Firewall baseado em zona do IOS: Exemplo de configuração de conexão PSTN de local único ou filial CME/CUE/GW

Contents

Introduction

Os Cisco Integrated Service Routers (ISRs) oferecem uma plataforma escalável para atender aos requisitos de rede de dados e voz para uma ampla variedade de aplicativos. Embora o cenário de ameaças de redes privadas e conectadas à Internet seja um ambiente muito dinâmico, o Cisco IOS Firewall oferece recursos de inspeção stateful e inspeção e controle de aplicativos (AIC) para definir e aplicar uma postura de rede segura, ao mesmo tempo em que permite a capacidade e a continuidade dos negócios.

Este documento descreve as considerações de projeto e configuração para aspectos de segurança de firewall de cenários específicos de aplicativos de voz e dados baseados em Cisco ISR. A configuração de serviços de voz e firewall é fornecida para cada cenário de aplicativo. Cada cenário descreve as configurações de VoIP e de segurança separadamente, seguidas por toda a configuração do roteador. Sua rede pode exigir outras configurações para serviços como QoS e VPN para manter a qualidade e a confidencialidade da voz.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Plano de Fundo do Firewall IOS

O Cisco IOS Firewall é normalmente implantado em cenários de aplicativos que diferem dos modelos de implantação de firewalls de dispositivos. As implantações típicas incluem aplicativos para funcionários remotos, escritórios remotos ou pequenos e aplicativos de varejo, onde se deseja uma baixa contagem de dispositivos, integração de vários serviços e menor desempenho e profundidade de recursos de segurança.

Embora a aplicação da inspeção de firewall, juntamente com outros serviços integrados nos produtos ISR, possa parecer atraente do ponto de vista de custo e operacional, considerações específicas devem ser avaliadas para determinar se um firewall baseado em roteador é apropriado. A aplicação de cada recurso adicional incorre em custos de memória e processamento e provavelmente contribuirá para taxas de transferência de encaminhamento reduzidas, maior latência de pacotes e perda de capacidade de recursos durante períodos de pico de carga se uma solução baseada em roteador integrado com baixa energia for implantada.

Siga estas diretrizes ao decidir entre um roteador e um dispositivo:

- Os roteadores com vários recursos integrados habilitados são mais adequados para filiais ou escritórios remotos, onde menos dispositivos oferecem uma solução melhor.
- Os aplicativos de alta largura de banda e alto desempenho geralmente são mais bem tratados com dispositivos: O Cisco ASA e o Cisco Unified Call Manager Server devem ser aplicados para lidar com NAT e políticas de segurança e processamento de chamadas, enquanto os roteadores lidam com a aplicação de política de QoS, terminação de WAN e requisitos de conectividade de VPN site a site.

Antes da introdução do Cisco IOS Software versão 12.4(20)T, o Classic Firewall e o Zone-Based Policy Firewall (ZFW) não podiam suportar totalmente os recursos necessários para tráfego VoIP e serviços de voz baseados em roteador, exigindo grandes aberturas em políticas de firewall seguras para acomodar tráfego de voz e oferecendo suporte limitado para a sinalização VoIP em evolução e protocolos de mídia.

Implantação do Cisco IOS Zone-Based Policy Firewall

O Cisco IOS Zone-Based Policy Firewall, semelhante a outros firewalls, só pode oferecer um firewall seguro se os requisitos de segurança da rede forem identificados e descritos pela política de segurança. Há duas abordagens fundamentais para chegar a uma política de segurança: a perspectiva *confiável*, em oposição à perspectiva *suspeita*.

A perspectiva *confiável* supõe que todo o tráfego é confiável, exceto o que pode ser especificamente identificado como mal-intencionado ou indesejado. Uma política específica é implementada que nega apenas o tráfego indesejado. Isso normalmente é feito por meio do uso de entradas de controle de acesso específicas ou ferramentas baseadas em assinatura ou comportamento. Essa abordagem tende a interferir menos nos aplicativos existentes, mas exige um conhecimento abrangente do cenário de ameaças e vulnerabilidades e exige vigilância constante para lidar com novas ameaças e explorações à medida que elas surgem. Além disso, a comunidade de usuários deve desempenhar um papel importante na manutenção da segurança adequada. Um ambiente que permite ampla liberdade com pouco controle para os ocupantes oferece oportunidades substanciais para problemas causados por indivíduos descuidados ou mal-intencionados. Um problema adicional dessa abordagem é que ela depende muito mais de ferramentas de gerenciamento eficazes e controles de aplicativos que oferecem flexibilidade e desempenho suficientes para poder monitorar e controlar dados suspeitos em todo o tráfego de rede. Embora a tecnologia esteja atualmente disponível para acomodar isso, a carga operacional frequentemente excede os limites da maioria das empresas.

A perspectiva *suspeita* supõe que todo o tráfego de rede é indesejado, exceto para o *bom* tráfego *identificado especificamente*. Uma política aplicada que nega todo o tráfego do aplicativo, exceto aquela explicitamente permitida. Além disso, a AIC (Application Inspection and Control, inspeção e controle de aplicativos) pode ser implementada para identificar e negar o tráfego mal-intencionado criado especificamente para explorar aplicativos "bons", bem como o tráfego indesejado que está sendo mascarado como um bom tráfego. Novamente, os controles de aplicativos impõem carga operacional e de desempenho na rede, embora a maioria do tráfego indesejado deva ser controlada por filtros stateless, como listas de controle de acesso (ACLs) ou política de firewall de política baseada em zona (ZFW), portanto, deve haver substancialmente menos tráfego que deve ser tratado pelo AIC, sistema de prevenção de invasão (IPS) ou outros controles baseados em assinatura, como correspondência de pacotes flexível (FPM) ou reconhecimento de aplicativos baseado em rede (NBAR). Assim, se apenas as portas de aplicativos desejadas (e o tráfego dinâmico específico de mídia proveniente de conexões ou sessões de controle conhecidas) forem especificamente permitidos, o único tráfego indesejado que deve estar presente na rede deve cair em um subconjunto específico e mais facilmente reconhecido, o que reduz a carga operacional e de engenharia imposta para manter o controle sobre o tráfego indesejado.

Este documento descreve as configurações de segurança VoIP com base na perspectiva *suspeita*; assim, somente o tráfego permitido nos segmentos de rede de voz é permitido. As políticas de dados tendem a ser mais permissivas, conforme descrito pelas notas na configuração de cada cenário de aplicação.

Todas as implantações de políticas de segurança devem seguir um ciclo de feedback de loop fechado; as implantações de segurança normalmente afetam a capacidade e a funcionalidade dos aplicativos existentes e devem ser ajustadas para minimizar ou resolver esse impacto.

Para obter mais informações sobre como configurar o firewall de política baseado em zona, consulte o Guia de design e aplicativos do firewall de política baseado em zona do Cisco IOS

Firewall.

Considerações para ZFW em ambientes VoIP

O Guia de Design e Aplicações do Firewall de Política Baseado em Zona do Cisco IOS oferece uma breve discussão para proteger o roteador com o uso de políticas de segurança para e da zona *própria* do roteador, bem como recursos alternativos que são fornecidos por meio de vários recursos do Network Foundation Protection (NFP). Os recursos de VoIP baseados em roteador são hospedados na zona autônoma do roteador, portanto, as políticas de segurança que protegem o roteador devem estar cientes dos requisitos para tráfego de voz, para acomodar a sinalização de voz e a mídia originada e destinada aos recursos do Cisco Unified CallManager Express, Survivable Remote-Site Telephony e do Voice Gateway. Antes da versão 12.4(20)T do software Cisco IOS, o Firewall Clássico e o Firewall de Política Baseado em Zona não podiam acomodar totalmente os requisitos de tráfego VoIP, portanto, as políticas de firewall não foram otimizadas para proteger totalmente os recursos. As políticas de segurança de zona autônoma que protegem os recursos VoIP baseados em roteador dependem muito dos recursos introduzidos no 12.4(20)T.

Aprimoramentos de voz do IOS Firewall - 12.4(20)T

O Cisco IOS Software Release 12.4(20)T introduziu vários aprimoramentos para habilitar o Zone Firewall co-residente e os recursos de voz. Três recursos principais se aplicam diretamente a aplicativos de voz seguros:

- Aprimoramentos SIP: Inspeção e Controle de Aplicativos e Gateway da Camada de AplicaçãoAtualiza o suporte da versão SIP para SIPv2, conforme descrito pelo RFC 3261Amplia o suporte de sinalização SIP para reconhecer uma variedade maior de fluxos de chamadasApresenta o SIP Application Inspection and Control (AIC) para aplicar controles granulares para lidar com vulnerabilidades e explorações específicas no nível do aplicativoExpande a inspeção de zona automática para poder reconhecer a sinalização secundária e os canais de mídia resultantes do tráfego SIP destinado/originado localmente
- Suporte para tráfego local Skinny e CMEAtualiza o suporte do SCCP para a versão 16 (versão 9 suportada anteriormente)Apresenta o AIC (Application Inspection and Control, inspeção e controle de aplicativos) do SCCP para aplicar controles granulares para lidar com vulnerabilidades e explorações específicas no nível do aplicativoExpande a inspeção de zona automática para poder reconhecer a sinalização secundária e os canais de mídia resultantes do tráfego SCCP com origem/destino local
- Suporte para H.323 v3/v4Atualiza o suporte de H.323 para v3 e v4 (v1 e v2 anteriormente suportados)Apresenta o AIC (Application Inspection and Control, inspeção e controle de aplicativos) H.323 para aplicar controles granulares para lidar com vulnerabilidades específicas em nível de aplicativos e explorações

As configurações de segurança do roteador descritas neste documento incluem recursos oferecidos por esses aprimoramentos, com explicação para descrever a ação aplicada pelas políticas. Para obter detalhes completos sobre os recursos de inspeção de voz, consulte os documentos de recursos individuais listados na seção Informações Relacionadas deste documento.

Caveats

Para reforçar os pontos mencionados anteriormente, a aplicação do Cisco IOS Firewall com recursos de voz baseados em roteador deve aplicar o Zone-Based Policy Firewall. O Firewall IOS clássico não inclui a capacidade necessária para suportar totalmente as complexidades de sinalização e o comportamento do tráfego de voz.

Conversão de endereço de rede

O Cisco IOS Network Address Translation (NAT) é frequentemente configurado simultaneamente com o Cisco IOS Firewall, especialmente nos casos em que as redes privadas devem fazer interface com a Internet ou se redes privadas diferentes devem se conectar, especialmente se o espaço de endereço IP sobreposto estiver em uso. O software Cisco IOS inclui os gateways da camada de aplicação (ALGs) NAT para SIP, Skinny e H.323. Idealmente, a conectividade de rede para voz IP pode ser acomodada sem a aplicação do NAT, já que o NAT apresenta complexidade adicional para a solução de problemas e aplicativos de política de segurança, especialmente nos casos em que a sobrecarga de NAT é usada. O NAT deve ser aplicado somente como uma solução de último caso para tratar das preocupações de conectividade de rede.

Cisco Unified Presence Client

Este documento não descreve as configurações que suportam o uso do Cisco Unified Presence Client (CUPC) com IOS Firewall, pois o CUPC ainda não é suportado pelo Zone ou Classic Firewall a partir do Cisco IOS Software Release 12.4(20)T1. O CUPC será suportado em uma versão futura do Cisco IOS Software.

Conexão PSTN de local único ou filial CME/CUE/GW

Esse cenário apresenta telefonia baseada em roteador segura de Voz sobre IP para empresas de pequeno a médio porte em um único local ou para organizações de vários locais maiores que desejam implantar processamento de chamadas distribuídas, mantendo conexões antigas para a Rede Telefônica Pública Comutada (PSTN - Public Switched Telephone Network). O controle de chamadas VoIP é acomodado através da aplicação de um Cisco Unified Call Manager Express.

A conectividade PSTN pode ser mantida a longo prazo ou pode ser migrada para uma rede de voz e dados IP de longa distância convergida, conforme descrito no exemplo de aplicativo discutido na seção CME/CUE/GW Single Site ou Branch Office com Tronco SIP para CCM em HQ ou Voice Provider deste documento.

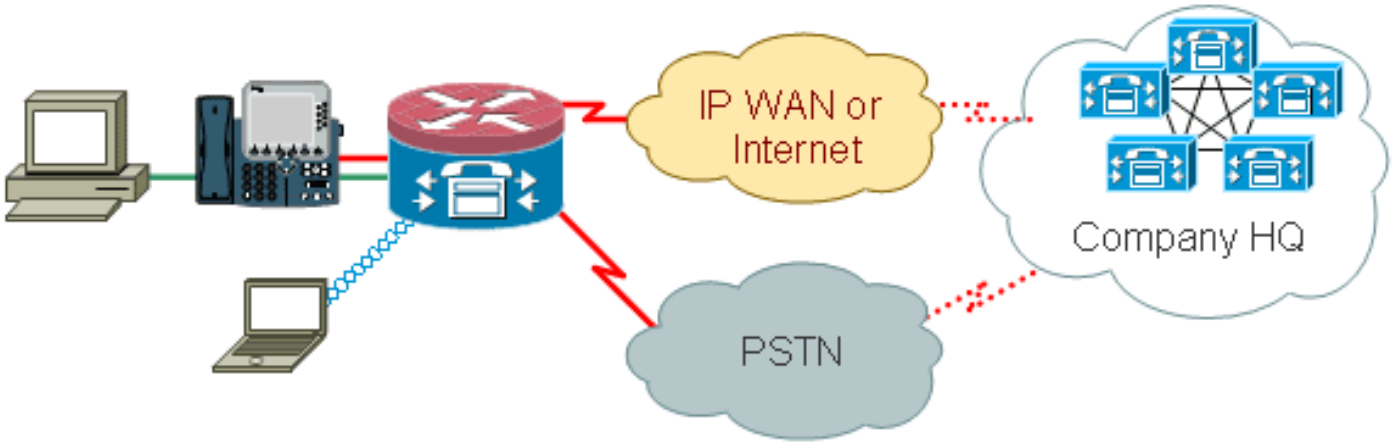
As organizações devem considerar a implementação deste tipo de cenário de aplicação para circunstâncias em que ambientes VoIP diferentes são usados entre locais ou se VoIP é impraticável devido à conectividade inadequada de dados de WAN ou restrições específicas de local sobre o uso de VoIP em redes de dados. Os benefícios e as melhores práticas da telefonia IP de um único local são descritos no SRND do Cisco Unified CallManager Express.

Histórico do cenário

O cenário do aplicativo incorpora telefones com fio (VLAN de voz), PCs com fio (VLAN de dados) e dispositivos sem fio (que incluem dispositivos VoIP, como o IP Communicator).

A configuração de segurança fornece:

- Inspeção de sinalização iniciada pelo roteador entre o CME e os telefones locais (SCCP e/ou SIP)
- Orifícios da mídia de voz para comunicação entre:Segmentos locais com e sem fioCME e os telefones locais para MoHCUE e os telefones locais para correio de voz
- Aplicar AIC (Application Inspection and Control, inspeção e controle de aplicativos) a:Limite de taxa de mensagens de conviteGaranta a conformidade do protocolo em todo o tráfego SIP.



Vantagens e desvantagens

O benefício mais óbvio do aspecto de VoIP do cenário é o caminho de migração oferecido pela integração da infraestrutura de rede de voz e dados existente em um ambiente POTS/TDM existente, antes de migrar para uma rede de voz/dados convergida para serviços de telefonia para o mundo além da LAN. Os números de telefone são mantidos para empresas menores, e o serviço central ou DID existente pode ser mantido no lugar para empresas maiores que desejam uma migração para a telefonia de pacote de desvio de tarifa.

As desvantagens incluem a perda de economia de custos que poderia ser obtida com o desvio de tarifa, migrando para uma rede convergente de voz e dados, bem como as limitações sobre a flexibilidade de chamadas e a falta de integração e portabilidade de comunicações em toda a empresa que poderiam ser realizadas com uma rede de voz e dados totalmente convergida.

Do ponto de vista da segurança, esse tipo de ambiente de rede minimiza as ameaças à segurança de VoIP, evitando a exposição dos recursos de VoIP à rede pública ou WAN. No entanto, o Cisco Call Manager Express incorporado no roteador ainda estaria vulnerável a ameaças internas, como tráfego mal-intencionado ou tráfego de aplicativos com mau funcionamento. Assim, é implementada uma política que permite o tráfego específico de voz que atenda às verificações de conformidade do protocolo, e ações VoIP específicas (por exemplo, CONVITE SIP) são limitadas de modo a reduzir a probabilidade de falhas de software mal-intencionado ou não intencional que afetem negativamente os recursos e a usabilidade de VoIP.

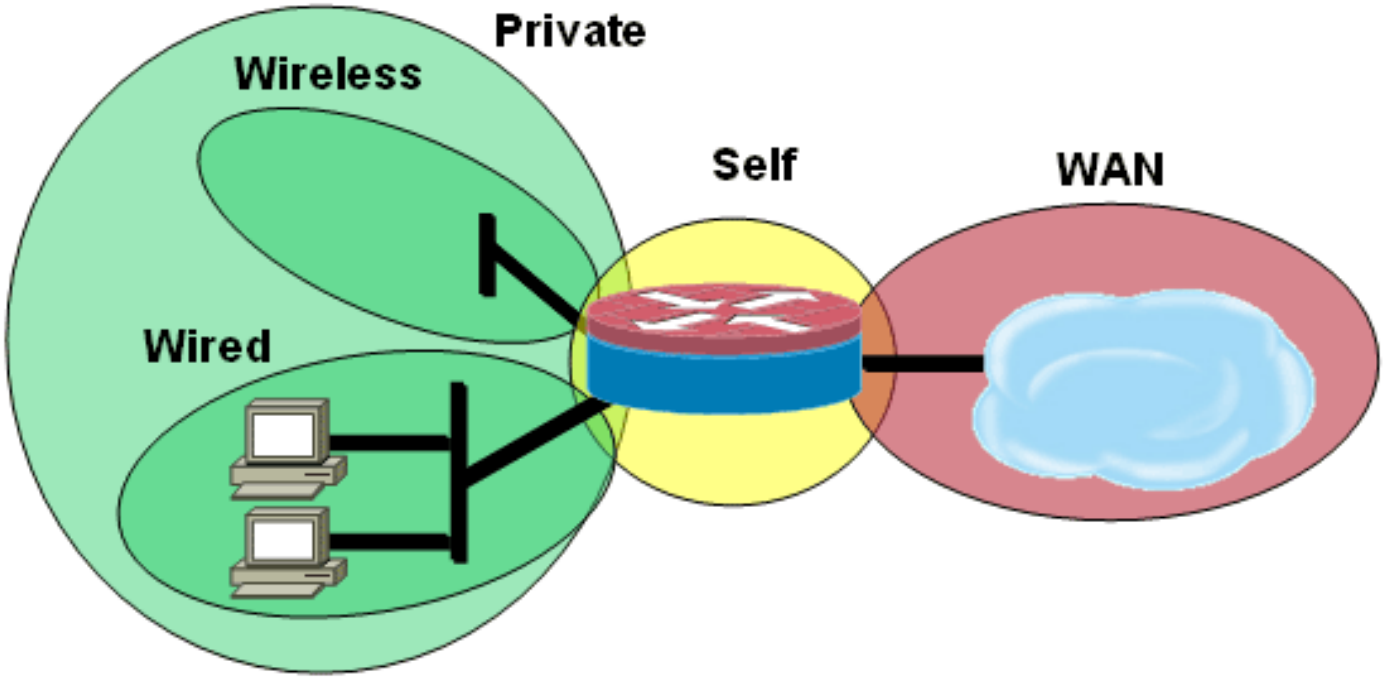
Políticas de dados, firewall baseado em zona, segurança de voz e configurações do CCME

A configuração descrita aqui ilustra um 2851 com uma configuração de serviço de voz para conectividade CME e CUE:

!

```
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
!
```

Configuração do firewall de política baseada em zona, composto de zonas de segurança para segmentos de LAN com e sem fio, LAN privada (composta por segmentos com e sem fio), um segmento de WAN pública onde a conectividade não confiável com a Internet é alcançada e a zona autônoma onde os recursos de voz do roteador estão localizados.



Configuração de segurança

```
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
```

Configuração completa do roteador

```
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
!
ntp server 172.16.1.1
end
```

Provisionamento, gerenciamento e monitoramento

O provisionamento e a configuração de recursos de telefonia IP baseados em roteador e firewall de política baseada em zona geralmente são mais bem acomodados com o Cisco Configuration Professional. O CiscoSecure Manager não suporta firewall de política baseada em zona ou telefonia IP baseada em roteador.

O Cisco IOS Classic Firewall suporta monitoramento SNMP com o Cisco Unified Firewall MIB. No entanto, o firewall de política baseado em zona ainda não é suportado na MIB do Unified Firewall. Como tal, o monitoramento de firewall deve ser tratado através de estatísticas na interface de linha de comando do roteador ou com ferramentas de GUI, como o Cisco Configuration Professional.

O Cisco Secure Monitoring And Reporting System (CS-MARS) oferece suporte básico para o Zone-Based Policy Firewall, embora as alterações de registro que melhoraram a correlação de mensagens de registro com o tráfego que foram implementadas em 12.4(15)T4/T5 e 12.4(20)T ainda não tenham sido totalmente suportadas no CS-MARS.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

O Cisco IOS Zone Firewall fornece comandos **show** e **debug** para exibir, monitorar e solucionar problemas da atividade do firewall. Esta seção fornece uma introdução aos comandos **debug** do Zone Firewall que fornecem informações detalhadas sobre a solução de problemas.

Comandos debug

Os comandos de depuração são úteis no caso de você usar uma configuração atípica ou não suportada e precisar trabalhar com o Cisco TAC ou com os serviços de suporte técnico de outros produtos para resolver problemas de interoperabilidade.

Observação: a aplicação de comandos **debug** a recursos ou tráfego específicos pode causar um número muito grande de mensagens do console, o que faz com que o console do roteador não responda. Mesmo que você precise habilitar a depuração, talvez queira fornecer acesso alternativo à interface de linha de comando, como uma janela telnet que não monitore a caixa de diálogo do terminal. Você só deve habilitar a depuração em equipamentos off-line (ambiente de laboratório) ou durante uma janela de manutenção planejada, uma vez que habilitar a depuração pode afetar substancialmente o desempenho do roteador.

Informações Relacionadas

- Guia de projeto de rede de referência da solução Cisco Unified CallManager Express
- Integração do Cisco Unity Connection com o Cisco Unified CME-as-SRST
- Referência de comandos do Cisco Unified Communications Manager Express
- Exemplo de configuração do Cisco CallManager Express/Cisco Unity Express
- Suporte MIB SNMP Cisco CallManager Express 3.4
- Guia de aplicativos e design de firewall de política baseada em zona
- Suporte Técnico e Documentação - Cisco Systems