ASA-toegangscontrolelijst configureren voor verschillende scenario's

Inhoud

Inleiding

Dit document beschrijft hoe u een toegangscontrolelijst (ACL) kunt configureren op de adaptieve security applicatie (ASA) voor verschillende scenario's.

Voorwaarden

Vereisten

Cisco raadt u aan kennis van ASA te hebben.

Gebruikte componenten

De informatie in dit document is gebaseerd op een ASA-softwareversie 8.3 en hoger.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

ACL's worden door de ASA gebruikt om te bepalen of verkeer is toegestaan of geweigerd. Door gebrek, verkeer dat van een **lagere** interface van het veiligheidsniveau aan een **hogere** interface van het veiligheidsniveau overgaat wordt ontkend terwijl het verkeer van een **hogere** interface van het veiligheidsniveau aan een **lagere** interface van het veiligheidsniveau wordt toegestaan. Ook dit gedrag kan met een ACL worden gewijzigd.

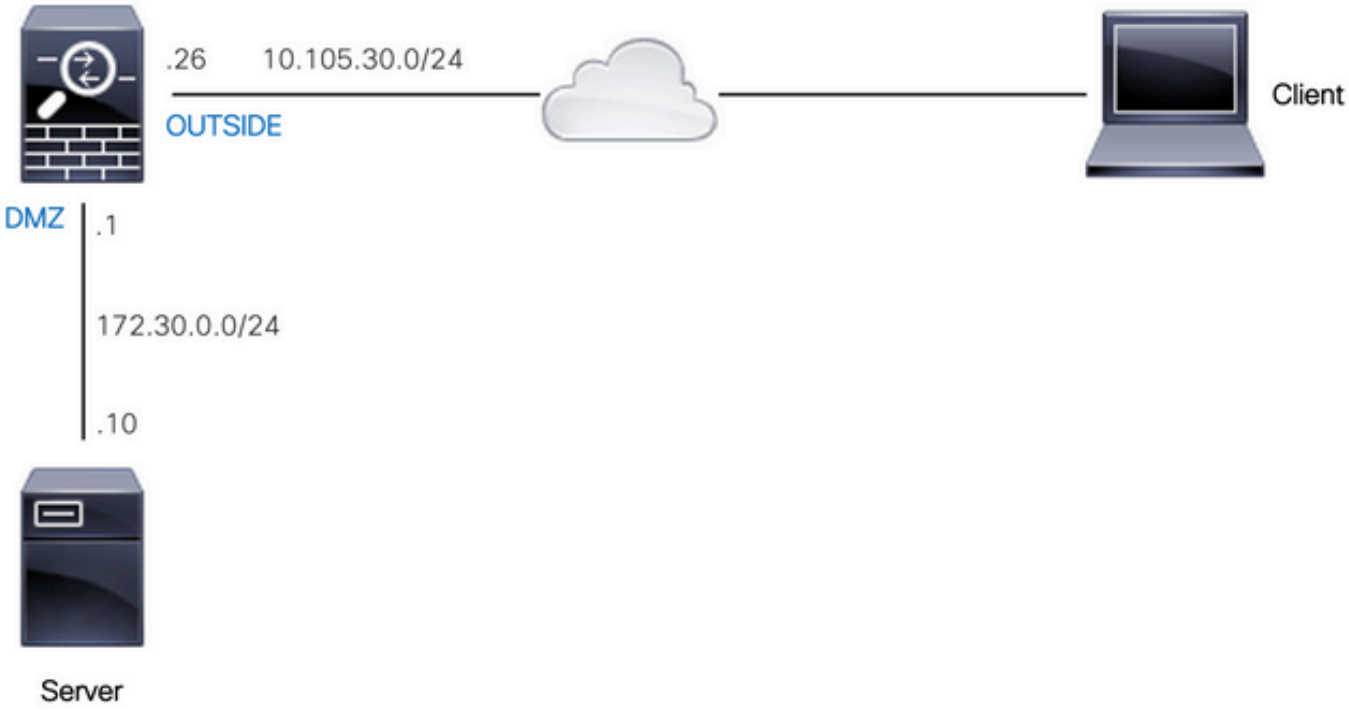
In aanwezigheid van NAT-regels controleert de ASA in eerdere versies van de ASA (8.2 en eerder) de ACL voordat de omzetting van het pakket op basis van de NAT-regel wordt gedemonteerd. In versie 8.3 en hoger annuleert de ASA het pakket voordat de ACL's worden gecontroleerd. Dit betekent dat voor een ASA versie 8.3 en hoger verkeer is toegestaan of geweigerd op basis van het echte IP-adres van de host in plaats van het vertaalde IP-adres. ACL's bestaan uit een of meer toegangscontrolevermeldingen (ACE's).

Configureren

Scenario 1. Een ACE configureren om toegang tot een webserver achter de DMZ mogelijk te maken

De client op het internet, die zich achter de buiteninterface bevindt, wil toegang tot een webserver die wordt gehost achter de DMZ-interface die luistert op TCP-poorten 80 en 443.

Netwerkdiagram



Het echte IP-adres van de webserver is 172.30.0.10. Een statische één-op-één NAT-regel is geconfigureerd om internetgebruikers toegang te geven tot de webserver met een vertaald IP-adres 10.105.130.27. ASA voert proxy-arp voor 10.105.130.27 standaard op de 'buiten'-interface uit wanneer een statische NAT-regel is geconfigureerd met een vertaald IP-adres dat in hetzelfde subnet valt als het 'buiten'-interface-IP-adres 10.105.130.26:

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

Configureer deze ACE zodat een IP-bronadres op het internet alleen op TCP-poorten 80 en 443 verbinding kan maken met de webserver. Wijs de ACL toe aan de buiteninterface in de inkomende richting:

```
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
```

Verifiëren

Start een pakkettraceropdracht met deze velden. Ingress-interface waarop u pakket kunt overtrekken: buiten

Protocol: TCP

IP-bronadres: elk IP-adres op het internet

IP-bronpoort: elke tijdelijke poort

IP-adres bestemming: vertaald IP-adres van de webserver (10.105.130.27)

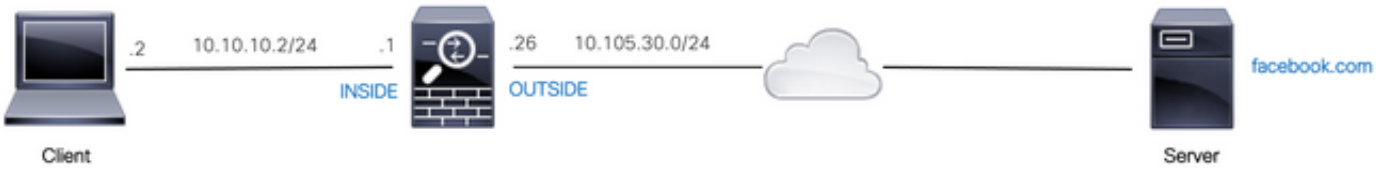
Doelpoort: 80 of 443

```
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. Een ACE configureren om toegang tot een webserver met een FQDN toe te staan

De client met IP-adres 10.10.10.2 in het Local Area Network (LAN) heeft toegang tot facebook.com.

Netwerkdiagram



Zorg ervoor dat de DNS-server correct op de ASA is geconfigureerd:

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

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

Configureer dit netwerkobject, FQDN-object en ACE om de client met IP-adres 10.10.10.2 toegang te geven tot 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
```

Verifiëren

De output van **show dns** toont het opgeloste IP adres voor FQDN facebook.com:

```
ciscoasa# show dns

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

De toegangslijst toont het FQDN-object zoals **opgelost** en toont ook het opgeloste IP-adres:

```
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. Een ACE configureren om alleen toegang tot een website toe te staan voor een specifieke tijdsduur in een dag

De client in het LAN heeft alleen toegang tot een website met IP-adres 10.02.20 uur per dag van 12 tot 2 uur per dag.

Netwerkdiagram

Zorg ervoor dat de tijdzone op de ASA correct is geconfigureerd:

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

Configureer een tijdbereikobject voor de gewenste tijdsduur:

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

Configureer deze netwerkobjecten en ACE om het IP-bronadres in het LAN toe te staan om de website alleen te openen tijdens de periode die wordt vermeld in het tijdbereikobject met de naam **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
```

Verifiëren

Het tijdbereikobject is **actief** wanneer de klok op de ASA een tijd aangeeft die binnen het tijdbereikobject valt:

```
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
```

Het tijdbereikobject en de ACE zijn **inactief** wanneer de klok op de ASA een tijd aangeeft die buiten het tijdbereikobject valt:

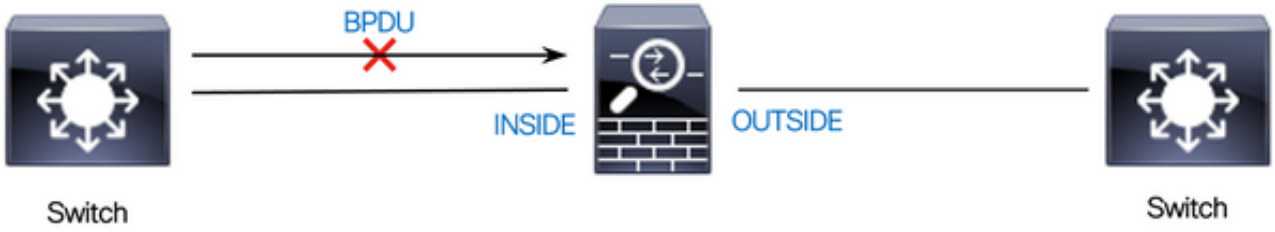
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


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. Configureer een ACE om Bridge Protocol Data Units (BPDU) te blokkeren via een ASA in Transparent Mode

Om lijnen met het Spanning Tree Protocol (STP) te voorkomen, worden BPDU's standaard door de ASA in transparante modus doorgegeven. Om BPDUs te blokkeren, moet u een regel van EtherType vormen om hen te ontkennen.

Netwerkdiagram



Configureer de EtherType ACL om BPDU's te blokkeren van het doorlopen van de 'binnen'-interface van de ASA in de inkomende richting zoals hier wordt getoond:

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

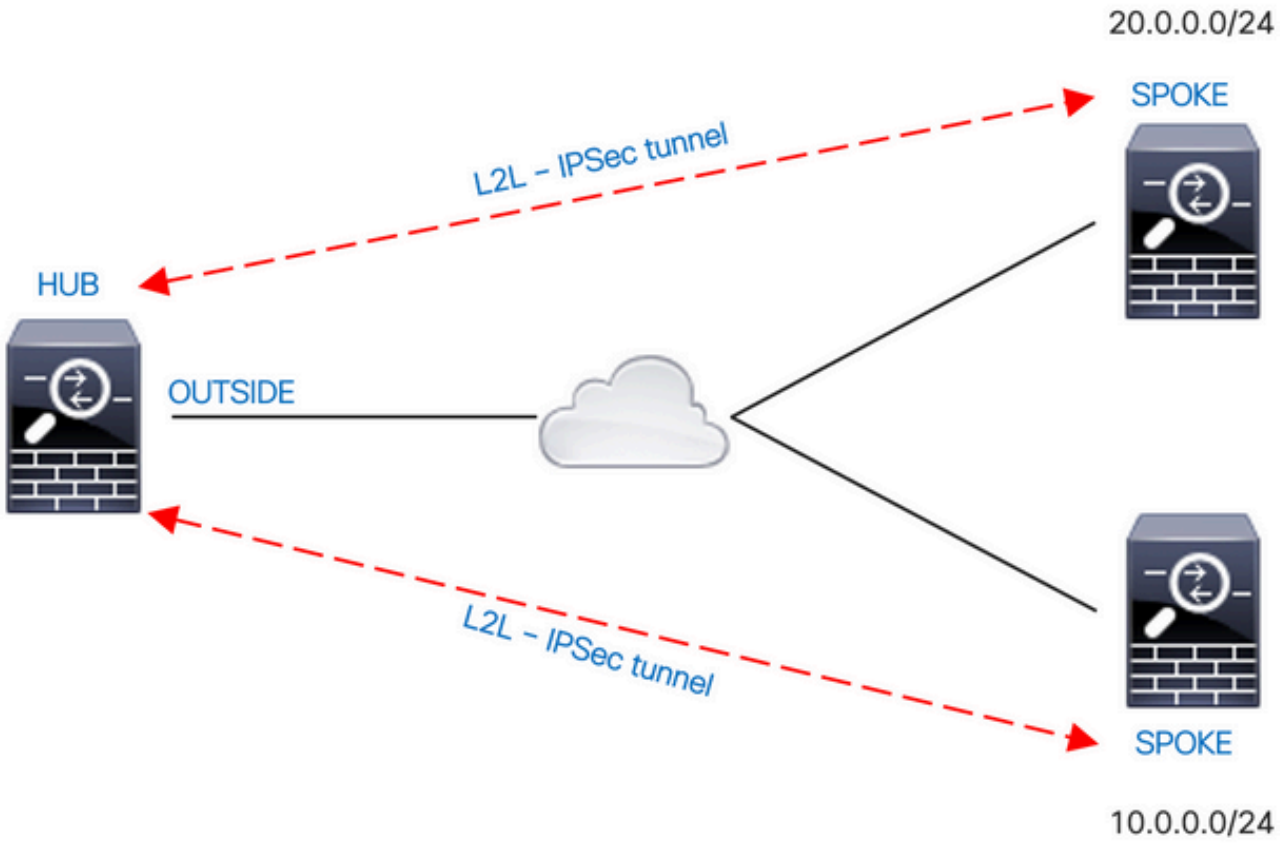
Verifiëren

Controleer het aantal treffers in de toegangslijst om te verifiëren dat BPDU's door de ASA worden geblokkeerd:

```
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. Sta verkeer toe om tussen interfaces met hetzelfde beveiligingsniveau door te gaan

Netwerkdiagram



Standaard wordt het verkeer tussen interfaces van hetzelfde beveiligingsniveau geblokkeerd. Om communicatie tussen interfaces met gelijke beveiligingsniveaus toe te staan, of om verkeer toe te staan om dezelfde interface in te voeren en te verlaten (hairpin/u-turn), gebruikt u de opdracht **zelfde-security-traffic** in de globale configuratiemodus.

Deze opdracht toont hoe communicatie tussen verschillende interfaces met hetzelfde beveiligingsniveau mogelijk moet worden gemaakt:

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

Dit voorbeeld laat zien hoe u communicatie in en vanuit dezelfde interface kunt toestaan:

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

Deze optie is handig voor VPN-verkeer dat een interface betreedt maar vervolgens uit dezelfde interface wordt gerouteerd. Bijvoorbeeld, als je een hub-and-spoke VPN-netwerk hebt waar deze ASA de hub is en de externe VPN-netwerken spokes zijn, zodat men kan communiceren met een ander spaak, moet het verkeer naar de ASA gaan en dan weer naar de ander spaak.

Verifiëren

Zonder het bevel van de **vergunning van het zelfde-veiligheid-verkeer interfacebevel**, wijst de output van pakket-tracer erop dat het verkeer dat tussen verschillende interfaces van het zelfde veiligheidsniveau overgaat wegens een **impliciete regel** zoals hier getoond wordt geblokkeerd:

```
!--- 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
```

Zonder het bevel van de **vergunning van het zelfde-veiligheid-verkeer intra-interface**, wijst de output van pakket-tracer erop dat het verkeer dat in en uit de zelfde interface overgaat wegens een **impliciete regel** zoals hier getoond wordt geblokkeerd:

```
!--- 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. Een ACE configureren om verkeer via de brievenbus te beheren

Het sleutelwoord **control-plane** specificeert als de ACL wordt gebruikt om het verkeer in de box te controleren. Toegangscontroleregels voor verkeer met alleen de box (gedefinieerd door opdrachten als **http**, **ssh** of **telnet**) hebben een hogere prioriteit dan een regel voor beheertoegang die wordt toegepast met de optie **control-plane**. Daarom moet zulk toegelaten beheersverkeer worden toegestaan om binnen te komen zelfs als uitdrukkelijk ontkend door de aan-de-doos ACL.

In tegenstelling tot reguliere toegangsregels is er geen impliciete ontkenning aan het eind van een verzameling beheerregels voor een interface. In plaats daarvan wordt elke verbinding die niet voldoet aan een toegangsregel voor het beheer vervolgens geëvalueerd door reguliere toegangscontroleregels. U kunt ook ICMP-regels gebruiken om ICMP-verkeer naar het apparaat te controleren.

Netwerkdiagram

Een ACL is geconfigureerd met het trefwoord **control-plane** om verkeer te blokkeren dat afkomstig is van het IP-adres 10.65.63.155 en bestemd is voor het 'buiten'-interface-IP-adres van de 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
```

Verifiëren

Controleer het aantal treffers in de toegangslijst om te controleren of het verkeer door de ACL wordt geblokkeerd:

```
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
```

Syslog-berichten geven aan dat het verkeer op de 'identiteits'-interface is verbroken:

```
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]
```

Vastlegging

Met het **logboeksleutelwoord** worden de registratieopties ingesteld wanneer een ACE een pakket aanpast voor netwerktoegang (een ACL die wordt toegepast met de opdracht **toegangsgroep**). Als u het **logwoord** zonder argumenten invoert, schakelt u het systeemlogbericht 106100 op het standaardniveau (6) en voor het standaardinterval (300 seconden) in. Als u het logsleutelwoord niet invoert, wordt het standaardbericht 106023 van het systeemlogboek gegenereerd voor geweigerde pakketten. De logopties zijn:

- niveau — een ernstniveau tussen 0 en 7. De standaardwaarde is 6 (informatief). Als u dit niveau wijzigt voor een actief ACE, is het nieuwe niveau van toepassing op nieuwe verbindingen; bestaande verbindingen blijven worden vastgelegd op het vorige niveau.
- **interval** secs — Het tijdsinterval in seconden tussen syslog-berichten, van 1 tot 600. De standaardwaarde is 300. Deze waarde wordt ook gebruikt als de timeout waarde voor het verwijderen van een inactieve stroom uit de cache die gebruikt wordt om drop-statistieken te verzamelen.
- **uitschakelen** — Schakelt alle ACE-logboekregistratie uit.
- **standaard** — hiermee kan worden ingelogd op 106023. Deze instelling is hetzelfde als het niet opnemen van de logoptie.

Syslog-bericht 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]
```

Uitleg:

Een echt IP-pakket werd door de ACL ontkend. Dit bericht verschijnt zelfs als u niet de logboekoptie hebt die voor ACL wordt toegelaten. Het IP-adres is het echte IP-adres in plaats van de waarden die via NAT worden weergegeven. Zowel de informatie van de gebruikersidentiteit als de informatie FQDN wordt verstrekt voor de IP adressen als geëvenaarde wordt gevonden. De Secure Firewall ASA registreert identiteitsinformatie (domein\gebruiker) of FQDN (als de gebruikersnaam niet beschikbaar is). Als de identiteitsinformatie of FQDN beschikbaar is, registreert de Secure Firewall ASA deze informatie voor zowel de bron als de bestemming.

Voorbeeld:

```
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]
```

Syslog-bericht 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
```

Uitleg:

Het eerste voorkomen of het totale aantal voorvallen tijdens een interval worden vermeld. Dit bericht geeft meer informatie dan 106023, die alleen ontkende pakketten vastlegt, en bevat niet de hit count of een configureerbaar niveau.

Wanneer een toegangslijst het *logargument* heeft, wordt verwacht dat deze bericht-ID kan worden geactiveerd vanwege een niet-gesynchroniseerd pakket dat bij de Secure Firewall ASA aankomt en door de toegangslijst wordt geëvalueerd. Als er bijvoorbeeld een ACK-pakket wordt ontvangen op de Secure Firewall ASA (waarvoor geen TCP-verbinding bestaat in de verbindingstabel), kan de Secure Firewall ASA 106100 genereren, die aangeeft dat het pakket is toegestaan. Het pakket wordt echter later op de juiste manier verwijderd omdat er geen overeenkomende verbinding is.

De lijst beschrijft de berichtwaarden:

- geautoriseerd | geweigerd | Toegestaan-Deze waarden specificeren als het pakket werd toegelaten of door ACL werd ontkend. Als de waarde wordt ingesteld, wordt het pakket ontkend door de ACL maar voor een reeds gevestigde sessie toegestaan (bijvoorbeeld, wordt een interne gebruiker toegang tot internet verleend, en worden antwoordpakketten die normaal door de ACL zouden worden ontkend, aanvaard).
- protocol — TCP, UDP, ICMP of een IP-protocolnummer.
- interface_name — De interfacenaam voor de bron of de bestemming van de geregistreerde stroom. De VLAN-interfaces worden ondersteund.
- source_address — Het IP-bronadres van de gelogde stroom. Het IP-adres is het echte IP-adres in plaats van de waarden die via NAT worden weergegeven.
- dest_address — Het IP-adres van de bestemming van de gelogde stroom. Het IP-adres is het echte IP-adres in plaats van de waarden die via NAT worden weergegeven.
- source_port — De bronpoort van de geregistreerde stroom (TCP of UDP). Voor ICMP is het nummer na de bronpoort het berichttype.
- idfw_user — De gebruikersnaam voor de gebruikersidentiteit, met de domeinnaam die wordt toegevoegd aan de bestaande syslog wanneer de Secure Firewall ASA de gebruikersnaam voor het IP-adres kan vinden.
- sg_info — De beveiligingsgroeptag die aan de syslog wordt toegevoegd wanneer de Secure Firewall ASA een beveiligingsgroeptag voor het IP-adres kan vinden. De naam van de beveiligingsgroep wordt weergegeven met de tag voor de beveiligingsgroep, indien beschikbaar.
- dest_port — De bestemmingshaven van de geregistreerde stroom (TCP of UDP). Voor ICMP is het nummer na de bestemmingshaven de ICMP-berichtcode, die beschikbaar is voor bepaalde berichttypen. Voor type 8 is het altijd 0. Zie de URL voor een lijst met ICMP-berichttypen: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt nummer — het aantal keren dat deze stroom werd toegestaan of ontkend door deze ACL-ingang in het ingestelde tijdsinterval. De waarde is 1 wanneer de Secure Firewall ASA

het eerste bericht voor deze stroom genereert.
- Eerste treffer — Het eerste bericht dat voor deze stroom wordt gegenereerd.
- aantal - tweede interval - het interval waarin de klaptelling wordt geaccumuleerd. Stel dit interval in met de opdracht **toegangslijst** met de optie **interval**.
- hashcodes — Er worden altijd twee gedrukt voor de objectgroep ACE en de samenstellende gewone ACE. De waarden worden bepaald waarop ACE het pakket sloeg. Om deze hashcodes weer te geven, voert u de opdracht **show-access list in**.

Voorbeeld:

```
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]
```

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

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.