ASA/PIX: تكوين تجاوز الفشل النشط/النشط في الوضع الشفاف

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 معباً 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/نشط في الوضع الشفاف على جهاز أمان 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 ASA/PIX 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.

تجاوز الفشل النشط/النشط

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

نظرة عامة على تجاوز الفشل النشط/النشط

لا يتوفر تجاوز الفشل النشط/النشط إلا لأجهزة الأمان في وضع السياق المتعدد. في تكوين نشط/نشط لتجاوز الفشل، يمكن لكل من أجهزة الأمان تمرير حركة مرور الشبكة.

في حالة تجاوز الفشل النشط/النشط، يمكنك تقسيم سياقات الأمان الموجودة على جهاز الأمان إلى مجموعات تجاوز الفشل. مجموعة تجاوز الفشل هي ببساطة مجموعة منطقية لسياق أمان واحد أو أكثر. يمكنك إنشاء مجموعتي تجاوز فشل كحد أقصى على جهاز الأمان. دائما ما يكون سياق الإدارة عضوا في مجموعة تجاوز الفشل 1. يعد أي سياق أمان غير معين أيضا أعضاء في مجموعة تجاوز الفشل 1 بشكل افتراضي.

تشكل مجموعة تجاوز الفشل الوحدة الأساسية لتجاوز الفشل في تجاوز الفشل النشط/النشط. تعد مراقبة أعطال الواجهة وتجاوز الفشل والحالة النشطة/الاحتياطية كلها سمات لمجموعة تجاوز الأعطال بدلا من الوحدة. عند فشل مجموعة نشطة لتجاوز الفشل، فإنها تتغير إلى حالة الاستعداد بينما تصبح مجموعة التغلب على الأعطال في وضع الاستعداد نشطة. يفترض الواجهات في مجموعة تجاوز الفشل التي تصبح نشطة عناوين MAC و IP الخاصة بواجهات مجموعة تجاوز الفشل التي فشلت. تتسلم الواجهات في مجموعة تجاوز الفشل الموجودة الآن في حالة الاستعداد عناوين MAC و IP في وضع الاستعداد.

ملاحظة: لا يعني فشل مجموعة تجاوز الفشل في وحدة ما أن الوحدة قد فشلت. لا يزال بإمكان الوحدة الحصول على مجموعة أخرى لتجاوز الأعطال التي تمرر حركة مرور البيانات عليها.

الحالة الأساسية/الثانوية والحالة النشطة/الاحتياطية

وكما هو الحال في الوحدات النشطة/الاحتياطية للتغلب على الأعطال، يتم تخصيص وحدة واحدة في زوج نشط/نشط للتغلب على الأعطال للوحدة الأساسية، بينما يتم تعيين الوحدة الأخرى للوحدة الثانوية. على عكس تجاوز الفشل النشط/الاحتياطي، لا يشير هذا التعيين إلى الوحدة التي تصبح نشطة عندما تبدأ كلتا الوحدتين في وقت واحد. وبدلا من ذلك، فإن التصنيف الأولي/الثانوي يقوم بأمرين:

- تحديد الوحدة التي توفر التكوين الجاري تشغيله للزوج عند التمهيد في الوقت نفسه.
- تحديد الوحدة التي تظهر فيها كل مجموعة تجاوز فشل في الحالة النشطة عند تمهيد الوحدات في وقت واحد. يتم تكوين كل مجموعة تجاوز فشل في التكوين باستخدام تفضيل وحدة أساسية أو ثانوية. يمكنك تكوين كلتا مجموعتي تجاوز الفشل في الحالة النشطة على وحدة واحدة في الزوج، مع الوحدة الأخرى التي تحتوي على مجموعات تجاوز الفشل في حالة الاستعداد. ولكن، تتمثل التهيئة الأكثر نموذجية في تخصيص كل مجموعة لتجاوز الفشل تفضيل دور مختلف لجعل كل واحدة نشطة على وحدة مختلفة، وتوزيع حركة مرور البيانات عبر الأجهزة.**ملاحظة: لا** يوفر جهاز الأمان خدمات موازنة الأحمال. يجب معالجة موازنة التحميل بواسطة حركة مرور موجه إلى جهاز الأمان.

يتم تحديد الوحدة التي تصبح كل مجموعة تجاوز فشل نشطة عليها كما هو موضح

- عندما يتم تمهيد الوحدة أثناء عدم توفر وحدة النظير، تصبح كلتا مجموعتي تجاوز الفشل نشطة على الوحدة.
- عندما يتم تمهيد الوحدة أثناء نشاط وحدة النظير (مع وجود مجموعتي تجاوز الفشل في الحالة النشطة)، تظل مجموعات تجاوز الفشل في الحالة النشطة للوحدة النشطة بغض النظر عن التفضيل الأساسي أو الثانوي لمجموعة تجاوز الفشل حتى حدوث أحد هذه الحالات:يحدث تجاوز فشل.يمكنك فرض مجموعة تجاوز الفشل يدويا على الوحدة الأخرى باستخدام الأمر no fail over activeلقد قمت بتهيئة مجموعة تجاوز الفشل باستخدام الأمر **الوقائي**، والذي يتسبب في أن تصبح مجموعة تجاوز الفشل نشطة تلقائيا على الوحدة المفضلة عند توفر الوحدة.
- وعند تمهيد كلتا الوحدتين في نفس الوقت، تصبح كل مجموعة لتجاوز الفشل نشطة على وحدتها المفضلة بعد مزامنة التكوينات.

تهيئة الجهاز ومزامنة التكوين

تحدث مزامنة التكوين عندما تكون إحدى الوحدات أو كلتا الوحدتين في تمهيد زوج تجاوز الفشل. تتم مزامنة التكوينات كما هو موضح:

- عندما يتم تمهيد الوحدة أثناء نشاط وحدة النظير (مع وجود كلتا مجموعتي تجاوز الفشل نشطتين عليها)، تتصل وحدة التمهيد بالوحدة النشطة للحصول على التكوين الجاري تشغيله بغض النظر عن تسمية وحدة التمهيد الأساسية أو الثانوية.
- عندما يتم تحميل كلتا الوحدتين في نفس الوقت، تحصل الوحدة الثانوية على التكوين الجاري تشغيله من الوحدة الأساسية.

عند بدء النسخ المتماثل، تقوم وحدة تحكم جهاز الأمان على الوحدة التي ترسل التكوين بعرض الرسالة " : "، وعندما يكتمل، يعرض جهاز الأمان الرسالة " . أثناء النسخ المتماثل، لا يمكن للأوامر التي تم إدخالها على الوحدة التي ترسل التكوين إجراء النسخ المتماثل بشكل صحيح إلى وحدة النظير، ويمكن الكتابة فوق الأوامر التي تم إدخالها على الوحدة التي تتلقى التكوين بواسطة التكوين الذي يتم إستلامه. لا تقم بإصدار أوامر على أي من الوحدات في زوج تجاوز الفشل أثناء عملية نسخ التكوين المتماثل. قد تستغرق عملية النسخ المتماثل، والتي تعتمد على حجم التكوين، من بضع ثوان إلى عدة دقائق.

على الوحدة التي تستلم التكوين، يوجد التكوين فقط في الذاكرة قيد التشغيل. لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة) بعد المزامنة، أدخل الأمر write memory all في مساحة تنفيذ النظام على الوحدة التي تحتوي على مجموعة تجاوز الفشل 1 في الحالة النشطة. يتم نسخ الأمر نسخا متماثلا إلى وحدة النظير، والتي تنتقل إلى كتابة التكوين الخاص بها إلى ذاكرة Flash (الذاكرة المؤقتة). يتسبب إستخدام الكلمة الأساسية **all** مع هذا الأمر في حفظ النظام وجميع تكوينات السياق.

ملاحظة: يمكن الوصول إلى تكوينات بدء التشغيل المحفوظة على الخوادم الخارجية من أي من الوحدتين عبر الشبكة ولا يلزم حفظها بشكل منفصل لكل وحدة. بدلا من ذلك، يمكنك نسخ ملفات تكوين السياقات من القرص الموجود على الوحدة الأساسية إلى خادم خارجي، ثم نسخها إلى قرص على الوحدة الثانوية، حيث تصبح متوفرة عند إعادة تحميل الوحدة.

نسخ الأوامر

بعد تشغيل كلا الوحدتين، يتم نسخ الأوامر من وحدة إلى أخرى كما هو موضح:

- يتم نسخ الأوامر التي تم إدخالها ضمن سياق الأمان نسخا متماثلا من الوحدة التي يظهر عليها سياق الأمان في الحالة النشطة إلى وحدة النظير.**ملاحظة:** يتم مراعاة السياق في الحالة النشطة لوحدة ما إذا كانت مجموعة تجاوز الفشل التي تنتمي إليها في الحالة النشطة لتلك الوحدة.
- يتم نسخ الأوامر التي تم إدخالها في مساحة تنفيذ النظام من الوحدة التي توجد عليها مجموعة تجاوز الفشل 1 في الحالة النشطة إلى الوحدة التي توجد عليها مجموعة تجاوز الفشل 1 في حالة الاستعداد.
- يتم نسخ الأوامر التي تم إدخالها في سياق الإدارة نسخا متماثلا من الوحدة التي توجد عليها مجموعة تجاوز الفشل 1 في الحالة النشطة إلى الوحدة التي توجد عليها مجموعة تجاوز الفشل 1 في حالة الاستعداد.

كل أوامر التكوين والملف (**نسخة، إعادة تسمية، حذف،** rmdir ،**mkdir**، وهكذا) يتم نسخها، مع هذه الاستثناءات. لا يتم نسخ أوامر **وحدة الشبكة المحلية show و debug و mode** وجدار الحماية و**تجاوز الفشل**.

يؤدي الفشل في إدخال الأوامر على الوحدة المناسبة لنسخ الأوامر إلى عدم مزامنة التكوينات. من المحتمل أن تفقد هذه التغييرات في المرة التالية التي يتم فيها مزامنة التكوين الأولي.

يمكنك إستخدام الأمر **write standby** لإعادة مزامنة التكوينات التي أصبحت غير متزامنة. بالنسبة للإستعداد النشط/**الكتابة** تجاوز الأعطال النشط، يتصرف أمر **الكتابة في وضع الاستعداد** كما هو موضح:

- إذا قمت بإدخال الأمر **write standby** في مساحة تنفيذ النظام، فسيتم كتابة تكوين النظام والتكوينات لجميع سياقات الأمان على جهاز الأمان إلى وحدة النظير. ويتضمن ذلك معلومات التكوين لسياقات الأمان الموجودة في حالة الاستعداد. يجب إدخال الأمر في مساحة تنفيذ النظام على الوحدة التي تحتوي على مجموعة تجاوز الفشل 1 في الحالة النشطة.**ملاحظة:** في حالة وجود سياقات أمان في الحالة النشطة على وحدة النظير، يتسبب الأمر **write** standby في إنهاء الاتصالات النشطة من خلال هذه السياقات. أستخدم الأمر **تجاوز الفشل** النشط على الوحدة التي توفر التكوين للتأكد من أن جميع السياقات نشطة على تلك الوحدة قبل إدخال الأمر **write standby**.
- إذا قمت بإدخال الأمر **write standby** في سياق أمان، فسيتم كتابة التكوين لسياق الأمان فقط إلى وحدة النظير. يجب إدخال الأمر في سياق الأمان على الوحدة التي يظهر فيها سياق الأمان في الحالة النشطة.

لا يتم حفظ الأوامر المنسوخة نسخا متماثلا في ذاكرة Flash (الذاكرة المؤقتة) عند نسخها نسخا متماثلا إلى وحدة النظير. تتم إضافتها إلى التكوين الجاري تشغيله. لحفظ الأوامر المنسوخة نسخا متماثلا إلى ذاكرة Flash (الذاكرة المؤقتة) على كلا الوحدتين، أستخدم الأمر **write memory** أو **copy running-config startup-config** على الوحدة التي قمت بإجراء التغييرات عليها. يتم نسخ الأمر نسخا متماثلا إلى وحدة النظير ويتسبب في حفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة) على وحدة النظير.

مشغلات تجاوز الفشل

في حالة تجاوز الفشل النشط/النشط، يمكن تشغيل تجاوز الفشل على مستوى الوحدة في حالة حدوث أحد هذه الأحداث:

- الوحدة بها عطل في الجهاز.
- الوحدة لديها عطل في الطاقة.
- الوحدة لديها فشل برمجي.
- يتم إدخال الأمر **no failed over active** أو **faultover active** في مساحة تنفيذ النظام.

يتم تشغيل تجاوز الفشل على مستوى مجموعة تجاوز الفشل عند حدوث أحد هذه الأحداث:

- فشل العديد من الواجهات المراقبة في المجموعة.
- يتم إدخال الأمر **no failed over active group_id** أو **failed over active group_id**.

إجراءات تجاوز الفشل

في التهيئة النشطة/النشطة للتغلب على الأعطال، يحدث تجاوز الأعطال على أساس مجموعة تجاوز الأعطال، وليس على أساس النظام. على سبيل المثال، إذا قمت بتحديد كل من مجموعتي تجاوز الفشل كنشاطتين في الوحدة الأساسية، وفشلت مجموعة تجاوز الفشل 1، عندئذ تظل مجموعة تجاوز الفشل 2 نشطة في الوحدة الأساسية، بينما تصبح مجموعة تجاوز الفشل 1 نشطة في الوحدة الثانوية.

ملاحظة: عند تكوين تجاوز الفشل النشط/النشط، تأكد من أن حركة المرور المجمعة لكلا الوحدتين ضمن سعة كل وحدة.

يوضح هذا الجدول إجراء تجاوز الفشل لكل حدث فشل. بالنسبة لكل حدث فشل، يتم تحديد النهج، سواء حدث تجاوز الفشل أم لا، والإجراءات الخاصة بمجموعة تجاوز الفشل النشطة والإجراءات الخاصة بمجموعة تجاوز الفشل الاحتياطية.

حدث الفشل	السياسة	فعل جماعي نشط	إجراء المجموعة الاحتياطية	ملاحظات
الوحدة تتعرض لفشل في الطاقة أو البرمجيات	تجاوز الفشل	أصبح علامة إستعداد كعلامة فشل	كن في وضع الاستعداد. وضع علامة "نشط" كفشل	عند فشل وحدة في زوج تجاوز الفشل، يتم تمييز أي مجموعات نشطة لتجاوز الفشل على تلك الوحدة على أنها فاشلة وتصبح نشطة على وحدة النظير.
فشل الواجهة على مجموعة تجاوز الفشل النشطة التي تتجاوز الحد	تجاوز الفشل	وضع علامة "فشل" على المجموعة النشطة	نشيطا	None
فشل الواجهة على مجموعة تجاوز الفشل في وضع الاستعداد فوق الحد	لا يوجد تجاوز فشل	لا يوجد إجراء	وضع علامة "فشل" على مجموعة الاستعداد	عندما يتم وضع علامة "فشل" على مجموعة تجاوز الفشل الاحتياطية، لا تحاول مجموعة تجاوز الفشل النشطة تجاوز الفشل، حتى في حالة تجاوز حد فشل الواجهة.
عمليات إسترداد مجموعة	لا يوجد	لا	لا	ما لم يتم

تجاوز الفشل النشطة سابقا	تجاوز فشل	يوجد إجراء	يوجد إجراء	تكوينها باستخدام الأمر **الوقائي**، فإن مجموعات تجاوز الفشل تبقى نشطة على وحدتها الحالية.
فشل إرتباط تجاوز الفشل عند بدء التشغيل	لا يوجد تجاوز فشل	نشيطا	نشيطا	إذا كان إرتباط تجاوز الفشل معطلا عند بدء التشغيل، فإن كلتا مجموعتي تجاوز الفشل على 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 إرتباط تجاوز الفشل أثناء التشغيل	لا يوجد تجاوز فشل	غير متوفر	غير متوفر	تقوم كل وحدة بتمييز واجهة تجاوز الفشل على أنها فاشلة. يجب عليك إستعادة إرتباط تجاوز الفشل في أقرب وقت

				ممكن لأن الوحدة لا يمكن أن تتعطل إلى الوحدة الاحتياطية بينما إرتباط تجاوز الفشل معطل.

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 (عندما يتم تشغيله 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 بإدارة المكالمات. يحدث هذا لعدم وجود معلومات جلسة عمل لرسالة تعليق CTIQBE على الوحدة

الاحتياطية. عندما لا يتلقى عميل IP SoftPhone إستجابة من "إدارة المكالمات" خلال فترة زمنية معينة، فإنه يعتبر "إدارة المكالمات" غير قابلة للوصول ويلغي التسجيل نفسه.

قيود تكوين تجاوز الفشل

لا يمكنك تكوين تجاوز الفشل باستخدام هذه الأنواع من عناوين IP:

- عناوين IP التي تم الحصول عليها من خلال DHCP
- عناوين IP التي تم الحصول عليها من خلال PPPoE
- عناوين IPv6

وبالإضافة إلى ذلك، تنطبق هذه القيود:

- لا يتم دعم تجاوز الفشل ذو الحالة على جهاز الأمان القابل للتكيف طراز ASA 5505.
- لا يتم دعم تجاوز الفشل النشط/النشط على جهاز الأمان القابل للتكيف ASA 5505.
- لا يمكنك تكوين تجاوز الفشل عندما يتم تمكين ميزة Easy VPN Remote على جهاز الأمان القابل للتكيف ASA 5505.
- تجاوز فشل VPN غير مدعوم في وضع السياق المتعدد.

ميزات غير مدعومة

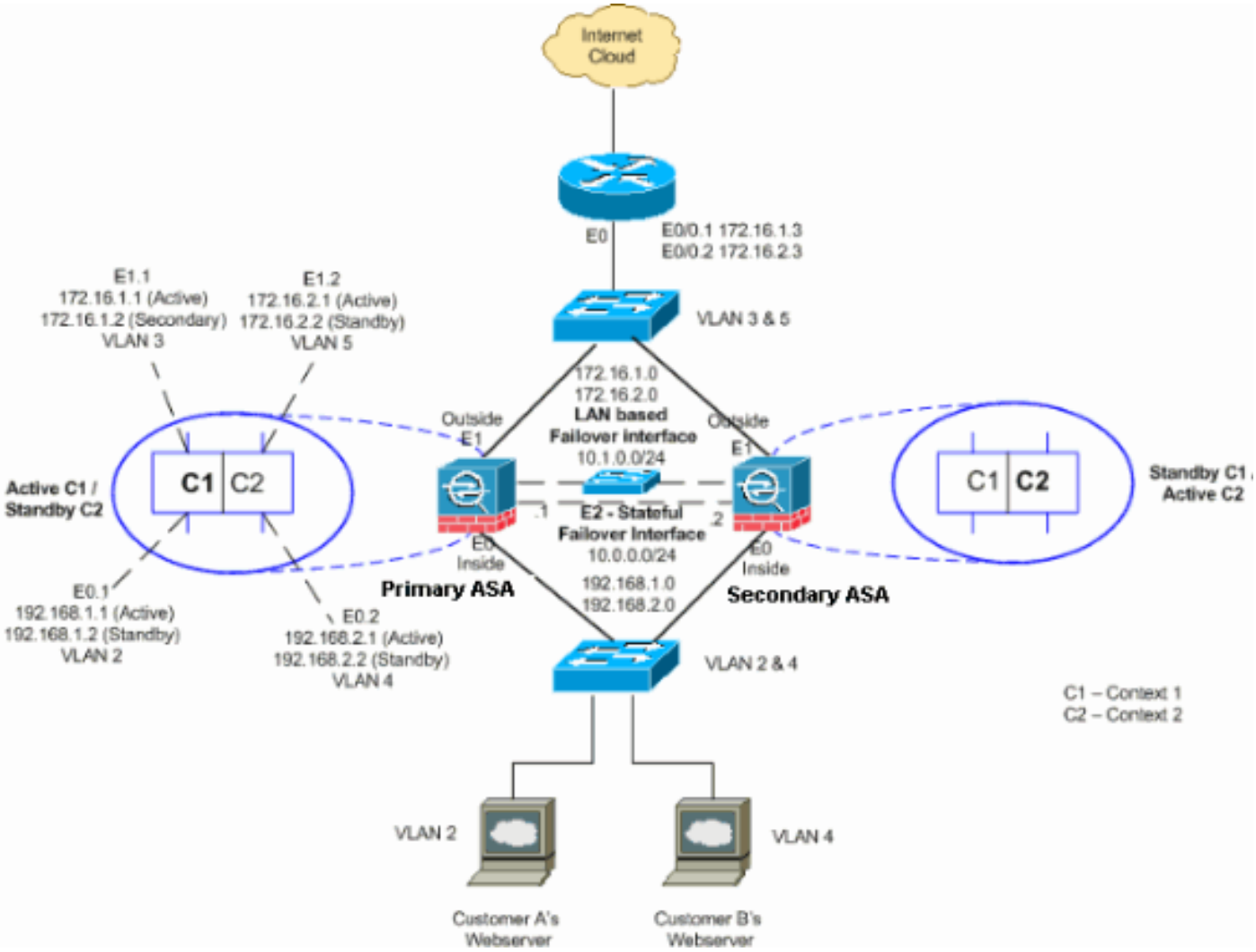
لا يدعم وضع السياق المتعدد هذه الميزات:

- بروتوكولات التوجيه الديناميكيةلا تدعم سياقات الأمان إلا المسارات الثابتة. لا يمكنك تمكين OSPF أو RIP في وضع سياق متعدد.
- VPN
- البث المتعدد

تكوين نشط/نشط لتجاوز الفشل مستند إلى شبكة LAN

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



يوضح هذا القسم كيفية تكوين تجاوز الفشل النشط/النشط 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: بدلا من كبل إيثرنت عكسي لربط الوحدات مباشرة، توصي Cisco باستخدام محول مخصص بين الوحدات الأساسية والثانوية.

يتضمن هذا القسم الموضوعات كما هو موضح:

- تكوين الوحدة الأساسية
- تكوين الوحدة الثانوية

تكوين الوحدة الأساسية

أكمل هذه الخطوات لتكوين الوحدة الأساسية في تكوين نشط/نشط لتجاوز الفشل:

1. إذا لم تكن قد قمت بذلك بالفعل، قم بتكوين عناوين IP النشطة والاحتياطية لكل واجهة بيانات (الوضع الموجه)، أو لعنوان IP الخاص بالإدارة (الوضع الشفاف)، أو للواجهة الخاصة بالإدارة فقط. يتم إستخدام عنوان IP الاحتياطي على جهاز الأمان الذي يمثل حاليا الوحدة الاحتياطية. يجب أن يكون في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط.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. في وضع جدار الحماية الشفاف، يجب إدخال عنوان IP للإدارة لكل سياق.**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 تحدد الحالة في خطوة لاحقة.

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

في المثال، يتم تكوين الواجهة الخارجية للسياق 1 من ASA الأساسي بهذه الطريقة:

```
ASA/context1(config)#ip address 172.16.1.1 255.255.255.0
 standby 172.16.1.2
```

للسياق 2:

```
ASA/context2(config)#ip address 192.168.2.1 255.255.255.0
 standby 192.168.2.2
```

في وضع جدار الحماية الموجه ولواجهة الإدارة فقط، يتم إدخال هذا الأمر في وضع تكوين الواجهة لكل واجهة. في وضع جدار الحماية الشفاف، يتم إدخال الأمر في وضع التكوين العام.

2. قم بتكوين معلمات تجاوز الفشل الأساسية في مساحة تنفيذ النظام.(جهاز أمان PIX فقط) تمكين التغلب على الأعطال القائم على الشبكة المحلية (LAN):

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

تعيين الوحدة كوحدة رئيسية:

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

حدد إرتباط تجاوز الفشل:

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

في هذا المثال، نستخدم الواجهة إيثرنت 3 كواجهة تجاوز الفشل المستندة إلى شبكة LAN.

```
ASA(config)#failover lan interface LANFailover ethernet3
```

تقوم وسيطة if_name بتعيين اسم منطقي للواجهة المحددة بواسطة وسيطة phy_if. يمكن أن تكون وسيطة phy_if هي اسم المنفذ الفعلي، مثل Ethernet1، أو واجهة فرعية تم إنشاؤها مسبقا، مثل Ethernet0/2.3. في جهاز الأمان القابل للتكيف ASA 5505، يحدد PHY_IF شبكة VLAN. لا يجب إستخدام هذه الواجهة لأي غرض آخر (باستثناء إرتباط تجاوز الفشل ذو الحالة (إختياريا).حدد عناوين IP النشطة وحديثة الاستعداد لارتباط تجاوز الفشل:

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

على سبيل المثال، نستخدم 10.1.0.1 كنشاط و 10.1.0.2 كعناوين IP إحتياطية لواجهة تجاوز الفشل.

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

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

تكوين الوحدة الثانوية

عند تكوين تجاوز الفشل النشط/النشط القائم على شبكة LAN، يلزمك تمهيد الوحدة الثانوية للتعرف على إرتباط تجاوز الفشل. وهذا يسمح للوحدة الثانوية بالاتصال بالتكوين الجاري تشغيله واستقباله من الوحدة الأساسية.

أكمل هذه الخطوات لتمهيد الوحدة الثانوية في تكوين تجاوز الفشل النشط/النشط:

1. (جهاز أمان PIX فقط) تمكين تجاوز الفشل المستند إلى شبكة LAN.

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

تحديد واجهة تجاوز الفشل. أستخدم نفس الإعدادات التي أستخدمتها للوحدة الأساسية:حدد الواجهة التي سيتم2. إستخدامها كواجهة تجاوز الفشل.

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

```
ASA(config)#failover lan interface LANFailover ethernet3
```

تقوم وسيطة if_name بتعيين اسم منطقي للواجهة المحددة بواسطة وسيطة phy_if. يمكن أن تكون وسيطة phy_if هي اسم المنفذ الفعلي، مثل Ethernet1، أو واجهة فرعية تم إنشاؤها مسبقا، مثل Ethernet0/2.3. في جهاز الأمان القابل للتكيف ASA 5505، يحدد PHY_IF شبكة VLAN.قم بتعيين عنوان IP النشط والاحتياطي لارتباط تجاوز الفشل:

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

```
ASA(config)#failover interface ip LANFailover 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.يجب أن يكون عنوان IP الاحتياطي في الشبكة الفرعية نفسها الخاصة بعنوان IP النشط. لا تحتاج إلى تعريف قناع الشبكة الفرعية للعنوان الاحتياطي.مكنت القارن.

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

3. تعيين هذه الوحدة كوحدة ثانوية:

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

ملاحظة: هذه الخطوة إختيارية لأنه يتم تعيين الوحدات الثانوية بشكل افتراضي ما لم يتم تكوينها مسبقا بطريقة أخرى.

4. تمكين تجاوز الفشل.

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

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 الاقتران والنهاية لإجراء النسخ المتماثل** على وحدة التحكم النشطة للوحدة.**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.

5 بعد أن ينتهي التكوين الجاري تشغيله من النسخ المتماثل، أدخل هذا الأمر لحفظ التكوين في ذاكرة Flash (الذاكرة المؤقتة):

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

6. عند الضرورة، فرض أي مجموعة تجاوز فشل نشطة على الحالة الأساسية إلى الحالة النشطة على الوحدة الثانوية. لإجبار مجموعة تجاوز الفشل على أن تصبح نشطة على الوحدة الثانوية، أدخل هذا الأمر في مساحة تنفيذ النظام على الوحدة الأساسية:

```
hostname#no failover active group group_id
```

تحدد وسيطة group_id المجموعة التي تريد أن تصبح نشطة على الوحدة الثانوية.

التكوينات

يستخدم هذا المستند التكوينات التالية:

ASA أساسي - تكوين السياق 1

```
ASA/context1(config)#show running-config
Saved :
:
(ASA Version 7.2(3



!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside_context1
nameif inside
security-level 100
Configure the active and standby IP's for the ---!
logical inside !--- interface of the context1. ip
address 192.168.1.1 255.255.255.0 standby 192.168.1.2
!
interface outside_context1
nameif outside
security-level 0
Configure the active and standby IP's for the ---!
logical outside !--- interface of the context1. ip
address 172.16.1.1 255.255.255.0 standby 172.16.1.2
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list 100 extended permit tcp any host 172.16.1.1
eq www
pager lines 24
mtu inside 1500
mtu outside 1500
monitor-interface inside
monitor-interface outside
icmp unreachable rate-limit 1 burst-size 1
asdm image flash:/asdm-522.bin
no asdm history enable
arp timeout 14400
static (inside,outside) 172.16.1.1 192.168.1.5 netmask
255.255.255.255
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
telnet timeout 5
ssh timeout 5
!
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
Cryptochecksum:00000000000000000000000000000000
                                             end :
```

ASA الأساسي - تكوين السياق2

```
                    ASA/context2(config)#show running-config
                                             Saved :
                                                   :
                                  (ASA Version 7.2(3









                                                   !
                                    hostname context2
                enable password 8Ry2YjIyt7RRXU24 encrypted
                                               names
                                                   !
                             interface inside_context2
                                      nameif inside
                                   security-level 100
        Configure the active and standby IP's for the ---!
         logical inside !--- interface of the context2. ip
      address 192.168.2.1 255.255.255.0 standby 192.168.2.2
                                                   !
                            interface outside_context2
                                      nameif outside
                                   security-level 0
        Configure the active and standby IP's for the ---!
         logical outside !--- interface of the context2. ip
      address 172.16.2.1 255.255.255.0 standby 172.16.2.2
                                                   !
                         passwd 2KFQnbNIdI.2KYOU encrypted
    access-list 100 extended permit tcp any host 172.16.2.1
                                             eq www
                                    pager lines 24
                                   mtu inside 1500
                                  mtu outside 1500
```

```
                                    monitor-interface inside
                                   monitor-interface outside
                        icmp unreachable rate-limit 1 burst-size 1
                                asdm image flash:/asdm-522.bin
                                    no asdm history enable
                                         arp timeout 14400
  static (inside,outside) 172.16.2.1 192.168.2.5 netmask
                                               255.255.255.255
                             access-group 100 in interface outside
                        route outside 0.0.0.0 0.0.0.0 172.16.2.3 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
                                            telnet timeout 5
                                               ssh timeout 5
                                                           !
                                 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
                    Cryptochecksum:00000000000000000000000000000000
                                                    end :
```

ASA الأولي

```
                                ASA(config)#show running-config
                                                    Saved :
                                                           :
                                    <ASA Version 7.2(3) <system
                                                           !
      Use the firewall transparent command !--- in ---!
    global configuration mode in order to !--- set the
                             .firewall mode to transparent mode

                                           firewall transparent
```

```
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
no mac-address auto
!
interface Ethernet0
!
interface Ethernet0.1
vlan 2
!
interface Ethernet0.2
vlan 4
!
interface Ethernet1
!
interface Ethernet1.1
vlan 3
!
interface Ethernet1.2
vlan 5
!
Configure "no shutdown" in the stateful failover ---!
interface as well as !--- LAN Failover interface of both
Primary and secondary ASA/PIX. interface Ethernet2
description STATE Failover Interface
!
interface Ethernet3
description LAN Failover Interface
!
interface Ethernet4
shutdown
!
interface Ethernet5
shutdown
!
class default
limit-resource All 0
limit-resource ASDM 5
limit-resource SSH 5
limit-resource Telnet 5
!


ftp mode passive
pager lines 24
failover
failover lan unit primary
Command to assign the interface for LAN based ---!
failover failover lan interface LANFailover Ethernet3
Configure the Authentication/Encryption key ---!
***** failover key
failover link stateful Ethernet2
Configure the active and standby IP's for the LAN ---!
based failover failover interface ip LANFailover
10.1.0.1 255.255.255.0 standby 10.1.0.2
failover interface ip stateful 10.0.0.1 255.255.255.0
standby 10.0.0.2
failover group 1
failover group 2
secondary
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
```

```
                                config-url flash:/admin.cfg
                                                          !


                                                context context1
                                 allocate-interface Ethernet0.1 inside_context1
                                allocate-interface Ethernet1.1 outside_context1
                                             config-url flash:/context1.cfg
                                                     join-failover-group 1
                                                          !


                                                context context2
                                 allocate-interface Ethernet0.2 inside_context2
                                allocate-interface Ethernet1.2 outside_context2
                                             config-url flash:/context2.cfg
                                                     join-failover-group 2
                                                          !


                                                prompt hostname context
                                  Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
                                                              end :
```

ASA الثانوي

```
ASA#show running-config

                                                              failover
                                                failover lan unit secondary
                                    failover lan interface LANFailover Ethernet3
                                                         ***** failover key
failover interface ip LANFailover 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 fail over **show**. على كل وحدة، يمكنك التحقق من حالة تجاوز الفشل باستخدام الأمر **show failover**.

ASA الأولي

```
ASA(config-subif)#show failover
                                                        Failover On
                                Cable status: N/A - LAN-based failover enabled
                                                    Failover unit Primary
                                (Failover LAN Interface: LANFailover Ethernet3 (up
                                Unit Poll frequency 15 seconds, holdtime 45 seconds
                                Interface Poll frequency 5 seconds, holdtime 25 seconds
                                                         Interface Policy 1
                                             Monitored Interfaces 4 of 250 maximum
                                                 (Version: Ours 7.2(3), Mate 7.2(3
                                Group 1 last failover at: 06:12:45 UTC Jan 17 2009
                                Group 2 last failover at: 06:12:43 UTC Jan 17 2009

                                                          This host:    Primary
                                                Group 1       State:          Active
                                                 (Active time:    359610 (sec
                                               Group 2       State:          Standby Ready
                                                  (Active time:    3165 (sec
```

```
context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal
context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal

                                    Other host:   Secondary
                Group 1       State:          Standby Ready
                      (Active time:    0 (sec
                       Group 2       State:          Active
                   (Active time:    3900 (sec

context1 Interface inside (192.168.1.2): Normal
context1 Interface outside (172.16.1.2): Normal
context2 Interface inside (192.168.2.1): Normal
context2 Interface outside (172.16.2.1): Normal

                  Stateful Failover Logical Update Statistics
                       (Link : stateful Ethernet2 (up
    Stateful Obj    xmit       xerr       rcv        rerr
       General         48044      0          48040      1
       sys cmd         48042      0          48040      1
       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         2          0          0          0
       Xlate_Timeout   0          0          0          0

                         Logical Update Queue Information
                Cur     Max     Total
                Recv Q:         0       1       72081
                Xmit Q:         0       1       48044
```

ASA الثانوي

```
                                    ASA(config)#show failover
                                                 Failover On
                    Cable status: N/A - LAN-based failover enabled
                                      Failover unit Secondary
                (Failover LAN Interface: LANFailover Ethernet3 (up
                   Unit Poll frequency 15 seconds, holdtime 45 seconds
              Interface Poll frequency 5 seconds, holdtime 25 seconds
                                           Interface Policy 1
                          Monitored Interfaces 4 of 250 maximum
                              (Version: Ours 7.2(3), Mate 7.2(3
                Group 1 last failover at: 06:12:46 UTC Jan 17 2009
                Group 2 last failover at: 06:12:41 UTC Jan 17 2009

                                    This host:    Secondary
                Group 1       State:          Standby Ready
                      (Active time:    0 (sec
                       Group 2       State:          Active
                   (Active time:    3975 (sec

context1 Interface inside (192.168.1.2): Normal
context1 Interface outside (172.16.1.2): Normal
context2 Interface inside (192.168.2.1): Normal
context2 Interface outside (172.16.2.1): Normal

                                     Other host:   Primary
                          Group 1       State:          Active
                    (Active time:    359685 (sec
```

```
                    Group 2       State:          Standby Ready
                       (Active time:    3165 (sec

context1 Interface inside (192.168.1.1): Normal
context1 Interface outside (172.16.1.1): Normal
context2 Interface inside (192.168.2.2): Normal
context2 Interface outside (172.16.2.2): Normal

                      Stateful Failover Logical Update Statistics
                           (Link : stateful Ethernet2 (up
    Stateful Obj    xmit       xerr       rcv        rerr
       General         940        0          942        2
       sys cmd         940        0          940        2
       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          2          0
       Xlate_Timeout   0          0          0          0

                         Logical Update Queue Information
                    Cur     Max     Total
                     Recv Q:         0       1       1419
                     Xmit Q:         0       1       940
```

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

ASA الأولي

```
                                    ASA(config)#show failover state

State          Last Failure Reason      Date/Time
                                          This host  -   Primary
                                Group 1    Active         None
                                Group 2    Standby Ready  None
                                         Other host -   Secondary
                                Group 1    Standby Ready  None
                                Group 2    Active         None

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

الوحدة الثانوية

```
                                    ASA(config)#show failover state

State          Last Failure Reason      Date/Time
                                          This host  -   Secondary
                                Group 1    Standby Ready  None
                                Group 2    Active         None
                                           Other host -   Primary
                                Group 1    Active         None
                                Group 2    Standby Ready  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(config)#show failover interface
                    interface stateful Ethernet2
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
                 interface LANFailover Ethernet3
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
```

الوحدة الثانوية

```
ASA(config)#show failover interface
                interface LANFailover Ethernet3
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 stateful Ethernet2
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، - أمر في شامل تشكيل أسلوب. دخلت في يتعدد سياق أسلوب، - ضمن سياق.

ملاحظة: لتمكين مراقبة السلامة على واجهة معينة، أستخدم الأمر monitor-interface في وضع التكوين العام:

```
<monitor-interface <if_name
```

ASA الأولي

```
ASA/context1(config)#show monitor-interface
        This host: Secondary - Active
  Interface inside (192.168.1.1): Normal
  Interface outside (172.16.1.1): Normal
     Other host: Secondary - Standby Ready
  Interface inside (192.168.1.2): Normal
  Interface outside (172.16.1.2): Normal
```

ASA الثانوي

```
ASA/context1(config)#show monitor-interface
      This host: Secondary - Standby Ready
  Interface inside (192.168.1.2): Normal
  Interface outside (172.16.1.2): Normal
           Other host: Secondary - Active
  Interface inside (192.168.1.1): Normal
  Interface outside (172.16.1.1): Normal
```

ملاحظة: إذا لم تقم بإدخال عنوان IP لتجاوز الفشل، يعرض الأمر show failover 0.0.0 لعنوان IP، ولا تزال مراقبة الواجهات في حالة . يجب عليك تعيين عنوان IP لتجاوز الفشل حتى تعمل ميزة تجاوز الفشل. ارجع إلى إظهار تجاوز الفشل للحصول على مزيد من المعلومات حول الحالات المختلفة لتجاوز الفشل.

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 failed over** 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 واجهات مختلفة.
2. فرض تجاوز الفشل على الوحدة الاحتياطية باستخدام هذا الأمر:بالنسبة لتجاوز الفشل النشط/النشط، أدخل هذا الأمر على الوحدة التي تكون فيها مجموعة تجاوز الفشل، والتي تحتوي على الواجهة التي تصل بمضيفيك نشطة:
```
hostname(config)#no failover active group group_id
```
3. استعملت FTP in order to أرسلت آخر مبرد بين ال نفسه إثنان مضيف.
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/النشط، أدخل هذا الأمر على الوحدة التي تكون فيها مجموعة تجاوز الفشل، والتي تحتوي على الواجهة التي تصل بمضيفيك نشطة:
```
hostname(config)#failover active group group_id
```

تجاوز الفشل المفروض

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

أدخل هذا الأمر في مساحة تنفيذ النظام للوحدة حيث تكون مجموعة تجاوز الفشل في حالة الاستعداد:

```
hostname#failover active group group_id
```

أو، أدخل هذا الأمر في مساحة تنفيذ النظام للوحدة حيث تكون مجموعة تجاوز الفشل في الحالة النشطة:

```
hostname#no failover active group group_id
```

عندما تقوم بإدخال هذا الأمر في النظام، فإن حيز التنفيذ يؤدي إلى أن تصبح كل مجموعات تجاوز الفشل نشطة:

```
hostname#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 تجاوز الفشل)، راجع قسم تجاوز الفشل الإجباري.

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 فاشل Active/Active تجاوز الفشل مجموعة إلى حالة غير فاشل، هذا أمر:

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

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). والاستثناء هو مجموعة تجاوز الفشل التي تم تكوينها باستخدام الأمر **الوقائي**. إذا كانت نشطة في السابق، فإن مجموعة تجاوز الفشل تصبح نشطة إذا تم تكوينها باستخدام الأمر **الوقائي** وإذا كانت الوحدة التي فشلت فيها هي وحدتها المفضلة.

استكشاف الأخطاء وإصلاحها

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

1. رسائل نظام تجاوز الفشل
2. رسائل تصحيح الأخطاء
3. SNMP

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.

إتصالات تجاوز الفشل الأساسية المفقودة مع رفيق الزواج على interface_name

يتم عرض رسالة تجاوز الفشل هذه إذا لم تعد وحدة واحدة من زوج تجاوز الفشل قادرة على الاتصال بالوحدة الأخرى من الزوج. كما يمكن إدراج الأساسي على أنه ثانوي للوحدة الثانوية.

(أساسي) فقد الاتصالات مع رفيق الزواج عبر الواجهة_name لتجاوز الفشل

تحقق من أن الشبكة المتصلة بالواجهة المحددة تعمل بشكل صحيح.

رسائل تصحيح الأخطاء

لعرض رسائل تصحيح الأخطاء، أدخل الأمر **debug fover**. راجع مرجع أمر جهاز الأمان من Cisco، الإصدار 7.2 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، الإصدار 7.2 للحصول على مزيد من المعلومات.

زمن تجاوز الفشل

لتحديد وقت إجراء إستطلاع وحدة تجاوز الفشل وأوقات الانتظار، قم بإصدار الأمر **تجاوز الفشل لوقت الانتظار** في وضع التكوين العام.

تمثل `[time]` الفاصل الزمني للتحقق من وجود وحدة الاستعداد عن طريق رسائل الترحيب بالاستطلاع.

وعلى نحو مماثل، تمثل `[]` الفترة الزمنية التي يجب أن تتلقى الوحدة خلالها رسالة ترحيب على إرتباط تجاوز الفشل، وبعد ذلك يتم الإعلان عن فشل وحدة النظير.

ارجع إلى وقت دراسة تجاوز الفشل للحصول على مزيد من المعلومات.

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.

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).