IOS Zone-gebaseerde firewall: Configuratievoorbeeld van CME/CUE/GW single-Site of Branch Office PSTN-verbinding

Inhoud

Inleiding

Cisco Integrated Service Routers (ISR's) biedt een schaalbaar platform om gegevens en spraaknetwerkvereisten voor een brede reeks toepassingen aan te pakken. Hoewel het bedreigingslandschap van zowel privé als internet-verbonden netwerken een zeer dynamisch milieu is, biedt Cisco IOS Firewall stateful inspection and Application Inspection and Control (AIC) mogelijkheden om een veilige netwerkfunctie te definiëren en af te dwingen, terwijl het zaken vermogen en continuïteit toelaat.

Dit document beschrijft ontwerp- en configuratieoverwegingen voor firewallbeveiligingsaspecten van specifieke Cisco ISR-gebaseerde gegevens en spraaktoepassingsscenario's. Voor elk toepassingsscenario wordt de configuratie voor spraakservices en firewalls geboden. Elk scenario beschrijft de VoIP en de veiligheidsconfiguraties afzonderlijk, gevolgd door de gehele routerconfiguratie. Uw netwerk kan andere configuratie voor services zoals QoS en VPN vereisen om spraakkwaliteit en -vertrouwelijkheid te handhaven.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

IOS-firewallachtergrond

Cisco IOS Firewall wordt doorgaans ingezet in toepassingsscenario's die verschillen van de implementatiemodellen van wasmiddelfirewalls. Standaard implementaties omvatten telewerktoepassingen, kleine of bijkantoren en kleinschalige toepassingen, waar een laag aantal apparaten, integratie van meerdere services en een lagere prestatie- en beveiligingscapaciteit gewenst is.

Terwijl de toepassing van een inspectie van firewalls, samen met andere geïntegreerde services in de ISR-producten, vanuit kostenoogpunt en vanuit operationeel oogpunt aantrekkelijk zou kunnen lijken, moeten specifieke overwegingen worden geëvalueerd om te bepalen of een op router gebaseerde firewall geschikt is. De toepassing van elke extra eigenschap holt geheugen en verwerkingskosten uit en zal waarschijnlijk bijdragen aan het verminderen van het verzenden doorvoersnelheid, verhoogde pakketlatentie, en het verlies van eigenschap vermogen tijdens periodes van pieklading als een onderaangedreven geïntegreerde router-gebaseerde oplossing wordt ingezet.

Volg deze aanwijzingen wanneer u tussen een router en een apparaat beslist:

- Routers met meerdere geïntegreerde functies die ingeschakeld zijn, zijn het meest geschikt voor filialen of telecommunicatiesites waar minder apparaten een betere oplossing bieden.
- Grote bandbreedte, hoge prestaties, toepassingen worden meestal beter met apparaten aangepakt: Cisco ASA en Cisco Unified Call Manager Server moeten worden toegepast op de verwerking van NAT en beveiligingsbeleid en gespreksverwerking, terwijl routers de QoS-beleidstoepassing, WAN-beëindiging en VPN-aansluitingsvereisten voor site-to-site adresseren.

Vóór de introductie van Cisco IOS-softwarerelease 12.4(20)T, was Classic Firewall en Zone-Based Policy Firewall (ZFW) niet in staat om de functies die vereist zijn voor VoIP-verkeer en op router gebaseerde spraakservices volledig te ondersteunen, waardoor er grote openingen nodig zijn in anderszins veilig firewallbeleid om spraakverkeer aan te passen en beperkte ondersteuning

biedt voor evoluerende VoIP-signalering en mediaprotocollen.

Het implementeren van Cisco IOS Zone-Based Policy Firewall

Cisco IOS Zone-Based Policy Firewall, vergelijkbaar met andere firewalls, kan alleen een beveiligde firewall bieden als de beveiligingsvereisten van het netwerk worden geïdentificeerd en beschreven door beveiligingsbeleid. Er zijn twee fundamentele benaderingen om tot een veiligheidsbeleid te komen: het *vertrouwen* , in tegenstelling tot het *verdacht* perspectief .

Het *betrouwbare* perspectief veronderstelt dat al het verkeer betrouwbaar is, behalve dat wat specifiek kan worden geïdentificeerd als kwaadwillig of ongewenst. Er wordt een specifiek beleid ten uitvoer gelegd dat alleen het ongewenste verkeer ontkent. Dit wordt normaal bereikt door de gebruiks-specifieke access-control items, of op handtekening of gedrag gebaseerde tools. Deze benadering interfereert meestal minder met bestaande toepassingen, maar vereist een uitgebreide kennis van de bedreiging en het kwetsbaarheidslandschap, en vereist constant waakzaamheid om nieuwe bedreigingen en uitbuitingen aan te pakken zoals ze lijken. Daarnaast moet de gebruikersgemeenschap een grote rol spelen bij het handhaven van een adequate veiligheid. Een omgeving die ruime vrijheid biedt met weinig controle voor de bewoners biedt een substantiële kans voor problemen veroorzaakt door onachtzame of kwaadaardige individuen. Een bijkomend probleem van deze benadering is dat zij veel meer steunt op effectieve beheersinstrumenten en toepassingscontroles die voldoende flexibiliteit en prestaties bieden om verdachte gegevens in al het netwerkverkeer te kunnen controleren en controleren. Hoewel er momenteel technologie beschikbaar is om hieraan tegemoet te komen, overstijgt de operationele last dikwijls de limieten van de meeste organisaties.

Het *verdachte* perspectief veronderstelt al netwerkverkeer ongewenst is, behalve voor specifiek geïdentificeerd *goed* verkeer. Een beleid dat wordt toegepast dat al het toepassingsverkeer ontkent, behalve het verkeer dat uitdrukkelijk is toegestaan. Bovendien kan er met de inspectie en controle van toepassingen (AIC) rekening worden gehouden bij het identificeren en ontkennen van kwaadaardig verkeer dat specifiek is ontworpen voor het exploiteren van "goede" toepassingen, alsook van ongewenst verkeer dat zich als goed verkeer verspreidt. Toepassingscontroles leggen het netwerk opnieuw operationele en prestatieverplichtingen op, hoewel het meeste ongewenste verkeer moet worden gecontroleerd door stateless filters zoals toegangscontrolelijsten (ACL's) of Zone-Based Policy Firewall (ZFW) beleid, zodat er aanzienlijk minder verkeer moet worden verwerkt door AIC, inbraakpreventiesysteem (IPS) of andere op handtekening gebaseerde controles zoals flexibele pakketmatching (FPM) of op netwerk gebaseerde Application Recognition (NBAR). Indien alleen gewenste toepassingspoorten (en dynamisch mediaspecifiek verkeer dat voortvloeit uit bekende besturingsaansluitingen of sessies) uitdrukkelijk zijn toegestaan, dan moet het enige ongewenste verkeer dat op het netwerk aanwezig zou moeten zijn, vallen in een specifieke, gemakkelijker herkende subset, die de technische en operationele lasten vermindert die worden opgelegd om de controle over het ongewenste verkeer te behouden.

In dit document worden VoIP-beveiligingsconfiguraties beschreven op basis van het *verdachte* perspectief. derhalve is alleen verkeer toegestaan dat in de spraaknetwerksegmenten is toegestaan. Het gegevensbeleid heeft de neiging meer permissief te zijn, zoals wordt beschreven in opmerkingen in de configuratie van elk toepassingsscenario.

Alle implementaties van het beveiligingsbeleid moeten een terugkoppelingscyclus met een gesloten lus volgen; beveiligingsimplementaties hebben doorgaans gevolgen voor de capaciteit en de functionaliteit van bestaande toepassingen en moeten worden aangepast om deze impact te minimaliseren of op te lossen .

Raadpleeg voor meer informatie over het configureren van de Zone-Based Policy Firewall de Cisco IOS Firewall Zone-Based Policy Firewall Design en Application Guide.

OVERWEGINGEN VOOR ZFW IN VoIP-OMGEVINGEN

De Cisco IOS Firewall Zone-Based Policy Firewall Design en Application Guide biedt een korte discussie voor het beveiligen van de router met het gebruik van beveiligingsbeleid naar en van de eigen zone *van de router*, evenals alternatieve mogelijkheden die worden geboden door verschillende NFP-functies (Network Foundation Protection). De op router gebaseerde VoIP mogelijkheden worden aangeboden binnen de zelfzone van de router, zodat het veiligheidsbeleid dat de router beschermt zich bewust moet zijn van de vereisten voor spraakverkeer, om de spraaksignalering en de media aan te passen die door Cisco Unified CallManager Express, Survivable Remote-Site telefonie en de bronnen van de spraakgateway zijn geïnitieerd en bestemd zijn voor Cisco Unified CallManager Express. Vóór Cisco IOS-softwarerelease 12.4(20)T, was de Klastic Firewall en de Zone-Based Policy Firewall niet in staat om de vereisten van VoIP-verkeer volledig aan te passen, zodat het firewallbeleid niet optimaal was beschermd. Veiligheidsbeleid dat gericht is op het beschermen van routergebaseerde VoIP-bronnen is sterk afhankelijk van functies die in 12.4(20)T geïntroduceerd zijn.

IOS-spraakverbeteringen - 12.4(20)T

Cisco IOS-softwarerelease 12.4(20)T heeft verschillende verbeteringen geïntroduceerd om gelijktijdige inwoner Zone Firewall en spraakfuncties mogelijk te maken. Drie belangrijkste functies zijn direct van toepassing op beveiligde spraaktoepassingen:

- Verbeteringen in SIP: Toepassingslaag - gateway en toepassingsinspectie en -controleOndersteuning van SIP-versie voor SIPv2, zoals beschreven door RFC 3261Breedt SIP-signaleringsondersteuning uit om een breder scala aan callstromen te herkennenInleiding over SIP-toepassingsinspectie en -controle (AIC) om granulaire controles toe te passen om specifieke kwetsbaarheden op toepassingsniveau aan te pakken en misbruik te makenVergroot de inspectie van de zelfzone om secundaire signalering en mediakanalen te kunnen herkennen die het gevolg zijn van lokaal voorbestemd/van oorsprong SIP-verkeer
- Ondersteuning van Skinny Local Traffic and CMEOndersteuning van SCCP voor versie 16 (eerder ondersteunde versie 9)Inleiding over SCCP Application Inspection and Control (AIC) om granulaire controles toe te passen om specifieke kwetsbaarheden op toepassingsniveau aan te pakken en misbruik te maken vanVergroot de inspectie van de zelfzone om secundaire signalering en mediakanalen te kunnen herkennen die het gevolg zijn van lokaal voorbestemd/van oorsprong SCCP-verkeer
- Ondersteuning van H.323 v3/v4Ondersteuning van H.323 voor v3 en v4 bijwerken (voorheen ondersteund v1 en v2)Inleiding over H.323 Application Inspection and Control (AIC) om granulaire controles toe te passen op specifieke kwetsbaarheden op toepassingsniveau en exploitatie daarvan

De routerbeveiligingsconfiguraties die in dit document worden beschreven, bieden mogelijkheden die door deze verbeteringen worden geboden, met verklaring om de actie te beschrijven die door het beleid wordt toegepast. Raadpleeg voor volledige informatie over de functies voor spraakinspectie de afzonderlijke functiedocumenten die in het gedeelte Verwante informatie van dit document zijn opgenomen.

Caveats

Om eerder genoemde punten te versterken, moet de toepassing van Cisco IOS Firewall met routergebaseerde spraakmogelijkheden de op Zone gebaseerde beleidsfirewall toepassen. Classic IOS-firewall bevat niet de benodigde capaciteit om de signaleringscomplexiteiten en het gedrag van spraakverkeer volledig te ondersteunen.

Netwerkadresomzetting

Cisco IOS-netwerkadresomzetting (NAT) wordt vaak tegelijkertijd met Cisco IOS-firewall geconfigureerd, in het bijzonder in gevallen waarin particuliere netwerken moeten interface met het internet, of als afzonderlijke particuliere netwerken moeten verbinden, in het bijzonder als overlappende IP-adresruimte in gebruik is. Cisco IOS-software omvat NAT-toepassingslaaggateways (ALG's) voor SIP, Skinny en H.323. Idealiter kan de netwerkconnectiviteit voor IP-spraak worden aangepast zonder de toepassing van NAT, omdat NAT extra complexiteit veroorzaakt voor de probleemoplossing en security-beleidtoepassingen, in het bijzonder in gevallen waarin NAT-overload wordt gebruikt. NAT dient alleen te worden toegepast als oplossing voor het laatste geval om problemen met de netwerkconnectiviteit aan te pakken.

Cisco Unified Presence-client

Dit document beschrijft geen configuraties die het gebruik van Cisco Unified Presence Client (CUPC) met IOS-firewall ondersteunen, omdat CUPC nog niet ondersteund wordt door Zone of Clastic Firewall vanaf Cisco IOS-softwarerelease 12.4(20)T1. CUPC zal worden ondersteund in een toekomstige release van Cisco IOS-software.

CME/CUE/GW Single Site of Branch PSTN-verbinding

Dit scenario introduceert veilige router-gebaseerde Voice-over-IP telefonie voor kleine tot middelgrote bedrijven op één locatie of voor grotere multi-site organisaties die gedistribueerde gespreksverwerking willen implementeren, met behoud van bestaande verbindingen naar het openbare telefoonnetwerk (PSTN). De VoIP Call Control wordt geïntegreerd door de toepassing van een Cisco Unified Call Manager Express.

PSTN-connectiviteit kan op lange termijn worden onderhouden of naar een geconvergeerd spraak-en-data-IP-breedband netwerk worden gemigreerd, zoals wordt beschreven in het toepassingsvoorbeeld dat in de Single Site van CME/CUE/GW of het Vestigingsbureau met SIP Trunk naar CCM wordt besproken op het Hoofdkantoor of de sectie van de Spraakprovider van dit document.

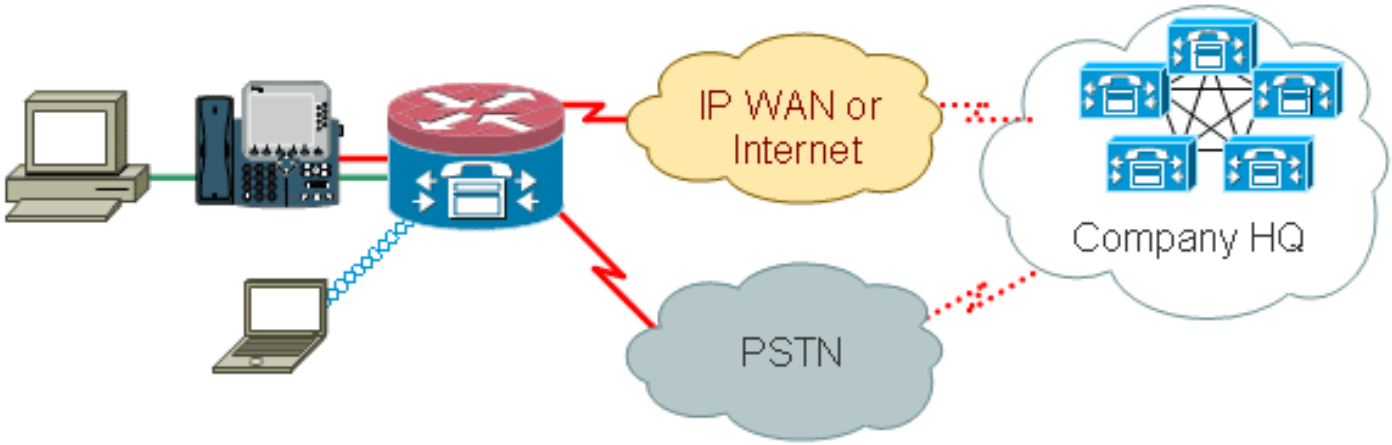
Organisaties zouden moeten overwegen dit type toepassingsscenario uit te voeren voor omstandigheden waarin verschillende VoIP-omgevingen tussen sites worden gebruikt of als VoIP niet praktisch is vanwege een ontoereikende WAN-gegevensconnectiviteit of locale-specifieke beperkingen op VoIP-gebruik op gegevensnetwerken. Voordelen en beste praktijken van IP-telefonie op één locatie worden beschreven in de Cisco Unified CallManager Express SRND.

Scenario Background

Het toepassingsscenario neemt bekabelde telefoons (spraak VLAN), bekabelde PC's (data VLAN), en draadloze apparaten (die VoIP apparaten zoals IP Communicator omvatten) in.

De veiligheidsconfiguratie voorziet in:

- Op router geïnitieerde signaleringsinspectie tussen CME en lokale telefoons (SCCP en/of SIP)
- Spraak-media gaten voor communicatie tussen:Lokale, bekabelde en draadloze segmentenCME en de lokale telefoons voor MoHCUE en de lokale telefoons voor spraak-mail
- Toepassingsinspectie en -controle (AIC) toepassen op:Offerte:Zorg dat het protocol conforme is op al het SIP-verkeer.



Voordelen en nadelen

Het meest voor de hand liggende voordeel van het VoIP-aspect van scenario is de migratiepad die wordt aangeboden door bestaande spraak- en datanetwerkinfrastructuur te integreren in een bestaande POTS/TDM-omgeving, voordat wordt overgestapt naar een geconvergeerd spraak/datanetwerk voor telefoniediensten naar de wereld buiten het LAN. Telefoonnummers worden onderhouden voor kleinere bedrijven en bestaande centrex- of DID-service kan worden gehandhaafd voor grotere organisaties die een gefaseerde migratie naar pakkettelefonie willen omzeilen.

De nadelen omvatten het verlies van kostenbesparingen die met tolbypass zouden kunnen worden verwezenlijkt door naar een geconvergeerd spraak-en-data netwerk te bewegen, zowel als beperkingen op het roepen van flexibiliteit en het gebrek aan organisatie-brede communicatie integratie en portabiliteit die met een volledig geconvergeerd spraak-en-data netwerk verwezenlijkt zouden kunnen worden.

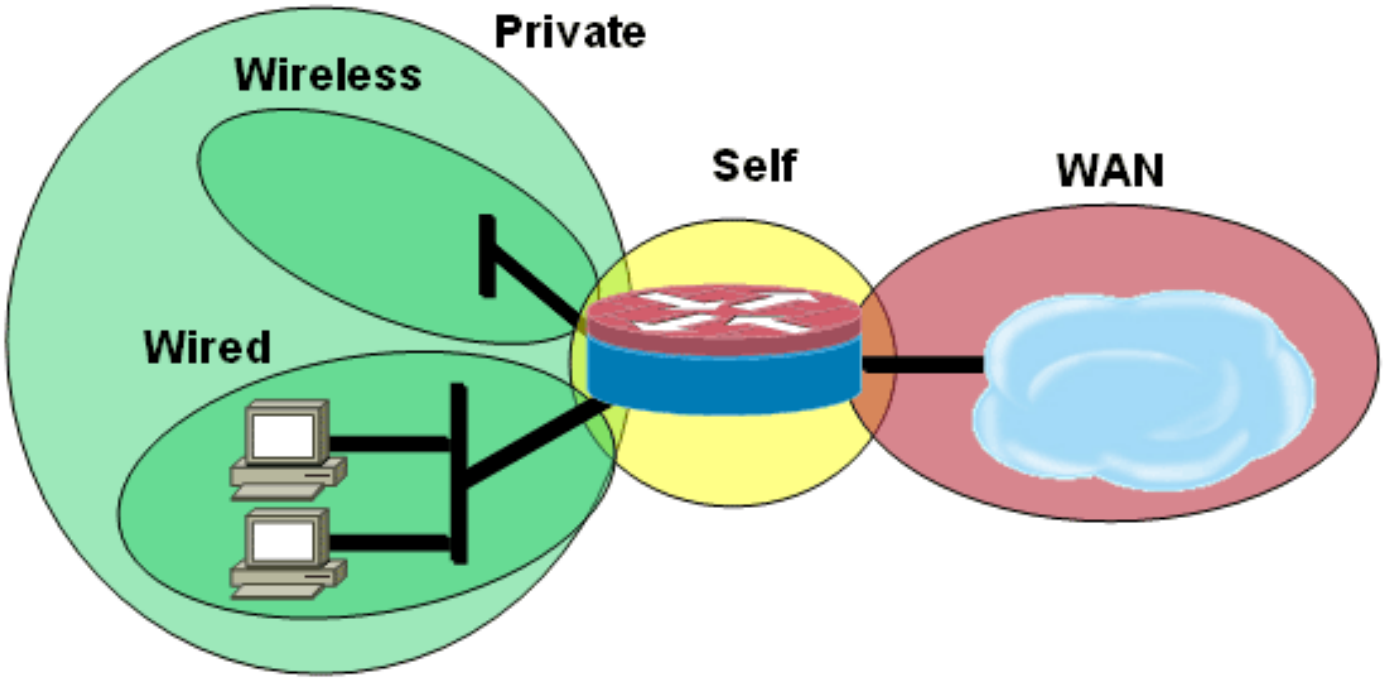
Vanuit een veiligheidsperspectief minimaliseert dit type netwerkomgeving VoIP-beveiligingsbedreigingen, door blootstelling van VoIP-bronnen aan het openbare netwerk of WAN te voorkomen. Maar de Cisco Call Manager Express die in de router is ingesloten, zou nog steeds kwetsbaar zijn voor interne bedreigingen zoals kwaadaardig verkeer of slecht functionerend toepassingsverkeer. Er wordt dus beleid gevoerd dat spraakspecifiek verkeer mogelijk maakt dat aan de controle van de conformiteit van het protocol voldoet, en er zijn specifieke VoIP-acties (d.w.z. SIP INVITE) beperkt om de kans op kwaadaardige of onbedoelde softwarestoringen die de VoIP-middelen en de bruikbaarheid negatief beïnvloeden, te verminderen.

Gegevensbeleid, op zone gebaseerde firewall, spraakbeveiliging en CCME-configuraties

De configuratie die hier wordt beschreven, illustreert een 2851-netwerk met een spraakconfiguratie voor CME en CUE-connectiviteit:

```
!
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
!
```

Zone-Based Policy Firewall Configuration, samengesteld uit beveiligingszones voor bekabelde en draadloze LAN-segmenten, privé LAN (samengesteld uit bekabelde en draadloze segmenten), een openbaar WAN-segment waar de onvertrouwde internetconnectiviteit is bereikt, en de zelfzone waar de spraakbronnen van de router zich bevinden.



Beveiligingsconfiguratie

```
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
```

Configuratie van volledige router

```
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
```

Provisioning, beheer en bewaking

Provisioning en configuratie voor zowel router-gebaseerde IP-telefonie-bronnen als Zone-Based Policy Firewall wordt over het algemeen het beste ingepast bij Cisco Configuration Professional. Cisco Secure Manager biedt geen ondersteuning voor Zone-Based Policy firewall of router-gebaseerde IP-telefonie.

Cisco IOS Clastic Firewall ondersteunt SNMP-bewaking met de Cisco Unified Firewall MIB. Zone-Based Policy Firewall wordt echter nog niet ondersteund in Unified Firewall MIB. Als dergelijke, moet de controle van de firewall via statistieken op de bevel-lijn interface van de router, of met GUI tools zoals Cisco Configuration Professional worden behandeld.

Cisco Secure Monitoring and Reporting System (CS-MARS) biedt basisondersteuning voor de Zone-Based Policy Firewall, hoewel de wijzigingen in de houtkap een betere correlatie tussen de logberichten en het verkeer mogelijk maken, die zijn geïmplementeerd in 12.4(15)T4/T5 en 12.4(20)T, nog niet volledig zijn ondersteund in CS-MARS.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Cisco IOS Zone Firewall biedt opdrachten voor **tonen** en **debug** van opdrachten om de activiteit van de firewall te bekijken, te controleren en op te lossen. Deze sectie verschaft een inleiding tot de **debug** van de Zone Firewall opdrachten die gedetailleerde informatie over probleemoplossing bevatten.

Opdrachten debug

Debug-opdrachten zijn handig als u een atypische of niet-ondersteunde configuratie gebruikt en u moet werken met de Cisco TAC of de technische ondersteuningsdiensten van andere producten om interoperabiliteitsproblemen op te lossen.

Opmerking: de toepassing van **debug** opdrachten naar bepaalde functies of verkeer kan een zeer groot aantal consoleboodschappen veroorzaken, waardoor de routerconsole niet meer reageert. In het zelfs dat u het debuggen moet inschakelen, zou u voor alternatieve opdrachtregel interface toegang kunnen bieden, zoals een telnet venster dat geen controle terminal dialoog. U dient alleen het debug op offline (labomgeving) apparatuur of tijdens een gepland onderhoudsvenster in te schakelen, aangezien het inschakelen van debug substantieel van invloed kan zijn op de routerprestaties.

Gerelateerde informatie

- Cisco Unified CallManager Express Solution Referentienetwerkgids
- Integratie met Cisco Unity Connection met Cisco Unified CME-as-SRST
- Referentie van Cisco Unified Communications Manager Express
- Cisco CallManager Express/Cisco Unity Express Configuratievoorbeeld

- Ondersteuning van Cisco CallManager Express 3.4 SNMP MIB
- Zone-Based Policy Firewall Design and Application Guide
- Technische ondersteuning en documentatie – Cisco Systems