配置ZBFW高可用性並對其進行故障排除

目錄

簡介

本指南提供用於主用/備用設定的區域防火牆高可用性(HA)的基本配置，以及故障排除命令和功能中出現的常見問題。

Cisco IOS®區域型防火牆(ZBFW)支援HA，因此可以在主用/備用或主用/主用設定中配置兩台Cisco IOS路由器。這樣可允許冗餘，以防止單點故障。

必要條件

需求

您必須擁有高於Cisco IOS軟體版本15.2(3)T的版本。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

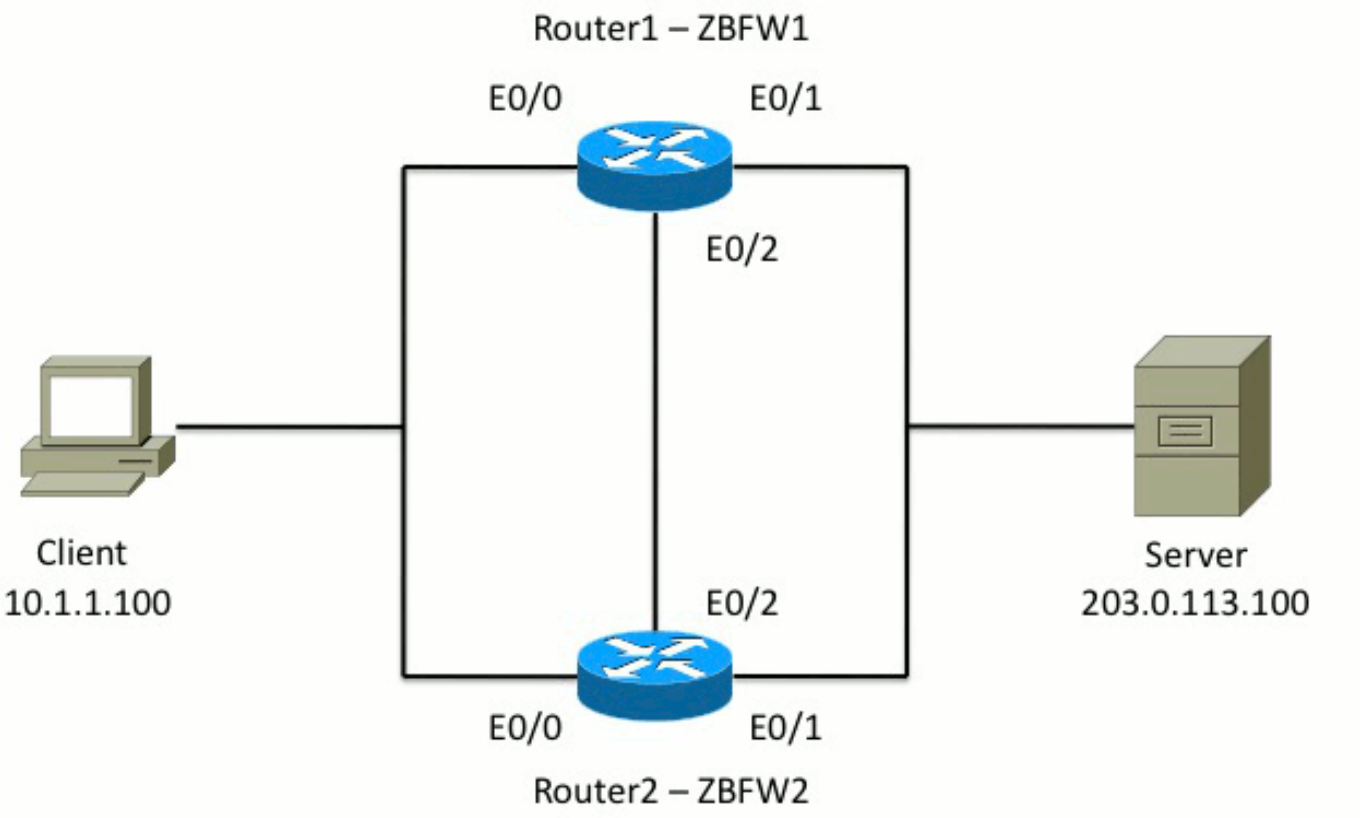
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

此圖顯示配置示例中使用的拓撲。



在範例1所示的組態中，設定ZBFW是為了檢查TCP、UDP和網際網路控制訊息通訊協定(ICMP)從內部到外部的流量。粗體顯示的配置設定HA功能。在Cisco IOS路由器中，HA是通過**redundancy** subconfig命令配置的。為了配置冗餘，第一步是在全域性檢查引數對映中啟用冗餘。

啟用冗餘後，輸入**application redundancy**子配置，然後選擇用於**控制**和**資料**的介面。控制介面用於

交換有關每台路由器狀態的資訊。資料介面用於交換有關應複製的連線的資訊。

在範例2中，如果路由器1和路由器2均正常運行，**priority**命令也會設定為使路由器1成為配對中的活動單元。使用**preempt**命令（在本文檔中還將進一步討論）以確保在優先順序更改後出現故障。

最後一步是將**冗餘介面識別符號(RII)**和**冗餘組(RG)**分配給每個介面。每個介面的**RII**組號必須是唯一的，但是對於同一子網中的介面，它必須在裝置之間匹配。當兩台路由器同步配置時，RII僅用於批次同步過程。這就是兩台路由器同步冗餘介面的方式。**RG**用於指示通過該介面的連線被複製到HA連線表中。

在範例2中，**redundancy group 1**命令用於在內部介面上建立虛擬IP(VIP)位址。這可以確保高可用性，因為所有內部使用者只與活動裝置處理的VIP通訊。

外部介面沒有任何RG配置，因為這是廣域網介面。Router 1和Router 2的外部介面不屬於同一個Internet服務提供商(ISP)。 在外部介面上，需要動態路由協定來確保流量通過正確的裝置。

範例 1：Router 1配置片段（主機名ZBFW1）

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly in
```

```
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
redundancy rii 200
```

範例 2：路由器2配置片段（主機名ZBFW2）

```
parameter-map type inspect global
redundancy
log dropped-packets enable
!
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 200
control Ethernet0/2 protocol 1
data Ethernet0/2
!
class-map type inspect match-any PROTOCOLS
match protocol tcp
match protocol udp
match protocol icmp
class-map type inspect match-all INSIDE_TO_OUTSIDE_CMAP
match class-map PROTOCOLS
match access-group name INSIDE_TO_OUTSIDE_ACL
!
policy-map type inspect INSIDE_TO_OUTSIDE_PMAP
class type inspect INSIDE_TO_OUTSIDE_CMAP
inspect
class class-default
drop
!
ip access-list extended INSIDE_TO_OUTSIDE_ACL
permit ip any any
!
zone security INSIDE
zone security OUTSIDE
zone-pair security INSIDE_TO_OUTSIDE source INSIDE destination OUTSIDE
service-policy type inspect INSIDE_TO_OUTSIDE_PMAP
!
interface Ethernet0/0
ip address 10.1.1.2 255.255.255.0
ip nat inside
ip virtual-reassembly in
zone-member security INSIDE
redundancy rii 100
redundancy group 1 ip 10.1.1.3 exclusive
!
interface Ethernet0/1
ip address 203.0.113.2 255.255.255.0
ip nat outside
ip virtual-reassembly in
zone-member security OUTSIDE
```

```
redundancy rii 200
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

確認裝置之間可以通訊

為了確認裝置可以相互看到，您必須驗證冗餘應用程式組的運行狀態是否為up。然後，確保每台裝置都承擔了正確的角色，並且可以看到其對等裝置的正確角色。在示例3中，ZBFW1處於活動狀態並檢測其對等體為備用。在ZBFW2上則相反。當兩台裝置同時顯示運行狀態為開啟狀態並檢測到其對等體存在時，兩台路由器可以通過控制鏈路成功通訊。

範例 3:對等存在檢測

```
ZBFW1# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: ACTIVE
Peer RF state: STANDBY COLD-BULK
!
ZBFW2# show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
RF state: STANDBY COLD-BULK
Peer RF state: ACTIVE
```

示例4中的輸出顯示了有關兩台路由器的控制介面的更精細輸出。輸出確認用於控制流量的物理介面，還確認對等體的IP地址。

範例 4:精細輸出

```
ZBFW1#  show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.2 Standby RGs: 1 BFD handle: 0

ZBFW1# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
!
ZBFW2# show redundancy application control-interface group 1
The control interface for rg[1] is Ethernet0/2
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.60.1.1 Active RGs: 1 BFD handle: 0

ZBFW2# show redundancy application data-interface group 1
The data interface for rg[1] is Ethernet0/2
```

建立通訊後，示例5中的命令可幫助您瞭解為什麼每台裝置都處於其特定角色。ZBFW1處於活動狀態，因為它具有比其對等體更高的優先順序。ZBFW1的優先順序為200，而ZBFW2的優先順序為150。此輸出以粗體突出顯示。

範例 5：角色狀態和優先順序

```
ZBFW1#  show redundancy application protocol group 1

RG Protocol RG 1
Role: Active
Negotiation: Enabled
Priority: 200
Protocol state: Active
Ctrl Intf(s) state: Up
Active Peer: Local
Standby Peer: address 10.60.1.2, priority 150, intf Et0/2
Log counters:
role change to active: 1
role change to standby: 0
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Active
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 249, Bytes 15438, HA Seq 0, Seq Number 249, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Standby Peer: Present. Hold Timer: 10000
Pkts 237, Bytes 8058, HA Seq 0, Seq Number 252, Pkt Loss 0
```

```
!
ZBFW2# show redundancy application protocol group 1

RG Protocol RG 1
------------------
Role: Standby
Negotiation: Enabled
Priority: 150
Protocol state: Standby-cold
Ctrl Intf(s) state: Up
Active Peer: address 10.60.1.1, priority 200, intf Et0/2
Standby Peer: Local
Log counters:
role change to active: 0
role change to standby: 1
disable events: rg down state 0, rg shut 0
ctrl intf events: up 1, down 0, admin_down 0
reload events: local request 0, peer request 0

RG Media Context for RG 1
--------------------------
Ctx State: Standby
Protocol ID: 1
Media type: Default
Control Interface: Ethernet0/2
Current Hello timer: 3000
Configured Hello timer: 3000, Hold timer: 10000
Peer Hello timer: 3000, Peer Hold timer: 10000
Stats:
Pkts 232, Bytes 14384, HA Seq 0, Seq Number 232, Pkt Loss 0
Authentication not configured
Authentication Failure: 0
Reload Peer: TX 0, RX 0
Resign: TX 0, RX 0
Active Peer: Present. Hold Timer: 10000
Pkts 220, Bytes 7480, HA Seq 0, Seq Number 229, Pkt Loss 0
```

最後一次確認是為了確保RII組ID已分配給每個介面。如果在兩台路由器上輸入此命令，則它們會進行雙重檢查，以確保裝置之間同一子網上的介面對分配了相同的RII ID。如果沒有使用相同的唯一RII ID配置連線，則連線不會在兩個裝置之間複製。請參見示例6。

範例 6：確認已分配RII組ID

```
ZBFW1# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200           0
Ethernet0/0 : 100           0
!
ZBFW2# show redundancy rii
No. of RIIs in database: 2
Interface RII Id decrement
Ethernet0/1 : 200           0
Ethernet0/0 : 100           0
```

驗證連線是否複製到對等路由器

在示例7中，ZBFW1主動傳遞連線流量。連線已成功複製到備用裝置ZBFW2。若要檢視區域防火牆

處理的連線，請使用show policy-firewall session命令。

範例 7：已處理的連線

```
ZBFW1#show policy-firewall session
Session B2704178 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:31, Last heard 00:00:30
Bytes sent (initiator:responder) [37:79]
HA State: ACTIVE, RG ID: 1
Established Sessions = 1

ZBFW2#show policy-firewall session
Session B2601288 (10.1.1.100:52980)=>(203.0.113.100:23) tcp
SIS_OPEN/TCP_ESTAB
Created 00:00:51, Last heard never
Bytes sent (initiator:responder) [0:0]
HA State: STANDBY, RG ID: 1
Established Sessions = 1
```

請注意，連線會複製，但傳輸的位元組不會更新。通過資料介面定期更新連線狀態（TCP資訊），以確保發生故障轉移事件時不會影響流量。

如需更精細的輸出，請輸入show policy-firewall session zone-pair <ZP> ha 指令。它提供的輸出與示例7類似，但它允許使用者將輸出限製為僅指定區域對。

收集調試輸出

本節介紹用於產生相關輸出的debug命令，以便對此功能進行疑難排解。

在繁忙的路由器上，啟用調試可能非常困難。因此，在啟用這些功能之前，您應該先瞭解其影響。

- debug redundancy application group rii event

  此命令用於確保連線與正確複製的RII組匹配。當流量到達ZBFW時，將檢查源介面和目標介面的RII組ID。然後，此資訊將通過資料鏈路傳輸到對等體。當備用對等體的RII組與活動單元對齊時，生成示例8中的系統日誌，並確認用於複製連線的RII組ID:

  範例 8：系統日誌

  ```
  debug redundancy application group rii event
  debug redundancy application group rii error
  !
  *Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:100
  *Feb 1 21:13:01.378: [RG-RII-EVENT]: get idb: rii:200
  ```

- debug redundancy application group protocol all

  此命令是用來確認兩個對等點是否可看到彼此。對等IP地址在調試中確認。如示例9所示，ZBFW1看到其對等體處於IP地址為10.60.1.2的備用狀態。對於ZBFW2，情況正好相反。

範例 9：確認調試中的對等IP

```
debug redundancy application group protocol all
!
ZBFW1#
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Standby,
addr=10.60.1.2, present=exist, reload=0, intf=Et0/2, priority=150.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] set peer_status 0.
*Feb 1 21:35:58.213: RG-PRTCL-MEDIA: [RG 1] [Active/Active] priority_event
'media: low priority from standby', role_event 'no event'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] select fsm event,
priority_event=media: low priority from standby, role_event=no event.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] process FSM event
'media: low priority from standby'.
*Feb 1 21:35:58.213: RG-PRTCL-EVENT: [RG 1] [Active/Active] no FSM transition

ZBFW2#
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: RG Media event, rg_id=1, role=Active,
addr=10.60.1.1, present=exist, reload=0, intf=Et0/2, priority=200.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot]
set peer_status 0.
*Feb 1 21:36:02.283: RG-PRTCL-MEDIA: [RG 1] [Standby/Standby-hot] priority_event
'media: high priority from active', role_event 'no event'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] select
fsm event, priority_event=media: high priority from active, role_event=no event.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] process
FSM event 'media: high priority from active'.
*Feb 1 21:36:02.283: RG-PRTCL-EVENT: [RG 1] [Standby/Standby-hot] no FSM
transition
```

常見問題

本節詳細介紹遇到的一些常見問題。

控制和資料介面選擇

以下是控制和資料VLAN的一些提示：

- 請勿在ZBFW配置中包括控制介面和資料介面。它們僅用於相互通訊；因此，無需保護這些介面。
- 控制介面和資料介面可以位於同一介面或VLAN上。這會保留路由器上的埠。

缺席RII組

RII組必須應用於LAN和WAN介面。LAN介面必須位於同一子網中，但WAN介面可以位於不同的子網中。如果介面上沒有RII組，則在**debug redundancy application group rii event**和**debug redundancy application group rii error**的輸出中會出現此系統日誌：

```
000515: Dec 20 14:35:07.753 EST: FIREWALL*: RG not found for ID 0
```

自動容錯移轉

為了配置自動故障轉移，必須配置ZBFW HA以跟蹤服務級別協定(SLA)對象，並根據此SLA事件動態降低優先順序。在示例10中，ZBFW HA跟蹤GigabitEthernet0介面的鏈**路狀**態。如果此介面關閉，優先順序會降低，以便更青睞對等裝置。

範例 10：ZBFW HA自動故障切換配置

```
redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 230
control Vlan801 protocol 1
data Vlan801
track 1 decrement 200
!
track 1 interface GigabitEthernet0 line-protocol

redundancy
application redundancy
group 1
name ZBFW_HA
preempt
priority 180
control Vlan801 protocol 1
data Vlan801
```

有時ZBFW HA不會自動進行故障切換，即使出現優先順序降低事件也是如此。這是因為兩台裝置都沒有設定**preempt**關鍵字。**preempt**關鍵字的功能與熱待命路由器協定(HSRP)或自適應安全裝置(ASA)故障轉移中的功能不同。在ZBFW HA中，如果裝置的優先順序發生變化，**preempt**關鍵字允許發生故障切換事件。安全配置指南：基於區域的策略防火牆，Cisco IOS版本15.2M&T。以下是「基於區域的策略防火牆高可用性」一章的摘錄：

「在其他情況下可能會切換到備用裝置。另一個可能導致切換的因素是可以在每台裝置上配置的優先順序設定。具有最高優先順序值的裝置是活動裝置。如果活動或備用裝置發生故障，裝置的優先順序將減少一個可配置的量，稱為權重。如果主用裝置的優先順序低於備用裝置的優先順序，則會發生切換，備用裝置成為主用裝置。可以通過禁用冗餘組的搶佔屬性來覆蓋此預設行為。您也可以將每個介面配置為在介面的第1層狀態關閉時降低優先順序。配置的優先順序會覆蓋冗餘組的預設優先順序。

這些輸出指示正確的狀態：

```
ZBFW01#show redundancy application group 1
Group ID:1
Group Name:ZBFW_HA

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes

RF Domain: btob-one
```

```
RF state: ACTIVE
Peer RF state: STANDBY HOT

ZBFW01#show redundancy application faults group 1
Faults states Group 1 info:
Runtime priority: [230]
RG Faults RG State: Up.
Total # of switchovers due to faults: 0
Total # of down/up state changes due to faults: 0
```

這些日誌是在ZBFW上生成的，未啟用任何調試。此日誌顯示裝置何時變為活動狀態：

```
*Feb  1 21:47:00.579: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
*Feb 1 21:47:09.309: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Standby
to Active
*Feb 1 21:47:19.451: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:19.456: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
```

此日誌顯示裝置何時進入待機狀態：

```
*Feb  1 21:47:07.696: %RG_VP-6-BULK_SYNC_DONE: RG group 1 BULK SYNC to standby
complete.
*Feb 1 21:47:07.701: %RG_VP-6-STANDBY_READY: RG group 1 Standby router is in
SSO state
*Feb 1 21:47:09.310: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from Active
to Init
*Feb 1 21:47:19.313: %RG_PROTOCOL-5-ROLECHANGE: RG id 1 role change from
Init to Standby
```

非對稱路由

非對稱路由支援在非對稱路由支援指南中列出。

要配置非對稱路由，請將功能新增到冗餘應用組全域性配置和介面子配置中。必須注意的是，不能在同一介面上啟用非對稱路由和RG，因為它不受支援。這是因為非對稱路由的工作原理。當介面被指定進行非對稱路由時，它不能作為該點的HA連線複製的一部分，因為路由不一致。配置RG會混淆路由器，因為RG指定介面是HA連線複製的一部分。

範例 11：非對稱路由配置

```
redundancy
application redundancy
group 1
asymmetric-routing interface Ethernet0/3

interface Ethernet0/1
redundancy asymmetric-routing enable
```

此組態必須應用於HA對中的兩台路由器。

前面列出的Ethernet0/3介面是兩台路由器之間的新專用鏈路。此連結專門用於在兩台路由器之間傳遞非對稱路由流量。因此，它應該是相當於面向外部介面的專用鏈路。

相關資訊

- 安全配置指南：基於區域的策略防火牆，Cisco IOS版本15.2M&T
- 基於區域的策略防火牆高可用性安全配置指南
- Cisco IOS 15.2M&T
- Cisco IOS 防火牆
- 安全產品現場通知
- 技術支援與文件 - Cisco Systems