使用Cisco IOS XE強化指南

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

安全操作

監控Cisco安全建議及響應

利用身份驗證、授權和記帳

集中記錄收集與監控

儘可能使用安全協定

透過NetFlow獲得流量可視性

組態管理

管理平面

一般管理平面強化

- 密碼管理
- 增強型密碼安全
- 登入密碼重試鎖定
- No Service Password-Recovery
- 停用未使用的服務
- EXEC超時
- TCP會話的Keepalive
- 管理介面使用
- 記憶體臨界值通知
- CPU閾值通知
- 網路時間協定

使用基礎設施ACL限制網路訪問

- ICMP封包過濾
- 過濾IP片段
- 對過濾IP選項的ACL支援
- 對基於TTL值過濾的ACL支援

安全互動式管理會話

- 管理平面保護
- 控制平面保護
- 加密管理會話
- SSHv2
- 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

- 控制vty和tty線路的傳輸
- 警告標語

驗證、授權和記帳

- TACACS+ 驗證
- 驗證後援
- 使用型別7密碼
- TACACS+命令授權
- TACACS+命令記帳
- 冗餘AAA伺服器

增強簡單網路管理協定

- SNMP社群字串
- SNMP社群字串與ACL
- 基礎架構ACL
- SNMP檢視
- SNMP版本3
- 管理平面保護

日誌記錄最佳實踐

- 將日誌傳送到中央位置
- 記錄日誌層次
- 不記錄到主控台或監視階段作業
- 使用緩衝記錄日誌
- 配置日誌記錄源介面
- 配置日誌記錄時間戳

Cisco IOS XE軟體組態管理

- 配置替換和配置回滾
- 獨佔配置更改訪問
- 數位簽章的思科軟體
- 配置更改通知和日誌記錄

控制平面

一般控制層面強化

- IP ICMP重定向
- ICMP不可達
- 代理 ARP
- NTP控制消息

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

- 基於TTL的安全保護
- 使用MD5進行BGP對等驗證

- 配置最大字首數
- 使用字首清單過濾BGP字首
- 使用自治系統路徑訪問清單過濾BGP字首

安全內部網關協定

使用消息摘要5的路由協定驗證和驗證

- Passive-interface命令
- 路由過濾
- 製程處理資源消耗

安全第一跳冗餘協定

資料平面

一般資料平面強化

- IP選項選擇性丟棄
- 停用IP源路由
- 停用ICMP重定向
- 停用或限制IP定向廣播

使用傳輸ACL過濾傳輸流量

- ICMP封包過濾
- 過濾IP片段
- 對過濾IP選項的ACL支援

反欺騙保護

- 單播RPF
- IP來源防護
- 連線埠安全性
- 反欺騙ACL

限制資料平面流量對CPU的影響

- 影響CPU的功能和資料流型別
- 按TTL值篩選
- 基於是否存在IP選項過濾
- 控制平面保護

流量辨識和回溯

- Netflow
- 分類ACL
- 使用PACL進行訪問控制
- 隔離VLAN
- 社群VLAN

結論

致謝

附錄：Cisco IOS XE裝置強化清單

管理平面

控制平面

資料平面

簡介

本檔案介紹保護Cisco IOS® XE系統裝置所需的資訊，可提升網路檔案的整體安全性。

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

本文檔圍繞網路裝置功能可分類的三個平面進行了構建，概述了每個功能和相關專案的參考。

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。

1. 管理平面-管理平面管理傳送到思科IOS XE裝置的流量，由安全外殼(SSH)和簡單網路管理協定(SNMP)等應用和協定組成。
2. 控制平面-網路裝置的控制平面處理對於維護網路基礎設施的功能至關重要的流量。控制平面包括網路裝置之間的應用和協定，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)。
3. 資料平面-資料平面透過網路裝置轉發資料。資料平面不包括傳送到本地Cisco IOS XE裝置的流量。

   本檔案的安全性功能範圍通常提供足夠詳細資訊，讓您設定功能。但是，在不使用的情況下，會以某種方式解釋特徵，以便您可以評估是否需要對該特徵給予額外注意。如果可能和適當，本文檔包含實施後有助於保護網路安全的建議。

安全操作

安全網路操作是一個重要主題。雖然本文檔的大部分內容都用於Cisco IOS XE裝置的安全配置，但僅靠配置並不能完全保護網路。網路上使用的操作過程與底層裝置的配置一樣有助於提高安全性。

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Cisco安全建議及響應

思科產品安全事件響應團隊(PSIRT)針對思科產品的安全相關問題建立和維護出版物，通常稱為PSIRT建議。用於不太嚴重問題的通訊方法是Cisco Security Response。在思科安全建議和響應中提供了安全建議及響應

思科安全漏洞策略中提供了有關這些通訊工具的其他資訊

為了維護安全網路，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。有關此評估過程的幫助，請參閱安全漏洞通告風險分類。

利用身份驗證、授權和記帳

身份驗證、授權和記帳(AAA)架構對於保護網路裝置安全至關重要。AAA架構提供管理會話的身份驗證，還可以將使用者限制為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、授權和記賬部分。

集中記錄收集與監控

要瞭解與安全事件相關的當前、新興和歷史事件，您的組織必須具有統一的事件日誌記錄和關聯策略。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和可定製的關聯功能。

實施集中記錄後，您必須開發一種結構化方法來執行日誌分析和事件跟蹤。根據您組織的需要，此方法範圍廣泛，從對日誌資料的簡單認真稽核到基於規則的高級分析。

有關如何在Cisco IOS XE網路裝置中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

許多協定用於傳輸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，在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)來取代FTP或TFTP。

有關安全管理Cisco IOS XE裝置的詳細資訊，請參閱本文檔的安全互動式管理會話部分。

透過NetFlow獲得流量可視性

NetFlow允許您監控網路中的流量流。NetFlow最初旨在將流量資訊導出到網路管理應用程式，但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流經網路。無論流量資訊是否導出到遠端收集器，都建議您配置NetFlow的網路裝置，以便在需要時可反應性地使用。

有關此功能的詳細資訊可在本文檔的資料流標識和回溯部分中找到，也可以在Cisco IOS NetFlow中找到（僅限註冊使用者）。

組態管理

組態管理是建議、稽核、批准和部署配置更改的過程。在Cisco IOS XE裝置配置環境中，組態管理的另外兩個方面至關重要：配置存檔和安全性。

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，還可以使用配置存檔來確定進行了哪些安全更改以及更改發生的時間。與AAA日誌資料結合使用時，此資訊有助於網路裝置的安

全審計。

Cisco IOS XE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 XE裝置配置的儲存庫。對此類資訊的不安全訪問可能會破壞整個網路的安全。

管理平面

管理平面包括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性時，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，您可能無法恢復或穩定網路。

以下各節詳細介紹Cisco IOS XE軟體中用於幫助加強管理平面的安全功能和配置。

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流量以便運行這些功能的平面。您必須同時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。以下協定清單由管理平面使用：

1. 簡單網路管理協定
2. Telnet
3. 安全殼層通訊協定
4. 檔案傳輸通訊協定
5. 超文本傳輸協定/安全超文本傳輸協定
6. 簡單檔案傳輸協定
7. 安全複製協定
8. TACACS+
9. RADIUS
10. Netflow
11. 網路時間協定
12. 系統日誌

必須採取措施確保管理和控制平面在安全事件期間繼續存在。如果其中一種飛機被成功利用，所有飛機都可能遭到入侵。

密碼管理

密碼控制對資源或裝置的訪問。這可透過定義用於驗證請求的密碼或金鑰來實現。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，並且訪問可以根據結果被授予、拒絕或限制。作為安全最佳實踐，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服務發生故障，仍然需要本地配置的用於特權訪問的密碼。裝置還可以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 XE系統的特權管理訪問許可權的口令。必須使用

enable secret命令，而不是更舊的enable password命令。enable password 命令使用的是一種加密強度較低的加密演算法。

如果未設定使能加密口令並且為控制檯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，即使是從遠端虛擬tty (vty)會話也是如此。此操作幾乎肯定是不需要的，這也是確保配置啟用加密的另外一個原因。

service password-encryption 全局配置命令指示Cisco IOS XE軟體對口令、質詢握手身份驗證協定(CHAP)加密口令和儲存在其配置檔案中的類似資料進行加密。這種加密有助於防止臨時觀察者讀取密碼，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Vigenre加密。此演演算法並非設計用來保護組態檔，使其免受即使是略為複雜的攻擊者的嚴重分析，因此不得用於此目的。任何包含加密口令的Cisco IOS XE配置檔案都必須謹慎對待，就像對待這些相同口令的明文清單一樣。

雖然enable secret 命令並不使用這一加密強度較低的加密演算法，但enable password 全局配置命令以及password 行配置命令均使用該加密演算法。必須去除這種型別的口令，並需要使用enable secret 命令或增強的口令安全功能。

enable secret 命令和「增強的口令安全」功能將消息摘要5 (MD5)用於口令雜湊。這種演算法已經過相當多的公開審查，目前還不知道是否可逆。但是，該演算法會受到詞典攻擊。在詞典攻擊中，攻擊者嘗試詞典或其他候選密碼清單中的每個單詞，以查詢匹配項。因此，必須安全地儲存配置檔案，並且僅與受信任的個人共用。

增強型密碼安全

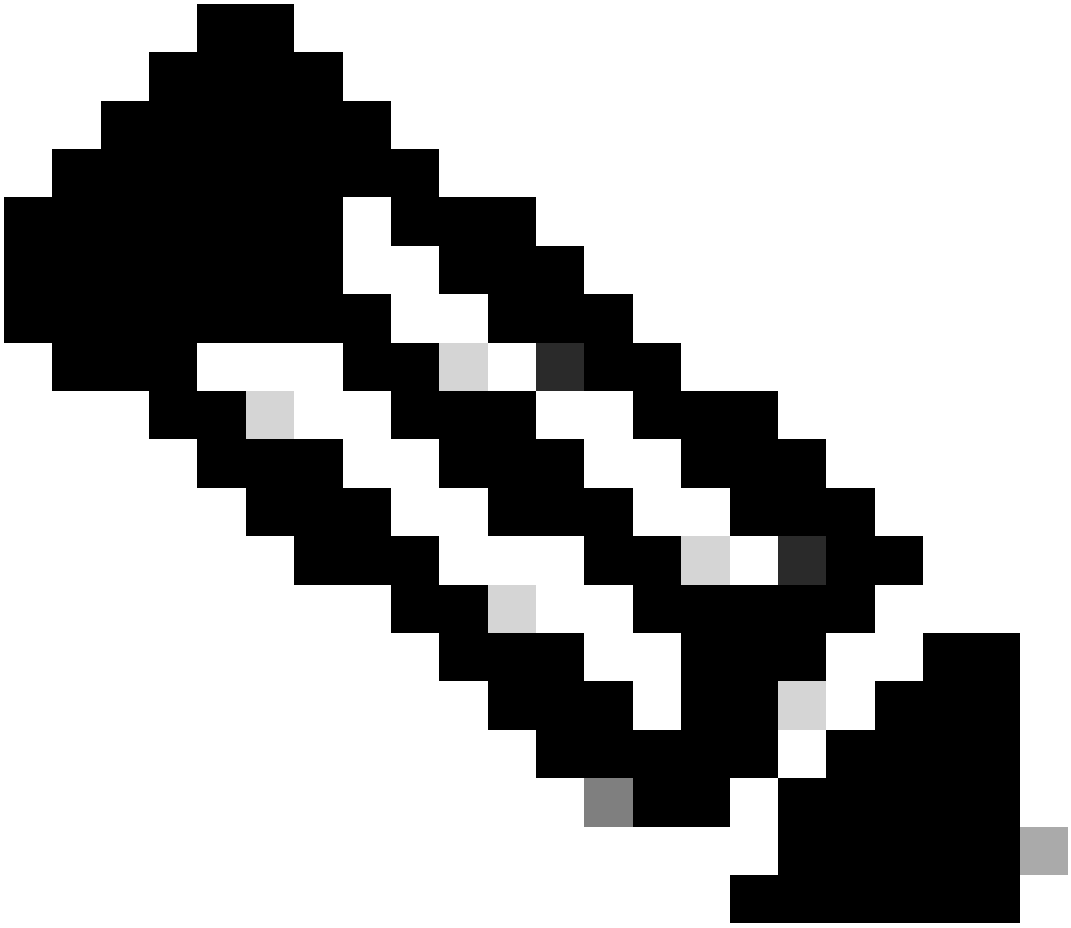
「增強的口令安全」功能自第一版Cisco IOS XE軟體版本16.6.4起生效，它允許管理員為username命令配置MD5口令雜湊。在此功能之前，有兩種型別的密碼：型別0（為明文密碼）和型別7（使用Vigen re密碼的演算法）。「增強的口令安全」功能不能用於要求可檢索明文口令的協定，例如CHAP。

要使用MD5雜湊功能加密使用者口令，請發出username secret全局配置命令。

username <name> secret <password>

登入密碼重試鎖定

自第一版Cisco IOS XE軟體版本16.6.4開始運作的「登入密碼重試鎖定」功能，可讓您在經過設定的失敗登入嘗試次數後，鎖定本機使用者帳戶。鎖定使用者後，其帳號會一直鎖定，直到您將其解除鎖定為止。使用許可權等級15設定的授權使用者無法使用此功能鎖定。必須將許可權級別為15的使用者數保持在最低水準。



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，惡意使用者可能會透過多次嘗試使用有效使用者名稱進行身份驗證來建立拒絕服務(DoS)條件。

此示例說明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。

No Service Password-Recovery

在Cisco IOS XE軟體版本16.6.4及更高版本中，無服務口令恢復功能不允許任何具有控制檯訪問許可權的使用者以不安全的方式訪問裝置配置並清除口令。它還不允許惡意使用者更改配置暫存器值並訪問NVRAM。

no service password-recovery

Cisco IOS XE軟體提供密碼復原程式，該程式依賴於對ROM Monitor Mode (ROMMON)的存取，並在系統啟動期間使用Break鍵。在ROMMON中，可以重新載入裝置軟體，以提示包含新口令的新系統配置。

目前的密碼復原程式可讓任何具有主控台存取許可權的使用者存取裝置及其網路。無服務口令恢復功能可阻止完成Break鍵序列並在系統啟動期間輸入ROMMON。

如果裝置上未啟用服務口令恢復，建議儲存裝置配置的離線副本，並實施配置存檔解決方案。啟用此功能後，如果需要恢復Cisco IOS XE裝置的口令，則刪除整個配置。

停用未使用的服務

作為安全最佳做法，必須停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和其他透過資料包過濾阻止的攻擊。

必須停用TCP和UDP小型服務。這些服務包括：

1. echo （埠號7）
2. 捨棄（連線埠號碼9）
3. 白天（埠號13）
4. chargen （連線埠號碼19）

   雖然透過反欺騙訪問清單可以避免或降低濫用小型服務的風險，但必須在網路中可訪問的任何裝置上停用這些服務。Cisco IOS XE軟體版本16.6.4及更高版本預設停用小型服務。在更低版本的軟體中，可以發出no service tcp-small-servers 和no service udp-small-servers 全局配置命令來停用它們。

   這是未使用時必須停用的其他服務清單：
5. 請發出no ip finger 全局配置命令以停用Finger服務。預設情況下，高於16.1的Cisco IOS XE軟體版本停用此服務。
6. 請發出no ip bootp server 全局配置命令以停用Bootstrap協定(BOOTP)。預設情況下，高於16.1的Cisco IOS XE軟體版本停用此服務。
7. 在Cisco IOS XE軟體版本16.6.4及更高版本中，請在全局配置模式下發出ip dhcp bootp ignore命令以停用BOOTP。這樣動態主機設定通訊協定(DHCP)服務就會保持啟用狀態。
8. 如果不需要DHCP中繼服務，則可以停用DHCP服務。在全局配置模式下發出no service dhcp命令。
9. 請在介面配置模式下發出no mop enabled 命令以停用維護操作協定(MOP)服務。
10. 請發出no ip domain-lookup全局配置命令以停用域名系統(DNS)解析服務。
11. 請在全局配置模式下發出no service pad 命令以停用用於X.25網路的分組拆/裝器(PAD)服務。
12. 在全局配置模式下，可使用 no ip http server命令停用HTTP伺服器，並可使用 no ip http secure-server 全局配置命令以停用安全HTTP (HTTPS)伺服器。
13. 除非Cisco IOS XE裝置在啟動期間從網路中檢索配置，否則必須使用no service config全局配置命令。這可防止Cisco IOS XE裝置嘗試使用TFTP在網路上查詢配置檔案。
14. Cisco探索通訊協定(CDP)是一種網路通訊協定，用於探索其他啟用CDP的裝置，以進行鄰居鄰接和網路拓朴。網路管理系統(NMS)或故障排除期間可使用CDP。必須在連線到不受信任網

路的所有介面上停用CDP。使用no cdp enable介面命令可完成此操作。或者，也可以使用no cdp run 全局配置命令全局停用CDP。請注意，惡意使用者可能使用CDP進行偵測和網路對映。

15. 鏈路層發現協定(LLDP)是在802.1AB中定義的IEEE協定。LLDP與CDP類似。但是，此協定允許不支援CDP的其他裝置之間的互操作性。LLDP必須以與CDP相同的方式處理，並在連線到不受信任網路的所有介面上停用。為了完成此操作，請發出no lldp transmit和no lldp receive介面配置命令。請發出no lldp run 全局配置命令以全局停用LLDP。惡意使用者也可以使用LLDP進行偵測和網路對映。
16. 對於支援從sdflash啟動的交換機，可以透過從快閃記憶體啟動並使用no sdflash配置命令停用sdflash來增強安全性。

EXEC超時

要設定EXEC命令解釋程式在終止會話之前等待使用者輸入的時間間隔，請發出exec-timeout 行配置命令。必須使用exec-timeout 命令註銷vty或tty線路上處於空閒狀態的會話。依預設，工作階段會在閒置十分鐘後中斷連線。

line con 0

exec-timeout <分鐘> [秒]

line vty 0 4

exec-timeout <分鐘> [秒]

TCP會話的Keepalive

service tcp-keepalives-in 和service tcp-keepalives-out 全局配置命令允許裝置傳送TCP keepalive以進行TCP會話。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。這可以確保連線遠端端的裝置仍然可訪問，並且從本地Cisco IOS XE裝置中移除半開放或孤立的連線。

service tcp-keepalives-in

service tcp-keepalives-out

管理介面使用

在物理或邏輯管理介面上以帶內或帶外方式訪問裝置的管理平面。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。環回介面始終處於打開狀態，而物理介面可以更改狀態，並且介面可能無法訪問。建議為每個裝置增加一個環回介面作為管理介面，並且僅用於管理平面。這允許管理員在整個網路中為管理平面應用策略。一旦在裝置上配置了環回介面，管理平面協定（如SSH、SNMP和syslog）就可以使用該介面來傳送和接收流量。

interface Loopback0

ip address 192.168.1.1 255.255.255.0

記憶體臨界值通知

在Cisco IOS XE軟體版本16.6.4中增加的記憶體閾值通知功能使您可以緩解裝置記憶體不足的情況。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」會生成日誌消息，以指示裝置上的可用記憶體已低於配置的閾值。本配置示例說明如何使用memory free low-watermark 全局配置命令啟用此功能。這允許裝置在可用空閒記憶體低於指定閾值時生成通知，並在可用空閒記憶體高於指定閾值時再次生成通知。

記憶體可用低水位線處理器<threshold>

記憶體可用低水印io <閾值>

使用記憶體保留，以便有足夠的記憶體可供重要通知使用。此組態範例示範如何啟用此功能。這可以確保在裝置的記憶體耗盡時，管理進程仍可繼續運行。

memory reserve critical <value>

CPU閾值通知

在Cisco IOS XE軟體版本16.6.4中引入的CPU閾值通知功能允許您在裝置上的CPU負載超過配置的閾值時進行檢測並收到通知。當超過閾值時，裝置將生成並傳送SNMP陷阱消息。Cisco IOS XE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

處理程式cpu臨界值型別<type>上升<percentage>間隔<seconds> [下降<percentage>間隔<seconds>]

process cpu statistics limit entry-percentage <number> [size <seconds>]

網路時間協定

網路時間協定(NTP)不是特別危險的服務，但任何不需要的服務都可能代表攻擊媒介。如果使用NTP，則明確配置受信任的時間源並使用適當的身份驗證非常重要。需要準確可靠的時間來完成syslog目的，例如在潛在攻擊的取證調查過程中，以及依靠證書進行第1階段身份驗證的VPN連線是否成功。

1. NTP時區-配置NTP時，需要配置時區，以便準確關聯時間戳。通常有兩種方法可以配置具有全局狀態的網路中的裝置的時區。一種方法是使用協調世界時(UTC)(之前為葛林威治標準時間(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可在思科產品文檔的時鐘時區中找到。
2. NTP身份驗證-如果配置NTP身份驗證，則可確保在受信任的NTP對等裝置之間交換NTP消息。

使用NTP身份驗證的示例配置：

使用者端：

(config)#ntp authenticate

(config)#ntp authentication-key 5 md5 ciscotime

(config)#ntp trusted-key 5

(config)#ntp server 172.16.1.5 key 5 Server：

(config)#ntp authenticate

(config)#ntp authentication-key 5 md5 ciscotime

(config)#ntp trusted-key 5

使用基礎設施ACL限制網路訪問

基礎設施訪問控制清單(iACL)旨在防止未經授權直接與網路裝置通訊，是可在網路中實施的最關鍵的安全控制之一。基礎架構ACL會利用幾乎所有的網路流量都會經過網路，而且並非以網路本身為目的地。

構建和應用iACL是為了指定需要允許的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。在允許所需的連線後，到基礎設施的所有其他流量都會被顯式拒絕。然後會明確地允許所有透過網路且並非目的地為基礎架構裝置的傳輸流量。

iACL提供的保護與管理和控制層面都有關。透過對網路基礎設施裝置使用不同的編址，可以簡化iACL的實施。有關IP編址的安全含義的詳細資訊，請參閱面向安全的IP編址方法。

以下示例iACL配置說明了開始iACL實施過程時必須作為起點使用的結構：

ip access-list extended ACL-INFRASTRUCTURE-IN

— 允許路由協定和網路管理所需的連線

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

— 拒絕所有其他IP流量傳輸至任何網路裝置

deny ip any <infrastructure-address-space> <wildcard-mask>

— 允許中轉流量

permit ip any any

建立iACL後，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、遠端訪問網段、使用者網段和資料中心網段的介面。

有關基礎架構ACL的詳細資訊，請參閱保護您的核心：基礎架構保護訪問控制清單。

ICMP封包過濾

網際網路控制訊息通訊協定(ICMP)是設計為IP控制通訊協定。因此，它傳達的消息通常會對整個TCP和IP協定產生深遠的影響。雖然網路故障排除工具ping和traceroute使用ICMP，但網路的正常運行很少需要外部ICMP連線。

Cisco IOS XE軟體提供特定功能，以便根據名稱或型別和程式碼過濾ICMP訊息。此範例ACL必須搭配先前範例中的存取控制專案(ACE)使用，允許來自受信任管理站和NMS伺服器的ping並封鎖所有其他的ICMP封包：

ip access-list extended ACL-INFRASTRUCTURE-IN

— 允許來自受信任管理站和伺服器的ICMP響應(ping)

permit icmp host <trusted-management-stations> any echo

permit icmp host <trusted-netmgmt-servers> any echo

— 拒絕所有其他IP流量傳輸至任何網路裝置

deny ip any <infrastructure-address-space> <wildcard-mask>

— 允許中轉流量

permit ip any any

過濾IP片段

分段的IP資料包的過濾過程可能對安全裝置構成挑戰。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 XE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 XE軟體根據ACL評估這些非初始分段，並忽略任何第4層過濾資訊。這將導致非初始分段僅在任何已配置ACE的第3層部分上進行評估。

在此示例配置中，如果發往埠22上的192.168.1.1的TCP資料包在傳輸過程中分段，則根據資料包中的第4層資訊，初始ACE將如預期那樣丟棄初始分段。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）分段。此情況顯示在此組態中：

ip access-list extended ACL-FRAGMENT-示例

permit tcp any host 192.168.1.1 eq 80

deny tcp any host 192.168.1.1 eq 22

由於分段處理的非直觀性質，ACL經常會無意中允許IP分段。分段還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分段經常用於攻擊，並且為什麼必須在任何已配置iACL的頂部顯式過濾這些分段。此示例ACL包括對IP分段的全面過濾。此範例中的功能必須與先前範例的功能搭配使用。

ip access-list extended ACL-INFRASTRUCTURE-IN

— 拒絕使用特定於協定的ACE幫助的IP分段

— 攻擊流量分類

拒絕tcp any any片段

deny udp any any fragments

拒絕icmp any any片段

deny ip any any fragments

— 拒絕所有其他IP流量傳輸至任何網路裝置

deny ip any <infrastructure-address-space> <wildcard-mask>

— 允許中轉流量

permit ip any any

有關ACL如何處理分段IP資料包的詳細資訊，請參閱訪問控制清單和IP分段。

對過濾IP選項的ACL支援

Cisco IOS XE軟體版本16.6.4新增了對使用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。這需要CPU工作水準，而通常在網路中傳輸的資料包不需要這種水準。資料包中存在IP選項也可能表示試圖破壞網路中的安全控制或改變資料包的傳輸特性。正是由於這些原因，必須在網路邊緣過濾帶有IP選項的資料包。

此示例必須與前面示例中的ACE一起使用，以便包括完整過濾包含IP選項的IP資料包：

ip access-list extended ACL-INFRASTRUCTURE-IN

— 拒絕包含IP選項的IP資料包

deny ip any any option any-options

— 拒絕所有其他IP流量傳輸至任何網路裝置

deny ip any <infrastructure-address-space> <wildcard-mask>

— 允許中轉流量

permit ip any any

對基於TTL值過濾的ACL支援

Cisco IOS XE軟體版本16.6.4新增了ACL支援，可根據存留時間(TTL)值篩選IP封包。當資料包從源流向目標時，IP資料包的TTL值由每台網路裝置遞減。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。需要將TTL遞減到零並因此丟棄資料包的裝置來生成並向資料包的源傳送ICMP超時消息。

這些報文的生成和傳輸是一個例外過程。當到期的IP資料包數量少時，路由器可以執行此功能，但如果到期的資料包數量高，則生成和傳輸這些消息會佔用所有可用的CPU資源。這就構成了DoS攻擊媒介。正是由於這個原因，需要針對利用即將到期的高速率IP資料包的DoS攻擊強化裝置。

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。

在本範例中，ACL會過濾TTL值小於六的封包。這可以為寬度最多五跳的網路提供保護，以抵禦TTL到期攻擊。

ip access-list extended ACL-INFRASTRUCTURE-IN

— 拒絕TTL值不足以穿越網路的IP資料包

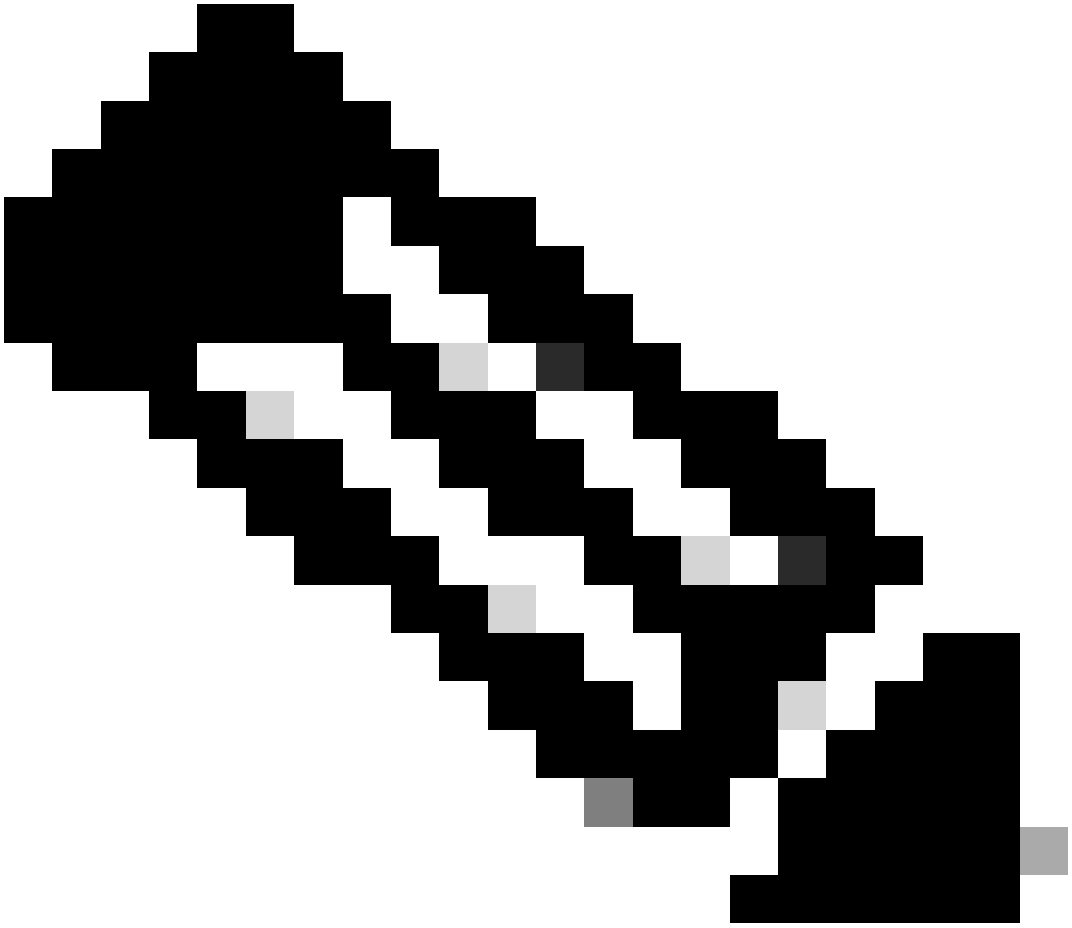
deny ip any any ttl lt 6

— 拒絕所有其他IP流量傳輸至任何網路裝置

deny ip any <infrastructure-address-space> <掩碼>

— 允許中轉流量

permit ip any any



注意：某些協定會合法使用具有低TTL值的資料包。eBGP就是其中之一。有關儘量避免受到基於TTL到期的攻擊的詳細資訊，請參閱「辨識和防範TTL到期攻擊」。

安全互動式管理會話

透過裝置管理會話，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、受到危害並被用於執行其他攻擊。任何對裝置進行特權訪問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 XE軟體版本16.6.4及更高版本中，功能管理平面保護(MPP)允許管理員限制裝置可以接收的管理流量的介面。這允許管理員對裝置及其訪問方式進行額外的控制。

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

控制平面主機

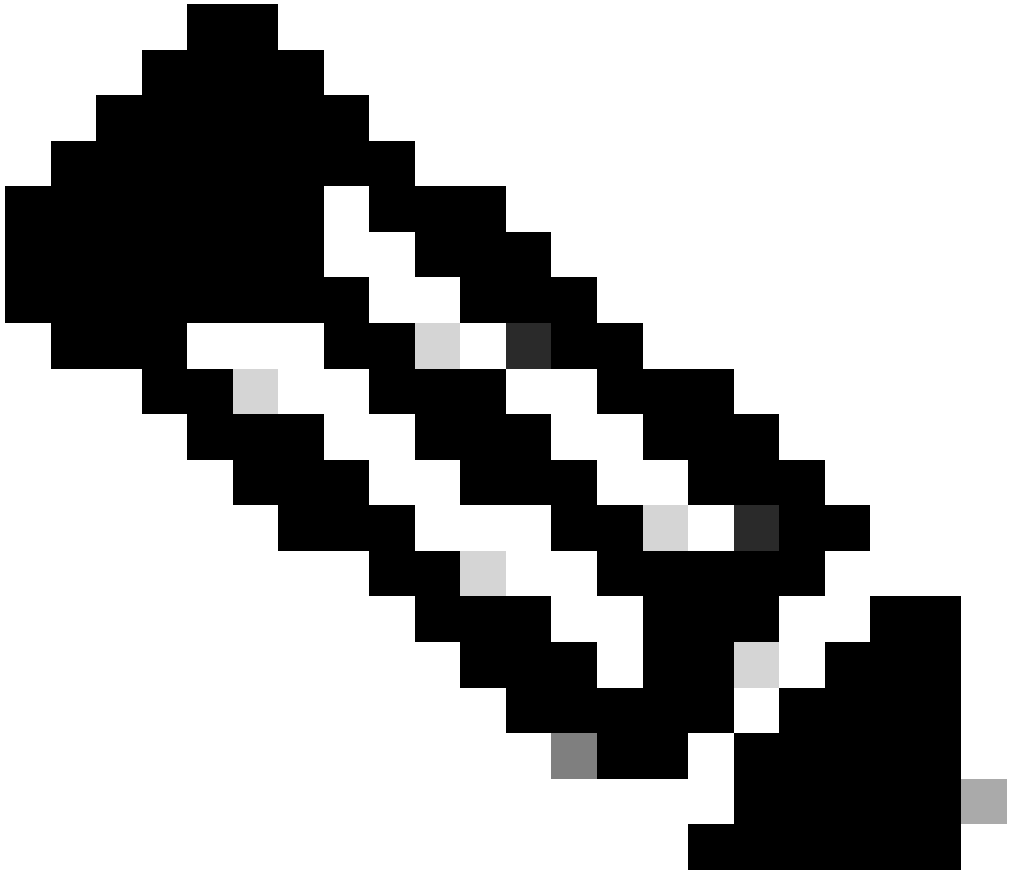
管理介面GigabitEthernet 0/1允許ssh https

控制平面保護

控制層面保護(CPPr)建立在控制層面策略功能的基礎上，以限制和管制發往IOS-XE裝置路由處理器的控制層面流量。CPPr將控制平面劃分為不同的控制平面類別，這些類別稱為子介面。存在三個控制平面子介面：Host、Transit和CEF-Exception。此外，CPPr還包括以下額外的控制層面保護功能：

1. 埠過濾功能-此功能用於管制或丟棄傳送到已關閉或非偵聽TCP和UDP埠的資料包。
2. 隊列閾值策略功能-此功能可限制控制平面IP輸入隊列中允許的指定協定資料包數。

CPPr允許管理員透過主機子介面對傳送到裝置進行分類、管制和限制流量以便進行管理。針對主機子介面類別分類的資料包示例包括管理流量（例如SSH或Telnet）以及路由協定。



注意：CPPr不支援IPv6，並且僅限於IPv4輸入路徑。

有關Cisco CPPr功能的詳細資訊，請參閱控制層面策略。

加密管理會話

由於資訊可以在互動式管理會話中公開，因此必須加密此流量，以便惡意使用者無法訪問傳輸的資料。流量加密允許到裝置的安全遠端訪問連線。如果管理會話的流量以明文形式透過網路傳送，攻擊者可以獲得有關裝置和網路的敏感資訊。

管理員能夠使用SSH或安全超文本傳輸協定(HTTPS)功能建立到裝置的加密安全遠端訪問管理連線。Cisco IOS XE軟體支援SSH版本2.0 (SSHv2)和使用Secure Sockets Layer (SSL)和Transport Layer Security (TLS)進行身份驗證和資料加密的HTTPS。

Cisco IOS XE軟體也支援安全複製通訊協定(SCP)，可透過加密和安全連線來複製裝置組態或軟體映像。SCP依賴SSH。

此示例配置在Cisco IOS XE裝置上啟用SSH：

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh超時60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

line vty 0 4

傳輸輸入ssh

此配置示例啟用SCP服務：

ip scp server enable

以下是HTTPS服務的組態範例：

crypto key generate rsa modulus 2048

ip http secure-server

SSHv2

Cisco IOS XE在第一個版本16.6.4中引入了SSHv2功能，允許使用者配置SSHv2。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提供了一種透過網路安全訪問並安全執行另一台電腦或裝置上的命令的方法。透過SSH隧道傳輸的安全複製協定(SCP)功能允許安全傳輸檔案。

如果未明確配置ip ssh version 2命令，則Cisco IOS XE會啟用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，可能對系統產生不利影響。如果已啟用SSH，則建議使用ip ssh version 2命令停用SSHv1。

此示例配置在Cisco IOS XE裝置上啟用SSHv2（停用SSHv1）：

hostname router

ip domain-name example.com

crypto key generate rsa modulus 2048

ip ssh超時60

ip ssh authentication-retries 3

ip ssh source-interface GigabitEthernet 0/1

ip ssh版本2

line vty 0 4

傳輸輸入ssh

有關使用SSHv2的更多資訊，請參閱安全外殼版本2支援。

適用於RSA金鑰的SSHv2增強功能

Cisco IOS XE 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增強功能還支援客戶端和伺服器的基於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有/公共金鑰對進行身份驗證。使用者必須在客戶端上生成私有/公共金鑰對，並在Cisco IOS XE SSH伺服器上配置公共金鑰以完成身份驗證。

嘗試建立憑證的SSH使用者會提供具有私密金鑰的加密簽名。簽名和使用者的公鑰將傳送到SSH伺服器進行身份驗證。SSH伺服器透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，使用者根據加密簽名被認證或被拒絕訪問。

對於伺服器身份驗證，Cisco IOS XE 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。如果客戶端上啟用了嚴格主機金鑰檢查標誌，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。如果伺服器成功透過身份驗證，會話建立將繼續；否則將終止並顯示「伺服器身份驗證失敗」消息。

此示例配置允許在思科IOS XE裝置上使用RSA金鑰和SSHv2：

配置裝置的主機名

hostname router

配置域名

ip domain-name example.com

啟用SSH伺服器，以便在使用SSH

「crypto key generate」命令。

對於SSH版本2，模數大小必須至少為768位

crypto key generate rsa usage-keys label sshkeys modulus 2048

指定要用於SSH的RSA金鑰對的名稱（在本例中為「sshkeys」）

ip ssh rsa keypair-name sshkeys

配置ssh超時（以秒為單位）。

下一個輸出會為SSH連線啟用120秒的超時。

ip ssh超時120

設定五個驗證重試次數的限制。

ip ssh authentication-retries 5

配置SSH第2版。

ip ssh版本2

有關使用RSA金鑰及SSHv2的更多資訊，請參閱適用於RSA金鑰的安全外殼版本2增強功能。

此示例配置使Cisco IOS XE SSH伺服器能夠執行基於RSA的使用者身份驗證。如果使用客戶端上儲存的公鑰或私鑰對驗證儲存在伺服器上的RSA公鑰，則使用者身份驗證成功。

配置裝置的主機名。

hostname router

配置域名。

ip域名cisco.com

生成使用2048位模數的RSA金鑰對。

crypto key generate rsa modulus 2048

在SSH伺服器上為使用者和伺服器身份驗證配置SSH-RSA金鑰。

ip ssh pubkey-chain

設定 SSH 使用者名稱。

在SSH伺服器上為使用者和伺服器身份驗證配置SSH-RSA金鑰。

ip ssh pubkey-chain

設定 SSH 使用者名稱。

使用者名稱ssh-user

指定遠端對等點的 RSA 公開金鑰。

然後，您必須配置key-string命令

（後跟遠端對等體的RSA公鑰）或

key-hash命令（後跟SSH金鑰型別和版本）。

有關使用RSA金鑰及SSHv2的更多資訊，請參閱配置思科IOS XE SSH伺服器以執行基於RSA的使用者驗證部分。

此示例配置使Cisco IOS XE 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.com

產生 RSA 金鑰配對。

crypto key generate rsa

在SSH伺服器上為使用者和伺服器身份驗證配置SSH-RSA金鑰。

ip ssh pubkey-chain

在路由器上啟用SSH伺服器進行公鑰身份驗證。

伺服器SSH-server-name

指定遠端對等裝置的RSA公鑰。

然後，您必須配置key-string命令

（後跟遠端對等體的RSA公鑰）或

key-hash <key-type> <key-name>命令（後跟SSH金鑰）

型別和版本)。

確保進行伺服器身份驗證-連線為

在失敗時終止。

ip ssh stricthostkeycheck

有關使用RSA金鑰及SSHv2的更多資訊，請參閱配置思科IOS XE SSH客戶端以執行基於RSA的伺服器驗證部分。

控制檯和AUX埠

在Cisco IOS XE裝置中，控制檯和輔助(AUX)埠是可用於對裝置進行本地和遠端訪問的非同步線路。您必須瞭解Cisco裝置上的控制檯埠具有特殊許可權。這些許可權尤其可讓管理員執行密碼復原程式。要執行口令恢復，未經驗證的攻擊者需要訪問控制檯埠，並需要能夠中斷裝置的電源或導致裝置崩潰。

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相同的方式加以保護。如果數據機連線到控制檯，用於保護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，則管理員可以取消執行使用no service password-recovery 全局配置命令的口令恢復過程的能力；但是，一旦啟用no service password-recovery 命令，管理員將無法再對裝置執行口令恢復。

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

行aux 0

傳輸輸入無

傳輸輸出無

no exec exec-timeout 0 1

無密碼

控制vty和tty線路

Cisco IOS XE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以本地訪問裝置，也可以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，在該伺服器中，可以透過網路與連線到tty線路的裝置的控制檯埠建立連線。還必須控制網路中用於這些反向連線的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）。為了確保裝置能夠透過本地或遠端管理會話進行訪問，必須在vty和tty線路上實施適當的控制。Cisco IOS XE裝置具有數量有限的vty線路；可用的線路數量可透過show line EXEC命令確定。當所有vty線路都處於使用狀態時，無法建立新管理會話，這會為裝置訪問建立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，而不考慮裝置在網路中的位置。這對vty線路至關重要，因為它們可以透過網路訪問。連線到用於遠端訪問裝置的數據機的tty線路，或者連線到其它裝置控制檯埠的tty線路，也可以透過網路訪問。使用transport input或access-class配置命令、CoPP和CPPr功能或在裝置上對介面應用訪問清單，也可以執行其他形式的vty和tty訪問控制。

身份驗證可以透過使用AAA來執行，這是使用本地使用者資料庫對裝置進行身份驗證訪問的推薦方法，也可以透過直接在vty或tty線路上配置的簡單密碼身份驗證來執行。

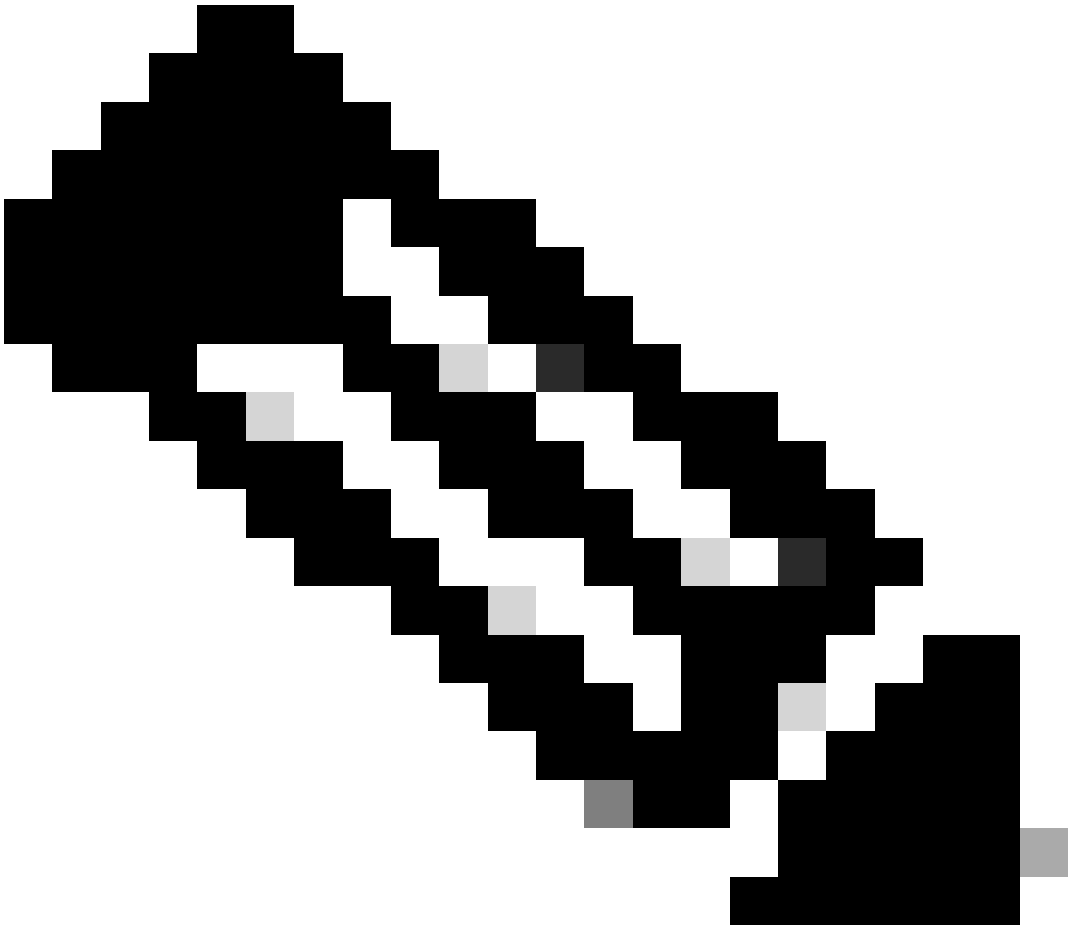
必須使用exec-timeout命令註銷vty或tty線路上處於空閒狀態的會話。另外，也必須使用service tcp-keepalives-in 命令才能對裝置的傳入連線啟用TCP keepalive。這可以確保連線遠端端的裝置仍然

可訪問，並且從本地IOS-XE裝置中移除半開放或孤立的連線。

控制vty和tty線路的傳輸

可以配置vty和tty，以便僅接受到裝置或透過該裝置（如果用作控制檯伺服器）的加密和安全的遠端訪問管理連線。本節介紹tty，因為此類線路可以連線到其他裝置上的控制檯埠，這些埠允許透過網路訪問tty。為了防止資訊洩露或未經授權訪問在管理員和裝置之間傳輸的資料，可以使用transport input ssh來代替明文協定，如Telnet和rlogin。在tty上啟用transport input none配置，該配置實際上會禁止將tty線路用於反向控制檯連線。

vty和tty線路都允許管理員連線到其他裝置。為了限制管理員能夠用於傳出連線的傳輸型別，請使用transport output line 配置命令。如果不需要傳出連線，則可以使用transport output none。但是，如果允許傳出連線，則可以透過使用transport output ssh對連線執行加密的安全遠端訪問方法。



注意：如果支援IPSec，它可用於對裝置進行加密和安全遠端訪問連線。如果使用IPSec，也會為裝置增加額外CPU開銷。但是，即使使用IPSec，仍必須將SSH作為傳輸來執行。

警告標語

在某些法律管轄區，除非收到不允許使用系統的通知，否則不可能起訴惡意使用者並對其進行非法監控。提供此通知的一種方法是，將此資訊放入使用Cisco IOS XE軟體標語登入命令配置的標語消息中。

法律通知要求很複雜，因管轄區和情況而異，可與法律顧問討論。即使在司法管轄區內，法律意見也可能不同。與律師合作時，橫幅可以提供以下部分或全部資訊：

1. 請注意，系統只能由經過特別授權的人員登入或使用，可能還包括有關誰可以授權使用的資訊。
2. 請注意，任何未經授權的使用系統都是非法的，可能受到民事和刑事處罰。
3. 請注意，任何系統使用都可被記錄或監控，無需進一步通知，而生成的日誌可作為法庭證據。
4. 在地法律要求的特定通知。

   從安全的角度來看，登入標語不能包含有關路由器名稱、型號、軟體或所有權的任何特定資訊，而不是合法的資訊。此資訊可能被惡意使用者濫用。

驗證、授權和記帳

身份驗證、授權和記帳(AAA)架構對於保護對網路裝置的互動式訪問至關重要。AAA架構提供了高度可配置的環境，可以根據網路的需求進行定製。

TACACS+ 驗證

TACACS+是Cisco IOS XE裝置可用於對遠端AAA伺服器的管理使用者進行身份驗證的身份驗證協定。這些管理使用者可透過SSH、HTTPS、Telnet或HTTP訪問IOS-XE裝置。

TACACS+身份驗證（更常見的是AAA身份驗證）提供為每個網路管理員使用單個使用者帳戶的功能。當您不依賴於單個共用密碼時，網路安全性會得到提高，您的責任也會得到增強。

RADIUS是一種與TACACS+類似的通訊協定；但是，它只會加密在網路中傳送的密碼。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，可以將TACACS+優先用於RADIUS。有關比較這兩種協定的詳細資訊，請參閱比較TACACS+和RADIUS。

可以使用與以下示例類似的配置在Cisco IOS XE裝置上啟用TACACS+身份驗證：

```
aaa new-model

aaa authentication login default group tacacs+

tacacs server <server_name>

 address ipv4 <tacacs_server_ip_address>

 鍵<key>
```

可以將先前的配置用作特定於組織的AAA身份驗證模板的起點。

方法清單是一個順序清單，它描述了為驗證使用者而要查詢的驗證方法。方法清單可讓您指定一或多個要用於驗證的安全性通訊協定，如此可確保備份系統在初始方法失敗時進行驗證。Cisco IOS XE軟體使用第一個列出的方法，可成功接受或拒絕使用者。只有在早期方法由於伺服器不可用或配置錯誤而失敗時，才會嘗試後續方法。

有關配置指定方法清單的詳細資訊，請參閱指定的身份驗證方法清單。

驗證後援

如果所有已設定的TACACS+伺服器都變為無法使用，則Cisco IOS XE裝置可以依賴次要驗證通訊協定。典型配置包括：如果所有配置的TACACS+伺服器均不可用，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。首選使用使能加密口令，因為使用單向演算法雜湊加密口令比使用型別7口令進行線路或本地身份驗證的加密演算法本身更安全。

但是，在支援對本地定義的使用者使用加密口令的Cisco IOS XE軟體版本上，可能需要回退到本地身份驗證。這允許為一或多個網路管理員建立本機定義的使用者。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。雖然此動作可加強網路管理員在TACACS+服務中斷時的責任，但由於必須維護所有網路裝置上的本機使用者帳戶，因此可大幅增加管理負擔。

此配置示例建立在先前的TACACS+驗證示例基礎之上，以便為使用enable secret 命令在本地配置的密碼包含回退驗證：

```
enable secret <password>

aaa new-model

aaa authentication login default group tacacs+ enable

tacacs server <server_name>

 address ipv4 <tacacs_server_ip_address>

 鍵<key>
```

有關將AAA與回退驗證一起使用的詳細資訊，請參閱配置驗證。

使用型別7密碼

Type 7密碼最初設計用於快速解密儲存的密碼，但它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。除非在Cisco IOS XE裝置上使用的功能有要求，否則可以避免使用型別7密碼。

可以儘可能使用第9類（加密）：

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

廢除此型別的口令可以透過使用AAA驗證和增強型口令安全功能來幫助實現；後者允許對透過username 全局配置命令在本地定義的使用者使用加密口令。如果無法完全禁止使用型別7密碼，請考慮將這些密碼混淆而不是加密。

有關刪除型別7口令的詳細資訊，請參閱本文檔的一般管理平面強化部分。

TACACS+命令授權

TACACS+和AAA的命令授權提供一種機制，可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 XE會將每個命令傳送到已配置的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。

此配置可增加到前面的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+命令記帳

配置後，AAA命令記賬將向配置的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、執行的日期和輸入命令的使用者名稱。RADIUS不支援指令計量。

此示例配置啟用了AAA命令，該命令記下在許可權級別0、1和15輸入的EXEC命令。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+
```

有關配置AAA記賬的詳細資訊，請參閱配置記賬。

冗餘AAA伺服器

在環境中使用的AAA伺服器可以是冗餘的，並以容錯方式部署。這有助於確保在AAA伺服器不可用時，可以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：

1. AAA伺服器在潛在網路故障期間的可用性
2. 地理位置分散的AAA伺服器放置
3. 在穩定狀態和故障情況下載入單個AAA伺服器
4. 網路接入伺服器和AAA伺服器之間的網路延遲
5. 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。

增強簡單網路管理協定

本節重點介紹幾種方法，可用於保護IOS-XE裝置中的SNMP部署。SNMP必須妥善保護，以保護網路資料和傳輸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運行狀況的豐富資訊。可以保護此資訊，使其免受惡意使用者的攻擊，這些惡意使用者希望利用此資料對網路執行攻擊。

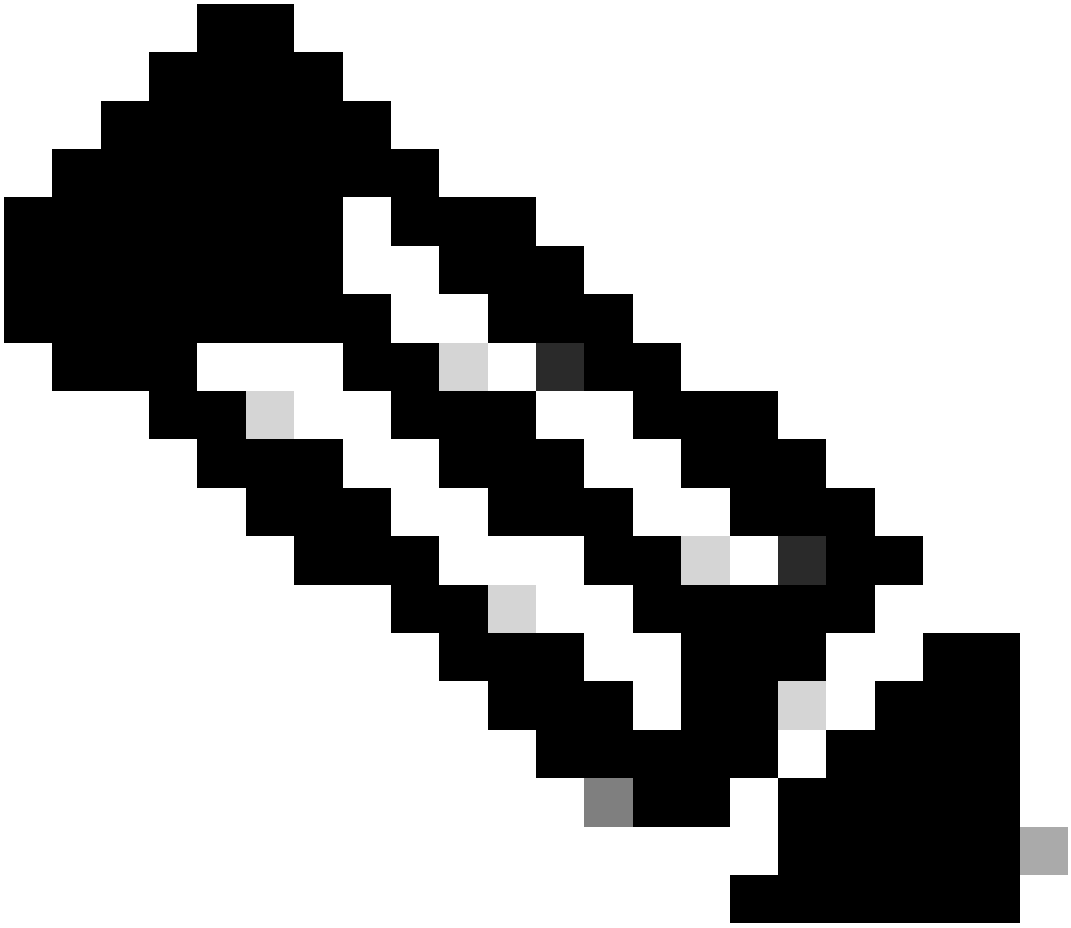
SNMP社群字串

社群字串是套用至IOS-XE裝置的密碼，用於限制對裝置上SNMP資料的唯讀和讀取/寫入存取許可權。與所有密碼一樣，可以仔細選擇這些社群字串，以確保它們並非微不足道。社群字串可以按照網路安全策略定期更改。

例如，當網路管理員變更角色或離開公司時，可以變更字串。

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

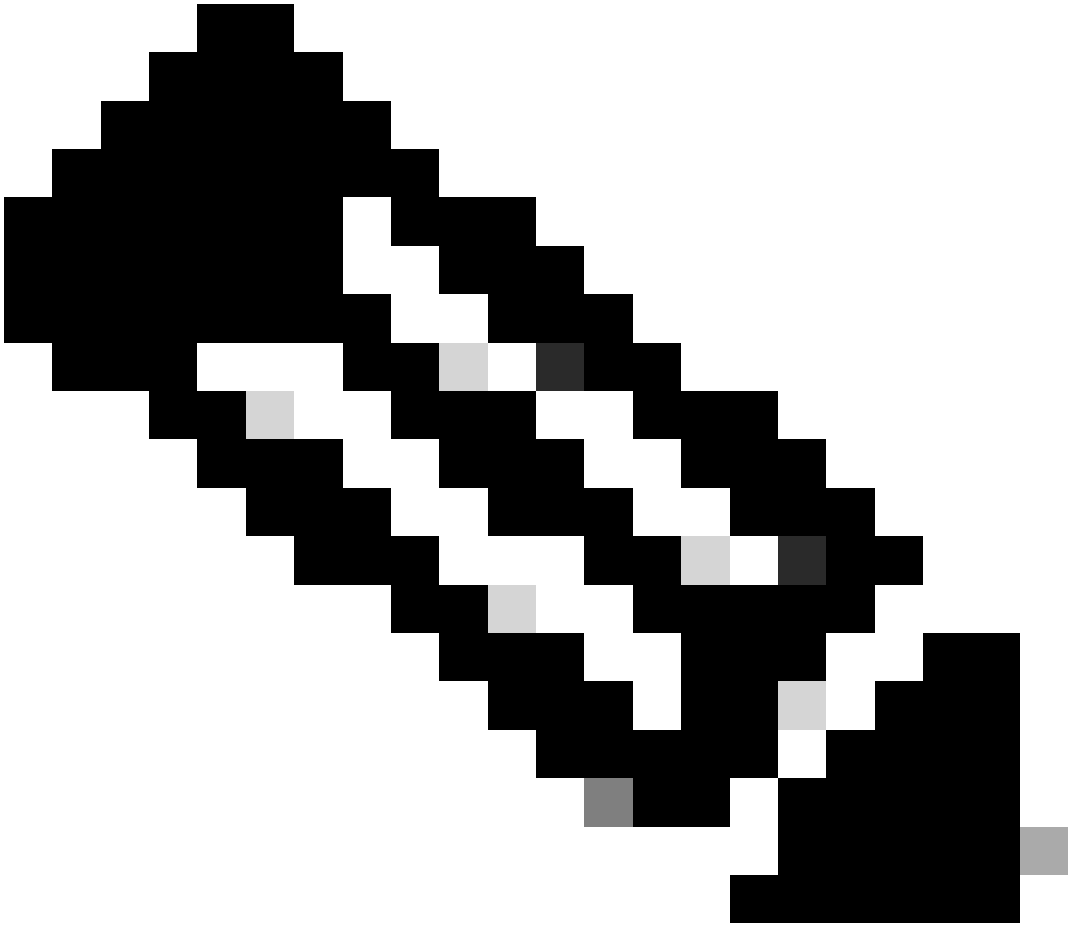
```
snmp-server community READONLY RO

snmp-server community READWRITE RW
```



注意：選擇前面的社群字串示例是為了清楚地說明這些字串的使用。對於生產環境，可以謹慎選擇社群字串，該字串可以包含一系列字母、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。

SNMP社群字串與ACL

除社群字串之外，還可以應用ACL，進一步限制對一組特定源IP地址的SNMP訪問。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。



注意：這些ACL允許的裝置需要正確的社群字串才能訪問請求的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 XE網路管理命令參考」中的snmp-server community。

基礎架構ACL

可部署基礎架構ACL (iACL)，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-XE裝置。iACL可以包含拒絕UDP埠161上未授權SNMP資料包的策略。

有關使用iACL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。建立檢視並使用snmp-server community community string view全局配置命令將其應用於社群字串後，如果您訪問MIB資料，您將被限制為只能使用該檢視定義的許可權進行訪問。建議您在適當時使用檢視來將SNMP的使用者限制在他們需要的資料中。

本配置示例使用社群字串LIMITED將MIB訪問限制為位於系統組中的MIB資料：

snmp-server view <view_name> <mib_view_family_name> [包含/排除]

snmp-server community <community_string>view <view_name> RO

有關詳細資訊，請參閱配置SNMP支援。

SNMP版本3

SNMP第3版(SNMPv3)是由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協定。SNMPv3可透過網路驗證資料包並選擇性地加密資料包，從而提供對裝置的安全訪問。在受支援的地方，部署SNMP時，可以使用SNMPv3增加另一層安全性。SNMPv3包含三個主要配置選項：

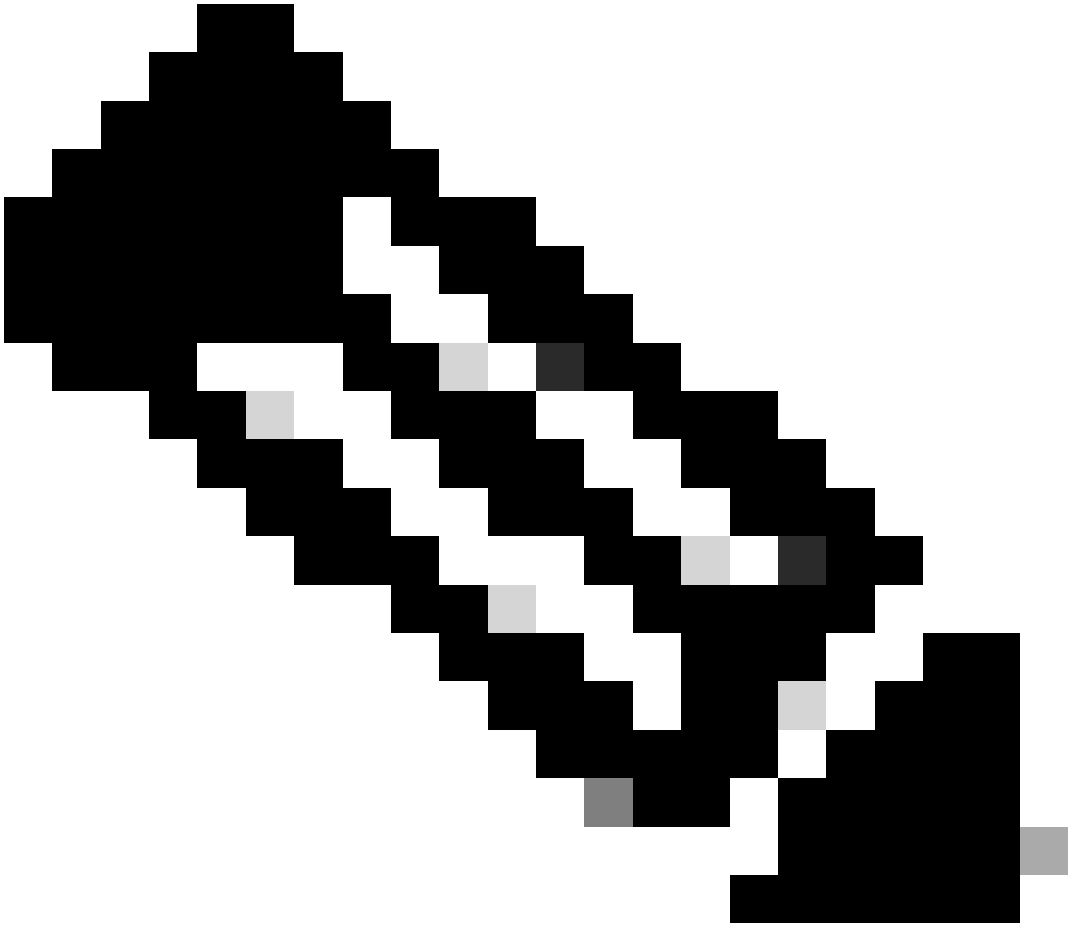
1. no auth -此模式不需要任何身份驗證，也不需要對SNMP資料包進行任何加密。
2. auth -此模式需要驗證SNMP資料包，而不進行加密。
3. priv -此模式要求每個SNMP資料包同時進行身份驗證和加密（隱私）。

必須存在授權引擎ID，才能使用SNMPv3安全機制進行身份驗證或身份驗證和加密-以處理SNMP資料包；預設情況下，引擎ID在本地生成。使用show snmp engineID命令可以顯示引擎ID，如本示例所示：

router#show snmp engineID

本地SNMP引擎ID： 800000090300000152BD35496

遠端引擎ID IP-addr埠



注意：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為SNMPv3配置Cisco IOS XE裝置，並僅使用auth關鍵字對此組啟用身份驗證：

snmp-server group AUTHGROUP v3 auth

此命令使用SNMP伺服器組為SNMPv3配置思科IOS XE裝置。

PRIVGROUP並使用priv關鍵字對此組啟用身份驗證和加密：

snmp-server group PRIVGROUP v3 priv

此命令使用MD5身份驗證口令authpassword和3DES加密口令privpassword配置SNMPv3使用者snmpv3user：

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

請注意，根據RFC 3414的要求，snmp-server user 配置命令不會顯示在該裝置的配置輸出中；因此，使用者密碼無法從配置中檢視。要檢視已配置的使用者，請輸入show snmp user命令，如本示例所示：

router#show snmp user

使用者名稱：snmpv3user Engine ID： 800000090300000152BD35496

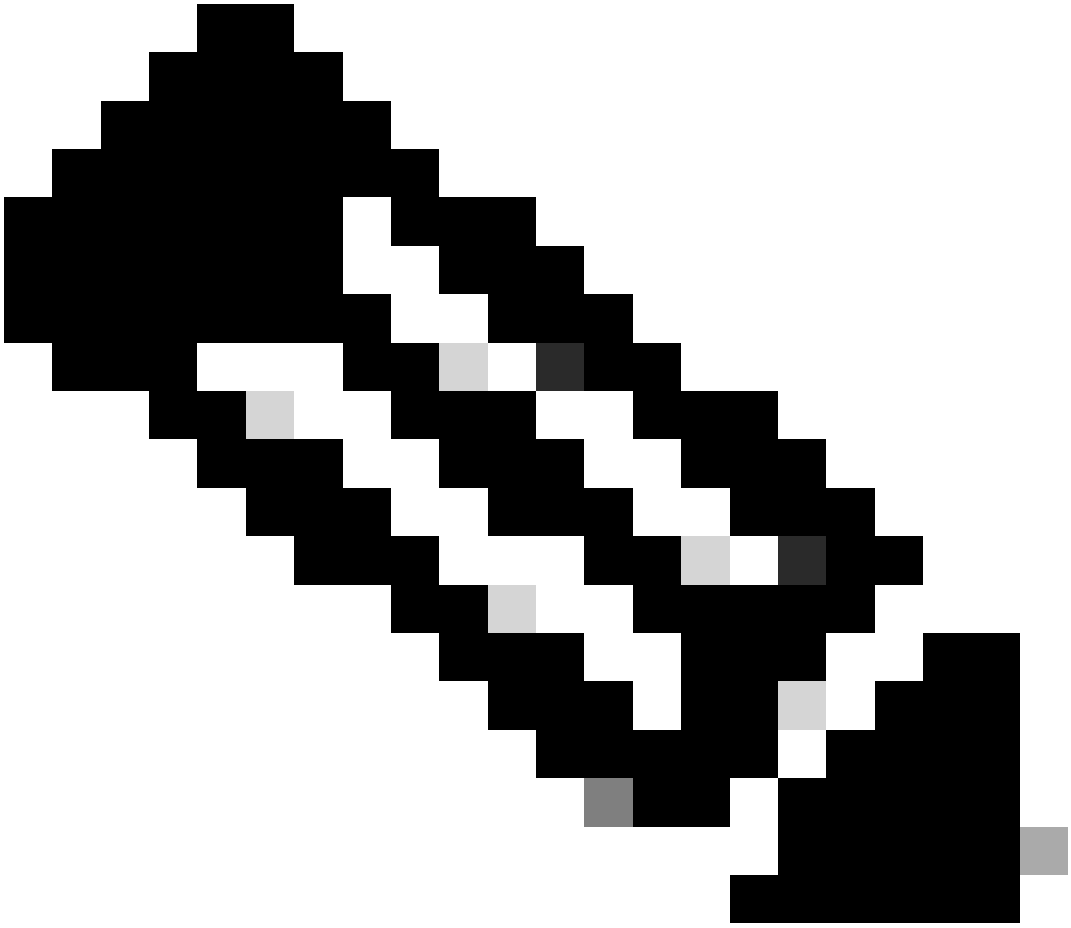
storage-type：非易失主動

身份驗證協定：MD5
隱私協定：3DES
群組名稱：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 XE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流量在裝置上可透過哪些介面終止。MPP功能允許管理員指定一個或多個介面作為管理介面。僅允許管理流量透過這些管理介面進入裝置。啟用MPP後，除了指定的管理介面，其他介面均不接受發往裝置的網路管理流量。



註：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，請參閱瞭解控制層面保護。

在本示例中，MPP用於限制僅對FastEthernet 0/0介面的SNMP和SSH訪問：

控制平面主機

management-interface FastEthernet0/0允許ssh snmp

有關詳細資訊，請參閱管理平面保護功能指南。

日誌記錄最佳實踐

透過事件記錄，您可以檢視Cisco IOS XE裝置的運行情況及其部署到的網路。Cisco IOS XE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，並將日誌記錄對

Cisco IOS XE裝置的影響降至最低。

將日誌傳送到中央位置

建議您將日誌記錄資訊傳送到遠端系統日誌伺服器。這使得能夠更有效地關聯和審計網路裝置之間的網路和安全事件。請注意，系統日誌消息透過UDP以明文形式傳輸時不可靠。因此，可以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），以包括syslog流量。

此配置示例配置Cisco IOS XE裝置，以便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-XE路由器Syslog事件辨識突發事件。

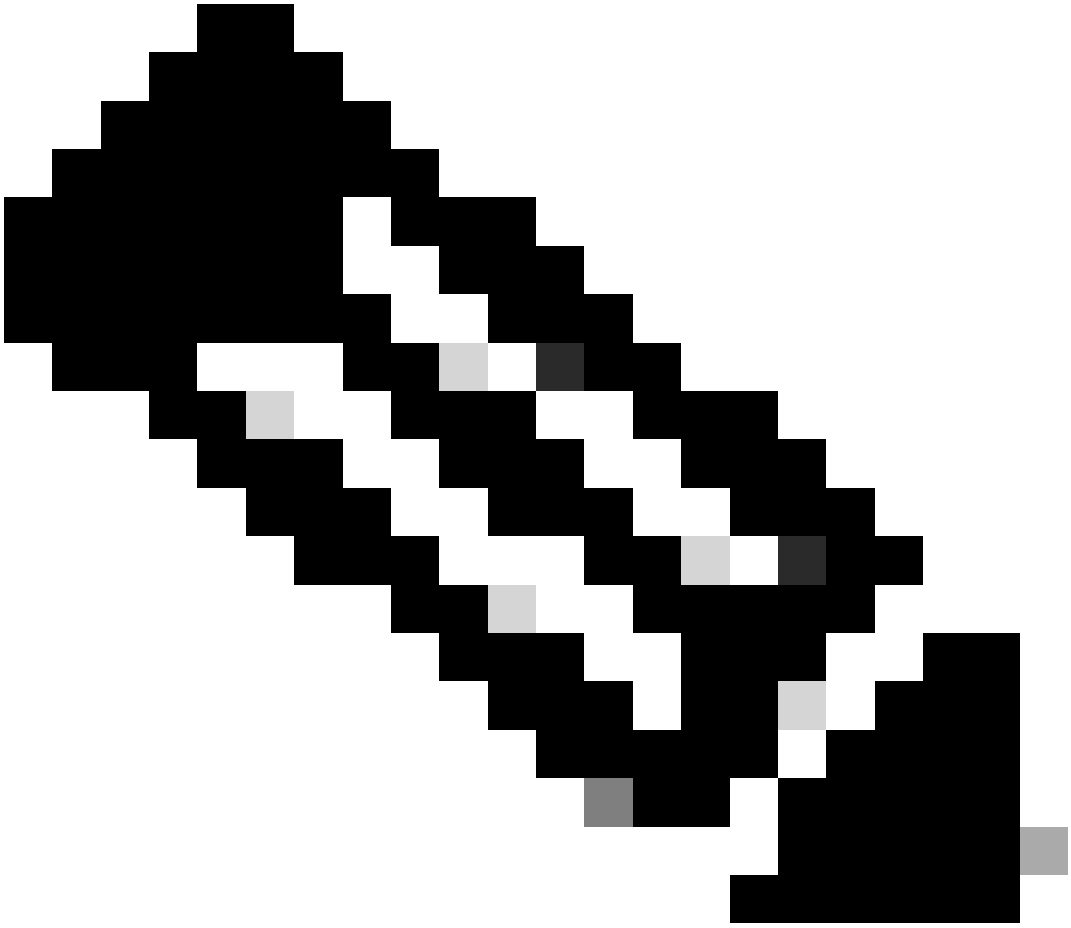
記錄至本機非揮發性儲存體（ATA磁碟）功能可讓系統記錄訊息儲存在進階技術附件(ATA)快閃磁碟上。重新啟動路由器後，儲存在ATA驅動器上的消息將持續存在。

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：

日誌記錄已緩衝。

記錄持續url disk0：/syslog大小134217728 filesize 16384

在將日誌記錄消息寫入ATA磁碟上的檔案之前，Cisco IOS XE軟體會檢查是否有足夠的磁碟空間。否則，將刪除記錄消息的最早檔案（按時間戳），並儲存當前檔案。檔名格式為log_month：day：year：：time。



註：ATA快閃記憶體驅動器的磁碟空間有限，因此需要對其進行維護，以避免儲存資料過載。

本示例顯示如何在維護過程中將日誌記錄消息從路由器ATA隨身碟複製到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，請參閱本地非易失性儲存（ATA磁碟）的日誌記錄。

記錄日誌層次

由Cisco IOS XE裝置生成的每個日誌消息都被分配從級別0（緊急狀態）到級別7（調試）的八個嚴重性之一。除非特別要求，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。

使用全局配置命令 logging trap level可指定要傳送至遠端系統日誌伺服器的日誌記錄消息。指定的級別指示傳送的最低嚴重性消息。對於緩衝的日誌記錄，可以使用logging buffered級別命令。

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制為嚴重性級別6（資訊）到0（緊急）：

logging trap 6

logging buffered 6

不記錄到主控台或監視階段作業

使用Cisco IOS XE軟體，可以將日誌消息傳送到監視會話(監視會話是已發出EXEC命令terminal monitor的互動式管理會話)和控制檯。但是，這可能會提高IOS-XE裝置的CPU負載，因此不推薦使用。建議您將日誌記錄資訊傳送到本地日誌緩衝區，然後可以使用show logging命令檢視這些資訊。

要禁止日誌記錄傳送至控制檯和監視會話，請使用全局配置命令no logging console和no logging monitor。此組態範例顯示使用以下命令：

無記錄主控台

無記錄監視器

有關全局配置命令的詳細資訊，請參閱Cisco IOS XE網路管理命令參考。

使用緩衝記錄日誌

Cisco IOS XE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。強烈建議對控制檯或監視會話使用緩衝日誌記錄，而不是使用日誌記錄。

在配置緩衝的日誌記錄時，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局配置命令logging buffered size來配置。使用logging buffered severity命令配置緩衝區中包括的最低嚴重性。管理員可以透過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

有關緩衝的日誌記錄的詳細資訊，請參閱Cisco IOS XE設定消息顯示目標裝置。

配置日誌記錄源介面

為了在收集和檢視日誌消息時提高一致性級別，建議靜態配置日誌記錄源介面。

透過logging source-interface interface命令可完成此配置，靜態配置日誌記錄源介面可確保從單個CiscoIOS裝置傳送的所有日誌記錄消息中都顯示同一個IP地址。為了增加穩定性，建議您將環回介面用作日誌記錄源。

此配置示例描述了如何使用logging source-interface介面全局配置命令，指定用於所有日誌消息的

環回0介面的IP地址：

logging source-interface Loopback 0

有關詳細資訊，請參閱Cisco IOS XE嵌入式系統日誌管理器。

配置日誌記錄時間戳

記錄時間戳的配置可幫助您跨網路裝置關聯事件。必須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。記錄時間戳可以配置為包括精度為毫秒的日期和時間，並包括裝置上使用的時區。

本示例包括在協調世界時(UTC)區域內以毫秒精度配置日誌記錄時間戳：

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，並配置在生成的日誌消息中顯示該資訊。此範例顯示太平洋標準時間(PST)區域的裝置組態：

時鐘時區PST -8

service timestamps log datetime msec localtime show-timezone

Cisco IOS XE軟體組態管理

Cisco IOS XE軟體套件括多項功能，這些功能可在Cisco IOS XE裝置上啟用某種形式的組態管理。這些功能包括存檔配置和將配置回滾到上一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 XE軟體版本16.6.4及更高版本中，配置替換和配置回滾功能允許您將裝置上的Cisco IOS XE裝置配置存檔。使用configure replace filename命令，可將當前運行的配置替換為此存檔中手動或自動儲存的配置。這與copy filename running-config命令形成對比。configure replace filename命令替換正在運行的配置，而copy命令執行合併操作。

建議您在網路中的所有Cisco IOS XE裝置上啟用此功能。一旦啟用，管理員可使用archive config privileged EXEC命令使當前正在運行的配置增加到檔案中。使用show archive EXEC命令可檢視存檔的配置。

此示例說明了自動配置存檔的配置。它還指示Cisco IOS XE裝置將存檔的配置作為名為archived-config-N的檔案儲存在disk0：檔案系統上，最多保留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）。

查扣

path disk0：archived-config

最大14

time-period 1440

雖然配置存檔功能可以最多儲存14個備份配置，但是，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

在Cisco IOS XE軟體版本16.6.4中增加的獨佔配置更改訪問功能可確保每次僅有一個管理員對Cisco IOS XE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產生的不良影響。使用全局配置命令configuration mode exclusive模式可配置此功能，它可在兩種模式中的任一模式下運行：auto和manual。在自動模式下，當管理員發出configure terminal EXEC命令時，配置自動鎖定。在手動模式下，管理員可在進入配置模式時使用configure terminal lock 命令鎖定配置。

此範例說明自動組態鎖定功能的組態：

配置模式獨佔

數位簽章的思科軟體

在Cisco IOS XE軟體版本16.1及更高版本中增加，數位簽章的思科軟體功能透過使用安全的不對稱（公鑰）加密技術，促進了使用數位簽章的受信任的Cisco IOS XE軟體。

數位簽章的影像會攜帶其本身的加密（私密金鑰）雜湊。在檢查時，裝置從其在金鑰儲存中的金鑰中用相應的公鑰解密該雜湊，並且還計算其自己的影象雜湊。如果解密的雜湊與計算的影象雜湊匹配，則表示影象未被篡改，並且可以信任。

數位簽章的思科軟體金鑰透過金鑰的型別和版本進行標識。金鑰可以是特殊、生產或變換金鑰型別。Production和特殊鍵型別具有關聯的鍵版本，每當撤消和替換鍵時，該鍵版本按字母順序遞增。當您使用數位簽章的思科軟體功能時，ROMMON和常規Cisco IOS XE映像都使用特殊或生產金鑰進行簽名。ROMMON映像可升級，必須使用與載入的特定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isr4300-universalk9.16.06.04.SPA.bin的完整性：

show software authenticity file bootflash：isr4300-universalk9.16.06.04.SPA.bin

有關此功能的詳細資訊，請參閱數位簽章的思科軟體。

然後，可以將新映像(isr4300-universalk9.16.10.03.SPA.bin)複製到要載入的快閃記憶體中，並使用新增加的特殊金鑰驗證映像的簽名

copy /verify tftp://<server_ip>/isr4300-universalk9.16.10.03.SPA.bin flash：

配置更改通知和日誌記錄

在Cisco IOS XE軟體版本16.6.4中增加的配置更改通知和日誌記錄功能使記錄對Cisco IOS XE裝置所做的配置更改成為可能。該日誌在Cisco IOS XE裝置上維護，包含進行更改的個人的使用者資訊、輸入的配置命令以及更改的時間。使用logging enable配置更改記錄器配置模式命令可啟用此功能。由於預設配置會防止記錄密碼資料，要改善預設配置並增加更改日誌的長度，可使用可選命令

hide keys和logging size條目。

建議您啟用此功能，以便更輕鬆地瞭解Cisco IOS XE裝置的配置更改歷史記錄。此外，建議您使用notify syslog 配置命令以允許在做出配置更改時生成syslog消息。

查扣

日誌配置

logging enable

記錄大小200

隱藏鍵

通知系統日誌

啟用「配置更改通知和日誌記錄」功能後，可以使用特權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進程，以便將資料從源裝置移動到目的地。其中包括路由通訊協定，例如邊界閘道通訊協定，以及ICMP和資源保留通訊協定(RSVP)。

管理和資料平面中的事件不能對控制平面產生負面影響，這一點很重要。當資料層面事件（例如DoS攻擊）影響控制層面時，整個網路可能變得不穩定。有關Cisco IOS XE軟體功能和配置的這些資訊有助於確保控制平面的恢復能力。

一般控制層面強化

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

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

IP ICMP重定向

當資料包在同一介面上接收和傳輸時，路由器可生成ICMP重定向消息。在這種情況下，路由器會轉送封包，並將ICMP重新導向訊息傳送回原始封包的傳送者。此行為允許傳送方繞過路由器，將未來的資料包直接轉發到目的地（或靠近目的地的路由器）。在正常運行的IP網路中，路由器僅將重定向消息傳送到其本地子網上的主機。換句話說，ICMP重定向絕不會超出第3層邊界。

ICMP重定向消息有兩種型別：重定向主機地址和重定向整個子網。惡意使用者可以透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，從而強制路由器使用ICMP重定向消息做出響應，並會對路由器的CPU和效能造成負面影響。要防止路由器傳送ICMP重定向消息，請使用no ip redirects介面配置命令。

ICMP不可達

使用介面訪問清單進行過濾可以將ICMP不可達消息傳送回已過濾流量的源。產生這些訊息可能會增加裝置上的CPU使用率。在Cisco IOS XE軟體中，預設情況下，ICMP不可達生成限制為每500毫秒生成一個資料包。使用介面配置命令no ip unreachables可停用生成ICMP不可達消息。使用全局配置命令ip icmp rate-limit unreachable interval-in-ms可更改預設的ICMP不可達消息速率限制。

代理 ARP

代理ARP是一種技術，在該技術中，一台裝置（通常是路由器）應答用於另一台裝置的ARP請求。透過偽造身份，路由器承擔將資料包路由到實際目的地的責任。代理ARP可以幫助子網中的電腦到達遠端子網，而無需配置路由或預設網關。代理ARP在RFC 1027中進行定義。

代理ARP利用率有幾個缺點。它會導致網段上的ARP流量增加，造成資源耗盡和中間人攻擊。代理ARP會呈現資源耗盡攻擊向量，因為每個代理ARP請求會佔用少量記憶體。如果攻擊者傳送大量ARP請求，則可能用盡所有可用的記憶體。

中間人攻擊使網路中的主機能夠欺騙路由器的MAC地址，從而導致毫無戒備的主機向攻擊者傳送流量。使用介面配置命令no ip proxy-arp可停用代理ARP。

有關此功能的詳細資訊，請參閱啟用和停用代理ARP。

NTP控制消息

NTP控制消息查詢是NTP的功能，在建立和利用更好的網路管理功能之前，NTP可協助網路管理(NM)功能。除非您的組織仍在使用NTP for NM功能，否則網路安全最佳做法是將它們一起完全停用。如果使用它們，則它們可以是被防火牆或其他外部裝置阻止的內部網路專用型別服務。它們甚至已從除標準IOS和IOS-XE版本之外的所有版本中刪除，因為IOS-XR和NX-OS不支援它們。

如果您選擇停用此功能，命令是

```
Router (config)# no ntp allow mode control
```

然後，此命令在running-config中顯示為no ntp allow mode control 0。透過執行此操作，您已停用裝置上的NTP控制消息並保護裝置免受攻擊。

限制控制平面流量對CPU的影響

保護控制平面至關重要。由於如果沒有資料和管理流量，應用效能和終端使用者體驗可能會受到影響，因此控制平面的生存能力可確保其他兩個平面的維護和運行。

瞭解控制平面流量

為了適當保護Cisco IOS XE裝置的控制平面，必須瞭解CPU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 XE裝置，必須直接由Cisco IOS XE裝置CPU處理。此流量包含接收鄰接流量類別。此流量包含思科快速轉發(CEF)表中的條目，因此路由器下一跳是裝置本身(透過show ip cef CLI輸出中的詞語receive指示)。此指示適用於需要由

Cisco IOS XE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-目的地超出Cisco IOS XE裝置本身的流量-這需要CPU進行特殊處理。雖然不是影響資料平面流量的詳盡的CPU清單，但這些型別的流量是進程交換的，因此可能影響控制平面的運行：

1. 訪問控制清單日誌記錄- ACL日誌記錄流量包括因使用日誌關鍵字的ACE匹配（允許或拒絕）而生成的任何資料包。
2. 單播反向路徑轉發（單播RPF） -單播RPF與ACL一起使用，可能導致某些資料包的處理交換。
3. IP選項-任何包含選項的IP資料包都必須由CPU處理。
4. 分段-任何需要分段的IP資料包都必須傳遞給CPU進行處理。
5. 存留時間(TTL)到期- TTL值小於或等於一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。
6. ICMP不可達-因路由、MTU或過濾導致ICMP不可達消息的資料包由CPU處理。
7. 需要ARP 請求的流量-不存在ARP條目的目的地需由CPU處理。
8. 非IP流量-所有非IP流量由CPU處理。

   此清單詳細列出了幾種方法，用於確定思科IOS XE裝置CPU處理哪些型別的流量：
9. show ip cef命令提供CEF表中包含的每個IP字首的下一跳資訊。如前所述，包含作為下一跳接收的資料項將被視為接收鄰接，並指示資料流必須直接傳送到CPU。
10. show interface switching命令提供有關裝置進行處理交換的資料包數量的資訊。
11. show ip traffic命令提供有關具有以下特徵的IP資料包的數量的資訊：本地目標（接收鄰接流量）：需要分段的選項，這些選項傳送到傳送到廣播地址空間，然後傳送到多播地址空間。
12. 接收鄰接關係資料流可以透過使用show ip cache flow 命令來辨識。任何目的地為Cisco IOS XE裝置的流量都具有Destination Interface (DstIf) of local。
13. 可以使用控制層面策略來確定到達Cisco IOS XE裝置控制層面的資料流的型別和速率。控制層面策略可以透過使用粒度分類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)會限制與網路裝置之間的外部通訊。

本文檔的「使用基礎設施ACL限制網路訪問」部分詳細介紹了基礎架構ACL。

建議您實施iACL以保護所有網路裝置的控制平面。

接收 ACL

rACL可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，而中轉流量不受rACL的影響。因此，示例ACL條目中使用的目標IP地址any僅指路由器的物理或虛擬IP地址。接收ACL也被視為網路安全最佳實踐，可視為良好網路安全性的長期補充。

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

— 允許來自允許進入裝置的受信任主機的SSH。

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22

— 拒絕從所有其他來源到RP的SSH。

access-list 151 deny tcp any any eq 22

— 允許到裝置的所有其他流量。

— 根據安全策略和配置。

access-list 151 permit ip any any

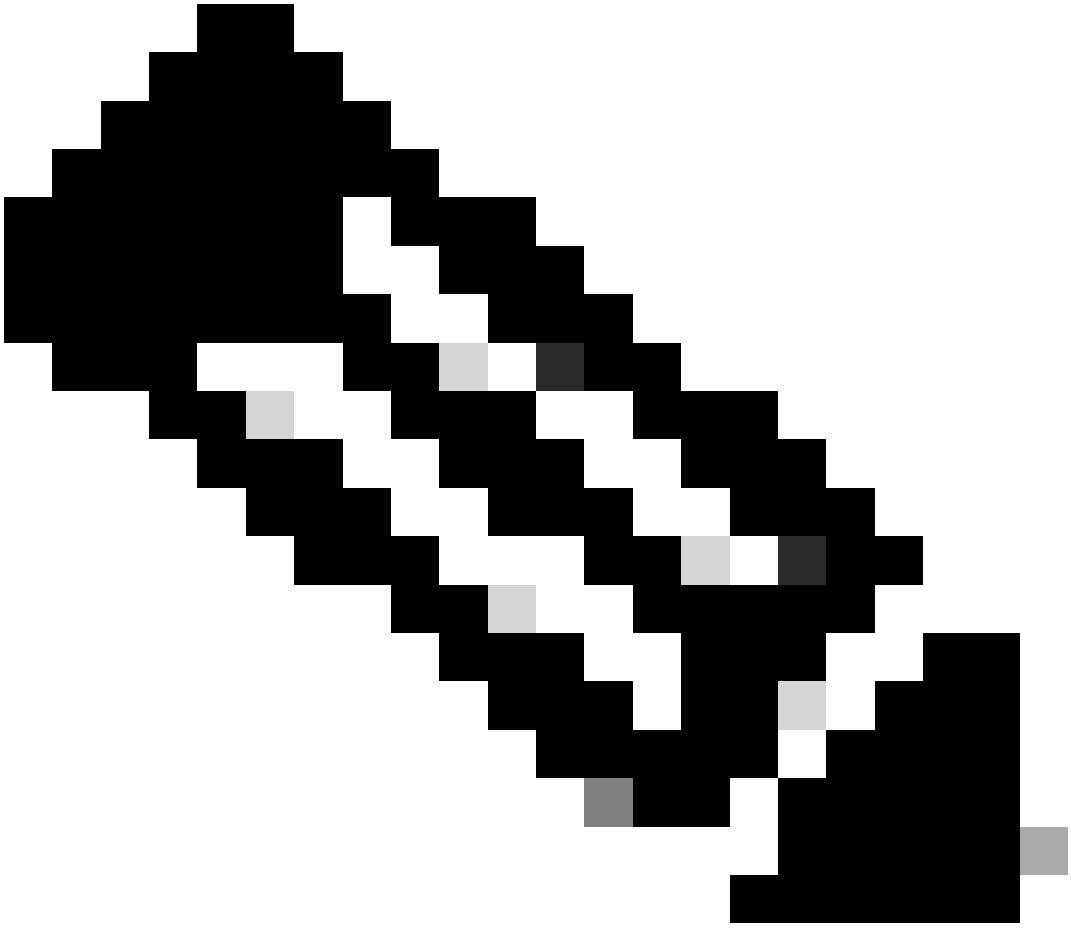
— 將此訪問清單應用於接收路徑。

ip receive access-list 151

請參閱訪問控制清單以幫助標識合法資料流並允許其進入裝置，同時拒絕所有不需要的資料包。

CoPP

CoPP功能還可用於限制發往基礎設施裝置的IP資料包。在本示例中，僅允許來自受信任主機的SSH流量到達Cisco IOS XE裝置CPU。



注意：丟棄來自未知或不受信任的IP地址的流量會阻止具有動態分配IP地址的主機連線到Cisco IOS XE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

控制平面服務策略輸入COPP-INPUT-POLICY

在前面的CoPP示例中，將未授權的資料包與permit操作進行匹配的ACL條目導致這些資料包被policy-map drop函式丟棄，而與deny操作匹配的資料包並不會受到policy-map drop函式的影響。

Cisco IOS XE軟體版本中提供CoPP。

有關配置和使用CoPP功能的詳細資訊，請參閱控制層面策略。

控制平面保護

在Cisco IOS XE軟體版本16.6.4中引入的控制層面保護(CPPr)可用於限制或管制目的地為Cisco IOS XE裝置CPU的控制層面流量。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。存在主機、中轉和CEF-Exception流量類別的子介面。此外，CPPr還包括以下控制層面保護功能：

1. 埠過濾功能-此功能用於管制和丟棄傳送到已關閉或非偵聽TCP或UDP埠的資料包。
2. 隊列閾值功能-此功能限制控制平面IP輸入隊列中允許的指定協定資料包的數量。

有關配置和使用CPPr功能的詳細資訊，請參閱控制層面保護和瞭解控制層面保護(CPPr)。

硬體速率限制器

Cisco Catalyst 6500系列Supervisor引擎32和Supervisor引擎720支援平台特定的基於硬體的速率限制器(HWRL)，適用於特殊網路場景。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預先定義的IPv4、IPv6、單點傳送及多點傳送DoS案例。HWRL可以保護Cisco IOS XE裝置免受需要CPU處理資料包的各種攻擊。

安全BGP

邊界網關協定(BGP)是網際網路的路由基礎。因此，任何連線要求高於一般要求的組織都經常使用BGP。BGP經常成為攻擊者的攻擊目標，因為它無處不在，而且它在較小的組織中設定並忘記了BGP配置的性質。但是，有許多特定於BGP的安全功能可用於提高BGP配置的安全性。

這提供了最重要的BGP安全功能的概述。在適當情況下，會提出配置建議。

基於TTL的安全保護

每個IP資料包包含一個稱為生存時間(TTL)的1位元組欄位。IP資料包經過的每個裝置都會將此值遞減1。起始值因作業系統而異，通常介於64到255之間。當封包的TTL值達到零時，就會捨棄該封包。

基於TTL的安全保護稱為通用TTL安全機制(GTSM)和BGP TTL安全攻擊(BTSH)，它利用IP資料包的TTL值，以確保收到的BGP資料包來自直接連線對等體。此功能通常需要來自對等路由器的協調；但是，一旦啟用，它就可以完全抵禦許多針對BGP的基於TCP的攻擊。

可以使用BGP路由器配置命令neighbor的ttl-security選項啟用用於BGP的GTSM。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>

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

使用MD5進行BGP對等驗證

使用MD5進行的對等驗證會建立作為BGP會話一部分傳送的每個資料包的MD5摘要。具體來說，IP和TCP報頭、TCP負載和金鑰的一部分用於生成摘要。

然後，建立的摘要將儲存在TCP選項Kind 19中，該選項是RFC 2385專門為了此目的而建立的。接收BGP揚聲器使用相同的演算法和金鑰來重新生成消息摘要。如果接收和計算的摘要不相同，資料包將被丟棄

使用neighbor BGP路由器配置命令的password選項配置使用MD5進行的對等驗證。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>

有關使用MD5進行BGP對等驗證的詳細資訊，請參閱鄰居路由器驗證。

配置最大字首數

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必須消耗的記憶體就越多。在某些配置中，可以儲存所有Internet字首的子集，例如在僅利用預設路由或提供商使用者網路的路由的配置中。

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對等體配置一個限制。

使用neighbor maximum-prefix BGP路由器配置命令配置此功能時，需要使用一個引數：在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>

有關對等最大字首的詳細資訊，請參閱配置BGP最大字首功能。

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透過BGP傳送或接收的特定字首。儘可能使用首碼清單，以確保網路流量透過預期路徑傳送。字首清單可以在入站和出站方向應用到每個eBGP對等體。

配置的字首清單將傳送或接收的字首限制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不可行，則可將字首清單配置為專門阻止已知的不良字首。這些已知的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。出站字首清單可以配置為僅專門允許組織打

算通告的字首。

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

有關BGP字首過濾的全面介紹，請參閱基於字首的出站路由過濾。

使用自治系統路徑訪問清單過濾BGP字首

BGP自主系統(AS)路徑訪問清單允許使用者根據字首的AS-path屬性過濾已接收和通告的字首。這可以與字首清單結合使用，以便建立一組強大的過濾器。

此配置示例使用AS路徑訪問清單，以便將入站字首限制為遠端AS發出的字首，將出站字首限制為本地自治系統發出的字首。源自所有其他自治系統的字首會被過濾，而不會安裝在路由表中。

ip as-path access-list 1 permit

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

安全內部網關協定

網路正確轉發流量並從拓撲更改或故障中恢復的能力取決於拓撲的準確檢視。通常可以運行內部網關協定(IGP)來提供此檢視。預設情況下，IGP是動態的，會發現與使用中的特定IGP通訊的其他路由器。IGP還會發現網路鏈路故障期間可以使用的路由。

以下小節概述了最重要的IGP安全功能。

在適當的時候提供了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的路由協定驗證和驗證

如果無法保護路由資訊交換，攻擊者就會將錯誤的路由資訊引入網路。透過在路由器之間使用密碼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。

當您將MD5雜湊功能增加到身份驗證過程時，路由更新不再包含明文密碼，並且路由更新的整個內容更不易被篡改。但是，如果選擇弱密碼，則MD5身份驗證仍然容易遭受暴力攻擊和詞典攻擊。建議您使用具有足夠隨機化的密碼。由於MD5身份驗證比密碼身份驗證安全得多，因此這些示例特定於MD5身份驗證。IPSec也可用於驗證和保護路由協定，但是這些示例沒有詳細介紹其用法。

EIGRP和RIPv2使用金鑰鏈作為配置的一部分。有關配置和使用「金鑰鏈」的詳細資訊，請參閱key。

以下是使用MD5進行EIGRP路由器身份驗證的示例配置：

金鑰鏈<金鑰名稱>

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。

金鑰鏈<金鑰名稱>

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的OSPF路由器身份驗證的示例配置。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

可以使用有助於對路由資訊的通告進行控制的passive-interface 命令來防範資訊洩漏或IGP中引入偽造的資訊。建議不要將任何資訊通告給不受您管理控制的網路。

此範例示範此功能的用法：

router eigrp <as-number> passive-interface default

no passive-interface <interface>

路由過濾

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，路由將在介面上發生，但被通告或處理的資訊將受到限制。

對於EIGRP和RIP，使用distribute-list命令及out關鍵字可限制通告的資訊，而使用in關鍵字可限制處理的更新。distribute-list命令可用於OSPF，但它並不能禁止路由器傳播已過濾的路由。可以改用 area filter-list 命令。

本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>

本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通告和處理的更多資訊，請參閱EIGRP路由過濾。

本OSPF示例將字首清單與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>

製程處理資源消耗

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其他字首而增加。為了防止資源耗盡，必須配置路由協定以限制資源消耗。如果使用Link State Database Overload Protection（鏈路狀態資料庫超載保護）功能，OSPF中可能會出現這種情況。

此示例演示了OSPF鏈路狀態資料庫超載保護功能的配置：

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

有關OSPF鏈路狀態資料庫超載保護的詳細資訊，請參閱限制OSPF進程的自生成LSA的數量。

安全第一跳冗餘協定

第一跳冗餘協定(FHRP)為充當預設網關的裝置提供恢復能力和冗餘。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。此類通訊可使攻擊者偽裝成講FHRP的裝置，從而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，思科IOS XE軟體支援的所有FHRP都包含具有MD5或文本字串的身份驗證功能。由於未經身份驗證的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

GLBP身份驗證***的說***

glbp 1身份驗證md5 key-string <glbp-secret>

glbp 1 ip 10.1.1.1

interface FastEthernet 2

HSRP身份驗證******說明

standby 1 authentication md5 key-string <hsrp-secret>

standby 1 ip 10.2.2.1

interface FastEthernet 3

VRRP身份驗證******說明

vrrp 1 authentication md5 key-string <vrrp-secret>

vrrp 1 ip 10.3.3.1

資料平面

雖然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。因此，保護網路裝置安全時，保護管理和控制平面（優先於資料平面）非常重要。

但是，在資料平面本身中，有許多功能和配置選項可以幫助保護流量。以下各節詳細介紹這些功能和選項，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，這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的使用也與資料層面的強化相關。

有關詳細資訊，請參閱本文檔的使用中轉ACL過濾中轉資料流部分。

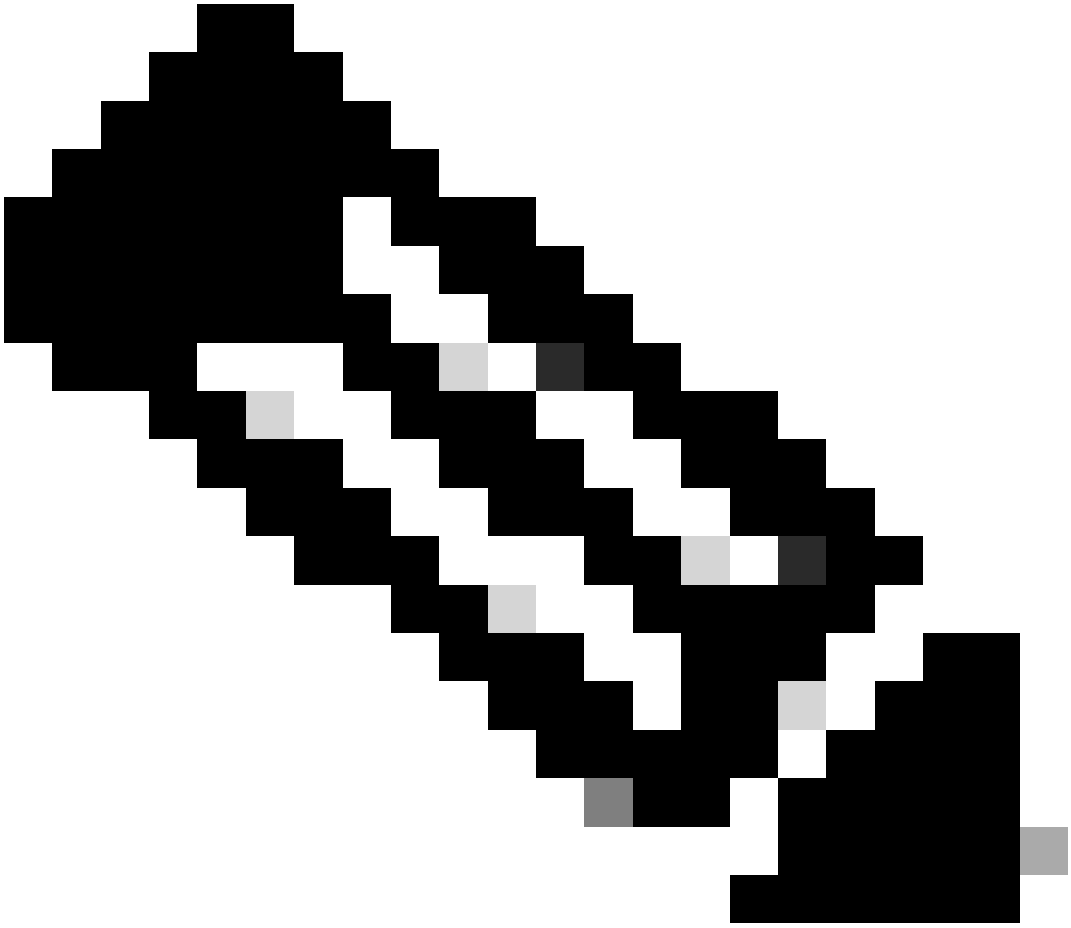
IP選項選擇性丟棄

IP選項存在兩個安全問題。包含IP選項的流量必須由Cisco IOS XE裝置進行進程交換，這可能導致更高的CPU負載。IP選項還包括更改流量透過網路的路徑的功能，這可能會使其破壞安全控制。

由於這些問題，全局配置命令ip options {drop | ignore}被增加到Cisco IOS XE軟體版本16.6.4及更高版本。使用此命令的第一種形式(即ip options drop)時，所有由Cisco IOS XE裝置接收的包含IP選項的IP資料包都會被丟棄。這可以防止IP選項所啟用的高CPU負載和可能的安全控制被顛覆。

使用此命令的第二種形式(即ip options ignore)可以將Cisco IOS XE裝置配置為忽略接收的資料包中包含的IP選項。雖然這確實可以緩解與本地裝置的IP選項相關的威脅，但存在IP選項可能會影響下游裝置。正是由於此原因，強烈建議使用此命令的drop形式。以下組態範例說明了其中原由：

ip options drop



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

一旦啟用「IP選項選擇性丟棄」，就可以使用show ip traffic EXEC命令確定由於存在IP選項而被丟棄的資料包的數量。此資訊顯示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。

停用IP源路由

IP來源路由會同時使用鬆散來源路由和記錄路由選項，或嚴格來源路由和記錄路由選項，以使IP資料包的來源能夠指定封包採用的網路路徑。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」功能完全停用IP選項，則停用IP源路由非常重要。預設情況下，所有Cisco IOS XE軟體版本中均已啟用IP源路由，該功能可透過no ip source-route全局配置命令停用。

此組態範例說明此命令的使用：

no ip source-route

停用ICMP重定向

ICMP重定向用於向網路裝置通知指向IP目標的更好路徑。預設情況下，Cisco IOS XE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，攻擊者可能會導致Cisco IOS XE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重定向傳輸。使用介面配置no ip redirects命令可停用ICMP重定向，如示例配置中所示：

interface FastEthernet 0

no ip redirects

停用或限制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。到達遠端網路後，轉發IP裝置將資料包作為第2層廣播傳送到子網上的所有站點。這種定向廣播功能已被用作包括smurf攻擊在內的若干攻擊中的放大和反射輔助。

Cisco IOS XE軟體的當前版本預設情況下停用此功能；但是，可以透過ip directed-broadcast介面配置命令啟用此功能。預設情況下，12.0之前的Cisco IOS XE軟體版本會啟用此功能。

如果網路確實需要定向廣播功能，則可以控制其使用。使用訪問控制清單作為ip directed-broadcast命令的選項可實現此目標。此配置示例將定向廣播限制為源自受信任網路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定向廣播100

使用傳輸ACL過濾傳輸流量

使用傳輸ACL (tACL)可以控制哪些流量經過網路。這與基礎架構ACL相反，後者會尋求過濾發往網路本身的流量。當需要過濾到特定裝置組的流量或流經網路的流量時，tACL提供的過濾是有益的。

傳統上，此類過濾由防火牆執行。但是，在某些情況下，對網路中的Cisco IOS XE裝置執行此過濾可能會有幫助，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適當位置。

有關詳細資訊，請參閱本文檔的反欺騙保護部分。

有關tACL的詳細資訊，請參閱傳輸訪問控制清單：在邊緣進行過濾。

ICMP封包過濾

網際網路控制訊息通訊協定(ICMP)是設計為IP的控制通訊協定。因此，它傳達的消息一般對TCP和IP協定會有深遠的影響。網路故障排除工具ping和traceroute以及路徑MTU發現都使用ICMP；但是，網路的正常運行很少需要外部ICMP連線。

Cisco IOS XE軟體提供特定功能，可按名稱或型別及代碼過濾ICMP訊息。此範例ACL允許來自信任網路的ICMP，但會封鎖來自其他來源的所有ICMP封包：

ip access-list extended ACL-TRANSIT-IN

— 僅允許來自受信任網路的ICMP資料包

permit icmp host <trusted-networks> any

— 拒絕所有其他IP流量傳輸至任何網路裝置

拒絕icmp any any

過濾IP片段

如本文檔前面的使用基礎架構ACL限制對網路的訪問部分中的詳細說明，過濾分段的IP資料包可能會對安全裝置提出難題。

由於分段處理的非直觀性質，ACL經常會無意中允許IP分段。分段還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分段經常用於攻擊，並且可以在任何已配置的tACL的頂部顯式過濾。

ACL包括對IP分段的全面過濾。此範例中所示的功能必須與先前範例的功能搭配使用：

ip access-list extended ACL-TRANSIT-IN

— 拒絕使用特定於協定的ACE幫助的IP分段

— 攻擊流量分類

拒絕tcp any any片段

deny udp any any fragments

拒絕icmp any any片段

deny ip any any fragments

有關ACL處理分段的IP資料包的詳細資訊，請參閱分段的訪問清單處理。

對過濾IP選項的ACL支援

在Cisco IOS XE軟體版本16.6.4及更高版本中，Cisco IOS XE軟體支援使用ACL根據資料包中包含的IP選項過濾IP資料包。資料包中存在IP選項可能表示有人試圖破壞網路中的安全控制，或者更改資料包的傳輸特性。正是由於這些原因，才可以在網路邊緣過濾帶有IP選項的資料包。

此示例必須與前面示例中的內容一起使用，以包括對包含IP選項的IP資料包進行完全過濾：

ip access-list extended ACL-TRANSIT-IN

— 拒絕包含IP選項的IP資料包

deny ip any any option any-options

反欺騙保護

許多攻擊使用源IP地址欺騙來達到有效目的，或者隱藏攻擊的真正來源並阻止準確回溯。Cisco IOS XE軟體提供單點傳播RPF和IP來源防護(IPSG)，可防止依賴來源IP位址詐騙的攻擊。此外，ACL和空路由通常作為防止欺騙的手動方法部署。

IP源防護透過執行交換機埠、MAC地址和源地址驗證，最大限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網路的欺騙攻擊。埠安全可用於驗證接入層的MAC地址。動態地址解析協定(ARP)檢測(DAI)緩解了在本地網段上使用ARP毒化的攻擊媒介。

單播RPF

單播RPF使裝置能夠驗證轉發資料包的源地址是否可透過接收該資料包的介面到達。不能依賴單播RPF作為唯一防止欺騙的保護。如果存在通向源IP地址的適當返迴路由，則偽造的資料包可以透過啟用了單播RPF的介面進入網路。單播RPF依賴於您在每台裝置上啟用思科快速轉發，並且基於每個介面進行配置。

單播RPF可以配置為兩種模式之一：鬆散或嚴格。在存在非對稱路由的情況下，首選鬆散模式，因為已知嚴格模式在這些情況下會丟棄資料包。在配置ip verify介面配置命令期間，關鍵字any用於配置鬆散模式，而關鍵字rx用於配置嚴格模式。

此範例說明此功能的設定：

ip cef

interface <interface>

ip verify unicast source reachable-via <mode>

有關配置和使用單播RPF的詳細資訊，請參閱瞭解單播反向路徑轉發。

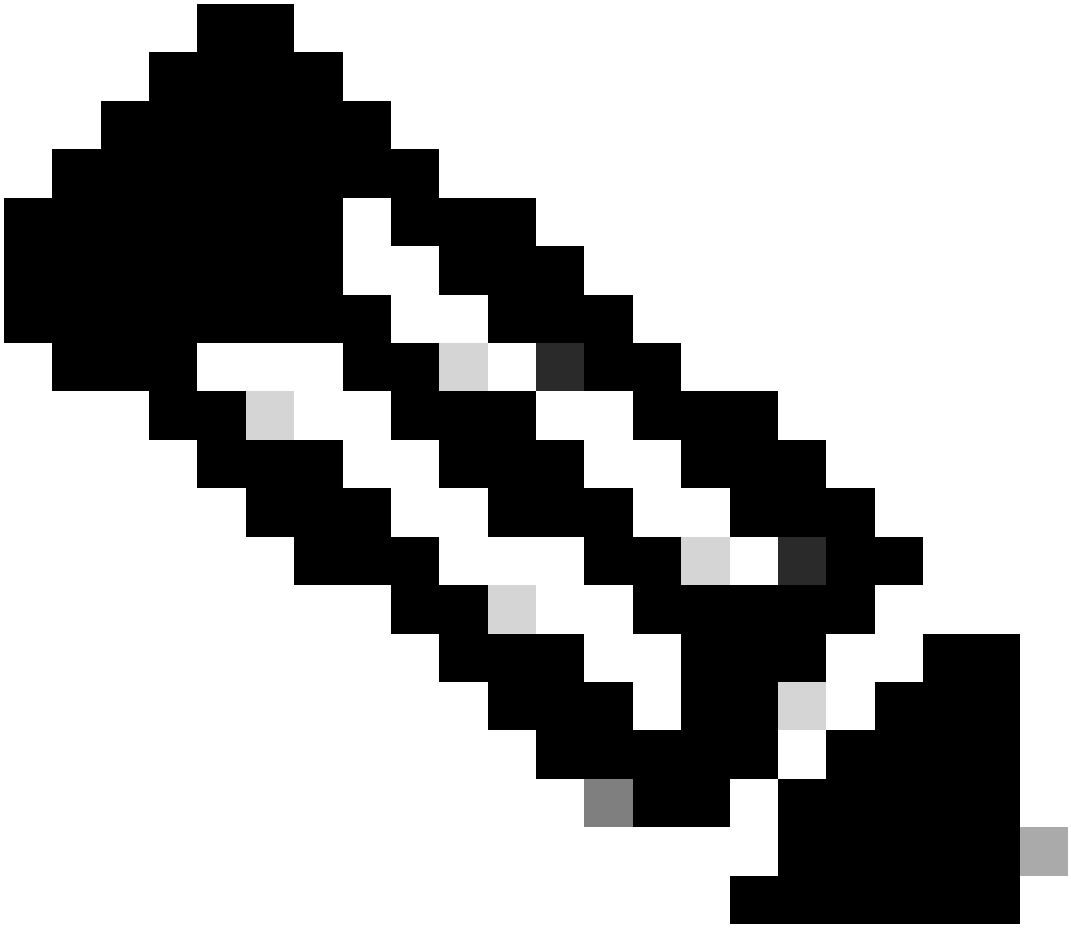
IP來源防護

IP源防護是一種有效的防止欺騙手段，如果您可以控制第2層介面，就可以使用該方法。IP源防護使用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。這些命令啟用DHCP監聽：

ip dhcp snooping

ip dhcp snooping vlan <vlan-range>



註：要支援IP源防護，機箱/路由器需要第2層交換模組。

可以使用ip verify source port security interface 配置命令來啟用埠安全。這需要使用全局配置命令ip dhcp snooping information option；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IP源防護。

連線埠安全性

埠安全用於緩解接入介面上的MAC地址欺騙。埠安全可以使用動態獲取的（粘滯）MAC地址來簡化初始配置。一旦連線埠資安判斷出MAC違規，就可以使用四種違規模式之一。這些模式包括protect、restrict、shutdown和shutdown VLAN。在埠僅使用標準協定為單個工作站提供訪問的情況下，最多可以有一個足夠的數量。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

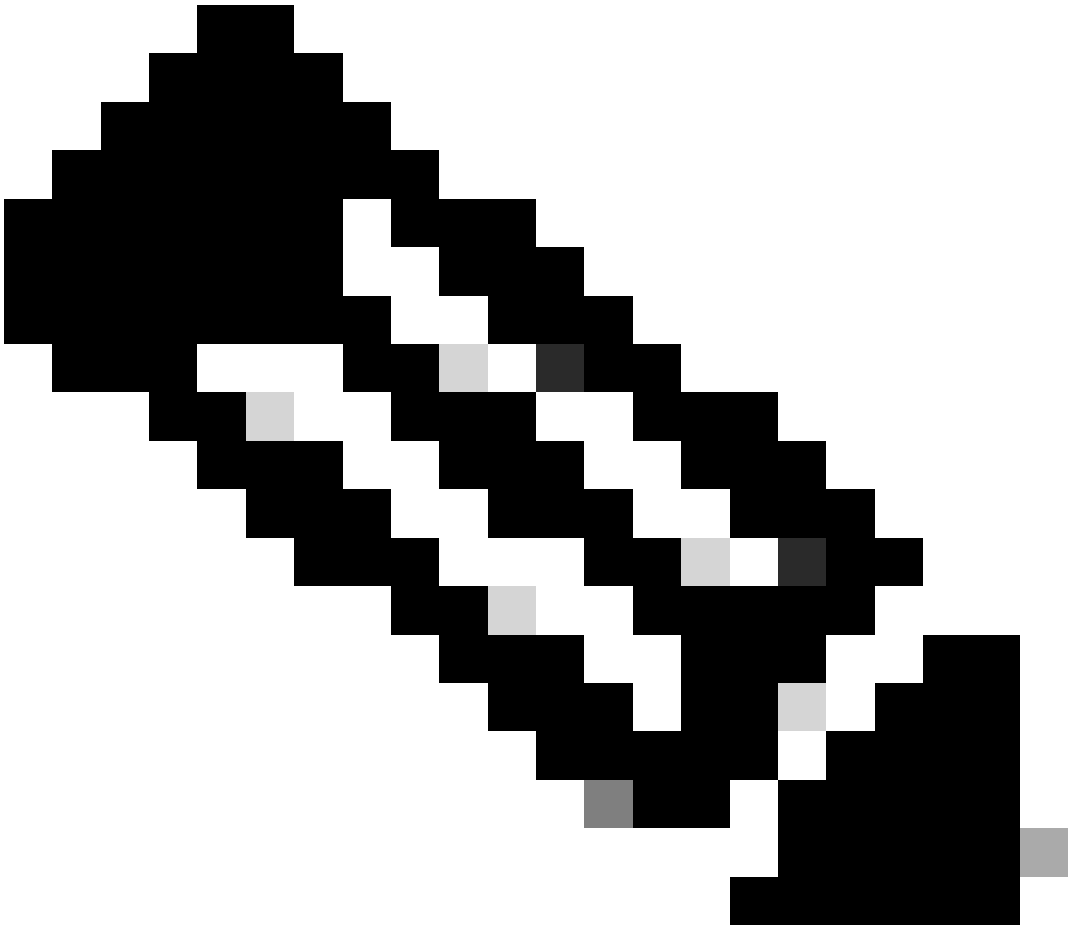
switchport mode access

switchport port-security

switchport port-security mac-address sticky

switchport port-security maximum <number>

switchport port-security violation <violation-mode>



注意：為了支援埠安全，機箱/路由器需要第2層交換模組。

有關埠安全配置的詳細資訊，請參閱配置埠安全。

反欺騙ACL

手動配置的ACL可以提供靜態防欺騙保護，防止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的一個元件應用於網路邊界處的入口流量。反欺騙ACL需要定期

監控，因為它們可能會頻繁更改。如果應用出站ACL將流量限制到有效的本地地址，則可以從本地網路發起的流量中最小化欺騙。

此示例演示如何使用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。如果配置這些型別的ACL，請查詢具有結論性的最新參考。

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

有關如何配置訪問控制清單的詳細資訊，請參閱配置IPv4 ACL。

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透過裝置將資料包和幀轉發到最終目的地。這些資料包傳輸網路中部署的裝置，可能會影響裝置的CPU操作。可對資料平面（包括經過網路裝置的流量）進行保護，以確保管理和控制平面的運行。如果中轉流量會導致裝置處理交換機流量，則裝置的控制平面可能會受到影響，從而導致運行中斷。

影響CPU的功能和資料流型別

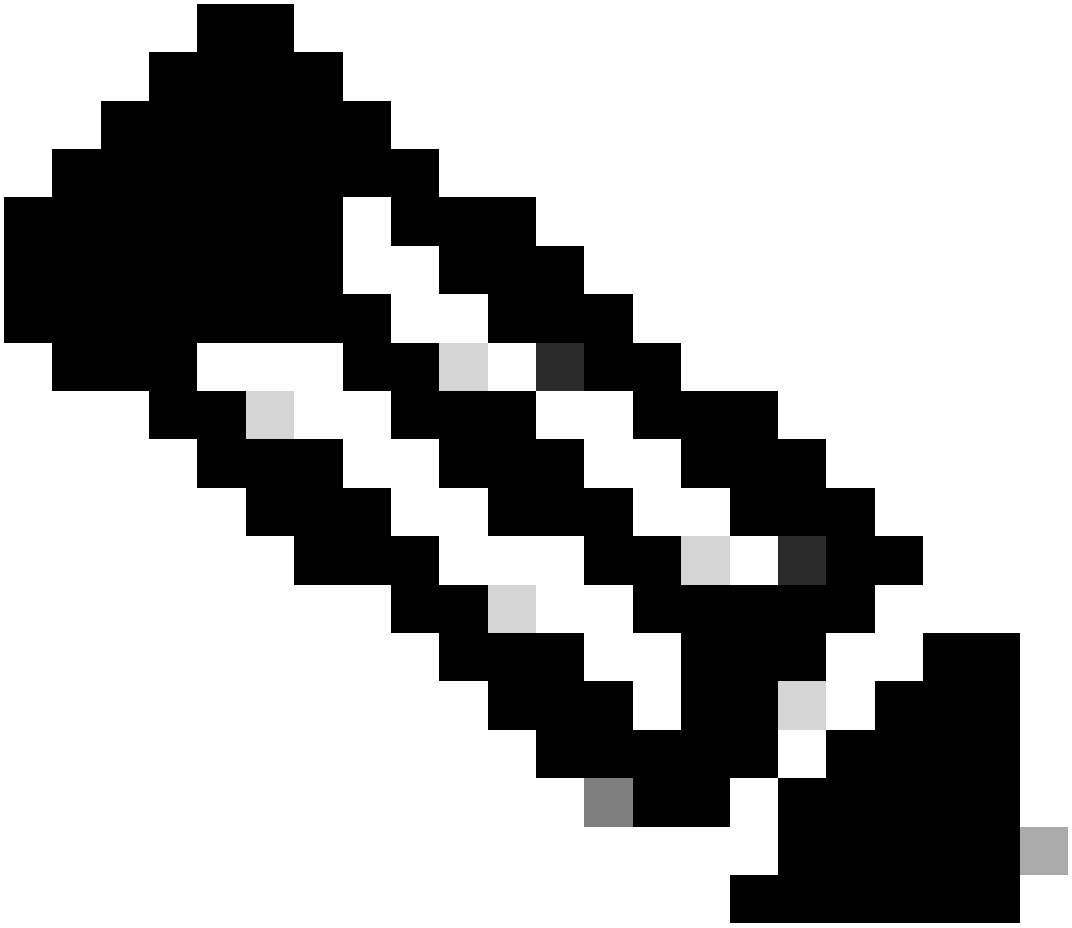
雖然並非詳盡無遺，但此清單包含需要特殊CPU處理且由CPU進行進程交換的資料平面流量型別：

1. ACL日誌記錄- ACL日誌記錄流量包括因使用日誌關鍵字的ACE匹配（允許或拒絕）而生成的任何資料包。
2. 單播RPF -單播RPF與ACL一起使用可能會導致某些資料包的處理交換。
3. IP選項-任何包含選項的IP資料包都必須由CPU處理。
4. 分段-任何需要分段的IP資料包都必須傳遞給CPU進行處理。
5. 存留時間(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。
6. ICMP不可達-因路由、MTU或過濾導致ICMP不可達消息的資料包由CPU處理。
7. 需要ARP請求的流量-不存在ARP條目的目標需要CPU進行處理。
8. 非IP流量-所有非IP流量由CPU處理。

有關資料層面強化的詳細資訊，請參閱本文檔的一般資料層面強化部分。

按TTL值篩選

您可以使用Cisco IOS XE軟體版本16.6.4中引入的擴充IP存取清單中之「根據TTL值過濾的ACL支援」功能，根據TTL值過濾封包。此功能可用於保護接收中轉流量的裝置，其中TTL值為0或1。還可以使用基於TTL值過濾資料包，以確保TTL值不小於網路的直徑，從而保護下游基礎設施裝置的控制平面免受TTL到期攻擊。



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

此ACL示例建立了一個策略，用於過濾TTL值小於6的IP資料包。

— 建立過濾具有TTL值的IP資料包的ACL策略。

— 小於6

ip access-list extended ACL-TRANSIT-IN

deny ip any any ttl lt 6

permit ip any any

— 將access-list應用於入口方向的介面。

interface GigabitEthernet 0/0

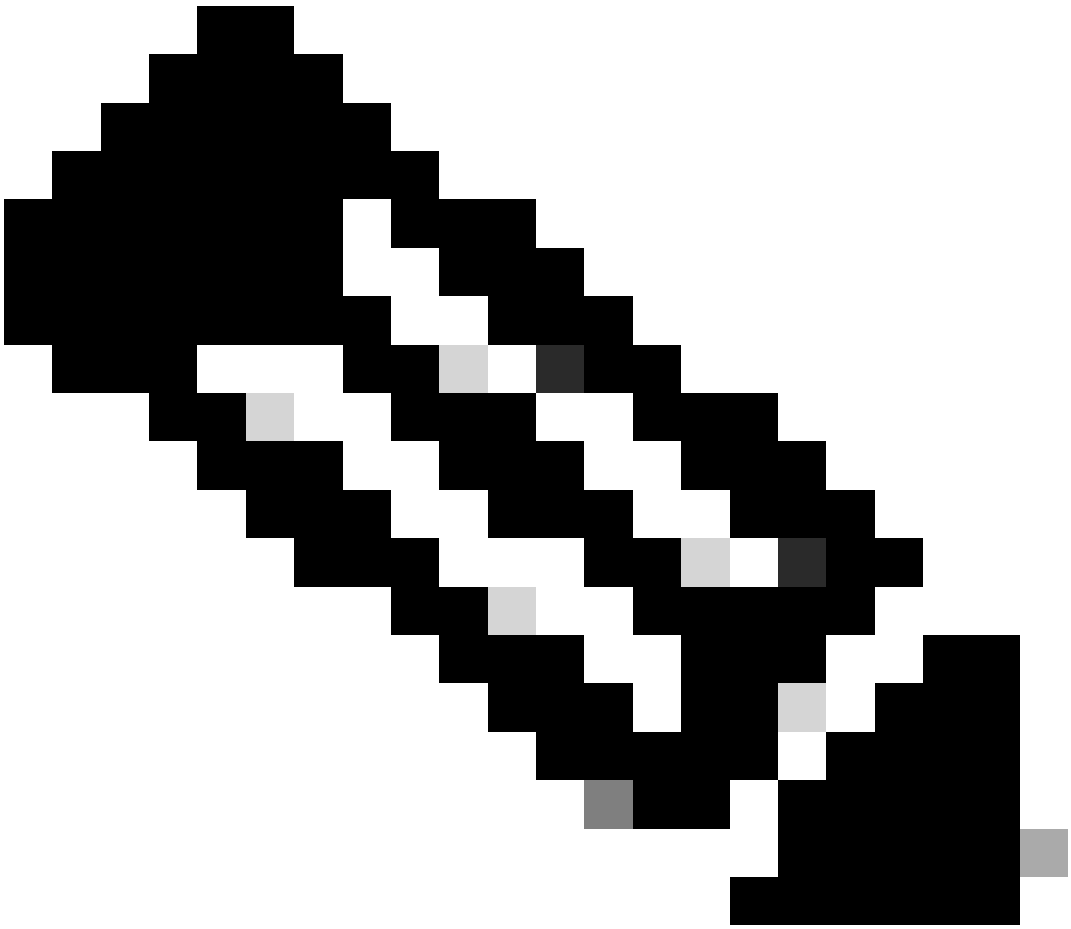
ip access-group ACL-TRANSIT-IN

有關基於TTL值過濾資料包的詳細資訊，請參閱辨識和防範TTL到期攻擊。

有關此功能的詳細資訊，請參閱對按TTL值過濾的ACL支援。

基於是否存在IP選項過濾

在Cisco IOS XE軟體版本16.6.4及更高版本中，可以在命名擴展IP訪問清單中使用ACL對過濾IP選項的支援功能來過濾具有IP選項的IP資料包。還可以使用基於存在IP選項過濾IP資料包，以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。



注意：對過濾IP選項的ACL支援功能只能用於命名擴展ACL。

還可以注意到，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將無法正常運行。如果網路中使用這些協定，則可以使用ACL對過濾IP選項的支援；但是，ACL IP選項選擇性丟棄功能可能會丟棄此流量，並且這些協定無法正常運行。如果沒有使用需要IP選項的協定，則首選使用ACL IP選項選擇性丟棄來丟棄這些資料

包。

此ACL示例建立過濾包含任何IP選項的IP資料包的策略：

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

此示例ACL演示了一個策略，該策略使用五個特定IP選項過濾IP資料包。包含這些選項的資料包將被拒絕：

1. 0選項清單結尾(eool)
2. 7記錄路由(record-route)
3. 68時間戳記（時間戳記）
4. 131 -鬆散源路由(lsr)
5. 137 -嚴格源路由(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選項lsr

deny ip any any選項ssr

permit ip any any

interface GigabitEthernet 0/0

ip access-group ACL-TRANSIT-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層面強化部分。

Cisco IOS XE軟體中的另一個功能可用於使用IP選項篩選封包，是CoPP。在Cisco IOS XE軟體版本16.6.4及更高版本中，CoPP允許管理員過濾控制平面資料包的流量。支援Cisco IOS XE軟體版本16.6.4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策略將丟棄裝置收到的中轉資料包：

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

police 80000 conform transmit exceed drop

控制平面

service-policy input COPP-POLICY ！

存在以下IP選項時，此CoPP策略丟棄裝置接收的中轉資料包：

1. 0選項清單結尾(eool)
2. 7記錄路由(record-route)
3. 68時間戳記（時間戳記）
4. 131鬆散源路由(lsr)
5. 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

police 80000 conform transmit exceed drop

控制平面

service-policy input COPP-POLICY

在前面的CoPP策略中，將資料包與permit操作進行匹配的訪問控制清單條目(ACE)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，則不會受到policy-map drop函式的影響。

有關CoPP功能的詳細資訊，請參閱部署控制層面策略。

控制平面保護

在Cisco IOS XE軟體版本16.6.4和更新版本中，可以使用控制層面保護(CPPr)來限制或管制Cisco IOS XE裝置的CPU控制層面流量。與CoPP類似，CPPr能夠限制或管制使用比CoPP更精細粒度的流量。CPPr將聚合控制平面劃分為三個單獨的控制平面類別，稱為子介面：存在主機、中轉和CEF-Exception子介面。

此CPPr策略丟棄TTL值小於6的裝置接收的中轉資料包，以及TTL值為零或1的裝置接收的中轉或非中轉資料包。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

警察80000符合動作丟棄

class ACL-IP-OPTIONS-CLASS

警方8000符合動作刪除

policy-map CPPR-TRANSIT-POLICY

class ACL-IP-TTL-LOW-CLASS

警方8000符合動作刪除

控制平面傳輸

service-policy input CPPR-TRANSIT-POLICY

在前面的CPPr策略中，將資料包與permit操作進行匹配的訪問控制清單條目導致這些資料包被policy-map drop函式丟棄，而與deny操作（未顯示）匹配的資料包，則不會受到policy-map drop函式的影響。

有關CPPr功能的詳細資訊，請參閱控制層面策略。

流量辨識和回溯

有時，您需要快速辨識和回溯網路流量，尤其是在事件響應或網路效能不佳期間。NetFlow和分類ACL是使用Cisco IOS XE軟體實現此目標的兩種主要方法。NetFlow可提供對網路上所有流量的可視性。此外，NetFlow可以透過收集器實施，這些收集器可以提供長期趨勢和自動化分析。分類ACL是ACL的一個元件，需要預先規劃以辨識特定流量並在分析期間進行手動干預。以下各節提供每個功能的簡要概述。

Netflow

NetFlow透過跟蹤網路流量來辨識異常且與安全相關的網路活動。可以透過CLI檢視和分析NetFlow資料，也可以將資料導出到商業或免費的NetFlow收集器以進行聚合和分析。NetFlow收集器可透過長期趨勢分析提供網路行為和使用情況分析。NetFlow透過分析IP資料包中的特定屬性並建立流來運行。版本5是最常用的NetFlow版本，但版本9更易於擴展。NetFlow流可以在高流量環境中使用取樣流量資料建立。

CEF或分散式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組態。在Cisco IOS XE軟體的早期版本中，用於在介面上啟用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>

下面是CLI的NetFlow輸出示例。SrcIf屬性有助於回溯。

router#show ip cache flow IP packet size distribution(資料包總數26662860)：

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 .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

IP流交換快取，4456704位元組

55個活動，65481個非活動，1014683增加

41000680 ager輪詢，0個流分配失敗

活動流在2分鐘內超時

非活動流超時時間為60秒

IP子流快取，336520位元組

110 active、16274 inactive、2029366 added1014683added to flow

0分配失敗，0強制釋放1個資料塊，15個資料塊增加最後清除統計資訊從未

協定總流資料包位元組資料包活動（秒）空閒（秒）

--------流/秒/流/包/秒/流/流

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

合計：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本地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本地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Flexible NetFlow。

分類ACL

分類ACL提供對穿越介面的流量的可視性。分類ACL不會改變網路的安全策略，其構建通常是為了對各個協定、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。這種對特定ACE中的流量進行更精細的分類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，以幫助辨識被拒絕流量的型別。

管理員可以透過將分類ACL與show access-list和clear ip access-list counters EXEC命令一起使用來加快事件響應速度。

此示例說明了分類ACL的配置，該配置用於在預設拒絕之前辨識SMB流量：

ip access-list extended ACL-SMB-CLASSIFY

註釋ACL的現有內容

註釋特定於SMB的TCP流量的分類

deny tcp any any eq 139

deny tcp any any eq 445

deny ip any any

要標識使用分類ACL的資料流，可以使用show access-list acl-name

EXEC命令。使用clear ip access-list counters aclname EXEC命令可清除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個匹配）

20 deny tcp any any eq 445（9個匹配）

30 deny ip any any（184個匹配）

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對非路由流量或第2層流量提供訪問控制。建立PACL的語法高於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。

此範例使用擴充的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> <目標地址> <目標埠> ！

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

有關配置PACL的詳細資訊，請參閱使用埠ACL配置網路安全的「埠ACL」部分。

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只能有一個隔離VLAN，並且只有混合埠可以與隔離VLAN中的埠通訊。隔離VLAN可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。此示例還將介面FastEthernet 1/1配置為VLAN 11中的隔離埠：

vlan 11專用vlan隔離

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

配置為社群VLAN的輔助VLAN允許VLAN成員之間的通訊，以及主要VLAN中任意混雜埠的通訊。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。必須使用Community VLAN將需要連線的伺服器分組，但不需要連線到VLAN中的所有其它裝置。這種情況常見於可公開訪問的網路或伺服器向不可信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 12是主VLAN 20的輔助VLAN。

vlan 12專用vlan社群

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

結論

本檔案簡要概述可用於保護Cisco IOS XE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。在本概述中，將討論管理、控制和資料層面的保護，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，為您提供進一步評估所需的資訊。

致謝

本文檔中的一些功能說明由思科資訊開發團隊編寫。

附錄：Cisco IOS XE裝置強化清單

本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 XE裝置使用的所有強化功能，即使該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每個選項的潛在風險。

管理平面

1. 密碼
   啟用和本機使用者密碼的MD5雜湊（密碼選項）設定密碼重試鎖定停用密碼復原（考慮風險

）
2. 停用未使用的服務
3. 為管理會話配置TCP keepalive
4. 設定記憶體和CPU閾值通知
5. 設定
   記憶體和CPU閾值通知保留記憶體供控制檯訪問記憶體洩漏檢測器緩衝區溢位檢測增強的崩潰資訊收集
6. 使用iACL限制管理訪問
7. 篩選（考慮風險）
   ICMP資料包IP片段IP選項TTL資料包值
8. 控制平面保護
   配置埠過濾配置隊列閾值
9. 管理存取
   使用管理平面保護來限制管理介面設定exec超時對CLI訪問使用加密傳輸協定（例如SSH）對vty和tty線路使用控制傳輸（訪問類選項）警告應使用標語
10. 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
11. SNMP
    配置SNMPv2社群並應用ACL配置SNMPv3
12. 記錄
    配置集中記錄設定所有相關元件的記錄級別設定記錄源介面配置記錄時間戳粒度
13. 組態管理
    替換和回滾獨佔配置更改訪問軟體可復原配置配置更改通知。

控制平面

1. 停用（考慮風險）
   ICMP重定向ICMP不可達代理ARP
2. 如果使用NTP，則配置NTP身份驗證
3. 配置控制層面策略/保護（埠過濾、隊列閾值）
4. 安全路由協定
   BGP（TTL、MD5、最大字首、字首清單、系統路徑ACL）IGP（MD5、被動介面、路由過濾、資源消耗）
5. 配置硬體速率限制器
6. 安全第一躍點備援通訊協定(GLBP、HSRP、VRRP)

資料平面

1. 配置IP選項選擇性丟棄
2. 停用（考慮風險）
   IP源路由IP定向廣播ICMP重定向
3. 限制IP定向廣播
4. 配置tACL（考慮風險）
   過濾器ICMPFilter IP fragmentsFilter IP optionsFilter TTL值

5. 配置所需的反欺騙保護
   ACL IP源防護動態ARP檢測單播RPLIP埠安全
6. 控制層面保護（控制層面cef-excef）
7. 配置NetFlow和分類ACL以辨識流量
8. 配置所需的訪問控制ACL（VLAN對映、PACL、MAC）
9. 配置專用VLAN

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。