使用Cisco IOS防火牆允許來自已知站點的Java Applet，同時拒絕其他站點

目錄

簡介

此示例配置演示如何使用Cisco IOS®防火牆允許來自指定Internet站點的Java小程式並拒絕所有其他程式。這種型別的阻止會拒絕訪問未嵌入到存檔或壓縮檔案中的Java applet。Cisco IOS防火牆是在Cisco IOS軟體版本11.3.3.T和12.0.5.T中引入的。只有在購買了某些功能集時，才會出現該功能。

您可以使用Software Advisor（僅限註冊客戶）檢視哪些Cisco IOS功能集支援IOS防火牆。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科1751路由器
- Cisco IOS軟體版本c1700-k9o3sy7-mz.123-8.T.bin

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

拒絕來自Internet的Java Applet

請遵循以下步驟：

1. 建立存取控制清單(ACL)。
2. 將**ip inspect http java**命令新增到配置。
3. 對外部介面應用**ip inspect**和**access-list**命令。**注意：**在本示例中，ACL 3允許來自友好站點(10.66.79.236)的Java Applet，但隱式拒絕來自其他站點的Java Applet。路由器外部顯示的地址不能通過Internet路由，因為此示例是在實驗室中配置和測試的。**注意：**如果使用Cisco IOS軟體版本12.3.4T或更高版本，則無需在外部介面上應用訪問清單。此功能記錄在新的防火牆ACL繞過功能中。

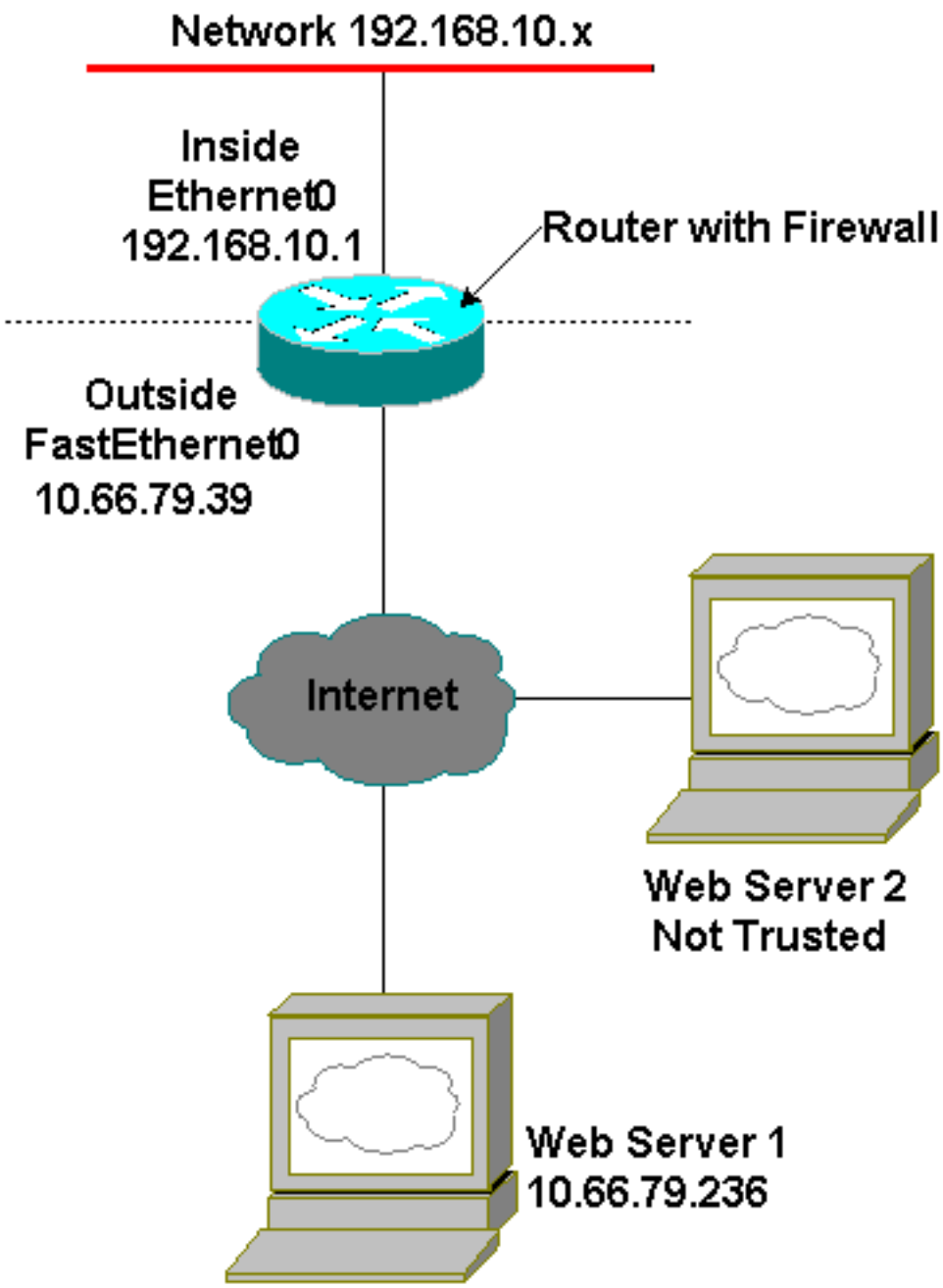
設定

本節提供可用於設定本檔案中所述功能的資訊。

注意：要查詢有關本文檔使用的命令的更多資訊，請參閱命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

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
```

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

- **show ip inspect sessions** ***[detail]*** — 顯示Cisco IOS防火牆目前追蹤和檢查的現有作業階段。可選關鍵字**detail**顯示有關這些作業階段的其他資訊。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

注意：發出debug指令之前，請參閱有關Debug指令的重要資訊。

- **no ip inspect alert-off** — 啟用Cisco IOS防火牆警報消息。如果配置了http拒絕，則可以從控制檯檢視它們。
- **debug ip inspect** — 顯示有關Cisco IOS防火牆事件的消息。

嘗試連線到10.66.79.236上的Web伺服器和另一個具有Java小程式（如ACL中所定義）的非受信任站點後，**debug ip inspect detail**命令的輸出示例如下。

Java拒絕日誌

```
*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)
```

JAVA允許的日誌

```
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)
```

相關資訊

- IOS防火牆支援頁面
- 內容型存取控制：簡介和配置
- 提高Cisco路由器的安全性
- 技術支援與文件 - Cisco Systems