Configurazione dell'elenco di controllo di accesso ASA per diversi scenari

Sommario

Introduzione

In questo documento viene descritto come configurare un Access Control List (ACL) sull'appliance ASA (Adaptive Security Appliance) per diversi scenari.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dell'appliance ASA.

Componenti usati

Per questo documento, è stato usato un software ASA versione 8.3 e successive.

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

Gli ACL vengono usati dall'appliance ASA per determinare se il traffico è autorizzato o rifiutato. Per impostazione predefinita, il traffico che passa da un'interfaccia con livello di sicurezza **inferiore** a un'interfaccia con livello di sicurezza **superiore** viene rifiutato, mentre il traffico proveniente da un'interfaccia con livello di sicurezza **superiore** a un'interfaccia con **livello di** sicurezza **inferiore** viene consentito. Questo comportamento può essere ignorato anche con un ACL.

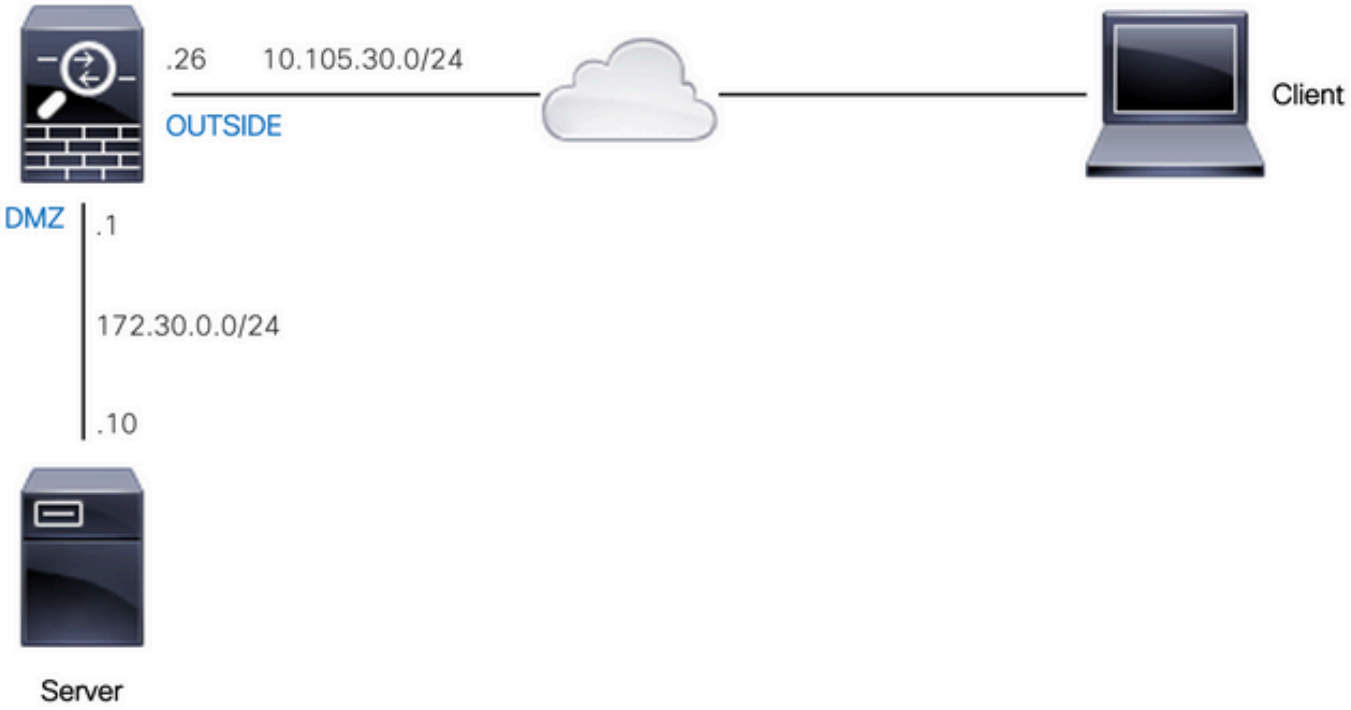
In presenza di regole NAT, nelle versioni precedenti dell'ASA (8.2 e precedenti), l'ASA controlla l'ACL prima di annullare la conversione del pacchetto in base alla regola NAT a cui è stata trovata una corrispondenza. Nella versione 8.3 e successive, l'ASA annulla la conversione del pacchetto prima di controllare gli ACL. Pertanto, per un'ASA versione 8.3 e successive, il traffico viene autorizzato o rifiutato in base all'indirizzo IP reale dell'host, anziché all'indirizzo IP tradotto. Gli ACL sono costituiti da una o più voci di controllo di accesso (ACE, Access Control Entries).

Configurazione

Scenario 1. Configurare un server Ace per consentire l'accesso a un server Web dietro la DMZ

Il client su Internet, situato dietro l'interfaccia esterna, desidera accedere a un server Web ospitato dietro l'interfaccia DMZ in ascolto sulle porte TCP 80 e 443.

Esempio di rete



L'indirizzo IP reale del server Web è 172.30.0.10. Una regola NAT statica uno-a-uno è configurata per consentire agli utenti di Internet di accedere al server Web con un indirizzo IP tradotto 10.105.130.27. Per impostazione predefinita, l'ASA esegue il proxy-arp per la versione 10.105.130.27 sull'interfaccia 'esterna' quando una regola NAT statica è configurata con un indirizzo IP convertito che rientra nella stessa subnet dell'indirizzo IP dell'interfaccia 'esterna' 10.105.130.26:

```
object network web-server
nat (dmz,outside) static 10.105.130.27
```

Configurare questa voce di controllo di accesso per consentire a qualsiasi indirizzo IP di origine su Internet di connettersi al server Web solo sulle porte TCP 80 e 443. Assegnare l'ACL all'interfaccia esterna nella direzione in entrata:

```
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq www
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
access-group OUT-IN in interface outside
```

Verifica

Eseguire un comando packet-tracer con questi campi. Interfaccia in ingresso su cui tracciare il pacchetto: esterna

Protocollo: TCP

Source IP address: qualsiasi indirizzo IP su Internet

Porta IP di origine: qualsiasi porta effimera

Indirizzo IP di destinazione: indirizzo IP tradotto del server Web (10.105.130.27)

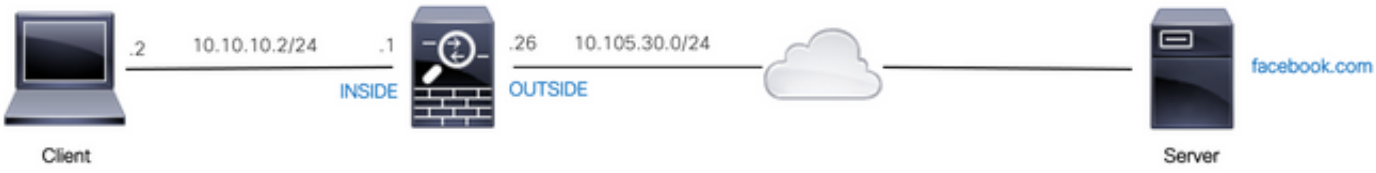
Porta di destinazione: 80 o 443

```
ciscoasa# packet-tracer input outside tcp 10.0.50.50 1234 10.105.130.27 443

!--- NAT untranslate from 10.105.130.27/443 to 172.30.0.10/443


Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
object network web-server
nat (dmz,outside) static 10.105.130.27
Additional Information:
NAT divert to egress interface dmz
Untranslate 10.105.130.27/443 to 172.30.0.10/443

!--- The configured ACL is permitting this packet to 172.30.0.10 on TCP port 443


Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group OUT-IN in interface outside
access-list OUT-IN extended permit tcp any host 172.30.0.10 eq https
Additional Information:

!--- Final result shows allow from the outside interface to the dmz interface

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: dmz
output-status: up
output-line-status: up
Action: allow
```

Scenario 2. Configurare un ACE per consentire l'accesso a un server Web con un FQDN

Il client con indirizzo IP 10.10.10.2 situato nella rete locale (LAN) può accedere a facebook.com.

Esempio di rete



Verificare che il server DNS sia configurato correttamente sull'appliance ASA:

```
ciscoasa# show run dns
dns domain-lookup outside
dns server-group DefaultDNS
```

```
name-server 10.0.2.2
name-server 10.0.8.8
```

Configurare questo oggetto di rete, l'oggetto FQDN e l'ACE per consentire al client con indirizzo IP 10.10.10.2 di accedere a facebook.com.

```
object network obj-10.10.10.2
host 10.10.10.2

object network obj-facebook.com
fqdn facebook.com

access-list IN-OUT extended permit ip object obj-10.10.10.2 object obj-facebook.com
access-group IN-OUT in interface inside
```

Verifica

L'output di **show dns** visualizza l'indirizzo IP risolto per l'FQDN facebook.com:

```
ciscoasa# show dns

Host Flags Age Type Address(es)
facebook.com (temp, OK) 0 IP 10.0.228.35
```

Nell'elenco degli accessi viene visualizzato l'oggetto FQDN come **risolto** e l'indirizzo IP risolto:

```
ciscoasa# show access-list IN-OUT
access-list IN-OUT; 2 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip object obj-10.10.10.2 object obj-facebook.com
(hitcnt=1) 0x22075b2a
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 fqdn facebook.com (resolved)
0xfea095d7
access-list IN-OUT line 1 extended permit ip host 10.10.10.2 host 10.0.228.35 (facebook.com)
(hitcnt=1) 0x22075b2a
```

Scenario 3. Configurare un server Ace in modo da consentire l'accesso a un sito Web solo per una durata specifica di un giorno

Il client che si trova nella LAN è autorizzato ad accedere a un sito Web con indirizzo IP 10.0.20.20 ogni giorno solo dalle 12:00 alle 24:00 IST.

Esempio di rete

Verificare che il fuso orario sia configurato correttamente sull'appliance ASA:

```
ciscoasa# show run clock
clock timezone IST 5 30
```

Configurare un oggetto intervallo di tempo per la durata richiesta:

```
time-range BREAK_TIME
periodic daily 12:00 to 14:00
```

Configurare questi oggetti di rete e ACE in modo da consentire a qualsiasi indirizzo IP di origine situato nella LAN di accedere al sito Web solo durante il periodo di tempo indicato nell'oggetto dell'intervallo di tempo denominato **BREAK_TIME:**

```
object network obj-website
host 10.0.20.20


access-list IN-OUT extended permit ip any object obj-website time-range BREAK_TIME
access-group IN-OUT in interface inside
```

Verifica

L'oggetto intervallo di tempo è **attivo** quando l'orologio sull'appliance ASA indica un'ora compresa nell'oggetto intervallo di tempo:

```
ciscoasa# show clock
12:03:41.987 IST Mon Oct 4 2021


ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (active)
periodic daily 12:00 to 14:00
used in: IP ACL entry


ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
(hitcnt=12) 0x5a66c8f9
```

L'oggetto intervallo di tempo e l'ACE **non** sono **attivi** quando l'orologio sull'ASA indica un'ora esterna all'oggetto intervallo di tempo:

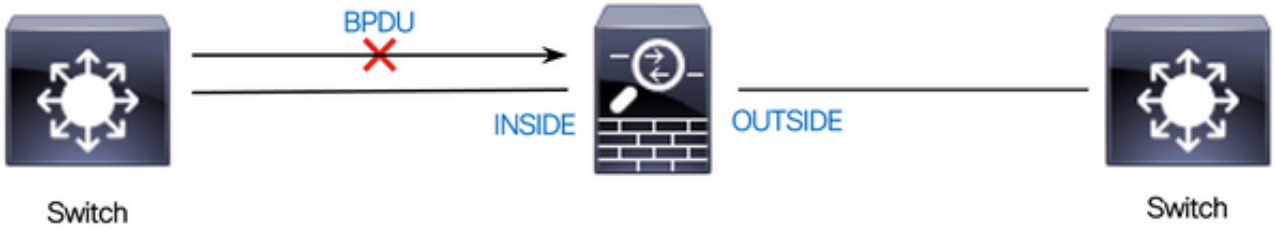
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


ciscoasa# show time-range BREAK_TIME

time-range entry: BREAK_TIME (inactive)
periodic daily 12:00 to 14:00
used in: IP ACL entry


ciscoasa# show access-list IN-OUT
access-list IN-OUT; 1 elements; name hash: 0x1b5ff18e
access-list IN-OUT line 1 extended permit ip any object obj-website time-range BREAK_TIME
(hitcnt=0) (inactive) 0x5a66c8f9
access-list IN-OUT line 1 extended permit ip any host 10.0.20.20 time-range BREAK_TIME
```

```
(hitcnt=0) (inactive) 0x5a66c8f9
```

Scenario 4. Configurazione di un ACE per bloccare le unità BDPU (Bridge Protocol Data Unit) tramite un'ASA in modalità trasparente

Per impostazione predefinita, per impedire la formazione di loop con il protocollo Spanning Tree Protocol (STP), i BPDU vengono passati attraverso l'ASA in modalità trasparente. Per bloccare le BPDU, è necessario configurare una regola EtherType per negarle.

Esempio di rete



Configurare l'ACL EtherType in modo che i BPDU non passino attraverso l'interfaccia "interna" dell'ASA nella direzione in entrata, come mostrato di seguito:

```
access-list block-bpdu ethertype deny dsap bpdu
access-list block-bpdu ethertype permit any
access-group block-bpdu in interface inside
```

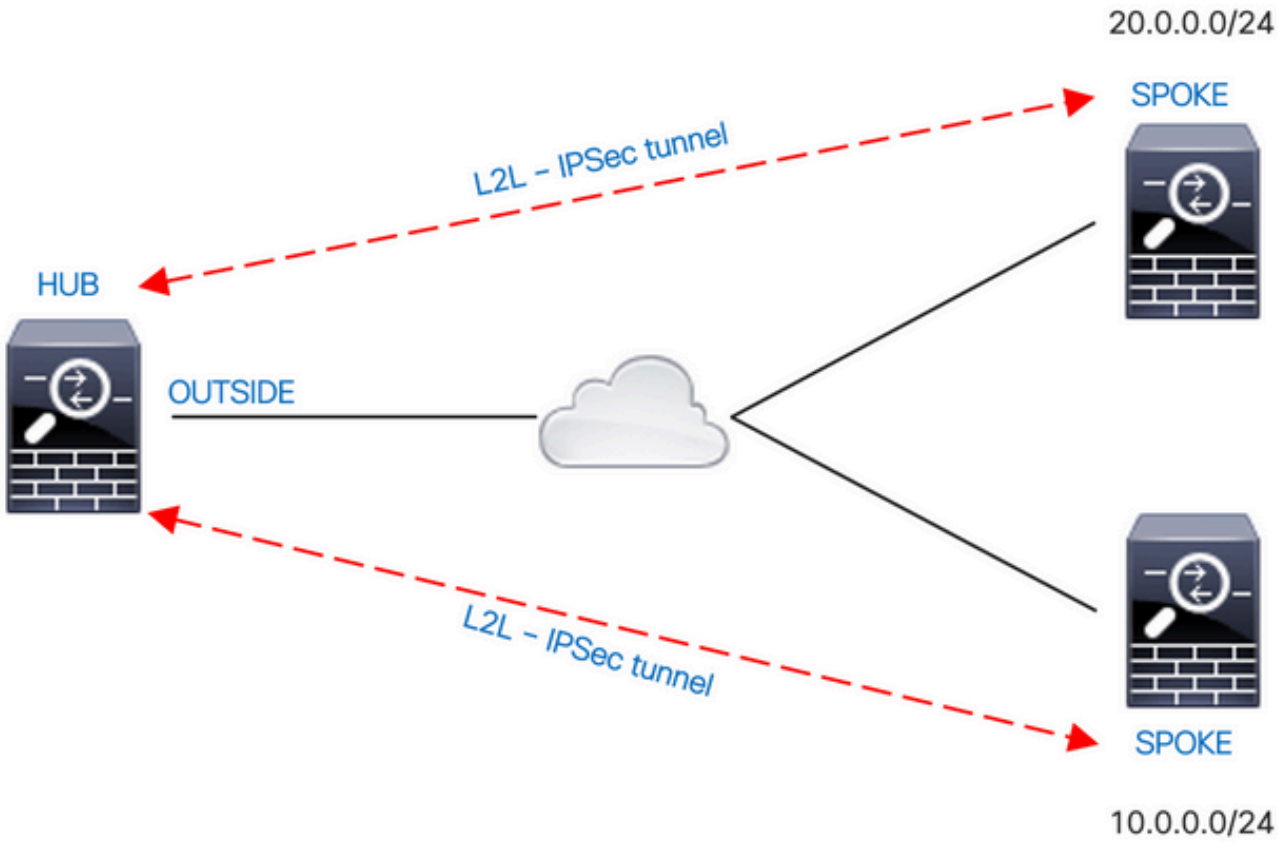
Verifica

Controllare il numero di accessi nell'elenco per verificare che le BPDU siano bloccate dall'ASA:

```
ciscoasa# show access-list block-bpdu
access-list block-bpdu; 2 elements
access-list block-bpdu ethertype deny dsap bpdu(hitcount=14)
access-list block-bpdu ethertype permit any (hitcount=48)
```

Scenario 5. Consenti il passaggio del traffico tra interfacce con lo stesso livello di sicurezza

Esempio di rete



Per impostazione predefinita, il traffico che passa tra interfacce con lo stesso livello di protezione viene bloccato. Per consentire la comunicazione tra interfacce con pari livelli di sicurezza o il traffico in entrata e in uscita dalla stessa interfaccia (hairpin/u-turn), usare il comando **same-security-traffic** in modalità di configurazione globale.

Questo comando mostra come consentire la comunicazione tra diverse interfacce con lo stesso livello di sicurezza:

```
same-security-traffic permit inter-interface
```

Nell'esempio viene mostrato come consentire la comunicazione in entrata e in uscita dalla stessa interfaccia:

```
same-security-traffic permit intra-interface
```

Questa funzionalità è utile per il traffico VPN che entra in un'interfaccia ma che viene quindi instradato all'esterno della stessa interfaccia. Ad esempio, se si ha una rete VPN hub e spoke in cui l'ASA è l'hub e le reti VPN remote sono spoke, per consentire a uno spoke di comunicare con un altro spoke, il traffico deve essere indirizzato all'ASA e quindi nuovamente indirizzato all'altro spoke.

Verifica

Senza il comando **same-security-traffic-allow-inter-interface**, l'output del comando packet-tracer indica che il traffico che passa tra diverse interfacce con lo stesso livello di sicurezza è bloccato da una **regola implicita**, come mostrato di seguito:

```
!--- The interfaces named 'test' and 'outside' have the same security level of 0
```

```
ciscoasa# show nameif
Interface Name Security
GigabitEthernet0/0 inside 100
GigabitEthernet0/1 dmz 50
GigabitEthernet0/2 test 0
GigabitEthernet0/5 outside 0
Management0/0 mgmt 0

!--- Traffic between different interfaces of same security level is blocked by an implicit rule

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed


Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a2ff90, priority=110, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=test, output_ifc=any

Result:
input-interface: test
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA


!--- After running the command 'same-security-traffic permit inter-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit inter-interface

!--- Traffic between different interfaces of same security level is allowed

ciscoasa# packet-tracer input test tcp 172.16.20.10 1234 10.0.8.8 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a352d0, priority=2, domain=permit, deny=false
hits=2, user_data=0x0, cs_id=0x0, flags=0x3000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=test, output_ifc=any

Result:
```

```
input-interface: test
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Senza il comando **same-security-traffic-allow intra-interface**, l'output del comando packet-tracer indica che il traffico in entrata e in uscita dalla stessa interfaccia è bloccato da una **regola implicita**, come mostrato di seguito:

```
!--- Traffic in and out of the same interface is blocked by an implicit rule

ciscoasa# packet-tracer input outside tcp 10.0.0.10 1234 10.1.0.10 443 detailed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f9960a32f30, priority=111, domain=permit, deny=true
hits=0, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
input_ifc=outside, output_ifc=outside

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame
0x00005638dfd7da57 flow (NA)/NA

!--- After running the command 'same-security-traffic permit intra-interface'

ciscoasa# show running-config same-security-traffic
same-security-traffic permit intra-interface


!--- Traffic in and out of the same interface is allowed

Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in id=0x7f99609291c0, priority=3, domain=permit, deny=false
hits=1, user_data=0x0, cs_id=0x0, flags=0x4000, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none
```

```
input_ifc=outside, output_ifc=outside


Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

Scenario 6. Configurazione di un'ACE per il controllo del traffico diretto

La parola chiave **control-plane** specifica se l'ACL viene usato per controllare il traffico diretto. Le regole di controllo d'accesso per il traffico di gestione diretto (definito da comandi come **http**, **ssh** o **telnet**) hanno la precedenza su una regola di accesso alla gestione applicata con l'opzione **control-plane**. Pertanto, il traffico di gestione autorizzato deve poter entrare anche se rifiutato esplicitamente dall'ACL predefinito.

A differenza delle regole di accesso standard, alla fine di un insieme di regole di gestione per un'interfaccia non è presente alcuna negazione implicita. Al contrario, qualsiasi connessione che non corrisponde a una regola di accesso alla gestione viene valutata da regole di controllo di accesso normali. In alternativa, è possibile utilizzare le regole ICMP per controllare il traffico ICMP verso il dispositivo.

Esempio di rete

Per configurare un ACL, usare la parola chiave **control-plane** per bloccare il traffico diretto all'indirizzo IP 10.65.63.155 e destinato all'indirizzo IP dell'interfaccia 'esterna' dell'ASA.

```
access-list control-plane-test extended deny ip host 10.65.63.155 any
access-group control-plane-test in interface outside control-plane
```

Verifica

Controllare il numero di accessi nell'elenco degli accessi per verificare che il traffico sia bloccato dall'ACL:

```
ciscoasa# show access-list control-plane-test
access-list control-plane-test; 1 elements; name hash: 0x6ff5e700
access-list control-plane-test line 1 extended deny ip host 10.65.63.155 any (hitcnt=4)
0xedad4c6f
```

I messaggi syslog indicano che il traffico sull'interfaccia 'identity' è stato interrotto:

```
Dec 27 2021 13:19:44: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:45: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:46: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
Dec 27 2021 13:19:47: %ASA-4-106023: Deny tcp src outside:10.65.63.155/54108 dst
identity:10.105.130.26/8000 by access-group "control-plane-test" [0xedad4c6f, 0x0]
```

Registrazione

La parola chiave **log** imposta le opzioni di registrazione quando una voce ACE corrisponde a un pacchetto per l'accesso alla rete (un ACL applicato con il comando **access-group**). Se si immette la parola chiave **log** senza argomenti, si abilita il messaggio di log del sistema 106100 al livello predefinito (6) e per l'intervallo predefinito (300 secondi). Se non si immette la parola chiave log, viene generato il messaggio log predefinito 106023 per i pacchetti negati. Le opzioni del registro sono:

- livello: un livello di gravità compreso tra 0 e 7. Il valore predefinito è 6 (informativo). Se si modifica questo livello per una voce ACE attiva, il nuovo livello verrà applicato alle nuove connessioni. Le connessioni esistenti continueranno a essere registrate al livello precedente.
- **interval** secs: l'intervallo di tempo in secondi tra i messaggi syslog, da 1 a 600. Il valore predefinito è 300. Questo valore viene utilizzato anche come valore di timeout per eliminare un flusso inattivo dalla cache utilizzato per raccogliere le statistiche di rilascio.
- **disable** — disabilita tutte le registrazioni ACE.
- **default** — Abilita la registrazione al messaggio 106023. Questa impostazione equivale a non includere l'opzione di registrazione.

Messaggio Syslog 106023:

```
Message:
%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port ] [([idfw_user
|FQDN_string ], sg_info )] dst interface_name :dest_address /dest_port [([idfw_user |FQDN_string
], sg_info )] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]
```

Spiegazione:

Un pacchetto IP reale è stato negato dall'ACL. Questo messaggio viene visualizzato anche se l'opzione log non è abilitata per un ACL. L'indirizzo IP è l'indirizzo IP reale anziché i valori visualizzati tramite NAT. Per gli indirizzi IP vengono fornite sia le informazioni sull'identità utente che le informazioni sul nome di dominio completo (FQDN), se ne viene trovata una corrispondente. L'appliance ASA Secure Firewall registra le informazioni sull'identità (dominio\utente) o il nome di dominio completo (se il nome utente non è disponibile). Se le informazioni sull'identità o il nome di dominio completo (FQDN) sono disponibili, l'appliance ASA Secure Firewall registra queste informazioni sia per l'origine che per la destinazione.

Esempio:

```
Dec 27 2021 14:58:25: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
Dec 27 2021 14:58:26: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
```

```
Dec 27 2021 14:58:27: %ASA-4-106023: Deny tcp src outside:10.65.63.155/56166 dst
inside:10.5.0.30/8000 by access-group "OUT-IN" [0x902a8ee8, 0x0]
```

Messaggio Syslog 106100:

```
Message:

%ASA-6-106100: access-list acl_ID {permitted | denied | est-allowed} protocol interface_name
/source_address (source_port ) (idfw_user , sg_info ) interface_name /dest_address (dest_port )
(idfw_user , sg_info ) hit-cnt number ({first hit | number -second interval}) hash codes
```

Spiegazione:

Vengono elencate l'occorrenza iniziale o il numero totale di occorrenze durante un intervallo. Questo messaggio fornisce più informazioni del messaggio 106023, che registra solo i pacchetti negati e non include il numero di accessi o un livello configurabile.

Quando una riga dell'elenco degli accessi contiene l'argomento *log*, è probabile che questo ID messaggio venga attivato perché un pacchetto non sincronizzato arriva all'appliance ASA Secure Firewall e viene valutato dall'elenco degli accessi. Ad esempio, se si riceve un pacchetto ACK sull'appliance ASA Secure Firewall (per la quale non esiste una connessione TCP nella tabella delle connessioni), l'appliance ASA Secure Firewall può generare il messaggio 106100 per indicare che il pacchetto è stato autorizzato. Il pacchetto, tuttavia, viene successivamente scartato correttamente a causa della mancanza di una connessione corrispondente.

L'elenco descrive i valori del messaggio:

- consentito | negato | Set-allowed: questi valori specificano se il pacchetto è stato autorizzato o rifiutato dall'ACL. Se il valore è impostato come consentito, il pacchetto è stato rifiutato dall'ACL ma è stato consentito per una sessione già stabilita (ad esempio, un utente interno può accedere a Internet e vengono accettati i pacchetti di risposta che normalmente verrebbero negati dall'ACL).
- protocollo: TCP, UDP, ICMP o un numero di protocollo IP.
- interface_name: il nome dell'interfaccia per l'origine o la destinazione del flusso registrato. Interfacce VLAN supportate.
- source_address: l'indirizzo IP di origine del flusso registrato. L'indirizzo IP è l'indirizzo IP reale anziché i valori visualizzati tramite NAT.
- dest_address: l'indirizzo IP di destinazione del flusso registrato. L'indirizzo IP è l'indirizzo IP reale anziché i valori visualizzati tramite NAT.
- source_port - Porta di origine del flusso registrato (TCP o UDP). Per ICMP, il numero dopo la porta di origine è il tipo di messaggio.
- idfw_user: nome utente e identità, con il nome di dominio aggiunto al syslog esistente quando l'appliance ASA Secure Firewall riesce a trovare il nome utente per l'indirizzo IP.
- sg_info — Tag del gruppo di sicurezza aggiunto al syslog quando l'appliance ASA Secure Firewall può trovare un tag del gruppo di sicurezza per l'indirizzo IP. Il nome del gruppo di sicurezza viene visualizzato con il tag del gruppo di sicurezza, se disponibile.
- dest_port: porta di destinazione del flusso registrato (TCP o UDP). Per ICMP, il numero dopo la porta di destinazione è il codice messaggio ICMP, disponibile per alcuni tipi di messaggi. Per il tipo 8, è sempre 0. Per un elenco dei tipi di messaggi ICMP, vedere l'URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt number — Il numero di volte in cui il flusso è stato autorizzato o negato da questa voce ACL nell'intervallo di tempo configurato. Il valore è 1 quando l'appliance ASA Secure Firewall

genera il primo messaggio per questo flusso.
- primo hit: il primo messaggio generato per questo flusso.
- numero - secondo intervallo - L'intervallo in cui viene accumulato il conteggio delle visite. Impostare questo intervallo con il comando **access-list** con l'opzione **interval**.
- Codici hash - vengono sempre stampati due per il gruppo di oggetti ACE e l'elemento ACE normale costitutivo. I valori vengono determinati in base all'ACE con cui il pacchetto ha avuto accesso. Per visualizzare questi codici hash, immettere il comando **show-access list**.

Esempio:

```
Dec 27 2021 15:09:58: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56261) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:15: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56266) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
Dec 27 2021 15:10:55: %ASA-6-106100: access-list OUT-IN permitted tcp
outside/10.65.63.155(56270) -> inside/10.5.0.30(8000) hit-cnt 1 first hit [0xa26b11fb,
0x00000000]
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

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).