Konfigurieren der ASA-Zugriffskontrollliste für verschiedene Szenarien

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine Zugriffskontrollliste (ACL) auf der Adaptive Security Appliance (ASA) für verschiedene Szenarien konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse der ASA verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der ASA Software Version 8.3 und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Anhand von ACLs bestimmt die ASA, ob Datenverkehr zugelassen oder abgelehnt wird. Standardmäßig wird Datenverkehr, der von einer Schnittstelle **mit niedrigerer** Sicherheitsstufe an eine Schnittstelle mit **höherer** Sicherheitsstufe weitergeleitet wird, verweigert, wohingegen Datenverkehr von einer Schnittstelle mit **höherer** Sicherheitsstufe an eine Schnittstelle mit **niedrigerer** Sicherheitsstufe zulässig ist. Dieses Verhalten kann ebenfalls mit einer ACL außer Kraft gesetzt werden.

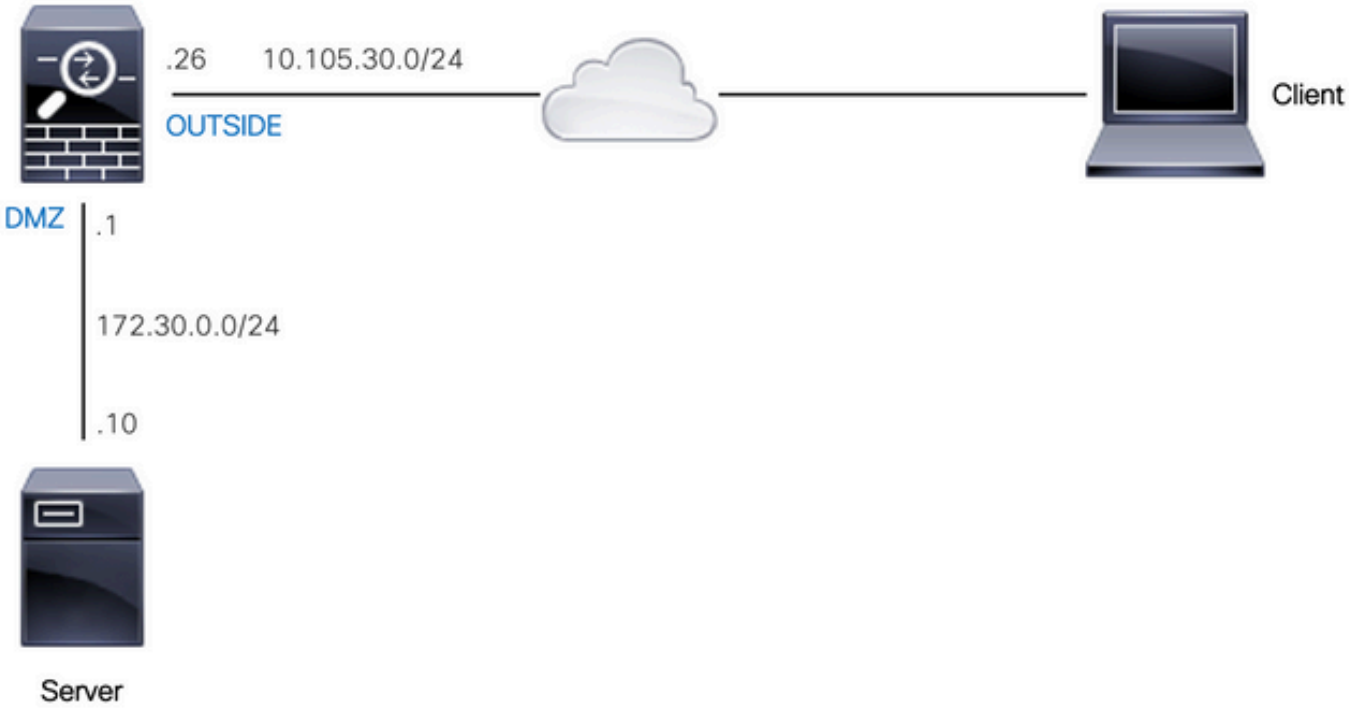
Bei Vorhandensein von NAT-Regeln überprüft die ASA in früheren Versionen der ASA-Version (8.2 und früher) die ACL, bevor sie die Übersetzung des Pakets auf der Grundlage der abgeglichenen NAT-Regel aufhebt. In Version 8.3 und höher wird die Übersetzung des Pakets von der ASA entfernt, bevor die ACLs überprüft werden. Das bedeutet, dass bei einer ASA-Version 8.3 und höher der Datenverkehr entweder zugelassen wird oder abgelehnt wird, basierend auf der tatsächlichen IP-Adresse des Hosts, anstatt der umgewandelten IP-Adresse. ACLs bestehen aus einem oder mehreren Zugriffskontrolleinträgen (Access Control Entries, ACEs).

Konfigurieren

Szenario 1. Konfigurieren eines ACE für den Zugriff auf einen Webserver hinter der DMZ

Der Client im Internet, der sich hinter der externen Schnittstelle befindet, möchte auf einen Webserver zugreifen, der hinter der DMZ-Schnittstelle gehostet wird und die TCP-Ports 80 und 443 abhört.

Netzwerkdiagramm



Die tatsächliche IP-Adresse des Webservers lautet 172.30.0.10. Eine statische One-to-One NAT-Regel wird konfiguriert, um Internetbenutzern den Zugriff auf den Webserver mit der übersetzten IP-Adresse 10.105.130.27 zu ermöglichen. Die ASA führt standardmäßig Proxy-ARP für 10.105.130.27 an der externen Schnittstelle durch, wenn eine statische NAT-Regel mit einer umgewandelten IP-Adresse konfiguriert wird, die in dasselbe Subnetz fällt wie die IP-Adresse der externen Schnittstelle 10.105.130.26:

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

Konfigurieren Sie diesen ACE so, dass jede IP-Quelladresse im Internet nur über die TCP-Ports 80 und 443 eine Verbindung zum Webserver herstellen kann. Weisen Sie der externen Schnittstelle die ACL in Eingangsrichtung zu:

```
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
```

Überprüfung

Führen Sie einen Paket-Tracer-Befehl mit diesen Feldern aus. Eingangsschnittstelle, an der das Paket verfolgt werden soll: außen

Protokoll: TCP

Quell-IP-Adresse: Jede IP-Adresse im Internet

Quell-IP-Port: jeder ephemere Port

Ziel-IP-Adresse: Übersetzte IP-Adresse des Webservers (10.105.130.27)

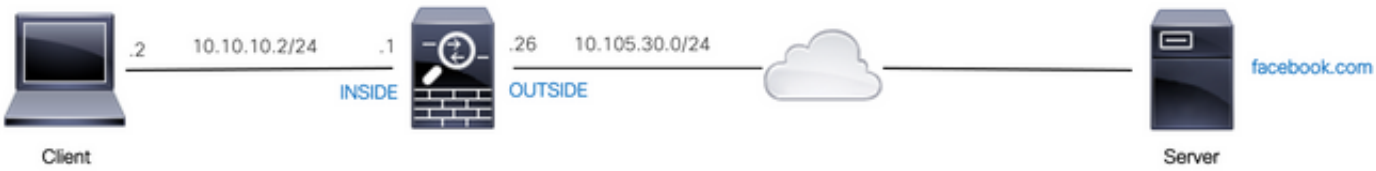
Zielport: 80 oder 443

```
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
```

Szenario 2. Konfigurieren eines ACE zum Zulassen des Zugriffs auf einen Webserver mit einem FQDN

Clients mit der IP-Adresse 10.10.10.2, die sich im LAN (Local Area Network) befindet, können auf facebook.com zugreifen.

Netzwerkdiagramm



Stellen Sie sicher, dass der DNS-Server auf dem ASA-Gerät korrekt konfiguriert ist:

```
ciscoasa# show run dns
dns domain-lookup outside
```

```
dns server-group DefaultDNS
name-server 10.0.2.2
name-server 10.0.8.8
```

Konfigurieren Sie dieses Netzwerkobjekt, das FQDN-Objekt und den ACE, damit der Client mit der IP-Adresse 10.10.10.2 auf facebook.com zugreifen kann.

```
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
```

Überprüfung

Die Ausgabe von **show dns** zeigt die aufgelöste IP-Adresse für den FQDN facebook.com:

```
ciscoasa# show dns

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

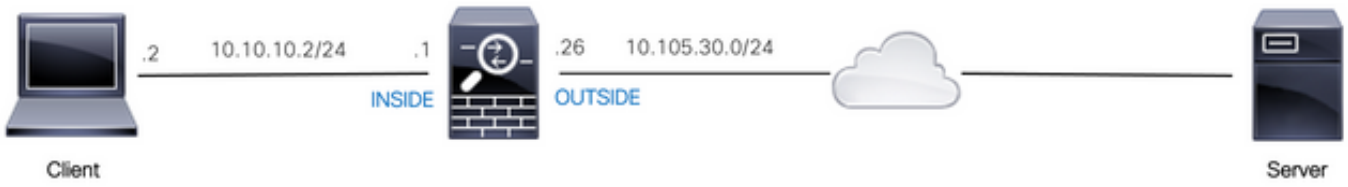
In der Zugriffsliste wird das FQDN-Objekt als **aufgelöst** sowie die aufgelöste IP-Adresse angezeigt:

```
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
```

Szenario 3. Konfigurieren eines ACE, um den Zugriff auf eine Website nur für eine bestimmte Zeitdauer an einem Tag zu ermöglichen

Der Client im LAN darf nur auf eine Website mit der IP-Adresse 10.0.20.20 täglich von 12:00 Uhr bis 14:00 Uhr IST zugreifen.

Netzwerkdiagramm



Stellen Sie sicher, dass die Zeitzone auf dem ASA-Gerät korrekt konfiguriert ist:

```
ciscoasa# show run clock
```

```
clock timezone IST 5 30
```

Konfigurieren Sie ein Zeitbereichsobjekt für die erforderliche Zeitdauer:

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

Konfigurieren Sie diese Netzwerkobjekte und den ACE so, dass jede beliebige Quell-IP-Adresse im LAN nur während des Zeitraums auf die Website zugreifen kann, der im Zeitbereichsobjekt **BREAK_TIME** angegeben ist:

```
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
```

Überprüfung

Das Zeitbereichsobjekt ist **aktiv,** wenn die Uhr auf dem ASA-Gerät eine Zeit anzeigt, die innerhalb des Zeitbereichsobjekts liegt:

```
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
```

Sowohl das Zeitbereichsobjekt als auch der ACE ist **inaktiv,** wenn die Uhr auf der ASA eine Zeit anzeigt, die außerhalb des Zeitbereichsobjekts liegt:

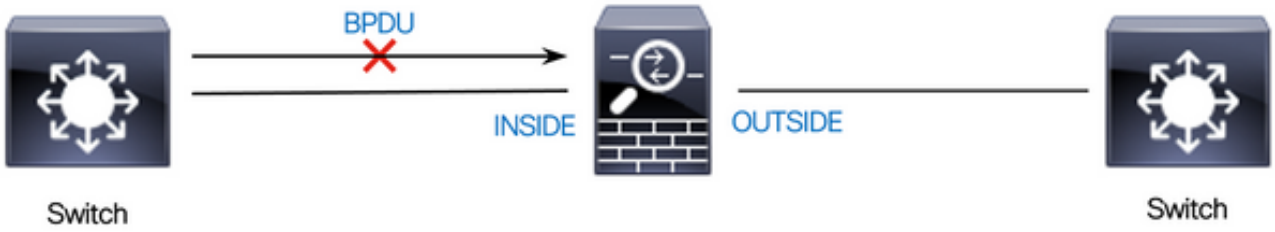
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021

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
```

Szenario 4. Konfigurieren eines ACE zum Blockieren von Bridge-Protokoll-Dateneinheiten (BPDU) über ein ASA im transparenten Modus

Um Schleifen mit dem Spanning Tree Protocol (STP) zu verhindern, werden BPDUs standardmäßig im transparenten Modus über die ASA geleitet. Um BPDUs zu blockieren, müssen Sie eine EtherType-Regel konfigurieren, um sie abzulehnen.

Netzwerkdiagramm



Konfigurieren Sie die EtherType-ACL so, dass BPDUs die interne Schnittstelle der ASA nicht in eingehender Richtung passieren können, wie hier gezeigt:

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

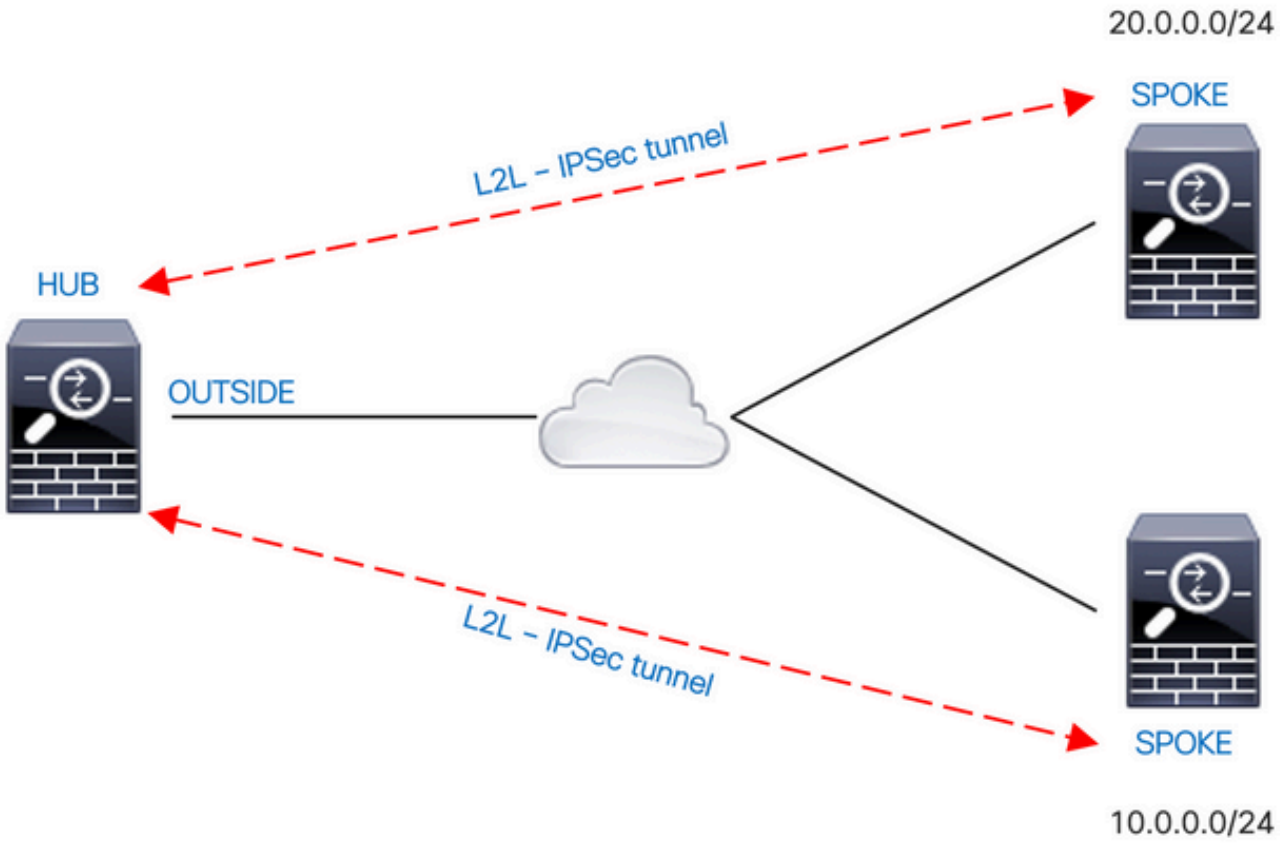
Überprüfung

Überprüfen Sie die Trefferanzahl in der Zugriffsliste, um sicherzustellen, dass BPDUs von der ASA blockiert werden:

```
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)
```

Szenario 5. Datenverkehr zwischen Schnittstellen mit derselben Sicherheitsstufe passieren lassen

Netzwerkdiagramm



Standardmäßig wird der Datenverkehr zwischen Schnittstellen derselben Sicherheitsstufe blockiert. Um die Kommunikation zwischen Schnittstellen mit gleichen Sicherheitsstufen zu ermöglichen oder um zu ermöglichen, dass Datenverkehr über die gleiche Schnittstelle (Hairpin/U-Turn) eingeht und diese verlässt, verwenden Sie den Befehl **same-security-traffic** im globalen Konfigurationsmodus.

Dieser Befehl zeigt, wie die Kommunikation zwischen verschiedenen Schnittstellen mit derselben Sicherheitsstufe zugelassen wird:

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

Dieses Beispiel zeigt, wie die Kommunikation innerhalb und außerhalb derselben Schnittstelle zugelassen wird:

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

Diese Funktion ist für VPN-Datenverkehr nützlich, der über eine Schnittstelle eingeht, dann aber über dieselbe Schnittstelle weitergeleitet wird. Wenn Sie beispielsweise ein Hub-and-Spoke-VPN-Netzwerk haben, bei dem diese ASA der Hub ist und die Remote-VPN-Netzwerke Spokes sind, muss der Datenverkehr, damit eine Spoke mit einer anderen Spoke kommunizieren kann, zur ASA und dann wieder zur anderen Spoke geleitet werden.

Überprüfung

Ohne den Befehl **same-security-traffic permit inter-interface** gibt die Ausgabe von Packet-Tracer an, dass der Datenverkehr zwischen verschiedenen Schnittstellen derselben Sicherheitsstufe aufgrund einer **impliziten Regel** blockiert wird, wie hier gezeigt:

```
!--- 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
```

Ohne den **Befehl "same-security-traffic permit intra-interface"** gibt die Ausgabe von Packet-Tracer an, dass der Datenverkehr, der über dieselbe Schnittstelle ein- und ausgeht, aufgrund einer **impliziten Regel** blockiert wird, wie hier gezeigt:

```
!--- 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
```

Szenario 6. Konfigurieren eines ACE zur Steuerung des Datenverkehrs

Das Schlüsselwort **control-plane** gibt an, ob die ACL zur Steuerung des standardmäßigen Datenverkehrs verwendet wird. Zugriffskontrollregeln für sofort nutzbaren Verwaltungsdatenverkehr (definiert durch Befehle wie **http, ssh** oder **telnet)** haben eine höhere Priorität als eine Verwaltungszugriffsregel, die mit der Option **Kontrollebene** angewendet wird. Aus diesem Grund muss der Eintritt des zugelassenen Management-Datenverkehrs auch dann erlaubt sein, wenn er von der sofort einsatzbereiten ACL ausdrücklich verweigert wird.

Im Gegensatz zu regulären Zugriffsregeln gibt es am Ende einer Reihe von Verwaltungsregeln für eine Schnittstelle keine implizite Ablehnung. Stattdessen wird jede Verbindung, die nicht mit einer Management-Zugriffsregel übereinstimmt, von regulären Zugriffskontrollregeln ausgewertet. Alternativ können Sie ICMP-Regeln verwenden, um den ICMP-Datenverkehr zum Gerät zu steuern.

Netzwerkdiagramm

Eine ACL wird mit dem **Kontrollebenen-**Schlüsselwort konfiguriert, um sofort verfügbaren Datenverkehr zu blockieren, der von der IP-Adresse 10.65.63.155 stammt und für die "externe" Schnittstellen-IP-Adresse der ASA bestimmt ist.

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

Überprüfung

Überprüfen Sie die Trefferanzahl in der Zugriffsliste, um sicherzustellen, dass der Datenverkehr von der ACL blockiert wird:

```
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-Meldungen weisen darauf hin, dass Datenverkehr an der Identitätsschnittstelle verloren geht:

```
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]
```

Protokollieren

Das Schlüsselwort **log** legt Protokollierungsoptionen fest, wenn ein ACE mit einem Paket für den Netzwerkzugriff übereinstimmt (eine ACL, die mit dem Befehl **access-group** angewendet wird). Wenn Sie das **log-**Schlüsselwort ohne Argumente eingeben, aktivieren Sie die Systemprotokollmeldung 106100 auf der Standardebene (6) und für das Standardintervall (300 Sekunden). Wenn Sie das Schlüsselwort log nicht eingeben, wird die Standard-Systemprotokollmeldung 106023 für abgelehnte Pakete generiert. Folgende Protokolloptionen stehen zur Verfügung:

- level - Ein Schweregrad zwischen 0 und 7. Der Standardwert ist 6 (informativ). Wenn Sie diese Ebene für einen aktiven ACE ändern, gilt die neue Ebene für neue Verbindungen; bestehende Verbindungen werden weiterhin auf der vorherigen Ebene protokolliert.
- **interval** secs - Das Zeitintervall in Sekunden zwischen Syslog-Meldungen, von 1 bis 600. Der Standardwert ist 300. Dieser Wert wird auch als Timeoutwert zum Löschen eines inaktiven Flusses aus dem Cache verwendet, der zum Erfassen von Verwerfungsstatistiken verwendet wird.
- **disable** - Deaktiviert die gesamte ACE-Protokollierung.
- **default** — Aktiviert die Protokollierung in Meldung 106023. Diese Einstellung entspricht dem Verzicht auf die Protokolloption.

Syslog-Meldung 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]
```

Erläuterung:

Ein echtes IP-Paket wurde von der ACL abgelehnt. Diese Meldung wird auch angezeigt, wenn die Protokolloption für eine ACL nicht aktiviert ist. Die IP-Adresse ist die tatsächliche IP-Adresse, nicht die Werte, die über NAT angezeigt werden. Für die IP-Adressen werden sowohl Benutzeridentitätsinformationen als auch FQDN-Informationen bereitgestellt, wenn eine übereinstimmende gefunden wird. Die Secure Firewall ASA protokolliert entweder Identitätsinformationen (Domäne\Benutzer) oder FQDN (wenn der Benutzername nicht verfügbar ist). Wenn Identitätsinformationen oder FQDN verfügbar sind, protokolliert die Secure Firewall ASA diese Informationen sowohl für die Quelle als auch das Ziel.

Beispiel:

```
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-Meldung 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
```

Erläuterung:

Der erste Vorfall oder die Gesamtzahl der Vorfälle während eines Intervalls werden aufgelistet. Diese Nachricht enthält mehr Informationen als die Nachricht 106023, in der nur abgelehnte Pakete protokolliert werden, jedoch weder die Trefferanzahl noch eine konfigurierbare Ebene.

Wenn eine Zugriffslistenzeile das *log*-Argument enthält, wird erwartet, dass diese Nachrichten-ID ausgelöst werden kann, weil ein nicht synchronisiertes Paket bei der Secure Firewall ASA eingeht und von der Zugriffsliste ausgewertet wird. Wenn beispielsweise ein ACK-Paket auf der Secure Firewall ASA empfangen wird (für das in der Verbindungstabelle keine TCP-Verbindung vorhanden ist), kann die Secure Firewall ASA die Meldung 106100 generieren, die angibt, dass das Paket zulässig war. Das Paket wird jedoch später korrekt verworfen, da keine übereinstimmende Verbindung besteht.

Die Liste beschreibt die Nachrichtenwerte:

- erlaubt | abgelehnt | est-allowed - Diese Werte geben an, ob die ACL das Paket zugelassen oder abgelehnt hat. Wenn der Wert "set-allowed" lautet, wurde das Paket von der ACL abgelehnt, aber für eine bereits eingerichtete Sitzung zugelassen (z. B. kann ein interner Benutzer auf das Internet zugreifen, und antwortende Pakete, die normalerweise von der ACL abgelehnt werden, werden akzeptiert).
- Protokoll - TCP, UDP, ICMP oder eine IP-Protokollnummer.
- interface_name - Der Schnittstellenname für die Quelle oder das Ziel des protokollierten Datenflusses. Die VLAN-Schnittstellen werden unterstützt.
- source_address - Die Quell-IP-Adresse des protokollierten Datenflusses. Die IP-Adresse ist die tatsächliche IP-Adresse, nicht die Werte, die über NAT angezeigt werden.
- dest_address - Die Ziel-IP-Adresse des protokollierten Datenflusses. Die IP-Adresse ist die tatsächliche IP-Adresse, nicht die Werte, die über NAT angezeigt werden.
- source_port - Der Quellport des protokollierten Datenflusses (TCP oder UDP). Bei ICMP ist die Nummer nach dem Quellport der Meldungstyp.
- idfw_user - Der Benutzername für die Benutzeridentität mit dem Domänennamen, der dem vorhandenen Syslog hinzugefügt wird, wenn die Secure Firewall ASA den Benutzernamen für die IP-Adresse finden kann.
- sg_info - Das Sicherheitsgruppen-Tag, das dem Syslog hinzugefügt wird, wenn die Secure Firewall ASA ein Sicherheitsgruppen-Tag für die IP-Adresse finden kann. Der

Sicherheitsgruppenname wird zusammen mit dem Sicherheitsgruppentag angezeigt, falls verfügbar.

- dest_port - Der Zielport des protokollierten Datenflusses (TCP oder UDP). Für ICMP ist die Nummer nach dem Zielport der ICMP-Nachrichtencode, der für einige Nachrichtentypen verfügbar ist. Beim Typ 8 ist es immer 0. Eine Liste der ICMP-Nachrichtentypen finden Sie unter der URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt-Nummer - Die Anzahl der zulässigen oder abgelehnten Datenflüsse durch diesen ACL-Eintrag im konfigurierten Zeitintervall. Der Wert ist 1, wenn die Secure Firewall ASA die erste Nachricht für diesen Fluss generiert.
- Erster Treffer - Die erste für diesen Fluss generierte Nachricht.
- number - second interval (Zahl - Sekunden-Intervall): Intervall, in dem die Trefferanzahl kumuliert wird. Legen Sie dieses Intervall mit dem Befehl **access-list** mit der Option **interval (Intervall) fest**.
- Hash-Codes - Für die Objektgruppe ACE und den konstituierenden regulären ACE werden immer zwei ausgegeben. Es werden Werte ermittelt, auf welchen ACE das Paket trifft. Um diese Hash-Codes anzuzeigen, geben Sie den Befehl **show-access list** ein.

Beispiel:

```
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]
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.