基于 Cisco IOS 区域的防火墙：通过 SIP 中继到总部 CCM 的 CME/CUE/GW 单站点或分支机构

目录

简介

Cisco 集成服务路由器 (ISR) 为满足各种应用程序的数据和语音网络需求提供了一个可扩展的平台。虽然私有网络和互联网连接网络的威胁形势是一个非常动态的环境，但Cisco IOS®防火墙提供状态检测和应用检测与控制(AIC)功能来定义和实施安全网络状态，同时支持业务功能和连续性。

本文描述特定Cisco基于ISR的数据和语音应用方案的防火墙安全方面的设计和配置注意事项。提供了针对每个应用方案的语音服务和防火墙配置。每个方案分别描述 VoIP 和安全配置，后跟整个路由器配置。您的网络可能需要配置其他服务（如 QoS 和 VPN）以保持语音质量和机密性。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

IOS 防火墙背景

Cisco IOS 防火墙通常部署在不同于设备防火墙部署模式的应用方案中。典型的配置包括远程操作人员应用、小型或分行办公室站点和零售应用，非常需要低设备多个服务计数、集成和更低性能和安全功能。

虽然从成本和操作角度来看，将防火墙检查和 ISR 产品中的其他集成服务一起应用可能很有吸引力，但是必须评估一些特定的考虑事项以确定基于路由器的防火墙是否是适用的。如果部署一个动力不足的基于集成路由器的解决方案，则应用每个附加功能都会导致内存和处理成本增加，并可能导致转发吞吐率降低、数据包延迟增加，以及峰值负载时段内的功能损失。在路由器和设备之间做出选择时，请遵循以下准则：

- 支持多个集成功能的路由器最适合少量设备可提供更佳解决方案的分支机构或远程办公人员场所。
- 使用设备通常可以更好地处理高带宽、高性能的应用程序；必须应用 Cisco ASA 和 Cisco Unified Call Manager Server 来处理 NAT 和安全策略应用和呼叫处理，而使用路由器来处理 QoS 策略应用、WAN 终端和站点到站点 VPN 连接需求。

在引入 Cisco IOS 软件版本 12.4(20)T 以前，传统防火墙和基于区域的策略防火墙 (ZFW) 无法完全支持 VoIP 数据流和基于路由器的语音服务所需的功能，这些功能需要安全防火墙策略中的巨大间隙来容纳语音数据流，并只能提供对不断发展的 VoIP 信令和媒体协议的有限支持。

部署 Cisco IOS 基于区域的策略防火墙

如果网络的安全要求由安全策略确定并描述，则 Cisco IOS 基于区域的策略防火墙与其他防火墙一样只能提供一个安全防火墙。有两个到达安全策略的基本途径：*信任 角度，与怀疑角度相对。*

*信任 角度假设，除可以专门标识为恶意数据流或不需要的数据流以外的所有数据流都可信。*将实施一个仅拒绝不需要的数据流的特定策略。这通常通过使用特定访问控制条目或基于签名或基于行为的工具实现。此方法倾向于较少干预现有应用程序，但需要全面了解威胁和漏洞环境，并需要经常保持警惕以在新的威胁和漏洞出现时进行处理。此外，用户社区在维护足够的安全性方面必须起到很大的作用。允许很大自由度、只对占用者进行很少控制的环境为粗心或恶意个人引起的问题提供了大量机会。此方法的另一个问题是它更依赖于提供足够的灵活性和性能以能够监视和控制所有网络数据流中的可疑数据的有效管理工具和应用程序控制。当目前的技术可以适应这些时，操作的负担会频繁地超出多数组织的极限。

*怀疑 角度假设，除专门标识的良好数据流以外的所有网络数据流都是不需要的。*它是一个应用后将拒绝除明确允许的数据流以外所有应用程序数据流的策略。此外，可以实施应用程序检查和控制 (AIC) 来标识和拒绝专门为了利用*良好 应用程序而生成的恶意数据流，以及伪装成良好数据流的不需要的数据流。*应用程序控制又会在网络上施加操作和性能负担，然而大多数不需要的数据流必须受控于无状态过滤器（如访问控制列表 (ACL) 或基于区域的策略防火墙 (ZFW) 策略），因此，必须由 AIC、入侵防御系统 (IPS) 或其他基于签名的控制（如灵活数据包匹配 (FPM) 或基于网络的应用程序识别 (NBAR)）处理的数据流实质上就非常少了。 如果只专门允许所需的应用程序端口（和从已知控制连接或会话产生的动态媒体特定数据流），则网络上存在的唯一不需要的数据流必须进入特定的、更易于识别的子网，这可减少保持对不需要数据流的控制所施加的工程和操作负担。

本文档介绍基于*怀疑 角度的 VoIP 安全配置，因此仅允许在语音网络段中允许的数据流。*数据策略倾向于较宽松的控制，如每个应用方案配置中的注释所述。

所有安全策略部署都必须遵循闭环反馈循环；安全部署通常会影响现有应用程序的容量和功能，并且必须进行调整以最大程度地减小此影响或消除此影响。

如果需要配置基于区域的策略防火墙的附加背景信息，请查看区域防火墙设计和应用指南。

VoIP 环境中 ZFW 的注意事项

区域防火墙设计和应用指南简要论述了对路由器的*自身区域 使用安全策略和从路由器的自身区域使用安全策略的路由器安全功能，以及通过各种网络基础保护 (NFP) 功能提供的替代功能。*基于路由器的 VoIP 功能托管在路由器的*自身区域 中，因此保护路由器的安全策略必须知道语音数据流的需求才能满足源自和去往 Cisco Unified CallManager Express、Survivable Remote-Site Telephony 和语音网关资源的语音信令和媒体的要求。*在 Cisco IOS 软件版本 12.4(20)T 以前，传统防火墙和基于区域的策略防火墙无法完全满足 VoIP 数据流的要求，因此防火墙策略未进行优化，无法充分保护资源。保护基于路由器的 VoIP 资源的自身区域安全策略在很大程度上依赖于 12.4(20)T 中引入的功能。

IOS 防火墙语音功能

Cisco IOS 软件版本 12.4(20)T 引入了几个增强功能以支持共存区域防火墙和语音功能。三个主要功能直接地适用获取语音应用：

- SIP 增强功能：应用层网关和应用程序检查和控制更新SIP版本以支持SIPv2，如所描述由RFC 3261扩展 SIP 信令支持以识别更多类型的呼叫流引入 SIP 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞扩展自身区域检查以能够识别由发往/源自本地的 SIP 数据流导致的辅助信令和介质信道
- 对 Skinny 本地数据流和 CME 的支持更新SCCP技术的支持版本16(以前支持的版本9)引入 SCCP 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞扩展自身区域检查以能够识别由发往/源自本地的 SCCP 数据流导致的辅助信令和介质信道
- 对版本 3 和 4 的 H.323 支持将 H.323 支持更新到版本 3 和 4（以前支持版本 1 和 2）引入 H.323 应用程序检查和控制 (AIC) 以应用精确的控制来解决特定的应用程序级弱点和漏洞

本文档中介绍的路由器安全配置包括由这些增强提供的功能以及描述由这些策略应用的操作的说明。如果希望查看语音检查功能的完整详细信息，可单击本文档相关信息部分中各个功能文档的超链接。

注意事项

为了强化前面提到的要点，应用带有基于路由器的语音功能的 Cisco IOS 防火墙必须应用基于区域

的策略防火墙。传统 IOS 防火墙不包括完全支持语音数据流的信令复杂性或行为所需的功能。

网络地址转换 (NAT)

Cisco IOS 网络地址转换 (NAT) 常常与 Cisco IOS 防火墙同时配置，特别是在专用网络必须与 Internet 连接，或者必须连接不同的专用网络（特别是 IP 地址空间重叠）的情况下。Cisco IOS软件包括用于SIP、Skinny和H.323的NAT应用层网关(ALG)。理想情况下，IP语音的网络连接无需应用NAT即可实现，因为NAT会为故障排除和安全策略应用带来额外的复杂性，尤其是在使用NAT过载的情况下。NAT 只能作为最后一种情况的解决方案进行应用以解决网络连接相关问题。

Cisco Unified Presence 客户端 (CUPC)

本文档不介绍支持将Cisco Unified Presence Client(CUPC)与IOS防火墙配合使用的配置，因为自Cisco IOS软件版本12.4(20)T1起，区域或传统防火墙尚不支持CUPC。CUPC将在Cisco IOS软件的未来版本中受支持。

使用到位于总部或语音提供商处的 CCM 的 SIP 中继的 CME/CUE/GW 单站点或分支机构

此方案在本文档前面部分（连接到 PSTN 的 CME/CUE/GW 单站点或分支机构）所述的单站点/分布式呼叫处理/PSTN 连接的模型和在本文档中所述第三个方案中定义的多站点/集中呼叫处理/已收敛语音和数据网络之间提供折衷。此方案仍使用本地 Cisco Unified CallManager Expres，但是长距离拨号和总部/远程站点电话通讯主要通过站点到站点 SIP 中继来提供，其中本地拨号和紧急拨号通过本地 PSTN 连接提供。即使在大部分旧 PSTN 连接已被删除的情况下，也建议使用基本级别的 PSTN 容量来适应基于 WAN 的“toll bypass”拨号和由拨号计划描述的本地区域拨号出现故障的情况。此外，本地法律通常要求提供某种类型的本地 PSTN 连接以提供紧急 (911) 拨号。此方案采用分布式呼叫处理，它具有一些优点并遵循最佳实践，如 Cisco Unified CallManager Express SRND 中所述。

组织可以在以下情况下实施此类型的应用方案：

- 在站点之间使用了不同的 VoIP 环境，但仍希望使用 VoIP 来代替长途 PSTN。
- 拨号计划管理需要逐个站点实现自治。
- 不管 WAN 可用性如何，都需要完全的呼叫处理功能。

方案背景

此应用方案合并了有线电话（语音 VLAN）、有线 PC（数据 VLAN）和无线设备（包括 VoIP 设备，如 IP Communicator）。

安全配置提供以下功能：

1. CME 和本地电话（SCCP 和 SIP）之间以及 CME 和远程 CUCM 群集 (SIP) 之间由路由器启动的信令检查。
2. 以下对象之间用于通信的语音媒体“针孔”：本地有线和无线段用于 MoH 的 CME 和本地电话用于语音邮件的 CUE 和本地电话电话和远程呼叫实体
3. 应用程序检查和控制 (AIC)，应用该功能可以实现以下目的：发送速率限制邀请消息确保所有 SIP 数据流上的协议符合性

优点/缺点

此应用程序提供降低成本的优点，因为它在 WAN 数据链路上传送站点到站点语音数据流。

此方案的缺点是需要更详细的 WAN 连接计划。站点到站点呼叫质量可能受到 WAN 上许多因素的影响，例如非法/不需要的数据流（蠕虫、病毒和对等文件共享）或确定可能由于运营商网络上的流量工程导致的延迟问题的困难。必须适当调整 WAN 连接的大小以便为语音和数据流提供足够的带宽；对延迟不十分敏感的数据流（例如，电子邮件、SMB/CIFS 文件数据流）可以分类为 QoS 的低优先级数据流以保持语音质量。

此方案的另一个问题是缺少集中呼叫处理和排除呼叫处理故障过程中可能出现的困难。同样地，此方案最适用于在较大的组织中作为迁移到集中呼叫处理过程中的中间步骤。完成到 Cisco CallManager 的迁移后，可以将本地 Cisco CME 转换为充当全功能的 SRST 后备系统。

从安全角度来看，此环境增加的复杂性使得有效的安全实施和故障排除更加困难，因为 WAN 上或公共 Internet 的 VPN 上的连接会显著增加对安全造成威胁的环境，特别是在安全策略需要*信任角度（其中对通过 WAN 的数据流施加的限制非常少）的情况下*。鉴于这一点，本文档中提供的配置示例实施一个更*多疑的策略，该策略允许特定业务关键数据流，然后由协议符合性检查对这些数据流进行检查*。此外，还将限制特定 VoIP 操作（即，SIP 邀请），以降低对 VoIP 资源和可用性造成负面影响的恶意或无意的软件故障的可能性。

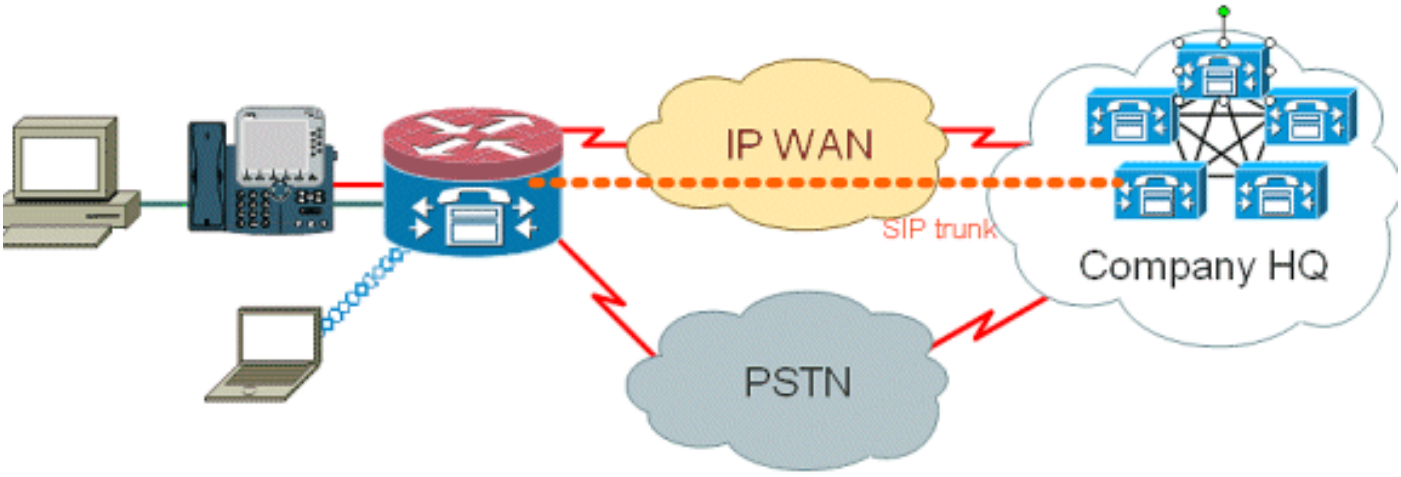
配置

数据策略、基于区域的防火墙、语音安全和 CCME 的配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用以下网络设置：



配置

此处描述的配置说明 Cisco 2851 集成服务路由器。

本文档使用以下配置：

- CME 和 CUE 连接的语音服务配置
- 基于区域的策略防火墙配置
- 安全配置

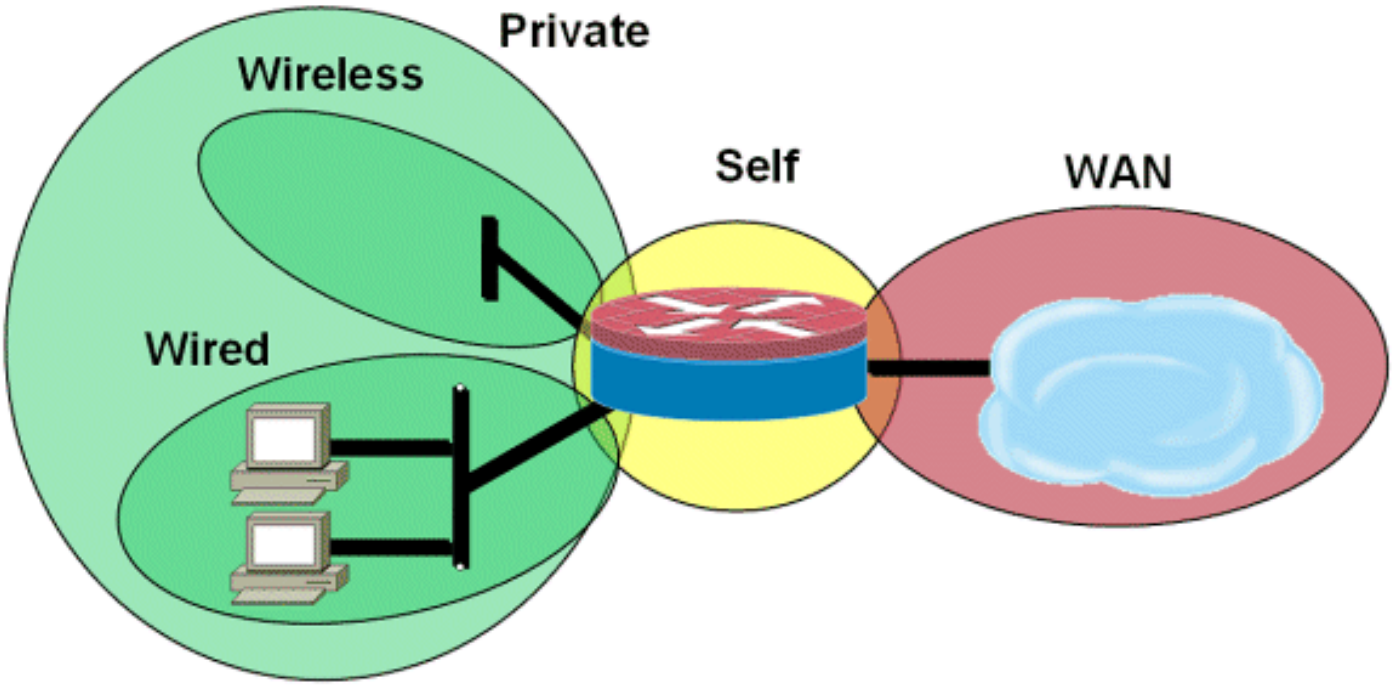
以下是 CME 和 CUE 连接的语音服务配置：

CME 和 CUE 连接的语音服务配置

```
!
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

!
```

以下是基于区域的策略防火墙配置，由有线和无线 LAN 网段的安全区域、专用 LAN（由有线和无线网段组成）、受信任 WAN 连接到达的 WAN 网段和路由器的语音资源所在的自身区域组成：



以下是安全配置：

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
```

配置、管理和监控

基于路由器的 IP 电话资源和基于区域的策略防火墙的提供和配置通常最好使用 Cisco Configuration Professional 进行。Cisco Secure Manager 不支持基于区域的策略防火墙或基于路由器的 IP 电话。

Cisco IOS 传统防火墙支持使用 Cisco 统一防火墙 MIB 的 SNMP 监控，但是统一防火墙 MIB 尚不支持基于区域的策略防火墙。同样地，必须通过路由器的命令行界面上的统计信息或使用 GUI 工具（如 Cisco Configuration Professional）处理防火墙监控。

虽然在 12.4(15)T4/T5 和 12.4(20)T 中实施的用于改进日志消息与数据流的相关性的日志记录更改在 Cisco 安全监控和报告系统 (CS-MARS) 上尚未得到完全支持，但 CS-MARS 提供对基于区域的策略防火墙的基本支持。

容量计划

来自印度的防火墙呼叫检查性能测试结果尚有待确定。

验证

当前没有可用于此配置的验证过程。

故障排除

Cisco IOS 区域防火墙提供 **show 和 debug 命令来查看和监控防火墙的活动并进行故障排除。**此部分描述使用 **show 命令监控基本防火墙活动的方法，并介绍用于排除配置故障或在与技术支持的讨论需要更详细的信息时使用的区域防火墙的 debug 命令。**

故障排除命令

Cisco IOS 防火墙提供几个 **show 命令来查看安全策略配置和活动。**其中的许多命令可以通过应用 **alias 命令替换为更短的命令。**

注意：在使用debug命令之前，请参阅有关Debug命**令的**重要信息。

如果您正在使用一种非典型或不支持的配置，并且需要与 Cisco TAC 或其他产品的技术支持服务协作以解决互操作性问题，debug 命令可能很有用。

注意：将debug命令应**用**于特定功能或流量可能导致大量控制台消息，从而导致路由器控制台无响应。如果需要进行调试，您可以提供不监控终端对话的替代命令行界面访问，如 Telnet 窗口。请只在脱机（实验室环境）设备上或在计划维护窗口内启用调试，因为调试可能显著影响路由器性能。

相关信息

- Cisco Unified CallManager Express 解决方案参考网络设计指南
- Cisco CallManager Express 安全最佳实践 (CME SRND)

- 将 Cisco Unity Connection 与 Cisco Unified CME-as-SRST 集成
- Cisco Unified Communications Manager Express命令参考
- Cisco CallManager Express/Cisco Unity Express 配置示例
- Cisco CallManager Express 3.4 SNMP MIB 支持
- 区域策略防火墙设计和应用指南
- Cisco IOS 防火墙：SIP 增强功能：ALG 和 AIC
- 软件 Cisco IOS 防火墙 H.323 支持
- Cisco IOS 防火墙对 Skinny 本地数据流和 CME 的支持
- 技术支持和文档 - Cisco Systems