تكوين التحكم في الوصول المستند إلى السياق (CBAC)

المحتويات

المقدمة

توفر ميزة التحكم في الوصول المستند إلى السياق (CBAC) الخاصة بمجموعة ميزات جدار الحماية من Cisco IOS® فحص النشاط المووجود خلف جدار الحماية بشكل فعال. يحدد CBAC حركة المرور التي يلزم السماح لها بالدخول وحركة المرور التي يلزم السماح لها باستخدام قوائم الوصول (بنفس الطريقة التي يستخدم بها Cisco IOS قوائم الوصول). ومع ذلك، تتضمن قوائم الوصول إلى CBAC عبارات فحص IP التي تسمح بفحص البروتوكول للتأكد من عدم العبث به قبل انتقال البروتوكول إلى الأنظمة المووجودة خلف جدار الحماية.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

كما يمكن إستخدام CBAC مع ترجمة عنوان الشبكة (NAT)، ولكن التكوين في هذا المستند يتعامل بشكل أساسي مع الفحص النقي. إن زجن أنت NAT، أنت تحتاج قائمة ميلان إلى جانب أن يعكس العنوان شامل، ال العنوان حقيقي.

قبل التكوين، فكر في هذه الأسئلة.

ما هي حركة المرور التي تريد إخراجها؟

تعتمد حركة المرور التي ترغب في إخراجها على سياسة أمان الموقع، ولكن في هذا المثال العام، يتم السماح بكل شيء بالإرسال إلى الخارج. إذا رفضت قائمة الوصول الخاصة بك كل شيء، فلن تتمكن حركة المرور من المغادرة. تحديد حركة المرور الصادرة باستخدام قائمة الوصول الموسعة هذه:

```
access-list 101 permit ip [source-network] [source-mask] any
access-list 101 deny ip any any
```

ما هي حركة المرور التي تريد السماح لها بالدخول؟

تعتمد حركة المرور التي تريد السماح لها بالدخول على سياسة أمان الموقع الخاصة بك. ومع ذلك، فإن الإجابة المنطقية هي أي شيء ال يلحق الضرر بشبكتك.

في هذا المثال، هناك قائمة حركة مرور تبدو منطقية للسماح بالدخول. تكون حركة مرور بروتوكول رسائل التحكم في الإنترنت (ICMP) مقبولة بشكل عام، ولكن يمكن أن تسمح ببعض إمكانيات هجمات رفض الخدمة (DoS). هذه عينة قائمة وصول لحركة المرور الواردة:

قائمة الوصول الموسعة إلى IP 101

```
permit tcp 10.10.10.0 0.0.0.255 any (84 matches)
permit udp 10.10.10.0 0.0.0.255 any
permit icmp 10.10.10.0 0.0.0.255 any (3 matches)
deny ip any any
```

قائمة الوصول إلى IP الموسعة 102

```
permit eigrp any any (486 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply (1 match)
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo (1 match)
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
deny ip any any (62 matches)

access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any
```

```
access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
access-list 102 permit icمp any 10.10.10.0 0.0.0.255 echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
access-list 102 deny ip any any
```

قائمة الوصول 101 خاصة بحركة المرور الصادرة. قائمة الوصول 102 خاصة بحركة المرور الواردة. تسمح قائمة الوصول إلى البروتوكول توجيه البروتوكول توجيه العبارة الداخلي الوارد. ICMP حركة مرور الواردة المحددة و(EIGRP) المحسن.

في المثال، يمكن الوصول إلى خادم على جانب الإيثرنت من الموجه من الإنترنت. تمنع قائمة الوصول من إنشاء جلسة عمل. ولتسهيل الوصول إليه، يجب تعديل قائمة الوصول للسماح بالمحادثة. لتغيير قائمة وصول، قم بإزالة قائمة الوصول وتحريرها وإعادة تطبيق قائمة الوصول المحدثة.

ملاحظة: يرجع السبب وراء إزالة قائمة الوصول 102 قبل التحرير وإعادة التطبيق إلى "رفض ip any" في نهاية قائمة الوصول. في هذه الحالة، إذا كنت تريد إضافة إدخال جديد قبل إزالة قائمة الوصول، يظهر الإدخال الجديد بعد الرفض. لذلك، لا يتم فحصها أبدا.

يضيف هذا المثال البروتوكول البسيط لنقل رسائل البريد (SMTP) لـ 10.10.10.1 فقط.

قائمة الوصول إلى IP الموسعة 102

```
permit eigrp any any (385 matches)
permit icmp any 10.10.10.0 0.0.0.255 echo-reply
permit icmp any 10.10.10.0 0.0.0.255 unreachable
permit icmp any 10.10.10.0 0.0.0.255 administratively-prohibited
permit icmp any 10.10.10.0 0.0.0.255 packet-too-big
permit icmp any 10.10.10.0 0.0.0.255 echo
permit icmp any 10.10.10.0 0.0.0.255 time-exceeded
permit tcp any host 10.10.10.1 eq smtp (142 matches)
!--- In this example, you inspect traffic that has been !--- initiated from the inside network.
```

ما هي حركة المرور التي تريد فحصها؟

يدعم CBAC ضمن Cisco IOS:

اسم القائمة الأساسية	البروتوكول
كيوزيمإ	بروتوكول CUSeeMe
ftp	بروتوكول نقل الملفات
h323	بروتوكول H.323 (على سبيل المثال Microsoft NetMeeting أو Intel Video Phone)
http	بروتوكول HTTP
rcmd	أوامر R (r-exec، r-login، r-sh)
ريال أوديو	بروتوكول الصوت الحقيقي
RPC	بروتوكول إستدعاء الإجراء البعيد
smtp	بروتوكول نقل البريد البسيط
sqlnet	بروتوكول SQL Net

انسياب	بروتوكول StreamWorks
tcp	بروتوكول التحكم في الإرسال
tftp	بروتوكول TFTP
udp	بروتوكول مخطط بيانات المستخدم
فساطيط	بروتوكول VDOLive

يتم ربط كل بروتوكول باسم كلمة أساسية. قم بتطبيق اسم الكلمة الأساسية على واجهة تريد فحصها. على سبيل المثال، يقوم هذا التكوين بفحص FTP و SMTP و telnet:

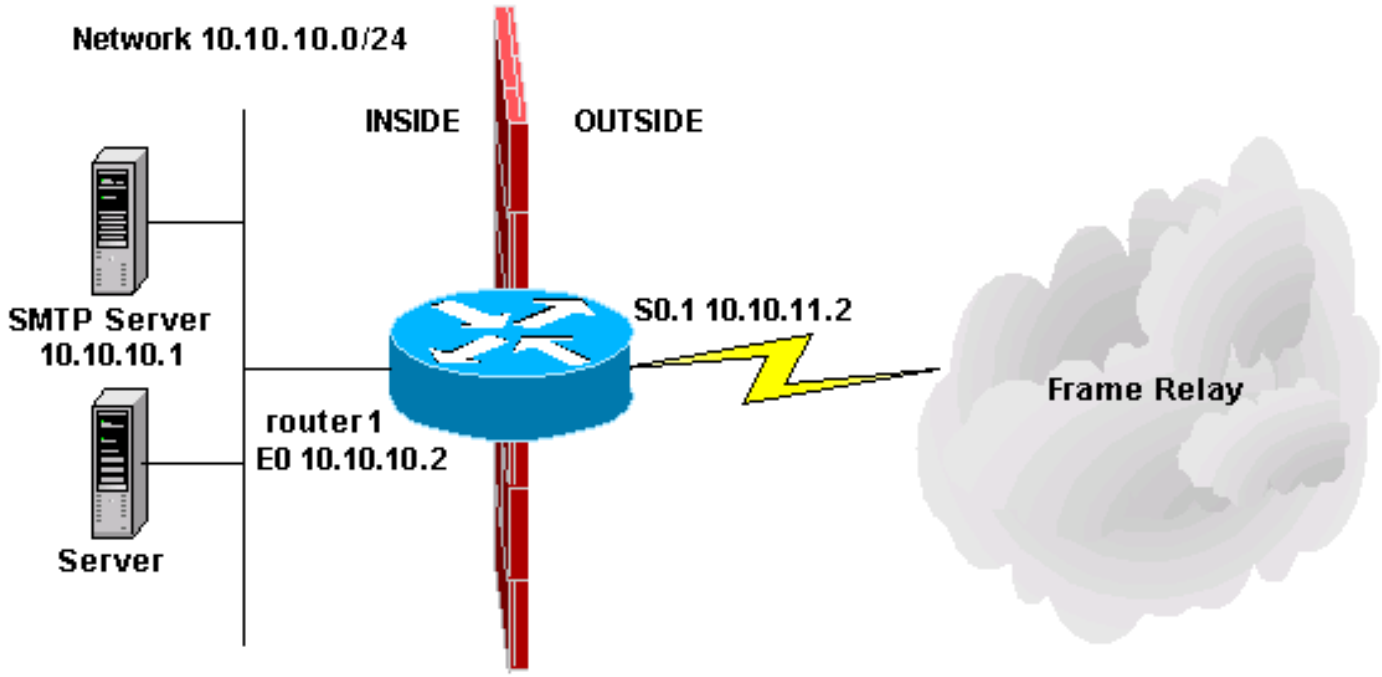
```
router1#configure
Configuring from terminal, memory, or network [terminal]? Enter configuration
commands, one per line. End with CNTL/Z.
router1(config)#ip inspect name mysite ftp
router1(config)#ip inspect name mysite smtp
router1(config)#ip inspect name mysite tcp
router1#show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500]connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50.
Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name mysite

ftp timeout 3600
smtp timeout 3600
tcp timeout 3600
```

يتوانى هذا المستند حركة المرور التي تريد السماح لها، وحركة المرور التي تريد السماح لها بالدخول، وحركة المرور التي تريد فحصها. الآن بعد أن أصبحت مستعدا لتكوين CBAC، أكمل الخطوات التالية:

1. تطبيق التكوين.
2. أدخل قوائم الوصول كما تم تكوينها أعلاه.
3. تكوين كشوف التفتيش.
4. تطبيق قوائم الوصول على الواجهات.

بعد هذا الإجراء، يظهر التكوين الخاص بك كما هو موضح في هذا المخطط والتكوين.



تكوين التحكم في الوصول المستند إلى السياق

```
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname router1
!
!
no ip domain-lookup
ip inspect name mysite ftp
ip inspect name mysite smtp
ip inspect name mysite tcp
!
interface Ethernet0
ip address 10.10.10.2 255.255.255.0
ip access-group 101 in
ip inspect mysite in


no keepalive
!
interface Serial0
no ip address
encapsulation frame-relay
no fair-queue
!
interface Serial0.1 point-to-point
ip address 10.10.11.2 255.255.255.252
ip access-group 102 in
frame-relay interface-dlci 200 IETF
!
router eigrp 69
network 10.0.0.0
no auto-summary
!
ip default-gateway 10.10.11.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.10.11.1
```

```
access-list 101 permit tcp 10.10.10.0 0.0.0.255 any
access-list 101 permit udp 10.10.10.0 0.0.0.255 any
access-list 101 permit icmp 10.10.10.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit eigrp any any
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
echo-reply
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
unreachable
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
administratively-prohibited
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
packet-too-big
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
echo
access-list 102 permit icmp any 10.10.10.0 0.0.0.255
time-exceeded
access-list 102 permit tcp any host 10.10.10.1 eq smtp
access-list 102 deny ip any any
!
line con 0
line vty 0 4
login
!
end
```

معلومات ذات صلة

- صفحة دعم جدار حماية Cisco IOS
- الدعم التقني والمستندات - Cisco Systems

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).