Cisco IOS區域型防火牆：CME/CUE/GW單站點或分支辦公室，通過SIP中繼連線到HQ的CCM

目錄

簡介

思科整合多業務路由器(ISR)提供可擴展的平台，以滿足各種應用的資料和語音網路需求。雖然私有和網際網路連線的網路的威脅環境非常動態，但Cisco IOS®防火牆提供狀態檢測和應用檢測和控制(AIC)功能來定義和執行安全網路狀態，同時支援業務功能和連續性。

本文檔介紹基於Cisco ISR的特定資料和語音應用場景防火牆安全方面的設計和配置注意事項。每個應用場景都提供了語音服務和防火牆的配置。每個場景分別描述VoIP和安全配置，然後是整個路由器配置。您的網路可能需要對服務進行其他配置（例如QoS和VPN），以維護語音品質和保密性。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

IOS防火牆背景

Cisco IOS防火牆通常部署在與裝置防火牆部署模式不同的應用方案中。典型的部署包括遠端工作人員應用程式、小型或分支辦公室站點以及零售應用程式，在這些部署中，需要低裝置數量、多服務整合和更低的效能和安全功能深度。

雖然從成本和運營角度看，防火牆檢查的應用以及ISR產品中的其他整合服務看起來頗具吸引力，但必須評估具體考慮因素以確定基於路由器的防火牆是否合適。如果部署了基於路由器的整合式解決方案，則應用每個附加功能將產生記憶體和處理成本，並可能導致轉發吞吐量降低、資料包延遲增加以及峰值負載期間功能丟失。當您在路由器和裝置之間進行選擇時，請遵循以下准則：

- 啟用多種整合功能的路由器最適合擁有更少裝置的分支機構或遠端辦公站點，能夠提供更好的解決方案。
- 高頻寬、高效能應用通常可以通過裝置更好地解決；必須應用Cisco ASA和Cisco Unified Call Manager Server來處理NAT和安全策略應用以及呼叫處理，同時路由器應滿足QoS策略應用、WAN終止和站點到站點VPN連線要求。

在引入Cisco IOS軟體版本12.4(20)T之前，傳統防火牆和基於區域的策略防火牆(ZFW)無法完全支援VoIP流量和基於路由器的語音服務所需的功能，這需要在其他安全防火牆策略中留出較大差距，以適應語音流量，並且為不斷發展的VoIP信令和媒體協定提供了有限的支援。

部署Cisco IOS基於區域的策略防火牆

Cisco IOS基於區域的策略防火牆與其他防火牆類似，只有在安全策略識別並描述網路的安全要求時，才能提供安全防火牆。制定安全策略有兩種基本方法：*信任*角度，而不是可疑*的*角度。

*trusting*視角假定所有流量都是可信任的，可明確識別為惡意或有害的流量除外。實施特定策略，僅拒絕不需要的流量。這通常通過使用特定的訪問控制項或基於簽名或行為的工具來實現。此方法傾向於較少干擾現有應用程式，但需要全面瞭解威脅和漏洞情況，並需要時刻保持警惕，以便在新的威脅和漏洞出現時加以解決。此外，使用者群必須在維護足夠的安全性方面發揮很大作用。一個允許廣泛的自由而幾乎不控制居住者的環境，為疏忽或惡意的個人造成的問題提供了巨大的機會。此方法的另一個問題是，它更加依賴有效的管理工具和應用控制，這些工具和應用控制可提供足夠的靈活性和效能，以便可以監視和控制所有網路流量中的可疑資料。雖然目前已有技術可以解決這一問題，但運營負擔往往超過大多陣列織的限制。

*suspective*視角假定除明確標識的正常流量外，所有網路流量都是不需*要的*情況。應用的策略會拒

絕所有應用流量，但明確允許的應用流量除外。此外，還可以實施應用檢測和控制(AIC)，以識別和拒絕專門構建的利用良好應用的惡意流*量，以及偽裝為良好流量的不需要*流量。同樣，應用控制會給網路帶來操作和效能上的負擔，儘管大多數不需要的流量必須由無狀態過濾器(如訪問控制清單(ACL)或基於區域的策略防火牆(ZFW)策略)控制，因此AIC、入侵防禦系統(IPS)或其他基於簽名的控制(如靈活資料包匹配(FPM)或基於網路的應用識別(NBAR)必須處理的流量要少得多。 如果僅專門允許所需的應用埠（以及來自已知控制連線或會話的動態媒體特定流量），則網路上存在的唯一不需要的流量必須落入一個特定的、更容易識別的子集中，這降低了為保持對不需要的流量的控制而帶來的工程和操作負擔。

本檔案從*可疑*的角度介紹VoIP安全配置，因此只允許語音網段中允許的流量。資料策略往往更加寬容，如每個應用程式方案配置中的註釋所述。

所有安全策略部署都必須遵循閉環反饋週期；安全部署通常會影響現有應用程式的效能和功能，必須進行調整以儘量減少或解決這種影響。

如果您需要配置基於區域的策略防火牆的其他背景，請檢視區域防火牆設計和應用指南。

VoIP環境中ZFW的注意事項

Zone Firewall Design and Application Guide簡要討論了路由器安全，使用進出路由器自*身區域的安全策略，以及通過各種網路基礎保護(NFP)功能提供的備用功能*。基於路由器的VoIP功能託管在路由器的自*身區域*內，因此保護路由器的安全策略必須瞭解語音流量的要求，以便容納由Cisco Unified CallManager Express發起和發往該平台的語音信令和媒體、Survivable Remote-Site Telephony和語音網關資源。在Cisco IOS軟體版本12.4(20)T之前，傳統防火牆和基於區域的策略防火牆無法完全滿足VoIP流量的要求，因此防火牆策略未進行最佳化以完全保護資源。保護基於路由器的VoIP資源的自分割槽安全策略在很大程度上依賴於12.4(20)T中引入的功能。

IOS防火牆語音功能

Cisco IOS軟體版本12.4(20)T匯入了幾種增強功能，以支援共駐區防火牆和語音功能。以下三個主要功能直接適用於安全語音應用：

- SIP增強功能：應用層網關與應用檢測和控制將SIP版本支援更新為SIPv2，如RFC 3261中所述擴展SIP信令支援以識別更多種的呼叫流引入SIP應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞擴展自區域檢測，以便能夠識別源自本地發往/源自SIP流量的輔助信令和媒體通道
- 支援精簡型本地流量和CME將SCCP支援更新到版本16（以前支援的版本9）引入SCCP應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞擴展自區域檢測，能夠識別由本地發往/源自SCCP流量產生的輔助信令和媒體通道
- 適用於版本3和4的H.323支援將H.323支援更新為版本3和版本4（以前支援的版本1和2）引入H.323應用檢測和控制(AIC)，以應用精細控制來解決特定的應用級漏洞和漏洞

本文所述的路由器安全配置包括這些增強功能提供的功能，並提供了說明策略應用的操作的說明。如果您希望檢視語音檢測功能的完整詳細資訊，請參閱本文檔的相關資訊部分中提供的各個功能文檔的超連結。

注意事項

為了強化前面提到的觀點，應用具有基於路由器的語音功能的Cisco IOS防火牆必須應用基於區域的策略防火牆。傳統IOS防火牆不包括充分支援語音流量的信令複雜性或行為所需的功能。

網路位址轉譯(NAT)

Cisco IOS網路地址轉換(NAT)經常與Cisco IOS防火牆同時配置，尤其是在私有網路必須與Internet介面的情況下，或者如果不同的私有網路必須連線，尤其是在IP地址空間重疊的情況下。Cisco IOS軟體包括適用於SIP、Skinny和H.323的NAT應用層網關(ALG)。理想情況下，無需應用NAT即可實現IP語音的網路連線，因為NAT為故障排除和安全策略應用帶來了額外的複雜性，在使用NAT過載的情況下尤其如此。NAT只能作為解決網路連線問題的最後方案來應用。

Cisco Unified Presence Client(CUPC)

本檔案沒有說明支援將Cisco Unified Presence Client(CUPC)與IOS防火牆一起使用的設定，因為自Cisco IOS軟體版本12.4(20)T1起，區域或傳統防火牆尚未支援CUPC。將來的Cisco IOS軟體版本會支援CUPC。

CME/CUE/GW單站點或分支辦公室，具有SIP中繼到總部或語音提供商的CCM

此方案提供本文檔前面介紹的單站點/分散式呼叫處理/PSTN連線模型（連線到PSTN的CME/CUE/GW單站點或分支辦公室）與本文檔描述的第三個方案中所定義的多站點/集中呼叫處理/融合語音和資料網路之間的折衷。此方案仍使用本地Cisco Unified CallManager Express，但長途撥號和總部/遠端站點電話主要通過站點到站點SIP中繼提供，通過本地PSTN連線進行本地撥號和緊急撥號。即使刪除了大部分傳統PSTN連線，也建議使用基本的PSTN容量來適應基於WAN的收費旁路撥號失敗以及撥號方案所述的本地撥號失敗。此外，本地法律通常要求提供某種型別的本地PSTN連線以適應緊急(911)撥號。此方案採用分散式呼叫處理，提供優勢並遵守Cisco Unified CallManager Express SRND中所述的最佳實踐。

組織可以在以下情況下實施此類應用場景：

- 站點之間使用不同的VoIP環境，但仍需要VoIP來代替長途PSTN。
- 撥號方案管理需要逐個站點的自主權。
- 無論WAN是否可用，都需要完整的呼叫處理功能。

場景背景

該應用場景包含有線電話（語音VLAN）、有線PC（資料VLAN）和無線裝置（包括VoIP裝置，如IP Communicator）。

安全配置提供以下功能：

1. CME和本地電話（SCCP和SIP）以及CME和遠端CUCM集群(SIP)之間的路由器啟動的信令檢查。
2. 用於在這些裝置之間通訊的語音媒體針孔：本地有線和無線網段CME和MoH的本地電話CUE和本地語音郵件電話電話和遠端呼叫實體
3. 應用檢測與控制(AIC)，可用於實現以下目標：速率限制邀請消息確保所有SIP流量的協定一致性

優點/缺點

此應用具有成本降低的優勢，因為它在WAN資料鏈路上傳輸站點到站點語音流量。

此方案的缺點是需要更詳細的WAN連線計畫。站點到站點呼叫品質可能受WAN上許多因素的影響，例如非法/不需要的流量（蠕蟲、病毒、點對點檔案共用），或者難以識別由於運營商網路上的流量工程而導致的延遲問題。WAN連線的規模必須適當，以便為語音和資料流量提供足夠的頻寬；對延遲不太敏感的資料流量（例如電子郵件、SMB/CIFS檔案流量）可以歸類為QoS的低優先順序流量，以保持語音品質。

此方案的另一個問題是缺乏集中式呼叫處理，以及排除呼叫處理故障時可能出現的困難。因此，此方案最適合作為向集中式呼叫處理遷移的中間步驟的大型組織。當完成向Cisco CallManager的遷移時，可將本地Cisco CME轉換為功能齊全的SRST回退。

從安全形度看，此環境日益增加的複雜性使有效的安全實施和故障排除變得更加困難，因為通過WAN或公共Internet上的VPN進行連線會顯著增加威脅環境，尤其是在安全策略需要信任視角的情況下，這種情況下對通過WAN的流量幾乎沒有任何限制。考慮到這一點，本文檔提供的配置示例實施了一個更可疑的*策略，該策略允許特定的關鍵業務流量，然後由協定一致性檢查檢查該流量*。此外，具體的VoIP操作（即SIP INVITE）也受到限制，以減少惡意或無意軟體故障的可能性，從而對VoIP資源和可用性產生負面影響。

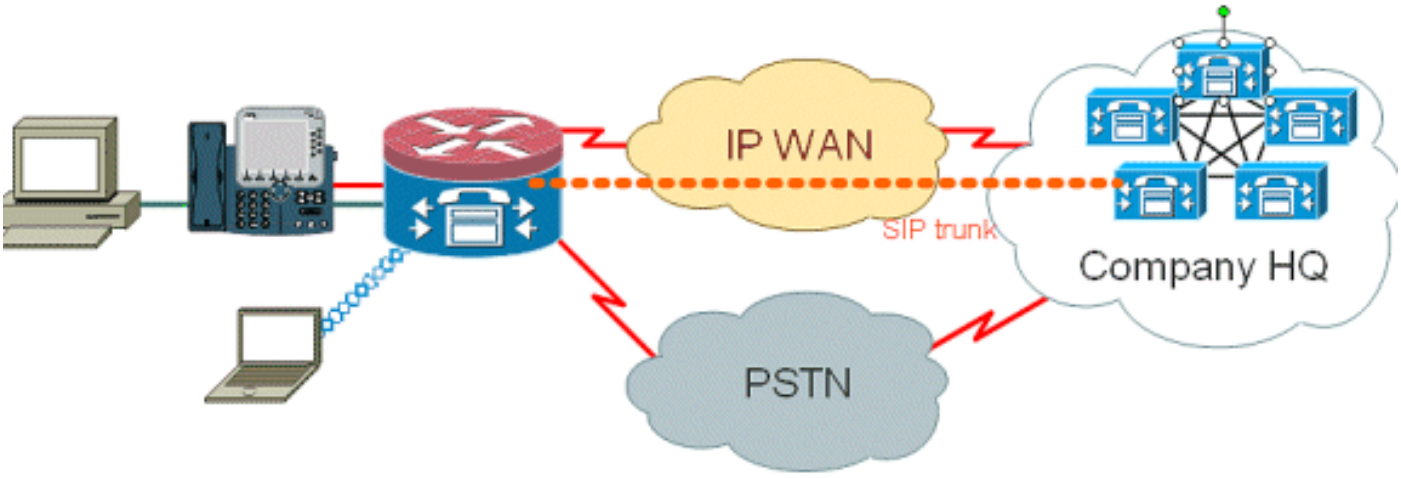
設定

資料策略、基於區域的防火牆、語音安全、CCME的配置

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用以下網路設定：



組態

此處描述的配置說明了Cisco 2851整合多業務路由器。

本檔案會使用以下設定：

- CME和CUE連線的語音服務配置
- 基於區域的策略防火牆配置
- 安全配置

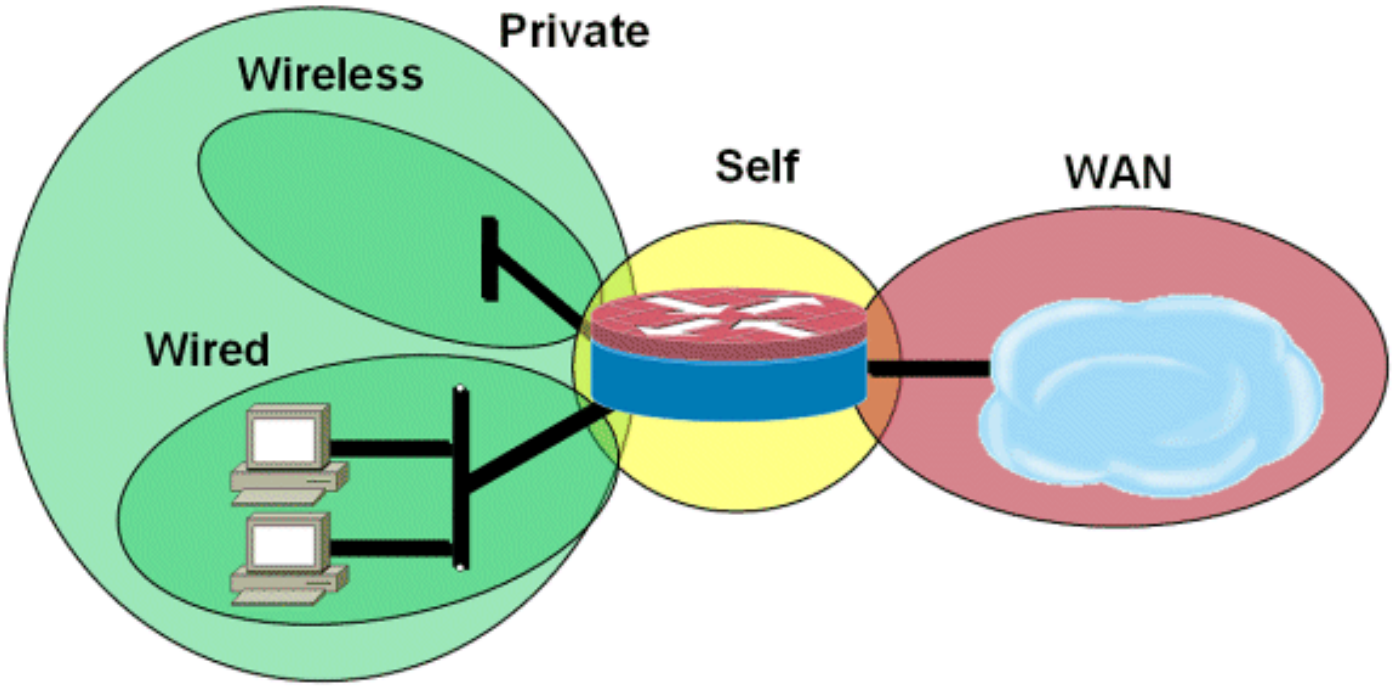
這是CME和CUE連線的語音服務配置：

CME和CUE連線的語音服務配置

```
!
telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp 7960 Jun 10 2008 15:47:13

!
```

這是基於區域的策略防火牆配置，由有線和無線LAN網段的安全區域、專用LAN（由有線和無線網段組成）、可達到可信WAN連線的WAN網段以及路由器語音資源所在的自身區域組成：



以下是安全組態：

安全配置

```
class-map type inspect match-all acl-cmap
match access-group 171
class-map type inspect match-any most-traffic-cmap
match protocol tcp
match protocol udp
match protocol icmp
match protocol ftp
!
!
policy-map type inspect most-traffic-pmap
class type inspect most-traffic-cmap
inspect
class class-default
drop
```

```
policy-map type inspect acl-pass-pmap
class type inspect acl-cmap
pass
 !
zone security private
zone security public
zone security wired
zone security wireless
!
zone-pair security priv-pub source private destination public
service-policy type inspect most-traffic-pmap
zone-pair security priv-vpn source private destination vpn
service-policy type inspect most-traffic-pmap
zone-pair security acctg-pub source acctg destination public
service-policy type inspect most-traffic-pmap
zone-pair security eng-pub source eng destination public
service-policy type inspect most-traffic-pmap
!
!
!
interface GigabitEthernet0/0
ip virtual-reassembly
zone-member security eng

Entire router configuration:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2851-cme2
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring

!
dot11 syslog
ip source-route

!
!
ip cef
no ip dhcp use vrf connected

!
ip dhcp pool pub-112-net
network 172.17.112.0 255.255.255.0
default-router 172.17.112.1
dns-server 172.16.1.22
option 150 ip 172.16.1.43
domain-name bldrtme.com

!

ip dhcp pool priv-112-net
network 192.168.112.0 255.255.255.0
default-router 192.168.112.1
dns-server 172.16.1.22
```

```
domain-name bldrtme.com
option 150 ip 192.168.112.1

!
!
ip domain name yourdomain.com

!

no ipv6 cef
multilink bundle-name authenticated

!
!
!
!

voice translation-rule 1
rule 1 // /1001/

!
!

voice translation-profile default
translate called 1

!
!

voice-card 0
no dspfarm

!
!
!
!
!

interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 172.16.112.10 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto

!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
 !
interface GigabitEthernet0/1.132
encapsulation dot1Q 132
ip address 172.17.112.1 255.255.255.0

!

interface GigabitEthernet0/1.152
encapsulation dot1Q 152
ip address 192.168.112.1 255.255.255.0
ip nat inside
ip virtual-reassembly
```

```
!

interface FastEthernet0/2/0

!

interface FastEthernet0/2/1

!

interface FastEthernet0/2/2

!

interface FastEthernet0/2/3

!

interface Vlan1
ip address 198.41.9.15 255.255.255.0

!

router eigrp 1
network 172.16.112.0 0.0.0.255
network 172.17.112.0 0.0.0.255
no auto-summary
!

ip forward-protocol nd
ip http server ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:/gui

 !!

ip nat inside source list 111 interface
GigabitEthernet0/0 overload

!

access-list 23 permit 10.10.10.0 0.0.0.7
access-list 111 deny
ip 192.168.112.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.112.0 0.0.0.255 any

!
!
!
!
!
!tftp-server flash:/phone/7940-7960/
P00308000400.bin alias P00308000400.bin
tftp-server flash:/phone/7940-7960/
P00308000400.loads alias P00308000400.loads
tftp-server flash:/phone/7940-7960/
P00308000400.sb2 alias P00308000400.sb2
tftp-server flash:/phone/7940-7960/
P00308000400.sbn alias P00308000400.sbn

!
```

```
control-plane

!
!
!

voice-port 0/0/0
connection plar 3035452366
description 303-545-2366
caller-id enable

!

voice-port 0/0/1 description FXO

!

voice-port 0/1/0
description FXS

!

voice-port 0/1/1 description FXS


!
!
!
!
!
dial-peer voice 804 voip
destination-pattern 5251...
session target ipv4:172.16.111.10
!
dial-peer voice 50 pots
destination-pattern A0
port 0/0/0
no sip-register

!
!
!
!

telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp
7960 Jun 10 2008 15:47:13

 !!

ephone-dn 1
number 1001
trunk A0

!
!
```

```
ephone-dn 2
number 1002

!
!
ephone-dn 3
number 3035452366
label 2366
trunk A0

!
!

ephone 1
device-security-mode none
mac-address 0003.6BC9.7737
type 7960
button 1:1 2:2 3:3

!
!
!

ephone 2
device-security-mode none
mac-address 0003.6BC9.80CE
type 7960
button 1:2 2:1 3:3

!
!
!

ephone 5
device-security-mode none

!
!
!

line con 0
exec-timeout 0 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh

line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh

!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp server 172.16.1.1
end
```

調配、管理和監控

Cisco Configuration Professional通常最能滿足基於路由器的IP電話資源和基於區域的策略防火牆的調配和配置。Cisco Secure Manager不支援基於區域的策略防火牆或基於路由器的IP電話。

Cisco IOS經典防火牆支援使用Cisco統一防火牆MIB進行SNMP監控，但統一防火牆MIB中尚不支援基於區域的策略防火牆。因此，必須通過路由器命令列介面上的統計資訊或GUI工具（如Cisco Configuration Professional）處理防火牆監控。

思科安全監控和報告系統(CS-MARS)為基於區域的策略防火牆提供基本支援，儘管在12.4(15)T4/T5和12.4(20)T中實施的日誌記錄更改改進了日誌消息與流量的關聯，但CS-MARS尚未完全支援。

容量計畫

印度防火牆通話檢查效能測試結果待定。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

Cisco IOS Zone Firewall提供**show**和**debug**命令，以檢視、監控防火牆的活動並對此進行故障排除。本節介紹如何使用**show**命令監控基本防火牆活動，以及區域防火牆的**debug**命令簡介以對您的配置進行疑難排解，或者與技術支援人員的討論是否需要更多詳細資訊。

疑難排解指令

Cisco IOS防火牆提供多個**show**命令來檢視安全策略配置和活動。這些命令中的許多命令都可以通過**alias**命令的應用替換為較短的命令。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

Debug命令在您使用非典型或不受支援的組態且需要與Cisco TAC或其他產品的技術支援服務合作以解決互通性問題時可能有用。

注意：對特定功能或流量應用**debug**命令可能會導致大量控制檯消息，從而導致路由器控制檯無響應。即使您需要調試，您也可以提供替代命令列介面訪問，例如不監視終端對話方塊的Telnet視窗。僅在離線（實驗室環境）裝置上或在計畫的維護視窗中啟用調試，因為調試會顯著影響路由器效能。

相關資訊

- Cisco Unified CallManager Express解決方案參考網路設計手冊
- Cisco CallManager Express安全最佳實踐(CME SRND)
- 將Cisco Unity Connection與Cisco Unified CME-as-SRST整合
- Cisco Unified Communications Manager Express命令參考
- Cisco CallManager Express/Cisco Unity Express配置示例
- Cisco CallManager Express 3.4 SNMP MIB支援

- 基於區域的策略防火牆設計和應用指南
- Cisco IOS防火牆：SIP增強功能：ALG和AIC
- 軟體Cisco IOS防火牆H.323支援
- 適用於精簡型本地流量和CME的Cisco IOS防火牆支援
- 技術支援與文件 - Cisco Systems