다양한 시나리오에 대한 ASA 액세스 제어 목록 구성

목차

소개

이 문서에서는 다양한 시나리오에서 ASA(Adaptive Security Appliance)에 ACL(Access Control List)을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

ASA에 대한 지식이 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 ASA 소프트웨어 버전 8.3 이상을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ACL은 ASA에서 트래픽의 허용 또는 거부 여부를 확인하는 데 사용됩니다. 기본적으로 **더 낮은** 보안 수준 인터페이스에서 **더 높은** 보안 수준 인터페이스로 전달되는 트래픽은 거부되는 반면, **더 높은** 보안 수준 인터페이스에서 **더 낮은** 보안 수준 인터페이스로 전달되는 트래픽은 허용됩니다. 이 동작은 ACL로 재정의할 수도 있습니다.

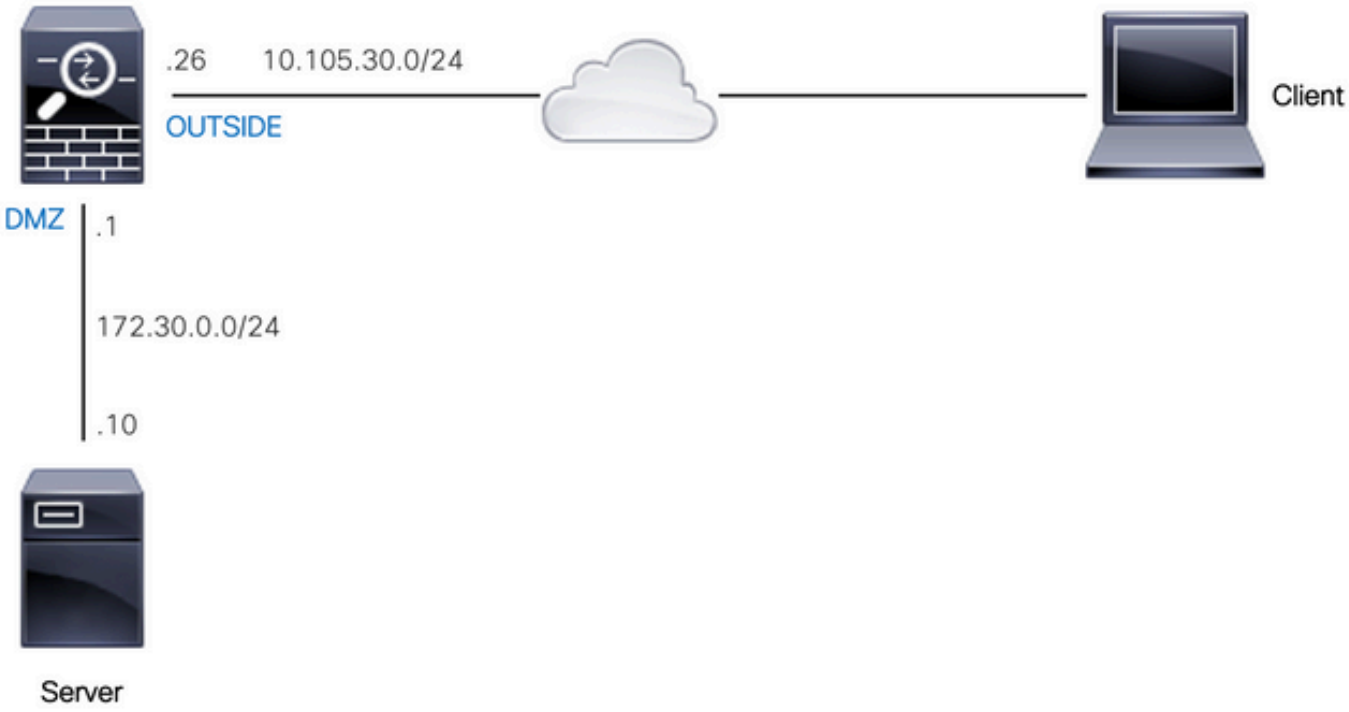
NAT 규칙이 있는 경우 이전 버전의 ASA(8.2 이하)에서는 ASA가 일치하는 NAT 규칙을 기반으로 패킷을 변환하지 않기 전에 ACL을 확인합니다. 버전 8.3 이상에서는 ASA가 ACL을 확인하기 전에 패킷을 변환하지 않습니다. 즉, ASA 버전 8.3 이상에서는 변환된 IP 주소 대신 호스트의 실제 IP 주소를 기준으로 트래픽이 허용되거나 거부됩니다. ACL은 하나 이상의 ACE(Access Control Entry)로 구성됩니다.

구성

시나리오 1. DMZ 뒤에 있는 웹 서버에 대한 액세스를 허용하도록 Ace 구성

외부 인터페이스 뒤에 있는 인터넷의 클라이언트는 TCP 포트 80 및 443에서 수신하는 DMZ 인터페이스 뒤에 호스트되는 웹 서버에 액세스하려고 합니다.

네트워크 다이어그램



웹 서버의 실제 IP 주소는 172.30.0.10입니다. 인터넷 사용자가 변환된 IP 주소 10.105.130.27을 사용하여 웹 서버에 액세스할 수 있도록 고정 일대일 NAT 규칙이 구성됩니다. 고정 NAT 규칙이 '외부' 인터페이스 IP 주소 10.105.130.26과 동일한 서브넷에 속하는 변환된 IP 주소로 구성된 경우 ASA는 기본적으로 '외부' 인터페이스에서 10.105.130.27에 대해 프록시 ARP를 수행합니다.

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

인터넷의 모든 소스 IP 주소가 TCP 포트 80 및 443에서만 웹 서버에 연결되도록 이 ACE를 구성합니다. 인바운드 방향의 외부 인터페이스에 ACL을 할당합니다.

```
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
```

다음을 확인합니다.

이러한 필드에서 packet-tracer 명령을 실행합니다. 패킷을 추적할 인그레스 인터페이스: 외부

프로토콜: TCP

Source IP address(소스 IP 주소): 인터넷에 있는 모든 IP 주소

Source IP Port(소스 IP 포트): 모든 임시 포트

대상 IP 주소: 웹 서버의 변환된 IP 주소(10.105.130.27)

Destination Port(대상 포트): 80 또는 443

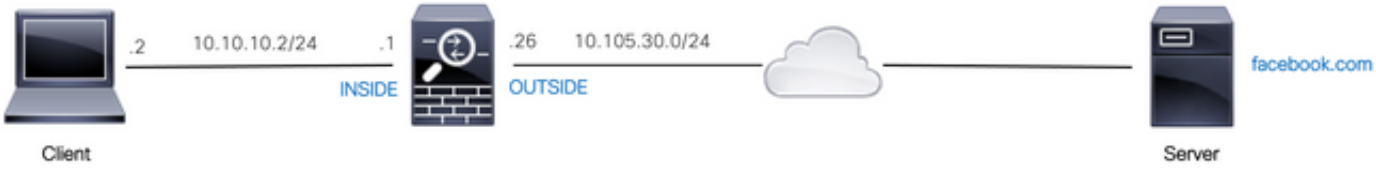
```
ciscoasa# packet-tracer input outside tcp 10.0.50.50 1234 10.105.130.27 443

!--- 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
```

시나리오 2. FQDN을 사용하여 웹 서버에 대한 액세스를 허용하도록 Ace 구성

LAN(Local Area Network)에 IP 주소가 10.10.10.2인 클라이언트는 facebook.com에 액세스할 수 있습니다.

네트워크 다이어그램



DNS 서버가 ASA에 올바르게 구성되어 있는지 확인합니다.

```
ciscoasa# show run dns
dns domain-lookup outside
dns server-group DefaultDNS
name-server 10.0.2.2
name-server 10.0.8.8
```

IP 주소가 10.10.10.2인 클라이언트가 facebook.com에 액세스할 수 있도록 이 네트워크 개체, FQDN 개체 및 ACE를 구성합니다.

```
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
```

다음을 확인합니다.

show dns의 **출력에는** FQDN facebook.com에 대한 확인된 IP 주소가 표시됩니다.

```
ciscoasa# show dns

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

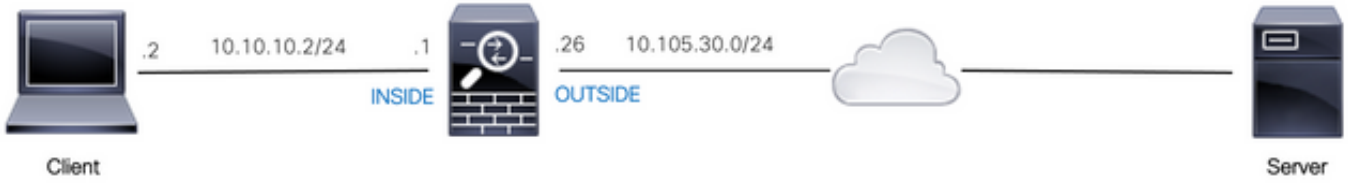
액세스 목록은 FQDN 객체를 **확인된** 것으로 표시하고 확인된 IP 주소도 표시합니다.

```
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
```

시나리오 3. 하루 중 특정 기간에만 웹 사이트 액세스를 허용하도록 Ace 구성

LAN에 있는 클라이언트는 IP 주소가 10.0.20.20인 웹 사이트에 매일 오후 12시부터 오후 2시까지만 액세스할 수 있습니다.

네트워크 다이어그램



ASA에서 표준 시간대가 올바르게 구성되었는지 확인합니다.

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

필요한 기간에 대한 시간 범위 객체를 구성합니다.

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

LAN에 있는 모든 소스 IP 주소가 BREAK_TIME이라는 시간 범위 객체에 언급된 기간 동안에만 웹 사이트에 액세스하도록 허용하려면 다음 네트워크 객체 및 ACE를 **구성합니다.**

```
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
```

다음을 확인합니다.

ASA의 클럭이 time-range 개체 내에 있는 시간을 나타낼 경우 time-range 개체는 활성화됩니다.

```
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
```

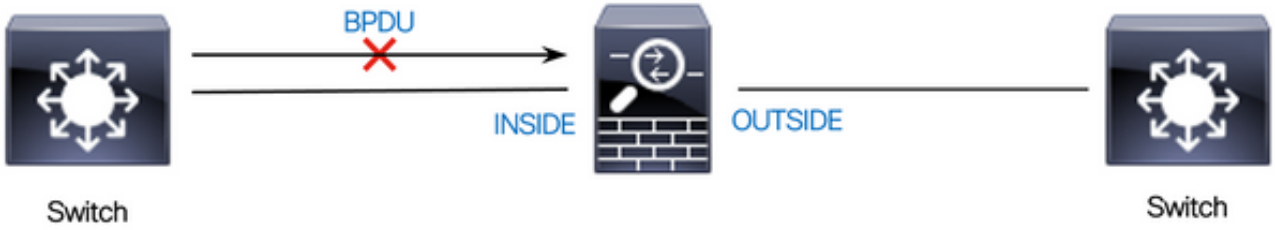
ASA의 시계가 시간 범위 객체를 벗어난 시간을 나타낼 경우 시간 범위 객체와 ACE는 **비활성** 상태입니다.

```
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
```

시나리오 4. 투명 모드에서 ASA를 통해 Bpdu(Bridge Protocol Data Unit)를 차단하도록 Ace 구성

STP(Spanning Tree Protocol)와의 루프를 방지하기 위해 BPDU는 기본적으로 투명 모드에서 ASA를 통과합니다. BPDU를 차단하려면 EtherType 규칙을 구성하여 거부해야 합니다.

네트워크 다이어그램



다음과 같이 BPDU가 인바운드 방향으로 ASA의 '내부' 인터페이스를 통과하지 못하도록 EtherType ACL을 구성합니다.

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

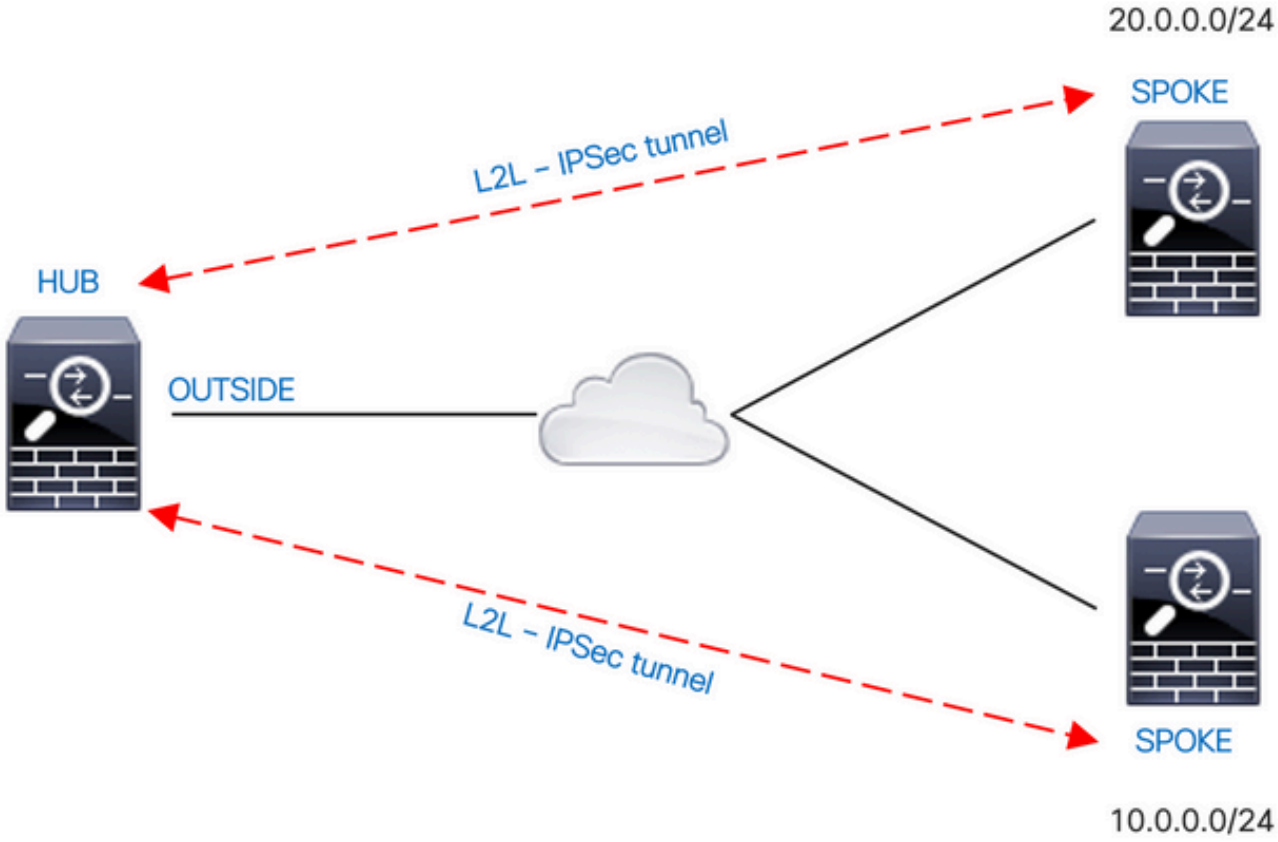
다음을 확인합니다.

BPDU가 ASA에 의해 차단되었는지 확인하려면 access-list에서 hit count를 확인합니다.

```
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)
```

시나리오 5. 보안 수준이 동일한 인터페이스 간에 트래픽 전달 허용

네트워크 다이어그램



기본적으로 동일한 보안 수준의 인터페이스 사이를 통과하는 트래픽은 차단됩니다. 보안 수준이 동일한 인터페이스 간의 통신을 허용하거나 트래픽이 동일한 인터페이스(헤어핀/u-turn)로 들어오고 나가도록 허용하려면 글로벌 컨피그레이션 모드에서 same-**security-traffic 명령**을 사용합니다.

이 명령은 보안 수준이 동일한 서로 다른 인터페이스 간의 통신을 허용하는 방법을 보여줍니다.

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

다음 예에서는 동일한 인터페이스에서 들어오고 나가는 통신을 허용하는 방법을 보여 줍니다.

same-security-traffic permit intra-interface
이 기능은 인터페이스에 진입하지만 동일한 인터페이스에서 라우팅되는 VPN 트래픽에 유용합니다. 예를 들어, 이 ASA가 허브이고 원격 VPN 네트워크가 스포크인 허브 앤 스포크 VPN 네트워크가 있는 경우 한 스포크가 다른 스포크와 통신하려면 트래픽이 ASA로 이동한 다음 다시 다른 스포크로 전달되어야 합니다.

다음을 확인합니다.

same-**security-traffic permit inter-interface** 명령이 없으면 packet-tracer의 출력은 동일한 보안 레벨의 서로 다른 인터페이스 사이를 통과하는 트래픽이 다음과 같이 **암시적 규칙**으로 인해 차단되었음을 나타냅니다.

```
!--- 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
```

same-**security-traffic permit intra-interface** 명령이 없으면 packet-tracer의 출력은 다음과 같이 **암시적 규칙**으로 인해 동일한 인터페이스로 들어오고 나가는 트래픽이 차단됨을 나타냅니다.

```
!--- 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
```

시나리오 6. To-The-Box 트래픽을 제어하기 위한 Ace 구성

control-plane 키워드는 ACL을 사용하여 to-the-box 트래픽을 제어할지 여부를 지정합니다. to-the-box 관리 트래픽에 대한 액세스 제어 규칙(http, ssh 또는 텔넷 같은 명령으로 정의됨)은 control-plane 옵션이 적용된 관리 액세스 규칙보다 우선 순위가 높습니다. 따라서 이렇게 허용된 관리 트래픽은 to-the-box ACL에 의해 명시적으로 거부된 경우에도 허용되어야 합니다.

일반 액세스 규칙과 달리 인터페이스에 대한 관리 규칙 집합의 끝에는 암시적 거부가 없습니다. 대신 관리 액세스 규칙과 일치하지 않는 연결은 일반 액세스 제어 규칙에 의해 평가됩니다. 또는 ICMP 규칙을 사용하여 디바이스에 대한 ICMP 트래픽을 제어할 수 있습니다.

네트워크 다이어그램

ACL은 IP 주소 10.65.63.155에서 소싱되고 ASA의 '외부' 인터페이스 IP 주소로 전달되는 to-the-box 트래픽을 차단하기 위해 control-plane 키워드로 구성됩니다.

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

다음을 확인합니다.

액세스 목록에서 적중 횟수를 확인하여 트래픽이 ACL에 의해 차단되는지 확인합니다.

```
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 메시지는 트래픽이 'ID' 인터페이스에서 삭제되었음을 나타냅니다.

```
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]
```

로깅

log **키워드**는 ACE가 네트워크 액세스를 위해 패킷에 매칭할 때 로깅 옵션을 설정합니다(access-group **명령**과 함께 적용되는 ACL). 인수 없이 **log 키워드**를 입력할 경우 시스템 로그 메시지 106100을 기본 수준(6)과 기본 간격(300초)으로 활성화합니다. log 키워드를 입력하지 않으면 거부된 패킷에 대해 기본 시스템 로그 메시지 106023이 생성됩니다. 로그 옵션은 다음과 같습니다.

- level — 0~7 사이의 심각도 레벨입니다. 기본값은 6(정보 제공)입니다. 활성 ACE에 대해 이 레벨을 변경할 경우 새 레벨이 새 연결에 적용됩니다. 기존 연결은 계속 이전 레벨에서 로깅됩니다.
- **interval** secs — syslog 메시지 간의 시간 간격(초)으로, 1부터 600까지입니다. 기본값은 300입니다. 이 값은 삭제 통계 수집에 사용된 캐시에서 비활성 흐름을 삭제하기 위한 시간 초과 값으로도 사용됩니다.
- **disable** — 모든 ACE 로깅을 비활성화합니다.
- **default** — 메시지 106023 로깅을 활성화합니다. 이 설정은 log 옵션을 포함하지 않는 것과 동일합니다.

시스템 로그 메시지 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]
```

설명:

실제 IP 패킷이 ACL에 의해 거부되었습니다. 이 메시지는 ACL에 대해 log 옵션이 활성화되지 않은 경우에도 나타납니다. IP 주소는 NAT를 통해 표시되는 값 대신 실제 IP 주소입니다. 일치하는 IP 주소가 있는 경우 IP 주소에 대해 사용자 ID 정보와 FQDN 정보가 모두 제공됩니다. 보안 방화벽 ASA는 ID 정보(domain\user) 또는 FQDN(사용자 이름을 사용할 수 없는 경우)을 기록합니다. ID 정보 또는 FQDN을 사용할 수 있는 경우 Secure Firewall ASA는 소스 및 대상 모두에 대해 이 정보를 로깅합니다.

예:

```
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]
```

시스템 로그 메시지 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
```

설명:

초기 어커런스 또는 해당 간격 동안의 총 어커런스 수가 나열됩니다. 이 메시지는 거부된 패킷만 로깅하는 메시지 106023보다 더 많은 정보를 제공하며 적중 횟수 또는 구성 가능한 레벨은 포함하지 않습니다.

access-list 라인에 *log 인*수가 있는 경우, 동기화되지 않은 패킷이 Secure Firewall ASA에 도착하고 액세스 목록에 의해 평가되므로 이 메시지 ID를 트리거할 수 있습니다. 예를 들어, 연결 테이블에 TCP 연결이 없는 보안 방화벽 ASA에서 ACK 패킷이 수신되면 보안 방화벽 ASA는 패킷이 허용되었음을 나타내는 메시지 106100을 생성할 수 있습니다. 그러나 나중에 일치하는 연결이 없기 때문에 패킷이 올바르게 삭제됩니다.

이 목록에서는 메시지 값을 설명합니다.

- 허용됨 | 거부됨 | est-allowed - 이 값은 패킷이 ACL에 의해 허용 또는 거부되었는지 여부를 지정합니다. 이 값이 set-allowed이면 패킷은 ACL에서 거부되었지만 이미 설정된 세션에 대해 허용되었습니다(예: 내부 사용자가 인터넷에 액세스할 수 있으며 일반적으로 ACL에서 거부되는 응답 패킷이 허용됨).
- protocol — TCP, UDP, ICMP 또는 IP 프로토콜 번호입니다.
- interface_name — 로깅된 플로우의 소스 또는 목적지에 대한 인터페이스 이름입니다. VLAN 인터페이스가 지원됩니다.
- source_address — 로깅된 플로우의 소스 IP 주소입니다. IP 주소는 NAT를 통해 표시되는 값 대신 실제 IP 주소입니다.
- dest_address — 로깅된 플로우의 목적지 IP 주소입니다. IP 주소는 NAT를 통해 표시되는 값 대신 실제 IP 주소입니다.
- source_port — 로깅된 흐름(TCP 또는 UDP)의 소스 포트입니다. ICMP의 경우 소스 포트 뒤의 숫자는 메시지 유형입니다.
- idfw_user — Secure Firewall ASA가 IP 주소의 사용자 이름을 찾을 수 있는 경우 기존 syslog에 추가되는 도메인 이름을 사용하는 사용자 ID 사용자 이름입니다.
- sg_info — Secure Firewall ASA가 IP 주소에 대한 보안 그룹 태그를 찾을 수 있는 경우 syslog에 추가되는 보안 그룹 태그입니다. 보안 그룹 이름이 보안 그룹 태그와 함께 표시됩니다(사용 가능한 경우).
- dest_port — 로깅된 흐름의 목적지 포트(TCP 또는 UDP)입니다. ICMP의 경우 목적지 포트 뒤의 숫자는 일부 메시지 유형에서 사용 가능한 ICMP 메시지 코드입니다. 유형 8의 경우 항상 0입니다. ICMP 메시지 유형 목록은 URL http://www.iana.org/assignments/icmp-

parameters/icmp-parameters.xml을 참조하십시오.

- hit-cnt number — 구성된 시간 간격 동안 이 ACL 항목에 의해 이 흐름이 허용되거나 거부된 횟수입니다. 보안 방화벽 ASA에서 이 흐름에 대한 첫 번째 메시지를 생성할 경우 값은 1입니다.
- first hit — 이 흐름에 대해 생성된 첫 번째 메시지입니다.
- number - second interval - 적중 횟수가 누적되는 간격입니다. interval 옵션으로 **access-list** 명령을 사용하여 이 **간격을** 설정합니다.
- 해시 코드 — 객체 그룹 ACE 및 구성 정규식 ACE에 대해 항상 2개가 인쇄됩니다. 값은 패킷이 적중하는 ACE에 따라 결정됩니다. 이러한 해시 코드를 표시하려면 show-**access list 명령을** 입력합니다.

예:

```
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]
```

문제 해결

현재 이 설정에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.