PIX/ASA 7.x والإصدارات الأحدث: منع حركة مرور (P2P) من نظير إلى نظير للبيانات والمراسلة الفورية (IM) باستخدام مثال تكوين MPF

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين أجهزة الأمان Cisco PIX/ASA باستخدام إطار عمل السياسة النمطية (MPF) لحظر حركة مرور البيانات من نظير إلى نظير (P2P) والمراسلة الفورية (IM)، مثل MSN Messenger و Yahoo Messenger، من الشبكة الداخلية إلى الإنترنت. كما يوفر هذا المستند معلومات حول كيفية تكوين PIX/ASA للسماح للمضيفين باستخدام تطبيقات IM بينما تظل باقي الأجهزة المضيفة محظورة.

ملاحظة: يمكن أن يقوم ASA بحظر تطبيقات النوع P2P فقط إذا كان يتم إنشاء قنوات لحركة مرور البيانات P2P عبر HTTP. كما يمكن أن تسقط ASA حركة مرور P2P إذا تم إنشاء قنوات لها من خلال HTTP.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند تكوين جهاز أمان Cisco وأنه يعمل بشكل صحيح.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من السلسلة Cisco 5500 Series الذي يشغل الإصدار 7.0 من البرنامج والإصدارات الأحدث.

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

المنتجات ذات الصلة

كما يمكن إستخدام هذا التكوين مع جدار حماية Cisco 500 Series PIX الذي يشغل الإصدار 7.0 من البرنامج والإصدارات الأحدث.

الاصطلاحات

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

نظرة عامة على إطار عمل السياسة النمطية

توفر ميزة "حماية مستوى الإدارة (MPF)" طريقة متناسقة ومرنة لتكوين ميزات جهاز الأمان. على سبيل المثال، يمكنك إستخدام ميزة "حماية مستوى الإدارة (MPF)" لإنشاء تكوين مهلة محدد لتطبيق TCP معين، بدلا من واحد ينطبق على جميع تطبيقات TCP.

تدعم ميزة "حماية مستوى الإدارة (MPF)" الميزات التالية:

- تطبيع TCP، وحدود اتصال TCP و UDP، وحالات انتهاء المهلة، وترقيم رقم تسلسل TCP عشوائيا
- CSC
- فحص التطبيق
- IPS
- وضع سياسات إدخال جودة الخدمة
- وضع سياسات إخراج جودة الخدمة
- قائمة انتظار أولوية جودة الخدمة

يتكون تكوين ميزة "حماية مستوى الإدارة (MPF)" من أربع مهام:

1. قم بتعريف حركة مرور الطبقة 3 و 4 التي تريد تطبيق العمليات عليها. راجع تحديد حركة المرور باستخدام خريطة فئة الطبقة 4/3 للحصول على مزيد من المعلومات.
2. (فحص التطبيق فقط) حدد الإجراءات الخاصة لحركة مرور فحص التطبيق. راجع تكوين الإجراءات الخاصة لتفتيش التطبيقات للحصول على مزيد من المعلومات.
3. تطبيق إجراءات على حركة مرور الطبقة 3 و 4. راجع تحديد الإجراءات باستخدام خريطة سياسة الطبقة 4/3 للحصول على مزيد من المعلومات.
4. قم بتنشيط الإجراءات على واجهة. راجع تطبيق سياسة الطبقة 4/3 على واجهة تستخدم سياسة الخدمة للحصول على مزيد من المعلومات.

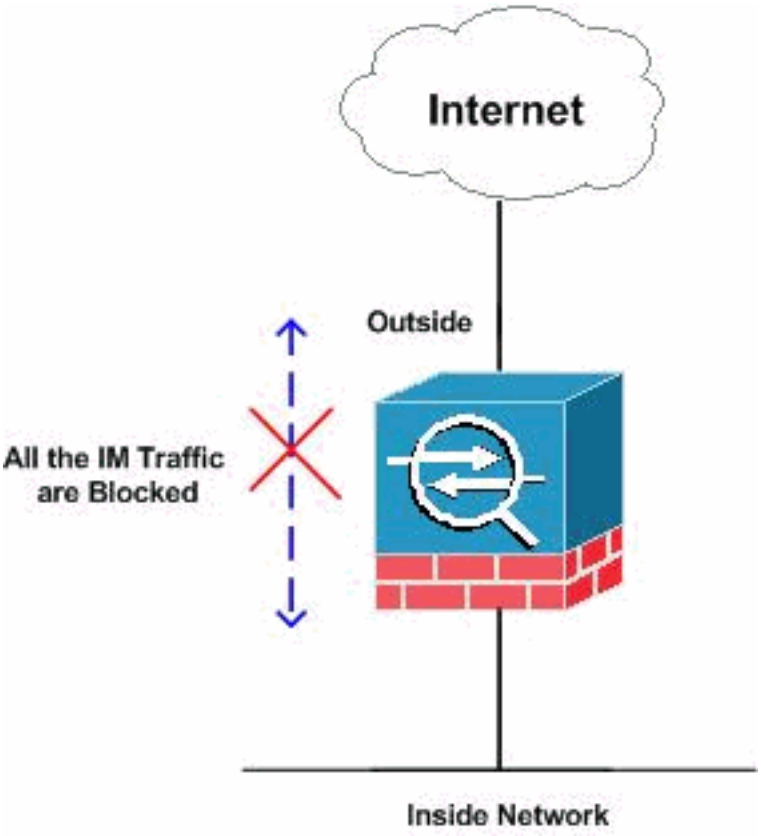
تكوين حظر حركة مرور بيانات المراسلة الفورية و P2P

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



التكوين 7.0 و 7.1 ل PIX/ASA

حظر تكوين حركة مرور بيانات P2P و IM ل PIX/ASA 7.0 و 7.1

```
CiscoASA#show run
Saved :
:
(ASA Version 7.1(1
!
hostname CiscoASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!

Output Suppressed http-map inbound_http ---!
 content-length min 100 max 2000 action reset log
 content-type-verification match-req-rsp action reset
log
 max-header-length request 100 action reset log
 max-uri-length 100 action reset log
 port-misuse p2p action drop
 port-misuse im action drop
 port-misuse default action allow

The http-map "inbound_http" inspects the http ---!
traffic !--- as per various parameters such as content
 length, header length, !--- url-length as well as
 matches the P2P & IM traffic and drops them. ! !---
Output Suppressed ! class-map inspection_default match
 default-inspection-traffic class-map http-port
```

```
                                                match port tcp eq www

    The class map "http-port" matches !--- the http ---!
          traffic which uses the port 80. ! ! policy-map
      global_policy class inspection_default inspect dns
maximum-length 512 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 policy-map
                                                  inbound_policy
                                                   class http-port
                                             inspect http inbound_http

   The policy map "inbound_policy" matches !--- the ---!
   http traffic using the class map "http-port" !--- and
drops the IM traffic as per http map !--- "inbound_http"
          inspection. ! service-policy global_policy global
                service-policy inbound_policy interface inside

  Apply the policy map "inbound_policy" !--- to the ---!
                                                inside interface.
   Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
                                                        #CiscoASA
```

ارجع إلى قسم تكوين خريطة HTTP للتحكم في الفحص الإضافي في دليل تكوين سطر أوامر Cisco Security Appliance للحصول على مزيد من المعلومات حول الأمر **http map** والمعلمات المختلفة المقترنة به.

PIX/ASA 7.2 والتكوين اللاحق

ملاحظة: يتم إهمال الأمر **http-map** من الإصدار 7.2 من البرنامج والإصدارات الأحدث. لذلك، يلزمك إستخدام الأمر **policy-map type inspection im** لحظر حركة مرور IM.

حظر تكوين حركة مرور بيانات P2P و IM ل PIX/ASA 7.2 والإصدارات الأحدث

```
                                        CiscoASA#show running-config
                                                          Saved :
                                                              :
                                                  (ASA Version 8.0(2
                                                              !
                                                 hostname pixfirewall
                                enable password 8Ry2YjIyt7RRXU24 encrypted
                                                           names


    Output Suppressed class-map inspection_default ---!
     match default-inspection-traffic class-map imblock
                                                     match any

  The class map "imblock" matches !--- all kinds of ---!
                                                  traffic. class-map P2P
                                                match port tcp eq www

  The class map "P2P" matches !--- http traffic. ! ---!
  policy-map type inspect dns preset_dns_map parameters
  message-length maximum 512 policy-map type inspect im
                                                       impolicy
                                                     parameters
                                  match protocol msn-im yahoo-im
                                                drop-connection
```

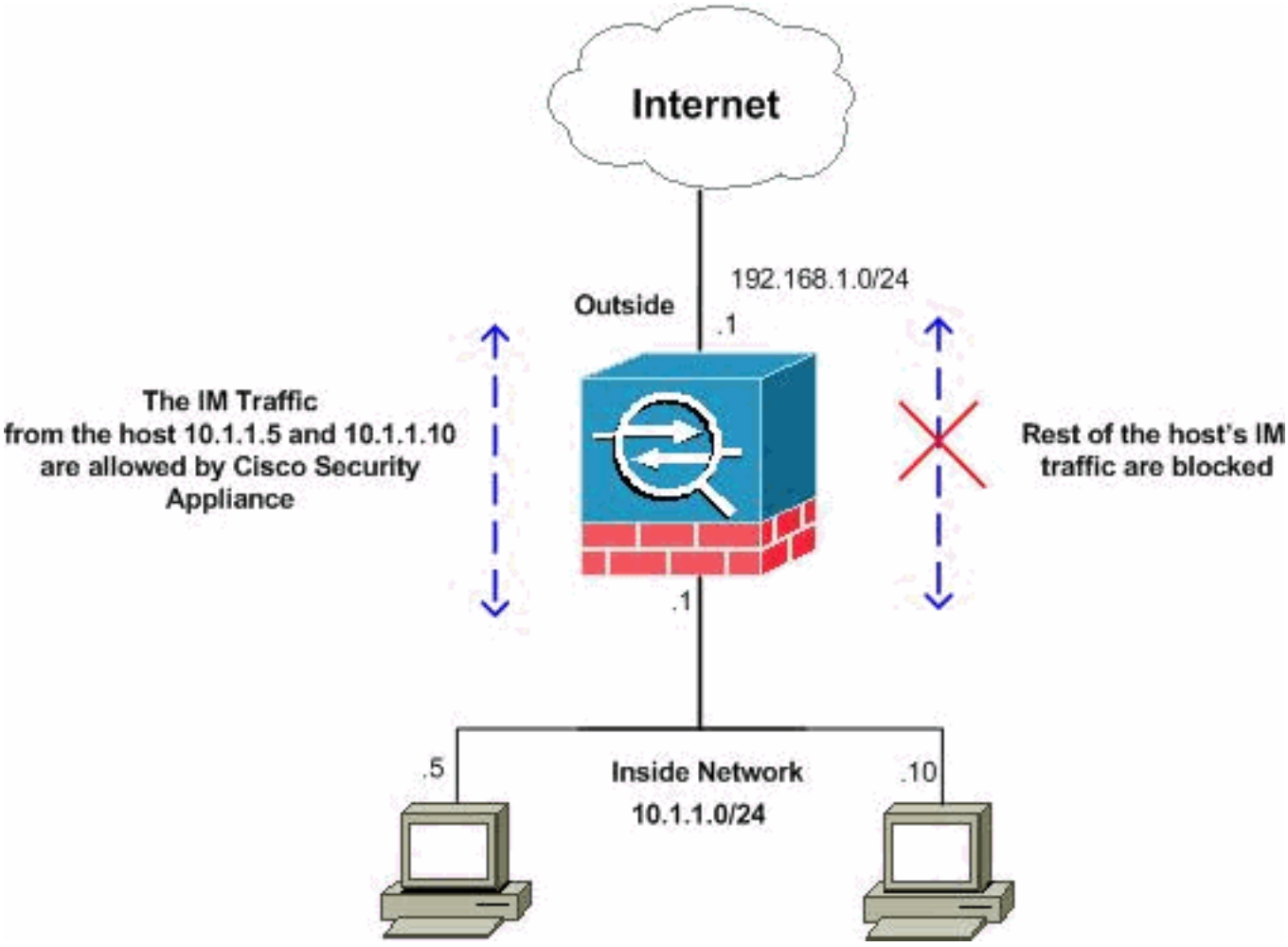
```
The policy map "impolicy" drops the IM !--- traffic ---!
   such as msn-im and yahoo-im . policy-map type inspect
                                                http P2P_HTTP
                                                  parameters
                                  match request uri regex _default_gator
                                                drop-connection log
                          match request uri regex _default_x-kazaa-network
                                                drop-connection log

          The policy map "P2P_HTTP" drops the P2P !--- ---!
          traffic that matches the some built-in reg exp's.
                                              policy-map IM_P2P
                                                 class imblock
                                              inspect im impolicy
                                                    class P2P
                                            inspect http P2P_HTTP


     The policy map "IM_P2P" drops the !--- IM traffic ---!
          matched by the class map "imblock" as well as P2P
             traffic matched by class map "P2P". policy-map
        global_policy class inspection_default inspect dns
      preset_dns_map inspect ftp inspect h323 h225 inspect
         h323 ras inspect netbios inspect rsh inspect rtsp
       inspect skinny inspect esmtp inspect sqlnet inspect
sunrpc inspect tftp inspect sip inspect xdmcp ! service-
         policy global_policy global service-policy IM_P2P
                                                interface inside

     Apply the policy map "IM_P2P" !--- to the inside ---!
                              interface. prompt hostname context
     Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
                                                      #CiscoASA
```

قائمة التعبيرات المنتظمة المضمنة

```
                "regex _default_GoToMyPC-tunnel "machinekey
      "regex _default_GoToMyPC-tunnel_2 "[/\\]erc[/\\]Poll
                    "regex _default_yahoo-messenger "YMSG
        regex _default_httport-tunnel "photo[.]exectech[-
                                                  "]va[.]com
  "regex _default_gnu-http-tunnel_uri "[/\\]index[.]html
       "regex _default_firethru-tunnel_1 "firethru[.]com
                              "regex _default_gator "Gator
            regex _default_firethru-tunnel_2 "[/\\]cgi[-
                                                "]bin[/\\]proxy
          "regex _default_shoutcast-tunneling-protocol "1
        "regex _default_http-tunnel "[/\\]HT_PortLog.aspx
                    regex _default_x-kazaa-network "[xX]-
      "[[kK][aA][zZ][aA][aA]-[nN][eE][tT][wW][oO][rR][kK
                              regex _default_msn-messenger
"[Aa][Pp][Pp][Ll][Ii][Cc][Aa][Tt][Ii][Oo][Nn][/\\][Xx][-
                                          [-][][Mm][Ss][Nn
                    "[Mm][Ee][Ss][Ss][Ee][Nn][Gg][Ee][Rr]
                              regex _default_aim-messenger
"[Hh][Tt][Tt][Pp][.][Pp][Rr][Oo][Xx][Yy][.][Ii][Cc][Qq][
                                          "[.][Cc][Oo][Mm
                "regex _default_gnu-http-tunnel_arg "crap
              regex _default_icy-metadata "[iI][cC][yY]-
                        "[[mM][eE][tT][aA][dD][aA][tT][aA
   "regex _default_windows-media-player-tunnel "NSPlayer
```

PIX/ASA 7.2 والإصدارات الأحدث: السماح للمضيفين باستخدام حركة مرور IM

يستعمل هذا قسم هذا شبكة setup:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هذا rfc 1918 عنوان، أي يتلقى يكون استعملت في مختبر بيئة.

إذا كنت ترغب في السماح بحركة مرور IM من العدد المحدد من البيئات المضيفة، فأنت بحاجة إلى إكمال هذا التكوين كما هو موضح. في هذا المثال، يتم السماح للمضيفين 10.1.1.5 و 10.1.1.10 من الشبكة الداخلية باستخدام تطبيقات المراسلة الفورية مثل MSN Messenger و Yahoo Messenger. ومع ذلك، لا يزال غير مسموح بحركة مرور IM من البيئات المضيفة الأخرى.

تكوين حركة مرور IM ل PIX/ASA 7.2 والإصدارات الأحدث للسماح بمضيفين
CiscoASA#**show running-config** Saved : : (ASA Version 8.0(2 ! hostname pixfirewall enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0 nameif inside security-level 100 ip address 10.1.1.1 255.255.255.0

```
!
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.1.1 255.255.255.0
!

Output Suppressed passwd 2KFQnbNIdI.2KYOU encrypted ---!
 ftp mode passive access-list 101 extended deny ip host
 10.1.1.5 any
 access-list 101 extended deny ip host 10.1.1.10 any
 access-list 101 extended permit ip any any

The ACL statement 101 is meant for deny the IP !--- ---!
 traffic from the hosts 10.1.1.5 and 10.1.1.10 !---
 whereas it allows the rest of the hosts. pager lines 24
 mtu inside 1500 mtu outside 1500 no failover icmp
 unreachable rate-limit 1 burst-size 1 no asdm history
 enable arp timeout 14400 timeout xlate 3:00:00 timeout
 conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp
0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00
 mgcp 0:05:00 mgcp-pat timeout sip 0:30:00 sip_media
 0:02:00 sip-invite 0:03:00 sip-disconnect timeout uauth
 0:05:00 absolute dynamic-access-policy-record
 DfltAccessPolicy no snmp-server location no snmp-server
 contact snmp-server enable traps snmp authentication
linkup linkdown coldstart no crypto isakmp nat-traversal
telnet timeout 5 ssh timeout 5 console timeout 0 threat-
 detection basic-threat threat-detection statistics
 access-list ! class-map type inspect im match-all im-
 traffic
 match protocol msn-im yahoo-im

 The class map "im-traffic" matches all the IM ---!
 traffic !--- such as msn-im and yahoo-im. class-map
 im_inspection
 match access-list 101

 The class map "im_inspection" matches the access ---!
list !--- number 101. 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 policy-map
 type inspect im im-policy
 parameters
 class im-traffic
 drop-connection log

 The policy map "im-policy" drops and logs the !--- ---!
IM traffic such as msn-im and yahoo-im. policy-map impol
 class im_inspection
 inspect im im-policy

The policy map "impol" inspects the IM traffic !--- ---!
as per traffic matched by the class map "im_inspection".
!--- So, it allows the IM traffic from the host 10.1.1.5
 !--- and 10.1.1.10 whereas it blocks from rest. !
service-policy global_policy global service-policy impol
 interface inside
```

```
Apply the policy map "impol" to the inside !--- ---!
interface. prompt hostname context
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e : end
```

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show running-config http-map**— يعرض خرائط HTTP التي تم تكوينها.

```
CiscoASA#show running-config http-map http-policy
!
http-map http-policy
 content-length min 100 max 2000 action reset log
 content-type-verification match-req-rsp reset log
 max-header-length request bytes 100 action log reset
 max-uri-length 100 action reset log
!
```

- **show running-config policy-map**— يعرض جميع تكوينات خريطة السياسة بالإضافة إلى تكوين خريطة السياسة الافتراضي.

```
CiscoASA#show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map type inspect im impolicy
 parameters
  match protocol msn-im yahoo-im
   drop-connection
policy-map imdrop
 class imblock
  inspect im impolicy
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
```

يمكنك أيضا إستخدام الخيارات في هذا الأمر كما هو موضح هنا:

```
| show running-config [all] policy-map [policy_map_name
                                [[type inspect [protocol
```

```
CiscoASA#show running-config policy-map type inspect im
!
policy-map type inspect im impolicy
```

```
                                parameters
                    match protocol msn-im yahoo-im
                                  drop-connection
                                                !
```

- **show running-config class-map**— يعرض المعلومات حول تكوين خريطة الفئة.

```
CiscoASA#show running-config class-map
                                                !
                                    class-map inspection_default
                                match default-inspection-traffic
                                            class-map imblock
                                                  match any
```

- **show running-config service-policy**—يعرض جميع تكوينات نهج الخدمة الجاري تشغيلها حاليا.

```
CiscoASA#show running-config service-policy
                                service-policy global_policy global
                            service-policy imdrop interface outside
```

- **show running-config access-list**— يعرض تكوين قائمة الوصول التي يتم تشغيلها على جهاز الأمان.

```
CiscoASA#show running-config access-list
                    access-list 101 extended deny ip host 10.1.1.5 any
                    access-list 101 extended deny ip host 10.1.1.10 any
                            access-list 101 extended permit ip any any
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

- **debug im**— يعرض رسائل تصحيح الأخطاء لحركة مرور IM.
- **show service-policy**— يعرض سياسات الخدمة التي تم تكوينها.

```
CiscoASA#show service-policy interface outside

                                        :Interface outside
                                  Service-policy: imdrop
                                    Class-map: imblock
                    Inspect: im impolicy, packet 0, drop 0, reset-drop 0
```

- **show access-list**— يعرض العدادات الخاصة بقائمة الوصول.

```
                                        CiscoASA#show access-list
            (access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096
                                               alert-interval 300
                                                  access-list 101; 3 elements
        access-list 101 line 1 extended deny ip host 10.1.1.5 any (hitcnt=0) 0x7ef4dfbc
        access-list 101 line 2 extended deny ip host 10.1.1.10 any (hitcnt=0) 0x32a50197
                access-list 101 line 3 extended permit ip any any (hitcnt=0) 0x28676dfa
```

معلومات ذات صلة

- صفحة دعم ASA سلسلة Cisco 5500
- صفحة دعم أجهزة الأمان Cisco PIX 500 Series Security Appliances
- 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).