تكوين قائمة التحكم في الوصول إلى ASA لسيناريوهات مختلفة

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين قائمة التحكم في الوصول (ACL) على جهاز الأمان القابل للتكيف (ASA) لمختلف السيناريوهات.

المتطلبات الأساسية

المتطلبات

cisco يوصي أنت تلقى أنت معرفة من ASA.

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى برنامج ASA الإصدار 8.3 والإصدارات الأحدث.

تم إنشاء المعلومات الواردة في هذه المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذه المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يتم إستخدام قوائم التحكم في الوصول (ACL) من قبل ASA لتحديد ما إذا كان يتم السماح بحركة المرور أو رفضها. بشكل افتراضي، يتم رفض حركة المرور التي تنتقل من واجهة **أقل** مستوى الأمان إلى واجهة **مستوى** الأمان **الأعلى** في حين يتم السماح بحركة المرور من واجهة مستوى الأمان إلى واجهة مستوى الأمان **الأقل** مستوى الأمان **الأعلى**. يمكن أيضا تجاوز هذا السلوك باستخدام قائمة التحكم في الوصول (ACL).

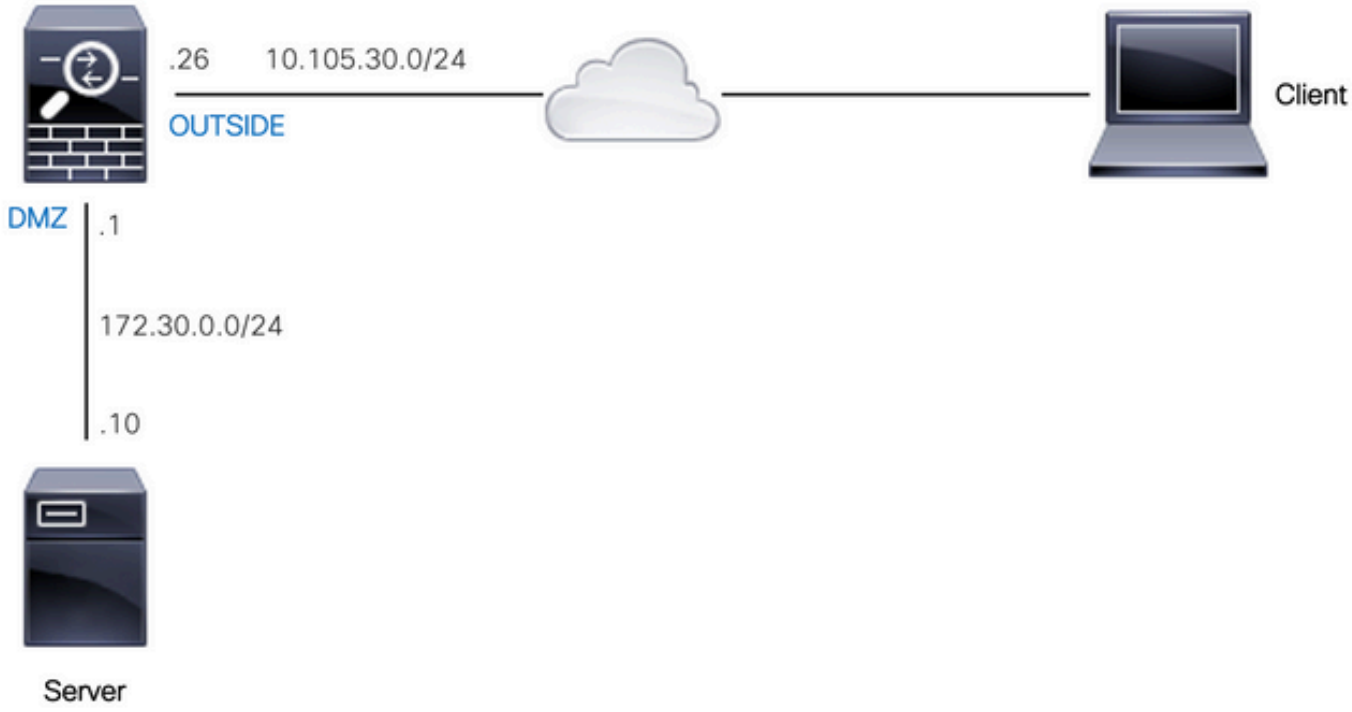
في وجود قواعد NAT، في الإصدارات السابقة من ASA (8.2 والإصدارات الأقدم)، يتحقق ASA من قائمة التحكم في الوصول (ACL) قبل إلغاء ترجمة الحزمة استنادا إلى قاعدة NAT التي تم مطابقتها. في الإصدار 8.3 والإصدارات الأحدث، الموقع ASA بترجمة الحزمة قبل التحقق من قوائم التحكم في الوصول (ACLs). هذا يعني أنه بالنسبة لإصدار ASA 8.3 والإصدارات الأحدث، يتم السماح بحركة المرور أو رفضها استنادا إلى عنوان IP الحقيقي للمضيف بدلا من عنوان IP المترجم. تتكون قوائم التحكم في الوصول من إدخال أو أكثر من إدخالات التحكم في الوصول (ACEs).

التكوين

السيناريو 1. تكوين ACE للسماح بالوصول إلى خادم ويب موجود خلف DMZ

يريد العميل على الإنترنت، الموجود خلف الواجهة الخارجية الوصول إلى خادم ويب مستضاف خلف واجهة DMZ أثناء الاستماع إلى منافذ TCP 80 و 443.

الرسم التخطيطي للشبكة



عنوان IP الحقيقي لخادم الويب هو 172.30.0.10. شكلت ساكن إستاتيكي واحد إلى واحد nat قاعدة أن يسمح مستعمل إنترنت أن ينفذ ال web ناد ل مع ترجمة عنوان 10.105.130.27. يزج nat إستاتيكي ساكن عندما افتراضي 10.105.130.27 على القارن 'خارجي' ل ASA وكيل-arp قاعدة يكون شكلت مع ترجمة عنوان أن يقع في ال نفس subnet بما أن القارن 'خارجي' عنوان 10.105.130.26:

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

قم بتكوين ACE هذا للسماح لأي عنوان IP للمصدر على الإنترنت بالاتصال بخادم الويب الخاص بك على منفذ TCP 80 و 443. تعيين قائمة التحكم في الوصول (ACL) إلى الواجهة الخارجية في الإتجاه الوارد:

```
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
```

التحقق من الصحة

قم بتشغيل أمر packet-tracer مع هذه الحقول. واجهة الدخول التي تريد تتبع الحزمة عليها: خارج

البروتوكول: TCP

عنوان IP المصدر: أي عنوان IP على الإنترنت

منفذ IP المصدر: أي منفذ مؤقت

عنوان IP للوجهة: عنوان IP المترجم لخادم الويب (10.105.130.27)

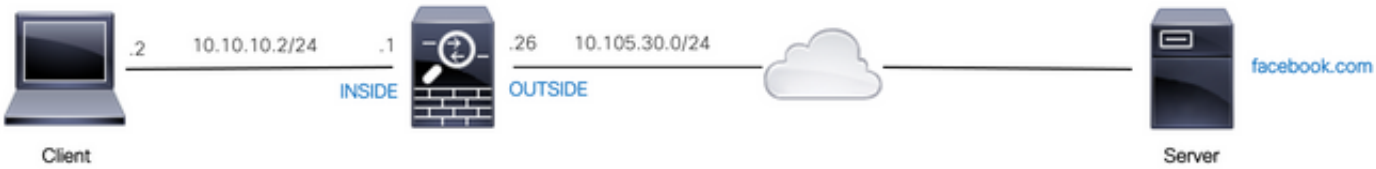
غاية ميناء: 80 أو 443

```
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
```

السيناريو 2. تكوين ACE للسماح بالوصول إلى خادم ويب باستخدام FQDN

يسمح للعميل الذي له عنوان IP 10.10.10.2 الموجود في شبكة المنطقة المحلية (LAN) بالوصول إلى facebook.com.

الرسم التخطيطي للشبكة



تأكد من تكوين خادم DNS بشكل صحيح على 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
```

قم بتكوين كائن الشبكة هذا وكائن FQDN و ACE للسماح للعميل بعنوان IP 10.10.10.2 بالوصول إلى 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
```

التحقق من الصحة

يعرض إخراج **عرض dns** عنوان IP الذي تم تحليله ل FQDN facebook.com:

```
ciscoasa# show dns

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

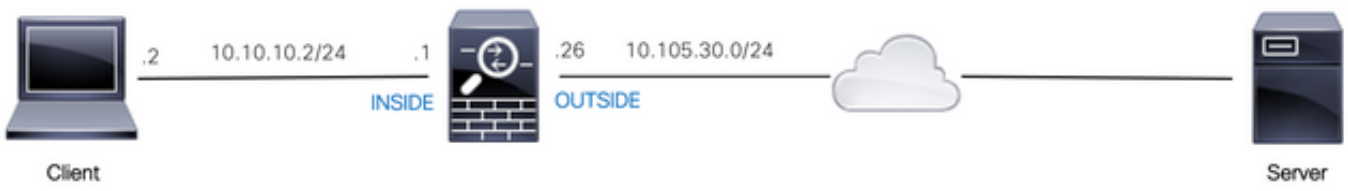
تظهر قائمة الوصول كائن FQDN كما **تم حله** كما تعرض عنوان IP الذي تم تحليله:

```
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
```

السيناريو 3. تكوين ACE للسماح بالوصول إلى موقع ويب فقط لفترة زمنية محددة في اليوم

يسمح للعميل الموجود في الشبكة المحلية بالوصول إلى موقع ويب بعنوان IP 10.0.20.20 فقط IST من 12 مساء إلى 2 مساء يوميا.

الرسم التخطيطي للشبكة



تأكد من تكوين المنطقة الزمنية بشكل صحيح على ASA:

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

تكوين كائن نطاق زمني للمدة الزمنية المطلوبة:

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

قم بتكوين كائنات الشبكة هذه و ACE للسماح لأي عنوان IP للمصدر الموجود في شبكة LAN للوصول إلى موقع الويب فقط أثناء الفترة الزمنية المذكورة في كائن النطاق الزمني المسمى 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
```

التحقق من الصحة

يكون كائن النطاق الزمني **نشط** عندما تشير الساعة الموجودة على ASA إلى وقت يقع ضمن كائن النطاق الزمني:

```
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
```

يكون كائن النطاق الزمني وكذلك ACE **غير نشط** عندما تشير الساعة على ASA إلى وقت خارج كائن النطاق الزمني:

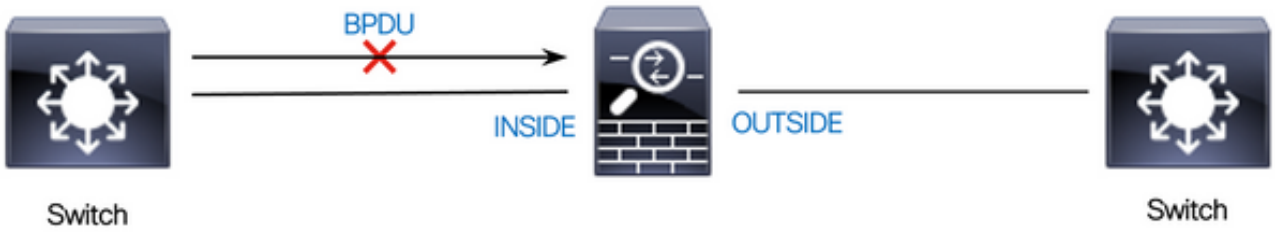
```
ciscoasa# show clock
14:15:44.409 IST Mon Oct 4 2021


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
```

4. تكوين ACE لحظر وحدات بيانات بروتوكول الجسر (BPDU) من السيناريو

خلال ASA في الوضع الشفاف

لمنع حلقات التكرار مع بروتوكول الشجرة المتفرعة (STP)، يتم تمرير وحدات بيانات بروتوكول الجسر (BPDUs) من خلال ASA في الوضع الشفاف بشكل افتراضي. لحظر وحدات بيانات بروتوكول الجسر (BPDUs)، يلزمك تكوين قاعدة EtherType لرفضها.

الرسم التخطيطي للشبكة



قم بتكوين قائمة التحكم في الوصول من EtherType لحظر وحدات بيانات بروتوكول الجسر (BPDUs) من المرور عبر واجهة "الداخل" ل ASA في الإتجاه الوارد كما هو موضح هنا:

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

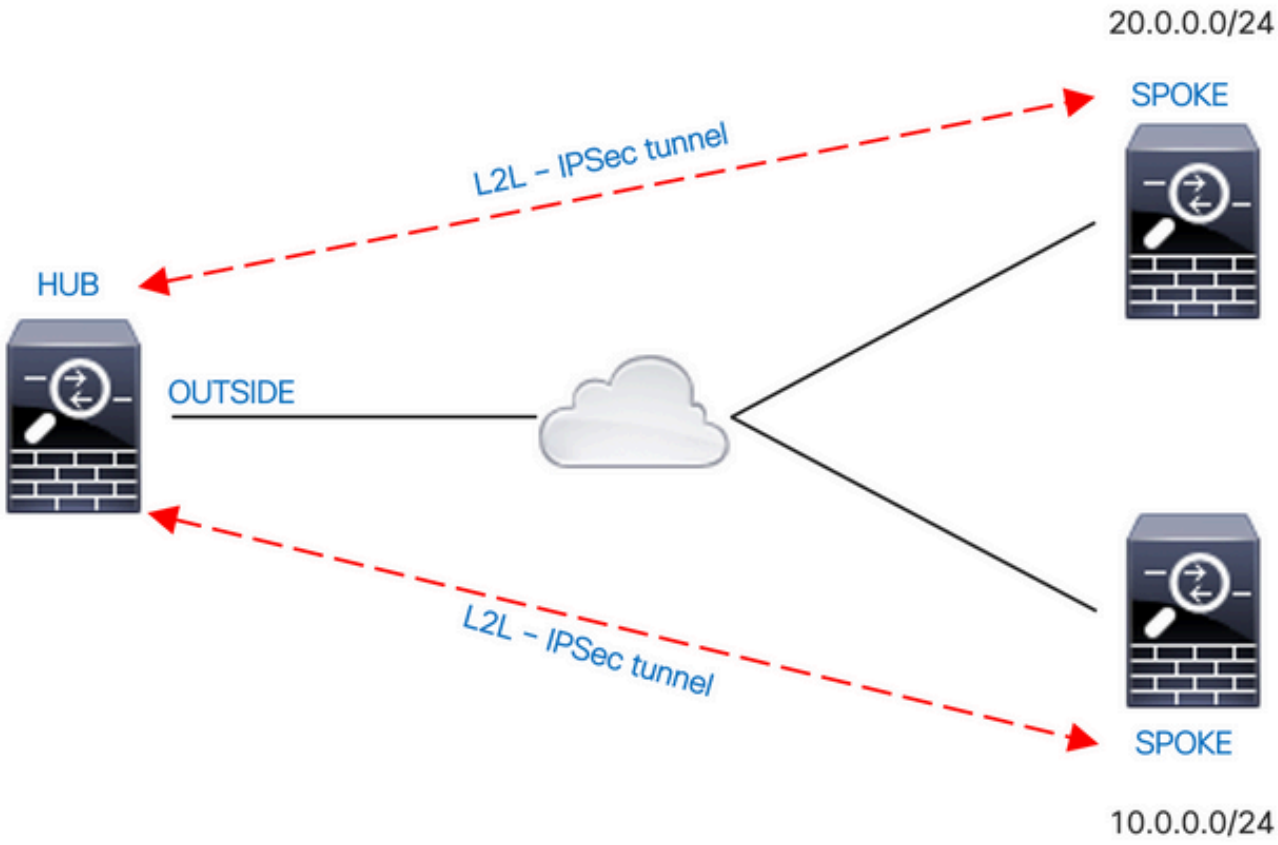
التحقق من الصحة

تحقق من عدد مرات الوصول في قائمة الوصول للتحقق من حظر وحدات بيانات بروتوكول الجسر (BPDUs) بواسطة 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)
```

السيناريو 5. السماح لحركة المرور بالمرور بين الواجهات التي لها نفس مستوى الأمان

الرسم التخطيطي للشبكة



بشكل افتراضي، يتم حظر حركة المرور التي تمر بين الواجهات من نفس مستوى الأمان. للسماح بالاتصال بين الواجهات ذات مستويات الأمان المتساوية، أو للسماح لحركة المرور بإدخال نفس الواجهة والخروج منها (حافة/u-turn)، أستخدم الأمر **نفسه-security-traffic** في وضع التكوين العام.

يوضح هذا الأمر كيفية السماح بالاتصال بين الواجهات المختلفة التي لها مستوى الأمان نفسه:

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

يوضح هذا المثال كيفية السماح بالاتصال من الواجهة نفسها وإليها:

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

هذا سمة مفيد ل VPN حركة مرور أن يدخل قارن غير أن بعد ذلك وجهت خارج أن القارن نفسه. على سبيل المثال، إذا كان لديك شبكة شبكة VPN تدعم تقنية التوصيل المحوري حيث يكون ASA هذا وهو الوصل وتكون شبكات VPN البعيدة فرعية، فلكي يتصل أحدها بالآخر الذي يتحدث، يجب أن تنتقل حركة المرور إلى ASA ثم تخرج مرة أخرى إلى الآخر الذي يتحدث.

التحقق من الصحة

بدون الأمر **نفسه-security-traffic allowed inter-interface**، يشير إخراج الأمر packet-tracer إلى حظر حركة مرور البيانات التي تمر بين الواجهات المختلفة من نفس مستوى الأمان بسبب **قاعدة ضمنية** كما هو موضح هنا:

```
!--- 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
```

بدون الألمر **نفسه-security-traffic allowed intra-interface**، يشير إخراج أداة تتبع الحزم إلى حظر حركة المرور التي تمر من نفس الواجهة وإليها بسبب **قاعدة ضمنية** كما هو موضح هنا:

```
!--- 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
```

السيناريو 6. تكوين ACE للتحكم في حركة مرور البيانات إلى المربع

تحدد الكلمة الأساسية control-plane ما إذا كانت قائمة التحكم في الوصول (ACL) مستخدمة للتحكم في حركة مرور المربع. قواعد التحكم في الوصول لحركة مرور الإدارة إلى المربع لها أسبقية أعلى من قاعدة وصول (المعرفة بواسطة مثل هذه الأوامر مثل telnet وأ ssh وأ http) control-plane. لذلك، يجب السماح بحركة مرور الإدارة التي يتم تطبيقها مع خيار control-plane بشكل صريح بواسطة قائمة التحكم في الوصول (ACL) إلى المربع.

على عكس قواعد الوصول العادية، لا يوجد رفض ضمني في نهاية مجموعة من قواعد الإدارة للواجهة. وبدلا من ذلك، يتم بعد ذلك تقييم أي اتصال لا يطابق قاعدة وصول إلى الإدارة بواسطة قواعد التحكم في الوصول العادية. وبدلا من ذلك، يمكن إستخدام قواعد ICMP للتحكم في حركة مرور ICMP إلى الجهاز.

الرسم التخطيطي للشبكة

يتم تكوين قائمة تحكم في الوصول (ACL) باستخدام الكلمة الأساسية control-plane وتم حظر حركة مرور بيانات المربع التي يتم الحصول عليها من عنوان IP 10.65.63.155 وتوجيهها إلى عنوان IP للواجهة "الخارجية" من 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
```

التحقق من الصحة

تحقق من عدد مرات الوصول في قائمة الوصول للتحقق من حظر حركة المرور بواسطة قائمة التحكم في الوصول (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
```

تشير رسائل syslog إلى إسقاط حركة مرور البيانات على واجهة 'identity':

```
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]
```

التسجيل

تعمل الكلمة الأساسية **السجل** على تعيين خيارات التسجيل عندما يطابق ACE مع حزمة للوصول إلى الشبكة (قائمة التحكم في الوصول التي تم تطبيقها مع الأمر **access-group**). إذا قمت بإدخال الكلمة الأساسية **log** بدون أي وسيطات، فإنك توقت بتمكين رسالة سجل النظام 106100 في المستوى الافتراضي (6) وللفاصل الافتراضي (300 ثانية). إذا لم تقم بإدخال الكلمة الأساسية السجل، سيتم إنشاء رسالة سجل النظام الافتراضية 106023 للحزم المرفوضة. خيارات السجل هي:

- المستوى — مستوى خطورة يتراوح بين 0 و 7. الافتراضي هو 6 (إعلامي). إذا قمت بتغيير هذا المستوى للحصول على إدخال تحكم في الوصول (ACE) نشط، فإن المستوى الجديد ينطبق على الاتصالات الجديدة، ويستمر تسجيل الاتصالات الموجودة في المستوى السابق.
- **interval** — الفاصل الزمني بالثواني بين رسائل syslog، من 1 إلى 600. الافتراضي هو 300. يتم استخدام هذه القيمة أيضا كقيمة المهلة لحذف تدفق غير نشط من ذاكرة التخزين المؤقت المستخدمة لجمع الإحصائيات الإسقاط.
- **disable** — يعطل كل تسجيل ACE.
- **افتراضي** — يمكن التسجيل إلى الرسالة 106023. هذا الإعداد هو نفسه عدم تضمين خيار السجل.

رسالة 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]
```

الشرح:

تم رفض حزمة IP حقيقية بواسطة قائمة التحكم في الوصول (ACL). تظهر هذه الرسالة حتى إذا لم يتم تمكين خيار السجل لقائمة التحكم في الوصول (ACL). عنوان IP هو عنوان IP الحقيقي بدلا من القيم التي يتم عرضها من خلال NAT. يتم توفير كل من معلومات الهوية ومعلومات FQDN لعناوين IP إذا تم العثور على واحد مطابق. يقوم جدار الحماية ASA بتسجيل معلومات الهوية (domain\user) أو FQDN (إذا لم يكن اسم المستخدم متوفرا). إذا كانت معلومات الهوية أو FQDN متوفرة، يقوم جدار الحماية ASA بتسجيل هذه المعلومات لكل من المصدر والوجهة.

مثال:

```
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]
```

رسالة 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
```

الشرح:

يتم سرد التكرار الأولي أو إجمالي عدد التكرارات أثناء الفاصل الزمني. توفر هذه الرسالة معلومات أكثر من الرسالة 106023، التي تسجل الحزم المرفوضة فقط، والتي تتضمن عدد مرات الوصول أو مستوى قابل للتكوين.

عندما يحتوي سطر قائمة الوصول على وسيطة *السجل*، من المتوقع أن يتم تشغيل معرف الرسالة هذا بسبب وصول حزمة غير متزامنة إلى ASA لجدار الحماية الآمن وتقييمها بواسطة قائمة الوصول. على سبيل المثال، إذا تم تلقي حزمة ACK على ASA لجدار الحماية الآمن (الذي لا يوجد له اتصال TCP في جدول الاتصال)، يمكن أن يقوم ASA لجدار الحماية الآمن بإنشاء الرسالة 106100، مما يشير إلى أنه تم السماح للحزمة؛ ومع ذلك، يتم إسقاط الحزمة بشكل صحيح بسبب عدم وجود اتصال مطابق.

تصف القائمة قيم الرسالة:

- أباح | مرفوض | EST-ALLOWED— تحدد هذه القيمة ما إذا كان قد تم السماح للحزمة أو رفضها بواسطة قائمة التحكم في الوصول (ACL). إذا كانت القيمة مسموح بها على النحو الأمثل، فسيتم رفض الحزمة بواسطة قائمة التحكم في الوصول (ACL) ولكن تم السماح بها لجلسة عمل تم إنشاؤها بالفعل (على سبيل المثال، يتم السماح لمستخدم داخلي بالوصول إلى الإنترنت، ويتم قبول حزم الاستجابة التي عادة ما يتم رفضها بواسطة قائمة التحكم في الوصول).
- بروتوكول — TCP أو UDP أو ICMP أو رقم بروتوكول IP.
- interface_name — اسم الواجهة للمصدر أو الوجهة الخاصة بالتدفق المسجل. واجهات VLAN مدعومة.
- source_address — عنوان IP المصدر للتدفق المسجل. عنوان IP هو عنوان IP الحقيقي بدلا من القيمة التي يتم عرضها من خلال NAT.
- dest_address — عنوان IP للوجهة الخاص بالتدفق الذي تم تسجيله. عنوان IP هو عنوان IP الحقيقي بدلا من القيمة التي يتم عرضها من خلال NAT.
- source_port — منفذ المصدر للتدفق المسجل (TCP أو UDP). بالنسبة ل ICMP، يكون الرقم بعد منفذ المصدر هو نوع الرسالة.
- idfw_user — اسم مستخدم معرف المستخدم، باسم المجال الذي تمت إضافته إلى syslog الموجود عندما يمكن أن يعثر ASA لجدار الحماية الآمن على اسم المستخدم لعنوان IP.
- sg_info — علامة مجموعة الأمان التي تمت إضافتها إلى syslog عندما يمكن ل ASA لجدار الحماية الآمن العثور على علامة مجموعة أمان لعنوان IP. يتم عرض اسم مجموعة الأمان مع علامة مجموعة الأمان، إذا كانت متوفرة.
- dest_port — منفذ الوجهة للتدفق المسجل (TCP أو UDP). ل ICMP، الرقم بعد الغاية نوع. بالنسبة للنوع 8، رمز رسالة ICMP أي يكون يتوفر ل بعض رسالة نوع يكون دائما 0. للحصول على قائمة بأنواع رسائل بروتوكول ICMP، راجع عنوان URL: http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml.
- عدد مرات السماح بهذا التدفق أو رفضه بواسطة إدخال قائمة التحكم في الوصول (ACL) في الفاصل الزمني الذي تم تكوينه. القيمة هي 1 عندما يقوم جدار الحماية الآمن ASA بإنشاء الرسالة الأولى لهذا التدفق.

- الوصول الألول — الرسالة الألولى التي تم إنشاؤها لهذا التدفق.
- عدد - الفاصل الزمني الثاني — الفاصل الزمني الذي يتم فيه تجميع عدد مرات الوصول. قم بتعييني هذا الفاصل الزمني باستخدام الألمر **access-list** باستخدام خيار **interval**.
- شفرات التجزئة — تتم طباعة إثنين دائما من أجل إدخال التحكم بالوصول (ACE) لمجموعة الكائنات وإدخال التحكم في الوصول (ACE) المنتظم الخاص بالمكون. يتم تحديد القيم على أي إدخال تحكم في الوصول (ACE) إلى الحزمة. لعرض أكواد التجزئة هذه، أدخل الألمر **show-access list**.

مثال:

```
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]
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).