PIX/ASA 7.x: تمكين/تعطيل الاتصال بين الواجهات

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين أشكال الاتصال المختلفة بين الواجهات على جهاز أمان ASA/PIX.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- عناوين IP وتعيين البوابة الافتراضية
- اتصال الشبكة الفعلي بين الأجهزة
- تم تحديد منفذ الاتصال # للخدمة التي تم تنفيذها

المكونات المستخدمة

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

- جهاز الأمان القابل للتكيف الذي يشغل الإصدار x.7 من البرنامج والإصدارات الأحدث
- خوادم Windows 2003
- محطات عمل Windows XP

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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع إصدارات الأجهزة والبرامج التالية:

- جدران الحماية من الجيل التالي طراز PIX 500 التي تعمل بنظام التشغيل x.7 والإصدارات الأحدث

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

معلومات أساسية

يوضح هذا المستند الخطوات المطلوبة للسماح بتدفق الاتصال بين الواجهات المختلفة. وتناقش اشكال الاتصال كهذه:

1. الاتصال من البيئات المضيفة الموجودة على الخارج التي تتطلب الوصول إلى الموارد الموجودة في المنطقة المنزوعة السلاح
2. الاتصال من الأجهزة المضيفة على الشبكة الداخلية التي تتطلب الوصول إلى الموارد الموجودة في المنطقة المنزوعة السلاح
3. الاتصال من الأجهزة المضيفة في الداخل وشبكة DMZ التي تتطلب الوصول إلى الموارد من الخارج

nat

في المثال، نستخدم ترجمة عنوان الشبكة (NAT) وترجمة عنوان المنفذ (PAT) في التكوين الخاص بنا. تستبدل ترجمة العنوان الحقيقي (محلي) في حزمة بعنوان معين (عام) يكون قابل للتوجيه على الشبكة الوجهة. nat يتألف من خطوتين: العملية التي فيها تتم ترجمة عنوان حقيقي إلى عنوان معين ثم العملية أن تراجع الترجمة لحركة المرور التي ترجع. هناك إثنان شكل من العنوان ترجمة أن نحن نستعمل في هذا تشكيل مرشد: ساكن إستاتيكي وحركي.

تتيح الترجمات الديناميكية لكل مضيف إستخدام عنوان أو منفذ مختلف لكل ترجمة تالية. يمكن إستخدام الترجمات الديناميكية عندما يقوم المضيفون المحليون بمشاركة عنوان عمومي واحد أو أكثر أو "الاختباء وراءه". في هذا الوضع، لا يمكن لعنوان محلي واحد حجز عنوان عمومي بشكل دائم للترجمة. وبدلا من ذلك، تحدث ترجمة العنوان على أساس من عدة إلى واحد أو على أساس من عدة إلى العديد، ويتم إنشاء إدخالات الترجمة فقط عند الحاجة إليها. بمجرد أن يكون إدخال الترجمة خاليا من الاستخدام، يتم حذفه وإتاحته للمضيفين المحليين الآخرين. يكون هذا النوع من الترجمة أكثر إفادة للاتصالات الصادرة، والتي يتم فيها تعيين عنوان ديناميكي أو رقم منفذ للمضيفين الداخليين فقط أثناء إجراء الاتصالات. هناك شكلان من ترجمة العنوان الديناميكي:

- nat حركي - ترجمت عنوان محلي إلى التالي يتوفر عنوان عالمي في بركة. تحدث الترجمة على أساس واحد إلى واحد، لذلك من الممكن استنفاد مجموعة العناوين العالمية إذا عدد أكبر من المضيفين المحليين يحتاجون إلى ترجمة في وقت معين.
- (PAT NAT Overload) - يترجم عنوان محلي إلى عنوان عالمي وحيد؛ كل توصيل يكون فريد عندما التالي يتوفر high-order port رقم من العنوان شامل عينت كمصدر من التوصيل. تحدث الترجمة على أساس متعدد إلى واحد

لأن العديد من البيئات المضيفة المحلية تشترك في عنوان عمومي واحد مشترك.
تقوم الترجمة الثابتة بإنشاء ترجمة ثابتة للعنوان (العناوين) الحقيقي إلى العناوين (العناوين) المعينة. يترجم تشكيل ساكن إستاتيكي nat ال نفسه عنوان ل كل توصيل بمضيف وثابت ترجمة قاعدة. يتم إستخدام ترجمات العناوين الثابتة عندما يحتاج المضيف الداخلي أو المحلي إلى الحصول على نفس العنوان العمومي لكل اتصال. تتم ترجمة العنوان على أساس واحد إلى واحد. يمكن تعريف الترجمات الثابتة لمضيف واحد أو لجميع العناوين الموجودة في شبكة IP الفرعية.

الفرق الرئيسي بين NAT الديناميكي ونطاق من العناوين ل NAT ساكن إستاتيكي أن NAT يسمح مضيف بعيد ببدء اتصال بمضيف مترجم (إذا كان هناك قائمة وصول تسمح به)، بينما لا يسمح NAT حركي. أنت تحتاج أيضا عدد متساو من العنوان يخطط مع ساكن إستاتيكي nat.

يترجم جهاز الأمان عنوانا عندما تطابق قاعدة NAT حركة مرور. إذا لم تتطابق قاعدة NAT، تستمر معالجة الحزمة. الاستثناء هو عندما يمكن أنت nat عنصر تحكم. يتطلب التحكم في NAT أن تتطابق الحزم التي تجتاز من واجهة أمان أعلى (في الداخل) إلى مستوى أمان أقل (في الخارج) مع قاعدة NAT، أو معالجة أخرى لحزم التوقف. لعرض معلومات التكوين المشتركة، ارجع إلى مستند PIX/ASA 7.x NAT و PAT. للحصول على فهم أعمق لكيفية عمل NAT، راجع دليل كيفية عمل NAT.

تلميح: عندما تغير تكوين NAT، يوصى بمسح ترجمات NAT الحالية. يمكنك مسح جدول الترجمة باستخدام الأمر **clear xlate**. **ومع ذلك، توخ الحذر عند القيام بذلك** لأن مسح جدول الترجمة يؤدي إلى قطع اتصال كافة الاتصالات الحالية التي تستخدم الترجمات. البديل لمسح جدول الترجمة هو الانتظار حتى تنتهي الترجمات الحالية، ولكن لا يوصى بذلك لأن السلوك غير المتوقع يمكن أن ينتج عنه إنشاء إتصالات جديدة باستخدام القواعد الجديدة.

مستويات الأمان

تتحكم قيمة مستوى الأمان في كيفية تفاعل الأجهزة/البيئات المضيفة على الواجهات المختلفة مع بعضها البعض. وبشكل افتراضي، يمكن للمضيفين/الأجهزة المتصلة بواجهات ذات مستويات أمان أعلى الوصول إلى الأجهزة المضيفة/الأجهزة المتصلة بالواجهة ذات مستويات الأمان الأقل. لا يمكن للمضيفين/الأجهزة المتصلة بالواجهات ذات واجهات الأمان المنخفض الوصول إلى الأجهزة المضيفة/الأجهزة المتصلة بالواجهات ذات واجهات الأمان الأعلى دون إذن من قوائم الوصول.

يعد الأمر **security-level** جديدا على الإصدار 7.0 ويستبدل جزء من الأمر **namelf** الذي يعين مستوى الأمان لواجهة. هناك واجهتان، الواجهات "الداخلية" و"الخارجية"، لديهما مستويات أمان افتراضية، ولكن يمكن تجاوز هذه المستويات باستخدام الأمر **مستوى الأمان**. إذا قمت بتسمية واجهة "داخل"، فإنها تمنح مستوى أمان افتراضي من 100؛ وتمنح الواجهة المسماة "خارج" مستوى أمان افتراضي من 0. تتلقى جميع الواجهات الأخرى التي تمت إضافتها حديثا مستوى أمان افتراضي من 0. لتخصيص مستوى أمان جديد لواجهة، أستخدم الأمر **security-level** في وضع أمر الواجهة. تتراوح مستويات الأمان من 1 إلى 100.

ملاحظة: يتم إستخدام مستويات الأمان فقط لتحديد كيفية فحص جدار الحماية لحركة مرور البيانات ومعالجتها. على سبيل المثال، تتم إعادة توجيه حركة المرور التي تنتقل من واجهة أعلى أمان إلى واجهة أقل صرامة بسياسات افتراضية أقل صرامة من حركة المرور التي تأتي من واجهة أقل أمانا إلى واجهة أكثر أمانا. لمزيد من المعلومات حول مستويات الأمان، ارجع إلى دليل مرجع الأوامر ASA/PIX 7.x.

كما وفر ASA/PIX 7.x القدرة على تكوين واجهات متعددة بنفس مستوى الأمان. على سبيل المثال، يمكن توفير مستوى أمان يبلغ 50 لجميع الواجهات المتعددة المتصلة بالشركاء أو بمناطق البيانات الموزعة (DMZ) الأخرى. بشكل افتراضي، لا يمكن لواجهات الأمان نفسها هذه الاتصال ببعضها البعض. ومن أجل التعامل مع هذه المشكلة، تم إدخال الأمر **نفسه-inter-interface** permit **security-traffic**. يسمح هذا الأمر بالاتصال بين الواجهات من نفس مستوى الأمان. أحلت ل كثير معلومة على ال نفسه أمن بين قارن، الأمر مرجع مرشد يشكل قارن معلم، ويرى هذا مثال.

ACL

تتألف قوائم التحكم في الوصول عادة من إدخالات متعددة للتحكم في الوصول (ACE) يتم تنظيمها داخليا بواسطة جهاز الأمان في قائمة مرتبطة. تصف قوائم التحكم في الوصول (ACEs) مجموعة من حركة المرور مثل تلك الواردة

من مضيف أو شبكة وتسرد إجراء لتطبيقه على حركة المرور هذه، وعادة ما تسمح بذلك أو ترفضه. عندما يتم إخضاع الحزمة للتحكم في قائمة الوصول، يبحث جهاز أمان Cisco في هذه القائمة المرتبطة من ACEs للعثور على حزمة تطابق الحزمة. **ACE الأول الذي يطابق جهاز الأمان هو الذي يتم تطبيقه على الحزمة.** بمجرد العثور على المطابقة، يتم تطبيق الإجراء الموجود في ACE (السماح أو الرفض) على الحزمة.

يتم السماح بقائمة وصول واحدة فقط لكل واجهة، لكل إتجاه. هذا يعني أنه يمكنك أن يكون لديك قائمة وصول واحدة فقط تنطبق على حركة المرور الواردة على واجهة وقائمة وصول واحدة تنطبق على حركة المرور الصادرة على واجهة. قوائم الوصول التي لا يتم تطبيقها على الواجهات، مثل قوائم التحكم في الوصول إلى NAT، غير محدودة.

ملاحظة: بشكل افتراضي، تحتوي جميع قوائم الوصول على إدخال تحكم في الوصول (ACE) ضمني في النهاية ينكر جميع حركة المرور، لذلك تتطابق جميع حركة المرور التي لا تطابق أي إدخال تحكم في الوصول التي تدخلها في قائمة الوصول مع الرفض الضمني في النهاية ويتم إسقاطها. يجب أن يكون لديك عبارة سماح واحدة على الأقل في قائمة الوصول إلى الواجهة لحركة المرور لكي تتدفق. بدون بيان تصريح، يتم رفض جميع حركات المرور.

ملاحظة: يتم تنفيذ قائمة الوصول باستخدام أوامر **access-list** و**access-group**. يتم إستخدام هذه الأوامر بدلا من أوامر **القناة** و**الصادر**، والتي تم إستخدامها في الإصدارات السابقة من برنامج جدار حماية PIX. لمزيد من المعلومات حول قوائم التحكم في الوصول، ارجع إلى تكوين قائمة الوصول إلى IP.

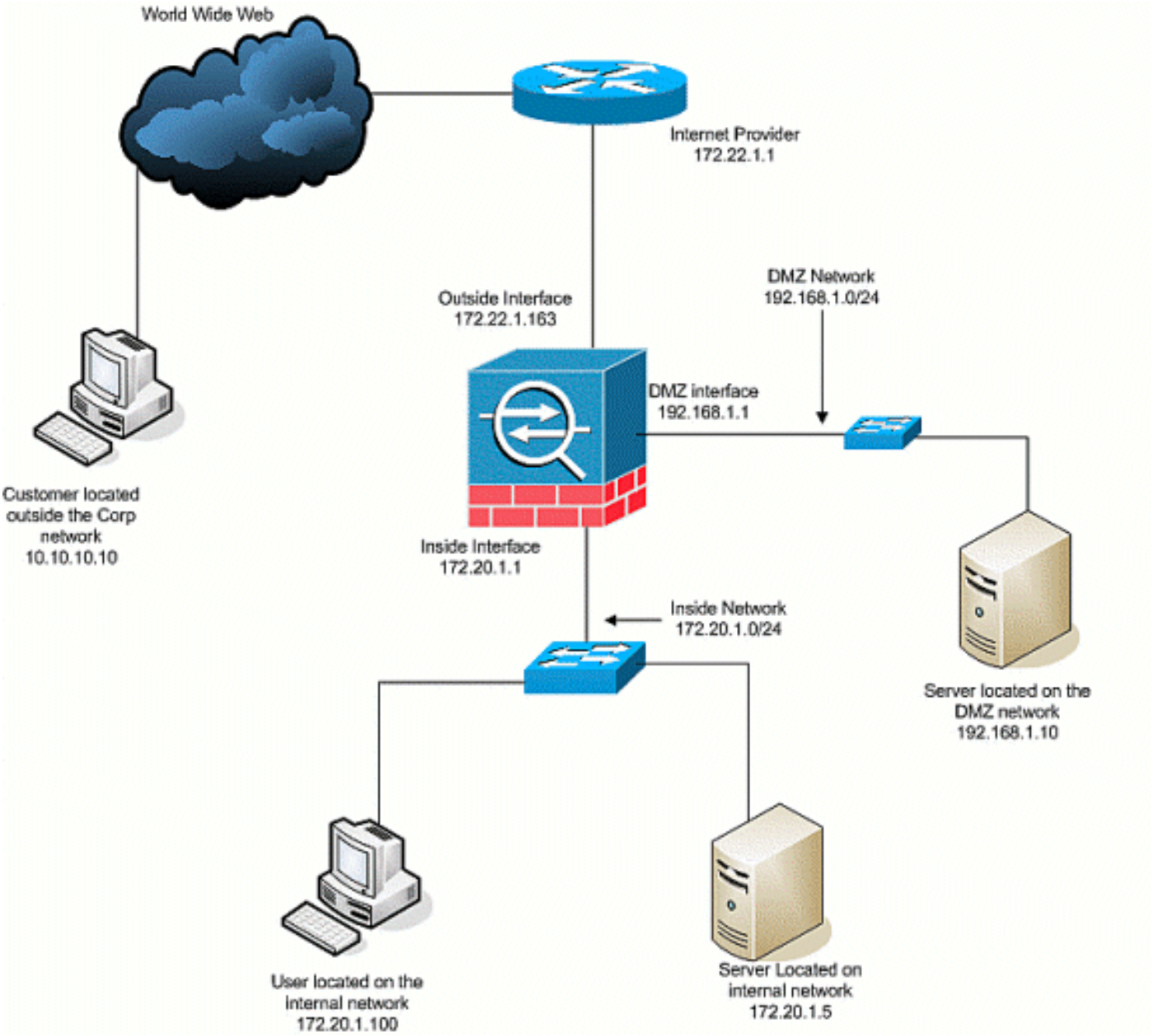
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التهيئة الأولية

يستخدم هذا المستند التكوينات التالية:

- مع هذا أساسي جدار حماية تشكيل، هناك حاليا ما من nat/ساكن إستاتيكي جمل.
- لا توجد قوائم التحكم في الوصول (ACL) مطبقة، لذلك يتم حاليا إستخدام ACE الضمني .

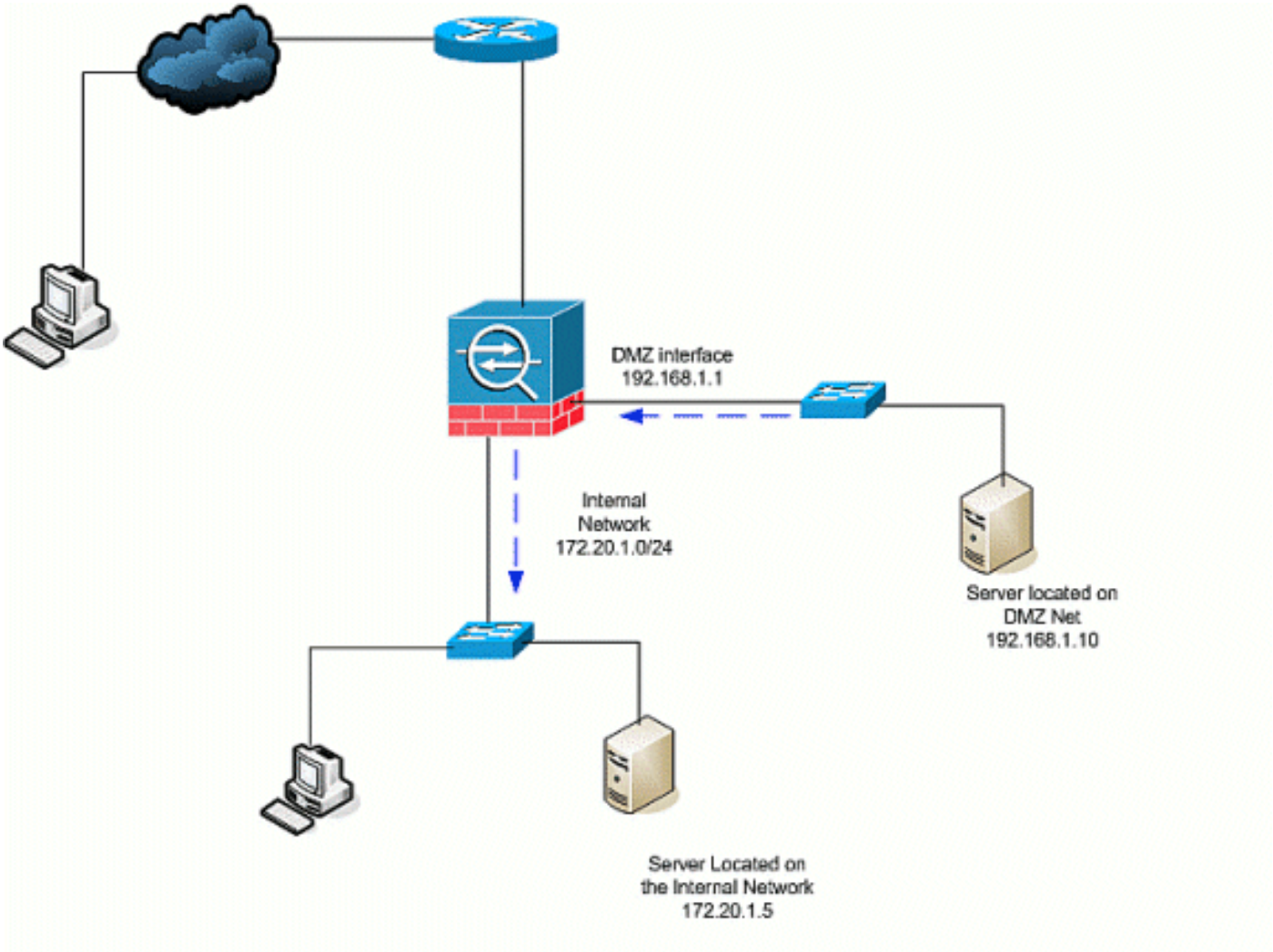
اسم الجهاز 1
ASA-AIP-CLI(config)#**show running-config** (ASA Version 7.2(2 ! hostname ASA-AIP-CLI domain-name corp.com enable password WwXYvtKrnjXqGbu1 encrypted names ! interface Ethernet0/0 nameif Outside

```
                                        security-level 0
                  ip address 172.22.1.163 255.255.255.0
                                                      !
                                     interface Ethernet0/1
                                            nameif inside
                                      security-level 100
                    ip address 172.20.1.1 255.255.255.0
                                                      !
                                     interface Ethernet0/2
                                              nameif DMZ
                                    security-level 50
                   ip address 192.168.1.1 255.255.255.0
                                                      !
                                     interface Ethernet0/3
                                     nameif DMZ-2-testing
                                       security-level 50
                  ip address 192.168.10.1 255.255.255.0
                                                      !
                                  interface Management0/0
                                               shutdown
                                             no nameif
                                         no security-level
                                             no ip address
                                                      !
                       passwd 2KFQnbNIdI.2KYOU encrypted
                                          ftp mode passive
                              dns server-group DefaultDNS
                                     domain-name corp.com
                                            pager lines 24
                                           mtu inside 1500
                                          mtu Outside 1500
                                              mtu DMZ 1500
                                           no failover
             icmp unreachable rate-limit 1 burst-size 1
                                    no asdm history enable
                                         arp timeout 14400
                                               nat-control
             route Outside 0.0.0.0 0.0.0.0 172.22.1.1 1
                                        timeout xlate 3:00:00
    timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
                                                 icmp 0:00:02
   timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
                                      0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
                                    sip-disconnect 0:02:00
                            timeout uauth 0:05:00 absolute
                                   no snmp-server location
                                   no snmp-server contact
     snmp-server enable traps snmp authentication linkup
                                        linkdown coldstart
                                      telnet timeout 5
                                         ssh timeout 5
                                    console timeout 0
                                                      !
                                 class-map inspection_default
                           match default-inspection-traffic
                                                      !
                                                      !
             policy-map type inspect dns preset_dns_map
                                                parameters
                              message-length maximum 512
                                  policy-map global_policy
                                 class inspection_default
                                inspect dns preset_dns_map
```

```
                                                    inspect ftp
                                                inspect h323 h225
                                                 inspect h323 ras
                                                  inspect netbios
                                                      inspect rsh
                                                    inspect rtsp
                                                  inspect skinny
                                                   inspect esmtp
                                                  inspect sqlnet
                                                  inspect sunrpc
                                                    inspect tftp
                                                     inspect sip
                                                   inspect xdmcp
                                                               !
                                        service-policy global_policy global
                                                prompt hostname context
                                Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
                                                            end :
                                                #(ASA-AIP-CLI(config
```

DMZ إلى الداخل

استعملت in order to سمحت إتصال من ال DMZ إلى شبكة مضيف داخلي، هذا أمر. في هذا المثال، يحتاج خادم ويب الموجود على DMZ إلى الوصول إلى خادم AD و DNS الموجود بالداخل.

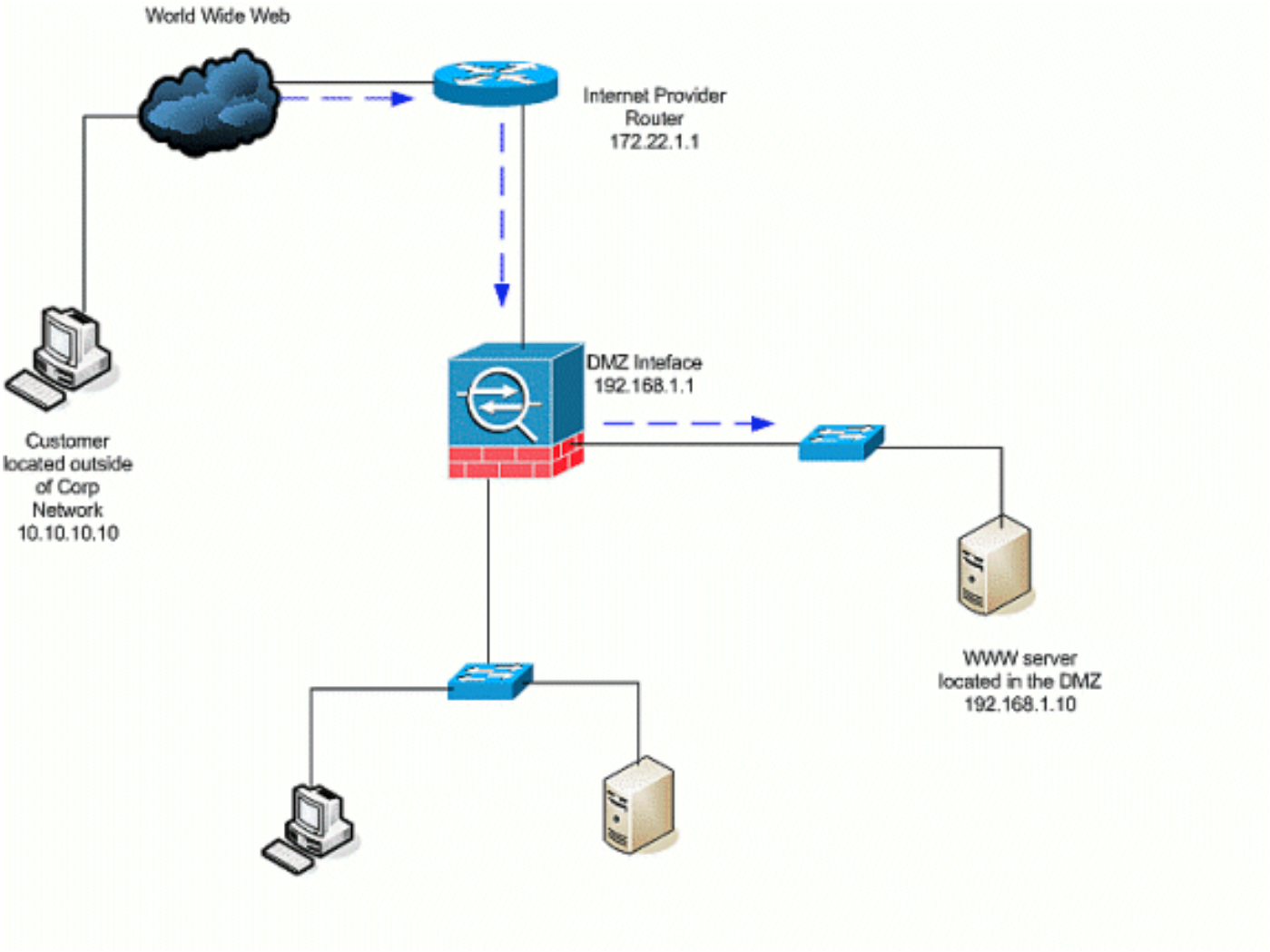


1. قم بإنشاء إدخال NAT ثابت لخادم AD/DNS على DMZ. nat ساكن إستاتيكي يخلق ترجمة ثابتة من عنوان حقيقي إلى عنوان يخطط. هذا العنوان المعين هو عنوان يمكن للمضيفين في DMZ إستخدامه للوصول إلى

الخادم من الداخل دون الحاجة إلى معرفة العنوان الحقيقي للخادم. يقوم هذا الأمر بتعيين عنوان DMZ 192.168.2.20 إلى العنوان الداخلي الحقيقي 172.20.1.5.
```
ASA-AIP-CLI(config)# static (DMZ,DMZ) 192.168.2.20 172.20.1.5 netmask 255.255.255.255
```
2. قوائم التحكم في الوصول (ACL) مطلوبة للسماح لواجهة ذات مستوى أمان أقل بالوصول إلى مستوى أمان أعلى. في هذا المثال، نقدم لخادم الويب الموجود على وصول DMZ (Security 50) إلى خادم AD/DNS الموجود بالداخل (Security 100) مع منافذ الخدمة المحددة التالية: DNS و Kerberos و LDAP.
```
ASA-AIP-CLI(config)# access-list DMZtoInside Extended Permit UDP host 192.168.2.20 eq 389 host 192.168.1.10
ASA-AIP-CLI(config)# access-list DMZtoInside Extended Permit TCP host 192.168.2.20 eq 88 host 192.168.1.10
ASA-AIP-CLI(config)# access-list DMZtoInside Extended Permit UDP host 192.168.2.20 eq 88 host 192.168.1.10
```
ملاحظة: تسمح قوائم التحكم في الوصول (ACL) بالوصول إلى العنوان المعين لخادم AD/DNS الذي تم إنشاؤه في هذا المثال وليس العنوان الداخلي الحقيقي.
3. في هذه الخطوة، تقوم بتطبيق قائمة التحكم في الوصول (ACL) على واجهة DMZ في الإتجاه الوارد باستخدام هذا الأمر:
```
ASA-AIP-CLI(config)# access-group DMZtoInside in interface DMZ
```
ملاحظة: إذا كنت تريد حظر المنفذ 88 أو تعطيله، حركة المرور من DMZ إلى الداخل، على سبيل المثال، أستخدم هذا:
```
ASA-AIP-CLI(config)# no access-list DMZtoInside extended permit tcp host 192.168.1.10 host 192.168.2.20 eq 88
```
تلميح: عندما تغير تكوين NAT، يوصى بمسح ترجمات NAT الحالية. يمكنك مسح جدول الترجمة باستخدام الأمر **clear xlate**. **توخ الحذر عند القيام بذلك** نظرا لأن مسح جدول الترجمة يؤدي إلى قطع اتصال كافة الاتصالات الحالية التي تستخدم الترجمات. البديل لمسح جدول الترجمة هو الانتظار حتى تنتهي الترجمات الحالية، ولكن لا يوصى بذلك لأن السلوك غير المتوقع يمكن أن ينتج عنه إنشاء إتصالات جديدة باستخدام القواعد الجديدة.تتضمن التكوينات الشائعة الأخرى ما يلي:خوادم البريد في DMZوصول SSH داخل وخارجالسماح بجلسات عمل سطح المكتب البعيد من خلال أجهزة PIX/ASAحلول DNS الأخرى عند إستخدامها في DMZ

الإنترنت إلى DMZ

للسماح بالاتصال من المستخدمين على الإنترنت، أو الواجهة الخارجية (Security 0)، إلى خادم ويب الموجود في DMZ (Security 50)، أستخدم الأوامر التالية:



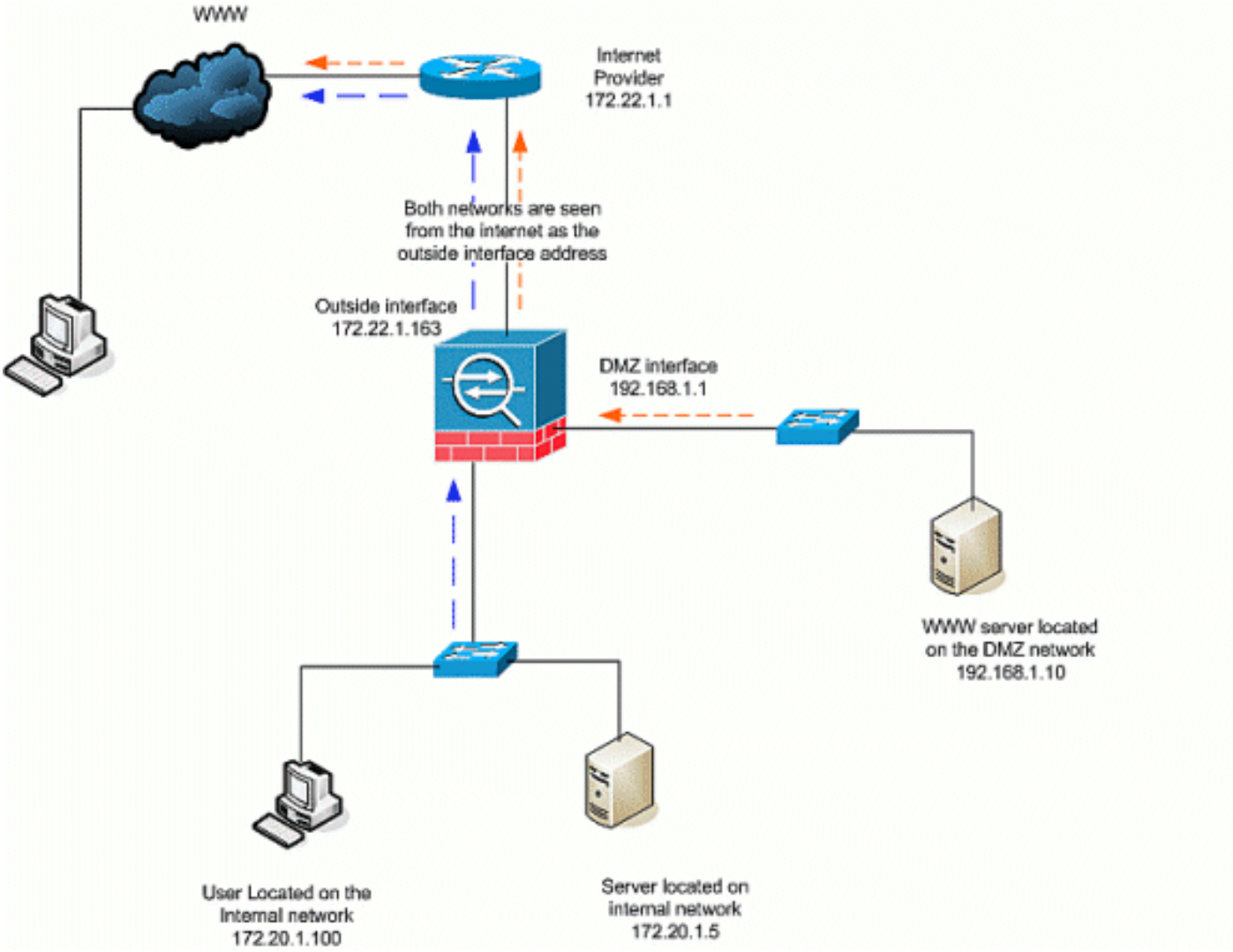
1. قم بإنشاء ترجمة ثابتة لخادم الويب في DMZ إلى الخارج. nat ساكن إستاتيكي يخلق ترجمة ثابتة من عنوان حقيقي إلى عنوان يخطط. هذا العنوان المعين هو عنوان يمكن للمضيفين على الإنترنت إستخدامه للوصول إلى خادم الويب على DMZ بدون الحاجة إلى معرفة العنوان الحقيقي للخادم. يقوم هذا الأمر بتعيين العنوان الخارجي 172.22.1.25 إلى العنوان DMZ الحقيقي 192.168.1.10.`#(ASA-AIP-CLI(config.  ( DMZ)`
`netmask 255.255.255.255 192.168.1.10 172.22.1.25`
2. قم بإنشاء قائمة تحكم في الوصول (ACL) تسمح للمستخدمين من الخارج بالوصول إلى خادم الويب من خلال العنوان المعين. لاحظ أن خادم الويب يستضيف أيضا FTP.`ASA-AIP-CLI(config)# access-list`
`eq wwASA-AIP-CLI(config)# access-list 172.22.1.25  OutsidetoDMZ Extended Permit`
`eq ftp 172.22.1.25  OutsidetoDMZ Extended Permit`
3. تتمثل الخطوة الأخيرة في هذا التكوين في تطبيق قائمة التحكم في الوصول (ACL) على الواجهة الخارجية لحركة المرور في الإتجاه الوارد.`ASA-AIP-CLI(config)# access-group OutToDMZ` **ملاحظة:** تذكر، يمكنك تطبيق قائمة وصول واحدة فقط لكل واجهة، لكل إتجاه. إذا كانت لديك بالفعل قائمة تحكم في الوصول (ACL) واردة مطبقة على الواجهة الخارجية، فلا يمكنك تطبيق مثال قائمة التحكم في الوصول (ACL) هذا عليه. بدلا من ذلك، قم بإضافة إدخالات التحكم في الوصول (ACEs) في هذا المثال إلى قائمة التحكم في الوصول (ACL) الحالية التي يتم تطبيقها على الواجهة.**ملاحظة:** إذا كنت تريد حظر حركة مرور FTP من الإنترنت إلى DMZ أو تعطيلها، على سبيل المثال، أستخدم ما يلي:

```
ASA-AIP-CLI(config)# no access-list OutsidetoDMZ extended permit
tcp any host 172.22.1.25 eq ftp
```

تلميح: عندما تغير تكوين NAT، يوصى بمسح ترجمات NAT الحالية. يمكنك مسح جدول الترجمة باستخدام الأمر **clear xlate**. **توخ الحذر عند القيام بذلك** نظرا لأن مسح جدول الترجمة يؤدي إلى قطع اتصال كافة الاتصالات الحالية التي تستخدم الترجمات. البديل لمسح جدول الترجمة هو الانتظار حتى تنتهي الترجمات الحالية، ولكن لا يوصى بذلك لأن السلوك غير المتوقع يمكن أن ينتج عنه إنشاء إتصالات جديدة باستخدام القواعد الجديدة.

داخل/DMZ إلى الإنترنت

في هذا السيناريو، يتم توفير الأجهزة المضيفة الموجودة على الواجهة الداخلية (Security 100) لجهاز الأمان بإمكانية الوصول إلى الإنترنت على الواجهة الخارجية (Security 0). ويتحقق ذلك مع PAT، أو حمل زائد ل nat، شكل nat حركي. بخلاف السيناريوهات الأخرى، لا يلزم وجود قائمة تحكم في الوصول (ACL) في هذه الحالة لأن الأجهزة المضيفة الموجودة على أجهزة مضيفة للوصول إلى واجهة عالية الأمان على واجهة منخفضة الأمان.



1. حدد مصدر (مصادر) حركة المرور التي يجب ترجمتها. هنا يتم تحديد **قاعدة** NAT رقم 1، ويتم السماح بجميع حركات مرور البيانات من الداخل والبيئات المضيفة ل DMZ.`ASA-AIP-CLI(config)# nat () 1 172.20.1.0 255.255.255.0 192.168.1.0 1 () 255.255.255.0ASA-AIP-CLI(config)# nat`
2. عينت ما عنوان، عنوان بركة، أو قارن ال NATed حركة مرور ينبغي استعملت عندما هو ينفذ القارن خارجي. في هذه الحالة، أنجزت ضرب مع القارن خارجي عنوان. ويكون هذا مفيدا بشكل خاص عندما لا يكون عنوان الواجهة الخارجية معروفا مسبقا، مثل تكوين DHCP. هنا، يتم إصدار الأمر العام بنفس معرف **1** NAT، والذي يربطه بقواعد NAT من نفس المعرف.`ASA-AIP-CLI(config)# global () 1 interface`

تلميح: عندما تغير تكوين NAT، يوصى بمسح ترجمات NAT الحالية. يمكنك مسح جدول الترجمة باستخدام الأمر **clear xlate**. **توخ الحذر عند القيام بذلك** نظرا لأن مسح جدول الترجمة يؤدي إلى قطع اتصال كافة الاتصالات الحالية التي تستخدم الترجمات. البديل لمسح جدول الترجمة هو الانتظار حتى تنتهي الترجمات الحالية، ولكن لا يوصى بذلك لأن السلوك غير المتوقع يمكن أن ينتج عنه إنشاء إتصالات جديدة باستخدام القواعد الجديدة.

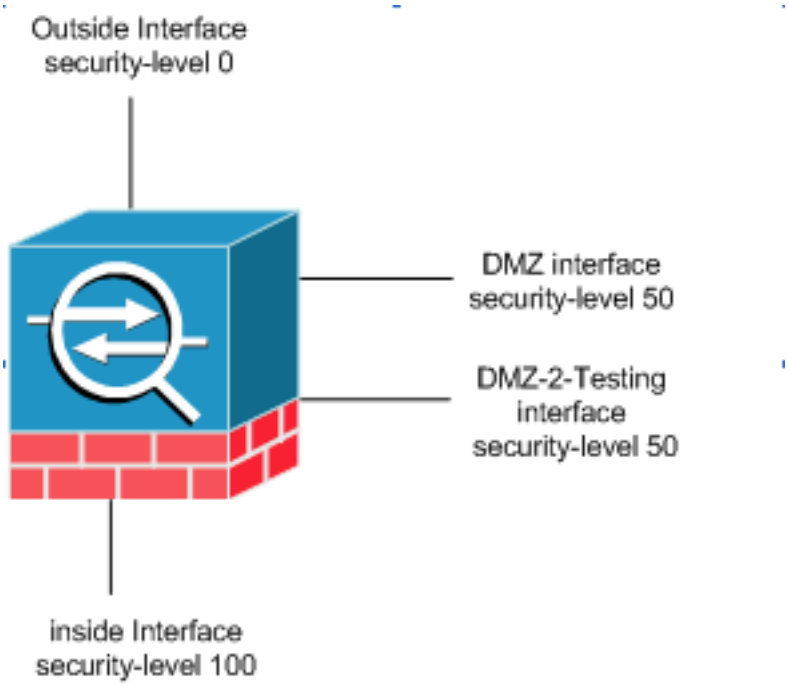
ملاحظة: إذا كنت ترغب في حظر حركة المرور من منطقة الأمان الأعلى (في الداخل) إلى منطقة الأمان الأدنى (الإنترنت/DMZ)، فقم بإنشاء قائمة تحكم في الوصول (ACL) وتطبيقها على الواجهة الداخلية ل PIX/ASA كداخل.

ملاحظة: على سبيل المثال: لحظر حركة مرور المنفذ 80 من المضيف 172.20.1.100 على الشبكة الداخلية إلى الإنترنت، أستخدم ما يلي:

```
ASA-AIP-CLI(config)#access-list InsidetoOutside extended deny tcp host 172.20.1.100 any eq www
ASA-AIP-CLI(config)#access-list InsidetoOutside extended permit tcp any any
ASA-AIP-CLI(config)#access-group InsidetoOutside in interface inside
```

التواصل على نفس المستوى الأمني

يوضح التكوين الأولي أن الواجهات "DMZ" و"DMZ-2-test" تم تكوينها بمستوى الأمان (50)؛ وبشكل افتراضي، لا يمكن لهاتين الواجهات التحدث. هنا نسمح لهذه الواجهات بالتحدث مع هذا الأمر:




```
ASA-AIP-CLI(config)# SAME-security-traffic permit inter-interface
```

ملاحظة: على الرغم من تكوين "حركة مرور تصريح حركة مرور داخلية ذات أمان واحد" لنفس واجهات مستوى الأمان ("DMZ" و"DMZ-2-test")، فإنها لا تزال بحاجة إلى قاعدة ترجمة (ثابتة/ديناميكية) للوصول إلى الموارد الموضوعة في تلك الواجهات.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

- أستكشاف أخطاء الاتصالات وإصلاحها من خلال PIX و ASA
- التحقق nat Configuration من nat واستكشاف الأخطاء وإصلاحها

معلومات ذات صلة

- مرجع أمر ASA من Cisco
- مرجع أمر PIX من Cisco
- خطأ Cisco ASA ورسائل الأنظمة
- رسائل خطأ PIX والأنظمة من Cisco
- 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).