强化 IOS 设备

目录

- 简介
- 先决条件
  - 要求
  - 使用的组件
- 背景
- 确保运行安全
  - 监视 Cisco 安全建议及响应
  - 利用身份验证、授权和记账
  - 集中日志收集和监控流程
  - 尽可能使用安全协议
  - 使用 NetFlow 获得数据流可见性
  - 配置管理
- 管理平面
  - 一般管理平面强化
  - 密码管理
    - 增强的口令安全
    - 登录密码重试锁定
    - No Service Password-Recovery
    - 禁用未使用的服务
    - EXEC 超时
    - TCP 会话的 Keepalive
    - 管理接口用法
    - 内存阈值通知
    - CPU 阈值通知
    - 保留内存以用于控制台访问
    - 内存泄漏探测器
    - 缓冲区溢出：检测并修复 Redzone 损坏
    - 改进的 Crashinfo 文件收集
    - 网络时间协议 (NTP)
    - 禁用智能安装
    - 仅使用SMI功能进行零接触部署的客户
    - 利用SMI功能进行非零接触部署的客户
  - 利用基础设施 ACL 限制网络访问
    - ICMP 数据包过滤
    - 过滤 IP 分段
    - 过滤IP选项的ACL支持
    - 对基于 TTL 值过滤的 ACL 支持
  - 安全交互式管理会话
    - 管理平面保护
    - 控制层面保护
    - 加密管理会话
    - SSHv2
    - 适用于 RSA 密钥的 SSHv2 增强功能

- 控制台和 AUX 端口
- 控制 vty 和 tty 线路
- 控制 vty 和 tty 线路的传输
- 警告标志

- 验证、授权和记帐
  - TACACS+ 身份验证
  - 身份验证回退
  - 使用类型 7 口令
  - TACACS+ 命令授权
  - TACACS+ 命令记账
  - 冗余 AAA 服务器

- 增强简单网络管理协议
  - SNMP 社区字符串
  - SNMP 社区字符串与 ACL
  - 基础架构 ACL
  - SNMP 视图
  - SNMP 版本 3
  - 管理平面保护

- 日志记录最佳实践
  - 将日志发送到中央位置
  - 日志记录级别
  - 请勿记录到控制台或监视会话中
  - 使用缓冲日志
  - 配置日志记录源接口
  - 配置日志时间戳

- Cisco IOS 软件配置管理
  - 配置替换和配置回滚
  - 以独占方式进行配置更改访问
  - Cisco IOS 软件弹性配置
  - 数字签名的思科软件
  - 配置更改通知和日志

控制层面

- 一般控制层面强化
  - IP ICMP 重定向
  - ICMP 不可达
  - 代理 ARP

- 限制控制平面流量对 CPU 的影响
  - 了解控制平面流量
  - 基础架构 ACL
  - 接收 ACL
  - CoPP
  - 控制层面保护
  - 硬件速率限制器

- 安全 BGP
  - 基于 TTL 的安全保护
  - 使用 MD5 进行 BGP 对等验证
  - 配置最大前缀数
  - 使用前缀列表过滤 BGP 前缀
  - 使用自治系统路径访问列表过滤 BGP 前缀

- 安全内部网关协议
  - 使用消息摘要 5 的路由协议验证和验证
  - Passive-interface 命令

- 路由过滤
- 路由进程资源消耗
- 安全第一跳冗余协议

数据层面

- 一般数据层面强化
  - IP 选项选择性丢弃
  - 禁用 IP 源路由
  - 禁用 ICMP 重定向
  - 禁用或限制 IP 定向广播
- 使用传输 ACL 过滤传输流量
  - ICMP 数据包过滤
  - 过滤 IP 分段
  - 过滤IP选项的ACL支持
- 反欺骗保护
  - 单播 RPF
  - IP 源防护
  - 端口安全性
  - 动态 ARP 检查
  - 反欺骗 ACL
- 限制数据平面流量对 CPU 的影响
  - 影响 CPU 的功能和数据流类型
  - 基于 TTL 值过滤
  - 基于是否存在 IP 选项过滤
  - 控制层面保护
- 数据流标识和回溯
  - Netflow
  - 分类 ACL
- 使用 VLAN 映射和端口访问控制列表进行访问控制
  - 使用 VLAN 映射进行访问控制
  - 使用 PACL 进行访问控制
  - 使用 MAC 进行访问控制
- 专用 VLAN 使用
  - 隔离 VLAN
  - 社区 VLAN
  - 混合端口

结论

鸣谢

附录：思科 IOS 设备强化清单

- 管理平面
- 控制层面
- 数据层面

简介

本文档介绍如何保护Cisco IOS®系统设备并提高网络的整体安全性。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景

当您保护Cisco IOS系统设备时，网络的整体安全性会增加。

网络的整体安全性围绕网络设备功能可归入的三个层面来构建。网络的三个功能层面分别是：管理平面、控制平面和数据平面，每个平面提供需要保护的不同功能。本文档提供了每个所含功能的概述以及对相关文档的参考。

- 管理平面 — 管理平面管理发送到Cisco IOS设备的流量，由应用程序和协议组成，例如安全外壳(SSH)和简单网络管理协议(SNMP)。
- 控制平面 - 网络设备的控制平面处理对于维护网络基础设施功能最重要的流量。控制平面包括网络设备之间的应用和协议，例如边界网关协议(BGP)以及内部网关协议(IGP)。 还包括增强型内部网关路由协议(EIGRP)和开放最短路径优先(OSPF)。
- 数据平面 - 数据平面通过网络设备转发数据。数据平面不包括发送到本地Cisco IOS设备的流量。

本文档中涉及的安全功能通常提供足够详细信息，以便您配置所述功能。但是，如果没有详细信息，则以某种方式解释该功能，以便您可以评估是否需要对该功能给予更多关注。在可能和适当的情况下，本文档包含一些建议，这些建议在实施后将有助于确保网络安全。

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

思科产品安全事件响应小组 (PSIRT) 针对思科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。思科安全公告中提供了安全公告和响应。

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。

要维护安全网络，请注意已发布的思科安全建议和响应。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。如需与此评估流程相关的帮助，请参阅“安全漏洞风险分类公告”。

利用身份验证、授权和记账

身份验证、授权和记帐 (AAA) 框架对于确保网络设备安全至关重要。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。有关如何利用 AAA 的更多信息，请参阅本文档的身份验证、授权和记帐部分。

集中日志收集和监控流程

要了解与安全事件相关的当前、紧急和历史事件，您的组织必须具有事件日志和关联的统一策略。此统一策略必须利用来自所有网络设备的日志，并使用预打包的可自定义关联功能。

实施集中日志后，您必须开发一种结构化方法来记录分析和跟踪事故。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

使用多个协议来传输敏感的网络管理数据。尽可能使用安全协议。安全协议选择包括使用SSH而不是Telnet，因此身份验证数据和管理信息都会被加密。此外，在复制配置数据时使用安全文件传输协议。例如，使用安全复制协议 (SCP) 代替 FTP 或 TFTP。

有关思科 IOS 设备安全管理的更多信息，请参阅本文档的安全交互式管理会话部分。

使用 NetFlow 获得数据流可见性

NetFlow使您能够监控网络上的流量。NetFlow最初用于将流量信息导出到网络管理应用程序，但也可以用于显示路由器上的流量信息。使用此功能可以实时查看经过网络的数据流。无论是否将流信息导出到远程收集器，都建议您为NetFlow配置网络设备，以便在需要时可反应性地使用它。

有关此功能的详细信息，请参阅本文档的流量识别和回溯部分和Cisco IOS NetFlow。

注意：只有思科注册用户才能访问内部工具和信息。

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。

使用配置存档回滚对网络设备所做的更改。在安全情景中，还可以使用配置存档来确定进行了哪些安全更改以及更改发生的时间。此信息与AAA日志数据一起有助于网络设备的安全审计。

Cisco IOS 设备的配置包含许多敏感的详细信息。用户名、密码和访问控制列表的内容都是此类敏感信息的示例。需要保护用于存档Cisco IOS设备配置的存储库。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。其中包括使用 SSH 的交互式管理会话，以及使用 SNMP 或 Netflow 的统计信息收集功能。当您考虑网络设备的安全时，保护管理平面至关重要。如果安全事件能够破坏管理平面的功能，则可能无法恢复或稳定网络。

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，以及监控其运行和部署设备的网络。管理平面接收并发送用于这些功能操作的流量。保护设备的管理平面和控制平面，因为控制平面操作直接影响管理平面的操作。管理平面使用的协议包括：

- 简单网络管理协议 (SNMP)
- Telnet
- Secure Shell 协议 (SSH)
- 文件传输协议
- 超文本传输协议/安全超文本传输协议

- 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)
- 系统日志

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。如果任一平面被成功利用，所有平面都可能被入侵。

密码管理

口令控制对资源或设备的访问。这是通过用于验证请求的密码实现的。当收到访问资源或设备的请求时，该请求会受到质询以验证密码和身份，并且可以根据结果授予、拒绝或限制访问。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。但是，当TACACS+或RADIUS服务发生故障时，仍需要本地配置特权访问密码。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。

命令**enable secret**用于设置授予对Cisco IOS系统的特权管理访问权限的密码。必须使用命令enable secret，而不是旧的命enable password令。该命enable password令使用弱加密算法。

如果没**enable secret**有设置且为控制台tty线路配置了口令，则控制台口令可用于接收特权访问，甚至可以从远程虚拟tty(vty)会话接收特权访问。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。

全局**service password-encryption**配置命令指示Cisco IOS软件加密密码、质询握手身份验证协议(CHAP)密钥和保存在其配置文件中的类似数据。这种加密有助于防止偶然观察者观察密码，例如当他们看到管理员肩膀上的屏幕时。但是，该命令使用的算**service password-encryption**法是简单的Vigen re密码。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。

虽然该命令不使用此弱加密算法，但全局配置命令以及线路配置命令都使用了该算法**enable secretenable password**。必须消除此类密码，并且需**enable secret**要使用命令或Enhanced Password安全功能。

命令enable secret和增强密码安全功能使用消息摘要5(MD5)进行密码散列。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，攻击者会尝试字典或其他候选密码列表中的每个字来查找匹配项。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

Cisco IOS软件版本12.2(8)T中引入的增强密码安全功能允许管理员为命令配置MD5密码散列username。在此功能之前，有两种类型的密码：类型 0 和类型 7，前者是明文密码，后者使用基于 Vigenre 加密的算法。“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散列加密用户密码，请发出全局username secret 配置命令。

```
!

username <name> secret <password>

!
```

登录密码重试锁定

思科 IOS 软件版本 12.3(14)T 中添加了登录密码重试锁定功能，允许您在本地用户帐户尝试登录失败次数达到配置的次数后将其锁定。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。使用此功能不能锁定配置权限级别为15的授权用户。将权限级别为15的用户数保持为最小值。

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>
```

```
!
```

此功能也适用于身份验证方法，例如CHAP和密码身份验证协议(PAP)。

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软件提供密码恢复过程，该过程依赖于访问ROM监控模式(ROMMON)，该模式在系统启动期间使用Break键。在ROMMON中，可以重新加载设备软件，以提示包含新密码的新系统配置。

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。在系统启动期间，“无密码恢复”功能可防止 Break 键序列完成和进入 ROMMON 模式。

如果**no service password-recovery**在设备上启用，则建议保存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。

有关此功能的更多信息，请参阅安全 ROMMON 配置示例。

禁用未使用的服务

作为安全最佳实践，请禁用任何不必要的服务。不需要的服务，尤其是使用用户数据报协议(UDP)的服务，很少用于合法目的，但可用于发起DoS和其他通过数据包过滤阻止的攻击。

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）

尽管通过反欺骗访问列表可以避免或降低滥用小型服务的危险，但在网络中可访问的任何设备上禁用这些服务。默认情况下，Cisco IOS软件版本12.0及更高版本禁用小型服务。在早期的软件中，**no service tcp-small-servers**可以**no service udp-small-servers**发出and全局配置命令来禁用它们。

如果不使用，必须禁用的其他服务包括：

- 发出no ip finger global configuration命令以禁用Finger服务。默认情况下，高于12.1(5)和12.1(5)T的Cisco IOS软件版本禁用此服务。
- 发出全局配置命令no ip bootp server，以禁用引导协议(BOOTP)。
- 在Cisco IOS软件版本12.2(8)T及更高版本中，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。
- 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。
- 发出no ip domain-lookup全局配置命令以禁用域名系统(DNS)解析服务。
- 在全局配置模式下发出no service pad命令，以禁用用于X.25网络的数据包组装器/分解器(PAD)服务。
  在全局配置模式下，可使用 no ip http server 命令禁用 HTTP 服务器，并可使用 no ip http secure-server 全局配置命令以禁用安全 HTTP (HTTPS) 服务器。
  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。这样可防止思科 IOS 设备尝试使用 TFTP 查找网络中的配置文件。
  Cisco发现协议(CDP)是一种网络协议，用于发现其它支持CDP的设备以实现邻居邻接和网络拓扑。网络管理系统(NMS)可以在发生故障隔离时使用CDP。必须在连接到不可信网络的所有接口上禁用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，恶意用户可以使用CDP进行侦察和映射网络。
- 链路层发现协议(LLDP)是802.1AB中定义的IEEE协议，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。为此，请发出no lldp transmit和no lldp receive接口配置命令。发出no lldp run全局配置命令以全局禁用LLDP。恶意用户也可以使用LLDP进行侦察和映射网络。

- 对于支持从sdflash引导的交换机，可以通过“no sdflash”配置命令增强从闪存引导和禁用sdflash的安全性。

EXEC 超时

要设置间隔，EXEC命令解释程序在终止会话之前等待用户输入，请发出exec-timeout线路配置命令。使用exec-timeout命令注销闲置的vty或tty线路上的会话。默认情况下，会话会在处于非活动状态 10 分钟后断开。

```
!
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 全局配置命令允许设备发送 TCP keepalive 以进行 TCP 会话。使用此配置可在设备的入站连接和设备的出站连接上启用TCP keepalive。这样可以确保连接远程端的设备仍然可访问，并且从本地Cisco IOS设备中删除半开连接或孤立连接。

```
!

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

管理接口用法

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，每个网络设备都有带内和带外管理访问，因此可以在网络中断期间访问管理平面。

用于设备带内访问的最常见接口之一是逻辑环回接口。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。建议为每个设备添加一个环回接口作为管理接口，并且只用于管理平面。这使得管理员可以在整个网络中应用管理平面策略。一旦在设备上配置了环回接口，管理平面协议（如SSH、SNMP和系统日志）就可以使用环回接口来发送和接收流量。

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

内存阈值通知

通过Cisco IOS软件版本12.3(4)T中添加的内存阈值通知功能，您可以缓解设备上的内存不足问题。此功能使用两种方法实现这一目的：“内存阈值通知”和“内存保留”。

Memory Threshold Notification会生成日志消息，指示设备上的可用内存已低于配置的阈值。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>
!
```

使用内存预留，以便有足够的内存可用于关键通知。此配置示例演示如何启用此功能，以确保设备内存用尽时管理进程继续运行。

```
!

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

在Cisco IOS软件版本12.3(4)T中引入的CPU阈值通知功能允许您在设备的CPU负载超过配置的阈值时检测并接收通知。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使用阈值方法：“上升阈值”和“下降阈值”。

此示例配置显示如何启用上升和下降阈值以触发CPU阈值通知消息：

```
!

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，“为控制台访问保留内存”功能可用于保留足够的内存，以确保对Cisco IOS设备的控制台访问，用于管理和故障隔离。当设备内存不足时，此功能尤其有用。您可以发出memory reserve console全局配置命令来启用此功能。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
!
```

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。内存泄漏检测器可以发现所有内存池、数据包缓冲区和数据块中的泄漏。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。可以使用show memory debug leaks EXEC命令检测是否存在内存泄漏。

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：可以在设备上启用检测和纠正Redzone损坏功能，以检测和纠正内存块溢出并继续操作。

全局配置命令可用于启用此功能。配置完成后，show memory overflow命令可用于显示缓冲区溢出检测和更正统计信息。

```
!
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。当设备崩溃时，该功能（Cisco IOS 软件版本 12.3(11)T 中已添加）允许设备回收空间以创建新的 crashinfo 文件。此功能还允许配置要保存的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)不是一种危险的服务，但任何不需要的服务都可能代表攻击媒介。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。系统日志需要准确可靠的时间，例如对潜在攻击进行取证调查期间，以及依赖证书进行第1阶段身份验证时成功的VPN连接。

- NTP Time Zone — 配置NTP时，需要配置时区，以便准确关联时间戳。为具有全局在线状态的网络上的设备配置时区有两种典型方法。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。有关此功能的详细信息，请参阅思科产品文档中的“clock timezone”。
- NTP 身份验证 - 如果配置 NTP 身份验证，则可确保在受信任的 NTP 对等设备之间交换 NTP 消息。

以下是使用NTP身份验证的示例配置：

客户端：

<#root>

```
(config)#

ntp authenticate


(config)#

ntp authentication-key 5 md5 ciscotime


(config)#

ntp trusted-key 5


(config)#

ntp server 172.16.1.5 key 5
```

服务器：

```
<#root>

(config)#

ntp authenticate


(config)#

ntp authentication-key 5 md5 ciscotime


(config)#

ntp trusted-key 5
```

禁用智能安装

思科智能安装(SMI)功能的安全最佳实践取决于该功能在特定用户环境中的使用方式。思科将这些使用案例区分开来：

- 不使用SMI功能的用户。
- 仅使用SMI功能进行零接触部署的用户。
- 利用Smart InstallSMI功能进行零接触部署（配置和映像管理）的用户。

以下部分详细介绍了每个场景：

- 不使用SMI功能的用户。
- 不使用SMI功能，并且在命令可用时运行Cisco IOS和Cisco IOS XE软件版本的用户可以使用no vstack命令禁用SMI功能。

注意：vstack命令在Cisco IOS版本12.2(55)SE03中引入。

以下是禁用SMI客户端功能的Cisco Catalyst交换机上show vstack命令的输出示例：

```
<#root>

switch#

show vstack


config Role: Client (SmartInstall disabled)
```

```
Vstack Director IP address: 0.0.0.0
```

仅使用SMI功能进行零接触部署的客户

零接触安装完成后，禁用SMI客户端功能或使用no vstack命令。

要将no vstack命令传播到网络中，请使用以下方法之一：

- 在所有客户端交换机上输入no vstack命令（手动输入或使用脚本）。
- 添加no vstack命令作为Cisco IOS配置的一部分，该配置作为零接触安装的一部分推送到每个SMI客户端。
- 在不支持vstack命令的版本(Cisco IOS版本12.2(55)SE02及更早版本)中，在客户端交换机上应用访问控制列表(ACL)以阻止TCP端口4786上的流量。

要稍后启用SMI客户端功能，请在所有客户端交换机上输入vstack命令（手动输入或使用脚本）。

利用SMI功能进行非零接触部署的客户

在SMI架构的设计中，请注意使基础设施IP地址空间不被不受信任方访问。在不支持vstack命令的版本中，确保只有SMI指挥交换机与端口4786上的所有SMI客户端具有TCP连接。

管理员可以使用以下安全最佳实践在受影响设备上进行SMI部署：

- 接口ACL
- 控制平面策略(CoPP)。 并非所有Cisco IOS软件版本都提供此功能。

此示例显示一个接口ACL，其SMI指挥交换机IP地址为10.10.10.1,SMI客户端IP地址为10.10.10.200:

```
ip access-list extended SMI_HARDENING_LIST
Permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
deny tcp any any eq 4786
permit ip any any
```

此ACL必须部署在所有客户端的所有IP接口上。指挥交换机也可以在首次部署时由指挥交换机推送。

要进一步限制对基础设施内所有客户端的访问，管理员可以在网络上的其他设备上使用这些最佳安全实践：

- 基础设施访问控制列表(iACL)
- VLAN访问控制列表(VACL)

利用基础设施 ACL 限制网络访问

iACL旨在防止未经授权直接与网络设备通信，是网络中实施的最关键的安全控制之一。iACL的理念是，几乎所有网络流量都流经网络，而不是发往网络本身。

因此，可以构建并应用 iACL 来指定来自主机或网络的、需要被允许访问网络设备的连接。这些连接类型的常见示例包括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。通过对网络基础设施设备使用不同的地址，可以简化iACL的实施。有关IP地址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，它传达的消息可能会与TCP和IP协议发生显着交互。当使用ICMP进行故障排除的网络工具ping和traceroute时，正确的网络操作很少需要外部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。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 IP 分段

对安全设备而言，分片IP数据包的过滤过程可能是一项挑战。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 软件使用特定方法，根据配置的访问列表来检查非初始分段。Cisco IOS软件根据ACL评估这些非初始分段，并忽略任何第4层过滤信息。这会导致仅在任何已配置ACE的第3层部分上评估非初始分段。

在此示例配置中，如果端口22上发往192.168.1.1的TCP数据包在传输过程中分段，则根据数据包中的第4层信息，第二个ACE会按预期丢弃初始分段。但是，完全基于数据包和ACE中的第3层信息，第一个ACE允许剩余的所有（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。分段通常用于尝试逃避入侵检测系统的检测。出于这些原因，IP分段经常用于攻击，以及为什么必须在任何已配置的iACL的顶部显式过滤它们。本示例ACL包括对IP分段的全面过滤。本示例中的功能必须与前面示例中的功能配合使用。

```
!

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
!
```

有关 ACL 如何处理分段 IP 数据包的更多信息，请参阅访问控制列表和 IP 分段。

过滤IP选项的ACL支持

Cisco IOS软件版本12.3(4)T增加了对使用ACL根据数据包中包含的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。这要求有一定程度的CPU工作量，而对于通过网络传输的典型数据包则不需要这种工作量。数据包中存在IP选项也表示有人试图破坏网络的安全控制，或者以其他方式改变数据包的中转特征。因此，必须在网络边缘过滤具有IP选项的数据包。

此示例必须与前面示例中的ACE一起使用，以包括完全过滤包含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
!
```

对基于 TTL 值过滤的 ACL 支持

Cisco IOS软件版本12.4(2)T添加了ACL支持，根据生存时间(TTL)值过滤IP数据包。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。虽然初始值因操作系统而异，但当数据包的TTL达到零时，必须丢弃该数据包。将 TTL 递减到零并因此丢弃数据包的设备需要生成一条“ICMP 超时”消息，并将该消息发送到数据包的源。

生成和传输这些消息属于异常处理。当到期的IP数据包数量较少时，路由器可以执行此功能，但是如果到期的数据包数量较多，则生成和传输这些消息会占用所有可用的CPU资源。这提供了一个 DoS 攻击矢量。因此，需要对设备进行强化，使其免受使用高速率IP数据包（即将到期）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。完全过滤TTL值不足以穿越网络的数据包，从而缓解基于TTL的攻击威胁。

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：有些协议使用 TTL 值较小的数据包是合法的。eBGP 就是这样一个协议。有关缓解基于TTL到期的攻击的详细信息，请参阅TTL到期攻击识别和缓解。

安全交互式管理会话

通过设备管理会话，可以查看和收集有关设备及其操作的信息。如果向恶意用户披露此信息，设备可能会成为攻击目标、被入侵并用于执行其他攻击。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。必须保护管理会话的安全，以防止信息泄露和未经授权的访问。

管理平面保护

在Cisco IOS软件版本12.4(6)T及更高版本中，管理平面保护(MPP)功能允许管理员对设备收到的不同接口管理流量施加限制。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。

本示例说明如何启用 MPP 以仅在 GigabitEthernet0/1 接口上允许 SSH 和 HTTPS：

```
!

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。

注意：MPP不支持IPv6，且仅限于IPv4输入路径。因为IPv6未过滤，所以在混合IPv4/IPv6环境中使用CoPP。

控制层面保护

控制平面保护(CPPr)建立在控制平面策略功能的基础上，用于限制和管制发往Cisco IOS设备的路由

处理器的控制平面流量。在Cisco IOS软件版本12.4(4)T中添加时，CPPr将控制平面分为不同的控制平面类别，称为子接口。共有三种控制层面子接口：主机、传输和CEF异常。此外，CPPr还包括以下控制平面保护功能：

- 端口过滤功能 — 允许管理员管制或丢弃进入关闭或非侦听TCP和UDP端口的数据包。
- Queue-threshold policy feature — 限制控制平面IP输入队列中允许的指定协议的数据包数量。

CPPr允许管理员对发送到设备的流量进行分类、管制和限制，以便通过主机子接口进行管理。主机子接口类别的数据包示例包括管理流量（如SSH或Telnet）和路由协议。

 注意：CPPr 不支持 IPv6，仅限于 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。

加密管理会话

由于信息可以在交互式管理会话中公开，因此必须加密此流量，以便恶意用户无法访问传输的数据。流量加密可确保与设备建立安全的远程访问连接。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。

管理员可以使用 SSH 或 HTTPS（安全超文本传输协议）功能与设备建立加密的安全远程访问管理连接。思科 IOS 软件支持 SSH 版本 1.0 (SSHv1)、SSH 版本 2.0 (SSHv2) 和 HTTPS，其中 HTTPS 使用安全套接字层 (SSL) 和传输层安全 (TLS) 进行身份验证和数据加密。SSHv1 和 SSHv2 不兼容。SSHv1不安全，且不标准化，因此如果选择SSHv2，则不建议使用SSHv1。

Cisco IOS软件还支持安全复制协议(SCP)，该协议允许通过加密和安全连接来复制设备配置或软件映像。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
!
```

此配置示例适用于HTTPS服务：

```
!

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

Cisco IOS软件版本12.3(4)T中引入的SSHv2支持功能允许用户配置SSHv2。（SSHv1支持在Cisco IOS软件的早期版本中实施。）SSH 在可靠的传输层之上运行，并提供强大的身份验证和加密功能。为SSH定义的唯一可靠传输是TCP。SSH提供了一种通过网络在其它计算机或设备上安全访问并安全执行命令的方法。通过SSH隧道传输的安全复制协议(SCP)功能允许安全传输文件。

如果未明确配置ip ssh version 2命令，则Cisco IOS启用SSH版本1.99。SSH版本1.99允许SSHv1和SSHv2连接。SSHv1被认为是不安全的，可能会对系统产生不利影响。如果启用了SSH，建议使用ip ssh version 2命令禁用SSHv1。

本示例配置在思科 IOS 设备上启用了 SSHv2（且禁用了 SSHv1）：

```
!

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

!
```

有关使用 SSHv2 的更多信息，请参阅 安全外壳版本 2 支持。

适用于 RSA 密钥的 SSHv2 增强功能

思科 IOS SSHv2 支持键盘交互式和基于密码的身份验证方法。适用于 RSA 密钥的 SSHv2 增强功能还支持针对客户端和服务器执行基于 RSA 的公钥身份验证。

对于用户验证，基于 RSA 的用户验证使用与每个用户关联的私钥/公钥对进行身份验证。用户必须在客户端上生成私钥/公钥对，并在Cisco IOS SSH服务器上配置公钥以完成身份验证。

由尝试建立凭证的 SSH 用户使用私钥提供加密的签名。加密签名和用户公钥将发送到SSH服务器进行身份验证。SSH 服务器基于该用户提供的公钥计算散列值。散列用于确定服务器是否有匹配的条目。如果找到匹配项，将使用公钥执行基于 RSA 的消息验证。因此，根据加密的签名验证用户或拒绝访问。

对于服务器验证，思科 IOS SSH 客户端必须为每个服务器分配一个主机密钥。当客户端尝试与服务器建立 SSH 会话时，它将作为密钥交换消息的一部分收到服务器的签名。如果在客户端上启用了严格主机密钥检查标志，则客户端将检查它是否具有与预先配置的服务器对应的主机密钥条目。如果找到匹配项，客户端将尝试使用服务器主机密钥验证签名。如果服务器验证成功，将继续建立会话；否则，将终止验证并显示服务器验证失败消息。

本示例配置在思科 IOS 设备上启用了 RSA 密钥及 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
!
```

有关使用 RSA 密钥及 SSHv2 的更多信息，请参阅[适用于 RSA 密钥的安全外壳版本 2 增强功能。]

本示例配置支持思科 IOS SSH 服务器执行基于 RSA 的用户验证。如果使用客户端上存储的公钥或私钥对验证服务器上存储的 RSA 公钥，则用户验证将成功。

```
!
! 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.)
!
```

有关使用 RSA 密钥及 SSHv2 的更多信息，请参阅[配置思科 IOS SSH 服务器以执行基于 RSA 的用户验证部分。]

此配置示例支持思科 IOS SSH 客户端执行基于 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
!
```

有关使用 RSA 密钥及 SSHv2 的更多信息，请参阅配置思科 IOS SSH 客户端以执行基于 RSA 的服务器验证部分。

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。请注意，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。要执行密码恢复，未经身份验证的攻击者需要访问控制台端口并中断设备电源或导致设备崩溃的能力。

任何用于访问设备控制台端口的方法都必须以与对设备进行特权访问所实施的安全性同等的方式加以保护。用于保护访问的方法必须包括使用AAA、exec-timeout和调制解调器密码（如果调制解调器连接到控制台）。

如果不需要口令恢复，则管理员可以通过no service password-recovery全局配置命令删除执行口令恢复过程的能力；但是，一旦启用了no service password-recovery命令，管理员就无法在设备上执行密码恢复。

在大多数情况下，必须禁用设备AUX端口以防止未经授权的访问。通过以下命令可禁用 Aux 端口：

```
!

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。为确保本地或远程管理会话可以访问设备，必须在vty和tty线路上实施适当的控制。Cisco IOS 设备具有的 vty 线路的数量有限；使用 show line EXEC 命令可确定可用的线路数。当所有vty线路都在使用时，无法建立新的管理会话，这可以为访问设备创建DoS条件。

对设备的vty或tty的最简单访问控制是在所有线路上使用身份验证，而不考虑设备在网络上的位置。这对于vty线路至关重要，因为网络可以访问这些线路。连接到用于远程访问设备的调制解调器的tty线路，或者连接到其他设备的控制台端口的tty线路，也可以被网络访问。使用 transport input 或 access-class 配置命令、CoPP 和 CPPr 功能或在设备上对接口应用访问列表，也可以执行其他形式的 vty 和 tty 访问控制。

通过将 AAA（对于验证的设备访问，建议使用此方法）与本地用户数据库搭配使用或使用在 vty 或 tty 线路上直接配置的简单密码身份验证，可执行身份验证。

必须使用exec-timeout命令注销vty或tty线路上闲置的会话。还必须使用service tcp-keepalives-in命令对设备的传入连接启用TCP keepalive。这可确保连接远程端的设备仍然可访问，并且从本地Cisco IOS设备中删除半开放或孤立的连接。

控制 vty 和 tty 线路的传输

将vty和tty配置为仅接受到设备或通过该设备（如果用作控制台服务器）的加密安全远程访问管理连接。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。为防止信息泄露或未经授权访问管理员和设备之间传输的数据，请使用transport input ssh而不是明文协议，如Telnet和rlogin。可以在tty上启用transport input none配置，这会禁止对反向控制台连接使用tty线路。

vty 和 tty 线路都允许管理员连接到其他设备。要限制管理员可用于传出连接的传输类型，请使用 transport output line configuration命令。如果不需要传出连接，则使用transport output none。但是，如果允许传出连接，则使用transport output ssh对连接执行加密且安全的远程访问方法。



注意：如果受支持，可对设备使用 IPSec 执行加密的安全远程访问连接。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IPSec，也必须将SSH作为传输来实施。

警告标志

在某些法律管辖区，除非恶意用户被告知他们无权使用该系统，否则不可能对其进行起诉或对其实施非法监控。提供此通知的一种方法是将此信息放入使用Cisco IOS软件banner login命令配置的标语消息中。

法律通知的要求很复杂，因管辖区和情况而异，并且需要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。与律师合作时，标语可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，对系统的任何使用都可以在不另行通知的情况下进行记录或监控，生成的日志也可在法庭上用作证据。
- 本地法律需要的特定通知。

从安全而非法律角度来看，登录标语不得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

身份验证、授权和记帐(AAA)框架对于保护对网络设备的交互式访问至关重要。AAA框架提供可高度配置的环境，可以根据网络需求进行定制。

TACACS+ 身份验证

TACACS+是Cisco IOS设备可用于针对远程AAA服务器对管理用户进行身份验证的身份验证协议。这些管理用户可以通过SSH、HTTPS、Telnet或HTTP访问Cisco 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。如果您不依赖于单个共享密码，则可提高网络安全性并强化您的责任。

RADIUS 是一种协议，其用途与 TACACS+ 类似；不过，它只能对网络范围内发送的密码加密。相反，TACACS+ 可对整个 TCP 有效负载加密，包括用户名和密码。因此，当AAA服务器支持TACACS+时，请使用TACACS+而不是RADIUS。有关比较这两种协议的详细信息，请参阅比较 TACACS+ 和 RADIUS。

在配置与以下示例类似的思科 IOS 设备上，可启用 TACACS+ 身份验证：

```
!
aaa new-model
```

```
aaa authentication login default group tacacs+
!

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

之前的配置可用作组织特定的AAA身份验证模板的起点。

方法列表是描述要查询以验证用户的身份验证方法的顺序列表。方法列表使您可以指定一个或多个用于身份验证的安全协议，从而在初始方法失败时确保身份验证的备份系统。思科 IOS 软件使用列出的第一种方法成功接受或拒绝用户。只有在早期方法由于服务器不可用或配置错误而失败时，才尝试后续方法。

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。每个选项都有优势。首选使用密码，因为使用单向算法散列密钥，其固有安全性高于线路或本地身份验证的**enable secret**第7类密码所用的加密算法。

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+完全不可用，则每个管理员可以使用其本地用户名和密码。虽然在 TACACS+ 出现故障时，此操作不会加大网络管理员的责任，但会大大增加管理负担，因为必须维护所有网络设备中的本地用户帐户。

此配置示例建立在前面的TACACS+身份验证示例之上，以包括回退身份验证到使用命令本地配置的口**enable secret**令：

```
!

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>
!
```

使用类型 7 口令

最初旨在允许对存储的口令进行快速解密的类型 7 口令并不是一种安全的口令存储形式。有许多工具可以轻松解密这些密码。避免使用第7类密码，除非Cisco IOS设备上正在使用的功能需要。

尽可能使用类型9（加密）：

```
username <username> privilege 15 algorithm-type scrypt secret <secret>
```

可以通过AAA身份验证和使用Enhanced Password Security功能删除此类密码，该功能允许对全局配置命令本地定义的用户使用加密密码**username**。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。

有关删除类型7密码的详细信息，请参阅常规管理平面强化部分。

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。AAA服务器使用其配置的策略允许或拒绝该特定用户的命令。

此配置可以添加到前面的AAA身份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
!
```

TACACS+ 命令记账

配置后，AAA命令记帐会将输入的每个EXEC命令的相关信息发送到已配置的TACACS+服务器。发送到TACACS+服务器的信息包括执行的命令、执行的日期和输入命令的用户名。不支持使用 RADIUS 进行命令记帐。

此示例配置为在权限级别0、1和15输入的EXEC命令启用AAA命令记帐。此配置建立在包括TACACS服务器配置的先前示例的基础上。

```
!

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
!
```

冗余 AAA 服务器

环境中使用的 AAA 服务器支持冗余配置和容错部署。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）。

在设计或实施冗余 AAA 服务器解决方案时，请记住以下注意事项：

- 发生潜在网络故障时AAA服务器的可用性
- AAA 服务器在地理上的分散放置
- 在稳定状态和故障条件下各个 AAA 服务器上的负载
- 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。

增强简单网络管理协议

本部分重点介绍可用于保护Cisco IOS设备中SNMP部署的几种方法。正确保护SNMP以保护网络数据和数据传输所经过的网络设备的机密性、完整性和可用性至关重要。SNMP提供大量有关网络设备运行状况的信息。防止恶意用户利用这些数据对网络进行攻击，从而保护此信息。

SNMP 社区字符串

团体字符串是应用于Cisco IOS设备的密码，用于限制对设备上SNMP数据的只读和读写访问。与所有密码一样，这些社区字符串经过精心选择，以确保它们并非无关紧要。按照网络安全策略定期更改团体字符串。例如，当网络管理员更改角色或离开公司时更改字符串。

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：前面几个社区字符串示例被选择用来清楚地解释这些字符串的使用。对于生产环境，请谨慎选择社区字符串，并在字符串中包含一系列字母、数字和非字母数字符号。

有关此功能的详细信息，请参阅Cisco IOS SNMP命令参考。

SNMP 社区字符串与 ACL

除社区字符串外，应用进一步限制SNMP访问一组选定的源IP地址的ACL。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：这些ACL允许的设备需要正确的社区字符串才能访问请求的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
!
```

有关此功能的更多信息，请参阅“思科 IOS 网络管理命令参考”中的 snmp-server community 。

基础架构 ACL

基础设施ACL(iACL)可以部署以确保只有具有受信任IP地址的终端主机才能将SNMP流量发送到Cisco IOS设备。理想情况下，iACL包含拒绝UDP端口161上未授权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。在适当时，使用视图将SNMP的用户限制为所需数据。

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。SNMPv3 提供安全访问设备的权限，因为它可验证网络中的数据包并可选择性地对其加密。在受支持的情况下，部署SNMP时，可以使用SNMPv3添加另一个安全层。SNMPv3 包括三个主要的配置选项：

- no auth — 此模式不需要对SNMP数据包进行任何身份验证或加密
- auth - 此模式需要验证 SNMP 数据包，而不进行加密
- priv - 此模式既需要验证每个 SNMP 数据包，又需要对其加密（保密）

必须存在授权引擎ID才能使用SNMPv3安全机制（身份验证或身份验证和加密）处理SNMP数据包；默认情况下，该引擎 ID 在本地生成。引擎ID可以使用命令显**show snmp engineID**示，如下例所示：

<#root>

```
router#

show snmp engineID
```

```
   Local SNMP engineID: 800000090300000152BD35496
   Remote Engine ID          IP-addr    Port
```

注意：如果引擎 ID 发生变化，则必须重新配置所有 SNMP 用户帐户。

下一步是配置 SNMPv3 组。此命令使用 SNMP 服务器组 AUTHGROUP 为 SNMPv3 配置思科 IOS 设备，并仅使用 auth 关键字对此组启用身份验证：

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

此命令使用 SNMP 服务器组 PRIVGROUP 为 SNMPv3 配置思科 IOS 设备，并使用 priv 关键字对此组启用身份验证和加密；

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

此命令使用MD5身份验证密码和3DES加密密码配置SNMPv3用**authpassword**户snmpv3user**privpassword**:

```
!

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

请注意**snmp-server user**，配置命令不会按照RFC 3414的要求显示在设备的配置输出中。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**show snmp user**入命令，如以下示例所示：

<#root>

```
router#

show snmp user


User name: snmpv3user
Engine ID: 80000009030000152BD35496
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

Cisco IOS软件中的管理平面保护(MPP)功能可用于帮助保护SNMP，因为它会限制SNMP流量在设备上终止时可以通过的接口。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。

MPP是CPPr功能的子集，需要支持CPPr的Cisco IOS版本。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访问限制为仅访问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

事件日志提供对Cisco IOS设备操作及其部署所在网络的可视性。Cisco IOS软件提供多个灵活的日志配置选项，可帮助实现组织的网络管理和可视性目标。

这些部分提供一些基本的日志功能最佳实践，可帮助管理员成功利用日志功能，同时最大限度地减少对Cisco IOS设备上的日志功能的影响。

将日志发送到中央位置

建议您将日志信息发送到远程系统日志服务器。这样，可更加有效地关联和审查网络设备范围的网络和安全事件。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。因此，网络为管理流量提供的任何保护（例如加密或带外访问）都可以扩展为包括系统日志流量。

此示例配置Cisco IOS设备以将日志信息发送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Cisco IOS路由器系统日志事件识别事件。

Logging to Local Involatile Storage(ATA Disk)功能集成在Cisco IOS 12.4(15)T中，最初在12.0(26)S中引入，使系统日志消息可以保存在高级技术附件(ATA)闪存盘上。重新启动路由器后，ATA 驱动中保存的消息仍会存在。

这些配置行将日志消息的134,217,728字节(128 MB)配置到ATA闪存(disk0)的syslog目录中，指定文件大小为16,384字节：

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

在将日志消息写入ATA磁盘上的文件之前，Cisco IOS软件会检查以确定是否有足够的磁盘空间。否则，将删除最早的日志文件消息（按时间戳），并保存当前文件。文件名的格式为**log_month:day:year::time**PDF。

注意：ATA闪存驱动器磁盘空间有限，因此需要对其进行维护以避免覆盖存储数据的可能性。

本示例展示如何在维护过程中将日志消息从路由器ATA闪存盘复制到FTP服务器192.168.1.129上的外部磁盘：

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

有关此功能的更多信息，请参阅本地非易失性存储（ATA 磁盘）的日志记录。

日志记录级别

Cisco IOS设备生成的每条日志消息都分配了从0级（紧急）到7级（调试）的八个严重性之一。除非特别需要，否则建议您避免使用第7级日志。第7级日志会增加设备上的CPU负载，这可能导致设备和网络不稳定。

全局配置命令**logging trap**级别用于指定将哪些日志消息发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。对于缓冲日志，**logging buffered**使用level命令。

此配置示例将发送到远程系统日志服务器和本地日志缓冲区的日志消息限制为严重性6（信息）至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，可以将日志消息发送到监控会话和控制台，监控会话是发出EXEC命令的交互式管理会话**terminal monitor**。但是，这会增加Cisco IOS设备的CPU负载，因此不建议这样做。相反，将日志信息发送到可通过命令查看的本地日志缓**show logging**冲区。

使用全局配置命**no logging console**令和**no logging monitor**禁用控制台和监控会话的日志。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。

使用缓冲日志

Cisco IOS软件支持使用本地日志缓冲区，因此管理员可以查看本地生成的日志消息。强烈建议使用缓冲日志，而不是将日志记录到控制台或监控器会话。

配置缓冲日志时，有两个相关的配置选项：日志缓冲区大小和存储在缓冲区中的消息严重性。使用全局配置命**logging buffer**令配置的大小。使用**logging buffered size**.log buffered severity命令配置缓冲区中包含的最低严重性。管理员可以通过EXEC命令查看日志缓冲区**show logging**的内容。

此配置示例包括配置16,384字节的日志缓冲区，以及严重性为6, Informational的日志缓冲区，表示存储级别为0（紧急）至6(Informational)的消息：

```
!

logging buffered 16384 6
!
```

有关缓冲日志的详细信息，请参阅Cisco IOS网络管理命令参考。

配置日志记录源接口

为了在收集和审核日志消息时提供更高水平的一致性，建议您静态配置日志记录源接口。这通过interface命令来**logging source-interface**完成。静态配置的日志记录源接口可确保从单个Cisco IOS设备发送的所有日志消息中出现相同的IP地址。为了提高稳定性，请使用环回接口作为日志源。

此配置示例说明如何使用interface全局配置命令指定用于所有日志消息的loopback 0接口的IP地址**logging source-interface**：

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

有关详细信息，请参阅 Cisco IOS 命令参考。

配置日志时间戳

日志时间戳的配置有助于跨网络设备关联事件。必须实施正确且一致的日志时间戳配置，以确保可以关联日志数据。配置日志时间戳，以毫秒精度包含日期和时间，并包括设备上正在使用的时区。

本示例包括在协调世界时(UTC)区域内以毫秒精度配置日志时间戳：

```
!
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软件包含多种功能，可在Cisco IOS设备上启用某种形式的配置管理。这些功能包括存档配置和将配置回滚到先前版本以及创建详细的配置更改日志的功能。

配置替换和配置回滚

在思科 IOS 软件版本 12.3(7)T 和更高版本中，配置替换和配置回滚功能允许您在设备上对思科 IOS 设备配置存档。手动或自动存储后，此存档中的配置可用于用filename命令替换当前运**configure replace**行配置。这与filename命令**copy**对**running-config**比。filename**configure replace**命令取代运行配置，而不是命令执行的合**copy**并。

建议您在网络上的所有Cisco IOS设备上启用此功能。启用后，管理员可以使用命令将当前运行配置添加到存档**archive config EXEC**中。可使用命令查看存档的配**show archive EXEC**置。

本示例说明了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，最多保留14个备份，并在管理员发出该命令时每天存档一次（1440分钟**write memory EXEC**）。

```
!

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

虽然配置存档功能可以存储最多14个备份配置，但建议您在使用命令之前考虑空间要**maximum**求。

以独占方式进行配置更改访问

添加到思科IOS软件版本12.3(14)T中，独占配置更改访问功能可确保仅有一名管理员在指定时间对思科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。此功能通过全局配置命令模式进行配置，**configuration mode exclusive**并在以下两种模式之一中运行：自动或手动

。在自动模式下，配置会在管理员发出命令时自动锁**configure terminal EXEC**定。在手动模式下，管理员在进**configure terminal lock**入配置模式时使用命令锁定配置。

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

在Cisco IOS软件版本12.3(8)T中添加了弹性配置功能，该功能可以安全地存储Cisco IOS设备当前使用的Cisco IOS软件映像和设备配置的副本。启用此功能后，将无法更改或删除这些备份文件。建议您启用此功能以防止在无意中或恶意尝试删除这些文件。

```
!
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。此功能的当前状态可以通过命令显**show secure boot EXEC**示。

数字签名的思科软件

在适用于Cisco 1900、2900和3900系列路由器的Cisco IOS软件版本15.0(1)M中添加了数字签名思科软件功能，该功能使用安全的不对称（公钥）加密技术，便于使用数字签名因而受到信任的Cisco IOS软件。

数字签名的映像可传递其自身的加密（使用私钥）散列值。在检查后，设备使用其密钥存储中的密钥解密关联公钥的散列，并且还会计算其自己的映像散列。如果解密的散列值与计算的映像散列值匹配，则映像没有受损，可以信任。

数字签名的思科软件密钥按密钥类型和版本标识。密钥可以是特殊、生产或滚动类型。生产和特殊密钥类型有一个关联的密钥版本，密钥在撤消和替换时按字母顺序递增。当使用“数字签名的思科软件”功能时，ROMMON 和常规思科 IOS 映像都使用特殊或生产密钥签名。ROMMON 映像可升级，且必须使用与加载的特殊或生产映像相同的密钥签名。

此命令使用设备密钥存储中的密钥验证闪存中映像 c3900-universalk9-mz.SSA 的完整性：

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

另外，思科 Catalyst 4500 E 系列交换机的思科 IOS XE 版本 3.1.0.SG 中也集成了“数字签名的思科软件”功能。

有关此功能的更多信息，请参阅数字签名的思科软件。

在思科 IOS 软件版本 15.1(1)T 及更高版本中，引入了“数字签名的思科软件”的密钥替换功能。密钥替换和撤销从平台密钥存储中替换和删除用于数字签名的思科软件检查的密钥。在密钥泄露的情况下，只能撤消特殊和生产密钥。

用于（特殊或生产）图像的新（特殊或生产）密钥来自（生产或撤销）图像，该图像用于撤销先前的特殊或生产密钥。使用平台中预存储的滚动密钥可验证撤消映像的完整性。滚动密钥不可更改。当您撤销生产密钥时，在加载撤销映像后，它携带的新密钥将添加到密钥存储中，并且关联的旧密钥可以撤销，只要升级ROMMON映像并引导新的生产映像即可。如果撤消特殊密钥，将加载生产映像。此映像将添加新的特殊密钥，并撤消旧的特殊密钥。升级 ROMMON 后，即可启动新的特殊映像。

本示例描述了撤销特殊密钥的操作。这些命令将新的特殊密钥从当前生产映像添加到密钥库，将新的ROMMON映像(C3900_rom-monitor.srec.SSB)复制到存储区域(usbflash0:)，升级ROMMON文件，并撤消旧的特殊密钥：

```
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
```

然后，可将新的特殊映像 (c3900-universalk9-mz.SSB) 复制到要加载的闪存中，并可使用新添加的特殊密钥 (.SSB) 来验证该映像的签名：

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

运行思科 IOS XE 软件的 Catalyst 4500 E 系列交换机不支持密钥撤消和替换，但这些交换机支持“数字签名的思科软件”功能。

有关此功能的更多信息，请参阅数字签名的思科软件指南的数字签名的思科软件密钥撤消和替换部分。

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。日志在Cisco IOS设备上维护，包含更改者的用户信息、输入的配置命令以及更改的时间。此功能通过configuration change logger**logging enable** configuration mode命令启用。可选命令**hidekeys**和**logging size**条目用于改进默认配置，因为它们会阻止密码数据日志并增加更改日志的长度。

建议您启用此功能，以便更容易理解Cisco IOS设备的配置更改历史记录。此外，建议您使用**notify syslog**配置命令在更改配置时生成系统日志消息。

```
!

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**show archive log config all**权EXEC命令查看配置日志。

控制层面

控制层面功能包含协议和进程，用于在网络设备之间进行通信以将数据从源移到目标。这包括路由协议（如边界网关协议）以及ICMP和资源预留协议(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。如果数据平面事件（例如DoS攻击）影响控制平面，则整个网络可能变得不稳定。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

保护网络设备的控制平面至关重要，因为控制平面可确保管理和数据平面得到维护并正常运行。如果控制平面在安全事件期间变得不稳定，则可能无法恢复网络的稳定性。

在许多情况下，您可以禁用接口上某些消息类型的接收和传输，以最大程度减少处理不必要数据包所需的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重定向通常不会超出第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。恶意用户可能会利用路由器发送ICMP重定向的能力，不断向路由器传输数据包，迫使路由器使用ICMP重定向消息做出响应，从而对CPU和路由器性能造成负面影响。要防止路由器传输ICMP重定向，请使用接**no ip redirects**口配置命令。

ICMP 不可达

使用接口访问列表过滤会导致ICMP不可达消息传回已过滤流量的源。生成这些消息会增加设备上的CPU使用率。默认情况下，在Cisco IOS软件中，ICMP不可达生成被限制为每500毫秒生成一个数据包。可使用接口配置命令禁用ICMP不可达消息生**no ip unreachables**成。使用全局配置命令interval-in-ms，可以从默认设置更**ip icmp rate-limit unreachable**改ICMP不可达速率限制。

代理 ARP

代理ARP是一种技术，通过这种技术，一台设备（通常是路由器）可以应答发往另一台设备的ARP请求。通过伪造身份，路由器承担将数据包路由到实际目的地的责任。代理ARP可以帮助子网中的计算机到达远程子网，而无需路由配置或默认网关。RFC 1027 中定义了代理 ARP。

代理ARP的使用也有缺点。它会导致网段中的 ARP 流量增加、资源耗尽及中间人攻击。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。如果攻击者发送大量ARP请求，他们可能会耗尽所有可用内存。

中间人攻击使网络中的主机能够欺骗路由器的MAC地址，从而导致主机无意间将流量传输到攻击者。可使用接口配置命令禁用代理ARP **no ip proxy-arp**.

限制控制平面流量对 CPU 的影响

保护控制层面是至关重要的。由于应用程序性能和最终用户体验可能会因没有数据和管理流量而受到影响，控制平面的生存能力可确保其他两个平面得到维护并可以正常运行。

了解控制平面流量

要正确保护Cisco IOS设备的控制平面，必须了解CPU进行进程交换的流量类型。进程交换流量通常包括两种不同的流量类型。第一种流量类型定向到Cisco IOS设备，必须由Cisco IOS设备CPU直接处理。此类流量包含接收邻接流量类别。此流量包含思科快速转发(CEF)表中的条目，其中下一路由器跳是设备本身，CLI输出中的术语receive**show ip cef**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。

CPU处理的第二种流量类型是数据平面流量 — 目的地超出Cisco IOS设备本身的流量，这需要CPU进行特殊处理。虽然数据平面流量对CPU的影响并不详尽，但这些流量类型是进程交换的，因此可能会影响控制平面操作：

- 访问控制列表日志记录 — ACL日志流量包括由于使用log关键字的ACE的匹配（允许或拒绝）而生成的任何数据包。
- 单播逆向路径转发（单播RPF） — 单播RPF与ACL配合使用，可能导致某些数据包的过程交换。
- IP 选项 - 包含选项的任何 IP 数据包必须由 CPU 处理。
- 分段 — 需要分段的任何IP数据包都必须传递到CPU进行处理。
- 生存时间(TTL)到期 - TTL值小于或等于一个的数据包需要发送互联网控制消息协议超时（ICMP类型11，代码0）消息，这会导致CPU处理。
- ICMP不可达 — 因路由、MTU或过滤而导致ICMP不可达消息的数据包由CPU处理。
- 需要ARP请求的流量 — 不存在ARP条目的目标由CPU处理。
- 非 IP 流量 - 所有非 IP 流量由 CPU 处理。

此列表详细说明了确定Cisco IOS设备CPU处理哪些流量类型的几种方法：

- 命令**show ip cef**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。
- 该命**show interface switching**令提供有关由设备进行进程交换的数据包数量的信息。
- 命令**show ip traffic**提供有关IP数据包数量的信息：
  - 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。发往Cisco IOS设备的所有流都有一个本地目的接口(DstIf)。
- 控制平面策略可用于标识流向Cisco IOS设备控制平面的流量的类型和速率。通过使用精细分类ACL、日志和命令，可以执行控制平面策**show policy-map control-plane**略。

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。本文档的使用基础设施ACL限制对网络的访问部分详细介绍了iACL。

建议您实施 iACL 以保护所有网络设备的控制层面。

接收 ACL

对于分布式平台，Receive ACL(rACL)可以是Cisco IOS软件版本12.0(21)S2(适用于12000(GSR))、12.0(24)S（适用于7500）和12.0(31)S（适用于10720）的选项。rACL可在流量影响路由处理器之前保护设备免受有害流量的影响。rACL仅用于保护配置它的设备，而中转流量不会受到rACL的影响。因此，图中所示示例ACL条目中使用的目标IP地址“any”仅指路由器的物理或虚拟IP地址。rACL还被视为网络安全最佳实践，可视为良好的网络安全性的长期补充。

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，以帮助识别并允许流向设备的合法流量并拒绝所有不必要的数据包。

CoPP

CoPP功能还可用于限制发往基础设施设备的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：从未知或不可信IP地址丢弃的流量可能会阻止具有动态分配IP地址的主机建立与Cisco IOS设备的连接。

```
!

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，将非授权数据包与允许操作匹配的 ACL 条目会导致策略映射丢弃功能丢弃这些数据包，而与拒绝操作匹配的数据包则不受策略映射丢弃功能影响。

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。

控制层面保护

Cisco IOS软件版本12.4(4)T中引入的控制平面保护(CPPr)可用于限制或管制发往Cisco IOS设备CPU的控制平面流量。与CoPP类似，CPPr可以更精细地限制流量。CPPr将汇聚控制平面划分为三个单独的控制平面类别，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：

- 端口过滤功能 — 此功能允许对发送到已关闭或非侦听TCP或UDP端口的数据包进行管制和丢弃。
- 队列阈值功能 — 此功能限制控制平面IP输入队列中允许的指定协议的数据包数量。

有关使用CPPr功能的详细信息，请参阅了解控制平面保护(CPPr)。

硬件速率限制器

Cisco Catalyst 6500系列管理引擎32和管理引擎720支持平台特定的基于硬件的速率限制器(HWRL)，适用于特殊网络场景。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设备免受各种需要CPU处理数据包的攻击。

默认情况下启用多个HWRL。有关HWRL的详细信息，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。因此，连接需求大的任何组织通常都使用 BGP。BGP经常成为攻击者的攻击目标，因为它在小型组织中非常普遍，并且设置并忽略BGP配置的性质。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。

其中概述了最重要的BGP安全功能，并在适当情况下提出了配置建议。

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起始值因操作系统而异，通常范围为64到255。数据包的TTL值达到零时将被丢弃。

基于TTL的安全保护既称为基于TTL的通用安全机制(GTSM)，也称为BGP TTL安全攻击(BTSH)，它利用IP数据包的TTL值来确保收到的BGP数据包来自直接连接的对等体。此功能通常需要来自对等路由器的协调；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。

使用BGP路由器配置命令**ttl-security**的选项启**neighbor**用GTSM for BGP。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，会检查TTL值，该值必须大于或等于255，减去指定的跳数。

使用 MD5 进行 BGP 对等验证

使用 MD5 进行对等验证会针对 BGP 会话中发送的每个数据包创建一份 MD5 摘要。具体而言，IP和TCP报头的部分、TCP负载和密钥用于生成摘要。

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。接收方BGP扬声器使用相同的算法和密钥来重新生成消息摘要。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。

使用BGP路由器配置命令的选项配**password**置了使用MD5**neighbor**的对等身份验证。此命令的使用说明如下：

```
!

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。

配置最大前缀数

BGP 前缀由路由器存储在内存中。路由器必须保存的前缀越多，BGP消耗的内存就越多。在某些配置中，可以存储所有Internet前缀的子集，例如在仅利用默认路由或提供商用户网络路由的配置中。

为防止内存耗尽，请配置每个对等体接受的最大前缀数量。建议为每个 BGP 对等体配置一个限制值。

当您使用BGP路由器配置命**neighbor maximum-prefix**令配置此功能时，需要一个参数：在对等体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。此数字表示最大前缀值相对于日志消息发送时间的百分比。

```
!

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。

使用前缀列表过滤 BGP 前缀

前缀列表允许网络管理员允许或拒绝BGP发送或接收的特定前缀。如果可能，请使用前缀列表确保网络流量通过预定路径发送。将前缀列表应用于入站和出站方向的每个eBGP对等体。

配置的前缀列表将发送或接收的前缀限制为网络路由策略明确允许的前缀。如果由于收到大量前缀而无法执行该操作，请配置前缀列表以专门阻止已知错误前缀。这些已知错误前缀包括未分配的IP地址空间和由RFC 3330为内部或测试目的保留的网络。配置出站前缀列表以专门允许组织要通告的前缀。

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前缀过滤器信息的完整覆盖范围，请参阅使用外部BGP连接到服务提供商。

使用自治系统路径访问列表过滤 BGP 前缀

BGP自主系统(AS)路径访问列表允许用户根据前缀的AS路径属性过滤接收和通告的前缀。这可以与前缀列表结合使用，以建立强大的过滤器集合。

本配置示例使用 AS 路径访问列表将入站前缀限制为那些源自远程 AS 的前缀，并将出站前缀限定为那些源自本地自治系统的前缀。源自所有其他自治系统的前缀将被过滤，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

网络正确转发流量并从拓扑变化或故障中恢复的能力取决于拓扑的准确视图。通常可以运行内部网关协议(IGP)来提供此视图。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还发现可在网络链路发生故障时使用的路由。

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。在路由器之间使用路由协议进行口令验证来帮助确保网络安全。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。

在身份验证过程中添加MD5哈希功能后，路由更新不再包含明文密码，并且路由更新的全部内容更加防篡改。但是，如果使用弱密码，MD5身份验证仍然容易遭受暴力攻击和字典攻击。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介绍其用途。

EIGRP和RIPv2都使用密钥链作为配置的一部分。有关配置和使用“密钥链”的详细信息，请参阅 key。

以下是使用 MD5 的 EIGRP 路由器身份验证的示例配置：

```
!

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路由器身份验证配置示例。RIPv1不支持身份验证。

```
!

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进行OSPF路由器身份验证的示例配置。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

通过使用有助于控制路由信息通告的命令，可以缓解信息泄漏或向IGP引入虚假信息的问passive-interface题。建议您不要将任何信息通告给管理控制范围之外的网络。

此示例演示了此功能的使用：

```
!

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

```
!
```

路由过滤

为了减少在网络上引入虚假路由信息的可能性，请使用路由过滤。与路由器**passive-interface**配置命令不同，一旦启用了路由过滤，接口上就会发生路由，但通告或处理的信息有限。

对于EIGRP和RIP，使用带有**distribute-list**关键字**out**的命令可限制通告的信息，而使用关键字**in**可限制处理的更新。此命**distribute-list**令可用于OSPF，但它不会阻止路由器传播已过滤的路由。相反，可**area filter-list**以使用该命令。

此EIGRP示例使用命令和前缀列**distribute-list**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>
!
```

此OSPF示例使用包含OSPF特定地址的前缀列表 **area filter-list** command:

```
!

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

路由协议前缀由路由器存储在内存中，并且资源消耗会随着路由器必须保留的附加前缀而增加。为防止资源耗尽，请配置路由协议以限制资源消耗。如果使用链路状态数据库超载保护功能，则通过 OSPF 可实现此目标。

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>
!
```

安全第一跳冗余协议

第一跳冗余协议 (FHRP) 为作为默认网关的设备提供弹性和冗余保障。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，这些协议可与未经验证的通信联络。此类通信可使攻击者伪装成符合FHRP标准的设备，以承担网络上的默认网关角色。此接管允许攻击者执行中间人攻击并拦截所有离开网络的用户流量。

为了防止此类攻击，Cisco IOS软件支持的所有FHRP都包含具有MD5或文本字符串的身份验证功能。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

尽管数据平面负责将数据从源移动到目的地，但在安全环境中，数据平面是三个平面中最不重要的平面。因此，当您保护网络设备时，保护管理和控制平面优先于数据平面非常重要。

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。以下部分详细介绍功能和选项，以便您可以更轻松地保护网络。

一般数据层面强化

绝大多数数据平面流量通过网络路由配置确定。但是，使用 IP 网络功能可以修改经过网络的数据包的路径。IP选项（特别是源路由选项）等功能构成了当今网络面临的安全挑战。

使用传输ACL也有助于强化数据平面。

有关详细信息，请参阅使用中转ACL过滤中转流量部分。

IP 选项选择性丢弃

IP 选项造成了两个安全问题。包含IP选项的流量必须由Cisco IOS设备进行进程交换，这会导致CPU负载增加。IP选项还包括更改流量通过网络的路径的功能，此功能可能会使其破坏安全控制。

出于这些考虑，Cisco IOS软件版本12.3(4)T、12.0(22)S和12.2(25)S中添加了全局配置命**ip options {drop | ignore}**令。在此命令的第一种形式中，**ip options drop**包含Cisco IOS设备接收的IP选项的所有IP数据包都会被丢弃。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。

此命令的第二个形式**ip options ignore**将Cisco IOS设备配置为忽略接收数据包中包含的IP选项。虽然这样可以缓解与本地设备的IP选项相关的威胁，但下游设备可能会受到IP选项的影响。因此，强烈建**drop**议使用此命令的形式。如本配置示例所示：

```
!
ip options drop
!
```

某些协议（例如RSVP）合法地使用IP选项。这些协议的功能会受到此命令的影响。

启用IP Options Selective Drop后，该命令可用于确定由于存在IP选项而丢弃的数据包数量**show ip traffic EXEC**。此信息存在于 forced drop 计数器中。

禁用 IP 源路由

IP源路由同时利用松散源路由和记录路由选项；或者使用严格源路由(Strict Source Route)以及Record Route选项，使IP数据报源能够指定数据包采用的网络路径。此功能可用于尝试在网络中的安全控制周围路由流量。

如果IP选项选择性丢弃功能尚未完全禁用IP选项，则必须禁用IP源路由。IP源路由（在所有Cisco IOS软件版本中默认启用）通过全局配置命**no ip source-route**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重定向用于通知网络设备通向IP目标的更好路径。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。

在某些情况下，攻击者可能会使Cisco IOS设备发送许多ICMP重定向消息，这会导致CPU负载增加。因此，建议禁用ICMP重定向传输。ICMP重定向通过接口配置命令禁**no ip redirects**用，如以下示例配置所示：

```
!

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设备将数据包作为第2层广播发送到子网上的所有站点。此定向广播功能已被用作几次攻击（包括smurf攻击）中的放大和反射帮助。

默认情况下，当前版本的Cisco IOS软件已禁用此功能；但是，可以通过接口配置命**ip directed-broadcast**令启用它。默认情况下，12.0之前的Cisco IOS软件版本启用此功能。

如果网络确实需要定向广播功能，请控制其使用。使用ACL作为命令的选项可以实现此功**ip directed-broadcast**能。此配置示例将定向广播限制为源自受信任网络192.168.1.0/24的UDP数据包：

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

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

使用传输 ACL 过滤传输流量

使用中转 ACL (tACL) 可控制通过网络的流量。 这与iACL不同，iACL会设法过滤发往网络本身的流量。当目标是过滤流向特定设备组的流量或流经网络的流量时，tACL提供的过滤器是有益的。

传统上，防火墙执行此过滤器类型。但是，在某些情况下，在网络上的Cisco IOS设备上执行此过滤器会非常有用。例如，必须执行过滤，但不存在防火墙。

tACL也是实施静态反欺骗保护的合适位置。

有关详细信息，请参阅反欺骗保护部分。

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，它传达的消息可能会对TCP和IP协议产生重大影响。工具和使用ICMP来**ping**排**traceroute**除网络故障，以及路径MTU发现。但是，正常的

网络运行很少需要外部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。此示例ACL允许来自受信任网络的ICMP，同时阻止来自其他源的所有ICMP数据包：

```
!

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 IP 分段

如本文档前面的使用基础设施ACL限制对网络的访问部分中所述，对分段IP数据包的过滤可能会对安全设备构成挑战。

由于分段控制的非直观性质，ACL经常会无意中允许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。出于这些原因，IP分段经常用于攻击，并且可以在任何已配置的tACL的顶部显式过滤。列出的ACL示例包括IP分段的综合过滤器。本示例中所示的功能必须与前面示例的功能配合使用：

```
!

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
!
```

有关 ACL 如何处理分段 IP 数据包的更多信息，请参阅访问控制列表和 IP 分段。

过滤IP选项的ACL支持

在Cisco IOS软件版本12.3(4)T及更高版本中，Cisco IOS软件支持使用ACL根据数据包中包含的IP选项过滤IP数据包。数据包中存在IP选项可能表示有人试图破坏网络的安全控制，或者以其他方式改变数据包的中转特征。出于这些原因，建议在网络边缘过滤具有IP选项的数据包。

使用此示例以及前面示例中的内容，为包含IP选项的IP数据包提供完整的过滤器：

```
!

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

许多攻击者都使用源 IP 地址欺骗进行有效攻击或隐瞒真正的攻击源，并阻碍准确进行追踪。Cisco IOS 软件提供单播 RPF 和 IP 源防护 (IPSG) 以阻止那些依靠源 IP 地址欺骗的攻击。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。

IPSG通过交换机端口、MAC地址和源地址验证的性能，在直接管理控制下最大限度地减少网络欺骗。单播RPF提供源网络验证，可以减少未受直接管理控制的网络的欺骗攻击。端口安全可用于验证接入层的MAC地址。动态地址解析协议 (ARP) 检查 (DAI) 可减少在本地网段中使用 ARP 下毒的攻击矢量。

单播 RPF

单播RPF使设备能够验证转发数据包的源地址是否可以通过接收该数据包的接口到达。不要依赖单播RPF作为防止欺骗的唯一保护。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 需要您在每个设备上启用思科快速转发，并在每个接口上配置思科快速转发。

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。在配置接口配置命**ip verify**令期间，关键字**any**配置松散模式，而关键字rx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)，拒绝来自IP源绑定表中未关联的IP地址的任何流量。

IP源防护可应用于属于启用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
!
```

可以使用接口配置命令启**Tip verify source port security**用端口安全。这还需要全局配置**ip dhcp snooping information option**;命令，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

端口安全用于缓解接入接口的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 MAC 违规，可以使用四种违规模式之一。这些模式包括：保护、限制、关闭和关闭VLAN。在某些情况下，如果一个端口仅为使用标准协议的单个工作站提供访问，最大值设置为 1 即足够。当最大数量设置为1时，利用虚拟MAC地址（例如HSRP）的协议不起作用。

```
!

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>
!
```

有关端口安全配置的更多信息，请参阅配置端口安全。

动态 ARP 检查

动态ARP检测(DAI)可用于缓解对本地网段的ARP毒化攻击。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。此信息旨在破坏其他设备的 ARP 缓存。攻击者通常使用ARP毒化来执行中间人攻击。

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 环境下，DAI 使用 DHCP 监听功能生成的数据。在受信任接口上接收的ARP数据包不会经过验证，并且会丢弃不受信任接口上的无效数据包。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，需要使用ARP ACL来启用DAI。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>
!
```

DAI还可以基于每个接口启用，无论支持哪个接口。

```
ip arp inspection limit rate <rate_value> burst interval <interval_value>
```

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

对于使用已知未用和不受信任地址空间的攻击，手动配置的 ACL 可提供静态反欺骗保护。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。反欺骗ACL需要定期监控间隔，因为它们可能频繁更改。如果应用出站 ACL 限制传至有效本地地址的流量，可尽可能地减少来自本地网络的流量中的欺骗。

本示例演示如何使用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。如果配置这些ACL类型，请查找最终确定的最新参考。

```
!

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。有关如何过滤未使用地址的其他信息，请参阅Bogon Reference 页。

限制数据平面流量对 CPU 的影响

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。保护数据平面（包括流经网络设备的流量），以确保管理和控制平面的运行。如果中转流量可能导致设备处理交换机流量，则设备的控制平面可能会受到影响，从而导致运营中断。

影响 CPU 的功能和数据流类型

尽管并不详尽，但此列表包含需要特殊CPU处理且由CPU进行进程交换的数据平面流量类型：

- ACL日志记录 — ACL日志流量包括因使用日志关键字的ACE的匹配（允许或拒绝）而生成的任何数据包。
- 单播RPF — 与ACL一起使用的单播RPF可能导致某些数据包的过程交换。
- IP 选项 - 包含选项的任何 IP 数据包必须由 CPU 处理。
- 分段 - 需要分段的任何 IP 数据包必须传递到 CPU 进行处理。
- 存活时间 (TTL) 到期 - TTL 值低于或等于 1 的数据包需要发送互联网控制消息协议超时（ICMP 类型 11，代码 0）消息，从而交由 CPU 进行处理。
- ICMP不可达 — 因路由、MTU或过滤而导致ICMP不可达消息的数据包由CPU处理。
- 需要ARP请求的流量 — 不存在ARP条目的目标由CPU处理。
- 非 IP 流量 - 所有非 IP 流量由 CPU 处理。

有关数据平面强化的详细信息，请参阅一般数据平面强化部分。

基于 TTL 值过滤

您可以使用Cisco IOS软件版本12.4(2)T中引入的ACL Support for Filtering on TTL Value功能在扩展IP访问列表中根据TTL值过滤数据包。此功能可以保护接收TTL值为0或1的中转流量的设备。还可以使用基于TTL值的数据包过滤来确保TTL值不低于网络的直径，这样可以保护下游基础设施设备的控制平面免受TTL到期攻击。

某些应用程序和工具，例如**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
!
```

有关如何根据TTL值过滤数据包的详细信息，请参阅TTL到期攻击识别和缓解。

有关此功能的详细信息，请参阅对按 TTL 值过滤的 ACL 支持。

在思科 IOS 软件版本 12.4(4)T 及更高版本中，灵活数据包匹配 (FPM) 功能允许管理员基于数据包的任意位进行匹配。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
!
```

基于是否存在 IP 选项过滤

在 Cisco IOS 软件版本 12.3(4)T 及更高版本中，您可以在已命名的扩展 IP 访问列表中使用“对过滤 IP 选项的 ACL 支持”功能，以过滤具有 IP 选项的 IP 数据包。还可以使用基于IP选项的IP数据包过

滤来防止基础架构设备的控制平面需要在CPU级别处理这些数据包。

过滤IP选项的ACL支持功能只能用于命名扩展ACL。RSVP、多协议标签交换流量工程、IGMP版本2和3以及使用IP选项数据包的其他协议，如果丢弃这些协议的数据包，则无法正常工作。如果网络上正在使用这些协议，则可以使用ACL Support for Filtering IP Options。但是，ACL IP选项选择性丢弃功能可以丢弃此流量，并且这些协议无法正常工作。如果目前未使用需要 IP 选项的协议，则首选“ACL IP 选项选择性丢弃”功能来丢弃这些数据包。

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平面强化部分。

请参阅中转访问控制列表：在Your Edge上过滤，了解有关如何过滤中转和边缘流量的详细信息。

Cisco IOS软件中可用于使用IP选项过滤数据包的另一个功能是CoPP。在思科 IOS 软件版本 12.3(4)T 和更高版本中，CoPP 允许管理员过滤控制平面数据包的流量。支持Cisco IOS软件版本12.3(4)T中引入的过滤IP选项的CoPP和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
!
```

在之前的CoPP策略中，将数据包与permit操作匹配的访问控制列表条目(ACE)导致这些数据包被策略映射丢弃功能丢弃，而与deny操作（未显示）匹配的数据包不受策略映射丢弃功能的影响。

控制层面保护

在Cisco IOS软件版本12.4(4)T及更高版本中，控制平面保护(CPPr)可用于通过Cisco IOS设备的CPU限制或管制控制平面流量。虽然与CoPP类似，但CPPr可以限制或管制比CoPP更精细的流量。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
!
```

在前一个CPPr策略中，将数据包与permit操作结果匹配的访问控制列表条目是，这些数据包被policy-map drop功能丢弃，而与deny操作（未显示）匹配的数据包则不受策略映射丢弃功能的影响。

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是使用Cisco IOS软件实现此目标的两种主要方法。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通过跟踪网络流量来识别与安全相关的异常网络活动。NetFlow数据可以通过CLI查看和分析，也可以导出到商业或免费的NetFlow收集器进行聚合和分析。NetFlow收集器可通过长期趋势提

供网络行为和使用分析。NetFlow对IP数据包中的特定属性进行分析，并创建流。第5版是最常用的NetFlow版本；但是，第9版具有更高的可扩展性。利用在大容量环境下采样的流量数据，可创建Netflow 流。

CEF 或分布式 CEF 是启用 NetFlow 的先决条件。NetFlow 可以配置在路由器和交换机上。

本示例说明NetFlow的基本配置。在Cisco IOS软件的先前版本中，在接口上启用NetFlow的命令是**ip route-cache flow**而不是 **ip flow {ingress | egress}**.

```
!

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。将流量更精细地分类到特定ACE有助于提供网络流量的可视性，因为每个流量类别都有自己的命中计数器。管理员还可以将ACL末尾的隐式deny分隔为精细ACE，以帮助识别被拒绝的流量类型。

管理员可以通过使用分类ACL和EXEC命令来加**show access-list**快事**clear ip access-list counters**件响应。

此示例显示分类ACL的配置，用于在默认拒绝之前识别SMB流量：

```
!

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
!
```

要识别使用分类ACL的流量，请使用命**show access-list EXEC**令。可以使用命令清除ACL计数**clear ip access-list counters EXEC**器。

```
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。

这些部分概述了VACL和PACL的功能、优势和潜在的使用场景。

使用 VLAN 映射进行访问控制

VACL或应用于所有进入VLAN的数据包的VLAN映射能够对VLAN内流量实施访问控制。此功能不适用于路由接口上的 ACL。例如，VLAN映射可用于防止同一个VLAN中包含的主机相互通信，从而减少本地攻击者或蠕虫利用同一网段上的主机的机会。要拒绝数据包使用VLAN映射，请创建匹配流量的访问控制列表(ACL)，并在VLAN映射中将操作设置为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，它们不支持日志或IPv6 ACL。

本示例使用扩展的命名访问列表来说明此功能的配置：

```
!

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>
!
```

本示例演示使用VLAN映射拒绝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。创建 PACL 的优先权高于 VLAN 映射和路由器 ACL，其语法与路由器 ACL 相同。如果某个 ACL 应用于第 2 层接口，则它会被称为 PACL。配置包含创建 IPv4、IPv6 或 MAC ACL，并将它们应用到第 2 层接口。

此示例使用扩展命名访问列表来说明此功能的配置：

```
!

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

MAC访问控制列表或扩展列表可以在IP网络上应用，在接口配置模式下使用此命令：

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

注意：MAC访问控制列表用于将第3层数据包分类为第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。

此接口命令必须应用于入口接口，并指示转发引擎不检查IP报头。结果是，您可以在IP环境中使用MAC访问列表。

专用 VLAN 使用

专用VLAN(PVLAN)是第2层安全功能，它限制了VLAN上工作站或服务器之间的连接。没有PVLAN，第 2 层 VLAN 中的所有设备均可自由通信。存在因单个VLAN上设备之间的通信限制而有助于安全性的网络情况。例如，PVLAN通常用于禁止公共可访问子网上的服务器之间的通信。如果一台服务器受损，由于PVLAN的应用导致无法连接到其他服务器，则可能有助于限制对一台服务器的危害。

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会完全阻止辅助VLAN上的设备之间的通信。每个主要VLAN只能有一个隔离VLAN，并且只有混杂端口可以与隔离VLAN上的端口通信。隔离 VLAN 可用于不受信任的网络（如支持访客的网络）。

此配置示例将VLAN 11配置为隔离VLAN，并将其与主VLAN VLAN 20关联。此示例还将接口

FastEthernet 1/1配置为VLAN 11上的隔离端口：

```
!

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成员之间以及与主要VLAN上的任意混杂端口进行通信。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。必须将社区VLAN用于对需要彼此连接，但不要求连接到VLAN上所有其他设备的服务器进行分组。这种情况常见于公开访问的网络或服务器向不受信任的客户端提供内容的任何位置。

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

置于主VLAN中的交换机端口称为混杂端口。混杂端口可以与主要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
!
```

实施PVLAN时，必须确保现有的第3层配置支持PVLAN施加的限制，并且不允许颠覆PVLAN配置。带有路由器ACL或防火墙的第3层过滤器可以防止PVLAN配置被破坏。

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广泛概述。如果您保护设备，将会提高您管理的网络的整体安全性。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

本文档中介绍的一些功能由思科信息开发团队编写。

附录：思科 IOS 设备强化清单

本核对表是本指南中介绍的加固设备的所有步骤的集合。管理员可使用它来提醒您思科 IOS 设备使用和考虑的所有强化功能，即使某项功能由于未应用而没有实施亦不例外。建议管理员在实施选项之前，评估每个选项的潜在风险。

管理平面

- 密码
  - 为 enable 和 local 用户密码启用 MD5 散列（secret 选项）
  - 配置密码重试锁定
  - 禁用密码恢复（考虑风险）
- 禁用未使用的服务
- 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
  - 保留内存以用于控制台访问
  - 内存泄漏探测器
  - 缓冲区溢出检测
  - 改进的 Crashinfor 收集
- 使用 iACL 限制管理访问
- 过滤（考虑风险）
  - ICMP 数据包
  - IP 片段
  - IP 选项
  - 数据包中的 TTL 值
- 控制层面保护
  - 配置端口过滤
  - 配置队列阈值
- 管理访问
  - 使用管理平面保护限制管理接口
  - 设置 exec 超时
  - 针对 CLI 访问使用加密的传输协议（例如 SSH）

    - 控制 vty 和 tty 线路的传输（访问级别选项）
    - 使用横幅发出警告
- AAA
    - 使用 AAA 进行身份验证和回退
    - 使用 AAA (TACACS+) 进行命令授权
    - 将AAA用于帐户用途
    - 使用冗余 AAA 服务器
- SNMP
    - 配置 SNMPv2 社区并应用 ACL
    - 配置 SNMPv3
- 日志记录
    - 配置集中日志
    - 设置所有相关组件的日志级别
    - Set log source-interface
    - 配置日志时间戳粒度
- 配置管理
    - 替换和回滚
    - 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（考虑风险）
    - ICMP 重定向
    - ICMP 不可达
    - 代理 ARP
- 如果要使用NTP，请配置NTP身份验证
- 配置控制平面策略/保护（端口过滤器、队列阈值）
- 安全路由协议
    - BGP（TTL、MD5、最大前缀数、前缀列表、系统路径 ACL）
    - IGP（MD5、被动接口、路由过滤器、资源消耗）
- 配置硬件速率限制器
- 安全第一跳冗余协议（GLBP、HSRP、VRRP）

数据层面

- 配置 IP 选项选择性丢弃
- 禁用（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 tACL（考虑风险）
    - 过滤 ICMP
    - 过滤 IP 分段
    - 过滤 IP 选项
    - 过滤 TTL 值
- 配置所需的反欺骗保护
    - ACL
    - IP 源防护
    - 动态 ARP 检查
    - 单播 RPF
    - 端口安全性
- 控制平面保护（控制平面 CEF 异常）
- 配置 NetFlow 和分类 ACL 以标识流量
- 配置所需的访问控制 ACL（VLAN 映射、PACL、MAC）
- 配置专用 VLAN

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。