-POLICY
!

policy-map CPPR-TRANSIT-POLICY
class ACL-IP-TTL-LOW-CLASS
 drop
!

control-plane transit
service-policy input CPPR-TRANSIT-POLICY
!
```

在上一个CPPr策略，匹配有permit操作的数据包的访问控制表条目导致策略映射丢弃功能丢弃的这些数据包，而匹配拒绝操作的数据包(没显示)没有影响的是受策略映射丢弃功能的。

有关 CPPr 功能的详细信息，请参阅了解控制层面保护和控制层面保护。

数据流标识和回溯

有时，特别是在事件响应或网络性能不佳的时候，您可能需要迅速标识和回溯网络数据流。Netflow和分类ACL是完成此的两主要方法与Cisco IOS软件。使用 NetFlow 可以看到网络上的所有数据流。此外，NetFlow 还可以与能够提供长期趋势和自动分析的收集器一起实施。分类 ACL 是 ACL 的一个组件，需要进行预先规划以标识特定的数据流，并且需要在分析期间手动干预。以下这些部分提供每项功能的简要概述。

Netflow

NetFlow 通过跟踪网络数据流来标识与安全相关的异常网络活动。NetFlow数据可以通过CLI查看和被分析，或者数据可以导出到聚合和分析的一台商务或免费软件NetFlow收集器。NetFlow 收集器可以通过长期趋势跟踪提供网络行为和使用情况分析。NetFlow 通过对 IP 数据包中的特定属性执行分析和创建数据流来发挥其作用。版本 5 是最常用的 NetFlow 版本，但是，版本 9 的可扩展性更强。Netflow流可以创建与在大容积环境的被采样的数据流数据。

CEF或者分布式CEF，是前提条件对启用Netflow。NetFlow 可以配置在路由器和交换机上。

本示例说明此功能的基本配置。在 Cisco IOS 软件的早期版本中，用于在接口上启用 NetFlow 的命令是 ip route-cache flow，而不是 ip flow {ingress|出口}。

```
!

ip flow-export destination <ip-address> <udp-port>
ip flow-export version <version>
!

interface <interface>
ip flow <ingess|egress>
!
```

这是来自 CLI 的 NetFlow 输出示例。SrcIf 属性有助于执行回溯。

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
  1-32   64   96  128 160  192  224  256  288  320  352  384 416  448  480
  .741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
 55 active, 65481 inactive, 1014683 added
 41000680 ager polls, 0 flow alloc failures
 Active flows timeout in 2 minutes
 Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
 110 active, 16274 inactive, 2029366 added, 1014683 added to flow
 0 alloc failures, 0 force free
 1 chunk, 15 chunks added
 last clearing of statistics never
Protocol  Total   Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
```

```
--------  Flows    /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet  11512     0.0        15    42      0.2      33.8      44.8
TCP-FTP    5606     0.0  3     45      0.0      59.5      47.1
TCP-FTPD   1075     0.0        13    52      0.0       1.2      61.1
TCP-WWW   77155     0.0        11   530      1.0      13.9      31.5
TCP-SMTP   8913     0.0  2     43      0.0      74.2      44.4
TCP-X     351     0.0  2    40      0.0       0.0      60.8
TCP-BGP     114     0.0  1     40      0.0       0.0      62.4
TCP-NNTP    120     0.0  1     42      0.0       0.7      61.4
TCP-other 556070     0.6  8   318      6.0       8.2      38.3
UDP-DNS  130909     0.1  2     55      0.3      24.0      53.1
UDP-NTP  116213     0.1  1     75      0.1       5.0      58.6
UDP-TFTP    169     0.0  3     51      0.0      15.3      64.2
UDP-Frag      1     0.0  1   1405      0.0       0.0      86.8
UDP-other  86247     0.1       226    29     24.0      31.4      54.3
ICMP   19989     0.0        37    33      0.9      26.0      53.9
IP-other    193     0.0  1     22      0.0       3.0      78.2
Total:        1014637     1.2        26    99     32.8      13.8      43.9

SrcIf       SrcIPaddress    DstIf     DstIPaddress    Pr SrcP DstP Pkts
Gi0/1       192.168.128.21  Local     192.168.128.20  11 CB2B 07AF   3
Gi0/1       192.168.150.60  Gi0/0     10.89.17.146    06 0016 101F  55
Gi0/0       10.89.17.146    Gi0/1     192.168.150.60  06 101F 0016   9
Gi0/1       192.168.150.60  Local     192.168.206.20  01 0000 0303  11
Gi0/0       10.89.17.146    Gi0/1     192.168.150.60  06 07F1 0016   1
```

有关 NetFlow 功能的详细信息，请参阅 Cisco IOS NetFlow。

有关 NetFlow 功能的技术概述，请参阅 Cisco IOS NetFlow 简介 - 技术概述。

分类 ACL

使用分类 ACL 可以看到经过接口的数据流。分类 ACL 不会更改网络的安全策略，通常，构建它们的目的是为了将各个协议、源地址或目标进行分类。例如，可以将允许所有数据流的 ACE 按照特定的协议或端口进行划分。由于每个数据流类别都有自己的命中计数器，因此，这种将数据流更细致地按特定 ACE 进行分类的做法有助于了解网络数据流。管理员也许也分离隐式拒绝在ACL结束时到粒状ACE帮助识别通信类型拒绝的数据流。

管理员可以通过将分类 ACL 与 show access-list 和 clear ip access-list counters EXEC 命令一起使用来加快事件响应速度。

本示例说明一个用于在执行默认拒绝操作之前标识 SMB 数据流的分类 ACL 的配置：

```
!

ip access-list extended ACL-SMB-CLASSIFY
remark Existing contents of ACL
remark Classification of SMB specific TCP traffic
deny tcp any any eq 139
deny tcp any any eq 445
deny ip any any
!
```

要标识使用分类 ACL 的数据流，可以使用 show access-list acl-name EXEC 命令。ACL计数器可以被与exec命令clear ip access-list counters的ACL NAME清除。

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
   10 deny tcp any any eq 139 (10 matches)
   20 deny tcp any any eq 445 (9 matches)
   30 deny ip any any (184 matches)
```

有关如何在 ACL 中启用日志记录功能的详细信息，请参阅了解访问控制列表日志记录。

使用 VLAN 映射和端口访问控制列表进行访问控制

使用 VLAN 访问控制列表 (VACL) 或使用 VLAN 映射和端口 ACL (PACL)，可以对非路由数据流执行比应用于路由接口的访问控制列表更接近于端点设备的访问控制。

以下这些部分概述了 VACL 和 PACL 的功能、优点和可能的使用方案。

使用 VLAN 映射进行访问控制

使用 VACL 或应用于所有进入 VLAN 的数据包的 VLAN 映射，可以对 VLAN 内部的数据流执行访问控制。这对在路由接口的ACL不是可能的。例如， VLAN地图也许用于为了防止在从通信的同样VLAN内包含彼此，减少本地攻击者或蠕虫病毒的机会能利用在同一个网段的一台主机的主机。为通过使用 VLAN 映射拒绝数据包，可以创建与数据流匹配的访问控制表 (ACL)，然后，在 VLAN 映射中将 action 设置为 drop。配置 VLAN 映射后，将根据配置的 VLAN 映射按顺序对所有进入 LAN 的数据包进行评估。VLAN 访问映射支持 IPv4 和 MAC 访问列表；但是，它们不支持日志记录或 IPv6 ACL。

此示例使用说明此功能的配置的一延长的指定访问表：

```
!

ip access-list extended <acl-name>
permit <protocol> <source-address> <source-port> <destination-address>
    <destination-port>
!

vlan access-map <name> <number>
match ip address <acl-name>
action <drop|forward>
!
```

此示例展示使用VLAN地图为了拒绝TCP端口139和445以及VINES IP协议：

```
!

ip access-list extended VACL-MATCH-ANY
permit ip any any
!

ip access-list extended VACL-MATCH-PORTS
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!

mac access-list extended VACL-MATCH-VINES
permit any any vines-ip
!

vlan access-map VACL 10
match ip address VACL-MATCH-VINES
action drop
!

vlan access-map VACL 20
match ip address VACL-MATCH-PORTS
action drop
!

vlan access-map VACL 30
match ip address VACL-MATCH-ANY
action forward
!

vlan filter VACL vlan 100
!
```

有关配置 VLAN 映射的详细信息，请参阅使用 ACL 配置网络安全。

使用 PACL 进行访问控制

PACL 只能应用于交换机第 2 层物理接口的入站方向。与 VLAN 映射类似，PACL 可以提供对非路由或第 2 层数据流的访问控制。PACLs创建的语法，优先于VLAN地图和路由器ACL，是相同的象路由器ACL。如果某个 ACL 应用于第 2 层接口，则它会被称为 PACL。配置介入IPv4,IPv6的创建或者MAC ACL和应用程序它对第二层接口。

此示例使用一延长的指定访问表为了说明此功能的配置：

```
!

ip access-list extended <acl-name>
permit <protocol> <source-address> <source-port> <destination-address>
    <destination-port>
!

interface <type> <slot/port>
switchport mode access
switchport access vlan <vlan_number>
ip access-group <acl-name> in
!
```

有关配置 PACL 的详细信息，请参阅使用 ACL 配置网络安全的“端口 ACL”部分。

使用 MAC 进行访问控制

可以通过在接口配置模式下使用以下命令将 MAC 访问控制列表或扩展列表应用于 IP 网络：

```
Cat6K-IOS(config-if)#mac packet-classify
```

注意：它将第 3 层数据包归类为第 2 层数据包。Cisco IOS 软件版本 12.2(18)SXD（用于 Sup 720）和 Cisco IOS 软件版本 12.2(33)SRA 或更高版本支持此命令。

此interface命令在入口接口必须应用，并且指示转发引擎不检查IP报头。结果是您能使用在IP环境的一MAC访问列表。

专用VLAN使用

专用 VLAN (PVLAN) 属于第 2 层安全功能，可用于限制 VLAN 中的工作站或服务器之间的连接。没有PVLAN，在Layer2 VLAN的所有设备能自由地连通。在某些联网情况下，通过限制单一 VLAN 上的设备之间的通信，可以帮助提高安全性。例如，PVLAN 常用于禁止可公开访问的子网中的服务器之间的通信。如果单个服务器变得折衷，缺乏对其他服务器的连接由于PVLAN的应用程序也许帮助对这一个服务器限制妥协。

专用 VLAN 共分为三种类型：隔离 VLAN、社区 VLAN 和主 VLAN。PVLAN 的配置利用了主 VLAN 和辅助 VLAN。主 VLAN 包含所有混合端口（如后所述），并包括一个或多个辅助 VLAN，这些辅助 VLAN 可以是隔离 VLAN 或社区 VLAN。

隔离 VLAN

将辅助 VLAN 配置为隔离 VLAN 可完全阻止辅助 VLAN 中的设备之间的通信。也许只有每主VLAN一隔离VLAN，并且仅混合端口能用隔离VLAN的端口沟通。应在不受信任的网络（如支持来宾的网络）上使用隔离 VLAN。

本配置示例将 VLAN 11 配置为隔离 VLAN 并将其与主 VLAN（即 VLAN 20）关联起来。下面的示例还将接口 FastEthernet 1/1 配置为 VLAN 11 中的隔离端口：

```
!

vlan 11
private-vlan isolated
!

vlan 20
private-vlan primary
private-vlan association 11
!

interface FastEthernet 1/1
description *** Port in Isolated VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 11
!
```

社区 VLAN

配置为社区 VLAN 的辅助 VLAN 允许 VLAN 的成员之间相互通信，并允许与主 VLAN 中的任何混合端口进行通信。但是，在任何两个社区 VLAN 之间，或者在社区 VLAN 与隔离 VLAN 之间，无法进行通信。必须使用社区 VLAN 对需要在彼此之间建立连接但不需要连接到 VLAN 中的所有其他设备的服务器进行分组。此方案在可公开访问的网络中或在服务器向不受信任客户端提供内容的情况下十分常见。

本示例配置一个社区 VLAN 并将交换机端口 FastEthernet 1/2 配置为该 VLAN 的成员。社区 VLAN（即 VLAN 12）是主 VLAN 20 的辅助 VLAN。

```
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 12
!

interface FastEthernet 1/2
description *** Port in Community VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 12
!
```

混合端口

位于主 VLAN 中的交换机端口称为混合端口。混合端口可以与主 VLAN 和辅助 VLAN 中的所有其他端口通信。路由器或防火墙接口是这些 VLAN 上最常见的设备。

本配置示例结合了前面的隔离和社区 VLAN 示例，并添加了作为混合端口的接口 FastEthernet 1/12 的配置：

```
!

vlan 11
private-vlan isolated
!

vlan 12
private-vlan community
!

vlan 20
private-vlan primary
private-vlan association 11-12
!

interface FastEthernet 1/1
description *** Port in Isolated VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 11
!

interface FastEthernet 1/2
description *** Port in Community VLAN ***
switchport mode private-vlan host
switchport private-vlan host-association 20 12
!

interface FastEthernet 1/12
description *** Promiscuous Port ***
switchport mode private-vlan promiscuous
switchport private-vlan mapping 20 add 11-12
!
```

当您实现PVLAN时，请注意到位第3层配置支持PVLAN强加的限制，并且不允许PVLAN配置将被推翻。与路由器ACL或防火墙的第3层过滤可以防止PVLAN配置的颠覆。

有关使用和配置专用 VLAN 的详细信息，请参阅位于 LAN 安全主页上的专用 VLAN (PVLAN) - 混合 VLAN、隔离 VLAN、社区 VLAN。

结论

本文档对可用于保护 Cisco IOS 系统设备的方法进行了粗略的概述。如果您对设备加以保护，您管理的网络的总体安全也会随之增强。本概述讨论了管理平面、控制层面和数据层面的保护，并提供了一些配置建议。在可能的情况下，我们为每一种相关功能的配置提供了足够详细的信息。但是，在所有的情况下，我们都为您提供了做出进一步评估所需的全面参考资料。

鸣谢

在本文的一些功能描述由思科信息开发组写入。

附录：硬化清单的Cisco IOS设备

此清单是在此指南被提交所有硬化的步骤的一集。管理员能使用它，当提醒所有硬化以为特色使用和考虑为Cisco IOS设备，即使功能未实现，因为没有应用。在他们实现选项前，管理员建议评估其潜伏风险的每个选项。

管理平面

- 密码
  - 启用切细(秘密选项)为enable (event)和本地用户密码的MD5
  - 配置密码重试次数中断
  - 禁用密码恢复(请考虑风险)
- 禁用未使用服务
- 配置管理会话的TCP Keepalive
- 设置内存和CPU阈值通知
- 配置
  - 内存和CPU阈值通知
  - 控制台访问的保留内存
  - 内存泄漏检漏仪
  - 缓冲区溢出检测
  - 增强版Crash信息集
- 请使用iACLs限制管理访问
- 过滤(请考虑风险)
  - ICMP数据包
  - IP段
  - IP 选项
  - 在数据包的TTL值

- 控制层面保护
  - 配置端口过滤器
  - 配置队列阈值
- 管理访问
  - 请使用管理层面保护限制管理接口
  - 设置exec超时
  - 请使用一个已加密传输协议(例如SSH) CLI访问
  - 控制VTY和tty线路的(访问Class选项)传输
  - 警告使用标语
- AAA
  - 请使用AAA验证和fallback
  - 请使用AAA (TACACS+) authorization命令
  - 请使用AAA核算
  - 请使用冗余的AAA服务器
- SNMP
  - 配置SNMPv2社区并且应用ACL
  - 配置SNMPv3
- 记录
  - configure集中了记录日志
  - 设置所有相关组件的日志级别
  - 设置logging source-interface
  - 配置记录时间戳粒度
- 配置管理
  - 替换和回退
  - 以独占方式进行配置更改访问
  - 软件弹性配置
  - 配置更改通知

控制层面

- 禁用(请考虑风险)
  - ICMP重定向
  - ICMP 不可达
  - 代理 ARP
- 如果使用，请配置NTP认证NTP
- 配置控制平面策略/保护(端口过滤器，队列阈值)
- 获取路由协议
  - BGP (TTL， MD5、最大前缀，前缀列表，系统路径ACL)
  - IGP (MD5、无源接口、路由过滤，消耗的资源)
- 配置硬件速率防幅器
- 获取第一份跳跃冗余协议(GLBP、HSRP， VRRP)

数据层面

- 配置Ip options有选择性的丢弃
- 禁用(请考虑风险)
  - IP 源路由
  - IP 定向广播
  - ICMP重定向
- 限制IP定向广播
- 配置tACLs (请考虑风险)
  - 过滤ICMP
  - 过滤IP段
  - 过滤Ip options
  - 过滤TTL值
- configure要求反欺骗保护
  - ACL
  - IP 源防护
  - 动态 ARP 检查
  - 单播 RPF
  - 端口安全性
- 控制层面保护(控制面板CEF例外)
- 配置流量识别的Netflow和分类ACL
- configure要求访问控制ACL (VLAN地图， PACLs， MAC)
- 配置专用VLAN

文件创建日期: 2016 年 6 月 22 日

http://www.cisco.com/cisco/web/support/CN/107/1078/1078022_21.html