Cisco ASA上的VPN過濾器配置示例

目錄

簡介

本檔案將詳細介紹VPN過濾器，並適用於LAN到LAN(L2L)、Cisco VPN使用者端和Cisco AnyConnect安全行動化使用者端。

過濾器由一些規則組成，這些規則根據源地址、目標地址和協定等標準來確定是允許還是拒絕通過安全裝置的隧道資料包。您可以設定存取控制清單(ACL)來允許或拒絕各種型別的流量。可在組策略、使用者名稱屬性或動態訪問策略(DAP)上配置過濾器。

DAP取代在使用者名稱屬性和組策略下配置的值。如果DAP未分配任何篩選器，則username屬性值將取代組策略值。

必要條件

需求

思科建議您瞭解以下主題：

- L2L VPN隧道配置
- VPN客戶端遠端訪問(RA)配置
- AnyConnect RA配置

採用元件

本檔案中的資訊是根據Cisco 5500-X系列調適型安全裝置(ASA)版本9.1(2)。

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

sysopt connection permit-vpn命令允許通過VPN隧道進入安全裝置的所有流量繞過介面訪問清單。組策略和每使用者授權訪問清單仍適用於流量。

vpn過濾器應用於在流量退出通道後解密的流量，以及在流量進入通道前預加密的流量。用於vpn過濾器的ACL不應也用於介面訪問組。

將vpn過濾器應用於管理遠端訪問VPN客戶端連線的組策略時，應該在ACL的src_ip位置配置客戶端分配的IP地址，在ACL的dest_ip位置配置本地網路。將vpn過濾器應用於管理L2L VPN連線的組策略時，應該在ACL的src_ip位置配置遠端網路，在ACL的dest_ip位置配置本地網路。

設定

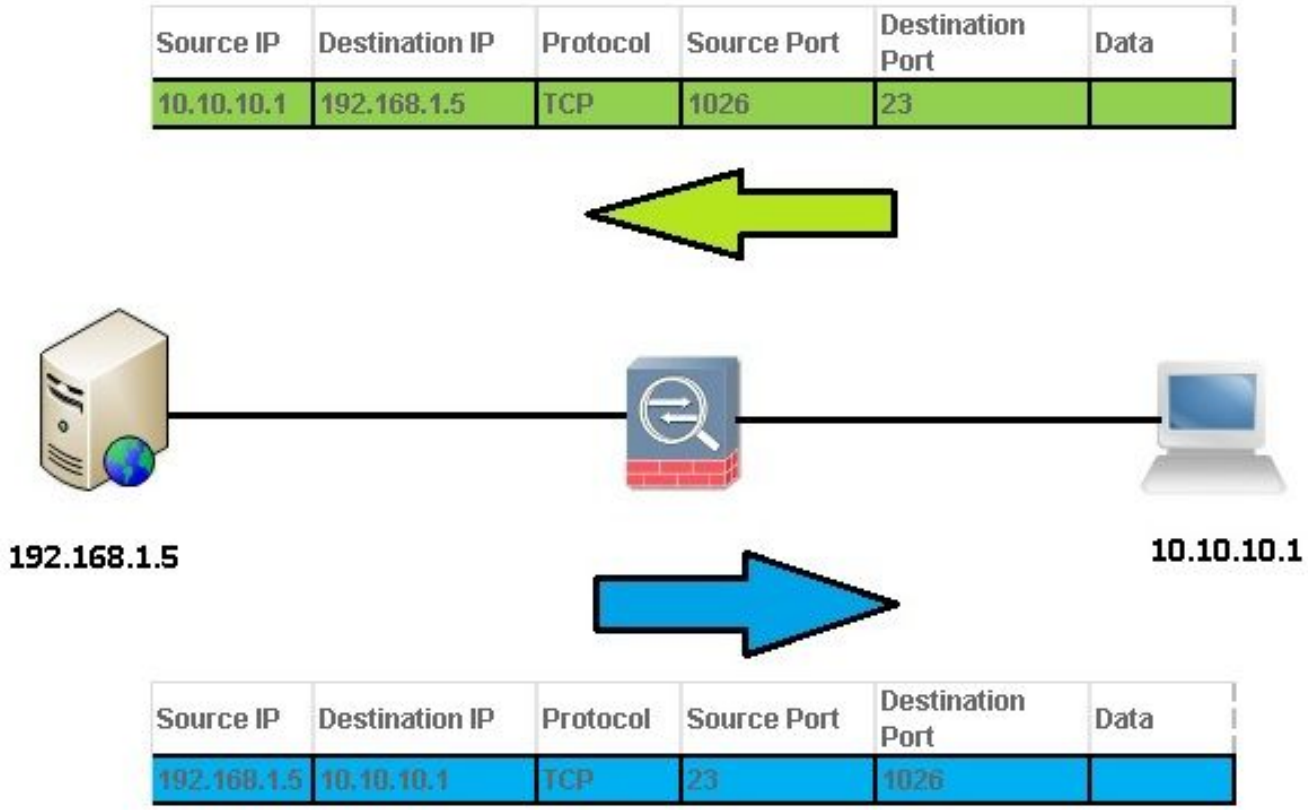
雖然規則仍然雙向應用，但必須在入站方向上配置VPN過濾器。增強功能CSCsf99428已開啟，用於支援單向規則，但尚未計畫/提交實施。

示例1.使用AnyConnect或VPN客戶端的vpn-filter

假設客戶端分配的IP地址為10.10.10.1/24，本地網路為192.168.1.0/24。

此訪問控制條目(ACE)允許AnyConnect客戶端Telnet到本地網路：

```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```

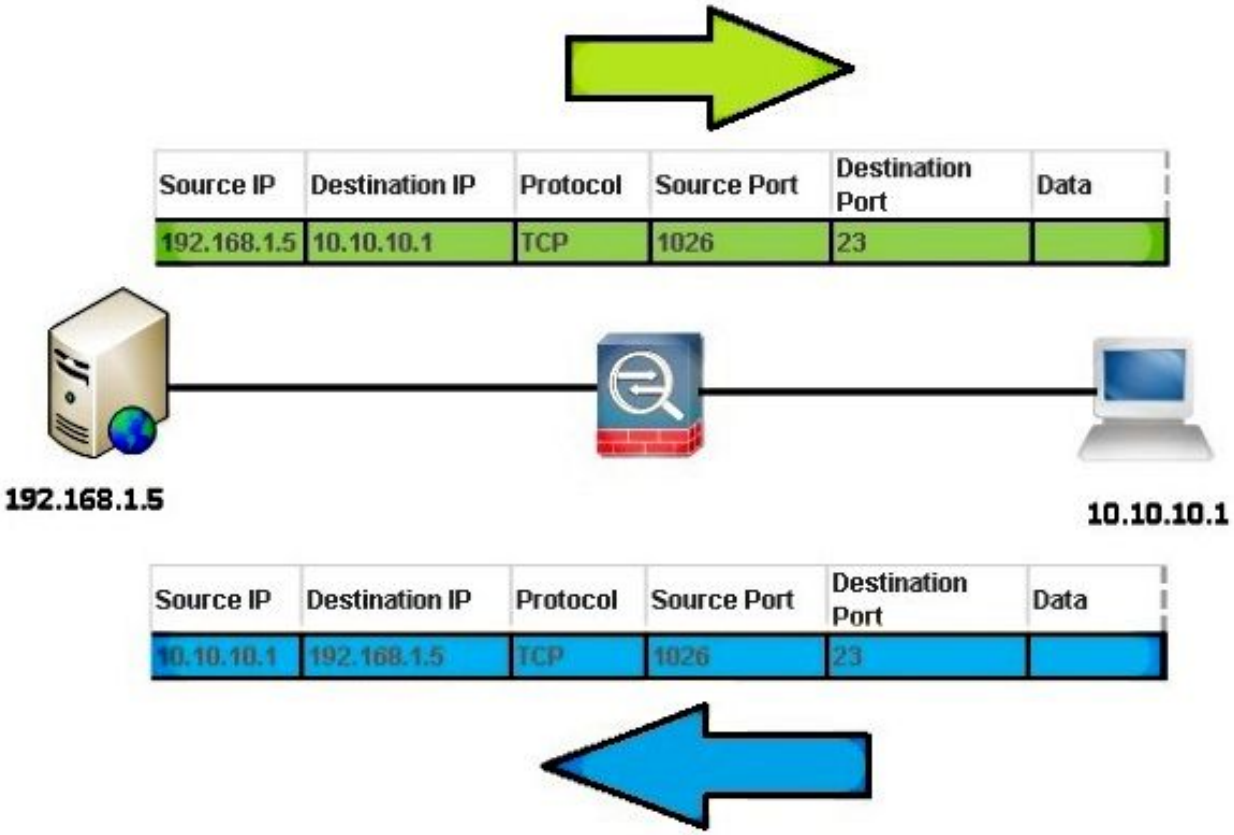


附註：ACE access-list vpnfilt-ra permit tcp 10.10.1 255.255.255.255 192.168.1.0

255.255.255.0 eq 23還允許本地網路在任何TCP埠（如果它使用源埠23）上啟動與RA客戶端的連線。

此ACE允許本地網路Telnet至AnyConnect客戶端：

```
access-list vpnfilt-ra permit tcp 10.10.10.1 255.255.255.255
eq 23 192.168.1.0 255.255.255.0
```



附註：ACE訪問清單vpnfilt-ra permit tcp 10.10.10.1 255.255.255 eq 23 192.168.1.0 255.255.255.0還允許RA客戶端在使用源埠23的任何TCP埠上發起到本地網路的連線。

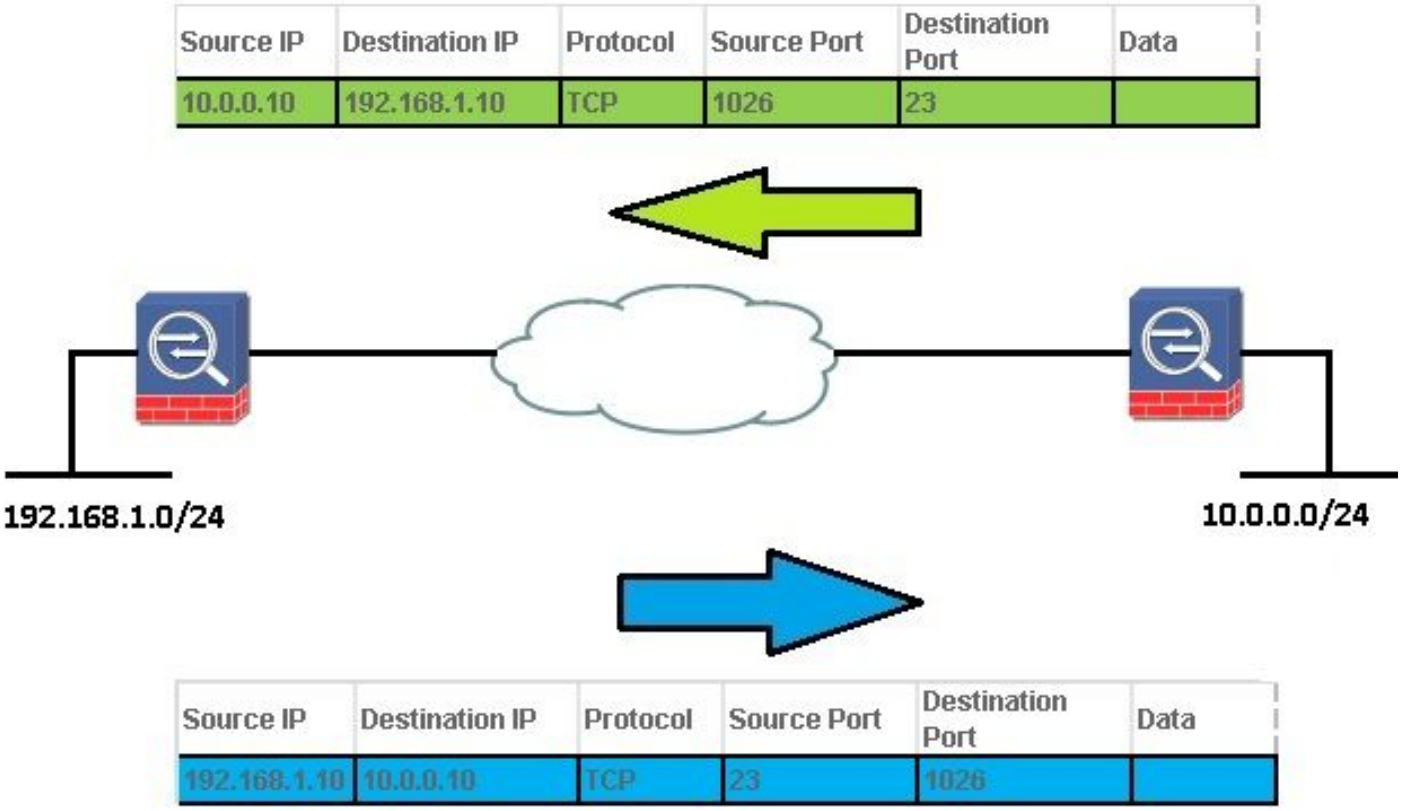
注意：vpn-filter功能允許僅在入站方向過濾流量，並且自動編譯出站規則。因此，建立網際網路控制訊息通訊協定(ICMP)存取清單時，如果要設定方向過濾器，請不要在存取清單格式中指定ICMP型別。

範例2.使用L2L VPN連線的vpn-filter

假設遠端網路為10.0.0.0/24，本地網路為192.168.1.0/24。

此ACE允許遠端網路Telnet到本地網路：

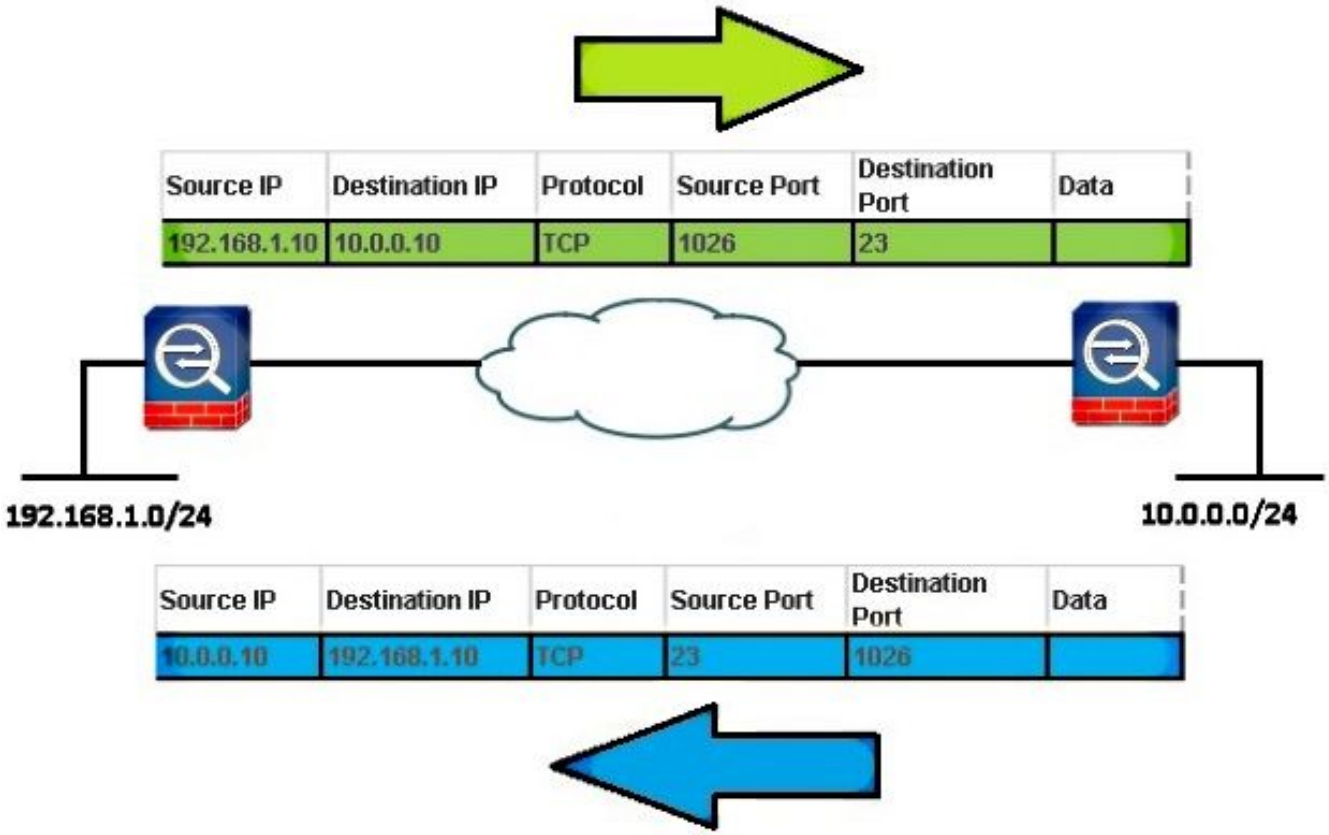
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



註:ACE access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23還允許本地網路在使用源埠23的任何TCP埠上發起到遠端網路的連線。

此ACE允許本地網路Telnet到遠端網路：

```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23
192.168.1.0 255.255.255.0
```



註:ACE access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0還允許遠端網路在使用源埠23的任何TCP埠上發起到本地網路的連線。

注意：vpn-filter功能允許僅在入站方向過濾流量，並且自動編譯出站規則。因此，當您建立ICMP訪問清單時，如果您需要方向過濾器，請不要在訪問清單格式中指定ICMP型別。

VPN過濾器和每使用者覆蓋訪問組

VPN流量不按介面ACL進行過濾。命令**no sysopt connection permit-vpn**可用於更改預設行為。在這種情況下，兩個ACL可以套用到使用者流量：首先檢查介面ACL，然後檢查vpn過濾器。

per-user-override關鍵字（僅用於入站ACL）允許為進行使用者授權而下載的動態使用者ACL，以便覆蓋分配給介面的ACL。例如，如果介面ACL拒絕來自10.0.0.0的所有流量，但動態ACL允許來自10.0.0.0的所有流量，則動態ACL會覆蓋該使用者的介面ACL，且允許流量。

示例(**未配置sysopt connection permit-vpn**時):

- no per-user-override， no vpn-filter — 根據介面ACL匹配流量
- no per-user-override， vpn-filter — 首先根據介面ACL匹配流量，然後根據vpn-filter匹配流量
- per-user-override， vpn-filter — 流量僅與vpn-filter匹配

驗證

使用本節內容，確認您的組態是否正常運作。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 show 指令。使用 Cisco CLI Analyzer 檢視 **show 指令輸出的分析。**

- **show asp table filter [access-list <*acl-name*>] [hits]**

  要調試加速安全路徑過濾器表，請在特權EXEC模式下使用**show asp table filter**命令。將過濾器應用於VPN隧道後，過濾器規則將安裝到過濾器表中。如果通道已指定過濾器，則在加密前和解密後檢查過濾器表，以確定應該允許還是拒絕內部封包。

```
 USAGE
show asp table filter [access-list
```

```
 SYNTAX <acl-name>      Show installed filter for access-list <acl-name>
hits Show filter rules which have non-zero hits values
```

- **clear asp table filter [access-list <*acl-name*>]**

  此命令將清除ASP篩選器表條目的命中計數器。

```
 USAGE
clear asp table filter [access-list
```

```
 SYNTAX
<acl-name> Clear hit counters only for specified access-list <acl-name>
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

Cisco CLI Analyzer（僅供已註冊客戶使用）支援某些 show 指令。使用 Cisco CLI Analyzer 檢視 show 指令輸出的分析。

> **附註**：使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

- **debug acl filter**

此命令啟用VPN過濾器調試。它可用於幫助排除VPN過濾器在ASP過濾器表中的安裝/刪除故障。對於[示例1。使用AnyConnect或VPN客戶端的vpn-filter](#)。

使用者1連線時調試輸出：

```
 ACL FILTER INFO: first reference to inbound filter vpnfilt-ra(2): Installing
rule into NP.
ACL FILTER INFO: first reference to outbound filter vpnfilt-ra(2): Installing
rule into NP.
```

使用者2連線時調試輸出（在使用者1和同一過濾器之後）：

```
 ACL FILTER INFO: adding another reference to outbound filter vpnfilt-ra(2): refCnt=2
ACL FILTER INFO: adding another reference to inbound filter vpnfilt-ra(2): refCnt=2
```

user2斷開連線時調試輸出：

```
 ACL FILTER INFO: removing a reference from inbound filter vpnfilt-ra(2): remaining
refCnt=1
ACL FILTER INFO: removing a reference from outbound filter vpnfilt-ra(2): remaining
refCnt=1
```

user1斷開連線時調試輸出：

```
 ACL FILTER INFO: releasing last reference from inbound filter vpnfilt-ra(2): Removing
rule into NP.
ACL FILTER INFO: releasing last reference from outbound filter vpnfilt-ra(2): Removing
rule into NP.
```

- **show asp table**

以下是**user1連線之前的show asp table filter**輸出。對於傳入和傳出方向的IPv4和IPv6，僅安裝隱式拒絕規則。

```
 Global Filter Table:
in id=0xd616ef20, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
in id=0xd616f420, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
dst ip=::/0, port=0
out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
src ip=0.0.0.0, mask=0.0.0.0, port=0
dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
src ip=::/0, port=0
```

```
dst ip=::/0, port=0
```

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）。