使用指南保護ASA防火牆

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

- 相關產品
- 慣例

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

- 強化管理平面
  - 密碼管理
- 啟用HTTP服務
- 啟用SSH
- 設定登入階段作業逾時
- 密碼管理
- 配置本地使用者和加密密碼
- 設定啟用密碼
- 為啟用模式配置AAA身份驗證
- 驗證、授權和記帳
  - TACACS+ 驗證
- ASA映像簽名和驗證
- 配置時鐘時區
- 配置NTP
- DHCP伺服器服務（若未使用）
- Control-Plane Access-list
- 從ASA

用於直通流量

- TCP序列號隨機化
- TTL遞減
- dnsguard
- 設定片段鏈片段檢查
- 配置協定檢查
- 配置單播反向路徑轉發

威脅檢測
殭屍網路過濾器
為未連線的子網增加ARP快取
記錄與監控
配置SNMP
SNMP社群字串
啟用SNMP讀取訪問
啟用SNMP陷阱
配置系統日誌
配置控制檯日誌記錄嚴重性級別
配置日誌消息中的時間戳
配置Netflow
保護配置
配置中的密碼
服務密碼復原
疑難排解

簡介

本文檔介紹用於幫助您保護Cisco ASA裝置的資訊，這些裝置可提高網路的整體安全性。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科主動安全裝置(ASA) 9.16(1)及更高版本。

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

本文檔分為4部分。

1. 管理平面強化-這適用於所有與ASA相關的管理/SNMP、SSH等裝置流量。
2. Securing config -用於停止為運行配置等填充密碼的命令。
3. 日誌記錄和監控-這適用於與ASA上的日誌記錄相關的任何設定。
4. 透過流量-這適用於透過ASA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。

相關產品

此配置還可用於Cisco ASA軟體版本9.1x。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

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思科ASA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PSIRT上可以找到安全建議及響應。

在Cisco安全漏洞策略中可以找到有關這些通訊手段的其他資訊。

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、授權和記帳部分。

集中記錄收集與監控

要瞭解與安全事件相關的現有、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。

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。

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。

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 ASA裝置配置中，組態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 ASA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 ASA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。

強化管理平面

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。以下協定清單由管理平面使用：

- 簡單網路管理協定
- 安全殼層通訊協定
- 檔案傳輸通訊協定
- 簡單檔案傳輸協定
- 安全複製協定
- TACACS+
- RADIUS
- Netflow
- 網路時間協定
- 系統日誌
- ICMP
- 中小企業

 注意：建議不要啟用TELNET，因為它是純文字檔案。

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。

ASA 9.7(1)引入了本地口令的PBKDF2雜湊功能。所有長度的本地使用者名稱和啟用口令都使用基於口令的金鑰派生函式2 (PBKDF2)雜湊儲存在配置中。以前，32個字元或更短的密碼使用基於MD5的雜湊方法。現有的密碼將繼續使用基於MD5的雜湊，除非您輸入新密碼。有關降級指南，請參閱《一般操作配置指南》中的「軟體和配置」一章。

啟用HTTP服務

要使用ASDM，您需要啟用HTTPS伺服器，並允許HTTPS連線到ASA。安全裝置允許每個情景最多有5個併發ASDM例項（如果有），所有情景之間最多有32個ASDM例項。要配置ASDM訪問，請使用：

```
http server enable <port>
```

僅允許ACL清單中所需的IP。允許廣泛的訪問不是一種好的做法。

```
http 0.0.0.0 0.0.0.0 <interface>
```

配置ASDM訪問控制：

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

```
// Set server version
ASA(config)# ssl server-version tlsv1 tlsv1.1 tlsv.1.2

// Set client version
ASA(config) # ssl client-version tlsv1 tlsv1.1 tlsv.1.2
```

ASA按預設順序啟用了這些密碼。

```
ciscoasa(config)# ssl cipher ?

configure mode commands/options:
  default   Specify the set of ciphers for outbound connections
  dtlsv1    Specify the ciphers for DTLSv1 inbound connections
  dtlsv1.2  Specify the ciphers for DTLSv1.2 inbound connections
  tlsv1     Specify the ciphers for TLSv1 inbound connections
  tlsv1.1   Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2   Specify the ciphers for TLSv1.2 inbound connections
ciscoasa(config)# ssl cipher dtlsv1 ?

configure mode commands/options:
  all     Specify all ciphers
  low     Specify low strength and higher ciphers
  medium  Specify medium strength and higher ciphers
  fips    Specify only FIPS-compliant ciphers
  high    Specify only high-strength ciphers
  custom  Choose a custom cipher configuration string.
```

預設ishigh。

- all關鍵字指定使用所有密碼：hmac-sha1 hmac-sha1-96 hmac-sha2-256 hmac-md5 hmac-md5-96
- custom關鍵字指定自定義密碼加密配置字串，用冒號分隔。
- fips關鍵字僅指定符合FIPS的密碼：hmac-sha1 hmac-sha2-256
- high關鍵字僅指定高強度密碼（預設）： hmac-sha2-256
- low關鍵字指定低、中、高強度密碼：hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256
- medium關鍵字指定中等強度和高強度密碼：hmac-sha1 hmac-sha1-96hmac-sha2-256

預設情況下，ASA使用臨時自簽名證書，該證書在每次重新啟動時更改。如果您正在尋找單一憑證，您可以使用此連結來產生永久自簽憑證。

ASA支援TLS 1.2版用於ASDM、無客戶端SSVPN和AnyConnect VPN的安全消息傳輸。 已引入或修改了以下命令：ssl client-version、ssl server-version、ssl cipher、ssl trust-point、ssl dh-group、show ssl、show ssl cipher、show vpn-sessiondb。

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
```

```
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
```

```
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

啟用SSH

ASA允許SSH連線到ASA以進行管理。ASA允許每個情景最多5個併發SSH連線（如果有），每個情景之間最多分配100個連線。

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

預設金鑰對型別為常規金鑰。預設模數大小為1024。用於儲存金鑰對的NVRAM空間量因ASA平台而異。如果生成超過30個金鑰對，則可以達到限制。

要刪除指定型別（rsa或dsa）的金鑰對，

```
crypto key zeroize { rsa | eddsa | ecdsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

為遠端裝置訪問配置SSH：

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

要使用Diffie-Hellman (DH)組1、DH組14或Curve25519金鑰交換方法交換金鑰，請在全局配置模式下使用ssh key-exchange命令，從9.1(2)開始，ASA支援SSH的dh-group14-sha1。

```
ASA(config)#ssh key-exchange group dh-group14-sha256
```

設定登入階段作業逾時

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

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。

配置本地使用者和加密密碼

```
username <local_username> password <local_password> encrypted
```

設定啟用密碼

```
enable password <enable_password> encrypted
```

為啟用模式配置AAA身份驗證

```
ASA(config)#aaa authentication enable console LOCAL
```

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+是一種身份驗證協定，ASA可以使用該協定對遠端AAA伺服器的管理使用者進行身份驗

證。這些管理使用者可透過SSH、HTTPS、Telnet或HTTP訪問ASA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。

可以使用如下示例的類似配置在Cisco ASA裝置上啟用TACACS+身份驗證：

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

ASA映像簽名和驗證

從軟體版本9.3.1開始，現在使用數位簽章對ASA映像進行簽名。數位簽章在ASA啟動後驗證。

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Embedded Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
Computed Hash SHA-512: 0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
CCO Hash      SHA-512: 1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
Signature Verified


ASA(config)# verify /signature running
Requesting verify signature of the running image...

Starting image verification
Hash Computation:    100% Done!
Computed Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c


Get key records from key storage: PrimaryASA, key_store_type: 6
Embedded Hash   SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
                      26ce7a5fb4b424e5e21636c6c8a7d665
                      1e688834203dfb7ffa6eaefc7fdf9d3d
                      1d0a063a20539baba72c2526ca37771c

Returned. rc: 0, status: 1
The digital signature of the running image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
 Signer Information
```

```
 Common Name : abraxas
 Organization Unit : ASAv
 Organization Name : CiscoSystems
 Certificate Serial Number : 550DBBD5
 Hash Algorithm : SHA2 512
 Signature Algorithm : 2048-bit RSA
 Key Version : A
```

配置時鐘時區

```
clock timezone GMT <hours offset>
```

配置NTP

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。系統日誌需要準確可靠的時間，例如在潛在攻擊的取證調查期間，以及依靠證書進行第1階段身份驗證時，VPN連線是否成功。

- 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。 ntp server ip_address [key key_id] [source interface_name] [prefer]
- 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 authenticate命令啟用身份驗證，為此伺服器設定受信任的金鑰ID。如果您啟用身份驗證，則ASA僅會在資料包中使用正確的受信任金鑰時與NTP伺服器通訊。要啟用NTP伺服器的身份驗證，請在全局配置模式下使用ntp authenticate命令。

```
ASA(config)#ntp authenticate
```

DHCP伺服器服務（若未使用）

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

注意：ASA不支援CDP。

Control-Plane Access-list

直接到裝置管理資料流(由http、ssh或telnet等命令定義)的訪問控制規則的優先順序高於使用控制平面選項應用的訪問清單。因此，即使裝置訪問清單明確拒絕此類允許的管理流量，也可以允許它們進入。

```
access-list <name> in interface <Interface_name> control-plane
```

從ASA

以下是可用於將檔案複製/傳輸到ASA的協定。

純文字：

- FTP
- HTTP
- TFTP
- 中小企業

安全：

- HTTPS
- Secure Copy Client (SCP) ASA支援SCP客戶端向SCP伺服器傳輸檔案或從SCP伺服器傳輸檔案。

用於直通流量

TCP序列號隨機化

每個TCP連線都有兩個ISN：一個由客戶端生成，另一個由伺服器生成。ASA隨機分配在入站和出站方向傳遞的TCP SYN的ISN。

隨機化受保護主機的ISN可防止攻擊者為新連線預置下一個ISN並可能劫持新會話。

如果需要，可以停用TCP初始序列號隨機化。舉例來說：

- 如果另一個串聯防火牆也在隨機化初始序列號，則無需兩個防火牆執行此操作，即使此操作不會影響流量。
- 如果您透過ASA使用eBGP多跳，並且eBGP對等體使用MD5。隨機化會中斷MD5校驗和。
- 如果我們使用的WAAS裝置要求ASA不隨機化連線序列號。

TTL遞減

預設情況下，IP報頭中的TTL不會遞減，因為在執行Traceroute時ASA不會顯示為路由器躍點。

dnsguard

每個查詢強制執行一個DNS響應。可在全局配置模式下使用命令啟用該功能。

```
ASA(config)#dns-guard
```

設定片段鏈片段檢查

要對資料包分段進行附加管理並改進與NFS的相容性，請在全局配置模式下使用fragment命令。

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

配置協定檢查

對於在使用者資料包中嵌入IP定址資訊的服務，或在動態分配的埠上打開輔助通道的服務，需要檢查引擎。這些協定要求ASA執行深度資料包檢測，而不是透過快速路徑傳輸資料包。因此，檢測引擎可能會影響整體吞吐量。有關應用層協定檢查的詳細資訊，請參閱ASA 9.4配置指南。

可以使用此命令在ASA上啟用檢測。

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

預設情況下，ASA全局啟用了global_policy。

配置單播反向路徑轉發

```
ip verify reverse-path interface <interface_name>
```

當流量由於RPF檢查而被丟棄時，這會顯示ASA增量上的asp丟棄計數器。

<#root>

```
ASA(config)# show asp drop

Frame drop:
  Invalid TCP Length (invalid-tcp-hdr-length)                    21

  Reverse-path verify failed (rpf-violated)                      90


// Check Reverse path statistics

ASA(config)# sh ip verify statistics

interface inside: 11 unicast rpf drops


interface outside: 79 unicast rpf drops
```

威脅檢測

威脅檢測為防火牆管理員提供了必要的工具，以便在攻擊到達內部網路基礎設施之前辨識、瞭解和阻止攻擊。為此，該功能依賴於許多不同的觸發器和統計資訊，以下各節將對此進行更詳細的介紹。

有關ASA上的威脅檢測的詳細說明，請參閱ASA威脅檢測功能和配置。

殭屍網路過濾器

BotNet流量過濾器監控內部DNS客戶端和外部DNS伺服器之間的域名伺服器(DNS)請求和響應。處理DNS響應時，會根據已知惡意域資料庫檢查與響應相關聯的域。如果存在匹配項，則會阻止發往DNS響應中存在的IP地址的任何進一步流量。

惡意軟體是安裝在未知主機上的惡意軟體。當惡意軟體開始與已知錯誤IP地址連線時，殭屍網路流量過濾器可以檢測到試圖傳送私有資料（密碼、信用卡號、擊鍵或專有資料）等網路活動的惡意軟體。殭屍網路流量過濾器根據包含已知錯誤域名和IP地址的動態資料庫（阻止清單）檢查傳入和傳出連線，然後記錄或阻止任何可疑活動。

您還可以將所選阻止清單地址增加到靜態阻止清單中，以補充思科動態資料庫。如果動態資料庫包含您認為無法阻止列出的被阻止清單地址，您可以手動將其輸入到靜態允許清單中。允許的清單地址仍會生成系統日誌消息，但由於您僅針對阻止的清單系統日誌消息，因此它們僅供參考。有關詳細資訊，請參閱配置殭屍網路流量過濾器。

為未連線的子網增加ARP快取

預設情況下，對於非直接連線的子網IP地址，ASA不會對ARP做出響應。如果ASA上的NAT IP不屬於該ASA介面的同一子網IP，則可能必須在ASA上為NATted IP啟用arp permit-nonconnected to proxy-ARP。

```
arp permit-nonconnected
```

始終建議上游和下游裝置上使用正確的路由，這樣NAT才能在不啟用之前命令的情況下正常工作。

記錄與監控

配置SNMP

本節重點介紹幾種方法，可用於保護ASA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

團體字串是應用於ASA裝置的密碼，用於限制對裝置上SNMP資料的訪問，包括只讀和讀寫訪問。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。

啟用SNMP讀取訪問

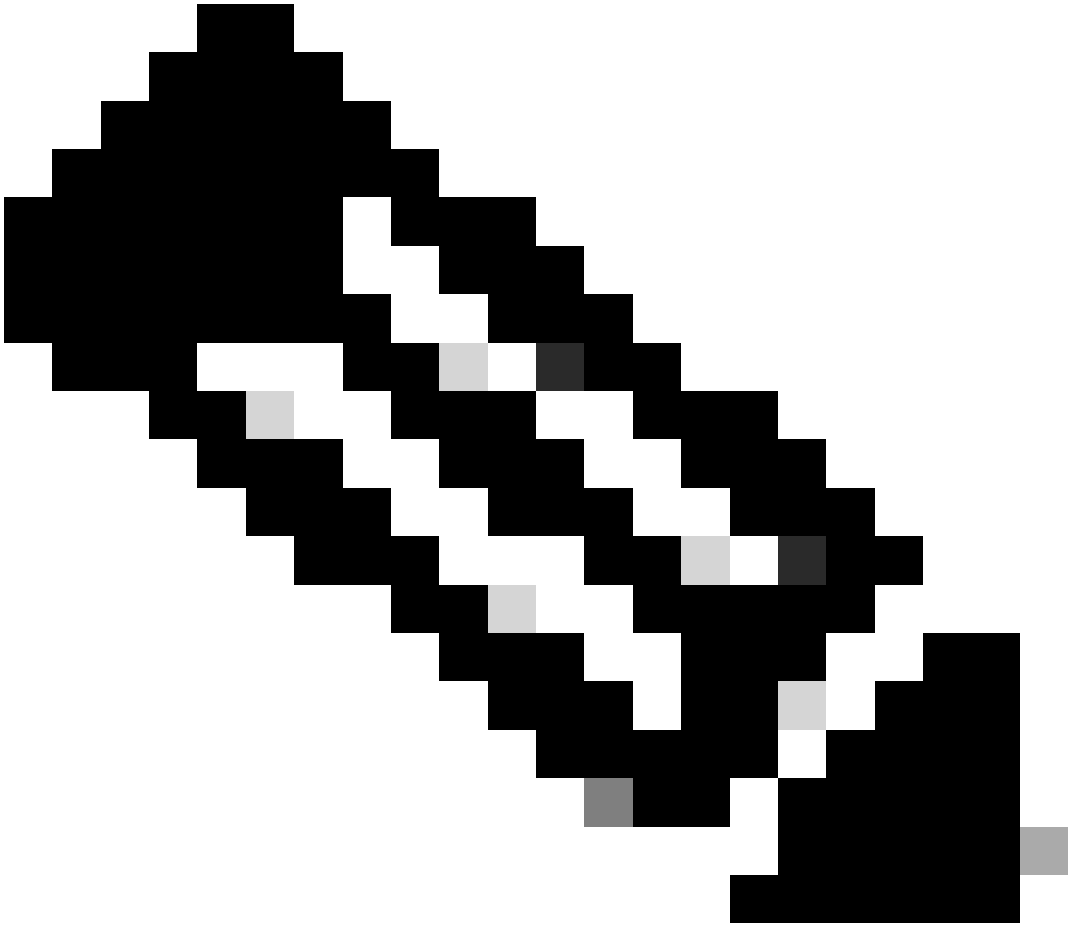
```
snmp-server host <interface_name> <remote_ip_address>
```

啟用SNMP陷阱

```
snmp-server enable traps all
```

配置系統日誌

建議向遠端系統日誌伺服器傳送日誌記錄資訊。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。



注意：UDP以明文形式傳輸系統日誌消息是不可靠的。

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。可將日誌配置為從ASA傳送到此目標：

- ASDM
- 緩衝區
- 快閃記憶體
- 電子郵件
- FTP伺服器
- SNMP伺服器作為陷阱
- 系統日誌伺服器

配置控制檯日誌記錄嚴重性級別

```
logging console critical
```

還提供基於TCP的系統日誌。所有系統日誌都可以以明文形式或加密形式傳送到TCP情況下的系統日誌伺服器。

純文字

logging host interface_name syslog_ip [tcp/埠

已加密

logging host interface_name syslog_ip [tcp/埠 | [安全]

如果無法與syslogs伺服器建立TCP連線，則會拒絕所有新連線。可以透過輸入logging permit-hostdown 命令更改此預設行為。

配置日誌消息中的時間戳

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。

```
logging timestamp
```

有關與syslog相關的其他資訊，請參閱ASA Syslog配置示例。

配置Netflow

有時，您可能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。

Cisco ASA支援NetFlow版本9服務。NSEL的ASA和ASASM實施提供了一種有狀態IP流跟蹤方法，該方法僅導出指示流中重大事件的記錄。在有狀態流跟蹤中，跟蹤流經過一系列狀態更改。NSEL事件用於導出有關流狀態的資料，並由導致狀態更改的事件觸發。

有關ASA上的Netflow的詳細資訊，請參閱Cisco ASA NetFlow實施指南：

保護配置

配置中的密碼

所有密碼和金鑰都經過加密或混淆（例如，加密或混淆）。show running-config不會顯示實際密碼。

此類備份不能用於ASA上的備份/恢復。出於恢復目的而執行的備份將使用命令more system：running-config執行。 ASA配置密碼可以使用主要密碼短語加密。有關詳細資訊，請參閱

口令加密。

服務密碼復原

停用此選項可以停用口令恢復機制並停用對ROMMON的訪問。從丟失或忘記的密碼中恢復的唯一方法可以是ROMMON擦除所有檔案系統，包括配置檔案和映像。您可以備份配置，並具備從ROMMON命令列恢復映像的機制。

疑難排解

沒有可用的故障排除資訊。

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）。