さまざまなシナリオ用のASAアクセスコントロールリストの設定

内容

概要

このドキュメントでは、さまざまなシナリオに合わせて適応型セキュリティアプライアンス(ASA)でアクセスコントロールリスト(ACL)を設定する方法について説明します。

前提条件

要件

ASAに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、ASAソフトウェアバージョン8.3以降に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

ACLは、トラフィックが許可されるか拒否されるかを決定するためにASAによって使用されます。デフォルトでは、**低い**セキュリティレベルのインターフェイスから**高い**セキュリティレベルのインターフェイスに渡されるトラフィックは拒否されますが、**高い**セキュリティレベルのインターフェイスから**低い**セキュリティレベルのインターフェイスへのトラフィックは許可されます。この動作も ACL で上書きできます。

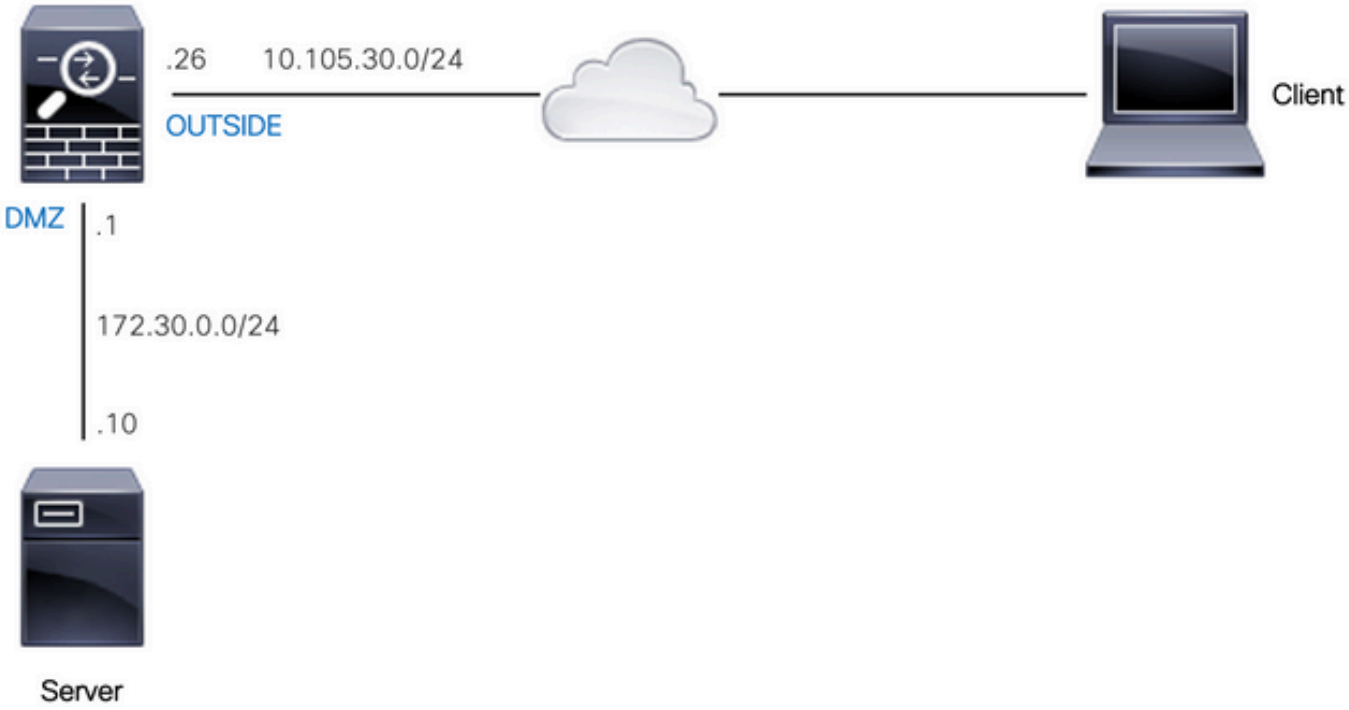
NATルールが存在する場合、ASAの以前のバージョン（8.2以前）では、ASAは、一致したNATルールに基づいてパケットを変換し直す前にACLをチェックします。バージョン8.3以降では、ASAはACLをチェックする前にパケットを逆変換します。つまり、ASAバージョン8.3以降では、変換されたIPアドレスではなく、ホストの実際のIPアドレスに基づいてトラフィックが許可または拒否されます。ACLは、1つ以上のアクセスコントロールエントリ(ACE)で構成されます。

設定

シナリオ 1.DMZの背後にあるWebサーバへのアクセスを許可するためのAceの設定

外部インターフェイスの背後にあるインターネット上のクライアントが、TCPポート80および443をリッスンするDMZインターフェイスの背後にホストされているWebサーバにアクセスしようとしています。

ネットワーク図



Webサーバの実際のIPアドレスは172.30.0.10です。スタティックな1対1のNATルールは、変換されたIPアドレス10.105.130.27を使用してインターネットユーザがWebサーバにアクセスできるように設定されています。スタティックNATルールが、「outside」インターフェイスIPアドレス10.105.130.26と同じサブネットにある変換IPアドレスを使用して設定されている場合、ASAはデフォルトで「outside」インターフェイスで10.105.130.27のproxy-arpを実行します。

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

インターネット上の任意の送信元IPアドレスがTCPポート80および443上でのみWebサーバに接続できるように、このACEを設定します。インバウンド方向でACLを外部インターフェイスに割り当てます。

```
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
```

確認

次のフィールドでpacket-tracerコマンドを実行します。 パケットをトレースする入力インターフェイス:outside

プロトコル：TCP

送信元IPアドレス：インターネット上の任意のIPアドレス

送信元IPポート：任意の一時的なポート

宛先IPアドレス：Webサーバの変換されたIPアドレス(10.105.130.27)

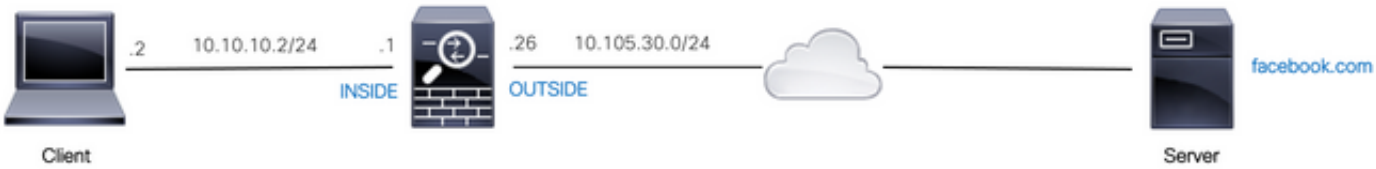
宛先ポート：80または443

```
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
```

シナリオ 2.FQDNを使用してWebサーバへのアクセスを許可するためのAceの設定

ローカルエリアネットワーク(LAN)にあるIPアドレス10.10.10.2のクライアントは、facebook.comへのアクセスを許可されます。

ネットワーク図



DNSサーバがASAで正しく設定されていることを確認します。

```
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アドレス10.10.10.2のクライアントがfacebook.comにアクセスできるように、このネットワークオブジェクト、FQDNオブジェクト、およびACEを設定します。

```
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
```

確認

show dnsの出力には、FQDN facebook.comの解決されたIPアドレスが表示されます。

```
ciscoasa# show dns

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

アクセスリストは、FQDNオブジェクトを**解決済み**として示し、解決済みのIPアドレスも示します。

```
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
```

シナリオ 3.1日の特定の期間だけWebサイトへのアクセスを許可するようにAceを設定する

LANにあるクライアントは、IPアドレス10.0.20.20のWebサイトに毎日12 PM ~ 2 PM ISTの間のみアクセスできます。

ネットワーク図

ASAでタイムゾーンが正しく設定されていることを確認します。

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

必要な期間の時間範囲オブジェクトを設定します。

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

次のネットワークオブジェクトとACEを設定して、LAN内にある任意の送信元IPアドレスが、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
```

確認

時間範囲オブジェクトは、ASAのクロックが時間範囲オブジェクト内の時間を示す場合に**アクティブ**になります。

```
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
```

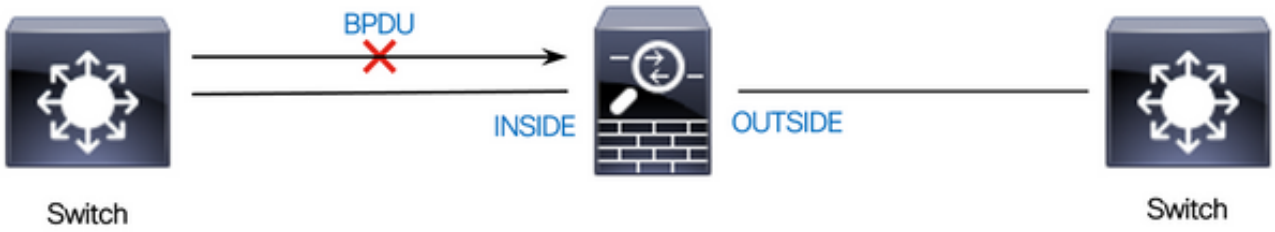
ASAのクロックが時間範囲オブジェクト外の時間を示している場合、ACEと同様に時間範囲オブジェクトも**非アクティブ**になります。

```
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
```

シナリオ 4.トランスペアレントモードでASAを介してBridge Protocol Data Unit (Bpdu ; ブリッジプロトコルデータユニット) をブロックするようにAceを設定する

スパニングツリープロトコル(STP)によるループを防ぐために、BPDUはデフォルトでトランスペアレントモードでASAを通過します。BPDUをブロックするには、BPDUを拒否するようにEtherTypeルールを設定する必要があります。

ネットワーク図



次に示すように、BPDUがASAの「内部」インターフェイスをインバウンド方向に通過しないようにEtherType ACLを設定します。

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

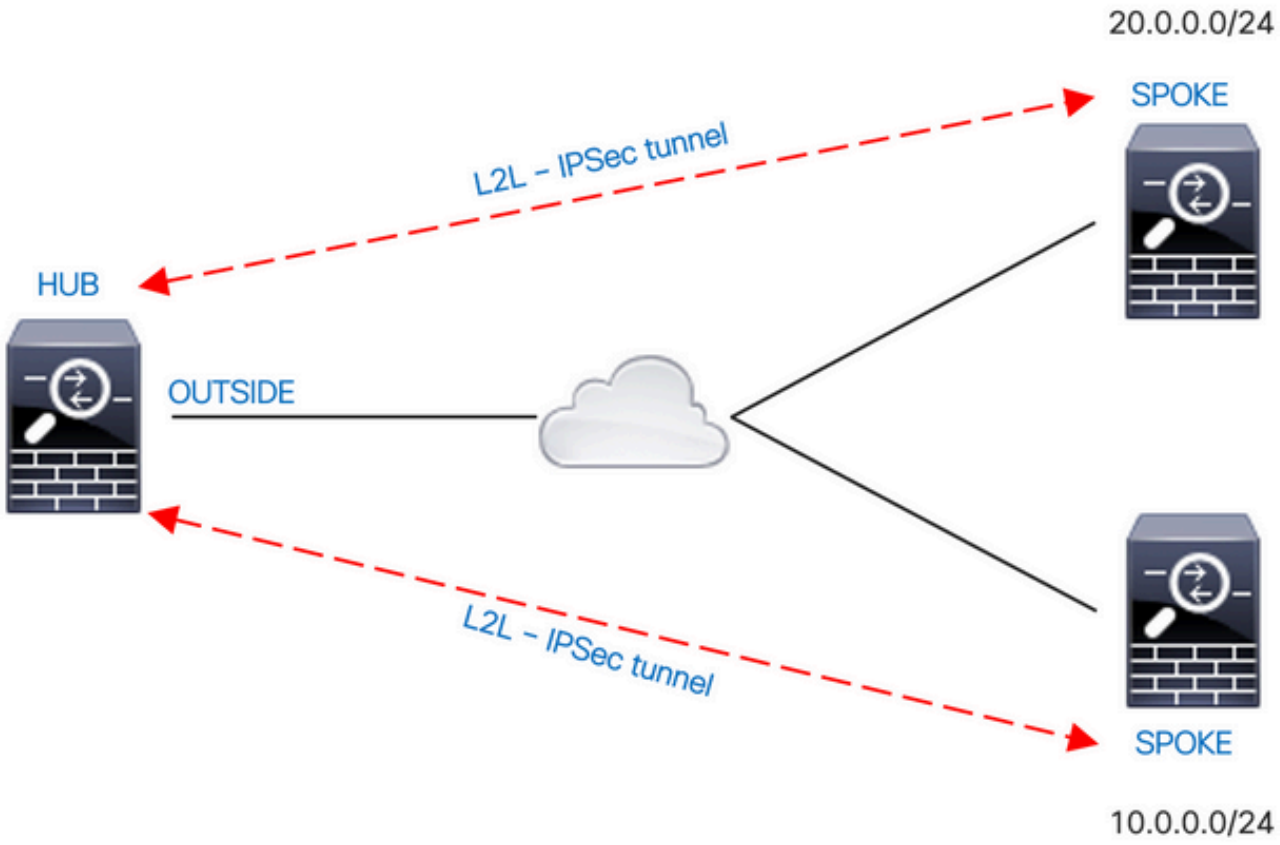
確認

アクセスリストのヒットカウントをチェックして、BPDUがASAによってブロックされていることを確認します。

```
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)
```

シナリオ 5.同じセキュリティレベルのインターフェイス間でのトラフィックの通過を許可する

ネットワーク図



デフォルトでは、同じセキュリティレベルのインターフェイス間を通過するトラフィックはブロックされます。セキュリティレベルが等しいインターフェイス間の通信を許可するか、トラフィックが同じインターフェイスに出入りできるようにするには（ヘアピン/Uターン）、グローバルコンフィギュレーションモードで**same-security-traffic**コマンドを使用します。

次のコマンドは、同じセキュリティレベルを持つ異なるインターフェイス間の通信を許可する方法を示しています。

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

次の例は、同じインターフェイスで送受信される通信を許可する方法を示しています。

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

この機能は、あるインターフェイスに着信した後に同じインターフェイスからルーティングされる VPN トラフィックに対して便利な機能です。たとえば、このASAがハブで、リモートVPNネットワークがスポークであるハブアンドスポークVPNネットワークがある場合、あるスポークが別のスポークと通信するためには、トラフィックがASAに送信された後、別のスポークに再び送信される必要があります。

確認

same-security-traffic permit inter-interfaceコマンドを使用しない場合、パケットトレーサの出力には、同じセキュリティレベルの異なるインターフェイス間を通過するトラフィックが、次に示すように**暗黙のルール**によってブロックされていることが示されます。

```
!--- 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コマンドがない場合、パケットトレーサの出力には、次に示すように、同じインターフェイスに出入りするトラフィックが**暗黙のルール**によってブロックされていることが示されます。

```
!--- 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
```

シナリオ 6.To-The-Boxトラフィックを制御するためのAceの設定

control-planeキーワードは、To-the-Boxトラフィックの制御にACLを使用するかどうかを指定します。to-the-box管理トラフィック(http、ssh、またはtelnetなどのコマンドで定義)のアクセスコントロールルールは、control-planeオプションで適用される管理アクセスルールよりも優先されます。したがって、このような許可された管理トラフィックは、to-the-box ACLによって明示的に拒否された場合でも、着信を許可する必要があります。

通常のアクセスルールとは異なり、インターフェイスの一連の管理ルールの最後には暗黙のdenyは存在しません。その代わり、管理アクセスルールに一致しない接続は、通常のアクセスコントロールルールによって評価されます。または、ICMPルールを使用して、デバイスへのICMPトラフィックを制御できます。

ネットワーク図

IPアドレス10.65.63.155を送信元とし、ASAの「外部」インターフェイスIPアドレスを宛先とするto-the-boxトラフィックをブロックするように、control-planeキーワードを使用してACLを設定します。

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

確認

アクセスリストのヒットカウントをチェックして、トラフィックがACLによってブロックされていることを確認します。

```
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メッセージは、トラフィックが「identity」インターフェイスでドロップされたことを示します。

```
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]
```

Logging

logキーワードは、ACEがネットワークアクセスのパケット(access-groupコマンドで適用されるACL)と一致する場合に、ロギングオプションを設定します。引数を指定せずにlogキーワードを入力すると、デフォルトのレベル(6)とデフォルトの間隔（300秒）でシステムログメッセージ106100が有効になります。logキーワードを入力しないと、拒否されたパケットに対してデフォルトのシステムログメッセージ106023が生成されます。ログオプションは次のとおりです。

- level:0 ~ 7の重大度レベル。デフォルトは6(informational)です。アクティブなACEに対してこのレベルを変更すると、新しいレベルが新しい接続に適用されます。既存の接続は引き続き前のレベルでログに記録されます。
- interval secs:syslogメッセージ間の秒単位の時間間隔(1 ~ 600)。デフォルト値は 300 です。この値は、ドロップ統計情報の収集に使用されるキャッシュから非アクティブフローを削除するためのタイムアウト値としても使用されます。
- disable：すべてのACEロギングを無効にします。
- default：メッセージ106023へのロギングを有効にします。この設定は、logオプションを含めないのと同じです。

syslog メッセージ 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]
```

説明：

実際のIPパケットがACLによって拒否されました。このメッセージは、ACLのログオプションが有効になっていない場合でも表示されます。IPアドレスは、NATで表示される値ではなく、実際のIPアドレスです。一致するIPアドレスが見つかった場合、ユーザID情報とFQDN情報の両方がIPアドレスに提供されます。セキュアファイアウォールASAは、ID情報（ドメイン\ユーザ）またはFQDN（ユーザ名が使用できない場合）をログに記録します。ID情報またはFQDNが使用可能な場合、セキュアファイアウォールASAは送信元と宛先の両方についてこの情報をログに記録します。

例：

```
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 メッセージ 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

説明：

そのインターバルの間の最初のオカレンスまたはオカレンスの合計数が表示されます。このメッセージは、拒否されたパケットだけをログに記録し、ヒットカウントや設定可能なレベルを含まないメッセージ106023よりも多くの情報を提供します。

アクセスリスト行に*log*引数がある場合、同期されていないパケットがセキュアファイアウォールASAに到着し、アクセスリストによって評価されるため、このメッセージIDがトリガーされることが予想されます。たとえば、セキュアファイアウォールASAでACKパケットを受信した場合（接続テーブルにTCP接続が存在しない場合）、セキュアファイアウォールASAはパケットが許可されたことを示すメッセージ106100を生成できます。ただし、一致する接続がないため、パケットは後で正しくドロップされます。

次のリストに、メッセージの値を示します。

- 許可された | denied | est-allowed：これらの値は、パケットがACLによって許可されたか拒否されたかを指定します。値がest-allowedの場合、パケットはACLによって拒否されましたが、すでに確立されたセッションに対しては許可されていました（たとえば、内部ユーザがインターネットへのアクセスを許可され、通常はACLによって拒否される応答パケットが受け入れられました）。
- protocol:TCP、UDP、ICMP、またはIPプロトコル番号。
- interface_name：ログに記録されたフローの送信元または宛先のインターフェイス名。VLANインターフェイスがサポートされています。
- source_address：ログに記録されたフローの送信元IPアドレス。IPアドレスは、NATで表示される値ではなく、実際のIPアドレスです。
- dest_address：ログに記録されたフローの宛先IPアドレス。IPアドレスは、NATで表示される値ではなく、実際のIPアドレスです。
- source_port：ログに記録されたフローの送信元ポート（TCPまたはUDP）。ICMPの場合、送信元ポートの後の番号はメッセージタイプです。
- idfw_user：ユーザIDのユーザ名。このユーザ名は、Secure Firewall ASAがIPアドレスのユーザ名を見つけたときに既存のsyslogに追加されるドメイン名と一緒です。
- sg_info:Secure Firewall ASAがIPアドレスのセキュリティグループタグを検出できる場合にsyslogに追加されるセキュリティグループタグ。セキュリティグループ名とセキュリティグループタグが表示されます（使用可能な場合）。
- dest_port：ログに記録されたフローの宛先ポート（TCPまたはUDP）。ICMPの場合、宛先ポートの後の番号はICMPメッセージコードです。これは一部のメッセージタイプで使用できます。タイプ8の場合は常に0です。ICMPメッセージタイプのリストについては、URL http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xmlを参照してください。
- hit-cnt number：設定された期間内にこのACLエントリによってこのフローが許可または拒否された回数。セキュアファイアウォールASAがこのフローの最初のメッセージを生成する場合、値は1です。
- first hit：このフローに対して生成された最初のメッセージ。

- number - second interval：ヒットカウントが累積される間隔。この間隔は、**interval**オプションを指定した**access-list**コマンドで設定します。
- ハッシュコード：オブジェクトグループACEと構成規則型ACEに対して、常に2つが出力されます。値は、パケットがヒットしたACEに基づいて決定されます。これらのハッシュコードを表示するには、**show-access list**コマンドを入力します。

例：

```
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]
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。