تكوين ASA nat والتوصيات الخاصة بتنفيذ Expressway-E المزدوج وواجهات شبكة

المحتويات

المقدمة

يوضح هذا المستند كيفية تنفيذ تكوين ترجمة عنوان الشبكة (NAT) المطلوب في جهاز الأمان القابل للتكيف (ASA) من Cisco لتنفيذ واجهات الشبكة المزدوجة Expressway-E.

تلميح: هذا النشر هو الخيار الموصى به لتنفيذ Expressway-E، بدلا من تنفيذ بطاقة واجهة شبكة (NIC) واحدة مع انعكاس NAT.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التكوين الأساسي ل Cisco ASA وتكوين NAT
- التكوين الأساسي ل Cisco Expressway-E و Expressway-C

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- أجهزة سلسلة Cisco ASA 5500 و X-5500 التي تشغل الإصدار 8.0 من البرنامج والإصدارات الأحدث.
الإصدار X8. 0 من Cisco Expressway والإصدارات الأحدث.

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

ملاحظة: من خلال المستند بالكامل، تتم الإشارة إلى أجهزة Expressway على أنها Expressway-E و Expressway-C. ومع ذلك، يتم تطبيق التكوين نفسه على Expressway لخادم إتصالات الفيديو (VCS) وأجهزة التحكم في VCS.

معلومات أساسية

بحكم التصميم، يمكن وضع Cisco Expressway-E إما في منطقة مجردة من السلاح (DMZ) أو باستخدام واجهة واجهة على الإنترنت، بينما تكون قادرة على الاتصال ب Cisco Expressway-C في شبكة خاصة. عندما يتم وضع Cisco Expressway-E في منطقة DMZ، فهذه هي الميزات الإضافية:

في السيناريو الأكثر شيوعا، تتم إدارة Cisco Expressway-E بواسطة الشبكة الخاصة. عندما يكون Expressway-E من Cisco في DMZ، يمكن إستخدام جدار حماية محيط (خارجي) لحظر الوصول غير المرغوب فيه إلى Expressway من الشبكات الخارجية عبر طلبات بروتوكول نقل النص التشعبي الآمن (HTTPS) أو طبقة الأمان (SSH).

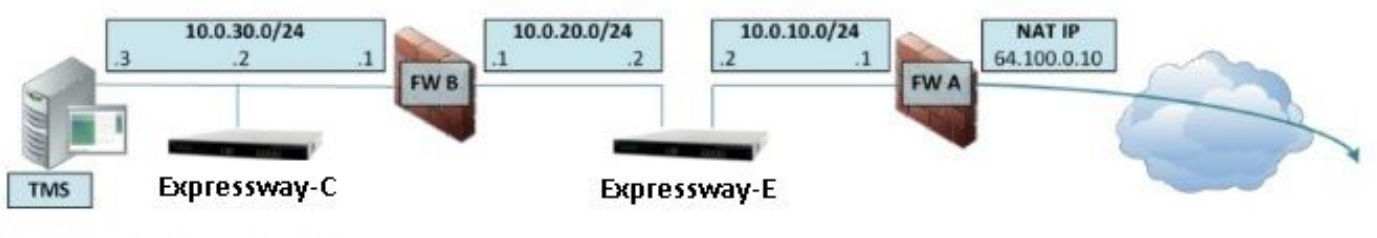
- وإذا لم تسمح المنطقة المجردة من السلاح (DMZ) بالتوصلات المباشرة بين الشبكات الداخلية والخارجية، يلزم توفر خوادم مخصصة لمعالجة حركة مرور البيانات التي تجتاز المنطقة المجردة من السلاح. يمكن أن يعمل Expressway من Cisco كخادم وكيل لبروتوكول بدء جلسة العمل (SIP) و/أو حركة مرور الصوت والفيديو للطراز H.323. في هذه الحالة، يمكنك إستخدام خيار واجهات الشبكة المزدوجة الذي يسمح ExpressWay من Cisco بأن يكون لديك عنوانا IP مختلفين، واحد لحركة مرور البيانات من/إلى جدار الحماية الخارجي، وواحد لحركة مرور البيانات من/إلى جدار الحماية الداخلي.

يمنع هذا الإعداد الاتصالات المباشرة من الشبكة الخارجية إلى الشبكة الداخلية. يؤدي ذلك إلى تحسين أمان الشبكة الداخلية بشكل عام.

طرف: للحصول على مزيد من التفاصيل حول تنفيذ TelePresence، ارجع إلى Cisco Expressway-E و Expressway-C - دليل نشر التكوين الأساسي ووضع الطريق السريع Cisco VCS في منطقة DMZ بدلا من الإنترنت العام.

ExpressWay C و E - واجهات الشبكة المزدوجة/تنفيذ بطاقة واجهة الشبكة (NIC) المزدوجة

تظهر هذه الصورة مثالا لنشر Expressway-E مع واجهات شبكة مزدوجة و NAT ثابت. يعمل Expressway-C كعميل للمرور العابر. هناك حائطان للحريق (Fw A و FWB). بشكل نموذجي، في تكوين DMZ هذا، لا يمكن أن يقوم FW A بتوجيه حركة المرور إلى FW B، وتتطلب أجهزة مثل Expressway-E التحقق من حركة المرور وإعادة توجيهها من الشبكة الفرعية FW A إلى الشبكة الفرعية FW B (والعكس صحيح).



يتكون هذا النشر من هذه المكونات.

الشبكة الفرعية DMZ 1 - 10.0.10.0/24

حفظ واجهة داخلية - 10.0.10.1
واجهة Expressway-E LAN2 - 10.0.10.2
الشبكة الفرعية DMZ 2 - 10.0.20.0/24

الواجهة الخارجية FW B - 10.0.20.1
واجهة Expressway-E LAN1 - 10.0.20.2
شبكة LAN الفرعية - 24/10.0.30.0

الواجهة الداخلية FW B - 10.0.30.1
واجهة Expressway-C LAN1 - 10.0.30.2
واجهة شبكة خادم Cisco TelePresence Management Suite (TMS) - 10.0.30.3
تفاصيل هذا التطبيق:

FW A هو جدار الحماية الخارجي أو المحيط، ويتم تكوينه باستخدام IP NAT IP العام) من 64.100.0.10 والذي تتم ترجمته بشكل ثابت إلى 10.0.10.2 (واجهة Expressway-E LAN2)
FW B هو جدار الحماية الداخلي
Expressway-E LAN1 يتلقى ساكن إستاتيكي nat أسلوب يعجز
- Expressway-E LAN2 يتلقى ساكن إستاتيكي nat أسلوب يمكن مع ساكن إستاتيكي nat عنوان 64.100.0.10
- يحتوي Expressway-C على منطقة عميل متقاطعة تشير إلى 10.0.20.2 (واجهة Expressway-E LAN1)

لا يوجد توجيه بين الشبكات الفرعية 24/10.0.20.0 و 24/10.0.10.0. تعمل Expressway-E على جسر هذه الشبكات الفرعية وتعمل كوكيل لوسائط إرسال إشارات SIP/H.323 وبروتوكول النقل في الوقت الفعلي (RTP) / بروتوكول التحكم في بروتوكول RTP) RTCP).
تحتوي Cisco TMS على Expressway-E تم تكوينه باستخدام عنوان IP 10.0.20.2

المتطلبات/القيود

الشبكات الفرعية غير المتداخلة

إذا تم تكوين Expressway-E لاستخدام كلا واجهات LAN، فيجب تحديد موقع واجهات LAN1 و LAN2 في الشبكات الفرعية غير المتراكبة لضمان إرسال حركة مرور البيانات إلى الواجهة الصحيحة.

تجميع

عند تجميع أجهزة Expressway باستخدام خيار الشبكة المتقدمة الذي تم تكوينه، يلزم تكوين كل نظير نظام مجموعة باستخدام عنوان واجهة LAN1 الخاص به. in addition، مجموعة ينبغي كنت شكلت على قارن أن لا يتلقى ساكن إستاتيكي nat أسلوب يمكن. لذلك، من المستحسن أن يستعمل أنت LAN2 كالقارن خارجي، على أي أنت يستطيع طبقت وشكلت NAT ساكن إستاتيكي حيثما أمكن.

إعدادات واجهة LAN الخارجية

إعدادات تكوين واجهة شبكة LAN الخارجية على التحكم في صفحة تكوين IP التي تستخدم واجهة الشبكة المحولة باستخدام الارسال حول TURN) NAT). في تكوين واجهة شبكة Expressway-E مزدوجة، يتم تعيين ذلك عادة على واجهة Expressway-E الخارجية للشبكة المحلية (LAN).

المسارات الثابتة

يجب تكوين ExpressWay-E باستخدام عنوان عبارة افتراضي بقيمة 10.0.10.1 لهذا السيناريو. هذا يعني أن كل حركة مرور يرسل عبر LAN2، افتراضيا، أرسلت إلى العنوان 10.0.10.1.

إذا ترجم FW B حركة مرور البيانات المرسلة من الشبكة الفرعية 24/10.0.30.0 إلى واجهة Expressway-E LAN1 (على سبيل المثال، حركة مرور عميل العبور Expressway-C أو حركة مرور إدارة خادم TMS)، تظهر حركة المرور هذه لأنها تأتي من الواجهة الخارجية (10.0.20.1 FWB) حيث إنها تصل إلى شبكة Expressway-E LAN1. وبعد ذلك، يمكن ل Expressway-E الرد على حركة المرور هذه عبر واجهة LAN1 الخاصة بها نظرا لوجود المصدر الظاهري لحركة المرور هذه على الشبكة الفرعية نفسها.

إذا تم تمكين NAT على المحول FW B، فستظهر حركة المرور التي يتم إرسالها من Expressway-C إلى Expressway-E LAN1 بأنها تأتي من 10.0.30.2. إذا لم يكن Expressway لديه مسار ثابت مضاف للشبكة الفرعية 24/10.0.30.0، فإنه يرسل الردود الخاصة بحركة المرور هذه إلى العبارة الافتراضية (10.0.10.1) خارج الشبكة المحلية (LAN2)، نظرا لأنه لا يعلم أن الشبكة الفرعية 24/10.0.30.0 موجودة خلف جدار الحماية الداخلي (FW B). لذلك، يلزم إضافة مسار ثابت، قم بتشغيل أمر واجهة سطر الأوامر CLI **xCommand RouteAdd** من خلال جلسة SSH إلى Expressway.

في هذا المثال الخاص، يجب أن يعرف Expressway-E أنه يمكنه الوصول إلى الشبكة الفرعية 24/10.0.30.0 الموجودة خلف الشبكة الفرعية FW B، والتي يمكن الوصول إليها عبر واجهة LAN1. للقيام بذلك، قم بتشغيل الأمر:

```
xCommand RouteAdd Address: 10.0.30.0 PrefixLength: 24 Gateway: 10.0.20.1 Interface: LAN1
```

بطاقة: Sيمكن تطبيق تكوين المسار الثابت من خلال واجهة المستخدم الرسومية (GUI) الخاصة ب Expressway-E بالإضافة إلى **نظام/شبكة** القسم **> الواجهات/المسارات الثابتة**.

في هذا المثال، يمكن أيضا تعيين معلمة الواجهة على **تلقائي** نظرا لأن عنوان البوابة (10.0.20.1) هو فقط القابل للوصول عبر LAN1.

إذا لم يتم تمكين NAT على FW B ويحتاج Expressway-E إلى الاتصال بالأجهزة في الشبكات الفرعية (بخلاف 24/10.0.30.0) التي تقع أيضا خلف FW B، فيجب إضافة المسارات الثابتة لهذه الأجهزة/الشبكات الفرعية.

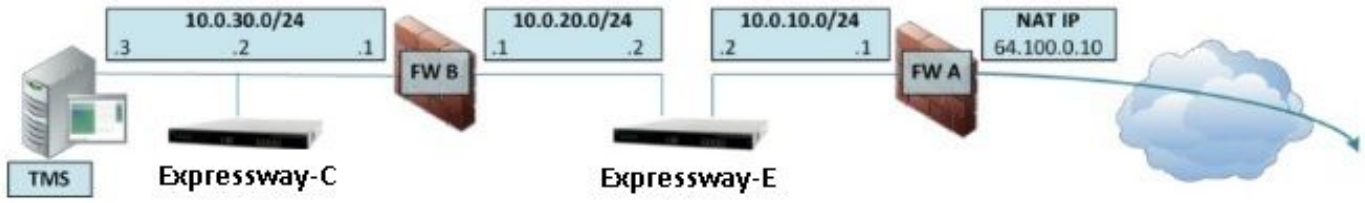
ملاحظة: ويشمل ذلك توصيلات SSH و HTTPS من محطات عمل إدارة الشبكة أو لخدمات الشبكة مثل NTP أو DNS أو LDAP/AD أو Syslog.

يتم وصف الأمر **xCommand RouteAdd** وصياغة الجملة بالتفصيل الكامل في دليل مسؤول VCS.

التكوين

يصف هذا قسم كيف أن يشكل الساكن إستاتيكي NAT مطلوب ل ال expressway-E مزدوج شبكة قارن تنفيذ على ال ASA. تم تضمين بعض توصيات تكوين إطار سياسة معياري ASA الإضافية (MPF) لمعالجة حركة مرور SIP/H323.

Expressway C و E - واجهات شبكة مزدوجة/تنفيذ بطاقة واجهة الشبكة (NIC) المزدوجة



في هذا المثال، تعيين عنوان IP هو التالي.

عنوان بروتوكول الإنترنت Expressway-C: 10.0.30.2/24

(Expressway-C default-gateway: 10.0.30.1 (FW-B

عناوين IP الخاصة ب Expressway-E:

على الشبكة المحلية LAN2: 10.0.10.2/24

على الشبكة المحلية LAN1: 10.0.20.2/24

(Expressway-E default-gateway: 10.0.10.1 (FW-A

عنوان TMS IP: 10.0.30.3/24

تكوين FW-A

الخطوة 1. تشكيل ساكن إستاتيكي nat ل ال Expressway-E.

كما هو موضح في قسم معلومات الخلفية في هذا المستند، يحتوي FW-A على ترجمة NAT ثابتة للسماح بالوصول إلى Expressway-E من الإنترنت باستخدام عنوان IP العام 64.100.0.10. هذا الأخير من NATed إلى Expressway-E LAN2 عنوان 24/10.0.10.2. بعد ذلك، هذا هو المطلوب FW-A ساكن إستاتيكي nat.

لإصدارات ASA 8.3 والإصدارات الأحدث:

```
:To use PAT with specific ports range !

object network obj-10.0.10.2
host 10.0.10.2

object service obj-udp_3478-3483 service udp source range 3478 3483 object service obj-
udp_24000-29999 service udp source range 24000 29999 object service obj-udp_36002-59999 service
udp source range 36002 59999 object service obj-tcp_5222 service tcp source eq 5222 object
service obj-tcp_8443 service tcp source eq 8443 object service obj-tcp_5061 service tcp source
eq 5061 object service obj-udp_5061 service udp source eq 5061 nat (inside,outside) source
```

```
static obj-10.0.10.2 interface service obj-udp_3478-3483 obj-udp_3478-3483 nat (inside,outside)
      source static obj-10.0.10.2 interface service obj-udp_24000-29999 obj-udp_24000-29999 nat
        (inside,outside) source static obj-10.0.10.2 interface service obj-udp_36002-59999 obj-
udp_36002-59999 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5222
   obj-tcp_5222 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_8443
   obj-tcp_8443 nat (inside,outside) source static obj-10.0.10.2 interface service obj-tcp_5061
   obj-tcp_5061 nat (inside,outside) source static obj-10.0.10.2 interface service obj-udp_5061
       obj-udp_5061 OR ! To use with static one-to-one NAT: object network obj-10.0.10.2 nat
                                                    (inside,outside) static interface
```

تحذير: عندما يطبق أنت الساكن إستاتيكي ضرب أمر أنت تستلم هذا خطأ رسالة على ال ASA أمر خط قارن، **خطأ: nat يعجز أن يحجز ميناء**. بعد هذا، قم بالمتابعة لمسح الإدخالات xlate على ASA، ولهذا، قم بتشغيل الأمر **clearXlatelocal x.x.x.x**،من حيث يتوافق x.x.x.x مع ASA خارج عنوان IP. يعمل هذا الأمر على مسح جميع الترجمات المرتبطة بعنوان IP هذا، وتشغيله بحذر في بيئات الإنتاج.

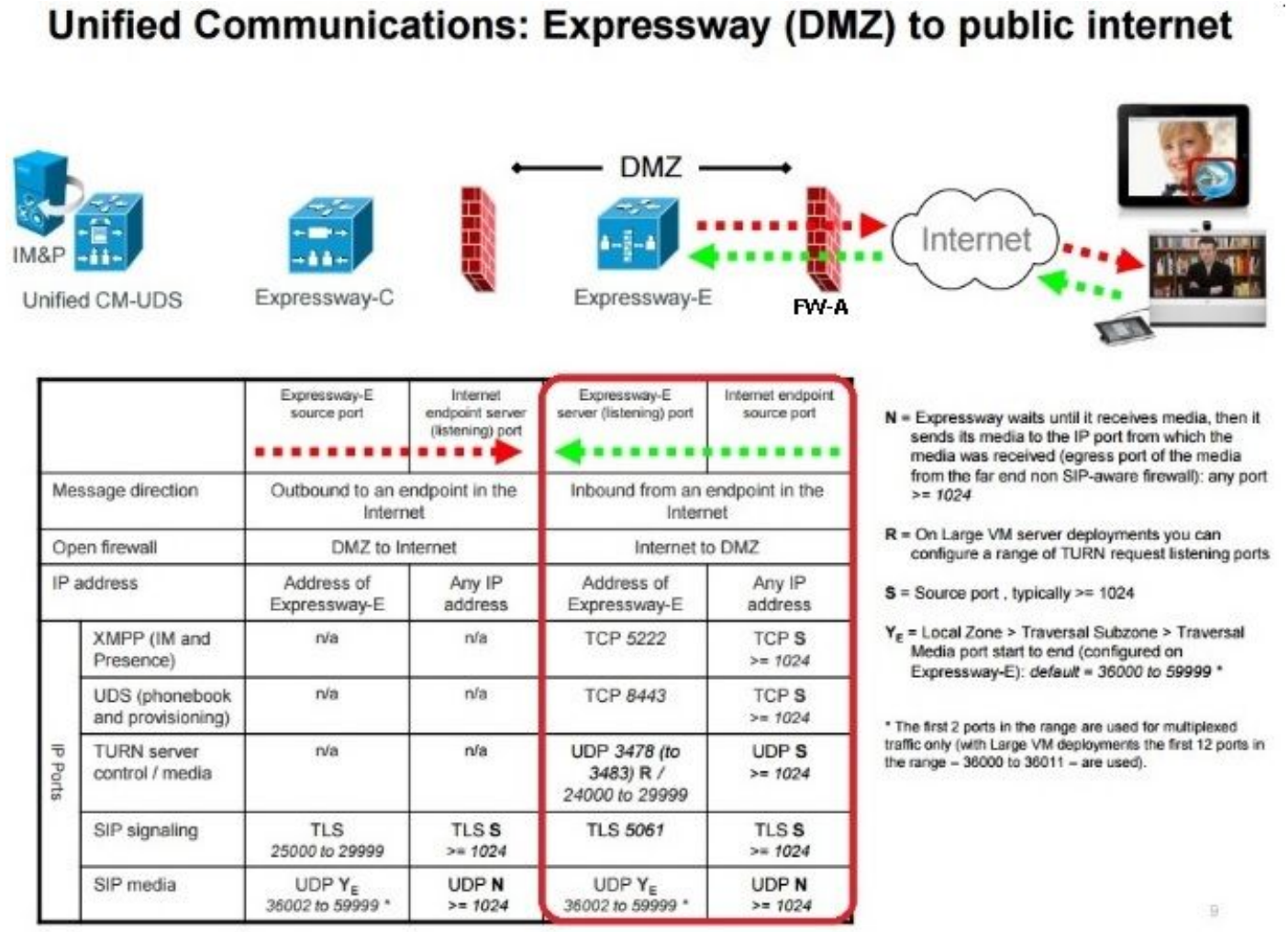
لإصدارات ASA 8.2 والإصدارات الأقدم:

```
Static PAT for a Range of Ports is Not Possible - A configuration line is required per port. !
                                                    .This example shows only when Static one-to-one NAT is used

                                    static (inside,outside) interface 10.0.10.2 netmask  255.255.255.255
```

الخطوة 2. يسمح تكوين قائمة التحكم في الوصول (ACL) بالمنافذ المطلوبة من الإنترنت إلى Expressway-E.

وفقا للاتصالات الموحدة: من Expressway (DMZ) إلى وثائق الإنترنت العامة، يتم توضيح قائمة منافذ TCP و UDP التي يتطلب Expressway-E السماح بها في FW-A، كما هو موضح في الصورة:



		Expressway-E source port	Internet endpoint server (listening) port	Expressway-E server (listening) port	Internet endpoint source port
Message direction		Outbound to an endpoint in the Internet		Inbound from an endpoint in the Internet	
Open firewall		DMZ to Internet		Internet to DMZ	
IP address		Address of Expressway-E	Any IP address	Address of Expressway-E	Any IP address
IP Ports	XMPP (IM and Presence)	n/a	n/a	TCP *5222*	TCP **S** *>= 1024*
	UDS (phonebook and provisioning)	n/a	n/a	TCP *8443*	TCP **S** *>= 1024*
	TURN server control / media	n/a	n/a	UDP *3478 (to 3483)* **R** / *24000 to 29999*	UDP **S** *>= 1024*
	SIP signaling	TLS *25000 to 29999*	TLS **S** *>= 1024*	TLS *5061*	TLS **S** *>= 1024*
	SIP media	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*	UDP Y_E *36002 to 59999* *	UDP **N** *>= 1024*

N = Expressway waits until it receives media, then it sends its media to the IP port from which the media was received (egress port of the media from the far end non SIP-aware firewall): any port *>= 1024*

R = On Large VM server deployments you can configure a range of TURN request listening ports

S = Source port , typically >= 1024

Y_E = Local Zone > Traversal Subzone > Traversal Media port start to end (configured on Expressway-E): *default = 36000 to 59999* *

* The first 2 ports in the range are used for multiplexed traffic only (with Large VM deployments the first 12 ports in the range – 36000 to 36011 – are used).

هذا هو تكوين قائمة التحكم في الوصول (ACL) المطلوب كما هو وارد في الواجهة الخارجية بنظام FW-A.

لإصدارات ASA 8.3 والإصدارات الأحدث:

```
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
access-list outside-in extended permit udp any host 10.0.10.2 lt 3484
access-list outside-in extended permit udp any host 10.0.10.2 gt 23999
access-list outside-in extended permit udp any host 10.0.10.2 lt 30000
access-list outside-in extended permit udp any host 10.0.10.2 gt 36001
access-list outside-in extended permit udp any host 10.0.10.2 lt 60000
access-list outside-in extended permit udp any host 10.0.10.2 eq 5061
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061

access-group outside-in in interface outside
```

لإصدارات ASA 8.2 والإصدارات الأقدم:

```
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5222
access-list outside-in extended permit tcp any host 64.100.0.10 eq 8443
access-list outside-in extended permit udp any host 64.100.0.10 gt 3477
access-list outside-in extended permit udp any host 64.100.0.10 lt 3484
access-list outside-in extended permit udp any host 64.100.0.10 gt 23999
access-list outside-in extended permit udp any host 64.100.0.10 lt 30000
access-list outside-in extended permit udp any host 64.100.0.10 gt 36001
access-list outside-in extended permit udp any host 64.100.0.10 lt 60000
access-list outside-in extended permit udp any host 64.100.0.10 eq 5061
access-list outside-in extended permit tcp any host 64.100.0.10 eq 5061

access-group outside-in in interface outside
```

تكوين FW-B

كما هو موضح في قسم معلومات الخلفية في هذا المستند، قد يتطلب FW B تكوين NAT أو PAT ديناميكي للسماح بترجمة الشبكة الفرعية الداخلية 24/10.0.30.0 إلى عنوان IP 10.0.20.1 عندما تنتقل إلى الواجهة الخارجية من FW B.

لإصدارات ASA 8.3 والإصدارات الأحدث:

```
object network obj-10.0.30.0
 subnet 10.0.30.0 255.255.255.0
nat (inside,outside) dynamic interface
```

لإصدارات ASA 8.2 والإصدارات الأقدم:

```
nat (inside) 1 10.0.30.0 255.255.255.0
global (outside) 1 interface
```

تلميح: تأكد من أن جميع منافذ TCP و UDP المطلوبة تسمح ل Expressway-C بالعمل بشكل صحيح وتكون مفتوحة في FW B، تماما كما هو محدد في مستند Cisco هذا: إستخدام منفذ Cisco من ExpressWay IP لجدار الحماية

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يمكن إستخدام تعقب الحزمة على ASA لتأكيد أن ترجمة Expressway-E الثابتة ل NAT تعمل كما هو مطلوب.

Packet Tracer إلى إختبار 64.100.0.10 في TCP/5222

```
FW-A#packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5222

                                                Phase: 1
                                              Type: UN-NAT
                                           Subtype: static
                                             Result: ALLOW
                                                    :Config
                                    object network obj-10.0.10.2
                                 nat (inside,outside) static interface
                                             :Additional Information
                                  NAT divert to egress interface inside
                               Untranslate 64.100.0.10/5222 to 10.0.10.2/5222

                                                Phase: 2
                                            Type: ACCESS-LIST
                                                 Subtype: log
                                              Result: ALLOW
                                                    :Config
                                 access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5222
                                             :Additional Information

                                                Phase: 3
                                            Type: IP-OPTIONS
                                                    :Subtype
                                              Result: ALLOW
                                                    :Config
                                          :Additional Information

                                                Phase: 4
                                               Type: NAT
                                          Subtype: rpf-check
                                              Result: ALLOW
                                                    :Config
                                    object network obj-10.0.10.2
                                 nat (inside,outside) static interface
                                             :Additional Information

                                                Phase: 5
                                            Type: IP-OPTIONS
                                                    :Subtype
                                              Result: ALLOW
                                                    :Config
                                          :Additional Information

                                                Phase: 6
                                         Type: FLOW-CREATION
                                                    :Subtype
                                              Result: ALLOW
                                                    :Config
                                          :Additional Information
                  New flow created with id 13, packet dispatched to next module

                                                    :Result
                                        input-interface: outside
```

```
                                                input-status: up
                                              input-line-status: up
                                            output-interface: inside
                                                output-status: up
                                              output-line-status: up
                                                Action: allow
```

Packet Tracer إلى إختبار 64.100.0.10 في TCP/8443

```
FW-A# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 8443

                                                        Phase: 1
                                                    Type: UN-NAT
                                                  Subtype: static
                                                    Result: ALLOW
                                                           :Config
                                              object network obj-10.0.10.2
                                     nat (inside,outside) static interface
                                                :Additional Information
                                      NAT divert to egress interface inside
                                  Untranslate 64.100.0.10/8443 to 10.0.10.2/8443

                                                        Phase: 2
                                                  Type: ACCESS-LIST
                                                       Subtype: log
                                                    Result: ALLOW
                                                           :Config
                                        access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 8443
                                                :Additional Information

                                                        Phase: 3
                                                  Type: IP-OPTIONS
                                                           :Subtype
                                                    Result: ALLOW
                                                           :Config
                                                :Additional Information

                                                        Phase: 4
                                                     Type: NAT
                                                Subtype: rpf-check
                                                    Result: ALLOW
                                                           :Config
                                              object network obj-10.0.10.2
                                     nat (inside,outside) static interface
                                                :Additional Information

                                                        Phase: 5
                                                  Type: IP-OPTIONS
                                                           :Subtype
                                                    Result: ALLOW
                                                           :Config
                                                :Additional Information

                                                        Phase: 6
                                               Type: FLOW-CREATION
                                                           :Subtype
                                                    Result: ALLOW
                                                           :Config
                                                :Additional Information
                New flow created with id 14, packet dispatched to next module

                                                           :Result
```

```
input-interface: outside
        input-status: up
   input-line-status: up
output-interface: inside
       output-status: up
  output-line-status: up
              Action: allow
```

Packet Tracer إلى إختبار 64.100.0.10 في TCP/5061

```
FW-1# packet-tracer input outside tcp 4.2.2.2 1234 64.100.0.10 5061

                                                Phase: 1
                                              Type: UN-NAT
                                           Subtype: static
                                             Result: ALLOW
                                                    :Config
                                    object network obj-10.0.10.2
                          nat (inside,outside) static interface
                                         :Additional Information
                          NAT divert to egress interface inside
                  Untranslate 64.100.0.10/5061 to 10.0.10.2/5061

                                                Phase: 2
                                         Type: ACCESS-LIST
                                              Subtype: log
                                           Result: ALLOW
                                                    :Config
                                access-group outside-in in interface outside
access-list outside-in extended permit tcp any host 10.0.10.2 eq 5061
                                         :Additional Information

                                                Phase: 3
                                         Type: IP-OPTIONS
                                                 :Subtype
                                           Result: ALLOW
                                                    :Config
                                       :Additional Information

                                                Phase: 4
                                              Type: NAT
                                        Subtype: rpf-check
                                             Result: ALLOW
                                                    :Config
                                    object network obj-10.0.10.2
                          nat (inside,outside) static interface
                                         :Additional Information

                                                Phase: 5
                                         Type: IP-OPTIONS
                                                 :Subtype
                                           Result: ALLOW
                                                    :Config
                                       :Additional Information

                                                Phase: 6
                                     Type: FLOW-CREATION
                                                 :Subtype
                                           Result: ALLOW
                                                    :Config
                                       :Additional Information
                  New flow created with id 15, packet dispatched to next module
```

```
                                                                  :Result
                                                 input-interface: outside
                                                         input-status: up
                                                    input-line-status: up
                                                 output-interface: inside
                                                        output-status: up
                                                   output-line-status: up
                                                           Action: allow
```

Packet Tracer إلى إختبار 64.100.0.10 في UDP/24000

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 24000

                                                          Phase: 1
                                                       Type: UN-NAT
                                                    Subtype: static
                                                      Result: ALLOW
                                                             :Config
                                             object network obj-10.0.10.2
                                      nat (inside,outside) static interface
                                                  :Additional Information
                                       NAT divert to egress interface inside
                                  Untranslate 64.100.0.10/24000 to 10.0.10.2/24000

                                                          Phase: 2
                                                    Type: ACCESS-LIST
                                                         Subtype: log
                                                      Result: ALLOW
                                                             :Config
                                    access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
                                                  :Additional Information

                                                          Phase: 3
                                                   Type: IP-OPTIONS
                                                             :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                  :Additional Information

                                                          Phase: 4
                                                       Type: NAT
                                                    Subtype: rpf-check
                                                      Result: ALLOW
                                                             :Config
                                             object network obj-10.0.10.2
                                      nat (inside,outside) static interface
                                                  :Additional Information

                                                          Phase: 5
                                                   Type: IP-OPTIONS
                                                             :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                  :Additional Information

                                                          Phase: 6
                                                Type: FLOW-CREATION
                                                             :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                  :Additional Information
                          New flow created with id 16, packet dispatched to next module
```

```
                                                                  :Result
                                                 input-interface: outside
                                                         input-status: up
                                                    input-line-status: up
                                                 output-interface: inside
                                                        output-status: up
                                                   output-line-status: up
                                                          Action: allow
```

Packet Tracer إلى إختبار 64.100.0.10 في UDP/36002

```
ASA1# packet-tracer input outside udp 4.2.2.2 1234 64.100.0.10 36002

                                                          Phase: 1
                                                       Type: UN-NAT
                                                    Subtype: static
                                                      Result: ALLOW
                                                             :Config
                                                object network obj-10.0.10.2
                                       nat (inside,outside) static interface
                                                :Additional Information
                                        NAT divert to egress interface inside
                                    Untranslate 64.100.0.10/36002 to 10.0.10.2/36002

                                                          Phase: 2
                                                   Type: ACCESS-LIST
                                                        Subtype: log
                                                      Result: ALLOW
                                                             :Config
                                          access-group outside-in in interface outside
access-list outside-in extended permit udp any host 10.0.10.2 gt 3477
                                                :Additional Information

                                                          Phase: 3
                                                   Type: IP-OPTIONS
                                                           :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information

                                                          Phase: 4
                                                       Type: NAT
                                                  Subtype: rpf-check
                                                      Result: ALLOW
                                                             :Config
                                                object network obj-10.0.10.2
                                       nat (inside,outside) static interface
                                                :Additional Information

                                                          Phase: 5
                                                   Type: IP-OPTIONS
                                                           :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information

                                                          Phase: 6
                                               Type: FLOW-CREATION
                                                           :Subtype
                                                      Result: ALLOW
                                                             :Config
                                                :Additional Information
```

```
New flow created with id 17, packet dispatched to next module

                                                                :Result
                                                      input-interface: outside
                                                              input-status: up
                                                         input-line-status: up
                                                      output-interface: inside
                                                             output-status: up
                                                       output-line-status: up
                                                                Action: allow
```

استكشاف الأخطاء وإصلاحها

الخطوة 1. مقارنة مجموعات الحزم.

يمكن التقاط الحزم في كل من واجهات مدخل ومخرج ASA.

```
                                                                FW-A# sh cap
                                  capture capout interface outside match ip host 64.100.0.100 host 64.100.0.10
                                    capture capin interface inside match ip host 64.100.0.100 host 10.0.10.2
```

حزم التقاط ل 64.100.0.10 في TCP/5222:

```
                                                                FW-A# sh cap capout

                                                                 packets captured 2
S 4178032747:4178032747(0) win 4128 :64.100.0.10.5222 < 64.100.0.100.21144 21:39:33.646954 :1
                                                                                  <<mss 1460
S 4178032747:4178032747(0) win 4128 :64.100.0.10.5222 < 64.100.0.100.21144 21:39:35.577652 :2
                                                                                  <<mss 1460
                                                                    packets shown 2

                                                                FW-A# sh cap capin

                                                                 packets captured 2
    S 646610520:646610520(0) win 4128 :10.0.10.2.5222 < 64.100.0.100.21144 21:39:33.647290 :1
                                                                                  <<mss 1380
    S 646610520:646610520(0) win 4128 :10.0.10.2.5222 < 64.100.0.100.21144 21:39:35.577683 :2
                                                                                  <<mss 1380
                                                                    packets shown 2
```

حزم التقاط ل 64.100.0.10 في TCP/5061:

```
                                                                FW-A# sh cap capout
                                                                 packets captured 2

S 2023539318:2023539318(0) win 4128 :64.100.0.10.5061 < 64.100.0.100.50820 21:42:14.920576 :1
                                                                                  <<mss 1460
S 2023539318:2023539318(0) win 4128 :64.100.0.10.5061 < 64.100.0.100.50820 21:42:16.992380 :2
                                                                                  <<mss 1460
                                                                    packets shown 2
 FW-A# sh cap capin 2 packets captured 1: 21:42:14.920866 64.100.0.100.50820 > 10.0.10.2.5061: S
             2082904361:2082904361(0) win 4128 <mss 1380> 2: 21:42:16.992410 64.100.0.100.50820 >
                   10.0.10.2.5061: S 2082904361:2082904361(0) win 4128 <mss 1380> 2 packets shown
```

الخطوة 2. فحص لقطات حزمة إسقاط مسار الأمان السريع (ASP).

يتم التقاط عمليات إسقاط الحزمة بواسطة ASA بواسطة التقاط ASA ASP. على قبض الخيار **all**، كل الأسباب المحتملة لما أسقط ال ASA ربط. ويمكن تضييق نطاق ذلك إذا كان هناك أي سبب مشكوك فيه. للحصول على قائمة بالأسباب التي يستخدمها ASA لتصنيف هذه عمليات الإسقاط، قم بتشغيل الأمر **show asp drop.**

```
capture asp type asp-drop all

show cap asp

OR

show cap asp | i 64.100.0.10
show cap asp | i 10.0.10.2
```

تلميح: يتم إستخدام التقاط ASA ASP في هذا السيناريو لتأكيد ما إذا كان ASA يسقط الحزم بسبب تكوين قائمة التحكم في الوصول (ACL) أو NAT مفقود، والذي قد يتطلب فتح منفذ TCP أو UDP محدد ل Expressway-E.

تلميح: حجم المخزن المؤقت الافتراضي لكل التقاط ASA هو 512 كيلوبايت. إذا تم إسقاط العديد من الحزم بواسطة ASA، يتم ملء المخزن المؤقت بسرعة. يمكن زيادة حجم المخزن المؤقت باستخدام خيار **المخزن المؤقت**.

التوصيات

تأكد من أن فحص SIP/H.323 معطل تماما على جدران الحماية المعنية.

يوصى بشدة بتعطيل فحص SIP و H.323 على جدران الحماية التي تتعامل مع حركة مرور الشبكة من أو إلى Expressway-E. عند تمكين هذا الخيار، غالبا ما يؤثر فحص SIP/H.323 سلبا على وظيفة إجتياز جدار الحماية/NAT المدمج في Expressway.

هذا مثال على كيفية تعطيل عمليات تفتيش SIP و H.323 على ASA:

```
policy-map global_policy
class inspection_default
  no inspect h323 h225
  no inspect h323 ras
    no inspect sip
```

تنفيذ ExpressWay بديل VCS

هناك حل بديل لتنفيذ تقنية Expressway-E مع واجهات شبكة مزدوجة/بطاقة واجهة شبكة (NIC) مزدوجة، وهو تنفيذ تقنية Expressway-E ولكن بتكوين انعكاس لبطاقة واجهة شبكة (NIC) واحدة وبطاقة واجهة الشبكة (NAT) على جدران الحماية. يوضح الارتباط التالي تفاصيل إضافية حول هذا التنفيذ [قم بتكوين انعكاس NAT على ASA لأجهزة TelePresence عبر الطريق السريع VCS].

تلميح: التنفيذ الموصى به ل VCS ExpressWay هو واجهات الشبكة المزدوجة/تنفيذ NIC ExpressWay المزدوج الموضح في هذا المستند.

معلومات ذات صلة

- تكوين انعكاس NAT على ASA لأجهزة VCS Expressway TelePresence
- الدعم التقني والمستندات - Cisco Systems
- Cisco Expressway-E و Expressway-C - دليل نشر التكوين الأساسي
- وضع Cisco VCS ExpressWay في المنطقة المنزوعة السلاح بدلا من وضعه في الإنترنت العام
- إستخدام منفذ Expressway IP من Cisco لمرور الجدار الناري

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).