الشبكات الآمنة باستخدام شبكات VLAN الخاصة وقوائم التحكم في الوصول إلى شبكة VLAN (VACLs)

المحتويات

المقدمة

أحد العوامل الرئيسية لبناء تصميم أمان شبكة ناجح هو تحديد نموذج ثقة مناسب وتنفيذه. يحدد نموذج الثقة المناسب من الذي يحتاج إلى التحدث إلى من ونوع حركة المرور التي يجب تبادلها، كما يجب رفض جميع حركات المرور الأخرى. بمجرد تحديد نموذج الثقة المناسب، يجب أن يقرر مصمم الأمان كيفية فرض النموذج. ومع توافر المزيد من الموارد الحيوية على الصعيد العالمي وتطور أشكال جديدة من هجمات الشبكات، تميل البنية التحتية لأمان الشبكة إلى أن تصبح أكثر تطورا، وتتوفر المزيد من المنتجات. تعد جدران الحماية والموجهات ومحولات الشبكة المحلية (LAN) وأنظمة اكتشاف الاقتحام وخوادم AAA والشبكات الخاصة الظاهرية (VPN) بعض التقنيات والمنتجات التي يمكنها المساعدة في فرض النموذج. بطبيعة الحال، كل من هذه المنتجات والتكنولوجيات يلعب دورا خاصا في التنفيذ الأمني الشامل، ومن الضروري للمصمم أن يفهم كيف يمكن نشر هذه العناصر.

قبل البدء

الاصطلاحات

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

المتطلبات الأساسية

يصف هذا المستند تكوينات PVLAN على المحولات التي تعمل بنظام التشغيل CatOS فقط. للحصول على أمثلة تكوين جنبا إلى جنب لشبكات VLAN الخاصة على المحولات التي تشغل نظام التشغيل Cisco IOS و CatOS، ارجع إلى المستند تكوين شبكات VLAN الخاصة المعزولة على محولات Catalyst Switches.

لا تدعم كل المحولات وإصدارات البرامج شبكات VLAN الخاصة. ارجع إلى مصفوفة دعم محول Catalyst VLAN الخاص لتحديد ما إذا كان نظامك الأساسي وإصدار البرنامج يدعمان شبكات VLAN الخاصة.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

معلومات أساسية

يبدو تحديد نموذج ثقة مناسب وتنفيذه مهمة أساسية للغاية، لكن بعد سنوات عديدة من دعم عمليات تنفيذ الإجراءات الأمنية، تشير تجربتنا إلى أن الحوادث الأمنية غالبا ما تكون مرتبطة بتصاميم أمنية سيئة. وعادة ما تكون هذه التصميمات الرديئة نتيجة مباشرة لعدم تطبيق نموذج ثقة مناسب، أحيانا لأن ما هو ضروري لا يفهم، وأحيانا أخرى لمجرد أن التكنولوجيات المعنية لا تفهم بالكامل أو يساء إستخدامها.

يشرح هذا المستند بالتفصيل كيف يمكن لميزتين متوفرتين في محولات Catalyst الخاصة بنا، شبكات VLAN الخاصة (PVLANs) وقوائم التحكم في الوصول إلى شبكة VLAN (VACLs)، المساعدة على ضمان نموذج ثقة مناسب في كل من بيئات المؤسسة وكذلك مزود الخدمة.

أهمية فرض نموذج الثقة المناسب

ومن النتائج المباشرة لعدم إنفاذ نموذج ثقة مناسب أن التنفيذ الأمني العام يصبح أقل مناعة من الأنشطة الضارة. وتنفذ المناطق المجردة من السلاح عادة دون إنفاذ السياسات الصحيحة، مما ييسر نشاط الدخيل المحتمل. ويحلل هذا القسم الكيفية التي تنفذ بها المناطق المتوسطية في أغلب الأحيان وعواقب التصميم الرديء. وسوف نشرح في وقت لاحق كيفية تخفيف هذه العواقب، أو تجنبها في أفضل الحالات.

عادة، من المفترض أن تقوم خوادم DMZ بمعالجة الطلبات الواردة من الإنترنت فقط، وبدء الاتصالات في نهاية المطاف ببعض الخوادم الخلفية الموجودة في جزء داخلي أو مقطع DMZ آخر، مثل خادم قاعدة بيانات. وفي الوقت نفسه، ليس من المفترض أن تتحدث خوادم DMZ مع بعضها البعض أو تبدأ أي إتصالات بالعالم الخارجي. يحدد هذا بوضوح تدفقات حركة المرور الضرورية في نموذج ثقة بسيط، ومع ذلك، غالبا ما نرى هذا النوع من النماذج غير مطبق بشكل كاف.

يميل المصممون عادة إلى تنفيذ DMZ باستخدام جزء مشترك لكل الخوادم بدون أي تحكم على حركة المرور فيما بينهم. على سبيل المثال، يتم تحديد موقع جميع الخوادم في شبكة VLAN مشتركة. بما أنه لا شيء يتحكم في حركة المرور ضمن شبكة VLAN نفسها، إذا تم أختراق أحد الخوادم، يمكن إستخدام الخادم نفسه كمصدر هجوم إلى أي من الخوادم والأجهزة المضيفة في نفس المقطع. فهذا يؤدي بوضوح إلى تسهيل نشاط الدخيل المحتمل الذي يقوم بإعادة توجيه المنفذ أو هجوم على طبقة التطبيقات.

وعادة، لا يتم إستخدام جدران الحماية وعوامل تصفية الحزم إلا للتحكم في الاتصالات الواردة، ولكن لا يتم عادة القيام بأي شيء لتقييد الاتصالات التي تم إنشاؤها من المنطقة DMZ. منذ بعض الوقت كان هناك نقطة ضعف معروفة في برنامج cgi-bin النصي الذي يسمح للمتسلل ببدء جلسة عمل X-term عن طريق إرسال تدفق HTTP فقط، هذه هي حركة المرور التي يجب أن يسمح بها جدار الحماية. وإذا كان المتطفل محظوظا بالقدر الكافي، فسوف يكون بوسعه أن يستخدم علاجا آخر للحصول على إشارة الجذر، وهو عادة ما يشكل نوعا من هجوم تجاوز سعة التخزين المؤقت. وفي معظم الأحيان يمكن تجنب هذا النوع من المشاكل بفرض نموذج ثقة مناسب. أولا، ليس من المفترض أن تتحدث الخوادم مع بعضها البعض، وثانيا، يجب ألا تنشأ أي إتصالات من هذه الخوادم إلى العالم الخارجي.

تنطبق نفس التعليقات على العديد من السيناريوهات الأخرى، بدءا من أي مقطع غير موثوق به بشكل منتظم حتى مزارع الخوادم في موفري خدمة التطبيقات.

يمكن أن تساعد شبكات VLAN الخاصة وقوائم التحكم في الوصول إلى شبكة VLAN (VACLs) على محولات Catalyst في ضمان نموذج ثقة مناسب. ستساعد شبكات VLAN الخاصة بتقييد حركة المرور بين الأجهزة المضيفة في مقطع مشترك، بينما ستسهم قوائم التحكم في الوصول إلى شبكة VLAN من خلال توفير مزيد من التحكم في أي تدفق حركة مرور تم إنشاؤه أو توجيهه إلى مقطع معين. وتناقش هذه الميزات في الاقسام التالية.

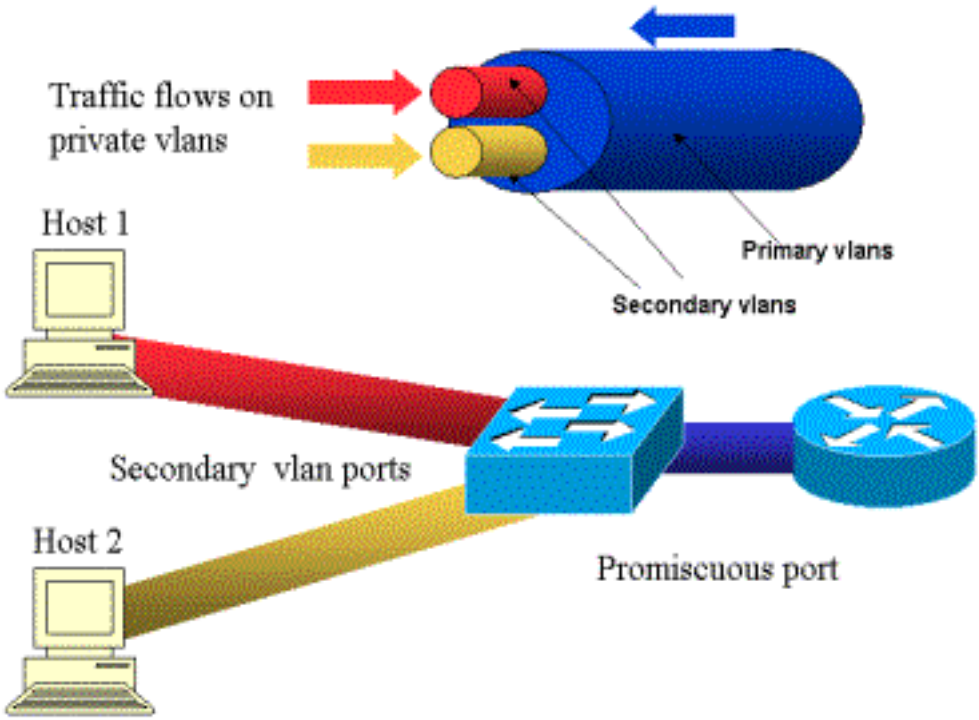
شبكات VLAN الخاصة

PVLANs يتوفر على المادة حفازة 6000 يركض CatOS 5.4 أو متأخر، على المادة حفازة 4000، 2980G، 2980G-A، 2948G، و 4912G يركض CatOS 6.2 أو متأخر.

من وجهة نظرنا، فإن شبكات VLAN الخاصة هي أداة تسمح بفصل حركة المرور في الطبقة 2 (L2) بتحويل مقطع البث إلى مقطع غير بث يشبه الوصول المتعدد. يمكن لحركة مرور البيانات التي تأتي إلى محول من منفذ مختلط (وهو، منفذ قادر على إعادة توجيه شبكات VLAN الأساسية والثانوية) أن تخرج على جميع المنافذ التي تنتمي إلى شبكة VLAN الأساسية نفسها. يمكن إعادة توجيه حركة المرور التي تأتي إلى محول من منفذ معين إلى شبكة VLAN الثانوية (يمكن أن تكون إما شبكة VLAN معزولة أو مجتمع أو شبكة VLAN مجتمعية ثنائية الإتجاه) إلى منفذ مختلط أو منفذ ينتمي إلى شبكة VLAN المجتمعية نفسها. يتعدد ميناء يعين إلى ال نفسه VLAN يعجز تبادل أي حركة مرور.

توضح الصورة التالية المفهوم.

الشكل 1: شبكات VLAN الخاصة



يتم تمثيل شبكة VLAN الأساسية باللون الأزرق، بينما يتم تمثيل شبكات VLAN الثانوية باللون الأحمر والأصفر. يتصل المضيف-1 بمنفذ من المحول الذي ينتمي إلى شبكة VLAN الثانوية باللون الأحمر. يتصل المضيف-2 بمنفذ من المحول الذي ينتمي إلى شبكة VLAN الثانوية الصفراء.

عندما يرسل مضيف، الحركة مرور يكون في الثانوي VLAN. على سبيل المثال، عندما يرسل المضيف-2، الحركة مرور هو يذهب على VLAN أصفر. عندما يستلم هذا مضيف، الحركة مرور يأتي من ال VLAN أزرق، أي يكون ال VLAN أساسي.

المنافذ التي يتم فيها توصيل الموجهات وجدران الحماية هي منافذ مختلطة لأن هذه المنافذ يمكن أن تعيد توجيه حركة

مرور البيانات الواردة من كل شبكة VLAN الثانوية المحددة في التخطيط وكذلك شبكة VLAN الأساسية. الميناء يربط إلى كل مضيف يستطيع فقط أرسلت الحركة مرور قادم من ال VLAN أساسي وال VLAN ثانوي يشكل على أن ميناء.

يمثل الرسم شبكات VLAN الخاصة كمواسير مختلفة تربط الموجهات والمضيفين: الأنبوب الذي يجمع كل الآخرين هو شبكة VLAN الأساسية (أزرق)، وحركة المرور على شبكة VLAN الزرقاء تتدفق من الموجهات إلى الأجهزة المضيفة. المواسير الداخلية إلى شبكة VLAN الأساسية هي شبكات VLAN الثانوية، وحركة المرور التي تنتقل على هذه المواسير من البيئات المضيفة تجاه الموجه.

بما أن الصورة يتم إظهارها، VLAN أساسي يستطيع حزمت one or much ثانوي VLANs.

في وقت سابق من هذه الوثيقة قلنا إن شبكات VLAN الخاصة تساعد في فرض نموذج الثقة المناسب عن طريق ضمان فصل الأجهزة المضيفة ببساطة داخل جزء مشترك. والآن بعد أن أصبحنا نعرف المزيد عن شبكات VLAN الخاصة، فدعونا نرى كيف يمكن تنفيذ هذا في سيناريو المنطقة الزمنية الفاصلة (DMZ) الأولي. ليس من المفترض أن تتحدث الخوادم مع بعضها البعض، ولكنها لا تزال بحاجة إلى التحدث إلى جدار الحماية أو الموجه المتصل به. في هذه الحالة، يجب توصيل الخوادم بالمنافذ المعزولة بينما يجب إرفاق الموجهات وجدران الحماية بالمنافذ المختلطة. ومن خلال القيام بذلك، إذا تم أختراق أحد الخوادم، فلن يتمكن الدخيل من إستخدام نفس الخادم كمصدر هجوم إلى خادم آخر داخل نفس المقطع. سيقوم المحول بإسقاط أي حزمة بسرعة سلكية، دون أي عقوبة تتعلق بالأداء.

ملاحظة هامة أخرى هي أنه يمكن تنفيذ هذا النوع من التحكم فقط على جهاز L2 لأن جميع الخوادم تنتمي إلى الشبكة الفرعية نفسها. لا يمكن لجدار الحماية أو الموجه القيام بأي شيء حيث ستحاول الخوادم الاتصال مباشرة. خيار آخر هو تخصيص منفذ جدار حماية لكل خادم، ولكن من المحتمل أن يكون هذا باهظ التكلفة وصعب التنفيذ ولا يتم تطويره.

في قسم لاحق، نحن نصف بالتفصيل بعض السيناريوهات النموذجية الأخرى التي يمكنك فيها إستخدام هذه الميزة.

قوائم التحكم في الوصول إلى شبكة VLAN

تتوفر قوائم التحكم في الوصول إلى شبكة VLAN على السلسلة Catalyst 6000 Series التي تشغل CatOS 5.3 أو الأحدث.

يمكن تكوين قوائم التحكم في الوصول إلى شبكة VLAN على محول Catalyst 6500 في L2 دون الحاجة إلى موجه (تحتاج فقط إلى بطاقة ميزة سياسة (PFC)). يتم فرضها بسرعة سلكية لذلك لا يوجد عقوبة أداء في تكوين قوائم التحكم في الوصول إلى شبكة VLAN على مادة حفازة 6500. ونظرا لأنه يتم إجراء البحث عن قوائم التحكم في الوصول إلى شبكة VLAN في الأجهزة، بغض النظر عن حجم قائمة الوصول، فإن معدل إعادة التوجيه يظل دون تغيير.

يمكن تعيين قوائم التحكم في الوصول إلى شبكة VLAN بشكل منفصل إلى شبكات VLAN الأساسية أو الثانوية. إن تكوين قائمة التحكم في الوصول إلى شبكة VLAN الثانوية يسمح بتصفية حركة المرور التي تم إنشاؤها بواسطة الأجهزة المضيفة دون لمس حركة المرور التي تم إنشاؤها بواسطة الموجهات أو جدران الحماية.

من خلال دمج قوائم التحكم في الوصول إلى شبكة VLAN وشبكات VLAN الخاصة، من الممكن تصفية حركة المرور استنادا إلى إتجاه حركة المرور نفسها. على سبيل المثال، إذا كان هناك موجهان متصلان بنفس المقطع مثل بعض البيئات المضيفة (الخوادم على سبيل المثال)، يمكن تكوين قوائم التحكم في الوصول إلى شبكة VLAN الثانوية حتى تتم تصفية حركة المرور التي تم إنشاؤها بواسطة الأجهزة المضيفة فقط بينما لا يتم لمس حركة المرور المتبادلة بين الموجهات.

يمكن نشر قوائم التحكم في الوصول إلى شبكة VLAN بسهولة لفرض نموذج الثقة المناسب. دعونا نحلل حالة DMZ لدينا. من المفترض أن تخدم الخوادم في المنطقة المنزوعة السلاح الاتصالات الواردة فقط، ومن غير المتوقع أن تبدأ الاتصالات مع العالم الخارجي. يمكن تطبيق قائمة التحكم في الوصول إلى شبكة VLAN الثانوية الخاصة بهم للتحكم في حركة مرور البيانات التي تترك هذه الخوادم. من المهم ملاحظة أنه عند إستخدام قوائم التحكم في الوصول إلى شبكة (VACLs)، يتم إسقاط حركة المرور في الأجهزة لذلك لا يوجد تأثير على وحدة المعالجة المركزية للموجه أو

المحول. حتى في حالة تورط أحد الخوادم في هجوم رفض الخدمة الموزع (DDoS) كمصدر، سيقوم المحول بإسقاط جميع حركات المرور غير الشرعية بسرعة سلكية، دون أية عقوبة تتعلق بالأداء. يمكن تطبيق عوامل تصفية مماثلة في الموجه أو جدار الحماية حيث يتم توصيل الخوادم، ولكن عادة ما يكون لهذا تأثير شديد على الأداء.

لا تعمل قوائم التحكم في الوصول (ACL) المستندة إلى MAC بشكل جيد مع حركة مرور IP، لذلك يوصى بقوائم التحكم في الوصول إلى شبكة VLAN (VACLs) لمراقبة / تعقب شبكات VLAN الخاصة.

قيود معروفة على قوائم التحكم في الوصول إلى شبكة VLAN وشبكات VLAN الخاصة

عند تكوين التصفية باستخدام قوائم التحكم في الوصول إلى المنفذ (VACLs)، يجب أن تكون حذرا فيما يتعلق بمعالجة الجزء على PFC، وأن التكوين يتم ضبطه وفقا لمواصفات الأجهزة.

بافتراض تصميم الأجهزة ل PFC من المشرف 1 من المادة حفازة 6500، فمن الأفضل أن ينكر صراحة أجزاء ICMP. والسبب هو أن الأجهزة تعتبر أجزاء بروتوكول رسائل التحكم في الإنترنت (ICMP) ورد الفعل نفسه، ويتم برمجة الأجهزة بشكل افتراضي للسماح بالأجزاء بشكل صريح. لذلك إذا كنت تريد إيقاف حزم الرد على الصدى من مغادرة الخوادم، فيجب عليك بشكل صريح تكوين هذا مع **رفض** السطر **أي جزء من ICMP**. وتضع التكوينات الواردة في هذا المستند هذا الأمر في الاعتبار.

هناك قيود أمان معروفة على شبكات VLAN الخاصة، وهي إمكانية أن يقوم الموجه بإعادة توجيه حركة المرور إلى الخلف من نفس الشبكة الفرعية التي جاء منها. يمكن للموجه توجيه حركة مرور البيانات عبر المنافذ المعزولة مما يؤدي إلى تقويض الغرض من شبكات VLAN الخاصة. ويرجع هذا القيد إلى حقيقة أن شبكات VLAN الخاصة هي أداة توفر العزل في L2، وليس في الطبقة 3 (L3).

لا تعمل إعادة توجيه المسار العكسي للبث الأحادي (uRPF) بشكل جيد مع منافذ مضيف شبكة VLAN الخاصة، لذلك يجب ألا يتم إستخدام uRPF بالاشتراك مع شبكة PVLAN.

هناك إصلاح لهذه المشكلة، ويتحقق ذلك من خلال قوائم التحكم في الوصول إلى شبكة VLAN التي تم تكوينها على شبكات VLAN الأساسية. توفر دراسة الحالة قوائم التحكم في الوصول إلى شبكة VLAN التي يلزم تكوينها على شبكة VLAN الأساسية لإسقاط حركة المرور التي تم إنشاؤها بواسطة الشبكة الفرعية نفسها وإعادة التوجيه إلى الشبكة الفرعية نفسها.

في بعض بطاقات الخط، يخضع تكوين تعيينات / خرائط / منافذ توصيل شبكات VLAN الخاصة لبعض القيود حيث يجب أن تنتمي تعيينات شبكات VLAN المتعددة إلى دوائر مدمجة خاصة بتطبيق منفذ مختلف (ASICs) من أجل الحصول على تكوين. تتم إزالة هذه القيود على ملف ASIC الجديد للمنفذ 3. يرجى الرجوع إلى أحدث وثائق Catalyst switch على تكوين البرامج للحصول على هذه التفاصيل.

مثال لدراسات الحالة

يصف القسم التالي ثلاث دراسات حالة، نعتقد أنها تمثل معظم عمليات التنفيذ وتقدم التفاصيل المتعلقة بنشر أمان شبكات VLAN الخاصة وقوائم التحكم في الوصول إلى شبكة VLAN.

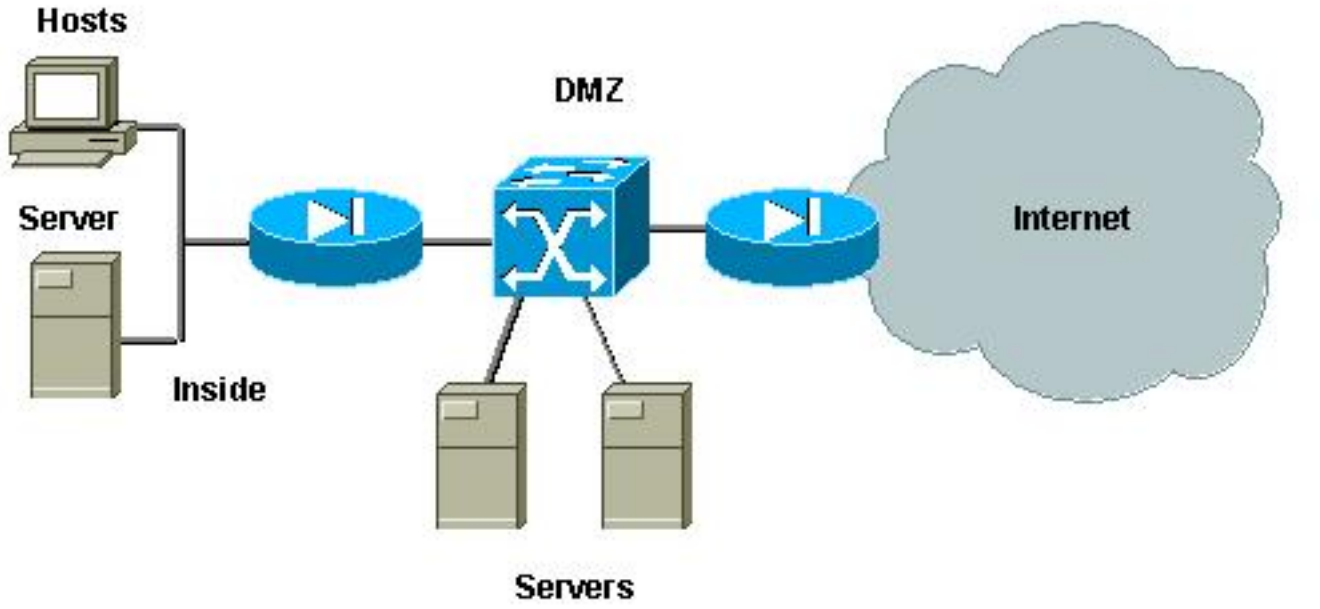
هذه السيناريوهات هي:

- Pass-Through DMZ
- DMZ خارجي
- مركز VPN بالتوازي مع جدار الحماية

Pass-Through DMZ

وهذا واحد من السيناريوهات الأكثر انتشارا. في هذا المثال، يتم تنفيذ المنطقة المجردة من السلاح كمنطقة عبور بين موجهات جدار حماية كما هو موضح في الصورة أدناه.

الشكل 2: مرور عبر المنطقة المنزوعة السلاح



في هذا المثال، من المفترض أن يتم الوصول إلى خوادم DMZ من قبل المستخدمين الخارجيين والداخليين على حد سواء، ولكنها لا تحتاج إلى الاتصال ببعضها البعض. وفي بعض الحالات، تحتاج خوادم DMZ إلى فتح نوع ما من الاتصال بمضيف داخلي. وفي الوقت نفسه، من المفترض أن يدخل العملاء الداخليون الإنترنت دون قيود. وسيكون المثال الجيد هو المثال مع خوادم الويب في المنطقة المنزوعة السلاح، والتي تحتاج إلى الاتصال بخادم قاعدة بيانات موجود في الشبكة الداخلية، والحصول على عملاء من الداخل يصلون إلى الإنترنت.

يتم تكوين جدار الحماية الخارجي للسماح بالاتصالات الواردة إلى الخوادم الموجودة في المنطقة DMZ، ولكن عادة لا يتم تطبيق أي عامل تصفية أو قيود على حركة المرور الصادرة، وخاصة حركة المرور التي تم إنشاؤها في المنطقة DMZ. وكما ناقشنا في وقت سابق في هذا المستند، يمكن أن يؤدي ذلك إلى تسهيل نشاط المهاجم لسببين: أولهما أنه بمجرد أختراق أحد الأجهزة المضيفة للمنطقة العسكرية المجردة من السلاح، يتم فضح جميع الأجهزة المضيفة الأخرى للمنطقة المجردة من السلاح؛ وثانيهما، أنه يمكن للمهاجم إستغلال الاتصال الصادر بسهولة.

ونظرا لأن خوادم DMZ لا تحتاج إلى التحدث إلى بعضها البعض، فإن التوصية هي التأكد من عزلها عند المستوى الثاني. سيتم تعريف منافذ الخوادم على أنها منافذ PVLANs المعزولة، بينما سيتم تعريف المنافذ المتصلة بجدران الحماية على أنها مختلطة. تعريف شبكة VLAN أساسية لجدران الحماية، وستقوم شبكة VLAN الثانوية لخوادم DMZ بتحقيق ذلك.

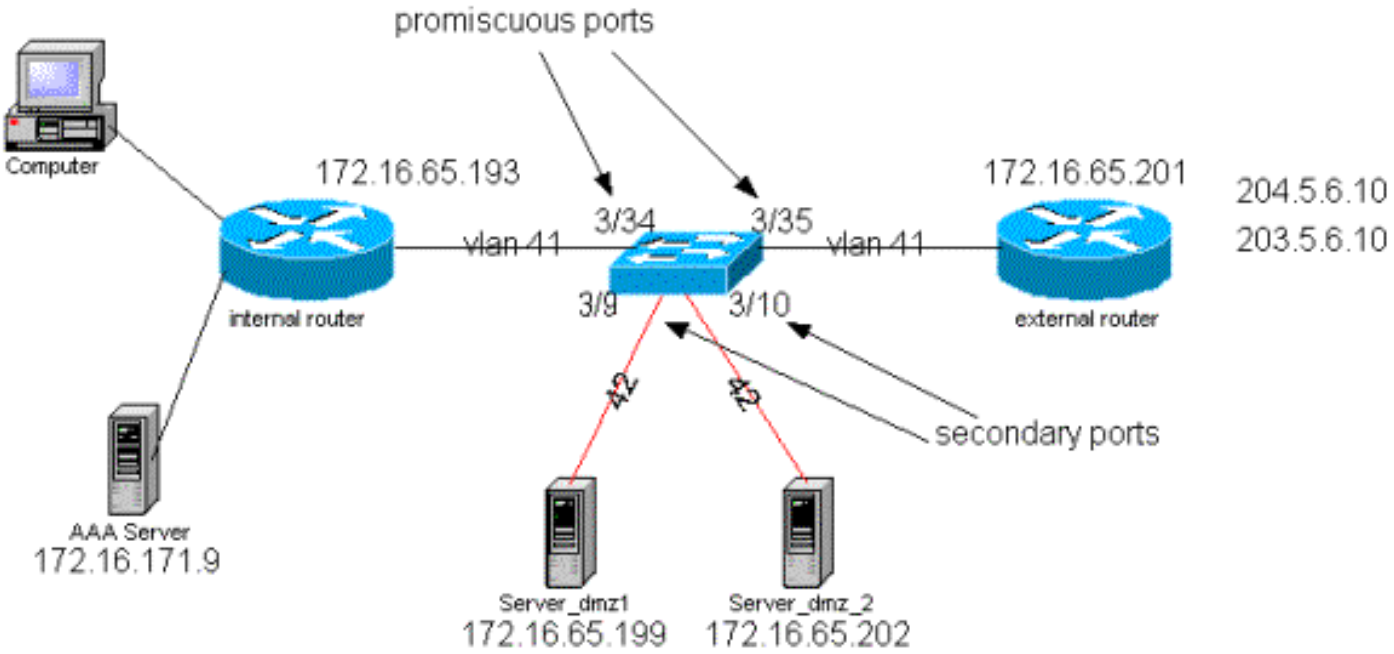
سيتم إستخدام قوائم التحكم في الوصول إلى شبكة VLAN للتحكم في حركة المرور التي تم إنشاؤها في DMZ. وهذا سيمنع المهاجم من فتح اتصال صادر غير مشروع. من المهم أن تضع في الاعتبار أن خوادم DMZ لن تحتاج فقط إلى الرد على حركة المرور المقابلة لجلسات عمل العميل، ولكنها ستحتاج أيضا إلى بعض الخدمات الإضافية، مثل نظام اسم المجال (DNS) واكتشاف مسار وحدة الإرسال القصوى (MTU). لذلك، يجب أن تسمح قائمة التحكم في الوصول (ACL) بجميع الخدمات التي تحتاجها خوادم DMZ.

مرور الاختبار DMZ

في بيئة الاختبار التي قمنا بها، قمنا بتطبيق مقطع DMZ مع موجهين تم تكوينهما كخوادم صغيرة و server_dmz1 و server_dmz2. من المفترض أن يتم الوصول إلى هذه الخوادم من خلال العملاء الخارجيين وكذلك من داخل العملاء، ويتم مصادقة جميع إتصالات HTTP باستخدام خادم RADIUS داخلي (CiscoSecure ACS ل UNIX). تم

تكوين كل من الموجهات الداخلية والخارجية كجدران حماية لعامل تصفية الحزم. وتوضح الصورة التالية قاع الاختبار، بما في ذلك مخطط العنونة المستخدم.

الشكل 3: إجتياز إختبار المنطقة المنزوعة السلاح



تجمع القائمة التالية خطوات التكوين الأساسية لشبكات VLAN الخاصة. استعملت المادة حفازة 6500 كال l2 مفتاح في ال DMZ.

- يتصل server_dmz_1 بالمنفذ 9/3
- يتصل server_dmz_2 بالمنفذ 10/3
- الموجه الداخلي متصل بالمنفذ 34/3
- الموجه الخارجي متصل بالمنفذ 35/3

اخترنا شبكات VLAN التالية:

- 41 هي شبكة VLAN الأساسية
- 42 هو شبكة VLAN المعزولة

تكوين شبكة VLAN الخاصة

يعمل التكوين التالي على تعيين شبكات VLAN الخاصة على المنافذ المعنية.

```
ecomm-6500-2 (enable) set vlan 41 pvlan primary
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 41 configuration successful

ecomm-6500-2 (enable) sh pvlan
Primary Secondary Secondary-Type   Ports
------------ ---------------- --------- -------
-         -       41
ecomm-6500-2 (enable) set vlan 42 pvlan isolated
,VTP advertisements transmitting temporarily stopped
.and will resume after the command finishes
Vlan 42 configuration successful
ecomm-6500-2 (enable) set pvlan 41 42 3/9-10
```

```
:Successfully set the following ports to Private Vlan 41,42
3/9-10

ecomm-6500-2 (enable) set pvlan mapping 41 42 3/35
Successfully set mapping between 41 and 42 on 3/35
ecomm-6500-2 (enable) set pvlan mapping 41 42 3/34
Successfully set mapping between 41 and 42 on 3/34

        Port  Name                 Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
 server_dmz1       connected  41,42      a-half  a-10 10/100BaseTX  3/9
 server_dmz2       connected  41,42      a-half  a-10 10/100BaseTX 3/10

   to_6500_1         connected   41        auto  auto 10/100BaseTX 3/34
 external_router_dm connected  41        a-half  a-10 10/100BaseTX 3/35
```

تكوين VACL على شبكة VLAN الأساسية

يعد هذا القسم أمرا بالغ الأهمية لتحسين الأمان في المنطقة المنزوعة السلاح. كما هو موضح في قسم قيود قوائم التحكم في الوصول إلى شبكة VLAN (VACLs) وشبكات VLAN الخاصة، حتى إذا كانت الخوادم تنتمي إلى شبكتي VLAN ثانويتين مختلفتين أو إلى شبكة VLAN المعزولة نفسها، فلا تزال هناك طريقة يمكن للمهاجم إستخدامها لجعلها تتصل ببعضها البعض. إذا حاولت الخوادم الاتصال مباشرة، فلن تتمكن من القيام بذلك في المستوى الثاني بسبب شبكات VLAN الخاصة. إذا تم أختراق الخوادم ثم تم تكوينها من قبل الدخيل بطريقة يتم من خلالها إرسال حركة مرور البيانات لنفس الشبكة الفرعية إلى الموجه، فسيقوم هذا الأمر بإعادة توجيه حركة مرور البيانات على الشبكة الفرعية نفسها، وبالتالي إحباط الغرض من شبكات VLAN الخاصة.

لذلك، يحتاج VACL أن يكون شكلت على ال VLAN أساسي (ال VLAN أن يحمل الحركة مرور من المسحاج تخديد) مع التالي سياسة:

- السماح بحركة المرور التي يكون مصدر IP هو IP الخاص بالموجه
- رفض حركة المرور باستخدام كل من عناوين IP للمصدر والوجهة التي تكون الشبكة الفرعية DMZ
- السماح ببقية حركة المرور

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
set security acl ip protect_pvlan
------------------------------------------------
permit ip host 172.16.65.193 any .1
permit ip host 172.16.65.201 any .2
deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15 .3
permit ip any any .4

ecomm-6500-2 (enable) sh sec acl
ACL                                 Type VLANS
----- ----  ---------------------------------
protect_pvlan                       IP   41
```

لن تؤثر قائمة التحكم في الوصول (ACL) هذه على حركة المرور التي تم إنشاؤها بواسطة الخوادم؛ ولن تمنع الموجهات إلا من توجيه حركة مرور البيانات الواردة من الخوادم مرة أخرى إلى شبكة VLAN نفسها. تتيح الجملتان الأولان للموجهات إرسال رسائل مثل إعادة توجيه ICMP أو ICMP الذي يتعذر الوصول إليه إلى الخوادم.

تكوين VACL على شبكة VLAN الثانوية

يتم إستخدام سجلات التكوين التالية لإظهار كيفية إعداد قائمة التحكم في الوصول إلى شبكة VACL لتصفية حركة مرور البيانات التي تم إنشاؤها بواسطة الخوادم. من خلال تكوين قائمة التحكم في الوصول إلى شبكة VACL هذه، نريد تحقيق ما يلي:

- السماح **إختبار الاتصال** من الخوادم (السماح **بالصدى**)
- منع ردود **الارتداد** من مغادرة الخوادم

- السماح باتصالات HTTP التي تم إنشاؤها من الخارج
- السماح لحركة مرور مصادقة RADIUS (منفذ UDP 1645) والمحاسبة (منفذ UDP 1646)
- السماح بحركة مرور DNS (UDP ميناء 53)

نريد أن نمنع كل المرور.

فيما يتعلق بالتجزئة، نفترض ما يلي على جزء الخادم:

- لن تقوم الخوادم بإنشاء حركة مرور مجزأة
- قد تتلقى الخوادم حركة مرور مجزأة

بافتراض تصميم الأجهزة ل PFC من المشرف 1 من Catalyst 6500، فمن الأفضل رفض أجزاء ICMP بشكل صريح السبب هو أن أجزاء ICMP و echo-reply يتم اعتبارها نفسها بواسطة الجهاز، وبشكل افتراضي تتم برمجة الأجهزة للسماح بالشظايا بشكل صريح. لذلك إذا كنت تريد إيقاف حزم الرد على الصدى من ترك الخوادم، فعليك بشكل صريح تكوين هذا مع **رفض** الخط **ل ICMP أي جزء**.

```
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out deny icmp any any fragment
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.199 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit icmp host 172.16.65.202 any echo
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.199 eq 80 any
                                                                                    established
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit tcp host 172.16.65.202 eq 80 any
                                                                                    established
          ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
                                                                  eq 1645 host 172.16.171.9 eq 1645
          ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
                                                                  eq 1645 host 172.16.171.9 eq 1645
          ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199
                                                                  eq 1646 host 172.16.171.9 eq 1646
          ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202
                                                                  eq 1646 host 172.16.171.9 eq 1646
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.199 any eq 53
ecomm-6500-2 (enable) Set sec acl ip dmz_servers_out permit udp host 172.16.65.202 any eq 53

                                                ecomm-6500-2 (enable) Commit sec acl all

                                          ecomm-6500-2 (enable) Set sec acl map dmz_servers_out 42

                                                        ecomm-6500-2 (enable) sh sec acl
                                                ACL                                 Type VLANS
                                                ----- ----  --------------------------------
                                                   protect_pvlan                     IP   41
                                                   dmz_servers_out                   IP   42

                                              ecomm-6500-2 (enable) sh sec acl info dmz_servers_out
                                                             set security acl ip dmz_servers_out
                                                  ---------------------------------------------------
                                                                        deny icmp any any fragment .1
                                                                  permit icmp host 172.16.65.199 any echo .2
                                                                  permit icmp host 172.16.65.202 any echo .3
                                                        permit tcp host 172.16.65.199 eq 80 any established .4
                                                        permit tcp host 172.16.65.202 eq 80 any established .5
                                    permit udp host 172.16.65.199 eq 1645 host 172.16.171.9 eq 1645 .6
                                    permit udp host 172.16.65.202 eq 1645 host 172.16.171.9 eq 1645 .7
                                    permit udp host 172.16.65.199 eq 1646 host 172.16.171.9 eq 1646 .8
                                    permit udp host 172.16.65.202 eq 1646 host 172.16.171.9 eq 1646 .9
                                                  permit udp host 172.16.65.199 any eq 53 .10
                                                  permit udp host 172.16.65.202 any eq 53 .11
```

[إختبار التكوين]

تم التقاط الإخراج التالي عند شبكات VLAN الخاصة التي تم تكوينها ولكن لم يتم تطبيق قائمة التحكم في الوصول إلى شبكة VLAN بعد. يوضح هذا الاختبار أنه من الموجه الخارجي يمكن للمستخدم **إختبار اتصال** الموجه الداخلي بالإضافة إلى الخوادم.

```
external_router#ping 172.16.65.193
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds
!!!!

external_router#ping 172.16.65.202
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
external_router#ping 172.16.65.199
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

يوضح المثال التالي أننا قادرون على **إختبار الاتصال** من الخوادم إلى الشبكة الخارجية، البوابة الافتراضية، ولكن ليس الخوادم التي تنتمي إلى شبكة VLAN الثانوية نفسها.

```
server_dmz1#ping 203.5.6.10

.Type escape sequence to abort
  :Sending 5, 100-byte ICMP Echos to 203.5.6.10, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds
!!!!!
  Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

server_dmz1#ping 172.16.65.202
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.202, timeout is 2 seconds
.....
(Success rate is 0 percent (0/5
```

بعد تعيين قوائم التحكم في الوصول إلى شبكة VACL (قوائم التحكم في الوصول إلى شبكة VLAN)، لن ينجح **إختبار الاتصال** من الموجه الخارجي بعد الآن:

```
external_router#ping 172.16.65.199
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.199, timeout is 2 seconds
.....
(Success rate is 0 percent (0/5
```

يوضح المثال التالي الخادم الذي يستقبل طلبات HTTP GET من الشبكة الداخلية:

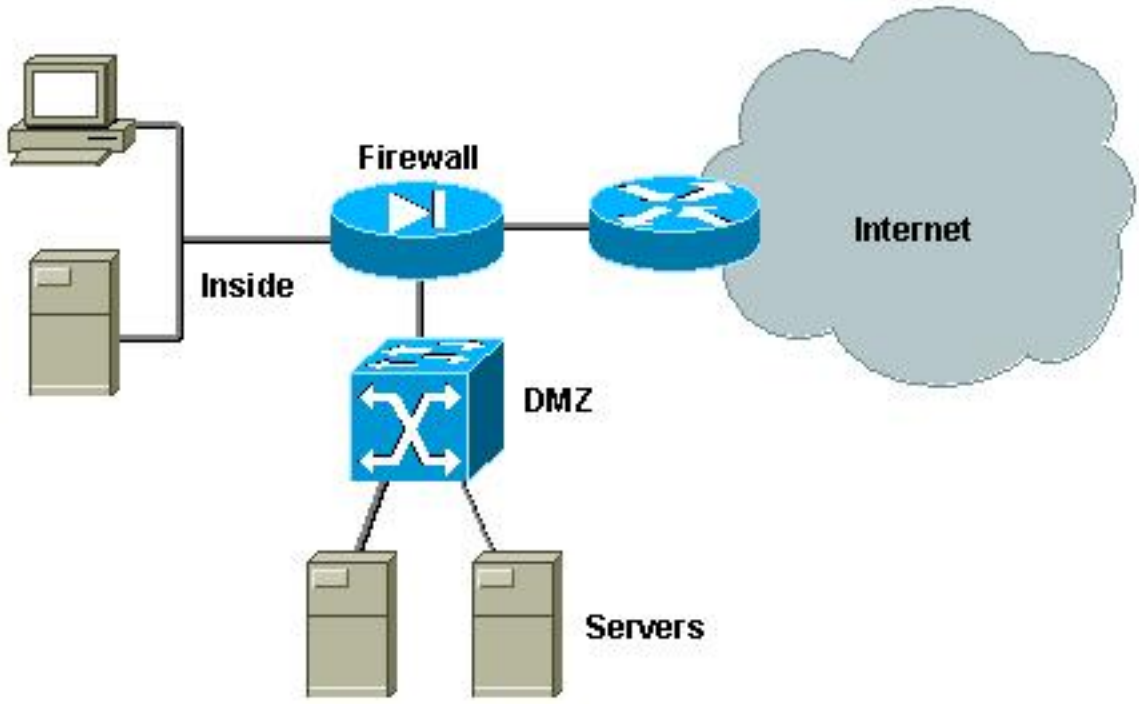
```
server_dmz1#debug ip http url
    HTTP URL debugging is on
server_dmz1#debug ip hhtp tran
  HTTP transactions debugging is on
server_dmz1#debug ip http auth
HTTP Authentication debugging is on
server_dmz1#
```

```
                                                '/' Mar  7 09:24:03.092 PST: HTTP: parsed uri*
                                            Mar  7 09:24:03.092 PST: HTTP: client version 1.0*
                                        Mar  7 09:24:03.092 PST: HTTP: parsed extension Connection*
                                            Mar  7 09:24:03.092 PST: HTTP: parsed line  Keep-Alive*
                                        Mar  7 09:24:03.092 PST: HTTP: parsed extension User-Agent*
    (Mar  7 09:24:03.092 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u*
                                              Mar  7 09:24:03.092 PST: HTTP: parsed extension Host*
                                           Mar  7 09:24:03.092 PST: HTTP: parsed line  172.16.65.199*
                                              Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept*
/Mar  7 09:24:03.092 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image*
                                    Mar  7 09:24:03.092 PST: HTTP: parsed extension Accept-Encoding*
                                             Mar  7 09:24:03.092 PST: HTTP: parsed line  gzip*
                                    Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Language*
                                              Mar  7 09:24:03.096 PST: HTTP: parsed line  en*
                                     Mar  7 09:24:03.096 PST: HTTP: parsed extension Accept-Charset*
                                     Mar  7 09:24:03.096 PST: HTTP: parsed line  iso-8859-1,*,utf-8*
      '/' Mar  7 09:24:03.096 PST: HTTP: Authentication for url '/' '/' level 15  privless*
 Mar  7 09:24:03.096 PST: HTTP: authentication required, no authentication information was*
                                                                                      provided
                                           Mar  7 09:24:03.096 PST: HTTP: authorization rejected*
                                                  '/' Mar  7 09:24:22.528 PST: HTTP: parsed uri*
                                              Mar  7 09:24:22.532 PST: HTTP: client version 1.0*
                                          Mar  7 09:24:22.532 PST: HTTP: parsed extension Connection*
                                              Mar  7 09:24:22.532 PST: HTTP: parsed line  Keep-Alive*
                                          Mar  7 09:24:22.532 PST: HTTP: parsed extension User-Agent*
    (Mar  7 09:24:22.532 PST: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u*
                                            Mar  7 09:24:22.532 PST: HTTP: parsed extension Host*
                                         Mar  7 09:24:22.532 PST: HTTP: parsed line  172.16.65.199*
                                            Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept*
/Mar  7 09:24:22.532 PST: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image*
                                    Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Encoding*
                                             Mar  7 09:24:22.532 PST: HTTP: parsed line  gzip*
                                    Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Language*
                                              Mar  7 09:24:22.532 PST: HTTP: parsed line  en*
                                     Mar  7 09:24:22.532 PST: HTTP: parsed extension Accept-Charset*
                                     Mar  7 09:24:22.532 PST: HTTP: parsed line  iso-8859-1,*,utf-8*
                                      Mar  7 09:24:22.532 PST: HTTP: parsed extension Authorization*
                                     Mar  7 09:24:22.532 PST: HTTP: parsed authorization type Basic*
      '/' Mar  7 09:24:22.532 PST: HTTP: Authentication for url '/' '/' level 15  privless*
Mar  7 09:24:22.532 PST: HTTP: Authentication username = 'martin' priv-level = 15 auth-type =*
                                                                                          aaa
                                                '' Mar  7 09:24:22.904 PST: HTTP: received GET*
```

DMZ خارجي

وربما يكون سيناريو المنطقة المنزوعة السلاح الخارجي هو التنفيذ الأكثر قبولا وانتشارا. يتم تنفيذ DMZ خارجي باستخدام واجهة واحدة أو أكثر من واجهات جدار الحماية، كما هو موضح الشكل أدناه.

الشكل 4: المنطقة المنزوعة السلاح الخارجية



عادة ما تكون متطلبات المناطق التجارية المعينة هي نفسها بغض النظر عن تنفيذ التصميم. وكما هو الحال في الحالة السابقة، من المفترض أن تكون خوادم DMZ قابلة للوصول إليها من العملاء الخارجيين وكذلك من الشبكة الداخلية. ستحتاج خوادم DMZ في نهاية المطاف إلى الوصول إلى بعض الموارد الداخلية، وليس من المفترض أن تتحدث مع بعضها البعض. وفي الوقت نفسه، يجب عدم بدء حركة مرور البيانات من المنطقة المجردة من السلاح إلى الإنترنت، ويجب على خوادم DMZ هذه الرد فقط على حركة المرور المقابلة للاتصالات الواردة.

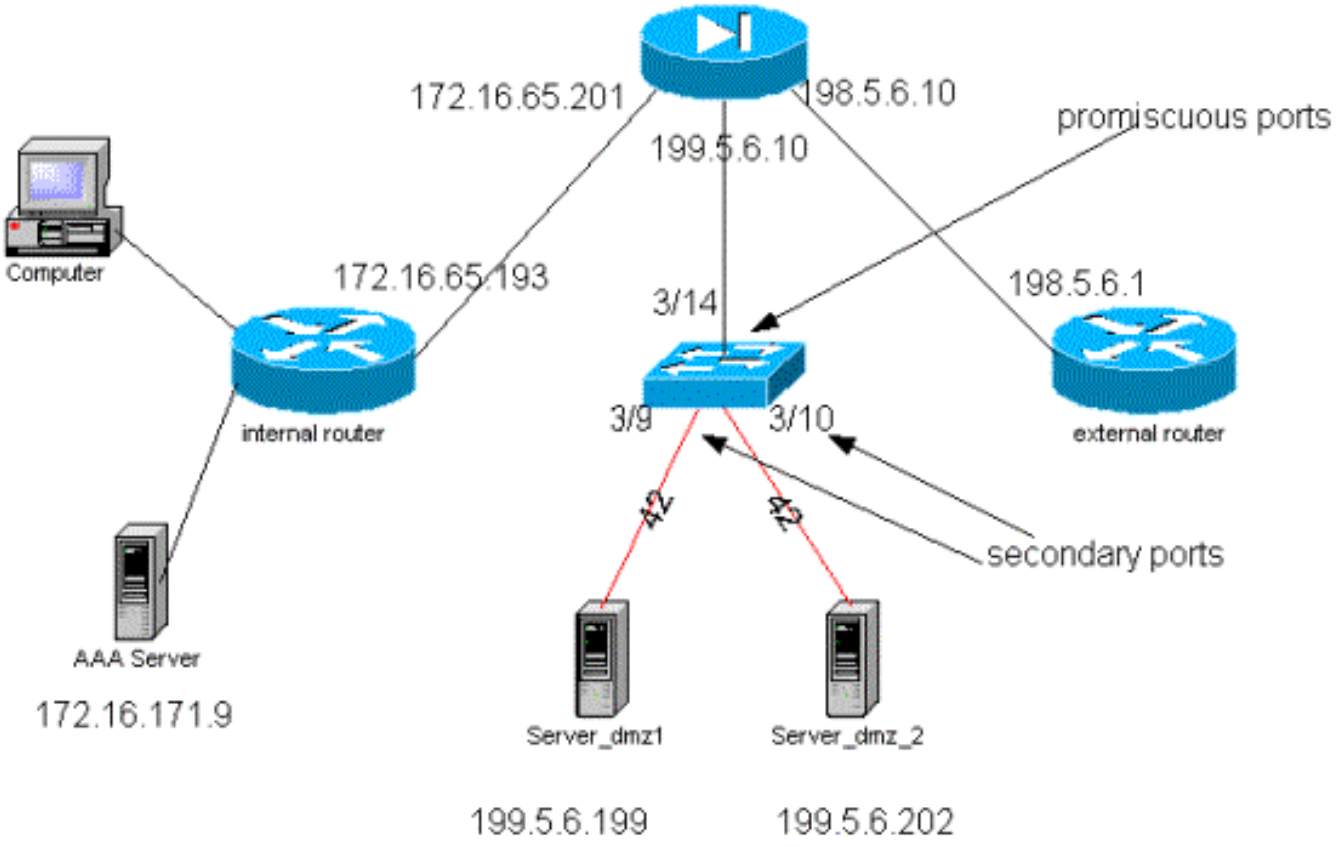
وكما هو الحال في دراسة الحالة السابقة، تتمثل خطوة التكوين الأولى في تحقيق العزل عند المستوى الثاني باستخدام شبكات VLAN الخاصة، والتأكد من أن خوادم DMZ لا يمكنها التحدث إلى بعضها البعض بينما يمكن للمضيفين الداخليين والخارجيين الوصول إليها. يتم تنفيذ هذا الإجراء من خلال تعيين الخوادم في شبكة VLAN الثانوية باستخدام المنافذ المعزولة. يجب تحديد جدار الحماية في شبكة VLAN أساسية مع منفذ مختلط. سيكون جدار الحماية الجهاز الوحيد ضمن شبكة VLAN الأساسية هذه.

تتمثل الخطوة الثانية في تحديد قوائم التحكم في الوصول (ACL) للتحكم في حركة المرور التي تم إنشاؤها في DMZ. عند تحديد قوائم التحكم في الوصول (ACL) هذه، نحتاج إلى التأكد من أنه مسموح بحركة المرور الضرورية فقط.

إختبار DMZ الخارجي

توضح الصورة التالية قاع الاختبار الذي تم تنفيذه لدراسة الحالة هذه، حيث إستخدمنا جدار حماية PIX مع واجهة ثالثة ل DMZ. يتم إستخدام نفس مجموعة الموجهات كخوادم ويب، وتتم مصادقة جميع جلسات HTTP باستخدام خادم RADIUS نفسه.

الشكل 5: سرير إختبار DMZ الخارجي



بالنسبة لهذا السيناريو، نقوم بإرفاق المقتطفات الأكثر إثارة للاهتمام من ملفات التكوين فقط، نظرا لأنه قد تم شرح تكوينات شبكات VLAN الخاصة و VACL بالتفصيل في دراسة الحالة السابقة.

تكوين PIX

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
ip address outside 198.5.6.10 255.255.255.0
ip address inside 172.16.65.201 255.255.255.240
ip address dmz 199.5.6.10 255.255.255.0
global (outside) 1 198.5.6.11
global (dmz) 1 199.5.6.11
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 199.5.6.199 199.5.6.199 netmask 255.255.255.255 0 0
static (dmz,outside) 199.5.6.202 199.5.6.202 netmask 255.255.255.255 0 0
static (inside,dmz) 172.16.171.9 172.16.171.9 netmask 255.255.255.255 0 0
static (inside,dmz) 171.68.10.70 171.68.10.70 netmask 255.255.255.255 0 0
static (inside,dmz) 171.69.0.0 171.69.0.0 netmask 255.255.0.0 0 0
conduit permit tcp host 199.5.6.199 eq www any
conduit permit tcp host 199.5.6.202 eq www any
conduit permit udp any eq domain any
conduit permit icmp any any echo-reply
conduit permit icmp any any unreachable
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.202
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.202
conduit permit icmp any host 199.5.6.199 echo
conduit permit icmp any host 199.5.6.202 echo
route outside 0.0.0.0 0.0.0.0 198.5.6.1 1
route inside 171.69.0.0 255.255.0.0 172.16.65.193 1
route inside 171.68.0.0 255.255.0.0 172.16.65.193 1
```

```
route inside 172.16.0.0 255.255.0.0 172.16.65.193 1
```

تهيئة RADIUS

تكوين *NAS*

```
aaa new-model
aaa authentication login default radius local
aaa authentication login consoleauth none
aaa authorization exec default radius local
aaa authorization exec consoleautho none
aaa accounting exec default start-stop radius
aaa accounting exec consoleacct none
radius-server host 172.16.171.9 auth-port 1645 acct-port 1646
radius-server key cisco123
!
line con 0
exec-timeout 0 0
password ww
authorization exec consoleautho
accounting exec consoleacct
login authentication consoleauth
transport input none
line aux 0
line vty 0 4
password ww
!
end
```

RADIUS Server CSUX

```
User Profile Information
}user = martin
profile_id = 151
profile_cycle = 5
} radius=Cisco
} =check_items
cisco=2
{
} =reply_attributes
6=6
{
{

{

User Profile Information
}user = NAS.172.16.65.199
profile_id = 83
profile_cycle = 2
"NASName="172.16.65.199
"SharedSecret="cisco123
"RadiusVendor="Cisco
"Dictionary="DICTIONARY.Cisco

{
```

تكوين Catalyst

يجب ملاحظة أنه في هذا التكوين لا توجد حاجة لتكوين قائمة تحكم في الوصول إلى شبكة VLAN الأساسية لأن PIX لا يقوم بإعادة توجيه حركة مرور البيانات من نفس الواجهة التي جاءت منها. سيكون قائمة التحكم في الوصول

إلى شبكة VLAN (قائمة التحكم في الوصول إلى شبكة VACL) كما هو موضح في تكوين قائمة التحكم في الوصول إلى شبكة VLAN الأساسية زائدا.

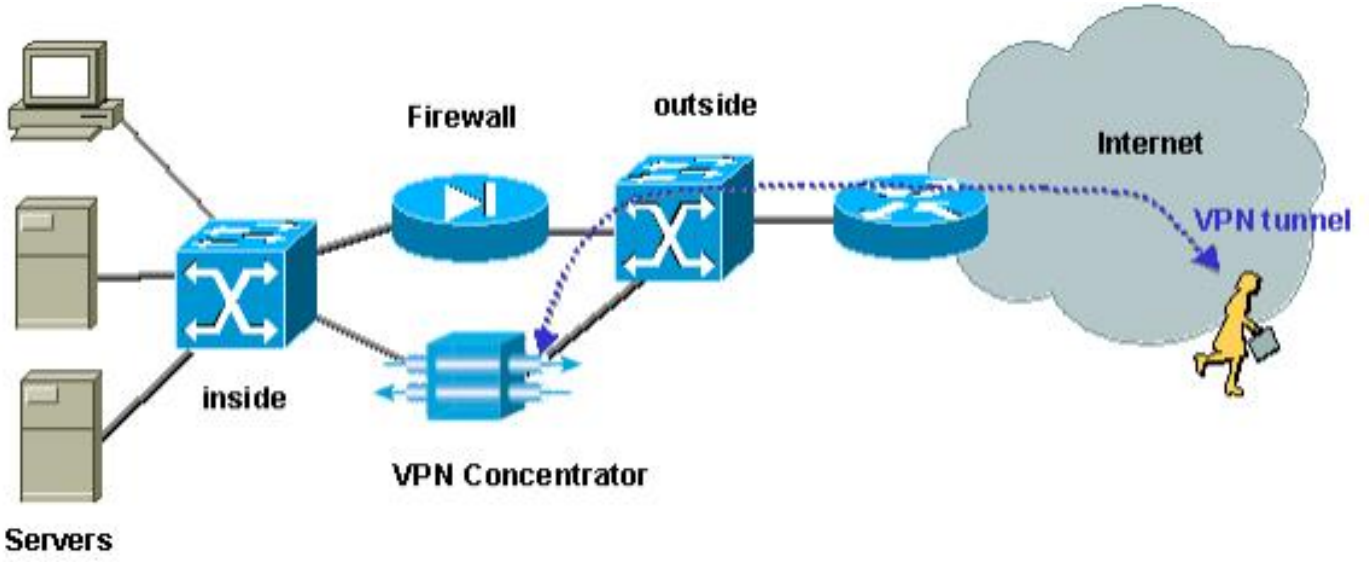
```
                                        set security acl ip dmz_servers_out
                                    ---------------------------------------------
                                                deny icmp any any fragment .1
                                        permit icmp host 199.5.6.199 any echo .2
                                        permit icmp host 199.5.6.202 any echo .3
                                    permit tcp host 199.5.6.199 eq 80 any established .4
                                    permit tcp host 199.5.6.202 eq 80 any established .5
                          permit udp host 199.5.6.199 eq 1645 host 172.16.171.9 eq 1645 .6
                          permit udp host 199.5.6.202 eq 1645 host 172.16.171.9 eq 1645 .7
                          permit udp host 199.5.6.199 eq 1646 host 172.16.171.9 eq 1646 .8
                          permit udp host 199.5.6.202 eq 1646 host 172.16.171.9 eq 1646 .9
                                    permit udp host 199.5.6.199 any eq 53 .10
                                    permit udp host 199.5.6.202 any eq 53 .11
                                              ecomm-6500-2 (enable) sh pvlan
                                     Primary Secondary Secondary-Type   Ports
                                ------------ ---------------- --------- -------
                                      isolated         3/9-10        42      41

                                        ecomm-6500-2 (enable) sh pvlan mapping
                                                      Port Primary Secondary
                                                      ---------- ------- ----
                                                            42      41 3/14
                                                            42      41 3/34
                                                            42      41 3/35
                                                   ecomm-6500-2 (enable) sh port
        Port  Name                 Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
server_dmz1        connected  41,42      a-half  a-10 10/100BaseTX  3/9
server_dmz2        connected  41,42      a-half  a-10 10/100BaseTX 3/10
to_pix_port_2      connected  41           full   100 10/100BaseTX 3/14
external_router_dm notconnect 41           auto  auto 10/100BaseTX 3/35
```

مركز VPN بالتوازي مع جدار الحماية

عند تنفيذ شبكات Access الخاصة الظاهرية (VPN)، لا شك أن التصميم المتوازي (الموضح في الصورة أدناه) هو أحد الأساليب المفضلة. يفضل العملاء عادة أسلوب التصميم هذا نظرا لأنه سهل التنفيذ ولا يؤثر بأي شكل تقريبا على البنية الأساسية الموجودة، ولأنه يتسم بسهولة التطوير نسبيا استنادا إلى مرونة الجهاز.

وفي النهج الموازي، يتصل مركز الشبكة الخاصة الظاهرية (VPN) بالأجزاء الداخلية والخارجية على حد سواء. تنتهي جميع جلسات الشبكة الخاصة الظاهرية (VPN) عند مركز التركيز دون المرور عبر جدار الحماية. يتوقع عادة أن يكون لعملاء شبكات VPN وصول غير مقيد إلى الشبكة الداخلية، ولكن يمكن في بعض الأحيان تقييد وصولهم إلى مجموعة من الخوادم الداخلية (مزرعة الخوادم). أحد الميزات المرغوب فيها هو فصل حركة مرور VPN عن حركة مرور الإنترنت العادية، على سبيل المثال، لا يسمح لعملاء VPN بالوصول إلى الإنترنت عبر جدار حماية الشركة.

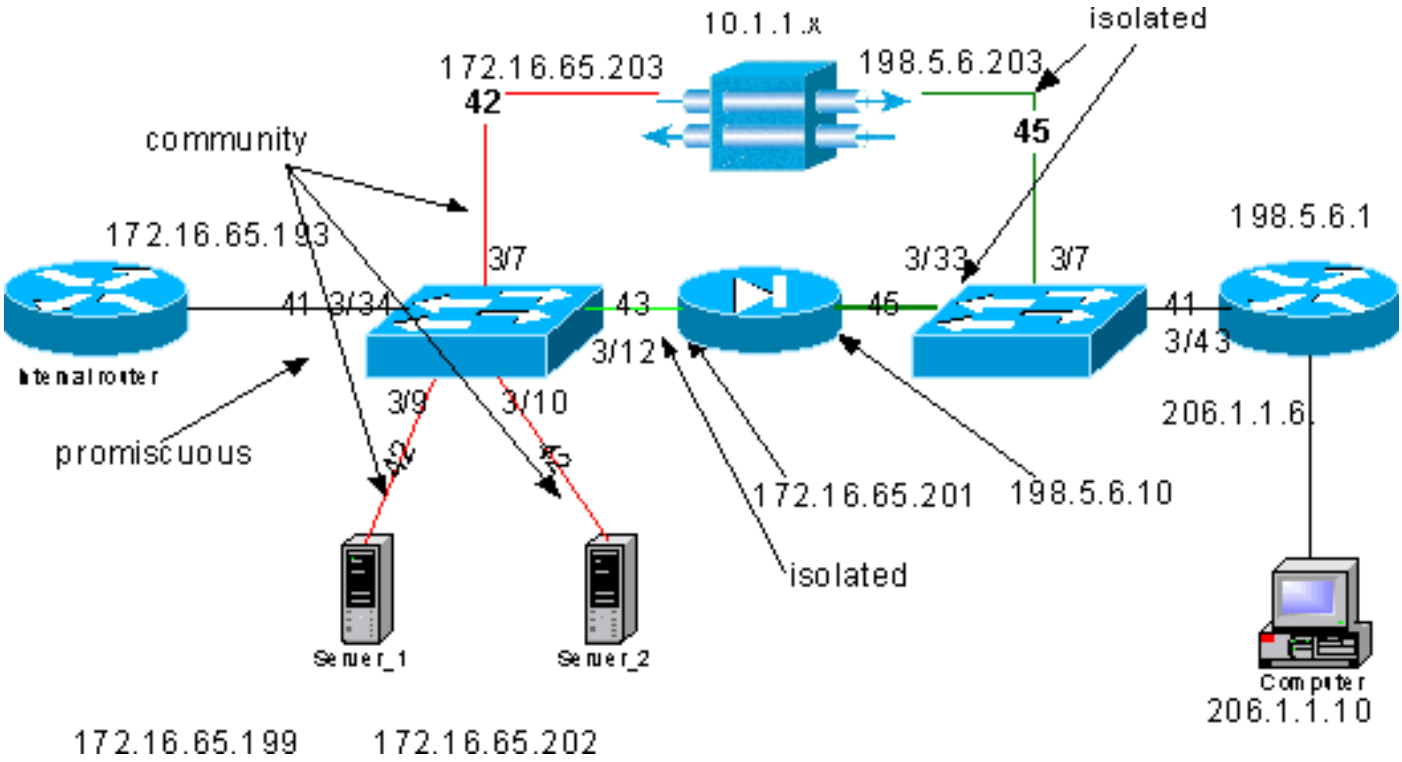
الشكل 6: مركز الشبكة الخاصة الظاهرية (VPN) بمحاذاة جدار الحماية



إختبار مركز الشبكة الخاصة الظاهرية (VPN) بالتوازي مع جدار الحماية

في هذا المثال، إستخدمنا برنامج تركيز VPN 5000، والذي تم تثبيته بالتوازي مع جدار حماية PIX. تم تثبيت الموجهين اللذين تم تكوينهما كخوادم ويب في المقطع الداخلي كمزرعة خوادم داخلية. يسمح لعملاء VPN فقط بالوصول إلى مزرعة الخوادم، ويجب فصل حركة مرور الإنترنت عن حركة مرور IPSec) VPN). يظهر الشكل التالي سرير الاختبار.

الشكل 7: مركز الشبكة الخاصة الظاهرية (VPN) بالتوازي مع قاع إختبار الجدار الناري



وفي هذا السيناريو لدينا مجالان رئيسيان محل اهتمام:

- المحول الداخلي L2
- المحول الخارجي L2

يتم تحديد تدفقات حركة مرور البيانات لمحول L2 الداخلي استنادا إلى الجمل التالية:

- يتمتع عملاء شبكة VPN بالوصول الكامل إلى مجموعة محددة مسبقا من الخوادم الداخلية (مزرعة الخوادم)
- يسمح للعملاء الداخليين أيضا بالوصول إلى مزرعة الخوادم

- يتمتع العملاء الداخليون بإمكانية الوصول غير المقيد إلى الإنترنت
- يجب عزل حركة المرور الواردة من مركز VPN عن جدار حماية PIX

يتم تحديد تدفقات حركة مرور البيانات لمحول L2 الخارجي على النحو التالي:

- يجب أن تكون حركة المرور القادمة من الموجه قادرة على الانتقال إما إلى مركز الشبكة الخاصة الظاهرية (VPN) أو إلى PIX
- يجب عزل حركة المرور الواردة من PIX عن حركة المرور القادمة من شبكة VPN

بالإضافة إلى ذلك، من الممكن أن يريد المسؤول منع حركة مرور البيانات من الشبكة الداخلية من أن تكون قادرة على شق طريقها إلى مضيفي الشبكة الخاصة الظاهرية (VPN)، ويمكن تحقيق ذلك من خلال قوائم التحكم في الوصول إلى شبكة VLAN التي تم تكوينها على شبكة VLAN الأساسية (سيقوم VACL بتصفية حركة مرور البيانات التي تترك من الموجه الداخلي فقط، ولن تتأثر حركة مرور أخرى).

تكوين شبكة PVLAN

بما أن الهدف الرئيسي في هذا التصميم هو إبقاء حركة المرور القادمة من PIX منفصلة عن حركة المرور القادمة من الخوادم ومن مركز VPN، فإننا نجهز PIX على شبكة VLAN مختلفة عن شبكة VLAN الخاصة التي تم تكوين الخوادم ومحشد VPN عليها.

يجب أن تكون حركة المرور الواردة من الشبكة الداخلية قادرة على الوصول إلى مزرعة الخوادم بالإضافة إلى مركز الشبكة الخاصة الظاهرية (VPN) و PIX. ونتيجة لذلك، سيكون المنفذ الذي يتصل بالشبكة الداخلية منفذا مختلطا.

تنتمي الخوادم ومجمع الشبكة الخاصة الظاهرية (VPN) إلى شبكة VLAN الثانوية نفسها لأنها ستكون قادرة على الاتصال ببعضها البعض.

بالنسبة للمحول الخارجي من المستوى الثاني، يتم توصيل الموجه الذي يوفر الوصول إلى الإنترنت (والذي ينتمي عادة إلى موفر خدمة الإنترنت (ISP)) بمنفذ مختلط بينما ينتمي مركز الشبكة الخاصة الظاهرية (VPN) وبروتوكول PIX إلى شبكات VLAN نفسها الخاصة والمعزولة (حتى لا يمكنها تبادل أي حركة مرور). من خلال القيام بذلك، يمكن لحركة المرور الواردة من مزود الخدمة أخذ إما المسار إلى مركز الشبكة الخاصة الظاهرية (VPN) أو المسار إلى PIX. يتميز مركز PIX و VPN بقدر أكبر من الحماية نظرا لعزلتهما.

تكوين شبكة VLAN الخاصة بمحول L2 الداخلي

```
                                                                  sh pvlan
      Primary Secondary Secondary-Type   Ports
----------- ---------- --------- -------
community        3/7,3/9-10        42       41
      isolated         3/12        43       41

                                        ecomm-6500-2 (enable) sh pvlan map
                                                Port Primary Secondary
                                                --------- ------- ----
                                                   42-43      41 3/34

                                                        ecomm-6500-2 (enable) sh port 3/7
        Port  Name                 Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
to_vpn_conc        connected  41,42      a-half  a-10 10/100BaseTX  3/7

                                                        ecomm-6500-2 (enable) sh port 3/9
        Port  Name                 Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
server_1           connected  41,42      a-half  a-10 10/100BaseTX  3/9
```

```
                                        ecomm-6500-2 (enable) sh port 3/10
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
server_2           connected  41,42      a-half  a-10 10/100BaseTX 3/10

                                        ecomm-6500-2 (enable) sh port 3/12
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
to_pix_intf1       connected  41,43      a-full a-100 10/100BaseTX 3/12


                                        ecomm-6500-2 (enable) sh pvlan map
                                                    Port Primary Secondary
                                                    --------- ------- ----
                                                       42-43      41 3/34

                                        ecomm-6500-2 (enable) sh port 3/34
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
to_int_router      connected  41         a-full a-100 10/100BaseTX 3/34
```

تكوين شبكة VLAN الخاصة بمحول L2 الخارجي

```
                                                                sh pvlan
                                        Primary Secondary Secondary-Type   Ports
                                    ------------ ---------- --------- -------
                                        isolated         3/7,3/33        45      41

                                             ecomm-6500-1 (enable) sh pvlan mapping
                                                    Port Primary Secondary
                                                    --------- ------- ----
                                                          45      41 3/43

                                         ecomm-6500-1 (enable) sh port 3/7
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
from_vpn           connected  41,45      a-half  a-10 10/100BaseTX  3/7

                                        ecomm-6500-1 (enable) sh port 3/33
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
to_pix_intf0       connected  41,45      a-full a-100 10/100BaseTX 3/33

                                        ecomm-6500-1 (enable) sh pvlan map
                                                    Port Primary Secondary
                                                    --------- ------- ----
                                                          45      41 3/43
                                        ecomm-6500-1 (enable) sh port 3/43
        Port  Name               Status     Vlan       Duplex Speed Type
------------ ----- ------ ---------- ---------- ------------------ -----
to_external_router connected  41         a-half  a-10 10/100BaseTX 3/43
```

إختبار التكوين

توضح هذه التجربة أنه يمكن للموجه الداخلي المرور عبر جدار الحماية والوصول إلى الموجه الخارجي (موجه جدار الحماية الخارجي الذي تكون واجهة الموجه 198.5.6.1).

```
ping 198.5.6.1
```

```
Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

توضح هذه التجربة ما يلي، كل ذلك من الخادم 1:

- يمكن للخادم 1 إختبار اتصال الموجه الداخلي:

```
server_1#ping 172.16.65.193

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.193, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- يمكن للخادم 1 إختبار اتصال الشبكة الخاصة الظاهرية (VPN):

```
server_1#ping 172.16.65.203

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.203, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

- يتعذر على الخادم 1 إختبار اتصال واجهة PIX الداخلية:

```
server_1#ping 172.16.65.201

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 172.16.65.201, timeout is 2 seconds
.....
(Success rate is 0 percent (0/5
```

- يتعذر على الخادم 1 إختبار اتصال الموجه الخارجي:

```
server_1#ping 198.5.6.1

.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds
.....
(Success rate is 0 percent (0/5
```

توضح التجربة التالية أنه يمكن فتح جلسات عمل HTTP من الشبكة الداخلية إلى مزرعة الخوادم.

```
server_2#
'/' 1w1d: HTTP: parsed uri
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
(1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
/1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
'/' 1w1d: HTTP: Authentication for url '/' '/' level 15  privless
1w1d: HTTP: authentication required, no authentication information was provided
1w1d: HTTP: authorization rejected
'/' 1w1d: HTTP: parsed uri
1w1d: HTTP: processing URL '/' from host 171.68.173.3
1w1d: HTTP: client version 1.0
```

```
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
(1w1d: HTTP: parsed line  Mozilla/4.7 [en] (X11; I; SunOS 5.5.1 sun4u
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
1w1d: HTTP: parsed extension Accept
/1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
1w1d: HTTP: parsed extension Authorization
1w1d: HTTP: parsed authorization type Basic
'/' 1w1d: HTTP: Authentication for url '/' '/' level 15  privless
1w1d: HTTP: Authentication username = 'maurizio' priv-level = 15 auth-type = aaa
'' 1w1d: HTTP: received GET
```

توضح التجربة التالية أن حركة مرور HTTP من شبكة VPN يمكن أن تشق طريقها إلى مزرعة الخوادم (لاحظ العنوان 10.1.1.1).

```
'/' 1w1d: HTTP: parsed uri
1w1d: HTTP: processing URL '/' from host 10.1.1.1
1w1d: HTTP: client version 1.0
1w1d: HTTP: parsed extension Connection
1w1d: HTTP: parsed line  Keep-Alive
1w1d: HTTP: parsed extension User-Agent
(1w1d: HTTP: parsed line  Mozilla/4.76 [en] (Windows NT 5.0; U
1w1d: HTTP: parsed extension Host
1w1d: HTTP: parsed line  172.16.65.202
\1w1d: HTTP: parsed extension Accept
/1w1d: HTTP: parsed line  image/gif, image/x-xbitmap, image/jpeg, image
1w1d: HTTP: parsed extension Accept-Encoding
1w1d: HTTP: parsed line  gzip
1w1d: HTTP: parsed extension Accept-Language
1w1d: HTTP: parsed line  en
1w1d: HTTP: parsed extension Accept-Charset
1w1d: HTTP: parsed line  iso-8859-1,*,utf-8
'/' 1w1d: HTTP: Authentication for url '/' '/' level 15  privless
1w1d: HTTP: authentication required, no authentication information was provided
```

وفيما يلي تكوين مركز الشبكة الخاصة الظاهرية (VPN):

```
[ IP Ethernet 0:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask = 255.255.255.240
IPAddress                = 172.16.65.203

[ General ]
IPsecGateway = 198.5.6.1
"DeviceName                = "VPN5008
"EnablePassword            = "ww
"Password                  = "ww
EthernetAddress          = 00:30:85:14:5c:40
DeviceType               = VPN 5002/8
ConcentratorConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from 171.68.173.3

[ IP Static ]
255.255.255.0 206.1.1.0
```

```
10.0.0.0 198.5.6.1
1 172.16.65.193 0.0.0.0

[ IP Ethernet 1:0 ]
ipbroadcast = 172.16.65.255
mode = routedSubnetMask = 255.255.255.0
IPAddress = 198.5.6.203

[ IKE Policy ]
Protecction = MD5_DES_G1

[ "VPN Group "RemoteUsers ]
maxconnections = 10IPNet = 172.16.65.0/24
LocalIPNet = 10.1.1.0/24
(Transform = esp(des,md5

[ VPN Users ]
"martin Config="RemoteUsers
"SharedKey="mysecretkey
"maurizio Config="RemoteUsers
"SharedKey="mysecretkey
```

يظهر الأمر التالي قائمة المستخدمين المتصلين:

```
sh VPN user
Port        User        Group        Client        Local        ConnectNumber
            Address     Address      Time
-------------------------------------------------------------------------------
VPN 0:1     martin      RemoteUsers  206.1.1.10    10.1.1.1     00:00:11:40
```

يجب ملاحظة أن العبارة الافتراضية على الخوادم هي الموجه الداخلي 172.16.65.193، والذي سيقوم بإصدار إعادة توجيه ICMP إلى 172.16.65.203. يتسبب هذا التطبيق في تدفقات حركة المرور غير المثالية، لأن المضيف سيرسل أول حزمة من التدفق إلى الموجه، وعند إستلام إعادة التوجيه، فإنه سيرسل الحزم التالية إلى البوابة الأكثر ملاءمة لمعالجة حركة المرور هذه. وبدلا من ذلك، يمكن للمرء تكوين مسارين مختلفين على الخوادم نفسها للإشارة إلى شبكة VPN لعناوين x.x.x.10 و 172.16.65.193 لباقي حركة المرور. في حال تكوين البوابة الافتراضية على الخوادم فقط، فيجب علينا التأكد من تكوين واجهة الموجه باستخدام "ip redirect".

ومن النقاط المثيرة للاهتمام التي لاحظناها خلال الاختبار ما يلي: إذا حاولنا **إختبار اتصال** عنوان خارجي مثل 198.5.6.1 من الخوادم أو من شبكة VPN، فستقوم البوابة الافتراضية بإرسال إعادة توجيه بروتوكول ICMP إلى 172.16.65.201.

```
:Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds
.1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201
.1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201
.1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201
.1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201
.1w1d: ICMP: redirect rcvd from 172.16.65.193 -- for 198.5.6.1 use gw 172.16.65.201
(Success rate is 0 percent (0/5
```

ستقوم الخوادم أو شبكة VPN عند هذه النقطة بإرسال طلب لبروتوكول تحليل العنوان (ARP) للحصول على 172.16.65.201 ولن تحصل على أي إستجابة بعد عام 201 لأنها موجودة على شبكة VLAN ثانوية أخرى، وهذا ما توفره لنا شبكة VLAN الخاصة. في الواقع هناك طريقة سهلة للالتفاف حول هذا، وهو إرسال حركة مرور إلى MAC الخاص ب .193 ومع IP الوجهة 172.16.65.201.

سيقوم الموجه .193 بتوجيه حركة مرور البيانات مرة أخرى إلى الواجهة نفسها، ولكن نظرا لأن واجهة الموجه عبارة عن منفذ مختلط، فإن حركة المرور ستصل إلى .201، وهو ما أردنا منعه. تم شرح هذه المشكلة في قسم المحددات المعروفة لقوائم التحكم في الوصول إلى شبكة VLAN وشبكات VLAN الخاصة.

تكوين VACL

يعد هذا القسم حاسما لتحسين الأمان في مزرعة الخوادم. كما هو موضح في قسم قيود قوائم التحكم في الوصول إلى شبكة VLAN (VACLs) وشبكات VLAN الخاصة، حتى إذا كانت الخوادم و PIX ينتسبون إلى شبكتي VLAN ثانويتين مختلفتين، فلا يزال هناك طريقة يمكن للمهاجم إستخدامها لجعلها تتصل ببعضها البعض. إذا حاولوا الاتصال مباشرة، فلن يتمكنوا من القيام بذلك بسبب شبكات VLAN الخاصة. إذا تم أختراق الخوادم ثم تم تكوينها من قبل الدخيل بطريقة يتم من خلالها إرسال حركة مرور البيانات لنفس الشبكة الفرعية إلى الموجه، فسيقوم هذا الأمر بإعادة توجيه حركة مرور البيانات على الشبكة الفرعية نفسها، وبالتالي إحباط الغرض من شبكات VLAN الخاصة.

لذلك، يحتاج VACL أن يكون شكلت على ال VLAN أساسي (ال VLAN أن يحمل الحركة مرور من المسحاج تخديد) مع التالي سياسة:

- السماح بحركة المرور التي يكون مصدر IP هو IP الخاص بالموجه
- رفض حركة المرور مع كل من عناوين IP للمصدر والوجهة كشبكة فرعية لمزرعة الخوادم
- السماح ببقية حركة المرور

```
ecomm-6500-2 (enable) sh sec acl info protect_pvlan
                    set security acl ip protect_pvlan
-------------------------------------------------
                    permit ip host 172.16.65.193 any .1
deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15 .2
                    permit ip any any .3

                    ecomm-6500-2 (enable) sh sec acl
ACL                                 Type VLANS
----- ----  --------------------------------
   protect_pvlan                    IP   41
```

لن تؤثر قائمة التحكم في الوصول (ACL) هذه على حركة المرور التي تم إنشاؤها بواسطة الخوادم أو بواسطة PIX، بل ستمنع الموجهات فقط من توجيه حركة المرور الواردة من الخوادم إلى شبكة VLAN نفسها مرة أخرى. تتيح الجملتان الأولان للموجهات إرسال رسائل مثل إعادة توجيه ICMP أو ICMP الذي يتعذر الوصول إليه إلى الخوادم.

لقد تعرفنا على تدفق حركة مرور آخر قد يرغب المسؤول في إيقافه بواسطة قوائم التحكم في الوصول إلى شبكة VPN (قوائم التحكم في الوصول إلى شبكة VPN)، وهذا التدفق من الشبكة الداخلية إلى مضيفي الشبكة الخاصة الظاهرية (VPN). للقيام بذلك، يمكن تعيين قائمة التحكم في الوصول إلى شبكة VLAN الأساسية (41) ودمجها مع الشبكة السابقة:

```
show sec acl info all

set security acl ip protect_pvlan

deny ip any 10.1.1.0 0.0.0.255 .1
permit ip host 172.16.65.193 any .2
deny ip 172.16.65.192 0.0.0.15 172.16.65.192 0.0.0.15 .3
permit ip any any .4
```

إختبار التكوين

يتم الآن فحص المضيف 10.1.1.1 من الموجه .193 (zundapp). قبل تعيين قائمة التحكم في الوصول إلى شبكة VACL، نجح **إختبار الاتصال**.

```
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

بعد تعيين قائمة التحكم في الوصول إلى شبكة VLAN رقم 41، لن ينجح **إختبار الاتصال** نفسه:

```
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds
.....
(Success rate is 0 percent (0/5
```

ومع ذلك، لا يزال يمكننا **إختبار اتصال** الموجه الخارجي:

```
.Type escape sequence to abort
:Sending 5, 100-byte ICMP Echos to 198.5.6.1, timeout is 2 seconds
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/171/192 ms
```

معلومات ذات صلة

- تكوين قوائم التحكم في الوصول - وثائق Catalyst 6000
- الدعم الفني - 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).