基于 Cisco IOS 区域的防火墙：办公室使用isco Unity Express/SRST/PSTN网关并连接到集中化的Cisco CallManager

目录

简介
先决条件
要求
使用的组件
规则
Cisco IOS防火墙背景
配置
Cisco IOS基于区域的策略防火墙的部署
注意事项
使用Cisco Unity Express/SRST/PSTN网关（连接到集中式Cisco CallManager）的Office
调配、管理和监控
容量规划
验证
故障排除
故障排除命令
显示命令
调试命令
相关信息

简介

思科集成多业务路由器(ISR)提供可扩展的平台，可满足各种应用的数据和语音网络需求。虽然私有网络和互联网连接网络的威胁形势非常动态，但Cisco IOS®防火墙提供状态检测和应用检测与控制(AIC)功能，以定义和实施安全网络状态，同时实现业务功能和连续性。

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。为每个应用场景提供语音服务和防火墙配置。每个场景分别描述VoIP和安全配置，然后按整个路由器配置进行描述。您的网络可能需要对QoS和VPN等服务进行其他配置，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。

Cisco IOS防火墙背景

Cisco IOS防火墙通常部署在与设备防火墙的部署模式不同的应用场景中。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。

虽然从成本和运营角度看，防火墙检查的应用以及ISR产品中的其他集成服务看起来颇具吸引力，但必须评估特定考虑因素，以确定基于路由器的防火墙是否合适。如果部署了基于路由器的集成解决方案，应用每个附加功能会产生内存和处理成本，并可能导致转发吞吐率降低、数据包延迟增加以及在高峰负载期间丢失功能。在路由器和设备之间做出选择时，请遵循以下准则：

- 启用了多个集成功能的路由器最适合分支机构或远程工作人员站点，其中设备较少，可提供更好的解决方案
- 高带宽、高性能应用通常能通过设备得到更好的解决。应应用Cisco ASA和Cisco Unified Call Manager服务器来处理NAT和安全策略应用和呼叫处理，而路由器应满足QoS策略应用、WAN终端和站点到站点VPN连接要求。

在引入Cisco IOS软件版本12.4(20)T之前，传统防火墙和基于区域的策略防火墙(ZFW)无法完全支持VoIP流量和基于路由器的语音服务所需的功能，并且在其他安全防火墙策略中需要大的开口，以适应语音流量，并对不断发展的VoIP信令和媒体提供有限支持协议。

配置

Cisco IOS基于区域的策略防火墙的部署

Cisco IOS基于区域的策略防火墙与其他防火墙类似，只有在安全策略识别和描述网络信任的安全要求时，才能提供安全防火墙。有两个到达安全策略的基本途径：而不是可疑的*视*角。

*信任*视角假设所有流量都是可信的，但可以明确识别为恶意或不需要的流量除外。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行为的工具来实现。此方法对现有应用的干扰较少，但需要全面了解威胁和漏洞形势，并且需要持续保持警惕，以应对新的威胁和漏洞。此外，用户社区必须在维护足够的安全性方面发挥很大作用。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。

可疑*视角*假设所有网络流量都是不理想的，但特别确定的良好*流量*除外。这是应用的策略，它拒绝除明确允许的流量外的所有应用流量。此外，可实施应用检测和控制(AIC)，以识别和拒绝专门设计为利用良好应用的恶意流*量*，以及伪装成良好流量的不*需要*流量。同样，应用控制会对网络造成运营和性能负担，尽管大多数不需要的流量应由无状态过滤器(如访问控制列表(ACL)或基于区域的策略防火墙(ZFW)策略)控制，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)或网络)处理的流量应大幅减少基于应用识别(NBAR)。 因此，如果仅允许所需的应用端口和由已知控制连接或会话产生的动态媒体特定流量，则网络上应存在的唯一不需要的流量应落

入一个特定的、更易于识别的子集中，从而减轻为保持对不需要的流量的控制而施加的工程和操作负担。

本文档基于可疑角度描述VoIP安全*配*置；因此，仅允许语音网段中允许的流量。数据策略往往更为宽松，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的功能和功能，必须进行调整以尽量减少或解决此影响。

有关配置基于区域的策略防火墙的详细信息和其他背景，请参阅《基于区域的策略防火墙设计和应用指南》。

VoIP 环境中 ZFW 的注意事项

前面提到的《设计和应用指南》简要介绍了路由器的安全性，包括路由器自身区域之间使用的安全策略，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内，因此保护路由器的安全策略必须了解语音流量的要求，以便适应由Cisco Unified CallManager Express、可存活远程站点电话和语音网关资源发起并发往的语音信令和媒体。在Cisco IOS软件版本12.4(20)T之前，传统防火墙和基于区域的策略防火墙无法完全满足VoIP流量的要求，因此防火墙策略未优化以完全保护资源。保护基于路由器的VoIP资源的自区域安全策略严重依赖Cisco IOS软件版本12.4(20)T中引入的功能。

Cisco IOS防火墙语音功能

思科IOS软件版本12.4(20)T引入了多项增强功能，以实现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区域检查，以便能够识别由本地发往/源自SIP流量产生的辅助信令和媒体信道
- 支持瘦本地流量和Cisco CallManager Express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区域检查，以便能够识别从本地发往/源自SCCP流量产生的辅助信令和媒体信道
- H.323 v3/v4支持将H.323支持更新到v3和v4（以前支持v1和v2），如所述引入 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

本文档中描述的路由器安全配置包括这些增强功能提供的功能，以及描述策略所应用的操作的说明。如果您想查看语音检查功能的完整详细信息，可在本文档结尾的“相关信息”部分中找到指向各个功能文档的超链接。

注意事项

Cisco IOS防火墙应用具有基于路由器的语音功能，必须应用基于区域的策略防火墙，以强化之前提到的要点。传统IOS防火墙不包含完全支持语音流量的信令复杂性和行为所需的功能。

NAT

Cisco IOS网络地址转换(NAT)经常与Cisco IOS防火墙同时配置，特别是在专用网络必须与Internet接口或者不同专用网络必须连接时，尤其是在使用重叠的IP地址空间时。Cisco IOS软件包括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应仅作为解决网络连接问题的最后一个案例解决方案。

CUPC

本文档不介绍支持将Cisco Unified Presence Client(CUPC)与Cisco 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在Cisco IOS软件的未来版本中受支持。

使用Cisco Unity Express/SRST/PSTN网关（连接到集中式Cisco CallManager）的Office

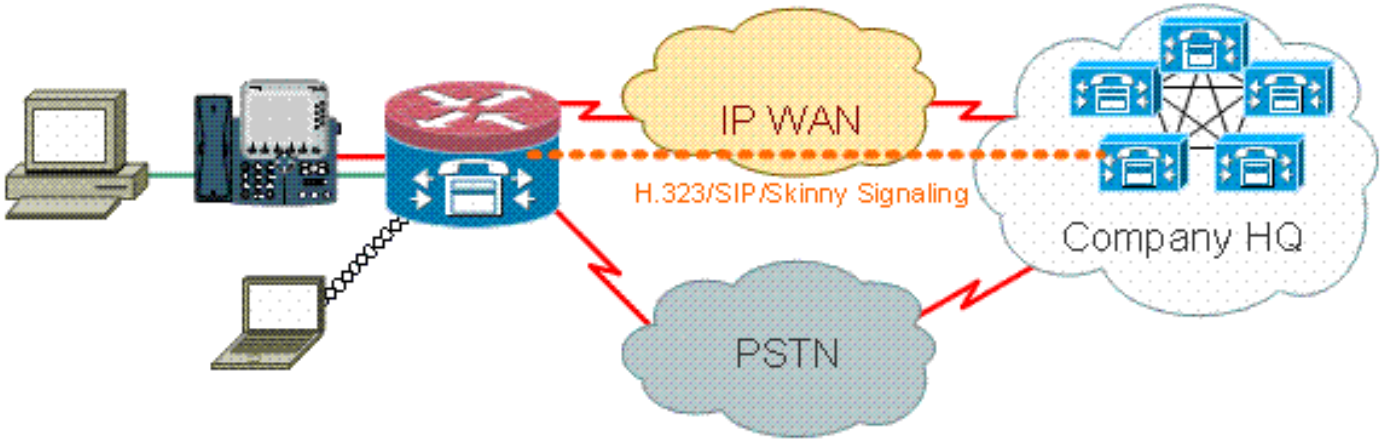
此场景与以前的应用不同，因为集中呼叫控制用于所有呼叫控制，而不是基于分布式路由器的呼叫处理。分布式语音邮件已应用，但是通过路由器上的Cisco Unity Express。路由器为紧急拨号和本地拨号提供可存活远程站点电话和PSTN网关功能。建议使用特定于应用的PSTN容量级别，以适应基于广域网的长途旁路拨号以及按拨号方案所述的局域网拨号的故障。此外，本地法律通常要求提供某种类型的本地 PSTN 连接以提供紧急 (911) 拨号。

此方案还可以将Cisco CallManager Express应用为SRST的呼叫处理代理，以防在WAN/CCM中断期间需要更高的呼叫处理功能。有关详细信息，请参阅将Cisco Unity Connection与Cisco Unified CME-as-SRST集成。

方案背景

应用场景包括有线电话（语音VLAN）、有线PC（数据VLAN）和无线设备（包括VoIP设备，如IP Communicator）。

1. 本地电话和远程CUCM集群（SCCP和SIP）之间的信令检查
2. 检查路由器和远程CUCM集群之间的H.323信令。
3. 当到远程站点的链路关闭且SRST处于活动状态时，检查本地电话和路由器之间的信令。
4. 语音媒体针孔，用于在以下设备之间通信：本地有线和无线段本地和远程电话远程MoH服务器和本地电话用于语音邮件的远程Unity服务器和本地电话
5. 将应用检测和控制(AIC)应用于：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

此方案的优势在于，大部分呼叫处理发生在中央Cisco CallManager集群中，从而减轻了管理负担。

与本文档中描述的其他情况相比，路由器通常必须解决较少的本地语音资源检查负担，因为除了处理往返于Cisco Unity Express的流量，以及在广域网或CUCM中断以及本地Cisco CallManager Express/SRST被调用以处理呼叫处理的情况外，大部分呼叫处理负担不会强加在路由器上。

在典型的呼叫处理活动中，本例的最大缺点是Cisco Unity Express位于本地路由器上。虽然从设计角度来看这很好，例如，Cisco Unity Express位于离持有语音邮件的最终用户最近的位置，但它会产生一些额外的管理负担，因为可以管理大量Cisco Unity Express。也就是说，中央Cisco Unity Express具有相反的缺点，即中央Cisco Unity Express距离远程用户更远，在中断期间可能无法访问。因此，将Cisco Unity Express部署到远程位置后，分布式语音邮件的功能优势提供了卓越的选择。

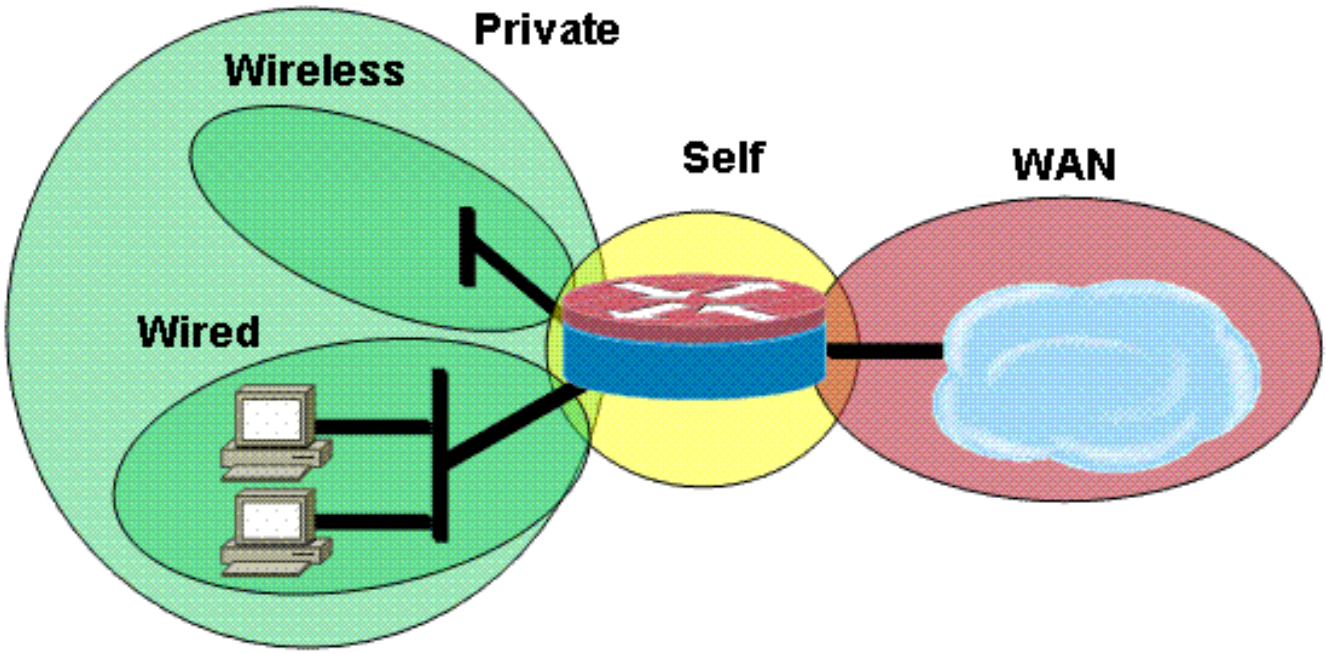
数据策略、基于区域的防火墙、语音安全、Cisco CallManager Express

路由器配置基于带NME-X-23ES和PRI HWIC的3845:

SRST和Cisco Unity Express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示例，由有线和无线LAN网段的安全区域、由有线和无线网段组成的专用LAN、到达可信WAN连接的WAN网段以及路由器语音资源所在的自身区域组成：



安全性配置:

```
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 3825-srst
!
!
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
ip cef
!
!
ip domain name cisco.com
```

```
ip name-server 172.16.1.22
ip vrf acctg
 rd 0:1
!
ip vrf eng
 rd 0:2
!
ip inspect WAAS enable
!
no ipv6 cef
multilink bundle-name authenticated
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
archive
 log config
  hidekeys
!
!
!
!
!
!
!
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 vpn
zone security eng
zone security acctg
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 Loopback101
 ip vrf forwarding acctg
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
!
interface Loopback102
 ip vrf forwarding eng
 ip address 10.255.1.5 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 172.16.1.103 255.255.255.0
 shutdown
!
interface GigabitEthernet0/0.109
 encapsulation dot1Q 109
 ip address 172.16.109.11 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 zone-member security public
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 media-type rj45
 no keepalive
!
interface GigabitEthernet0/1.129
 encapsulation dot1Q 129
 ip address 172.17.109.2 255.255.255.0
 standby 1 ip 172.17.109.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 track GigabitEthernet0/0.109
!
interface GigabitEthernet0/1.149
 encapsulation dot1Q 149
 ip address 192.168.109.2 255.255.255.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip nat inside
 ip virtual-reassembly
 zone-member security private
!
interface GigabitEthernet0/1.161
 encapsulation dot1Q 161
 ip vrf forwarding acctg
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly
 zone-member security acctg
!
interface GigabitEthernet0/1.162
 encapsulation dot1Q 162
 ip vrf forwarding eng
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
!
interface Serial0/3/0
 no ip address
 encapsulation frame-relay
 shutdown
 frame-relay lmi-type cisco
!
interface Serial0/3/0.1 point-to-point
 ip vrf forwarding acctg
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security acctg
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 321 IETF
!
interface Serial0/3/0.2 point-to-point
 ip vrf forwarding eng
 ip address 10.255.1.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 zone-member security eng
 snmp trap link-status
 no cdp enable
 frame-relay interface-dlci 322 IETF
!
interface Integrated-Service-Engine2/0
 no ip address
 shutdown
 no keepalive
!
interface GigabitEthernet3/0
 no ip address
 shutdown
!
router eigrp 1
 network 172.16.109.0 0.0.0.255
 network 172.17.109.0 0.0.0.255
 no auto-summary
!
router eigrp 104
 network 10.1.104.0 0.0.0.255
 network 192.168.109.0
 network 192.168.209.0
 no auto-summary
!
router bgp 1109
 bgp log-neighbor-changes
 neighbor 172.17.109.4 remote-as 1109
 !
 address-family ipv4
  neighbor 172.17.109.4 activate
  no auto-summary
```

```
  no synchronization
  network 172.17.109.0 mask 255.255.255.0
 exit-address-family
!
ip forward-protocol nd
ip route vrf acctg 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf acctg 10.1.2.0 255.255.255.0 10.255.1.2
ip route vrf eng 0.0.0.0 0.0.0.0 172.16.109.1 global
ip route vrf eng 10.1.2.0 255.255.255.0 10.255.1.2
!
!
ip http server
no ip http secure-server
ip nat pool acctg-nat-pool 172.16.109.21 172.16.109.22 netmask 255.255.255.0
ip nat pool eng-nat-pool 172.16.109.24 172.16.109.24 netmask 255.255.255.0
ip nat inside source list 109 interface GigabitEthernet0/0.109 overload
ip nat inside source list acctg-nat-list pool acctg-nat-pool vrf acctg overload
ip nat inside source list eng-nat-list pool eng-nat-pool vrf eng overload
ip nat inside source static 172.17.109.12 172.16.109.12 extendable
!
ip access-list extended acctg-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
ip access-list extended eng-nat-list
 deny   ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
 permit ip 10.0.0.0 0.255.255.255 any
!
logging 172.16.1.20
access-list 1 permit any
access-list 109 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 109 permit ip 192.168.0.0 0.0.255.255 any
access-list 111 deny   ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.0.0 0.0.255.255 any
access-list 141 permit ip 10.0.0.0 0.255.255.255 any
access-list 171 permit ip host 1.1.1.1 host 2.2.2.2
!
!
!
!
!
!
!
control-plane
!
!
!
!
!
!
!
!
gateway
 timer receive-rtp 1200
!
!
alias exec sh-sess show policy-map type inspect zone-pair sessions
!
line con 0
 exec-timeout 0 0
line aux 0
line 130
 no activation-character
 no exec
 transport preferred none
```

```
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line 194
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login
!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
!
webvpn context Default_context
 ssl authenticate verify all
 !
 no inservice
!
end
```

调配、管理和监控

Cisco Configuration Professional通常最适合调配和配置基于路由器的IP电话资源和基于区域的策略防火墙。CiscoSecure 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 Unified Firewall MIB进行SNMP监控。但是，统一防火墙MIB中尚不支持基于区域的策略防火墙。因此，防火墙监控必须通过路由器命令行界面上的统计信息或Cisco Configuration Professional等GUI工具进行处理。

CiscoSecure Monitoring and Reporting System(CS-MARS)为基于区域的策略防火墙提供基本支持，不过，日志记录更改改进了与在Cisco IOS软件版本12.4(15)T4/T5和Cisco IOS软件版本12.4(20)T中实施的流量的日志消息关联尚未在CS-MARS中得到完全支持。

容量规划

来自印度的防火墙呼叫检测性能测试结果待定。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

Cisco IOS区域防火墙提供**show**和**debug**命令，以便查看、监控和排除防火墙活动故障。本节介绍如何使用**show**命令来监控基本防火墙活动，以及如何介绍区域防火墙的**debug**命令以进行更详细的故障排除，或者如果与技术支持的讨论需要详细信息，则说明如何使用**debug**命令。

故障排除命令

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

显示命令

Cisco IOS防火墙提供多个show命令，用于查看安全策略配置和活动：

通过应用alias命令，这些命令中的许多都可以用较短的命令来替换。

调试命令

如果您使用非典型或不受支持的配置，并且需要与Cisco TAC或其他产品的技术支持服务合作以解决互操作性问题，则Debug命令可能非常有用。

注意：将debug命令应用于特定功能或流量会导致大量控制台消息，从而导致路由器控制台无响应。如果需要启用调试，则可以提供替代命令行界面访问，例如不监控终端对话框的telnet窗口。您应仅在离线（实验室环境）设备或计划维护窗口中启用调试，因为如果启用调试，这会严重影响路由器性能。

相关信息

- Cisco Unified CallManager Express 解决方案参考网络设计指南
- Cisco Unified CallManager Express安全最佳实践
- 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 防火墙对 Skinny 本地数据流和 CME 的支持
- Cisco IOS 防火墙
- 技术支持和文档 - Cisco Systems