用來強化 Cisco IOS 裝置的思科指南

目錄

適用於RSA金鑰的SSHv2增強功能
控制檯和AUX埠
控制vty和tty線路
vty和tty線路的控制傳輸
警告橫幅
驗證、授權及記帳
TACACS+ 驗證
驗證後援
使用7類密碼
TACACS+命令授權
TACACS+指令計量
冗餘AAA伺服器
強化簡單網路管理協定
SNMP社群字串
使用ACL的SNMP社群字串
基礎架構ACL
SNMP檢視
SNMP版本3
管理平面保護
記錄最佳實踐
將日誌傳送到中心位置
日誌記錄級別
不登入到控制檯或監控會話
使用緩衝日誌記錄
配置日誌記錄源介面
配置日誌記錄時間戳
Cisco IOS軟體組態管理
配置替換和配置回滾
獨佔配置更改訪問
Cisco IOS軟體彈性組態
數位簽章的思科軟體
組態變更通知和記錄
控制平面
一般控制平面加固
IP ICMP重新導向
ICMP不可達
代理 ARP
限制控制平面流量對CPU的影響
瞭解控制平面流量
基礎架構ACL
接收 ACL
CoPP
控制平面保護
硬體速率限制器
安全BGP

簡介

本文件說明的資訊可協助您保護 Cisco IOS® 系統裝置的安全，能夠提高您網路的整體資安。本文檔圍繞網路裝置功能可分類的三個平面進行設計，概述了每個功能並參考了相關文檔。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

網路的三個功能平面（管理平面、控制平面和資料平面）均提供需要保護的不同功能。

- **管理平**面 — 管理平面管理傳送到Cisco IOS裝置的流量，該流量由應用程式和協定組成，例如安全外殼(SSH)和簡單網路管理協定(SNMP)。
- **控制平**面 — 網路裝置的控制平面處理對維護網路基礎設施的功能至關重要的流量。控制平面由網路裝置之間的應用程式和協定組成，包括邊界網關協定(BGP)以及內部網關協定(IGP)，如增強型內部網關路由協定(EIGRP)和開放最短路徑優先(OSPF)。
- **資料平**面 — 資料平面通過網路裝置轉發資料。資料平面不包括傳送到本地Cisco IOS裝置的流量。

本檔案中的安全功能範圍通常會提供足夠詳細資訊，以便您設定功能。但是，如果它不這樣做，則以一種方式解釋該特徵，以便您可以評估是否需要對該特徵給予額外注意。如果可能而且適當，本文檔包含一些建議，這些建議在實施後將有助於確保網路的安全。

安全操作

安全網路操作是一個重要的主題。雖然本文的大部分內容都專門討論Cisco IOS裝置的安全配置，但僅靠配置並不能完全保護網路。在網路上使用的操作過程對安全性的貢獻不亞於對底層裝置的配置。

這些主題包含建議您實施的操作建議。這些主題重點介紹網路運營的特定關鍵領域，並不全面。

監控思科資安諮詢

思科產品安全事件響應團隊(PSIRT)針對思科產品中的安全相關問題建立和維護出版物，通常稱為PSIRT諮詢。用於不太嚴重問題的通訊方法是思科安全響應。有關安全建議和響應，請訪問http://www.cisco.com/go/psirt。

有關這些通訊工具的其他資訊，請參閱思科安全漏洞策略。

為了維護安全的網路，您需要瞭解已發佈的思科安全建議和響應。您需要先瞭解漏洞，然後才能評估漏洞對網路造成的威脅。請參閱安全漏洞公告的風險分類，以獲得此評估流程的幫助。

利用身份驗證、授權和記帳

身份驗證、授權和記帳(AAA)框架對於保護網路裝置安全至關重要。AAA框架提供管理會話的身份驗證，還可以將使用者限制到管理員定義的特定命令，並記錄所有使用者輸入的所有命令。有關如何利用AAA的詳細資訊，請參閱本文檔的身份驗證、授權和記帳部分。

集中日誌收集和監控

為了瞭解有關與安全事件相關的現有、新興和歷史事件的資訊，您的組織必須具有統一的事件記錄和相關策略。此策略必須利用來自所有網路裝置的日誌記錄並使用預打包的可定製關聯功能。

實施集中記錄後，您必須開發一種結構化方法來分析日誌和跟蹤事件。根據您組織的需要，此方法包括簡單勤奮的日誌資料審查以及高級的基於規則的分析。

有關如何在Cisco IOS網路裝置上實施日誌記錄的詳細資訊，請參閱本文檔的日誌記錄最佳實踐*部分*。

儘可能使用安全協定

許多協定用於傳送敏感的網路管理資料。必須儘可能使用安全協定。安全協定選擇包括使用SSH而不是Telnet，以便同時加密身份驗證資料和管理資訊。此外，複製配置資料時必須使用安全檔案傳輸協定。例如，使用安全複製通訊協定(SCP)來代替FTP或TFTP。

有關Cisco IOS裝置安全管理的詳細資訊，請參閱本文檔的安全互動式管理會話*部分*。

通過NetFlow獲得流量可視性

NetFlow使您能夠監控網路中的通訊流。NetFlow最初旨在將流量資訊匯出到網路管理應用程式，也可以用於顯示路由器上的流量資訊。此功能允許您即時檢視哪些流量通過網路。無論是否將流資訊匯出到遠端收集器，都建議您為NetFlow配置網路裝置，以便在需要時可以反應性地使用它。

有關此功能的更多資訊，請參閱本文檔的流量識別和回溯部分和http://www.cisco.com/go/netflow(僅限註冊客戶)。

組態管理

配置管理是建議、審查、批准和部署配置更改的流程。在Cisco IOS裝置配置環境中，配置管理的另

外兩個方面至關重要：配置存檔和安全。

您可以使用配置存檔來回滾對網路裝置所做的更改。在安全情景中，還可以使用配置歸檔檔案來確定進行了哪些安全更改以及更改發生的時間。結合AAA日誌資料，此資訊有助於網路裝置的安全審計。

Cisco IOS裝置的配置包含許多敏感詳細資訊。使用者名稱、密碼和訪問控制清單的內容都是此類資訊的示例。需要保護用於存檔Cisco IOS裝置配置的儲存庫。對這種資訊的不安全訪問可能會破壞整個網路的安全。

管理平面

管理平面包含實現網路管理目標的功能。這包括使用SSH的互動式管理會話，以及使用SNMP或NetFlow收集統計資訊。當您考慮網路裝置的安全時，保護管理平面至關重要。如果安全事件能夠破壞管理平面的功能，則無法恢復或穩定網路。

本文中的這些部分詳細說明了有助於加強管理平面的Cisco IOS軟體提供的安全功能和配置。

一般管理平面強化

管理平面用於訪問、配置和管理裝置，以及監控其操作和部署裝置的網路。管理平面是接收和傳送用於這些功能操作的流量的平面。您必須保護裝置的管理平面和控制平面，因為控制平面的操作會直接影響管理平面的操作。管理平面使用此協定清單：

- 簡單網路管理協定
- Telnet
- 安全殼層通訊協定
- 檔案傳輸通訊協定
- 超文本傳輸協定/安全超文本傳輸協定
- 簡單式檔案傳輸通訊協定
- 安全複製協定
- TACACS+
- RADIUS
- Netflow
- 網路時間協定
- 系統日誌

必須採取措施確保在發生安全事故時管理和控制平面能夠繼續存在。如果其中一種飛機被成功利用，所有飛機都可能被破壞。

密碼管理

密碼控制對資源或裝置的訪問。這是通過定義用於驗證請求的密碼或密碼實現的。當接收到訪問資源或裝置的請求時，該請求被詢問以驗證密碼和身份，並且基於該結果可以允許、拒絕或限制訪問。作為一種安全最佳實踐，密碼必須使用TACACS+或RADIUS身份驗證伺服器進行管理。但是請注意，如果TACACS+或RADIUS服務失敗，仍需要本地配置的特權訪問密碼。裝置還可在其配置中顯示其他密碼資訊，如NTP金鑰、SNMP社群字串或路由協定金鑰。

enable secret命令用於設定授予對Cisco IOS系統的特權管理訪問許可權的密碼。必須使用**enable secret**命令，而不是較舊的**enable password**命令。**enable password** 命令使用弱加密演算法。

如果沒有設定使能加密並且為控制檯tty線路配置了口令，則可以使用控制檯口令來接收特權訪問，甚至從遠端虛擬tty(vty)會話也是如此。此操作幾乎肯定是不希望執行的，也是確保配置啟用加密金鑰的另一個原因。

service password-encryption全域性配置命令指示Cisco IOS軟體加密密碼、質詢握手身份驗證協定(CHAP)機密以及儲存在其配置檔案中的類似資料。這種加密對於防止偶然觀察者讀取密碼很有用，例如當他們在管理員的集中檢視螢幕時。但是，**service password-encryption**命令使用的演算法是簡單的Vigen重新加密演算法。此演算法的設計目的不是保護配置檔案免遭即使是稍有經驗的攻擊者進行嚴重分析，因此不能用於此目的。任何包含加密密碼的Cisco IOS配置檔案都必須謹慎對待，如同處理這些相同密碼的明文清單一樣。

enable secret命令未使用此弱加密演算法，但**enable password**全域性配置命令以及**password**行配置命令都使用此弱加密演算法。必須消除此型別的密碼，並且需要使用**enable secret**命令或Enhanced Password Security功能。

enable secret命令和增強型口令安全功能使用消息摘要5(MD5)進行口令雜湊。這種演算法已經得到了廣泛的公眾評價，並且還不知道是可逆的。但是，該演算法容易受到字典攻擊。在字典攻擊中，攻擊者會嘗試字典或其他候選密碼清單中的每個字來查詢匹配項。因此，配置檔案必須安全儲存，且只能與受信任的個人共用。

增強型密碼安全

Cisco IOS軟體版本12.2(8)T中引入的增強型密碼安全功能允許管理員為**username**指令設定MD5密碼雜湊。在此功能之前，有兩種型別的密碼：輸入0（明文密碼）和輸入7（使用Vigen重新加密演算法）。增強型密碼安全功能不能用於要求可檢索明文密碼的協定，如CHAP。

若要使用MD5雜湊加密使用者密碼，請發出**username secret**全域性配置命令。

```
!
username <name> secret <password>
!
```

有關此功能的詳細資訊，請參閱增強型密碼安全。

登入密碼重試鎖定

Cisco IOS軟體版本12.3(14)T新增的登入密碼重試鎖定功能，允許您在已設定的失敗登入嘗試次數後鎖定本機使用者帳戶。使用者鎖定後，其帳戶將被鎖定，直到您解鎖該帳戶。不能使用此功能鎖定配置許可權級別15的授權使用者。許可權級別為15的使用者數必須保持最低。

請注意，如果達到不成功的登入嘗試次數，授權使用者可以將自己鎖定在裝置之外。此外，惡意使用者可反複嘗試使用有效使用者名稱進行身份驗證，從而建立拒絕服務(DoS)條件。

此範例顯示如何啟用登入密碼重試鎖定功能：

```
!

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

!

username <name> secret <password>

!
```

此功能也適用於CHAP和密碼驗證通訊協定(PAP)等驗證方法。

無服務密碼 — 恢復

在Cisco IOS軟體版本12.3(14)T和更新版本中，無服務密碼復原功能不允許任何具有主控台存取許可權的人以不安全的方式存取裝置組態並清除密碼。也不允許惡意使用者更改配置暫存器值和訪問NVRAM。

```
!

no service password-recovery

!
```

Cisco IOS軟體提供密碼恢復過程，該過程依賴於在系統啟動期間使用Break鍵訪問ROM監控模式(ROMMON)。在ROMMON中，可以重新載入裝置軟體以提示包含新密碼的新系統配置。

當前密碼恢復程式使任何擁有控制檯訪問許可權的人能夠訪問裝置及其網路。無服務密碼恢復功能可阻止在系統啟動期間完成Break按鍵順序並輸入ROMMON。

如果裝置上未啟用**服務密碼恢復**，建議儲存裝置配置的離線副本，並實施配置歸檔解決方案。啟用此功能後，如果需要恢復Cisco IOS裝置的密碼，則會刪除整個配置。

有關此功能的詳細資訊，請參閱安全ROMMON配置示例。

禁用未使用的服務

作為最佳安全實踐，必須禁用任何不必要的服務。這些不需要的服務，尤其是使用使用者資料包協定(UDP)的服務，很少用於合法目的，但可用於發起DoS和其他通過資料包過濾阻止的攻擊。

必須禁用TCP和UDP小型服務。這些服務包括：

- echo（埠號7）
- discard（埠號9）
- 白天（埠號13）

- chargen（埠號19）

雖然通過反欺騙訪問清單可以避免或降低對小型服務的濫用，但必須在網路中可訪問的任何裝置上禁用這些服務。Cisco IOS軟體版本12.0和更新版本預設停用小型服務。在早期的軟體中，可以發出**no service tcp-small-servers**和**no service udp-small-servers**全域性配置命令來禁用它們。

以下是如果不使用時必須禁用的其他服務清單：

- 發出**no ip finger** global configuration命令以停用Finger服務。預設情況下，12.1(5)和12.1(5)T以後的Cisco IOS軟體版本禁用此服務。
- 發出**no ip bootp server**全域組態命令，以停用啟動程式通訊協定(BOOTP)。
- 在Cisco IOS軟體版本12.2(8)T和更新版本中，在全域組態模式下發出**ip dhcp bootp ignore**命令以停用BOOTP。這會保持動態主機設定通訊協定(DHCP)服務處於啟用狀態。
- 如果不需要DHCP中繼服務，則可以禁用DHCP服務。在全域性配置模式下發出**no service dhcp**命令。
- 在介面組態模式中發出**no mop enabled**命令，以停用維護操作通訊協定(MOP)服務。
- 發出**no ip domain-lookup**全域性配置命令，以禁用域名系統(DNS)解析服務。
- 在全域組態模式下發出**no service pad**命令，以停用用於X.25網路的資料包彙編器/反彙編器(PAD)服務。
- 在全域性配置模式下，可以使用**no ip http server**命令禁用HTTP伺服器，可以使用**no ip http secure-server**全域性配置命令禁用安全HTTP(HTTPS)伺服器。
- 除非Cisco IOS裝置在啟動期間從網路檢索配置，否則必須使用**no service config**全域性配置命令。這可防止Cisco IOS裝置嘗試使用TFTP在網路上查詢配置檔案。
- Cisco Discovery Protocol(CDP)是一種網路協定，用於發現其它啟用CDP的裝置以實現鄰居鄰接和網路拓撲。CDP可由網路管理系統(NMS)或在故障排除期間使用。必須在連線到不受信任網路的所有介面上禁用CDP。這可以通過**no cdp enable interface**命令完成。或者，可以使用**no cdp run**全域性配置命令全域性禁用CDP。請注意，惡意使用者可能使用CDP進行偵測和網路對映。
- 連結層探索通訊協定(LLDP)是在802.1AB中定義的IEEE通訊協定。LLDP與CDP類似。但是此通訊協定允許不支援CDP的其他裝置之間的互通性。LLDP必須採用與CDP相同的方式處理，並在連線到不可信網路的所有介面上禁用。為此，請發出**no lldp transmit**和**no lldp receive**介面配置命令。發出**no lldp run** 全域性配置命令，以全域性禁用LLDP。惡意使用者也可以使用LLDP進行偵測和網路對映。
- 對於支援從sdflash引導的交換機，可以通過從快閃記憶體引導並使用「no sdflash」配置命令禁用sdflash來增強安全性。

EXEC超時

要設定EXEC命令直譯器在終止會話之前等待使用者輸入的間隔，請發出**exec-timeout**線路配置命令。必須使用**exec-timeout**命令，才能註銷閒置的vty或tty線路上的會話。預設情況下，會話在處於非活動狀態十分鐘後斷開。

```
!

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

TCP作業階段的Keepalive

service tcp-keepalive-in和**service tcp-keepalive-out**全域性配置命令使裝置能夠為TCP會話傳送TCP keepalive。必須使用此配置才能對裝置的入站連線和裝置的出站連線啟用TCP keepalive。這可確保連線的遠端裝置仍然可訪問，並從本地Cisco IOS裝置中刪除半開放或孤立的連線。

```
!

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

管理介面使用

裝置的管理平面在物理或邏輯管理介面上被帶內訪問或帶外訪問。理想情況下，每個網路裝置都有帶內和帶外管理訪問，以便在網路中斷期間訪問管理平面。

用於裝置帶內訪問的最常見介面之一是邏輯環回介面。環回介面始終處於開啟狀態，而物理介面可以更改狀態，並且介面可能不可訪問。建議為每個裝置新增一個環回介面作為管理介面，並且只將其用於管理平面。這允許管理員在整個網路中為管理平面應用策略。在裝置上配置環回介面後，管理平面協定（如SSH、SNMP和syslog）就可以使用環回介面來傳送和接收流量。

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

記憶體閾值通知

Cisco IOS軟體版本12.3(4)T新增的記憶體臨界通知功能可協助您減輕裝置上的低記憶體狀況。此功能使用兩種方法來完成此操作：記憶體閾值通知和記憶體保留。

「記憶體閾值通知」會生成一條日誌消息，以指示裝置上的可用記憶體已低於配置的閾值。此配置示例說明如何使用**memory free low-watermark**全域性配置命令啟用此功能。這使得裝置在可用空閒記憶體低於指定閾值時生成通知，在可用空閒記憶體高於指定閾值達到5%時再次生成通知。

```
!

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

使用記憶體保留以便有足夠的記憶體可用於關鍵通知。此組態範例示範如何啟用此功能。這可確保當裝置的記憶體耗盡時，管理進程繼續運行。

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

有關此功能的詳細資訊，請參閱記憶體閾值通知。

CPU閾值通知

Cisco IOS軟體版本12.3(4)T中引入的CPU閾值通知功能可讓您檢測裝置上的CPU負載超過設定閾值時並收到通知。超過閾值時，裝置會生成並傳送SNMP陷阱消息。Cisco IOS軟體支援兩種CPU利用率閾值方法：上升閾值和下降閾值。

此示例配置顯示如何啟用觸發CPU閾值通知消息的上升和下降閾值：

```
!

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>]
!
```

有關此功能的詳細資訊，請參閱CPU閾值通知。

為控制檯訪問保留記憶體

在Cisco IOS軟體版本12.4(15)T和更新版本中，可以使用保留記憶體以存取主控台功能來保留足夠的記憶體，以確保主控台可以存取Cisco IOS裝置以進行管理和疑難排解。當裝置記憶體不足時，此功能尤其有用。您可以發出**memory reserve console**全域性配置命令以啟用此功能。此示例配置一個Cisco IOS裝置以為此保留4096 KB。

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

有關此功能的詳細資訊，請參閱為控制檯訪問保留記憶體。

儲存器洩漏檢測器

記憶體洩漏檢測器功能在Cisco IOS軟體版本12.3(8)T1中引入，可用於檢測裝置上的記憶體洩漏。記憶體洩漏檢測器能夠發現所有記憶體池、資料包緩衝區和區塊中的洩漏。記憶體洩漏是記憶體的靜態或動態分配，不能用於任何有用的用途。此功能側重於動態記憶體分配。您可以使用**show memory debug leaks** EXEC命令檢測是否存在記憶體洩漏。

緩衝區溢位：紅色區域損壞的檢測和糾正

在Cisco IOS軟體版本12.3(7)T和更新版本中，緩衝區溢位：可以在裝置上啟用檢測和糾正Redzone損壞功能，以檢測和糾正記憶體塊溢位並繼續操作。

可以使用這些全域性配置命令來啟用此功能。配置完成後，可以使用**show memory overflow**命令顯示緩衝區溢位檢測和更正統計資訊。

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

增強型Crashinfo檔案收集

增強的Crashinfo檔案收集功能會自動刪除舊的crashinfo檔案。此功能新增在Cisco IOS軟體版本12.3(11)T中，允許裝置重新取得空間，以便在裝置崩潰時建立新的crashinfo檔案。此功能還允許配置要儲存的crashinfo檔案的數量。

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

網路時間協定

網路時間協定(NTP)不是特別危險的服務，但任何不必要的服務都可能代表攻擊媒介。如果使用NTP，必須顯式配置受信任的時間源並使用正確的身份驗證。系統日誌需要準確可靠的時間，例如對潛在攻擊進行取證調查期間，以及依賴證書進行第1階段身份驗證時成功的VPN連線。

- **NTP時區** — 配置NTP時，需要配置時區，以便可以準確地關聯時間戳。通常有兩種方法為全域性存在網路中的裝置配置時區。一種方法是使用協調世界時(UTC)(以前為格林尼治標準時間(GMT))配置所有網路裝置。 另一種方法是使用本地時區配置網路裝置。有關此功能的詳細資訊，請參閱思科產品文檔中的「時鐘時區」。

- **NTP驗證** — 如果配置NTP驗證，則可確保可信NTP對等體之間交換NTP消息。

使用NTP身份驗證的配置示例：

客戶端：

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

伺服器:

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

禁用智慧安裝

思科智慧安裝(SMI)功能的安全最佳實踐取決於如何在特定客戶環境中使用該功能。思科區分這些使用案例：

- 不使用智慧安裝功能的客戶。
- 僅將智慧安裝功能用於零接觸部署的客戶。
- 利用智慧安裝功能進行零接觸部署（配置和映像管理）的客戶。

以下各節詳細描述了每個場景：

- 不使用智慧安裝功能的客戶。
- 如果客戶不使用思科智慧安裝功能，並在命令可用時運行思科IOS和思科IOS XE軟體版本，則應使用**no vstack**命令禁用智慧安裝功能。

  附註：**vstack**命令是在Cisco IOS版本12.2(55)SE03中匯入。

以下是已停用智慧安裝使用者端功能的Cisco Catalyst交換器上**show vstack**指令的輸出範例：

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

僅利用智慧安裝功能進行零接觸部署的客戶

零接觸安裝完成後禁用智慧安裝客戶端功能，或使用**no vstack**命令。

若要將**no vstack**指令傳播到網路中，請使用以下方法之一：

- 在所有客戶端交換機上手動或使用指令碼輸入**no vstack**命令。
- 將**no vstack**命令新增為推入每個智慧安裝客戶端的Cisco IOS配置的一部分，作為零接觸安裝的一部分。
- 在不支援**vstack**命令的版本中(Cisco IOS版本12.2(55)SE02和較低版本)，請在使用者端交換器上套用存取控制清單(ACL)，以封鎖TCP連線埠4786上的流量。

若要以後啟用智慧安裝客戶端功能，請手動或使用指令碼在所有客戶端交換機上輸入**vstack**命令。

利用智慧安裝功能進行非零接觸部署的客戶

在設計智慧安裝架構時，應小心使基礎設施IP地址空間不可被不受信任的各方訪問。在不支援**vstack**命令的版本中，確保只有智慧安裝指揮交換機才能與埠4786上的所有智慧安裝客戶端建立TCP連線。

管理員可以將這些最佳安全實踐用於受影響裝置上的思科智慧安裝部署：

- 介面ACL
- 控制階段管制(CoPP)。 並非所有Cisco IOS軟體版本都提供此功能。

以下範例顯示智慧安裝導向器IP位址為10.10.10.1、智慧安裝使用者端IP位址為10.10.10.200的介面ACL:

```
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
```

必須在所有客戶端的所有IP介面上部署此ACL。也可以在首次部署交換機時通過指揮交換機來推送它。

為了進一步限制對基礎設施中所有客戶端的訪問，管理員可以在網路中的其他裝置上使用以下安全最佳做法：

- 基礎架構存取控制清單(iACL)
- VLAN存取控制清單(VACL)

使用基礎架構ACL限制對網路的訪問

基礎架構存取控制清單(iACL)旨在防止未經授權而直接與網路裝置通訊，是網路中可以實作的最關鍵安全控制之一。基礎架構ACL利用這樣一種理念：幾乎所有網路流量都流經網路，而不是流向網路本身。

構建並應用iACL以指定從主機或網路到網路裝置的連線。這些連線型別的常見示例包括eBGP、SSH和SNMP。在所需連線被允許後，到基礎設施的所有其他流量都會被明確拒絕。然後會明確允許所有穿越網路且目的地不是基礎設施裝置的傳輸流量。

iACL提供的保護與管理和控制平面都相關。通過對網路基礎設施裝置使用不同的編址，可以更輕鬆地實施iACL。有關IP編址安全影響的詳細資訊，請參閱面向安全的IP編址方法。

以下iACL配置示例說明了在開始iACL實施過程時必須用作起點的結構：

```
!

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
!
```

建立後，iACL必須應用到面向非基礎設施裝置的所有介面。這包括連線到其他組織、遠端訪問段、使用者段和資料中心段的介面。

*請參閱*保護您的核心：基礎架構保護存取控制清單以瞭解更多有關基礎架構ACL的資訊。

ICMP封包過濾

網際網路控制訊息通訊協定(ICMP)是作為IP控制通訊協定而設計的。因此，它傳達的消息可能會對一般的TCP和IP協定產生深遠的影響。雖然網路疑難排解工具**ping**和**traceroute**使用ICMP，但網路正常運作幾乎不需要外部ICMP連線。

Cisco IOS軟體提供功能，以便根據名稱或型別和代碼專門過濾ICMP訊息。此範例ACL必須與前面範例中的存取控制專案(ACE)搭配使用，它允許從受信任的管理站和NMS伺服器執行ping，並封鎖所有其他ICMP封包：

```
!

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
!
```

篩選IP片段

分段的IP資料包的過濾過程可能會給安全裝置帶來挑戰。這是因為用於過濾TCP和UDP封包的第4層資訊僅存在於初始片段中。Cisco IOS軟體使用特定方法根據已設定的存取清單檢查非初始片段。Cisco IOS軟體會根據ACL評估這些非初始片段，並忽略任何第4層篩選資訊。這會導致任何已配置的ACE的第3層部分僅評估非初始片段。

在此範例組態中，如果連線埠22上目的地為192.168.1.1的TCP封包在傳輸過程中分段，則根據封包中的第4層資訊，第二個ACE會按照預期方式捨棄初始分段。但是，完全基於資料包和ACE中的第3層資訊，第一個ACE允許所有剩餘的（非初始）片段。此情況顯示在此組態中：

```
!

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
!
```

由於片段處理的不直觀性質，ACL經常會無意中允許IP片段。分段也經常用於嘗試逃避入侵檢測系統的檢測。正是由於這些原因，IP片段經常用於攻擊，也正是因為如此，必須在任何已配置的iACL的頂部顯式過濾這些片段。此範例ACL包括IP片段的全面過濾。此示例的功能必須與前面示例的功能結合使用。

```
!

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
!
```

請參閱存取控制清單和IP片段，*以取得更多有關ACL如何處理分段的IP封包的資訊。*

適用於篩選IP選項的ACL支援

Cisco IOS軟體版本12.3(4)T新增對使用ACL根據封包中包含的IP選項過濾IP封包的支援。IP選項對網路裝置來說是一個安全挑戰，因為這些選項必須作為例外資料包處理。這要求有一定的CPU工作量，而對於通過網路傳輸的典型資料包則不需要這種工作量。封包中存在IP選項也表示有人企圖破壞網路中的安全控制，或以其他方式變更封包的傳輸特徵。正是由於這些原因，必須在網路邊緣過濾具有IP選項的資料包。

此示例必須與前面示例中的ACE一起使用，以便包括對包含IP選項的IP資料包進行完全過濾：

```
!

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
!
```

可依照TTL值過濾的ACL支援

Cisco IOS軟體版本12.4(2)T新增了ACL支援，以根據生存時間(TTL)值篩選IP封包。當資料包從源流向目標時，每台網路裝置都會減少IP資料包的TTL值。雖然初始值因作業系統而異，但當資料包的TTL達到零時，必須丟棄該資料包。若要產生並向封包的來源傳送ICMP超出時間訊息，需要將TTL減為零並因此捨棄封包的裝置。

這些消息的生成和傳輸是一個異常過程。當即將到期的IP資料包數量較少時，路由器可以執行此功能，但是如果即將到期的資料包數量較大，則生成和傳輸這些消息會佔用所有可用的CPU資源。這表示一個DoS攻擊向量。正是由於這個原因，需要強化裝置以抵禦DoS攻擊，這些攻擊利用高速率IP資料包即將過期。

建議組織過濾網路邊緣具有低TTL值的IP資料包。完全過濾TTL值不足以穿越網路的資料包可以緩解基於TTL的攻擊威脅。

此範例ACL會過濾TTL值小於六的資料包。這樣可為寬度最多五跳的網路提供保護，以抵禦TTL過期攻擊。

```
!

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
!
```

> **附註**：某些協定合法使用具有低TTL值的資料包。eBGP就是這樣一個通訊協定。請參閱TTL到期攻擊識別和緩解，瞭解有關緩解TTL到期攻擊的更多資訊。

有關此功能的詳細資訊，請參閱ACL支援以過濾TTL值。

安全的互動式管理會話

通過裝置管理會話，您可以檢視和收集有關裝置及其操作的資訊。如果向惡意使用者披露此資訊，裝置可能會成為攻擊目標、遭到破壞並被用於執行其他攻擊。任何擁有裝置特權訪問許可權的人都能夠對該裝置進行完全管理控制。必須保護管理會話的安全，以防止資訊洩露和未經授權的訪問。

管理平面保護

在Cisco IOS軟體版本12.4(6)T和更新版本中，功能管理平面保護(MPP)允許管理員限制裝置可以接收管理流量的介面。這樣，管理員可以進一步控制裝置及其訪問方式。

此範例顯示如何啟用MPP，以便僅允許GigabitEthernet0/1介面上的SSH和HTTPS:

```
!

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

有關MPP的詳細資訊，請參閱管理平面保護。

控制平面保護

控制平面保護(CPPr)建立在控制平面策略功能的基礎上，用於限制和管制目的地為IOS裝置路由處理器的控制平面流量。CPPr新增在Cisco IOS軟體版本12.4(4)T中，將控制平面劃分為單獨的控制平面類別，這些類別稱為子介面。存在三個控制平面子介面：主機、傳輸和CEF異常。此外，CPPr還包括以下額外的控制平面保護功能：

- **連線埠過濾功**能 — 此功能提供管制或捨棄前往關閉或非偵聽TCP和UDP連線埠的封包。
- **Queue-threshold policy feature** — 此功能限制控制平面IP輸入隊列中允許的指定協定的資料包數。

CPPr允許管理員對傳送到裝置的流量進行分類、管制和限制，以便通過主機子介面進行管理。針對主機子介面類別分類的資料包示例包括SSH或Telnet等管理流量以及路由協定。

附註：CPPr不支援IPv6，且僅限於IPv4輸入路徑。

有關Cisco CPPr功能的詳細資訊，請參閱控制平面保護功能指南 — 12.4T*和*瞭解控制平面保護。

加密管理會話

因為資訊可以在互動管理會話中公開，所以必須加密此流量，以便惡意使用者無法訪問傳輸的資料。流量加密允許與裝置建立安全的遠端訪問連線。如果管理會話的流量以明文形式通過網路傳送，攻擊者可以獲取有關裝置和網路的敏感資訊。

管理員可以建立到具有SSH或HTTPS（安全超文本傳輸協定）功能的裝置的加密安全遠端訪問管理連線。Cisco IOS軟體支援SSH版本1.0(SSHv1)、SSH版本2.0(SSHv2)和HTTPS，後者使用安全套接字層(SSL)和傳輸層安全(TLS)進行身份驗證和資料加密。SSHv1和SSHv2不相容。SSHv1不安全，也不標準化，因此如果選擇SSHv2，則不建議使用SSHv1。

Cisco IOS軟體也支援安全複製協定(SCP)，藉此允許加密且安全的連線來複製裝置設定或軟體映像。SCP依賴SSH。此示例配置在Cisco IOS裝置上啟用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
!
```

此配置示例啟用SCP服務：

```
!

ip scp server enable
!
```

以下是HTTPS服務的配置示例：

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

有關Cisco IOS軟體SSH功能的詳細資訊，請參閱在執行Cisco IOS和Secure Shell(SSH)的路由器和交換機上配置Secure Shell。

SSHv2

Cisco IOS軟體版本12.3(4)T中引入的SSHv2支援功能允許使用者設定SSHv2。（SSHv1支援是在較早版本的Cisco IOS軟體中實施的。）SSH在可靠的傳輸層上運行，並提供強大的身份驗證和加密功能。為SSH定義的唯一可靠傳輸是TCP。SSH提供了一種通過網路在其它電腦或裝置上安全訪問並安全執行命令的方法。通過SSH隧道傳輸的安全複製協定(SCP)功能允許安全傳輸檔案。

如果沒有明確配置**ip ssh version 2**命令，則Cisco IOS啟用SSH版本1.99。SSH版本1.99允許SSHv1和SSHv2連線。SSHv1被認為是不安全的，可能會對系統產生不利影響。如果已啟用SSH，建議使用**ip ssh version 2命令禁用SSHv**1。

此示例配置在Cisco IOS裝置上啟用SSHv2（禁用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

!
```

有關使用SSHv2的詳細資訊，請參閱安全Shell版本2支援。

適用於RSA金鑰的SSHv2增強功能

Cisco IOS SSHv2支援鍵盤互動和基於密碼的身份驗證方法。針對RSA金鑰的SSHv2增強功能還支援對客戶端和伺服器進行基於RSA的公鑰身份驗證。

對於使用者身份驗證，基於RSA的使用者身份驗證使用與每個使用者關聯的私鑰/公鑰對進行身份驗證。使用者必須在客戶端生成私鑰/公鑰對，並在Cisco IOS SSH伺服器上配置公鑰以完成身份驗證。

嘗試建立憑證的SSH使用者使用私鑰提供加密簽名。簽名和使用者的公鑰將傳送到SSH伺服器進行身份驗證。SSH伺服器通過使用者提供的公鑰計算雜湊。雜湊用於確定伺服器是否有匹配的條目。如果找到匹配項，則使用公鑰執行基於RSA的消息驗證。因此，系統會根據加密簽名對使用者進行身份驗證或拒絕訪問。

對於伺服器身份驗證，Cisco IOS SSH客戶端必須為每個伺服器分配一個主機金鑰。當客戶端嘗試與伺服器建立SSH會話時，它會在金鑰交換消息中接收伺服器的簽名。如果在客戶端上啟用了嚴格主機金鑰檢查標誌，則客戶端將檢查它是否具有與預配置的伺服器對應的主機金鑰條目。如果找到匹配項，客戶端將嘗試使用伺服器主機金鑰驗證簽名。如果伺服器成功通過驗證，作業階段建立繼續進行；否則它會終止並顯示一條**Server Authentication Failed**消息。

此示例配置允許在Cisco IOS裝置上對SSHv2使用RSA金鑰：

```
!
! 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
!
```

有關使用RSA金鑰和SSHv2的詳細資訊，請參閱RSA金鑰的安全外殼版本2增強功能。

此示例配置使Cisco IOS SSH伺服器能夠執行基於RSA的使用者身份驗證。如果伺服器中儲存的RSA公鑰用客戶端中儲存的公鑰或私鑰對進行驗證，則使用者身份驗證成功。

```
!
! 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.)
!
```

有關使用RSA金鑰和SSHv2的詳細資訊，請參閱配置Cisco IOS SSH伺服器以執行基於RSA的使用者身份驗證。

此示例配置使Cisco IOS SSH客戶端能夠執行基於RSA的伺服器身份驗證。

```
!
!

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
!
```

有關使用RSA金鑰和SSHv2的詳細資訊，請參閱配置Cisco IOS SSH客戶端以執行基於RSA的伺服器身份驗證。

控制檯和AUX埠

在Cisco IOS裝置中，控制檯和輔助(AUX)埠是非同步線路，可用於對裝置進行本地和遠端訪問。您必須瞭解Cisco IOS裝置上的控制檯埠具有特殊許可權。特別地，這些許可權允許管理員執行密碼恢復過程。為了執行密碼恢復，未經身份驗證的攻擊者需要擁有對控制檯埠的訪問許可權，以及中斷裝置電源或導致裝置崩潰的能力。

任何用於訪問裝置控制檯埠的方法都必須以與對裝置進行特權訪問所實施的安全性同等的方式加以保護。如果數據機連線到控制檯，用於安全訪問的方法必須包括使用AAA、exec-timeout和數據機口令。

如果不需要口令恢復，則管理員可以使用**no service password-recovery全域性配置命令刪除執行口令恢復過程**的功能；但是，一旦啟用了**no service password-recovery**命令，管理員就無法在裝置上執行密碼恢復。

在大多數情況下，必須禁用裝置的AUX埠，以防止未經授權的訪問。可以使用以下命令禁用AUX埠：

```
!

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

控制vty和tty線路

Cisco IOS軟體中的互動式管理會話使用tty或虛擬tty(vty)。tty是一種本地非同步線路，終端可以連線到該線路上，以便本地訪問裝置，或者連線到數據機以撥號訪問裝置。請注意，ttys可用於連線到其他裝置的控制檯埠。此功能允許具有tty線路的裝置充當控制檯伺服器，通過該伺服器，可以通過網路與連線到tty線路的裝置的控制檯埠建立連線。此外，還必須控制通過網路進行反向連線的tty線路。

vty線路用於裝置支援的所有其他遠端網路連線，而不考慮協定（例如SSH、SCP或Telnet）。 為了確保可以通過本地或遠端管理會話訪問裝置，必須在vty和tty線路上實施適當的控制。Cisco IOS裝置的vty線路數量有限；可使用show line EXEC命令確定可用線路數。當所有vty線路都在使用時，無法建立新的管理會話，從而建立訪問裝置的DoS條件。

對裝置的vty或tty進行訪問控制的最簡單形式是在所有線路上使用身份驗證，而不管裝置在網路中的位置如何。這對於vty線路至關重要，因為它們可以通過網路訪問。連線到用於遠端訪問裝置的數據機的tty線路，或連線到其他裝置的控制檯埠的tty線路，也可通過網路訪問。其他形式的vty和tty訪問控制可以通過**transport input**或**access-class**配置命令實施，使用CoPP和CPPr功能，或者將訪問清單應用於裝置上的介面。

身份驗證可以通過使用AAA（推薦的通過身份驗證訪問裝置的方法）、使用本地使用者資料庫，或者通過直接在vty或tty線路上配置的簡單密碼身份驗證來實現。

必須使用**exec-timeout**命令，才能註銷閒置的vty或tty線路上的會話。還必須使用**service tcp-keepalive-in**命令，才能在對裝置的傳入連線上啟用TCP keepalive。這可確保連線遠端端的裝置仍然可訪問，並且從本地IOS裝置中刪除半開放或孤立的連線。

vty和tty線路的控制傳輸

vty和tty的配置應僅接受到裝置或通過該裝置（如果用作控制檯伺服器）的加密和安全遠端訪問管理連線。本節介紹tty，因為此類線路可以連線到其它裝置上的控制檯埠，從而允許通過網路訪問tty。為了防止資訊洩漏或未經授權訪問在管理員和裝置之間傳輸的資料，應使用**transport input ssh**而不是明文協定，如Telnet和rlogin。可以在tty上啟用**transport input none**配置，這實際上會禁用對反向控制檯連線使用tty線路。

vty和tty線路均允許管理員連線到其他裝置。若要限制管理員可用於傳出連線的傳輸型別，請使用**transport output**線路配置命令。如果不需要傳出連線，則應**使用transport output none**。但是，如果允許傳出連線，則應通過使用**transport output ssh**對連線實施加密且安全的遠端訪問方法。

> **附註**：如果支援，IPSec可用於到裝置的加密安全遠端訪問連線。如果使用IPSec，也會為裝置增加額外的CPU開銷。但是，即使使用IPSec，也必須將SSH作為傳輸實施。

警告橫幅

在某些司法管轄區，除非通知惡意使用者不允許使用該系統，否則不可能起訴或非法監控惡意使用者。提供此通知的一種方法是將此資訊放入使用Cisco IOS軟體banner login命令配置的標語消息中。

法律通知的要求很複雜，因管轄權和情況而異，應與法律顧問討論。即使在司法轄區內，法律意見也可能不同。與律師合作，標語可提供以下部分或全部資訊：

- 請注意，系統只能登入或僅由特別授權的人員使用，可能還需要有關授權使用者的資訊。

- 請注意，任何未經授權使用系統均屬非法，可能受到民事和刑事處罰。
- 請注意，對系統的任何使用都可以在不另行通知的情況下進行記錄或監控，而生成的日誌可作為證據用於法庭。
- 當地法律要求的特定通知。

從安全的角度來看，登入標語不應包含有關路由器名稱、型號、軟體或所有權的任何特定資訊。這些資訊可能被惡意使用者濫用。

驗證、授權及記帳

身份驗證、授權和記帳(AAA)框架對於保護對網路裝置的互動式訪問至關重要。AAA框架提供可高度配置的環境，可以根據網路需求進行定製。

TACACS+ 驗證

TACACS+是Cisco IOS裝置可用於對遠端AAA伺服器進行管理使用者身份驗證的身份驗證協定。這些管理使用者可以通過SSH、HTTPS、telnet或HTTP訪問IOS裝置。

TACACS+驗證（更一般是AAA驗證）可以為每個網路管理員使用單獨的使用者帳戶。當您不依賴於單個共用密碼時，網路安全性會得到提高，您的責任會得到加強。

RADIUS是一種與TACACS+類似的通訊協定；但是，它只加密通過網路傳送的密碼。相反，TACACS+會加密整個TCP負載，包括使用者名稱和密碼。因此，當AAA伺服器支援TACACS+時，應優先使用TACACS+而不是RADIUS。請參閱TACACS+和RADIUS比較，以取得這兩個通訊協定的更詳細比較。

可以使用與以下範例類似的設定在Cisco IOS裝置上啟用TACACS+驗證：

```
!

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

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

先前的配置可用作組織特定的AAA身份驗證模板的起點。有關AAA配置的詳細資訊，請參閱身份驗證、授權和記帳。

方法清單是一個順序清單，描述了為驗證使用者而要查詢的驗證方法。通過方法清單，您可以指定一個或多個用於身份驗證的安全協定，從而確保在初始方法失敗時提供用於身份驗證的備份系統。Cisco IOS軟體使用第一個成功接受或拒絕使用者的方法。只有在早期方法由於伺服器不可用或配置不正確而失敗的情況下，才會嘗試後續方法。

有關配置命名方法清單的詳細資訊，請參閱用於身份驗證的命名方法清單。

驗證後援

如果所有已配置的TACACS+伺服器都不可用，則Cisco IOS裝置可以依靠輔助身份驗證協定。典型

配置包括：如果所有配置的TACACS+伺服器都不可用，則使用本地身份驗證或啟用身份驗證。

裝置內身份驗證選項的完整清單包括enable、local和line。這些選項各有優勢。最好使用使能加密碼，因為加密碼使用單向演算法進行雜湊，它本身比用於線路或本地身份驗證的7類密碼使用的加密演算法更安全。

但是，在支援對本地定義的使用者使用加密口令的Cisco IOS軟體版本上，最好回退到本地身份驗證。這樣，便可以為一個或多個網路管理員建立本地定義的使用者。如果TACACS+完全不可用，則每個管理員可以使用其本地使用者名稱和密碼。儘管此操作確實會加強網路管理員在TACACS+中斷時的責任制，但由於必須維護所有網路裝置上的本地使用者帳戶，因此大大增加了管理負擔。

此組態範例建立在上一個TACACS+驗證範例的基礎上，為了包括對於使用**enable secret**指令在本地設定的密碼的回退驗證：

```
!

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>
!
```

有關使用AAA進行回退身份驗證的詳細資訊，請參閱配置身份驗證。

使用7類密碼

最初設計為允許快速解密儲存的密碼，第7類密碼不是一種安全的密碼儲存形式。有許多工具可以輕鬆解密這些密碼。應避免使用7類密碼，除非在Cisco IOS裝置上使用的功能需要該密碼。

應儘可能使用型別9（加密）：

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

通過AAA驗證和使用Enhanced Password Security功能(該功能允許對通過**username**全域性配置命令在本地定義的使用者使用加密密碼)，可以方便移除此類密碼。如果不能完全禁止使用7類密碼，請考慮對這些密碼進行模糊處理，而不是加密。

有關刪除第7類密碼的詳細資訊，請參閱本文檔的一般管理平面強化*部分*。

TACACS+命令授權

使用TACACS+和AAA的命令授權提供一種機制，允許或拒絕管理使用者輸入的每個命令。當使用者輸入EXEC命令時，Cisco IOS會將每個命令傳送到配置的AAA伺服器。然後，AAA伺服器使用其配置的策略來允許或拒絕該特定使用者的命令。

此配置可以新增到前面的AAA身份驗證示例中以實現命令授權：

```
!
```

```
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
!
```

有關命令授權的詳細資訊，請參閱配置授權。

TACACS+指令計量

配置後，AAA命令記帳會向已配置的TACACS+伺服器傳送有關輸入的每個EXEC命令的資訊。傳送到TACACS+伺服器的資訊包括執行的命令、執行的日期以及輸入該命令的使用者的使用者名稱。RADIUS不支援指令計量。

此配置示例啟用在許可權級別0、1和15輸入的EXEC命令的AAA命令記帳。此配置基於包括TACACS伺服器配置的先前示例。

```
!

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
!
```

有關AAA記帳配置的詳細資訊，請參閱配置記帳。

冗餘AAA伺服器

在環境中使用的AAA伺服器應冗餘並以容錯方式部署。這有助於確保在AAA伺服器不可用時能夠進行互動式管理訪問，例如SSH。

設計或實施冗餘AAA伺服器解決方案時，請記住以下注意事項：

- 發生潛在網路故障時AAA伺服器的可用性
- AAA伺服器的地理位置分散
- 在穩態和故障狀態下載入各個AAA伺服器
- 網路接入伺服器和AAA伺服器之間的網路延遲
- AAA伺服器資料庫同步

有關詳細資訊，請參閱部署訪問控制伺服器。

強化簡單網路管理協定

本節重點介紹幾種可用於保護IOS裝置內SNMP部署的方法。正確保護SNMP至關重要，這樣才能保護網路資料和傳輸此資料的網路裝置的機密性、完整性和可用性。SNMP可提供有關網路裝置健康狀況的許多資訊。應保護此資訊免受惡意使用者的侵害，這些使用者希望利用此資料對網路執行攻擊。

SNMP社群字串

社群字串是套用到IOS裝置的密碼，用於限制對裝置上SNMP資料的存取許可權（包括唯讀和讀取/寫入許可權）。這些社群字串，如同所有密碼，應謹慎選取，以確保其並非無關緊要。應根據網路安全策略定期更改社群字串。例如，當網路管理員更改角色或離開公司時，應更改字串。

這些配置行配置只讀社群字串READONLY和讀寫社群字串READWRITE:

```
!

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

> **附註**：已選擇之前的社群字串範例，以清楚說明這些字串的使用方式。對於生產環境，應謹慎選擇社群字串，該字串應包含一系列字母、數字和非字母數字元號。有關選擇非簡單密碼的詳細資訊，請參閱建立強密碼的建議。

有關此功能的詳細資訊，請參閱IOS SNMP命令參考。

使用ACL的SNMP社群字串

除了社群字串之外，還應該套用ACL，進一步限制對特定來源IP位址群組的SNMP存取許可權。此配置限制對位於192.168.100.0/24地址空間中的終端主機裝置的SNMP只讀訪問，並限制對位於192.168.100.1的終端主機裝置的SNMP讀寫訪問。

> **附註**：這些ACL允許的裝置需要正確的社群字串才能存取要求的SNMP資訊。

```
!

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
!
```

有關此功能的詳細資訊，請參閱《Cisco IOS Network Management命令參考》中的snmp-server community。

基礎架構ACL

基礎架構ACL(iACL)可以部署，以確保只有具有受信任IP位址的終端主機才能將SNMP流量傳送到IOS裝置。iACL應包含拒絕在UDP埠161上使用未授權SNMP資料包的策略。

有關iACL使用的詳細資訊，請參閱本文檔的使用基礎架構ACL限制對網路的訪問*部分*。

SNMP檢視

SNMP檢視是一項安全功能，可允許或拒絕訪問某些SNMP MIB。一旦使用**snmp-server community**

community-string view全域性配置命令建立檢視並將其應用到社群字串後，如果您訪問MIB資料，則將限制您對該檢視定義的許可權。如果適用，建議您使用檢視將SNMP使用者限制到所需的資料。

此配置示例使用社群字串LIMITED將SNMP訪問限製為位於系統組中的MIB資料：

```
!

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

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

如需詳細資訊，請參閱設定SNMP支援。

SNMP版本3

SNMP第3版(SNMPv3)由RFC3410、RFC3411、RFC3412、RFC3413、RFC3414和RFC3415定義，是一種可互操作的基於標準的網路管理通訊協定。SNMPv3提供對裝置的安全訪問，因為它通過網路驗證資料包並選擇性地對其進行加密。在支援的地方，SNMPv3可用於在部署SNMP時新增另一個安全層。SNMPv3包含三個主要配置選項：

- **no auth** — 此模式不需要對SNMP封包進行任何驗證或加密
- **auth** — 此模式要求對未加密的SNMP封包進行驗證
- **priv** — 此模式要求對每個SNMP資料包進行身份驗證和加密（隱私）

必須存在授權引擎ID，才能使用SNMPv3安全機制（身份驗證或身份驗證和加密）處理SNMP資料包；預設情況下，引擎ID在本地生成。引擎ID可以使用**show snmp engineID**命令顯示，如以下範例所示：

```
router#show snmp engineID
Local SNMP engineID: 800000090300000152BD35496
Remote Engine ID IP-addr Port
```

附註：如果更改了engineID，則必須重新配置所有SNMP使用者帳戶。

下一步是配置SNMPv3組。此命令使用SNMP伺服器組AUTHGROUP配置用於SNMPv3的Cisco IOS裝置，並僅使用**auth**關鍵字為此組啟用身份驗證：

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

此命令使用SNMP伺服器組PRIVGROUP配置用於SNMPv3的Cisco IOS裝置，並使用**priv**關鍵字為此組啟用身份驗證和加密：

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

此命令使用MD5身份驗證密碼**authpassword**和3DES加密密碼**privpassword**配置SNMPv3使用者

snmpv3使用者：

```
!

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

請注意，**snmp-server user**配置命令不會按照RFC 3414的要求顯示在裝置的配置輸出中；因此，無法從配置中檢視使用者密碼。若要檢視已設定的使用者，請輸入**show snmp user**命令，如以下範例所示：

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

有關此功能的詳細資訊，請參閱配置SNMP支援。

管理平面保護

Cisco IOS軟體中的管理平面保護(MPP)功能可用於協助保護SNMP，因為它會限制SNMP流量在裝置上終止的介面。MPP功能允許管理員將一個或多個介面指定為管理介面。僅允許管理流量通過這些管理介面進入裝置。啟用MPP後，除指定管理介面外，其他介面均不會接受發往裝置的網路管理流量。

請注意，MPP是CPPr功能的子集，需要支援CPPr的IOS版本。有關CPPr的詳細資訊，請參閱瞭解控制平面保護。

在本示例中，使用MPP僅限制對FastEthernet 0/0介面的SNMP和SSH訪問：

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

有關詳細資訊，請參閱管理平面保護功能指南。

記錄最佳實踐

通過事件記錄，您可以檢視Cisco IOS裝置的運行情況以及部署該裝置的網路。Cisco IOS軟體提供多種靈活的日誌記錄選項，可幫助實現組織的網路管理和可視性目標。

以下各節提供一些基本的日誌記錄最佳實踐，可幫助管理員成功利用日誌記錄，同時將日誌記錄對Cisco IOS裝置的影響降至最低。

將日誌傳送到中心位置

建議您將日誌記錄資訊傳送到遠端系統日誌伺服器。這樣可以更有效地關聯和審計網路裝置中的網路和安全事件。請注意，UDP以明文形式傳輸系統日誌消息並不可靠。因此，應擴展網路為管理流量提供的任何保護（例如加密或帶外訪問），以便包括系統日誌流量。

此配置示例配置Cisco IOS裝置以將日誌記錄資訊傳送到遠端系統日誌伺服器：

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

有關日誌關聯的詳細資訊，請參閱使用防火牆和IOS路由器系統日誌事件識別事件。

12.4(15)T中整合了Logging to Local Involatile Storage(ATA Disk)功能，該功能最初是在12.0(26)S中引入的，它允許將系統日誌記錄消息儲存在高級技術附件(ATA)快閃記憶體磁碟上。ATA驅動器上儲存的消息在路由器重新啟動後仍然存在。

此配置行將日誌記錄消息的134,217,728位元組(128 MB)配置到ATA快閃記憶體(disk0)的syslog目錄，並指定16,384位元組的檔案大小：

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

在將日誌記錄消息寫入ATA磁碟上的檔案之前，Cisco IOS軟體會檢查是否有足夠的磁碟空間。如果不是，則刪除最舊的日誌記錄消息檔案（按時間戳），並儲存當前檔案。檔名格式為**log_month:day:year::time**。

附註：ATA快閃記憶體驅動器磁碟空間有限，因此需要對其進行維護以避免覆蓋儲存的資料。

本示例展示如何在維護過程中將日誌記錄消息從路由器ATA快閃記憶體磁碟複製到FTP伺服器192.168.1.129上的外部磁碟：

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

有關此功能的詳細資訊，請參閱記錄到本地非易失性儲存（ATA磁碟）。

日誌記錄級別

由Cisco IOS裝置生成的每條日誌消息都分配了從0級、緊急事件到7級、調試的八個嚴重性之一。除非有特殊要求，否則建議您避免在第7級記錄。在第7級記錄會導致裝置上的CPU負載增加，從而導致裝置和網路不穩定。

全域性配置命令**logging trap**級別用於指定將哪些日誌記錄消息傳送到遠端系統日誌伺服器。指定的級別表示傳送的最低嚴重性消息。對於緩衝日誌記錄，使用**logging buffered** level命令。

此配置示例將傳送到遠端系統日誌伺服器和本地日誌緩衝區的日誌消息限製為從6（資訊）到0（緊急）的嚴重性：

```
!

logging trap 6
logging buffered 6
!
```

如需詳細資訊，請參閱疑難排解、故障管理和記錄。

不登入到控制檯或監控會話

通過Cisco IOS軟體，可以將日誌消息傳送到監控會話(監控會話是已發出**terminal monitor**EXEC命令的互動管理會話)以及控制檯。但是，這可能會增加IOS裝置的CPU負載，因此不建議這樣做。相反，建議您將日誌記錄資訊傳送到本地日誌緩衝區，該緩衝區可以使用**show logging**命令檢視。

使用全域性配置命令**no logging console**和**no logging monitor**禁用登入到控制檯和監控器會話。此組態範例顯示以下命令的使用方式：

```
!

no logging console
no logging monitor
!
```

有關全域性配置命令的詳細資訊，請參閱Cisco IOS網路管理命令參考。

使用緩衝日誌記錄

Cisco IOS軟體支援使用本地日誌緩衝區，以便管理員可以檢視本地生成的日誌消息。強烈建議使用緩衝日誌記錄而不是記錄到控制檯或監控器會話。

配置緩衝日誌記錄時，有兩個相關的配置選項：日誌記錄緩衝區大小和儲存在緩衝區中的消息嚴重性。日誌記錄緩衝區**的大小**使用全域性配置命令**logging buffered size進行**配置。使用logging buffered severity命令配置緩衝區中包含的最低嚴重性。管理員可以通過**show logging** EXEC命令檢視日誌記錄緩衝區的內容。

此配置示例包括配置16384位元組的日誌記錄緩衝區，以及嚴重性為6（資訊），表示儲存級別為0（緊急）至6（資訊）的消息：

```
!

logging buffered 16384 6
!
```

有關緩衝日誌記錄的詳細資訊，請參閱Cisco IOS網路管理命令參考。

配置日誌記錄源介面

為了在收集和審閱日誌消息時提供更高水準的一致性，建議您靜態配置日誌記錄源介面。通過**logging source-interface**介面命令完成，靜態配置日誌記錄源介面可確保從單個Cisco IOS裝置傳送的所有日誌記錄消息中顯示相同的IP地址。為了提高穩定性，建議您使用環回介面作為日誌記錄源。

此配置示例說明如何使用**logging source-interface** interface global configuration命令來指定loopback 0介面的IP地址用於所有日誌消息：

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

*有關詳*細資訊，請參閱Cisco IOS命令參考。

配置日誌記錄時間戳

日誌記錄時間戳的配置有助於跨網路裝置關聯事件。實施正確且一致的日誌記錄時間戳配置以確保能夠關聯日誌記錄資料非常重要。日誌記錄時間戳應配置為包括精度為毫秒的日期和時間，並包括裝置上正在使用的時區。

本示例包括在協調世界時(UTC)區域內以毫秒精度配置日誌時間戳：

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

如果您不希望記錄相對於UTC的時間，可以配置特定的本地時區，並將該資訊配置為顯示在生成的日誌消息中。此範例顯示太平洋標準時間(PST)區域的裝置組態：

```
!

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

Cisco IOS軟體組態管理

Cisco IOS軟體包括多種功能，可在Cisco IOS裝置上啟用某種形式的配置管理。這些功能包括將配置存檔、將配置回滾到先前版本以及建立詳細的配置更改日誌的功能。

配置替換和配置回滾

在Cisco IOS軟體版本12.3(7)T及更高版本中，配置替換和配置回滾功能允許您在裝置上存檔Cisco IOS裝置配置。可以手動或自動儲存此歸檔檔案中的配置，以便使用**configure replace** filename命令替換當前運行的配置。這與**copy** filename **running-config**命令相反。**configure replace** filename命令取代運行配置，而不是通過**copy**命令執行的合併。

建議您在網路中的所有Cisco IOS裝置上啟用此功能。啟用後，管理員可以使用**archive config**特權EXEC命令將當前運行配置新增到歸檔中。可以使用**show archive** EXEC命令檢視歸檔的配置。

此示例說明了自動配置歸檔的配置。此示例指示Cisco IOS裝置將歸檔的配置儲存為disk0上名為archived-config-N的檔案：檔案系統，最多保持14個備份，並在管理員發出**write memory** EXEC命令時每天存檔一次（1440分鐘）。

```
!

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

雖然配置存檔功能最多可以儲存14個備份配置，但建議您在使用**maximum**命令之前考慮空間要求。

獨佔配置更改訪問

新增到Cisco IOS軟體版本12.3(14)T中的獨佔配置更改訪問功能可確保僅有一名管理員在給定時間對Cisco IOS裝置進行配置更改。此功能有助於消除同時更改相關配置元件所造成的不利影響。此功能使用全域性配置命令**configuration mode exclusive**模式進行配置，並在以下兩種模式之一中運行

：自動和手動。在自動模式下，當管理員發出**configure terminal** EXEC命令時，配置會自動鎖定。在手動模式下，管理員使用**configure terminal lock**命令以在配置進入配置模式時鎖定配置。

此範例說明此功能用於自動組態鎖定的組態：

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

Cisco IOS軟體彈性組態

在Cisco IOS軟體版本12.3(8)T中新增了彈性配置功能，該功能可以安全儲存Cisco IOS裝置當前使用的Cisco IOS軟體映像和裝置配置的副本。啟用此功能後，將無法更改或刪除這些備份檔案。建議您啟用此功能，以防止無意和惡意嘗試刪除這些檔案。

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

啟用此功能後，便可以恢復已刪除的組態或Cisco IOS軟體映像。可以使用**show secure boot** EXEC命令顯示此功能的當前運行狀態。

數位簽章的思科軟體

在Cisco 1900、2900和3900系列路由器的Cisco IOS軟體版本15.0(1)M中新增了數位簽章思科軟體功能，該功能通過使用安全的不對稱（公鑰）加密技術，便於使用數位簽章並因此受信任的Cisco IOS軟體。

數位簽章的影象攜帶其自身的加密（私鑰）雜湊。在檢查後，裝置使用相應的公鑰從它在其金鑰儲存中的金鑰解密該雜湊，並且還計算它自己的影象的雜湊。如果解密的雜湊值與計算的影象雜湊值匹配，則說明影象未被篡改，因此可以信任影象。

數位簽章的思科軟體金鑰由金鑰的型別和版本標識。金鑰可以是特殊、生產或全反金鑰型別。生產和特殊金鑰型別具有一個關聯的金鑰版本，每當撤消和替換金鑰時，該版本就會按字母順序遞增。當您使用數位簽章思科軟體功能時，ROMMON和常規Cisco IOS映像都使用特殊或生產金鑰進行簽名。ROMMON映像可以升級，並且必須使用與載入的特殊或生產映像相同的金鑰進行簽名。

此命令使用裝置金鑰庫中的金鑰驗證快閃記憶體中的映像c3900-universalk9-mz.SSA的完整性：

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

Cisco Catalyst 4500 E系列交換機的Cisco IOS XE 3.1.0.SG中也整合了數位簽章思科軟體功能。

有關此功能的詳細資訊，請參閱數位簽章的思科軟體。

在Cisco IOS軟體版本15.1(1)T和更新版本中，引入了數位簽名的思科軟體的金鑰替代功能。金鑰替換和撤銷從平台的金鑰儲存中替換並刪除用於數位簽章思科軟體檢查的金鑰。只有特殊和生產金鑰在金鑰受損的情況下才能吊銷。

用於（特殊或生產）影象的新（特殊或生產）金鑰來自用於撤銷先前特殊或生產金鑰的（生產或撤銷）影象。使用預儲存在平台上的滾動更新金鑰來驗證撤銷映像的完整性。滾動更新金鑰不會更改。當您撤銷生產金鑰時，在載入了撤銷映像後，它攜帶的新金鑰將新增到金鑰儲存中，並且只要ROMMON映像升級且新生產映像啟動，相應的舊金鑰就可以被撤銷。撤銷特殊金鑰時，將載入生

產映像。此影象將新增新的特殊金鑰，並且可以撤銷舊的特殊金鑰。升級ROMMON後，可以引導新的特殊映像。

此示例說明撤銷特殊金鑰。這些命令將新的特殊金鑰新增到當前生產映像中的金鑰儲存中，將新的ROMMON映像(C3900_rom-monitor.srec.SSB)複製到儲存區域(usbflash0:)，升級ROMMON檔案，並撤消舊的特殊金鑰：

```
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
```

然後，可以將新的特殊映像(c3900-universalk9-mz.SSB)複製到要載入的快閃記憶體中，並使用新增的特殊金鑰(.SSB)驗證映像的簽名：

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

執行Cisco IOS XE軟體的Catalyst 4500 E系列交換器不支援金鑰撤銷和替換，雖然這些交換器支援的是數位簽名的思科軟體功能。

*有關此功能*的更多資訊，請參閱數位簽章的思科軟體指南的數位簽章的思科軟體金鑰撤銷和替換部分。

組態變更通知和記錄

在Cisco IOS軟體版本12.3(4)T中新增的配置更改通知和日誌記錄功能可以記錄對Cisco IOS裝置所做的配置更改。日誌儲存在Cisco IOS裝置上，包含更改者的使用者資訊、輸入的配置命令以及更改的時間。此功能是使用**logging enable** configuration change logger configuration mode命令啟用的。可選命令**hidekeys**和**logging size**條目用於改進預設配置，因為它們會阻止密碼資料的日誌記錄並增加更改日誌的長度。

建議您啟用此功能，以便可以更輕鬆地瞭解Cisco IOS裝置的配置更改歷史記錄。此外，建議您使用**notify syslog**配置命令，以在進行配置更改時生成系統日誌消息。

```
!

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

啟用配置更改通知和日誌記錄功能後，可使用特權EXEC命令**show archive log config all**檢視配置日誌。

控制平面

控制平面功能包括網路裝置之間通訊的協定和過程，用於將資料從源裝置移動到目的裝置。其中包括邊界閘道通訊協定等路由通訊協定，以及ICMP和資源保留通訊協定(RSVP)等通訊協定。

管理和資料平面中的事件不對控制平面產生負面影響，這一點非常重要。如果資料平面事件（例如

DoS攻擊）影響控制平面，則整個網路可能變得不穩定。此有關Cisco IOS軟體功能和配置的資訊有助於確保控制平面的恢復能力。

一般控制平面加固

保護網路裝置的控制平面至關重要，因為控制平面可確保管理和資料平面得到維護和運行。如果控制平面在安全事件期間變得不穩定，則您可能無法恢復網路的穩定性。

在許多情況下，您可以禁用介面上特定型別消息的接收和傳輸，以最大程度減少處理不必要資料包所需的CPU負載。

IP ICMP重新導向

路由器可以在同一介面上接收和傳輸資料包時生成ICMP重定向消息。在這種情況下，路由器將轉送封包並向原始封包的傳送者傳送ICMP重新導向訊息。此行為允許傳送者繞過路由器，將未來的封包直接轉送到目的地（或靠近目的地的路由器）。 在正常運行的IP網路中，路由器僅將重定向傳送到其本地子網上的主機。換句話說，ICMP重新導向決不能超越第3層邊界。

ICMP重定向消息有兩種型別：重定向主機地址，然後重定向整個子網。惡意使用者可以通過不斷向路由器傳送資料包來利用路由器傳送ICMP重定向的能力，從而迫使路由器使用ICMP重定向消息做出響應，並造成對路由器的CPU和效能的不利影響。為了防止路由器傳送ICMP重定向，請使用**no ip redirects**介面配置命令。

ICMP不可達

使用介面存取清單進行過濾會誘使ICMP無法到達訊息傳輸回已過濾流量的來源。生成這些消息會提高裝置的CPU利用率。在Cisco IOS軟體中，預設情況下，ICMP無法到達的產生限製為每500毫秒產生一個封包。可以使用介面組態指令**no ip unreachables**停用ICMP無法到達訊息產生。使用全域性配置命令**ip icmp rate-limit unreachable** interval-in-ms，可以從預設設定更改ICMP無法到達速率限制。

代理 ARP

代理ARP是一種技術，利用這種技術，裝置（通常是路由器）應答針對其他裝置的ARP請求。通過「偽裝」身份，路由器承擔將資料包路由到實際目的地的責任。代理ARP可以幫助子網中的機器到達遠端子網，而無需配置路由或預設網關。代理ARP在RFC 1027中定義。

代理ARP利用率存在幾個缺點。它可能導致網段上的ARP流量增加、資源耗盡和中間人攻擊。代理ARP呈現資源耗盡攻擊向量，因為每個代理ARP請求消耗的記憶體量很小。如果攻擊者傳送大量ARP請求，則攻擊者能夠耗盡所有可用記憶體。

中間人攻擊使網路中的主機能夠偽裝路由器的MAC地址，從而導致毫無防範的主機向攻擊者傳送流量。可以使用介面組態指令**no ip proxy-arp**停用代理ARP。

有關此功能的詳細資訊，請參閱啟用代理ARP。

限制控制平面流量對CPU的影響

保護控制平面至關重要。由於應用程式效能和終端使用者體驗可能會受到影響，而不存在資料和管理流量，因此控制平面的生存能力可確保其他兩個平面得到維護和運行。

瞭解控制平面流量

為了正確保護Cisco IOS裝置的控制平面，必須瞭解CPU進行進程交換的流量型別。處理交換流量通常包括兩種不同型別的流量。第一種型別的流量定向到Cisco IOS裝置，必須直接由Cisco IOS裝置CPU處理。此流量包括*接收鄰接流量*類別。此流量在Cisco Express Forwarding(CEF)表中包含一專案，因此下一個路由器躍點是裝置本身，這在**show ip cef** CLI輸出中以receive一詞表示。此指示適用於需要由Cisco IOS裝置CPU直接處理的任何IP地址，包括介面IP地址、組播地址空間和廣播地址空間。

CPU處理的第二種流量型別是資料平面流量 — 目的地超過Cisco IOS裝置本身的流量 — 這需要CPU進行特殊處理。雖然並非影響資料平面流量的詳盡清單，但這些型別的流量是進程交換的，因此可能會影響控制平面的操作：

- **訪問控制清單日**志記錄 — ACL日誌記錄流量包括因使用log關鍵字的ACE的匹配（允許或拒絕）而生成的任何資料包。
- **單點傳送反向路徑轉送（單點傳送RPF）** — 單點傳送RPF（與ACL結合使用）可能會導致某些封包的程式交換結果。
- **IP選項** — 任何包含選項的IP資料包都必須由CPU處理。
- **分段** — 需要分段的任何IP資料包都必須傳遞到CPU進行處理。
- **生存時間(TTL)到期** - TTL值小於或等於1的資料包需要傳送網際網路控制消息協定超時（ICMP型別11，代碼0）消息，這將導致CPU處理。
- **ICMP不可達**項 — 由於路由、MTU或過濾而導致ICMP無法到達消息的資料包由CPU處理。
- **需要ARP請求的流**量 — 不存在ARP條目的目標需要CPU進行處理。
- **非IP流量** — 所有非IP流量均由CPU處理。

此清單詳細介紹了確定Cisco IOS裝置CPU處理哪些型別的流量的幾種方法：

- **show ip cef**命令會提供CEF表中包含的每個IP首碼的下一跳資訊。如前所述，包含接收作為「下一跳」的條目將被視為接收鄰接關係，指示流量必須直接傳送到CPU。
- **show interface switching**命令會提供有關裝置進行處理交換的封包數量的資訊。
- **show ip traffic**命令會提供有關IP封包數量的資訊：

  本地目的地（即接收鄰接流量）包含選項需要分段傳送到廣播地址空間傳送到組播地址空間

- 可以使用**show ip cache flow**命令識別接收鄰接流量。任何目的地為Cisco IOS裝置的流量都有一個目的地介面(DstIf)為本地。
- **控制平**面原則制定可用於識別到達Cisco IOS裝置控制平面的流量的型別和速率。控制平面策略可通過使用粒度分類ACL、日誌記錄以及使用**show policy-map control-plane**命令來執行。

基礎架構ACL

基礎架構ACL(iACL)會限制與網路裝置的外部通訊。基礎架構ACL詳見本檔案的使用基礎架構ACL限制對網路的訪問一節。

建議您實施iACL以保護所有網路裝置的控制平面。

接收 ACL

對於分散式平台，接收ACL(rACL)可以是適用於Cisco IOS軟體版本12.0(21)S2(適用於12000(GSR))、12.0(24)S（適用於7500）和12.0(31)S(適用於10720)的選項。rACL會在流量影響路由處理器之前，保護裝置免受有害流量的影響。接收ACL僅用於保護配置它的裝置，而傳輸流量不受rACL的影響。因此，以下示例ACL條目中使用的目標IP地址any僅引用路由器的物理或虛擬IP地址。接收ACL也被視為網路安全的最佳實踐，應視為良好網路安全性的長期補充。

以下是已寫入的接收路徑ACL，允許來自192.168.100.0/24網路上受信任主機的SSH（TCP連線埠22）流量：

```
!
!--- 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
!
```

請參閱 GSR：接收存取控制清單，以幫助識別並允許到裝置的合法流量，以及拒絕所有不需要的封包。

CoPP

CoPP功能也可用於限制發往基礎架構裝置的IP資料包。在此示例中，僅允許來自受信任主機的SSH流量到達Cisco IOS裝置CPU。

> **附註**：丟棄來自未知或不可信IP地址的流量可能會阻止具有動態分配IP地址的主機連線到Cisco IOS裝置。

```
!
```

```
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
!
```

在上一個CoPP示例中，將未授權資料包與permit操作匹配的ACL條目導致策略對映丟棄功能丟棄這些資料包，而與deny操作匹配的資料包不會受到策略對映丟棄功能的影響。

CoPP可用於Cisco IOS軟體版本系列12.0S、12.2SX、12.2S、12.3T、12.4和12.4T。

請參閱部署控制平面策略，*以瞭解更多有關CoPP功能的配置和使用資訊。*

控制平面保護

Cisco IOS軟體版本12.4(4)T中引入的控制平面保護(CPPr)可用於限制或管制目的地為Cisco IOS裝置CPU的控制平面流量。與CoPP類似，CPPr能夠更精細地限制流量。CPPr將聚合控制平面分為三個單獨的控制平面類別，稱為子介面。存在用於主機、傳輸和CEF-Exception流量類別的子介面。此外，CPPr還包括以下控制平面保護功能：

- **連線埠過濾功**能 — 此功能提供管制和捨棄傳送到關閉或非偵聽TCP或UDP連線埠的封包。

- Queue-thresholding feature — 此功能限制控制平面IP輸入隊列中允許的指定協定的資料包數。

請參閱控制平面保護*和*瞭解控制平面保護(CPPr)，*以瞭解更多有關CPPr功能的配置和使用的資訊。*

硬體速率限制器

Cisco Catalyst 6500系列監督器引擎32和Supervisor引擎720支援針對特殊網路方案的平台特定的、基於硬體的速率限制器(HWRL)。這些硬體速率限制器稱為特殊情況速率限制器，因為它們涵蓋一組特定的預定義的IPv4、IPv6、單播和多播DoS方案。HWRL可以保護Cisco IOS裝置免受需要CPU處理資料包的各種攻擊。

預設情況下啟用多個HWRL。有關詳細資訊，請參閱PFC3基於硬體的速率限制器預設設定。

有關HWRL的詳細資訊，請參閱PFC3上的基於硬體的速率限制器。

安全BGP

邊界網關協定(BGP)是Internet的路由基礎。因此，任何組織只要滿足過適度的連線要求，通常都會使用BGP。BGP經常成為攻擊者的攻擊目標，因為它在較小的組織*中是無處不在*的，並且設定並忘記BGP配置的性質。但是，可使用許多BGP特定安全功能來提高BGP配置的安全性。

這提供了最重要的BGP安全功能的概述。如果適用，還會提供配置建議。

基於TTL的安全保護

每個IP資料包都包含一個1位元組欄位，稱為生存時間(TTL)。 IP資料包經過的每個裝置都會將此值減一。起始值因作業系統而異，通常範圍從64到255。資料包的TTL值達到零時將丟棄。

一種稱為通用TTL型安全機制(GTSM)和BGP TTL安全破解(BTSH)的基於TTL的安全保護利用IP封包的TTL值，以確保收到的BGP封包來自直接連線的同儕節點。此功能通常需要來自對等路由器的協調；但是，一旦啟用，它可以完全抵禦許多針對BGP的基於TCP的攻擊。

使用**neighbor** BGP路由器配置命令的**ttl-security**選項啟用GTSM for BGP。此範例說明此功能的設定：

```
!

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

接收BGP封包時，會檢查TTL值，該值必須大於或等於255減去指定的躍點計數。

使用MD5的BGP對等驗證

使用MD5的對等驗證會為作為BGP會話一部分傳送的每個資料包建立MD5摘要。具體來說，IP和TCP報頭、TCP負載和金鑰的部分用於生成摘要。

然後，所建立的摘要儲存在TCP選項Kind 19中，該選項是由RFC 2385專門為此而建立的。接收BGP的揚聲器使用相同的演算法和金鑰來重新生成消息摘要。如果接收的摘要和計算的摘要不同，則丟棄資料包。

使用MD5的對等身份驗證是使用**neighbor** BGP路由器配置命令的**password**選項配置的。此命令的使用說明如下：

```
!

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

請參閱鄰居路由器身份驗證，*以瞭解有關使用MD5的BGP對等身份驗證的詳細資訊。*

配置最大字首

BGP字首由路由器儲存在記憶體中。路由器必須保留的字首越多，BGP必須使用的記憶體就越多。在某些配置中，可以儲存所有Internet字首的子集，例如在僅利用提供商客戶網路的預設路由或路由的配置中。

為防止記憶體耗盡，必須配置每個對等體接受的最大字首數。建議為每個BGP對等點配置限制。

使用**neighbor maximum-prefix** BGP路由器配置命令配置此功能時，需要一個引數：對等體關閉之前接受的最大字首數。或者，也可以輸入1到100之間的數字。此數字表示傳送日誌消息時的最大字首值的百分比。

```
!

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

請參閱設定BGP最大首碼功能*以瞭解更多有關每個對等體最大首碼的資訊。*

使用字首清單過濾BGP字首

字首清單允許網路管理員允許或拒絕通過BGP傳送或接收的特定字首。應儘可能使用首碼清單，以確保網路流量透過預期路徑傳送。應在入站和出站方向將字首清單應用於每個eBGP對等體。

配置的字首清單將傳送或接收的字首限製為網路路由策略明確允許的字首。如果由於收到大量字首而無法執行該操作，則應配置字首清單以專門阻止已知的錯誤字首。這些已知錯誤字首包括未分配的IP地址空間和RFC 3330為內部或測試目的保留的網路。出站字首清單應配置為僅專門允許組織要通告的字首。

此配置示例使用字首清單來限制獲知和通告的路由。具體而言，字首清單BGP-PL-INBOUND只允許預設路由入站，並且字首192.168.2.0/24是BGP-PL-OUTBOUND允許通告的唯一路由。

```
!

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
!
```

請參閱使用外部BGP連線到服務提供商，*以瞭解BGP字首過濾的完整覆蓋範圍。*

使用自主系統路徑存取清單篩選BGP字首

BGP自治系統(AS)路徑存取清單允許使用者根據首碼的AS-path屬性篩選已接收和通告的字首。此功能可搭配首碼清單使用，以建立一套健全的篩選條件。

此配置示例使用AS路徑訪問清單將入站字首限製為遠端AS發起的入站字首，將出站字首限製為本地自治系統發起的出站字首。來自所有其他自治系統的字首將被過濾，不會安裝在路由表中。

```
!

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
!
```

安全內部閘道通訊協定

網路正確轉發流量並從拓撲變化或故障中恢復的能力取決於拓撲的準確檢視。您通常可以運行內部閘道通訊協定(IGP)以提供此檢視。預設情況下，IGP是動態的，會發現與正在使用的特定IGP通訊的其他路由器。IGP還發現可在網路鏈路故障期間使用的路由。

以下小節概述了最重要的IGP安全功能。在適當時，會提供涵蓋路由資訊協定版本2(RIPv2)、增強型內部網關路由協定(EIGRP)和開放最短路徑優先(OSPF)的建議和示例。

使用消息摘要5的路由協定身份驗證和驗證

如果無法保護路由資訊交換，則攻擊者可以將錯誤的路由資訊引入網路。通過在路由器之間使用口令身份驗證和路由協定，您可以幫助確保網路安全。但是，由於此身份驗證是以明文形式傳送的，因此攻擊者很容易破壞此安全控制。

通過在身份驗證過程中新增MD5雜湊功能，路由更新不再包含明文密碼，並且路由更新的全部內容更不易被篡改。但是，如果選擇了弱密碼，MD5身份驗證仍然容易遭受暴力攻擊和字典攻擊。建議您使用具有足夠隨機化的密碼。因為MD5身份驗證與密碼身份驗證相比更安全，所以這些示例特定於MD5身份驗證。IPSec也可用於驗證和保護路由協定，但這些示例並未詳細介紹其用途。

EIGRP和RIPv2將金鑰鏈用作配置的一部分。請參閱key，*瞭解有關配置和使用金鑰鏈的詳細資訊。*

以下是使用MD5的EIGRP路由器身份驗證的配置示例：

```
!

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>
!
```

以下是RIPv2的MD5路由器身份驗證配置示例。RIPv1不支援身份驗證。

```
!

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

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

以下是使用MD5進行OSPF路由器身份驗證的配置示例。OSPF不使用金鑰鏈。

```
!

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
!
```

有關詳細資訊，請參閱配置OSPF。

Passive-Interface命令

通過使用有助於控制路由資訊通告的**passive-interface**命令，可以緩解資訊洩漏或向IGP引入虛假資訊。建議您不要將任何資訊通告給不受您的管理控制的網路。

此範例示範此功能的使用方式：

```
!

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

路由篩選

為了降低在網路中引入虛假路由資訊的可能性，必須使用路由過濾。與**passive-interface**路由器配置命令不同，一旦啟用路由過濾，路由就會在介面上發生，但通告或處理的資訊是有限的。

對於EIGRP和RIP，使用帶有**out**關鍵字的**distribute-list**命令可限制通告的資訊，而使用**in**關鍵字可限制處理哪些更新。**distribute-list**命令可用於OSPF，但它不會阻止路由器傳播已過濾的路由。您可以使用**area filter-list**指令。

此EIGRP示例使用**distribute-list**命令和字首清單過濾出站通告：

```
!

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>
!
```

此EIGRP示例使用字首清單過濾入站更新：

```
!

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>
!
```

有關如何控制路由更新的通告和處理過程的詳細資訊，請參閱配置IP路由協定無關功能。

此OSPF示例使用OSPF特定的**area filter-list命令的字首列**表：

```
!

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

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

工藝路線流程資源消耗

路由協定字首由路由器儲存在記憶體中，並且資源消耗會隨著路由器必須保留的附加字首而增加。為防止資源耗盡，必須配置路由協定以限制資源消耗。如果使用Link State Database Overload Protection（鏈路狀態資料庫過載保護）功能，OSPF可能會出現這種情況。

此示例演示了OSPF鏈路狀態資料庫過載保護功能的配置：

```
!

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

有關OSPF鏈路狀態資料庫過載保護的詳細資訊，請參閱限制OSPF進程的自生成LSA數。

安全第一躍點備援通訊協定

第一躍點備援通訊協定(FHRP)為擔任預設閘道的裝置提供復原力和備援。這種情況和這些協定在這樣的環境中很常見：一對第3層裝置為包含伺服器或工作站的網路段或VLAN集提供預設網關功能。

閘道負載平衡通訊協定(GLBP)、熱待命路由器通訊協定(HSRP)和虛擬路由器備援通訊協定(VRRP)都是FHRP。預設情況下，這些協定與未經身份驗證的通訊通訊。此類通訊允許攻擊者偽裝成講FHRP的裝置，承擔網路上的預設網關角色。此接管操作將允許攻擊者執行中間人攻擊並攔截退出網路的所有使用者流量。

為了防止此類攻擊，Cisco IOS軟體支援的所有FHRP都包含具有MD5或文字字串的驗證功能。由於未經驗證的FHRP所帶來的威脅，建議這些協定的例項使用MD5身份驗證。此配置示例演示了GLBP、HSRP和VRRP MD5身份驗證的使用：

```
!

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
!
```

資料平面

儘管資料平面負責將資料從源移動到目的地，但在安全環境中，資料平面是三個平面中最不重要的部分。因此，當您保護網路裝置時，保護管理和控制平面優先於資料平面非常重要。

但是，在資料平面本身，有許多功能和配置選項可以幫助保護流量。以下各節詳細說明了這些功能和選項，以便您可以更輕鬆地保護網路。

一般資料平面強化

絕大部分資料平面流量流經網路，具體取決於網路的路由配置。但是，IP網路功能可用於更改資料包在網路中的路徑。IP選項（特別是源路由選項）等功能構成了當今網路的安全挑戰。

傳輸ACL的使用也與資料平面的強化相關。

如需詳細資訊，請參閱本檔案的使用傳輸ACL過濾傳輸流量 *一節*。

IP選項選擇性捨棄

IP選項有兩個安全隱患。包含IP選項的流量必須由Cisco IOS裝置進行進程交換，這會導致CPU負載增加。IP選項還包括更改流量通過網路的路徑的功能，這可能允許流量破壞安全控制。

出於這些考慮，全域性配置命令**ip options {drop | ignore}**已新增到Cisco IOS軟體版本12.3(4)T、12.0(22)S和12.2(25)S。在此命令的第一種形式(**ip options drop**)中，會丟棄包含Cisco IOS裝置所接收的IP選項的所有IP資料包。這可防止IP選項可以啟用的高CPU負載和可能的安全控制被顛覆。

此命令的第二個形式**ip options ignore**將Cisco IOS裝置配置為忽略接收資料包中包含的IP選項。雖然這確實減輕了本地裝置與IP選項相關的威脅，但存在IP選項可能會影響下游裝置。因此強烈建議使用此指令的**drop**形式。以下組態範例說明此情況：

```
!
ip options drop
!
```

請注意，某些通訊協定（例如RSVP）可合法使用IP選項。這些通訊協定的功能會受到此命令的影響。

啟用IP選項選擇性丟棄後，可使用**show ip traffic** EXEC命令確定由於IP選項出現而丟棄的資料包數量。此資訊出現在強制丟棄計數器中。

有關此功能的詳細資訊，請參閱ACL IP選項選擇性丟棄。

禁用IP源路由

IP源路由會同時利用「鬆散源路由」和「記錄路由」選項，或利用「嚴格源路由」和「記錄路由」選項，使IP資料包的源能夠指定資料包採用的網路路徑。此功能可用於嘗試在網路中的安全控制周

圍路由流量。

如果尚未通過IP選項選擇性丟棄功能完全禁用IP選項，則務必禁用IP源路由。所有Cisco IOS軟體版本預設會啟用IP來源路由，但會透過**no ip source-route** 全域組態指令停用。此組態範例說明此命令的使用方式：

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

禁用ICMP重定向

ICMP重新導向用於通知網路裝置到達IP目的地的更好路徑。預設情況下，Cisco IOS軟體會在收到必須透過所接收介面路由的封包時傳送重新導向。

在某些情況下，攻擊者可能會使Cisco IOS裝置傳送許多ICMP重定向消息，從而導致CPU負載增加。因此，建議停用ICMP重新導向傳輸。使用interface configuration **no ip redirects**命令禁用ICMP重定向，如示例配置所示：

```
!

interface FastEthernet 0
no ip redirects
!
```

禁用或限制IP定向廣播

IP定向廣播可以將IP廣播資料包傳送到遠端IP子網。一旦到達遠端網路，轉發IP裝置會將該資料包作為第2層廣播傳送到子網上的所有站點。此定向廣播功能已被用作幾次攻擊（包括smurf攻擊）中的放大和反射幫助。

目前版本的Cisco IOS軟體預設會停用此功能；但是可以通過**ip directed-broadcast**介面配置命令來啟用它。12.0之前的Cisco IOS軟體版本預設啟用此功能。

如果網路絕對需要定向廣播功能，則應控制其使用。可以使用訪問控制清單作為**ip directed-broadcast**命令的選項。此配置示例將定向廣播限製為來自受信任網路192.168.1.0/24的UDP資料包：

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!

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

使用傳輸ACL過濾傳輸流量

您可以使用傳輸ACL(tACL)控制哪些流量經過網路。 這與基礎架構ACL相反，後者會尋求過濾目的地為網路本身的流量。tACL提供的過濾對於過濾流向特定裝置組的流量或流經網路的流量很有用。

此類過濾通常由防火牆執行。但是，在某些情況下，對網路中的Cisco IOS裝置執行此過濾可能很有用，例如，必須執行過濾但是不存在防火牆。

傳輸ACL也是實施靜態反欺騙保護的合適位置。

有關詳細資訊，請參閱本文檔的反欺騙保護*部分*。

*請參閱*傳輸存取控制清單：在邊緣進行過濾以瞭解有關tACL的詳細資訊。

ICMP封包過濾

網際網路控制訊息通訊協定(ICMP)是作為IP的控制通訊協定而設計的。因此，它傳達的訊息可能會對一般的TCP和IP通訊協定產生深遠的影響。網路疑難排解工具**ping**和**traceroute**以及路徑MTU探索使用ICMP;但是，網路的正常運行很少需要外部ICMP連線。

Cisco IOS軟體提供特定功能，可按名稱、型別和代碼過濾ICMP訊息。此範例ACL會允許來自受信任網路的ICMP，但會封鎖來自其他來源的所有ICMP封包：

```
!

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
!
```

篩選IP片段

如本檔案的使用基礎架構ACL限制存取網路一節先前詳述，過濾分段的IP封包可能對安全裝置構成挑戰。

由於片段處理的不直觀性質，ACL經常會無意中允許IP片段。分段也經常用於嘗試逃避入侵檢測系統的檢測。正是由於這些原因，IP片段經常用於攻擊，因此應在任何已設定tACL的頂部明確過濾。以下ACL包括對IP片段的全面過濾。本示例中所示的功能必須與前面示例的功能結合使用：

```
!

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
!
```

請參閱存取控制清單和IP片段，*以取得更多有關分段IP封包的ACL處理資訊。*

適用於篩選IP選項的ACL支援

在Cisco IOS軟體版本12.3(4)T和更新版本中，Cisco IOS軟體支援使用ACL根據封包中包含的IP選項來過濾IP封包。封包中存在IP選項可能表示有人企圖破壞網路中的安全控制，或以其他方式變更封包的傳輸特徵。正是由於這些原因，才應該在網路邊緣過濾具有IP選項的資料包。

此範例必須與前面範例的內容一起使用，以包括對包含IP選項的IP封包的完整過濾：

```
!

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

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

反欺騙保護

許多攻擊使用源IP地址欺騙來有效或隱藏攻擊的真正來源並阻止準確回溯。Cisco IOS軟體提供單點傳播RPF和IP來源防護(IPSG)，以震懾依賴來源IP位址偽造的攻擊。此外，ACL和空路由通常作為防止欺騙的手動方式部署。

IP Source Guard通過執行交換機埠、MAC地址和源地址驗證，最大程度地減少受直接管理控制的網路的欺騙。單播RPF提供源網路驗證，可以減少來自非直接管理控制的網路的欺騙攻擊。埠安全可用於驗證接入層的MAC地址。動態位址解析通訊協定(ARP)檢查(DAI)可緩解在本地網段上使用ARP毒化的攻擊媒介。

單點傳播RPF

單播RPF使裝置能夠驗證轉發資料包的源地址是否可以通過接收該資料包的介面到達。不能依賴單播RPF作為防止欺騙的唯一保護。如果存在到源IP地址的適當返迴路由，則欺騙資料包可以通過啟用單點傳播RPF的介面進入網路。單播RPF依靠您在每台裝置上啟用思科快速轉發，並根據每個介面進行配置。

單播RPF可以配置為以下兩種模式之一：寬鬆或嚴格。在有非對稱路由的情況下，最好選擇鬆散模式，因為已知嚴格模式在此類情況下會丟棄資料包。在**ip verify** interface configuration命令的配置過程中，關鍵字**any**將配置鬆散模式，而關鍵字**rx**將配置嚴格模式。

此範例說明此功能的組態：

```
!

ip cef
!

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

有關單播RPF的配置和使用的詳細資訊，請參閱瞭解單播反向路徑轉發。

IP來源防護

IP源防護是一種有效的欺騙防護手段，如果您能控制第2層介面，就可以使用它。IP源防護使用來自

DHCP監聽的資訊在第2層介面上動態配置埠訪問控制清單(PACL)，拒絕來自IP源繫結表中未關聯的IP地址的任何流量。

IP源防護可應用於屬於啟用DHCP監聽的VLAN的第2層介面。以下命令啟用DHCP監聽：

```
!

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

啟用DHCP監聽後，以下命令啟用IPSG:

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

可以使用**ip verify source port security**介面配置命令啟用埠安全。這要求使用全域性配置命令**ip dhcp snooping information** ;此外，DHCP伺服器必須支援DHCP選項82。

有關此功能的詳細資訊，請參閱配置DHCP功能和IP源保護。

連線埠安全性

連線埠資安用於減輕存取介面的MAC位址欺騙。埠安全可以使用動態獲取的（粘滯）MAC地址來簡化初始配置。一旦連線埠資安確定發生MAC違規，它可以使用以下四種違規模式之一。這些模式包括保護、限制、關閉和關閉VLAN。在埠只為使用標準協定的單個工作站提供訪問的情況下，最多一個可能就足夠了。當最大數量設定為1時，利用HSRP等虛擬MAC地址的協定不起作用。

```
!

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>
!
```

有關埠安全配置的詳細資訊，請參閱配置埠安全。

動態ARP檢測

動態ARP檢測(DAI)可用於緩解對本地網段的ARP中毒攻擊。ARP中毒攻擊是指攻擊者將偽造的ARP資訊傳送到本地網段的方法。此資訊旨在損壞其他裝置的ARP快取。攻擊者通常使用ARP中毒來執行中間人攻擊。

DAI攔截並驗證不受信任埠上的所有ARP資料包的IP到MAC地址關係。在DHCP環境中，DAI使用由DHCP監聽功能生成的資料。不會驗證受信任介面上接收到的ARP資料包，而會丟棄不受信任介面上的無效資料包。在非DHCP環境中，需要使用ARP ACL。

以下命令啟用DHCP監聽：

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

啟用DHCP監聽後，以下命令將啟用DAI:

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

在非DHCP環境中，需要ARP ACL來啟用DAI。此範例示範使用ARP ACL的DAI的基本設定：

```
!

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

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

只要受支援，也可以基於每個介面啟用DAi。

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

有關如何配置DAI的詳細資訊，請參閱配置動態ARP檢測。

反欺騙ACL

手動配置的ACL可提供靜態防欺騙保護，抵禦使用已知未使用和不可信地址空間的攻擊。通常，這些反欺騙ACL會作為較大ACL的元件應用於網路邊界上的輸入流量。反欺騙ACL需要定期監控，因為它們可能經常更改。如果您應用將流量限製為有效本地地址的出站ACL，則可以從本地網路發起的流量中最小化欺騙。

此範例示範如何使用ACL來限制IP欺騙。此ACL應用於所需介面的入站流量。組成此ACL的ACE並不全面。如果設定這些型別的ACL，請尋找結論性的最新參考。

```
!

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
!
```

有關如何配置訪問控制清單的詳細資訊，請參閱配置常用的IP ACL。

未分配Internet地址的官方清單由Cymru團隊維護。有關過濾未使用地址的其他資訊，請參閱Bogon參考頁面。

限制資料平面流量對CPU的影響

路由器和交換機的主要用途是通過裝置將資料包和幀轉發到最終目的地。這些資料包傳輸在整個網路中部署的裝置，可能會影響裝置的CPU操作。應保護資料平面（由經過網路裝置的流量組成），以確保管理和控制平面的運行。如果傳輸流量可能引起裝置處理交換機流量，則裝置的控制平面可能受到影響，從而導致運行中斷。

影響CPU的功能和流量型別

儘管並不詳盡，但此清單包含需要特殊的CPU處理並由CPU進行進程交換的資料平面流量型別：

- **ACL日誌**記錄 — ACL日誌記錄流量包括因使用log關鍵字的ACE的匹配（允許或拒絕）而生成**的**任何資料包。
- **單播RPF** — 與ACL結合使用的單播RPF可能會導致某些資料包的過程交換。
- **IP選項** — 任何包含選項的IP資料包都必須由CPU處理。
- **分段** — 需要分段的任何IP資料包都必須傳遞到CPU進行處理。
- **生存時間(TTL)到期** - TTL值小於或等於1的資料包需要傳送網際網路控制消息協定超時（ICMP型別11，代碼0）消息，這將導致CPU處理。
- **ICMP不可達**項 — 由於路由、MTU或過濾而導致ICMP無法到達消息的資料包由CPU處理。
- **需要ARP請求的流**量 — 不存在ARP條目的目標需要CPU進行處理。
- **非IP流量** — 所有非IP流量均由CPU處理。

*有關*資料平面強化的詳細資訊，請參閱本文檔的一般資料平面強化部分。

按TTL值篩選

您可以使用Cisco IOS軟體版本12.4(2)T中引入的ACL支援過濾TTL值功能，在延伸型IP存取清單中根據TTL值過濾封包。此功能可用於保護TTL值為零或1的接收傳輸流量的裝置。還可以使用基於TTL值的過濾資料包來確保TTL值不低於網路直徑，從而保護下游基礎設施裝置的控制平面免受TTL過期攻擊。

請注意，某些應用程式和工具(如**traceroute**)將TTL過期資料包用於測試和診斷目的。某些通訊協定（例如IGMP）可合法使用1的TTL值。

此ACL示例建立一個策略，用於過濾TTL值小於6的IP資料包。

```
!
!--- 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
!
```

請參閱TTL到期攻擊識別和緩解，*瞭解有關根據TTL值過濾資料包的詳細資訊。*

有關此功能的詳細資訊，請參閱ACL支援以過濾TTL值。

在Cisco IOS軟體版本12.4(4)T和更新版本中，彈性封包比對(FPM)允許管理員對封包的任意位元進行比對。此FPM策略丟棄TTL值小於六的資料包。

```
!

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
!
```

有關此功能的詳細資訊，請參閱Cisco IOS靈活資料包匹配*首頁上的*靈活資料包匹配。

根據是否存在IP選項進行過濾

在Cisco IOS軟體版本12.3(4)T和更新版本中，可以在命名延伸型IP存取清單中使用篩選IP選項的ACL支援，以篩選具有IP選項的IP封包。還可以使用基於IP選項的存在的過濾IP資料包來防止基礎設施裝置的控制平面必須在CPU級別處理這些資料包。

請注意，適用於篩選IP選項的ACL支援功能只能用於命名型延伸型ACL。還應注意，如果丟棄了用於這些協定的資料包，RSVP、多協定標籤交換流量工程、IGMP版本2和3以及使用IP選項資料包的其他協定可能無法正常工作。如果網路中使用這些通訊協定，則可使用ACL Support for Filtering IP Options;但是，ACL IP選項選擇性丟棄功能可能會丟棄此流量，而且這些協定可能無法正常工作。如果沒有使用的協定需要IP選項，則ACL IP選項選擇性丟棄是丟棄這些資料包的首選方法。

此ACL示例將建立一個策略，過濾包含任何IP選項的IP資料包：

```
!

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
!
```

此示例ACL演示了一個使用五個特定IP選項過濾IP資料包的策略。包含這些選項的資料包將被拒絕

：

- 0選項清單結束(eool)
- 7記錄路由（記錄路由）
- 68時間戳（時間戳）
- 131 — 鬆散源路由(lsr)
- 137 — 嚴格來源路由(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
!
```

有關ACL IP選項選擇性丟棄的詳細資訊，請參閱本文檔的一般資料平面強化*部分*。

*請參閱*傳輸存取控制清單：在邊緣進行過濾以瞭解更多有關過濾傳輸和邊緣流量的資訊。

Cisco IOS軟體中的另一個功能可用於使用IP選項過濾封包，即CoPP。在Cisco IOS軟體版本12.3(4)T和更新版本中，CoPP允許管理員過濾控制平面封包的流量流。支援Cisco IOS軟體版本12.3(4)T中引入的過濾IP選項的CoPP和ACL支援的裝置可以使用訪問清單策略來過濾包含IP選項的資料包。

如果存在任何IP選項，此CoPP策略將丟棄裝置接收的傳輸資料包：

```
!

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
!
```

如果存在以下IP選項，此CoPP策略將丟棄裝置接收的傳輸資料包：

- 0選項清單結束(eool)
- 7記錄路由（記錄路由）
- 68時間戳（時間戳）
- 131寬鬆來源路由(lsr)
- 137嚴格源路由(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，將資料包與permit操作匹配的訪問控制清單條目(ACE)導致這些資料包被策略對映丟棄功能丟棄，而與deny操作（未顯示）匹配的資料包不受策略對映丟棄功能的影響。

有關CoPP功能的詳細資訊，請參閱部署控制平面策略。

控制平面保護

在Cisco IOS軟體版本12.4(4)T和更新版本中，控制平面保護(CPPr)可用於限制或管制Cisco IOS裝置的CPU的控制平面流量。雖然與CoPP類似，但CPPr能夠使用比CoPP更精細的粒度來限制或管制流量。CPPr將聚合控制平面分為三個單獨的控制平面類別，稱為子介面：存在主機、傳輸和CEF-Exception子介面。

此CPPr策略丟棄TTL值小於6的裝置接收的傳輸資料包以及TTL值為零或1的裝置接收的傳輸或非傳輸資料包。CPPr策略還會丟棄裝置接收到具有選定IP選項的資料包。

```
!

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
!
```

在上一個CPPr策略中，將資料包與permit操作匹配的訪問控制清單條目會導致這些資料包被policy-map drop函式丟棄，而與deny操作（未顯示）匹配的資料包不受策略對映丟棄函式的影響。

有關CPPr功能的詳細資訊，請參閱瞭解控制平面保護*和*控制平面保護。

流量識別和回溯

有時，您可能需要快速識別和回溯網路流量，尤其是在事件響應或網路效能較差期間。NetFlow和分類ACL是使用Cisco IOS軟體完成此操作的兩種主要方法。NetFlow可提供對網路上所有流量的可見性。此外，NetFlow還可以通過可提供長期趨勢和自動化分析的收集器來實施。分類ACL是ACL的一個元件，需要預先規劃來確定特定流量，並在分析期間進行手動干預。以下各節簡要概述每個功能。

Netflow

NetFlow通過跟蹤網路流量來識別異常且與安全相關的網路活動。可以通過CLI檢視和分析NetFlow資料，也可以將資料匯出到商業或免費的NetFlow收集器進行彙總和分析。NetFlow收集器可通過長期趨勢分析提供網路行為和使用情況分析。NetFlow通過分析IP資料包中的特定屬性並建立流來發揮作用。第5版是NetFlow最常用的版本，但第9版擴展性更強。NetFlow流可以在高流量環境中使用抽樣流量資料建立。

CEF（即分散式CEF）是啟用NetFlow的先決條件。可以在路由器和交換機上配置NetFlow。

此範例說明此功能的基本設定。在Cisco IOS軟體的先前版本中，在介面上啟用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>
!
```

以下是CLI的NetFlow輸出示例。SrcIf屬性可幫助進行回溯。

```
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
```

有關NetFlow功能的詳細資訊，請參閱Cisco IOS NetFlow。

有關NetFlow的技術概述，請參閱Cisco IOS NetFlow簡介 — 技術概述。

分類ACL

分類ACL提供對穿越介面的流量的可見性。分類ACL不會改變網路的安全策略，而且其構造通常用於對單個協定、源地址或目標進行分類。例如，允許所有流量的ACE可以分成特定的協定或埠。將流量更精細地分類到特定ACE有助於瞭解網路流量，因為每個流量類別都有自己的命中計數器。管理員還可以將ACL末尾的隱式deny分隔為精細ACE，以幫助識別拒絕流量的型別。

管理員可以通過**show access-list**和**clear ip access-list counters** EXEC命令使用分類ACL來加快事件響應。

此示例說明分類ACL的配置，該配置用於在預設拒絕之前識別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
!
```

若要識別使用分類ACL的流量，請使用**show access-list** acl-name EXEC命令。可以使用**clear ip access-list counters** acl-name EXEC命令清除ACL計數器。

```
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)
```

有關如何在ACL中啟用日誌記錄功能的詳細資訊，請參閱瞭解訪問控制清單日誌記錄。

使用VLAN對映和埠訪問控制清單進行訪問控制

VLAN存取控制清單(VACL)或VLAN對映和連線埠ACL(PACL)提供這樣一種功能：對比應用於路由介面的存取控制清單更接近終端裝置的非路由流量執行存取控制。

這些部分概述了VACL和PACL的功能、優勢和潛在的使用場景。

使用VLAN對映進行訪問控制

適用於進入VLAN的所有封包的VACL或VLAN對應，提供對VLAN內流量執行存取控制的功能。路由介面上的ACL無法實現此功能。例如，可以使用VLAN對映來防止包含在同一個VLAN中的主機相互通訊，這樣可以減少本地攻擊者或蠕蟲利用同一網段上的主機的機會。為了拒絕資料包使用VLAN對映，您可以建立匹配流量的訪問控制清單(ACL)，並在VLAN對映中將操作設定為drop。配置VLAN對映後，所有進入LAN的資料包都會根據配置的VLAN對映依次進行評估。VLAN存取對映支援IPv4和MAC存取清單；但是，它們不支援日誌記錄或IPv6 ACL。

此範例使用說明此功能組態的延伸命名存取清單：

```
!

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

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

此範例示範使用VLAN對應來拒絕TCP連線埠139和445以及vines-ip通訊協定：

```
!

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
!
```

有關VLAN對映配置的詳細資訊，請參閱使用ACL配置網路安全。

使用PACL進行訪問控制

PACL只能應用於交換機第2層物理介面的入站方向。與VLAN對映類似，PACL為非路由流量或第2層流量提供訪問控制。建立PACL的語法優先於VLAN對映和路由器ACL，與路由器ACL的語法相同。如果ACL應用於第2層介面，則稱為PACL。配置包括建立IPv4、IPv6或MAC ACL並將其應用到第2層介面。

此範例使用延伸命名存取清單來說明此功能的組態：

```
!

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
!
```

*有關PACL配*置的詳細資訊，請參閱使用ACL配置網路安全的埠ACL部分。

使用MAC的存取控制

MAC訪問控制清單或擴展清單可以在介面配置模式下使用以下命令應用於IP網路：

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

> **附註**：這是為了將第3層封包分類為第2層封包。Cisco IOS軟體版本12.2(18)SXD（適用於Sup 720）和Cisco IOS軟體版本12.2(33)SRA或更新版本支援此命令。

此介面命令必須應用於輸入介面，它指示轉發引擎不檢查IP報頭。結果是，您可以在IP環境中使用MAC訪問清單。

專用VLAN使用

專用VLAN(PVLAN)是限制VLAN中工作站或伺服器之間連線的第2層安全功能。沒有PVLAN，第2層VLAN中的所有裝置都可以自由通訊。存在可通過限制單個VLAN上的裝置之間的通訊來幫助安全性的網路情況。例如，PVLAN通常用於禁止公共可訪問子網中的伺服器之間的通訊。如果一台伺服器受損，由於PVLAN的應用而導致無法連線到其他伺服器，這可能有助於限制對一台伺服器的危害。

有三種型別的專用VLAN:隔離VLAN、社群VLAN和主VLAN。PVLAN的配置使用主要和輔助VLAN。主要VLAN包含所有混雜埠（稍後將對此進行說明），並包括一個或多個輔助VLAN，輔助VLAN可以是隔離的VLAN也可以是社群VLAN。

隔離VLAN

將輔助VLAN配置為隔離VLAN會完全阻止輔助VLAN中的裝置之間的通訊。每個主VLAN可能只有一個隔離VLAN，並且只有混雜埠可以與隔離VLAN中的埠通訊。隔離VLAN應該用於不受信任的網路

（如支援訪客的網路）。

此配置示例將VLAN 11配置為隔離VLAN，並將其與主VLAN VLAN 20關聯。以下示例還將介面FastEthernet 1/1配置為VLAN 11中的隔離埠：

```
!

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
!
```

社群VLAN

設定為社群VLAN的輔助VLAN允許VLAN成員之間以及主要VLAN中的任何混雜連線埠進行通訊。但是，任何兩個社群VLAN之間或社群VLAN與隔離VLAN之間無法通訊。必須將社群VLAN用於對需要相互連線，但不要求連線到VLAN中所有其它裝置的伺服器進行分組。這種情況常見於可公開訪問的網路或伺服器向不受信任的客戶端提供內容的任何位置。

此示例配置單個社群VLAN並將交換機埠FastEthernet 1/2配置為該VLAN的成員。社群VLAN(VLAN 12)是主VLAN 20的輔助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
!
```

混雜埠

放置在主VLAN中的交換機埠稱為混雜埠。混雜連線埠可與主要和輔助VLAN中的所有其他連線埠通訊。路由器或防火牆介面是這些VLAN中最常見的裝置。

此組態範例結合之前的隔離和群體VLAN範例，將介面FastEthernet 1/12的組態新增為混雜連線埠：

```
!

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
!
```

實作PVLAN時，必須確保現有的第3層配置支援PVLAN施加的限制，並且不允許顛覆PVLAN配置。使用路由器ACL或防火牆的第3層過濾可以防止PVLAN配置的顛覆。

請參閱LAN安全*首頁上的*專用VLAN(PVLAN) — 混雜、隔離、社群*，瞭解有關使用和配置專用VLAN的詳細資訊。*

結論

本檔案簡要概述可用於保護Cisco IOS系統裝置的方法。如果保護裝置，就會提高所管理網路的整體安全性。在此概述中，將討論管理、控制和資料平面的保護，並提供配置建議。在可能的情況下，為每個相關特徵的配置提供了足夠的細節。但是，在所有情況下，系統都會提供全面的參考資料，以向您提供進行進一步評估所需的資訊。

確認

本文檔中的一些功能說明是由思科資訊開發團隊編寫的。

附錄：Cisco IOS裝置加固檢查表

此核對表是本指南中介紹的所有強化步驟的集合。管理員可以使用它來提醒Cisco IOS裝置使用和考慮的所有強化功能，即使某項功能因未應用而未實施也是如此。建議管理員在實施每個選項之前評估其潛在風險。

管理平面

- 密碼

  對啟用和本地使用者密碼啟用MD5雜湊（加密選項）配置密碼重試鎖定禁用密碼恢復（考慮風險）

- 禁用未使用的服務

- 為管理作業階段設定TCP keepalive

- 設定記憶體和CPU閾值通知

- 設定

  記憶體和CPU閾值通知為控制檯訪問保留記憶體儲存器洩漏檢測器緩衝區溢位檢測增強的crashinfo集合

- 使用iACL限制管理訪問

- 篩選（考慮風險）

  ICMP資料包IP片段IP選項資料包中的TTL值

- 控制平面保護

  配置埠過濾配置隊列閾值

- 管理訪問

  使用管理平面保護來限制管理介面設定exec超時使用加密的傳輸協定（如SSH）進行CLI訪問控制vty和tty線路的傳輸（訪問類選項）使用橫幅發出警告

- AAA

  使用AAA進行身份驗證和回退使用AAA(TACACS+)進行命令授權使用AAA進行記帳使用冗餘AAA伺服器

- SNMP

  配置SNMPv2社群並應用ACL配置SNMPv3

- 記錄

  配置集中日誌記錄設定所有相關元件的日誌記錄級別Set logging source-interface配置日誌記錄時間戳粒度

- 組態管理

替換和回滾獨佔配置更改訪問軟體可復原性配置配置更改通知

控制平面

- 禁用（考慮風險）

  ICMP 重新導向ICMP不可達代理 ARP

- 配置NTP身份驗證（如果正在使用NTP）
- 配置控制平面策略/保護（埠過濾、隊列閾值）
- 安全路由協定

  BGP（TTL、MD5、最大字首、字首清單和系統路徑ACL）IGP（MD5，被動介面，路由過濾，資源消耗）

- 配置硬體速率限制器
- 安全第一躍點備援通訊協定(GLBP、HSRP、VRRP)

資料平面

- 設定IP選項選擇性捨棄
- 禁用（考慮風險）

  IP來源路由IP定向廣播ICMP 重新導向

- 限制IP定向廣播
- 配置tACL（考慮風險）

  篩選ICMP篩選IP片段篩選IP選項篩選TTL值

- 配置所需的反欺騙保護

  ACLIP來源防護動態ARP檢測單點傳播RPF連線埠安全性

- 控制平面保護（控制平面cef-exception）
- 配置NetFlow和分類ACL以識別流量
- 配置所需的訪問控制ACL（VLAN對映、PACL和MAC）
- 配置專用VLAN