تكوين انعكاس NAT على ASA لأجهزة VCS Expressway TelePresence

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
بروتوكول اجتياز NAT لتسلسل التحقق من الإطارات (VCS) C و E لتنفيذ بوابة الموصى بها غير Cisco
شبكة DMZ واحدة VCS Expressway LAN واحدة مع واجهة واحدة
DMZ واحدة VCS Expressway LAN واحدة مع واجهة 3-Port FW
التكوين
شبكة DMZ واحدة VCS Expressway LAN واحدة مع واجهة واحدة
DMZ واحدة VCS Expressway LAN واحدة مع واجهة 3-Port FW
التحقق من الصحة
شبكة DMZ واحدة VCS Expressway LAN واحدة مع واجهة واحدة
DMZ واحدة VCS Expressway LAN واحدة مع واجهة 3-Port FW
استكشاف الأخطاء وإصلاحها
سيناريو حزمة التقاط تم تطبيقها "واجهة VCS Expressway LAN واحدة مع واجهة 3-Port FW DMZ"
سيناريو حزمة التقاط تم تطبيقها "واجهة VCS Expressway LAN المفردة مع واجهة DMZ المفردة الشبكة الفرعية"
التوصيات
1. تجنب تنفيذ أي مخطط غير مدعوم
2. تأكد من أن فحص SIP/H.323 معطل تمامًا على جدران الحماية المعنية
3. تأكد من أن التنفيذ الفعلي الخاص بك في Expressway يتوافق مع المتطلبات التالية التي اقترحها موظفو Cisco TelePresence
تنفيذ بوابة VCS Expressway الموصى بها
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تنفيذ تكوين انعكاس ترجمة عنوان الشبكة (NAT) على أجهزة Cisco TelePresence الخاصة التي تتطلب هذا النوع من تكوين NAT على جدار الحماية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- التكوين الأساسي لـ Cisco ASA (جهاز الأمان القابل للتكيف) NAT.

- التحكم في Cisco TelePresence Video Communication Server (VCS) والتكوين الأساسي VCS Expressway.

  ملاحظة: لا يتم إستخدام هذا المستند إلا في حالة تعذر إستخدام طريقة النشر الموصى بها لواجهة VCS-Expressway أو Expressway-Edge مع كل واجهات NIC في مناطق DMZ مختلفة. لمزيد من المعلومات حول النشر الموصى به باستخدام بطاقات واجهة الشبكة (NICs) المزدوجة، يرجى التحقق من الارتباط التالي في الصفحة 60: دليل النشر Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)

المكونات المستخدمة

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

- أجهزة سلسلة Cisco ASA 5500 و 5500-X التي تشغل الإصدار 8.3 من البرنامج والإصدارات الأحدث.
- Cisco VCS الإصدار X8.x والإصدارات الأحدث.

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

ملاحظة: من خلال المستند بالكامل، تتم الإشارة إلى أجهزة VCS باسم Expressway من VCS والتحكم في VCS. ومع ذلك، ينطبق التكوين نفسه على أجهزة Expressway-E و Expressway-C.

معلومات أساسية

طبقا لوثائق Cisco TelePresence، هناك نوعان من سيناريوهات TelePresence حيث يكون قناة التحكم VCS بالاتصال بطريقة تكوين انعكاس NAT مطلوبا على FWs للسماح لعنصر تحكم VCS ExpressWay الخاص ب VCS عبر عنوان IP العام الخاص ب VCS ExpressWay.

يتضمن السيناريو الأول منطقة فرعية واحدة خالية من الأسلحة (DMZ) تستخدم واجهة VCS Expressway LAN واحدة، ويتضمن السيناريو الثاني منطقة DMZ ذات 3 منافذ FW تستخدم واجهة LAN Expressway واحدة من VCS.

تلميح: للحصول على مزيد من التفاصيل حول تنفيذ TelePresence، ارجع إلى دليل النشر Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway).

طوبولوجيا Cisco غير الموصى بها لتنفيذ تسلسل التحقق من الإطارات (VCS) C و E

من المهم ملاحظة أن المخططات التالية لا توصي بها Cisco. تتمثل منهجية النشر الموصى بها لجدار الحماية VCS Expressway أو Expressway Edge في إستخدام منطقتين DMZ مختلفتين مع Expressway المتصل بمحولات واجهة شبكة (NIC) في كل منطقة خالية من العناصر المتفجرة. يقصد بهذا الدليل أن يتم إستخدامه في البيئات التي لا يمكن فيها إستخدام أسلوب النشر الموصى به.

DMZ شبكة فرعية واحدة مع واجهة VCS Expressway LAN واحدة

في هذا السيناريو، يمكن أن يقوم FW A بتوجيه حركة المرور إلى FW B (والعكس بالعكس). يسمح الطريق السريع VCS لحركة مرور الفيديو أن تتم تمريرها من خلال FW B دون تقليل تدفق حركة المرور على FW B من الخارج إلى الواجهات الداخلية. كما يقوم الطريق السريع ل VCS بمعالجة إجتياز FW على جانبه العام.

هنا مثال من هذا السيناريو:

يستخدم هذا النشر المكونات التالية:

- DMZ شبكة فرعية واحدة (10.0.10.0/24) تحتوي على:
  الواجهة الداخلية ل FW A (10.0.10.1)الواجهة الخارجية للطراز FW B (10.0.10.2)ال LAN1 قارن من ال VCS Expressway (10.0.10.3)
- شبكة LAN فرعية (10.0.30.0/24) تحتوي على:
  الواجهة الداخلية ل FW B (10.0.30.1)ال LAN1 قارن من ال VCS تحكم (10.0.30.2)واجهة شبكة خادم إدارة نظام TelePresence (TMS) من Cisco (10.0.30.3)

شكلت ساكن إستاتيكي واحد إلى واحد NAT على FW A، أي ينجز ال NAT للعنوان العام ب VCS Expressway. ال ساكن إستاتيكي nat مكنت أسلوب عنوان من ال LAN1 إلى 64.100.0.10 ل ال LAN1 قارن على ال VCS Expressway، مع ساكن إستاتيكي nat عنوان 64.100.0.10.

> **ملاحظة**: يجب إدخال اسم المجال المؤهل بالكامل (FQDN) من Expressway ل VCS على منطقة عميل المرور الآمنة (عنوان النظير) الخاصة بالتحكم في VCS بالطريقة التي تم توجيهها بها من خارج الشبكة. السبب وراء هذا هو أن في وضع NAT الثابت، يطلب أسلوب VCS Expressway أن تم إرسال الإشارات الواردة وحركة مرور الوسائط إلى FQDN الخارجي بدلا من اسمها الخاص. وهذا يعني أيضا أن FW الخارجي يجب أن يسمح بحركة المرور من التحكم في VCS إلى VCS Expressway FQDN الخارجي. وهذا يعرف بانعكاس NAT، وقد لا يكون مدعوما من قبل جميع أنواع FWs.

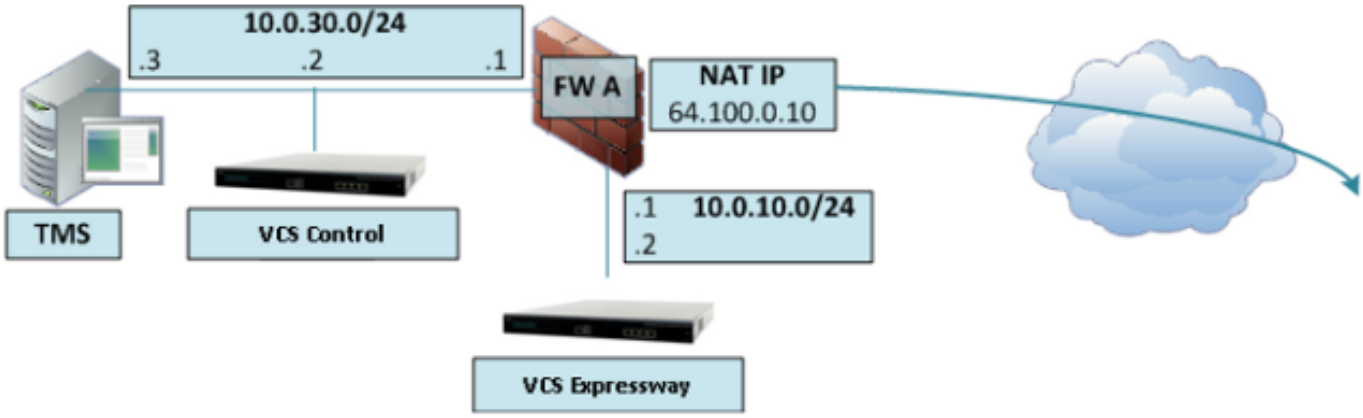
في هذا المثال، يجب أن يسمح FW B بانعكاس NAT لحركة المرور التي تأتي من عنصر التحكم في الشبكة الخاصة الظاهرية (VCS) الذي تم تعيينه لعنوان IP الخارجي (64.100.0.10) من طريق VCS السريع. يجب أن يكون لمنطقة التقاطع على عنصر تحكم VCS (بعد تحويل FQDN إلى IP) عنوان النظير 64.100.0.10.

يجب تكوين الطريق السريع VCS باستخدام بوابة افتراضية **10.0.10.1**. تعتمد ما إذا كانت FW B. قد تحدث FW A و إعدادات وإمكانيات على السيناريو هذا في مطلوبة الثابتة الموجهات الاتصال من التحكم في VCS إلى الطريق السريع VCS عبر عنوان IP 64.100.0.10 الخاص بالطريق السريع VCS؛ وقد يتعين على حركة المرور العائدة من الطريق السريع VCS إلى التحكم في VCS المرور عبر البوابة الافتراضية.

ال VCS Expressway يستطيع كنت أضفت إلى ال cisco TMS مع العنوان 10.0.10.3 (أو مع عنوان 64.100.0.10، إن يسمح FW b هذا)، بما أن ال cisco TMS إدارة إتصال ال يتأثر ب ساكن إستاتيكي nat أسلوب على ال VCS Expressway.

3-Port FW DMZ مع واجهة VCS Expressway LAN واحدة

هنا مثال من هذا سيناريو:



في هذا النشر، يتم إستخدام برنامج FW ذو الـ 3 منافذ من أجل إنشاء:

- شبكة فرعية DMZ (10.0.10.0/24) تحتوي على:
  واجهة DMZ الخاصة بـ FW A (10.0.10.1)الـ LAN1 قارن من الـ VCS Expressway (10.0.10.2)
- شبكة LAN فرعية (10.0.30.0/24) تحتوي على:
  واجهة شبكة LAN الخاصة بـ FW A (10.0.30.1)الـ LAN1 قارن من الـ VCS تحكم
  (10.0.30.2)واجهة شبكة TMS من Cisco (10.0.30.3)

شكلت ساكن إستاتيكي واحد إلى واحد NAT على FW A، أي ينجز الـ NAT من العام عنوان 64.100.0.10 إلى الـ LAN1 عنوان من الـ VCS Expressway. الـ ساكن إستاتيكي nat مكنت أسلوب الـ LAN1 قارن على الـ VCS Expressway، مع ساكن إستاتيكي nat عنوان 64.100.0.10.

يجب تكوين Expressway لـ VCS باستخدام بوابة افتراضية تبلغ 10.0.10.1. وانظر لأنه يجب إستخدام هذه البوابة لجميع حركات مرور البيانات التي تترك الطريق السريع لـ VCS، فلا يلزم وجود مسارات ثابتة في هذا النوع من النشر.

يجب تكوين منطقة عميل التقاطع على عنصر تحكم VCS باستخدام عنوان نظير يطابق عنوان NAT الثابت الخاص بـ VCS Expressway (64.100.0.10 في هذا المثال) لنفس الأسباب الموضحة في السيناريو السابق.

> **ملاحظة**: هذا يعني أن FW A يجب أن يسمح بحركة المرور من التحكم في VCS مع عنوان IP للوجهة 64.100.0.10. وهذا يعرف أيضا باعكاس NAT، وينبغي ملاحظة أن هذا لا تدعمه جميع أنواع العاملات الأجنبيات.

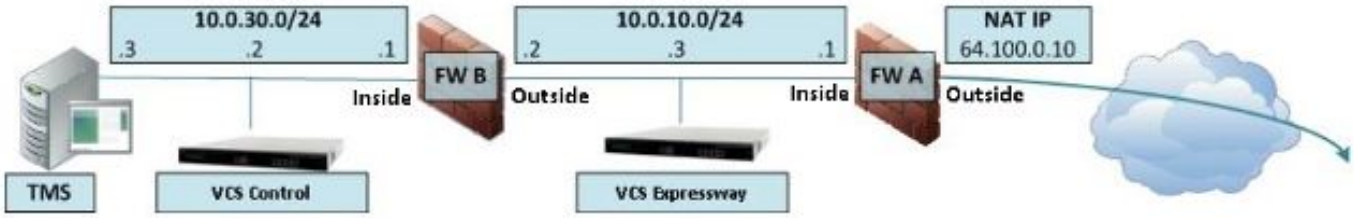
الـ VCS Expressway يستطيع كنت أضفت إلى الـ cisco TMS مع العنوان 10.0.10.2 (أو مع عنوان 64.100.0.10، إن سمح FW A هذا)، بما أن الـ cisco TMS إدارة إتصال الـ يتأثر بـ ساكن إستاتيكي nat أسلوب على الـ VCS Expressway.

التكوين

يصف هذا قسم كيف أن يشكل الـ nat انعكاس في الـ ASA لـ الإثنان مختلف VCS C و E تنفيذ سيناريو.

DMZ شبكة فرعية واحدة مع واجهة VCS Expressway LAN واحدة

للسيناريو الأول، يجب عليك تطبيق تكوين انعكاس NAT هذا على FW A للسماح بالاتصال من عنصر تحكم VCS (10.0.30.2) الموجه إلى عنوان IP الخارجي (64.100.0.10) من Expressway ل VCS:



في هذا المثال، عنوان IP الخاص بالتحكم في تسلسل التحقق من الإطارات (VCS) هو **10.0.10.3/24**. وعنوان IP الخاص ب VCS Expressway هو **10.0.30.2/24**.

إذا افترضت أن ال VCS تحكم عنوان 10.0.30.2 يبقى عندما هو يتحرك من الداخل إلى القارن خارجي من FW B عندما يبحث عن ال VCS Expressway مع الغاية عنوان 64.100.0.10، بعد ذلك ال nat انعكاس تشكيل أن أنت ينبغي طبقت على FW B أبدية في هذا مثال.

مثال على ASA الإصدارات 8.3 والإصدارات الأحدث:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.3
host 10.0.10.3

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.3

NOTE: After this NAT is applied in the ASA you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the outside interface is being redirected.
WARNING: Users may not be able to access any service enabled on the outside interface.
```

مثال لإصدارات ASA 8.2 والإصدارات الأقدم:

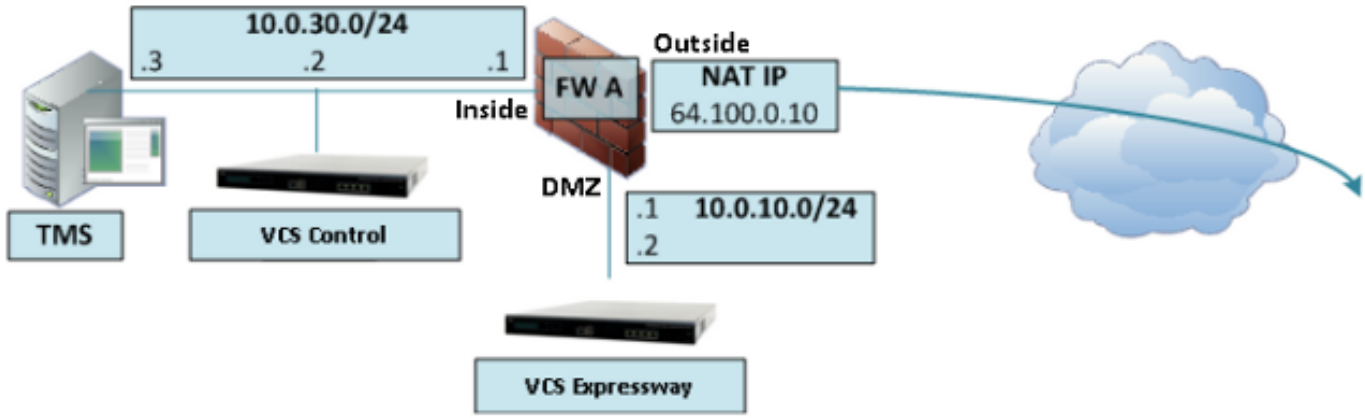
```
access-list IN-OUT-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE

access-list OUT-IN-INTERFACE extended permit ip host 10.0.10.3 host 10.0.30.2
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
```

ملاحظة: الهدف الرئيسي لتكوين انعكاس NAT هذا هو السماح لعنصر تحكم VCS بالوصول إلى الطريق السريع VCS، ولكن باستخدام عنوان IP الخاص الخاص بالطريق السريع VCS تحكم ال VCS من ال nat تشكيل للتحرك nat مع مرتين nat تشكيل بد من ال ةمجرت اذه ءانثا نوكي أن بد من عنوان IP الخاص به. إن غيرت المصدر عنوان من ال VCS تحكم السريع VCS، يظهر، ينتج عن VCS ExpressWay أن يرى حركة مرور من خاص عنوان عام، بعد ذلك خدمات الهاتف ل ال MRA أداة. اذه ليس عملية نشر مدعومة وفقا للقسم 3 في قسم التوصيات أدناه.

3-Port FW DMZ عم واجمة VCS Expressway LAN واحدة

للسيناريو الثاني، يجب تطبيق تكوين انعكاس NAT هذا على FW A للسماح بانعكاس للسيناريو الثاني، يجب تطبيق تكوين انعكاس NAT هذا على FW A للسماح بانعكاس حركة المرور الواردة من عنصر تحكم VCS 10.0.30.2 الذي يتم تعيينه إلى عنوان IP NAT الخارجي (64.100.0.10) من الطريق السريع ل VCS:



في هذا المثال، عنوان IP الخاص بالتحكم في تسلسل التحقق من الإطارات (VCS) هو **10.0.30.2/24**، وعنوان IP الخاص ب VCS Expressway هو **10.0.10.2/24**.

إذا افترضت أنا ال VCS تحكم عنوان 10.0.30.2 يبقى عندما هو يتحرك من الداخل إلى ال DMZ قارن من FW A عندما يبحث عن ال VCS Expressway مع الغاية عنوان 64.100.0.10، بعد ذلك ال nat انعكاس تشكيل أنا أنت ينبغي طبقت على FW A أبدية في هذا مثال.

مثال على ASA الإصدارات 8.3 والإصدارات الأحدث:

```
object network obj-10.0.30.2
host 10.0.30.2

object network obj-10.0.10.2
host 10.0.10.2

object network obj-64.100.0.10
host 64.100.0.10

nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination static
obj-64.100.0.10 obj-10.0.10.2

NOTE: After this NAT is applied you will receive a warning message as the following:

WARNING: All traffic destined to the IP address of the DMZ interface is being redirected.
WARNING: Users may not be able to access any service enabled on the DMZ interface.
```

مثال لإصدارات ASA 8.2 والإصدارات الأقدم:

```
access-list IN-DMZ-INTERFACE extended permit ip host 10.0.30.2 host 64.100.0.10
static (inside,DMZ) 10.0.30.2 access-list IN-DMZ-INTERFACE

access-list DMZ-IN-INTERFACE extended permit ip host 10.0.10.2 host 10.0.30.2
static (DMZ,inside) 64.100.0.10 access-list DMZ-IN-INTERFACE
```

ملاحظة: الهدف الرئيسي لتكوين انعكاس NAT هذا هو السماح لعنصر تحكم VCS بالوصول إلى الطريق السريع VCS، ولكن مع عنوان IP العام في الطريق السريع VCS. إن المصدر غير تعنون من ال VCS تحكم يكون أثناء هذا الدل من عنوان IP الخاص به. إذا كنت بحاجة إلى تشكيل nat قبل عرض، ينتج عن ترجمة nat مع مرتين nat تشكيل الدل من ال VCS ExpressWay ري حركة مرور من خاص عنوان IP، بعد ذلك خدمات الهاتف ل ال MRA أداة. هذا ليس عملية نشر مدعومة وفقا للقسم 3 في قسم التوصيات أدناه.

التحقق من الصحة

يوزي اذه قسم الربط tracer إنتاج أن أنت يستطيع رأيت في ال ASA in order to أكدت ال nat انعكاس تشكيل يعمل حسب الحاجة في كل من ال VCS C و E تنفيذ سيناريوهات.

VCS Expressway LAN واحد ةهجاو مع واحد ةيعرف ةكبش DMZ

انه ال FW B ربط tracer إنتاج ل ASA صيغة 8.3 ومتأخر:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/80 to 10.0.10.3/80

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,outside) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.3
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 2, packet dispatched to next module

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

هنا ال FW B ربط tracer إنتاج ل ASA صيغة 8.2 وما قبله:

```
FW-B# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
NAT divert to egress interface outside
Untranslate 64.100.0.10/0 to 10.0.10.3/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,outside) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 outside host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
```

```
Subtype: rpf-check
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (outside,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip outside host 10.0.10.3 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

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

3-Port FW DMZ عم اوجاه VCS Expressway LAN اوجاه

ه انا ل FW ربط tracer إنتاج ل ASA صيغة 8.3 وم أخر:

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/80 to 10.0.10.2/80

Phase: 2
```

```
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
Additional Information:
Static translate 10.0.30.2/1234 to 10.0.30.2/1234

Phase: 4
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (inside,DMZ) source static obj-10.0.30.2 obj-10.0.30.2 destination
static obj-64.100.0.10 obj-10.0.10.2
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 7, packet dispatched to next module

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

انه الـ FW a رطب tracer إنتاج لـ ASA صيغة 8.2 وما قبله:

```
FW-A# packet-tracer input inside tcp 10.0.30.2 1234 64.100.0.10 80

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:
```

```
NAT divert to egress interface DMZ
Untranslate 64.100.0.10/0 to 10.0.10.2/0 using netmask 255.255.255.255

Phase: 2
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:
Static translate 10.0.30.2/0 to 10.0.30.2/0 using netmask 255.255.255.255

Phase: 4
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (inside,DMZ) 10.0.30.2 access-list IN-OUT-INTERFACE
match ip inside host 10.0.30.2 DMZ host 64.100.0.10
static translation to 10.0.30.2
translate_hits = 1, untranslate_hits = 0
Additional Information:

Phase: 5
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 6
Type: NAT
Subtype: host-limits
Result: ALLOW
Config:
static (DMZ,inside) 64.100.0.10 access-list OUT-IN-INTERFACE
match ip DMZ host 10.0.10.2 inside host 10.0.30.2
static translation to 64.100.0.10
translate_hits = 0, untranslate_hits = 2
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
```

```
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1166, packet dispatched to next module

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

استكشاف الأخطاء وإصلاحها

تأكد من أنك تستطيع ping من ASA إلى كل جانب in order to تأكد من أن ترجمة NAT تحدث عندما يدخل الربط الجانب الداخلي وأن قواعد FW تسمح بالمرور.

تم تطبيق التقاط الحزمة لسيناريو "3-Port FW DMZ مع واجهة VCS Expressway LAN واحدة"

```
FW-A# sh cap
capture capin type raw-data interface inside [Capturing - 5735 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capdmz type raw-data interface DMZ [Capturing - 5735 bytes]
  match ip host 10.0.10.2 host 10.0.30.2
FW-A# sh cap capin

71 packets captured
   1: 22:21:37.095270 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:21:37.100672 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101313 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:21:37.114373 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157371 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:21:37.174429 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234164 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:21:39.238528 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261110 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:21:39.270234 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170614 10.0.30.2.38953 > 64.100.0.10.23: S 1841210281:1841210281(0)
win 4128 <mss 536> 12: 22:21:47.198933 64.100.0.10.23 > 10.0.30.2.38953: S
3354834096:3354834096(0)
ack 1841210282 win 4128 <mss 536> 13: 22:21:47.235186 10.0.30.2.38953 > 64.100.0.10.23: . ack
3354834097
win 4128 14: 22:21:47.242815 64.100.0.10.23 > 10.0.30.2.38953: P 3354834097:3354834109(12)
ack 1841210282 win 4128 15: 22:21:47.243014 10.0.30.2.38953 > 64.100.0.10.23: P
1841210282:1841210294(12)
ack 3354834097 win 4128 16: 22:21:47.243258 10.0.30.2.38953 > 64.100.0.10.23: . ack 3354834097
win 4128 17: 22:21:47.261094 64.100.0.10.23 > 10.0.30.2.38953: P 3354834109:3354834151(42)
ack 1841210282 win 4128 18: 22:21:47.280411 64.100.0.10.23 > 10.0.30.2.38953: P
3354834151:3354834154(3)
ack 1841210294 win 4116 19: 22:21:47.280625 64.100.0.10.23 > 10.0.30.2.38953: P
3354834154:3354834157(3)
ack 1841210294 win 4116 20: 22:21:47.280838 64.100.0.10.23 > 10.0.30.2.38953: P
3354834157:3354834163(6)
ack 1841210294 win 4116 21: 22:21:47.281082 10.0.30.2.38953 > 64.100.0.10.23: P
1841210294:1841210297(3)
ack 3354834109 win 4116 22: 22:21:47.281296 10.0.30.2.38953 > 64.100.0.10.23: P
1841210297:1841210300(3)
```

```
ack 3354834109 win 4116
FW-A# sh cap capdmz

71 packets captured
   1: 22:21:37.095621 10.0.30.2 > 10.0.10.2: icmp: echo request
   2: 22:21:37.100626 10.0.10.2 > 10.0.30.2: icmp: echo reply
   3: 22:21:37.101343 10.0.30.2 > 10.0.10.2: icmp: echo request
   4: 22:21:37.114297 10.0.10.2 > 10.0.30.2: icmp: echo reply
   5: 22:21:37.157920 10.0.30.2 > 10.0.10.2: icmp: echo request
   6: 22:21:37.174353 10.0.10.2 > 10.0.30.2: icmp: echo reply
   7: 22:21:39.234713 10.0.30.2 > 10.0.10.2: icmp: echo request
   8: 22:21:39.238452 10.0.10.2 > 10.0.30.2: icmp: echo reply
   9: 22:21:39.261659 10.0.30.2 > 10.0.10.2: icmp: echo request
  10: 22:21:39.270158 10.0.10.2 > 10.0.30.2: icmp: echo reply
  11: 22:21:47.170950 10.0.30.2.38953 > 10.0.10.2.23: S 2196345248:2196345248(0)
win 4128 <mss 536> 12: 22:21:47.198903 10.0.10.2.23 > 10.0.30.2.38953: S
1814294604:1814294604(0)
ack 2196345249 win 4128 <mss 536> 13: 22:21:47.235263 10.0.30.2.38953 > 10.0.10.2.23: . ack
1814294605 win 4128 14: 22:21:47.242754 10.0.10.2.23 > 10.0.30.2.38953: P
1814294605:1814294617(12)
ack 2196345249 win 4128 15: 22:21:47.243105 10.0.30.2.38953 > 10.0.10.2.23: P
2196345249:2196345261(12)
ack 1814294605 win 4128 16: 22:21:47.243319 10.0.30.2.38953 > 10.0.10.2.23: . ack 1814294605 win
4128 17: 22:21:47.260988 10.0.10.2.23 > 10.0.30.2.38953: P 1814294617:1814294659(42)
ack 2196345249 win 4128 18: 22:21:47.280335 10.0.10.2.23 > 10.0.30.2.38953: P
1814294659:1814294662(3)
ack 2196345261 win 4116 19: 22:21:47.280564 10.0.10.2.23 > 10.0.30.2.38953: P
1814294662:1814294665(3)
ack 2196345261 win 4116 20: 22:21:47.280777 10.0.10.2.23 > 10.0.30.2.38953: P
1814294665:1814294671(6)
ack 2196345261 win 4116 21: 22:21:47.281143 10.0.30.2.38953 > 10.0.10.2.23: P
2196345261:2196345264(3)
ack 1814294617 win 4116 22: 22:21:47.281357 10.0.30.2.38953 > 10.0.10.2.23: P
2196345264:2196345267(3)
ack 1814294617 win 4116
```

يتم تطبيق التقاط الحزمة لسيناريو "الشبكة الفرعية المفردة DMZ مع واجهة VCS Expressway LAN المفردة"

```
FW-B# sh cap
capture capin type raw-data interface inside [Capturing - 5815 bytes]
  match ip host 10.0.30.2 host 64.100.0.10
capture capout type raw-data interface outside [Capturing - 5815 bytes]
  match ip host 10.0.10.3 host 10.0.30.2

FW-B# sh cap capin

72 packets captured
   1: 22:30:06.783681 10.0.30.2 > 64.100.0.10: icmp: echo request
   2: 22:30:06.847856 64.100.0.10 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.877624 10.0.30.2 > 64.100.0.10: icmp: echo request
   4: 22:30:06.900710 64.100.0.10 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.971598 10.0.30.2 > 64.100.0.10: icmp: echo request
   6: 22:30:06.999551 64.100.0.10 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.075649 10.0.30.2 > 64.100.0.10: icmp: echo request
   8: 22:30:07.134499 64.100.0.10 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156409 10.0.30.2 > 64.100.0.10: icmp: echo request
  10: 22:30:07.177496 64.100.0.10 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.802525 10.0.30.2.41596 > 64.100.0.10.23: S 1119515693:1119515693(0)
win 4128 <mss 536> 12: 22:30:13.861100 64.100.0.10.23 > 10.0.30.2.41596: S
2006020203:2006020203(0)
ack 1119515694 win 4128 <mss 536> 13: 22:30:13.935864 10.0.30.2.41596 > 64.100.0.10.23: . ack
```

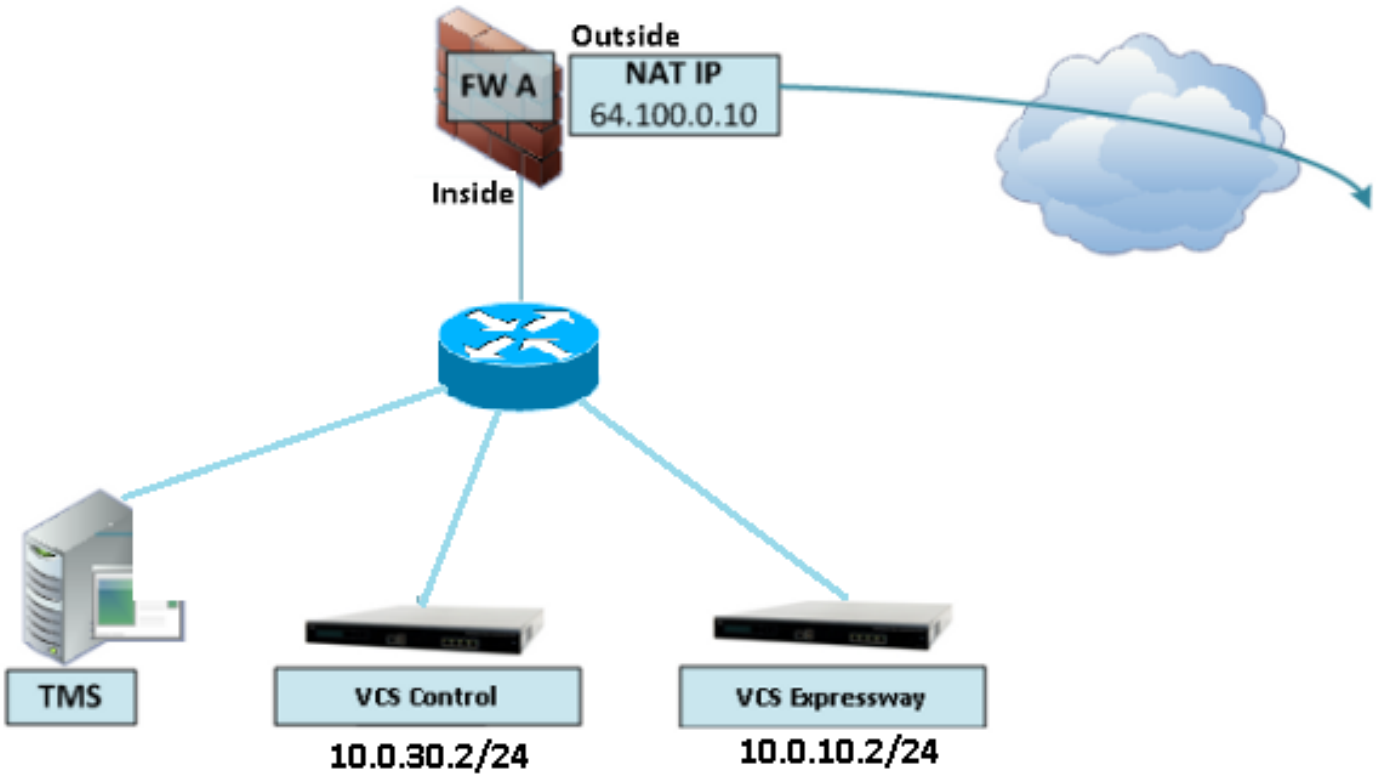
```
2006020204 win 4128 14: 22:30:13.946804 10.0.30.2.41596 > 64.100.0.10.23: P
1119515694:1119515706(12)
ack 2006020204 win 4128 15: 22:30:13.952679 10.0.30.2.41596 > 64.100.0.10.23: . ack 2006020204
win 4128 16: 22:30:14.013686 64.100.0.10.23 > 10.0.30.2.41596: P 2006020204:2006020216(12)
ack 1119515706 win 4116 17: 22:30:14.035352 64.100.0.10.23 > 10.0.30.2.41596: P
2006020216:2006020256(40)
ack 1119515706 win 4116 18: 22:30:14.045758 64.100.0.10.23 > 10.0.30.2.41596: P
2006020256:2006020259(3)
ack 1119515706 win 4116 19: 22:30:14.046781 64.100.0.10.23 > 10.0.30.2.41596: P
2006020259:2006020262(3)
ack 1119515706 win 4116 20: 22:30:14.047788 64.100.0.10.23 > 10.0.30.2.41596: P
2006020262:2006020268(6)
ack 1119515706 win 4116 21: 22:30:14.052151 10.0.30.2.41596 > 64.100.0.10.23: P
1119515706:1119515709(3)
ack 2006020256 win 4076 22: 22:30:14.089183 10.0.30.2.41596 > 64.100.0.10.23: P
1119515709:1119515712(3)
ack 2006020256 win 4076
ASA1# show cap capout

72 packets captured
   1: 22:30:06.784871 10.0.30.2 > 10.0.10.3: icmp: echo request
   2: 22:30:06.847688 10.0.10.3 > 10.0.30.2: icmp: echo reply
   3: 22:30:06.878769 10.0.30.2 > 10.0.10.3: icmp: echo request
   4: 22:30:06.900557 10.0.10.3 > 10.0.30.2: icmp: echo reply
   5: 22:30:06.972758 10.0.30.2 > 10.0.10.3: icmp: echo request
   6: 22:30:06.999399 10.0.10.3 > 10.0.30.2: icmp: echo reply
   7: 22:30:07.076808 10.0.30.2 > 10.0.10.3: icmp: echo request
   8: 22:30:07.134422 10.0.10.3 > 10.0.30.2: icmp: echo reply
   9: 22:30:07.156959 10.0.30.2 > 10.0.10.3: icmp: echo request
  10: 22:30:07.177420 10.0.10.3 > 10.0.30.2: icmp: echo reply
  11: 22:30:13.803104 10.0.30.2.41596 > 10.0.10.3.23: S 2599614130:2599614130(0)
win 4128 <mss 536> 12: 22:30:13.860947 10.0.10.3.23 > 10.0.30.2.41596: S
4158597009:4158597009(0)
ack 2599614131 win 4128 <mss 536> 13: 22:30:13.936017 10.0.30.2.41596 > 10.0.10.3.23: . ack
4158597010 win 4128 14: 22:30:13.946941 10.0.30.2.41596 > 10.0.10.3.23: P
2599614131:2599614143(12)
ack 4158597010 win 4128 15: 22:30:13.952801 10.0.30.2.41596 > 10.0.10.3.23: . ack 4158597010 win
4128 16: 22:30:14.013488 10.0.10.3.23 > 10.0.30.2.41596: P 4158597010:4158597022(12)
ack 2599614143 win 4116 17: 22:30:14.035108 10.0.10.3.23 > 10.0.30.2.41596: P
4158597022:4158597062(40)
ack 2599614143 win 4116 18: 22:30:14.045377 10.0.10.3.23 > 10.0.30.2.41596: P
4158597062:4158597065(3)
ack 2599614143 win 4116 19: 22:30:14.046384 10.0.10.3.23 > 10.0.30.2.41596: P
4158597065:4158597068(3)
ack 2599614143 win 4116 20: 22:30:14.047406 10.0.10.3.23 > 10.0.30.2.41596: P
4158597068:4158597074(6)
ack 2599614143 win 4116 21: 22:30:14.052395 10.0.30.2.41596 > 10.0.10.3.23: P
2599614143:2599614146(3)
ack 4158597062 win 4076 22: 22:30:14.089427 10.0.30.2.41596 > 10.0.10.3.23: P
2599614146:2599614149(3)
ack 4158597062 win 4076
```

التوصيات

1. تجنب تنفيذ أي مخطط غير مدعوم

عند استخدام VCS Expressway و VCS، إذا كان لديك أي عنصر تحكم متصل خلف جهاز ASA الداخلية، كما هو موضح في هذا السيناريو:



يتطلب هذا النوع من التنفيذ ترجمة عنوان IP الخاص بالتحكم في VCS إلى عنوان IP الداخلي الخاص ب ASA لإجبار حركة المرور العائدة على العودة إلى ASA لتجنب مشاكل المسار غير المتماثل لعكس NAT.

ملاحظة: إذا تم تغيير عنوان IP المصدر الخاص بعنصر التحكم في تسلسل التحقق من الشبكة (VCS) أثناء ترجمة أداة التحكم في الشبكة (NAT) هذه بتكوين مزدوج لبطاقة واجهة الشبكة (NAT) بدلا من تكوين انعكاس NAT المقترح، بعد ذلك سيرى ExpressWay من VCS حركة مرور البيانات من عنوان IP العام الخاص به، ثم لن يتم عرض خدمات الهاتف لأجهزة MRA. هذا ليس عملية نشر مدعومة وقفا للقسم 3 في قسم التوصيات أدناه.

ومع ذلك، يوصى بشدة بتنفيذ الطريق السريع VCS [كتنفيذ لواجهات شبكة](#) Expressway-E المزدوجة بدلا من بطاقة واجهة الشبكة (NIC) الفردية مع انعكاس nat.

2. 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 وأ 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
```

3. تأكد من أن التنفيذ الفعلي الخاص بك في Expressway يتوافق مع المتطلبات التالية

التي اقترحها مطورو Cisco TelePresence

- تكوين NAT بين Expressway-C و Expressway-E غير مدعوم.
- لا يتم دعمه عندما يقوم Expressway-C و Expressway-E، بتوصيل NATed إلى نفس عنوان IP العام، على سبيل المثال:
  يتم تكوين Expressway-C باستخدام عنوان IP 10.1.1.1
  Expressway-E لديه بطاقة واجهة شبكة (NIC) واحدة تم تكوينها باستخدام عنوان IP 10.2.2.1 وتم تكوين بطاقة واجهة شبكة (NAT) ثابتة في جدار الحماية باستخدام عنوان IP العام 64.100.0.10
  بعد ذلك، لا يمكن إستخدام Expressway-C مع NATs لنفس العنوان العام 64.100.0.10

تنفيذ VCS Expressway الموصى به

يعد التنفيذ الموصى به للطريقة السريعة VCS بدلا من الطريق السريع ل VCS مع تكوين انعكاس NAT وه تنفيذ الطريق السريع لواجهات الشبكة المزدوجة/تقنية NIC VCS المزدوجة، للحصول على مزيد من المعلومات، يرجى التحقق من الارتباط التالي.

تكوين ASA nat والتوصيات الخاصة بتنفيذ واجهات شبكة Expressway-E المزدوجة.

معلومات ذات صلة

- تكوين ASA nat والتوصيات الخاصة بتنفيذ واجهات شبكة Expressway-E المزدوجة
- دليل النشر Cisco TelePresence Video Communication Server Basic Configuration (Control with Expressway)
- إستخدام منفذ Expressway IP من Cisco لمرور الجدار الناري
- وضع Cisco VCS ExpressWay في المنطقة المنزوعة السلاح بدلا من وضعه في الإنترنت العام

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).