Cisco IOS Zone-gebaseerde firewall CME/CUE/GW Single Site of Branch Office met SIP Trunk naar CCM op hoofdkwartier

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 dynamische omgeving is, biedt Cisco IOS® Firewall stateful inspection and Application Inspection and Control (AIC) mogelijkheden om een veilige netwerkhouding te definiëren en af te dwingen, terwijl het bedrijfsvermogen en continuïteit mogelijk maakt.

Dit document beschrijft ontwerp- en configuratieoverwegingen voor firewallbeveiligingsaspecten van specifieke Cisco ISR-gebaseerde gegevens en spraaktoepassingsscenario's. De configuraties voor spraakservices en de firewall worden voor elk toepassingsscenario geleverd. Elk scenario beschrijft de VoIP en de veiligheidsconfiguraties afzonderlijk, gevolgd door de gehele routerconfiguratie. Uw netwerk kan andere configuratie voor de diensten, zoals QoS en VPN, nodig hebben 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.

Conventies

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

Achtergrondinformatie

IOS-firewallachtergrond

De Cisco IOS Firewall wordt doorgaans ingezet in toepassingsscenario's die afwijken 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.

Hoewel de toepassing van een inspectie van firewalls, samen met andere geïntegreerde services in de ISR-producten, uit kostenoogpunt en vanuit operationeel oogpunt aantrekkelijk kan lijken, moeten specifieke overwegingen worden geëvalueerd om te bepalen of een op router gebaseerde firewall geschikt is. De toepassing van elke extra eigenschap overschrijdt geheugen en verwerkingskosten, en kan waarschijnlijk bijdragen aan het verminderde door-verzenden doorvoersnelheden, verhoogde pakketlatentie, en het verlies van functievermogen binnen periodes van pieklading als een onderaangedreven geïntegreerde router-gebaseerde oplossing wordt ingezet. Neem deze richtlijnen in acht wanneer u tussen een router en een apparaat kiest:

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

Vóór de introductie van Cisco IOS-softwarerelease 12.4(20)T, waren 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, die grote gaten in anderszins veilig firewallbeleid vereiste om spraakverkeer aan te passen en beperkte ondersteuning boden voor evoluerende VoIP-signalering en mediaprotocollen.

Cisco IOS Zone-Based Policy Firewall implementeren

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 doorgaans bereikt door de gebruiks-specifieke access-control ingangen 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 aan te pakken en te exploiteren 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 dat al het netwerkverkeer ongewenst is, behalve voor specifiek geïdentificeerd *goed* verkeer. Het is een beleid dat wordt toegepast, dat alle toepassingsverkeer ontkent, behalve dat wat expliciet is toegestaan. Daarnaast kan Application inspection and Control (AIC) worden geïmplementeerd om kwaadaardig verkeer te identificeren en te ontkennen dat specifiek gemaakt is om *goede* toepassingen te exploiteren, evenals ongewenst verkeer dat zich voordeed als *goed* verkeer. 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 is dat 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, moet het enige ongewenste verkeer dat op het netwerk aanwezig is, vallen in een specifieke, gemakkelijker herkende subset, die de technische en operationele last vermindert die wordt opgelegd om de controle over het ongewenste verkeer te behouden.

Dit document beschrijft VoIP-beveiligingsconfiguraties op basis van het *verdachte* perspectief, zodat alleen verkeer dat toegestaan is in de spraak-netwerksegmenten is toegestaan. Het gegevensbeleid heeft de neiging meer permissief te zijn zoals beschreven door noten in de configuratie van elk toepassingsscenario.

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

minimaliseren of op te lossen .

Als u extra achtergrond nodig hebt om de Zone-Based Policy Firewall te configureren, controleert u de Zone Firewall Design en de Application Guide.

OVERWEGINGEN VOOR ZFW IN VoIP-OMGEVINGEN

De Zone Firewall Design and Application Guide biedt een korte discussie over routerbeveiliging met het gebruik van beveiligingsbeleid naar en vanuit de zone van de router, evenals alternatieve mogelijkheden die worden geboden door verschillende NFP-functies (Network Foundation Protection). De op router gebaseerde VoIP-functies worden aangeboden binnen de eigen zone van de router, zodat het beveiligingsbeleid dat de router beschermt moet zijn bewust van de vereisten voor spraakverkeer om de spraaksignalering en de media op te nemen die zijn gegenereerd door en bestemd zijn voor Cisco Unified CallManager Express, Survivable Remote Site telefonie en Voice Gateway-bronnen. Voorafgaand aan de Cisco IOS-softwarerelease 12.4(20)T was de Classic 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 om resources volledig te beschermen. 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-spraakfuncties

De 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 signaleringskanalen 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 vanHiermee wordt de inspectie van de zelfzone uitgebreid zodat secundaire signalering- en mediakanalen kunnen worden herkend die het gevolg zijn van lokaal voorbestemd/van oorsprong SCCP-verkeer
- Ondersteuning van H.323 voor versies 3 en 4Ondersteuning van updates H.323 voor versies 3 en 4 (voorheen ondersteunde versies 1 en 2)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 verklaringen om de actie te beschrijven die door het beleid wordt toegepast. De hyperlinks naar de afzonderlijke functiedocumenten zijn beschikbaar in het gedeelte Verwante informatie van dit document als u de volledige details voor de functies voor spraakinspectie wilt bekijken.

Caveats

Om eerder genoemde punten te versterken, moet de toepassing van de Cisco IOS Firewall met routergebaseerde spraakmogelijkheden de Zone-Based Policy Firewall toepassen. De klassieke IOS Firewall bevat niet de benodigde capaciteit om de signaleringscomplexiteiten of het gedrag van spraakverkeer volledig te ondersteunen.

Netwerkadresomzetting (NAT)

De Cisco IOS-netwerkadresvertaling (NAT) wordt vaak tegelijkertijd geconfigureerd met de Cisco IOS-firewall, in het bijzonder in gevallen waar particuliere netwerken moeten interface met het internet of als afzonderlijke particuliere netwerken moeten verbinden, in het bijzonder als IP-adresruimte overlapt. De Cisco IOS-software bevat 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 oplossing van problemen en security-beleidtoepassingen, in het bijzonder in gevallen waarin NAT-overload wordt gebruikt. NAT kan alleen worden toegepast als oplossing in het laatste geval om problemen met de netwerkconnectiviteit aan te pakken.

Cisco Unified Presence Client (CUPC)

Dit document beschrijft geen configuratie die het gebruik van Cisco Unified Presence Client (CUPC) met IOS-firewall ondersteunt omdat CUPC nog niet wordt ondersteund door Zone of Classic 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 Office met SIP Trunk naar CCM op hoofdkwartier of bij spraakproviders

Dit scenario biedt een compromis tussen het model met één-site/gedistribueerde gespreksverwerking/PSTN-verbinding dat eerder in dit document is beschreven (CME/CUE/GW Single Site of Branch Office dat op PSTN aangesloten is) en het model met meerdere sites/gecentraliseerde gespreksverwerking/geconvergeerde spraak-en-gegevensnetwerk dat in het derde scenario is beschreven dat in dit document wordt beschreven. Dit scenario gebruikt nog steeds een lokaal Cisco Unified CallManager Express, maar de lange-afstandsbediening en de HQ/externe-site telefonie worden primair ingebed door site-to-site SIP-trunks, met lokaal gesprek en noodsignaal door een lokale PSTN-verbinding. Zelfs in gevallen waar de meerderheid van de legacy-PSTN-connectiviteit wordt verwijderd, wordt een basisniveau van PSTN-capaciteit aanbevolen om fouten te maken in het WAN-gebaseerde tolpasserdraaien en in het lokale gebied draaien zoals in het kiesschema wordt beschreven. Bovendien, vereisen lokale wetten gewoonlijk dat een of ander soort lokale PSTN connectiviteit wordt voorzien om in noodgeval (911) te draaien. Dit scenario maakt gebruik van gedistribueerde gespreksverwerking, die voordelen biedt en de beste praktijken waarneemt zoals die in de Cisco Unified CallManager Express SRND worden beschreven.

Organisaties kunnen dit soort toepassingsscenario in deze omstandigheden toepassen:

- Er worden verschillende VoIP-omgevingen tussen verschillende locaties gebruikt, maar VoIP is nog steeds gewenst in plaats van lange-afstand PSTN.
- Zelfstandigheid van plek tot locatie is nodig voor het toedienen van kiesschema's.

- Volledige Call-verwerkingscapaciteit is nodig ongeacht de beschikbaarheid van WAN.

Scenario Background

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

De veiligheidsconfiguratie voorziet in:

1. Op router geïnitieerde signaleringsinspectie tussen CME en lokale telefoons (SCCP en SIP) en CME en de Remote CUCM-cluster (SIP).
2. Spraak-media gaten voor communicatie tussen deze apparaten:Lokale, bekabelde en draadloze segmentenCME en de lokale telefoons voor MoHCUE en de lokale telefoons voor spraak-mailTelefoons en externe gespreksentiteiten
3. Toepassingsinspectie en -controle (AIC), die kunnen worden toegepast om deze te bereiken:Offerte:Zorg ervoor dat het protocol conforme is op al het SIP-verkeer

Voordelen/nadelen

Deze toepassing biedt het voordeel van verminderde kosten aangezien het site-to-site spraakverkeer op WAN datalink transporteert.

Een nadeel van dit scenario is dat de gedetailleerdere plannen voor WAN connectiviteit vereist zijn. De site-to-site call kwaliteit kan worden beïnvloed door vele factoren op het WAN, zoals illegaal/ongewenst verkeer (wormen, virussen, peer-to-peer file-sharing) of moeilijk-te identificeren latentieproblemen die kunnen ontstaan door verkeerstechniek op draagraketnetwerken. WAN-verbindingen moeten op de juiste wijze worden gesorteerd om voldoende bandbreedte voor zowel spraak- als gegevensverkeer te bieden; minder latency-gevoelig gegevensverkeer, bijvoorbeeld, e-mail, het midden- en kleinbedrijf/CIFS-bestandsverkeer, kan als lager-prioriteitsverkeer voor QoS worden geclassificeerd om de spraakkwaliteit te behouden.

Een ander probleem met dit scenario is het gebrek aan gecentraliseerde gespreksverwerking en de problemen die zich kunnen voordoen bij het oplossen van problemen bij de verwerking van gesprekken. Als zodanig werkt dit scenario het best voor grotere organisaties als een tussenstap in een migratie naar gecentraliseerde afhandeling van oproepen. Local Cisco CME’s kunnen worden geconverteerd om als volledig geïntegreerde SRST-back-up te fungeren wanneer de migratie naar Cisco CallManager is voltooid.

Vanuit het veiligheidsperspectief maakt de toegenomen complexiteit van deze omgeving effectieve beveiligingsimplementatie en het oplossen van problemen moeilijker omdat de connectiviteit via een WAN, of via VPN op het openbare internet, de bedreigingsomgeving drastisch vergroot, vooral in gevallen waar het veiligheidsbeleid een *betrouwbaar* perspectief vereist, waar weinig beperking op verkeer via WAN wordt opgelegd. Met dit in het achterhoofd voeren de configuratievoorbeelden in dit document een *verdacht* beleid uit dat specifiek zakenkritisch verkeer mogelijk maakt, dat vervolgens wordt onderzocht door controle van de conformiteit van het protocol. Bovendien zijn specifieke VoIP-acties, dat wil zeggen SIP INVITE, beperkt tot het beperken van de kans op kwaadaardige of onbedoelde softwarestoringen die de VoIP-middelen en de bruikbaarheid negatief beïnvloeden.

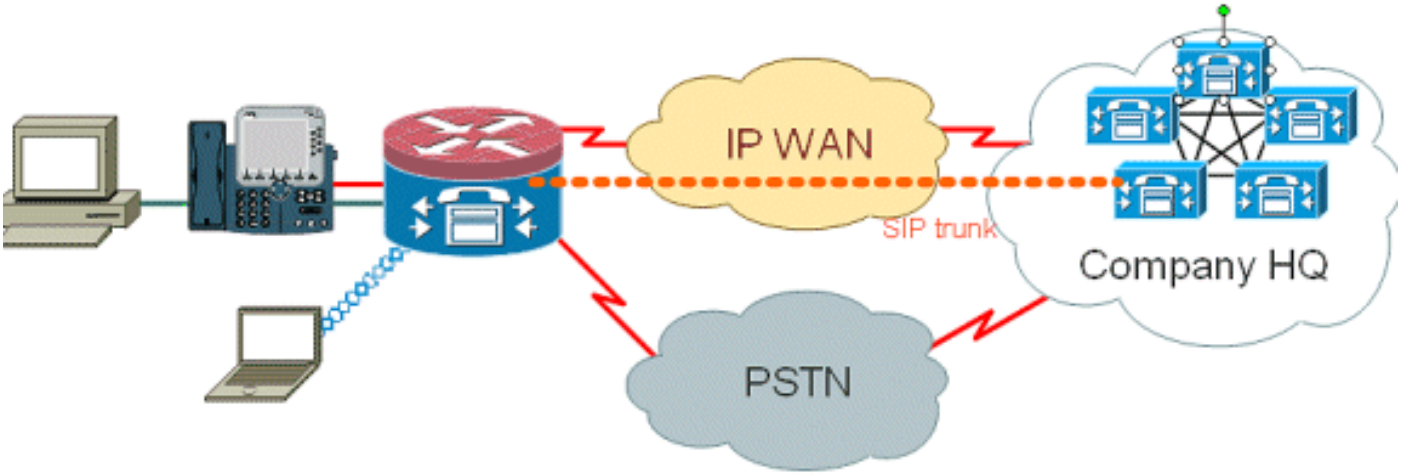
Configureren

Configuraties voor gegevensbeleid, zone-gebaseerde firewall, spraakbeveiliging en CCME

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

De configuratie die hier wordt beschreven, illustreert een Cisco 2851 geïntegreerde services router.

Dit document gebruikt deze configuraties:

- Configuratie van spraakservice voor CME en CUE-connectiviteit
- Configuratie van zone-gebaseerde beleidsfirewall
- Beveiligingsconfiguratie

Dit is de Voice Service Configuration voor CME en CUE-connectiviteit:

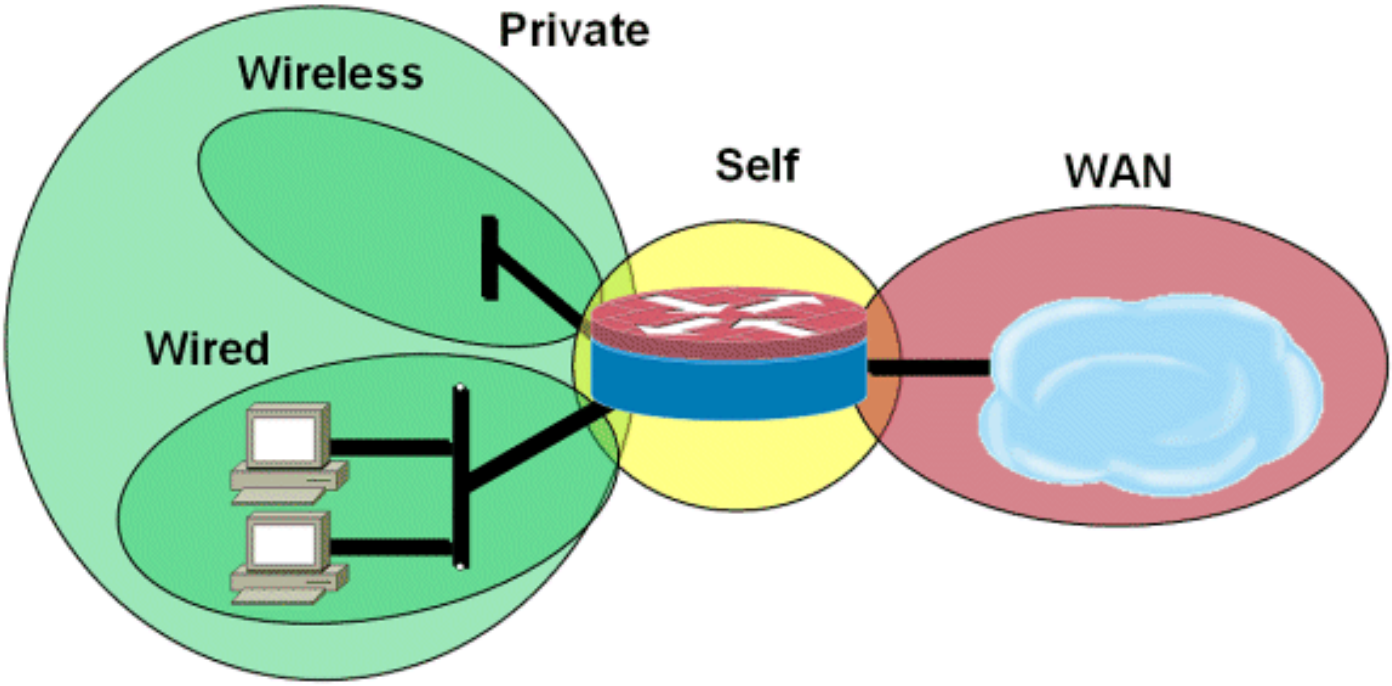
Configuratie van spraakservice voor CME en CUE-connectiviteit

```
!
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

!
```

Dit is de Zone-Based Policy Firewall Configuration, samengesteld uit beveiligingszones voor

bekabelde en draadloze LAN-segmenten, privé LAN (samengesteld uit bekabelde en draadloze segmenten), een WAN-segment waar de vertrouwde WAN-connectiviteit is bereikt en de zelfzone waarin de spraakbronnen van de router zich bevinden:



Dit is de Security Configuration:

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

Entire router configuration:

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 2851-cme2
!
!
logging message-counter syslog
logging buffered 51200 warnings
!
no aaa new-model
clock timezone mst -7
clock summer-time mdt recurring

!
dot11 syslog
ip source-route

!
!
ip cef
no ip dhcp use vrf connected

!
ip dhcp pool pub-112-net
network 172.17.112.0 255.255.255.0
default-router 172.17.112.1
dns-server 172.16.1.22
option 150 ip 172.16.1.43
domain-name bldrtme.com

!

ip dhcp pool priv-112-net
network 192.168.112.0 255.255.255.0
default-router 192.168.112.1
dns-server 172.16.1.22
domain-name bldrtme.com
option 150 ip 192.168.112.1

!
!
ip domain name yourdomain.com

!

no ipv6 cef
multilink bundle-name authenticated

!
!
!
!

voice translation-rule 1
```

```
rule 1 // /1001/

!
!

voice translation-profile default
translate called 1

!
!

voice-card 0
no dspfarm

!
!
!
!
!

interface GigabitEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
ip address 172.16.112.10 255.255.255.0
ip nat outside
ip virtual-reassembly
duplex auto
speed auto

!
interface GigabitEthernet0/1
no ip address
duplex auto
speed auto
 !
interface GigabitEthernet0/1.132
encapsulation dot1Q 132
ip address 172.17.112.1 255.255.255.0

!

interface GigabitEthernet0/1.152
encapsulation dot1Q 152
ip address 192.168.112.1 255.255.255.0
ip nat inside
ip virtual-reassembly

!

interface FastEthernet0/2/0

!

interface FastEthernet0/2/1

!

interface FastEthernet0/2/2

!

interface FastEthernet0/2/3

!
```

```
interface Vlan1
ip address 198.41.9.15 255.255.255.0

!

router eigrp 1
network 172.16.112.0 0.0.0.255
network 172.17.112.0 0.0.0.255
no auto-summary
!

ip forward-protocol nd
ip http server ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip http path flash:/gui

 !!

ip nat inside source list 111 interface
GigabitEthernet0/0 overload

!

access-list 23 permit 10.10.10.0 0.0.0.7
access-list 111 deny
ip 192.168.112.0 0.0.0.255 192.168.0.0 0.0.255.255
access-list 111 permit ip 192.168.112.0 0.0.0.255 any

!
!
!
!
!
!tftp-server flash:/phone/7940-7960/
P00308000400.bin alias P00308000400.bin
tftp-server flash:/phone/7940-7960/
P00308000400.loads alias P00308000400.loads
tftp-server flash:/phone/7940-7960/
P00308000400.sb2 alias P00308000400.sb2
tftp-server flash:/phone/7940-7960/
P00308000400.sbn alias P00308000400.sbn

!

control-plane

!
!
!

voice-port 0/0/0
connection plar 3035452366
description 303-545-2366
caller-id enable

!

voice-port 0/0/1 description FXO

!

voice-port 0/1/0
```

```
description FXS

!

voice-port 0/1/1 description FXS


!
!
!
!
!
dial-peer voice 804 voip
destination-pattern 5251...
session target ipv4:172.16.111.10
!
dial-peer voice 50 pots
destination-pattern A0
port 0/0/0
no sip-register

!
!
!
!

telephony-service
load 7960-7940 P00308000400
max-ephones 24
max-dn 24
ip source-address 192.168.112.1 port 2000
system message CME2
max-conferences 12 gain -6
transfer-system full-consult
create cnf-files version-stamp
7960 Jun 10 2008 15:47:13

 !!

ephone-dn 1
number 1001
trunk A0

!
!

ephone-dn 2
number 1002

!
!
ephone-dn 3
number 3035452366
label 2366
trunk A0

!
!

ephone 1
device-security-mode none
mac-address 0003.6BC9.7737
type 7960
button 1:1 2:2 3:3
```

```
!
!
!

ephone 2
device-security-mode none
mac-address 0003.6BC9.80CE
type 7960
button 1:2 2:1 3:3

!
!
!

ephone 5
device-security-mode none

!
!
!

line con 0
exec-timeout 0 0
login local
line aux 0
line vty 0 4
access-class 23 in
privilege level 15
login local
transport input telnet ssh

line vty 5 15
access-class 23 in
privilege level 15
login local
transport input telnet ssh

!
exception data-corruption buffer truncate
scheduler allocate 20000 1000
ntp server 172.16.1.1
end
```

Voorziening, beheer en bewaking

De voorziening en configuratie voor zowel routergebaseerde IP-telefonie-bronnen als Zone-Based Policy Firewall is over het algemeen het best geschikt voor Cisco Configuration Professional. Cisco Secure Manager ondersteunt geen Zone-Based Policy firewall of routergebaseerde IP-telefonie niet.

Cisco IOS Classic Firewall ondersteunt SNMP-bewaking met de Cisco Unified Firewall MIB, maar Zone-Based Policy Firewall wordt nog niet ondersteund in Unified Firewall MIB. Als dergelijk, moet de controle van de firewall door statistieken op de commando-lijn interface van de router, of met GUI tools, zoals de Cisco Configuration Professional.

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

Capaciteitsplannen

De testresultaten van de Call Inspection-test van firewalls in India zijn TBD.

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. In dit gedeelte wordt het gebruik van de opdrachten van de **show** beschreven om de fundamentele firewallactiviteit te controleren en wordt een inleiding naar de **debug** opdrachten van de Zone Firewall beschreven om uw configuratie problemen op te lossen of indien voor discussie met technische ondersteuning gedetailleerdere informatie nodig is.

Opdrachten voor troubleshooting

De Cisco IOS Firewall biedt verschillende opdrachten **voor** het bekijken van de configuratie en activiteit van het beveiligingsbeleid. Veel van deze opdrachten kunnen worden vervangen door een kortere opdracht door de toepassing van de opdracht **alias**.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Debug-opdrachten kunnen nuttig zijn in het geval dat u een atypische of niet-ondersteunde configuratie gebruikt en moeten werken met de Cisco TAC of de technische ondersteuning van andere producten om interoperabiliteitsproblemen op te lossen.

Opmerking: de toepassing van **debug** opdrachten naar specifieke functies of verkeer kan een zeer groot aantal consoleboodschappen veroorzaken, waardoor de routerconsole niet meer reageert. In het zelfs dat u moet zuiveren, kunt u voor alternatieve commando-lijn interfacetoegang, zoals een venster van Telnet verstrekken dat terminal geen dialoog controleert. Laat slechts toe om on-line (lab milieu) apparatuur of binnen een gepland onderhoudsvenster te debug kan substantieel van invloed zijn op routerprestaties.

Gerelateerde informatie

- Cisco Unified CallManager Express Solution Referentienetwerkgids
- Cisco CallManager Express security beste praktijken (CME SRND)
- 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
- Cisco IOS-firewall: Verbeteringen in SIP: ALG en AIC
- Ondersteuning van Cisco IOS-firewall H.323

- Cisco IOS-firewallondersteuning voor Snipperd lokaal verkeer en CME
- Technische ondersteuning en documentatie – Cisco Systems