Firewall baseado em zona do Cisco IOS: Office com gateway Cisco Unity Express/SRST/PSTN com conexão com o Cisco CallManager centralizado

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 AIC (Application Inspection and Control, inspeção e controle de aplicativos) 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 segurança separadamente, depois 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.

Conventions

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

Plano de fundo do Cisco IOS Firewall

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 contribui 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. Observe estas diretrizes ao decidir entre um roteador e um dispositivo:

- Roteador 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 são normalmente 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 Release 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, e exigiam grandes aberturas em políticas de firewall seguras para acomodar tráfego de voz e ofereciam suporte limitado para a sinalização VoIP em evolução e protocolos de mídia.

Configurar

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 confiança na rede forem identificados e descritos pela política de segurança. Há duas abordagens fundamentais para chegar a uma política de segurança: a perspectiva, 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*. Essa é 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 *bons* aplicativos, bem como o tráfego indesejado que está sendo mascarado como *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.

Consulte o Guia de Design e Aplicações do Firewall de Política Baseado em Zona para obter mais informações e informações adicionais sobre a configuração do Firewall de Política Baseado em Zona.

Considerações para ZFW em ambientes VoIP

O Guia de design e aplicativos mencionado anteriormente oferece uma breve discussão sobre a segurança do roteador com o uso de políticas de segurança para e da zona autônoma 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 de 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 do Cisco IOS Software Release 12.4(20)T, o Classic Firewall e o Zone-Based Policy Firewall não podiam acomodar totalmente os requisitos do 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 Cisco IOS Software Release 12.4(20)T.

Recursos de voz do Cisco IOS Firewall

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 Cisco CallManager ExpressAtualiza 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), conforme descrito porApresenta 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. Hiperlinks para os documentos de recursos individuais estão disponíveis na seção Informações Relacionadas no final deste documento, se você quiser revisar os detalhes completos dos recursos de inspeção de voz.

Caveats

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

NAT

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.

CUPC

Este documento não descreve a configuração que suporta o uso do Cisco Unified Presence Client (CUPC) com o Cisco 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 é suportado em uma versão futura do Cisco IOS Software.

Office com gateway Cisco Unity Express/SRST/PSTN que se conecta ao Cisco CallManager centralizado

Esse cenário difere dos aplicativos anteriores, pois o controle de chamadas centralizado é usado para todo o controle de chamadas, em vez do processamento de chamadas baseado em roteador distribuído. O correio de voz distribuído é aplicado, mas através do Cisco Unity Express no roteador. O roteador fornece a funcionalidade Survivable Remote Site Telephony e PSTN Gateway para discagem de emergência e discagem local. É recomendado um nível específico de capacidade de PSTN para acomodar falhas de discagem de desvio de tarifa baseada em WAN, bem como discagem de área local conforme descrito pelo plano de discagem. Além disso, as leis locais geralmente exigem que algum tipo de conectividade PSTN local seja fornecido para acomodar a discagem de emergência (911).

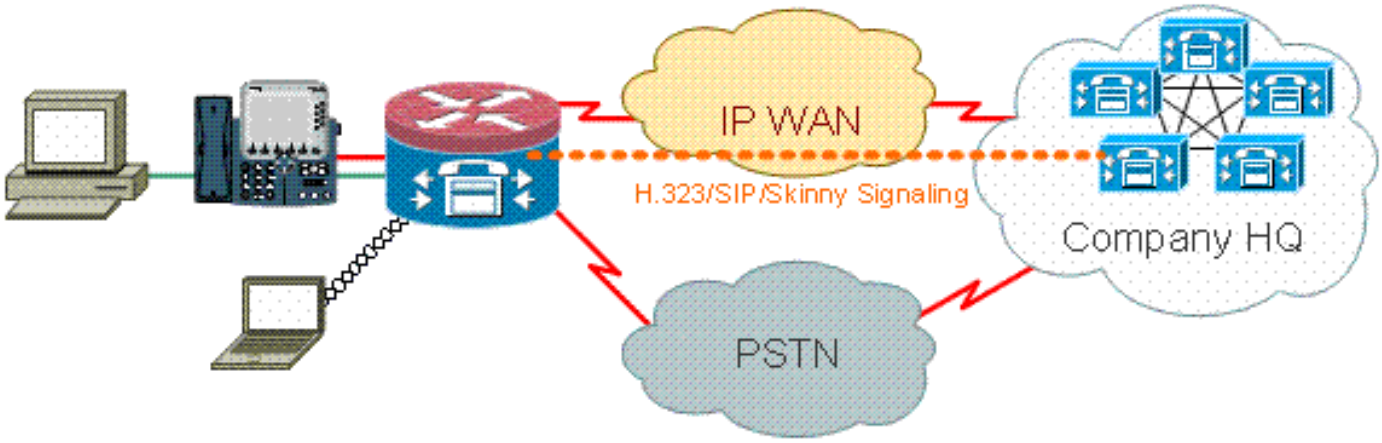
Esse cenário também pode aplicar o Cisco CallManager Express como o agente de processamento de chamadas para SRST, caso seja necessário um maior recurso de processamento de chamadas durante interrupções de WAN/CCM. Consulte Integração do Cisco Unity Connection com o Cisco Unified CME-as-SRST para obter mais informações.

Histórico do cenário

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

1. Inspeção de sinalização entre telefones locais e cluster remoto CUCM (SCCP e SIP)
2. Inspecione a sinalização H.323 entre o roteador e o cluster CUCM remoto.
3. Inspecione a sinalização entre os telefones locais e o roteador quando o link para o local remoto estiver inativo e o SRST estiver ativo.
4. Orifícios da mídia de voz para comunicação entre:Segmentos locais com e sem fioTelefones locais e remotosServidor MoH remoto e telefones locaisServidor Unity remoto e telefones locais para correio de voz
5. Aplicar AIC (Application Inspection and Control, inspeção e controle de aplicativos)

a:mensagens de convite de limite de taxaassegurar a conformidade do protocolo em todo o tráfego SIP.



Vantagens/Desvantagens

Esse cenário oferece o benefício de que a maioria do processamento de chamadas ocorre em um cluster central do Cisco CallManager, que oferece carga de gerenciamento reduzida. O roteador normalmente deve ter que lidar com menos carga de inspeção de recursos de voz locais em comparação com os outros casos descritos neste documento, já que a maior parte da carga de processamento de chamadas não é imposta ao roteador, exceto para tratar o tráfego de/para o Cisco Unity Express, e nos casos em que há uma interrupção de WAN ou CUCM, e o Cisco CallManager Express/SRST local é chamado para o processamento de chamadas.

A maior desvantagem desse caso, durante a atividade típica de processamento de chamadas, é que o Cisco Unity Express está localizado no roteador local. Embora isso seja bom do ponto de vista do projeto, por exemplo, o Cisco Unity Express está localizado mais próximo dos usuários finais onde o correio de voz é mantido, ele incorre em alguma carga adicional de gerenciamento, pois pode haver um grande número de Cisco Unity Express para gerenciar. Dito isso, com um Cisco Unity Express central para transportar as desvantagens opostas, pois um Cisco Unity Express central está mais distante dos usuários remotos e possivelmente não está acessível durante interrupções. Assim, os benefícios funcionais da oferta de correio de voz distribuído pela implantação do Cisco Unity Express para locais remotos oferecem a melhor opção.

Configurações para políticas de dados, firewall baseado em zona, segurança de voz, Cisco CallManager Express

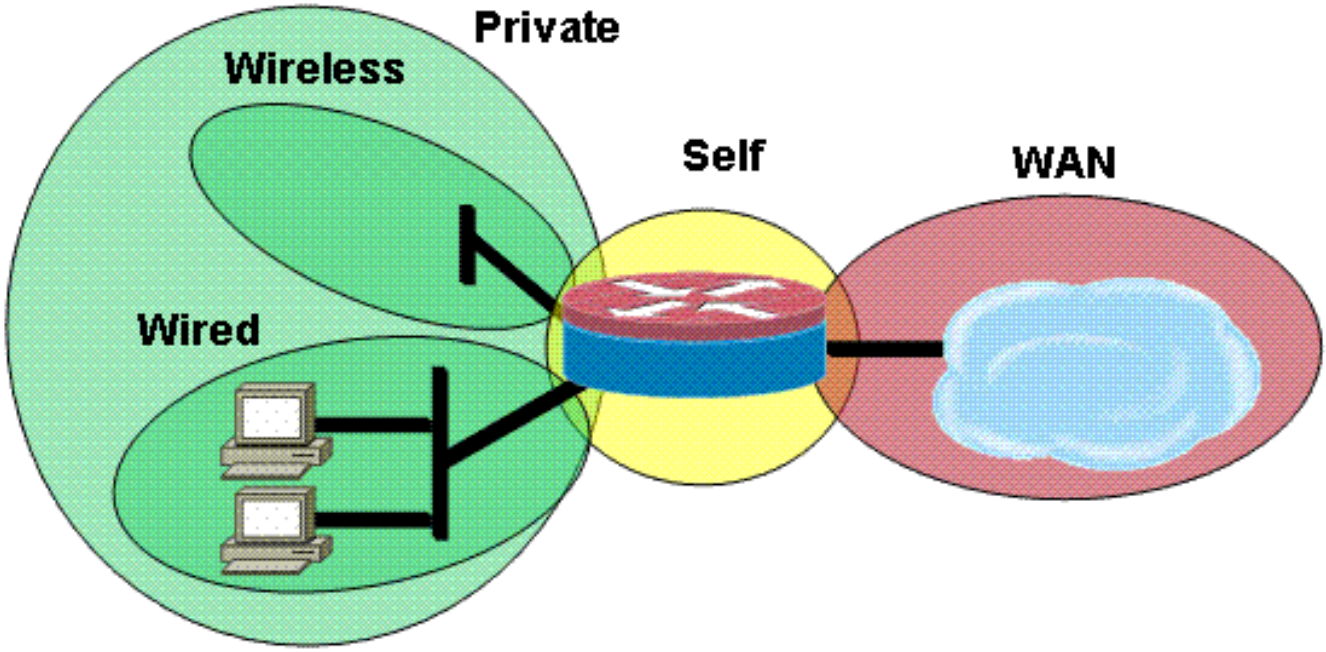
A configuração do roteador é baseada em um 3845 com um NME-X-23ES e um PRI HWIC:

Configuração do serviço de voz para conectividade SRST e Cisco Unity Express:

```
!
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
!
```

Este é um exemplo da Configuração do Firewall de Política Baseado em Zona, composta de zonas de segurança para segmentos de LAN com e sem fio, LAN privada, composta de segmentos com e sem fio, um segmento de WAN onde a conectividade de WAN confiável é alcançada e a zona de acesso à rede local 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
```

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
```

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. Mas o firewall de política baseado em zona ainda não é suportado no MIB do Unified Firewall. Como tal, o monitoramento de firewall deve ser tratado por meio 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 log com o tráfego que foram implementadas no Cisco IOS Software Release 12.4(15)T4/T5 e Cisco IOS Software Release 12.4(20)T ainda não tenham sido totalmente suportadas no CS-MARS.

Planejamento de capacidade

Resultados do teste de desempenho de inspeção de chamadas de firewall a ser definido pela Índia.

Verificar

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

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

O Cisco IOS Zone Firewall fornece comandos **show** e **debug** para exibir, monitorar e solucionar problemas da atividade do firewall. Esta seção descreve o uso dos comandos **show** para monitorar a atividade básica do firewall e uma introdução aos comandos **debug** do Zone Firewall para uma solução de problemas mais detalhada ou se a discussão com o suporte técnico exigir informações detalhadas.

Comandos para Troubleshooting

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

comandos show

O Cisco IOS Firewall oferece vários comandos **show** para visualizar a configuração e a atividade da política de segurança:

Muitos desses comandos podem ser substituídos por um comando mais curto por meio da aplicação do comando **alias**.

Comandos debug

Os comandos de **depuração** podem ser úteis no caso de você usar uma configuração atípica ou não suportada, e precisam trabalhar com o Cisco TAC ou 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 grande número de mensagens de console, o que faz com que o console do roteador não responda. Caso seja necessário ativar a depuração, é possível 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, porque se você habilitar a depuração, isso pode afetar substancialmente o desempenho do roteador.

Informações Relacionadas

- Guia de projeto de rede de referência da solução Cisco Unified CallManager Express
- Práticas recomendadas de segurança do 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 do Cisco IOS Firewall para tráfego local Skinny e CME
- Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems