硬化Cisco IOS设备的Cisco指南

目录

简介
先决条件
要求
使用的组件
背景信息
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
集中处理日志收集和监视
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
利用基础设施 ACL 限制网络访问
ICMP 数据包过滤
过滤 IP 分段
对过滤 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
使用缓冲的日志记录
配置日志记录源接口
配置日志记录时间戳
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
对过滤 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

本文档介绍有助于保护Cisco IOS®系统设备的信息，从而提高网络的整体安全性。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。

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。

背景信息

网络的三个功能平面为管理平面、控制层面和数据层面，每一个平面都提供了需要保护的不同功能。

- **管理平面 - 管理平面管理发送到思科 IOS 设备的流量，由安全外壳 (SSH) 和简单网络管理协议 (SNMP) 等应用和协议组成。**
- **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)。
- **数据平面 - 数据平面通过网络设备转发数据。**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。

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。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

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。

集中处理日志收集和监视

要了解与安全事件相关的现有、新型和历史事件，您的组织必须采取统一的事件日志记录和关联策略。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。

*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

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。

有关此功能的更多信息，请参阅本文档的流量识别和回溯部分及 http://www.cisco.com/go/netflow（仅限注册客户）。

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。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。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。您必须确保设备管理平面和控制平面的安全，因为控制平面的运行会直接影响管理平面的运行。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
- 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。但是请注意，如果 TACACS+ 或 RADIUS 服务出现故障，仍需要本地配置的密码才能进行特权访问。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。但是，**service password-encryption 命令使用的算法是简单的 Vigenre 加密。**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 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

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

!
```

思科 IOS 软件提供密码恢复过程，需要在系统启动期间使用 Break 键访问 ROM 监控模式 (ROMMON)。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。

*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

作为一项安全最佳实践，必须禁用任何不必要的服务。这些不需要的服务，特别是使用用户数据报

协议(UDP)的服务，不常用于合法目的，但可用于发起DoS和其他攻击，否则这些攻击会被数据包过滤阻止。

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。**
- 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，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。

- 对于支持从sdflash启动的交换机，可通过从闪存启动和使用“no sdflash”配置命令禁用sdflash来增强安全性。

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，会话在十分钟不活动后断开。

```
!

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。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，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。此功能通过两种方法完成此任务：“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。当设备出现故障时，思科 IOS 软件版本 12.3(11)T 中添加的此功能允许设备回收空间来创建新的 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 时区 - 在配置 NTP 时需要配置时区，以便准确关联时间戳。**对于网络中全局使用的设备，通常可通过两种方法为其配置时区。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。**

使用 NTP 身份验证的配置示例：

客户端：

```
(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：

```
(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客户环境中的使用方式。思科区分了这些使用案例：

- 不使用智能安装功能的客户。
- 仅将智能安装功能用于零接触部署的客户。
- 利用智能安装功能进行非接触部署（配置和映像管理）的客户。

以下各节详细描述了每个场景：

- 不使用智能安装功能的客户。
- 如果客户不使用思科智能安装功能，并在可用命令的情况下运行Cisco IOS和Cisco IOS XE软件版本，则应使用no vstack命令禁用智能安装功能。

  注意：Cisco IOS 12.2(55)SE03版中引入了**vstack**命令。

以下是禁用智能安装客户端功能的Cisco Catalyst交换机上**show vstack**命令的输出示例：

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

仅将智能安装功能用于零接触部署的客户

在零接触安装完成后禁用智能安装客户端功能，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手动输入**no vstack**命令，或使用脚本输入此命令。
- 将**no vstack**命令作为Cisco IOS配置的一部分添加，该配置作为零接触安装的一部分推送到每个智能安装客户端。
- 在不支持**vstack**命令(Cisco IOS版本12.2(55)SE02及更早版本)的版本中，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。

要稍后启用智能安装客户端功能，请在所有客户端交换机上手动或使用脚本输入**vstack**命令。

利用智能安装功能进行非零接触部署的客户

在智能安装架构的设计中，应小心谨慎，以免不受信任方无法访问基础设施IP地址空间。在不支持**vstack**命令的版本中，请确保只有智能安装指挥交换机与端口4786上的所有智能安装客户端具有TCP连接。

管理员可以在受影响的设备上使用以下思科智能安装部署安全最佳实践：

- 接口ACL
- 控制平面策略(CoPP)。 此功能并非在所有Cisco IOS软件版本中都可用。

本示例显示一个接口ACL，其智能安装指挥交换机IP地址为10.10.10.1，智能安装客户端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上的所有IP接口上。在首次部署交换机时，也可以通过指挥交换机推送。

为了进一步限制对基础设施内所有客户端的访问，管理员可以在网络中的其他设备上使用以下安全最佳实践：

- 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

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。

构建和应用 iACL 是为了指定需要允许从主机或网络到网络设备的连接。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。**

思科 IOS 软件提供了相关功能，以便专门按名称或类型和代码来过滤 ICMP 消息。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

分段 IP 数据包的过滤过程可能对安全设备构成挑战。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。思科 IOS 软件使用特定方法来根据配置的访问列表检查非初始分段。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
!
```

*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。

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
!
```

对基于 TTL 值过滤的 ACL 支持

思科 IOS 软件版本 12.4(2)T 中添加了对基于存活时间 (TTL) 值过滤 IP 数据包的 ACL 支持。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。为了生成 ICMP 超时消息并将其发送到数据包源，需要设备的 TTL 递减到零，由此丢弃数据包。

生成和传输这些消息属于异常处理。如果到期的 IP 数据包数量不多，则路由器可执行此功能；但如果到期的 IP 数据包数量很大，则生成和传输这些消息可能会耗尽所有可用的 CPU 资源。这提供了一个 DoS 攻击矢量。因此，需要针对利用大量到期 IP 数据包的 DoS 攻击强化设备。

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**：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。

安全交互式管理会话

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。为了防止信息泄露和非授权访问，非常有必要确保管理会话的安全。

管理平面保护

在思科 IOS 软件版本 12.4(6)T 和更高版本中，管理员可借助管理平面保护 (MPP) 功能来限制设备接收管理流量的接口。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。

本示例显示了如何启用 MPP，以便仅允许在千兆以太网 0/1 接口上使用 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。

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：

- **端口过滤功能 - 此功能用于管制或丢弃传输至封闭或非侦听 TCP 和 UDP 端口的数据包。**
- **队列阀值策略功能 - 此功能用于限制控制平面 IP 输入队列中允许的指定协议数据包数量。**

CPPr 允许管理员使用主机子接口分类、监控和限制发送到设备的管理流量。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，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

由于在交互式管理会话中可能会泄露信息，所以必须对这些流量加密，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不安全且未标准化，因此如果SSHv2是选项，则不建议使用它。

思科 IOS 软件还支持安全复制协议 (SCP)，该协议支持加密的安全连接，以便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
!
```

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

思科 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支持是在早期版本的Cisco IOS软件中实施的。）SSH在可靠传输层之上运行，并提供强大的身份验证和加密功能。TCP 是为 SSH 定义的唯一可靠的传输。SSH 提供在网络中的另一台计算机或设备上安全访问和执行命令的方法。安全复制协议 (SCP) 功能通过 SSH 运行，允许安全地传输文件。

如果**未显**式配置ip ssh verson 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被视为不安全，可能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一个私钥/公钥对，并在思科 IOS SSH 服务器上配置一个公钥，才能完成身份验证。

由尝试建立凭证的 SSH 用户使用私钥提供加密的签名。系统将签名和该用户的公钥发送到 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。使用散列值是为了确定服务器是否包含匹配的条目。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。如果客户端上启用了严查主机密钥的标志，则客户端将检查其中是否包含与服务器预配置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。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，以防止非授权访问。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；使用 show line EXEC 命令可确定可用的线路数。如果所有 vty 线路都在使用中，则无法建立新管理会话，这时将为设备访问创建一个 DoS 条件。

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。连接到调制解调器用于远程访问设备的 tty 线路或连接到其他设备控制台端口的 tty 线路，也可通过网络访问。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 线路上处于空闲状态的会话。**另外，也必须使用 **service tcp-keepalives-in 命令才能对设备的传入连接启用 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 IOS 设备上删除。

控制 vty 和 tty 线路的传输

要仅接受传至设备或通过设备（如果用作控制台服务器）的加密的安全远程访问管理连接，则应配置 vty 和 tty。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。**在 tty 上可启用 **transport input none 配置，该配置实际上会禁止将 tty 线路用于反向控制台连接。**

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：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，即使使用了 IPSec，也仍然必须执行 SSH 作为传输协议。

警告标志

在某些法律管辖区，无法检举和非法监控恶意用户，除非他们已被通知不得使用该系统。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

要确保对设备执行安全交互式访问，身份验证、授权和记帐 (AAA) 框架至关重要。AAA 框架提供了一种可高度配置的环境，环境配置可根据网络需求量身定制。

TACACS+ 身份验证

TACACS+ 是一种身份验证协议，思科 IOS 设备借此可根据远程 AAA 服务器验证管理用户。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。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，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。

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>
!
```

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。

方法列表是描述要查询的身份验证方法（用于验证用户身份）的顺序列表。通过方法列表，您可以指定一种或多种用于身份验证的安全协议，以确保在初始方法失败时可通过备用系统进行身份验证。思科 IOS 软件使用列出的第一种方法成功接受或拒绝用户。而对于后续方法，仅在前面的方法因服务器不可用或配置错误而失败的情况下才会尝试使用。

*有关配置指定方法列表的更多信息，请参阅*指定的身份验证方法列表。

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。首选使用 enable secret，因为 secret 是使用单向算法的散列值，从本质上比 line 或 local 身份验证的类型 7 密码所用的加密算法更加安全。

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。

此配置示例建立在先前的 TACACS+ 验证示例基础之上，以便为使用 **enable secret 命令本地配置的密码包含回退验证：**

```
!

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

类型 7 密码最初的设计目的是支持快速解密存储的密码，而不是安全的密码存储形式。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。

应尽可能使用第9类(scrypt):

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

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。

有关删除类型 7 密码的更多信息，请参阅本文档的一般管理平面强化部分。

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。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。发送至 TACACS+ 服务器的信息包括执行的命令、执行日期以及输入命令的用户的用户名。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中输入的EXEC命令启用AAA命令记帐。此配置基于包括TACACS服务器配置的先前示例。

```
!

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
!
```

有关 AAA 记帐配置的更多信息，请参阅配置记帐。

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）。

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：

- 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

- 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

本部分重点介绍几种可用于保护 IOS 设备内的 SNMP 部署的方法。正确保护 SNMP 非常重要，这样才能确保网络数据和传输这些数据的网络设备的机密性、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。这些信息应严加保护，以防恶意用户利用这些数据对网络进行攻击。

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：**为了清晰地说明如何使用这些字符串，我们选择的是前面的社区字符串。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：**这些 ACL 所允许的设备需要提供正确的社区字符串，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

为了确保只有使用受信任 IP 地址的终端主机才能向 IOS 设备发送 SNMP 流量，可以部署基础设施 ACL (iACL)。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。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。如果受支持，在部署 SNMP 时可以使用 SNMPv3 来增强安全性。SNMPv3 包括三个主要的配置选项：

- **no auth - 此模式不需要任何身份验证，亦无需对 SNMP 数据包进行任何加密**
- **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）**

只有存在授权引擎 ID，才能使用 SNMPv3 安全机制（身份验证或身份验证和加密）来处理 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: 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 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: 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

使用思科 IOS 软件中的管理平面保护 (MPP) 功能，可帮助保护 SNMP，因为该功能可限制 SNMP 流量在设备上终止的接口。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。

请注意，MPP 是 CPPr 功能的子集，并要求使用支持 CPPr 的 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，应扩展网络为管理流量提供的任何保护（例如加密或带外访问），以便将系统日志流量纳入进来。

此配置示例中配置了思科 IOS 设备，以便向远程系统日志服务器发送日志记录信息：

```
!
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。

本地非易失性存储（ATA 磁盘）的日志记录功能最早在 12.0(26)S 中引入，现集成在 12.4(15)T 中，支持在先进技术附件 (ATA) 闪存盘中保存系统日志记录消息。重新启动路由器后，ATA 驱动中保存的消息仍会存在。

这些配置行可向 ATA 闪存 (disk0) 的系统日志目录配置 134,217,728 个字节 (128 MB) 的日志记录消息，指定 16,384 个字节的文件大小：

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

在将日志记录消息写入到 ATA 磁盘中的文件之前，思科 IOS 软件会检查是否有充足的磁盘空间。否则，将删除最早的日志记录消息文件（按时间戳），而保留当前的文件。文件名格式**为 log_month:day:year::time**。

> **注意：**ATA 闪存盘的磁盘空间有限，因此需要加以维护以免覆盖原已存储的数据。

本示例显示了在维护过程中，如何将日志记录消息从路由器 ATA 闪存盘复制到 FTP 服务器 192.168.1.129 中的外部磁盘：

```
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。

使用全局配置命令 **logging trap level 可指定要发送至远程系统日志服务器的日志记录消息。**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

使用思科 IOS 软件，可以将日志消息发送到监视会话（监视会话是已发出 EXEC 命令 **terminal monitor 的交互式管理会话）和控制台。**但是，这样会增加 IOS 设备的 CPU 负载，所以建议不要执行此操作。相反，建议您将日志记录信息发送到本地日志缓冲区，使用 **show logging 命令可查看它们。**

要禁止日志记录传送至控制台和监视会话，请使用全局配置命令 **no logging console 和 no logging monitor。**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。缓冲区中包括的最低严重性级别使用 logging buffered severity 命令来配置。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 个字节的日志记录缓冲区配置，以及严重性级别 6“信息性”，表示存储的是级别 0（紧急）至级别 6（信息性）的消息：

```
!

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

为了提高收集和审查日志消息时的一致性，建议您静态配置一个日志记录源接口。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。

此配置示例描述了如何使用 **logging source-interface 接口全局配置命令，指定用于所有日志消息的环回接口 0 的 IP 地址：**

```
!
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。使用 **configure replace filename 命令，可将当前运行的配置替换为此存档中手动或自动存储的配置。**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，管理员可使用 **archive config 特权 EXEC 命令将当前运行的配置加入存档中。**使用 **show archive EXEC 命令可查看存档的配置。**

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
!
```

虽然配置存档功能最多可存储 14 个备份配置，但建议您在使用 **maximum 命令前考虑空间需求。**

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。使用全局配置命令 **configuration mode exclusive 模式可配置此功能，它可在两种模式中的任一模式下运行：**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。**在手动模式下，管理员可在进入配置模式时使用 **configure terminal lock 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

使用思科 IOS 软件版本 12.3(8)T 中添加的弹性配置功能，可安全地存储思科 IOS 设备当前所用的思科 IOS 软件映像和设备配置副本。启用此功能后，将无法更改或删除这些备份文件。建议您启用此功能来防止无意和恶意地尝试删除这些文件。

```
!
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。使用 **show secure boot EXEC 命令可显示此功能的当前运行状态。**

数字签名的思科软件

思科 1900、2900 和 3900 系列路由器的思科 IOS 软件版本 15.0(1)M 中添加的“数字签名的思科软件”功能，有助于使用数字签名和受信任的思科 IOS 软件及安全不对称的（公钥）加密算法。

数字签名的映像可传递其自身的加密（使用私钥）散列值。在检查时，设备使用其密钥存储中所含密钥的对应公钥解密散列值，同时计算其自身映像的散列值。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关联的密钥版本，在撤消和替换密钥时，版本将按字母顺序递增。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”可替换和删除平台密钥存储中用于“数字签名的思科软件”校验的密钥。在密钥泄露的情况下，只能撤消特殊和生产密钥。

为了撤消先前的特殊或 生产密钥，所用的映像（生产或撤消）中加入了一种用于（特殊或生产）映像的新（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。如果调用生产密钥，在加载撤消映像后，它所承载的新密钥将加入密钥存储；只要升级 ROMMON 映像并启动新生产映像，即可撤消对应的旧密钥。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。这些命令会向当前生产映像的密钥存储中添加新的特殊密钥，复制新 ROMMON 映像 (C3900_rom-monitor.srec.SSB) 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。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。使用 **logging enable 配置更改记录器配置模式命令可启用此功能。**由于默认配置会防止记录密码数据，要改善默认配置并增加更改日志的长度，可使用可选命令

hidekeys 和 logging size 条目。

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，建议您在更改配置时使用 **notify syslog 配置命令来生成系统日志消息。**

```
!

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，可以使用特权 EXEC 命令 **show archive log config all 查看配置日志。**

控制层面

控制平面功能包括网络设备之间通信的协议和进程，以便数据在源与目的地之间移动。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，您可以禁止接口接收和传输特定类型的消息，以尽可能地减少处理不必要的数据包所需的 CPU 负载量。

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。恶意用户可能会利用路由器的功能，通过向路由器连续发送数据包来发送 ICMP 重定向消息，这样会强制路由器响应 ICMP 重定向消息，并会对 CPU 和路由器性能造成不利影响。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。生成这些消息可能会增加设备中的 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。使用接口配置命令 **no ip unreachables** 可禁用生成 ICMP 不可达消息。使用全局配置命令 ip icmp rate-limit unreachable interval-in-ms 可更改默认的 ICMP 不可达消息速率限制。

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。

使用代理 ARP 利用率有几项不足。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，就可能耗尽所有可用的内存。

中间人攻击使网络中的主机能够伪装路由器的 MAC 地址，从而导致受信主机向攻击者发送流量。使用接口配置命令 **no ip proxy-arp** 可禁用代理 ARP。

*有关此功能的详细信息，请参阅*启用代理 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。

了解控制平面流量

为了正确保护Cisco IOS设备的控制平面，必须了解CPU交换的流量类型。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。此流量包含“接收邻*接流量*”类别。此流量包含Cisco快速转发(CEF)表中的一个条目，其中下一路由器跳是设备本身，该条目由show ip cef CLI输出中的**接收**术语表示。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 处理的第二种流量是数据平面流量，即目的地并非思科 IOS 设备本身的流量，该类流量需要 CPU 进行特殊处理。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：

- **访问控制列表日志记录 - ACL 日志记录流量包括因使用日志关键字的 ACE 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 一起使用，可能导致某些数据包的处理交换。**
- **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 值小于或等于 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 或过滤导致生成 ICMP 不可达信息的数据包，由 CPU 处理。**
- **需要 ARP 请求的流量 - 不存在 ARP 条目的目的地需由 CPU 处理。**
- **非 IP 流量 - 所有非 IP 流量由 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。
- **show interface switching 命令提供有关设备进行处理交换的数据包数量的信息。**
- **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。本文档的使用基础设施 ACL 限制网络访问部分详细介绍了基础架构 ACL。

建议您实施 iACL，以便保护所有网络设备的控制平面。

接收 ACL

对于分布式平台，接收ACL(rACL)是Cisco IOS软件版本12.0(21)S2的选项，12000(GSR)、7500的12.0(24)S和10720 R的12.0(31)S。ACL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。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。

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**：丢弃来自未知或不受信任 IP 地址的流量可能会阻止采用动态分配的 IP 地址的主机连接到思科 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，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。

*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：

- **端口过滤功能 - 此功能可管制和丢弃发送到封闭或非侦听 TCP 或 UDP 端口的数据包。**
- **队列阈值功能 - 此功能可限制控制平面 IP 输入队列中允许的指定协议数据包数。**

*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。因此，连接需求大的任何组织通常都使用 BGP。BGP通常是攻击者的目标，因为它无处不在，而且*BGP配置在较*小的组织中是设置和忘记的。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。起始值因操作系统而异，通常范围为64到255。当数据包的TTL值达到零时，就会丢弃该数据包。

基于 TTL 的安全保护机制（称为通用 TTL 安全机制 (GTSM) 和 BGP TTL 安全破解 (BTSH)）利用 IP 数据包的 TTL 值，确保收到的 BGP 数据包来自直连的对等设备。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。

使用 **neighbor BGP 路由器配置命令的 ttl-security 选项可启用 BGP 的 GTSM。**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

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 BGP 发言者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。

通过 **neighbor BGP 路由器配置命令的 password 选项可配置使用 MD5 进行对等验证。**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。

配置最大前缀数

BGP 前缀由路由器存储在内存中。路由器必须存储的前缀越多，BGP 必须耗用的内存就越多。在一些配置中（例如，在仅利用提供商用户网络的一个或多个默认路由的配置中），可以存储所有 Internet 前缀的一个子集。

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。

使用 **neighbor maximum-prefix BGP 路由器配置命令配置此功能时，需要一个参数：**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。

使用前缀列表过滤 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。前缀列表应尽可能地使用，以确保通过预期路径发送网络流量。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。

使用自治系统路径访问列表过滤 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。此功能可与前缀列表一起使用，从而建立一组强大的过滤器。

此配置示例使用 AS 路径访问列表限制远程 AS 发起目标的入站前缀和本地自治系统发起目标的出站前缀。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。通常，您可以通过运行内部网关协议 (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。但是，如果所选的密码安全性低，MD5 验证仍然易受暴力和字典攻击。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

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

要降低在网络中引入错误路由信息的可能性，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。**

对于 EIGRP 和 RIP，使用 **distribute-list 命令及 out 关键字可限制通告的信息，而使用 in 关键字可限制处理的更新。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>
!
```

*有关如何控制路由更新通告和处理的更多信息，请参阅*配置独立于 IP 路由协议的功能。

此 OSPF 示例将前缀列表与 OSPF 特定的 **area filter-list 命令配合使用：**

```
!

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>
!
```

*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。

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。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，思科 IOS 软件支持的所有 FHRP 均包含利用 MD5 或文本字符串验证的功能。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。因此，在保障网络设备的安全时，相比数据平面务必要优先保护管理和控制平面。

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

绝大多数的数据层面数据流都按照网络的路由配置流经网络。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）等功能形成了现今网络的安全难题。

使用中转 ACL 也与数据层面的强化有关。

*有关更多信息，请参阅本文档的*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。另外，IP 选项还包括修改流量通过网络的路径的功能，由此可能允许其破坏安全控制。

由于这些问题，全局配置命令 ip options {drop **| ignore}**已添加到Cisco IOS软件版本12.3(4)T、12.0(22)S和12.2(25)S。在第一种形式的命令 **ip options drop** 中，将丢弃思科 IOS 设备收到的包含 IP 选项的所有 IP 数据包。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。

在某些情况下，可能会有攻击者导致思科 IOS 设备发送许多 ICMP 重定向消息，从而造成 CPU 负载增加。为此，建议禁用 ICMP 重定向传输。使用接口配置 **no ip redirects 命令可禁用 ICMP 重定向，如示例配置中所示：**

```
!

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。使用访问控制列表作为 **ip directed-broadcast 命令的选项可实现此目标。**以下配置示例限制了来自受信任网络 192.168.1.0/24 的 UDP 数据包的定向广播：

```
!

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。如果希望过滤传至特定设备组的流量或通过网络的流量，则 tACL 过滤非常有用。

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。

*有关更多信息，请参阅本文档的*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。本示例 ACL 允许来自受信任网络的 ICMP，但会阻止其他来源的所有 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

在本文档的使用基础设施 ACL 限制网络访问部分已介绍，过滤分段的 IP 数据包可能对安全设备构成挑战。

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
!
```

*有关使用 ACL 处理分段的 IP 数据包的更多信息，请参阅*访问控制列表和 IP 分段。

对过滤 IP 选项的 ACL 支持

在思科 IOS 软件版本 12.3(4)T 和更高版本中，思科 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，试图破坏网络中的安全控制或修改数据包的中转特征。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

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。思科 IOS 软件提供单播 RPF 和 IP 源保护 (IPSG) 功能，以阻止依靠源 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。

IP 源保护旨在通过执行交换机端口、MAC 地址和源地址验证，尽可能地减少受到直接管理控制的网络欺骗。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 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 **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 MAC 违规，可以使用四种违规模式之一。这些模式包括保护模式、限制模式、关闭模式和关闭 VLAN 模式。在实例中，如果某个端口仅为使用标准协议的单一工作站提供访问权限，则最大数量设置为 1 可能足够。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>
!
```

*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

要减少本地网段中的 ARP 下毒攻击，可以使用动态 ARP 检查 (DAI)。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 环境下，DAI 使用 DHCP 监听功能生成的数据。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>
!
```

DAi也可以在支持的任何位置按接口启用。

```
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。由于反欺骗 ACL 时常变化，所以需要定期监控它们。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。应保障数据平面的安全，包括在网络设备中中转的流量，以确保管理平面和控制平面的操作。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 日志记录 - ACL 日志记录包含因使用 log 关键字的 ACE 匹配（允许或拒绝）而生成的任何数据包。**
- **单播 RPF - 单播 RPF 与 ACL 一起使用可能会导致某些数据包的处理交换。**
- **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 条目的目的地需由 CPU 处理。**
- **非 IP 流量 - 所有非 IP 流量由 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。

基于 TTL 值过滤

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
!
```

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。

基于是否存在 IP 选项过滤

在思科 IOS 软件版本 12.3(4)T 和更高版本中，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，以便使用存在的 IP 选项过滤 IP 数据包。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。另外，还应注意 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，如果这些协议的数据包被丢弃，它们可能无法正常运行。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”；但是，“ACL IP 选项选择性丢弃”功能可能会丢弃这些流量，所以这些协议可能无法正常运行。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 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。

*有关 CoPP 功能的更多信息，请参阅*部署控制平面管制。

控制层面保护

在思科 IOS 软件版本 12.4(4)T 和更高版本中，可以使用控制平面保护 (CPPr) 按思科 IOS 设备的 CPU 来限制或监控控制平面的流量。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 策略中，将数据包与允许操作匹配的访问控制列表条目会使这些数据包被策略映射丢弃功能丢弃，而与拒绝操作（不显示）匹配的数据包则不受策略映射丢弃功能影响。

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。使用思科 IOS 软件完成此任务的两种主要方法是 Netflow 和分类 ACL。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。可通过 CLI 查看和分析 NetFlow

数据，也可以将数据导出到商用或免费软件 NetFlow 收集器中进行汇聚和分析。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。利用在大容量环境下采样的流量数据，可创建 Netflow 流。

要启用 NetFlow，必须具备 CEF 或分布式 CEF。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。另外，管理员也可以在 ACL 末尾将隐式拒绝分成粒度 ACE，以帮助识别被拒绝流量的类型。

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。使用 **clear ip access-list counters acl-name EXEC 命令可清除 ACL 计数器。**

```
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。此功能不适用于路由接口上的 ACL。例如，可以使用 VLAN 映射来阻止相同 VLAN 内包含的主机相互通信，这样可降低本地攻击者或蠕虫利用同一网段中主机的机会。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。

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>
!
```

本示例展示了如何使用 VLAN 映射来拒绝 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。

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>
!

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。

此接口命令必须在入口接口上应用，它将指示转发引擎不检查 IP 信头。由此，您将可以在 IP 环境下使用 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，第 2 层 VLAN 中的所有设备均可自由通信。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。如果单一服务器被入侵，在应用了 PVLAN 而无法连接至其他服务器的情况下，可能有助于将入侵仅限于一台服务器。

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。每个主 VLAN 可能只有一个隔离 VLAN，并且只有混合端口才能与隔离 VLAN 中的端口通信。应在不受信任的网络（如支持来宾的网络）上使用隔离 VLAN。

此配置示例将VLAN 11配置为隔离VLAN，并将其与主VLAN(VLAN 20)关联。以下示例还将接口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
!
```

在实施 PVLAN 时，务必要确保存在的第 3 层配置支持 PVLAN 强加的限制，并且不允许 PVLAN 配置被破坏。第 3 层过滤加上路由器 ACL 或防火墙可防止 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

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

此清单是本指南中介绍的所有强化步骤的集合。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）警告使用标志

- AAA

  使用 AAA 进行身份验证和回退使用 AAA (TACACS+) 进行命令授权使用 AAA 进行记帐使用冗余 AAA 服务器

- SNMP

  配置 SNMPv2 社区并应用 ACL配置 SNMPv3

- 日志记录

  配置集中式日志记录设置所有相关组件的日志记录级别设置日志记录源接口配置日志记录时间戳粒度

- 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

- 配置 NTP 身份验证（如果正在使用 NTP）
- 配置控制平面管制/保护（端口过滤、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、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

  ACLIP 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