Cisco IOS Zone Based Firewall: Office with Cisco Unity Express/SRST/PSTN Gateway with Connection to Centralized Cisco CallManager

Contents

Introduction

Cisco Integrated Service Routers (ISRs) offer a scalable platform to address data and voice network requirements for a wide range of applications. Although the threat landscape of both private and Internet-connected networks is a very dynamic environment, Cisco IOS® Firewall offers stateful inspection and Application Inspection and Control (AIC) capabilities to define and enforce a secure network posture, while enabling business capability and continuity.

This document describes design and configuration considerations for firewall security aspects of specific Cisco ISR-based data and voice application scenarios. Configuration for voice services and firewall are provided for each application scenario. Each scenario describes the VoIP and security configurations separately, then by the entire router configuration. Your network can require other configuration for services such as QoS and VPN to maintain voice quality and confidentiality.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Cisco IOS Firewall Background

Cisco IOS Firewall is typically deployed in application scenarios that differ from the deployment models of appliance firewalls. Typical deployments include Teleworker applications, small- or branch-office sites, and retail applications, where low device count, integration of multiple services, and lower performance and security capability depth is desired.

While application of firewall inspection, along with other integrated services in the ISR products, can appear attractive from cost and operational perspective, specific considerations must be evaluated in order to determine if a router-based firewall is appropriate. Application of each additional feature incurs memory and processing costs, and likely contributes to reduced forwarding throughput rates, increased packet latency, and loss of feature capability during periods of peak load if an underpowered integrated router-based solution is deployed. Observe these guidelines when you decide between a router and an appliance:

- Router with multiple integrated features enabled are best suited for branch-office or telecommuter sites where less devices offer a better solution
- High-bandwidth, high-performance applications are typically better addressed with appliances. Cisco ASA and Cisco Unified Call Manager Server should be applied to handle NAT and security policy application and call processing, while routers address QoS policy application, WAN termination, and site-to-site VPN connectivity requirements.

Prior to the introduction of Cisco IOS Software Release 12.4(20)T, Classic Firewall and Zone-Based Policy Firewall (ZFW) was unable to fully support capabilities required for VoIP traffic and router-based voice services, and required large openings in otherwise secure firewall policies in order to accommodate voice traffic and offered limited support for evolving VoIP signaling and media protocols.

Configure

Deployment of Cisco IOS Zone-Based Policy Firewall

Cisco IOS Zone-Based Policy Firewall, similar to other firewalls, can only offer a secure firewall if the security requirements of the network *trusting*are identified and described by security policy. There are two fundamental approaches to arrive at a security policy: the perspective, as opposed

to the *suspicious* perspective.

The *trusting* perspective assumes all traffic is trustworthy, except that which can be specifically identified as malicious or unwanted. A specific policy is implemented that denies only the unwanted traffic. This is typically accomplished through the use specific access-control entries, or signature- or behavior-based tools. This approach tends to interfere less with existing applications, but requires a comprehensive knowledge of the threat and vulnerability landscape, and requires constant vigilance to address new threats and exploits as they appear. Additionally, the user community must play a large part in maintaining adequate security. An environment that allows broad freedom with little control for the occupants offers substantial opportunity for problems caused by careless or malicious individuals. An additional problem of this approach is that it relies much more on effective management tools and application controls that offer sufficient flexibility and performance to be able to monitor and control suspect data in all network traffic. While technology is presently available to accommodate this, the operational burden frequently exceeds the limits of most organizations.

The *suspicious* perspective assumes all network traffic is undesired, except for specifically identified *good* traffic. This is a policy that is applied which denies all application traffic except that which is explicitly permitted. Additionally, application inspection and control (AIC) can be implemented to identify and deny malicious traffic that is specifically crafted to exploit *good* applications, as well as unwanted traffic that is masquerading as *good* traffic. Again, application controls impose operational and performance burdens on the network, although most undesired traffic should be controlled by stateless filters such as access-control lists (ACLs) or Zone-Based Policy Firewall (ZFW) policy, so there should be substantially less traffic that must be handled by AIC, intrusion prevention system (IPS), or other signature-based controls such as flexible packet matching (FPM) or network-based application recognition (NBAR). Thus, if only desired application ports, and dynamic media-specific traffic arising from known control connections or sessions, are specifically permitted, the only unwanted traffic that should be present on the network should fall into a specific, more-easily-recognized subset, which reduces the engineering and operational burden imposed to maintain control over undesired traffic.

This document describes VoIP security configurations based on the *suspicious* perspective; thus, only traffic that is permissible in the voice-network segments is permitted. Data policies tend to be more permissive, as described by notes in the configuration of each application scenario.

All security policy deployments must follow a closed-loop feedback cycle; security deployments typically affect capability and functionality of existing applications, and must be adjusted in order to minimize or resolve this impact.

Refer to Zone-Based Policy Firewall Design and Application Guide for more information and additional background for the configuration of the Zone-Based Policy Firewall.

Considerations for ZFW in VoIP Environments

The previously mentioned Design and Application Guide offers a brief discussion for the security of the router with the use of security policies to and from the self zone of the router, as well as alternative capabilities that are provided through various Network Foundation Protection (NFP) features. Router-based VoIP capabilities are hosted within the self zone of the router, so security policies that protect the router must be aware of the requirements for voice traffic, in order to accommodate the voice signaling and media originated by and destined to Cisco Unified CallManager Express, Survivable Remote-Site Telephony, and Voice Gateway resources. Prior to Cisco IOS Software Release 12.4(20)T, Classic Firewall and Zone-Based Policy Firewall was

unable to fully accommodate the requirements of VoIP traffic, so firewall policies were not optimized to fully protect resources. Self-zone security policies that protect router-based VoIP resources rely heavily on capabilities introduced in Cisco IOS Software Release 12.4(20)T.

Cisco IOS Firewall Voice Features

Cisco IOS Software Release 12.4(20)T introduced several enhancements in order to enable co-resident Zone Firewall and voice capabilities. Three main features apply directly to secure voice applications:

- SIP Enhancements: Application-Layer Gateway and Application Inspection and ControlUpdates SIP version support to SIPv2, as described by RFC 3261Broadens SIP signaling support to recognize a wider variety of call flowsIntroduces SIP Application Inspection and Control (AIC) to apply granular controls to address specific application-level vulnerabilities and exploitsExpands self-zone inspection in order to be able to recognize secondary signaling and media channels resulting from locally-destined/-originated SIP traffic
- Support for Skinny Local Traffic and Cisco CallManager ExpressUpdates SCCP support to version 16 (previously supported version 9)Introduces SCCP Application Inspection and Control (AIC) to apply granular controls to address specific application-level vulnerabilities and exploitsExpands self-zone inspection to be able to recognize secondary signaling and media channels resulting from locally-destined/-originated SCCP traffic
- H.323 v3/v4 SupportUpdates H.323 support to v3 and v4 (previously supported v1 and v2), as described byIntroduces H.323 Application Inspection and Control (AIC) to apply granular controls to address specific application-level vulnerabilities and exploits

The router security configurations described in this document include capabilities offered by these enhancements, with explanation to describe the action applied by the policies. Hyperlinks to the individual feature documents are available in the Related Information section at the end of this document, if you wish to review the complete details for the voice inspection features.

Caveats

The application of Cisco IOS Firewall with router-based voice capabilities must apply the Zone-Based Policy Firewall in order to reinforce points that were previously mentioned. Classic IOS Firewall does not include the needed capability to fully support the signaling complexities and behavior of voice traffic.

NAT

Cisco IOS network address translation (NAT) is frequently configured concurrently with Cisco IOS Firewall, particularly in cases where private networks must interface with the Internet, or if disparate private networks must connect, particularly if overlapping IP address space is in use. Cisco IOS Software includes NAT application layer gateways (ALGs) for SIP, Skinny, and H.323. Ideally, network connectivity for IP voice can be accommodated without the application of NAT, as NAT introduces additionally complexity to troubleshooting and security-policy applications, particularly in cases where NAT overload is used. NAT should only be applied as a last case solution to address network connectivity concerns.

CUPC

This document does not describe configuration that supports the use of Cisco Unified Presence Client (CUPC) with Cisco IOS Firewall, as CUPC is not yet supported by Zone or Classic Firewall as of Cisco IOS Software Release 12.4(20)T1. CUPC is supported in a future release of Cisco IOS Software.

Office with Cisco Unity Express/SRST/PSTN Gateway that Connects to Centralized Cisco CallManager

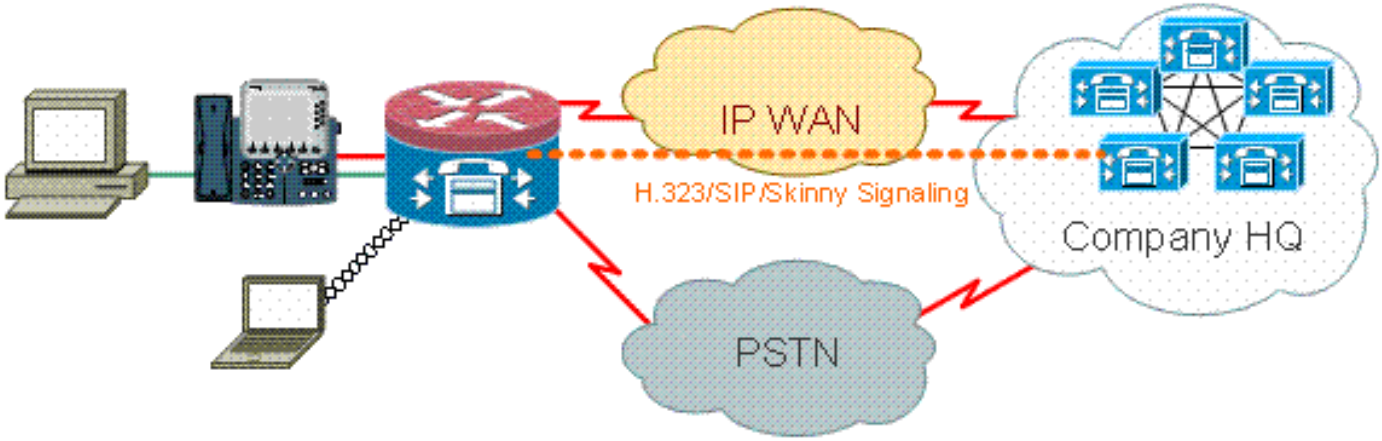
This scenario differs from the previous applications, in that centralized call-control is used for all call control, instead of distributed router-based call processing. Distributed voice mail is applied, but throughCisco Unity Express on the router. The router provides Survivable Remote-Site Telephony and PSTN Gateway functionality for emergency dialing and local-dial. An application-specific level of PSTN capacity is recommended to accommodate failure of WAN-based toll bypass dialing, as well as local-area dialing as described by the dial plan. Additionally, local laws typically require that some sort of local PSTN connectivity is provided to accommodate emergency (911) dialing.

This scenario can also apply Cisco CallManager Express as the call processing agent for SRST, in the event that greater call-processing capability is required during WAN/CCM outages. Refer to Integrating Cisco Unity Connection with Cisco Unified CME-as-SRST for more information.

Scenario Background

The application scenario incorporates wired phones (voice VLAN), wired PCs (data VLAN), and wireless devices (including VoIP devices such as IP Communicator).

1. Signaling inspection between local phones and remote CUCM cluster (SCCP and SIP)
2. Inspect H.323 signaling between the router and the remote CUCM cluster.
3. Inspect signaling between the local phones and the router when the link to the remote site is down and SRST is active.
4. Voice-media pinholes for communication between:Local wired and wireless segmentsLocal and remote phonesRemote MoH server and local phonesRemote Unity server and local phones for voice mail
5. Apply Application Inspection and Control (AIC) to:rate limit invite messagesassure protocol conformance on all SIP traffic.



Advantages/Disadvantages

This scenario offers the benefit that the majority of call processing occurs in a central Cisco CallManager cluster, which offers reduced management burden. The router should typically have to address less local voice-resource inspection burden as compared to the other cases described in this document, as the majority of the call-processing burden is not imposed on the router, except for handling traffic to/from the Cisco Unity Express, and in cases when there is a WAN or CUCM outage, and local Cisco CallManager Express/SRST is called into effect to address call processing.

The greatest drawback of this case, during typical call-processing activity, is that the Cisco Unity Express is located on the local router. While this is good from a design perspective, for example, the Cisco Unity Express is located closest to end-users where voicemail is held, it incurs some additional management burden, in that there can be a large number of Cisco Unity Express to manage. That said, with a central Cisco Unity Express to carry the opposite drawbacks, in that a central Cisco Unity Express is farther from remote users, and is possibly not accessible during outages. Thus, the functional benefits of distributed voicemail offer by the deployment of Cisco Unity Express to remote locations offers the superior choice.

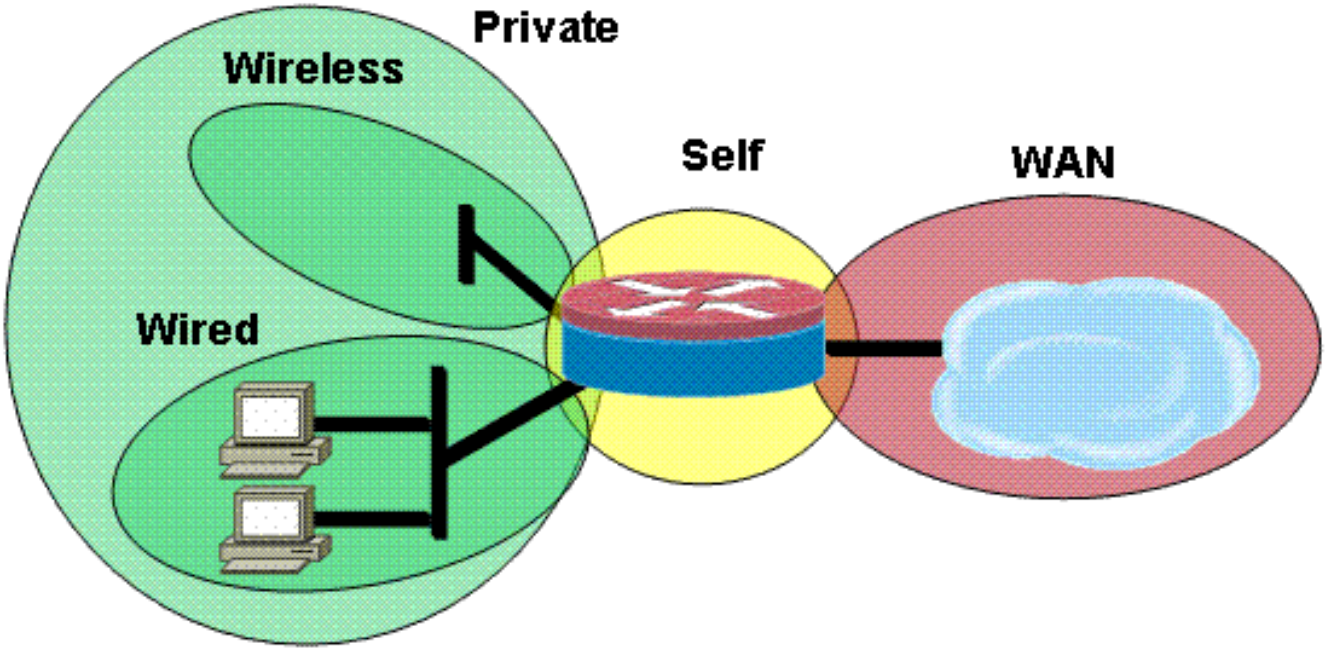
Configurations for Data Policies, Zone-Based Firewall, Voice Security, Cisco CallManager Express

Router configuration is based on a 3845 with a NME-X-23ES and a PRI HWIC:

Voice Service configuration for SRST and Cisco Unity Express connectivity:

```
!
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
!
```

This is an eample of the Zone-Based Policy Firewall Configuration, composed of security zones for wired and wireless LAN segments, private LAN, which is composed of wired and wireless segments, a WAN segment where trusted WAN connectivity is reached, and the self zone where the voice resources of the router are located:



Security configuration:

```
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, Management, and Monitoring

Provisioning and configuration for both router-based IP Telephony resources and Zone-Based Policy Firewall is generally best accommodated with Cisco Configuration Professional. CiscoSecure Manager does not support Zone-Based Policy firewall or router-based IP telephony.

Cisco IOS Classic Firewall supports SNMP monitoring with the Cisco Unified Firewall MIB. But, Zone-Based Policy Firewall is not yet supported in the Unified Firewall MIB. As such, firewall monitoring must be handled through statistics on the command-line interface of the router, or with GUI tools such as Cisco Configuration Professional.

CiscoSecure Monitoring And Reporting System (CS-MARS) offers basic support for the Zone-

Based Policy Firewall, although logging changes that improved log-message correlation to traffic which were implemented in Cisco IOS Software Release 12.4(15)T4/T5 and Cisco IOS Software Release 12.4(20)T have not yet been fully supported in CS-MARS.

Capacity Planning

Firewall call inspection performance test results from India TBD.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Cisco IOS Zone Firewall provides **show** and **debug** commands in order to view, monitor, and troubleshoot the activity of the firewall. This section describes the use of the **show** commands in order to monitor basic firewall activity, and an introduction to the **debug** commands of the Zone Firewall for more detailed troubleshooting, or if discussion with technical support requires detailed information.

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

Show Commands

Cisco IOS Firewall offers several **show** commands in order to view security policy configuration and activity:

Many of these commands can be replaced with a shorter command through application of the **alias** command.

Debug Commands

Debug commands can be useful in the event that you use an atypical or unsupported configuration, and need to work with the Cisco TAC or other products' technical support services in order to resolve interoperability issues.

Note: Application of **debug** commands to specific capabilities or traffic can cause a very large number of console messages, which causes the router console to become unresponsive. In the event that you need to enable debugging, it is possible to provide for alternative command-line interface access, such as a telnet window that does not monitor terminal dialogue. You should only enable debug on off-line (lab environment) equipment or during a planned maintenance window, because if you enable debug, this can substantially affect router performance.

Related Information

- Cisco Unified CallManager Express Solution Reference Network Design Guide
- Cisco Unified CallManager Express Security Best Practices
- Integrating Cisco Unity Connection with Cisco Unified CME-as-SRST
- Cisco Unified Communications Manager Express Command Reference
- Cisco CallManager Express/Cisco Unity Express Configuration Example
- Cisco CallManager Express 3.4 SNMP MIB Support
- Zone-Based Policy Firewall Design and Application Guide
- Cisco IOS Firewall Support for Skinny Local Traffic and CME
- Cisco IOS Firewall
- Technical Support & Documentation - Cisco Systems