فهم تصميم جدار الحماية القائم على المناطق

المحتويات

[المقدمة](#)
[المتطلبات الأساسية](#)
[المتطلبات](#)
[المكونات المستخدمة](#)
[الاصطلاحات](#)
[معلومات أساسية](#)
[نظرة عامة على السياسة المستندة إلى المناطق](#)
[نموذج تكوين السياسات المستند إلى المناطق](#)
[قواعد تطبيق جدار الحماية الخاص بالسياسات المستند إلى المناطق](#)
[أمان شبكة السياسات المستند إلى منطقة التصميم](#)
[إستخدام IPSec VPN مع جدار حماية السياسات المستند إلى المنطقة](#)
[تكوين لغة سياسة Cisco (CPL)](#)
[تكوين مخططات فئة جدار حماية السياسة المستندة إلى المنطقة](#)
[الجمع بين معايير "المطابقة": "التطابق - أي" مقابل "التطابق - الكل"](#)
[تطبيق قائمة التحكم في الوصول (ACL) كمعايير مطابقة](#)
[تكوين مخططات سياسة جدار الحماية المستندة إلى المنطقة](#)
[إجراءات جدار الحماية السياسية المستندة إلى المنطقة](#)
[تكوين معلمات-مخططات جدار حماية Zone-Policy](#)
[تطبيق التسجيل لسياسات جدار الحماية المستندة إلى المناطق](#)
[تحرير مخططات الفئة الخاصة بجدار حماية Zone-Policy ومخططات النهج](#)
[أمثلة التكوين](#)
[جدار حماية توجيه الفحص المعبر عن الحالة](#)
[تكوين نهج إنترنت خاص](#)
[تكوين سياسة DMZ الخاصة](#)
[تكوين نهج Internet DMZ](#)
[جدار الحماية الشفاف للتفتيش المعبر عن الحالة](#)
[تكوين نهج العملاء-الخوادم](#)
[تكوين نهج العملاء-الخوادم](#)
[نهج المعدل لجدار حماية السياسات المستند إلى المناطق](#)
[تكوين نهج ZFW](#)
[Session Control](#)
[فحص التطبيق](#)
[فحص تطبيق HTTP](#)
[تحسينات فحص تطبيق HTTP](#)
[تكوين تحسينات فحص تطبيق HTTP](#)
[دعم ZFW للمراسلة الفورية والتحكم في تطبيق نظير إلى نظير](#)
[قدم برنامج IOS الإصدار 12.4(9)T دعم ZFW لتطبيقات IM و P2P من Cisco.](#)
[فحص تطبيق P2P والتحكم فيه](#)

تكوين فحص P2P
فحص تطبيق المراسلة الفورية والتحكم فيه
تكوين فحص المراسلة الفورية
عوامل تصفية URL
التحكم في الوصول إلى الموجه
قيود سياسة المنطقة الذاتية
تكوين سياسة المنطقة الذاتية
خدمات التطبيقات واسعة النطاق وجدار الحماية القائم على المناطق
مراقبة جدار حماية السياسة المستند إلى المنطقة باستخدام أوامر show و debug
Tune منطقة على القائم الحماية لجدار الدخول من رفض الحماية
الملاحق
الملحق أ: التكوين الأساسي
الملحق ب: التكوين النهائي (الكامل)
الملحق ج: تكوين جدار حماية سياسة المنطقة الأساسي لمنطقتين
معلومات ذات صلة

المقدمة

يصف هذا المستند نموذج التكوين لمجموعة ميزات جدار حماية Cisco IOS®، جدار حماية السياسات المستند إلى المناطق (ZFW).

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

معلومات أساسية

يقدم نموذج التكوين الجديد هذا سياسات سهلة الاستخدام لموجهات الواجهة المتعددة وزيادة دقة تطبيق سياسة جدار الحماية وسياسة رفض الكل الافتراضية التي تمنع حركة المرور بين مناطق أمان جدار الحماية حتى يتم تطبيق سياسة صريحة للسماح بحركة المرور المرغوب فيها.

يتم دعم جميع ميزات جدار حماية Cisco IOS الكلاسيكية التي تم تنفيذها قبل برنامج Cisco IOS، الإصدار 12.4(6)T في واجهة فحص السياسة الجديدة المستندة إلى المناطق:

- فحص حزمة بيانات الحالة
- جدار حماية Cisco IOS المتوافق مع معيار VRF
- تصفية URL
- تخفيف رفض الخدمة (DoS)

أضاف الإصدار 12.4(9)T من برنامج Cisco IOS Software دعم ZFW لجلسة/اتصال لكل فئة وحدود إنتاجية، بالإضافة إلى فحص التطبيقات والتحكم فيها:

- HTTP
- بروتوكول مكتب البريد (POP3) وبروتوكول الوصول إلى بريد الإنترنت (IMAP) وبروتوكول نقل البريد البسيط/البروتوكول المحسن لنقل البريد البسيط (SMTP/ESMTP)
- إستدعاء الإجراء البعيد ل Sun (RPC)
- تطبيقات المراسلة الفورية:Microsoft Messenger وAOL مسنجر! المراسلة الفورية
- مشاركة الملفات بين نظير إلى نظير (P2P):بت تورنتكازاغونتيالإيدونكي

أضاف الإصدار 12.4(11)T من برنامج Cisco IOS Software إحصائيات من أجل ضبط حماية رفض الخدمة (DoS) بشكل أسهل.

بعض ميزات وإمكانات جدار الحماية التقليدي من Cisco IOS غير مدعومة بعد في برنامج ZFW في الإصدار 12.4(15)T من Cisco IOS Software:

- وكيل المصادقة
- تجاوز فشل جدار الحماية المعبر عن الحالة
- قاعدة معلومات الإدارة (MIB) عبر جدار الحماية الموحد
- فحص IPv6 الذي يحدد الحالة
- دعم TCP خارج الطلب

يحسن ZFW بشكل عام أداء Cisco IOS لمعظم أنشطة فحص جدار الحماية. لا يتضمن جدار الحماية التقليدي أو Cisco IOS ZFW دعم الفحص المعبر عن الحالة لحركة مرور البث المتعدد.

نظرة عامة على السياسة المستندة إلى المناطق

قام فحص جدار الحماية التقليدي من Cisco IOS (المعروف سابقا باسم التحكم في الوصول المستند إلى السياق، أو CBAC) باستخدام نموذج تكوين مستند إلى واجهة، تم فيه تطبيق سياسة فحص الحالة على واجهة. تلقت جميع حركات المرور التي تمر عبر هذه الواجهة سياسة التفتيش نفسها. وقد حد نموذج التكوين هذا من قوة سياسات جدار الحماية، وخاصة في مسبب في حدوث إرباك في التطبيق المناسب لسياسات جدار الحماية، وتسيناريوهات التي يجب فيها تطبيق سياسات جدار الحماية بين الواجهات المتعددة.

يعمل جدار الحماية الخاص بالسياسات المستند إلى المنطقة (المعروف أيضا باسم جدار حماية سياسة المنطقة، أو ZFW) على تغيير تكوين جدار الحماية من النموذج القديم القائم على الواجهة إلى نموذج يستند إلى منطقة أكثر مرونة وسهولة في الفهم. يتم تخصيص الواجهات للمناطق، ويتم تطبيق سياسة الفحص على حركة المرور التي تنتقل بين المناطق. وتوفر السياسات المشتركة بين المناطق قدرا كبيرا من المرونة والتحليل، بحيث يمكن تطبيق سياسات تفتيش مختلفة على مجموعات مضيفة متعددة متصلة بنفس واجهة الموجه.

يتم تكوين سياسات جدار الحماية باستخدام لغة سياسة Cisco (CPL)، والتي تستخدم بنية هرمية لتحديد التفتيش لبروتوكولات الشبكة ومجموعات البيانات المضيفة التي

يمكن تطبيق الفحص عليها.

نموذج تكوين السياسات المستند إلى المناطق

يغير ZFW بالكامل طريقة تكوين فحص جدار حماية Cisco IOS، مقارنة بجدار حماية Cisco IOS التقليدي.

يتمثل التغيير الرئيسي الأول في تكوين جدار الحماية في إدخال التكوين المستند إلى مناطق. جدار حماية Cisco IOS هو أول ميزة دفاع ضد التهديدات في برنامج Cisco IOS Software لتنفيذ نموذج تكوين منطقة. يمكن أن تعتمد الميزات الأخرى نموذج المنطقة عبر الوقت. يتم الحفاظ على نموذج التكوين المستند إلى واجهة فحص حالة جدار الحماية التقليدي (أو CBAC) من Cisco IOS الذي يستخدم مجموعة أوامر فحص ip لفترة من الوقت. ومع ذلك، هناك القليل من الميزات الجديدة، إن وجدت، القابلة للتكوين باستخدام واجهة سطر الأوامر الكلاسيكية (CLI). لا يستخدم ZFW أوامر الفحص أو CBAC المعبرة. يمكن استخدام طرازي التكوين بشكل متزامن على الموجهات، ولكن لا يتم دمجها على الواجهات. لا يمكن تكوين الواجهة كعضو في منطقة أمان ويتم تكوينها في الوقت نفسه لفحص ip .

تحدد المناطق حدود الأمان لشبكتك. تحدد المنطقة الحد الذي يتم فيه إخضاع حركة المرور لقيود السياسة أثناء عبورها إلى منطقة أخرى من شبكتك. سياسة ZFW الافتراضية بين المناطق هي رفض الكل. في حالة عدم تكوين أي نهج بشكل صريح، يتم حظر جميع حركات المرور التي تنتقل بين المناطق. هذا خروج كبير من نموذج الفحص المعبر عن الحالة حيث تم السماح بحركة المرور بشكل ضمني حتى تم حظرها بشكل صريح باستخدام قائمة التحكم في الوصول (ACL).

والتغيير الرئيسي الثاني هو إدخال لغة سياسة تكوين جديدة تعرف باسم CPL. يمكن للمستخدمين المعتادين على واجهة سطر الأوامر (MQC) الخاصة بجودة الخدمة النمطية (QoS) لبرنامج Cisco IOS Software التعرف على أن التنسيق مماثل لاستخدام جودة الخدمة الخاصة بجودة الخدمة (QoS) لخرائط الفئة لتحديد حركة المرور التي تتأثر بالإجراء المطبق في خريطة السياسة.

قواعد تطبيق جدار الحماية الخاص بالسياسات المستند إلى المناطق

يخضع أعضاء واجهة شبكة الموجه في المناطق إلى العديد من القواعد التي تحكم سلوك الواجهة، كما هو الحال في حركة المرور التي تنتقل بين واجهات أعضاء المنطقة:

- يجب تكوين منطقة قبل تعيين الواجهات إلى المنطقة.
- يمكن تعيين واجهة لمنطقة أمان واحدة فقط.
- يتم حظر جميع حركات المرور من وإلى واجهة معينة بشكل ضمني عندما يتم تعيين الواجهة على منطقة، باستثناء حركة المرور إلى الواجهات الأخرى في المنطقة نفسها، وحركة المرور إلى أي واجهة على الموجه.
- يسمح لحركة المرور ضمنيا بالتدفق بشكل افتراضي بين الواجهات التي تكون أعضاء في المنطقة نفسها.
- للسماح بحركة المرور من واجهة عضو المنطقة وإليها، يجب تكوين سياسة تسمح بحركة المرور أو تفحصها بين تلك المنطقة وأي منطقة أخرى.
- المنطقة الذاتية هي الاستثناء الوحيد لنهج رفض الكل الافتراضي. يتم السماح بجميع حركات المرور إلى أي واجهة موجه حتى يتم رفض حركة المرور بشكل صريح.
- لا يمكن لحركة المرور التدفق بين واجهة عضو المنطقة وأي واجهة ليس عضوا في المنطقة. لا يمكن تطبيق إجراءات المرور والفحص والإفلات إلا بين منطقتين.

- الواجهات التي لم يتم تعيينها لوظيفة منطقة كمنافذ موجه تقليدية والتي لا يزال بإمكانها استخدام الفحص التقليدي الذي يحدد الحالة/تكوين CBAC.
- إذا كان مطلوبا أن تكون الواجهة الموجودة على المربع جزء من نهج المنطقة/جدار الحماية. وقد يكون من الضروري وضع هذه الواجهة في منطقة ما وتكوين سياسة مرور الكل (ونوع من نهج وهمي) بين تلك المنطقة وأي منطقة أخرى يكون تدفق حركة المرور إليها مطلوبا.
- من السلوك السابق، يتبع ذلك، إذا كانت حركة المرور ستتدفق بين جميع الواجهات في الموجه، فيجب أن تكون جميع الواجهات جزء من نموذج التقسيم إلى مناطق (يجب أن تكون كل واجهة عضوا في منطقة واحدة وأخرى).
- الاستثناء الوحيد للسلوك السابق، وهو الرفض حسب النهج الافتراضي لحركة مرور البيانات من وإلى الموجه، والتي يتم السماح بها بشكل افتراضي. يمكن تكوين نهج صريح لتقييد حركة المرور هذه.

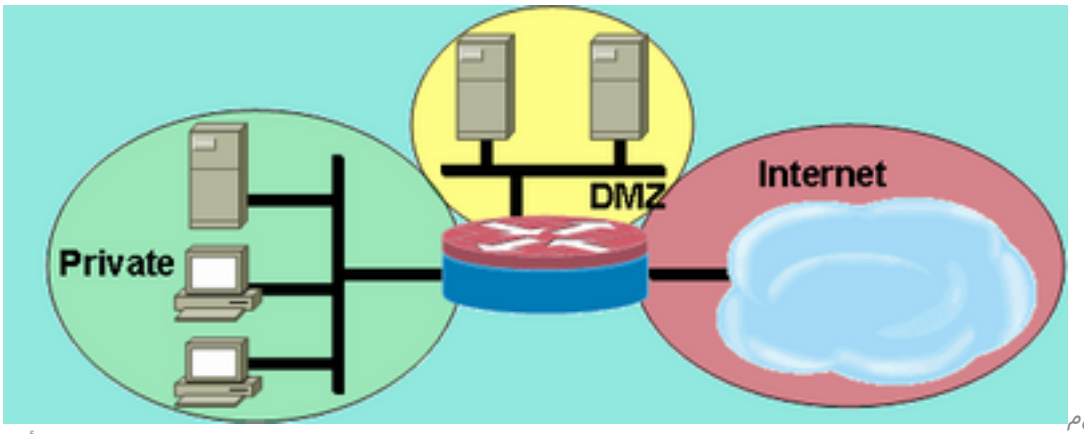
أمان شبكة السياسات المستند إلى منطقة التصميم

يجب تكوين منطقة أمان لكل منطقة ذات أمان نسبي داخل الشبكة، حتى يتم حماية جميع الواجهات التي يتم تعيينها إلى نفس المنطقة بمستوى أمان مماثل. على سبيل المثال، ضع في الاعتبار موجه وصول مزود بثلاث واجهات:

- واجهة واحدة متصلة بالإنترنت العامة
- واجهة واحدة متصلة بشبكة LAN خاصة يجب ألا تكون قابلة للوصول إليها من الإنترنت العامة
- واجهة واحدة متصلة بمنطقة مجردة من السلاح خاصة بخدمة الإنترنت (DMZ)، حيث يجب أن يكون خادم ويب وخادم نظام اسم المجال (DNS) وخادم البريد الإلكتروني قابل للوصول إليه بواسطة الإنترنت العام

يتم تعيين كل واجهة في هذه الشبكة إلى منطقتها الخاصة، على الرغم من أنه يمكن السماح بإدخال مختلف من الإنترنت العامة إلى مضيفين محددين في DMZ وسياسات استخدام تطبيقات متنوعة للمضيفين في شبكة LAN المحمية. (راجع الشكل 1.)

الشكل 1: مخطط منطقة الأمان الأساسية



مخطط منطقة الأمان الأساسية

في هذا المثال، تحتوي كل منطقة على واجهة واحدة فقط. إذا تمت إضافة واجهة إضافية إلى المنطقة الخاصة، فيمكن للمضيفين المتصلين بالواجهة الجديدة في المنطقة تمرير حركة مرور البيانات إلى جميع الأجهزة المضيفة على الواجهة الحالية في المنطقة نفسها. وبالإضافة إلى ذلك، تتأثر حركة مرور المضيف إلى الأجهزة المضيفة في المناطق الأخرى بشكل مماثل بالسياسات الحالية.

نموذجيا، تحتوي شبكة المثال على ثلاثة سياسات رئيسية:

- اتصال المنطقة الخاصة بالإنترنت
- اتصال المنطقة الخاصة بالأجهزة المضيفة DMZ
- اتصال منطقة الإنترنت بالأجهزة المضيفة DMZ

ونظرا لأن المنطقة المنزوعة السلاح معرضة للإنترنت العام، يمكن أن تتعرض مضيفات المنطقة المنزوعة السلاح لنشاط غير مرغوب فيه من الأفراد الضارين الذين يمكن أن ينجحوا في إلحاق الضرر بمضيف واحد أو أكثر من مضيفي المنطقة المنزوعة السلاح. إذا لم يتم توفير سياسة وصول للمضيفين في DMZ للوصول إما إلى مضيفي المنطقة الخاصة أو مضيفي منطقة الإنترنت، فلن يتمكن الأفراد الذين عرضوا للخطر مضيفي DMZ من إستخدام مضيفي DMZ لتنفيذ هجوم إضافي ضد مضيفي الإنترنت أو الخاص. يفرض ZFW وضع أمان افتراضي باهظ. لذلك، ما لم يتم توفير الأجهزة المضيفة ل DMZ خصيصا للوصول إلى الشبكات الأخرى، فسيتم حماية الشبكات الأخرى من أي إتصالات من الأجهزة المضيفة ل DMZ. وعلى نحو مماثل، لا يتم توفير أي وصول لمضيفي الإنترنت للوصول إلى مضيفي المنطقة الخاصة، وبالتالي تكون مضيفات المنطقة الخاصة آمنة من الوصول غير المرغوب من قبل مضيفي الإنترنت.

إستخدام IPSec VPN مع جدار حماية السياسات المستند إلى المنطقة

تعمل التحسينات الأخيرة التي تم إدخالها على شبكة VPN ل IPSec على تبسيط تكوين سياسة جدار الحماية لاتصال VPN. تسمح واجهة النفق الظاهرية (VTI) من IPSec و GRE+IPSec بتقييد إتصالات VPN من موقع إلى موقع والاتصالات العميل بمنطقة أمان معينة من خلال وضع واجهات النفق في منطقة أمان محددة. يمكن عزل الاتصالات في VPN DMZ إذا كان يجب تقييد الاتصال بواسطة نهج معين. أو، إذا كان اتصال VPN موثوق به ضمنيا، يمكن وضع اتصال VPN في نفس منطقة الأمان الخاصة بالشبكة الداخلية الموثوق بها.

إذا تم تطبيق بروتوكول IPSec غير VTI، فستتطلب سياسة جدار حماية اتصال VPN فحصا دقيقا للحفاظ على الأمان. يجب أن يسمح نهج المنطقة بالوصول بشكل خاص بواسطة عنوان IP لمضيفي الموقع البعيد أو عملاء VPN إذا كانت البيئات المضيفة الآمنة في منطقة مختلفة عن اتصال عميل VPN المشفر بالموجه. إذا لم يتم تكوين نهج الوصول بشكل صحيح، فقد ينتهي الأمر بالمضيفين الذين يجب حمايتهم إلى التعرض لمضيفين غير مرغوب فيهم، يحتمل أن يكونوا عدائيين. راجع [إستخدام شبكة VPN مع جدار حماية السياسة المستند إلى المنطقة](#) للحصول على مزيد من مناقشات المفهوم والتكوين.

تكوين لغة سياسة Cisco (CPL)

يمكن إستخدام هذا الإجراء لتكوين ZFW. تسلسل الخطوات ليس مهما، لكن بعض الأحداث يجب إكمالها بالترتيب. على سبيل المثال، يجب تكوين خريطة فئة قبل تعيين خريطة فئة إلى خريطة سياسة. وبالمثل، لا يمكنك تعيين تعيين سياسة لزوج مناطق حتى تقوم بتكوين النهج. إذا حاولت تكوين قسم يعتمد على جزء آخر من التكوين الذي لم تقم بتكوينه، فإن الموجه يستجيب برسالة خطأ.

1. تحديد المناطق.
2. تحديد أزواج المناطق.
3. قم بتعريف مخططات الفئة التي تصف حركة المرور التي يجب أن يكون لها نهج مطبق أثناء عبورها لزوج المناطق.

4. مق بتحديد مخططات السياسة لتطبيق الإجراء على حركة مرور خرائط الفئة.
5. تطبيق خرائط السياسة على أزواج المناطق.
6. مق بتخصيص الواجهات للمناطق.

تكوين مخططات فئة جدار حماية السياسة المستندة إلى المنطقة

تحدد مخططات الفئة حركة مرور البيانات التي يحددها جدار الحماية لتطبيق النهج. موقت ديدحت متي .انه ةجردملا رييعملا هذه ىلإ ادانتسا رورملا ةكرح زرفب ةعبارلا ةئفلا تاططخم هذه المعايير باستخدام أمر المطابقة في خريطة الفئة:

- مجموعة الوصول — يمكن لقائمة التحكم في الوصول (ACL) القياسية أو الموسعة أو المسماة تصفية حركة المرور استنادا إلى عناوين IP للمصدر والوجهة ومنفذ المصدر والوجهة.
- البروتوكول — يمكن تحديد بروتوكولات الطبقة الرابعة (TCP و UDP و ICMP) وخدمات الطبقات مثل HTTP و SMTP و DNS وما إلى ذلك من الخدمات المعروفة أو المعرفة من قبل المستخدم والمعروفة لتعيين تطبيق المنفذ.
- خريطة الفئة — يمكن تضمين خريطة فئة تابعة توفر معايير مطابقة إضافية داخل خريطة فئة أخرى.
- لا — يحدد المعيار not تحديد أي حركة مرور لا تتطابق مع خدمة محددة (بروتوكول) أو مجموعة الوصول أو خريطة الفئة الفرعية لخريطة الفئة.

الجمع بين معايير "المطابقة": "التطابق - أي" مقابل "التطابق - الكل"

يمكن أن تطبق خرائط الفئة عوامل لتشغيل المطابقة-any أو مطابقة-all لتحديد كيفية تطبيق معايير المطابقة. إذا تم تحديد match-any، فيجب أن تتطابق حركة المرور مع أحد معايير المطابقة فقط في خريطة الفئة. إذا تم تحديد تطابق-all، يجب أن تتطابق حركة المرور مع جميع معايير خريطة الفئة لكي تنتمي إلى هذه الفئة المحددة.

يجب تطبيق معايير التطابق من الأكثر تحديدا إلى الأقل تحديدا إذا كانت حركة المرور تطابق معايير متعددة. على سبيل المثال، ضع في اعتبارك هذه الخريطة للفئة:

```
class-map type inspect match-any my-test-cmap
 match protocol http
 match protocol tcp
```

يجب أن تواجه حركة مرور HTTP بروتوكول المطابقة http أولا للتأكد من معالجة حركة المرور بواسطة القدرات الخاصة بالخدمة لتفتيش HTTP. إذا تم عكس خطوط المطابقة، لذلك يواجه حركة المرور بيان TCP الخاص ببروتوكول المطابقة قبل أن يقارنها بمطابقة بروتوكول http، يتم تصنيف حركة المرور كحركة مرور TCP، ويتم فحصها استنادا إلى إمكانيات مكون فحص TCP لجدار الحماية. هذه مشكلة بالنسبة لخدمات معينة مثل FTP و TFTP والعديد من خدمات الوسائط المتعددة والإرسال إشارات الصوت مثل H.323 و SIP و Skinny و RTSP وغيرها. وتتطلب هذه الخدمات قدرات تفتيش إضافية للتعرف على الأنشطة الأكثر تعقيدا لهذه الخدمات.

تطبيق قائمة التحكم في الوصول (ACL) كمعايير مطابقة

يمكن لخرائط الفئة تطبيق قائمة تحكم في الوصول (ACL) كأحد معايير مطابقة تطبيق السياسة. إذا كانت قائمة التحكم في الوصول (ACL) هي معيار خريطة الفئة فقط وكانت قائمة التحكم في الوصول (ACL) هي معيار خريطة الفئة فقط وكانت خريطة الفئة مقترنة بخريطة السياسة التي تطبق إجراء الفحص، فإن المحرك يطبق فحص TCP أو UDP الأساسي لجميع حركة المرور المسموح بها من قبل قائمة التحكم في

الوصول (ACL)، باستثناء تلك التي يوفر ZFW الفحص المستند إلى التطبيقات. ويتضمن ذلك (ولكنه لا يقتصر على) FTP و SIP و Skinny (SCCP) و H.323 و Sun RPC و TFTP. إذا كان الفحص الخاص بالتطبيق متاحا وكانت قائمة التحكم في الوصول تسمح بقناة التحكم أو القناة الأساسية، يتم السماح بأي قناة ثانوية أو قناة وسائط مرتبطة بالتحكم/الأساسي، بغض النظر عما إذا كانت قائمة التحكم في الوصول تسمح بحركة المرور أم لا.

إذا كانت خريطة الفئة تطبق قائمة التحكم في الوصول (ACL) 101 فقط كمعيار مطابقة، تظهر قائمة التحكم في الوصول (ACL) 101 كما يلي:

```
access-list 101 permit ip any any
```

يتم السماح بجميع حركات المرور في إتجاه سياسة المنطقة المطبقة على زوج منطقة معين، ويتم السماح بحركة المرور العائدة التي تتطابق مع هذا في الإتجاه المعاكس. لذلك، يجب أن تضيف قائمة التحكم في الوصول (ACL) التقييد لتحديد حركة المرور إلى أنواع معينة مرغوبة. لاحظ أن قائمة PAM تتضمن خدمات تطبيقات مثل HTTP و NetBIOS و H.323 و DNS. ومع ذلك، على الرغم من معرفة PAM باستخدام التطبيق المحدد لمنفذ معين، فإن جدار الحماية يطبق فقط قدرة تطبيقية كافية للاستيعاب المتطلبات المعروفة جيدا لحركة مرور التطبيق. وبالتالي، يتم فحص حركة مرور التطبيقات البسيطة مثل Telnet و SSH والتطبيقات الأخرى ذات القناة الواحدة على أنها TCP، ويتم دمج إحصائياتها معا في إخراج أمر العرض. إذا كانت الرؤية الخاصة بالتطبيق في نشاط الشبكة مطلوبة، فأنت بحاجة إلى تكوين فحص الخدمات حسب اسم التطبيق (تكوين بروتوكول المطابقة HTTP، ومطابقة بروتوكول telnet، وما إلى ذلك).

قارن الإحصائيات المتاحة في إخراج الأمر show policy-map inspection type-pair zone من هذا التكوين مع سياسة جدار الحماية الأكثر وضوحا الموضحة بشكل إضافي أسفل الصفحة. يتم إستخدام هذا التكوين لفحص حركة المرور من هاتف Cisco IP، بالإضافة إلى العديد من محطات العمل التي تستخدم مجموعة متنوعة من حركة المرور، والتي تتضمن HTTP و FTP و NetBIOS و SSH و DNS:

```
class-map type inspect match-all all-private
 match access-group 101
!
policy-map type inspect priv-pub-pmap
 class type inspect all-private
  inspect
 class class-default
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

بينما يكون هذا التكوين سهل التحديد في جميع حركات المرور التي نشأت في المنطقة الخاصة (والتي تم التعرف عليها القياسية والموجهة بمنافذ حركة المرور طالما لاحظ حركة المرور المعروفة بواسطة PAM)، فإنه يوفر رؤية محدودة في نشاط الخدمة، ولا يوفر الفرصة لتطبيق حدود النطاق الترددي والجلسة الخاصة ب ZFW لأنواع محددة من حركة المرور. يعد

إخراج الأمر show policy-map type فحص المنطقة pair priv-pub اذه نتيجة للتكوين البسيط السابق الذي يستخدم طقف ةمئاق التحكم في الوصول (ACL) المسموح اهب ل IP [الشبكة الفرعية] بين أزواج المناطق. امك ىرت، يتم دع مظعم ةكرح رورم ةطحم العمل في إحصائيات TCP أو UDP الأساسية:

```
stg-871-L#show policy-map type insp zone-pair priv-pub
Zone-pair: priv-pub

  Service-policy inspect : priv-pub-pmap

    Class-map: all-private (match-all)
      Match: access-group 101
      Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [413:51589]
        udp packets: [74:28]
        icmp packets: [0:8]
        ftp packets: [23:0]
        tftp packets: [3:0]
        tftp-data packets: [6:28]
        skinny packets: [238:0]

        Session creations since subsystem startup or last reset 39
        Current session counts (estab/half-open/terminating) [3:0:0]
        Maxever session counts (estab/half-open/terminating) [3:4:1]
        Last session created 00:00:20
        Last statistic reset never
        Last session creation rate 2
        Maxever session creation rate 7
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        0 packets, 0 bytes
```

وعلى النقيض من ذلك، يوفر تكوين لثامم يضيف تائف ةصاخ بالتطبيق إحصائيات وتحكم تاقيبطت أكثر ةقد، الو يزال يستوعب نفس عرض الخدمات الذي تم عرضه في المثال الأول عند تحديد خريطة فئة الفرصة الأخيرة التي طباتق قائمة التحكم في الوصول فقط على أنها الفرصة الأخيرة في خريطة السياسة:

```
class-map type inspect match-all all-private
 match access-group 101
class-map type inspect match-all private-ftp
 match protocol ftp
 match access-group 101
class-map type inspect match-any netbios
 match protocol msrpc
 match protocol netbios-dgm
 match protocol netbios-ns
 match protocol netbios-ssn
class-map type inspect match-all private-netbios
 match class-map netbios
 match access-group 101
class-map type inspect match-all private-ssh
 match protocol ssh
 match access-group 101
class-map type inspect match-all private-http
 match protocol http
 match access-group 101
```

```
!
policy-map type inspect priv-pub-pmap
 class type inspect private-http
  inspect
 class type inspect private-ftp
  inspect
 class type inspect private-ssh
  inspect
 class type inspect private-netbios
  inspect
 class type inspect all-private
  inspect
 class class-default!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect priv-pub-pmap
!
interface FastEthernet4
 ip address 172.16.108.44 255.255.255.0
 zone-member security public
!
interface Vlan1
 ip address 192.168.108.1 255.255.255.0
 zone-member security private
!
access-list 101 permit ip 192.168.108.0 0.0.0.255 any
```

يوفر التكوين الأكثر تحديدا هذا الإخراج الجوهري متعدد المستويات لأمر show policy-map type inspection zone-pair priv-pub:

```
stg-871-L#sh policy-map type insp zone-pair priv-pub
 Zone-pair: priv-pub

   Service-policy inspect : priv-pub-pmap

     Class-map: private-http (match-all)
       Match: protocol http
       Match: access-group 101
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [0:2193]

         Session creations since subsystem startup or last reset 731
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [0:3:0]
         Last session created 00:29:25
         Last statistic reset never
         Last session creation rate 0
         Maxever session creation rate 4
         Last half-open session total 0

     Class-map: private-ftp (match-all)
       Match: protocol ftp
       Inspect
         Packet inspection statistics [process switch:fast switch]
         tcp packets: [86:167400]
         ftp packets: [43:0]

         Session creations since subsystem startup or last reset 7
         Current session counts (estab/half-open/terminating) [0:0:0]
         Maxever session counts (estab/half-open/terminating) [2:1:1]
         Last session created 00:42:49
```

```
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 4
    Last half-open session total 0

Class-map: private-ssh (match-all)
  Match: protocol ssh
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:62]

    Session creations since subsystem startup or last reset 4
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:34:18
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 2
    Last half-open session total 0

Class-map: private-netbios (match-all)
  Match: access-group 101
  Match: class-map match-any netbios
    Match: protocol msrpc
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-dgm
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ns
      0 packets, 0 bytes
      30 second rate 0 bps
    Match: protocol netbios-ssn
      2 packets, 56 bytes
      30 second rate 0 bps
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [0:236]

    Session creations since subsystem startup or last reset 2
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [1:1:1]
    Last session created 00:31:32
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 1
    Last half-open session total 0

Class-map: all-private (match-all)
  Match: access-group 101
  Inspect
    Packet inspection statistics [process switch:fast switch]
    tcp packets: [51725:158156]
    udp packets: [8800:70]
    tftp packets: [8:0]
    tftp-data packets: [15:70]
    skinny packets: [33791:0]

    Session creations since subsystem startup or last reset 2759
    Current session counts (estab/half-open/terminating) [2:0:0]
    Maxever session counts (estab/half-open/terminating) [2:6:1]
    Last session created 00:22:21
    Last statistic reset never
    Last session creation rate 0
```

```
    Maxever session creation rate 12
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop (default action)
    4 packets, 112 bytes
```

وهناك فائدة أخرى مضافة إلى إستخدام تكوين خريطة للفئة وللخريطة السياسية أكثر تقدم، كما ذكر آنفا، وهي الفرصة لتطبيق حدود خاصة بالفئة على قيم الجلسة والأسعار؛ ولضبط معلمات الفحص تحديدا بواسطة تطبيق خريطة للبارامترات لضبط كل سلوك فحص للفئة.

تكوين مخططات سياسة جدار الحماية المستندة إلى المنطقة

تطبق خريطة السياسة إجراءات سياسة جدار الحماية على واحد أو أكثر من خرائط الفئة لتعريف سياسة الخدمة التي يتم تطبيقها على زوج منطقة أمان. عند إنشاء خريطة سياسة من نوع الفحص، يتم تطبيق فئة افتراضية مسماة لفئة تقصير في نهاية الفئة. إجراء النهج الافتراضي لفئة الخدمة هو drop ولكن يمكن تغييره ليتم تمريره. يمكن إضافة خيار السجل مع إجراء الإسقاط. الي يمكن تطبيق الفحص على الفئة الافتراضية.

إجراءات جدار الحماية السياسية المستندة إلى المنطقة

يوفر ZFW ثلاثة إجراءات لحركة المرور التي تجتاز من منطقة إلى أخرى:

- drop — هذا هو الإجراء الافتراضي لجميع حركة المرور، كما هو مطبق بواسطة إعداد الفئة الافتراضي الذي ينهي كل خريطة سياسة من نوع الفحص. كما يمكن تكوين خرائط فئة أخرى داخل خريطة سياسة لإسقاط حركة المرور غير المرغوب فيها. يتم إسقاط حركة المرور التي تتم معالجتها بواسطة إجراء الإسقاط بصمت (بمعنى أنه لا يتم إرسال إعلام بالإفلات إلى المضيف النهائي ذي الصلة) بواسطة ZFW، مقارنة بسلوك قائمة التحكم في الوصول "مضيف يتعذر الوصول إليه" لبروتوكول الرسائل الذي أرسل حركة المرور المرفوضة. حاليا، لا يوجد خيار لتغيير ICMP إلى المضيف الذي تم إسقاط حركة مرور البيانات بواسطة جدار الحماية.
- Pass — يسمح هذا الإجراء للموجه بإعادة توجيه حركة مرور البيانات من منطقة إلى أخرى. يسمح المرور فقط بتتبع إجراء المرور حالة الاتصالات أو الجلسات داخل حركة المرور. يجب تطبيق سياسة موازية للسماح بحركة المرور العائدة لحركة المرور في إتجاه واحد. يدعم إجراء المرور مفيدا لبروتوكولات مثل IPSec ESP و IPSec AH و ISAKMP والبروتوكولات الأخرى التي تتمتع بسلوك بطبيعتها التي يمكن التنبؤ به. ومع ذلك، تتم معالجة معظم حركة مرور التطبيقات بشكل أفضل في ZFW باستخدام إجراء الفحص.
- فحص — يوفر إجراء الفحص مراقبة حركة المرور القائمة على الدولة. على سبيل المثال، إذا تم فحص حركة المرور من المنطقة الخاصة إلى منطقة الإنترنت في المثال السابق على الشبكة، يحتفظ الموجه بمعلومات الاتصال أو جلسة العمل لحركة مرور البروتوكول مخطط بيانات المستخدم (UDP). لذلك، يسمح الموجه بحركة المرور العائدة المرسلة من مضيف منطقة الإنترنت داخل منطقة الاتصال الخاصة. كما يمكن أن توفر عمليات الفحص فحص التطبيقات والتحكم فيها فيما يتعلق ببروتوكولات خدمة معينة يمكن أن تحمل حركة مرور تطبيقات حساسة أو ضعيفة. يمكن تطبيق سجل التدقيق باستخدام خريطة معلمة لتسجيل الاتصال/بدء جلسة العمل، والإيقاف، والمدة، ووحدة تخزين البيانات التي تم نقلها،

وعناوين المصدر والوجهة.

الإجراءات مقترنة بخرائط الفئة في خرائط السياسة:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

توفر مخططات المعلمات خيارات لتعديل معلمات الاتصال الخاصة بنهج فحص مخطط الفئة المحدد.

تكوين معلمات-مخططات جدار حماية Zone-Policy

تحدد مخططات المعلمات سلوك التفتيش ل ZFW، للمعلمات مثل حماية DoS، وتوقيت وأجهزة TCP/UDP، وإعداد تسجيل مسار التدقيق. كما يتم تطبيق خرائط المعلمات مع فئات جلسة الطبقة 7 ومخططات السياسات لتحديد السلوك الخاص بالتطبيق، مثل كائنات HTTP ومتطلبات مصادقة POP3 و IMAP والمعلومات الأخرى الخاصة بالتطبيق.

يتم تكوين خرائط معلمة الفحص ل ZFW كفحص عون، مماثل لفئة ZFW الأخرى وكائنات النهج:

```
stg-871-L(config)#parameter-map type inspect z1-z2-pmap stg-871-L(config-profile)#?
parameter-map commands:
  alert           Turn on/off alert
  audit-trail     Turn on/off audit trail
  dns-timeout     Specify timeout for DNS
  exit            Exit from parameter-map
  icmp            Config timeout values for icmp
  max-incomplete  Specify maximum number of incomplete connections before
                  clamping
  no              Negate or set default values of a command
  one-minute      Specify one-minute-sample watermarks for clamping
  sessions        Maximum number of inspect sessions
  tcp             Config timeout values for tcp connections
  udp             Config timeout values for udp flows
```

تحدد أنواع محددة من خرائط المعلمات المعلمات التي يتم تطبيقها بواسطة سياسات فحص تطبيق الطبقة 7. تعرف مخططات المعلمة من النوع regex تعبيري عادي للاستخدام مع تطبيق فحص تطبيق HTTP الذي يوفي بتصفية حركة المرور باستخدام تعبير عادي:

```
parameter-map type regex [parameter-map-name]
```

تقوم المعلمة-type-info-maps بتعريف أسماء الخوادم لاستخدامها مع فحص تطبيق المراسلة الفورية:

```
parameter-map type protocol-info [parameter-map-name]
```

يتم توفير تفاصيل التكوين الكاملة للتفتيش على تطبيق HTTP و IM في أقسام فحص التطبيق المعنية في هذا المستند.

تطبيق التسجيل لسياسات جدار الحماية المستندة إلى المناطق

يوفر ZFW خيارات التسجيل لحركة المرور التي يتم إسقاطها أو فحصها بشكل افتراضي أو إجراءات سياسة جدار الحماية التي تم تكوينها. يتوفر تسجيل لجس لجس التدقيق لحركة المرور التي يفحصها ZFW. يتم تطبيق لجس التدقيق عندما يتم تحديد لجس تدقيق في خريطة معلمة ويتم تطبيق خريطة المعلمة مع إجراء الفحص في خريطة السياسة:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [parameter-map-name (optional)]
```

يتوفر تسجيل الإسقاط لحركة المرور التي يسقط ZFW. يتم تكوين تسجيل الإسقاط عند إضافة لجس باستخدام إجراء الإسقاط في خريطة السياسة:

```
configure terminal
 policy-map type inspect z1-z2-pmap
  class type inspect service-cmap
   inspect|drop|allow [service-parameter-map]
```

تحرير مخططات الفئة الخاصة بجدار حماية Zone-Policy ومخططات النهج

ال يتضمن ZFW حاليا محرر يمكنه تعديل مختلف بنى ZFW مثل خرائط السياسة، خرائط الفئة، وخرائط المعاملات. من أجل إعادة ترتيب لمج التطابق في تطبيق خريطة الفئة أو الإجراء على مختلف خرائط الفئة الموجودة ضمن خريطة السياسة، يلزمك استكمال الخطوات التالية:

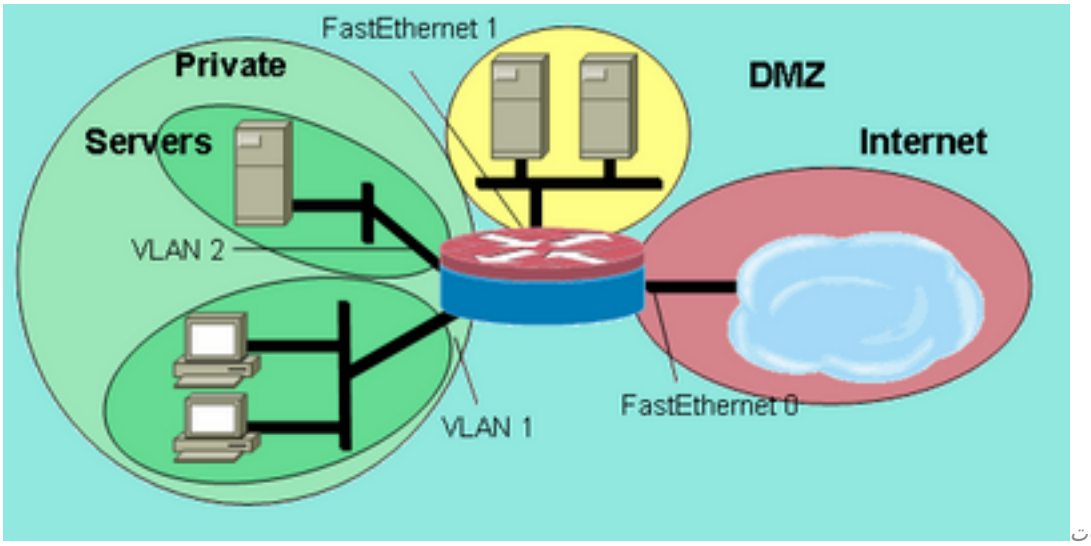
1. انسخ البنية الحالية إلى محرر نصوص مثل Microsoft Windows Notepad، أو محرر مثل VI على منصات Linux/Unix.
2. قم بإزالة البنية الحالية من تكوين الموجه.
3. قم بتحرير الهيكل في محرر النص الخاص بك.
4. انسخ البنية مرة أخرى إلى CLI للموجه.

أمثلة التكوين

يستخدم مثال التكوين هذا موجه الخدمات المدمجة الطراز 1811 من Cisco. يتوفر تكوين أساسي مع اتصال IP وتكوين شبكة VLAN والربط الشفاف بين جزئين من شبكة Ethernet LAN الخاصة في [الملحق أ]. يتم تقسيم الموجه إلى خمس مناطق:

- يتم توصيل الإنترنت العام ب FastEthernet 0 (منطقة الإنترنت)
- يتم توصيل خادم الإنترنت ب FastEthernet 1 (منطقة DMZ)
- تم تكوين منفذ التحويل Ethernet مع شبكتي VLAN:شبكة VLAN1 لمحطات العمل (منطقة العميل). تتصل شبكة VLAN2 بالشبكة المحلية الظاهرية (VLAN) رقم 2 (منطقة الخادم).توجد محطات العميل والخادم في الشبكة الفرعية نفسها. يتم تطبيق جدار حماية شفاف بين المناطق، لذلك فإن السياسات بين المناطق على هاتين الواجهتين يمكن أن تؤثر فقط على حركة المرور بين مناطق العميل والخادم.
- تتصل واجهات VLAN1 و VLAN2 بالشبكات الأخرى من خلال الواجهة الظاهرية للجسر (BVI1). تم تعيين هذه الواجهة للمنطقة الخاصة. (انظر الشكل 2.)

الشكل 2: تفاصيل مخطط المنطقة

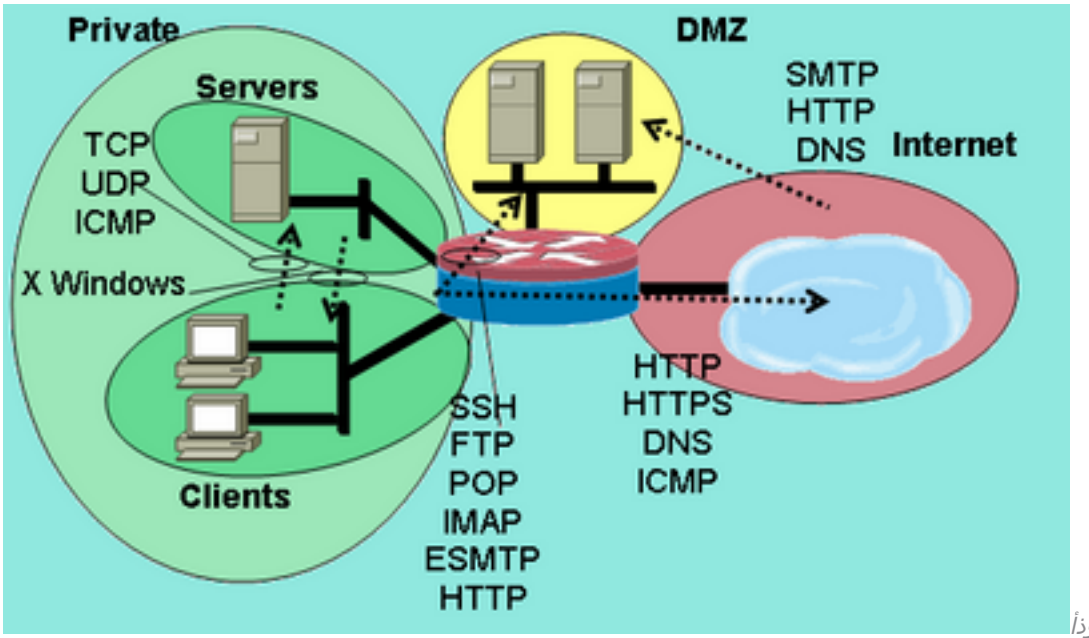


تفاصيل مخطط المنطقة

يتم تطبيق هذه السياسات، مع تحديد مناطق الشبكة مسبقا:

- يمكن للمضيفين في منطقة الإنترنت الوصول إلى خدمات DNS و SMTP و SSH على خادم واحد في DMZ. يوفر الخادم الآخر خدمات SMTP و HTTP و HTTPS. تعمل سياسة جدار الحماية على تقييد الوصول إلى الخدمات المحددة المتوفرة على كل مضيف.
- لا يمكن لمضيفي DMZ الاتصال بمضيفين في أي منطقة أخرى.
- يمكن للمضيفين في منطقة العميل الاتصال بالمضيفين في منطقة الخادم على جميع خدمات TCP و UDP و ICMP.
- لا يمكن للمضيفين في منطقة الخادم الاتصال بالمضيفين في منطقة العميل، إلا إذا كان بإمكان خادم التطبيق المستند إلى UNIX فتح جلسات عمل عميل X Windows إلى خوادم X Windows على أجهزة كمبيوتر سطح المكتب في منطقة العميل على المنافذ من 6900 إلى 6910.
- يمكن لجميع الأجهزة المضيفة في المنطقة الخاصة (والتي تتكون من عملاء وخوادم) الوصول إلى الأجهزة المضيفة في المنطقة DMZ على خدمات SSH و FTP و POP و IMAP و ESMTP و HTTP، وفي منطقة الإنترنت على خدمات HTTP و HTTPS و DNS و ICMP. علاوة على ذلك، يتم تطبيق فحص التطبيقات على إتصالات HTTP من المنطقة الخاصة إلى منطقة الإنترنت لضمان عدم حمل تطبيقات IM و P2P المدعومة على المنفذ 80. (انظر الشكل 3.)

الشكل 3: أذونات خدمة زوج المنطقة التي سيتم تطبيقها في مثال التكوين



أذونات خدمة زوج المنطقة

يتم تكوين سياسات جدار الحماية هذه وفقا للتعقيد:

1. فحص العملاء-الخوادم عبر بروتوكول TCP/UDP/ICMP
2. فحص SSH/FTP/POP/IMAP/ESMTP/HTTP من Private-DMZ
3. تم تقييد فحص Internet -DMZ SMTP/HTTP/DNS حسب عنوان المضيف
4. المكاتب-العملاء X فحص Windows باستخدام خدمة تعيين تطبيق المنفذ (PAM) المحددة
5. بروتوكول HTTP/HTTPS/DNS/ICMP الخاص عبر الإنترنت مع فحص تطبيق HTTP

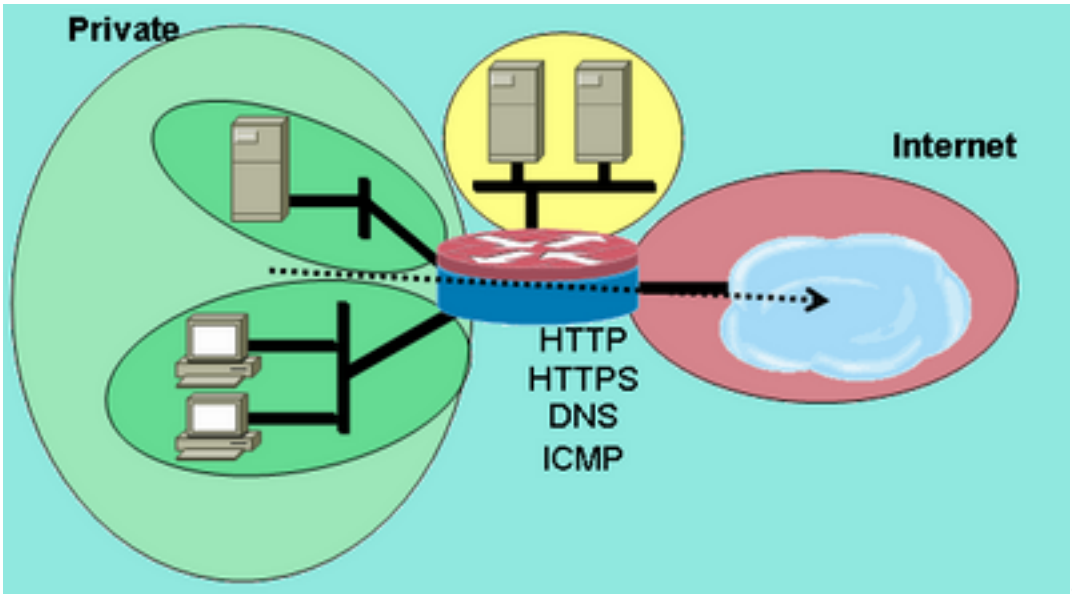
نظرا لأنك تقوم بتطبيق أجزاء من التكوين على مقاطع شبكة مختلفة في أوقات مختلفة، فمن المهم تذكر أن مقطع الشبكة يفقد الاتصال بمقاطع أخرى عند وضعه في منطقة ما. على سبيل المثال، عند تكوين المنطقة الخاصة، يفقد المضيفون في المنطقة الخاصة الاتصال بالمنطقة المنزوعة السلاح ومناطق الإنترنت حتى يتم تحديد سياساتهم الخاصة.

جدار حماية توجيه الفحص المعبر عن الحالة

تكوين نهج إنترنت خاص

الشكل 4 يوضح تكوين سياسة الإنترنت الخاصة.

الشكل 4: التفتيش على الخدمات من المنطقة الخاصة إلى منطقة الإنترنت



فحص الخدمة من المنطقة الخاصة إلى منطقة الإنترنت

تطبق سياسة الإنترنت الخاصة فحص الطبقة 4 على فحص HTTP و HTTPS و DNS و Layer 4 ل ICMP من المنطقة الخاصة إلى منطقة الإنترنت. وهذا يسمح بالاتصالات من المنطقة الخاصة إلى منطقة الإنترنت ويسمح بحركة المرور العائدة. يشتمل فحص الطبقة 7 على ميزات تحكم أكثر إحكاما في التطبيقات وأمان أفضل ودعم أفضل للتطبيقات التي تتطلب الإصلاح. ومع ذلك، يتطلب فحص الطبقة 7، كما هو مذكور، فهما أفضل لنشاط الشبكة، انظر لأنه غير مسموح ببروتوكولات الطبقة 7 التي لم يتم تكوينها للتفتيش بين المناطق.

1. حدد خرائط الفئة التي تصف حركة المرور التي تريد السماح بها بين المناطق، استنادا إلى السياسات الموضحة سابقا:

```
configure terminal
 class-map type inspect match-any internet-traffic-class
  match protocol http
  match protocol https
  match protocol dns
  match protocol icmp
```

2. قم بتكوين خريطة سياسة لفحص حركة المرور على خرائط الفئة التي تم بتعريفها للتو:

```
configure terminal
 policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
```

3. تكوين المناطق الخاصة ومناطق الإنترنت وتخصيص واجهات الموجه للمناطق الخاصة بها:

```
configure terminal
 zone security private
 zone security internet
 int bvi1
  zone-member security private
 int fastethernet 0
  zone-member security internet
```

قم بتكوين زوج المناطق وتطبيق خريطة السياسة المناسبة.

> **ملاحظة**: ما عليك سوى تكوين زوج منطقة الإنترنت الخاصة في الوقت الحالي من أجل فحص الاتصالات المصدرية في المنطقة الخاصة التي تنتقل إلى منطقة الإنترنت، والمبينة بعد ذلك:

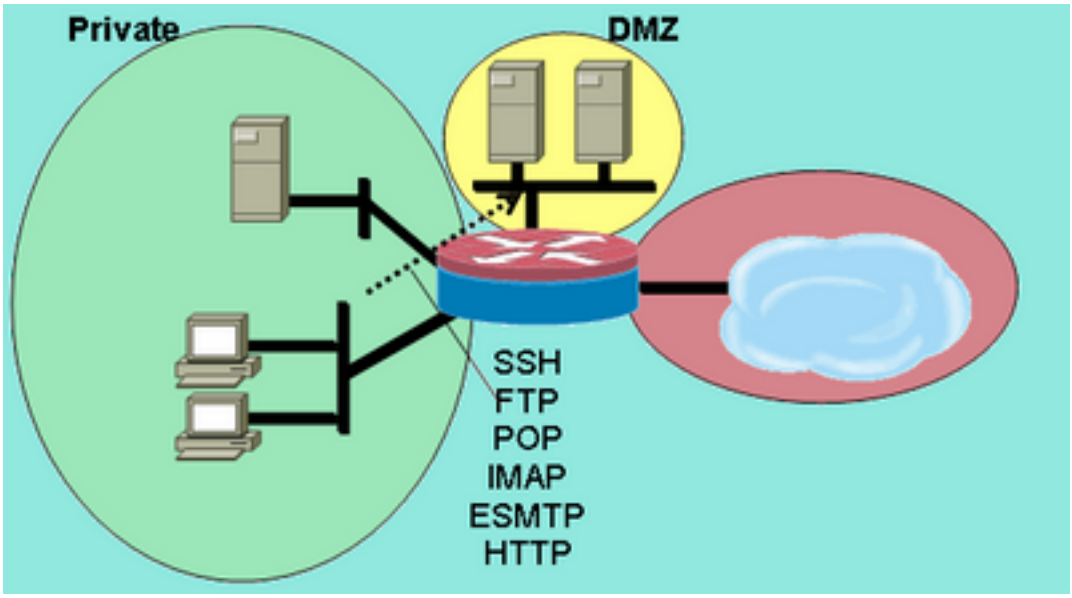
```
configure terminal
 zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
```

يؤدي هذا إلى اكتمال تكوين سياسة فحص الطبقة 7 على زوج مناطق الإنترنت الخاصة للسماح باتصالات HTTP و HTTPS و DNS و ICMP من منطقة العملاء إلى منطقة الخوادم وتطبيق فحص التطبيق على حركة مرور HTTP لضمان عدم السماح بحركة المرور غير المرغوب فيها بالمرور على منفذ خدمة TCP 80 و HTTP.

تكوين سياسة DMZ الخاصة

يوضح الشكل 5 تكوين سياسة DMZ الخاصة.

الشكل 5: التفتيش على الخدمات من المنطقة الخاصة إلى المنطقة المجردة من السلاح



فحص الخدمة من المنطقة الخاصة إلى المنطقة المجردة من السلاح

تضيف سياسة DMZ الخاصة تعقيدات لأنها تتطلب فهما أفضل لحركة مرور الشبكة بين المناطق. يطبق هذا النهج فحص الطبقة 7 من المنطقة الخاصة إلى DMZ. وهذا يسمح بالاتصالات من المنطقة الخاصة إلى DMZ ويسمح بحركة المرور العائدة. يشتمل فحص الطبقة 7 على ميزات تحكم أكثر إحكاما في التطبيقات وأمان أفضل ودعم أفضل للتطبيقات التي تتطلب الإصلاح. ومع ذلك، يتطلب فحص الطبقة 7، كما هو مذكور، فهما أفضل لنشاط الشبكة، نظرا لأنه غير مسموح ببروتوكولات الطبقة 7 التي لم يتم تكوينها للتفتيش بين المناطق.

1. حدد خرائط الفئة التي تصف حركة المرور التي تريد السماح بها بين المناطق، استنادا إلى السياسات الموضحة سابقا:
```
configure terminal
 class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
```
2. قم بتكوين خرائط السياسة لفحص حركة المرور على خرائط الفئة التي قمت بتعريفها للتو:
```
configure terminal
 policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
```
3. تكوين المناطق الخاصة و DMZ وتخصيص واجهات الموجه للمناطق الخاصة بها:
```
configure terminal
 zone security private
 zone security dmz
 int bvi1
  zone-member security private
 int fastethernet 1
  zone-member security dmz
```
4. قم بتكوين زوج المناطق وتطبيق خريطة السياسة المناسبة.

ملاحظة: ما عليك سوى تكوين زوج مناطق DMZ الخاص في الوقت الحالي من أجل فحص الاتصالات المصدرية في المنطقة الخاصة التي تنتقل إلى المنطقة DMZ، الموضحة بعد ذلك:

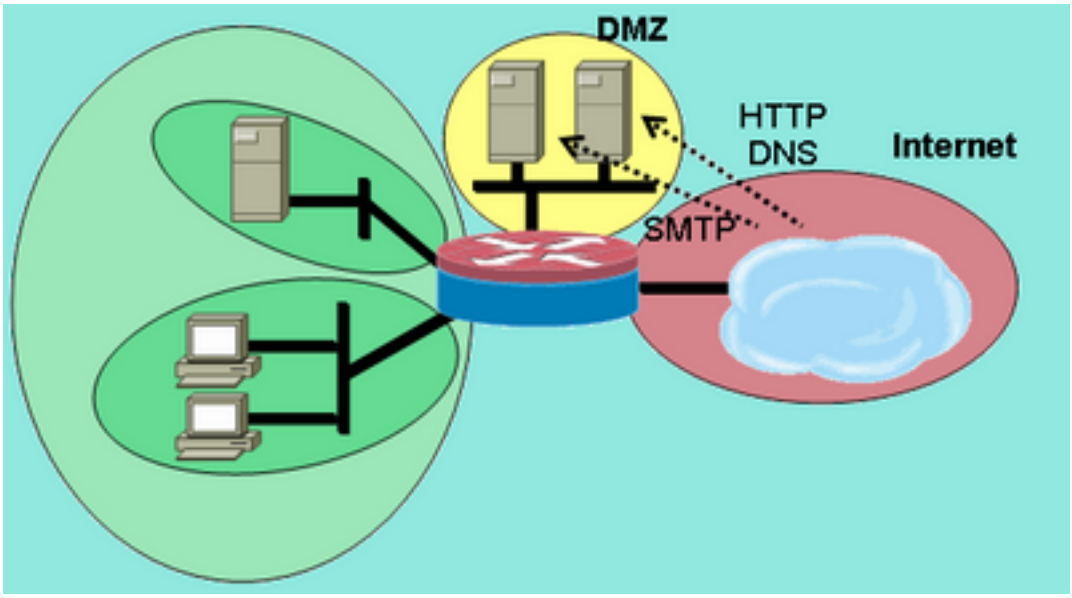
```
configure terminal
 zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
```

يؤدي هذا إلى اكتمال تكوين سياسة فحص الطبقة 7 على DMZ الخاصة للسماح بجميع إتصالات TCP و UDP و ICMP من منطقة العملاء إلى منطقة الخوادم. التطبيق النهج الإضافي للقنوات التابعة ولكنه يقدم مثال للنهج البسيط لاستيعاب معظم إتصالات التطبيقات.

تكوين نهج Internet DMZ

يوضح الشكل 6 تكوين نهج Internet DMZ.

الشكل 6: فحص الخدمات من منطقة الإنترنت إلى المنطقة المجردة من السلاح



فحص الخدمة من منطقة الإنترنت إلى منطقة DMZ

يطبق هذا النهج فحص الطبقة 7 من منطقة الإنترنت إلى DMZ. وهذا يسمح بالاتصالات من منطقة الإنترنت إلى DMZ ويسمح بحركة المرور العائدة من مضيف DMZ إلى مضيف الإنترنت الذي قاموا بإنشاء الاتصال. تجمع سياسة DMZ على الإنترنت بين فحص الطبقة 7 ومجموعات العناوين المحددة من قبل قوائم التحكم في الوصول لتقييد الوصول إلى خدمات معينة على مضيف محدد أو مجموعات مضيف أو شبكات فرعية. لإنجاز ذلك، عليك إنشاء خريطة فئة تحدد الخدمات ضمن خريطة فئة أخرى تشير إلى قائمة تحكم في الوصول (ACL) لتحديد عناوين IP.

1. حدد خرائط الفئة وقوائم التحكم في الوصول (ACL) التي تصف حركة المرور التي تريد السماح بها بين المناطق، استنادا إلى السياسات الموضحة مسبقا.يجب إستخدام العديد من مخططات الفئة للخدمات، حيث يتم تطبيق سياسات وصول مختلفة للوصول إلى خادمين مختلفين. يسمح لمضيف الإنترنت باتصالات DNS و HTTP إلى 172.16.2.2، ويتم السماح لاتصالات SMTP إلى 172.16.2.3. لاحظ الفرق في خرائط الفئة. تستخدم مخططات الفئة التي تحدد الخدمات الكلمة الأساسية match-any للسماح بأي من الخدمات المدرجة. تستخدم مخططات الفئة التي تربط قوائم التحكم في الوصول (ACL) مع خرائط فئة الخدمة الكلمة الأساسية match-all لطلب استيفاء كل الشرطين في خريطة الفئة للسماح بحركة المرور:
```
configure terminal
 access-list 110 permit ip any host 172.16.2.2
 access-list 111 permit ip any host 172.16.2.3
```

```
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
```

2. قم بتكوين خرائط السياسة لفحص حركة المرور على خرائط الفئة التي قمت بتعريفها للتو:

```
configure terminal
 policy-map type inspect internet-dmz-policy
  class type inspect dns-http-acl-class
   inspect
  class type inspect smtp-acl-class
   inspect
```

3. قم بتكوين مناطق Internet و DMZ وعينت واجهات الموجه للمناطق الخاصة بها. تخطي تكوين DMZ إذا قمت بإعداده في القسم السابق:

```
configure terminal
zone security internet
zone security dmz
int fastethernet 0
 zone-member security internet
int fastethernet 1
 zone-member security dmz
```

4. قم بتكوين زوج المناطق وتطبيق خريطة السياسة المناسبة.**ملاحظة**: ما عليك سوى تكوين زوج مناطق DMZ على الإنترنت في الوقت الحالي، لفحص الاتصالات المستمدة في منطقة الإنترنت التي تنتقل إلى المنطقة DMZ، والمبينة بعد ذلك:

```
configure terminal
 zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
```

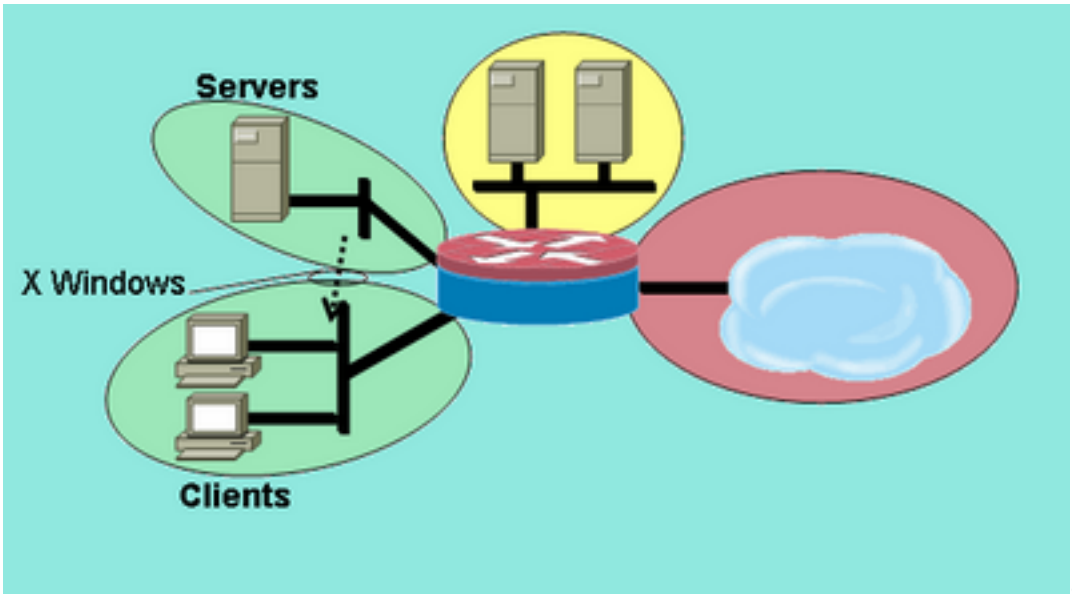
يؤدي هذا إلى اكتمال تكوين سياسة فحص الطبقة 7 الخاصة بالعنوان على زوج مناطق DMZ على الإنترنت.

جدار الحماية الشفاف للتفتيش المعبر عن الحالة

تكوين نهج العملاء-الخوادم

يوضح هذا الشكل التالي تكوين نهج الخادم-العميل.

الشكل 7: فحص الخدمات من منطقة الخوادم إلى منطقة العملاء



فحص الخدمة من منطقة الخوادم إلى منطقة العملاء

يطبق نهج عملاء الخوادم الفحص باستخدام خدمة معرفة من قبل المستخدم. يتم تطبيق فحص الطبقة 7 من منطقة الخوادم إلى منطقة العملاء. وهذا يسمح لاتصالات X Windows بنطاق منفذ معين من منطقة الخوادم إلى منطقة العملاء ويسمح بحركة مرور الإرجاع. X Windows ليس بروتوكول مدعوم من الأصل في PAM، لذلك يجب تحديد خدمة قام المستخدم بتكوينها في PAM حتى يمكن لـ ZFW التعرف على حركة المرور المناسبة وفحصها.

يتم تكوين واجهتين أو أكثر من واجهات الموجهات في مجموعة جسر IEEE لتوفير التوجيه لتوفير الربط بين الواجهات في مجموعة الجسر وللتوجيه إلى (IRB) الربط المتكامل والمجسر الظاهرية (BVI). تطبق سياسة جدار الحماية الشفافة شبكات فرعية أخرى عبر واجهة الجسر "التي تعبر الجسر"، ولكن ليس لحركة المرور التي تترك فحص جدار الحماية لحركة المرور التي تعبر مجموعة الجسر عبر BVI. تنطبق سياسة التفتيش فقط على حركة المرور التي تعبر مجموعة الجسر. لذلك، في هذا السيناريو، يتم تطبيق الفحص فقط على حركة المرور التي تنتقل بين مناطق العملاء والخوادم، والتي يتم تضمينها داخل المنطقة الخاصة. لا تدخل السياسة المطبقة بين المنطقة الخاصة والمناطق العامة والمناطق المنزوعة السلاح في حيز التنفيذ إلا عند خروج حركة المرور من مجموعة الجسر عبر BVI. عندما تغادر حركة المرور عبر BVI من مناطق العملاء أو الخوادم، لا يتم إستدعاء سياسة جدار الحماية الشفافة.

1. تكوين PAM باستخدام إدخال معرف من قبل المستخدم لـ X Windows.يفتح عملاء X Windows (حيث تتم إستضافة التطبيقات) الاتصالات الخاصة بعرض المعلومات للعملاء (حيث يعمل المستخدم) في نطاق يبدأ عند منفذ 6900.يستخدم كل اتصال إضافي منافذ متتالية، لذلك إذا عرض عميل 10 جلسات مختلفة على مضيف واحد، يستخدم الخادم المنافذ 6900-6909. لذلك، إن يفحص أنت الميناء مدى من 6900 إلى 6909، توصيل مفتوح إلى ميناء بعد 6909 يفشل:
```
configure terminal
 ip port-map user-Xwindows port tcp from 6900 to 6910
```
2. مراجعة مستندات PAM لمعالجة أسئلة PAM الإضافية أو التحقق من وثائق فحص البروتوكول متعدد المستويات للحصول على معلومات حول تفاصيل قابلية التشغيل البيني بين PAM وفحص جدار حماية Cisco IOS المعبر عن الحالة.
3. حدد خرائط الفئة التي تصف حركة المرور التي تريد السماح بها بين المناطق، استنادا إلى السياسات الموضحة سابقا:
```
configure terminal
 class-map type inspect match-any Xwindows-class
  match protocol user-Xwindows
```
4. قم بتكوين خرائط السياسة لفحص حركة المرور على خرائط الفئة التي قمت بتعريفها للتو:

```
configure terminal
 policy-map type inspect servers-clients-policy
  class type inspect Xwindows-class
   inspect
```

5. قم بتكوين مناطق العميل والخادم وتخصيص واجهات الموجه للمناطق الخاصة بها.إذا قمت بتكوين هذه المناطق وتعيين الواجهات في قسم تكوين سياسة العملاء-الخوادم، فيمكنك التخطي إلى تعريف زوج المناطق. يتم توفير جسر تكوين IRB من أجل التمام:

```
configure terminal
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
zone security clients
zone security servers
 int vlan 1
 bridge-group 1
 zone-member security clients
int vlan 2
 bridge-group 1
 zone-member security servers
```

6. قم بتكوين زوج المناطق وتطبيق خريطة السياسة المناسبة.**ملاحظة**: ما عليك سوى تكوين زوج منطقة الخوادم-العملاء في الوقت الحالي من أجل فحص الاتصالات التي يتم الحصول عليها من منطقة الخوادم التي تنتقل إلى منطقة العملاء، والتي يتم عرضها بعد ذلك:

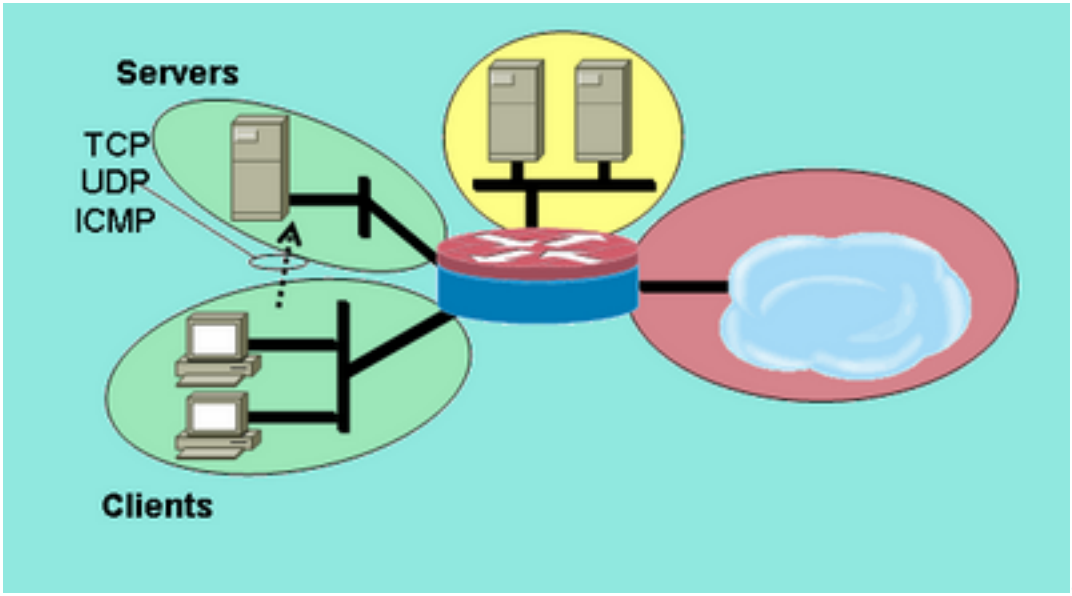
```
configure terminal
 zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
```

يؤدي هذا إلى اكتمال تكوين نهج الفحص المعرف من قبل المستخدم في زوج مناطق الخوادم-العملاء للسماح باتصالات X Windows من منطقة الخادم إلى منطقة العميل.

تكوين نهج العملاء-الخوادم

الشكل 8 يوضح تكوين نهج العميل-الخادم.

الشكل 8: فحص الخدمات من منطقة العملاء إلى منطقة الخوادم



فحص الخدمة من منطقة العملاء إلى منطقة الخوادم

نهج خوادم العميل أقل تعقيدا من السياسات الأخرى. يتم تطبيق فحص الطبقة الرابعة من

منطقة العملاء إلى منطقة الخوادم. وهذا يسمح بالاتصالات من منطقة العملاء إلى منطقة الخوادم ويسمح بحركة المرور العائدة. يحمل فحص الطبقة 4 ميزة البساطة في تكوين جدار الحماية، من حيث أنه يتطلب القليل من القواعد فقط للسماح بمعظم حركة مرور التطبيقات. ومع ذلك، يحمل فحص الطبقة الرابعة أيضا معايير رئيسية:

- عادة ما تتفاوض تطبيقات مثل FTP وأ خدمات الوسائط مع قناة فرعية إضافية من الخادم إلى العميل. عادة ما يتم إستيعاب هذه الوظيفة في إصلاح الخدمة الذي يراقب حوار قناة التحكم ويسمح بالقناة التابعة. ال توفر هذه الإمكانية في فحص الطبقة الرابعة.
- يسمح فحص الطبقة الرابعة بجميع حركات مرور البيانات تقريبا على مستوى التطبيقات. إذا كان يجب التحكم في إستخدام الشبكة حتى يتم السماح ببعض التطبيقات فقط من خلال جدار الحماية، فيجب تكوين قائمة التحكم في الوصول (ACL) على حركة المرور الصادرة للحد من الخدمات المسموح بها عبر جدار الحماية.

تم تكوين كل الواجهات الموجه في مجموعة جسر IEEE، لذلك يطبق نهج جدار الحماية هذا فحص جدار الحماية الشفاف. يتم تطبيق هذا النهج على واجهتين في مجموعة IEEE IP Bridge. ينطبق سياسة التفتيش فقط على حركة المرور التي تعبر مجموعة الجسر. وهذا يفسر سبب تدخل منطقة العملاء والخوادم داخل المنطقة الخاصة.

1. حدد خرائط الفئة التي تصف حركة المرور التي تريد السماح بها بين المناطق، استنادا إلى السياسات الموضحة سابقا:
```
configure terminal
 class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
```
2. قم بتكوين خرائط السياسة لفحص حركة المرور على خرائط الفئة التي قمت بتعريفها للتو:
```
configure terminal
 policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
```
3. قم بتكوين مناطق العملاء والخوادم وتخصيص واجهات الموجه للمناطق الخاصة بها:
```
configure terminal
 zone security clients
 zone security servers
 interface vlan 1
  zone-member security clients
 interface vlan 2
  zone-member security servers
```
4. قم بتكوين زوج المناطق وتطبيق خريطة السياسة المناسب. **ملاحظة**: كما هو موضح سابقا، لفحص الاتصالات التي يتم تكوين زوج مناطق العملاء-الخوادم في الوقت الحالي، والتي يتم عرضها على الحصول على منطقة العملاء التي تنتقل إلى منطقة الخوادم، بعد ذلك:
```
configure terminal
 zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
```
يؤدي هذا إلى اكتمال تكوين سياسة فحص الطبقة الرابعة لزوج مناطق العملاء-الخوادم. ال للسماح بجميع إتصالات TCP و UDP و ICMP من منطقة العميل إلى منطقة الخادم. هذا النهج البسيط يطبق الإصلاح للقنوات الفرعية ولكنه يقدم مثال على النهج البسيط الذي يطبق هذا النهج لاستيعاب معظم إتصالات التطبيقات.

نهج المعدل لجدار حماية السياسات المستند إلى المناطق

تستفيد شبكات البيانات غالبا مع القدرة على الحد من معدل الإرسال لأنواع معينة من حركة مرور الشبكة، والحد من تأثير حركة المرور الأقل أولوية على حركة مرور البيانات الأكثر أهمية للأعمال. يوفر برنامج Cisco IOS هذه الإمكانية مع تنظيم حركة المرور، والتي تحد من معدل حركة مرور تنظيم Cisco IOS software. يدعم برنامج وانفجاراتها. حركة المرور التي يسمح بها الحد من البيانات منذ الإصدار 12.1(5)T من Cisco IOS.

يوفر برنامج Cisco IOS الإصدار 12.4(9)T بزيادة ZFW لتحديد المعدل عندما يتم تكوين إضافة تعمل بين مناطق معينة فئة تطبق على فئات حركة المرور التي تنطبق على مراقبة معينة إمكانية الحد من حركة مرور حركة فصول واحدة يتم تكوين قائمة على معدل حركة المرور. هذا يوفر أخرى إلى ما مناطق الحماية من جدار الحماية ومعينة وتطبيق سياسة جدار الحماية والشرطة التي تستخدم النطاق الترددي العريض التي تختلف ZFW عن المستند إلى الواجهة من حيث أنه يوفر الإجراءات التي تقابلها، والإسقاط لحد التي يتم إرسال السياسة. يتعذر على ZFW تمييز حركة مرور البيانات لـ DSCP.

يمكن لـ ZFW تحديد إستخدام النطاق الترددي بالبايت/الثانية والحزمة/الثانية والنسبة إلى المستند أو بدون مستخدم. يمكن تطبيق ZFW بإستخدام غير مقدمة. النطاق الترددي للنسبة المئوية إلى الواجهة. لذلك، إذا كانت هناك حاجة إلى قدرات إضافية، يمكن تطبيق هذه الميزات إستنادا إلى الواجهة. إذا تم إستخدام المستند إلى الواجهة بالإقتران مع جدار الحماية، فتأكد من عدم تعارض السياسات.

تكوين نهج ZFW

يحدد تنظيم ZFW حركة مرور البيانات في خريطة فئة خريطة السياسة إلى قيمة معدل قابلة للتحديد للمستخدم تتراوح بين 8000 و 2000000000 بت في الثانية، مع قيمة اندفاع قابلة للتكوين في نطاق من 1000 إلى 51200000 بايت.

يتم تكوين تنظيم ZFW من خلال سطر تكوين إضافي في خريطة السياسة، يتم تطبيقه بعد إجراء السياسة:

```
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect
  police rate [bps rate value <8000-2000000000>] burst [value in bytes <1000-512000000>]
```

Session Control

قدمت سياسة ZFW أيضًا التحكم في الجلسة للحد من عدد جلسات العمل لحركة المرور في خريطة الفئة. وهذا يضيف إلى القدرة الحالية لتطبيق نهج خريطة سياسة تنطبق على خريطة الفئة لتوفير حماية رفض الخدمة (DoS) لكل خريطة فئة. وبشكل فعال، يسمح ذلك بالتحكم المتعدد الحبيبات في عدد جلسات العمل التي تنطبق على أي خريطة فئة معينة تعبر زوج المنطقة. إذا تم إستخدام نفس خريطة الفئة على مخططات سياسة متعددة أو أزواج مناطق متعددة، يمكن تطبيق حدود مختلفة للجلسات على تطبيقات خرائط الفئة المختلفة.

يتم تطبيق التحكم في جلسة العمل عند تكوين خريطة معلمة تحتوي على وحدة تخزين جلسة العمل المطلوبة، ثم يتم إلحاق خريطة المعلمة بإجراء الفحص المطبق على خريطة الفئة ضمن خريطة السياسة:

```
parameter-map type inspect my-parameters
 sessions maximum [1-2147483647]

policy-map type inspect private-allowed-policy
 class type inspect http-class
```

```
  inspect my-parameters
```

ال يمكن تطبيق خرائط المعلمات إال على إجراء الفحص وهي غير متوفرة على إجراءات المرور أو الإسقاط.

تكون أنشطة التحكم في جلسة عمل ZFW والتحكم مرئية باستخدام هذا الأمر:

```
show policy-map type inspect zone-pair
```

فحص التطبيق

يوفر فحص التطبيق إمكانية إضافية ل ZFW. يتم تطبيق سياسات فحص التطبيقات على الطبقة 7 من نموذج الاتصال المتبادل بين الأنظمة المفتوحة (OSI)، حيث توفر تطبيقات المستخدم إرسال واستقبال الرسائل التي تسمح للتطبيقات بتوفير إمكانيات مفيدة. يمكن أن توفر بعض التطبيقات قدرات غير مرغوب فيها أو ضعيفة، لذلك يجب تصفية الرسائل المرتبطة بهذه القدرات للحد من الأنشطة على خدمات التطبيقات.

يوفر برنامج Cisco IOS ZFW فحص التطبيقات والتحكم فيها على خدمات التطبيقات التالية:

- HTTP
- SMTP
- POP3
- إيماب
- Sun RPC
- حركة مرور تطبيق P2P
- تطبيقات المراسلة الفورية

يختلف فحص التطبيقات والتحكم فيها (AIC) من حيث القدرة لكل خدمة. يوفر فحص HTTP تصفية دقيقة لعدة أنواع من نشاط التطبيق، كما يوفر إمكانات للحد من حجم النقل وطول أسماء الويب ونشاط المستعرض لفرض التوافق مع معايير سلوك التطبيق والحد من أنواع المحتوى الذي يتم نقله عبر الخدمة. يمكن أن تحد AIC ل SMTP من طول المحتوى وأن تفرض الامتثال للبروتوكول. يمكن أن يساعد فحص POP3 و IMAP على ضمان استخدام المستخدمين آليات مصادقة آمنة لمنع أختراق وسوغات المستخدم.

يتم تكوين فحص التطبيق كمجموعة إضافية من خرائط الفئة الخاصة بالتطبيق وخرائط السياسة، والتي يتم تطبيقها بعد ذلك على خرائط فئة الفحص الحالية وخرائط السياسة عن طريق تحديد سياسة خدمة التطبيق في خريطة سياسة التفتيش.

فحص تطبيق HTTP

يمكن تطبيق فحص التطبيق على حركة مرور HTTP للتحكم في الاستخدام غير المرغوب فيه لمنفذ خدمة HTTP للتطبيقات الأخرى مثل المراسلة الفورية ومشاركة الملفات عبر بروتوكول P2P وتطبيقات إنشاء قنوات الاتصال النفقي التي يمكنها إعادة توجيه التطبيقات التي يتم التحكم فيها بخالف ذلك من خالل TCP 80.

قم بتكوين خريطة فئة فحص التطبيق لوصف حركة المرور التي تنتهك حركة مرور HTTP المسموح بها:

```
! configure the actions that are not permitted
class-map type inspect http match-any http-aic-cmap
```

```
 match request port-misuse any
 match req-resp protocol-violation
! define actions to be applied to unwanted traffic
policy-map type inspect http http-aic-pmap
 class type insp http http-aic-cmap
  reset
  log
! define class-map for stateful http inspection
class-map type inspect match-any http-cmap
 match protocol http
! define class-map for stateful inspection for other traffic
class-map type inspect match-any other-traffic-cmap
 match protocol smtp
 match protocol dns
 match protocol ftp
! define policy-map, associate class-maps and actions
policy-map type inspect priv-pub-pmap
 class type inspect http-cmap
  inspect
  service-policy http http-aic-pmap
 class type inspect other-traffic-cmap
  inspect
```

تحسينات فحص تطبيق HTTP

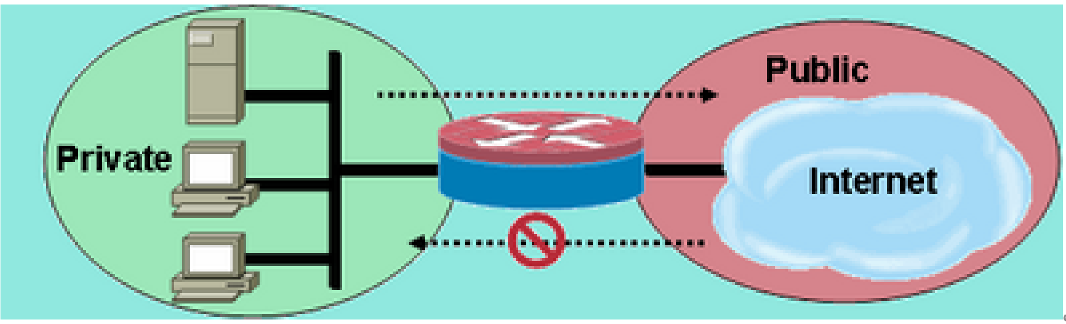
يقدم برنامج Cisco IOS الإصدار 12.4(9)T تحسينات على إمكانيات فحص HTTP ل ZFW. جدار حماية Cisco IOS الذي يقدم فحص تطبيق HTTP في البرنامج Cisco IOS Software، الإصدار 12.3(14)T. يعمل برنامج IOS الإصدار 12.4(9)T من Cisco على زيادة الإمكانات الحالية عند إضافة:

- القدرة على السماح بالطلبات والاستجابات ورفض ومراقبتها استنادا إلى اسم الرأس وقيم الرأس. يفيد ذلك في حظر الطلبات والاستجابات التي تحمل حقول رؤوس مضيفة.
- تعد إمكانية تحديد أحجام العناصر المختلفة في طلب HTTP ورؤوس الاستجابة مثل الحد الأقصى لطول URL، الحد الأقصى لطول الرأس، الحد الأقصى لعدد الرؤوس، الحد الأقصى لطول سطر الرأس، وما إلى ذلك مفيدة لمنع تجاوز سعة التخزين المؤقت.
- إمكانية حظر الطلبات والاستجابات التي تحمل رؤوس متعددة من نفس النوع، على سبيل المثال، طلب برأسين بطول المحتوى.
- إمكانية حظر الطلبات والاستجابات باستخدام رؤوس غير ASCII. وهذا مفيد لمنع الهجمات المختلفة التي تستخدم الحروف الثنائية وغيرها من الحروف غير ASCII لتقديم الديدان والمحتويات الضارة الأخرى إلى خوادم الويب.
- توفر القدرة على تجميع أساليب HTTP في فئات محددة من قبل المستخدم والمرونة لحظر/السماح/المراقبة لكل مجموعة. يسمح ال HTTP rfc مجموعة مقيد من طريقة HTTP. تتعتبر بعض الطرق القياسية غير آمنة لأنه يمكن إستخدامها لاستغلال نقاط الضعف على خادم ويب. العديد من الطرق غير القياسية لها سجل أمان سيئ.
- أسلوب حظر URIs معينة استنادا إلى تعبير عادي تم تكوينه من قبل المستخدم. تتيح هذه الميزة للمستخدم إمكانية حظر URI والاستعلامات المخصصة.
- القدرة على وصف أنواع الرؤوس (خاصة عن رأس الخادم) بسلسلة قابلة للتخصيص من قبل المستخدم. ويكون هذا مفيدا في حالة ما إذا قام المهاجم بتحليل استجابات خادم الويب ومعرفة أكبر قدر ممكن من المعلومات، ثم شن هجوم يستغل نقاط الضعف في خادم الويب هذا على وجه التحديد.
- القدرة على حظر تنبيهه وأ إصداره على اتصال HTTP إذا كانت قيمة معلمة HTTP وأحدة أو أكثر مطابقة للقيم التي أدخلها المستخدم كتعبير عادي. تتضمن بعض سياقات قيمة HTTP المحتملة الرأس، المتن، اسم المستخدم، كلمة المرور، وكيل المستخدم،

سطر الطلب، سطر الحالة، ومتغيرات CGI التي تم فك ترميزها.

تفترض أمثلة التكوين لتحسينات فحص تطبيق HTTP وجود شبكة بسيطة، كما هو موضح في الشكل 9.

الشكل 9: فحص التطبيق يفترض وجود شبكة بسيطة



يفترض فحص التطبيق وجود شبكة بسيطة

يقوم جدار الحماية بتجميع حركة المرور في فئتين:

- حركة مرور HTTP
- جميع حركات مرور TCP الأحادية القناة الأخرى و UDP و ICMP

يتم فصل HTTP للسماح بإجراء فحص محدد على حركة مرور الويب. وهذا يسمح لك بتكوين تنظيم في القسم الأول من هذا المستند، وفحص تطبيق HTTP في القسم الثاني. يمكنك تكوين خرائط فئة معينة وخرائط سياسة لحركة مرور P2P و IM في القسم الثالث من هذا المستند. الاتصال مسموح به من المنطقة الخاصة إلى المنطقة العامة. لم يتم توفير أي اتصال من المنطقة العامة إلى المنطقة الخاصة.

راجع الملحق (ج) للحصول على تكوين كامل يطبق السياسة الأولية.

تكوين تحسينات فحص تطبيق HTTP

يتطلب فحص تطبيق HTTP (بالإضافة إلى سياسات فحص التطبيقات الأخرى) تكوينا أكثر تعقيدا من تكوين الطبقة 4 الأساسي. يجب تكوين تصنيف حركة مرور الطبقة 7 والسياسة للتعرف على حركة مرور معينة ترغب في التحكم فيها، وتطبيق الإجراء المطلوب على حركة المرور المرغوب فيها وغير المرغوب فيها.

يمكن تطبيق فحص تطبيق HTTP (المماثل لأنواع أخرى من فحص التطبيق) فقط على حركة مرور HTTP. وبالتالي، يجب عليك تحديد خرائط الطبقة 7 وخرائط السياسة لحركة مرور HTTP معينة، ثم تحديد خريطة الطبقة 4 الخاصة ب HTTP تحديدا، وتطبيق سياسة الطبقة 7 على فحص HTTP في خريطة سياسة الطبقة 4، على سبيل المثال:

```
!configure the layer-7 traffic characteristics:
class-map type inspect http match-any http-l7-cmap
 match  req-resp protocol-violation
 match  request body length gt 4096
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect http http-l7-pmap
 class type inspect http http-l7-cmap
  reset
  log
!
!define the layer-4 inspection policy
```

```
class-map type inspect match-all http-l4-cmap
 match protocol http
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect http-l4-cmap
  inspect
  service-policy http http-l7-pmap
```

يتم تحديد جميع خصائص حركة مرور فحص تطبيق HTTP هذه في خريطة الطبقة 7:

- يوفر أمر فحص الرأس إمكانية السماح/الرفض/المراقبة للطلبات أو الاستجابات التي تطابق رأسها مع التعبير العادي الذي تم تكوينه. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو استجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  `APPFW-6-HTTP_HDR_REGEX_MATCHED`
  إستخدام الأمر:

```
match {request|response|req-resp} header regex <parameter-map-name>
```

نموذج حالة إستخدام

- قم بتكوين HTTP APPFW لحظر الطلب أو الاستجابة التي يحتوي رأسها على أحرف غير ASCII.

```
parameter-map type regex non_ascii_regex
   pattern "[^\x00-\x80]"
class-map type inspect http non_ascii_cm
   match req-resp header regex non_ascii_regex
policy-map type inspect http non_ascii_pm
   class type inspect http non_ascii_cm
      reset
```

فحص طول الرأس — يتحقق هذا الأمر من طول رأس الطلب أو الاستجابة ويطبق إجراء إذا تجاوز الطول الحد الذي تم تكوينه. الإجراء مسموح به أو إعادة تعيينه. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-4- HTTP_HEADER_LENGTH
```

إستخدام الأمر:

```
match {request|response|req-resp} header length gt <bytes>
```

نموذج حالة إستخدام

قم بتكوين HTTP APPFW لحظر الطلبات والاستجابات التي يزيد طول الرأس فيها عن 4096 بايت.

```
class-map type inspect http hdr_len_cm
   match req-resp header length gt 4096

policy-map type inspect http hdr_len_pm
   class type inspect http hdr_len_cm
      reset
```

فحص عدد الرؤوس — يتحقق هذا الأمر من عدد خطوط الرؤوس (الحقول) في طلب/إستجابة

ويطبق الإجراء عندما يتجاوز العدد الحد الذي تم تكوينه. الإجراء مسموح به وأ وإعادة تعيينه. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_HEADER_COUNT
```

إستخدام الأمر:

```
match {request|response|req-resp} header count gt <number>
```

نموذج حالة إستخدام

قم بتكوين نهج تطبيق http لحظر طلب يحتوي على أكثر من 16 حقل رأس.

```
class-map type inspect http hdr_cnt_cm
   match request header count gt 16

policy-map type inspect http hdr_cnt_pm
   class type inspect http hdr_cnt_cm
      reset
```

فحص حقل الرأس — يوفر هذه الأمر إمكانية السماح/الرفض/المراقبة/الطلبات/الاستجابات التي تحتوي على حقل رأس HTTP وقيمة محددين. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_HDR_FIELD_REGEX_MATCHED
```

إستخدام الأمر:

```
match {request|response|req-resp} header <header-name>
```

نموذج حالة إستخدام

تكوين نهج فحص تطبيق HTTP لحظر برامج التجسس/البرامج الدعائية:

```
parameter-map type regex ref_regex
   pattern “\.delfinproject\.com”
   pattern “\.looksmart\.com”

parameter-map type regex host_regex
   pattern “secure\.keenvalue\.com”
   pattern “\.looksmart\.com”

parameter-map type regex usragnt_regex
   pattern “Peer Points Manager”

class-map type inspect http spy_adwr_cm
   match request header refer regex ref_regex
   match request header host regex host_regex
   match request header user-agent regex usragnt_regex

policy-map type inspect http spy_adwr_pm
   class type inspect http spy_adwr_cm
      reset
```

فحص طول حقل الرأس — يوفر هذه الأمر إمكانية تحديد طول سطر حقل الرأس. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين

الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_HDR_FIELD_LENGTH
```

إستخدام الأمر:

```
match {request|response|req-resp} header <header-name> length gt <bytes>
```

نموذج حالة إستخدام

قم بتكوين نهج تطبيق http لحظر طلب يتجاوز طول حقل ملف تعريف الارتباط الخاص به 128 و 256 مستخدم ووكيل التالي.

```
class-map type inspect http hdrline_len_cm
   match request header cookie length gt 256
   match request header user-agnet length gt 128

policy-map type inspect http hdrline_len_pm
   class type inspect http hdrline_len_cm
      reset
```

فحص تكرار حقل الرأس — يتحقق هذا الأمر مما إذا كان الطلب أو الاستجابة لها لها حقول رأس متكررة. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. عند تمكين هذا الخيار، تتسبب إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_REPEATED_HDR_FIELDS
```

إستخدام الأمر:

```
match {request|response|req-resp} header <header-name>
```

نموذج حالة إستخدام

قم بتكوين نهج تطبيق http لحظر طلب أو إستجابة لها بدون رأس متعددة لطول المحتوى. هذا واحد من أفضل الظروف التي يمنع جلسة تهريب .

```
class-map type inspect http multi_occrns_cm
   match req-resp header content-length count gt 1

policy-map type inspect http multi_occrns_pm
   class type inspect http multi_occrns_cm
      reset
```

- فحص الطريقة — ال HTTP RFC مجموعة محظورة من أساليب HTTP. ومع ذلك، حتى بعض الأساليب القياسية تعتبر غير آمنة حيث يمكن إستخدام بعض الأساليب القياسية من الطرق غير القياسية للتغلب على خادم الويب. يستخدم العديد من الطرق غير القياسية بشكل متكرر للنشاط الضار. وهذا يتطلب الحاجة إلى تجميع الأساليب في فئات مختلفة وجعل المستخدم يختار الإجراء لكل فئة. يوفر هذه الأمر للمستخدم طريقة مرنة لتجميع الطرق إلى فئات مختلفة مثل الطرق الآمنة والطرق غير الآمنة أو أساليب RFC وأساليب WebDAV. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6-HTTP_METHOD
```

إستخدام الأمر:

```
match request method <method>
```

نموذج حالة إستخدام

قم بتكوين نهج HTTP appfw الذي يقوم بتجميع أساليب HTTP في ثلاث فئات: آمنة وغير آمنة و webDAV. وترد هذه في الجدول التالي. تكوين الإجراءات التي:

- كافة الطرق الآمنة مسموح بها بدون سجل
- كافة الأساليب غير الآمنة مسموح بها مع السجل
- تم حظر كافة طرق WebDAV باستخدام السجل.

آمن	غير آمن	WebDAV
احصل، رأس، خيار	نشر، وضع، اتصال، تتبع	نسخ، حذف، تحريك

```
http policy:

class-map type inspect http safe_methods_cm
   match request method get
   match request method head
   match request method option

class-map type inspect http unsafe_methods_cm
   match request method post
   match request method put
   match request method connect
   match request method trace

class-map type inspect http webdav_methods_cm
   match request method bcopy
   match request method bdelete
   match request method bmove

policy-map type inspect http methods_pm
   class type inspect http safe_methods_cm
      allow
   class type inspect http unsafe_methods_cm
      allow log
      class type inspect http webdav_methods_cm
      reset log
```

فحص URI—يوفر هذا الأمر القدرة على السماح/الرفض/المراقبة للطلبات التي يتطابق URI معها مع تكوين فحص منتظم. يتيح هذا للمستخدم إمكانية حظر عناوين URL المخصصة والاستعلامات. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_URI_REGEX_MATCHED
```

إستخدام الأمر:

```
match request uri regex <parameter-map-name>
```

نموذج حالة إستخدام

قم بتكوين نهج ملحق http لحظر طلب يطابق URI الخاص به أي من التعبيرات العادية

التالية:

- .*cmd.exe
- .*الجنس
- .*المقامرة

```
parameter-map type regex uri_regex_cm
   pattern “.*cmd.exe”
   pattern “.*sex”
   pattern “.*gambling”

class-map type inspect http uri_check_cm
   match request uri regex uri_regex_cm

policy-map type inspect http uri_check_pm
   class type inspect http uri_check_cm
      reset
```

- فحص طول URI — يتحقق هذا الأمر من طول URI الذي يتم إرساله في طلب ويطبق الإجراء الذي تم تكوينه عندما يتجاوز الطول الحد الذي تم تكوينه. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة.
  تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  APPFW-6- HTTP_URI_LENGTH
  إستخدام الأمر:
  match request uri length gt <bytes>
  نموذج حالة إستخدام

قم بتكوين نهج HTTP APPFW لرفع تنبيه كلما تجاوز طول URI للطلب ما 3076 بايت.

```
class-map type inspect http uri_len_cm
   match request uri length gt 3076

policy-map type inspect http uri_len_pm
   class type inspect http uri_len_cm
      log
```

فحص الوسيطة — يوفر هذا الأمر القدرة على السماح بالطلب أو رفضه أو مراقبته الذي تتطابق وسائطه (المعلمات) مع الفحص المنتظم الذي تم تكوينه. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6- HTTP_ARG_REGEX_MATCHED
```

إستخدام الأمر:

```
match request arg regex <parameter-map-name>
```

قم بتكوين نهج HTTP لحظر الطلب تتطابق وسيطاته مع أي من التعبيرات العادية التالية:

- .*رفش
- .*موجه

```
parameter-map type regex arg_regex_cm
   pattern “.*codered”
   pattern “.*attack”
```

```
class-map type inspect http arg_check_cm
   match request arg regex arg_regex_cm

policy-map type inspect http arg_check_pm
   class type inspect http arg_check_cm
      reset
```

- فحص طول الوسيطة — يتحقق هذا الأمر من طول الوسيطات التي يتم إرسالها في طلب ويطبق الإجراء الذي تم تكوينه عندما يتجاوز الطول الحد الذي تم تكوينه. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  `APPFW-6- HTTP_ARG_LENGTH`
  إستخدام الأمر:
  `match request arg length gt <bytes>`
  نموذج حالة إستخدام

قم بتكوين نهج HTTP APPFW لرفع تنبيه كلما تجاوز طول الوسيطة لطلب ما 512 بايت.

```
class-map type inspect http arg_len_cm
   match request arg length gt 512

policy-map type inspect http arg_len_pm
   class type inspect http arg_len_cm
      log
```

- فحص النص الأساسي — تسمح واجهة سطر الأوامر (CLI) هذه للمستخدم بتحديد قائمة التعبيرات العادية ليتم مطابقتها مع نص الطلب أو الاستجابة. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة.
  تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  `APPFW-6- HTTP_BODY_REGEX_MATCHED`
  إستخدام الأمر:
  `match {request|response|reg-resp} body regex <parameter-map-name>`
  نموذج حالة إستخدام

قم بتكوين HTTP appfw لحظر إستجابة تحتوي على النمط `.*[AA][TT][TT][CC][KK]`.

```
parameter-map type regex body_regex
   pattern ".*[Aa][Tt][Tt][Aa][Cc][Kk]"

class-map type inspect http body_match_cm
   match response body regex body_regex

policy-map type inspect http body_match_pm
   class type inspect http body_match_cm
      reset
```

فحص طول النص (المحتوى) — يتحقق هذا الأمر من حجم الرسالة التي يتم إرسالها من خلال إستجابة أو الطلب. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-4- HTTP_CONTENT_LENGTH
```

إستخدام الأمر:

```
match {request|response|req-resp} body length lt <bytes> gt <bytes>
```

نموذج حالة إستخدام

قم بتكوين نهج HTTP appfw لحظر جلسة عمل HTTP تحمل أكثر من 10 آلاف بايت في الطلب أو الاستجابة.

```
class-map type inspect http cont_len_cm
   match req-resp header content-length gt 10240

policy-map type inspect http cont_len_pm
   class type inspect http cont_len_cm
      reset
```

فحص سطر الحالة — يسمح الأمر للمستخدم بتعيين قائمة من التعبيرات العادية "إعادة التعيين" أو "السماح" لتطابقها مع سطر الحالة الاستجابة. يمكن تطبيق إجراء السماح أو إعادة التعيين على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:

```
APPFW-6-HTTP_STLINE_REGEX_MATCHED
```

إستخدام الأمر:

```
match response status-line regex <class-map-name>
```

نموذج حالة إستخدام

قم بتكوين تطبيق http لتسجيل تنبيه كلما تم إجراء محاولة للوصول إلى صفحة محظورة. تحتوي الصفحة المحظورة عادة على رمز حالة رقم 403، وبدي و سطر الحالة مثل HTTP/1.0 403 \r\n.

```
parameter-map type regex status_line_regex
   pattern “[Hh][Tt][Tt][Pp][/][0-9][.][0-9][ \t]+403”

class-map type inspect http status_line_cm
   match response status-line regex status_line_regex

policy-map type inspect http status_line_pm
   class type inspect http status_line_cm
      log
```

- فحص نوع المحتوى — يتحقق هذا الأمر مما إذا كان نوع محتوى رأس الرسالة موجودا في قائمة أنواع المحتويات المدعومة. كما يتحقق من تطابق نوع محتوى الرأس مع محتوى بيانات الرسالة أو عجز متن الكيان. إذا تم تكوين عدم تطابق الكلمة الأساسية، يتحقق الأمر من نوع محتوى رسالة الاستجابة مقابل قيمة حقل رسالة الطلب المقبولة. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog المناسبة:

  ```
  APPFW-4- HTTP_CONT_TYPE_VIOLATION
  APPFW-4- HTTP_CONT_TYPE_MISMATCH
  APPFW-4- HTTP_CONT_TYPE_UNKNOWN
  ```

  إستخدام الأمر:

  ```
  match {request|response|req-resp} header content-type [mismatch|unknown|violation]
  ```

  نموذج حالة إستخدام قم بتكوين نهج HTTP appFW لحظر جلسة عمل HTTP تحمل الطلبات والاستجابات التي تحتوي على نوع محتوى غير معروف.

  ```
  class-map type inspect http cont_type_cm
     match req-resp header content-type unknown

  policy-map type inspect http cont_type_pm
     class type inspect http cont_type_cm
        reset
  ```

فحص إساءة إستخدام المنفذ — يمكن إستخدام هذا الأمر لمنع إساءة إستخدام منفذ HTTP لمثل IM، P2P، Tunneling، وما إلى ذلك على إجراء السماح أو إعادة للتطبيقات الأخرى (80) الضبط على طلب أو إستجابة تطابق معايير خريطة الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog المنسابة:

```
APPFW-4- HTTP_PORT_MISUSE_TYPE_IM
APPFW-4-HTTP_PORT_MISUSE_TYPE_P2P
APPFW-4-HTTP_PORT_MISUSE_TYPE_TUNNEL
```

إستخدام الأمر:

```
match request port-misuse {im|p2p|tunneling|any}
```

نموذج حالة إستخدام

قم بتكوين نهج تطبيق http لحظر جلسة عمل http يساء إستخدامها لتطبيق المراسلة الفورية.

```
class-map type inspect http port_misuse_cm
   match request port-misuse im

policy-map type inspect http port_misuse_pm
   class type inspect http port_misuse_cm
      reset
```

- فحص HTTP المقيد — يتيح هذا الأمر التحقق المقيد من توافق البروتوكول مقابل طلبات HTTP واستجاباته. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  ```
  APPFW-4- HTTP_PROTOCOL_VIOLATION
  ```
  إستخدام الأمر:
  ```
  match req-resp protocol-violation
  ```
  نموذج حالة إستخدام قم بتكوين سياسة تطبيق HTTP لحظر الطلبات أو الاستجابات التي تخالف RFC 2616:
  ```
  class-map type inspect http proto-viol_cm
     match req-resp protocol-violation

  policy-map type inspect http proto-viol_pm
     class type inspect http proto-viol_cm
        reset
  ```
- Transfer- Encoding Inspection — يوفر هذا الأمر إمكانية السماح بالطلب/الاستجابة التي تطابق نوع ترميز النقل الخاص بها مع النوع الذي تم تكوينه وأرفضها أو مراقبتها. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
  ```
  APPFW-6- HTTP_TRANSFER_ENCODING
  ```
  إستخدام الأمر:
  ```
  match {request|response|req-resp} header transfer-encoding
  {regex <parameter-map-name> |gzip|deflate|chunked|identity|all}
  ```
  نموذج حالة إستخدام قم بتكوين نهج HTTP appFW لحظر طلب أو إستجابة تحتوي على تشفير نوع الضغط.
  ```
  class-map type inspect http trans_encoding_cm
     match req-resp header transfer-encoding type compress

  policy-map type inspect http trans_encoding_pm
     class type inspect http trans_encoding_cm
        reset
  ```

- فحص تطبيق Java — يتحقق هذا الأمر مما إذا كانت إستجابة ما تحتوي على تطبيق Java ويطبق الإجراء الذي تم تكوينه عند اكتشاف التطبيق الصغير. يمكن تطبيق إجراء "السماح" أو "إعادة التعيين" على طلب أو إستجابة تطابق معايير تعيين الفئة. تتسبب إضافة إجراء السجل في ظهور رسالة syslog:
```
APPFW-4- HTTP_JAVA_APPLET
```
إستخدام الأمر:
```
match response body java-applet
```
نموذج حالة إستخدام مقدم بتكوين نهج HTTP appFW لحظر تطبيقات جافا الصغيرة.
```
class-map type inspect http java_applet_cm
   match response body java-applet

policy-map type inspect http java_applet_pm
   class type inspect http java_applet_cm
      reset
```

دعم ZFW للمراسلة الفورية والتحكم في تطبيق نظير إلى نظير

قدم برنامج IOS الإصدار 12.4(9)T دعم ZFW لتطبيقات IM و P2P من Cisco.

قدم برنامج Cisco IOS أولا دعم التحكم في تطبيق IM في برنامج Cisco IOS الإصدار 12.4(4)T. لم يدعم الإصدار الأول من ZFW تطبيق المراسلة الفورية في واجهة ZFW. إذا كان التحكم في تطبيق المراسلة الفورية مطلوبا، تعذر على المستخدمين الترحيل إلى واجهة ZFW. يقدم برنامج IOS الإصدار 12.4(9)T من Cisco دعم ZFW لفحص IM، الذي يدعم Yahoo! Messenger (YM) و MSN Messenger (MSN) و AOL Instant Messenger (AIM). برنامج Cisco IOS الإصدار 12.4(9)T هو الإصدار الأول من برنامج Cisco IOS الذي يوفر دعم جدار حماية Cisco IOS الأصلي لتطبيقات مشاركة الملفات P2P.

يوفر كل من فحص IM و P2P سياسات الطبقة 4 والطبقة 7 لحركة مرور التطبيقات. وهذا يعني أنه يمكن لـ ZFW توفير الفحص الأساسي الذي يحدد الحالة للسماح بحركة المرور أو رفضها، بالإضافة إلى التحكم متعدد المستويات في أنشطة معينة في الطبقة 7 من البروتوكولات المتعددة، بحيث يتم السماح ببعض أنشطة التطبيق بينما يتم رفض أنشطة أخرى.

فحص تطبيق P2P والتحكم فيه

قام SDM 2.2 بإدخال التحكم في تطبيق P2P في قسم تكوين جدار الحماية الخاص به. قام SDM بتطبيق سياسة "التعرف على التطبيقات المستندة إلى الشبكة (NBAR)" و"جودة الخدمة" للكشف عن نشاط تطبيق P2P والتحكم فيه لدعم سطر أوامر حركة مرور P2P. أثار هذا المشكلة أن CLI مستعمل، أن يتوقع عدم دعم P2P في ال cisco ios جدار حماية CLI، كان يعجز أن يكشف P2P يدقيق منع في ال CLI ما لم يكن NBAR/QoS ليكشف. يقدم برنامج Cisco IOS الإصدار 12.4(9)T التحكم الأصلي في P2P في واجهة سطر الأوامر (CLI) من ZFW، للاستفادة من NBAR لاكتشاف نشاط تطبيق P2P. يدعم إصدار البرنامج هذا العديد من بروتوكولات تطبيق P2P:

- بت تورنت
- إيدونكي
- خدمة FastTrack
- غنوتيلا
- KaZaA / KaZaA2
- WinMx

من الصعب بعض الشيء اكتشاف تطبيقات P2P، وذلك نتيجة لسلوك "تخطي المنفذ"

والحيل الأخرى لتجنب الكشف، بالإضافة إلى المشاكل التي تنشأ عن التغييرات المتكررة والتحديثات لتطبيقات P2P التي تعمل على تعديل سلوك البروتوكولات. يجمع ZFW بين فحص حالة جدار الحماية الأصلي مع إمكانيات التعرف على حركة مرور البيانات ل NBAR لتوفير التحكم في تطبيق P2P في واجهة تكوين CPL الخاصة ب ZFW. توفر تقنية NBAR ميزتين رائعتين:

- التعرف الاختياري على التطبيقات القائمة على إرشادية للتعرف على التطبيقات بالرغم من السلوك المعقد الذي يصعب اكتشافه
- بنية أساسية قابلة للتوسيع توفر آلية تحديث للظل على دراية بتحديثات البروتوكول والتعديلات

تكوين فحص P2P

وكما تمت الإشارة إليه سابقا، يوفر الفحص والتحكم في بروتوكول P2P الفحص المعبر عن الحالة من الطبقة الرابعة والتحكم في التطبيقات من الطبقة 7. يتم تكوين فحص الطبقة 4 بشكل مشابه لخدمات التطبيقات الأخرى، إذا كان فحص منافذ خدمة التطبيق الأصلية كافيا:

```
class-map type inspect match-any my-p2p-class
match protocol [bittorrent | edonkey | fasttrack | gnutella | kazaa | kazaa2 | winmx ]
[signature (optional)]
!
policy-map type inspect private-allowed-policy
 class type inspect my-p2p-class
  [drop | inspect | pass]
```

لاحظ خيار التوقيع الإضافي في بروتوكول المطابقة [service-name]. عندما تتم إضافة خيار التوقيع في بيان بروتوكول المطابقة، يتم تطبيق استعلامات NBAR على حركة المرور للبحث عن بيانات teltele في حركة المرور التي تشير إلى نشاط تطبيق P2P معين. ويتضمن ذلك تخطي المنفذ وتغييرات أخرى في سلوك التطبيق لتجنب اكتشاف حركة مرور البيانات. يأتي هذا المستوى من فحص حركة المرور مقابل زيادة استخدام وحدة المعالجة المركزية (CPU) وتقليل إمكانية الخرج للشبكة. إذا لم يتم تطبيق خيار التوقيع، لا يتم تطبيق التحليل الاستخباراتي المستند إلى NBAR لاكتشاف سلوك تخطي المنفذ، واستخدام وحدة المعالجة المركزية (CPU) لا يتأثر بنفس المدى.

يحمل فحص الخدمة الأصلية العيب في أنه غير قادر على الحفاظ على التحكم في تطبيقات P2P في حالة "انتقال" التطبيق إلى منفذ مصدر ووجهة غير قياسي، أو إذا تم تحديث التطبيق لبدء الإجراء الخاص به على رقم منفذ غير معروف:

التطبيق	المنافذ الأصلية (كما هو متعرف عليه من قبل قائمة PAM الخاصة بالطراز 12.4(15)T)
بت تورنت	بروتوكول TCP 6881-6889
إدونكي	بروتوكول TCP رقم 4662
مسار سريع	بروتوكول TCP 1214
غنوتيلا	بروتوكول TCP 6346-6349 TCP 6355،5634 UDP 6346-6348
كازا 2	يعتمد على PAM
وينمكس	بروتوكول TCP 6699

إذا كنت ترغب في السماح بحركة مرور بيانات P2P (الفحص)، فيمكنك الحاجة إلى توفير تكوين إضافي. يمكن أن تستخدم بعض التطبيقات شبكات P2P متعددة أو تنفذ سلوكيات معينة قد تحتاج إلى إيوائها في تكوين جدار الحماية للسماح للتطبيق بالعمل:

- عادة ما يتصل عملاء BitTorrent ب "tracker" (خوادم دليل النظير) عبر HTTP التي تعمل على منفذ غير قياسي. هذا خاص بشكل TCP 6969، غير أن أنت يستطيع تحتاج أن

يفحص الو تنرت صاخ tracker ءانيم. إذا كنت ترغب في السماح ب BitTorrent، فإن أفضل طريقة لاستيعاب المنفذ الإضافي هي تكوين HTTP كأحد بروتوكوالت المطابقة وإضافة TCP 6969 إلى HTTP باستخدام الأمر ip port-map:

```
ip port-map http port tcp 6969
```

يجب تعريف http و bitBurst كمعايير مطابقة مطبقة في خريطة الفئة.

- يبدو أن eDonkey يبدأ االتصاالت التي يتم الكشف عنها على أنها كل من eDonkey و Gnutella.
- يعتمد فحص KaZaA تماما على كشف توقيع NBAR.

يزيد فحص الطبقة 7 (التطبيق) من المستوى 4 مع إمكانية التعرف على اإلجراءات الخاصة بالخدمة وتطبيقاتها، على سبيل المثال حظر أو السماح بالبحث في الملفات ونقل الملفات وإمكانات المحادثة النصية بشكل انتقائي. تختلف إمكانات الخدمة المحددة حسب الخدمة.

يشبه فحص تطبيق P2P فحص تطبيق HTTP:

```
!configure the layer-7 traffic characteristics:
class-map type inspect [p2p protocol] match-any p2p-l7-cmap
 match action
!
!configure the action to be applied to the traffic
!matching the specific characteristics:
policy-map type inspect [p2p protocol] p2p-l7-pmap
 class type inspect p2p p2p-l7-cmap
  [ reset | allow ]
  log
!
!define the layer-4 inspection policy
class-map type inspect match-all p2p-l4-cmap
 match protocol [p2p protocol]
!
!associate layer-4 class and layer-7 policy-map
!in the layer-4 policy-map:
policy-map type inspect private-allowed-policy
 class type inspect p2p-l4-cmap
  [ inspect | drop | pass ]
  service-policy p2p p2p-l7-pmap
```

يوفر فحص تطبيقات P2P إمكانات خاصة بالتطبيق لمجموعة فرعية من التطبيقات المدعومة بواسطة فحص الطبقة الرابعة:

- إدونكي
- رسائل فورية
- الينوتغ
- كازا 2

يوفر لك تطبيق من هذه التطبيقات خيارات متغيرة خاصة بالتطبيق لمعايير التوافق:

إدونكي

```
router(config)#class-map type inspect edonkey match-any edonkey-l7-cmap
router(config-cmap)#match ?
  file-transfer     Match file transfer stream
  flow              Flow based QoS parameters
  search-file-name  Match file name
  text-chat         Match text-chat
```

رسائل فورية

```
router(config)#class-map type inspect fasttrack match-any ftrak-l7-cmap
router(config-cmap)#match ?
  file-transfer  File transfer stream
  flow           Flow based QoS parameters
```

اليتونغ

```
router(config)#class-map type inspect gnutella match-any gtella-l7-cmap
router(config-cmap)#
```

ازاك 2

```
router(config)#class-map type inspect kazaa2 match-any kazaa2-l7-cmap
router(config-cmap)#match ?
  file-transfer  Match file transfer stream
  flow           Flow based QoS parameters
```

يمكن تحميل تعريفات بروتوكول P2P الجديدة أو التحديثات لبروتوكولات P2P الحالية بواسطة تحديث فئات PDLM الديناميكية ل NBAR. هذا هو أمر التكوين لتحميل PDLM الجديد:

```
ip nbar pdlm <file-location>
```

يتوفر البروتوكول الجديد في أوامر البروتوكول المطابقة لتفتيش نوع الفئة. إذا كان بروتوكول P2P الجديد يحتوي على خدمات (بروتوكولات فرعية)، فإن أنواع خريطة الفئة التي يتم فحصها من الطبقة 7 الجديدة، بالإضافة إلى معايير مطابقة الطبقة 7، تصبح متوفرة.

فحص تطبيق المراسلة الفورية والتحكم فيه

برنامج IOS الإصدار 12.4(4)T من Cisco، تم إدخال فحص تطبيق المراسلة الفورية والتحكم فيه. لم يتم إدخال دعم IM مع ZFW في 12.4(6)T، لذلك لم يتمكن المستخدمون من تطبيق التحكم في IM و ZFW في نفس جهاز جدار الحماية، نظرا لأنه لا يمكن أن توجد ميزات ZFW وجدار الحماية القديم معا على واجهة معينة.

يدعم برنامج Cisco IOS الإصدار 12.4(9)T الفحص حسب الحالة والتحكم في التطبيق لخدمات IM هذه:

- AOL المراسلة الفورية
- MSN Messenger
- ياهو! مسنجر

يختلف فحص التراسل الفوري بشكل طفيف عن معظم الخدمات، حيث يتحكم فحص التراسل الفوري في الوصول إلى مجموعة معينة من الأجهزة المضيفة لكل خدمة معينة. تعتمد خدمات المراسلة الفورية بشكل عام على مجموعة دائمة نسبيا من خوادم الدليل، والتي يجب أن يتمكن العملاء من الاتصال بها للوصول إلى خدمة المراسلة الفورية. لم يتم تطبيقات المراسلة الفورية إلى أن تكون صعبة جدا للتحكم من وجهة نظر البروتوكول أو الخدمة. الطريقة الأكثر فعالية للتحكم في هذه التطبيقات هي الحد من الوصول إلى خوادم المراسلة الفورية الثابتة.

تكوين فحص المراسلة الفورية

يوفر الفحص والتحكم في المراسلة الفورية فحص الحالة من الطبقة الرابعة

والتحكم في التطبيقات من المستوى 7.

يتم تكوين فحص الطبقة الرابعة بشكل مشابه لخدمات التطبيقات الأخرى:

```
class-map type inspect match-any my-im-class
match protocol [aol | msnmsgr | ymsgr ]
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  [drop | inspect | pass
```

يمكن لتطبيقات المراسلة الفورية الاتصال بخوادم على منافذ متعددة للحفاظ على وظائف. للسماح بخدمة IM معينة عم إجراء الفحص، ال يمكنك الحاجة إلى قائمة خوادم IM. وعم ذلك، عند تكوين خريطة فئة تحدد خدمة IM التي تريد الوصول المسموح بها إلى خوادم خدمة IM، مثل AOL Instant Messenger، وتطبيق إجراء السياسة الخريطة في طاقم عمل IM معينة، حيث يمكن أن تتسبب في قيام عميل IM بمحاولة تحديد موقع منفذ مختلف المقترنة يمكن أن يتم السماح بالاتصال بالإنترنت. إذا كنت ال ترغب في السماح بالاتصال بخدمة معينة، أو يتم السماح بالاتصال بالإنترنت. إذا كنت ترغب في تقييد إمكانية خدمة IM للدردشة النصية، فيجب عليك تحديد قائمة IM المقترنة بتطبيق خوادم التي يمكن ZFW من تحديد حركة مرور البيانات:

```
!configure the server-list parameter-map:
parameter-map type protocol-info <name>
  server name <name>
  server ip a.b.c.d
  server ip range a.b.c.d a.b.c.d
```

على سبيل المثال، يتم تعريف قائمة خوادم Yahoo IM على هذه النحو:

```
parameter-map type protocol-info ymsgr-pmap
  server name scs.msg.yahoo.com
  server name scsd.msg.yahoo.com
  server ip 10.0.77.88
  server ip range 172.16.0.77 172.16.0.99
```

تحتاج إلى تطبيق قائمة الخادم على تعريف البروتوكول:

```
class-map type inspect match-any ym-l4-cmap
 match protocol ymsgr ymsgr-pmap
```

يجب تكوين أوامر بحث ip domain و ip name-server ip.ad.re.ss لتمكين تحليل الاسم.

أسماء خوادم المراسلة الفورية ديناميكية إلى حد ما. يجب التحقق بشكل دوري من أن قوائم خادم المراسلة الفورية التي تم تكوينها كاملة وصحيحة.

يزيد الفحص من المستوى 7 (للتطبيق) من إمكانية الفحص من المستوى 4 مع إمكانية التعرف على الإجراءات الخاصة بالخدمة وتطبيقها، مثل حظر إمكانيات المحادثة النصية أو السماح بها بشكل انتقائي ورفض إمكانات الخدمة الأخرى.

يتيح فحص تطبيق المراسلة الفورية حالي إمكانية التمييز بين نشاط الدردشة النصية وجميع خدمات التطبيقات الأخرى. لتقييد نشاط المراسلة الفورية بالدردشة النصية، قم بتكوين سياسة من الطبقة 7:

```
class-map type inspect ymsgr match-any ymsgr-text-cmap
  match service text-chat
```

```
class-map type inspect ymsgr match-any ymsgr-default-cmap
  match service any

policy-map type inspect im ymsgr-l7-pmap
  class type inspect im ymsgr-text-cmap
    allow
    [log]
  class type inspect im ymsgr-text-cmap
    reset
    [log]
```

تطبيق سياسة الطبقة 7 على Yahoo! تم تكوين نهج Messenger مسبقا:

```
class-map type inspect match-any my-im-class
match protocol ymsgr
!
policy-map type inspect private-allowed-policy
 class type inspect my-im-class
  inspect
  service-policy im ymsgr-l7-pmap
```

عوامل تصفية URL

يوفر ZFW إمكانيات تصفية URL لتحديد الوصول إلى محتوى الويب إلى ما تم تحديده هاتالاجملا ءامسأ هيجوت ةداعإ لالخ نم وأ ،هجوملا ىلع ةفرعم ءادوس وأ ءاضيب ةمئاق ةطساوب إلى خادم تصفية URL للتحقق من الوصول إلى مجالات معينة. يتم تطبيق تصفية عناوين URL الخاص ب ZFW في الإصدار 12.4(6)T من برنامج Cisco IOS Software إلى الإصدار 12.4(15)T كإجراء سياسة إضافي، مماثل لفحص التطبيق.

لتصفية عنوان URL المستند إلى الخادم، يجب عليك تحديد خريطة معلمة تصف تكوين خادم عامل التصفية الأساسي:

```
parameter-map type urlfilter websense-parmap
 server vendor [n2h2 | websense] 10.1.1.1
```

إذا تم تفضيل القوائم البيضاء أو السوداء الثابتة، يمكنك تحديد قائمة مجالات أو مجالات فرعية يُسمح بها أو رفضها بشكل صريح، بينما يتم تطبيق الإجراء العكسي على حركة المرور التي لا تطابق القائمة:

```
parameter-map type urlfilter websense-parmap
 exclusive-domain deny .disallowed.com
 exclusive-domain permit .cisco.com
```

إذا تم تعريف قائمة URL السوداء باستخدام خيارات الرفض في تعريفات المجال الحصري، يتم السماح بجميع المجالات الأخرى. إذا تم تعريف أي تعريفات "السماح"، فيجب تحديد جميع المجالات المسموح بها بشكل صريح، وهو ما يماثل وظيفة قوائم التحكم في الوصول إلى IP.

إعداد خريطة فئة تطابق حركة مرور HTTP:

```
class-map type inspect match-any http-cmap
 match protocol http
```

تحديد خريطة سياسة تربط خريطة الفئة بإجراءات الفحص والتصفية:

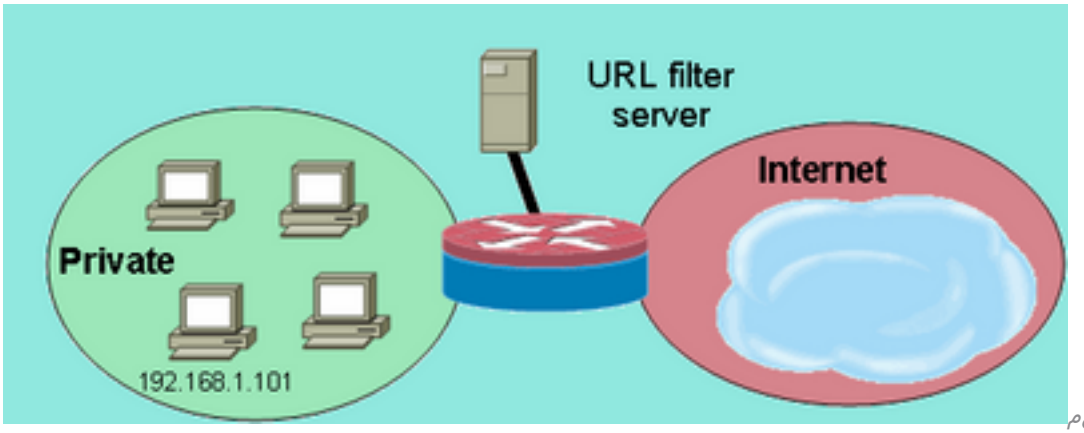
```
policy-map type inspect http-filter-pmap
```

```
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
```

يقوم هذا بتكوين الحد الأدنى من متطلبات الاتصال بخادم تصفية URL. تتوفر العديد من الخيارات لتحديد سلوك تصفية URL الإضافي.

ترى بعض عمليات نشر الشبكة تطبيق تصفية URL لبعض البيئات المضيفة أو الشبكات الفرعية، وتجاوز تصفية URL لمضيفين آخرين. على سبيل المثال، في الشكل 9، يجب أن يكون لدى جميع البيئات المضيفة في المنطقة الخاصة حركة مرور بيانات HTTP التي تم فحصها بواسطة خادم تصفية URL، باستثناء المضيف المحدد 192.168.1.101.

شكل 10: مخطط مثال تصفية URL



مخطط مثال تصفية URL

ويمكن تحقيق ذلك إذا قمت بتعريف خريطتي فئة مختلفتين:

- خريطة فئة واحدة تطابق حركة مرور HTTP فقط للمجموعة الأكبر من البيئات المضيفة، التي تتلقى تصفية URL.
- خريطة فئة واحدة للمجموعة الأصغر من البيئات المضيفة، التي لا تتلقى تصفية URL. تطابق خريطة الفئة الثانية حركة مرور HTTP، بالإضافة إلى قائمة بالمضيفين الذين تم إعفاؤهم من سياسة تصفية URL.

يتم تكوين كلا الخريطتين من الفئة في خريطة سياسة، ولكن يتلقى واحد فقط إجراء URLfilter:

```
class-map type inspect match-any http-cmap
 match protocol http
class-map type inspect match-all http-no-urlf-cmap
 match protocol http
 match access-group 101
!
policy-map type inspect http-filter-pmap
 class type inspect http-no-urlf-cmap
  inspect
 class type inspect http-cmap
  inspect
  urlfilter websense-parmap
!
access-list 101 permit ip 192.168.1.101 any
```

التحكم في الوصول إلى الموجه

يكون معظم مهندسي أمان الشبكة غير مرتاحين إذا قاموا بكشف واجهات إدارة الموجه (على

سبيل المثال، SSH و Telnet و HTTP و HTTPS و SNMP وما إلى ذلك) أمام الإنترنت العام، وفي ظل ورقة عمل معينة، تكون هناك حاجة إلى التحكم للوصول إلى شبكة LAN إلى الموجه أيضا. يوفر برنامج Cisco IOS software عدد من الخيارات للحد من الوصول إلى الواجهات المختلفة، والتي تتضمن مجموعة ميزات حماية أساس الشبكة (NFP) وآليات متنوعة للتحكم في الوصول ل ZFW. يجب عليك مراجعة الميزات الأخرى، مثل الوصول إلى واجهات الإدارة والمنطقة الذاتية وحماية مستوى الإدارة والتحكم في الوصول إلى شبكة VTY التحكم في الوصول SNMP وبروتوكول لتحديد أي مجموعة من ميزات التحكم في الموجه تعمل بشكل أفضل لتطبيق المحدد.

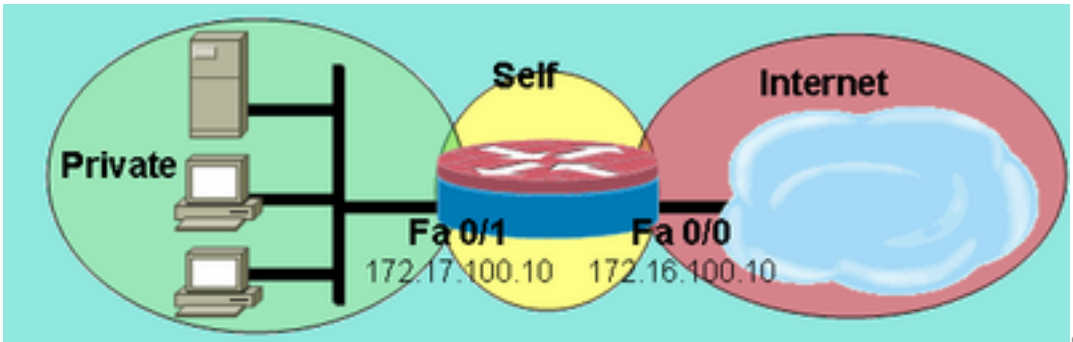
بشكل عام، تكون مجموعة ميزات NFP هي الأفضل للتحكم في حركة المرور الموجهة للموجه نفسه. ارجع إلى [نظرة عامة على أمان مستوى التحكم في برنامج Cisco IOS](#) للحصول على معلومات تصف حماية الموجه باستخدام ميزات NFP.

إذا قررت تطبيق ZFW للتحكم في حركة المرور من عناوين IP وإليها على الموجه نفسه، فيجب أن تفهم أن سياسة وإمكانات جدار الحماية الافتراضية تختلف عن تلك المتاحة لحركة مرور النقل. يتم تعريف حركة مرور النقل على أنها حركة مرور شبكة ال يتطابق عناوين IP للمصدر والوجهة الخاصة بها مع أي عناوين IP يتم تطبيقها على أي من واجهات الموجه، على سبيل المثال، رسائل التحكم الموجه، والا تتسبب حركة المرور في أن يرسل الموجه، أو رسائل الشبكة/المضيف التي يتعذر الوصول إليها.

يطبق ZFW سياسة رفض الكل افتراضية على حركة المرور التي تنتقل بين المناطق، باستثناء، كما هو مذكور في القواعد العامة، حركة المرور في أي منطقة تتدفق مباشرة إلى عناوين واجهات الموجه مسموح بها ضمنيا. هذا يضمن أن الاتصال بواجهات إدارة الموجه يتم الحفاظ عليه عند تطبيق تكوين جدار حماية منطقة على الموجه. إذا أثر نفس نوع الرفض الكل على الاتصال مباشرة بالموجه، فيجب تطبيق تكوين نوع إدارة كامل قبل تكوين المناطق على الموجه. من شأن ذلك أن يؤدي إلى تعطيل الاتصال بالإدارة إذا تم تنفيذ السياسة أو تطبيقها بشكل غير صحيح بالترتيب الخاطئ.

عند تكوين واجهة لتكون عضوا في منطقة، يتم تضمين البيئات المضيفة المتصلة بالواجهة في المنطقة. وعم ذلك، ال يتم التحكم في حركة المرور التي تتدفق إلى ومن عناوين IP الخاصة بواجهات الموجه بواسطة سياسات المنطقة (باستثناء الظروف الموضحة في الملاحظة في الشكل 10). بدل من ذلك، يتم تحويل جميع واجهات IP على الموجه تلقائيا إلى جزء من المنطقة الذاتية عند تكوين ZFW. من أجل التحكم في حركة مرور IP التي تنتقل إلى واجهات الموجه من المناطق المختلفة على الموجه، يجب تطبيق السياسات لحظر حركة المرور أو السماح بها/فحصها بين المنطقة والمنطقة الذاتية للموجه، والعكس (راجع الشكل 11).

الشكل 11: تطبيق السياسة بين مناطق الشبكة والمنطقة الذاتية للموجه



تطبيق السياسة بين مناطق الشبكة والمنطقة الذاتية للموجه

على الرغم من أن الموجه يوفر سياسة السماح الافتراضي بين جميع المناطق والمنطقة الذاتية، ولم يتم تكوين أي سياسة من هذا القبيل، فإن

أي سياسة من نفساه إلى المناطق المتصلة بالواجهة القابلة للتكوين من قبل الموجه، فإن جميع حركات المرور التي تم إنشاؤها من قبل الموجه تواجه سياسة المنطقة المتصلة إلى المنطقة الذاتية على إرجاع الموجه وتم حظرها. وبالتالي، يجب فحص حركة المرور التي تم إنشاؤها بواسطة الموجه للسماح بعودتها إلى المنطقة الذاتية.

> **ملاحظة**: يستخدم برنامج Cisco IOS Software دائما عنوان IP المرتبط بواجهة " أقرب " مضيفات وجهة لحركة المرور مثل syslog، و tftp، و telnet، وخدمات مستوى التحكم الأخرى، ويخضع حركة المرور هذه لسياسة جدار حماية المنطقة الذاتية. ومع ذلك، إذا كانت الخدمة تعرف واجهة معينة على أنها واجهة المصدر مع الأوامر التي تتضمن، ولكن لا تقتصر على تسجيل الواجهة المصدر [type number]، ip tftp source-interface [type number]، و ip telnet source-interface [type number]، فإن حركة المرور تخضع للمنطقة الذاتية.

> **ملاحظة**:تستخدم بعض الخدمات (خاصة خدمات الوصول عبر بروتوكول الإنترنت الخاصة بالموجهات) واجهات أو مؤقتة غير قابلة للتكوين لا يمكن تخصيصها لمناطق الأمان. يتعذر على هذه الخدمات العمل بشكل صحيح إذا تعذر اقتران حركة المرور الخاصة بها بمنطقة أمان تم تكوينها.

قيود سياسة المنطقة الذاتية

تستمد سياسة المنطقة الذاتية وظائف محدودة مقارنة بالسياسات المتوفرة لأزواج مناطق حركة المرور العابرة:

- كما هو الحال مع الفحص التقليدي الذي يحدد الحالة، يقتصر حركة المرور التي يتم إنشاؤها من الموجه على TCP و UDP و ICMP وفحص البروتوكول المعقد ل H.323.
- لا يتوفر فحص التطبيق لسياسات المنطقة الذاتية.
- لا يمكن تكوين جلسة العمل وتحديد المعدل على سياسات المنطقة الذاتية.

تكوين سياسة المنطقة الذاتية

في معظم الظروف، تكون هذه سياسات الوصول المرغوب فيها لخدمات إدارة الموجه:

- رفض جميع إتصالات Telnet، حيث أن بروتوكول النصوص غير المشفرة ل Telnet يكشف بسهولة بيانات اعتماد المستخدم والمعلومات الحساسة الأخرى.
- السماح باتصالات SSH من أي مستخدم في أي منطقة. يقوم SSH بتشفير بيانات اعتماد المستخدم وبيانات جلسة العمل، والتي توفر الحماية من المستخدمين الضارين الذين يستخدمون أدوات التقاط الحزم للتطفل على نشاط المستخدم والوسط لبيانات اعتماد المستخدم أو المعلومات الحساسة مثل تكوين الموجه. يوفر الإصدار 2 من SSH حماية أقوى ويعالج نقاط الضعف المحددة الكامنة في الإصدار 1 من SSH.
- السماح باتصال HTTP بالموجه من المناطق الخاصة إذا كانت المنطقة الخاصة جديرة بالثقة. وإلا، إذا كانت المنطقة الخاصة بها إمكانية قيام المستخدمين الضارين بتسوية المعلومات، فإن HTTP لا يستخدم التشفير لحماية حركة مرور الإدارة، ويمكن أن يكشف عن معلومات حساسة مثل بيانات اعتماد المستخدم أو التكوين.
- السماح باتصال HTTPS من أي منطقة. كما هو الحال مع بروتوكول SSH، يقوم بروتوكول HTTPS بتشفير بيانات الجلسة وبيانات اعتماد المستخدم.
- تقييد وصول SNMP إلى مضيف أو شبكة فرعية معينة. يمكن إستخدام SNMP لتعديل تكوين الموجه والكشف عن معلومات التكوين. يجب تكوين بروتوكول SNMP بالتحكم في الوصول على المجتمعات المختلفة.
- رفض طلبات ICMP من الإنترنت العام إلى عنوان المنطقة الخاصة (يفترض أن هذا عنوان

المنطقة الخاصة قابل للتوجيه). يمكن عرض عناوين عام واحد أو أكثر لحركة مرور ICMP الاستكشاف أخطاء الشبكة وإصلاحها، إذا لزم الأمر. يمكن استخدام العديد من جهات بروتوكول ICMP الإرسال كما موارد الموجه أو إصلاح ووبطولوجيا الشبكة وبنيتها.

يمكن للموجه تطبيق هذا النوع من النهج بإضافة أزواج مناطق لكل منطقة يجب التحكم في الموجه أو المنطقة الذاتية إلى الواردة والمرور لحركة مناطق زوج كل مطابقة يجب .فيها الصادرة منه بالسياسة المقابلة في الإتجاه المعاكس، ما لم يتم إنشاء حركة المرور في الإتجاه المعاكس. يمكن تطبيق تعيين سياسة واحدة لكل أزواج مناطق واردة وصادرة في حركة المرور بالكامل، أو يمكن تطبيق خرائط سياسة محددة لكل زوج مناطق. توفير تكوين خريطة سياسة ذات مستويات عرض لكل خريطة سياسة عدة مستويات مع كل أزواج مناطق النشاط الذي يتطابق مع كل خريطة سياسة.

على سبيل المثال، شبكة مع محطة إدارة SNMP على 172.17.100.11 وخادم TFTP على 172.17.100.17، يقدم هذا الإخراج مثال على سياسة الوصول إلى واجهة الإدارة بالكامل:

```
class-map type inspect match-any self—service-cmap
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol h323
!
class-map type inspect match-all to-self-cmap
 match class-map self—service-cmap
 match access-group 120
!
class-map type inspect match-all from-self-cmap
 match class-map self—service-cmap
!
class-map type inspect match-all tftp-in-cmap
 match access-group 121
!
class-map type inspect match-all tftp-out-cmap
 match access-group 122
!
policy-map type inspect to-self-pmap
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
zone security private
zone security internet
zone-pair security priv-self source private destination self
 service-policy type inspect to-self-pmap
zone-pair security net-self source internet destination self
 service-policy type inspect to-self-pmap
zone-pair security self-priv source self destination private
 service-policy type inspect from-self-pmap
zone-pair security self-net source self destination internet
 service-policy type inspect from-self-pmap

!
interface FastEthernet 0/0
 ip address 172.16.100.10
```

```
 zone-member security internet
!
interface FastEthernet 0/1
 ip address 172.17.100.10
 zone-member security private
!
access-list 120 permit icmp 172.17.100.0 0.0.0.255 any
access-list 120 permit icmp any host 172.17.100.10 echo
access-list 120 deny icmp any any
access-list 120 permit tcp 172.17.100.0 0.0.0.255 host 172.17.100.10 eq www
access-list 120 permit tcp any any eq 443
access-list 120 permit tcp any any eq 22
access-list 120 permit udp any host 172.17.100.10 eq snmp
access-list 121 permit udp host 172.17.100.17 host 172.17.100.10
access-list 122 permit udp host 172.17.100.10 host 172.17.100.17
```

لسوء الحظ، ال توفر سياسة المنطقة الذاتية القدرة على فحص عمليات نقل TFTP. وبالتالي، يجب أن يمرر جدار الحماية جميع حركات المرور من خادم TFTP وإليه إذا كان يجب أن يمر TFTP عبر جدار الحماية.

إذا قام الموجه بإنهاء إتصالات IPSec VPN، فيجب عليك أيضا تحديد سياسة لتمرير IPSec NAT-T IPSec (UDP 4500). و ISAKMP و IPSec AH و ESP. يعتمد ذلك على الخدمات التي تستخدمها. يمكن تطبيق هذه النهج التالي بالإضافة إلى النهج أعلاه. الحظ التغيير على حركة، وعادة، تمرير إرجاع VPN مرور حركة لحركة فئة خريطة حيث تم إدراج خارطة السياسة. تحتاج إلى التأكد من أن سياسة الأمان الخاصة بك على أنه يجب عليك المرور المشفرة جديرة بالثقة، ما لم تنص سياسة الأمان الخاصة بك على أنه يجب عليك السماح بحركة المرور المشفرة من نقاط النهاية المحددة وإليها.

```
class-map type inspect match-all crypto-cmap
 match access-group 123
!
policy-map type inspect to-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect to-self-cmap
  inspect
 class type inspect tftp-in-cmap
  pass
!
policy-map type inspect from-self-pmap
 class type inspect crypto-cmap
  pass
 class type inspect from-self-cmap
  inspect
 class type inspect tftp-out-cmap
  pass
!
access-list 123 permit esp any any
access-list 123 permit udp any any eq 4500
access-list 123 permit ah any any
access-list 123 permit udp any any eq 500
```

خدمات التطبيقات واسعة النطاق وجدار الحماية القائم على المناطق

عجار [ملاحظة الإصدار لخدمات التطبيقات الواسعة من Cisco (الإصدار 4.0.13) - الميزات الجديدة](#) [للبرنامج الإصدار 4.0.13](#) للحصول على ملاحظة تطبيق توفر أمثلة التكوين وإرشادات الاستخدام

مراقبة جدار حماية السياسة المستند إلى المنطقة باستخدام أوامر show و debug

يقدم ZFW أوامر جديدة لعرض تكوين النهج ومراقبة نشاط جدار الحماية.

عرض وصف المنطقة والواجهات المتضمنة في منطقة محددة:

```
show zone security [<zone-name>]
```

وفي حالة عدم تضمين اسم المنطقة، يعرض الأمر معلومات جميع المناطق التي تم تكوينها.

```
Router#show zone security z1
zone z1
  Description: this is test zone1
  Member Interfaces:
    Ethernet0/0
```

عرض المنطقة المصدر والمنطقة الوجهة والنهج المرتبط بزوج المنطقة:

```
show zone-pair security [source <source-zone-name>] [destination <destination-zone-name>]
```

في حالة عدم تحديد مصدر أو وجهة، يتم عرض جميع أزواج المناطق ذات المصدر والوجهة والنهج المقترن. عند ذكر منطقة المصدر/الوجهة فقط، يتم عرض جميع أزواج المناطق التي تحتوي على هذه المنطقة كمصدر/وجهة.

```
Router#show zone-pair security
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

عرض مخطط سياسة محدد:

```
show policy-map type inspect [<policy-map-name> [class <class-map-name]]
```

عندما لا يتم تحديد اسم خريطة السياسة، فإنها تعرض جميع خرائط السياسة الخاصة بفحص النوع (مع خرائط سياسة الطبقة 7 التي تحتوي على نوع فرعي).

```
Router#show policy-map type inspect p1
 Policy Map type inspect p1
   Class c1
    Inspect
```

عرض إحصائيات مخطط سياسة نوع فحص وقت التشغيل حاليا على زوج منطقة محدد.

```
show policy-map type inspect zone-pair [zone-pair-name] [sessions]
```

عند عدم ذكر اسم زوج منطقة، يتم عرض خرائط السياسة على جميع أزواج المناطق.

يعرض خيارا الجلسات جلسات التفتيش التي تم إنشاؤها بواسطة تطبيق خريطة السياسة على زوج المناطق المحدد.

```
Router#show policy-map type inspect zone-pair zp
 Zone-pair: zp

  Service-policy : p1

    Class-map: c1 (match-all)
      Match: protocol tcp
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [0:0:0]
        Last session created never
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0

    Class-map: c2 (match-all)
      Match: protocol udp
      Pass
        0 packets, 0 bytes

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

تعرض الكلمة الأساسية urlFilter الإحصاءات المرتبطة ب URLfilter والمتعلقة بخريطة السياسة المحددة (أو خرائط السياسة على جميع الأهداف عندما لا يتم تحديد اسم زوج مناطق):

```
show policy-map type inspect zone-pair [zone-pair-name] [urlfilter [cache]]
```

عندما يتم تحديد الكلمة الأساسية ذاكرة التخزين المؤقت مع URLfilter ، فإنها تعرض ذاكرة التخزين المؤقت ل URLfilter (العناوين IP).

ملخص الأمر show policy-map لفحص خرائط السياسة:

```
show policy-map type inspect inspect { <policy name> [class <class name>] |
                  zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```

الحماية من رفض الخدمة لجدار الحماية القائم على منطقة Tune

يوفر ZFW حماية رفض الخدمة (DoS) لتنبيه مهندسي الشبكة إلى التغييرات الكبيرة طاشن نشاط في الشبكة، ولتخفيف النشاط غير المرغوب فيه لتقليل تأثير تغييرات نشاط الشبكة. يحتفظ ZFW بعداد منفصل لكل خريطة فئة لخريطة السياسة. وبالتالي، إذا تم إستخدام خريطة فئة واحدة لخريطتي سياسة أزواج مناطق مختلفين، يتم تطبيق مجموعتين مختلفتين من عدادات حماية رفض الخدمة (DoS).

يوفر ZFW تخفيف وجوه رفض الخدمة (DoS) إعداد افتراضي على إصدارات برنامج Cisco IOS Software قبل 12.4(11)T. تم تغيير سلوك حماية DoS الافتراضي باستخدام برنامج Cisco

IOS، الإصدار 12.4(11)T.

ارجع إلى تحديد الاستراتيجيات للحماية من هجمات رفض خدمة TCP SYN للحصول على مزيد من المعلومات حول هجمات TCP SYN DoS.

الملاحق

الملحق أ: التكوين الأساسي

```
ip subnet-zero
ip cef
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 bridge-group 1
!
interface Vlan2
 no ip address
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 ip route-cache flow
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
bridge 1 protocol ieee
bridge 1 route ip
```

```
!
end
```

الملحق ب: التكوين النهائي (الكامل)

```
ip subnet-zero
ip cef
!
ip port-map user-Xwindows port tcp from 6900 to 6910
!
class-map type inspect match-any L4-inspect-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any L7-inspect-class
  match protocol ssh
  match protocol ftp
  match protocol pop
  match protocol imap
  match protocol esmtp
  match protocol http
class-map type inspect match-any dns-http-class
 match protocol dns
 match protocol http
class-map type inspect match-any smtp-class
 match protocol smtp
class-map type inspect match-all dns-http-acl-class
 match access-group 110
 match class-map dns-http-class
class-map type inspect match-all smtp-acl-class
 match access-group 111
 match class-map smtp-class
class-map type inspect match-any Xwindows-class
 match protocol user-Xwindows
class-map type inspect match-any internet-traffic-class
 match protocol http
 match protocol https
 match protocol dns
 match protocol icmp
class-map type inspect http match-any bad-http-class
 match  port-misuse all
 match  strict-http
!
policy-map type inspect clients-servers-policy
 class type inspect L4-inspect-class
  inspect
policy-map type inspect private-dmz-policy
  class type inspect L7-inspect-class
   inspect
policy-map type inspect internet-dmz-policy
 class type inspect dns-http-acl-class
  inspect
 class type inspect smtp-acl-class
  inspect
policy-map type inspect servers-clients-policy
 class type inspect Xwindows-class
  inspect
policy-map type inspect private-internet-policy
  class type inspect internet-traffic-class
   inspect
  class type inspect bad-http-class
   drop
!
```

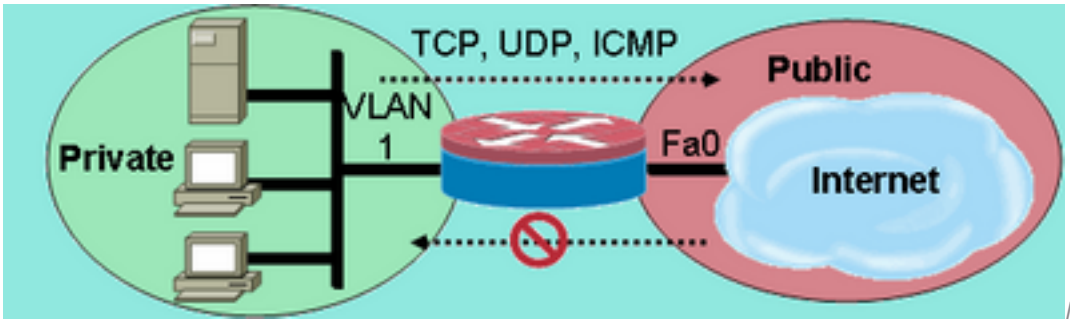
```
zone security clients
zone security servers
zone security private
zone security internet
zone security dmz
zone-pair security private-internet source private destination internet
  service-policy type inspect private-internet-policy
zone-pair security servers-clients source servers destination clients
  service-policy type inspect servers-clients-policy
zone-pair security clients-servers source clients destination servers
  service-policy type inspect clients-servers-policy
zone-pair security private-dmz source private destination dmz
  service-policy type inspect private-dmz-policy
zone-pair security internet-dmz source internet destination dmz
  service-policy type inspect internet-dmz-policy
!
bridge irb
!
interface FastEthernet0
 ip address 172.16.1.88 255.255.255.0
 zone-member internet
!
interface FastEthernet1
 ip address 172.16.2.1 255.255.255.0
 zone-member dmz
!
interface FastEthernet2
 switchport access vlan 2
!
interface FastEthernet3
 switchport access vlan 2
!
interface FastEthernet4
 switchport access vlan 1
!
interface FastEthernet5
 switchport access vlan 1
!
interface FastEthernet6
 switchport access vlan 1
!
interface FastEthernet7
 switchport access vlan 1
!
interface Vlan1
 no ip address
 zone-member clients
 bridge-group 1
!
interface Vlan2
 no ip address
 zone-member servers
 bridge-group 1
!
interface BVI1
 ip address 192.168.1.254 255.255.255.0
 zone-member private
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.1.1
!
access-list 110 permit ip any host 172.16.2.2
access-list 111 permit ip any host 172.16.2.3
!
```

```
bridge 1 protocol ieee
bridge 1 route ip
!
End
```

الملحق ج: تكوين جدار حماية سياسة المنطقة الأساسي لمنطقتين

يوفر هذا المثال تكوين بسيط كأساس لاختبار مميزات التحسينات على برنامج Cisco IOS Software ZFW. هذا التكوين هو تكوين نموذج لمنطقتين، كما هو مكون على موجه 1811. يتم تطبيق المنطقة الخاصة على منافذ المحول الثابت للموجه، لذلك يتم توصيل جميع البيئات المضيفة على منافذ المحول بشبكة VLAN رقم 1. يتم تطبيق المنطقة العامة على FastEthernet 0 (راجع الشكل 12).

الشكل 12: المنطقة العامة المطبقة على FastEthernet 0



المنطقة العامة المطبقة على FastEthernet 0

```
class-map type inspect match-any private-allowed-class
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all http-class
 match protocol http
!
policy-map type inspect private-allowed-policy
 class type inspect http-class
  inspect my-parameters
 class type inspect private-allowed-class
  inspect
!
zone security private
zone security public
zone-pair security priv-pub source private destination public
 service-policy type inspect private-allowed-policy
!
interface fastethernet 0
 zone-member security public
!
interface VLAN 1
 zone-member security private
```

معلومات ذات صلة

- [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).