Configurar a lista de controle de acesso do ASA para vários cenários

Contents

Introduction

Este documento descreve como configurar uma lista de controle de acesso (ACL) no Adaptive Security Appliance (ASA) para vários cenários.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do ASA.

Componentes Utilizados

As informações neste documento são baseadas em um software ASA versão 8.3 e posterior.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

As ACLs são usadas pelo ASA para determinar se o tráfego é permitido ou negado. Por padrão, o tráfego que passa de uma interface de nível de segurança **inferior** para uma interface de nível de segurança **superior** é negado, enquanto o tráfego de uma interface de nível de segurança **superior** para uma interface de nível de segurança **inferior** é permitido. Esse comportamento também pode ser cancelado com uma ACL.

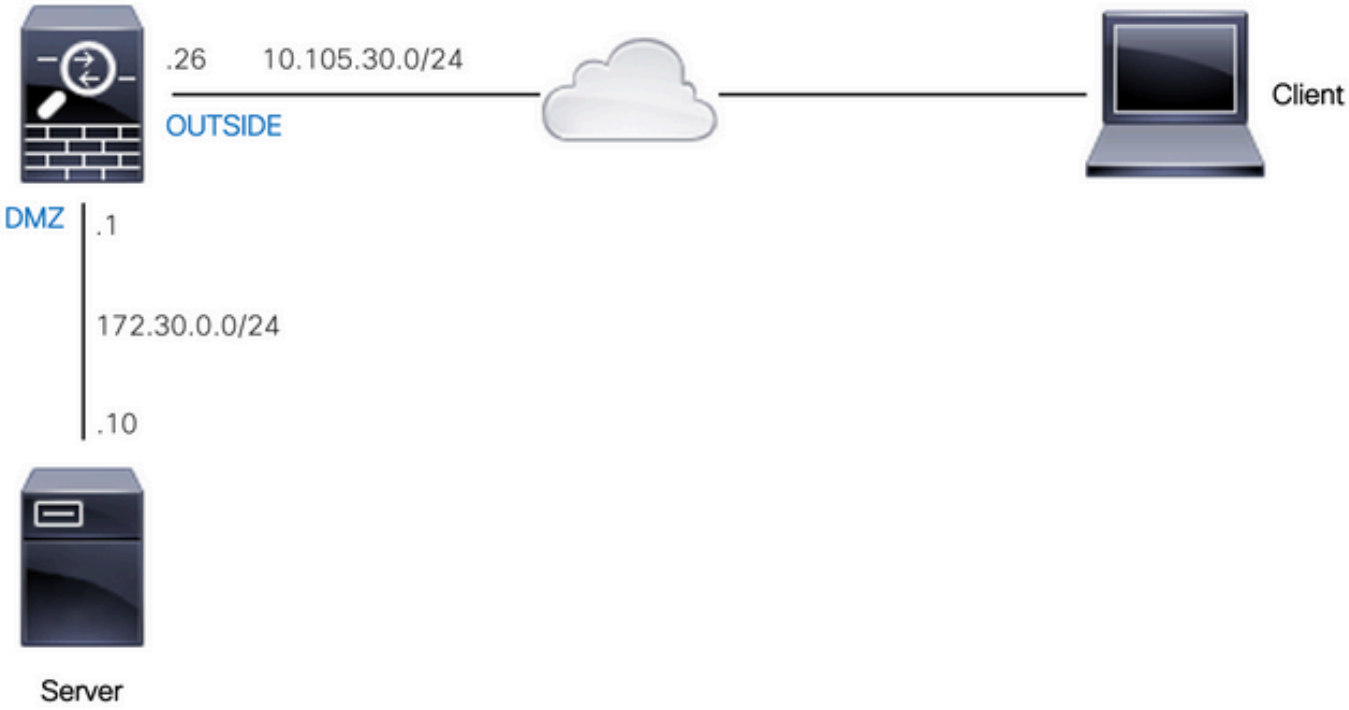
Na presença de regras de NAT, em versões anteriores do ASA (8.2 e anteriores), o ASA verifica a ACL antes de cancelar a conversão do pacote com base na regra de NAT que foi correspondida. Na versão 8.3 e posterior, o ASA desconverte o pacote antes de verificar as ACLs. Isso significa que para um ASA versão 8.3 e posterior, o tráfego é permitido ou negado com base no endereço IP real do host em vez do endereço IP convertido. As ACLs são compostas de uma ou mais entradas de controle de acesso (ACEs).

Configurar

Cenário 1. Configure uma Ace para permitir acesso a um servidor Web localizado atrás da DMZ

O cliente na Internet, localizado atrás da interface externa, deseja acessar um servidor web hospedado atrás da interface DMZ que ouve as portas TCP 80 e 443.

Diagrama de Rede



O endereço IP real do servidor Web é 172.30.0.10. Uma regra estática de NAT um para um é configurada para permitir que os usuários da Internet acessem o servidor da Web com um endereço IP 10.105.130.27 convertido. O ASA executa proxy-arp para 10.105.130.27 na interface 'externa' por padrão quando uma regra de NAT estático é configurada com um endereço IP convertido que esteja na mesma sub-rede do endereço IP da interface 'externa' 10.105.130.26:

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

Configure essa ACE para permitir que qualquer endereço IP de origem na Internet se conecte ao servidor Web somente nas portas TCP 80 e 443. Atribua a ACL à interface externa na direção de entrada:

```
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
```

Verificar

Execute um comando packet-tracer com esses campos. Interface de entrada na qual rastrear o pacote: externo

Protocolo: TCP

Endereço IP origem: qualquer endereço IP na Internet

Porta IP origem: qualquer porta efêmera

Endereço IP destino: endereço IP traduzido do servidor web (10.105.130.27)

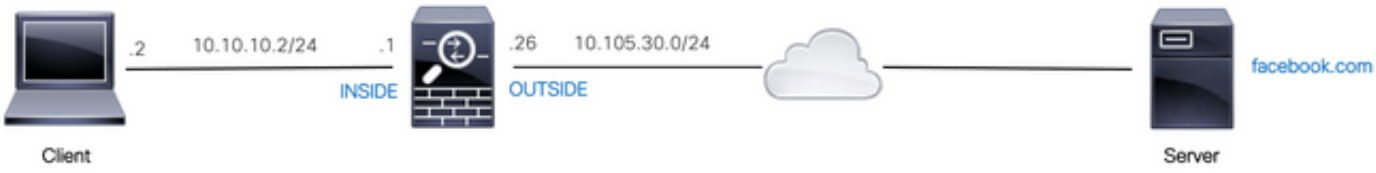
Porta de destino: 80 ou 443

```
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
```

Cenário 2. Configurar uma Ace para Permitir Acesso a um Servidor Web com um FQDN

O cliente com endereço IP 10.10.10.2 localizado na rede local (LAN) tem permissão para acessar facebook.com.

Diagrama de Rede



Verifique se o servidor DNS está configurado corretamente no 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
```

Configure esse objeto de rede, o objeto FQDN e a ACE para permitir que o cliente com o endereço IP 10.10.10.2 acesse 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
```

Verificar

A saída de **show dns** mostra o endereço IP resolvido para o FQDN facebook.com:

```
ciscoasa# show dns

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

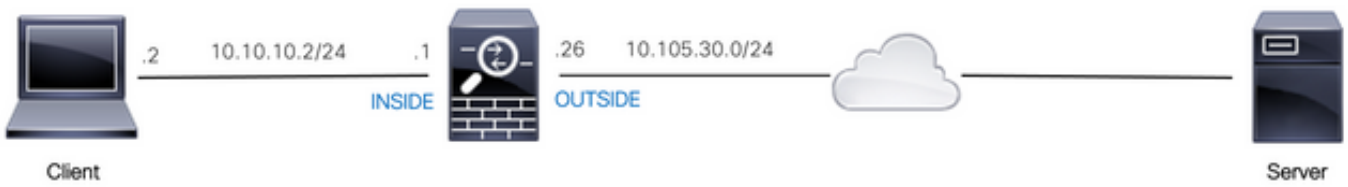
A lista de acesso mostra o objeto FQDN como **resolvido** e também mostra o endereço IP resolvido:

```
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
```

Cenário 3. Configurar um Ace para Permitir Acesso a um Site Somente por um Período Específico em um Dia

O cliente localizado na LAN tem permissão para acessar um site com o endereço IP 10.0.20.20 diariamente das 12 às 14 h IST apenas.

Diagrama de Rede



Verifique se o fuso horário está configurado corretamente no ASA:

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

Configure um objeto de intervalo de tempo para a duração de tempo necessária:

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

Configure esses objetos de rede e ACE para permitir que qualquer endereço IP de origem localizado na LAN acesse o site somente durante o período mencionado no objeto de intervalo de tempo chamado **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
```

Verificar

O objeto de intervalo de tempo está **ativo** quando o relógio no ASA indica um tempo que está dentro do objeto de intervalo de 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
```

O objeto de intervalo de tempo e a ACE ficam **inativos** quando o relógio no ASA indica um tempo que está fora do objeto de intervalo de tempo:

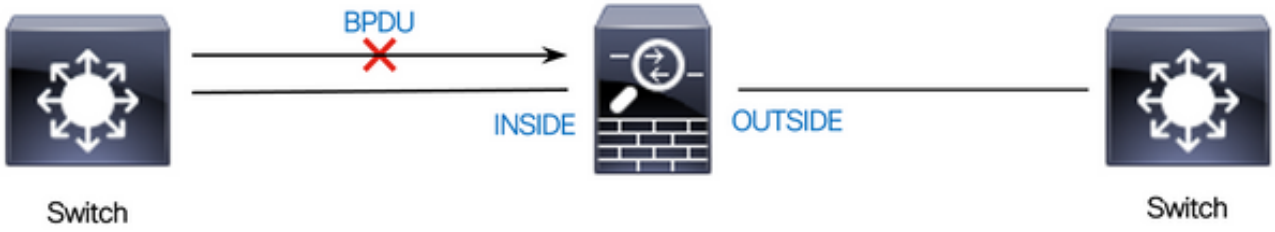
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


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
```

Cenário 4. Configurar uma Ace para bloquear unidades de dados de protocolo de ponte (Bpdu) através de um ASA no modo transparente

Para evitar loops com o Spanning Tree Protocol (STP), os BPDUs são passados através do ASA no modo transparente por padrão. Para bloquear BPDUs, você precisa configurar uma regra EtherType para negá-los.

Diagrama de Rede



Configure a ACL EtherType para bloquear a passagem de BPDUs através da interface 'interna' do ASA na direção de entrada como mostrado aqui:

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

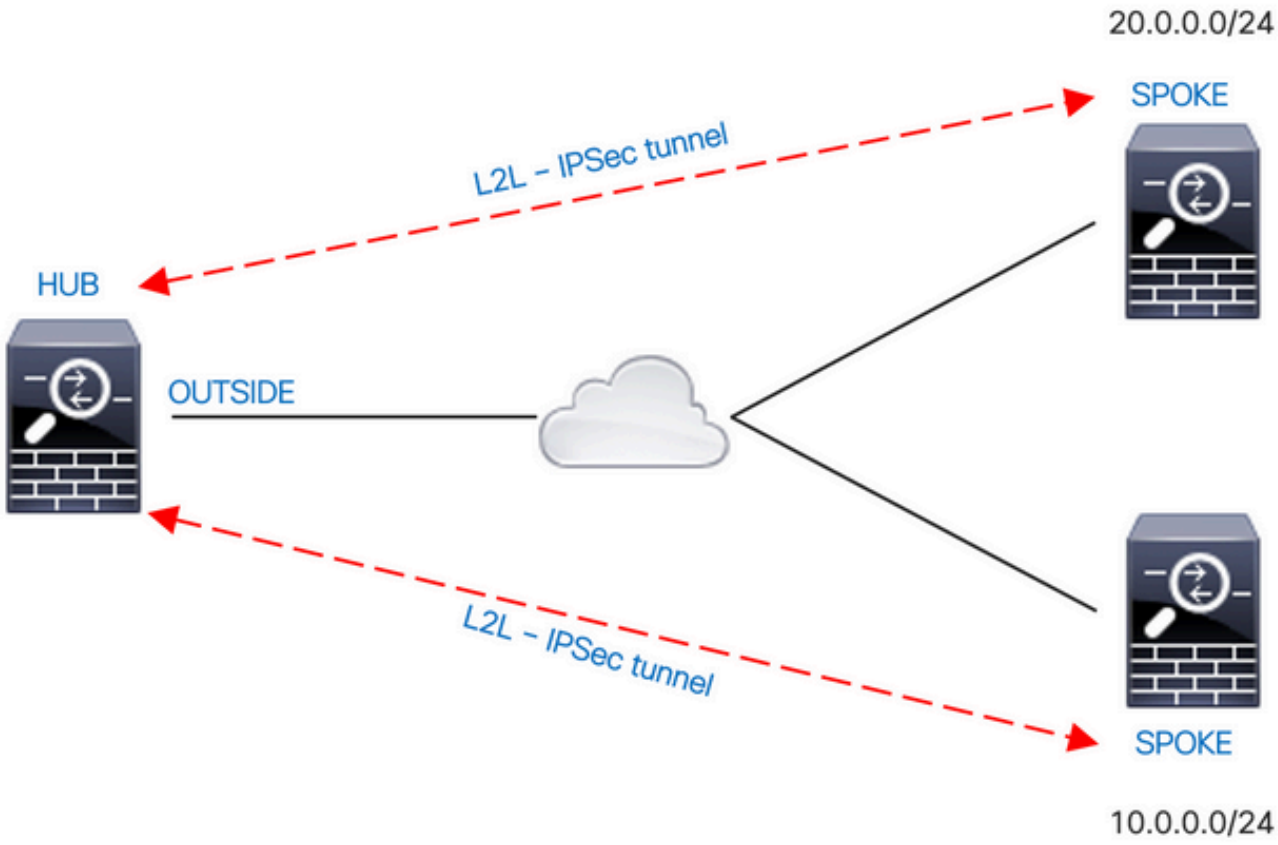
Verificar

Verifique a contagem de ocorrências na lista de acesso para verificar se as BPDUs estão bloqueadas pelo 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)
```

Cenário 5. Permitir que o tráfego passe entre interfaces com o mesmo nível de segurança

Diagrama de Rede



Por padrão, o tráfego que passa entre interfaces do mesmo nível de segurança é bloqueado. Para permitir a comunicação entre interfaces com níveis de segurança iguais, ou para permitir que o tráfego entre e saia da mesma interface (hairpin/u-turn), use o comando **same-security-traffic** no modo de configuração global.

Esse comando mostra como permitir a comunicação entre diferentes interfaces que têm o mesmo nível de segurança:

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

Este exemplo mostra como permitir a comunicação dentro e fora da mesma interface:

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

Esta característica é útil para o tráfego VPN que incorpora uma relação mas é então roteado fora dessa mesma relação. Por exemplo, se você tiver uma rede VPN hub-and-spoke em que esse ASA é o hub e as redes VPN remotas são spokes, para que um spoke se comunique com outro spoke, o tráfego deve ir para o ASA e, em seguida, sair novamente para o outro spoke.

Verificar

Sem o comando **same-security-traffic permit inter-interface**, a saída do packet-tracer indica que o tráfego que passa entre interfaces diferentes do mesmo nível de segurança está bloqueado devido a uma **regra implícita**, como mostrado aqui:

```
!--- 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
```

Sem o comando **same-security-traffic permit intrainterface**, a saída do packet-tracer indica que o tráfego que entra e sai da mesma interface está bloqueado devido a uma **regra implícita**, como mostrado aqui:

```
!--- 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
```

Cenário 6. Configurar um Ace para controlar o tráfego pronto para usar

A palavra-chave **control-plane** especifica se a ACL é usada para controlar o tráfego pronto para usar. As regras de controle de acesso para o tráfego de gerenciamento pronto para uso (definido por comandos como **http**, **ssh** ou **telnet**) têm precedência mais alta do que uma regra de acesso de gerenciamento aplicada com a opção **control-plane**. Portanto, esse tráfego de gerenciamento permitido deve ter permissão para entrar, mesmo que seja explicitamente negado pela ACL de acesso à caixa.

Diferentemente das regras de acesso regular, não há negação implícita no final de um conjunto de regras de gerenciamento para uma interface. Em vez disso, qualquer conexão que não corresponda a uma regra de acesso de gerenciamento é avaliada por regras de controle de acesso regulares. Como alternativa, você pode usar regras ICMP para controlar o tráfego ICMP para o dispositivo.

Diagrama de Rede

Uma ACL é configurada com a palavra-chave **control-plane** para bloquear o tráfego pronto originado do endereço IP 10.65.63.155 e destinado ao endereço IP da interface 'externa' do 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
```

Verificar

Verifique a contagem de ocorrências na lista de acesso para verificar se o tráfego está bloqueado pela 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
```

As mensagens de syslog indicam que o tráfego é descartado na interface de 'identidade':

```
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]
```

Registro

A palavra-chave **log** define opções de registro quando uma ACE corresponde a um pacote para acesso à rede (uma ACL aplicada com o comando **access-group**). Se você inserir a palavra-chave **log** sem nenhum argumento, você ativará a 106100 de mensagem de log do sistema no nível padrão (6) e para o intervalo padrão (300 segundos). Se você não digitar a palavra-chave log, a mensagem de log padrão do sistema 106023 será gerada para os pacotes negados. As opções de log são:

- level — Um nível de gravidade entre 0 e 7. O padrão é 6 (informativo). Se você alterar esse nível para uma ACE ativa, o novo nível será aplicado a novas conexões; as conexões existentes continuarão a ser registradas no nível anterior.
- **interval** secs — O intervalo de tempo em segundos entre mensagens de syslog, de 1 a 600. O padrão é 300. Esse valor também é usado como o valor de tempo limite para excluir um fluxo inativo do cache usado para coletar estatísticas de descarte.
- **disable** — Desabilita todos os logs ACE.
- **default** — Ativa o registro no 106023 de mensagens. Essa configuração é a mesma que não incluir a opção log.

Mensagem de 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]
```

Explicação:

Um pacote IP real foi negado pela ACL. Essa mensagem será exibida mesmo se você não tiver a opção de log ativada para uma ACL. O endereço IP é o endereço IP real, em vez dos valores exibidos através do NAT. As informações de identidade do usuário e as informações de FQDN são fornecidas para os endereços IP se um correspondente for encontrado. O Secure Firewall ASA registra informações de identidade (domínio\usuário) ou FQDN (se o nome de usuário não estiver disponível). Se as informações de identidade ou o FQDN estiverem disponíveis, o Secure Firewall ASA registrará essas informações para a origem e para o destino.

Exemplo:

```
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]
```

Mensagem de 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

Explicação:

A ocorrência inicial ou o número total de ocorrências durante um intervalo são listados. Essa mensagem fornece mais informações do que a mensagem 106023, que registra apenas os pacotes negados e não inclui a contagem de ocorrências ou um nível configurável.

Quando uma linha de lista de acesso tiver o argumento *log*, espera-se que essa ID de mensagem possa ser disparada porque um pacote não sincronizado chega ao ASA do Firewall Seguro e é avaliado pela lista de acesso. Por exemplo, se um pacote ACK for recebido no ASA do Firewall Seguro (para o qual não existe conexão TCP na tabela de conexão), o ASA do Firewall Seguro pode gerar 106100 de mensagem, indicando que o pacote foi permitido; no entanto, o pacote será descartado corretamente mais tarde, porque não há conexão correspondente.

A lista descreve os valores da mensagem:

- permitido | negado | est-allowed— Esses valores especificam se o pacote foi permitido ou negado pela ACL. Se o valor for definido como permitido, o pacote foi negado pela ACL, mas foi permitido para uma sessão já estabelecida (por exemplo, um usuário interno tem permissão para acessar a Internet e os pacotes de resposta que normalmente seriam negados pela ACL são aceitos).
- protocol — TCP, UDP, ICMP ou um número de protocolo IP.
- interface_name — O nome da interface para a origem ou o destino do fluxo registrado. As interfaces VLAN são suportadas.
- source_address — O endereço IP de origem do fluxo registrado. O endereço IP é o endereço IP real, em vez dos valores exibidos através do NAT.
- dest_address — O endereço IP destino do fluxo registrado. O endereço IP é o endereço IP real, em vez dos valores exibidos através do NAT.
- source_port — A porta de origem do fluxo registrado (TCP ou UDP). Para o ICMP, o número após a porta de origem é o tipo de mensagem.
- idfw_user — O nome de usuário da identidade do usuário, com o nome de domínio que é adicionado ao syslog existente quando o Secure Firewall ASA pode encontrar o nome de usuário para o endereço IP.
- sg_info — A tag de grupo de segurança que é adicionada ao syslog quando o Secure Firewall ASA pode encontrar uma tag de grupo de segurança para o endereço IP. O nome do grupo de segurança é exibido com a marca do grupo de segurança, se disponível.
- dest_port — A porta de destino do fluxo registrado (TCP ou UDP). Para o ICMP, o número após a porta de destino é o código de mensagem ICMP, que está disponível para alguns tipos de mensagem. Para o tipo 8, é sempre 0. Para obter uma lista de tipos de mensagem ICMP, consulte o URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- hit-cnt number — O número de vezes que esse fluxo foi permitido ou negado por essa entrada de ACL no intervalo de tempo configurado. O valor é 1 quando o Secure Firewall ASA gera a primeira mensagem para esse fluxo.

- primeiro acerto — A primeira mensagem gerada para esse fluxo.
- número - segundo intervalo — O intervalo no qual a contagem de ocorrências é acumulada. Defina esse intervalo com o comando **access-list** com a opção **interval**.
- Códigos hash — Dois são sempre impressos para o grupo de objetos ACE e o ACE regular constituinte. Os valores são determinados em qual ACE o pacote atingiu. Para exibir esses códigos de hash, insira o comando **show-access list**.

Exemplo:

```
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]
```

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.