فحص إتصالات SMTP و ESMTP باستخدام ميزة حماية جدار Cisco IOS مماثل تكوين

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين فحص إتصالات بروتوكول نقل البريد البسيط الوارد (SMTP) أو بروتوكول نقل البريد البسيط الموسع (ESMTP) باستخدام جدار حماية Cisco IOS® في Cisco IOS. وهذا الفحص مماثل لميزة MailGuard الموجودة في أجهزة الأمان Cisco PIX 500 Series Security Appliances.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

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

- برنامج IOS الإصدار 12.3(4)T من Cisco أو إصدار أحدث
- موجّه Cisco 3640

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.

الاصطلاحات

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

معلومات أساسية

يتسبب فحص SMTP في فحص أوامر SMTP بحثا عن أوامر غير قانونية. يتم تعديل الحزم التي تحتوي على أوامر غير قانونية إلى نمط "xxxx" وإعادة توجيهها إلى الخادم. تتسبب هذه العملية في إرسال الخادم ردا سلبيا، مما يفرض على العميل إصدار أمر صالح. أمر SMTP غير قانوني هو أي أمر ماعدا هذه الأوامر:

• البيانات • هيلو • المساعدة • البريد • نوب • إنهاء	• RCPT • RSET • سامل • إرسال • سومل • VRFY

يعمل فحص ESMTP بنفس الطريقة التي يعمل بها فحص SMTP. يتم تعديل الحزم ذات الأوامر غير القانونية إلى نمط "xxxx" وإعادة توجيهها إلى الخادم، مما يؤدي إلى تشغيل رد سلبي. أمر ESMTP غير قانوني هو أي أمر ماعدا هذه الأوامر:

• AUTH • البيانات • إهلو • إترن • هيلو • المساعدة • المساعدة • البريد	• نوب • إنهاء • RCPT • RSET • سامل • إرسال • سومل • VRFY

يفحص فحص ESMTP أيضا هذه الامتدادات من خلال فحص أوامر أعمق:

- تعريف حجم الرسالة (الحجم)
- إقرار معالجة قائمة الانتظار البعيدة (ETRN)
- MIME ثنائي (ثنائي محارم)
- أمر جزائي
- المصادقة
- إعلام حالة التسليم (DSN)
- رمز الحالة المحسن (ENHANCEDSTATUSuscode)
- تقنية MIMEtransport بمعدل 8 بت (8BITMIME)

ملاحظة: لا يمكن تكوين فحص SMTP و ESMTP في نفس الوقت. أدت محاولة تكوين كلا النتيجتين إلى ظهور رسالة خطأ.

ملاحظة: في الإصدار 12.3(4)T من البرنامج Cisco IOS Software والإصدارات الأحدث، لم يعد جدار حماية Cisco IOS يعمل على إنشاء إدخالات قائمة وصول ديناميكية للسماح بحركة المرور. يحتفظ جدار حماية Cisco IOS الآن بجدول حالة جلسة عمل للتحكم في أمان الاتصالات التي تم فحصها.

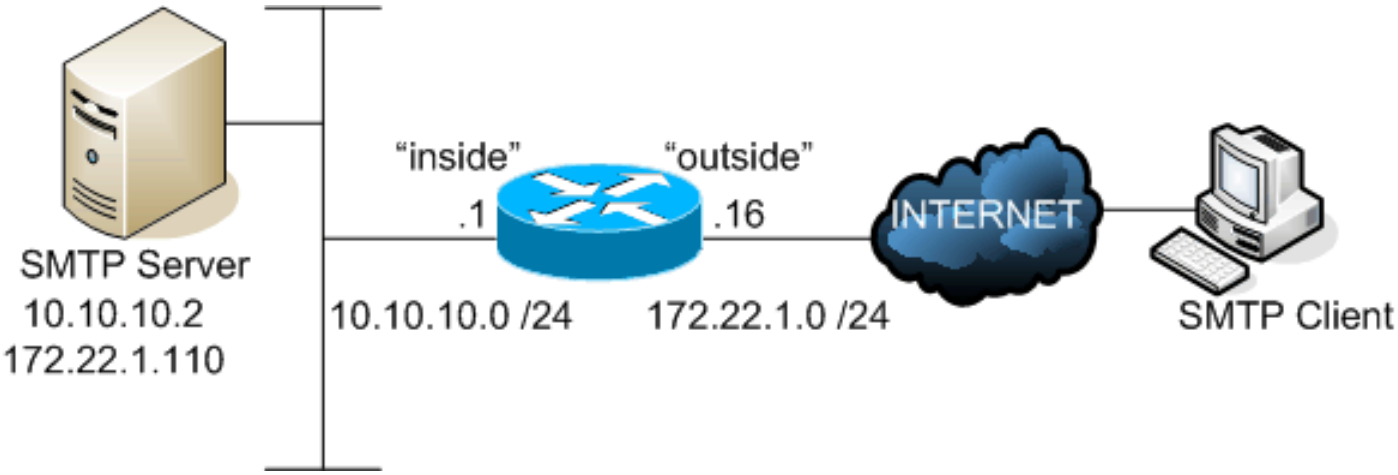
التكوين

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:



التكوينات

يستعمل هذا وثيقة هذا تشكيل:

الموجه 3640

```
3640-123#show running-config
...Building configuration

Current configuration : 1432 bytes
!
version 12.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 3640-123
!
boot-start-marker
boot-end-marker
!
enable password 7 02050D4808095E731F
!
no aaa new-model
!
resource policy
!
voice-card 3
!
ip subnet-zero
!
!
ip cef
no ip dhcp use vrf connected
!
!
```

```
This is the Cisco IOS Firewall configuration. !--- ---!
IN-OUT is the inspection rule for traffic that flows !--
- from the inside interface of the router to the outside
   interface. ip inspect name IN-OUT tcp ip inspect name
   IN-OUT udp ip inspect name IN-OUT ftp ip inspect name
  IN-OUT http ip inspect name IN-OUT icmp !--- OUT-IN is
the inspection rule for traffic that flows !--- from the
outside interface of the router to the inside interface.
        !--- This rule is where SMTP/ESMTP inspection is
specified. ip inspect name OUT-IN smtp ! no ip ips deny-
 action ips-interface ! no ftp-server write-enable ! ! !
! controller T1 3/0 framing sf linecode ami ! ! ! ! ! !-
      -- The outside interface. interface Ethernet2/0 ip
 address 172.22.1.16 255.255.255.0 !--- Apply the access
  list to permit SMTP/ESMTP connections !--- to the mail
     server. This also allows Cisco IOS Firewall !--- to
  inspect SMTP or ESMTP commands. ip access-group 101 in
    ip nat outside !--- Apply the inspection rule OUT-IN
   inbound on this interface. This is !--- the rule that
  defines SMTP/ESMTP inspection. ip inspect OUT-IN in ip
 virtual-reassembly half-duplex ! interface Serial2/0 no
        ip address shutdown ! !--- The inside interface.
             interface Ethernet2/1 ip address 10.10.10.1
   255.255.255.0 ip nat inside !--- Apply the inspection
rule IN-OUT inbound on this interface. ip inspect IN-OUT
in ip virtual-reassembly half-duplex ! ip http server no
     ip http secure-server ip classless ip route 0.0.0.0
  0.0.0.0 172.22.1.1 ! ! !--- The static translation for
 the mail server. ip nat inside source static 10.10.10.2
     172.22.1.110 ip nat inside source static 10.10.10.5
  172.22.1.111 ! !--- The access list to permit SMTP and
       ESMTP to the mail server. !--- Cisco IOS Firewall
   inspects permitted traffic. access-list 101 permit tcp
 any host 172.22.1.110 eq smtp ! ! ! control-plane ! ! !
voice-port 1/0/0 ! voice-port 1/0/1 ! voice-port 1/1/0 !
  voice-port 1/1/1 ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 password 7 121A0C0411045D5679 login ! ! 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 ip inspection all**—يتحقق من تكوين قواعد فحص جدار حماية Cisco IOS وتطبيقها على الواجهات.

```
3640-123#show ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
[max-incomplete sessions thresholds are [400:500
.max-incomplete tcp connections per host is 50. Block-time 0 minute
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
Inspection name IN-OUT
tcp alert is on audit-trail is off timeout 3600
udp alert is on audit-trail is off timeout 30
ftp alert is on audit-trail is off timeout 3600
```

```
                http alert is on audit-trail is off timeout 3600
                  icmp alert is on audit-trail is off timeout 10
                                                Inspection name OUT-IN
        smtp max-data 20000000 alert is on audit-trail is off timeout 3600

                                                Interface Configuration
                                                 Interface Ethernet2/1
                                        Inbound inspection rule is IN-OUT
                  tcp alert is on audit-trail is off timeout 3600
                    udp alert is on audit-trail is off timeout 30
                  ftp alert is on audit-trail is off timeout 3600
                http alert is on audit-trail is off timeout 3600
                  icmp alert is on audit-trail is off timeout 10
                                    Outgoing inspection rule is not set
                                         Inbound access list is not set
                                       Outgoing access list is not set
                                                 Interface Ethernet2/0
                                        Inbound inspection rule is OUT-IN
        smtp max-data 20000000 alert is on audit-trail is off timeout 3600
                                    Outgoing inspection rule is not set
                                            Inbound access list is 101
                                       Outgoing access list is not set
```

- **debug ip inspection smtp**—يعرض الرسائل المتعلقة بأحداث فحص SMTP لجدار حماية Cisco IOS.**ملاحظة:** ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

```
ausnml-3600-02#debug ip inspect smtp
INSPECT SMTP Inspection debugging is on
ausnml-3600-02#
Oct 18 21:51:35.886: CBAC SMTP: reply_type OTHERS*
Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY - Reply len: 64, match_len:64,*
                                                reply_re_state:18
Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:13*
Oct 18 21:51:35.886: CBAC SMTP: OTHER REPLY match id:10*
Oct 18 21:51:35.886: CBAC SMTP: End Of Reply Line - index:0 ,len:64*

        The client issues a command. *Oct 18 21:51:40.810: CBAC SMTP: VERB - Cmd len:1, ---!
 match_len:1, cmd_re_state:9 *Oct 18 21:51:40.994: CBAC SMTP: VERB - Cmd len:2, match_len:1,
             cmd_re_state:24 *Oct 18 21:51:41.190: CBAC SMTP: VERB - Cmd len:3, match_len:1,
             cmd_re_state:40 *Oct 18 21:51:41.390: CBAC SMTP: VERB - Cmd len:4, match_len:1,
    cmd_re_state:56 *Oct 18 21:51:41.390: CBAC SMTP: VERB - match id:5 *Oct 18 21:51:42.046:
    CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7 *Oct 18 21:51:43.462: CBAC
   SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2 *Oct 18 21:51:43.594: CBAC SMTP:
     CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2 *Oct 18 21:51:43.794: CBAC SMTP: CMD
 PARAM - Cmd len:9, match_len:2, cmd_re_state:2 *Oct 18 21:51:43.994: CBAC SMTP: CMD PARAM -
    Cmd len:10, match_len:1, cmd_re_state:2 *Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - Cmd
 len:12, match_len:2, cmd_re_state:3 *Oct 18 21:51:44.194: CBAC SMTP: CMD PARAM - match id:6
      *Oct 18 21:51:44.194: CBAC SMTP: End Of Command Line - index:1, len:12 !--- The server
replies. *Oct 18 21:51:44.198: CBAC SMTP: reply_type OTHERS *Oct 18 21:51:44.198: CBAC SMTP:
     OTHER REPLY - Reply len: 11, match_len:11, reply_re_state:18 *Oct 18 21:51:44.198: CBAC
 SMTP: OTHER REPLY match id:13 *Oct 18 21:51:44.198: CBAC SMTP: OTHER REPLY match id:10 *Oct
    18 21:51:44.198: CBAC SMTP: End Of Reply Line - index:1 ,len:11 !--- The client issues a
command. *Oct 18 21:51:49.482: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:3 *Oct
          18 21:51:50.222: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:15 *Oct 18
             21:51:50.618: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:31 *Oct 18
             21:51:50.954: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:46 *Oct 18
21:51:50.954: CBAC SMTP: VERB - match id:15 *Oct 18 21:51:51.642: CBAC SMTP: CMD PARAM - Cmd
  len:5, match_len:1, cmd_re_state:7 *Oct 18 21:51:51.914: CBAC SMTP: CMD PARAM - Cmd len:6,
        match_len:1, cmd_re_state:2 *Oct 18 21:51:52.106: CBAC SMTP: CMD PARAM - Cmd len:7,
        match_len:1, cmd_re_state:2 *Oct 18 21:51:54.754: CBAC SMTP: CMD PARAM - Cmd len:8,
        match_len:1, cmd_re_state:4 *Oct 18 21:51:55.098: CBAC SMTP: CMD PARAM - Cmd len:9,
       match_len:1, cmd_re_state:2 *Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - Cmd len:11,
 match_len:2, cmd_re_state:3 *Oct 18 21:51:55.322: CBAC SMTP: CMD PARAM - match id:6 *Oct 18
21:51:55.322: CBAC SMTP: End Of Command Line - index:2, len:11 !--- The server replies. *Oct
18 21:51:55.326: CBAC SMTP: reply_type OTHERS *Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY -
```

Reply len: 19, match_len:19, reply_re_state:3 *Oct 18 21:51:55.326: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:51:55.326: CBAC SMTP: End Of Reply Line - index:2 ,len:19 *Oct 18 21:51:57.070: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:3 *Oct 18 21:51:57.402: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:15 *Oct 18 21:51:58.162: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:31 *Oct 18 21:51:58.462: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:46 *Oct 18 21:51:58.466: CBAC SMTP: VERB - match id:15 *Oct 18 21:51:58.746: CBAC SMTP: CMD PARAM - Cmd len:5, match_len:1, cmd_re_state:7 *Oct 18 21:51:59.006: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:1, cmd_re_state:2 *Oct 18 21:51:59.234: CBAC SMTP: CMD PARAM - Cmd len:7, match_len:1, cmd_re_state:2 *Oct 18 21:51:59.418: CBAC SMTP: CMD PARAM - Cmd len:9, match_len:2, cmd_re_state:2 *Oct 18 21:51:59.618: CBAC SMTP: CMD PARAM - Cmd len:10, match_len:1, cmd_re_state:2 *Oct 18 21:51:59.818: CBAC SMTP: CMD PARAM - Cmd len:12, match_len:2, cmd_re_state:3 *Oct 18 21:51:59.818: CBAC SMTP: CMD PARAM - match id:6 *Oct 18 21:51:59.818: CBAC SMTP: End Of Command Line - index:3, len:12 *Oct 18 21:51:59.818: CBAC SMTP: reply_type OTHERS *Oct 18 21:51:59.818: CBAC SMTP: OTHER REPLY - Reply len: 19, match_len:19, reply_re_state:3 *Oct 18 21:51:59.822: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:51:59.822: CBAC SMTP: End Of Reply Line - index:3 ,len:19 *Oct 18 21:52:04.974: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:9 *Oct 18 21:52:05.170: CBAC SMTP: VERB - Cmd len:2, match_len:1, cmd_re_state:24 *Oct 18 21:52:05.326: CBAC SMTP: VERB - Cmd len:3, match_len:1, cmd_re_state:40 *Oct 18 21:52:05.526: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:55 *Oct 18 21:52:05.526: CBAC SMTP: VERB - match id:6 *Oct 18 21:52:05.742: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:2, cmd_re_state:3 *Oct 18 21:52:05.742: CBAC SMTP: CMD PARAM - match id:6 *Oct 18 21:52:05.742: CBAC SMTP: End Of Command Line - index:4, len:6 *Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 54, match_len:54, reply_re_state:3 *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:4 ,len:54 *Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 15, match_len:15, reply_re_state:3 *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:5 ,len:15 *Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY - Reply len: 15, match_len:15, reply_re_state:3 *Oct 18 21:52:05.746: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.746: CBAC SMTP: End Of Reply Line - index:6 ,len:15 *Oct 18 21:52:05.746: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_state:3 *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:7 ,len:6 *Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 19, match_len:19, reply_re_state:3 *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:8 ,len:19 *Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 17, match_len:17, reply_re_state:3 *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.750: CBAC SMTP: End Of Reply Line - index:9 ,len:17 *Oct 18 21:52:05.750: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_state:3 *Oct 18 21:52:05.750: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:10 ,len:6 *Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_state:3 *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:11 ,len:6 *Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 6, match_len:6, reply_re_state:3 *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:12 ,len:6 *Oct 18 21:52:05.754: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY - Reply len: 3, match_len:3, reply_re_state:3 *Oct 18 21:52:05.754: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:05.754: CBAC SMTP: End Of Reply Line - index:13 ,len:3 *Oct 18 21:52:15.646: CBAC SMTP: VERB - Cmd len:1, match_len:1, cmd_re_state:6 *Oct 18 21:52:15.838: CBAC SMTP: VERB - Cmd len:3, match_len:2, cmd_re_state:37 *Oct 18 21:52:16.206: CBAC SMTP: VERB - Cmd len:4, match_len:1, cmd_re_state:52 *Oct 18 21:52:16.206: CBAC SMTP: VERB - match id:9 *Oct 18 21:52:18.954: CBAC SMTP: CMD PARAM - Cmd len:6, match_len:2, cmd_re_state:3 *Oct 18 21:52:18.958: CBAC SMTP: CMD PARAM - match id:6 *Oct 18 21:52:18.958: CBAC SMTP: End Of Command Line - index:5, len:6 *Oct 18 21:52:18.958: CBAC SMTP: reply_type OTHERS *Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY - Reply len: 21, match_len:21, reply_re_state:18 *Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY match id:13 *Oct 18 21:52:18.958: CBAC SMTP: OTHER REPLY match id:10 *Oct 18 21:52:18.958: CBAC SMTP: End Of Reply Line - index:14 ,len:21

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- الأسئلة المتداولة حول مجموعة ميزات جدار حماية Cisco IOS
- صفحة دعم جدار حماية IOS
- 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).