ASA/PIX: تكوين تجاوز الفشل في الوضع الشافي النشط/الاحتياطي

المحتويات

المقدمة

تتطلب تهيئة التغلب على الأعطال توصيل جهازي أمان متطابقين ببعضهما البعض من خلال إرتباط مخصص للتغلب على الأعطال، وبشكل إختياري، إرتباط تجاوز الأعطال الذي يحدد الحالة. تتم مراقبة سلامة الواجهات والوحدات النشطة لتحديد ما إذا تم الوفاء بشروط محددة للتغلب على الأعطال. إذا تم استيفاء هذه الشروط، يحدث تجاوز الفشل.

يدعم جهاز الأمان عمليتي تهيئة للتغلب على الأعطال:

- تجاوز الفشل النشط/النشط
- التغلب على الأعطال في وضع الاستعداد/النشط

يكون لكل تكوين لتجاوز الفشل طريقته الخاصة لتحديد عملية تجاوز الفشل وتنفيذها. مع تجاوز الفشل النشط/النشط، يمكن لكلا الوحدتين تمرير حركة مرور الشبكة. يتيح لك ذلك تكوين موازنة الأحمال على الشبكة. لا يتوفر تجاوز الفشل النشط/النشط إلا على الوحدات التي تعمل في وضع سياق متعدد. مع تجاوز الأعطال في وضع الاستعداد/النشط، لا تتخطى حركة مرور البيانات إلا وحدة واحدة بينما تنتظر الوحدة الأخرى في حالة إستعداد. تتوفر ميزة التغلب على الأعطال في وضع الاستعداد/النشط على الوحدات التي تعمل في وضع سياق واحد أو متعدد. تدعم كل من عمليات التهيئة الخاصة بتجاوز الأعطال إمكانية تجاوز الأعطال عديم الحالة أو عديم الحالة (بشكل منتظم).

جدار الحماية الشفاف، هو جدار حماية من الطبقة 2 يعمل مثل *التضاريس في السلك*، أو *جدار حماية التسلل*، ولا يرى على أنه موجه موجه إلى الأجهزة المتصلة. يقوم جهاز الأمان بتوصيل الشبكة نفسها على المنافذ الداخلية والخارجية الخاصة بها. لأن جدار الحماية ليس خطوة موجهة، يمكنك بسهولة تقديم جدار حماية شفاف إلى شبكة موجودة، وليس من الضروري إعادة ضبط IP. يمكنك *ضبط* جهاز الأمان القابل للتكيف على التشغيل في الوضع الافتراضي لجدار الحماية الموجه أو وضع جدار الحماية الشفاف. عندما تقوم بتغيير الأوضاع، يقوم جهاز الأمان القابل للتكيف بمسح التكوين لأن العديد من الأوامر غير مدعومة في كلا الوضعين. إذا كان لديك تكوين معبأ بالفعل، فتأكد من إجراء نسخ إحتياطي لهذا التكوين قبل تغيير الوضع، يمكنك إستخدام تكوين النسخ الاحتياطي هذا للمرجع عند إنشاء تكوين جديد. راجع مثال تكوين جدار الحماية الشفاف للحصول على مزيد من المعلومات حول تكوين جهاز جدار الحماية في الوضع الشفاف.

يركز هذا المستند على كيفية تكوين تجاوز فشل نشط/إحتياطي في الوضع الشفاف على جهاز الأمان ASA.

ملاحظة: لا يتم دعم تجاوز فشل الشبكة الخاصة الظاهرية (VPN) على الوحدات التي تعمل في وضع سياق متعدد. تتوفر تقنية تجاوز فشل الشبكات الخاصة الظاهرية (VPN) لتكوينات **التغلب على الأعطال النشطة/الاحتياطية** فقط.

توصيك Cisco بعدم إستخدام واجهة الإدارة لتجاوز الفشل، وخاصة تجاوز الأعطال الذي يحدد الحالة والذي يرسل فيه جهاز الأمان معلومات الاتصال باستمرار من جهاز أمان إلى الآخر. يجب أن تكون واجهة تجاوز الفشل بنفس السعة على الأقل مثل الواجهات التي تمر بحركة المرور العادية، ومع أن الواجهات على ASA 5540 هي جيجابت، فإن واجهة الإدارة هي FastEthernet فقط. تم تصميم واجهة الإدارة لحركة مرور الإدارة فقط ويتم تحديدها كإدارة0/0. ولكن، يمكنك إستخدام الأمر **management-only** لتكوين أي واجهة لتكون واجهة إدارة فقط. أيضا، للإدارة 0/0، أنت يستطيع أعجزت إدارة أسلوب فقط لذلك القارن يستطيع مررت من خلال حركة مرور مثل أي قارن آخر. راجع Cisco Security Appliance Command Reference، الإصدار 8.0 للحصول على مزيد من المعلومات حول الأمر

management-only.

يوفر دليل التكوين هذا نموذجا للتكوين لتضمين مقدمة موجزة لتقنية PIX/ASA 7.x النشطة/الاحتياطية. ارجع إلى دليل مرجع أوامر ASA/PIX للحصول على شعور أكثر تعمقا للنظرية المستندة إلى هذه التقنية.

المتطلبات الأساسية

المتطلبات

متطلبات الأجهزة

يجب أن يكون لكلا الوحدتين في تهيئة تجاوز الفشل نفس تهيئة الأجهزة. يجب أن تكون بنفس الطراز، وأن تحتوي على نفس عدد الواجهات وأنواعها، مع نفس مقدار ذاكرة الوصول العشوائي (RAM).

ملاحظة: لا تحتاج الوحدتان إلى امتلاك ذاكرة Flash بنفس الحجم. إذا كنت تستخدم وحدات بأحجام مختلفة من ذاكرة Flash (الذاكرة المؤقتة) في تهيئة تجاوز الفشل، فتأكد من أن الوحدة ذات ذاكرة Flash الأصغر حجما تحتوي على مساحة كافية لاستيعاب ملفات صورة البرنامج وملفات التكوين. وإذا لم تكن كذلك، فإن مزامنة التكوين من الوحدة ذات ذاكرة Flash الأكبر حجما إلى الوحدة ذات ذاكرة Flash الأصغر حجما تفشل.

متطلبات البرامج

يجب أن تكون الوحدتان الموجودتان في تكوين تجاوز الفشل في أوضاع التشغيل (الموجهة أو الشفافة، أحادية أو متعددة السياق). يجب أن يكون لديهم إصدار البرنامج الرئيسي نفسه (الرقم الأول) والإصدار الثانوي (الرقم الثاني)، ولكن يمكنك إستخدام إصدارات مختلفة من البرنامج ضمن عملية ترقية، على سبيل المثال، يمكنك ترقية وحدة واحدة من الإصدار 7.0(1) إلى الإصدار 7.0(2) وتبقى عملية تجاوز الفشل نشطة. cisco يوصي أن يحسن أنت كلا وحدة إلى ال نفسه صيغة أن يضمن توافق طويل الأجل.

ارجع إلى قسم إجراء ترقيات التوقف عن العمل صفر لأزواج تجاوز الفشل في *دليل تكوين سطر أوامر Cisco Security Appliance، الإصدار 8.0* للحصول على مزيد من المعلومات حول كيفية ترقية البرنامج على زوج تجاوز الفشل.

متطلبات الترخيص

على النظام الأساسي لجهاز الأمان ASA، يجب أن يكون لدى وحدة واحدة على الأقل **ترخيص غير مقيد (UR)**.

ملاحظة: قد يكون من الضروري ترقية التراخيص الخاصة بزوج تجاوز الفشل للحصول على ميزات ومزايا إضافية. ارجع إلى ترقية مفتاح الترخيص على زوج تجاوز الفشل للحصول على مزيد من المعلومات.

ملاحظة: يجب أن تكون الميزات المرخصة (مثل نظائر SSL VPN أو سياقات الأمان) في كل من أجهزة الأمان التي تشارك في تجاوز الأعطال متطابقة.

المكونات المستخدمة

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

- جهاز أمان ASA مع الإصدار x.7 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.

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع إصدارات الأجهزة والبرامج التالية:

- جهاز أمان PIX مع الإصدار x.7 والإصدارات الأحدث

الاصطلاحات

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

التغلب على الأعطال في وضع الاستعداد/النشط

يصف هذا القسم تجاوز الفشل في وضع الاستعداد/النشط ويتضمن الموضوعات التالية:

نظرة عامة على تجاوز الفشل في وضع الاستعداد/النشط

تتيح لك ميزة التغلب على الأعطال في وضع الاستعداد/النشط إمكانية إستخدام جهاز أمان إحتياطي لتتولى مهام أية وحدة معطلة. وعندما تفشل الوحدة النشطة، تتغير إلى حالة الاستعداد بينما تتغير الوحدة الاحتياطية إلى الحالة النشطة. تفترض الوحدة التي تصبح نشطة عناوين IP، أو، بالنسبة لجدار حماية شفاف، عنوان IP للإدارة وعناوين MAC للوحدة الفاشلة وتبدأ في تمرير حركة مرور البيانات. تتسلم الوحدة الموجودة الآن في حالة الاستعداد عناوين IP وعناوين MAC في وضع الاستعداد. لأن أجهزة الشبكة لا ترى أي تغيير في اقتران عنوان MAC ب IP، فلا تتغير إدخالات ARP أو انتهت المهلة في أي مكان على الشبكة.

ملاحظة: بالنسبة لوضع السياق المتعدد، يمكن أن يفشل جهاز الأمان على الوحدة بأكملها، والتي تتضمن جميع السياقات، ولكن لا يمكن أن يفشل على السياقات الفردية بشكل منفصل.

الحالة الأساسية/الثانوية والحالة النشطة/الاحتياطية

وتتصل الفروق الرئيسية بين الوحدتين في زوج تجاوز الفشل بالوحدة النشطة وبالوحدة الاحتياطية، أي عناوين IP المطلوب إستخدامها والوحدة الأساسية التي تجتاز حركة مرور البيانات بنشاط.

توجد بعض الاختلافات بين الوحدات التي تستند إلى الوحدة الرئيسية، كما هو محدد في التكوين، والوحدة الثانوية:

- وتصبح الوحدة الأساسية دائما هي الوحدة النشطة إذا بدأت كلتا الوحدتين العمل في نفس الوقت (وصحتهما عمليتان متكافئتان).
- يتم دائما إقران عنوان MAC للوحدة الأساسية بعناوين IP النشطة. يحدث الاستثناء لهذه القاعدة عندما تكون الوحدة الثانوية نشطة ولا يمكنها الحصول على عنوان MAC الأساسي عبر إرتباط تجاوز الفشل. في هذه الحالة، يتم إستخدام عنوان MAC الثانوي.

تهيئة الجهاز ومزامنة التكوين

تحدث مزامنة التكوين عندما يتم تحميل أحد الجهازين أو كليهما في زوج تجاوز الفشل. تتم مزامنة التكوينات دائما من الوحدة النشطة إلى الوحدة الاحتياطية. عندما تكمل الوحدة الاحتياطية بدء التشغيل الأولي، فإنها تزيل التكوين الجاري تشغيلها، باستثناء أوامر تجاوز الفشل اللازمة للاتصال بالوحدة النشطة، وترسل الوحدة النشطة التكوين الكامل الخاص بها إلى الوحدة الاحتياطية.

يتم تحديد الوحدة النشطة من خلال ما يلي:

- إذا قامت وحدة ما بتحميل جهاز النظير النشط واكتشافه، تصبح هي الوحدة الاحتياطية.
- إذا جزمة وحدة ولم تكتشف النظير، تصبح الوحدة النشطة.
- إذا تم تحميل كلتا الوحدتين في وقت واحد، تصبح الوحدة الأساسية هي الوحدة النشطة، وتصبح الوحدة الثانوية هي الوحدة الاحتياطية.

ملاحظة: إذا تم تمهيد الوحدة الثانوية ولم يتم الكشف عن الوحدة الأساسية، فإنها تصبح الوحدة النشطة. وهو يستخدم عناوين MAC الخاصة به لعناوين IP النشطة. عندما تصبح الوحدة الأساسية متاحة، تغير الوحدة الثانوية عناوين MAC إلى عناوين الوحدة الأساسية، مما يمكن أن يسبب مقاطعة في حركة مرور الشبكة. لتجنب هذا، قم بتكوين زوج تجاوز الفشل باستخدام عناوين MAC الظاهرية. راجع قسم تكوين تجاوز الفشل النشط/الاحتياطي في هذا المستند للحصول على مزيد من المعلومات.

عند بدء النسخ المتماثل، تقوم وحدة تحكم جهاز الأمان على الوحدة النشطة بعرض الرسالة : وعندما يكتمل، يعرض جهاز الأمان الرسالة . ضمن عملية النسخ المتماثل، لا يمكن للأوامر التي تم إدخالها على الوحدة النشطة إجراء النسخ المتماثل بشكل صحيح إلى الوحدة الاحتياطية، ويمكن إستبدال الأوامر التي تم إدخالها على الوحدة الاحتياطية بواسطة التكوين الذي تم نسخه نسخا متماثلا من الوحدة النشطة. لا تدخل أوامر على أي من الوحدتين في زوج تجاوز الفشل ضمن عملية نسخ التكوين المتماثل. بناء على حجم التكوين، يمكن أن تستغرق عملية النسخ المتماثل من بضع ثوان إلى عدة دقائق.

من الوحدة الثانوية، يمكنك ملاحظة رسالة النسخ المتماثل أثناء مزامنتها من الوحدة الأساسية:

```
. <ASA

                Detected an Active mate
.Beginning configuration replication from mate
.End configuration replication from mate

<ASA
```

في الوحدة الاحتياطية، يوجد التكوين فقط في الذاكرة قيد التشغيل. لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة) بعد المزامنة، أدخل الأوامر التالية:

- بالنسبة لوضع السياق الواحد، أدخل الأمر **copy running-config startup-config** على الوحدة النشطة. يتم نسخ الأمر نسخا متماثلا إلى الوحدة الاحتياطية، والتي تنتقل إلى كتابة التكوين الخاص بها إلى ذاكرة Flash (الذاكرة المؤقتة).
- بالنسبة لوضع السياق المتعدد، أدخل الأمر **copy running-config startup-config** على الوحدة النشطة من مساحة تنفيذ النظام ومن داخل كل سياق على القرص. يتم نسخ الأمر نسخا متماثلا إلى الوحدة الاحتياطية، والتي تنتقل إلى كتابة التكوين الخاص بها إلى ذاكرة Flash (الذاكرة المؤقتة). يمكن الوصول إلى السياقات ذات تكوينات بدء التشغيل على الخوادم الخارجية من أي من الوحدتين عبر الشبكة ولا يلزم حفظها بشكل منفصل لكل وحدة. وبدلا من ذلك، يمكنك نسخ السياقات الموجودة على القرص من الوحدة النشطة إلى خادم خارجي، ثم نسخها إلى قرص على وحدة الاستعداد، حيث تصبح متوفرة عند إعادة تحميل الوحدة.

نسخ الأوامر

تتدفق نسخ الأوامر دائما من الوحدة النشطة إلى الوحدة الاحتياطية. كما يتم إدخال الأوامر على الوحدة النشطة، فإنها يتم إرسالها عبر إرتباط تجاوز الفشل إلى الوحدة الاحتياطية. أنت لا تحتاج أن ينقذ التشكيل نشط إلى ذاكرة Flash أن يكرر الأمر.

ملاحظة: لا يتم نسخ التغييرات التي تم إجراؤها على الوحدة الاحتياطية إلى الوحدة النشطة. إذا قمت بإدخال أمر على الوحدة الاحتياطية، يعرض جهاز الأمان الرسالة *** ***** . لم تعد التكوينات متزامنة. يتم عرض هذه الرسالة حتى إذا قمت بإدخال أوامر لا تؤثر على التكوين.

إذا قمت بإدخال الأمر **write standby** على الوحدة النشطة، فإن الوحدة الاحتياطية تعمل على مسح التكوين الجاري تشغيله، باستثناء أوامر تجاوز الفشل المستخدمة للاتصال بالوحدة النشطة، وترسل الوحدة النشطة التكوين الكامل الخاص بها إلى الوحدة الاحتياطية.

بالنسبة لوضع السياق المتعدد، عند إدخال الأمر **write standby** في مساحة تنفيذ النظام، يتم نسخ جميع السياقات. إذا قمت بإدخال الأمر write standby داخل سياق، فإن الأمر يقوم بنسخ تكوين السياق فقط.

يتم تخزين الأوامر المنسوخة نسخا متماثلا في التكوين الجاري تشغيله. لحفظ الأوامر المنسوخة نسخا متماثلا إلى ذاكرة Flash (الذاكرة المؤقتة) على الوحدة الاحتياطية، أدخل الأوامر التالية:

- بالنسبة لوضع السياق الواحد، أدخل الأمر **copy running-config startup-config** على الوحدة النشطة. يتم نسخ الأمر نسخا متماثلا إلى الوحدة الاحتياطية، والتي تنتقل إلى كتابة التكوين الخاص بها إلى ذاكرة Flash (الذاكرة المؤقتة).
- بالنسبة لوضع السياق المتعدد، أدخل الأمر **copy running-config startup-config** على الوحدة النشطة من مساحة تنفيذ النظام وداخل كل سياق على القرص. يتم نسخ الأمر نسخا متماثلا إلى الوحدة الاحتياطية، والتي تنتقل إلى كتابة التكوين الخاص بها إلى ذاكرة Flash (الذاكرة المؤقتة). يمكن الوصول إلى السياقات ذات تكوينات بدء التشغيل على الخوادم الخارجية من أي من الوحدتين عبر الشبكة ولا يلزم حفظها بشكل منفصل لكل وحدة. بدلا من ذلك، يمكنك نسخ السياقات الموجودة على القرص من الوحدة النشطة إلى خادم خارجي، ثم نسخها إلى قرص على الوحدة الاحتياطية.

مشغلات تجاوز الفشل

الوحدة يستطيع فشلت إن واحد من هذا حادث يقع:

- تعرضت الوحدة لعطل في الجهاز أو عطل في الطاقة.
- الوحدة لديها فشل برمجي.
- فشل العديد من الواجهات المراقبة.
- يتم إدخال الأمر **no fail over active** على الوحدة النشطة، أو يتم إدخال الأمر **تجاوز الفشل النشط** على الوحدة الاحتياطية.

إجراءات تجاوز الفشل

في حالات التغلب على الأعطال في وضع الاستعداد/النشط، يحدث تجاوز الأعطال على أساس الوحدة. حتى في الأنظمة التي تعمل في وضع سياق متعدد، لا يمكنك تجاوز الفشل الفردي أو مجموعات السياقات.

يوضح هذا الجدول إجراء تجاوز الفشل لكل حدث فشل. بالنسبة لكل حدث فشل، يوضح الجدول سياسة تجاوز الفشل (تجاوز الفشل أو عدم تجاوز الفشل) والإجراء المتخذ من قبل الوحدة النشطة والإجراء المتخذ من قبل الوحدة الاحتياطية وأي ملاحظات خاصة حول حالة تجاوز الفشل وإجراءاته. يوضح الجدول سلوك تجاوز الفشل.

حدث الفشل	السياسة	فعل نشط	الإجراء الاحتياطي	ملاحظات
فشل الوحدة النشطة (الطاقة أو الأجهزة)	تجاوز الفشل	غير متوفر	كن نشيطا،	لا يتم تلقي رسائل

			وضع علامة "فشل " على النشا ط	ترحيب على أي واجهة مراقبة أو إرتباط تجاوز الفشل.
عمليات إسترداد الوحدات النشطة سابقا	لا يوجد تجاوز فشل	كن في وضع الاستعدا د	لا يوجد إجراء	None
فشل وحدة الاستعداد (الطاقة أو الأجهزة)	لا يوجد تجاوز فشل	وضع علامة "فشل" على الاستعدا د	غير متوفر	عندما يتم وضع علامة "فشل" على الوحدة الاحتياطية ، لا تحاول الوحدة النشطة تجاوز الفشل، حتى في حالة تجاوز حد فشل الواجهة.
فشل إرتباط تجاوز الفشل ضمن العملية	لا يوجد تجاوز فشل	وضع علامة "فشل" على واجهة تجاوز الفشل	وضع علامة "فشل " على واجهة تجاوز الفش ل	يجب عليك إستعادة إرتباط تجاوز الفشل في أقرب وقت ممكن لأن الوحدة لا يمكنها تجاوز الفشل إلى وحدة الاستعداد بينما إرتباط تجاوز الفشل معطل.
فشل إرتباط تجاوز الفشل عند بدء التشغيل	لا يوجد تجاوز فشل	وضع علامة "فشل"	نشيطا	إذا كان إرتباط تجاوز

		على واجهة تجاوز الفشل		الفشل معطلا عند بدء التشغيل، فإن كلتا الوحدتين تصبح نشطة.
فشل إرتباط تجاوز الفشل ذو الحالة	لا يوجد تجاوز فشل	لا يوجد إجراء	لا يوجد إجراء	تصبح معلومات الحالة قديمة، ويتم إنهاء جلسات العمل إذا حدث تجاوز فشل.
فشل الواجهة على الوحدة النشطة أعلى من الحد	تجاوز الفشل	وضع علامة "نشط" كفشل	نشيطا	None
فشل الواجهة على الوحدة الاحتياطية أعلى من الحد	لا يوجد تجاوز فشل	لا يوجد إجراء	وضع علامة "فشل " على الاستعداد	عندما يتم تمييز الوحدة الاحتياطية على أنها فاشلة، فإن الوحدة النشطة لا تحاول الفشل حتى إذا تم تجاوز حد فشل الواجهة.

تجاوز الفشل العادي والحالي

يدعم جهاز الأمان نوعين من تجاوز الأعطال، وهما النوعان وبيان الحالة. يتضمن هذا القسم الموضوعات التالية:

- تجاوز الفشل العادي
- تجاوز الفشل ذو الحالة

تجاوز الفشل العادي

عند حدوث تجاوز فشل، يتم إسقاط جميع الاتصالات النشطة. يحتاج العملاء إلى إعادة إنشاء الاتصالات عند تولي الوحدة النشطة الجديدة زمام الأمور.

تجاوز الفشل ذو الحالة

عند تمكين تجاوز الفشل ذو الحالة، تقوم الوحدة النشطة باستمرار بتمرير معلومات حالة كل اتصال إلى الوحدة الاحتياطية. بعد حدوث تجاوز الفشل، تتوفر نفس معلومات الاتصال في الوحدة النشطة الجديدة. تطبيقات المستخدم النهائي المدعومة غير مطلوبة لإعادة الاتصال للاحتفاظ بنفس جلسة الاتصال.

تتضمن معلومات الحالة التي تم تمريرها إلى الوحدة الاحتياطية ما يلي:

- ال nat ترجمة طاولة
- حالات اتصال TCP
- حالات اتصال UDP
- جدول ARP
- جدول جسر الطبقة 2 (فقط عندما يتم تشغيل جدار الحماية في وضع **جدار الحماية الشفاف**)
- حالات اتصال HTTP (إذا تم تمكين النسخ المتماثل ل HTTP)
- جدول ISAKMP و IPSec SA
- قاعدة بيانات اتصال GTP PDP

وتتضمن المعلومات التي لا يتم تمريرها إلى وحدة الاستعداد عند تمكين تجاوز الفشل ذي الحالة ما يلي:

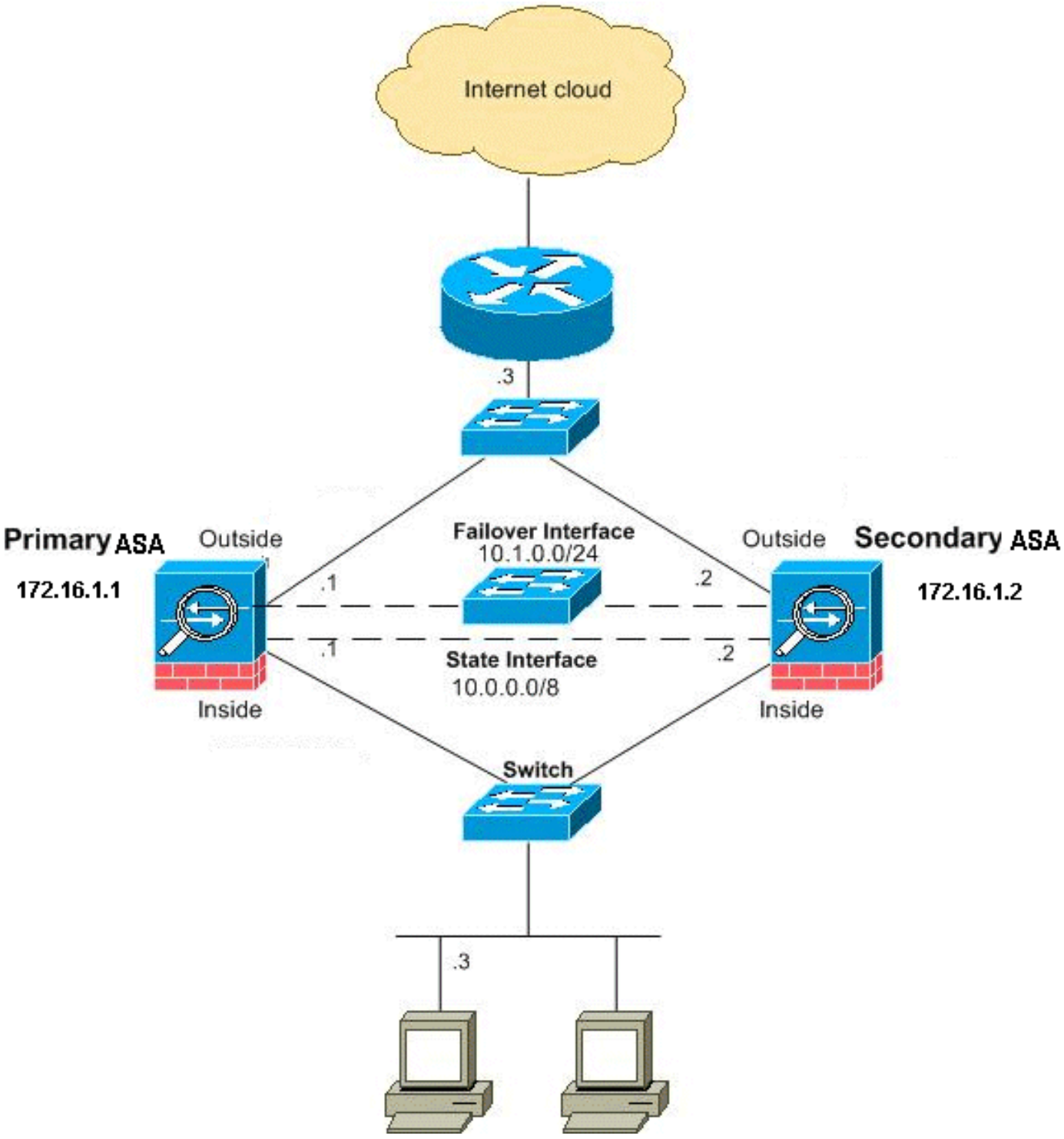
- جدول اتصال HTTP (ما لم يتم تمكين النسخ المتماثل ل HTTP)
- جدول مصادقة المستخدم (uauth)
- جداول التوجيه
- معلومات الحالة الخاصة بالوحدات النمطية لخدمة الأمان

ملاحظة: إذا حدث تجاوز الفشل داخل جلسة عمل Cisco IP SoftPhone نشطة، فإن المكالمة تظل نشطة لأنه يتم نسخ معلومات حالة جلسة عمل الاتصال إلى الوحدة الاحتياطية. عند إنهاء المكالمة، يفقد عميل IP SoftPhone الاتصال ب Cisco CallManager . يحدث هذا لعدم وجود معلومات جلسة عمل لرسالة تعليق CTIQBE على الوحدة الاحتياطية. عندما لا يتلقى عميل IP SoftPhone إستجابة من Cisco CallManager في غضون فترة زمنية معينة، فإنه يعتبر أن Cisco CallManager غير قابل للوصول ويلغي التسجيل نفسه.

تكوين نشط/إحتياطي لتجاوز الفشل يستند إلى شبكة LAN

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



يوضح هذا القسم كيفية تكوين تجاوز الفشل في وضع الاستعداد/النشط في وضع شفاف باستخدام إرتباط تجاوز فشل شبكة إيثرنت. عند تكوين تجاوز الفشل المستند إلى شبكة LAN، يجب عليك تمهيد الجهاز الثانوي للتعرف على إرتباط تجاوز الفشل قبل أن يتمكن الجهاز الثانوي من الحصول على التكوين الجاري تشغيله من الجهاز الأساسي.

ملاحظة: إذا قمت بالتغيير من تجاوز الفشل المستند إلى الكبلات إلى تجاوز الفشل المستند إلى الشبكة المحلية (LAN)، فيمكنك تخطي العديد من الخطوات، مثل تعيين عناوين IP النشطة والاحتياطية لكل واجهة، والتي قمت بإكمالها لتكوين تجاوز الفشل المستند إلى الكبلات.

تكوين الوحدة الأساسية

أكمل هذه الخطوات لتكوين الوحدة الأساسية في تكوين تجاوز الفشل النشط/الاحتياطي المستند إلى شبكة محلية. توفر هذه الخطوات الحد الأدنى من التهيئة اللازمة لتمكين تجاوز الفشل على الوحدة الأساسية. بالنسبة لوضع السياق المتعدد، يتم تنفيذ جميع الخطوات في مساحة تنفيذ النظام ما لم يذكر خلاف ذلك.

لتكوين الوحدة الأساسية في زوج التغلب على الأعطال في الوضع النشط/الاحتياطي، أكمل الخطوات التالية:

1. إذا لم تكن قد قمت بذلك بالفعل، فقم بتكوين عناوين IP النشطة والاحتياطية لواجهة الإدارة (الوضع الشفاف). يتم إستخدام عنوان IP الاحتياطي على جهاز الأمان الذي يمثل حاليا الوحدة الاحتياطية. يجب أن يكون في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط.**ملاحظة:** لا تقم بتكوين عنوان IP لارتباط تجاوز الفشل ذو الحالة إذا كنت تستخدم واجهة مخصصة لتجاوز الفشل تحدد الحالة. يمكنك إستخدام أمر **تجاوز الفشل لواجهة ip** لتكوين واجهة مخصصة للتغلب على الأعطال في خطوة لاحقة.

```
hostname(config-if)#ip address active_addr netmask
standby standby_addr
```

بخلاف الوضع الموجه، والذي يتطلب عنوان IP لكل واجهة، يحتوي جدار الحماية الشفاف على عنوان IP تم تعيينه للجهاز بالكامل. يستخدم جهاز الأمان عنوان IP هذا كعنوان مصدر للحزم التي تنشأ على جهاز الأمان، مثل رسائل النظام أو إتصالات AAA. في المثال، تم تكوين عنوان IP الخاص ب ASA الأساسي كما هو موضح أدناه:

```
hostname(config)#ip address 172.16.1.1 255.255.0.0 standby 172.16.1.2
```

هنا، 172.16.1.1 يستعمل للوحدة الأساسية، و 172.16.1.2 يعين للوحدة الثانوية (الاحتياطية).**ملاحظة:** في وضع السياق المتعدد، يجب تكوين عناوين الواجهة من داخل كل سياق. أستخدم الأمر **changeto context** للتبديل بين السياقات. يتغير موجه الأمر إلى hostname/context(config-if)#، حيث يكون السياق اسم السياق الحالي.

2. (النظام الأساسي لجهاز أمان PIX فقط) قم بتمكين تجاوز الفشل المستند إلى شبكة LAN.

```
hostname(config)#failover lan enable
```

3. تعيين الوحدة كوحدة رئيسية.

```
hostname(config)#failover lan unit primary
```

4. تحديد واجهة تجاوز الفشل.حدد الواجهة التي سيتم إستخدامها كواجهة تجاوز الفشل.

```
hostname(config)#failover lan interface if_name phy_if
```

في هذه الوثائق، يتم إستخدام "تجاوز الفشل" (اسم الواجهة ل Ethernet0) لواجهة تجاوز الفشل.

```
hostname(config)#failover lan interface failover Ethernet3
```

تقوم الوسيطة *if_name* بتعيين اسم للواجهة المحددة بواسطة الوسيطة *phy_if*. *ال phy_if* وسيطة يستطيع كنت ال physical ميناء name، مثل إثرنيت1، أو خلقت سابق قارن فرعي، مثل إثرنيت2.3/0.قم بتعيين عنوان IP النشط والاحتياطي لارتباط تجاوز الفشل

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

في هذه الوثائق، لتكوين إرتباط تجاوز الفشل، يتم إستخدام 10.1.0.1 للوحدة النشطة و 10.1.0.2 للوحدة الاحتياطية، و"تجاوز الفشل" هو اسم واجهة لشبكة الإيثرنت0.

```
hostname(config)#failover interface ip failover 10.1.0.1
standby 10.1.0.2 255.255.255.0
```

يجب أن يكون عنوان IP الاحتياطي في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط. لا تحتاج إلى تعريف قناع الشبكة الفرعية للعنوان الاحتياطي.لا يتغير عنوان IP لارتباط تجاوز الفشل وعنوان MAC عند تجاوز الفشل. يظل عنوان IP النشط لارتباط تجاوز الفشل دائما مع الوحدة الأساسية، بينما يظل عنوان IP الاحتياطي مع الوحدة الثانوية.تمكين الواجهة

```
hostname(config)#interface phy_if
```

```
hostname(config-if)#no shutdown
```

في المثال، يتم إستخدام Ethernet3 لتجاوز الفشل:

```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

5. (إختياري) لتمكين تجاوز الفشل ذو الحالة، قم بتكوين إرتباط تجاوز الفشل ذو الحالة.حدد الواجهة التي سيتم إستخدامها كارتباط تجاوز الفشل ذو الحالة.

```
hostname(config)#failover link if_name phy_if
```

أستخدم هذا المثال "الحالة" كاسم واجهة للإيثرنت 2 لتبادل معلومات حالة إرتباط تجاوز الفشل:

```
hostname(config)#failover link state Ethernet2
```

ملاحظة: إذا كان إرتباط تجاوز الفشل ذو الحالة يستخدم إرتباط تجاوز الفشل أو واجهة البيانات، فلن تحتاج إلا إلى توفير وسيطة *if_name*.تقوم الوسيطة *if_name* بتعيين اسم منطقي للواجهة المحددة بواسطة الوسيطة *phy_if*. يمكن أن تكون وسيطة *phy_if* اسم المنفذ الفعلي، مثل Ethernet1، أو واجهة فرعية تم إنشاؤها مسبقا، مثل Ethernet0/2.3. يجب عدم إستخدام هذه الواجهة لأي غرض آخر، باستثناء، إختياريا، كإرتباط لتجاوز الفشل.قم بتعيين عنوان IP نشط واحتياطي لارتباط تجاوز الفشل ذو الحالة.**ملاحظة:** إذا كان إرتباط تجاوز الفشل ذو الحالة يستخدم إرتباط تجاوز الفشل أو واجهة البيانات، فقم بتخطي هذه الخطوة. لقد قمت بالفعل بتعريف عناوين IP النشطة والاحتياطية للواجهة.

```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

يتم إستخدام 10.0.0.1 كعنوان IP نشط و 10.0.0.2 كعنوان IP إستعداد لارتباط تجاوز الفشل ذو الحالة في هذا المثال.

```
hostname(config)#failover interface ip state 10.0.0.1 255.0.0.0
                standby 10.0.0.2
```

يجب أن يكون عنوان IP الاحتياطي في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط. لا تحتاج إلى تعريف قناع الشبكة الفرعية للعنوان الاحتياطي.لا يتغير عنوان IP لعنوان MAC لارتباط تجاوز الفشل ذو الحالة عند تجاوز الفشل ما لم يستخدما واجهة بيانات. يبقى عنوان IP النشط دائما مع الوحدة الأساسية، بينما يبقى عنوان IP الاحتياطي مع الوحدة الثانوية.مكنت القارن.**ملاحظة:** إذا كان إرتباط تجاوز الفشل ذو الحالة يستخدم إرتباط تجاوز الفشل أو واجهة البيانات، فقم بتخطي هذه الخطوة. لقد قمت بتمكين الواجهة بالفعل.

```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

ملاحظة: على سبيل المثال، في هذا السيناريو، يتم إستخدام إيثرنت 2 لارتباط تجاوز الفشل ذو الحالة:

```
hostname(config)#interface ethernet2

hostname(config-if)#no shutdown
```

6. تمكين تجاوز الفشل.

```
hostname(config)#failover
```

ملاحظة: قم بإصدار الأمر **تجاوز الفشل** على الجهاز الأساسي أولا، ثم قم بإصداره على الجهاز الثانوي. بعد إصدار الأمر **تجاوز الفشل** على الجهاز الثانوي، يقوم الجهاز الثانوي على الفور بسحب التكوين من الجهاز الأساسي وتعيين نفسه على أنه *وضع الاستعداد*. يبقى ال ASA أساسي فوق ويمرر حركة مرور عادي ويعلم نفسه ك أداة *نشط*. ومن تلك النقطة فصاعدا، كلما حدث عطل في الجهاز النشط، يظهر الجهاز الاحتياطي نشطا.

7. احفظ تكوين النظام في ذاكرة Flash (الذاكرة المؤقتة).

```
hostname(config)#copy running-config startup-config
```

تكوين الوحدة الثانوية

والتكوين الوحيد المطلوب على الوحدة الثانوية هو لواجهة تجاوز الفشل. تتطلب الوحدة الثانوية أن تتصل هذه الأوامر بشكل مبدئي بالوحدة الأساسية. بعد أن ترسل الوحدة الأساسية التكوين الخاص بها إلى الوحدة الثانوية، يكون الاختلاف الدائم الوحيد بين التكوينين هو أمر **وحدة الشبكة المحلية (تجاوز الفشل)**، الذي يحدد كل وحدة على أنها أساسية أو ثانوية.

بالنسبة لوضع السياق المتعدد، يتم تنفيذ جميع الخطوات في مساحة تنفيذ النظام ما لم يذكر خلاف ذلك.

لتكوين الوحدة الثانوية، أكمل الخطوات التالية:

1. (النظام الأساسي لجهاز أمان PIX فقط) إمكانية التغلب على الأعطال القائمة على شبكة LAN.
```
hostname(config)#failover lan enable
```

2. تحديد واجهة تجاوز الفشل. أستخدم نفس الإعدادات التي أستخدمتها للوحدة الأساسية.حدد الواجهة التي سيتم إستخدامها كواجهة تجاوز الفشل.
```
hostname(config)#failover lan interface if_name phy_if
```

في هذه الوثائق، يتم إستخدام Ethernet0 لواجهة تجاوز فشل شبكة LAN.
```
hostname(config)#failover lan interface failover Ethernet3
```

تقوم الوسيطة *if_name* بتعيين اسم للواجهة المحددة بواسطة الوسيطة *phy_if*.قم بتعيين عنوان IP النشط والاستعداد لارتباط تجاوز الفشل.
```
hostname(config)#failover interface ip if_name ip_addr mask standby ip_addr
```

في هذه الوثائق، لتكوين إرتباط تجاوز الفشل، يتم إستخدام 10.1.0.1 للوحدة النشطة و 10.1.0.2 للوحدة الاحتياطية، و"تجاوز الفشل" هو اسم واجهة لشبكة الإيثرنت0.
```
hostname(config)#failover interface ip failover 10.1.0.1
    standby 10.1.0.2 255.255.255.0
```

ملاحظة: أدخل هذا الأمر تماما كما أدخلته على الوحدة الأساسية عند تكوين واجهة تجاوز الفشل على الوحدة الأساسية.مكنت القارن.
```
hostname(config)#interface phy_if

hostname(config-if)#no shutdown
```

على سبيل المثال، في هذا السيناريو، يتم إستخدام Ethernet0 لتجاوز الفشل.
```
hostname(config)#interface ethernet3

hostname(config-if)#no shutdown
```

3. (إختياري) قم بتعيين هذه الوحدة كوحدة ثانوية.
```
hostname(config)#failover lan unit secondary
```

ملاحظة: هذه الخطوة إختيارية لأنه، بشكل افتراضي، يتم تعيين الوحدات كوحدات ثانوية ما لم يتم تكوينها مسبقا.

4. تمكين تجاوز الفشل.
```
hostname(config)#failover
```

ملاحظة: بعد تمكين تجاوز الفشل، ترسل الوحدة النشطة التكوين في الذاكرة قيد التشغيل إلى الوحدة الاحتياطية. مع مزامنة التكوين، تظهر الرسائل *التي تبدأ عملية النسخ المتماثل للتكوين: الإرسال إلى التزامن والنسخ المتماثل للتكوين الطرفي* على وحدة التحكم النشطة للوحدة.

5. بعد أن ينتهي التكوين الجاري تشغيله من النسخ المتماثل، احفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة).
```
hostname(config)#copy running-config startup-config
```

التكوينات

يستخدم هذا المستند التكوينات التالية:

ASA الأولي

```
ASA#show running-config
(ASA Version 7.2(3
!
To set the firewall mode to transparent mode, !--- ---!
use the firewall transparent command !--- in global
.configuration mode

firewall transparent
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
nameif failover

description LAN Failover Interface
!
interface Ethernet1
nameif inside
security-level 100
!
interface Ethernet2
nameif outside
security-level 0

Configure no shutdown in the stateful failover ---!
.interface !--- of both Primary and secondary ASA

interface Ethernet3
nameif state
description STATE Failover Interface
!
interface Ethernet4
shutdown
no nameif
no security-level
no ip address
!
interface Ethernet5
shutdown
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
domain-name default.domain.invalid
access-list 100 extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
```

```
    Assign the IP address to the Primary and !--- ---!
  Seconday ASA Security Appliance. ip address 172.16.1.1
                                   255.255.255.0 standby 172.16.1.2

                                                          failover
                                              failover lan unit primary
                                 failover lan interface failover Ethernet0
                                                    failover lan enable
                                                    ****** failover key
                                          failover link state Ethernet3
                    failover interface ip failover 10.1.0.1 255.255.255.0
                                                        standby 10.1.0.2
                  failover interface ip state 10.0.0.1 255.0.0.0 standby
                                                              10.0.0.2

                                          asdm image flash:/asdm-522.bin
                                                  no asdm history enable
                                                       arp timeout 14400
                                      access-group 100 in interface outside
                                 route outside 0.0.0.0 0.0.0.0 172.16.1.3 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:d41d8cd98f00b204e9800998ecf8427e
```

```
end :
```

ASA الثانوي

```
ASA#show running-config
(ASA Version 7.2(3
!
hostname ASA
domain-name default.domain.invalid
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
failover
failover lan unit secondary
failover lan interface failover Ethernet0
failover lan enable
****** failover key
failover interface ip failover 10.1.0.1 255.255.255.0
standby 10.1.0.2
```

التحقق من الصحة

إستخدام أمر show failover

يصف هذا القسم إخراج أمر show fail over. على كل وحدة، يمكنك التحقق من حالة تجاوز الفشل باستخدام الأمر show failover.

ASA الأولي

```
ASA#show failover
Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
(Failover LAN Interface: failover Ethernet0 (up
Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
(Version: Ours 7.2(3), Mate 7.2(3
Last Failover at: 00:08:03 UTC Jan 1 1993
This host: Primary - Active
(Active time: 1820 (sec
Interface inside (172.16.1.1): Normal
Interface outside (172.16.1.1): Normal
Other host: Secondary - Standby Ready
(Active time: 0 (sec
Interface inside (172.16.1.2): Normal
Interface outside (172.16.1.2): Normal

Stateful Failover Logical Update Statistics
(Link : state Ethernet3 (up
Stateful Obj    xmit       xerr       rcv        rerr
  General         185          0          183          0
  sys cmd         183          0          183          0
  up time         0            0          0            0
  RPC services    0            0          0            0
  TCP conn        0            0          0            0
  UDP conn        0            0          0            0
  ARP tbl         0            0          0            0
```

```
L2BRIDGE Tbl    2          0          0          0
Xlate_Timeout   0          0          0          0

                    Logical Update Queue Information
                Cur     Max     Total
                 Recv Q:         0       1       7012
                  Xmit Q:         0       1       185
```

ASA الثانوي

```
ASA(config)#show failover
                                        Failover On
                    Cable status: N/A - LAN-based failover enabled
                                        Failover unit Secondary
                    (Failover LAN Interface: failover Ethernet0 (up
    Unit Poll frequency 200 milliseconds, holdtime 800 milliseconds
            Interface Poll frequency 5 seconds, holdtime 25 seconds
                                        Interface Policy 1
                                Monitored Interfaces 2 of 250 maximum
                                    (Version: Ours 7.2(3), Mate 7.2(3
                               Last Failover at: 16:39:12 UTC Aug 9 2009
                             This host: Secondary - Standby Ready
                                     (Active time: 0 (sec
                          Interface inside (172.16.1.2): Normal
                         Interface outside (172.16.1.2): Normal
                                     Other host: Primary - Active
                                (Active time: 1871 (sec
                          Interface inside (172.16.1.1): Normal
                         Interface outside (172.16.1.1): Normal

                        Stateful Failover Logical Update Statistics
                                    (Link : state Ethernet3 (up
      Stateful Obj    xmit       xerr       rcv        rerr
         General         183        0          183        0
         sys cmd         183        0          183        0
         up time         0          0          0          0
         RPC services    0          0          0          0
         TCP conn        0          0          0          0
         UDP conn        0          0          0          0
         ARP tbl         0          0          0          0
         L2BRIDGE Tbl    0          0          0          0
         Xlate_Timeout   0          0          0          0

                            Logical Update Queue Information
                        Cur     Max     Total
                         Recv Q:         0       1       7043
                          Xmit Q:         0       1       183
```

أستخدم الأمر **show failover state** للتحقق من الحالة.

ASA الأولي

```
                                        ASA#show failover state
                State          Last Failure Reason      Date/Time
                                                  This host  -   Primary
                                               Active         None
                                                Other host -   Secondary
Standby Ready  Comm Failure             00:02:36 UTC Jan 1 1993

                                            ===Configuration State====
                                                    Sync Done
                                            ===Communication State====
```

```
                                                    Mac set
```

الوحدة الثانوية

```
                                                ASA#show failover state
               State          Last Failure Reason      Date/Time
                                                    This host  -   Secondary
                                                Standby Ready  None
                                                      Other host -   Primary
                                                Active         None

                                                  ===Configuration State====
                                                Sync Done - STANDBY
                                                  ===Communication State====
                                                      Mac set
```

للتحقق من عناوين IP الخاصة بوحدة تجاوز الفشل، أستخدم الأمر **show failed over interface**.

الوحدة الأساسية

```
                                                ASA#show failover interface
                                             interface failover Ethernet0
                                System IP Address: 10.1.0.1 255.255.255.0
                                             My IP Address    : 10.1.0.1
                                             Other IP Address : 10.1.0.2
                                                interface state Ethernet3
                                System IP Address: 10.0.0.1 255.255.255.0
                                             My IP Address    : 10.0.0.1
                                             Other IP Address : 10.0.0.2
```

الوحدة الثانوية

```
                                                ASA#show failover interface
                                             interface failover Ethernet0
                                System IP Address: 10.1.0.1 255.255.255.0
                                             My IP Address    : 10.1.0.2
                                             Other IP Address : 10.1.0.1
                                                interface state Ethernet3
                                System IP Address: 10.0.0.1 255.255.255.0
                                             My IP Address    : 10.0.0.2
                                             Other IP Address : 10.0.0.1
```

عرض الواجهات المراقبة

دخلت in order to شاهدت الحالة من monitore قارن: في وحيد سياق أسلوب، العرض مدرب-قارن أمر في شامل تشكيل أسلوب. دخلت في يتعدد سياق أسلوب، **العرض مدرب-قارن** ضمن سياق.

ASA الأولي

```
                                        ASA(config)#show monitor-interface
                                      This host: Primary - Active
                           Interface inside (172.16.1.1): Normal
                          Interface outside (172.16.1.1): Normal
                                  Other host: Secondary - Standby Ready
                           Interface inside (172.16.1.2): Normal
                          Interface outside (172.16.1.2): Normal
```

ASA الثانوي

```
ASA(config)#show monitor-interface
        This host: Secondary - Standby Ready
  Interface inside (172.16.1.2): Normal
  Interface outside (172.16.1.2): Normal
                  Other host: Primary - Active
  Interface inside (172.16.1.1): Normal
  Interface outside (172.16.1.1): Normal
```

ملاحظة: إذا لم تقم بإدخال عنوان IP لتجاوز الفشل، فإن الأمر **show** failover يعرض 0.0.0.0 لعنوان IP ومراقبة الواجهة يظلان في حالة *انتظار*. راجع قسم show failover من *مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2* للحصول على مزيد من المعلومات حول حالات تجاوز الفشل المختلفة.

عرض أوامر تجاوز الفشل في التكوين الجاري تشغيله

لعرض أوامر تجاوز الفشل في التكوين الجاري، أدخل هذا الأمر:

```
hostname(config)#show running-config failover
```

يتم عرض جميع أوامر تجاوز الفشل. على الوحدات التي تعمل في وضع سياق متعدد، أدخل الأمر **show running-config failover** في مساحة تنفيذ النظام. أدخل الأمر **show running-config all failover** لعرض أوامر تجاوز الفشل في التكوين الجاري وتضمين الأوامر التي لم تقم بتغيير القيمة الافتراضية لها.

إختبارات وظائف تجاوز الفشل

أكمل هذه الخطوات لاختبار وظيفة تجاوز الفشل:

1. اختبر أن الوحدة النشطة أو مجموعة تجاوز الفشل تتجاوز حركة مرور البيانات كما هو متوقع مع FTP (على سبيل المثال) لإرسال ملف بين الأجهزة المضيفة على الواجهات المختلفة.
2. فرض تجاوز الفشل على الوحدة الاحتياطية باستخدام هذا الأمر:بالنسبة لتجاوز الفشل النشط/الاحتياطي، أدخل هذا الأمر على الوحدة النشطة:
```
hostname(config)#no failover active
```
3. أستخدم FTP لإرسال ملف آخر بين نفس مضيفين.
4. إذا لم يكن الاختبار ناجحا، فأدخل **الأمر show failover** للتحقق من حالة تجاوز الفشل.
5. عند الانتهاء، يمكنك إستعادة الوحدة أو مجموعة تجاوز الفشل إلى الحالة النشطة باستخدام هذا الأمر:بالنسبة لتجاوز الفشل النشط/الاحتياطي، أدخل هذا الأمر على الوحدة النشطة:
```
hostname(config)#failover active
```

تجاوز الفشل المفروض

لإجبار الوحدة الاحتياطية على أن تصبح نشطة، أدخل أحد الأوامر التالية:

أدخل هذا الأمر على الوحدة الاحتياطية:

```
hostname#failover active
```

أدخل هذا الأمر على الوحدة النشطة:

```
hostname#no failover active
```

تجاوز الفشل المعطل

دخلت in order to أعجزت تجاوز الفشل، هذا أمر:

```
hostname(config)#no failover
```

إذا قمت بتعطيل تجاوز الفشل على زوج نشط/إحتياطي، فإنه يؤدي إلى الحفاظ على حالة الاستعداد والنشاط لكل وحدة حتى تقوم بإعادة التشغيل. على سبيل المثال، تبقى الوحدة الاحتياطية في وضع الاستعداد بحيث لا تبدأ كلتا الوحدتين في تمرير حركة مرور البيانات. لجعل الوحدة الاحتياطية نشطة (حتى مع تعطيل التغلب على الأعطال)، راجع قسم فرض تجاوز الأعطال.

إذا قمت بتعطيل تجاوز الفشل على زوج نشط/نشط، فإنه يتسبب في بقاء مجموعات تجاوز الفشل في الحالة النشطة على أي وحدة هي نشطة فيها حاليا، بغض النظر عن الوحدة التي تم تكوينها لتفضلها. يمكن إدخال الأمر no fail over في مساحة تنفيذ النظام.

إستعادة وحدة معطلة

دخلت in order to أحيات وحدة فاشل إلى دولة غير فاشل، هذا أمر:

```
hostname(config)#failover reset
```

إذا قمت باستعادة وحدة معطلة إلى حالة عدم فشل، فإنها لا تجعلها نشطة تلقائيا؛ حيث تبقى الوحدات أو المجموعات التي تمت استعادتها في حالة الاستعداد حتى تصبح نشطة من خلال تجاوز الفشل (سواء كان ذلك مفروضا أو طبيعيا). الاستثناء هو مجموعة تجاوز الفشل التي تم تكوينها باستخدام الأمر المسبق. إذا كانت نشطة في السابق، فإن مجموعة تجاوز الفشل تصبح نشطة إذا تم تكوينها باستخدام الأمر المسبق وإذا كانت الوحدة التي فشلت فيها هي الوحدة المفضلة لها.

استكشاف الأخطاء وإصلاحها

عند حدوث تجاوز للفشل، يقوم كلا جهازي الأمان بإرسال رسائل النظام. يتضمن هذا القسم الموضوعات التالية

- مراقبة تجاوز الفشل
- فشل الوحدة
- ASA-3-210005: فشلت LU في توزيع الاتصال٪
- رسائل نظام تجاوز الفشل
- رسائل تصحيح الأخطاء
- SNMP
- مشكلات معروفة

مراقبة تجاوز الفشل

يوضح هذا المثال ما يحدث عندما لا يبدأ تجاوز الفشل في مراقبة واجهات الشبكة. لا يبدأ تجاوز الفشل في مراقبة واجهات الشبكة حتى يسمع حزمة الثانية من الوحدة الأخرى على تلك الواجهة. يستغرق ذلك حوالي 30 ثانية. إذا كانت الوحدة متصلة بمحول شبكة يشغل بروتوكول الشجرة المتفرعة (STP)، فإن ذلك يستغرق ضعف وقت الذي تم تكوينه في المحول، والذي يتم تكوينه عادة في 15 ثانية، بالإضافة إلى هذا التأخير الذي يبلغ 30 ثانية. وذلك نظرا لأنه في بدء تشغيل ASA ومباشرة بعد حدث تجاوز الفشل، يكتشف محول الشبكة حلقة جسر مؤقتة. على كشف من هذا

أنشوطة، يتوقف أن يرسل ربط على هذا قارن ل وقت. ثم يدخل وضع للحصول على وقت لإعادة التوجيه، وفي ذلك الوقت يستمع المحول لحلقات تكرار الجسر ولكنه لا يقوم بإعادة توجيه حركة مرور البيانات أو إعادة توجيه تجاوز الفشل بالحزم. بعد مرتين من وقت التأخير الأمامي (30 ثانية)، يتم إستئناف تدفق حركة المرور. يظل كل ASA في وضع حتى يسمع ما قيمته 30 ثانية من حزم من الوحدة الأخرى. في غضون الوقت الذي يقوم فيه ASA بتمرير حركة المرور، لا تفشل الوحدة الأخرى بناء على عدم سماع حزم . ولا تزال مراقبة تجاوز الأعطال الأخرى تحدث، أي الطاقة وفقدان الواجهة للارتباط بكبل تجاوز الأعطال.

بالنسبة لتجاوز الفشل، توصي Cisco بشدة بأن يقوم العملاء بتمكين PortFast على جميع منافذ المحول التي تتصل بواجهات ASA. in addition، أعجزت يقني و trunking على هذا ميناء. إذا سقطت واجهة ASA ضمن تجاوز الفشل، فلن يكون على المحول الانتظار لمدة 30 ثانية بينما يتم نقل المنفذ من حالة الاستماع إلى التعلم إلى إعادة التوجيه.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
This host: Primary - Active
(Active time: 6930 (sec
(Interface inside (172.16.1.1): Normal (Waiting
(Interface outside (172.16.1.1): Normal (Waiting
Other host: Secondary - Standby
(Active time: 15 (sec
(Interface inside (172.16.1.2): Normal (Waiting
(Interface outside (172.16.1.2): Normal (Waiting
```

وباختصار، تحقق من هذه الخطوات لتقليل مشاكل تجاوز الفشل:

- تحقق من كبلات الشبكة المتصلة بالقارن في حالة الانتظار/الفشل، وإذا كان ذلك ممكنا، استبدلها.
- إذا كان هناك محول متصل بين الوحدتين، فتحقق من أن الشبكات المتصلة بالقارن في وظيفة حالة الانتظار/الفشل بشكل صحيح.
- فحصت المفتاح ميناء يربط إلى القارن في الانتظار/failed دولة و، إن يكون هو يمكن، استعملت الآخر FE ميناء على المفتاح.
- فحصت أن أنت مكنت ميناء سريع وأعجزت على حد سواء trunking وقني على المفتاح ميناء أن يكون ربطت إلى القارن.

فشل الوحدة

في هذا المثال، كشف تجاوز الفشل عن فشل. لاحظ أن الواجهة 1 على الوحدة الأساسية هي مصدر الفشل. عادت الوحدات إلى وضع بسبب الفشل. أزالت الوحدة الفاشلة نفسها من الشبكة (الواجهات معطلة) ولم تعد ترسل حزم على الشبكة. تظل الوحدة النشطة في حالة حتى يتم إستبدال الوحدة المعطلة وتبدأ إتصالات تجاوز الأعطال من جديد.

```
Failover On
Cable status: Normal
Reconnect timeout 0:00:00
(This host: Primary - Standby (Failed
(Active time: 7140 (sec
(Interface inside (172.16.1.2): Normal (Waiting
(Interface outside (172.16.1.2): Failed (Waiting
Other host: Secondary - Active
(Active time: 30 (sec
(Interface inside (172.16.1.1): Normal (Waiting
(Interface outside (172.16.1.1): Normal (Waiting
```

فشل تخصيص الاتصال ل LU

قد توجد مشكلة في الذاكرة إذا تلقيت رسالة الخطأ هذه:

```
LU
```

وثقت هذا إصدار في cisco بق CSCte80027 id (يسجل زبون فقط). لحل هذه المشكلة، قم بترقية جدار الحماية إلى إصدار برنامج يتم فيه إصلاح هذا الخطأ. بعض إصدارات برنامج ASA التي تم إصلاح هذا الخطأ تحتها هي 8.2(4)، 8.3(2)، 8.4(2).

رسائل نظام تجاوز الفشل

يصدر جهاز الأمان عددا من رسائل النظام المتعلقة بتجاوز الفشل على مستوى الأولوية 2، مما يشير إلى وجود حالة حرجة. لعرض هذه الرسائل، ارجع إلى تكوين تسجيل دخول جهاز الأمان من Cisco ورسائل سجل النظام لتمكين التسجيل ورؤية أوصاف رسائل النظام.

ملاحظة: من خلال عملية التحويل، يتم إيقاف عملية تجاوز الفشل بشكل منطقي ثم يتم جلب الواجهات، التي تقوم بإنشاء رسائل **411001** و**411002**. هذا هو النشاط الطبيعي.

رسائل تصحيح الأخطاء

لعرض رسائل تصحيح الأخطاء، أدخل الأمر **debug fover**. راجع مرجع أمر جهاز أمان Cisco للحصول على مزيد من المعلومات.

ملاحظة: نظرا لأن إخراج تصحيح الأخطاء يتم تعيينه كأولوية عالية في عملية وحدة المعالجة المركزية، فقد يؤثر ذلك بشكل كبير على أداء النظام. ولهذا السبب، أستخدم أوامر **تصحيح الأخطاء** فقط لاستكشاف أخطاء معينة وإصلاحها أو داخل جلسات أستكشاف الأخطاء وإصلاحها مع موظفي الدعم الفني من Cisco.

SNMP

من أجل إستقبال ملائمات SNMP syslog لتجاوز الفشل، قم بتكوين عميل SNMP لإرسال ملائمات SNMP إلى محطات إدارة SNMP، وتحديد مضيف syslog، وتجميع قاعدة معلومات الإدارة (MIB) ل Cisco syslog في محطة إدارة SNMP لديك. راجع أوامر **خادم snmp** و**logging** في مرجع أوامر جهاز الأمان من Cisco للحصول على مزيد من المعلومات.

زمن تجاوز الفشل

لتحديد أوقات الانتظار واستطلاع آراء وحدة تجاوز الفشل، أستخدم الأمر **تجاوز الفشل** في وضع التكوين العام.

ترحب إستطلاعات (MSEC) بالرسائل لتمثل الفاصل الزمني للتحقق من وجود الوحدة الاحتياطية.

وبالمثل، تمثل [] الإعداد للفترة الزمنية التي يجب أن تتلقى الوحدة خلالها رسالة ترحيب على إرتباط تجاوز الفشل، وبعد ذلك يتم إعلان فشل وحدة النظير.

لتحديد أوقات الانتظار واستطلاع واجهة البيانات في تكوين نشط/إستعداد لتجاوز الفشل، أستخدم الأمر **FailOver Timeout interface** في وضع التكوين العام. لاستعادة الاستقصاء الافتراضي وأوقات الانتظار، أستخدم الصيغة **no** من هذا الأمر.

```
[failover polltime interface [msec] time [holdtime time
```

أستخدم أمر **تجاوز الفشل** في **واجهة** وقت **الدراسة** لتغيير التردد الذي يتم عنده إرسال حزم HELLO إلى واجهات

البيانات. هذا الأمر متوفر فقط للتغلب على الأعطال في وضع الاستعداد/النشط. بالنسبة لتجاوز الفشل النشط/النشط، أستخدم أمر **واجهة الوقت المستغرق** في وضع تكوين مجموعة تجاوز الفشل بدلا من أمر **واجهة وقت فحص تجاوز الفشل**.

لا يمكنك إدخال قيمة *Holdtime* أقل من 5 أضعاف وقت إستطلاع الواجهة. بفضل وقت الاستقصاء الأسرع، يمكن لجهاز الأمان اكتشاف الأعطال والتغلب على الأعطال بشكل أسرع. ومع ذلك، قد يؤدي الاكتشاف السريع إلى حدوث محولات غير ضرورية عند إزدحام الشبكة مؤقتا. يبدأ إختبار الواجهة عندما لا يتم سماع حزمة مرحبا على الواجهة لأكثر من نصف وقت الانتظار.

يمكنك تضمين كل من أوامر واجهة وقت تجاوز الفشل في تكوين وحدة زمن الاستجابة والتغلب على الأعطال.

يقوم هذا المثال بتعيين تكرار وقت إستطلاع الواجهة إلى 500 ملي ثانية ووقت الانتظار إلى 5 ثوان:

```
hostname(config)#failover polltime interface msec 500 holdtime 5
```

راجع قسم تجاوز الفشل والوقت المستغرق في *مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2* للحصول على مزيد من المعلومات.

تصدير الشهادة/المفتاح الخاص في تكوين تجاوز الفشل

يقوم الجهاز الأساسي تلقائيا بنسخ المفتاح/الشهادة الخاصة إلى الوحدة الثانوية. قم بإصدار الأمر **write memory** في الوحدة النشطة لنسخ التكوين، والذي يتضمن المفتاح الشهادة/الخاص، إلى الوحدة الاحتياطية. يتم مسح جميع المفاتيح/الشهادات الموجودة على الوحدة الاحتياطية وإعادة نشرها بواسطة تكوين الوحدة النشطة.

ملاحظة: يجب ألا تقوم باستيراد الشهادات والمفاتيح ونقاط الثقة يدويا من الجهاز النشط ثم تصديرها إلى جهاز الاستعداد.

تحذير: فشل فك تشفير رسالة تجاوز الفشل.

رسالة الخطأ:

```
Failover message decryption failure. Please make sure both units have the
same failover shared key and crypto license or system is not out of memory
```

تحدث هذه المشكلة بسبب تكوين مفتاح تجاوز الفشل. لحل هذه المشكلة، قم بإزالة مفتاح تجاوز الفشل، وتكوين المفتاح المشترك الجديد.

المشكلة: دائما ما يكون تجاوز الفشل مرفرفا بعد تكوين وضع الاستعداد/النشط المتعدد الشفاف لتجاوز الفشل

يكون تجاوز الفشل ثابتا عندما تكون الواجهات الداخلية لكل من الخادمين (ASA) متصلة مباشرة وتكون الواجهات الخارجية لكل من الخادمين (ASA) متصلة مباشرة. ولكن تجاوز الفشل يرفرف عندما يتم إستخدام محول ما بين المحولات.

الحل: قم بتعطيل وحدة بيانات بروتوكول الجسر (BPDU) على واجهات ASA لحل هذه المشكلة.

تجاوز فشل وحدات ASA

إذا تم إستخدام وحدة خدمات الأمان والفحص والمنع المتقدم (AIP-SSM) أو وحدة خدمات أمان المحتوى والتحكم في الأمان (CSC-SSM) في الوحدات النشطة والاحتياطية، فإنها تعمل بشكل مستقل عن ASA من حيث تجاوز

الفشل. **يجب تكوين الوحدات النمطية يدويا في الوحدات النشطة والاحتياطية، ولا يقوم تجاوز الفشل بنسخ تكوين الوحدة النمطية.**

ومن حيث تجاوز الفشل، يجب أن تكون كل من وحدات ASA التي تحتوي على وحدات AIP-SSM أو CSC-SSM من نفس نوع الجهاز. على سبيل المثال، إذا كانت الوحدة الأساسية تحتوي على وحدة ASA-SSM-10، فيجب أن تحتوي الوحدة الثانوية على وحدة ASA-SSM-10.

فشل تحويل كتلة رسالة تجاوز الفشل

رسالة خطأ `() :PIX|ASA-3-105010`

شرح: تم استنفاد ذاكرة الحظر. هذه رسالة مؤقتة، ويجب إسترداد جهاز الأمان. كما يمكن إدراج *الأساسي كثانوي* للوحدة الثانوية.

الإجراء الموصى به: أستخدم الأمر **show blocks** لمراقبة ذاكرة الكتلة الحالية.

مشكلة تجاوز فشل وحدة AIP

إذا كان لديك إثنان من ASAs في تكوين تجاوز الفشل وكان لكل واحد AIP-SSM، فيجب عليك نسخ تكوين AIP-SSMs يدويا. يتم نسخ تكوين ASA فقط بواسطة آلية تجاوز الفشل. لا يتم تضمين AIP-SSM في تجاوز الفشل.

أولا، تعمل دليل التحقق من سلامة طبقة الأمان (AIP-SSM) بشكل مستقل عن دليل الأمان من حيث تجاوز الفشل. ولتجاوز الفشل، فإن كل ما يلزم من منظور ASA هو أن تكون وحدات AIP من نفس نوع الجهاز. وفيما عدا ذلك، كما هو الحال مع أي جزء آخر من تجاوز الفشل، يجب أن يكون تكوين ASA بين الطراز النشط والحامل الاحتياطي متزامنا.

وفيما يتعلق بإنشاء دليل الطيران، فإن هذه الأجهزة هي أجهزة إستشعار مستقلة بصورة فعالة. لا يوجد تجاوز للفشل بين الاثنين، ولا يوجد لديهم وعي ببعضهم البعض. يمكنهم تشغيل إصدارات مستقلة من التعليمات البرمجية. أي أنها لا تحتاج إلى التطابق، و ASA لا يهمه إصدار الرمز على دليل الطيران فيما يتعلق بتجاوز الفشل.

يباشر ASDM توصيل إلى AIP من خلال الإدارة قارن IP أن أنت شكلت على AIP. بمعنى آخر، يتصل بالمستشعر بشكل نموذجي من خلال HTTPS، والذي يعتمد على كيفية إعداد المستشعر.

يمكنك إجراء تجاوز فشل ASA بشكل مستقل عن وحدات IPS (AIP). لا تزال متصلا بالمحول نفسه لأنك تتصل ب IP الخاص بإدارته. للاتصال بدليل الطيران الآخر، يجب عليك إعادة الاتصال ب IP الخاص بإدارته لتكوينه والوصول إليه.

ارجع إلى ASA: إرسال حركة مرور الشبكة من ASA إلى مثال تكوين AIP SSM للحصول على مزيد من المعلومات وعينة من التكوينات حول كيفية إرسال حركة مرور الشبكة التي تمر عبر جهاز الأمان القابل للتكيف (ASA 5500 Series إلى وحدة خدمات الأمان والفحص والمنع المتقدم (IPS) (AIP-SSM)

مشكلات معروفة

عندما تحاول الوصول إلى ASDM على ASA الثانوي مع برنامج الإصدار x.8 وإصدار ASDM 6.x لتكوين تجاوز الفشل، يتم إستلام هذا الخطأ:

:

في الشهادة، يكون عنوان المصدر واسم الموضوع هو عنوان IP للوحدة *النشطة*، وليس عنوان IP الخاص بوحدة *الاستعداد*.

في الإصدار x.8 من ASA، يتم نسخ الشهادة الداخلية (ASDM) من الوحدة النشطة إلى الوحدة الاحتياطية، مما يتسبب في رسالة الخطأ. ولكن، إذا كان جدار الحماية نفسه يعمل على رمز الإصدار x.7 مع ASDM.5 x وحاولت

الوصول إلى ASDM، فأنت تتلقى تحذير الأمان العادي هذا:

عند التحقق من الشهادة، يكون المصدر واسم الموضوع عنوان IP للوحدة الاحتياطية.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- برنامج جدار حماية Cisco PIX
- تكوين تجاوز فشل الوحدة النمطية لخدمات جدار الحماية (FWSM)
- أستكشاف أخطاء FWSM وإصلاحها
- كيفية عمل تجاوز الفشل على جدار حماية Cisco Secure PIX
- 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).