IOS Zone-Based ファイアウォール：CME/CUE/GW の 1 つの場所またはブランチオフィスの PSTN 接続の設定例

内容

概要

Cisco Integrated Service Router（ISR）は、さまざまなアプリケーションのデータおよび音声ネットワークの要件に対応する、スケーラブルなプラットフォームを提供します。プライベートおよびインターネットに接続されたネットワークの脅威の状況は非常に動的ですが、Cisco IOS Firewallは、ステートフルインスペクションおよびApplication Inspection and Control(AIC)機能を提供し、セキュアなネットワークポスチャを定義して適用すると同時に、ビジネス機能とのを実現します。

このドキュメントでは、特定の Cisco ISR ベースのデータおよび音声アプリケーションのシナリオに関して、ファイアウォール セキュリティの設計および設定の考慮事項について説明します。音声サービスおよびファイアウォールの設定は、アプリケーションのシナリオごとに示されます。各シナリオでは、VoIP およびセキュリティの設定が個別に説明され、その後、ルータ全体の設定が説明されます。ネットワークでは、音声品質と機密性を維持するために、QoSやVPNなどのサービスの他の設定が必要になる場合があります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

IOS ファイアウォールの背景説明

Cisco IOSファイアウォールは、通常、アプライアンスファイアウォールの導入モデルとは異なるアプリケーションシナリオで導入されます。典型的な導入には、少ないデバイス数、複数サービスの統合、低いパフォーマンスとセキュリティ機能深度が好まれる、在宅勤務者アプリケーション、小規模オフィスやブランチオフィスのサイト、およびリテール アプリケーションが含まれます。

ISR製品の他の統合サービスと同様にファイアウォールインスペクションを適用することはコスト面と運用面の観点から魅力的に見えますが、ルータベースのファイアウォールが適切かどうかを判断するには、具体的な考慮事項を評価する必要があります。各追加機能を適用すると、メモリと処理コストが削減され、負荷ピーク時の転送スループットレートの低下、パケット遅延の増加、および機能機能の喪失に貢献する可能性が高い統合ルータベースのソリューション。

ルータとアプライアンスを決定する際は、次のガイドラインに従ってください。

- 複数の統合機能が有効なルータは、デバイスが少ないブランチオフィスや在宅勤務者のサイトに最適で、優れたソリューションを提供します。
- 一般に、高帯域幅で高性能なアプリケーションは、次のアプライアンスを使用してより適切に対処できます。Cisco ASA および Cisco Unified CallManager サーバは、NAT、セキュリティ ポリシー アプリケーション、および呼処理を処理するために適用する必要があります。ルータは、QoS ポリシー アプリケーション、WAN の終端、およびサイト間 VPN 接続の要件に対応します。

Cisco IOSソフトウェアバージョン12.4(20)T以前は、Classic FirewallとZone-Based Policy Firewall(ZFW)は、VoIPトラフィックとルータベースの音声サービスに必要な機能を完全にサポートできませんでした。音声トラフィックに対応するには、大規模なな空が必要です。

Cisco IOSゾーンベースポリシーファイアウォールの導入

他のファイアウォールと同様に、Cisco IOSゾーンベースポリシーファイアウォールは、ネットワークのセキュリティ要件が特定され、セキュリティポリシーで説明されている場合にのみ、セキュアなファイアウォールを提供できます。セキュリティ ポリシーに対する 2 つの基本的なアプローチは次のとおりです。*信頼の観点*と、*対照的な疑いの観点*。

信頼の観点では、悪意のあるトラフィックまたは不要なトラフィックと明確に特定できるものを除き、すべてのトラフィックが信頼できると仮定されます。不要なトラフィックのみを拒否する特定のポリシーが実装されます。これは、通常、特定のアクセス制御エントリ、またはシグニチャや動作ベースのツールで実行されます。このアプローチの場合、既存アプリケーションへの影響は少ない傾向にありますが、脅威と脆弱性の展望に関する包括的な専門知識が必要であり、新たな脅威に対応し、現れる脅威をエクスプロイトするために常に警戒している必要があります。また、ユーザ コミュニティが、セキュリティの適切な維持の大部分を担当する必要があります。利用者に対する制限が少なく、自由度の高い環境では、多くの場合、不注意または悪意のある人物によって問題が引き起こされます。このアプローチのさらなる問題点は、すべてのネットワーク トラフィック内の疑わしいデータのモニタとコントロールを可能にするための、十分な柔軟性と性能を提供する効率的な管理ツールとアプリケーション制御への依存度がさらに増す点です。現在は、この点に対応するためのテクノロジーがありますが、多くの場合、運用上の負担はほとんどの組織の限界を超えています。

疑いの観点では、望ましいトラフィックだと明確に識別されたものを除き、すべてのネットワーク トラフィックが望ましくないと仮定されます。明示的に許可されているトラフィック以外のすべてのアプリケーショントラフィックを拒否するために適用されるポリシー。さらに、アプリケーション検査と制御(AIC)を実装して、「良い」アプリケーションを悪用するように特別に細工された悪意のあるトラフィックと、良いトラフィックのように偽装された不要なトラフィックを特定して拒否できます。繰り返しになりますが、望ましくないトラフィックの大部分は、アクセス コントロール リスト（ACL）やゾーンベース ポリシー ファイアウォール（ZFW）ポリシーなどのステートレス フィルタによって制御される必要がありますが、アプリケーション制御を行うことで、ネットワークに対する運用およびパフォーマンスの負担は生じます。したがって、AIC、侵入防御システム（IPS）、または Flexible Packet Matching（FPM）や Network-Based Application Recognition（NBAR; ネットワークベースのアプリケーション認識）などの他のシグニチャベース コントロールで処理する必要があるトラフィックは大幅に減少する必要があります。したがって、目的のアプリケーションポート（および既知の制御接続またはセッションから発生するダイナミックメディア固有のトラフィック）だけが明示的に許可されると、ネットワーク上に存在する不要なトラフィックだけが特定のサブセットに分類されます。

このドキュメントでは、*疑いの観点に基づいた VoIP セキュリティの設定について説明しています*。そのため、音声ネットワーク セグメントで許容されるトラフィックのみ許可されます。データポリシーは、各アプリケーションシナリオの設定に関するメモで説明されているように、より許容される傾向があります。

すべてのセキュリティ ポリシーの導入は、クローズドループ フィードバック サイクルに従う必要があります。セキュリティの導入は通常、既存のアプリケーションの機能に影響を与えるため、この影響を最小限に抑えるか、解決するように調整する必要があります。

ゾーンベースポリシーファイアウォールの設定方法の詳細については、『Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide』を参照してください。

VoIP 環境内の ZFW の考慮事項

『Cisco IOS Firewall Zone-Based Policy Firewall Design and Application Guide』では、ルータの

セルフゾーンとの間でセキュリティポリシーを使用してルータを保護するための簡単な説明と、さまざまなNetwork Foundation Protection(NFP)機能によって提供される代替機能について説明しています。ルータベースのVoIP機能はルータのセルフゾーン内でホストされるため、Cisco Unified CallManager Express、Survivable Remote-Site Telephony、およびVoice Gatewayリソースを発信元および宛先とする音声シグナリングとメディアに対応するために、ルータを保護するセキュリティポリシーは必要です。Cisco IOSソフトウェアバージョン12.4(20)T以前では、Classic Firewallとゾーンベースポリシーファイアウォールは VoIPトラフィックの要件に完全に対応できなかったため、ファイアウォールポリシーはリソースを完全に保護するように最適化されませんでした。ルータベースの VoIP リソースを保護するセルフゾーン セキュリティ ポリシーは、12.4(20)T で導入された機能に大きく依存しています。

IOSファイアウォールの音声拡張機能 – 12.4(20)T

Cisco IOSソフトウェアリリース12.4(20)Tでは、共存ゾーンファイアウォールと音声機能を有効にするために、いくつかの拡張機能が導入されました。3 つの主要機能は、セキュアな音声アプリケーションに直接適用されます。

- SIP の機能強化：アプリケーション層ゲートウェイおよび Application Inspection and ControlRFC 3261 で定義されている、SIPv2 への SIP バージョンのサポートを更新より広範なコール フローを認識するために、SIP シグナリングのサポートを拡大固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、SIP Application Inspection and Control（AIC）を導入セルフゾーン検査を拡張し、ローカルで送受信されるSIPトラフィックから生じるセカンダリシグナリングおよびメディアチャネルを認識できるようにします。
- Skinny Local Traffic および CME のサポートバージョン 16 に対する SCCP のサポートを更新（以前のサポート バージョンは 9）固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、SCCP Application Inspection and Control（AIC）を導入ローカルに送受信される SCCP トラフィックによって生じるセカンダリ シグナリングおよびメディア チャネルを認識できるようにするために、セルフゾーン検査を拡大
- H.323 v3/v4 のサポートH.323サポートをv3およびv4に更新（以前はv1およびv2をサポート）固有のアプリケーションレベルの脆弱性およびエクスプロイトに対応するためのきめ細かい制御を適用するために、H.323 Application Inspection and Control（AIC）を導入

このドキュメントで説明されているルータのセキュリティ設定には、これらの機能強化によってもたらされる機能、およびポリシーによって適用されるアクションに関する説明が含まれています。音声検査機能の詳細については、このドキュメントの「関連情報」の項に記載されている個々の機能ドキュメントを参照してください。

警告

前述のポイントを強調するために、ルータベースの音声機能を備えたCisco IOS Firewallを適用するには、ゾーンベースポリシーファイアウォールを適用する必要があります。Classic IOS Firewall には、シグナリングの複雑さと音声トラフィックの動作を完全にサポートするために必要な機能は含まれていません。

ネットワークアドレス変換

Cisco IOS ネットワーク アドレス変換（NAT）は、Cisco IOS Firewall と共に設定されることがよくあります。特に、プライベート ネットワークがインターネットとインターフェイス接続する必

要がある場合、または異種プライベート ネットワークを接続する必要がある場合（特に、オーバーラップ IP アドレス空間が使用されている場合）に設定されます。Cisco IOSソフトウェアには、SIP、Skinny、およびH.323用のNATアプリケーション層ゲートウェイ(ALG)が含まれています。NATではトラブルシューティングとセキュリティポリシーアプリケーションが複雑になるため、IP音声のネットワーク接続はNATの適用なしで行えます。NAT は、ネットワークの接続性の問題に対しては最後の解決策としてのみ適用する必要があります。

Cisco Unified Presence Client

このドキュメントでは、Cisco IOSソフトウェアリリース12.4(20)T1ではCUPCがゾーンまたはクラシックファイアウォールでサポートされていないため、IOSファイアウォールでのCisco Unified Presence Client(CUPC)の使用をサポートする設定については説明しません。

CME/CUE/GWシングルサイトまたはブランチPSTN接続

このシナリオでは、単一サイトの中小規模の企業や、分散型コール処理を導入する大規模なマルチサイト組織に対して、安全なルータベースのVoice over IP(VoIP)テレフォニーを導入し、公衆電話交換網(PSTN)へのレガシー接続を維持します。 VoIPコール制御は、Cisco Unified Call Manager Expressのアプリケーションを介して対応します。

このドキュメントの「HQまたは音声プロバイダーでのCCMへのSIPトランクを備えたCME/CUE/GW単一サイトまたはブランチオフィス」セクションで説明されているアプリケーション例に従って、PSTN接続を長期的に維持したり、統合できます。

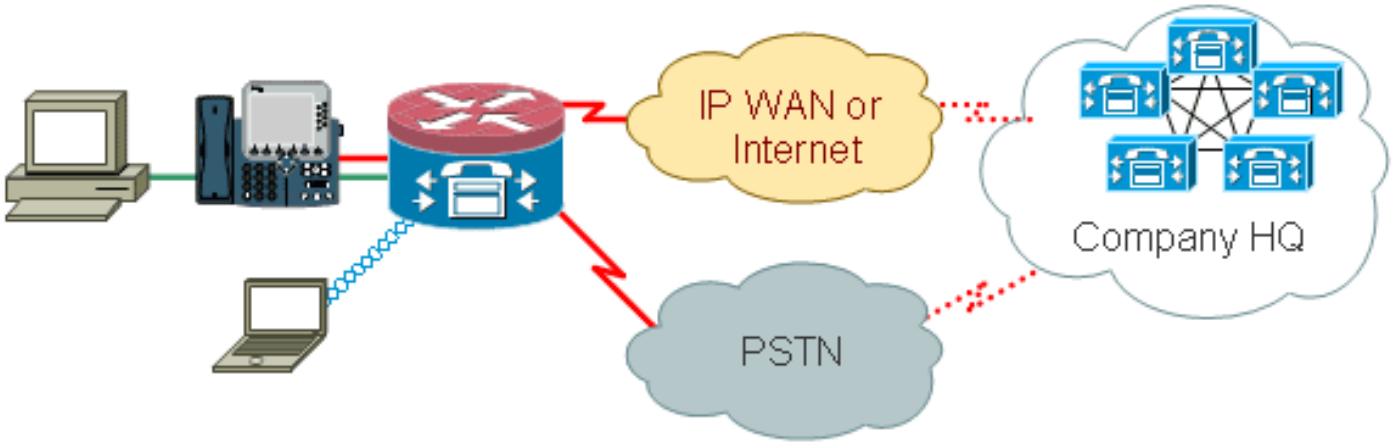
異なるVoIP環境がサイト間で使用される状況、またはWANデータ接続が不十分なためにVoIPが実用的でない場合、またはデータネットワークでのVoIPの使用に関するロケール固有の制限を考慮する必要があります。単一サイトのIPテレフォニーの利点とベストプラクティスについては、Cisco Unified CallManager Express SRNDを参照してください。

シナリオのバックグラウンド

アプリケーションシナリオには、有線電話（音声VLAN）、有線PC（データVLAN）、およびワイヤレスデバイス（IP CommunicatorなどのVoIPデバイスを含む）が含まれます。

セキュリティ設定には次の機能があります。

- CMEとローカル電話（SCCPまたはSIP）間のルータ開始シグナリングインスペクション
- 次の間における通信の音声メディア ピンホール：ローカルの有線およびワイヤレス セグメントCMEとMoHのローカル電話ボイスメール用のCUEおよびローカル電話
- Application Inspection and Control（AIC）の適用先：招待メッセージのレート制限すべてのSIP トラフィックのプロトコル準拠の保証



長所と短所

シナリオのVoIPの最も明白な利点は、既存の音声およびデータネットワークインフラストラクチャを既存のPOTS/TDM環境に統合し、テレフォニーサービス用の統合音声/データネットワークに移行する前に、移行パスを提供することです。電話番号は小規模な企業向けに維持され、既存のCentrexまたはDIDサービスは、トールバイパスパケットテレフォニーへの段階的な移行を希望する大規模な組織に残すことができます。

欠点は、音声とデータが統合されたネットワークに移行することでトールバイパスで実現できるコスト節約の損失、電話の柔軟性の制限、完全に統合された音声とデータのネットワークで実現できる組織全体の通信の統合とポータビリティの欠如です。

セキュリティの観点から見ると、このタイプのネットワーク環境では、VoIPリソースがパブリックネットワークまたはWANに公開されるのを回避することで、VoIPセキュリティの脅威を最小限に抑えます。ただし、ルータ内に組み込まれたCisco Call Manager Expressは、悪意のあるトラフィックや誤動作するアプリケーショントラフィックなどの内部の脅威に対して脆弱です。したがって、プロトコル適合性チェックを満たす音声固有のトラフィックを許可するポリシーが実装され、特定のVoIPアクション（SIP INVITEなど）が制限されるため、悪意のあるソフトウェアや意図しないソフトウェアの誤動作がVoIPリソースとユーザビリティに悪影響を削減します。

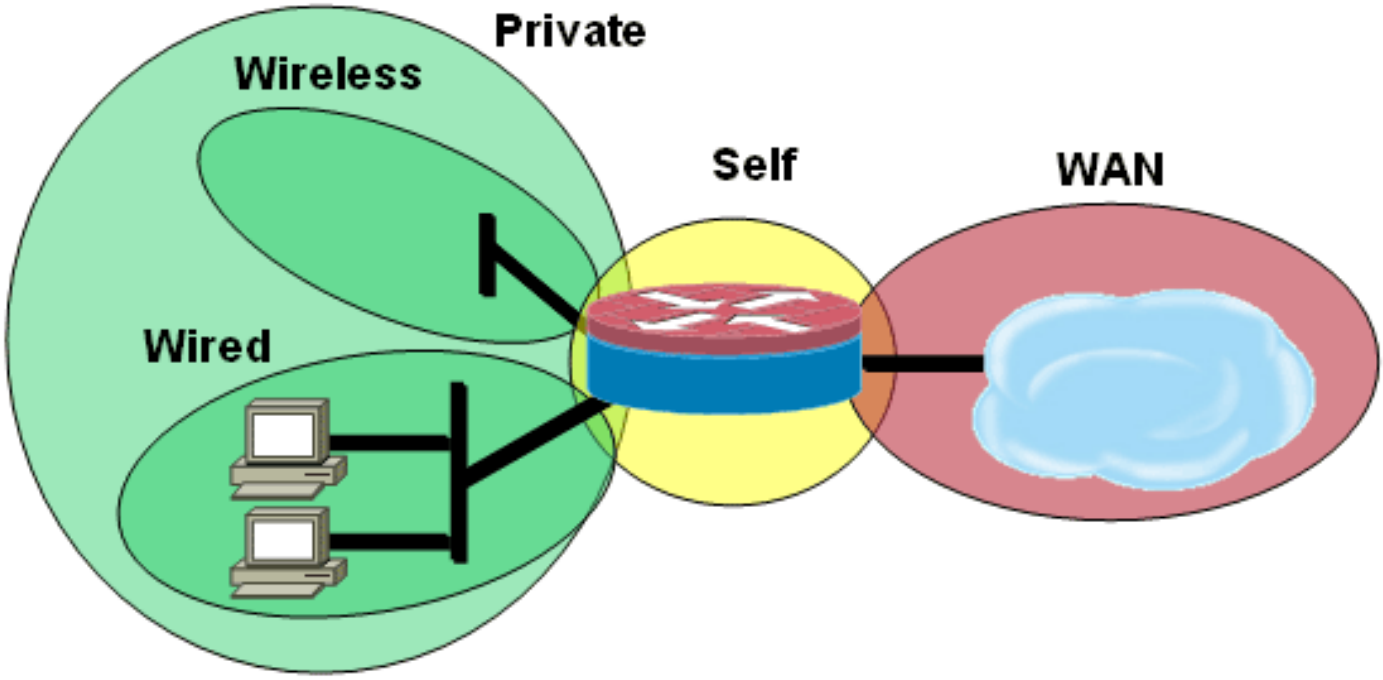
データポリシー、ゾーンベースファイアウォール、音声セキュリティ、およびCCMEの設定

ここで説明する設定は、CMEおよびCUE接続の音声サービス設定を使用した2851を示しています。

```
!
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
!
```

ゾーンベースポリシーファイアウォールの設定。有線および無線LANセグメントのセキュリティゾーン、プライベートLAN（有線および無線セグメントで構成）、信頼できないインターネット接続に到達するパブリックWANセグメント、ルータの音声リソースが配置されるセルフゾーンで

構成されます。



セキュリティ設定

```
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
```

ルータ全体の設定

```
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
```

プロビジョニング、管理、およびモニタリング

ルータベースの IP テレフォニー リソースおよびゾーンベース ポリシー ファイアウォールの両方のプロビジョニングと設定は、一般的に、Cisco Configuration Professional を使用して適用するのが最適です。Cisco Secure Manager は、ゾーンベース ポリシー ファイアウォールまたはルータベースの IP テレフォニーをサポートしていません。

Cisco IOS Classic Firewall は、Cisco Unified Firewall MIB による SNMP モニタリングをサポートしています。ただし、ゾーンベースポリシーファイアウォールは、Unified Firewall MIBではまだサポートされていません。そのため、ファイアウォールの監視は、ルータのコマンドラインインターフェイス(CLI)の統計情報、またはCisco Configuration ProfessionalなどのGUIツールを使用して処理する必要があります。

CiscoSecure Monitoring And Reporting System(CS-MARS)は、ゾーンベースポリシーファイアウォールの基本サポートを提供します。ただし、12.4(15)T4/T5および12.4(20)Tで実装されたトラフィックに対するログメッセージの相関がが向上する変更は、CS CS MARS CS CS CS-MARS

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

Cisco IOS Zone Firewallには、ファイアウォールのアクティビティを表示、監視、およびトラブルシュートするための**show**および**debug**コマンドが用意されています。このセクションでは、詳細なトラブルシューティング情報を提供するZone Firewallの**debug**コマンドの概要について説明します。

デバッグ コマンド

debugコマンドは、特殊またはサポートされていない設定を使用し、Cisco TACまたはその他の製品のテクニカルサポートサービスと連携して相互運用性の問題を解決する必要がある場合に便利です。

注：特定の機能またはトラフィックに**debug**コマンドを適用すると、非常に大量のコンソールメッセージが発生し、ルータのコンソールが応答しなくなる可能性があります。デバッグを有効にする必要がある場合でも、端末ダイアログを監視しないtelnetウィンドウなど、代替のコマンドラインインターフェイス(CLI)アクセスを提供する必要がある場合があります。デバッグを有効にすると、ルータのパフォーマンスに大きく影響する可能性があるため、デバッグはオフライン（ラボ環境）機器または計画されたメンテナンス時間帯にのみ有効にしてください。

関連情報

- Cisco Unified CallManager Express ソリューションのリファレンス ネットワーク設計ガイド
- Cisco Unity Connection と Cisco Unified CME の SRST としての統合
- Cisco Unified Communications Manager Express のコマンドリファレンス
- Cisco CallManager Express および Cisco Unity Express の設定例
- Cisco CallManager Express 3.4 SNMP MIB に関するサポート ページ
- ゾーンベース ポリシー ファイアウォールの設計と適用ガイド
- テクニカル サポートとドキュメント – Cisco Systems