Cisco IOS Zone Based Firewall: CME/CUE/GW Single Site or Branch Office with SIP Trunk to CCM at HQ

Contents

Introduction

The 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 it enables 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. The configurations for voice services and the firewall are provided for each application scenario. Each scenario describes the VoIP and security configurations separately, followed by the entire router configuration. Your network possibly 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.

Background Information

IOS Firewall Background

The 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 the 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 to determine if a router-based firewall is appropriate. The application of each additional feature incurs memory and processing costs, and can likely contribute to reduced forwarding throughput rates, increased packet latency, and loss of feature capability within 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:

- Routers with multiple integrated features enabled are best suited for branch-office or telecommuter sites where fewer devices offer a better solution.
- High-bandwidth, high-performance applications are typically better addressed with appliances; Cisco ASA and Cisco Unified Call Manager Server must 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 version 12.4(20)T, Classic Firewall and Zone-Based Policy Firewall (ZFW) were unable to fully support capabilities required for VoIP traffic and router-based voice services, which required large gaps in otherwise secure firewall policies to accommodate voice traffic, and offered limited support for evolving VoIP signaling and media protocols.

Deploy 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 are identified and described by security policy. There are two fundamental approaches to arrive at a security policy: the *trusting* perspective, as opposed to the *suspicious* perspective.

The *trusting* perspective assumes that 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 existent 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 the maintenance of 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 that all network traffic is undesired, except for specifically identified *good* traffic. It 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 masquerades as *good* traffic. Again, application controls impose operational and performance burdens on the network, although most undesired traffic must be controlled by stateless filters, such as access-control lists (ACLs) or Zone-Based Policy Firewall (ZFW) policy, so there is 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). 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 is present on the network must 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, so 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 the capability and functionality of existent applications and must be adjusted to minimize or resolve this impact.

If you need additional background to configure the Zone-Based Policy Firewall, review the Zone Firewall Design and Application Guide.

Considerations for ZFW in VoIP Environments

The Zone Firewall Design and Application Guide offers a brief discussion about router security 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 the Cisco IOS Software Version 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 12.4(20)T.

IOS Firewall Voice Features

The Cisco IOS Software Release 12.4(20)T introduced several enhancements 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 to be able to recognize secondary signaling and media channels that result from locally-destined/-originated SIP traffic
- Support for Skinny Local Traffic and CMEUpdates 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 that result from locally-destined/-originated SCCP traffic
- H.323 Support for Versions 3 and 4Updates H.323 support to versions 3 and 4 (previously supported versions 1 and 2)Introduces 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 explanations to describe the action applied by the policies. Hyperlinks to the individual feature documents are available in the Related Information section of this document if you wish to review the complete details for the voice inspection features.

Caveats

In order to reinforce points mentioned earlier, the application of the Cisco IOS Firewall with router-based voice capabilities must apply the Zone-Based Policy Firewall. The classic IOS Firewall does not include the needed capability to fully support the signaling complexities or behavior of voice traffic.

Network Address Translation (NAT)

The Cisco IOS network address translation (NAT) is frequently configured concurrently with the Cisco IOS Firewall, particularly in cases where private networks must interface with the Internet, or if disparate private networks must connect, particularly if IP address space overlaps. The 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 since NAT introduces additional complexity to troubleshooting and security-policy applications, particularly in cases where NAT overload is used. NAT can only be applied as a last-case solution to address network connectivity concerns.

Cisco Unified Presence Client (CUPC)

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

CME/CUE/GW Single Site or Branch Office with SIP Trunk to CCM at HQ or Voice Provider

This scenario offers a compromise between the single-site/distributed call-processing/PSTN-connected model described earlier in this document (CME/CUE/GW Single Site or Branch Office that connects to PSTN), and the multi-site/centralized call processing/converged voice-and-data network defined in the third scenario described in this document. This scenario still uses a local Cisco Unified CallManager Express, but long-distance dialing and HQ/remote-site telephony is accommodated primarily through site-to-site SIP trunks, with local-dial and emergency dialing through a local PSTN connection. Even in cases where the majority of legacy PSTN connectivity is removed, a basic 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 employs distributed call processing, which offers benefits and observes best practices as described in the Cisco Unified CallManager Express SRND.

Organizations can implement this type of application scenario in these circumstances:

- Disparate VoIP environments are used between sites, but VoIP is still desired in place of long-distance PSTN.
- Site-by-site autonomy is needed for dial-plan administration.
- Full call-processing capability is needed regardless of WAN availability.

Scenario Background

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

The security configuration provides these:

1. Router-initiated signaling inspection between CME and local phones (SCCP and SIP) and CME and the remote CUCM cluster (SIP).
2. Voice-media pinholes for communication between these:Local wired and wireless segmentsCME and the local phones for MoHCUE and the local phones for voice mailPhones and remote call entities
3. Application Inspection and Control (AIC), which can be applied to achieve these:Rate limit invite messagesAssure protocol conformance on all SIP traffic

Advantages/Disadvantages

This application offers the benefit of reduced costs since it carries site-to-site voice traffic on WAN data links.

A disadvantage of this scenario is that more detailed plans for WAN connectivity is required. Site-to-site call quality can be affected by many factors on the WAN, such as illegitimate/unwanted traffic (worms, viruses, peer-to-peer file-sharing) or difficult-to identify latency problems that can arise as a result of traffic engineering on carrier networks. WAN connections must be sized appropriately to offer sufficient bandwidth for both voice and data traffic; less latency-sensitive data traffic, for example, email, SMB/CIFS file traffic, can be classified as lower-priority traffic for QoS to preserve voice quality.

Another issue with this scenario is the lack of centralized call processing and the difficulties that can arise in troubleshooting call-processing failures. As such, this scenario works best for larger organizations as an intermediate step in a migration to centralized call-processing. Local Cisco CMEs can be converted to act as fully-featured SRST fallback as migration to Cisco CallManager is completed.

From the security perspective, the increased complexity of this environment makes effective security implementation and troubleshooting more difficult because connectivity over a WAN, or over VPN on the public Internet, dramatically increases the threat environment, particularly in cases where security policy requires a *trusting* perspective, where little restriction is imposed on traffic over the WAN. With this in mind, the configuration examples provided by this document implement a more *suspicious* policy that allows specific business-critical traffic, which is then examined by protocol conformance checks. Furthermore, specific VoIP actions, that is, SIP INVITE, are limited to reduce the likelihood of malicious or unintentional software malfunctions that negatively impact VoIP resources and usability.

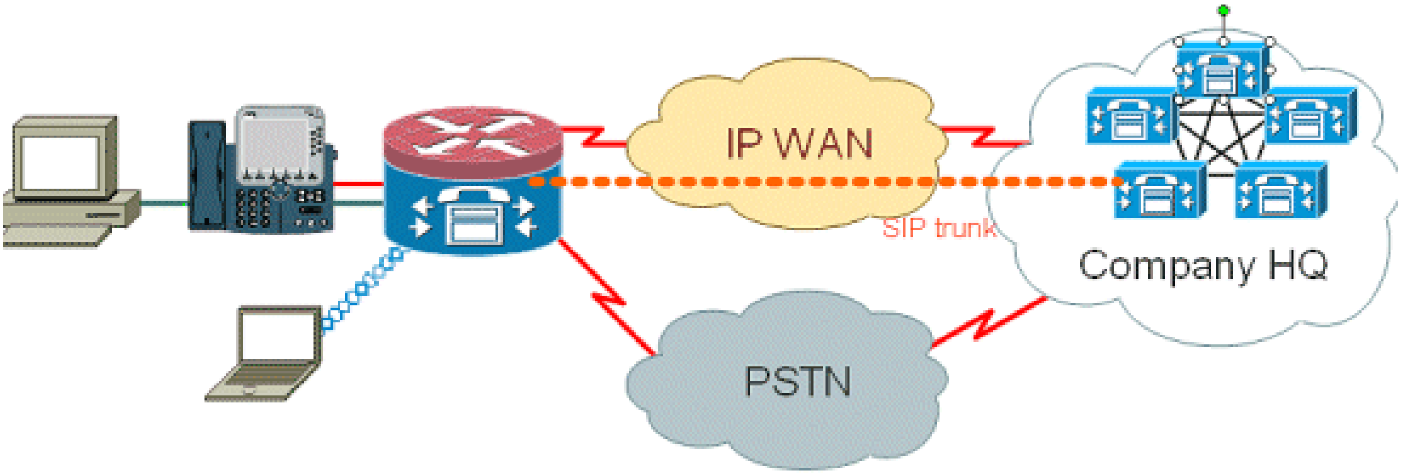
Configure

Configurations for Data Policies, Zone-based Firewall, Voice Security, CCME

In this section, you are presented with the information to configure the features described in this document.

Network Diagram

This document uses this network setup:



Configurations

The configuration described here illustrates a Cisco 2851 Integrated Services Router.

This document uses these configurations:

- Voice Service Configuration for CME and CUE Connectivity
- Zone-Based Policy Firewall Configuration
- Security Configuration

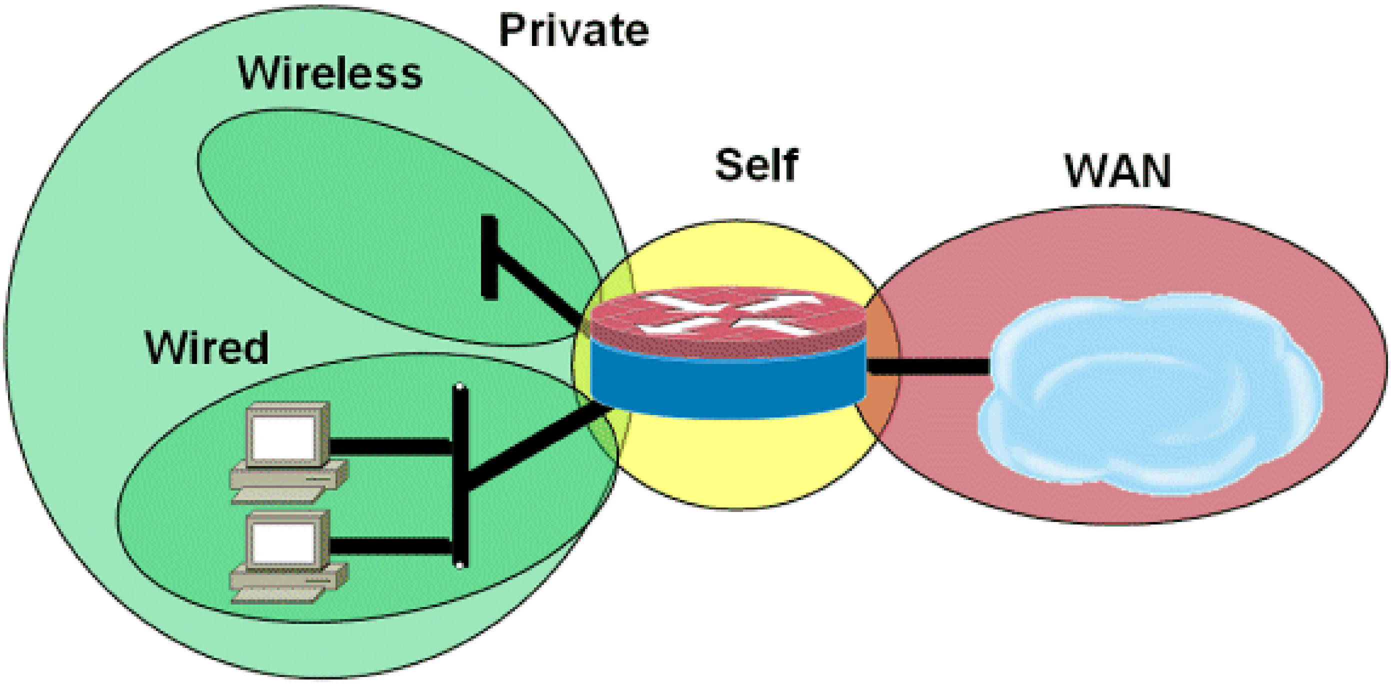
This is the Voice Service Configuration for CME and CUE connectivity:

Voice Service Configuration for CME and CUE 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 the Zone-Based Policy Firewall Configuration, composed of security zones for wired and wireless LAN segments, private LAN (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:



This is the Security Configuration:

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 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
```

Provision, Manage, and Monitor

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

The 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 the Cisco Configuration Professional.

The Cisco Secure 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 12.4(15)T4/T5 and 12.4(20)T, have not yet been fully supported in CS-MARS.

Capacity Plans

Firewall call inspection performance test results from India are TBD.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

Troubleshooting Commands

The Cisco IOS Firewall offers several **show** commands to view security policy configuration and activity. Many of these commands can be replaced with a shorter command through the application of the **alias** command.

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

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

Note: The 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 even that you need to debug, you can provide for alternative command-line interface access, such as a Telnet window that does not monitor terminal dialogue. Only enable debug on off-line (lab environment) equipment or within a planned maintenance window since debug can substantially affect router performance.

Related Information

- **Cisco Unified CallManager Express Solution Reference Network Design Guide**
- **Cisco CallManager Express Security Best Practices (CME SRND)**
- **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: SIP Enhancements: ALG and AIC**
- **Software Cisco IOS Firewall H.323 Support**
- **Cisco IOS Firewall Support for Skinny Local Traffic and CME**
- **Technical Support & Documentation - Cisco Systems**