IOS 영역 기반 방화벽:CME/CUE/GW 단일 사이트 또는 지사 PSTN 연결 구성 예

목차

소개

Cisco ISR(Integrated Service Router)은 광범위한 애플리케이션에 대한 데이터 및 음성 네트워크 요구 사항을 해결할 수 있는 확장 가능한 플랫폼을 제공합니다.프라이빗 및 인터넷 연결 네트워크의 위협 환경은 매우 동적인 환경이지만, Cisco IOS Firewall은 보안 네트워크 상태를 정의하고 적용하는 동시에 비즈니스 기능과 연속성을 가능하게 하는 상태 기반 검사 및 AIC(Application Inspection and Control) 기능을 제공합니다.

이 문서에서는 특정 Cisco ISR 기반 데이터 및 음성 애플리케이션 시나리오의 방화벽 보안 측면에 대한 설계 및 구성 고려 사항에 대해 설명합니다.각 애플리케이션 시나리오에 대해 음성 서비스 및 방화벽 구성이 제공됩니다.각 시나리오에서는 VoIP 및 보안 컨피그레이션을 개별적으로 설명하고 전체 라우터 컨피그레이션을 설명합니다.음성 품질과 기밀성을 유지하기 위해 네트워크에서 QoS 및 VPN 같은 서비스에 대한 다른 컨피그레이션이 필요할 수 있습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

IOS 방화벽 배경

Cisco IOS 방화벽은 일반적으로 어플라이언스 방화벽의 구축 모델과 다른 애플리케이션 시나리오에 구축됩니다.일반적인 구축 환경으로는 Teleworker 애플리케이션, 소규모 또는 지사 사이트, 소매 애플리케이션 등이 있는데, 여기에는 낮은 장치 수, 여러 서비스의 통합, 낮은 성능 및 보안 기능 수준이 필요합니다.

ISR 제품의 다른 통합 서비스와 함께 방화벽 검사 애플리케이션이 비용 및 운영 측면에서 매력적인 것처럼 보일 수 있지만, 라우터 기반 방화벽이 적절한지 확인하기 위해 구체적인 고려 사항을 평가해야 합니다.각각의 추가 기능을 적용하면 메모리 및 처리 비용이 발생하며, 성능이 낮은 통합 라우터 기반 솔루션을 구축할 경우 피크 로드 기간 동안 전달 처리량 속도 감소, 패킷 레이턴시 증가, 기능 기능 손실의 원인이 될 것입니다.

라우터와 어플라이언스를 결정할 때 다음 지침을 따르십시오.

- 여러 개의 통합 기능이 활성화된 라우터는 더 적은 장치가 더 나은 솔루션을 제공하는 지사 또는 재택 근무 사이트에 가장 적합합니다.
- 일반적으로 고대역폭, 고성능 애플리케이션은 어플라이언스로 더 효과적으로 처리됩니다.Cisco ASA 및 Cisco Unified Call Manager Server를 적용하여 NAT 및 보안 정책 애플리케이션 및 통화 처리를 처리하고 라우터는 QoS 정책 애플리케이션, WAN 종료 및 Site-to-Site VPN 연결 요구 사항을 해결해야 합니다.

Cisco IOS Software 버전 12.4(20)T가 도입되기 전에 Classic Firewall 및 ZFW(Zone-Based Policy Firewall)는 VoIP 트래픽 및 라우터 기반 음성 서비스에 필요한 기능을 완벽하게 지원할 수 없었으며, 음성 트래픽을 수용하기 위해 보안 방화벽 정책에 큰 구멍이 필요했으며, 진화하는 VoIP 신호 및 미디어 프로토콜을 제한적으로 지원할 수 있었습니다.

Cisco IOS Zone-Based Policy Firewall 구축

Cisco IOS Zone-Based Policy Firewall은 다른 방화벽과 유사하게 보안 정책에 의해 네트워크의 보안 요구 사항을 식별하고 설명하는 경우에만 보안 방화벽을 제공할 수 있습니다.보안 정책에 도달하기 위한 두 가지 기본적인 접근 방식이 있습니다.*의심스러운* 관점과 대조적으로 신뢰하는 관점.

신뢰하는 *관점*은 모든 트래픽이 신뢰할 수 있다고 가정합니다. 단, 악성 또는 원치 않는 트래픽으로 구체적으로 식별될 수 있습니다.원하지 않는 트래픽만 거부하는 특정 정책이 구현됩니다.이 작업은 일반적으로 특정 액세스 제어 항목 또는 시그니처 또는 동작 기반 툴을 사용하여 수행합니다.이러

한 접근 방식은 기존 애플리케이션에 방해가 되는 경향이 있지만, 위협 및 취약성 환경에 대한 포괄적인 지식이 필요하며, 새로운 위협과 익스플로잇을 나타나는 즉시 해결하기 위해 끊임없는 경계가 필요합니다.또한 사용자 커뮤니티는 적절한 보안을 유지하는 데 큰 역할을 해야 합니다.거주자에 대한 제어가 거의 없는 광범위한 자유를 허용하는 환경은 부주의한 또는 악의적인 개인들로 인해 야기되는 문제에 상당한 기회를 제공합니다.이 접근 방식의 또 다른 문제는 모든 네트워크 트래픽에서 의심스러운 데이터를 모니터링하고 제어할 수 있는 충분한 유연성과 성능을 제공하는 효과적인 관리 툴과 애플리케이션 제어에 훨씬 더 많이 의존한다는 것입니다.현재 기술을 사용할 수 있지만 운영 부담이 대부분의 조직의 한계를 초과하는 경우가 많습니다.

의심스러운 관점은 특별히 식별된 *양호한* 트래픽을 제외하고 모든 네트워크 트래픽이 바람직하지 않다고 가정합니다.명시적으로 허용된 애플리케이션 트래픽을 제외한 모든 애플리케이션 트래픽을 거부하는 정책이 적용됩니다.또한 AIC(Application Inspection and Control)를 구현하여 '정상' 애플리케이션을 악용하기 위해 특별히 제작된 악성 트래픽과 양호한 트래픽으로 가장하는 원치 않는 트래픽을 식별하고 거부할 수 있습니다.애플리케이션 제어는 ACL(Access-Control Lists) 또는 ZFW(Zone-Based Policy Firewall) 정책과 같은 스테이트리스(stateless) 필터에 의해 제어되어야 하지만, 네트워크에 운영 및 성능 부담을 가중시킵니다. 따라서 AIC, IPS(Intrusion Prevention System) 또는 FPM(Flexible Packet Matching) 또는 NBAR(network-based application recognition)과 같은 기타 시그니처 기반 제어를 통해 처리해야 하는 트래픽이 상당히 적습니다. 따라서 원하는 애플리케이션 포트(그리고 알려진 제어 연결 또는 세션으로 인해 발생하는 동적 미디어별 트래픽)만 특별히 허용될 경우, 네트워크에 존재해야 하는 불필요한 트래픽만 더 쉽게 인식되는 특정 하위 집합에 속해야 합니다. 그러면 원치 않는 트래픽에 대한 제어를 유지하기 위해 요구되는 엔지니어링 및 운영 부담이 줄어듭니다.

이 문서에서는 *의심스러운* 관점을 기준으로 VoIP 보안 컨피그레이션에 대해 설명합니다.따라서 음성 네트워크 세그먼트에서 허용되는 트래픽만 허용됩니다.각 애플리케이션 시나리오의 컨피그레이션에 있는 메모에 설명된 대로 데이터 정책은 더욱 허용적입니다.

모든 보안 정책 구축은 폐쇄 루프 피드백 주기를 따라야 합니다.보안 구축은 일반적으로 기존 애플리케이션의 기능 및 기능에 영향을 미치며 이러한 영향을 최소화하거나 해결하기 위해 조정되어야 합니다.

Zone-Based Policy Firewall을 구성하는 방법에 대한 자세한 내용은 Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide를 참조하십시오.

VoIP 환경에서 ZFW 고려 사항

Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide는 라우터의 *자체* 영역에 대한 보안 정책을 사용하여 라우터를 보호하는 간단한 논의와 다양한 NFP(Network Foundation Protection) 기능을 통해 제공되는 대체 기능을 제공합니다.라우터 기반 VoIP 기능은 라우터의 자체 영역 내에서 호스팅되므로, 라우터를 보호하는 보안 정책은 Cisco Unified CallManager Express, Survivable Remote-Site Telephony 및 Voice Gateway 리소스에 의해 시작되거나 전달될 음성 신호 및 미디어를 수용하기 위해 음성 트래픽에 대한 요구 사항을 인식해야 합니다.Cisco IOS Software Version 12.4(20)T 이전 버전에서는 Classic Firewall 및 Zone-Based Policy Firewall이 VoIP 트래픽의 요구 사항을 완전히 충족할 수 없었기 때문에 리소스를 완전히 보호할 수 있도록 방화벽 정책이 최적화되지 않았습니다.라우터 기반 VoIP 리소스를 보호하는 자체 영역 보안 정책은 12.4(20)T에 도입된 기능에 크게 의존합니다.

IOS Firewall Voice Enhancements - 12.4(20)T

Cisco IOS Software Release 12.4(20)T는 공동 상주 Zone Firewall 및 음성 기능을 지원하는 몇 가지 향상된 기능을 도입했습니다.보안 음성 애플리케이션에 3가지 주요 기능이 직접 적용됩니다.

- SIP 개선 사항:애플리케이션 레이어 게이트웨이 및 애플리케이션 검사 및 제어RFC 3261에 설명된 대로 SIP 버전 지원을 SIPv2에 업데이트SIP 신호 지원을 확장하여 더 다양한 통화 흐름을 인식합니다.특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 SIP AIC(Application Inspection and Control)를 소개합니다.자체 영역 검사를 확장하여 로컬로/시작된 SIP 트래픽으로 인해 발생하는 보조 신호 및 미디어 채널을 인식할 수 있습니다.
- Skinny Local Traffic 및 CME 지원SCCP 지원을 버전 16으로 업데이트(이전에 지원되었던 버전 9)특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 SCCP AIC(Application Inspection and Control)를 소개합니다.자체 영역 검사를 확장하여 로컬로/시작된 SCCP 트래픽으로 인해 발생하는 보조 신호 및 미디어 채널을 인식할 수 있습니다.
- H.323 v3/v4 지원v3 및 v4에 H.323 지원 업데이트(이전에 지원되었던 v1 및 v2)특정 애플리케이션 레벨 취약성 및 익스플로잇을 해결하기 위해 세분화된 제어를 적용할 수 있는 H.323 AIC(Application Inspection and Control)를 소개합니다.

이 문서에 설명된 라우터 보안 컨피그레이션에는 이러한 개선 사항에 의해 제공되는 기능과 정책에 의해 적용된 작업을 설명하는 설명이 포함되어 있습니다.음성 검사 기능에 대한 자세한 내용은 이 문서의 관련 정보 섹션에 나열된 개별 기능 문서를 참조하십시오.

주의 사항

앞서 언급한 포인트를 보강하기 위해 라우터 기반 음성 기능을 갖춘 Cisco IOS Firewall의 애플리케이션은 Zone-Based Policy Firewall을 적용해야 합니다.기존 IOS 방화벽은 음성 트래픽의 신호 복잡성과 동작을 완전히 지원하는 데 필요한 기능을 포함하지 않습니다.

네트워크 주소 변환

Cisco IOS NAT(Network Address Translation)는 Cisco IOS Firewall과 함께 자주 구성됩니다. 특히 사설 네트워크가 인터넷과 연결되어야 하거나, 개별 사설 네트워크가 연결해야 하는 경우, 특히 중복 IP 주소 공간이 사용 중인 경우 그렇습니다.Cisco IOS Software에는 SIP, Skinny 및 H.323용 NAT ALG(Application Layer Gateway)가 포함되어 있습니다. NAT는 문제 해결 및 보안 정책 애플리케이션에 대한 추가적인 복잡성을 초래하므로 IP 음성에 대한 네트워크 연결을 NAT의 애플리케이션 없이 수용하는 것이 좋습니다. 특히 NAT 오버로드가 사용되는 경우 더욱 그렇습니다.NAT는 네트워크 연결 문제를 해결하기 위한 마지막 사례 솔루션으로만 적용되어야 합니다.

Cisco Unified Presence 클라이언트

이 문서에서는 Cisco IOS Software Release 12.4(20)T1 현재 Zone 또는 Classic Firewall에서 CUPC를 지원하지 않으므로 IOS 방화벽에서 Cisco CUPC(Unified Presence Client) 사용을 지원하는 컨피그레이션에 대해 설명하지 않습니다. CUPC는 향후 Cisco IOS Software 릴리스에서 지원될 예정입니다.

CME/CUE/GW 단일 사이트 또는 브랜치 PSTN 연결

이 시나리오에서는 단일 사이트 SMB(중소, 중견, 성장 기업) 또는 분산형 통화 처리를 구축하려는 대규모 멀티 사이트 조직을 위한 안전한 라우터 기반 VoIP(Voice-over-IP) 텔레포니를 도입하여 PSTN(Public Switched Telephone Network)에 레거시 연결을 유지합니다. VoIP 통화 제어는 Cisco Unified Call Manager Express 애플리케이션을 통해 이루어집니다.

PSTN 연결은 장기간 유지 관리되거나 CME/CUE/GW 단일 사이트 또는 지사에서 SIP 트렁크가 있는 HQ 또는 음성 공급자 섹션의 CCM에 CCM으로 애플리케이션 예에 설명된 대로 통합 음성 및 데이터 IP 광역 네트워크로 마이그레이션할 수 있습니다.

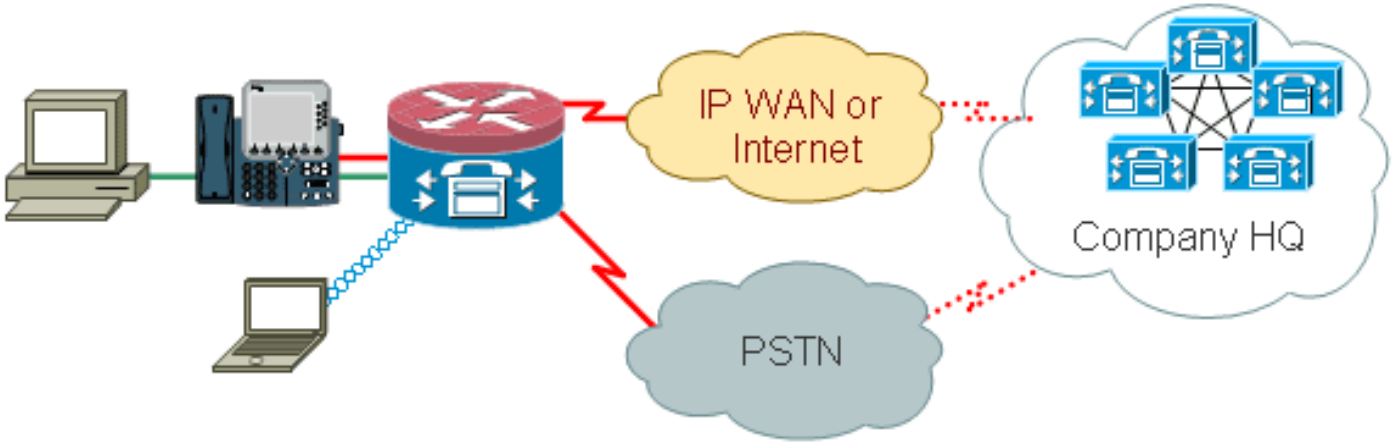
사이트 간에 서로 다른 VoIP 환경을 사용하는 상황이나 부적절한 WAN 데이터 연결 또는 데이터 네트워크에서 VoIP 사용에 대한 로캘별 제한 때문에 VoIP가 비실용적일 경우 조직은 이러한 유형의 애플리케이션 시나리오를 구현하는 것을 고려해야 합니다.단일 사이트 IP 텔레포니의 장점과 모범 사례는 Cisco Unified CallManager Express SRND에 설명되어 있습니다.

시나리오 배경

애플리케이션 시나리오에는 유선 전화(음성 VLAN), 유선 PC(데이터 VLAN) 및 무선 장치(IP Communicator와 같은 VoIP 장치 포함)가 포함됩니다.

보안 컨피그레이션에서는 다음을 제공합니다.

- CME와 로컬 전화(SCCP 및/또는 SIP) 간의 라우터에서 시작하는 신호 검사
- 다음 사이의 통신을 위한 음성 미디어 핀홀:로컬 유무선 부문MoH용 CME 및 로컬 전화음성 메일에 대한 CUE 및 로컬 전화
- AIC(Application Inspection and Control) 적용 대상:초대 메시지 속도 제한모든 SIP 트래픽에 대한 프로토콜 적합성을 보장합니다.



장점 및 단점

VoIP 시나리오의 가장 분명한 이점은 기존 POTS/TDM 환경에 기존 음성 및 데이터 네트워크 인프라를 통합하여 LAN을 넘어 전 세계로 텔레포니 서비스를 위한 통합 음성/데이터 네트워크로 전환하기 전에 제공하는 마이그레이션 경로입니다.소규모 비즈니스를 위해 전화 번호를 유지 관리하며, 유료 패킷 텔레포니로 사전 구성된 마이그레이션을 원하는 대규모 조직의 경우 기존 centrex 또는 DID 서비스를 그대로 사용할 수 있습니다.

단점으로는 통합된 음성 및 데이터 네트워크로 전환하여 유료 우회 비용을 절감할 수 있는 손실, 통화 유연성의 제한, 완전한 통합 음성 및 데이터 네트워크로 실현할 수 있는 조직 차원의 커뮤니케이션 통합 및 이동성의 결여 등이 있습니다.

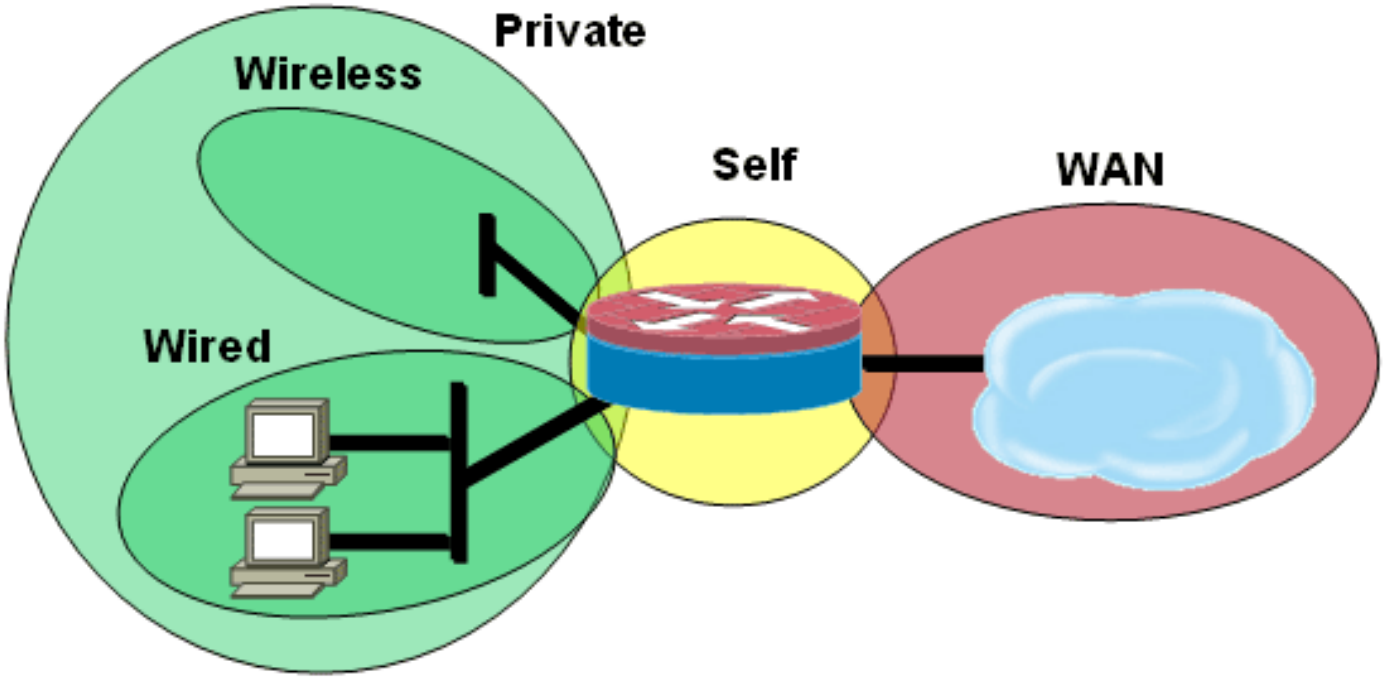
보안 측면에서 볼 때, 이러한 유형의 네트워크 환경은 공용 네트워크 또는 WAN에 VoIP 리소스가 노출되는 것을 방지하여 VoIP 보안 위협을 최소화합니다.그러나 라우터 내에 내장된 Cisco Call Manager Express는 여전히 악성 트래픽 또는 애플리케이션 트래픽 오작동과 같은 내부 위협에 취약합니다.따라서 프로토콜 적합성 확인을 충족하는 음성 전용 트래픽을 허용하는 정책이 구현되며, 특정 VoIP 작업(예: SIP INVITE)은 VoIP 리소스 및 유용성에 부정적인 영향을 주는 악성 또는 의도하지 않은 소프트웨어 악성코드의 가능성을 줄이기 위해 제한됩니다.

데이터 정책, 영역 기반 방화벽, 음성 보안 및 CCME 구성

여기에 설명된 컨피그레이션은 CME 및 CUE 연결을 위한 음성 서비스 컨피그레이션이 포함된 2851을 보여줍니다.

```
!
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
!
```

유선 및 무선 LAN 세그먼트의 보안 영역, 전용 LAN(유무선 세그먼트로 구성), 신뢰할 수 없는 인터넷 연결에 도달하는 공용 WAN 세그먼트, 라우터의 음성 리소스가 있는 자체 영역으로 구성된 영역 기반 정책 방화벽 구성



보안 구성

```
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
```

전체 라우터 컨피그레이션

```
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
```

프로비저닝, 관리 및 모니터링

라우터 기반 IP 텔레포니 리소스와 영역 기반 정책 방화벽 모두에 대한 프로비저닝 및 컨피그레이션은 일반적으로 Cisco Configuration Professional과 함께 사용하는 것이 가장 좋습니다.CiscoSecure Manager는 영역 기반 정책 방화벽 또는 라우터 기반 IP 텔레포니를 지원하지 않습니다.

Cisco IOS Classic Firewall은 Cisco Unified Firewall MIB를 사용하여 SNMP 모니터링을 지원합니다.그러나 영역 기반 정책 방화벽은 아직 Unified Firewall MIB에서 지원되지 않습니다.따라서 라우터의 명령줄 인터페이스 또는 Cisco Configuration Professional과 같은 GUI 툴을 사용하여 방화벽 모니터링을 처리해야 합니다.

CiscoSecure Monitoring and Reporting System(CS-MARS)은 CS-MARS에서 아직 완전히 지원되지 않는 12.4(15)T4/T5 및 12.4(20)T에서 구현된 트래픽에 대한 로그 메시지 상관성을 개선한 로깅 변경 사항을 통해 Zone-Based Policy Firewall에 대한 기본 지원을 제공합니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

Cisco IOS Zone Firewall은 방화벽 활동을 보고 모니터링하고 문제를 해결하기 위한 **show** 및 **debug** 명령을 제공합니다.이 섹션에서는 자세한 문제 해결 정보를 제공하는 Zone Firewall **debug** 명령을 소개합니다.

디버그 명령

디버그 명령은 암호화되지 않거나 지원되지 않는 컨피그레이션을 사용하고 상호 운용성 문제를 해결하기 위해 Cisco TAC 또는 기타 제품의 기술 지원 서비스와 함께 작업해야 하는 경우에 유용합니다.

참고: debug 명령을 특정 기능 또는 트래픽에 적용하면 콘솔 메시지 수가 매우 많아 라우터 콘솔이 응답하지 않을 수 있습니다.디버깅을 활성화해야 하는 경우에도 터미널 대화 상자를 모니터링하지 않는 텔넷 창과 같은 대체 명령줄 인터페이스 액세스를 제공할 수 있습니다.디버그를 활성화하면 라우터 성능에 큰 영향을 미칠 수 있으므로 오프라인(랩 환경) 장비 또는 계획된 유지 관리 기간 동안에만 디버그를 활성화해야 합니다.

관련 정보

- Cisco Unified CallManager Express 솔루션 참조 네트워크 설계 가이드
- Cisco Unity Connection과 Cisco Unified CME-as-SRST 통합
- Cisco Unified Communications Manager Express 명령 참조
- Cisco CallManager Express/Cisco Unity Express 컨피그레이션 예
- Cisco CallManager Express 3.4 SNMP MIB 지원

- Zone-Based Policy Firewall 설계 및 애플리케이션 가이드
- 기술 지원 및 문서 – Cisco Systems