Esempio di configurazione dei filtri VPN su Cisco ASA

Sommario

Introduzione

Questo documento descrive in dettaglio i filtri VPN e si applica a LAN-to-LAN (L2L), Cisco VPN Client e Cisco AnyConnect Secure Mobility Client.

I filtri sono costituiti da regole che determinano se consentire o rifiutare i pacchetti di dati di tunneling che passano attraverso l'appliance di sicurezza, in base a criteri quali l'indirizzo di origine, l'indirizzo di destinazione e il protocollo. È possibile configurare gli Access Control Lists (ACL) in modo da autorizzare o negare diversi tipi di traffico. È possibile configurare il filtro in base ai criteri di gruppo, agli attributi del nome utente o ai criteri di accesso dinamico (DAP).

Il protocollo DAP sostituisce il valore configurato sia negli attributi del nome utente che nei Criteri di gruppo. Il valore dell'attributo username sostituisce il valore di Criteri di gruppo se DAP non assegna alcun filtro.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione tunnel VPN L2L
- Configurazione di Accesso remoto client VPN
- Configurazione RA AnyConnect

Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco serie 5500-X Adaptive

Security Appliance (ASA) versione 9.1(2).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il comando **syst connection allow-vpn** permette a tutto il traffico che entra nell'appliance di sicurezza attraverso un tunnel VPN di ignorare gli elenchi degli accessi dell'interfaccia. I Criteri di gruppo e gli elenchi degli accessi con autorizzazione per utente sono ancora applicabili al traffico.

Il filtro vpn viene applicato al traffico post-decrittografato dopo l'uscita dal tunnel e al traffico precrittografato prima dell'ingresso nel tunnel. Un ACL utilizzato per un filtro vpn NON deve essere utilizzato anche per un access-group di interfaccia.

Quando si applica un filtro vpn a un criterio di gruppo che gestisce le connessioni client VPN di Accesso remoto, l'ACL deve essere configurato con gli indirizzi IP assegnati dal client nella posizione src_ip dell'ACL e la rete locale nella posizione dest_ip dell'ACL. Quando si applica un filtro vpn a un criterio di gruppo che gestisce una connessione VPN da L2L, l'ACL deve essere configurato con la rete remota nella posizione src_ip dell'ACL e la rete locale nella posizione dest_ip dell'ACL.

Configurazione

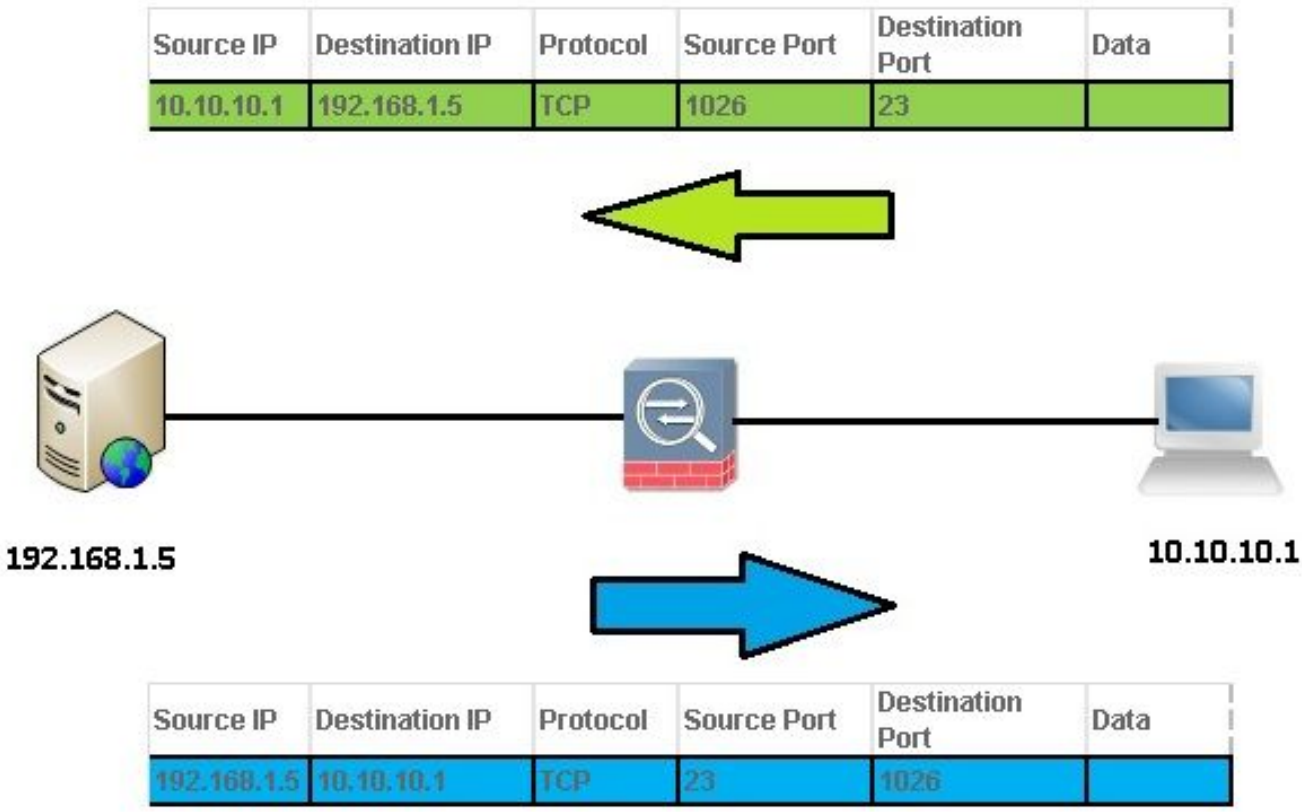
I filtri VPN devono essere configurati nella direzione in ingresso anche se le regole vengono ancora applicate in modo bidirezionale. Il miglioramento CSCsf99428 è stato aperto per supportare le regole unidirezionali, ma non è ancora stato pianificato/impegnato per l'implementazione.

Esempio 1. vpn-filter con AnyConnect o VPN Client

Si supponga che l'indirizzo IP assegnato dal client sia 10.10.10.1/24 e che la rete locale sia 192.168.1.0/24.

Questa voce di controllo di accesso (ACE) consente al client AnyConnect di connettersi in modalità Telnet alla rete locale:

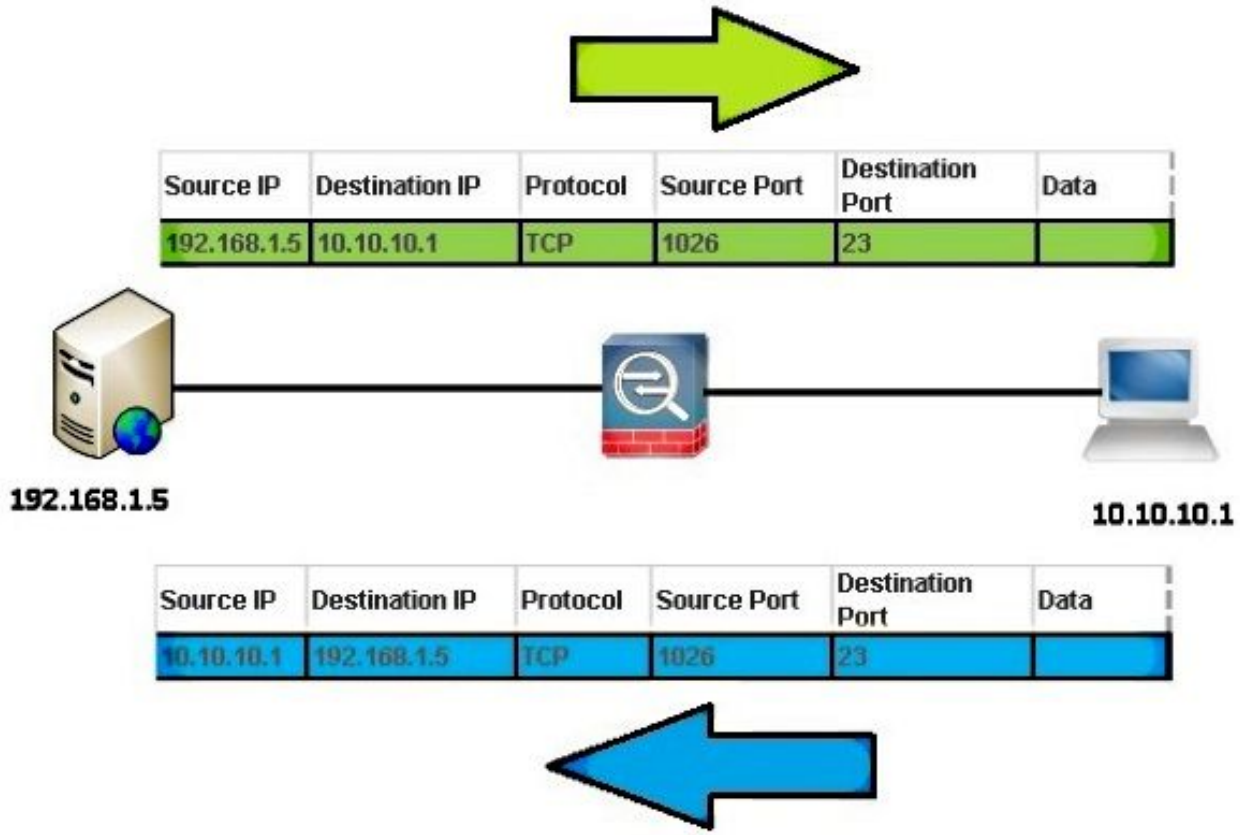
```
access-list vpnfilt-ra permit tcp
10.10.10.1 255.255.255.255 192.168.1.0 255.255.255.0 eq 23
```



Nota: L'elenco degli accessi ACE vpnfilt-ra consente a tcp 10.10.1 255.255.255.255.192.168.1.0 255.255.255.0 eq 23 anche di avviare una connessione con il client RA su qualsiasi porta TCP se usa una porta di origine di 23.

Questa voce di controllo di accesso consente alla rete locale di connettersi al client AnyConnect in modalità Telnet:

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



Nota: L'elenco degli accessi ACE vpnfilt-ra consente al client RSA di avviare una connessione alla rete locale su qualsiasi porta TCP se usa una porta di origine di 23. tcp 10.10.1 255.255.255.255 eq 23 192.168.1.0 255.255.255.0.

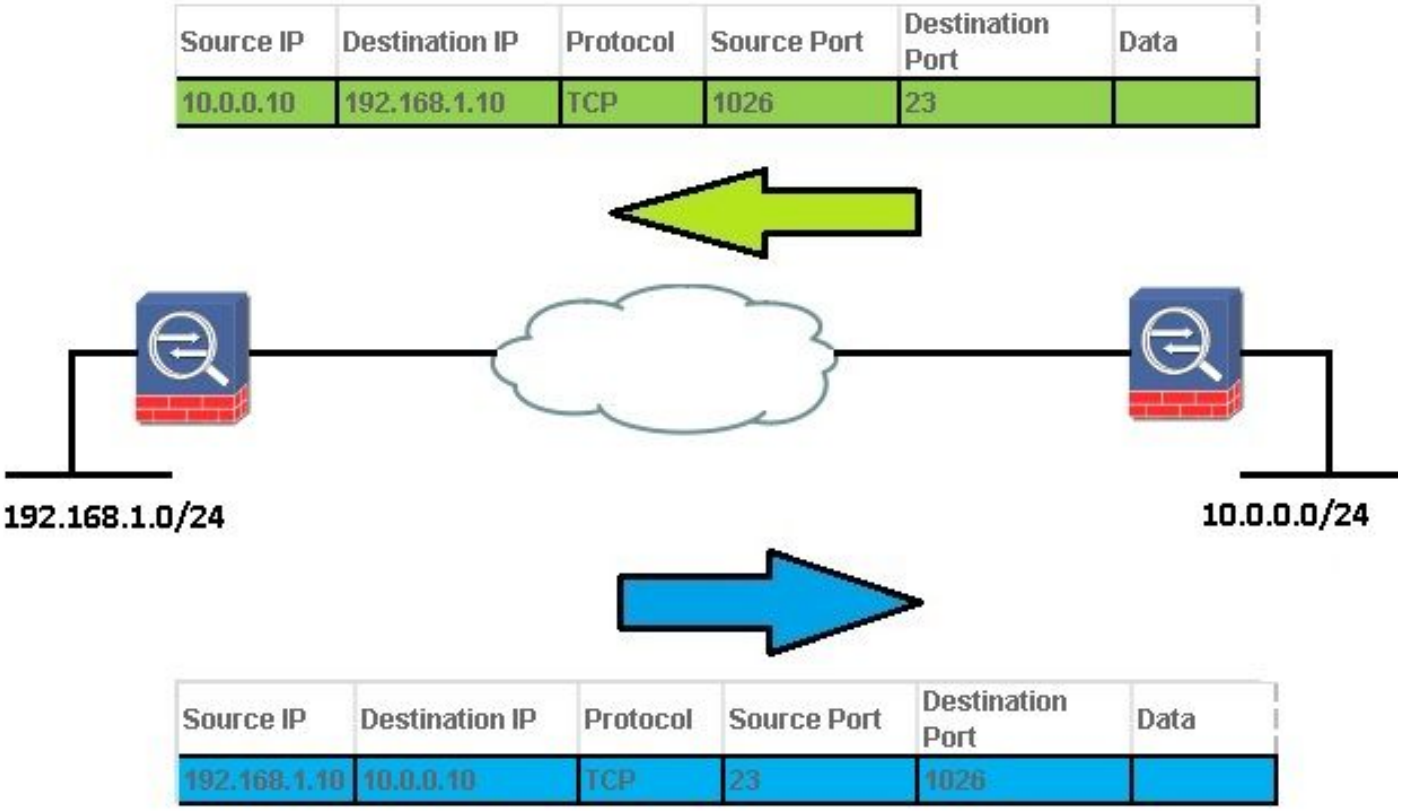
Attenzione: La funzione vpn-filter consente di filtrare il traffico solo nella direzione in entrata e di compilare automaticamente la regola in uscita. Pertanto, quando si crea un elenco degli accessi ICMP (Internet Control Message Protocol), non specificare il tipo ICMP nella formattazione dell'elenco degli accessi se si desidera utilizzare i filtri direzionali.

Esempio 2. vpn-filter con connessione VPN L2L

Si supponga che la rete remota sia 10.0.0.0/24 e la rete locale sia 192.168.1.0/24.

La voce ACE consente alla rete remota di connettersi alla rete locale in modalità Telnet:

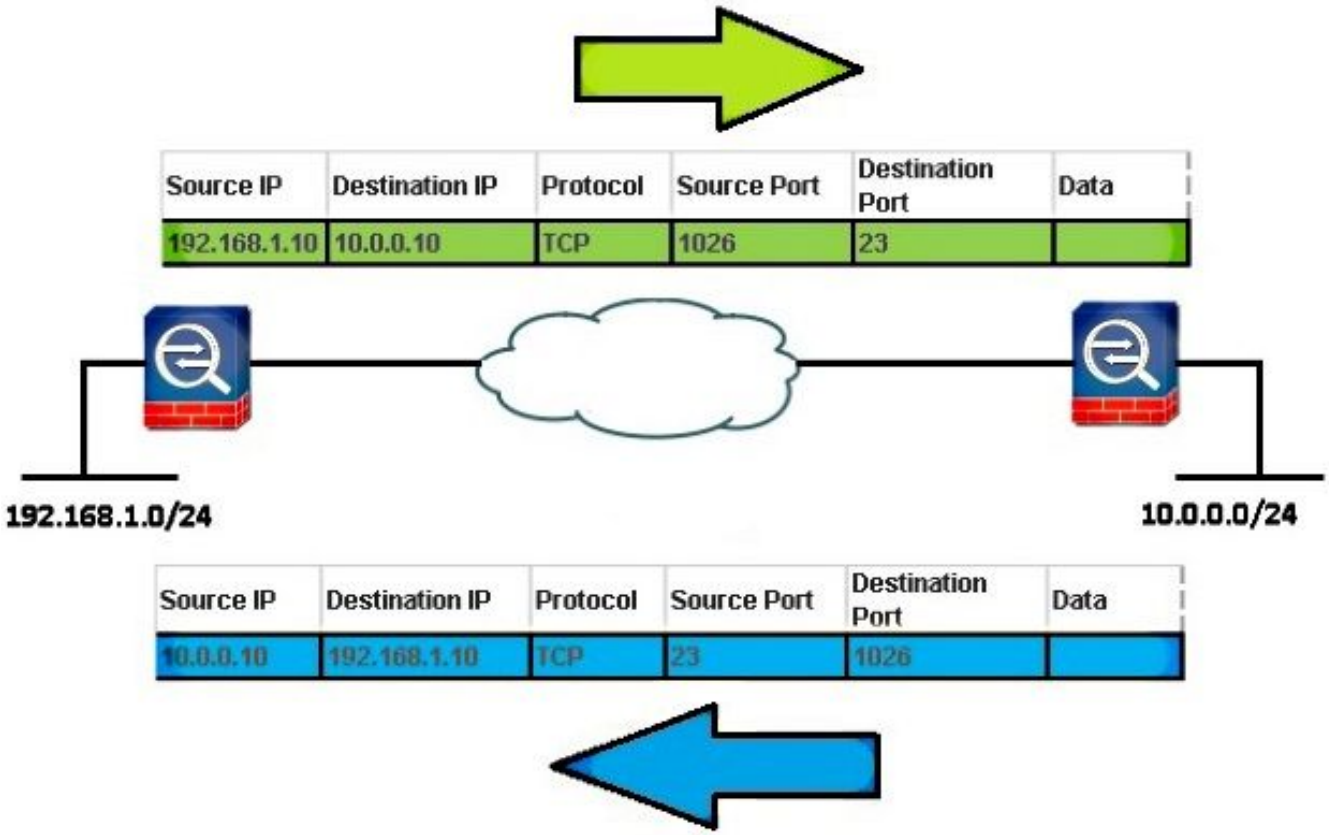
```
access-list vpnfilt-l2l permit tcp 10.0.0.0 255.255.255.0 192.168.1.0
255.255.255.0 eq 23
```



Nota: ACE access-list vpnfilt-l2l permette a tcp 10.0.0.0 255.255.255.0 192.168.1.0 255.255.255.0 eq 23 anche di avviare una connessione alla rete remota su qualsiasi porta TCP se usa una porta di origine di 23.

La voce ACE consente alla rete locale di connettersi in modalità Telnet alla rete remota:

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



Nota: ACE access-list vpnfilt-l2l permette a tcp 10.0.0.0 255.255.255.0 eq 23 192.168.1.0 255.255.255.0 anche di avviare una connessione alla rete locale su qualsiasi porta TCP se usa una porta di origine di 23.

Attenzione: La funzione vpn-filter consente di filtrare il traffico solo nella direzione in entrata e di compilare automaticamente la regola in uscita. Pertanto, quando si crea un elenco degli accessi ICMP, non specificare il tipo di formato dell'elenco degli accessi se si desidera utilizzare i filtri direzionali.

Filtri VPN e gruppi di accesso per utente

Il traffico VPN non è filtrato dagli ACL di interfaccia. Per modificare il comportamento predefinito, è possibile utilizzare il comando **no syspot connection allow-vpn**. In questo caso, è possibile applicare due ACL al traffico degli utenti: viene controllato prima l'ACL dell'interfaccia, quindi il filtro vpn.

La parola chiave **per-user-override** (solo per gli ACL in entrata) permette di scaricare gli ACL utente dinamici per l'autorizzazione dell'utente, in modo da ignorare l'ACL assegnato all'interfaccia. Ad esempio, se l'ACL di interfaccia nega tutto il traffico proveniente dalla versione 10.0.0.0, ma l'ACL dinamico consente tutto il traffico proveniente dalla versione 10.0.0.0, l'ACL dinamico sostituisce l'ACL di interfaccia per l'utente e il traffico in questione.

Esempi (quando **non** è configurata **alcuna connessione sysost allow-vpn**):

- no per-user-override, no vpn-filter - il traffico viene confrontato con l'ACL dell'interfaccia
- no per-user-override, vpn-filter - il traffico viene confrontato prima con l'ACL dell'interfaccia,

quindi con il vpn-filter

- per-user-override, vpn-filter - il traffico viene confrontato solo con vpn-filter

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi show. Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.

- **show asp table filter [access-list <*nome-acl*>] [riscontri]**

  Per eseguire il debug delle tabelle del filtro del percorso di sicurezza accelerato, usare il comando **show asp table filter** in modalità di esecuzione privilegiata. Quando si applica un filtro a un tunnel VPN, le regole di filtro vengono installate nella tabella dei filtri. Se per il tunnel è stato specificato un filtro, la tabella filtri viene controllata prima della crittografia e dopo la decrittografia per determinare se il pacchetto interno deve essere autorizzato o rifiutato.

```
 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*>]**

  Questo comando cancella i contatori delle corrispondenze trovate per le voci della tabella dei filtri ASP.

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

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

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Cisco CLI Analyzer (solo utenti registrati) supporta alcuni comandi show. Usare Cisco CLI Analyzer per visualizzare un'analisi dell'output del comando **show**.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

- **filtro debug acl**

  Questo comando abilita il debug del filtro VPN. Può essere utilizzato per facilitare la risoluzione dei problemi di installazione/rimozione dei filtri VPN nella tabella Filtri ASP. Nell'esempio 1. vpn-filter con AnyConnect o VPN Client.

  Output di debug alla connessione di user1:

```
 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.
```

  Output di debug alla connessione di user2 (dopo user1 e lo stesso filtro):

```
 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
```

  Output di debug alla disconnessione di user2:

```
 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
```

  Output di debug alla disconnessione di user1:

```
 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.
```

- **mostra tabella asp**

  Di seguito è riportato l'output del **filtro della tabella show asp** prima della connessione di user1. Per IPv4 e IPv6 vengono installate solo le regole di negazione implicita sia in entrata che in uscita.

```
 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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).