

تامدخ نيوكت لاثم ني كمت PIX/ASA 7.x: FTP/TFTP

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الرسم التخطيطي للشبكة
المنتجات ذات الصلة
الاصطلاحات
معلومات أساسية
معالجة البروتوكول المتقدمة
تكوين فحص تطبيق FTP الأساسي
مثال على التكوين
تكوين فحص بروتوكول FTP على منفذ TCP غير القياسي
تكوين فحص تطبيق TFTP الأساسي
مثال على التكوين
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
مشكلة: لا تعمل الصياغة في التكوين ويتم إستلام خطأ فحص خريطة الفئة
الحل
يتعذر تشغيل FTP (FTPS عبر SSL) عبر ASA
معلومات ذات صلة

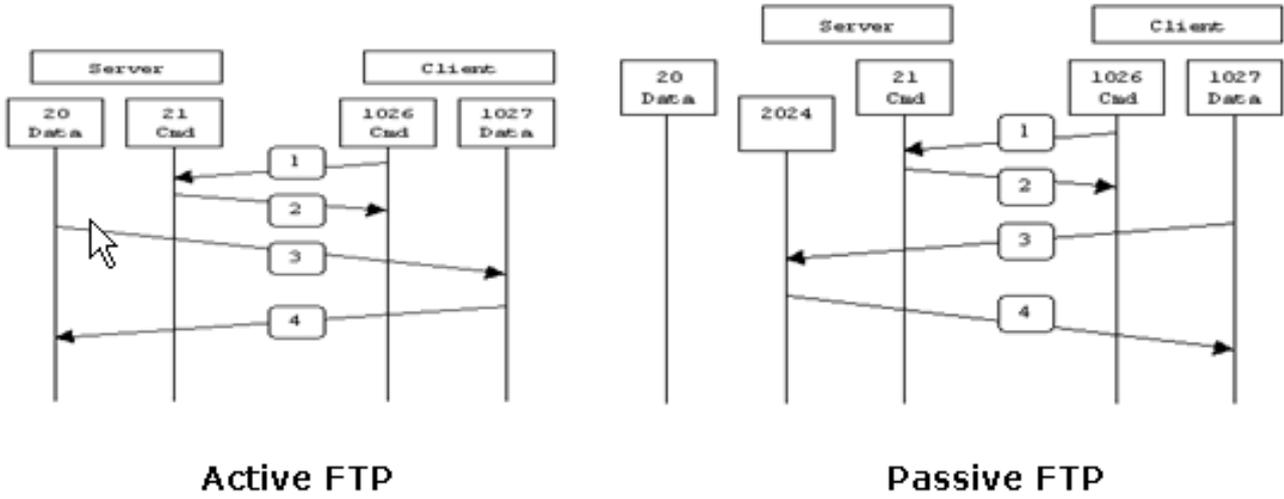
المقدمة

يشرح هذا المستند الخطوات المطلوبة للمستخدمين خارج الشبكة للوصول إلى خدمات FTP و TFTP في شبكة DMZ الخاصة بك.

بروتوكول نقل الملفات (FTP)

هناك شكلان من FTP:

- الوضع النشط
- الوضع الخامل



Active FTP :

command : client >1023 -> server 21
 data : client >1023 <- server 20

Passive FTP :

command : client >1023 -> server 21
 data : client >1023 -> server >1023

في وضع FTP النشط، يتصل العميل من منفذ عشوائي غير ذي امتيازات ($N > 1023$) إلى منفذ الأمر (21) من خادم FTP. ثم يبدأ العميل في الاستماع إلى المنفذ $N+1$ ويرسل منفذ أمر $N+1$ FTP إلى خادم FTP. ثم يتصل الخادم مرة أخرى بمنافذ البيانات المحددة للعميل من منفذ البيانات المحلي الخاص به، والذي هو المنفذ 20.

في وضع FTP السلبي، يقوم العميل بتهيئة كلا الاتصالات بالخادم، مما يحل مشكلة جدار الحماية الذي يقوم بتصفية اتصال منفذ البيانات الواردة بالعميل من الخادم. عند فتح اتصال FTP، يفتح العميل منفذين عشوائياً غير محظوظين محلياً ($N > 1023$ و $N+1$). يتصل المنفذ الأول بالخادم على المنفذ 21. ولكن بدلا من إصدار الأمر port والسماح للخادم بالاتصال مرة أخرى بمنفذ البيانات الخاص به، يصدر العميل الأمر PASV. والنتيجة من هذا أن الخادم بعد ذلك يفتح منفذا عشوائياً غير ذي امتيازات ($P > 1023$) ويرسل الأمر port P مرة أخرى إلى العميل. بعد ذلك يقوم العميل ببدء الاتصال من المنفذ $N+1$ إلى المنفذ P على الخادم لنقل البيانات. بدون تكوين أمر الفحص على جهاز الأمان، يعمل FTP من داخل المستخدمين الذين يترأسون الصادر فقط في الوضع الخامل. كما يتم رفض وصول المستخدمين خارج الإتجاه الوارد إلى خادم FTP.

ارجع إلى [ASA 8.3 والإصدارات الأحدث: تمكين مثال تكوين خدمات FTP/TFTP](#) للحصول على مزيد من المعلومات حول التكوين المتطابق باستخدام ASDM مع جهاز الأمان القابل للتكيف (ASA) من Cisco مع الإصدار 8.3 والإصدارات الأحدث.

بروتوكول نقل الملفات المبسط (TFTP)

يعد TFTP، كما هو موضح في [RFC 1350](#)، بروتوكولا بسيطا لقراءة الملفات وكتابتها بين خادم TFTP والعميل. يستخدم TFTP منفذ 69 UDP.

المتطلبات الأساسية

المتطلبات

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

- يوجد اتصال أساسي بين الواجهات المطلوبة.
- لديك خادم FTP تم تكوينه داخل شبكة DMZ.

المكونات المستخدمة

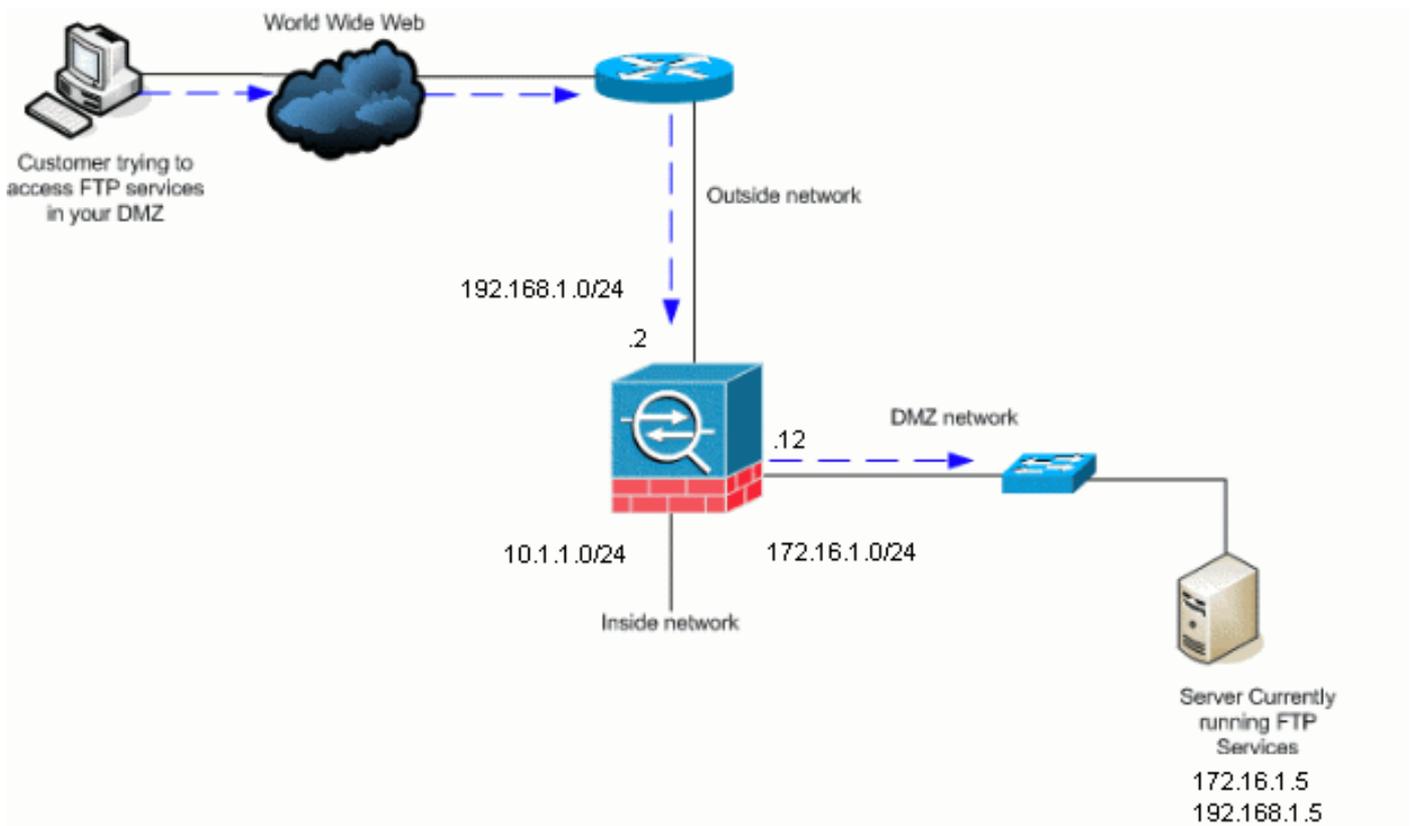
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- جهاز الأمان القابل للتكيف للASA 5500 Series الذي يشغل صورة البرنامج (2)7.2
- خادم Windows 2003 الذي يقوم بتشغيل خدمات FTP
- خادم Windows 2003 الذي يقوم بتشغيل خدمات TFTP
- كمبيوتر العميل الموجود خارج الشبكة

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

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوين RFC 1918 التي تم استخدامها في بيئة مختبرية.

المنتجات ذات الصلة

كما يمكن استخدام هذا التكوين مع جهاز الأمان PIX 7.x.

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

معلومات أساسية

يدعم جهاز الأمان فحص التطبيق من خلال وظيفة خوارزمية الأمان المعدلة. من خلال فحص التطبيقات الذي يحدد الحالة الذي تستخدمه خوارزمية الأمان المعدلة، يتتبع جهاز الأمان كل اتصال يعبر جدار الحماية ويضمن صلاحيته. كما يراقب جدار الحماية، من خلال الفحص المعبر عن الحالة، حالة الاتصال لتجميع المعلومات لوضعها في جدول حالة. باستخدام جدول الحالة بالإضافة إلى القواعد المحددة من قبل المسؤول، تستند قرارات التصفية إلى السياق الذي تم إنشاؤه بواسطة الحزم التي تم تمريرها مسبقاً عبر جدار الحماية. ويتألف تنفيذ عمليات تفتيش التطبيقات من الإجراءات التالية:

- حدد حركة المرور.
- تطبيق عمليات التفتيش على حركة المرور.
- تنشيط عمليات التفتيش على واجهة.

معالجة البروتوكول المتقدمة

FTP

تتطلب بعض التطبيقات معالجة خاصة بواسطة وظيفة فحص تطبيق جهاز الأمان من Cisco. تقوم هذه الأنواع من التطبيقات بتضمين معلومات عنوان IP في حزمة بيانات المستخدم أو فتح القنوات الثانوية على المنافذ المعينة بشكل ديناميكي. تعمل وظيفة فحص التطبيق مع ترجمة عنوان الشبكة (NAT) للمساعدة في تحديد موقع معلومات العنوان المضمنة.

بالإضافة إلى تعريف معلومات العنوان المضمنة، تراقب وظيفة فحص التطبيق جلسات عمل تحديد أرقام المنافذ للقنوات الثانوية. تفتح العديد من البروتوكولات منافذ TCP أو UDP الثانوية لتحسين الأداء. يتم استخدام الجلسة الأولية على منفذ معروف للتفاوض على أرقام المنافذ المعينة بشكل ديناميكي. تراقب وظيفة فحص التطبيق هذه الجلسات، وتعرف تعيينات المنفذ الديناميكية وتسمح بتبادل البيانات على هذه المنافذ طوال مدة الجلسات المحددة. تعرض تطبيقات الوسائط المتعددة و FTP هذا النوع من السلوك.

يتطلب بروتوكول FTP بعض المعالجة الخاصة بسبب استخدامه لمنفذين لكل جلسة FTP. يستخدم بروتوكول FTP منفذين عند تنشيطه لنقل البيانات: قناة التحكم وقناة البيانات التي تستخدم المنفذ 21 و 20، على التوالي. المستخدم، الذي يبدأ جلسة FTP عبر قناة التحكم، يقوم بكل طلبات البيانات من خلال تلك القناة. يقوم خادم FTP بعد ذلك ببدء طلب لفتح منفذ من منفذ الخادم 20 إلى كمبيوتر المستخدم. يستخدم FTP دائماً المنفذ 20 لاتصالات قناة البيانات. إذا لم يتم تمكين فحص FTP على جهاز الأمان، سيتم تجاهل هذا الطلب ولا تقوم جلسات FTP بإرسال أي بيانات مطلوبة. إذا تم تمكين فحص FTP على جهاز الأمان، فإن جهاز الأمان يراقب قناة التحكم ويحاول التعرف على طلب لفتح قناة البيانات. يدمج بروتوكول FTP مواصفات منفذ قناة البيانات في حركة مرور قناة التحكم، ويتطلب من جهاز الأمان فحص قناة التحكم لتغييرات منافذ البيانات. إذا قام جهاز الأمان بالتعرف على طلب ما، فإنه يقوم بإنشاء فتح مؤقت لحركة مرور قناة البيانات التي تستمر طوال فترة جلسة العمل. بهذه الطريقة، يراقب ال FTP تفتيش قناة التحكم، يعين data-port تنازل، ويسمح معطيات أن يكون تبادلت على المعطيات ميناء لطول الجلسة.

يفحص جهاز الأمان اتصالات المنفذ 21 لحركة مرور FTP بشكل افتراضي من خلال خريطة فئة الفحص العام. يتعرف جهاز الأمان أيضاً على الفرق بين جلسة FTP نشطة وسلبية. إذا كانت جلسات FTP تدعم نقل بيانات FTP السليبي، فإن جهاز الأمان، من خلال الأمر `inspection ftp`، يتعرف على طلب منفذ البيانات من المستخدم ويفتح منفذ بيانات جديد أكبر من 1023.

يقوم فحص تطبيق FTP بفحص جلسات FTP ويقوم بتنفيذ أربع مهام:

- إعداد اتصال بيانات ثانوي ديناميكي
- تعقب تسلسل أمر-إستجابة FTP
- إنشاء سجل تدقيق
- يترجم العنوان مدمج باستخدام NAT

يعد فحص تطبيق FTP القنوات الثانوية لنقل بيانات FTP. يتم تخصيص القنوات إستجابة لتحميل ملف أو تنزيل ملف أو حدث قائمة دليل، ويجب أن تكون خاضعة للتفاوض المسبق. يتم التفاوض على المنفذ من خلال أوامر المنفذ أو (PASV) (227).

TFTP

يتم تمكين فحص TFTP بشكل افتراضي.

يقوم جهاز الأمان بفحص حركة مرور بيانات TFTP ويقوم بإنشاء الاتصالات والترجمات بشكل ديناميكي، إذا لزم الأمر، للسماح بنقل الملفات بين عميل TFTP والخادم. وعلى وجه الخصوص، يقوم محرك الفحص بفحص طلبات قراءة (TFTP (RRQ وطلبات الكتابة (WRQ) وإعلامات الخطأ (الخطأ).

يتم تخصيص قناة ثانوية ديناميكية وترجمة PAT، إذا لزم الأمر، على إستقبال RRQ أو WRQ صالح. وبعد ذلك يتم إستخدام هذه القناة الثانوية من قبل TFTP لنقل الملفات أو الإعلام بالأخطاء.

يمكن لخادم TFTP فقط بدء حركة مرور البيانات عبر القناة الثانوية، ويمكن أن توجد قناة ثانوية غير مكتملة واحدة على الأكثر بين عميل TFTP والخادم. يؤدي إعلام الخطأ من الخادم إلى إغلاق القناة الثانوية.

يجب تمكين فحص TFTP إذا تم إستخدام ضرب ساكن إستاتيكي لإعادة توجيه حركة مرور TFTP.

تكوين فحص تطبيق FTP الأساسي

بشكل افتراضي، يتضمن التكوين سياسة تطابق كل حركة مرور فحص التطبيق الافتراضية وتطبيق الفحص على حركة المرور على جميع الواجهات (سياسة عامة). تتضمن حركة مرور فحص التطبيق الافتراضية حركة مرور البيانات إلى المنافذ الافتراضية لكل بروتوكول. يمكنك تطبيق سياسة عامة واحدة فقط، لذلك إذا كنت تريد تغيير السياسة العامة، على سبيل المثال، لتطبيق فحص على منافذ غير قياسية، أو لإضافة عمليات فحص لم يتم تمكينها بشكل افتراضي، تحتاج إما إلى تحرير السياسة الافتراضية أو تعطيلها وتطبيق سياسة جديدة. للحصول على قائمة بجميع المنافذ الافتراضية، ارجع إلى [سياسة التفتيش الافتراضية](#).

1. قم بإصدار الأمر `policy-map global_policy`.
ASA#AIP-CLI (config) #policy-map global_policy

2. قم بإصدار الأمر `class inspection_default`.
ASA#AIP-CLI (config-pmap) #class inspection_default

3. قم بإصدار الأمر `inspect FTP`.
ASA#AIP-CLI (config-pmap-c) #inspect FTP

هناك خيار أن يستعمل ال **فحص FTP صارم** أمر. يزيد هذا الأمر من أمان الشبكات المحمية بمنع متصفح الويب من إرسال أوامر مضمنة في طلبات FTP. بعد تمكين الخيار/المقيد على واجهة، يفرض فحص FTP هذا السلوك: يجب الاعتراف بأمر FTP قبل أن يسمح جهاز الأمان بأمر جديد. يقوم جهاز الأمان بإسقاط اتصال يرسل أوامر مضمنة. يتم التحقق من أوامر 227 و **port** لضمان عدم ظهورها في سلسلة خطأ. تحذير: قد يؤدي إستخدام الخيار/المقيد إلى فشل عملاء FTP الذين لا يلتزمون بشكل صارم ب RFCs FTP. راجع [إستخدام الخيار المقيد](#) للحصول على مزيد من المعلومات حول إستخدام الخيار/المقيد.

اسم الجهاز 1

```

ASA-AIP-CLI (config)#show running-config

                               (ASA Version 7.2(2
                               !
                               hostname ASA-AIP-CLI
                               domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted
                               names
                               !
                               interface Ethernet0/0
                               nameif Outside
                               security-level 0
                               ip address 192.168.1.2 255.255.255.0
                               !
                               interface Ethernet0/1
                               nameif Inside
                               security-level 100
                               ip address 10.1.1.1 255.255.255.0
                               !
                               interface Ethernet0/2
                               nameif DMZ
                               security-level 50
                               ip address 172.16.1.12 255.255.255.0
                               !
                               interface Ethernet0/3
                               no nameif
                               no security-level
                               no ip address
                               !
                               interface Management0/0
                               no nameif
                               no security-level
                               no ip address
                               !
                               Output is suppressed. !--- Permit inbound FTP ---!
                               control traffic. access-list 100 extended permit tcp any
                               host 192.168.1.5 eq ftp
                               Permit inbound FTP data traffic. access-list 100 ---!
                               extended permit tcp any host 192.168.1.5 eq ftp-data
                               !
                               Command to redirect the FTP traffic received on IP ---!
                               192.168.1.5 !--- to IP 172.16.1.5. static (DMZ,outside)
                               192.168.1.5 172.16.1.5 netmask 255.255.255.255
                               access-group 100 in interface outside
                               class-map inspection_default
                               match default-inspection-traffic
                               !
                               !
                               policy-map type inspect dns preset_dns_map
                               parameters
                               message-length maximum 512

                               policy-map global_policy
                               class inspection_default
                               inspect dns preset_dns_map
                               inspect ftp
                               inspect h323 h225
                               inspect h323 ras

```

```
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
This command tells the device to !--- use the ---!
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
end :
#(ASA-AIP-CLI(config)
```

تكوين فحص بروتوكول FTP على منفذ TCP غير القياسي

أنت تستطيع شملت ال FTP بروتوكول تفتيش لمنافذ TCP غير قياسية مع هذا تشكيل خط (استبدلت XXXX مع الجديد ميناء رقم):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
match access-list ftp-list
!
policy-map global_policy
class ftp-class
inspect ftp
```

تكوين فحص تطبيق TFTP الأساسي

بشكل افتراضي، يتضمن التكوين سياسة تطابق كل حركة مرور فحص التطبيق الافتراضية وتطبيق الفحص على حركة المرور على جميع الواجهات (سياسة عامة). تتضمن حركة مرور فحص التطبيق الافتراضية حركة مرور البيانات إلى المنافذ الافتراضية لكل بروتوكول. يمكنك تطبيق سياسة عمومية واحدة فقط. لذلك إذا كنت تريد تغيير السياسة العامة، على سبيل المثال، لتطبيق فحص على منافذ غير قياسية، أو لإضافة عمليات تفتيش غير ممكنة بشكل افتراضي، تحتاج إما لتحرير السياسة الافتراضية أو تعطيلها وتطبيق سياسة جديدة. للحصول على قائمة بجميع المنافذ الافتراضية، ارجع إلى [سياسة التفتيش الافتراضية](#).

1. قم بإصدار الأمر `policy-map global_policy`
ASA#AIP-CLI (config) #`policy-map global_policy`

2. قم بإصدار الأمر `class inspection_default`
ASA#AIP-CLI (config-pmap) #`class inspection_default`

3. قم بإصدار الأمر `TFTP` فحص
ASA#AIP-CLI (config-pmap-c) #`inspect TFTP`

مثال على التكوين

```
ASA-AIP-CLI(config)#show running-config

(ASA Version 7.2(2
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbul encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
 security-level 50
 ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 no nameif
 no security-level
 no ip address
!
Output is suppressed. !--- Permit inbound TFTP ---!
traffic. access-list 100 extended permit udp any host
192.168.1.5 eq tftp
!
Command to redirect the TFTP traffic received on IP ---!
192.168.1.5 !--- to IP 172.16.1.5. static (DMZ,outside)
192.168.1.5 172.16.1.5 netmask 255.255.255.255
access-group 100 in interface outside
 class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum 512

 policy-map global_policy
 class inspection_default
 inspect dns preset_dns_map
 inspect ftp
 inspect h323 h225
 inspect h323 ras
 inspect netbios
 inspect rsh
 inspect rtsp
 inspect skinny
 inspect esmtp
```

```
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
This command tells the device to !--- use the ---!
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
end :
#(ASA-AIP-CLI(config)
```

التحقق من الصحة

لضمان أن التكوين قد تم إتخاذه بنجاح، أستخدم الأمر `show service-policy` وحدد الإخراج على فحص FTP فقط، باستخدام الأمر `show service-policy inspection ftp`.

```
ASA#AIP-CLI# show service-policy inspect ftp

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: ftp, packet 0, drop 0, reset-drop 0
ASA#AIP-CLI# █
```

استكشاف الأخطاء وإصلاحها

مشكلة: لا تعمل الصياغة في التكوين ويتم إستلام خطأ فحص خريطة الفئة

لا تعمل الصياغة المقدمة في قسم التكوين وتلقى خطأ مثل هذا:

```
ERROR: % class-map inspection_default not configured
```

الحل

يعتمد هذا التكوين على عمليات الفحص الافتراضية الموجودة في التكوين. إذا لم تكن في التكوين، فعليك إعادة إنشائها باستخدام الأوامر التالية:

1. `class-map inspection_default` مطابقة فحص افتراضي-حركة مرور
2. معلمات فحص نوع خريطة السياسة `DNS preset_dns_map` الحد الأقصى لطول الرسالة 512
3. خريطة السياسة العامة السياسة العامة `class inspection_default` إعداد DNS المسبق `dns_map` فحص `h225 h323` فحص `FTP h323 ras` فحص `h323 ras` فحص `RSH` فحص `RTSP` فحص `esmtsp` فحص `sqlnet` فحص النخافة فحص `SunRPC` فحص `xdmcp` فحص `SIP` فحص `NetBIOS` فحص `TFTP`
4. عمومي `policy-service-policy`

تحذير: إذا تمت إزالة عمليات الفحص الافتراضية مسبقا لحل مشكلة أخرى، فقد تعود هذه المشكلة عند إعادة تمكين عمليات الفحص الافتراضية. يجب أن تعرف أنت أو المسؤول الخاص بك ما إذا كان قد تم إزالة عمليات الفحص الافتراضية مسبقا كخطوة لاستكشاف الأخطاء وإصلاحها.

بتعذر تشغيل (FTP عبر SSL) عبر ASA

لا يدعم FTP مع TLS/SSL (SFTP / FTPS) من خلال جهاز الأمان. يتم تشفير اتصال FTP، لذلك لا توجد طريقة يمكن بها لجدار الحماية فك تشفير الحزمة. ارجع إلى [PIX/ASA: الأسئلة المتداولة حول جهاز الأمان](#) للحصول على مزيد من المعلومات.

معلومات ذات صلة

- [أجهزة الأمان المعدلة ASA 5500 Series Adaptive Security Appliances](#)
- [مرجع أوامر جهاز الأمان من Cisco](#)
- [جهاز الأمان PIX 500 Series Security Appliance](#)
- [إشعارات وتوجيهات أمان Cisco](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل