VPN-filters bij Cisco ASA Configuration Voorbeeld

Inhoud

Inleiding

Dit document beschrijft VPN-filters in detail en is van toepassing op LAN-to-LAN (L2L), Cisco VPN-client en Cisco AnyConnect Secure Mobility Client.

Filters bestaan uit regels die bepalen of u gegevenspakketten met tunnels wilt toestaan of weigeren die door het security apparaat komen, op basis van criteria zoals bronadres, doeladres en protocol. U vormt Toegangscontrolelijsten (ACL's) om verschillende typen verkeer toe te staan of te weigeren. Het filter kan worden geconfigureerd op het groepsbeleid, gebruikersnaamkenmerken of Dynamic Access Policy (DAP).

DAP vervangt de waarde die is ingesteld onder zowel gebruikersnaameigenschappen als groepsbeleid. De waarde van het gebruikersbenamingsattribuut vervangt de waarde van het groepsbeleid voor het geval dat DAP geen filter toewijst.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- L2L VPN-tunnelconfiguratie
- Configuratie van VPN Client Remote Access (RSA)
- AnyConnect RJa-configuratie

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco 5500-X Series adaptieve security applicatie

(ASA) versie 9.1(2).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Met de opdracht **Verbindingsmachtiging-VPN** kan al het verkeer dat via een VPN-tunnel in het beveiligingsapparaat komt, toegangslijsten voor interfaces omzeilen. Het groepsbeleid en de toegangslijsten van de per-gebruikersvergunning zijn nog op het verkeer van toepassing.

Een VPN-filter wordt toegepast op postdecrypted verkeer nadat het een tunnel verlaat en op preencrypted verkeer alvorens het een tunnel ingaat. ACL die voor een VPN-filter wordt gebruikt zou NIET ook voor een interface access-groep moeten worden gebruikt.

Wanneer een VPN-filter wordt toegepast op een groepsbeleid dat de clientverbindingen van Remote Access VPN regelt, moet de ACL worden geconfigureerd met de aan de client toegewezen IP-adressen in de src_ip-positie van de ACL en het lokale netwerk in de dest_ip-positie van de ACL. Wanneer een VPN-filter wordt toegepast op een groepsbeleid dat een L2L VPN-verbinding regelt, moet de ACL worden geconfigureerd met het externe netwerk in de src_ip-positie van de ACL en het lokale netwerk in de dest_ip-positie van de ACL.

Configureren

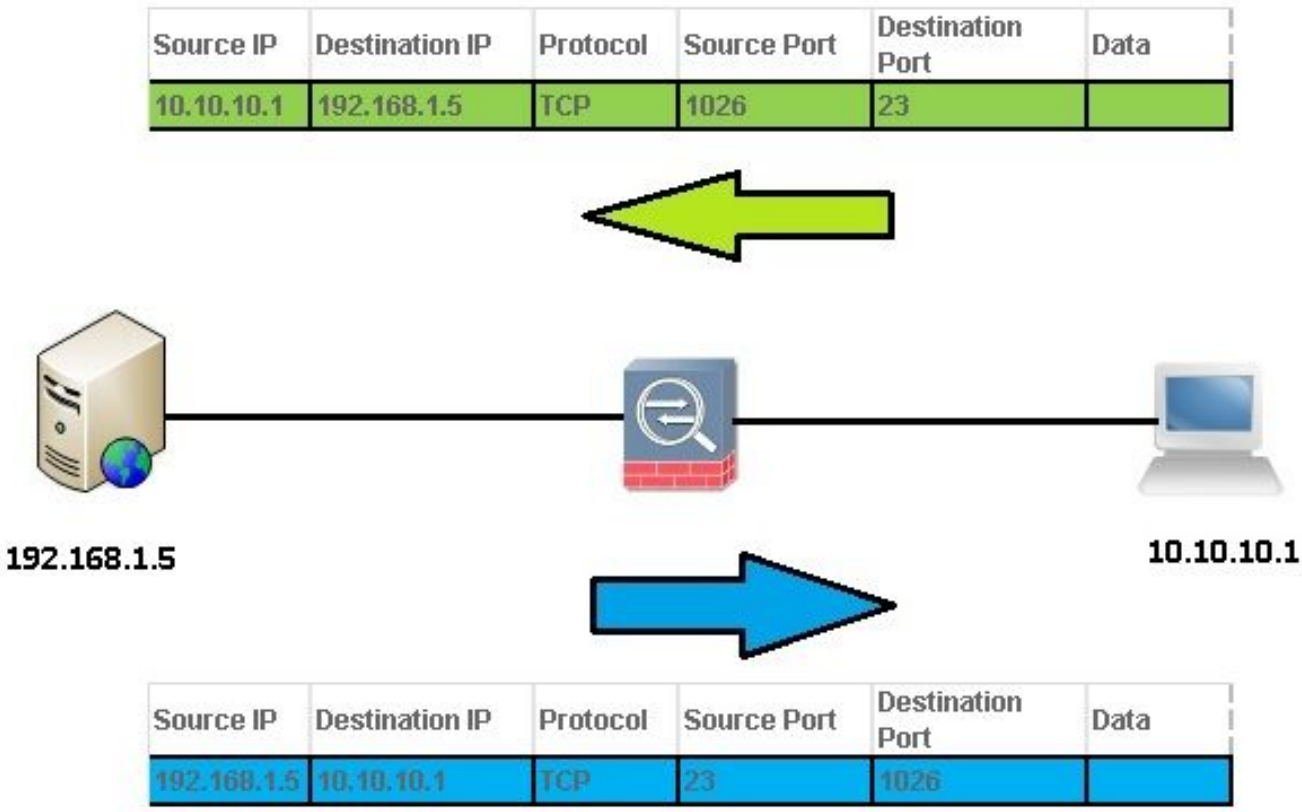
VPN-filters moeten in inkomende richting worden geconfigureerd, hoewel de regels nog steeds tweerichtings worden toegepast. De verbetering CSCsf99428 is geopend om unidirectionele regels te steunen, maar het is nog niet gepland/voor implementatie vastgelegd.

Voorbeeld 1. VPN-filter met AnyConnect of VPN-client

Ga ervan uit dat het aan de client toegewezen IP-adres 10.10.10.1/24 is en dat het lokale netwerk 192.168.1.0/24 is.

Met deze ingang voor toegangscontrole (ACE) kan de AnyConnect-client naar Telnet worden verbonden met het lokale netwerk:

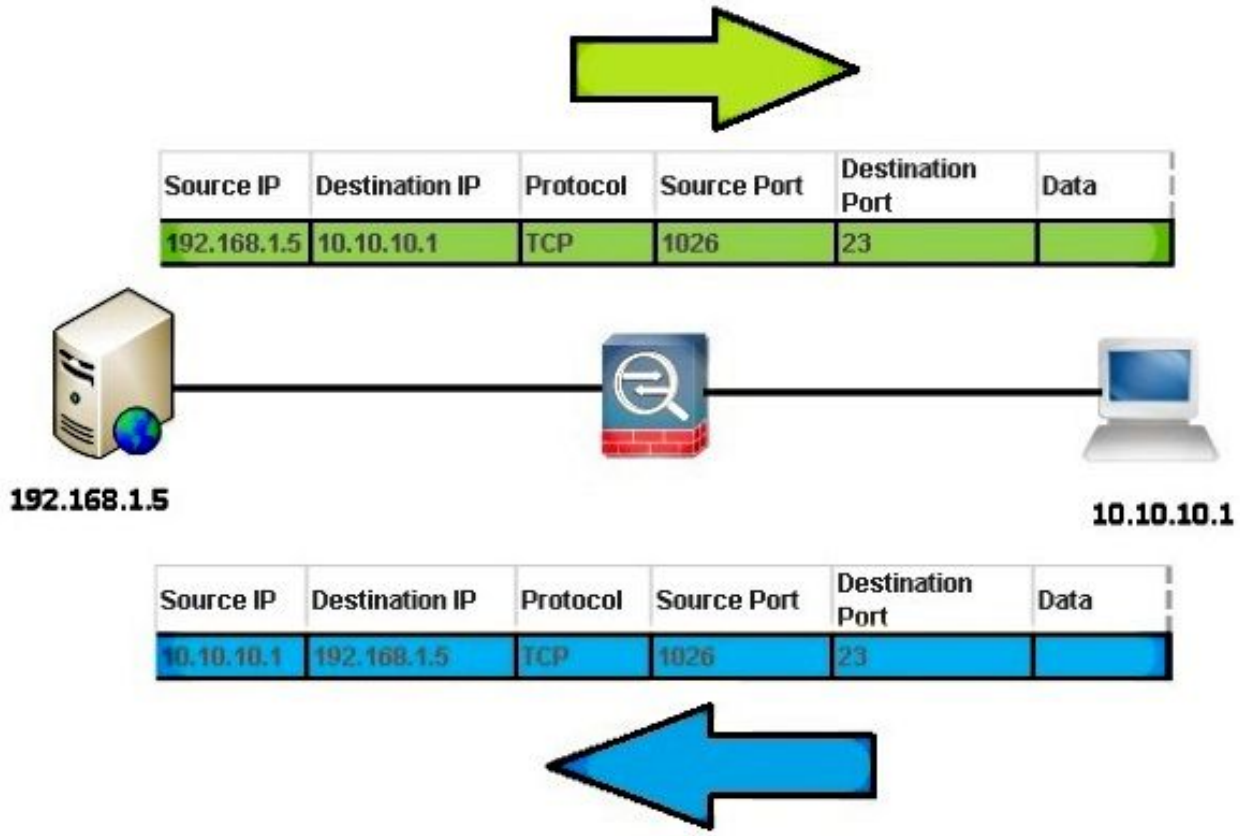
```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



Opmerking: De ACE-toegangslijst vpnfilt-ra-vergunning tcp 10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23 staat ook toe dat het lokale netwerk een verbinding met de RA-client op elke TCP-poort start als het een bronpoort van 23 gebruikt.

Met deze ACE kan het lokale netwerk Telnet gebruiken om de AnyConnect-client te activeren:

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



Opmerking: De ACE-toegangslijst vpnfilt-ra-vergunning tcp 10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0 stelt de RA-client ook in staat om op elke TCP-poort een verbinding met het lokale netwerk te initiëren als hij een bronpoort van 23 gebruikt.

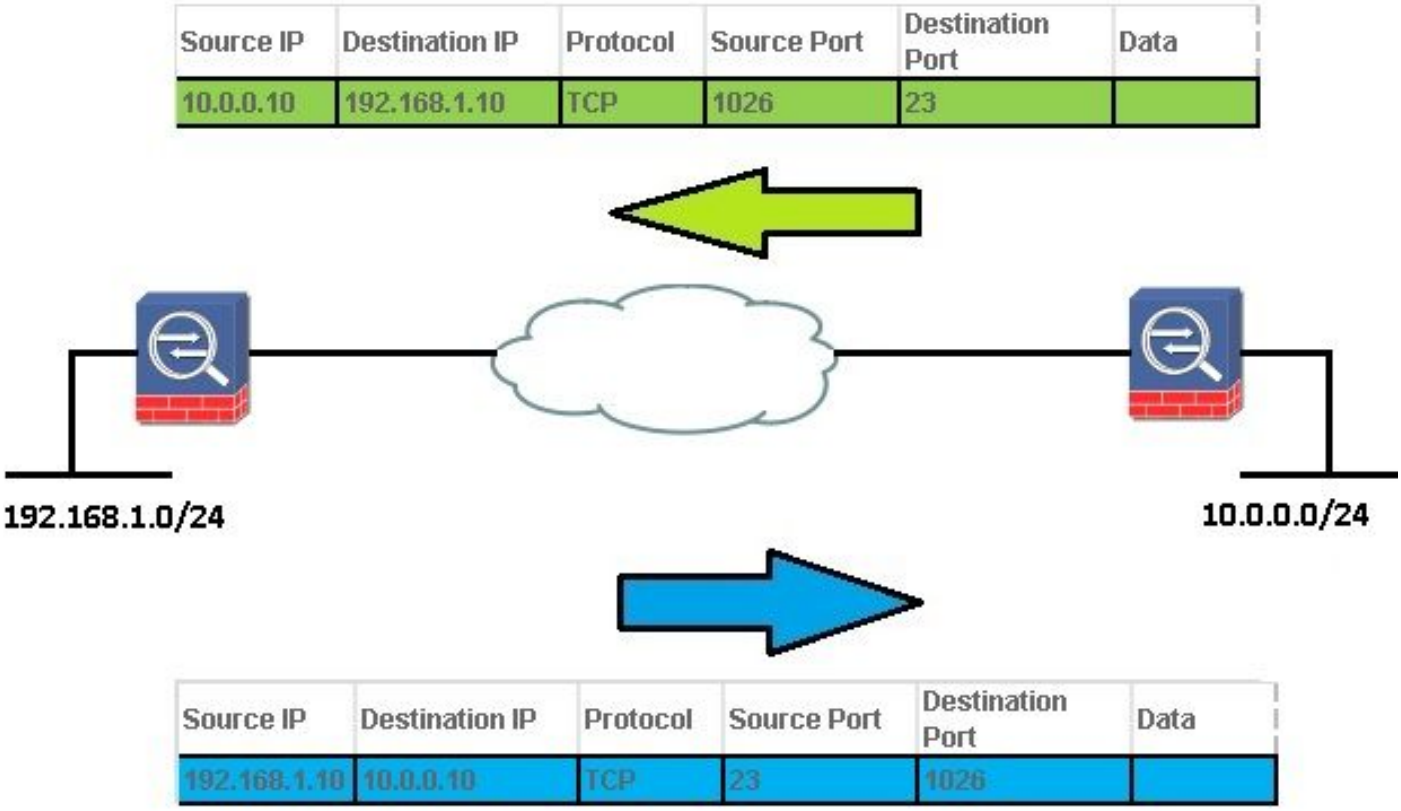
Voorzichtig: Met het VPN-filter kan verkeer alleen in de inkomende richting worden gefilterd en wordt de uitgaande regel automatisch gecompileerd. Daarom wanneer u een toegangslijst van Internet Control Message Protocol (ICMP) maakt, specificeert u niet het ICMP-type in de opmaak van de toegangslijst als u directionele filters wilt.

Voorbeeld 2. VPN-filter met L2L VPN-verbinding

Veronderstel dat het verre netwerk 10.0.0.0/24 en het lokale netwerk 192.168.1.0/24 is.

Deze ACE staat het verre netwerk aan Telnet aan het lokale netwerk toe:

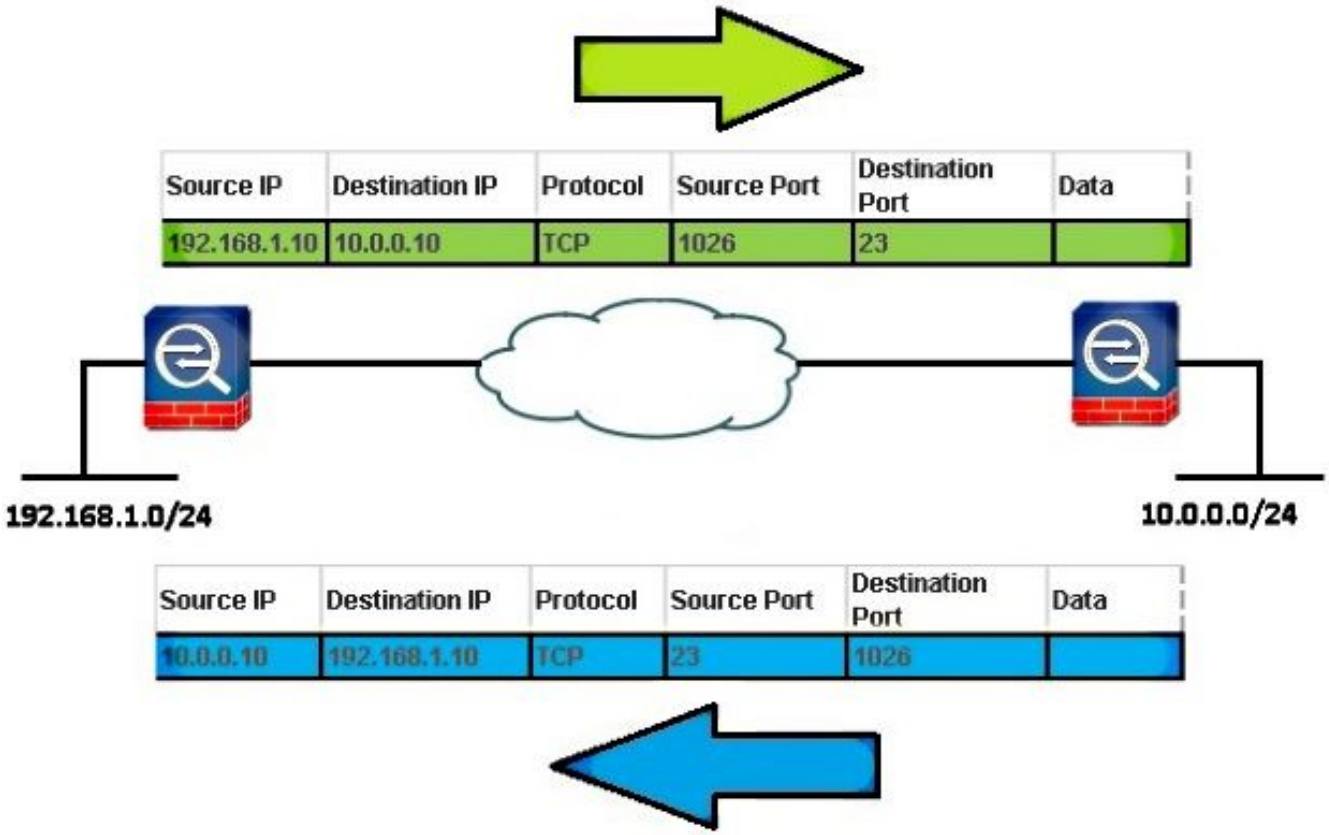
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



Opmerking: de ACE-toegangslijst vpnfilt-l2l-vergunning tcp 10.0.0.0 255.255.0 192.168.1.0 255.255.255.0 eq 23 staat ook toe dat het lokale netwerk een verbinding met het externe netwerk initieert op elke TCP-poort als het een bronpoort van 23 gebruikt.

Deze ACE staat het lokale netwerk toe om Telnet aan het verre netwerk toe te passen:

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



Opmerking: de ACE-toegangslijst vpnfilt-l2l-vergunning tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0 stelt het externe netwerk ook in staat om een verbinding met het lokale netwerk te initiëren op elke TCP-poort als het een bronpoort van 23 gebruikt.

Voorzichtig: Met het VPN-filter kan verkeer alleen in de inkomende richting worden gefilterd en wordt de uitgaande regel automatisch gecompileerd. Daarom wanneer u een ICMP-toegangslijst maakt, specificeert u niet het ICMP-type in de opmaak van de toegangslijst als u directionele filters wilt.

VPN-filters en per-gebruiker-override toegangsgroepen

VPN-verkeer wordt niet gefilterd door interface-ACL's. Het commando **no sysopt connection license-vpn** kan worden gebruikt om het standaardgedrag te veranderen. In dit geval kunnen twee ACL's worden toegepast op gebruikersverkeer: de interface ACL eerst wordt gecontroleerd en dan het VPN-filter.

Het trefwoord **per gebruiker-**override (alleen voor inkomende ACL's) staat dynamische gebruikers-ACL's toe die worden gedownload voor gebruikersautorisatie om de aan de interface toegewezen ACL te negeren. Als de interface-ACL bijvoorbeeld al het verkeer vanaf 10.0.0 ontkent, maar de dynamische ACL al het verkeer vanaf 10.0.0.0 toestaat, overschrijft de dynamische ACL de interface-ACL voor die gebruiker en het verkeer is toegestaan.

Voorbeelden (wanneer **geen sysopt connection license-vpn** is geconfigureerd):

- geen per-gebruiker-opheffing, geen VPN-filter - het verkeer wordt aangepast tegen interface ACL

- geen per-gebruiker-opheffing, vpn-filter - het verkeer wordt eerst tegen interface ACL, dan tegen de vpn-filter aangepast
- per-gebruiker-override, vpn-filter - het verkeer wordt alleen gekoppeld aan het vpn-filter

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show-**opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van **show** opdrachtoutput te bekijken.

- **asp-tabelfilter weergeven [access-list <*acl-name*>] [hits]**

  Om de versnelde de filterlijsten van de veiligheidspad te zuiveren, gebruik het bevel van de **asp- tabelfilter** in bevoorrechte wijze EXEC. Wanneer een filter is toegepast op een VPN-tunnel, worden de filterregels geïnstalleerd in de filtertabel. Als de tunnel een gespecificeerd filter heeft, dan wordt de filterlijst gecontroleerd voorafgaand aan encryptie en na decryptie om te bepalen of het binnenpakket zou moeten worden toegelaten of worden ontkend.

```
 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
```

- **asp-tabelfilter wissen [access-list <*acl-name*>]**

  Deze opdracht maakt de hit-tellers voor de ASP-filtertabelvermeldingen leeg.

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

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

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

De Cisco CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde **show-**opdrachten. Gebruik de Cisco CLI Analyzer om een analyse van **show** opdrachtoutput te bekijken.

> **Opmerking:** Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

- **acl-filter debuggen**

  Deze opdracht maakt VPN-filterdebugging mogelijk. Het kan worden gebruikt om het oplossen van problemen te helpen installaties/verwijdering van de VPN-filters in de ASP Filter tabel. Bijvoorbeeld 1. VPN-filter met AnyConnect of VPN-client.

  Debug uitvoer wanneer user1 verbinding maakt met:

```
 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.
```

  Debug uitvoer wanneer user2 verbinding maakt (na gebruiker1 en hetzelfde filter):

```
 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
```

  Debug uitvoer wanneer user2 de verbinding verbreekt:

```
 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
```

  Debug uitvoer als user1 de verbinding verbreekt:

```
 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.
```

- **ASP-tabel weergeven**

  Hier is de uitvoer van **asp tabelfilter tonen** voorafgaand aan wanneer user1 verbinding maakt. Alleen de impliciete ontkenningsregels zijn geïnstalleerd voor IPv4 en IPv6 in zowel de in- als de uitrichting.

```
 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
```

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.