Check Point
SOFTWARE TECHNOLOGIES LTD.

28 January 2020

VOIP

R80.40

Administration Guide

Check Point Copyright Notice

Important Information

Latest Software
We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications
For third party independent certification of Check Point products, see the Check Point Certifications page.

Check Point R80.40
For more about this release, see the R80.40 home page.

Latest Version of this Document
Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
28 January 2020	First release of this document

Table of Contents

Glossary

A

Administrator
A user with permissions to manage Check Point security products and the network environment.

API
In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols, and tools for building application software. In general terms, it is a set of clearly defined methods of communication between various software components.

Appliance
A physical computer manufactured and distributed by Check Point.

B

Bond
A virtual interface that contains (enslaves) two or more physical interfaces for redundancy and load sharing. The physical interfaces share one IP address and one MAC address. See "Link Aggregation".

Bonding
See "Link Aggregation".

Bridge Mode
A Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

CA
Certificate Authority. Issues certificates to gateways, users, or computers, to identify itself to connecting entities with Distinguished Name, public key, and sometimes IP address. After certificate validation, entities can send encrypted data using the public keys in the certificates.

Certificate
An electronic document that uses a digital signature to bind a cryptographic public key to a specific identity. The identity can be an individual, organization, or software entity. The certificate is used to authenticate one identity to another.

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
A Security Gateway that is part of a cluster.

CoreXL
A performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
Also CoreXL FW Instance. On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself. For details, see sk92449.

D

DAIP Gateway
A Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway where the IP address of the external interface is assigned dynamically by the ISP.

Data Type
A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforces the Policy accordingly.

Database
The Check Point database includes all objects, including network objects, users, services, servers, and protection profiles.

Distributed Deployment
The Check Point Security Gateway and Security Management Server products are deployed on different computers.

Domain
A network or a collection of networks related to an entity, such as a company, business unit or geographical location.

Domain Log Server
A Log Server for a specified Domain. It stores and processes logs from Security Gateways that are managed by the corresponding Domain Management Server. Acronym: DLS.

Domain Management Server
A virtual Security Management Server that manages Security Gateways for one Domain, as part of a Multi-Domain Security Management environment. Acronym: DMS.

E

Expert Mode
The name of the full command line shell that gives full system root permissions in the Check Point Gaia operating system.

External Network
Computers and networks that are outside of the protected network.

External Users
Users defined on external servers. External users are not defined in the Security Management Server database or on an LDAP server. External user profiles tell the system how to identify and authenticate externally defined users.

F

Firewall
The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restrictive shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for Check Point Gaia operating system.

H

Hotfix
A piece of software installed on top of the current software in order to fix some wrong or undesired behavior.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPv4
Internet Protocol Version 4 (see RFC 791). A 32-bit number - 4 sets of numbers, each set can be from 0 - 255. For example, 192.168.2.1.

IPv6
Internet Protocol Version 6 (see RFC 2460 and RFC 3513). 128-bit number - 8 sets of hexadecimal numbers, each set can be from 0 - ffff. For example, FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF.

L

Link Aggregation
Various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links should fail.

Log
A record of an action that is done by a Software Blade.

Log Server
A dedicated Check Point computer that runs Check Point software to store and process logs in Security Management Server or Multi-Domain Security Management environment.

M

Management High Availability
Deployment and configuration mode of two Check Point Management Servers, in which they automatically synchronize the management databases with each other. In this mode, one Management Server is Active, and the other is Standby. Acronyms: Management HA, MGMT HA.

Management Interface
Interface on Gaia computer, through which users connect to Portal or CLI. Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member.

Management Server
A Check Point Security Management Server or a Multi-Domain Server.

Multi-Domain Log Server
A computer that runs Check Point software to store and process logs in Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Security Management
A centralized management solution for large-scale, distributed environments with many different Domain networks.

Multi-Domain Server
A computer that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Acronym: MDS.

N

Network Object
Logical representation of every part of corporate topology (physical machine, software component, IP Address range, service, and so on).

O

Open Server
A physical computer manufactured and distributed by a company, other than Check Point.

P

Primary Multi-Domain Server
The Multi-Domain Server in Management High Availability that you install as Primary.

R

Rule
A set of traffic parameters and other conditions in a Rule Base that cause specified actions to be taken for a communication session.

Rule Base
Also Rulebase. All rules configured in a given Security Policy.

S

Secondary Multi-Domain Server
The Multi-Domain Server in Management High Availability that you install as Secondary.

SecureXL
Check Point product that accelerates IPv4 and IPv6 traffic. Installed on Security Gateways for significant performance improvements.

Security Gateway
A computer that runs Check Point software to inspect traffic and enforces Security Policies for connected network resources.

Security Management Server
A computer that runs Check Point software to manage the objects and policies in Check Point environment.

Security Policy
A collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

Single Sign-On
A property of access control of multiple related, yet independent, software systems. With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers. Acronym: SSO.

SmartConsole
A Check Point GUI application used to manage Security Policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard
A legacy Check Point GUI client used to create and manage the security settings in R77.30 and lower versions.

Software Blade
A software blade is a security solution based on specific business needs. Each blade is independent, modular and centrally managed. To extend security, additional blades can be quickly added.

SSO
See "Single Sign-On".

Standalone
A Check Point computer, on which both the Security Gateway and Security Management Server products are installed and configured.

T

Traffic
Flow of data between network devices.

U

Users
Personnel authorized to use network resources and applications.

V

VLAN
Virtual Local Area Network. Open servers or appliances connected to a virtual network, which are not physically connected to the same network.

VLAN Trunk
A connection between two switches that contains multiple VLANs.

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Securing Voice Over IP

Introduction to Check Point Secure VoIP

Check Point's R80.40 secures your VoIP environment. Check Point Security Gateways secure VoIP traffic in SIP, H.323, MGCP, and SCCP environments. VoIP calls involve complex protocols, each of which can carry potentially threatening information through many ports.

The Check Point Security Gateways confirm that the caller and receiver addresses are located where they are supposed to be, and that the caller and receiver are allowed to make and receive VoIP calls. The Gateways examine the contents of the packets and confirm that they carry only allowed information. Full stateful inspection on SIP, H.323, MGCP, and SCCP commands ensure that all VoIP packets are structurally valid, and that they arrive in a valid sequence.

This guide explains how to configure the Check Point Security Gateway when VoIP passes through it.

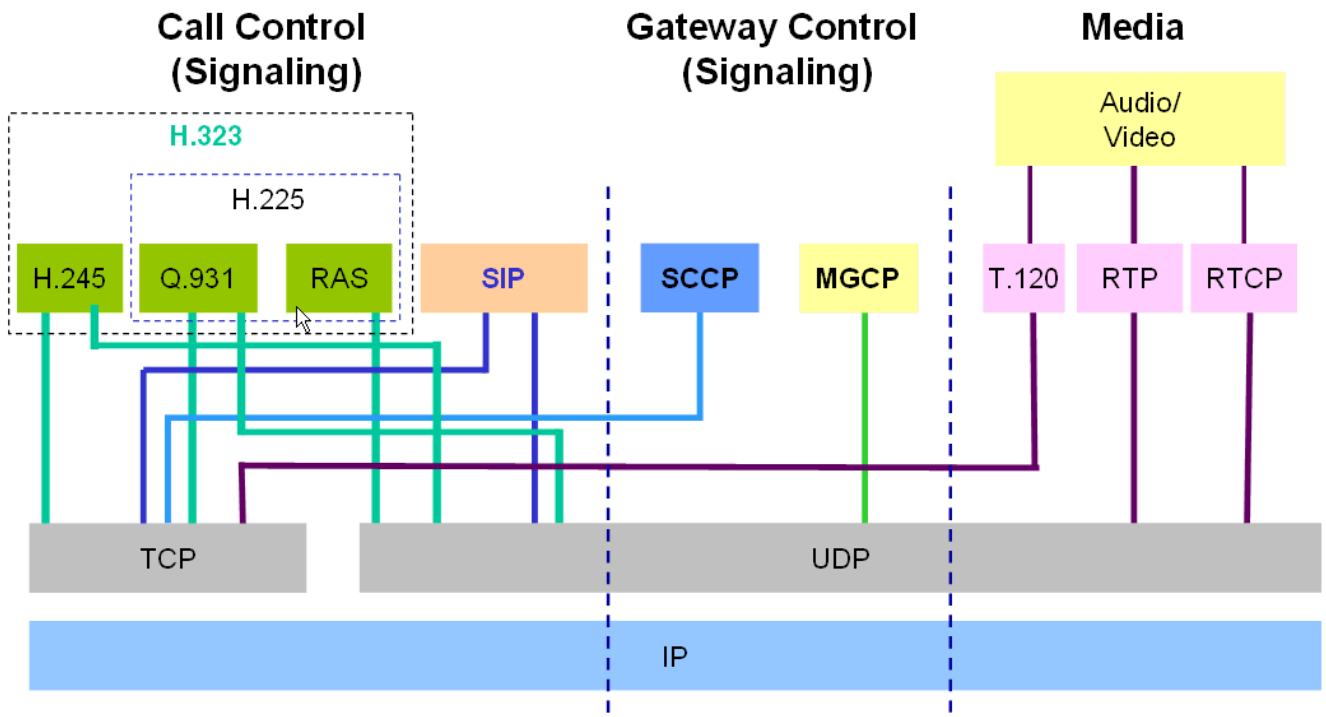
You can deploy VoIP over these protocols:

- SIP
- MGCP
- H.323
- SCCP

VoIP and the Security Gateway

The Security Gateway secures VoIP traffic in SIP, MGCP, H.323, and SCCP environments.

VoIP calls use a series of complex protocols, each of which can transmit potentially malicious data through many ports.



H.323 Version 4 supports H.245 over UDP/TCP and Q.931 over UDP/TCP and RAS over UDP.
SIP supports TCP and UDP.

The Security Gateway makes sure that:

- Caller and recipient addresses are where they claim to be
- Caller and recipient are allowed to make and receive VoIP calls

In addition, the Security Gateway examines the contents of the packets passing through all allowed ports to make sure the packets contain the correct information.

Full stateful inspection on all protocols makes sure that:

- All VoIP packets are structurally valid
- The packets arrive in a valid sequence

VoIP Security Deployments

This section offers several use cases for deployment:

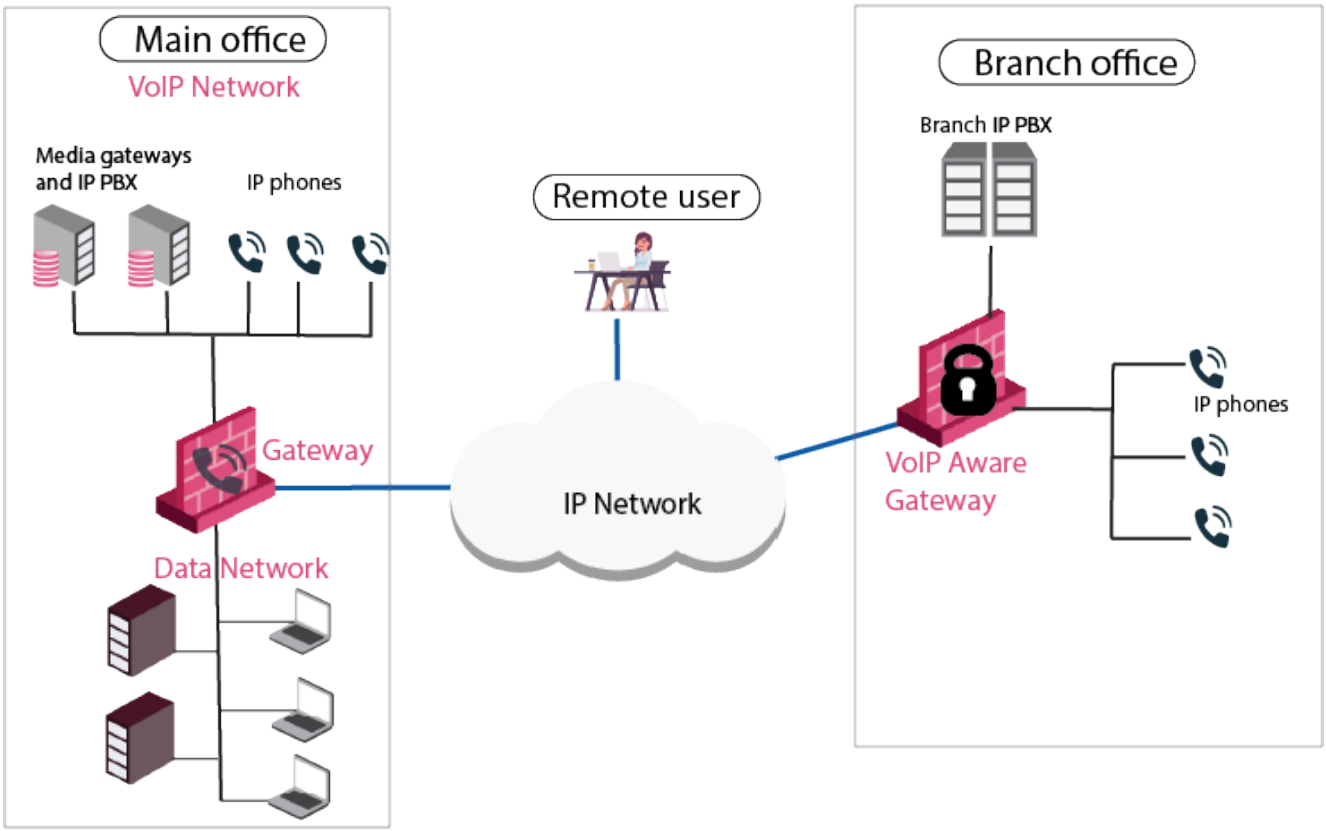
- Enterprises
  - Perimeter VoIP gateway
  - LAN segmentation
- Managed service providers

Use Case 1: Enterprise Deployment - Perimeter VoIP Gateway

In this enterprise environment, remote users and branch offices make VoIP calls to and from the protected enterprise network. The Security Gateway is used to set up IPsec encrypted VPNs.

For example, a VPN can be set up between the main office and branch offices. Security capabilities for VoIP include:

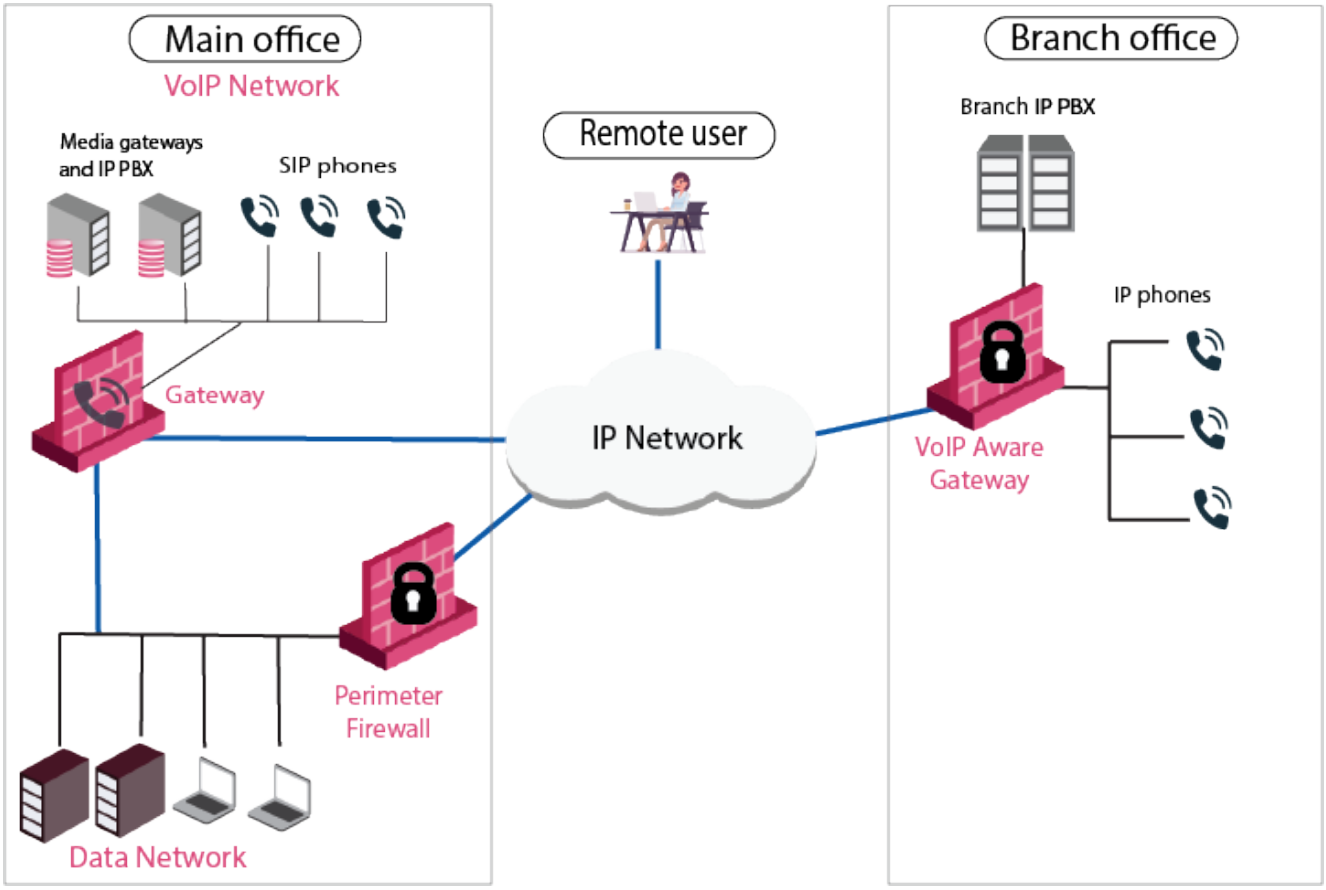
- Protecting servers and PBXs in the enterprise LAN against Denial of Service (DOS) attacks.
- Preventing unauthorized phone calls by means of Media Admission Control. Only Configured servers can set up calls.



Use Case 2: Enterprise Deployment - LAN Segmentation

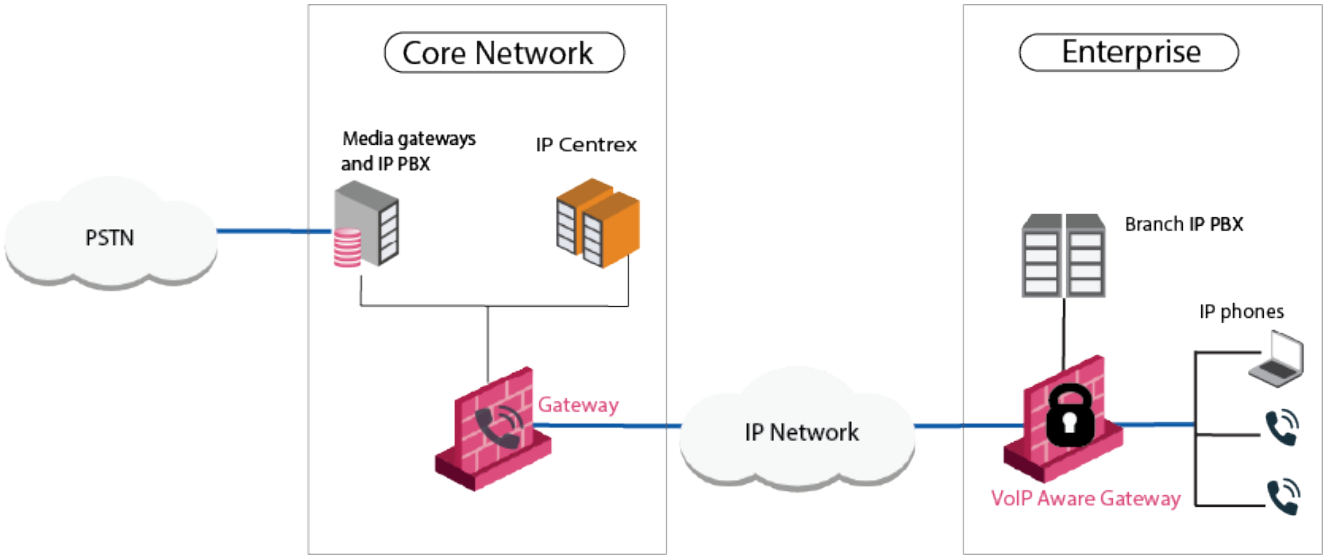
In this enterprise deployment, the Security Gateway is used for internal LAN segmentation of VoIP and data traffic.

Dedicated gateways are deployed for VoIP security. Security is required to protect the availability of VoIP equipment such as servers and PBXs in the enterprise LAN.



Use Case 3: Service Provider Deployment

A service provider environment enables secure enterprise services. The Security Gateway also makes it possible to implement strong security measures that are necessary for a high quality of service.


Core Network
Media gateways and IP PBX
IP Centrex
PSTN
Gateway
IP Network
Enterprise
Branch IP PBX
IP phones
VoIP Aware Gateway

VoIP Technology and Standards

Media and Control Signals

A phone call on an ordinary digital phone network and on a VoIP network is made up of media signals and control signals. The voice conversation is the media stream.

Dial tones and ringing tones, for example, are an indication that call control processes are occurring.

The different VoIP protocols use very different technologies, though they have the same aim. VoIP protocols handle these call control (or gateway) control and media functions:

- **Call Control** (signaling): Responsible for:
  - setting up the call
  - finding the peer
  - negotiating coding protocols
  - making the connection
  - ending the call
- **Gateway Control**: Responsible for control signals between VoIP gateways, rather than between endpoint phones. These gateways negotiate VoIP traffic on behalf of the phones.
- **Media**: The voice or video payload. VoIP networks and ordinary phone networks use RTP/RTCP for the media. RTP carries the actual media and RTCP carries status and control information.

Control signals open fixed (known) ports and dynamic ports. The parties on a call then use control signals to negotiate dynamically assigned ports that each side opens to receive the RTP/RTCP media stream.

Supported SIP RFCs and Standards

The Security Gateway supports these SIP RFCs and standards:

- RFC 3261 SIP: Session Initiation Protocol
- RFC 3372 Session Initiation Protocol for Telephones (SIP-T)
- RFC 3311 UPDATE message
- RFC 2976 INFO message
- RFC 3515 REFER message
- RFC 3265 SIP Events
- RFC 3262 Reliability of Provisional Responses
- RFC 3428 MESSAGE message
- RFC 4566 SDP Session Description Protocol
- RFC 3264 An Offer-Answer Model with Session Description Protocol
- RFC 3265 Specific Event Notification

- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3263 Locating SIP Servers
- RFC 3581 An Extension to the SIP for Symmetric Response Routing
- RFC 3892 SIP Referred-By Mechanism
- RFC 5194 Framework for Real-Time Text over IP Using SIP
- RFC 3326 The Reason Header Field for SIP

Supported MGCP RFCs and Standards

The Security Gateway supports these MGCP RFCs and standards:

- RFC-2705.
- RFC-3435 (version 1.0)
- ITU TGCP specification J.171.

Supported H.323 Protocols and Standards

Media in H.323 uses the RTP/RTCP and/or T.120 protocols.

Signaling is handled by these H.323 protocols:

- RAS manages registration, admission, and status. RAS uses a fixed port: UDP 1719.
- Q.931 manages call setup and termination. Q.931 uses a fixed port: TCP 1720.
- H.245 negotiates channel usage and capabilities. H.245 uses a dynamically assigned port.

As an H.323 call is processed by a gatekeeper, these protocols are used in sequence and then the media passes. To end a call, the signaling protocols are used in reverse order.

When an endpoint connects to a gateway, it does not use RAS. Otherwise, the protocol sequence for a gateway is the same as for a Gatekeeper.

The Security Gateway also supports H.245 tunneling and Fast Connect, an H.323 capability. That ensures that audio is available when the phone is answered. This feature is active by default, and is always available.

These H.323 ITU standards are supported:

- H.323 Versions 2, 3, and 4
- H.225 Versions 2, 3, and 4
- H.245 Versions 3, 5, and 7

Session Initiated Protocol (SIP)

Introduction to SIP

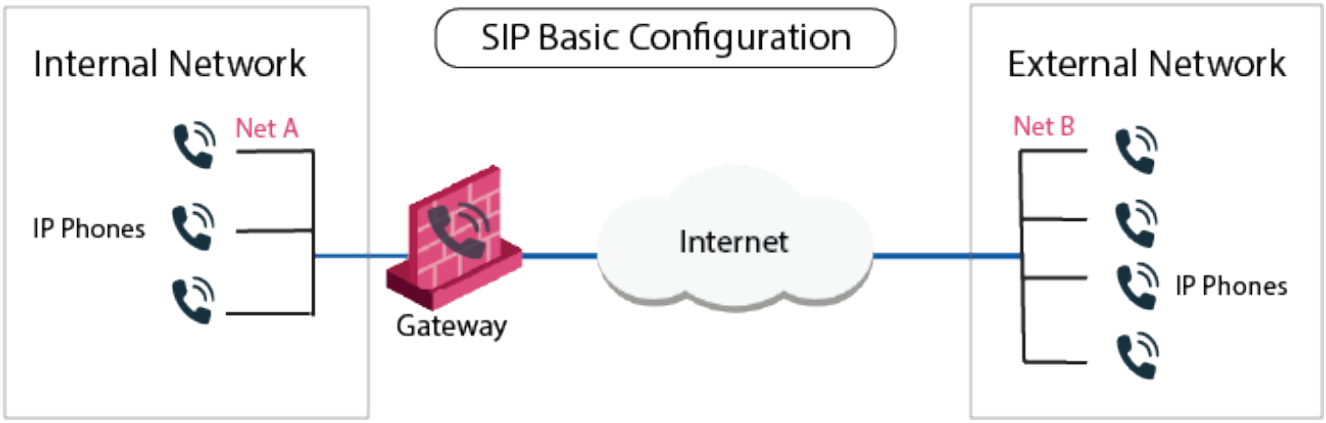
Session Initiation Protocol (SIP) is transported over UDP and TCP. It is an Application Layer control protocol that creates, modifies, and terminates sessions with one or more participants. SIP is a peer-to-peer protocol.

SIP uses design elements similar to the HTTP request/response transaction model. SIP clients usually use TCP or UDP on port numbers 5060 or 5061 to connect to SIP servers and other SIP endpoints. Port 5060 is commonly used for non-encrypted signaling traffic, whereas port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS).

To configure your environment with SIP in SmartConsole, see Setting Up Your Network with NAT for NAT rules, and SIP Security Rules for examples of Rule Base configuration.

Basic SIP Configuration

In a basic SIP configuration, a Security Gateway sits between an Internal Network and an External Network, with or without a proxy.



SIP-Specific services

These preconfigured SIP services are available for gateways of version R80.XX or higher.

Services	Port	Protocol Type	Description
`sip`	UDP 5060	`SIP_UDP`	This service enforces signal routing. Use a VoIP Domain in the source or destination of a rule, together with this service. When you use this service, registration messages are tracked and a database is maintained that includes the details of the IP phones and the users. If an incoming call is made to a Hide NATed address, the Security Gateway confirms the user exists in the SIP registration database. This can prevent DoS attacks.

Services	Port	Protocol Type	Description
sip_tcp	TCP 5060	SIP_TCP_PROTO	Used for SIP over TCP.
sip_dynamic_ports	Not set	Not set	This service allows a SIP connection to be opened on a dynamic port and not on the SIP well-known port.
sip_tls_not_inspected	TCP 5061	None	Allows SIP over TLS to pass without inspection. It requires that you open the media ports manually.
sip_tls_authentication	TCP 5061	SIP_TCP_PROTO	SIP over non-encrypted TLS and authenticated only. NAT is not supported for connections of this type.

These legacy SIP services are used for gateways of version R75.40 and below, if not enforcing handover. Do not use these services for R.80.xx (or higher).

Services	Purpose
sip_any	Use **sip_any** for VoIP equipment that uses SIP UDP. Do not place a VoIP Domain in the **Source** or **Destination** of a rule. Instead, use *** Any** or a Network Object, together with one of these services. **Note** - If a VoIP Domain is used with this service, the packet is dropped. **Important** - Do not use this service in the same rule with the **sip** service because they contradict each other.
sip-tcp_any	Use **sip-tcp_any** for VoIP equipment that uses SIP TCP. Use this service if you do not enforce signal routing. In that case, do not place a VoIP Domain in the **Source** or **Destination** of a rule. Instead, use *** Any** or a Network Object together with the **sip_any-tcp** service. **Note** - If a VoIP Domain is used with this service, the packet is dropped. **Important** -Do not use this service in the same rule with the **sip-tcp** service because they contradict each other.

Legacy Solution for SIP TLS Support

If you are not able to use the **sip_tls_authentication** service, add these two rules instead:

- A rule that uses the **udp-high-ports** service to open all high UDP ports for the entities sending dat

  AND

- A rule that uses the **sip_tls_not_inspected** service to open TCP port 5061 for the entities sending signaling

This can happen if connections are encrypted by TLS, or NAT must be done on the connections.

Important - SIP signaling and data is not inspected if you open all high UDP ports. The connection is not-secured.

To configure support for SIP TLS in environments where a secure solution is not available:

1. Configure Network Objects in SmartConsole for the SIP phones.
2. Configure a Network Object for the SIP proxy.
3. Configure a rule that opens all high UDP ports and TCP port 5061.

The rule below shows that the phones send data directly to each other, and not through the proxy.

No	Name	Source	Destination	VPN	Services & Applications	Action	Track
1	Transmit through proxy	SIP Proxy SIP Phones	SIP Phones SIP Proxy	* Any	TCP: sip_tls_not_ inspected	Accept	Log
2	Transmit directly	SIP Phones	SIP Phones	* Any	UDP: udp-high-ports	Accept	Log

Supported SIP Topologies and NAT Support

Below is a list of supported SIP topologies. The table also lists NAT that you can configure with each topology. it with. SIP can use a Proxy (or Registrar). If there is more than one proxy device, signaling passes through one or more of them. After the call is set up, the media can pass from endpoint to endpoint directly, or through one or more of the proxies.

Deployment	Supports No-NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Proxy - Static NAT	Description
SIP Endpoint to Endpoint	Yes	Static NAT only	Not applicable	■ Phones communicate directly without a proxy. ■ Static NAT can be configured for the phones on the internal side of the gateway.
SIP Proxy in External Network	Yes	Yes	Not applicable	■ IP phones use the services of a proxy on the external side of the gateway. ■ Enables the use of a proxy that is maintained by another organization. ■ Configure Hide NAT, Static NAT, or no-NAT for the phones on the internal side of the gateway.

Deployment	Supports No-NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Proxy - Static NAT	Description
SIP Proxy to SIP Proxy	Yes	Yes	Yes	■ Each proxy controls a separate endpoint domain. ■ Configure Static NAT for the internal proxy. ■ Configure Hide NAT or Static NAT for the internal phones.
SIP Proxy in DMZ	Yes	Yes	Yes	■ The same proxy controls both endpoint domains. This makes it possible to provide proxy services to other organizations. ■ Static NAT or no-NAT can be configured for the proxy. ■ Hide NAT, Static NAT, or no NAT can be configured for the phones on the internal side of the gateway.

For complete information on NAT configuration, see the *R80.40 Security Management Administration Guide*.

Below are some exceptions when you use SIP with NAT:

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Calls cannot be made from an external source to two endpoints on the trusted side of a gateway if only one of the endpoints is NAT enabled.
- You can use Automatic NAT for other deployments.

Opening Dynamic Ports for SIP Signaling

`sip_dynamic_ports` enables ports to open dynamically for SIP signaling. Therefore, if there is a port that is not Configured by one of the SIP services, it can still establish SIP connections. The Check Point Security Gateway opens and closes ports based on the inspection of SIP signaling messages.

Add the `sip_dynamic_ports`service to the **Services & Applications** column of the Rule Base when:

- You use a non-default port.
- The phones register themselves as a SIP server by associating their phone number with an unknown port.

  For example:

  A registration request for phone number 2001 with IP address 172.16.8.3 port 3000. An example of this contact header field is:

Contact:
`<sip:2001@`**172.16.8.3:3000**`;rinstance=64d25786c64e7975>;expires=3600`

The `rport` parameter is found in the **Via** header field when the port is relocated.

For example:

Via: `SIP/2.0/TCP 172.16.8.3:5060;branch=z9hG4bK-1193792f8039818cd82e34eec4112ae8;`**rport=4039**

See RFC 3581 - *An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing*.

Note - Use the `sip_dynamic_ports` service with at least one other SIP service in a rule.

Sample Rule With the sip_dynamic_ports Service

Example of SIP UDP rule:

Source	Destination	Services & Applications	Action
SIP_phone SIP_server	SIP_server SIP_phone	udp:sip sip_dynamic_ports	Accept

- `SIP_phone`is the IP address of the SIP phone.
- `SIP_server` is the IP address of the SIP server.

Important Information About Creating SIP Security Rules

- Make sure to check **Keep all connections** if you do not want in-progress calls to drop every time you **Install Policy**.
  1. From SmartConsole, the Gateways & Servers tab, double-click your gateway.

     The **Check Point Security Gateway** window shows.
  2. From**General Properties > Other > Connection Persistence > Keep all connections > OK**.

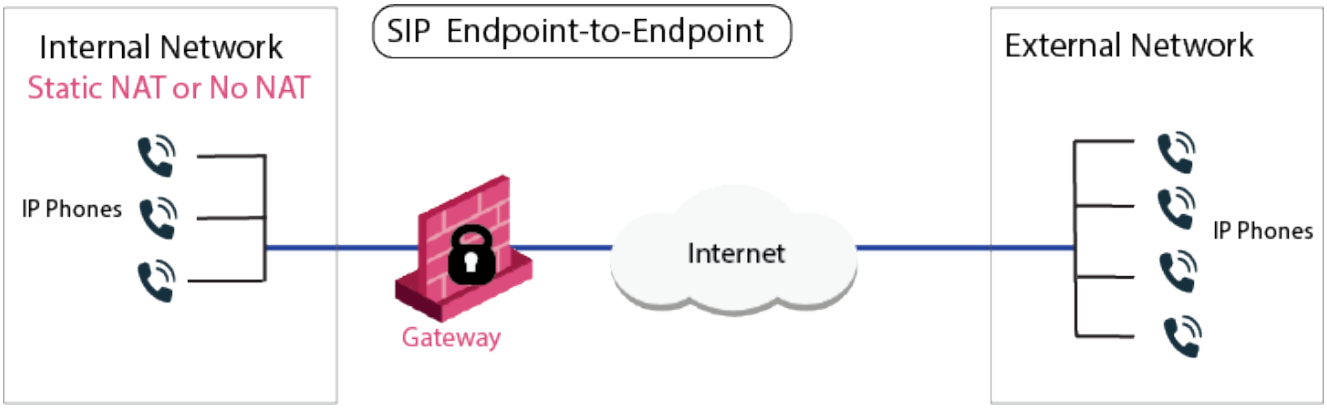
     Note - **Rematch connections** is selected by default.
- Do not configure special Network Objects to allow SIP signaling, use regular Network Objects. The Security Gateway dynamically opens ports for data connections (RTP/RTCP and others). Security Gateways support up to four different media channels per SIP SDP message.
- When you use **Hide NAT for SIP over UDP** and **Hide NAT for SIP over TCP**, include the hidden IP address in the **Destination** of the SIP rule. When you include the hidden IP address, this allows the initiation of the TCP handshake from the external network to the hidden IP.
- For NAT on SIP entities, we strongly recommended that you enable the Inspection Settings **Strict SIP Protocol Flow Enforcement**, see Configuring Inspection Settings.
- For Automatic configuration for **Static NAT**, you must add a NATed object to the **Destination** column in the Rule Base.

Important -You must configure anti-spoofing on the Check Point gateway interfaces for VoIP.

Note - The old policy rules are still intact for calls already in-progress and they will not be dropped.

Sample SIP Rules for an Endpoint-to-Endpoint Network

Sample VoIP Access Control:



Source	Destination	Services & Applications	Action	Comments

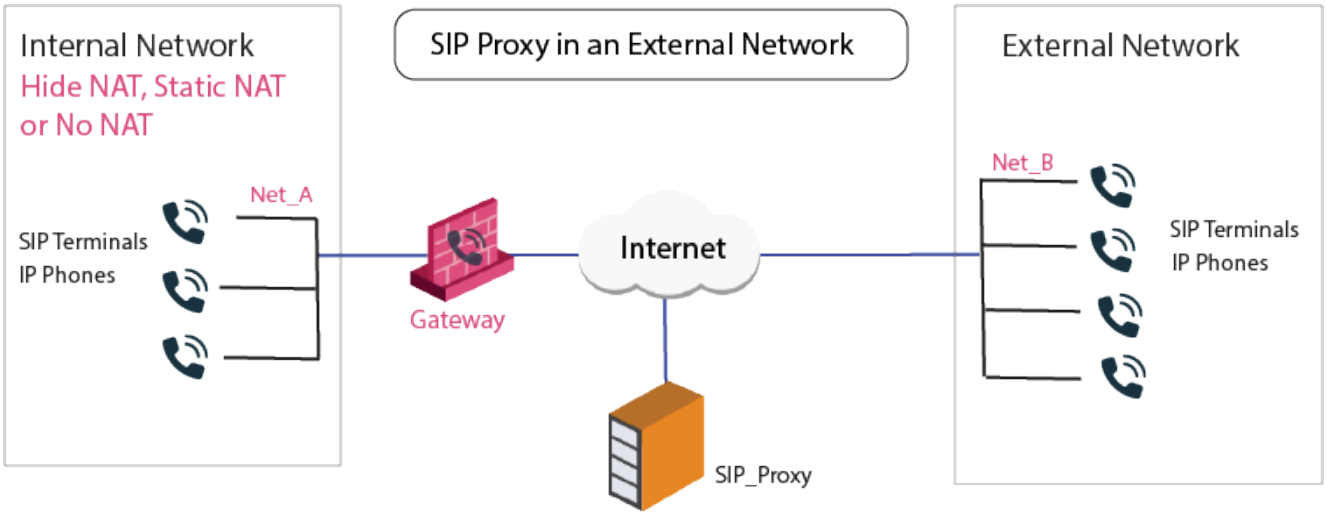
Net_A
Net_B
	Net_B
	Net_A
		`sip_any`
		OR
		`sip_any-tcp`
		OR
		`sip-tcp`
			Accept	SIP bidirectional calls

To configure bidirectional call rules for this peer-to-peer topology:

1. Configure an Access Control rule that allows IP phones in **Net_A** to call **Net_B** and the reverse.
2. Choose the applicable SIP service
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

Sample SIP Rules for a Proxy in an External Network

This illustration shows a SIP topology with a proxy in an external network.



Sample VoIP Access Control rules for this topology:

Source	Destination	Services & Applications	Action	Comments
SIP_Proxy Net_A	Net_A SIP_Proxy	UDP:sip	Accept	SIP over UDP Bidirectional Calls

OR

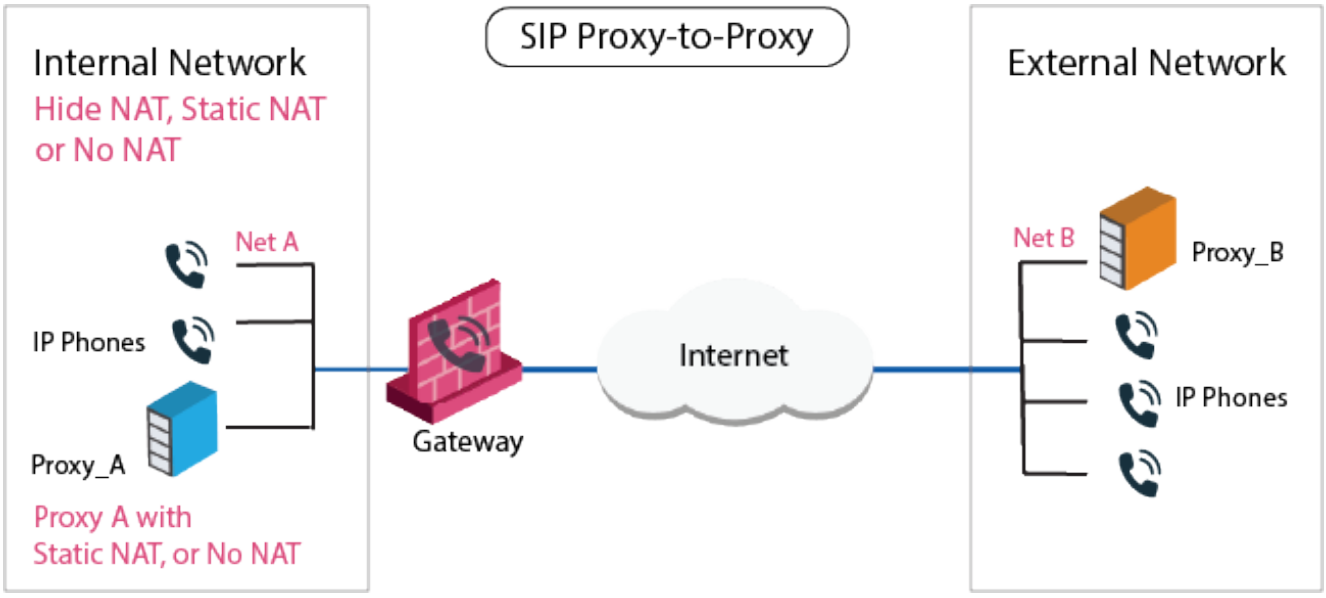
Source	Destination	Services and Applications	Action	Comments
SIP_Proxy Net_A	Net_A SIP_Proxy	SIP over TCP service	Accept	SIP over TCP Bidirectional Calls

To allow bidirectional calls between SIP phones in internal and external networks:

1. Configure Network Objects (nodes or networks) for IP phones that are:
   - Managed by the SIP Proxy or Registrar
   - Permitted to make calls, and those calls inspected by the gateway. In the image, these are **Net_A**.
2. Configure the Network Object for the SIP Proxy (`SIP_Proxy`).
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

Sample SIP Rules for a Proxy-to-Proxy Topology

The image illustrates a Proxy-to-Proxy topology with Net_A and Net_B on opposite sides of the gateway.



Sample VoIP Access Controlrules for this topology:

Source	Destination	Services & Applications	Action	Comments
Proxy_A Proxy_B	Proxy_B Proxy_A	UDP:sip	Accept	SIP over UDP Bidirectional calls

OR

Source	Destination	Services & Applications	Action	Comment
Proxy_A Proxy_B	Proxy_B Proxy_A	SIP over TCP	Accept	SIP over TCP Bidirectional calls

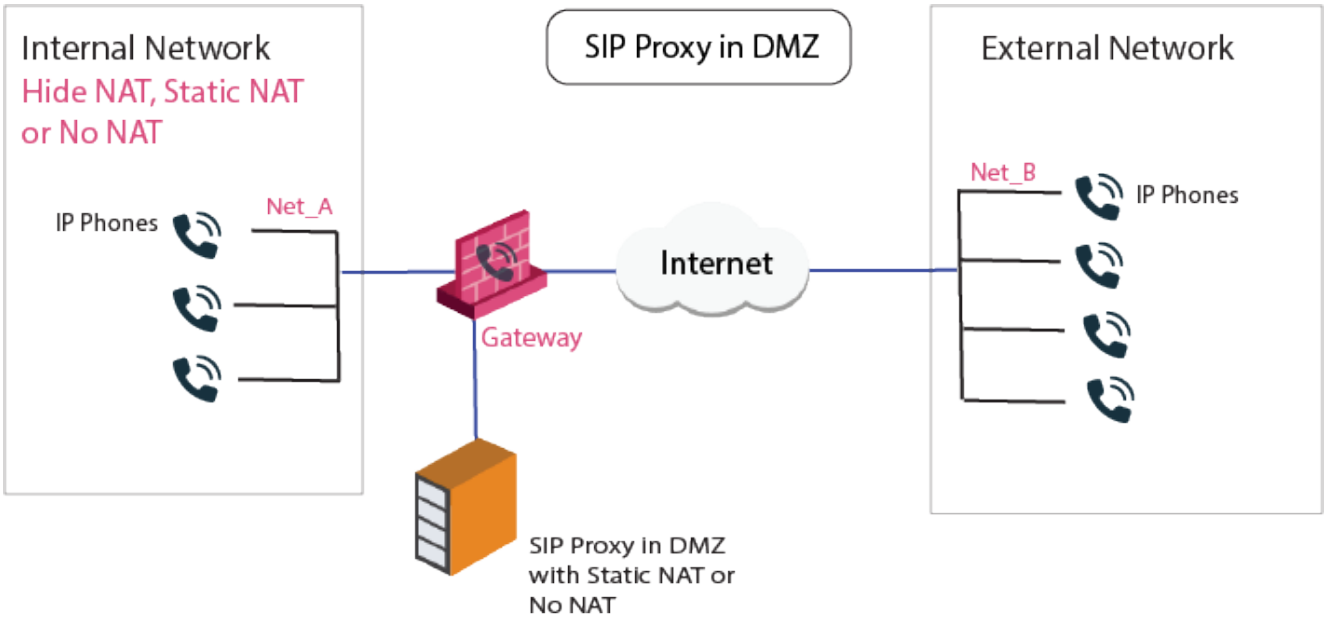
To allow bidirectional calls between phones:

1. Configure the Network Objects (nodes or networks) for the phones permitted to make calls, and the calls subject to gateway inspection.

   In the image above, **Net_A** represents these phones.
2. Configure the Network Object for the proxy objects (**Proxy_A** and **Proxy_B**).
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

Sample SIP Rules for a Proxy in DMZ Topology

The image illustrates a SIP-based VoIP topology where a proxy is installed in the DMZ.



Sample VoIP Access Controlrules for this topology:

Source	Destination	Services & Applications	Action	Comments
Proxy_DMZ Net_A Net_B	Net_A Net_B Proxy_DMZ	UDP:sip	Accept	SIP over UDP Bidirectional Calls

OR

Source	Destination	Services & Applications	Action	Comments
Proxy_DMZ Net_A Net_B	Net_A Net_B Proxy_DMZ	SIP over TCP Service	Accept	SIP over TCP Bidirectional Calls

Allow bidirectional calls between phones in internal and external networks (**Net_A** and **Net_B**) and Configure NAT for the internal phones and the proxy in the DMZ (**Proxy_DMZ**).

To configure bidirectional calls between phones in the internal and external networks:

1. Configure Network Objects (nodes or networks) for phones that are permitted to make calls and for calls inspected by the gateway. These are **Net_A** and **Net_B**.
2. Configure the Network Object for the proxy (**Proxy_DMZ**).
3. Configure the VoIP rules.
4. Configure **Hide NAT** or **Static NAT** for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

SIP Advanced Configuration

Gateway Clustering Support for SIP

Synchronizing SIP Connections

SIP calls can be made across a ClusterXL cluster or a third-party cluster.

The **Synchronize connections on Cluster** option must be selected for:

- ClusterXL
- Third party clusters
- When SIP connections can arrive asymmetrically
- All services used in rules that secure SIP connections through the cluster

To confirm that SIP connections through a cluster are synchronized:

1. Open SmartConsole.
2. Go to **Object Explorer** > **Services**.
3. Locate your service with the search box and double-click on it.
4. Select the **Advanced** tab.
5. Make sure the **Synchronize connections on Cluster** box is checked.

   Note - The **Synchronize connections on Cluster** option is enabled by default.
6. Click **OK**.
7. Install the Access Control policy.

Configuring SIP-T Support

To configure support for RFC 3372 Session Initiation Protocol for Telephones (SIP-T):

1. In the applicable $FWDIR/lib/user.def file on the Security Management Server (see sk98239), add this line:

   ```
   sipt_hosts = { <first_ip, second_ip> , <first_ip, second_ip> , ....
   ...., <first_ip, second_ip> } ;
   ```

   `first_ip` and `second_ip` are the IP addresses between which (bidirectional) SIP-T are allowed.

   For example, to allow SIP-T between 192.1.1.1 and 192.1.1.2, and between 192.1.1.1 and 192.1.1.3, add this line:

   ```
   sipt_hosts = { <192.1.1.1, 192.1.1.2> , <192.1.1.1, 192.1.1.3> } ;
   ```

   If the file does not exist, create it.
2. Save the file.
3. **Install Policy**.

SIP Protocol Anomaly Protection

RFC 3261 section 6, has rules for the structure of SIP headers:

- SIP messages are made up of a header and a body
  - A header is structured as a sequence of header fields
  - A header field can show as one or more header field rows
  - Each header field:
    - Consists of a field name
    - Is followed by a colon (:) and zero or more field values, **field-name:field-value**
- Multiple header field values on a given header field row are separated by commas
- Some header fields can only have a one header field value, and show as a single header field row

Protocol anomalies can result in buffer overflow conditions, parser errors, and malformed packets. Protocol anomalies in SIP messages make SIP applications vulnerable to attacks that send repeated, huge quantities of fraudulent data. The data that eventually overwhelms the server.

For example, many buffer-overflow attacks send repeated, large headers to the VoIP phone. Buffer overflow conditions can also result in arbitrary code execution.

Stateful and Stateless protocol validation is done on SIP headers. SIP messages with header values that do not match correct usage are blocked.

There are two header security protections found in the main Protocol Anomaly protection.

- General Header Securit

  In the general SIP header and not in specified header fields

- Specific Header Securit

  In specific SIP header fields

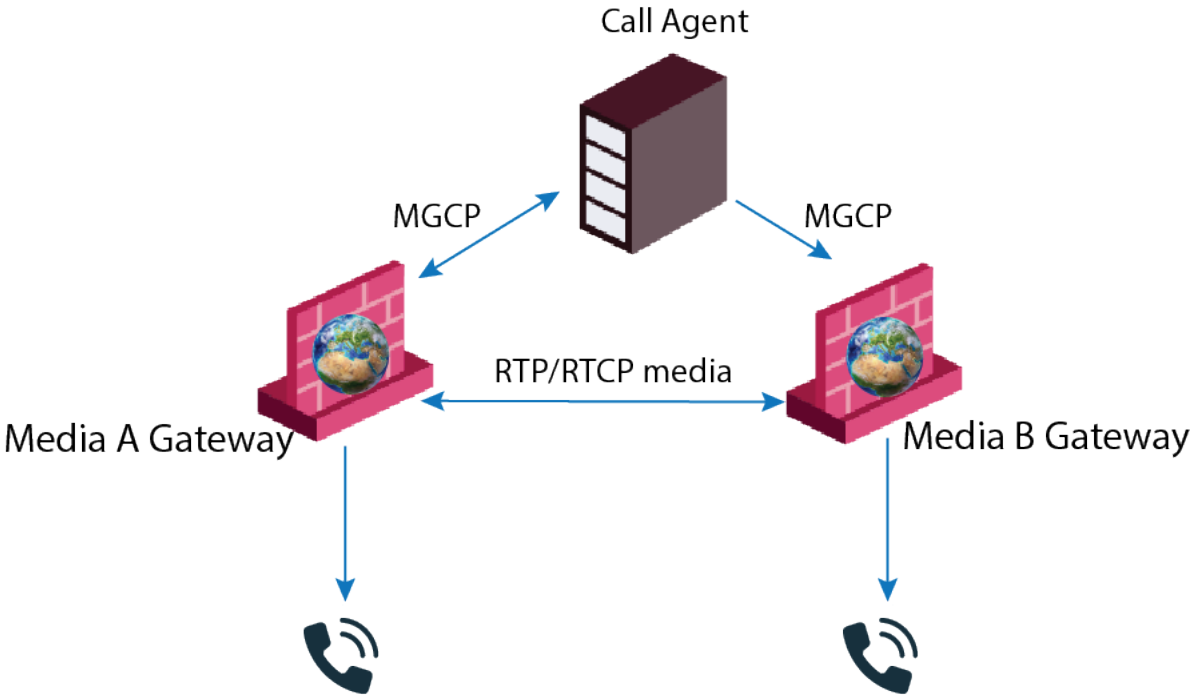
MGCP-Based VoIP

Introduction to MGCP

MGCP is a protocol used to control telephone gateways from external call control devices called Call Agents, and Media Gateway Controllers. MGCP is a master-slave protocol. The Call Agent is the master and the endpoints are the slaves. This protocol is different from SIP and H.323 which are peer-to-peer protocols.

With the MGCP protocol, Call Agents synchronize with each other to send commands to the devices they control (Media Gateway). Call Agents connect directly to IP phones. The Media Gateway and IP phones run with commands sent by the Call Agents. The image below shows the MGCP elements and call control actions. Media Gateway and MGCP IP phones can support features such as conference calls, 3-way brokering and supervisor inspection.

Depending on the Call Agent you use, MGCP can operate together with SIP and H.323.



MGCP-Specific services

Preconfigured MGCP-Specific Services

Service	Ports	Protocol Type	Description
mgcp_CA	UDP 2727	MGCP_UDP	Call-Agent, Media Gateway Controller port.

Service	Ports	Protocol Type	Description
mgcp_MG	UDP 2427	MGCP_UDP	Media Gateway port.
MGCP_dynamic_ports	Not set	Not set	Allows you to open an MGCP connection on a dynamic port and not on the MGCP well known port.

Supported MGCP Topologies and NAT Support

For complete information on NAT configuration, see the *R80.40 Security Management Administration Guide*.

The Security Gateway supports the MGCP deployments listed in the table. NAT is not supported on IP addresses behind an external Security Gateway interface.

Supported MGCP Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Description
Call Agent in External Network	Yes	Yes	■ The IP phones use the services of a Call Agent on the external side of the gateway. This enables the use of a Call Agent that is maintained by another organization. ■ You can configure Hide NAT, Static NAT, or No-NAT for the ph ones on the internal side of the gateway.
Call Agent in the DMZ	Yes	No	■ The same Call Agent controls both endpoint domains. ■ This topology makes it possible to provide Call Agent services to other organizations.
Call Agent to Call Agent	Yes	No	■ Each Call Agent controls a separate endpoint domain. ■ When there is one or more Call Agents, the signaling passes through each Call Agent. Once the call has been set up, the media can pass endpoint to endpoint.

Notes:

Below are the following exceptions for using MGCP with NAT:

- Manual NAT rules are not supported. You must use Automatic NAT.
- If only one endpoint is NAT enabled, calls cannot be made from an external source to two endpoints on the trusted side of a gateway.
- Bidirectional NAT of VoIP calls is not supported.

Sample MGCP Packet Before NAT

The image of this packet capture shows an MGCP packet from a phone with IP address 194.90.147.53, and source port 2427 - which is the default MGCP port.

```
Frame 19 (129 bytes on wire, 129 bytes captured)
Ethernet II, Src: 00:00:00:00:00:00, Dst: 69:31:65:74:68:31
Internet Protocol, Src Addr: 194.90.147.53 (194.90.147.53), Dst:
67.130.192.131 (67.130.192.131)
User Datagram Protocol, Src Port: 2427 (2427), Dst Port: 2727 (2727)
Media Gateway Control Protocol
   verb: NTFY
   Transaction ID: 22
   Endpoint: d001@00064ab42c2
   Version: MGCP 1.0
   The response to this request is in frame 57
   Parameters
     NotifiedEntity (N): cs@[67.130.192.131]:2727
     RequestIdentifier (x): 83ec66591c69
     ObservedEvents (o): L/hd
```

Sample MGCP Packet After Hide NAT When Option is Disabled

The image of the packet capture below shows the MGCP packet after Hide NAT, with the **Hide NAT changes source port for MGCP** option *disabled*. The IP address is translated to the Hide NAT address of 194.90.147.14, but the source port 2427 is unchanged.

```
Frame 16 (129 bytes on wire, 129 bytes captured)
Ethernet II, Src: 00:00:00:00:00:00, Dst: 4f:62:65:74:68:30
Internet Protocol, Src Addr: 194.90.147.14 (194.90.147.14), Dst:
67.130.192.131 (67.130.192.131)
User Datagram Protocol, Src Port: 2427 (2427), Dst Port: 2727 (2727)
Media Gateway Control Protocol
   verb: NTFY
   Transaction ID: 13
   Endpoint: d001@000364ab42c2
   Version: MGCP 1.0
   The response to this request is in frame 23
   Parameters
     NotifiedEntity (N): cs@[67.130.192.131]:2727
     RequestIdentifier (x): 83ec66591c69
     ObservedEvents (o): L/hd
```

In this environment, all the internal phones are registered with the same Source IP ,194.90.147.14, and the default MGCP source port, 2427.

Some MGCP servers can register a phone with only one IP address and port combination. As a result, only one of the phones behind that IP address will be registered successfully on the server.

Important Information about Creating MGCP Security Rules

You can configure the Security Rule Base so that the gateway allows MGCP calls.

Best practice - Configure anti-spoofing on the Check Point gateway interfaces.

- To allow MGCP conversations, create rules that let MGCP control signals through the gateway.

  It is not necessary to configure a rule that specifies which port to open and which endpoint can talk. The gateway automatically gets this information from the signaling. For VoIP signaling rules, the gateway automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream connections.

- Make sure to check **Keep all connections** or the firewall drops your connection every time you **Install Policy**.

  1. Double-click your gateway.

     The **Check Point Security Gateway** window shows.

  2. From **General Properties > Other > Connection Persistence > Keep all connections > OK**.

     Note - Rematch connections is selected by default.

Note - The old policy rules are still intact for calls already in-progress and they will not be dropped.

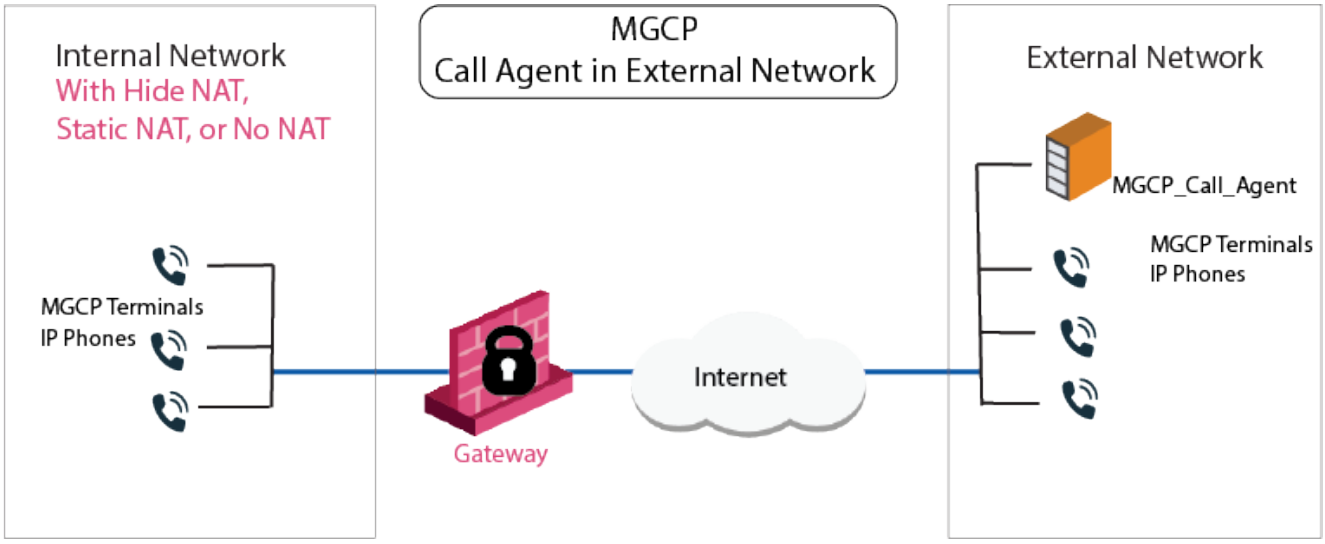
MGCP Rules for a Call Agent in the External Network

An MGCP topology with a Call Agent in the external network is shown in the image. You can configure Hide or Static NAT for the phones in the internal network.

In this image, the IP phones use a Call Agent on the external side of the gateway. This topology enables the a Call Agent that is maintained by another organization. It is possible to configure Hide NAT, Static NAT or no-NAT for the phones on the internal side of the gateway.

This procedure shows how to:

- Allow bidirectional calls between the MGCP phones in the internal network (Net_A) and phones in an external network (Net_B)
- Configure NAT for the internal phones



VoIP rule for this scenario:

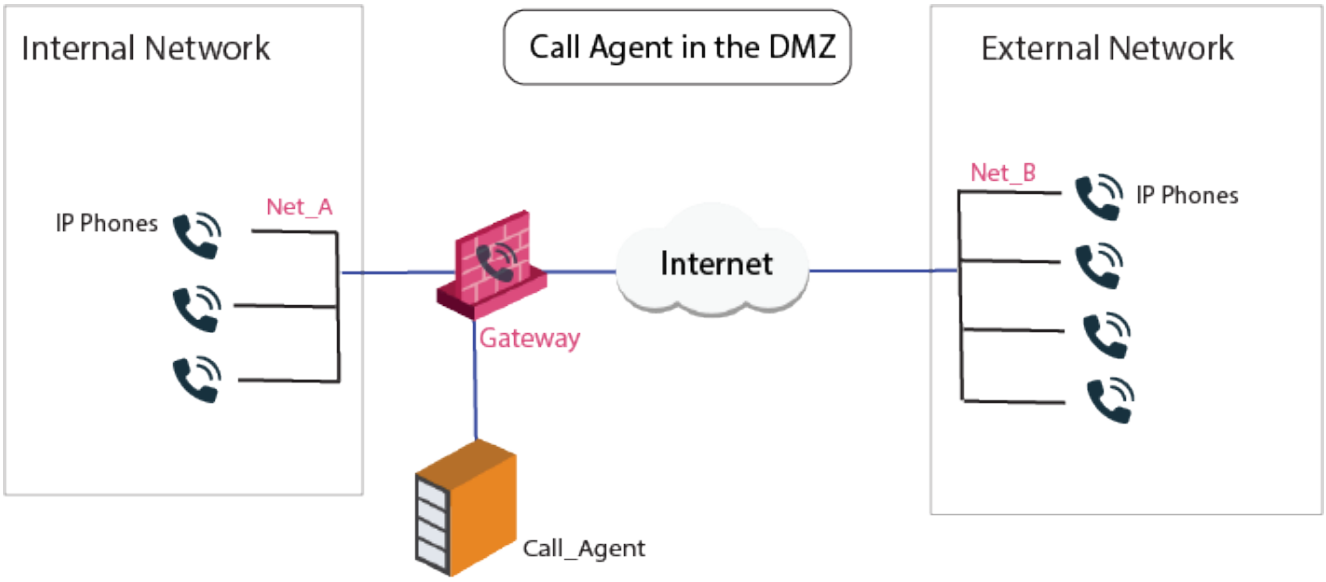
Source	Destination	Services & Applications	Action
MGCP_Call_Agent Net_A	Net_A MGCP_Call_Agent	mgcp_CA or mgcp_MG or mgcp_dynamic_ports	Accept

1. Configure the Network Objects (nodes or networks) for IP phones managed by the MGCP Call Agent and their calls, subject to gateway inspection.

   For the example in the image, these are Net_A and Net_B.
2. Configure the Network Object for the Call Agent (MGCP_Call_Agent).
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object. See Setting up your network for Network Address Translation.
5. **Install Policy**.

Sample MGCP Rules for a Call Agent in DMZ

In this image, the same Call Agent controls both endpoint domains. This topology makes it possible to provide Call Agent services to other organizations.



VoIP rule for this scenario:

Source	Destination	Services & Applications	Action	Comments
Net_A Net_B Call_Agent	Net_A Net_B Call_Agent	mgcp_CA or mgcp-MG	Accept	Bidirectional calls

To enable bidirectional calls between phones in internal and external networks (Net_A and Net_B):

1. Configure the Network Objects (nodes or networks) for the phones that are permitted to make calls and their calls subject to gateway inspection. In the image, these are Net_A and Net_B.
2. Configure the Network Object for the Call Agent (Call_Agent).
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

Sample MGCP Rules for a Call Agent to Call Agent

In this image, each Call Agent controls a separate endpoint domain. When there are one or more Call Agents, the signaling passes through each Call Agent. Whene the call has been set up, the media passes endpoint to endpoint. Here, a Call Agent-to-Call Agent topology shows Call Agents on opposite sides of the gateway.

VoIP rule for this scenario:

Source	Destination	Services & Applications	Action	Comments
Call_Agent_Int Call_Agent_Ext	Call_Agent_Ext Call_Agent_Int	mgcp_CA or mgcp-MG	Accept	Bidirectional calls

To enable bidirectional calls between phones in internal and external networks:

1. Configure the Network Object for the Proxy objects (Call_Agent_Int and Call_Agent_Ext).
2. Configure the VoIP rule.
3. To Configure Hide NAT or Static NAT for the phones in the internal network, edit the Network Object for Net_A.
   - Select the Network Object and double-click.
   - The **Network** window opens.
   - In the **NAT** tab, select **Add Automatic Address Translation Rules**, and then the **Translation method**, **Hide**, or **Static**.
   - Install the security policy.

H.323-Based VoIP

Introduction to H.323

H.323 is an International Telecommunication Union (ITU) standard that specifies the components, protocols and procedures that provide multimedia communication services, real-time audio, video, and data communications over packet networks, including IP based networks.

H.323 registration and alternate communication occurs on UDP port 1719, and H.323 call signaling occurs on TCP port 1720. H.323 is a peer-to-peer protocol.

The Security Gateway supports these H.323 architectural elements:

- **IP phones**

  Devices that:

  - Handle signaling (H.323 commands)
  - Connect to an H.323 Gatekeeper

  IP phones are Configured in SmartConsole, usually as a network of IP phones. It is usually not necessary to Configure Network Objects for individual IP Phones.

- **Standard telephones**

  Connect to an H.323 gateway. These are not IP devices. It is not necessary to Configure them in SmartConsole.

- **Gatekeeper**

  Manages a collection of H.323 devices, such as phones. A Gatekeeper converts phone numbers to IP addresses and can provide gateway services as well.

- **Gateway**

  Provides interoperability between different networks. The gateway translates between the telephony protocol and IP.

H.323 Specific Services

These preconfigured H.323 services are available:

Service	Purpose
TCP:H323	Allows a Q.931 to be opened (and if needed, dynamically opens an H.245 port), and dynamically opens ports for RTP/RTCP or T.120.
UDP:H323_ras	Allows a RAS port to be opened, and then dynamically opens a Q.931 port (an H.245 port if needed). Also dynamically opens and RTP/RTCP and T.120 ports.

Service	Purpose
UDP:H323_ras_only	Allows only RAS ports. Cannot be used to make calls. If this service is used, no *Application Intelligence Checks* (payload inspection or modification as NAT translation) are made. Do not use if you want to perform NAT on RAS messages. Do not use in the same rule as the `H323_ras` service.
TCP:H323_any	**Relevant only for versions prior to R75.40VS:** Similar to the H323 service, but also allows the **Destination** in the rule to be **ANY** rather than a Network Object. Only use `H323_any` if you do not know the VoIP topology, and are not enforcing media admission control (formerly known as Handover) using a VoIP domain. Do not use in the same rule as the `H.323` service.

Note - Make sure to use the `H.323` and `H.323_ras services`in H.323 Security Gateways rules.

Supported H.323 Deployments and NAT

For complete information on NAT configuration, see the *R80.40 Security Management Administration Guide*.

Supported H.323 deployments are listed the table. Hide NAT, or Static NAT can be configured for the phones in the internal network, and (where applicable) for the gatekeeper.

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Manual NAT rules are only supported in environments where the Gatekeeper is in the DMZ.

Supported H.323 Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Gatekeeper - Static NAT	Description
H.323 Endpoint to Endpoint	Yes	Static NAT only	N/A	• The IP Phones communicate directly, without a Gatekeeper or an H.323 gateway. Static NAT can be configured for the phones on the internal side of the gateway.

Supported H.323 Topology	Supports No NAT	Supports NAT for Internal Phones - Hide/Static NAT	Supports NAT for Gatekeeper - Static NAT	Description
H.323 Gatekeeper/Gateway in External Network	Yes	Yes	N/A	• The IP phones use the services of a Gatekeeper or H.323 gateway on the external side of the gateway. • This topology enables the use of the services of a Gatekeeper or an H.323 gateway that is maintained by another organization.
H.323 Gatekeeper/Gateway to Gatekeeper/Gateway	Yes	Yes	Yes	• Each Gatekeeper or H.323 gateway controls a separate endpoint domain. • Static NAT can be configured for the internal Gatekeeper. For the internal phones, Hide NAT or Static NAT can be configured.
H.323 Gatekeeper/Gateway in DMZ	Yes	Yes	Yes	• The same Gatekeeper or H.323 gateway controls both endpoint domains. This topology makes it possible to provide Gatekeeper or H.323 gateway services to other organizations. • Static NAT or No-NAT can be configured for the Gatekeeper or H.323 gateway. • Hide NAT or Static (or no NAT) can be configured for the phones on the internal side of the gateway.

Important Information about Creating H.323 Security Rules

Best practice - Configure anti-spoofing on the Check Point gateway interfaces.

- To allow H.323 traffic, create rules that let H.323 control signals through the gateway.

  It is not necessary to Configure a rule that specifies which port to open and which endpoint can talk. The gateway automatically gets this information from the signaling. For a given H.323 signaling rule (with RAS and/or H.323 services), the gateway automatically opens ports for the H.245 connections and RTP/RTCP media stream connections.

- Dynamic ports will only be opened if the port is not used by a different service. This prevents well-known ports from being used illegally.

  For example, if the **Connect** message identifies port 80 as the H.245 port, the port will not be opened.

- To allow H.323 traffic in the Security Rule Base, use regular Network Objects. It is not necessary to Configure special Network Objects.

- When you use Hide NAT for H.323, include the hidden IP address in the destination of the H.323 rule. When you include the hidden IP address, this allows the initiation of the TCP handshake from the external network to the hidden IP.

- Make sure to check **Keep all connections** or the firewall drops your connection every time you **Install Policy**.

  1. Double-click your gateway.

     The **Check Point Security Gateway** window shows.

  2. From **General Properties > Other > Connection Persistence > Keep all connections > OK**.

     Note - Rematch connections is selected by default.

Note - The old policy rules are still intact for calls already in-progress and they will not be dropped.

Sample H.323 Rules for an Endpoint-to-Endpoint Topology

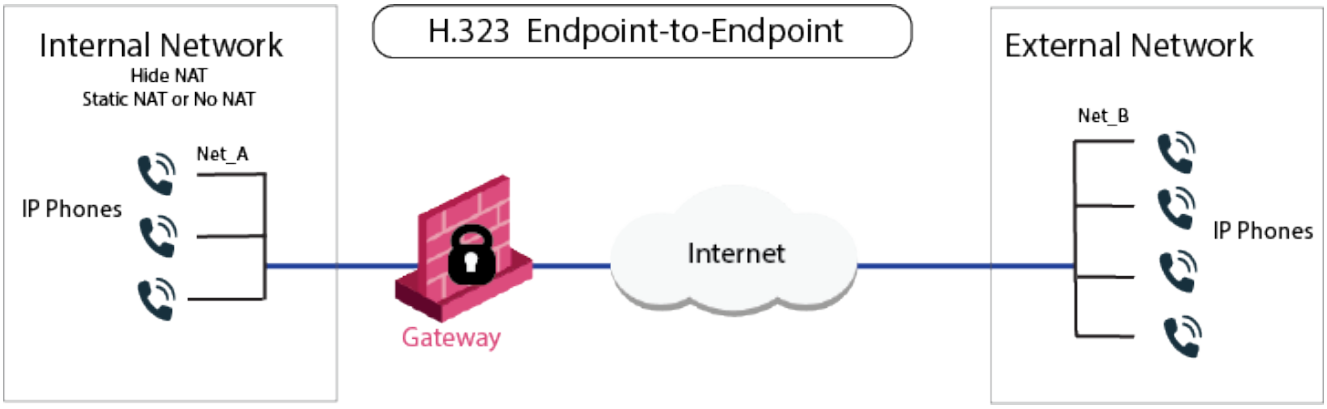
The IP Phones communicate directly, without a Gatekeeper or an H.323 gateway. Static NAT can be configured for the phones on the internal side of the gateway.

An endpoint-to-endpoint topology is shown in the image, with Net_A and Net_B on opposite sides of the gateway. This procedure explains:

- How to allow bidirectional calls between the phones in the internal network (Net_A) and phones in an external network (Net_B)

- How to Configure NAT for the internal phone

  No incoming calls can be made when Hide NAT is configured for the internal phones.



VoIP rule for this scenario:

Source	Destination	Services & Applications	Action
Net_A Net_B	Net_B Net_A	H323	Accept

To Configure an H.323 rule for endpoint-to-endpoint topology:

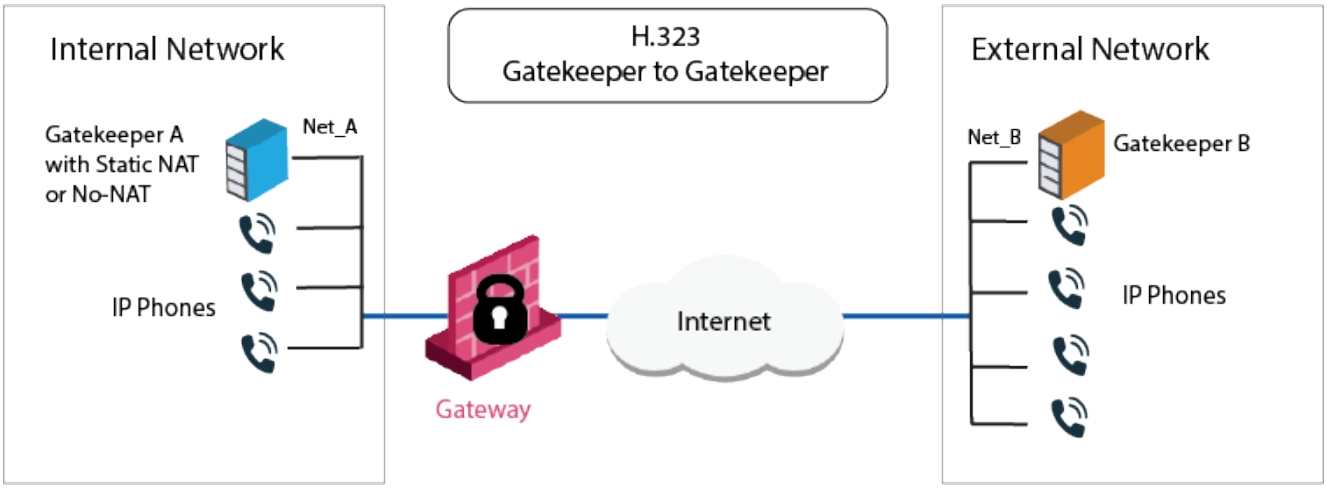
1. Configure an Access Control rule that allows IP phones in Net_A or Net_B to call each other.
2. Select the applicable service.
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network.
5. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
6. **Install Policy**.

Sample H.323 Rules for a Gatekeeper-to-Gatekeeper (or H.323 Gateway) Topology

Each Gatekeeper or H.323 gateway controls a separate endpoint domain. Static NAT can be configured for the Internal Gatekeeper. For the internal phones, Hide NAT or Static NAT can be configured.

The illustration shows a Gatekeeper-to-Gatekeeper or Gateway topology, with Net_A and Net_B on opposite sides of the gateway. This procedure shows you how to:

- Allow bidirectional calls between phones in the internal network (Net_A), and phones in an external network (Net_B)
- Define NAT for the internal phones and the internal gateway (GW_A) or Gatekeeper (GK_A).



VoIP Access Control rule for this scenario

Source	Destination	Service	Action	Comment
GK_A GK_B GW_A GW_B	GK_B GK_A GW_B GW_A	H323 H323_ras	Accept	Bidirectional calls

To define an H.323 rule for Gatekeeper-to-Gatekeeper topology:

1. Define an Access Control rule that allows IP phones in **Net_A** to call **Net_B** and the reverse.
2. Define the Network Objects for the gateway objects (GW_A and GW_B)

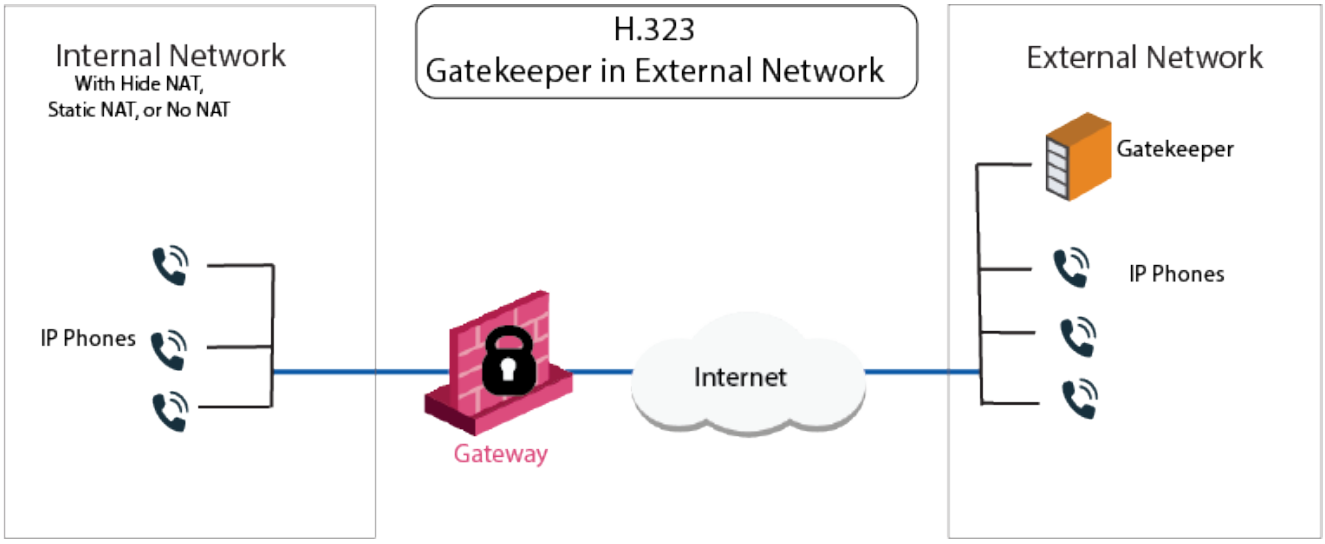
   OR
3. Define the Network Object for the Gatekeeper objects (GK_A and GK_B).
4. Define the VoIP rule.
5. Configure Static NAT for the Internal Gatekeeper.
6. Define Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
7. **Install Policy**.

Sample H.323 Rules for a Gatekeeper (or H.323 Gateway) in an External Network

The IP phones use the services of a Gatekeeper or H.323 gateway on the external side of the gateway. This topology enables the use of the services of a Gatekeeper or an H.323 gateway that is maintained by another organization. It is possible to configure Hide NAT or Static NAT (or No-NAT) for the phones on the internal side of the gateway.

The image shows an H.323 topology with a Gateway, with Net_A and Net_B on opposite sides of the gateway. This procedure shows you how to:

- Allow bidirectional calls between the phones in the internal network (Net_A) and phones in an external network (Net_B)
- Configure NAT for the internal phones



VoIP Access Control rule for this scenario:

Source	Destination	Services & Applications	Action	Comment
Net_A Net_B GK_B	GK_B Net_A	H323_ras H323	Accept	Bidirectional calls.

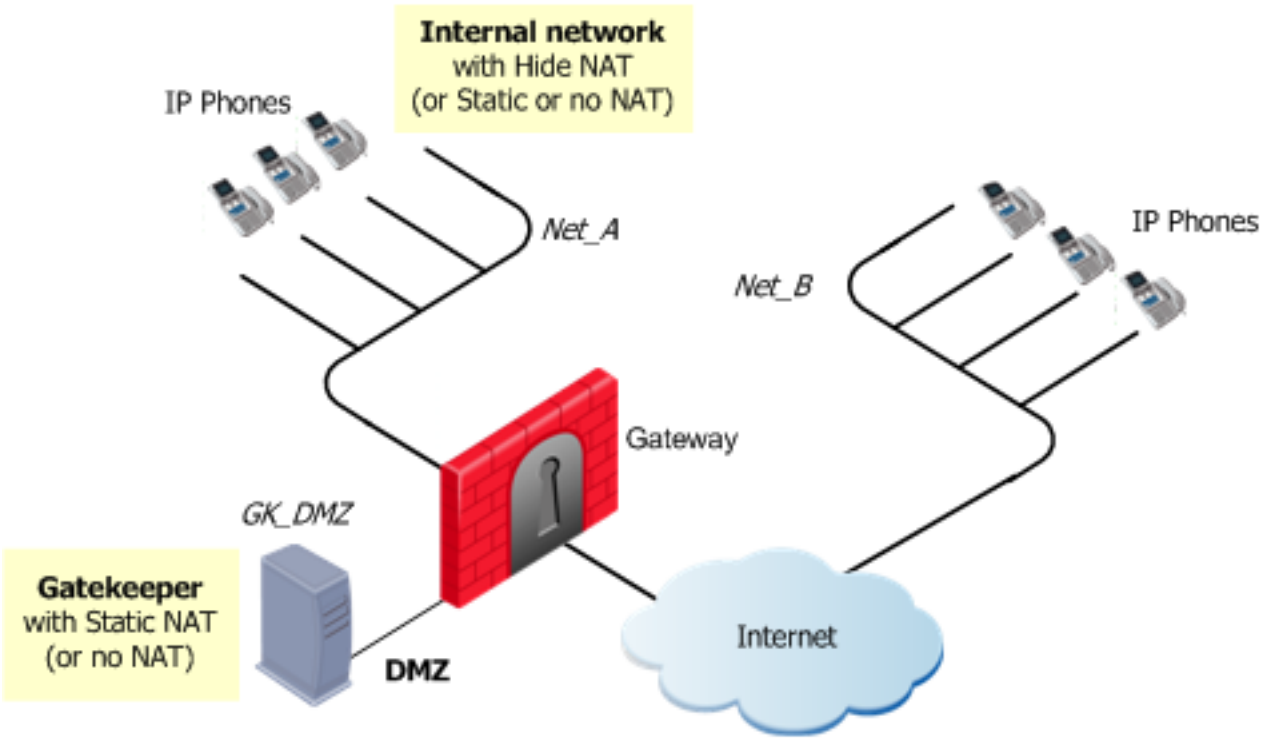
To configure an H.323 rule for a Gatekeeper in the external network:

1. Configure the Network Objects. In the image, these are **Net_A** and **Net_B**.
2. Configure the Network Object for the Gatekeeper (GK_B) or GW_B gateway.
3. Configure the VoIP rule.
4. Configure Hide NAT or Static NAT for the phones in the internal network. Do this by editing the Network Object for the internal network (**Net_A**). See Setting up your network for Network Address Translation.
5. **Install Policy**.

Defining H.323 Rules for a Gatekeeper in DMZ Topology

The image shows an H.323-based VoIP topology where a Gatekeeper is installed in the DMZ. This procedure explains how to:

- Allow bidirectional calls between the phones in the internal network (Net_A) and phones in an external network (Net_B)
- Define NAT for the internal phones and the Gatekeeper in the DMZ (GK_DMZ)



VoIP rule for this scenario:

Source	Destination	Services & Applications	Action	Comments
GK_DMZ Net_A Net_B	Net_A Net_B GK_DMZ	H323 H323_ras	Accept	Bidirectional calls.

Static NAT rules for the Gatekeeper in the DMZ:

Original			Translated			Comments
Source	Destination	Services & Applications	Source	Destination	Services & Applications	
GK_ DMZ	Net_B	*Any	GK_ DMZ: Static	=	=	Outgoing calls
Net_B	GK_DMZ_ NATed	*Any	=	GK_DMZ: Static	=	Incoming calls

To define an H.323 rule for a Gatekeeper in the DMZ:

1. Define the network objects (nodes or networks) for the phones that:
   - Use the Gatekeeper for registration
   - Are allowed to make calls, and their calls tracked by the gateway

In the image, these are Net_A and Net_B.

2. Define the network object for the Gatekeeper (GK_DMZ).
3. Configure the VoIP rule.

   To define Hide NAT or Static NAT for the phones in the internal network, edit the network object for Net_A.

   - Select **NAT** > **Advanced**.
   - Check the box **Add automatic address translation rules to hide this Gateway behind another Gateway**.
   - Select the **Translation method**, **Hide**, or **Static**.

     If you select **Hide NAT**:

     - Create a node object with the Hide NAT IP address
     - Select the **Security Policies tab**.
     - Add the service to the **Services & Applications** column.
     - Add the node object to the **Destination** of the rule.
4. Define **Static NAT** for the Gatekeeper in the DMZ:
   a. Create a Node object for the Static address of the Gatekeeper (for example: GK_DMZ_NATed).
   b. Define the manual Static NAT rules.
   c. Configure proxy-ARPs.

      You must associate the translated IP address with the MAC address of the gateway interface that is on the same network as the translated addresses. Use the `arp` command in UNIX or the `local.arp` file in Windows.

      The command `fw ctl arp` displays the ARP proxy table on gateways that run on Windows. On UNIX, use the `arp -a` command.
5. Make the time-out of the `H323_ras` service greater or equal to the Gatekeeper registration time-out.

   - In the**Manage & Settings** tab, go to **Blades** > **General**, select **Inspection Settings**.

     The **Inspection Settings** window opens.
   - From the **General tab**, in the search window, enter **H.323**.
   - The **H.323 - General Settings** window shows. Double-click the service. A window opens.
   - Configure the **Timeouts**
6. Click **OK**.
7. Install the Security Policy.

SCCP-Based VoIP

Introduction to SCCP Security and Connectivity

SCCP (Skinny Client Control Protocol) controls telephony gateways from external call control devices called Call Agents (also known as Media Gateway Controllers).

Connectivity and network level security for SCCP-based VoIP communication is supported. All SCCP traffic is inspected and legitimate traffic is allowed. Attacks are blocked. Other firewall gateway capabilities are supported, such as anti- spoofing and protection against denial of service attacks.

The validity of SCCP message states is verified for all SCCP messages. For a number of key messages, the existence and validity of the message parameters are also verified.

SCCP-Specific Services

These preconfigured SCCP services are available:

Service	Port	Protocol Type	
`SCCP`	2000	`SCCP_TCP`	Used for SCCP over TCP.
`high_udp_for_secure_SCCP`	N/A	N/A	Secure SCCP - Media to or from, on IP Protocol 17, ports above 1024. **Note** - Supported only on Security Management Servers and Security Gateways that run R75.40 and above.

SCCP Supported Deployments

NAT on SCCP devices is not supported.

The Security Gateway supports SCCP deployments listed in the table.

Supported SCCP Topology	Description
Call Manager in the Internal Network	The IP phones use the services of a Call Manager in an internal network.
Call Manager in the External Network	The IP phones use the services of a Call Manager on the external side of the gateway. This topology enables the use of the services of a Call Manager that is maintained by another organization.
Call Manager in the DMZ	The same Call Manager controls both endpoint domains. This topology makes it possible to provide Call Manager services to other organizations.

Important Information about Creating SCCP Security Rules

You can configure security rules that allow SCCP calls through the gateway. After the Rule Base is configured, all SCCP communication is fully secured by Inspection Settings.

Best practice - Configure anti-spoofing on the Check Point gateway interfaces. SCCP has a centralized call-control architecture.

- The Call Manager manages SCCP clients, VoIP endpoints, which can be IP phones or Cisco ATA analog phone adapters. The Call Manager controls all the features of the endpoints. The Call Manager requests data (such as station capabilities) and sends data (such as the button template and the date/time) to the VoIP endpoints.
- Configure the Call Managers in SmartConsole, as Host objects. Networks that contain directly-managed IP phones are also configured in SmartConsole. It is not usually necessary to configure Network Objects for individual phones. Cisco ATA devices that are managed by a Call Manager must be configured in SmartConsole, but the connected analog phones are not configured.
- To allow VoIP calls, you must create rules that let VoIP control signals pass through the gateway. It is not necessary to configure a media rule that specifies which ports to open and which endpoints can talk. The gateway gets this information from the signaling. For a given VoIP signaling rule, the gateway automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.
- Make sure to check **Keep all connections** or the firewall drops your connection every time you **Install Policy**.

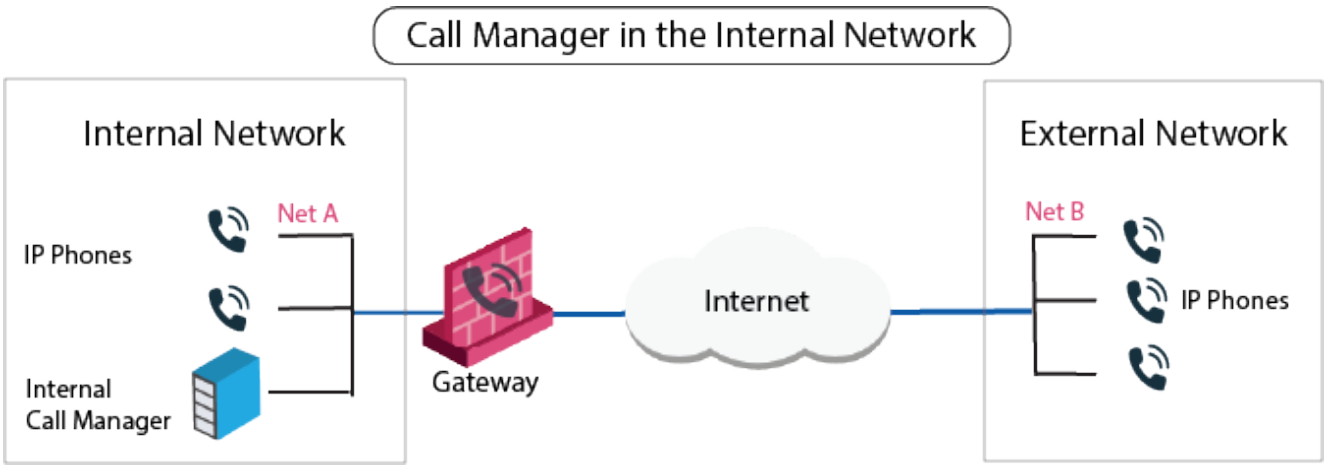
  1. Double-click your gateway.

     The **Check Point Security Gateway** window shows.

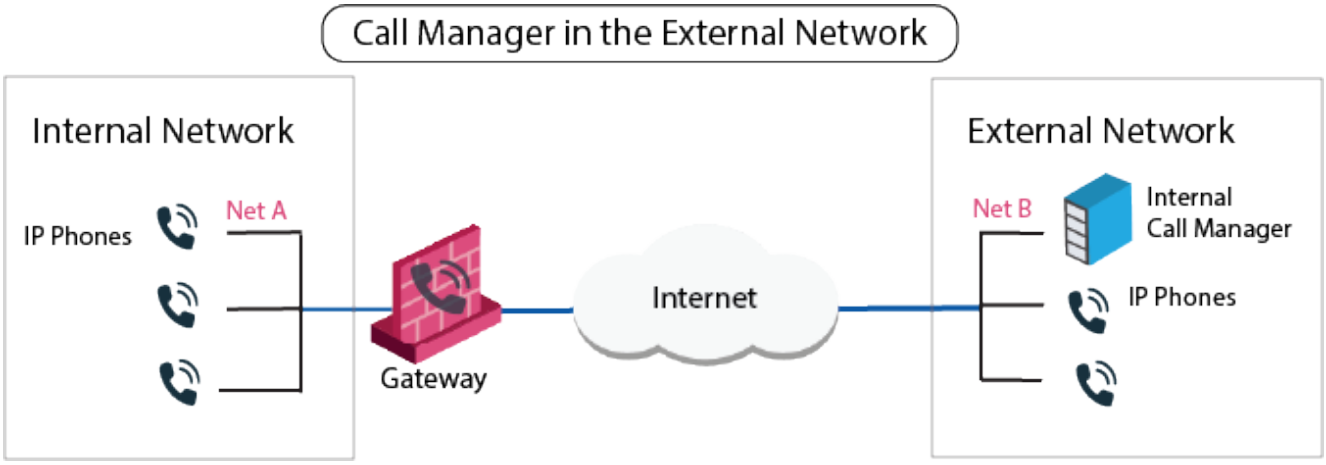
  2. From **General Properties > Other > Connection Persistence > Keep all connections > OK**.

     Note - Rematch connections is selected by default.

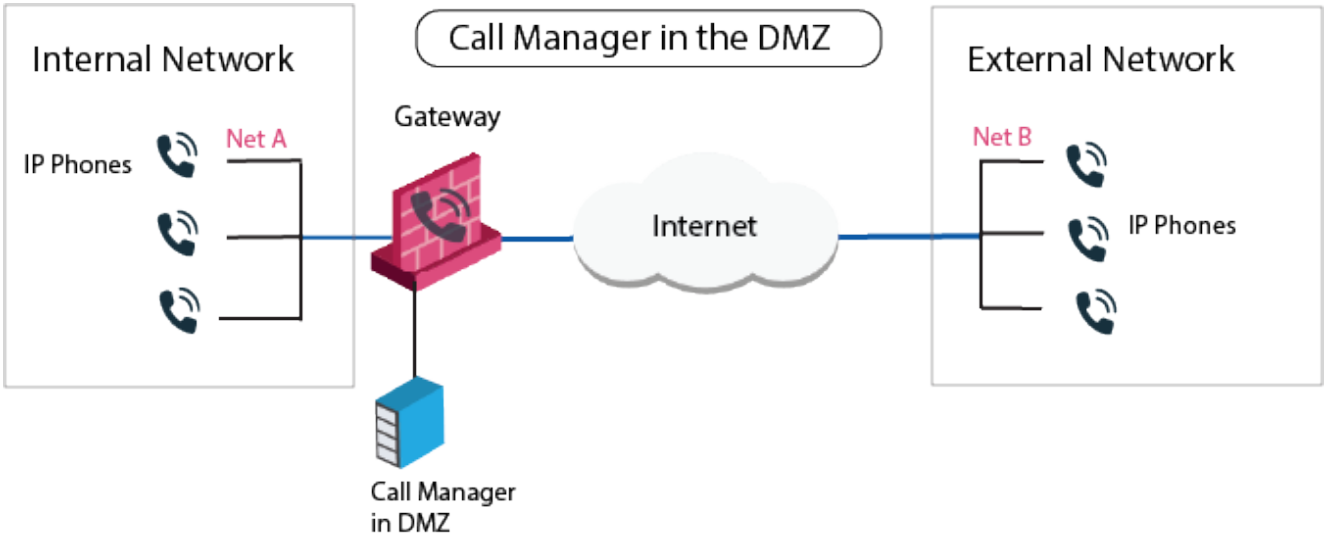
Sample SCCP Rules for Call Manager in Internal Network



Sample SCCP Rules for Call Manager in External Network



Sample SCCP Rules for Call Manager in the DMZ



Securing Encrypted SCCP

To secure encrypted SCCP, use these services in the Security Rule Base:

To create the rule TCP: Secure_SCCP:

1. Open **Manage > Services > New > TCP**.
2. The **Advanced TCP Service Properties** window opens.
3. Set the **Name** to: **Secure_SCCP**.
4. Set the port to: 2443.
5. Click **Advanced**.
6. The **Advanced TCP Service Properties** window opens.
7. Set the **Protocol Type** to: **Secure_SCCP_Proto**.
8. Other: `high_udp_for_secure_SCCP`

When an SCCP phone is turned on and identified as Secure SCCP, the phone's IP address is added to the database of secure SCCP phones.

When RTP traffic arrives at the gateway, it is allowed only if the source or destination is in the database of secure SCCP phones.

1. From SmartConsole, in the**Manage & Settings** tab, go to **Blades** > **General**, select **Inspection Settings**.

   The **Inspection Settings** window opens.

2. From the **General tab**, in the search window, enter **MGCP**.

   A list of **Settings** options shows.

3. Double-click the setting that you want to configure.

4. Make your changes and click **OK**.

Configuring VoIP for Check Point Security Gateways

Important Information about Configuring VoIP Security Rules

You can configure the Security Rule Base so that the gateway allows MGCP calls.

Best practice - Configure anti-spoofing on the Check Point gateway interfaces.

- For Automatic configuration for **Static NAT**, you must add a NATed object to the **Destination** column in the Rule Base.
- Make sure to check **Keep all connections** or the firewall drops your connection every time you **Install Policy**.

  1. Double-click your gateway.

     The **Check Point Security Gateway** window shows.

  2. From**General Properties > Other > Connection Persistence > Keep all connections > OK**.

     Note - Rematch connections is selected by default.

Note - The old policy rules are still intact for calls already in-progress and they will not be dropped.

Configuring Check Point Security Gateways in SmartConsole

Use SmartConsole to configure these areas of your gateway:

- Security Rules
- NAT
- Inspection Settings
- Ports

Setting Up Your Network with Network Address Translation (NAT)

You can configure these types of NAT rules for your Security Gateway:

- Hide NA

  Use Hide NAT to translate one or multiple IP addresses to an IP address of a specific object (for example, a Security Gateway), or to a specific IP address. The Security Gateway allows bi-directional connections to establish calls for the VoIP topology. The Security Gateway blocks connections for non-VoIP topologies.

- Static NA

  Use Static NAT to translate one IP address to a specific IP address. Each IP address on one network is translated to a different IP address on another network. Security Gateway allows connections to and from the computers, for which you configure the Static NAT.

- No-NA

  Use No-NAT to cancel the existing NAT rules.

  Example: You have an internal network of computers behind a Security Gateway. To represent the entire internal network, you create a Network Object and configure it to be NATed. An automatic NAT rule shows in Security Policies > Access Control > NAT. Now, you want to exclude one specific computer from this automatic NAT rule.

  To do this, you have to create a Host object and configure a Manual NAT rule that translates only this Host object to itself. You must place this Manual NAT rule above all Automatic NAT rules.

Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services
Host_ object	* Any	* Any	= Original	= Original	= Original

Configuring Inspection Settings in SmartConsole

There are many Inspection Settings profiles in SmartConsole that add means of protection to your gateway and protect against malicious attacks. You can configure the Inspection Settings to:

- Identify attack signatures
- Identify protocol anomalies
- Ensure RFC compliance
- Inspect signaling protocols, verify header formats, and protocol call flow state
- Establish granular VoIP security for maximum flexibility
- Generate detailed logs with packet captures on VoIP security events with Detect Mod

  SmartConsole allows you to configure rule exceptions. For example,if you add an exception that allows non-RFC compliant SIP traffic on a specified VoIP server, security is not compromised for all other VoIP traffic.

Inspection Settings can be configured for each profile and can prevent, detect, or be inactive.

To configure Inspection Settings for VoIP:

1. In the**Manage & Settings** tab, go to **Blades** > **General**, select **Inspection Settings**.

   The **Inspection Settings** window opens.
2. From the **General** page, in the search window, enter <*your_protocol*>.
3. Double-click the **Setting** you want to configure.
4. Double-click the applicable **Inspection Profile**.
5. On every page in this window, configure the applicable settings.
6. Click **OK** > **Close**.
7. Close the **Inspection Settings** window.
8. **Install Policy**.

Note for MGCP:

The Security Gateway has a number of Inspection Settings for MGCP. The inspection settings identify attack signatures and packets with protocol anomalies . Strict compliance is enforced with RFC-2705, RFC-3435 (version 1.0), and ITU TGCP specification J.171. Additionally, all inspection settings network security capabilities are supported, such as inspection of fragmented packets, anti-spoofing, and protection against Denial of Service (DoS) attacks.

Note for H.323:

- Inspection Settings does these application layer checks for H.323:
- Strict protocol enforcement, including the order and direction of packets
- Message length restrictions
- Stateful checks on RAS messages

Configuring VoIP Ports in SmartConsole

Use SmartConsole to configure VoIP phone and proxy ports. The gateway enforces security on that port. Each protocol uses port 5060 as a default port, but you can also configure new ports for your gateway.

To configure VoIP on a port:

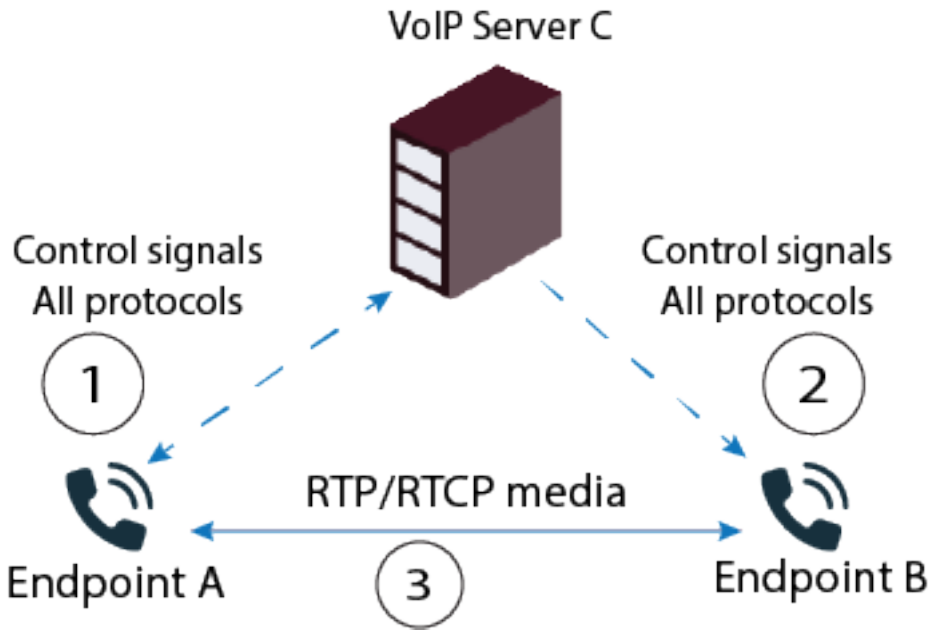
1. Open SmartConsole.
2. From the **Objects Explorer**, click **More object types** > **Service**.
3. Select <*your_protocol*>.

   The **New <*protocol*> Service** window shows.
4. In the **General** tab, enter an object name.
   a. In the **General** section > **Protocol**, select <*your_protocol*>
   b. In the **Match By** section, enter either the **Standard Port** or **Customize** your port..
5. Click **OK**.

VoIP Media Admission Control

Media admission control refers to how a VoIP Server lets one endpoint send media directly to a different endpoint. In earlier VoIP versions, Media Admission Control was known as *handover*.

To understand VoIP Media Admission Control, it is important to examine a typical flow for establishing a VoIP call.



Endpoint **A** initiates with endpoint **B**, using VoIP server **C**.

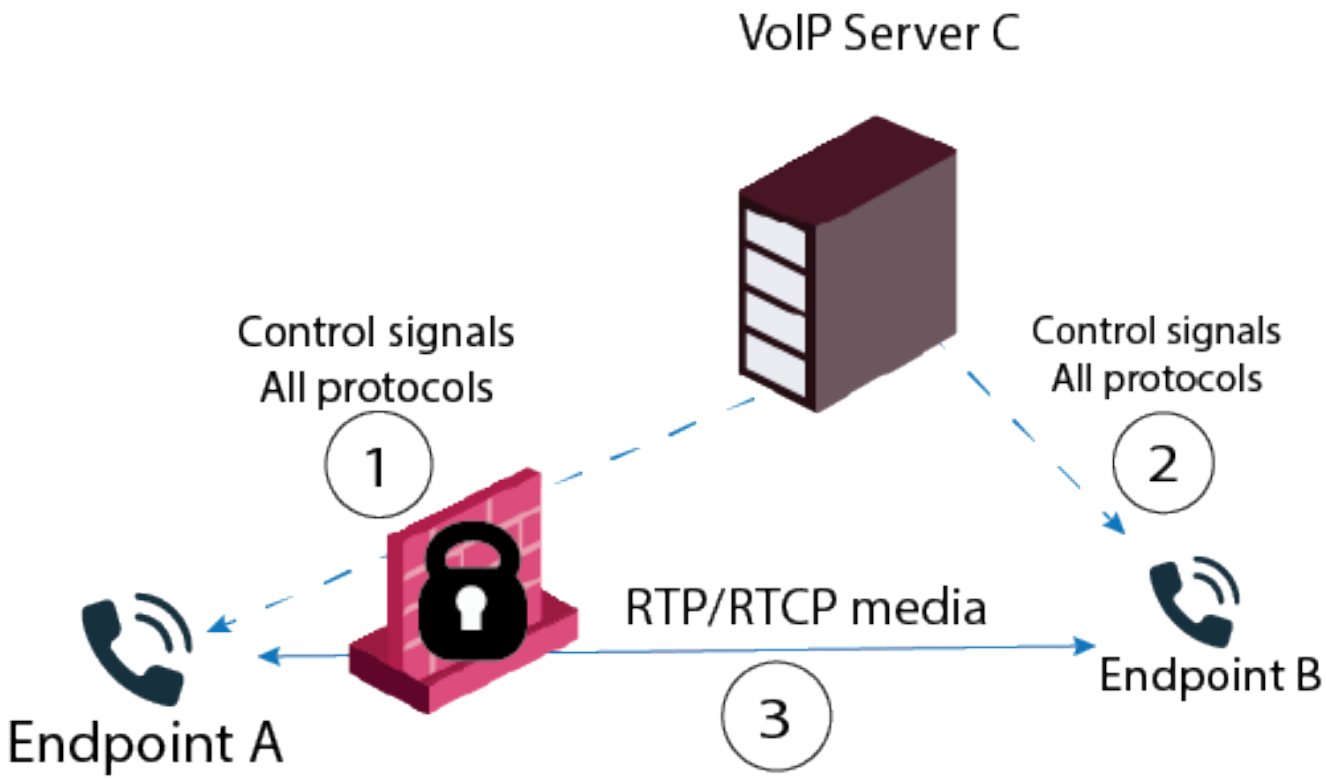
When Endpoint A wants to open a VoIP call with Endpoint B:

1. Endpoint A sends control signals to VoIP Server C. The signaling messages include details about the media capabilities of Endpoint A.
2. VoIP Server C sends control signals to Endpoint B.

   The signals are sent directly if it knows its physical location, (as shown in the diagram), or through a different VoIP Server.
3. If Endpoint B accepts the call, and the endpoints agree on the parameters of the media communication, the call is established.

Endpoints send the *control signals* to their designated VoIP Server, not to each other. The *media* (voice or video) can be sent through the endpoints designated VoIP servers or directly to each other. For the endpoints to send media directly to each other, each endpoint must first learn the physical location of the other endpoint. Physical location is contained in the control signals the endpoint receives from its designated VoIP Server.

Control signals must pass through the gateway. The gateway allows control signals through only if they are allowed by the Rule Base. According to the information the gateway derives from its inspection of allowed control signals, the gateway dynamically opens pinholes for media connections.



If no limitations are placed on VoIP Media Admission Control, attackers can craft control signals that:

- Open pinholes for unauthorized access
- Cause internal endpoints to send media to IP addresses of their choice
- Eavesdrop, modify, or disrupt communications

Media admission control protection is available for:

- SIP
- H.323
- SCCP
- MGCP

Media Admission Control is configured on each VoIP Server.

Configuring VoIP Media Admission Control

To configure VoIP Media Admission Control:

1. Create a Host object for the VoIP Server
2. Create a Host or a Network Object for VoIP endpoints.
3. Create a Group for VoIP endpoints:

   Network Objects > New > Groups > Simple Group.
4. Create a VoIP Domain:

   Network Objects > New > Others > VoIP Domains

a. Select one of the following:

- SIP Proxy
- H.323 Gatekeeper or gateway

Note - For H.323 Media admission control, you can configure a VoIP Domain H.323 gateway or a VoIP Domain H.323 Gatekeeper. There is no difference between the two types of domain. The routing mode tab on these domains can be safely ignored.

- MGCP Call Agent
- SCCP CallManager

b. In the **Related endpoints domain** section, select the group you created for the VoIP endpoints.

c. In the **VoIP Gateway installed at** section, select the VoIP Server Host you created.

5. In the Rule Base, add the VoIP Domain object to the **Source** and **Destination** columns of the VoIP rule.

Note - VoIP domains disable SecureXL templates. If you are using SecureXL, move rules with VoIP Domains in them to the end of the Rule Base. Enable the related Inspection Settings according to the VoIP protocol:

- **SIP > SIP Media Admission Control**
- **H.323 > H.323 Media Admission Control**
- **MGCP > MGCP Media Admission Control**
- **SCCP > SCCP Media Admission Control**

VoIP Logs and Queries in SmartConsole

Logs in SmartConsole

Logs show detailed, protocol-specific information for VoIP traffic. There are pre-configured VoIP log queries that supply enhanced troubleshooting capabilities.

To enable VoIP logging of VoIP calls:

1. From SmartConsole, in the **Security Policies** tab, select your rule.
2. From the **Track** column, select **Log**.

Note - If VoIP logging is disabled, only standard logging takes place. Standard logging includes the Source, Destination, and protocol information.

Logs are available for all protocols.

Queries from SmartConsole

To view preconfigured queries:

- From SmartConsole, in the **Logs & Monitor** tab, select **Queries**.
- In the **Predefined** list, the queries show.

You can also add queries to your **Favorite Queries** list.

To add queries to your Favorites list:

1. In the **Logs & Monitor** tab, select **Queries**.
2. Select the query that you want to add to your favorites list.

   That query shows in the window.
3. Select **Queries** > **Add to Favorites**.
4. Configure the fields in the **Add to Favorites** window that opens.
5. Select **Add**.

   Important - There are no logs available for RTP call sessions in SmartConsole, but you can find additional information from the gateway.

Predefined Query	Type	When Sent	Shows
Registration Session	Accept logs	After successful registration.	Registration IP address, phone number, port, and transport protocol (TCP/UDP). Registration period (seconds). IP address of the registrar server.
Other Session	Accept logs	After response to SIP requests. Such as: ■ Message or Update ■ Response to MGCP commands	Source IP address, port, and phone number. Destination IP address, port and phone number. SIP method or MGCP command type.
Security Events	Drop or Detect logs	Inspection Settings VoIP protection has detected a violation.	Source IP address, port and phone number. Destination IP address, port and phone number. Reason for log (*Attack* and *Attack Information* fields).
Call Session	Accept logs	After a call is established, and updated after the call is closed.	Source IP address, port and phone number. Destination IP address, port and phone number. State of call (open/closed), duration (seconds), direction (Inbound/Outbound), media. (If there are multiple media streams, shows data of the first one only.)
Policy Events	Drop or Detect logs	VoIP policy has detected a violation.	Source IP address, port and phone number. Destination IP address, port and phone number. Reason for log (*VoIP Reject Reason* and *VoIP Reject Reason Information* fields). Short configuration guidelines.

For complete information about logs and queries, see the *R80.40 Logging and Monitoring Administration Guide*.

Check Point Kernel Tables

For information on kernel tables for each protocol, see sk95369 > *Section (9) Relevant Check Point kernel tables.*

The Security Gateway stores SIP traffic data in these kernel table:

Kernel Table	Description
`sip_registration`	Holds one entry for each registered internal phone. An entry is entered when the registration is completed (200 OK). Timeout: The value from the expires header field, or default. To view a list of the online IP phones, run this command: `# fw tab -t sip_registration -f`

`sip_state`	Holds one entry for each SIP call (call-id + user tags). An entry is entered with the first packet of the call. Each SIP call has 2 - 4 SIP connections. Calls entries remain until the call is terminated.
	Timeout: 180 seconds, and it is refreshed as long as RTP is alive (for non-Int2Int calls).
	Note that the entries are per Call-ID. B2BUA may set 2 entries per call.
	To view information on current calls, run this command:
	`# fw tab -t sip_state -f`
	Output
	`Control connection (source, destination).`
	`RTP connection (endpoint IP addresses).`
	`Call state (established, ended, registration).`
	`Media type (audio, video, audio/video, application).`
	`Number of reinvites (number of participants in a conference call)`

`sip_cseq`	Holds one entry per transaction (SIP request + SIP response). An entry is entered with the SIP request. Timeout: 40 seconds. 20 seconds for retransmissions.
`sip_services`	Holds all the services that are defined as SIP in t0.he Rule Base.
`sip_dynamic_port`	Holds entries for SIP communication for non-5060 port traffic. Timeout: The value from the expires header field or default.
`fwx_sticky_port`	Holds port allocation entries only when you use NAT and sticky mechanism. Use this to translate the port consistently. Call entries remain until call is terminated.
`fwx_alloc`	Holds port allocation entries only when you use NAT. Same entries that are displayed in the `fwx_sticky_port` kernel table. Call entries remain until call is terminated.
`fwx_pending`	Used to store pending NAT instructions.

Kernel Table	Description
earlynat_sport	Holds five entries for each SIP UDP connection (1 entry and 1 link for each direction of the connection and 1 link for Bi-Directional SIP).

The Security Gateway stores H.323 traffic data in these kernel table:

	Description
h323_registration	Holds one entry for each registered internal phone.
fwx_sticky_port	Holds port allocation entries only when using NAT and sticky mechanism. Use this to translate the port consistently. Call entries remain until call is terminated.

The Security Gateway stores MGCP traffic data in these kernel table:

	Description
mgcp_registration	Holds one entry for each registered internal phone.
mgcp_services	Holds all the services that are defined as SIP in the Rule Base.
mgcp_dynamic_port	Holds entries for MGCP communication for non-MGCP well-known ports - only if mgcp_dynamic_portservice is used.
mgcp_cmd	Holds all the MGCP commands that take place. In MGCP SD you can add new MGCP commands. Add new entries to this table.
mgcp_conn	Holds MGCP control connections, such as sip_state kernel table. Has an entry for each MGCP call. Call entries remain until call is terminated.
mgcp_tid	Every command or transaction has its own TID (Transaction ID). Every new TIF is added to this kernel table. There is verification that every request has a matched response.

Command Line Reference

See the *R80.40 CLI Reference Guide*.

Working with Kernel Parameters on Security Gateway

See the *R80.40 Next Generation Security Gateway Guide*.

Kernel Debug on Security Gateway

See the *R80.40 Next Generation Security Gateway Guide*.

Debugging Procedure for SIP Over TCP

For detailed information about the Kernel Debug, see the *R80.40 Next Generation Security Gateway Guide*.

The most important information here, are the debug modules and debug flags.

Step	Action	Description

1	Prepare the kernel debug options.	`# fw ctl debug 0`
		`# fw ctl debug -buf 8200`
		`# fw ctl debug -m fw + conn drop vm nat xlate xltrc mgcp sip`
		`# fw ctl debug -m CPAS all`
		Best practice:
		Enable the `ld` flag in the `fw` module. This does, however, cause *extremely high* CPU load.

2	Verify the kernel debug options.	`# fw ctl debug -m fw` `# fw ctl debug -m CPAS`
3	Start the kernel debug	`# fw ctl kdebug -T -f > /var/log/debug.txt`
4	Start the traffic capture in another shell.	`# fw monitor -e "host(X.X.X.X), accept;" -o /var/log/fw_mon.cap`
5	Replicate the issue.	
6	Stop the kernel debug.	Press **CTRL+C**. `# fw ctl debug 0`
7	Stop the traffic capture in another shell.	Press **CTRL+C**.
8	Collect the debug output files.	`/var/log/debug.txt` `/var/log/fw_mon.cap`

Debugging Procedure for H.323 Traffic

For detailed information about the Kernel Debug, see the *R80.40 Next Generation Security Gateway Guide*.

The most important information here, are the debug modules and debug flags.

Step	Action	Description

1	Prepare the kernel debug options.	`# fw ctl debug 0`
		`# fw ctl debug -buf 8200`
		`# fw ctl debug -m fw + conn drop vm nat xlate xltrc mgcp sip`
		`# fw ctl debug -m h323 all`
		`# fw ctl debug -m CPAS all`
		Best practice:
		Enable the `'ld'` flag in the `'fw'` module. This does, however, cause *extremely high* CPU load.

2	Verify the kernel debug options.	`# fw ctl debug -m fw`
		`# fw ctl debug -m h323`
		`# fw ctl debug -m CPAS`

3	Start the kernel debug.	`# fw ctl kdebug -T -f > /var/log/debug.txt`
4	Start the traffic capture in another shell.	`# fw monitor -e "host(X.X.X.X), accept;" -o /var/log/fw_mon.cap`
5	Replicate the issue.	
6	Stop the kernel debug.	Press **CTRL+C**. `# fw ctl debug 0`
7	Stop the traffic capture in another shell.	Press **CTRL+C**.
8	Collect the debug output files.	`/var/log/debug.txt` `/var/log/fw_mon.cap`

Debugging Procedure for SIP Over UDP

For detailed information about the Kernel Debug, see the *R80.40 Next Generation Security Gateway Guide*.

The most important information here, are the debug modules and debug flags.

Step	Action	Description

1	Prepare the kernel debug options.	`# fw ctl debug 0`
		`# fw ctl debug -buf 8200`
		`# fw ctl debug -m fw + conn drop vm nat xlate xltrc mgcp sip`
		Best practice:
		Enable the '`ld`' flag in the '`fw`' module. This does, however, cause *extremely high* CPU load.

2	Verify the kernel debug options.	`# fw ctl debug -m fw`
3	Start the kernel debug.	`# fw ctl kdebug -T -f > /var/log/debug.txt`
4	Start the traffic capture in another shell.	`# fw monitor -e "host(X.X.X.X), accept;" -o /var/log/fw_mon.cap`
5	Replicate the issue.	
6	Stop the kernel debug.	Press **CTRL+C**. `# fw ctl debug 0`
7	Stop the traffic capture in another shell.	Press **CTRL+C**.
8	Collect the debug output files.	`/var/log/debug.txt` `/var/log/fw_mon.cap`

Debugging Procedure for SCCP (Skinny) Traffic

For detailed information about the Kernel Debug, see the *R80.40 Next Generation Security Gateway Guide*.

The most important information here, are the debug modules and debug flags.

Step	Action	Description

1	Prepare the kernel debug options.	`# fw ctl debug 0`
		`# fw ctl debug -buf 8200`
		`# fw ctl debug -m fw + conn drop vm nat xlate xltrc`
		`# fw ctl debug -m CPAS all`
		Best practice:
		Enable the '`ld`' flag in the '`fw`' module. This does, however, cause *extremely high* CPU load.

2	Verify the kernel debug options.	`# fw ctl debug -m fw` `# fw ctl debug -m CPAS`
3	Start the kernel debug.	`# fw ctl kdebug -T -f > /var/log/debug.txt`
4	Start the traffic capture in another shell.	`# fw monitor -e "host(X.X.X.X), accept;" -o /var/log/fw_mon.cap`
5	Replicate the issue.	
6	Stop the kernel debug.	Press **CTRL+C**. `# fw ctl debug 0`
7	Stop the traffic capture in another shell.	Press **CTRL+C**.
8	Collect the debug output files.	`/var/log/debug.txt` `/var/log/fw_mon.cap`