إستخدام بيان NAT و PAT على مثال تكوين جدار حماية Cisco Secure ASA

المحتويات

المقدمة

يزود هذا وثيقة مثال من أساسي شبكة عنوان ترجمة (NAT) وميناء عنوان ترجمة (PAT) تشكيل على ال cisco يأمن أمن مهايئ جهاز أمن (ASA) جدار حماية. كما يوفر هذا المستند مخططات شبكة مبسطة. ارجع إلى وثائق ASA الخاصة بإصدار برنامج ASA لديك للحصول على مزيد من المعلومات التفصيلية.

يقدم هذا المستند تحليلا مخصصا لجهاز Cisco لديك.

راجع تكوين NAT على ASA في أجهزة الأمان ASA 5500/5500-X Series للحصول على مزيد من المعلومات.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بجدار حماية Cisco Secure ASA.

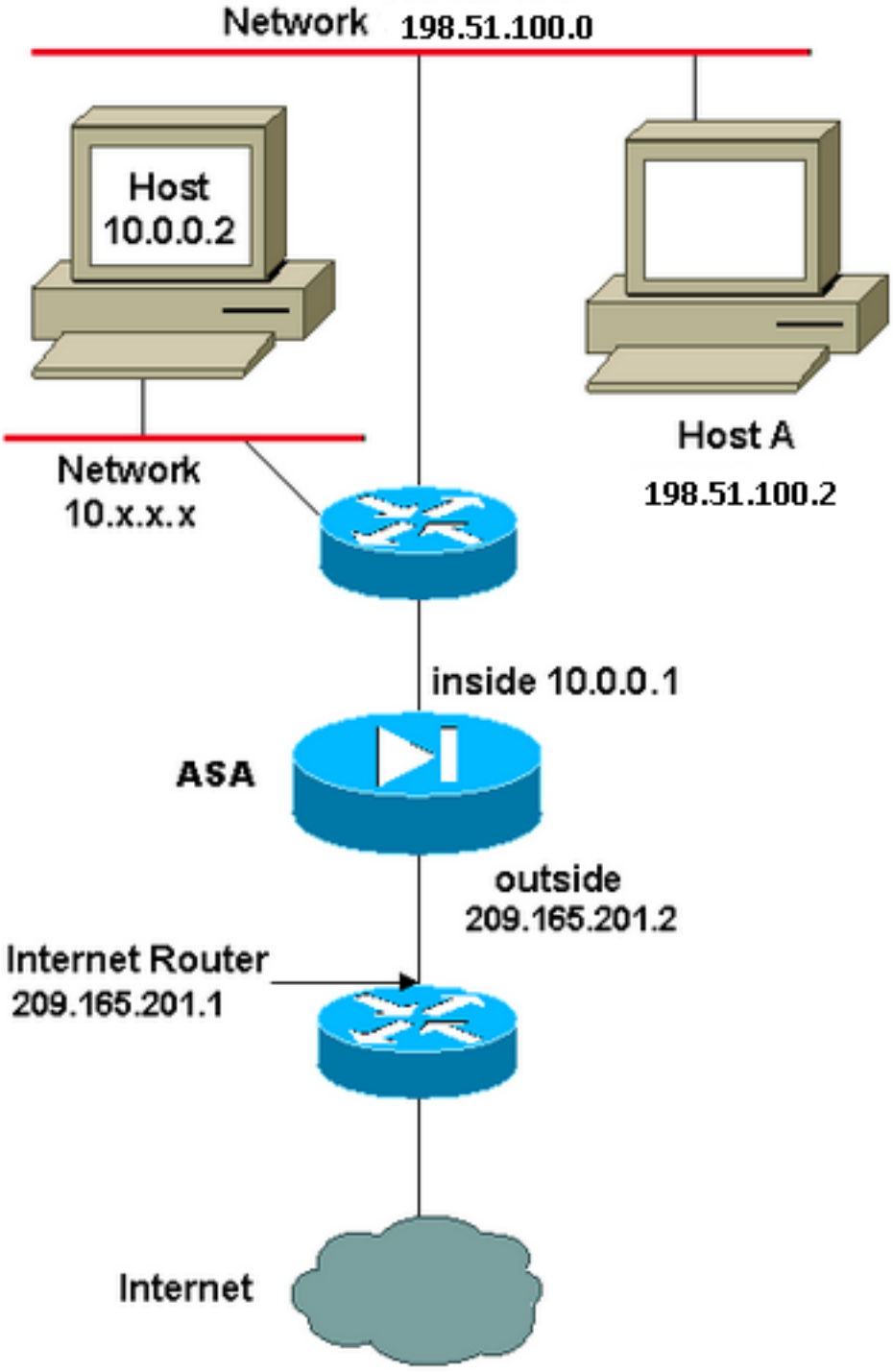
المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى برنامج جدار حماية Cisco Secure ASA الإصدار 8.4.2 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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تكوين - عبارات NAT متعددة باستخدام NAT اليدوي والتلقائي

الرسم التخطيطي للشبكة



في هذا المثال، يوفر ISP لمدير الشبكة كتلة عنوان IP 209.165.201.0/27 التي تتراوح من 209.165.201.1 إلى 209.165.201.30. يقرر مدير الشبكة تخصيص 209.165.201.1 للواجهة الداخلية على موجه الإنترنت، و 209.165.201.2 للواجهة الخارجية ل ASA.

مدير الشبكة لديه بالفعل عنوان من الفئة C معين للشبكة، 24/198.51.100.0، ولديه بعض محطات العمل التي تستخدم هذه العناوين للوصول إلى الإنترنت. لا تتطلب محطات العمل هذه أي ترجمة عناوين لأنها تحتوي بالفعل على عناوين صالحة. ومع ذلك، يتم تعيين عناوين لمحطات العمل الجديدة في شبكة 8/10.0.0.0 ويجب ترجمتها (لأن x.x.x.10 هي إحدى مساحات العناوين غير الموجهة لكل RFC 1918 .

in order to استعملت هذا شبكة تصميم، الشبكة مدير ينبغي استعملت إثنان nat عبارة وواحد شامل بركة في ال ASA تشكيل:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
nat (inside) 1 10.0.0.0 255.0.0.0 0 0
```

لا يترجم هذا تشكيل عنوان المصدر لأي حركة مرور صادرة من الشبكة 24/198.51.100.0. وهو يترجم عنوان مصدر في شبكة 8/10.0.0.0 إلى عنوان من النطاق 209.165.201.3 إلى 209.165.201.30.

ملاحظة: عندما يكون لديك واجهة مع سياسة NAT وإذا لم يكن هناك تجمع عالمي لواجهة أخرى، يلزمك إستخدام 0 NAT لإعداد إستثناء NAT.

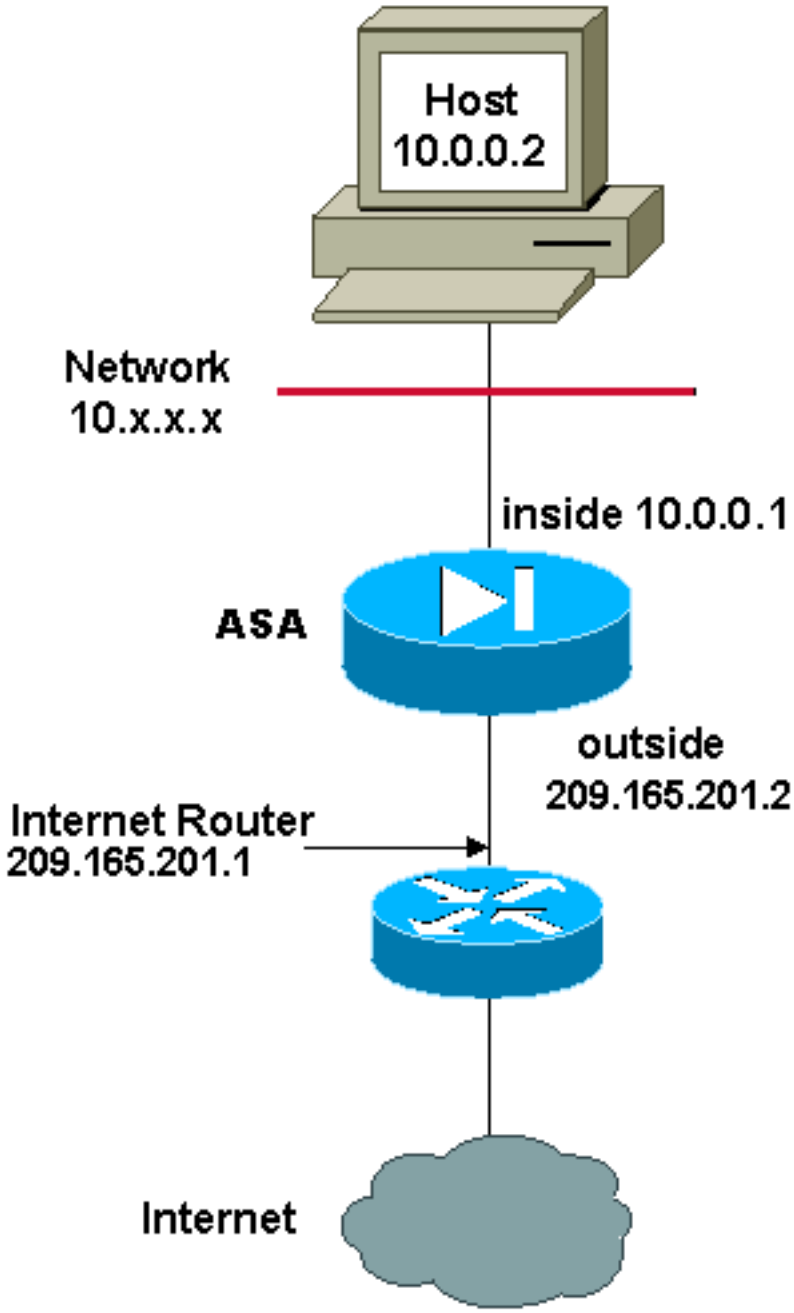
ASA الإصدار 8.3 والإصدارات الأحدث

هنا التكوين.

```
object network obj-10.0.0.0/8
 subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
 subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

object network any-1
subnet 0.0.0.0 0.0.0.0

Using the Manual Nat statements:

nat (inside,outside) source static obj-198.51.100.0/24 obj-198.51.100.0/24
destination static any-1 any-1

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted

Using the Auto Nat statements:

object network obj-10.0.0.0/8
 subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted

object network obj-198.51.100.0/24
 subnet 198.51.100.0 255.255.255.0
nat (inside,outside) static obj-198.51.100.0/24
```

التكوين - تجمعات عمومية متعددة

الرسم التخطيطي للشبكة



في هذا المثال، تحتوي إدارة الشبكة على نطاقات من عناوين IP المسجلة على الإنترنت. يجب على مدير الشبكة تحويل جميع العناوين الداخلية الموجودة في نطاق 8/10.0.0.0 إلى عناوين مسجلة. نطاقات عناوين IP التي يجب أن يستخدمها مدير الشبكة هي 209.165.201.1 حتى 209.165.201.30 و 209.165.200.225 حتى 209.165.200.254. يمكن لمدير الشبكة القيام بذلك باستخدام:

```
global (outside) 1 209.165.201.3-209.165.201.30 netmask 255.255.255.224
global (outside) 1 209.165.200.225-209.165.200.254 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

ملاحظة: يتم إستخدام مخطط عنونة حرف بدل في عبارة NAT. هذا البيان يقول ال ASA ان يترجم أي مصدر داخلي عنوان عندما يذهب إلى الإنترنت. يمكن أن يكون العنوان في هذا الأمر أكثر تحديدا إذا كان مطلوبا.

ASA الإصدار 8.3 والإصدارات الأحدث

هنا التكوين.

```
object network obj-natted
range 209.165.201.3 209.165.201.30

object network obj-natted-2
range 209.165.200.225 209.165.200.254

object network any-1
subnet 0.0.0.0 0.0.0.0
```

:Using the Manual Nat statements

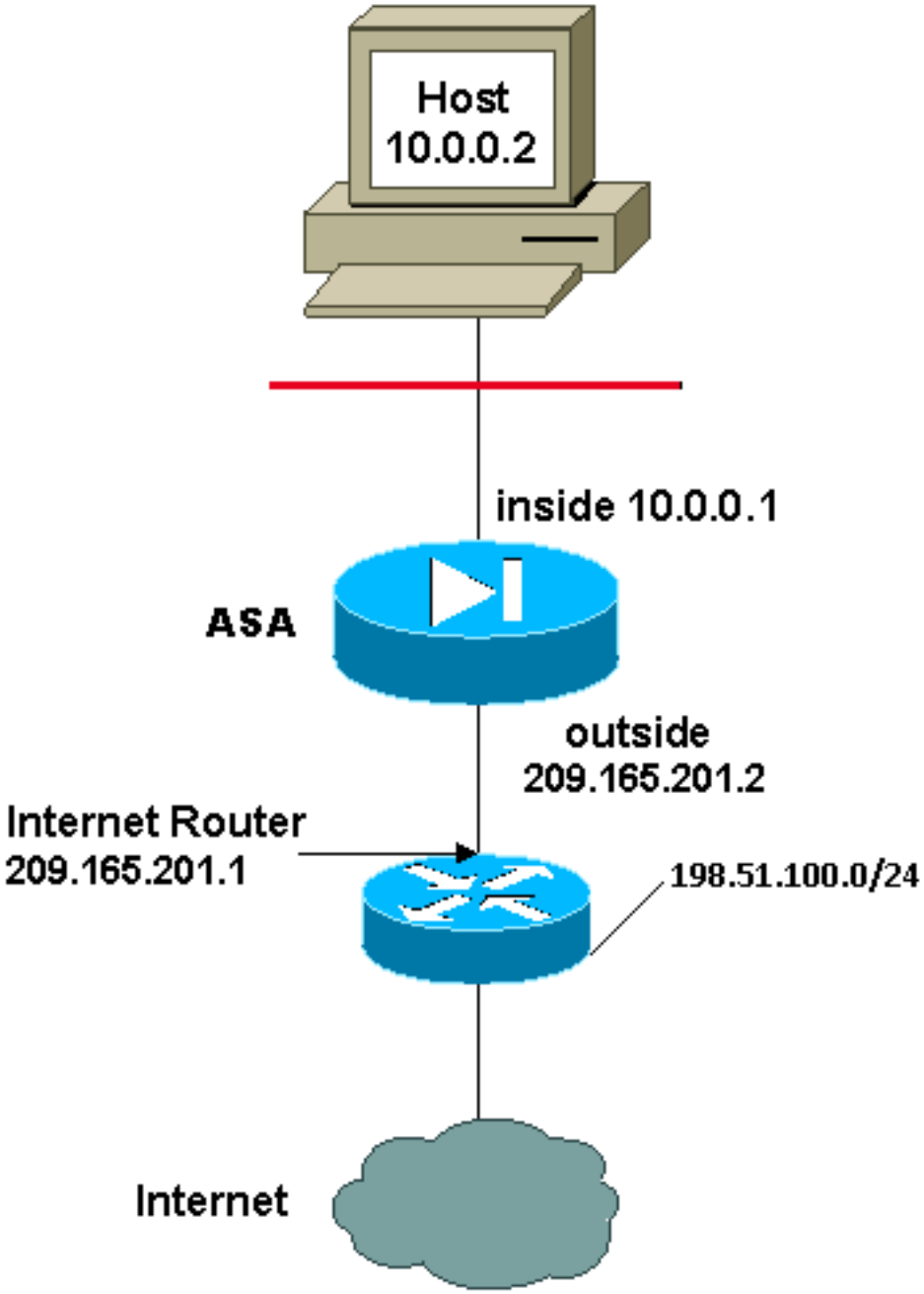
```
nat (inside,outside) source dynamic any-1 obj-natted
nat (inside,outside) source dynamic any-1 obj-natted-2
```

:Using the Auto Nat statements

```
object network any-1
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted

object network any-2
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic obj-natted-2
```

التكوين - مزج عبارات NAT و PAT

الرسم التخطيطي للشبكة



في هذا المثال، يوفر ISP مدير الشبكة بنطاق من العناوين من 209.165.201.1 إلى 209.165.201.30 للشركة لاستخدامها. قرر مدير الشبكة إستخدام 209.165.201.1 للواجهة الداخلية على موجه الإنترنت و 209.165.201.2 للواجهة الخارجية على ASA. يتبقى لديك بعد ذلك 209.165.201.3 إلى 209.165.201.30 للاستخدام لتجمع NAT. ومع ذلك، فإن مدير الشبكة يعرف أنه يمكن أن يكون هناك في أي وقت أكثر من 28 شخصا يحاولون الخروج من منطقة التخزين المؤقت. قرر مدير الشبكة أخذ 209.165.201.30 وجعله عنوان PAT بحيث يمكن للعديد من المستخدمين مشاركة عنوان واحد في نفس الوقت.

ترشد هذه الأوامر ASA لترجمة عنوان المصدر إلى 209.165.201.3 حتى 209.165.201.29 لأول 27 مستخدما داخليا للتمرير عبر ASA. بعد استنفاد هذه العناوين، بعد ذلك يترجم ال ASA كل مصدر عنوان إلى 209.165.201.30 حتى يصبح واحد من العنوان في ال nat بركة حر.

ملاحظة: يتم إستخدام مخطط عنونة حرف بدل في عبارة NAT. هذا البيان يقول ال ASA ان يترجم أي مصدر داخلي عنوان عندما يذهب إلى الإنترنت. يمكن أن يكون العنوان في هذا الأمر أكثر تحديدا إذا كان مطلوبا.

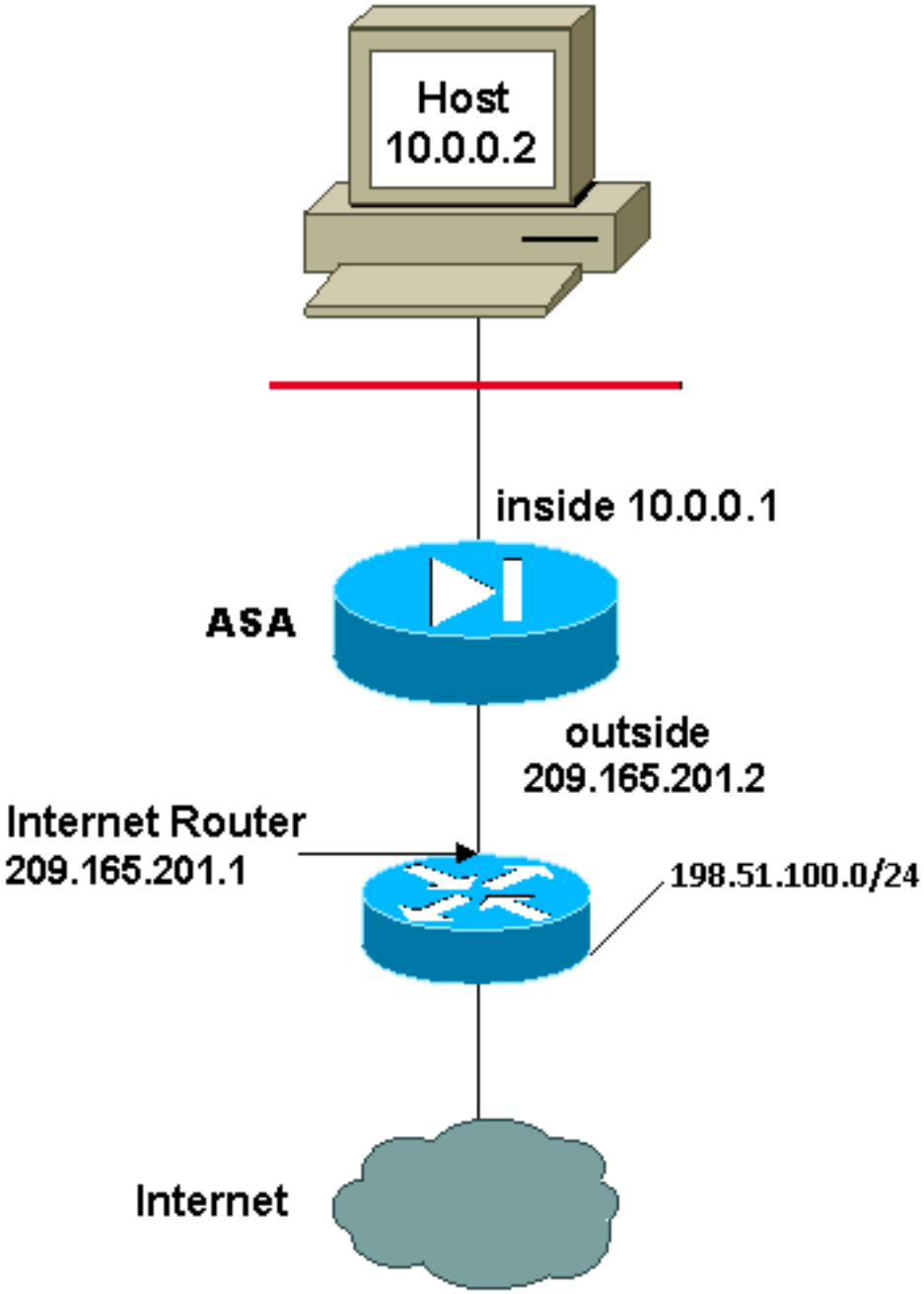
ASA الإصدار 8.3 والإصدارات الأحدث

هنا التكوين.

```
:Using the Manual Nat statements
                object network any-1
             subnet 0.0.0.0 0.0.0.0

                object network obj-natted
           range 209.165.201.3 209.165.201.30

                object network obj-natted-2
           subnet 209.165.201.30 255.255.255.224

  nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted
nat (inside,outside) source dynamic 0.0.0.0/0 obj-natted-2

:Using the Auto Nat statements

                object network any-1
             subnet 0.0.0.0 0.0.0.0
    nat (inside,outside) dynamic obj-natted

                object network any-2
             subnet 0.0.0.0 0.0.0.0
    nat (inside,outside) dynamic obj-natted-2
```

التكوين - عبارات NAT المتعددة ذات الكشوف اليدوية

الرسم التخطيطي للشبكة



في هذا المثال، يوفر ISP مرة أخرى مدير الشبكة بنطاق من العناوين من 209.165.201.1 إلى 209.165.201.30. يقرر مدير الشبكة تخصيص 209.165.201.1 للواجهة الداخلية على موجه الإنترنت و 209.165.201.2 للواجهة الخارجية ل ASA.

ومع ذلك، في هذا السيناريو، يتم طرح مقطع آخر من شبكة LAN الخاصة خارج موجه الإنترنت. يفضل مدير الشبكة عدم هدر العناوين من التجمع العالمي عندما يتحدث المضيفون في هاتين الشبكتين مع بعضهم البعض. لا يزال مدير الشبكة بحاجة إلى ترجمة عنوان المصدر لجميع المستخدمين الداخليين (8/10.0.0.0) عند خروجه إلى الإنترنت.

لا يترجم هذا تشكيل هذا عنوان أن مع مصدر عنوان 8/10.0.0.0 وغاية عنوان 24/198.51.100.0. وهو يترجم عنوان المصدر من أي حركة مرور تبدأ من داخل شبكة 8/10.0.0.0 وتكون موجهة إلى أي مكان آخر غير 24/198.51.100.0 إلى عنوان من النطاق 209.165.201.3 إلى 209.165.201.30.

إن يتلقى أنت الإنتاج من **كتابة terminal** أمر من ك cisco أداة، أنت يستطيع استعملت الإنتاج مترجم أداة (يسجل زبون فقط).

ASA الإصدار 8.3 والإصدارات الأحدث

هنا التكوين.

:Using the Manual Nat statements

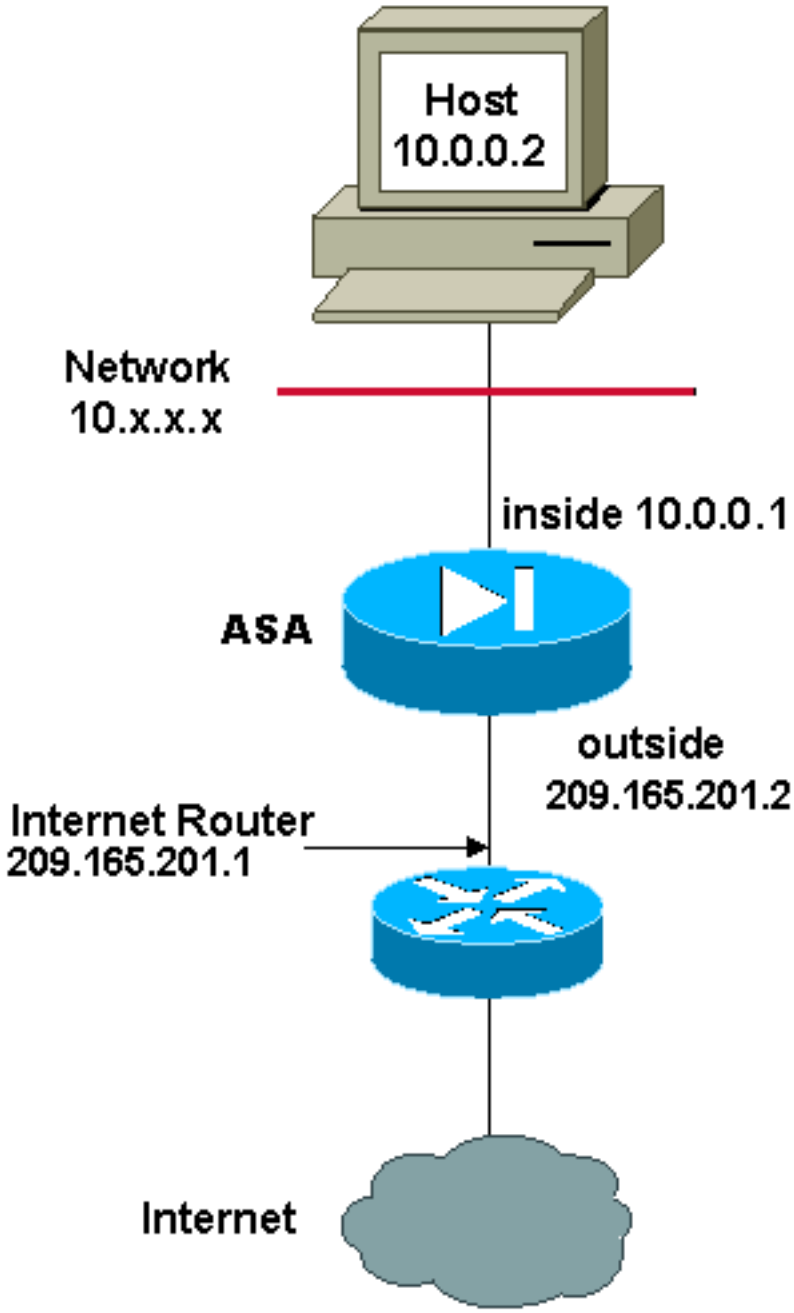
```
object network obj-10.0.0.0/8
    subnet 10.0.0.0 255.0.0.0

object network obj-198.51.100.0/24
 subnet 198.51.100.0 255.255.255.0

object network obj-natted
range 209.165.201.3 209.165.201.30

nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
                                static obj-198.51.100.0/24 obj-198.51.100.0/24

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-natted
```

:Using the Auto Nat statements

```
object network obj-natted
range 209.165.201.3 209.165.201.30
nat (inside,outside) source static obj-10.0.0.0/8 obj-10.0.0.0/8 destination
                                static obj-198.51.100.0/24 obj-198.51.100.0/24

object network obj-10.0.0.0/8
    subnet 10.0.0.0 255.0.0.0
nat (inside,outside) dynamic obj-natted
```

التكوين - إستخدام سياسة NAT

الرسم التخطيطي للشبكة



عندما يستعمل أنت منفذ قائمة مع ال **nat** أمر ل أي nat id آخر غير 0، أنت يمكن سياسة nat.

يسمح سياسة nat أنت أن يعين حركة مرور محلي لعنوان ترجمة بمواصفة من المصدر والوجهة عنوان (أو ميناء) في قائمة منفذ. يستعمل NAT عادي مصدر عنوان/ميناء فقط. يستعمل سياسة nat على حد سواء مصدر وغاية عنوان/ميناء.

ملاحظة: جميع أنواع NAT الخاصة بدعم سياسة دعم NAT باستثناء إستثناء access-list (nat 0 NAT). يستخدم إستثناء NAT قائمة التحكم في الوصول (ACL) لتحديد العناوين المحلية، ولكنه يختلف عن NAT الخاص بالسياسة نظرا لعدم إعتبار المنافذ.

مع سياسة nat، أنت يستطيع خلقت يتعدد nat أو جمل ساكن إستاتيكي أن يعين ال نفسه عنوان محلي بما أن المصدر/ميناء وغاية/ميناء خليط فريد لكل جملة. أنت يستطيع بعد ذلك طابقت عنوان مختلف إلى كل مصدر/ميناء وغاية/ميناء زوج.

في هذا مثال، الشبكة مدير أن يزود منفذ للغاية عنوان 172.30.1.11 لميناء 80 (ويب) وميناء 23 (telnet)، غير أن ينبغي استعملت إثنان مختلف عنوان كمصدر عنوان. يتم إستخدام 209.165.201.3 كعنوان مصدر للويب ويتم إستخدام 209.165.201.4 ل Telnet، ويجب أن يقوم بتحويل جميع العناوين الداخلية، الموجودة في نطاق 8/10.0.0.0. يمكن

لمدير الشبكة القيام بذلك باستخدام:

```
access-list WEB permit tcp 10.0.0.0 255.0.0.0
                                    eq 80 255.255.255.255 172.30.1.11
access-list TELNET permit tcp 10.0.0.0 255.0.0.0 172.30.1.11
                                    eq 23 255.255.255.255

                                       nat (inside) 1 access-list WEB
                                    nat (inside) 2 access-list TELNET
                              global (outside) 1 209.165.201.3 255.255.255.224
                              global (outside) 2 209.165.201.4 255.255.255.224
```

ASA الإصدار 8.3 والإصدارات الأحدث

هنا التكوين.

```
                                    :Using the Manual Nat statements

                                       object network obj-10.0.0.0/8
                                           subnet 10.0.0.0 255.0.0.0

                                     object network obj-172.30.1.11
                                                  host 172.30.1.11

                                   object network obj-209.165.201.3
                                                host 209.165.201.3

                                   object network obj-209.165.201.4
                                                host 209.165.201.4

                                              object service obj-23
                                  service tcp destination eq telnet

                                              object service obj-80
                                  service tcp destination eq telnet

nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.3 destination
                        static obj-172.30.1.11 obj-172.30.1.11 service obj-80 obj-80
nat (inside,outside) source dynamic obj-10.0.0.0/8 obj-209.165.201.4 destination
                        static obj-172.30.1.11 obj-172.30.1.11 service obj-23 obj-23
```

ملاحظة: للحصول على مزيد من المعلومات حول تكوين NAT و PAT على ASA الإصدار 8.4، ارجع إلى المعلومات حول NAT.

للحصول على مزيد من المعلومات حول تكوين قوائم الوصول في الإصدار 8.4 من ASA، ارجع إلى معلومات حول قوائم الوصول.

التحقق من الصحة

حاول الوصول إلى موقع ويب عبر HTTP باستخدام مستعرض ويب. يستخدم هذا المثال موقعا يتم إستضافته في 198.51.100.100. إذا نجح الاتصال، يمكن رؤية الإخراج في القسم التالي على واجهة سطر الأوامر (CLI) الخاصة ب ASA.

الاتصال

```
ASA(config)# show connection address 10.0.0.2
in use, 19 most used 16
,TCP outside 198.51.100.100:80 inside 10.0.0.2:57431, idle 0:00:06, bytes 9137
flags UIO
```

ASA هو جدار حماية ذو حالة، ويتم السماح لحركة مرور البيانات العائدة من خادم الويب عبر جدار الحماية لأنه يطابق ***اتصالا*** في جدول اتصال جدار الحماية. يسمح بحركة المرور التي تطابق اتصال موجود مسبقا من خلال جدار الحماية دون أن يتم حظرها بواسطة قائمة التحكم في الوصول (ACL) للواجهة.

في الإخراج السابق، قام العميل الموجود على الواجهة الداخلية بإنشاء اتصال بالمضيف 198.51.100.100 الموجود خارج الواجهة. يتم إجراء هذا الاتصال باستخدام بروتوكول TCP وقد كان خاملا لمدة ست ثوان. تشير علامات الاتصال إلى الحالة الحالية لهذا الاتصال. يمكن العثور على مزيد من المعلومات حول علامات الاتصال في علامات اتصال ASA TCP.

Syslog

```
ASA(config)# show log | in 10.0.0.2

:Jun 28 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside
to outside:209.165.201.3/57431 10.0.0.2/57431

:Jun 28 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside
(to inside:10.0.0.2/57431 (209.165.201.3/57431 (198.51.100.100/80) 198.51.100.100/80
```

يقوم جدار حماية ASA بإنشاء syslog أثناء التشغيل العادي. نطاق syslogs في النطاق الترددي استنادا إلى تكوين التسجيل. يظهر الإنتاج إثنان syslog أن يكون رأيت على المستوى ستة، أو **'information'** مستوى.

في هذا مثال، هناك إثنان syslog ولدت. الأولى هي رسالة سجل تشير إلى أن جدار الحماية قام بإنشاء **ترجمة**، وخاصة ترجمة TCP ديناميكية (PAT). هو يشير المصدر عنوان ومنفذ وال يترجم عنوان ومنفذ بما أن الحركة مرور يعبر من الداخل إلى الواجهات الخارجية.

ويشير syslog الثاني إلى أن جدار الحماية قام بإنشاء **اتصال** في جدول الاتصال الخاص به لحركة المرور المحددة بين العميل والخادم. إذا تم تكوين جدار الحماية لحظر محاولة الاتصال هذه، أو قام عامل آخر بمنع إنشاء هذا الاتصال (قيود الموارد أو احتمال حدوث خطأ في التكوين)، فلن يقوم جدار الحماية بإنشاء سجل يشير إلى إنشاء الاتصال. وبدلا من ذلك، سيقوم بتسجيل سبب رفض الاتصال أو مؤشر على العامل الذي منع إنشاء الاتصال.

ترجمات (NAT (Xlate

```
ASA(config)# show xlate local 10.0.0.2
1in use, 810 most used 3
,Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.0.0.2/58799 to outside:209.165.201.3/57431 flags ri idle
timeout 0:00:30 0:12:22
```

كجزء من هذا تشكيل، شكلت ضرب in order to ترجمت الداخلي مضيف عنوان إلى عنوان أن يكون routable على الإنترنت. in order to أكدت أن هذا ترجمة يكون خلقت، أنت يستطيع فحصت ال xlate (ترجمة) طاولة. يعرض الأمر **show xlate** ، عند دمجه مع الكلمة الأساسية **المحلية** وعنوان IP للمضيف الداخلي، جميع الإدخالات الموجودة في جدول الترجمة لذلك المضيف. تظهر المخرجات السابقة أن هناك ترجمة بنيت حاليا لهذا المضيف بين الواجهات الداخلية والخارجية. ترجمت المضيف الداخلي IP والمنفذ إلى العنوان 10.165.200.226 لكل تكوين.

تشير العلامات المدرجة، **r i**، إلى أن الترجمة **ديناميكية** و**portMap**. يمكن العثور على مزيد من المعلومات حول تكوينات NAT المختلفة في المعلومات حول NAT.

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).