使用Cisco IOS防火墙允许已知站点的Java程序而拒绝其他的

目录

简介

此示例配置展示了如何使用 Cisco IOS® 防火墙允许来自指定互联网站点的 Java applet 并拒绝所有其他站点的 Java applet。此类阻止会拒绝对未嵌入存档或压缩文件的 Java applet 的访问。Cisco IOS 防火墙是在 Cisco IOS 软件版本 11.3.3.T 和 12.0.5.T 中引入的。只有购买某些特定的功能集之后，才能使用此功能。

您可以使用 Software Advisor 查看支持 IOS 防火墙的 Cisco IOS 功能集（仅限注册用户）。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 1751 路由器
- Cisco IOS 软件版本 c1700-k9o3sy7-mz.123-8.T.bin

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

拒绝来自互联网的 Java Applet

遵循以下步骤：

1. 创建访问控制列表 (ACL)。
2. 将 **ip inspect http java 命令添加到配置。**
3. 将 **ip inspect 和 access-list 命令应用于外部接口。注意：**在本示例中，ACL 3允许来自友好站点(10.66.79.236)的Java小程序，而隐式拒绝来自其他站点的Java小程序。路由器外部所显示的地址无法通过 Internet 进行路由，因为此示例是在实验室中进行配置和测试的。**注意：**如果**使用Cisco IOS软件**版本12.3.4T或更高版本，则不再需要在外部接口上应用访问列表。这部分内容记录在新的防火墙 ACL 绕开功能中。

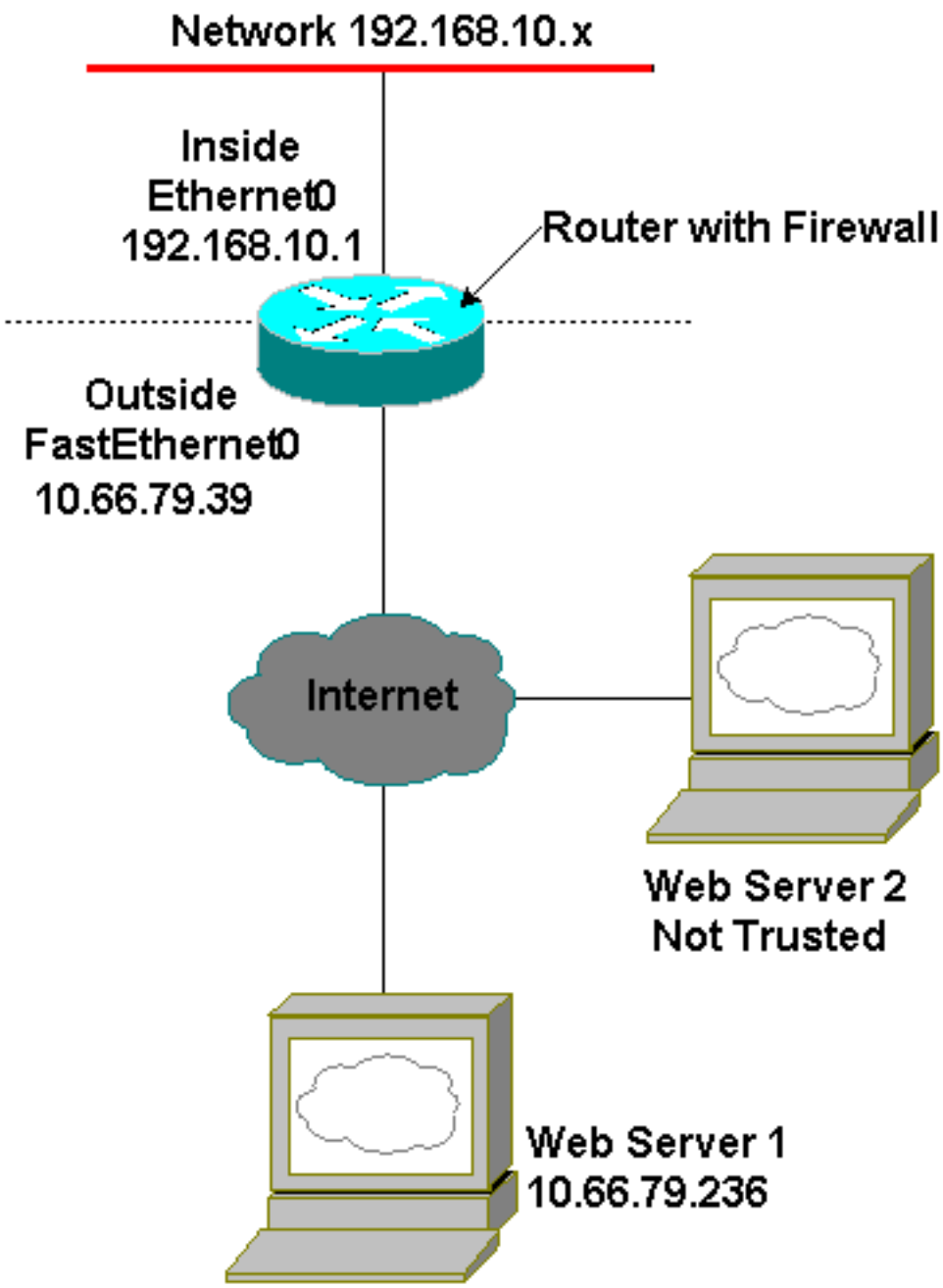
配置

本部分提供了可用于配置本文所述功能的信息。

注：要查找有关本文档使用的命令的其他信息，请参阅命令查找工具(仅注册客户)。

网络图

本文档使用以下网络设置：



配置

本文档使用以下配置：

路由器配置

```
Current configuration : 1224 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Australia
!
boot-start-marker
boot-end-marker
!
```

```
memory-size iomem 15
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
no aaa new-model
ip subnet-zero
!
ip cef
ip inspect name firewall tcp
ip inspect name firewall udp

!--- ACL used for Java. ip inspect name firewall http
java-list 3 audit-trail on
ip ips po max-events 100
no ftp-server write-enable
!
interface FastEthernet0/0
 ip address 10.66.79.39 255.255.255.224

!--- ACL used to block inbound traffic !--- except that
permitted by inspects. !--- This is no longer required
on Cisco IOS Software !--- Release 12.3.4T or later. ip
access-group 100 in
 ip nat outside
 ip inspect firewall out
 ip virtual-reassembly
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface Ethernet1/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 half-duplex
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.66.79.33
no ip http server
no ip http secure-server

!--- ACL used for Network Address Translation (NAT). ip
nat inside source list 1 interface FastEthernet0/0
overload
!

!--- ACL used for NAT. access-list 1 permit 192.168.10.0
0.0.0.255

!--- ACL used for Java. access-list 3 permit
10.66.79.236

!--- ACL used to block inbound traffic !--- except that
permitted by inspects. !--- This is no longer required
on Cisco IOS !--- Software Release 12.3.4T or later.
access-list 100 deny   ip any any
!
!
control-plane
!
```

```
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

验证

本部分提供了可用于确认您的配置是否正常运行的信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

- **show ip inspect sessions [detail]** — 显示 Cisco IOS 防火墙当前跟踪和检查的所有会话。可选关键字 **detail 用于显示有关这些会话的其他信息。**

故障排除

本部分提供了可用于对配置进行故障排除的信息。

故障排除命令

命令输出解释程序工具（仅限注册用户）支持某些 **show 命令，使用此工具可以查看对 show 命令输出的分析。**

注意：在发出debug命**令**之前，请参阅有关debug命令的重要信息。

- **no ip inspect alert-off — 启用 Cisco IOS 防火墙警报消息。**如果配置了 http 拒绝，您可以通过控制台查看它们。
- **debug ip inspect — 显示有关 Cisco IOS 防火墙事件的消息。**

下面是尝试连接到 10.66.79.236 上的 Web 服务器和另一个拥有 Java Applet 的不受信任的站点之后，来自 **debug ip inspect detail 命令的调试输出示例。**

拒绝 Java 日志

```
*Jan 12 21:43:42.919: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2673)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:43.571: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2673).
*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2673) sent 276 bytes
 -- responder (128.138.223.2:80) sent 0 bytes
*Jan 12 21:43:43.575: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2674)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:43.823: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2672) sent 486 bytes
 -- responder (10.66.79.236:80) sent 974 bytes
```

```
*Jan 12 21:43:44.007: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2674).
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2674) sent 276 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.011: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2675)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:44.439: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2675).
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2675) sent 233 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.443: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2676)
 -- responder (128.138.223.2:80)
*Jan 12 21:43:44.879: %FW-3-HTTP_JAVA_BLOCK:
 JAVA applet is blocked from (128.138.223.2:80) to (192.168.10.2:2676).
*Jan 12 21:43:44.879: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2676) sent 233 bytes
 -- responder (128.138.223.2:80) sent 1260 bytes
*Jan 12 21:43:44.899: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2677)
 -- responder (128.138.223.2:80)
```

允许 JAVA 日志

```
Jan 12 21:44:12.143: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2685)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:12.343: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2686)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:17.343: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2685) sent 626 bytes
 -- responder (10.66.79.236:80) sent 533 bytes
*Jan 12 21:44:17.351: %FW-6-SESS_AUDIT_TRAIL:
 Stop http session: initiator (192.168.10.2:2686) sent 314 bytes
 -- responder (10.66.79.236:80) sent 126 bytes
*Jan 12 21:44:23.803: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2687)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:27.683: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2691)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.411: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2692)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.451: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2693)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.463: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2694)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.475: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2695)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.487: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2696)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.499: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2697)
 -- responder (10.66.79.236:80)
```

```
*Jan 12 21:44:28.515: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2698)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.527: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2699)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.543: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2700)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:28.551: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2701)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.075: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2734)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.135: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2735)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.155: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2736)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.159: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2737)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.215: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2739)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.231: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2740)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.251: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2742)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.395: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2747)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.403: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2748)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:29.423: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2749)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.091: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2798)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.095: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2799)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.115: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2800)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.119: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2801)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.123: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2802)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.191: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2803)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.219: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2804)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.399: %FW-6-SESS_AUDIT_TRAIL_START:
```

```
 Start http session: initiator (192.168.10.2:2805)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.411: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2806)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:30.423: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2807)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.103: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2843)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.115: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2844)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.127: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2845)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.139: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2846)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.147: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2847)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.159: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2848)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.171: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2849)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.183: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2850)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.195: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2851)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:31.203: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2852)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.107: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2908)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.123: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2909)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.143: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2910)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.163: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2911)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.175: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2912)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.187: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2913)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.199: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2914)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.211: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2915)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.223: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2916)
```

```
 -- responder (10.66.79.236:80)
*Jan 12 21:44:32.235: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2917)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.151: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2982)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.163: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2983)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.175: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2984)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.187: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2985)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.199: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2986)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.211: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2987)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.223: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2988)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.235: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2989)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.251: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2990)
 -- responder (10.66.79.236:80)
*Jan 12 21:44:33.259: %FW-6-SESS_AUDIT_TRAIL_START:
 Start http session: initiator (192.168.10.2:2991)
 -- responder (10.66.79.236:80)
```

相关信息

- IOS防火墙支持页面
- 基于上下文的访问控制：简介和配置
- 改善 Cisco 路由器的安全性
- 技术支持和文档 - Cisco Systems