Cisco IOS Zone-gebaseerde firewall Office met Cisco Unity Express/SRST/PSTN-gateway met verbinding met Gecentraliseerde Cisco CallManager

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 netwerkpositie te definiëren en af te dwingen, terwijl u zaken en continuïteit mogelijk maakt.

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, dan 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.

Conventies

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

Cisco IOS-firewallachtergrond

Cisco IOS Firewall wordt gewoonlijk 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.

Terwijl de toepassing van een inspectie van firewalls, samen met andere geïntegreerde services in de ISR-producten, vanuit 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 draagt waarschijnlijk bij aan het verminderen van het verzenden van doorvoersnelheden, verhoogde pakketlatentie, en het verlies van eigenschap vermogen tijdens 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:

- Router met meerdere geïntegreerde functies die mogelijk zijn, is het meest geschikt voor filiaal-kantoor of telecommunicatiesites waar minder apparaten een betere oplossing bieden
- Hoge 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, en vereiste grote openingen in anderszins beveiligd firewallbeleid om spraakverkeer te ontvangen en heeft beperkte ondersteuning geboden voor evoluerende VoIP-signalering en mediaprotocollen.

Configureren

Invoering 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 de netwerkvertrouwen worden geïdentificeerd en beschreven door beveiligingsbeleid. Er zijn twee fundamentele benaderingen om tot een veiligheidsbeleid te komen: het perspectief , 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. Dit is een beleid dat wordt toegepast dat alle toepassingsverkeer ontkent, behalve het verkeer dat uitdrukkelijk 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 vermengd met *goed* verkeer, te identificeren. 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 de gewenste toepassingspoorten en het dynamische, op de media gerichte verkeer als gevolg van bekende regelverbindingen of sessies uitdrukkelijk zijn toegestaan, 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 machtiger te zijn, zoals wordt beschreven door opmerkingen 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.

Raadpleeg de Zone-Based Policy Firewall Design and Application Guide voor meer informatie en extra achtergrondinformatie voor de configuratie van de Zone-Based Policy Firewall.

OVERWEGINGEN VOOR ZFW IN VoIP-OMGEVINGEN

De eerder genoemde Design and Application Guide biedt een korte discussie voor de beveiliging van de router met het gebruik van beveiligingsbeleid naar en van de zelfzone 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 geoptimaliseerd was om resources volledig te beschermen. Een eigen beveiligingsbeleid dat routergebaseerde VoIP-bronnen beschermt, is sterk afhankelijk van functies die in Cisco IOS-softwarerelease 12.4(20)T zijn geïntroduceerd.

Cisco IOS-spraakfuncties

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 Snipperend lokaal verkeer en Cisco CallManager ExpressOndersteuning 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 (voorheen ondersteund v1 en v2) wordt bijgewerkt, zoals beschreven doorInleiding 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. De hyperlinks naar de afzonderlijke functiedocumenten zijn beschikbaar in het gedeelte Verwante informatie aan het eind van dit document als u de volledige details voor de functies voor spraakinspectie wilt bekijken.

Caveats

De toepassing van Cisco IOS Firewall met routergebaseerde spraakmogelijkheden moet de Zone-Based Policy Firewall toepassen om punten te versterken die eerder werden vermeld. Classic IOS-firewall bevat niet de benodigde capaciteit om de signaleringscomplexiteiten en het gedrag van spraakverkeer volledig te ondersteunen.

NAT

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 introduceert voor de oplossing van problemen en security-beleidtoepassingen, vooral 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.

CUPC

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

Office met Cisco Unity Express/SRST/PSTN-gateway voor verbindingen met Gecentraliseerde Cisco CallManager

Dit scenario verschilt van de vorige toepassingen, in die zin dat de gecentraliseerde aanroep-controle voor alle aanroep-controle wordt gebruikt, in plaats van gedistribueerde router-gebaseerde gespreksverwerking. Gedistribueerde spraak-mail wordt toegepast, maar via Cisco Unity Express op de router. De router biedt Survivable Remote Site telefonie en PSTN-gateway voor noodbellen en lokale inbellen. Een applicatiespecifiek niveau van PSTN-capaciteit wordt aanbevolen om fouten van WAN-gebaseerde toldobypass-dialing op te vangen, evenals een lokale gebiedsselectie zoals beschreven in het kiesschema. Bovendien, vereisen lokale wetten gewoonlijk dat een of ander soort lokale PSTN connectiviteit wordt voorzien om in noodgeval (911) te draaien.

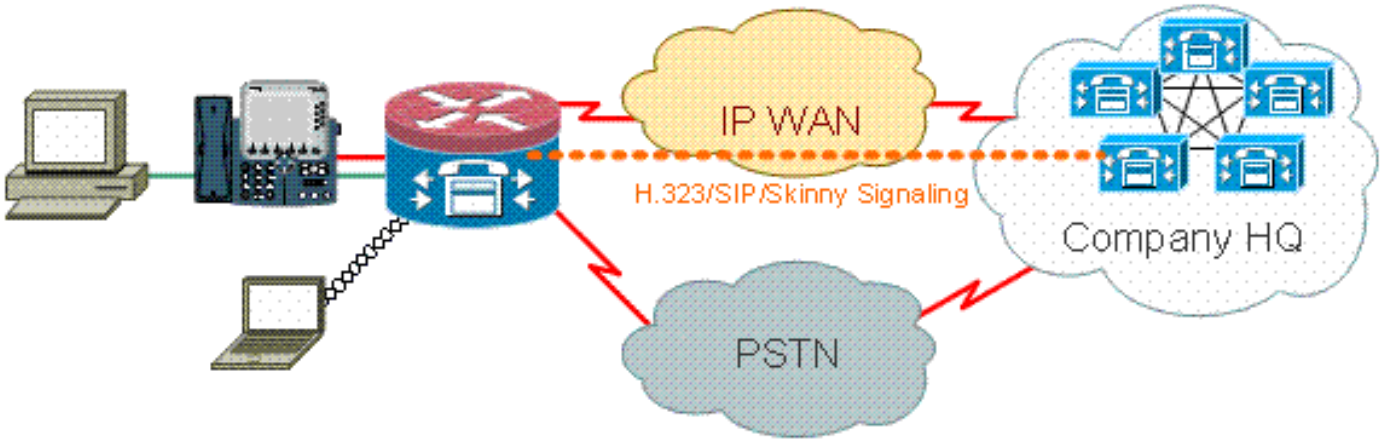
Dit scenario kan Cisco CallManager Express ook toepassen als de Call Processing Agent voor SRST, voor het geval dat er een grotere Call-verwerkingscapaciteit nodig is tijdens WAN/CCM-uitgangen. Raadpleeg voor Integratie met Cisco Unity Connection met Cisco Unified CME-as-SRST voor meer informatie.

Scenario Background

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

1. Signalering-inspectie tussen lokale telefoons en extern CUCM-cluster (SCCP en SIP)
2. Controleer H.323-signalering tussen de router en het elders geplaatste CUCM-cluster.
3. Inspecteer het signaleren tussen de lokale telefoons en de router wanneer de verbinding met de verre plaats is en SRST actief is.
4. Spraak-media gaten voor communicatie tussen:Lokale, bekabelde en draadloze segmentenLokale en externe telefoonsRemote MoH-server en lokale telefoonsRemote Unity server en lokale telefoons voor spraak-mail

5. Toepassingsinspectie en -controle (AIC) toepassen op:oproep tot indiening van voorstellenverzeker u protocol conformiteit op al het SIP-verkeer.



Voordelen/nadelen

Dit scenario biedt het voordeel dat de meerderheid van vraagverwerking in een centrale cluster van Cisco CallManager voorkomt, die verminderde beheerlasten biedt. De router moet normaal gesproken minder lokale inspectie van spraak-middelen moeten aanpakken in vergelijking met de andere gevallen die in dit document worden beschreven, aangezien de meerderheid van de last van de vraagverwerking niet op de router wordt opgelegd, behalve voor de verwerking van verkeer naar/van de Cisco Unity Express en in gevallen wanneer er een WAN of CUCM-uitgang is, en lokale Cisco CallManager Express/SRST wordt geroepen om telefoonverwerking aan te pakken.

Het grootste nadeel van deze case tijdens de typische call-processing activiteit, is dat Cisco Unity Express op de lokale router staat. Hoewel dit vanuit ontwerpperspectief goed is, ligt de Cisco Unity Express bijvoorbeeld het dichtst bij de eindgebruikers waar voicemail wordt bewaard, neemt het enige extra beheerlasten op, in die zin dat er een groot aantal Cisco Unity Express moet worden beheerd. Dit gezegd hebbende, met een centrale Cisco Unity Express om de tegenovergestelde nadelen te dragen, in die zin dat een centrale Cisco Unity Express verder verwijderd is van externe gebruikers, en mogelijk niet toegankelijk is tijdens tekorten. Dus de functionele voordelen van gedistribueerd voicemail aanbod door de plaatsing van Cisco Unity Express naar afgelegen locaties biedt de superieure keuze.

Configuraties voor gegevensbeleid, Zone-gebaseerde firewall, spraakbeveiliging, Cisco CallManager Express

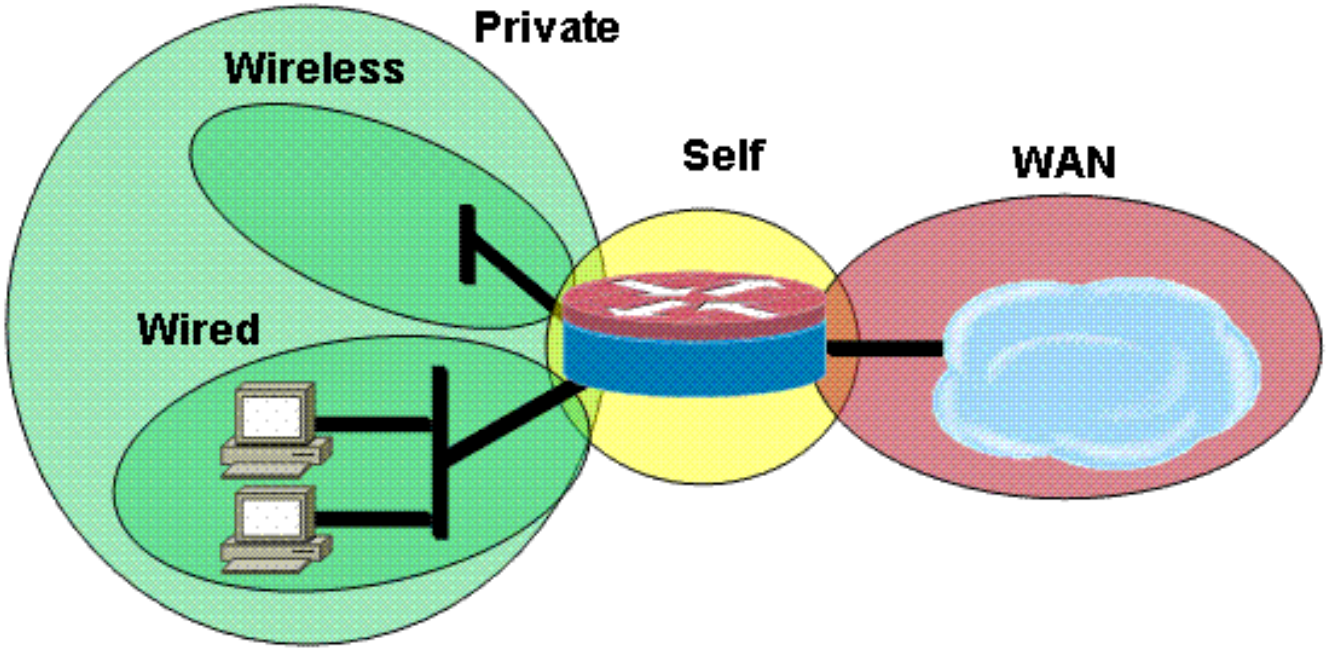
De routerconfiguratie is gebaseerd op een 3845 router met een NME-X-23ES en een PRI HWIC:

Spraakservicemodule voor SRST en Cisco Unity Express 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 een voorbeeld van de Zone-Based Policy Firewall Configuration, samengesteld uit beveiligingszones voor bekabelde en draadloze LAN-segmenten, privé LAN, dat bestaat uit bekabelde en draadloze segmenten, een WAN-segment waar een vertrouwde WAN-connectiviteit wordt 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
```

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
```

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. 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 Cisco Configuration Professional worden verwerkt.

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

Capaciteitsplanning

Resultaten van de in het firewall-systeem uitgevoerde prestatietest van de Indiase TBD.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Cisco IOS Zone Firewall biedt opdrachten voor **tonen** en **debug** van opdrachten om de activiteit van de firewall te bekijken, te controleren en problemen op te lossen. In dit gedeelte wordt het gebruik van de opdrachten van de **show** beschreven om de fundamentele firewallactiviteit te controleren en een inleiding op de **debug** opdrachten van de Zone Firewall voor een gedetailleerdere oplossing, of indien voor discussie met technische ondersteuning gedetailleerde informatie nodig is.

Opdrachten voor troubleshooting

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

Opdrachten weergeven

Cisco IOS Firewall biedt verschillende opdrachten om de configuratie en activiteit van het beveiligingsbeleid te bekijken:

Veel van deze opdrachten kunnen worden vervangen door een kortere opdracht door toepassing van de opdracht **alias**.

Opdrachten debug

Opdrachten Debug kunnen nuttig zijn voor het geval 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: toepassing van **debug** opdrachten naar specifieke functies of verkeer kan een zeer groot aantal consoleboodschappen veroorzaken, waardoor de routerconsole niet meer reageert. In het geval dat u het debuggen moet inschakelen, is het mogelijk om alternatieve verbinding tussen de opdrachtregel te bieden, zoals een telnet venster dat de terminaldialoog niet controleert. U dient alleen in te schakelen op off-line (lab-omgeving) apparatuur of tijdens een gepland onderhoudsvenster, omdat deze, als u debug toestaat, aanzienlijk van invloed kan zijn op de routerprestaties.

Gerelateerde informatie

- Cisco Unified CallManager Express Solution Referentienetwerkgids
- Beste praktijken voor Cisco Unified CallManager Express security
- 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-firewallondersteuning voor Snipperd lokaal verkeer en CME
- Cisco IOS Firewall
- Technische ondersteuning en documentatie – Cisco Systems