RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.

Refer to the Third Party copyright notices (http://www.checkpoint.com/3rd_party_copyright.html) for a list of relevant copyrights and third-party licenses.
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.

Latest Documentation
The latest version of this document is at: (http://supportcontent.checkpoint.com/documentation_download?ID=24855)
To learn more, visit the Check Point Support Center (http://supportcenter.checkpoint.com).
For more about this release, see the R77 home page (http://supportcontent.checkpoint.com/solutions?id=sk101208).

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 August 2014</td>
<td>Corrected GUI path to enable IPS protections for VoIP SIP protocol in Important Guidelines for SIP Security Rule Configuration (on page 21)</td>
</tr>
<tr>
<td></td>
<td>Removed Secure_SCCP as a predefined service in SCCP-Specific services (on page 50)</td>
</tr>
<tr>
<td>26 June 2014</td>
<td>Cover changed to be relevant for all R77 versions.</td>
</tr>
<tr>
<td>01 January 2014</td>
<td>Added a security rule configuration guideline to prevent dropped calls during Policy Install. See:</td>
</tr>
<tr>
<td></td>
<td>Important Guidelines for SIP Security Rule Configuration (on page 21)</td>
</tr>
<tr>
<td></td>
<td>Rule Base Configuration for MGCP (on page 34)</td>
</tr>
<tr>
<td></td>
<td>General Guidelines for H.323 Security Rule Configuration (on page 39)</td>
</tr>
<tr>
<td></td>
<td>General Guidelines for SCCP Security Rule Configuration (on page 49)</td>
</tr>
<tr>
<td>27 August 2013</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

Feedback
Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on VoIP R77 Versions Administration Guide).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td><strong>Securing Voice Over IP</strong></td>
<td>6</td>
</tr>
<tr>
<td>Introduction to Check Point Secure VoIP</td>
<td>6</td>
</tr>
<tr>
<td>VoIP Security Deployments</td>
<td>6</td>
</tr>
<tr>
<td>Enterprise Deployment 1: Perimeter VoIP Gateway</td>
<td>6</td>
</tr>
<tr>
<td>Enterprise Deployment 2: LAN Segmentation</td>
<td>7</td>
</tr>
<tr>
<td>Service Provider Deployment</td>
<td>9</td>
</tr>
<tr>
<td>VoIP Protocols</td>
<td>9</td>
</tr>
<tr>
<td>Signaling and Media Protocols</td>
<td>10</td>
</tr>
<tr>
<td>Supported Standards and Protocols</td>
<td>10</td>
</tr>
<tr>
<td>SmartDashboard Toolbar</td>
<td>11</td>
</tr>
<tr>
<td><strong>Basic Configuration</strong></td>
<td>13</td>
</tr>
<tr>
<td>VoIP in SmartDashboard</td>
<td>13</td>
</tr>
<tr>
<td>Basic Configuration Workflow</td>
<td>14</td>
</tr>
<tr>
<td>Defining the SIP Server</td>
<td>14</td>
</tr>
<tr>
<td>Defining the SIP Endpoints</td>
<td>14</td>
</tr>
<tr>
<td>Defining the Security Rule</td>
<td>15</td>
</tr>
<tr>
<td>Testing the Configuration</td>
<td>15</td>
</tr>
<tr>
<td><strong>SIP Based VoIP</strong></td>
<td>17</td>
</tr>
<tr>
<td>Supported SIP Deployments and NAT Support</td>
<td>17</td>
</tr>
<tr>
<td>Additional Conditions for Using NAT in SIP Networks</td>
<td>18</td>
</tr>
<tr>
<td>Hide NAT for SIP Traffic</td>
<td>18</td>
</tr>
<tr>
<td>SIP-Specific services</td>
<td>20</td>
</tr>
<tr>
<td>Important Guidelines for SIP Security Rule Configuration</td>
<td>21</td>
</tr>
<tr>
<td>SIP Rules for a Peer-to-Peer No-Proxy Topology</td>
<td>22</td>
</tr>
<tr>
<td>SIP Rules for a Proxy in an External Network</td>
<td>23</td>
</tr>
<tr>
<td>SIP Rules for a Proxy-to-Proxy Topology</td>
<td>24</td>
</tr>
<tr>
<td>SIP Rules for a Proxy in DMZ Topology</td>
<td>25</td>
</tr>
<tr>
<td>Using SIP on a Non-Default Port</td>
<td>27</td>
</tr>
<tr>
<td>Enabling Dynamic Opening of Ports for SIP Signaling</td>
<td>27</td>
</tr>
<tr>
<td>Example Rule With the sip_dynamic_ports Service</td>
<td>28</td>
</tr>
<tr>
<td><strong>SIP Advanced Configuration</strong></td>
<td>29</td>
</tr>
<tr>
<td>Gateway Clustering Support for SIP</td>
<td>29</td>
</tr>
<tr>
<td>Synchronizing SIP Connections</td>
<td>29</td>
</tr>
<tr>
<td>Load Sharing of SIP Connections</td>
<td>29</td>
</tr>
<tr>
<td>Configuring SIP-T Support</td>
<td>29</td>
</tr>
<tr>
<td>Troubleshooting SIP</td>
<td>30</td>
</tr>
<tr>
<td><strong>MGCP-Based VoIP</strong></td>
<td>31</td>
</tr>
<tr>
<td>Introduction to MGCP</td>
<td>31</td>
</tr>
<tr>
<td>MGCP Supported Deployments and NAT Support</td>
<td>31</td>
</tr>
<tr>
<td>Additional Conditions for Using NAT in MGCP Networks</td>
<td>32</td>
</tr>
<tr>
<td>Hide NAT for MGCP traffic</td>
<td>33</td>
</tr>
<tr>
<td>Rule Base Configuration for MGCP</td>
<td>34</td>
</tr>
<tr>
<td>MGCP-Specific services</td>
<td>34</td>
</tr>
<tr>
<td>MGCP Rules for a Call Agent in the External Network</td>
<td>34</td>
</tr>
<tr>
<td>MGCP Rules for Call Agent in DMZ</td>
<td>35</td>
</tr>
<tr>
<td>MGCP Rules for Call Agent to Call Agent</td>
<td>36</td>
</tr>
<tr>
<td><strong>H.323-Based VoIP</strong></td>
<td>37</td>
</tr>
<tr>
<td>Introduction to H.323</td>
<td>37</td>
</tr>
<tr>
<td>Supported H.323 Deployments and NAT Support</td>
<td>37</td>
</tr>
<tr>
<td>H.323 Security Rule Base Configuration</td>
<td>39</td>
</tr>
<tr>
<td>H.323 Specific Services</td>
<td>39</td>
</tr>
</tbody>
</table>
Chapter 1

Securing Voice Over IP

In This Section:

- Introduction to Check Point Secure VoIP .......................................................... 6
- VoIP Security Deployments ................................................................................. 6
- VoIP Protocols ................................................................................................. 9
- SmartDashboard Toolbar .................................................................................... 11

Introduction to Check Point Secure VoIP

IPS adds more than 80 IPS protections and VoIP settings to protect against malicious attacks. IPS protects by:

- Identifying attack signatures
- Identifying packets with protocol anomalies
- Ensuring RFC compliance
- Inspecting signaling protocols, verifying header formats and protocol call flow state

As part of IPS, VoIP Protections can be:

- Enforced for different gateways using IPS profiles
- Monitored using Detect Mode

IPS also lets you:

- Generate detailed logs with packet captures on VoIP security events
- Configure granular VoIP security for maximum flexibility in deployment and enforcement.
- Add exceptions to specified VoIP protections.
  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.

The Security Gateway interoperates with VoIP devices from many leading vendors and supports the SIP, H.323, MGCP and SCCP (Skinny) protocols.

VoIP Security Deployments

This section covers different deployments for enterprises, managed service providers, and telecom network providers.

**Enterprise Deployment 1: 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 branch offices. Security capabilities for VoIP include:

- Protecting servers and PBXs in the enterprise LAN against Denial of Service attacks.
- Preventing unauthorized phone calls by means of Media admission control. These checks let only defined servers set up calls for the phones.

**Enterprise Deployment 2: 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 availability of VoIP equipment such as servers and PBXs in the enterprise LAN.
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.

VoIP Protocols
The Security Gateway secures VoIP traffic in H.323, SIP, MGCP, 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 H.323, SIP, MGCP, and SCCP protocols makes sure that:

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

**Signaling and Media Protocols**

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 of a call then use control signals to negotiate dynamically assigned ports that each side opens to receive the RTP/RTCP media stream.

**Supported Standards and Protocols**

This section covers supported VoIP standards and protocols.

**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.
R77 also supports H.245 tunneling and Fast Connect, a 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

SmartDashboard Toolbar
You can use the SmartDashboard toolbar to do these actions:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🌐</td>
<td>Open the SmartDashboard menu. When instructed to select menu options, click this button to show the menu. For example, if you are instructed to select Manage &gt; Users and Administrators, click this button to open the Manage menu and then select the Users and Administrators option.</td>
</tr>
<tr>
<td>📝</td>
<td>Save current policy and all system objects.</td>
</tr>
<tr>
<td>🗂️</td>
<td>Open a policy package, which is a collection of Policies saved together with the same name.</td>
</tr>
<tr>
<td>⌚️</td>
<td>Refresh policy from the Security Management Server.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Open the Database Revision Control window.</td>
</tr>
<tr>
<td></td>
<td>Change global properties.</td>
</tr>
<tr>
<td></td>
<td>Verify Rule Base consistency.</td>
</tr>
<tr>
<td>![Install Policy]</td>
<td>Install the policy on Security Gateways or VSX Gateways.</td>
</tr>
<tr>
<td>![SmartConsole]</td>
<td>Open SmartConsole.</td>
</tr>
</tbody>
</table>
VoIP in SmartDashboard

VoIP in SmartDashboard is configured in two places:

- **On the Firewall tab**
  Use the Firewall tab to configure:
  - Security rules for VoIP traffic
  - Host and Network objects for VoIP Endpoints and Servers
  - NAT on VoIP Endpoint and Server objects

- **On the IPS tab**
  Use the IPS tab to:
  - Configure VoIP Engine settings for each protocol (SIP, H.323, MGCP and SCCP)
  - Apply VoIP IPS protections
  
  IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP
Basic Configuration Workflow

This section describes the workflow for a basic SIP configuration.

We assume:
- You have installed a Security Gateway and Security Management Server.
- The VoIP phones in the external networks are:
  - Not behind a NAT device or
  - Behind a NAT device that is VoIP-aware

To configure VoIP:
1. Log in to SmartDashboard.
2. Define the Security Gateway.
3. Define the VoIP server.
4. Define the VoIP endpoints.
5. Define a VoIP security rule.
6. Install the Security Policy.
7. Test the configuration.

Defining the SIP Server

To define a SIP server (also known as a SIP Proxy or a Registrar) use the regular Host object in:

SmartDashboard > Network Objects > New > Check Point > Host...

For example, name the host: sip_server_host.

Defining the SIP Endpoints

Define the internal VoIP phones (endpoints) by:
- Defining networks or host objects or
- A group of hosts and network objects

For example, a group of internal networks might be named: internal_net.
Defining the Security Rule

Configure a simple security rule that allows traffic between endpoints on the internal network and the SIP server in the external network.

1. Click the **Security** tab.
2. Add this rule and install the policy:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal-net</td>
<td>sip_server_host</td>
<td>sip</td>
<td>Accept</td>
</tr>
<tr>
<td>sip_server_host</td>
<td>internal-net</td>
<td>sip_dynamic_ports</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>sip-tcp</td>
<td></td>
</tr>
</tbody>
</table>

Testing the Configuration

Test the configuration by making phone calls from an:
- Internal phone to an internal phone.
- Internal phone to an external phone.
- External phone to an internal phone.

After making each call, see the resulting logs in SmartView Tracker.

**To see the VoIP logs:**
1. From the SmartDashboard **File** menu, select **Window > SmartView Tracker**. SmartView Tracker opens.
2. Under the **Predefined** queries, select the **Firewall Blade > Voice over IP > Call Session** filter.
3. Examine the resulting logs.

Typical Call Session VoIP log
The Figure shows a typical Call Session VoIP log for a successful call from an internal phone to an external one.

- See the **Call Direction** field in the **Record Details** window of the log. The call is from **Source IP-phone 6666** to **Destination IP-phone 4444**.
- The **Source IP-phone** and **Destination IP-phone** fields show the phone extension (the user).
- The **Source** and **Destination** fields show the connection through the gateway. For example, if the internal phone makes a connection to the SIP Server:
  - The **Source** field shows the **internal_phone_host node**
  - The **Destination** field shows the **sip_server_host node**
Chapter 3

SIP Based VoIP

In This Section:

- Supported SIP Deployments and NAT Support
- SIP-Specific services
- Important Guidelines for SIP Security Rule Configuration
- SIP Rules for a Peer-to-Peer No-Proxy Topology
- SIP Rules for a Proxy in an External Network
- SIP Rules for a Proxy-to-Proxy Topology
- SIP Rules for a Proxy in DMZ Topology
- Using SIP on a Non-Default Port
- Enabling Dynamic Opening of Ports for SIP Signaling

Supported SIP Deployments and NAT Support

The table shows a list of supported SIP deployments. NAT (Hide or Static) can be configured for:

- Phones on the internal network
- The proxy in the internal network

<table>
<thead>
<tr>
<th>SIP Endpoint-to-Endpoint Topology</th>
<th>No NAT</th>
<th>NAT for Internal Phones — Hide/Static NAT</th>
<th>NAT for Proxy — Static NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint to Endpoint</td>
<td>Yes</td>
<td>Static NAT only</td>
<td>Not applicable</td>
</tr>
<tr>
<td>SIP Proxy in External</td>
<td>Yes</td>
<td>Yes</td>
<td>Not applicable</td>
</tr>
<tr>
<td>SIP Proxy to Proxy</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SIP Proxy in DMZ</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The Proxy refers to a SIP proxy and/or registrar. If there is more than one proxy device, signaling passes through one or more Proxies or Registrars. After the call has been set up, the media passes from endpoint to endpoint, directly or through one or more Proxies.

The IP 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

The IP Phones use the services of a Proxy on the external side of the gateway. This topology enables using the services of a Proxy 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.

SIP Proxy to SIP Proxy

Each Proxy controls a separate endpoint domain. Static NAT can be configured for the internal Proxy. For the internal phones, Hide NAT (or Static NAT) can be configured.

SIP Proxy in DMZ

The same Proxy controls both endpoint domains. This topology makes it possible to provide Proxy services to other organizations. Static NAT (or no NAT) can be configured for the Proxy. Hide NAT (or Static or no NAT) can be configured for the phones on the internal side of the gateway.

Additional Conditions for Using NAT in SIP Networks

You can use SIP with Network Address Translation with these exceptions:

- NAT is not supported on IP addresses behind an external Check Point gateway interface.
- Manual NAT rules are only supported for proxy in DMZ deployments. (Use Automatic NAT as an alternative.)
- Calls cannot be made from an external source to two endpoints on the trusted side of a gateway if one of the endpoints is NATed and the other is not.

Hide NAT for SIP Traffic

In IPS > Protections > By Type > Engine Settings > SIP - General Settings, enabling the Hide NAT changes source port for SIP over UDP option configures the gateway to do Hide NAT on the:

- IP address of the SIP endpoint phones
- Source port of the SIP endpoint phones

For SIP over TCP, the source port is always translated if there is Hide NAT. With this option disabled, the gateway performs Hide NAT only on the IP address of the SIP endpoint phones.

This option must be enabled in environments where:

- (On the NAT tab of the related Network Object: node or network) the gateway is configured to do Hide NAT on the internal IP addresses of the endpoints and:
- The SIP server can register only one endpoint with a given IP address and port combination. (As with the Cisco Unified Communications Manager).
Note - For all internal phones to be registered successfully on the server, the source port of the REGISTER message sent by the phone must be the same as the port in the Contact header of the REGISTER message. In Cisco IP Phones, for example, this is done by selecting the "NAT Enabled" option.

This section covers changes in SIP packets if the Hide NAT changes source port for SIP over UDP option is selected.

SIP Packet Before NAT

The packet capture shown here shows a SIP packet from a phone with IP address 192.168.3.40, and source port 5060 (the default SIP port). The phone's extension is 4321.

Packet after Hide NAT when option is disabled

The packet capture shown here shows the SIP packet after Hide NAT, with the Hide NAT changes source port for SIP over UDP option disabled. The IP address is translated to the Hide NAT address of 172.16.8.232, but the source port 5060 is unchanged.

Here, all the internal phones are registered with the same Source IP: port combination, for example: sip:4321@172.16.8.232:5060. A different phone with extension 8765 would register as sip:8765@172.16.8.232:5060.

Some SIP servers can register a phone 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.
Packet after Hide NAT when option is enabled

This packet capture shows the SIP packet after Hide NAT, with the Hide NAT changes source port for SIP over UDP option enabled. The IP address is translated to the Hide NAT address of 172.16.8.232, and the source port is also translated to an allocated port of 10015.

Here, a different port is allocated for each internal phone. Each phone is registered with a different Source IP: port combination. For example: one phone is registered as sip:4321@172.16.8.232:10015 (as shown in the packet capture). A different phone with extension 8765 is registered as (for example) sip:8765@172.16.8.232:10016.

As a result, all of the internal phones are registered successfully on the server.

SIP-Specific services

These predefined SIP services are available:

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP:sip</td>
<td>Used for SIP over UDP.</td>
</tr>
<tr>
<td>TCP:sip-tcp</td>
<td>Used for SIP over TCP.</td>
</tr>
<tr>
<td>Other: sip_dynamic_ports</td>
<td>Enables the dynamic opening of ports for SIP signaling.</td>
</tr>
<tr>
<td>TCP:sip_tls_authentication</td>
<td>Used for unencrypted SIP over TLS (that is, authenticated only). NAT is not supported for connections of this type.</td>
</tr>
<tr>
<td>TCP:sip_tls_not_inspected</td>
<td>Insecure way of allowing SIP over TLS to pass without inspection.</td>
</tr>
</tbody>
</table>

These legacy SIP services are available for gateways of version R75.40 and below:

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP:sip_any</td>
<td>Used for gateways of version R75.40 and below, if not enforcing handover.</td>
</tr>
<tr>
<td>TCP:sip-tcp_any</td>
<td>Do not use for R77.</td>
</tr>
<tr>
<td></td>
<td>Do not place a VoIP domain in the source or destination of the rule. Instead, use *Any or a network object, together with one of these services. If a VoIP domain is used with these services, it is equivalent to the sip service.</td>
</tr>
<tr>
<td></td>
<td>For VoIP equipment that uses SIP TCP, use the sip-tcp_any service. When it uses SIP UDP, use the sip_any service.</td>
</tr>
</tbody>
</table>

For details on how to use these services, see the Securing Voice Over IP (VoIP) chapter of the R75.40 Firewall Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=13088).
**Note -**

- The services `sip` and `sip_any` cannot be used in the same rule. The services conflict with each other.
- The services `sip-tcp` and `sip-tcp_any` also conflict and cannot be used in the same rule.

**Legacy Solution for SIP TLS Support**

If using the `TCP:sip_tls_authentication` service is not possible (for example if connections are encrypted by TLS, or NAT must be done on the connections) add these two rules instead:

- A rule that uses the `udp-high-ports` service to open all high UDP ports for the entities sending data, and
- A rule that uses the `sip_tls_not_inspected` service to open TCP port 5061 for the entities sending signaling

**Important -** Opening all high UDP ports is very insecure. SIP signaling and data is not inspected.

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

1. Define Network objects in SmartDashboard for the SIP phones.
2. Define a Network object for the SIP proxy.
3. Configure a rule that opens all high UDP ports and TCP port 5061.

A typical rule that assumes the phones send data directly to each other, and not through the proxy, looks like this:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP Proxy</td>
<td>SIP Phones</td>
<td>TCP: sip_tls_not_inspected</td>
</tr>
<tr>
<td>SIP Phones</td>
<td>SIP Proxy</td>
<td></td>
</tr>
<tr>
<td>SIP Phones</td>
<td>SIP Phones</td>
<td>UDP: udp-high-ports</td>
</tr>
</tbody>
</table>

**Important Guidelines for SIP Security Rule Configuration**

- Anti-spoofing must be configured on the Check Point gateway interfaces. SIP entities on which NAT is configured must reside behind the gateway's internal interfaces.

- Do not define special Network objects to allow SIP signaling. Use regular Network objects. The firewall dynamically opens pinholes for data connections (RTP/RTCP and other). The R77 security gateway supports up to four different media channels per SIP SDP message.

- When using Hide NAT for SIP over UDP, do not include the hiding IP in the destination of the SIP rule.

- When using Hide NAT for SIP over TCP, you must include the hiding IP in the destination of the SIP rule. Doing this allows the initiation of TCP handshake from the external network to the hiding IP.

- For NAT on SIP entities, it is strongly recommended that you enable the IPS protection **Strict SIP Protocol Flow Enforcement**.

To enable the protection:

a) Enable the IPS Software Blade on the gateway.

b) In **IPS > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP > Protocol Anomaly > Strict SIP Protocol Flow Enforcement** set the **Action** to **Prevent**.

- Security rules can be defined that allow bidirectional calls, or only incoming or outgoing calls. The examples in the next sections explain how to define bidirectional rules.

- When configuring a security rule, if you want calls that are in progress not to be dropped during Install Policy, make sure to select **Keep connections open after Policy has been installed** in the **Service Properties** dialog box.

**Note –** even if the new policy does not allow calls like those in progress, they will not be dropped during Install Policy.
SIP Rules for a Peer-to-Peer No-Proxy Topology

VoIP rules for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>UDP:sip</td>
<td>Accept</td>
<td>SIP over UDP</td>
</tr>
<tr>
<td></td>
<td>Net_A</td>
<td></td>
<td></td>
<td>Bidirectional calls</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>SIP over TCP</td>
<td>Accept</td>
<td>SIP over TCP</td>
</tr>
<tr>
<td></td>
<td>Net_A</td>
<td>service</td>
<td></td>
<td>Bidirectional calls</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To configure SIP rules for this type of peer-to-peer topology.

1. Define a rule that allows IP phones in Net_A to call Net_B and, and vice versa:
   - The SIP over TCP services are:
     * TCP:sip-tcp
     * TCP:sip_tls_authentication
     * TCP:sip_tls_not_inspected

2. Define Hide NAT (or Static NAT) for the phones in the internal network by editing the Network object for Net_A.
   - In the NAT tab of the Network object:
     - Select **Add Automatic Address Translation Rules**
     - Select the Translation method (Hide or Static)
     - If you define Hide NAT:
       1. Create a node object with the Hide NAT IP address.
       2. Add the node object to the **Destination** of the SIP over TCP rule.

3. Install the security Policy.
SIP Rules for a Proxy in an External Network

The illustration shows a SIP topology with a Proxy in an external network.

VoIP Rules for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_Proxy</td>
<td>Net_A</td>
<td>UDP:sip</td>
<td>Accept</td>
<td>SIP over UDP Bidirectional calls</td>
</tr>
<tr>
<td>Net_A</td>
<td>SIP_Proxy</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_Proxy</td>
<td>Net_A</td>
<td>SIP over TCP</td>
<td>Accept</td>
<td>SIP over TCP Bidirectional calls</td>
</tr>
<tr>
<td>Net_A</td>
<td>SIP_Proxy</td>
<td>service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Define 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 figure, these are Net_A.
2. Define the Network object for the SIP Proxy or Registrar (SIP_Proxy).
   If the Proxy and Registrar are on a server that has one IP address, define only one object. If the Proxy
   and server are on the same server but have different IP addresses, define an object for each IP
   address.
3. Configure the VoIP rules.
   The SIP over TCP services are:
   - TCP:sip-tcp
   - TCP:sip_tls_authentication
   - TCP:sip_tls_not_inspected
4. Define Hide NAT (or Static NAT) for the phones in the internal network by editing the Network object for
   Net_A.
   - In the NAT tab, select Add Automatic Address Translation Rules, and then the Translation method
     (Hide or Static).
   - If Hide NAT is defined:
     (i) Create a node object with the Hide NAT IP address.
(ii) Add the node object to the **Destination** of the SIP over TCP rule.

(iii) Consider enabling the **Hide NAT changes source port for SIP over UDP** option under **IPS > Protections > By Type > Engine Settings > SIP - General Settings**.

5. Install the security Policy.

### SIP Rules for a Proxy-to-Proxy Topology

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

**VoIP rules for this scenario:**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_A</td>
<td>Proxy_B</td>
<td>UDP:sip</td>
<td>Accept</td>
<td>SIP over UDP</td>
</tr>
<tr>
<td>Proxy_B</td>
<td>Proxy_A</td>
<td></td>
<td></td>
<td>Bidirectional calls</td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_A</td>
<td>Proxy_B</td>
<td>SIP over TCP service</td>
<td>Accept</td>
<td>SIP over TCP</td>
</tr>
<tr>
<td>Proxy_B</td>
<td>Proxy_A</td>
<td></td>
<td></td>
<td>Bidirectional calls</td>
</tr>
</tbody>
</table>

**To allow bidirectional calls between phones:**

1. Define the Network objects (nodes or networks) for the phones permitted to make calls, and the calls subject to gateway inspection.
   - In the figure, Net_A represents these phones.
2. Define the Network object for the Proxy objects (Proxy_A and Proxy_B).
3. Configure the VoIP rule.
   - The SIP over TCP services are:
     - TCP:sip-tcp
     - TCP:sip_tls_authentication
     - TCP:sip_tls_not_inspected
4. 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).
   - In the **NAT** tab, select **Add Automatic Address Translation Rules** and then the Translation method (Hide or Static).
   - If Hide NAT is defined: add a node object with the Hide NAT IP address object to the **Destination** of the SIP over TCP rule.
5. Define Static NAT for the Proxy in the internal network by repeating step 4 for the Proxy object (Proxy_A).
6. Install the security policy.
SIP Rules for a Proxy in DMZ Topology

The figure illustrates a SIP-based VoIP topology where a Proxy is installed in the DMZ.

VoIP Rules for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_DMZ</td>
<td>Net_A</td>
<td>UDP:sip</td>
<td>Accept</td>
<td>SIP over UDP Bi-directional calls</td>
</tr>
<tr>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net_B</td>
<td>Proxy_DMZ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

or

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy_DMZ</td>
<td>Net_A</td>
<td>SIP over TCP service</td>
<td>Accept</td>
<td>SIP over TCP Bi-directional calls</td>
</tr>
<tr>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net_B</td>
<td>Proxy_DMZ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To allow bidirectional calls between phones in internal and external networks (Net_A and Net_B) and to define NAT for the internal phones and the Proxy in the DMZ (Proxy_DMZ):

1. Define Network objects (nodes or networks) for phones that are permitted to make calls and the calls inspected by the gateway. These are Net_A and Net_B.
2. Define the Network object for the Proxy (Proxy_DMZ).
3. Configure the VoIP rules.
   The SIP over TCP services are:
   - TCP:sip-tcp
   - TCP:sip_tls_authentication
   - TCP:sip_tls_not_inspected
4. Define Hide NAT (or Static NAT) for the phones in the internal network:
   a) To edit the Network object for Net_A:
      - In the NAT tab, select **Add Automatic Address Translation Rules**
      - Select the Translation method (Hide or Static)
   b) To configure Hide NAT:
      - Select the **Hide behind IP address** option
      - Enter the IP address of the Hiding address of the phones in the internal network

   If Hide NAT is defined:
   i) Create a node object with the Hide NAT IP address
(ii) Add the object to the Destination of the SIP over TCP rule defined in step 3.

Static NAT on Proxy in the DMZ

Static NAT on the proxy in the DMZ can be configured with manual NAT rules or with automatic NAT (simpler) if all internal endpoints for which NAT is defined:

- Use SIP over UDP to communicate with the proxy in DMZ and:
- Do not send the data (e.g., voice) through the proxy but directly to other endpoints

If one of these conditions is not true, NAT on the proxy in the DMZ can be configured only with manual NAT rules.

To define static NAT for the proxy in the DMZ using manual NAT rules:

<table>
<thead>
<tr>
<th>Original</th>
<th>Translated</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Source</strong></td>
<td><strong>Destination</strong></td>
<td><strong>Service</strong></td>
</tr>
<tr>
<td>Proxy_DMZ</td>
<td>Net_B</td>
<td>*Any</td>
</tr>
<tr>
<td>Net_B</td>
<td>Proxy_DMZ_ NATed</td>
<td>*Any</td>
</tr>
</tbody>
</table>

1. Create a node object for the Static address of the Proxy (for example, Proxy_DMZ_ NATed)
2. Add Proxy_DMZ_ NATed to the Destination of the Rule Base rule for sip services and sip-tcp services.
3. Add these manual NAT rules:
4. As for all manual NAT rules, configure Proxy-ARP.

To 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 `local.arp` file in UNIX or
- The `arp` command in Windows

The `fw ctl arp` command displays the proxy ARP table on gateways that run on UNIX. On Windows, use the `arp -a` command.

On UNIX-based (including SecurePlatform) gateways:

a) Create a file `$FWDIR/conf/local.arp`
b) Add the related entry, such as:

```
192.168.6.145 00:0D:60:83:B3:74
```

Where 192.168.6.145 is the static address, and 00:0D:60:83:B3:74 is the address of the external interface.
c) From the SmartDashboard File menu, select Policy > Global Properties, and in the NAT page, select Merge Manual Proxy ARP Configuration.
d) Install the security policy.
e) Make sure that the `fw ctl arp` command shows the new entry in the proxy ARP table.

To define static NAT for the proxy in the DMZ using automatic NAT rules:

You can define Static NAT for the Proxy in the DMZ by using automatic NAT rules. To use automatic NAT rules, edit the Network object for the proxy (Proxy_DMZ).

On the NAT page of the General Properties window:

1. Select Add Automatic Address Translation Rules.
2. Select Static as the Translation method.
Using SIP on a Non-Default Port

By default, SIP uses the UDP port 5060. However, SIP phones and SIP Proxies can be configured to use a different port. The gateway will enforce security on the port specified for SIP.

To configure a new port, a new UDP service must be defined in SmartDashboard. You can use the newly defined service and the predefined service (sip) in the same Security Rule Base rule.

**To configure a new SIP service:**

For UDP:
1. From the SmartDashboard File menu, select Manage > Services > New > UDP.
2. In the UDP Service Properties window, name the new service and specify the new SIP port.
3. Click Advanced….
4. In the Advanced UDP Service Properties window, select the Protocol Type: SIP_UDP
5. Click OK.
6. Define a rule in the Security Rule Base that uses the new service.

For TCP:
1. From the SmartDashboard main menu, select Manage > Services > New > TCP.
2. In the TCP Service Properties window, name the new service and specify the new SIP port.
3. Click Advanced….
4. In the Advanced TCP Service Properties window, select the Protocol Type: SIP_TCP_PROTO
5. Click OK.
6. Define a rule in the Security Rule Base that uses the new service.

Enabling Dynamic Opening of Ports for SIP Signaling

The `sip_dynamic_ports` service enables the dynamic opening of ports in the gateway for SIP signaling.

- **By default, port:**
  - 5060 is defined for SIP over UDP and TCP services,
  - 5061 is defined for SIP over TLS services.

- SIP services can be defined for non-default ports.

The service is used to enable the dynamic opening of ports that are not defined by one of the SIP services (default and non-default). Opening such ports allows the establishment of SIP connections. The Check Point gateway opens and closes ports based on the inspection of SIP signaling messages.

Add the `sip_dynamic_ports` service to the rule when:

1. The phones register themselves at a SIP server by associating their phone number with a port other than 5060 or 5061. For example, a registration request for phone number 2001 with IP address 172.16.8.3 port 3000. An example of such a Contact header field is as follows:
   - Contact: <sip:2001@172.16.8.3:3000;rinstance=64d25786c64e7975>;expires=3600

2. The "rport" parameter is used in the Via header field. 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 in a rule together with at least one other SIP service (over TCP or UDP).
Example Rule With the sip_dynamic_ports Service

Example of SIP UDP rule:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP_phone</td>
<td>SIP_server</td>
<td>udp:sip</td>
<td>Accept</td>
</tr>
<tr>
<td>SIP_server</td>
<td>SIP_phone</td>
<td>sip_dynamic_port</td>
<td></td>
</tr>
</tbody>
</table>

- SIP_phone is the IP address of the SIP phone.
- SIP_server is the IP address of the SIP server.
Chapter 4

SIP Advanced Configuration

In This Section:

- Gateway Clustering Support for SIP ................................................................. 29
- Configuring SIP-T Support .............................................................................. 29
- Troubleshooting SIP ......................................................................................... 30

This chapter covers some advanced aspects of SIP configuration and troubleshooting.

Gateway Clustering Support for SIP

This section covers gateway clustering support.

**Synchronizing SIP Connections**

SIP calls can be made across a ClusterXL gateway cluster or a third-party gateway cluster. For ClusterXL and third party gateway clusters (and when SIP connections must be synchronized across gateways): make sure that the **Synchronize connections on Cluster** option is selected. Select the option for all services used in rules that secure SIP connections through the gateway cluster.

To make sure SIP connections through a gateway cluster are synchronized:

1. In the SmartDashboard objects tree, select the Services tab.
2. Edit the SIP service that is used in rules that secure SIP connections through the gateway cluster.
3. In the Service Properties window of the SIP service, click Advanced.
4. Select Synchronize connections on Cluster.
   - **Note** - The Synchronize connections on Cluster option is enabled by default
5. Click OK.
6. Install the policy.

**Load Sharing of SIP Connections**

SIP calls can be made across a ClusterXL gateway in High Availability mode or Load Sharing mode. In Load Sharing Mode, the Sticky Decision Function must be enabled. For more on the Sticky Decision Function, see the *R77 ClusterXL Administration Guide* ([http://supportcontent.checkpoint.com/documentation_download?ID=24800](http://supportcontent.checkpoint.com/documentation_download?ID=24800)).

Configuring SIP-T Support

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

1. Add the $FWDIR/lib/user.def line on the Security Management Server:
   
   ```
   sipt_hosts = { < first_ip, second_ip> , < first_ip, second_ip> , ..... ....,< first_ip, second_ip> } ;
   ```

   Where `first_ip` and `second_ip` are the IP addresses between which (bi-directional) 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 the security policy.

Troubleshooting SIP

To get real-time information on SIP calls:

Run the `fw tab -t sip_state -f` command. This output is displayed:

- Control connection (source, destination).
- RTP connection (endpoint IP addresses).
- Call state (`Initial`, `Call_Established`, `Call_Terminated`...)
- Media type (audio, video, audio/video, application).
- Number of re-INVITE transactions used to implement VoIP features (such as `Call Hold`, `Conference Call`...).
Chapter 5

MGCP-Based VoIP

In This Section:

- Introduction to MGCP ................................................................. 31
- MGCP Supported Deployments and NAT Support.......................... 31
- Rule Base Configuration for MGCP .................................................... 34

Introduction to MGCP

MGCP is a protocol for controlling telephony gateways from external call control devices called Call Agents (also known as Media Gateway Controllers).

MGCP is a master-slave protocol, with the Call Agent as master and endpoints as slaves. (SIP and H.323 are peer-to-peer protocols.)

The MGCP protocol assumes call control devices, or Call Agents, synchronize with each other to send commands to the devices (Media Gateways) they control. Call Agents also connect directly to IP Phones. The Media Gateways or IP Phones are run commands sent by the Call Agents. The figure shows the MGCP elements and call control actions.

![MGCP Diagram]

Media Gateways and MGCP IP phones usually support features such as conference calls, 3-way brokering and supervisor inspection.

MGCP Supported Deployments and NAT Support

The Security Gateway supports the MGCP deployments listed in the table. It is possible to configure NAT (Hide or Static) for the phones in the internal network.
NAT is not supported on IP addresses behind an external Security Gateway interface.

The SmartDashboard configuration depends on the topology.

<table>
<thead>
<tr>
<th>Supported MGCP Topology</th>
<th>No NAT</th>
<th>NAT for Internal Phones - Hide/Static NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Agent in external network</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Agent in DMZ</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Call Agent to Call Agent</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

Call Agent in external network

The IP Phones use the services of a Call Agent on the external side of the gateway. This topology enables using the services of a Call Agent 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.

Call Agent in the DMZ

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

Each Call Agent controls a separate endpoint domain.

Where 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.

Additional Conditions for Using NAT in MGCP Networks

You can use MGCP with Network Address Translation (NAT), but:

- Manual NAT rules are not supported. Use Automatic NAT.
- Calls cannot be made from an external source to two endpoints on the trusted side of a gateway if one of the endpoints is NATed and the other is not.
- Bidirectional NAT of VoIP calls is not supported.

**Important** - Hide NAT can be used for all types of calls (incoming, outgoing, internal and external). For security reasons, when using Hide NAT for incoming calls, the **Destination** of the VoIP call in the Rule Base cannot be **Any**.
**Hide NAT for MGCP traffic**

Enabling the **Hide NAT changes source port for MGCP** option configures the gateway to do Hide NAT on the:

- IP address of the MGCP endpoint phones
- Source port of the MGCP endpoint phones.

Find the option on the:

IP tab > Protections > By Type > Engine Settings > MGCP - General Settings > Protection Details > General tab.

With this option **disabled**, the gateway performs Hide NAT only on the IP address of the MGCP endpoint phones. This option must be **selected** in environments where:

- The gateway is configured (in SmartDashboard) to do Hide NAT on the internal IP addresses of the endpoints.
- The MGCP server can register only one endpoint with a given IP address and port combination.

**MGCP Packet before NAT**

The packet capture shown here shows an MGCP packet from a phone with IP address 194.90.147.53, and source port 2427 (the default MGCP port).

**Packet after Hide NAT when Option is Disabled**

The packet capture shown here 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.

In this environment, all the internal phones are registered with the same Source IP (for example 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.

**Packet after NAT when Option is Enabled**

This packet capture shows the MGCP packet after Hide NAT, with the option **enabled**.

- The IP address is translated to the Hide NAT address of 194.90.147.14.
The source port is also translated to an allocated port of 10416.

In this environment, a different port is allocated for each internal phone. All phones are registered with a different Source IP: port combination. For example:

- One phone with source IP 194.90.147.14 and source port 10416 (as shown in the packet capture), and
- Another phone with source IP 194.90.147.14 and source port 10417.

As a result, all internal phone are registered successfully on the server.

**Rule Base Configuration for MGCP**

This section explains how to configure Security Rule Base Rules so that the gateway allows MGCP calls.

- It is recommended to 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 define a rule that specifies which ports to open and which endpoints can talk. The gateway derives this information from the signaling. For VoIP signaling rules, the gateway automatically opens ports for the endpoint-to-endpoint RTP/RTCP media stream.
- When configuring a security rule, if you want calls that are in progress not to be dropped during Install Policy, make sure to select *Keep connections open after Policy has been installed* in the Service Properties dialog box.
  
  **Note** – even if the new policy does not allow calls like those in progress, they will not be dropped during Install Policy.

**MGCP-Specific services**

These predefined MGCP services are available:

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP:mgcp_CA</td>
<td>Used for MGCP over UDP, for connections using the well known port is the Call-Agent port (2727).</td>
</tr>
<tr>
<td>UDP:mgcp_MG</td>
<td>Used for MGCP over UDP, and whose well known port is the Media Gateway port (2427).</td>
</tr>
<tr>
<td>Other:MGCP_dynamic_ports</td>
<td>Allows a MGCP connection to be opened on a dynamic port and not on the MGCP well-known port.</td>
</tr>
</tbody>
</table>

**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 figure.

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)
- Define NAT for the internal phones

**VoIP rule for this scenario:**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGCP_Call_Agent Net_A</td>
<td>Net_A MGCP_Call_Agent</td>
<td>mgcp_CA or mgcp_MG or mgcp_dynamic_ports</td>
<td>Accept</td>
</tr>
</tbody>
</table>

**To define an MGCP rule for a call agent in the external network:**

1. Define 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 figure, these are Net_A and Net_B.
2. Define the network object for the Call Agent (MGCP_Call_Agent).
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.
   a) On the NAT tab, select Add Automatic Address Translation Rules.
   b) Select the Translation method (Hide or Static).
4. Install the security policy.

**MGCP Rules for Call Agent in DMZ**

The illustration shows an MGCP-based VoIP topology where a Call Agent is installed in the DMZ.
VoIP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_A</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_B</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td></td>
</tr>
<tr>
<td>Call_Agent</td>
<td>Call_Agent</td>
<td>mgcp_CA or mgcp-MG</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

To enable bidirectional calls between phones in internal and external networks (Net_A and Net_B):
1. Define the Network objects (nodes or networks) for the phones that are permitted to make calls, and their calls subject to gateway inspection. In the figure, these are Net_A and Net_B.
2. Define the Network object for the Call Agent (Call_Agent).
3. Configure the VoIP rule.
4. Install the security Policy.

MGCP Rules for Call Agent to Call Agent

This illustration shows a Call Agent-to-Call Agent topology with the Call Agents on opposite sides of the gateway.

VoIP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call_Agent_Int</td>
<td>Call_Agent_Ext</td>
<td>mgcp_CA</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Call_Agent_Ext</td>
<td>Call_Agent_Int</td>
<td>mgcp_CA or mgcp-MG</td>
<td>Accept</td>
<td></td>
</tr>
</tbody>
</table>

To enable bidirectional calls between phones in internal and external networks:
1. Define the Network object for the Proxy objects (Call_Agent_Int and Call_Agent_Ext).
2. Configure the VoIP rule.
3. Install the security Policy.
Chapter 6

H.323-Based VoIP

In This Section:

Introduction to H.323 .......................................................... 37
Supported H.323 Deployments and NAT Support .................... 37
H.323 Security Rule Base Configuration ................................ 39

Introduction to H.323

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

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 defined in SmartDashboard, usually as a network of IP Phones. Usually it is not necessary to define Network objects for individual IP Phones.

- **Standard telephones** that connect to an H.323 gateway
  These are not IP devices. It is not necessary to define them in SmartDashboard

- **A Gatekeeper** that manages a collection of H.323 devices, such as phones
  Gatekeepers convert phone numbers to IP addresses. A Gatekeeper usually provides gateway services as well.

- **A Gateway** that provides interoperability between different networks
  The gateway translates between the telephony protocol and IP.

Supported H.323 Deployments and NAT Support

Supported H.323 deployments are listed the Table. NAT (Hide or Static) 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

<table>
<thead>
<tr>
<th></th>
<th>No NAT</th>
<th>NAT for Internal Phones — Hide/Static NAT</th>
<th>NAT for Gatekeeper — Static NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint to Endpoint</td>
<td>Yes</td>
<td>Static NAT only</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Gatekeeper/Gateway in External</td>
<td>Yes</td>
<td>Yes</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Gatekeeper/Gateway to Gatekeeper/Gateway</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Endpoint-to-Endpoint Communication

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.

### Gatekeeper or H.323 Gateway in External Network

The IP Phones use the services of a Gatekeeper or an H.323 Gateway on the external side of the gateway. This topology enables using 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.

### H.323 Gatekeeper/Gateway to Gatekeeper/Gateway

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.
Gatekeeper or H.323 Gateway in the DMZ

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.

H.323 Security Rule Base Configuration

This section explains how to configure rules that allow H.323 calls through the gateway.

H.323 Specific Services

These predefined H.323 services are available:

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP:H323</td>
<td>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.</td>
</tr>
<tr>
<td>UDP:H323_ras</td>
<td>Allows 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.</td>
</tr>
<tr>
<td>UDP:H323_ras_only</td>
<td>Allows only RAS. 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.</td>
</tr>
<tr>
<td>TCP:H323_any</td>
<td>Relevant only for versions prior to R75.40VS:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Note** - In general, use the H.323 and H.323_ras services in H.323 Security Rule Base rules.

**General Guidelines for H.323 Security Rule Configuration**

- It is recommended to configure anti-spoofing on the Check Point gateway interfaces.
- To allow H.323 traffic, create rules let H.323 control signals through the gateway.

It is not necessary to define a rule that specifies which ports to open and which endpoints can talk. The gateway derives 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. For example: if the Connect message identifies port 80 as the H.245 port, the port will not be opened. This prevents well-known ports from being used illegally.

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

- When using Hide NAT for H.323, include the hiding IP address in the destination of the H.323 rule. This allows the initiation of a TCP handshake from the external network to the hiding IP.

- When configuring a security rule, if you want calls that are in progress not to be dropped during Install Policy, make sure to select Keep connections open after Policy has been installed in the Service Properties dialog box.

  Note – even if the new policy does not allow calls like those in progress, they will not be dropped during Install Policy.

**H.323 Rule for an Endpoint-to-Endpoint Topology**

An endpoint-to-endpoint topology is shown in the figure, 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 define NAT for the internal phones

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

![](image)

**VoIP rule for this scenario:**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>H323</td>
<td>Accept</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Configure the VoIP rule.
2. 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):
     a) In the NAT tab, select Add Automatic Address Translation Rules
     b) Select the Translation method (Hide or Static)
   - If you define Hide NAT, add a Node object (with the Hide NAT IP address) to the Destination of the rule(s) defined in step 1.
3. Install the security policy.
**H.323 Rules for a Gatekeeper-to-Gatekeeper Topology**

A Gatekeeper-to-Gatekeeper topology is shown in the figure, 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)
- Define NAT for the internal phones and the internal Gatekeeper (GK_A)

VolP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GK_A</td>
<td>GK_B</td>
<td>H323</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>GK_B</td>
<td>GK_A</td>
<td>H323_ras</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Define the network objects (Nodes or Networks) for
   - Phones that use the Gatekeeper for registration
   - Allowed to make calls and their calls tracked by the gateway.
   In the figure, these are Net_A and Net_B.
2. Define the Network object for the Gatekeeper objects (GK_A and GK_B)
3. Define the VoIP rule.
4. Define Hide NAT (or Static NAT) for phones in the internal network.
   Do this by editing the network object for the internal network (Net_A):
   a) On the NAT tab, select Add Automatic Address Translation Rules
   b) Select the Translation method (Hide or Static).
5. To define Static NAT for the Gatekeeper or Gateway in the internal network: do step 4 again.
6. Make the time-out of the H323_ras service equal to or greater than the Gatekeeper registration time-out.
   Configure the time-outs in the Advanced Properties window of the Service object.
7. Install the security policy.

**H.323 Rules for a Gateway-to-Gateway Topology**

The illustration shows a Gateway-to-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).

**VoIP rule for this scenario:**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW_A</td>
<td>GW_B</td>
<td>H323</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>GW_B</td>
<td>GW_A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

1. Define the network objects (Nodes or Networks) for phones that are allowed to make calls and their calls tracked by the gateway.
   For this example, these are Net_A and Net_B.
2. Define the network object for the gateway objects (GW_A and GW_B)
3. Define this VoIP rule.
4. 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):
   a) On the NAT tab, select Add Automatic Address Translation Rules
   b) Select the Translation method (Hide or Static).
5. To define Static NAT for the Gatekeeper/Gateway in the internal network, do step 4 again for the Gatekeeper/Gateway object (GK_A).
6. Install the security policy.

**H.323 Rules for a Gatekeeper in the External Network**

This figure shows a H.323 topology with a Gatekeeper in the Internet, 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)
H.323-Based VoIP

- Define NAT for the internal phones

VolP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>GK_B</td>
<td>H323_ras</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_A</td>
<td>H323</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GK_B</td>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To define an H.323 rule for a gatekeeper in the external network:

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 figure, these are Net_A and Net_B.
2. Define the network object for the Gatekeeper (GK_B)
3. Configure the VoIP rule.
4. 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):
   a) On the NAT tab, select Add Automatic Address Translation Rules
   b) Select the Translation method (Hide or Static)
      If you define Hide NAT, add a Node object (with the Hide NAT IP address) to the Destination of the rule(s) configured in step 3.
5. Make the time-out of the H323_ras service greater or equal to the Gatekeeper registration time-out.
   Configure the time-outs in the Advanced Properties window of the Service object.
6. Install the security policy.

**H.323 Rules for a Gateway in the External Network**

The figure shows an H.323 topology with a Gateway in the Internet, 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)
VoIP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>GW_B</td>
<td>H323</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Net_B</td>
<td>GW_B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GW_B</td>
<td>Net_A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

To define an H.323 rule for a gateway in the external network:

1. Define network objects (Nodes or Networks) for phones that are allowed to make calls, and their calls tracked by the gateway.
   For the example, these are Net_A and Net_B.
2. Define the network object for the Gateway (GW_B)
3. Define the VoIP rule.
4. Define Hide NAT (or Static NAT) for the phones in the internal network.
   Do this by editing the object for the internal network (Net_A):
   a) On the NAT tab, select Add Automatic Address Translation Rules,
   b) Select the Translation method (Hide or Static).
      If using Hide NAT, add a Node object (with the Hide NAT IP address) to the Destination of the rule(s) defined in step 3.
5. Install the security policy.

**H.323 Rules for a Gatekeeper in DMZ Topology**

The figure shows a 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)

VolP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GK_DMZ</td>
<td>Net_A</td>
<td>H323</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td>H323_ras</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net_B</td>
<td>GK_DMZ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Static NAT rules for the Gatekeeper in the DMZ:

<table>
<thead>
<tr>
<th>Original</th>
<th>Translated</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Destination</td>
<td>Service</td>
</tr>
<tr>
<td>GK_DMZ</td>
<td>Net_B</td>
<td>*Any</td>
</tr>
<tr>
<td>Net_B</td>
<td>GK_DMZ_NA</td>
<td>*Any</td>
</tr>
</tbody>
</table>

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 figure, these are Net_A and Net_B.
2. Define the network object for the Gatekeeper (GK_DMZ).
3. Define the VolP rule.
4. Define Hide NAT (or Static NAT) for the phones in the internal network.
   Do this by editing the network object for Net_A:
   a) In the NAT tab, select Add Automatic Address Translation Rules
   b) Select the Translation method (Hide or Static).
      If using Hide NAT:
      (i) Select the Hide behind IP address option.
      (ii) Enter the IP address of the Hiding address of the phones in the internal network.
      (iii) Add a Node object with the Hide NAT IP address to the Destination of the rule(s) defined in step 3.
5. 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.

6. Make the time-out for the `H.323_ras` service greater than or equal to the Gatekeeper registration timeout. Configure the time-outs in the **Advanced Properties** window of the Service object.

7. Install the security policy.

**H.323 Rules for a Gateway in DMZ Topology**

The figure shows a H.323-based VoIP topology where a Gateway is installed in the DMZ. 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)
- Define NAT for the internal phones and the Gateway in the DMZ (GW_DMZ)

![H.323 Topology Diagram]

VolP rule for this scenario:

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW_DMZ</td>
<td>Net_A</td>
<td>H323</td>
<td>Accept</td>
<td>Bidirectional calls.</td>
</tr>
<tr>
<td>Net_A</td>
<td>Net_B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Net_B</td>
<td>GW_DMZ</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Static Nat rule for the Security Gateway in the DMZ:

<table>
<thead>
<tr>
<th>Original</th>
<th>Translated</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>GW_DMZ</td>
<td>Net_B</td>
<td><code>*Any</code></td>
<td><code>GW_DMZ: Static</code></td>
<td>=</td>
<td><code>GW_DMZ: Static</code></td>
<td>=</td>
<td>Outgoing calls</td>
<td></td>
</tr>
<tr>
<td>Net_B</td>
<td>GW_DMZ_NATed</td>
<td><code>*Any</code></td>
<td>=</td>
<td><code>GW_DMZ: Static</code></td>
<td>=</td>
<td>Incoming calls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To define an H.323 rule for a gateway in the DMZ:

1. Define network objects (Nodes or Networks) for phones that are allowed to make calls and their calls tracked by the gateway.
   In the figure, these are Net_A and Net_B.
2. Define the network object for the Gateway (GW_DMZ).
3. Define the VoIP rule:
4. Define Hide NAT (or Static NAT) for the phones in the internal network.
   Edit the network object for Net_A:
   a) On the NAT tab, select **Add Automatic Address Translation Rules**
   b) Select the **Translation method** (*Hide* or *Static*).
      If using Hide NAT:
      (i) Select the **Hide behind IP address**.
      (ii) Enter the IP address of the Hiding address of the phones in the internal network.
      (iii) Add a Node object with the Hide NAT IP address to the **Destination** of the rule(s) defined in step 3.
5. Define Static NAT for the Gateway in the DMZ, add manual NAT rules:
   a) Create a Node object for the Static address of the Gateway (for example: GW_DMZ_NATed).
   b) Define these manual NAT rules:
   c) As for all manual NAT rules, configure proxy-arps.
      You must associate the translated IP address with the MAC address of the Check Point 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.
6. Install the security policy.
Chapter 7

SCCP-Based VoIP

In This Section:

- Introduction to SCCP Security and Connectivity .................................................. 48
- Encrypted Protocol Support ....................................................................................... 48
- SCCP Supported Deployments .................................................................................. 48
- Configuring SCCP Connectivity and Security ......................................................... 49

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 is also verified.

Encrypted Protocol Support

The gateway enables secure connectivity for mixed secure and non-secure SCCP (Skinny) environments. In these environments, phones communicate using encrypted or clear text signaling protocols.

Encrypted protocols prevent traditional firewalls from identifying the secure phones or understanding the encrypted signaling stream. Ports must be kept permanently open for all phones. The gateway guarantees secure connectivity by:

- Dynamically identifying the secure phones
- Opening ports only for required phones
- Closing ports when the call completes

Non-secure SCCP uses TCP port 2000. Secure SCCP uses TCP port 2443. For more on encrypted protocol support, see the section on securing encrypted SCCP (“Securing Encrypted SCCP” on page 50).

SCCP Supported Deployments

These SCCP deployments supported:

- Call Manager in internal network
- Call Manager in the DMZ
- Call Manager in external network

Important - NAT on SCCP devices is not supported.
**Call Manager in the Internal Network**

The IP Phones use the services of a Call Manager in an internal network.

**Call Manager in an External Network**

The IP Phones use the services of a Call Manager on the external side of the gateway. This topology enables using 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.

---

**Configuring SCCP Connectivity and Security**

This section explains how to configure security rules that allow SCCP calls through the gateway. After the Rule Base is configured, all SCCP communication is fully secured by IPS.

**General Guidelines for SCCP Security Rule Configuration**

SCCP has a centralized call-control architecture. The CallManager manages SCCP clients (VoIP endpoints), which can be IP Phones or Cisco ATA analog phone adapters. The CallManager controls all the features of the endpoints. The CallManager requests data (such as station capabilities) and sends data (such as the button template and the date/time) to the VoIP endpoints.

The CallManager are defined in SmartDashboard, usually as Host objects. The networks containing directly-managed IP Phones are also defined in SmartDashboard. Usually it is not necessary to define network objects for individual phones. Cisco ATA devices that are managed by a CallManager must be defined in SmartDashboard, but the connected analog phones are not defined.
When configuring a security rule, if you want calls that are in progress not to be dropped during Install Policy, make sure to select **Keep connections open after Policy has been installed** in the **Service Properties** dialog box.

**Note** - even if the new policy does not allow calls like those in progress, they will not be dropped during Install Policy.

**SCCP-Specific Services**

These predefined SCCP services are available:

<table>
<thead>
<tr>
<th>Service</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP:SCCP</td>
<td>Used for SCCP over TCP</td>
</tr>
<tr>
<td>Other:high_udp_for_secure_SCCP</td>
<td>Used for media from Secure SCCP phones</td>
</tr>
</tbody>
</table>

**Securing Encrypted SCCP**

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

- TCP:Secure_SCCP
  - You must create this service in **SmartDashboard** by:
    a) Opening **Manage > Services > New > TCP**.
    - The **Advanced TCP Service Properties** window opens.
    b) Setting the **Name** to: **Secure_SCCP**.
    c) Setting the port to: 2443.
    d) Clicking **Advanced**.
    - The **Advanced TCP Service Properties** window opens.
    e) Setting the **Protocol Type** to: **Secure_SCCP_Protot**.

- 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.

**Configuring the Rule Base for SCCP**

To allow VoIP calls, you must create rules that let VoIP control signals pass through the gateway. It is not necessary to define a media rule that specifies which ports to open and which endpoints can talk. The gateway derives 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.

**Important** - Before configuring security rules for SCCP, makes sure that anti-spoofing is configured on the gateway interfaces.

**VoIP rule for this scenario:**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Net_A</td>
<td>Net_A</td>
<td>SCCP</td>
<td>Accept</td>
<td>Incoming and Outgoing calls</td>
</tr>
<tr>
<td>Net_B</td>
<td>Net_B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call_Manager</td>
<td>Call_Manager</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To configure the Rule Base for secure SCCP-based VoIP:

1. Define Network objects (Nodes or Networks) for SCCP endpoints (Cisco ATA devices or IP Phones) controlled by the CallManagers.
2. Define a host object for the CallManager.
3. Define the SCCP VoIP rules.
4. Define other rules for SCCP and the other VoIP protocols. (SCCP interoperates with other VoIP protocols.)
   - This rule let all phones in Net_A and Net_B make calls to each other:
     - Net_A is the internal IP phone network
     - Net_B is the external IP phone network
       - The CallManager (Call_Manager) can be in:
         - The internal or external network
         - A DMZ connected to a different interface of the gateway.
5. To secure encrypted SCCP over TCP connections:
   a) Create an identical rule
   b) In the Service cell, add only:
      - TCP:Secure_SCCP
      - Other:high_udp_for_secure_SCCP.
6. Install the policy.
Chapter 8

IPS for VoIP

In This Section:

Introduction to IPS for VoIP ................................................................. 52
SIP IPS Protections ................................................................................. 53
H.323 IPS Protections ............................................................................. 56
MGCP IPS Protections .......................................................................... 58
SCCP (Skinny) IPS Protections .............................................................. 61
VoIP Media Admission Control ............................................................. 61

Introduction to IPS for VoIP

IPS adds more than 80 IPS VoIP protections and VoIP settings to protect against attacks. IPS protects against malicious attacks by:

- Identifying attack signatures
- Identifying packets with protocol anomalies
- Ensuring RFC compliance
- Inspecting signaling protocols, for example verifying header formats and protocol call flow state
- Giving enhanced security and more granular settings for SIP, H.323, SCCP and MGCP

As part of IPS, different VoIP protections can be enforced for different gateways using IPS profiles. With IPS, it is possible to change VoIP protections to Detect mode. Running VoIP protections in Detect mode lets you:

- Monitor events
- Do troubleshooting
- Get detailed IPS logs with packet captures on VoIP security events

Note - Event monitoring and detailed logging are also available in Prevent Mode.

For non-RFC compliant VoIP traffic, you can add exceptions to specified VoIP protections. These exceptions prevent the traffic from being dropped (for example due to illegal implementation) without compromising other VoIP security.

VoIP Protections in SmartDashboard

VoIP Protections in SmartDashboard are found on the IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP
Important -

- To enforce enhanced VoIP Security protections, use the IPS recommended profile.
- These older VoIP protections are no longer used by R77 gateways and higher:

![Image of IPS protection settings]

The new VoIP protections introduced in R75.40VS replace them.

**Protocol Engine Settings in IPS**

IPS engine settings are found on the IPS tab > Protections > By Type > Engine Settings.

For each protocol you can find its General Settings. For example, double-clicking SIP - General Settings shows Timeout Configuration and NAT Configuration. For more, see the section on SIP Engine Settings.

**VoIP Call Initiation Rate Limiting**

VoIP Call Initiation Rate Limiting is a general protection for SIP, MGCP, H.323 and SCCP protocols. Configure this protection on the:

IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > VoIP Call Initiation Rate Limiting

**IPS Profiles**

Using IPS profiles, a range of VoIP protections can be enforced on different Security Gateways.

**SIP IPS Protections**

IPS protects against attacks by identifying attacks signatures, identifying packets with protocol anomalies, and ensuring RFC compliance.

The Security Gateway includes a large number of IPS protections for SIP.

IPS protections can be configured for each profile. For each profile, the protection can be:

- Prevent
- Detect
- Inactive

**Note -**

- Application Policy options are not intended to protect against attacks.
- Logging settings for each protection are configured for each profile.

**SIP Protections**

The IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP page has these protections:

- Block SIP Calls from Unregistered Users
- Block SIP Basic Authentication
- Block Unrecoverable SIP Inspection Errors
- SIP Maximum Allowed Retransmissions
- SIP Media Admission Control ("VoIP Media Admission Control" on page 61)
Block SIP Multicast Connections

**SIP Application Policy**

Specified VoIP services can be blocked if the services

- Consume more bandwidth than the IP infrastructure can support
- Do not comply with the organization’s security policy

Application policy options are not intended to protect against attacks.

These Application Policy options are available:

- Block SIP Audio
- Block SIP Instant Messaging
- Block SIP Proxy Failover
- SIP Block Push to Talk over Cellular
- Block SIP Video
- Block SIP Early Media
- Block SIP Keep Alive Messages
- SIP - Method Filtering

These SIP application policy options are on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP > Application Policy**

**SIP Protocol Anomaly**

A protocol anomaly is a field name or value in the protocol header that is RFC compliant, but deviates from usual use. For example a field value, which contains hundreds of characters where less than ten is usual, is an anomaly. If a protocol anomaly is found in the VoIP packet, this is a good indication that the VoIP network is being attacked.

These definitions are related to the structure of SIP headers. The definitions are based on RFC 3261 section 6.

- 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 again and again huge quantities of fraudulent data, eventually overwhelming the server. For example, many buffer-overflow attacks send again and again a very large header 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.

These options are available to protect against SIP protocol anomalies:

- SIP Max Allowed URI Length
- SIP Max Allowed Call-ID Length
- SIP Max Allowed Domain Length
- SIP Max Allowed Header Name Length
- SIP Max Allowed Header Value Length
- SIP Max Allowed SDP Length
- SIP Max Allowed Tag Length
- Strict SIP Protocol Flow Enforcement
- Block SIP Messages with Binary Characters

Find these protections on the:

IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP > Protocol Anomaly

**General Header Security**

These protections are related to protocol anomalies in the SIP header in general, rather than specified header fields:

- SIP Max Allowed Occurrences of the Same Field
- Verify Format of SIP Header
- Enforce SIP Mandatory Fields Existence
- Enforce Single Occurrence of Fields by SIP RFC
- Block SIP Messages with Invalid SDP Format

Find these protections under: IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP > Protocol Anomaly > General Header Security.

**Specific Header Security**

These protections are related to protocol anomalies in specified SIP header fields:

- Block SIP NOTIFY Messages with Invalid Subscription-State Header
- SIP Min Allowed 'Max-Forwards' Value
- SIP Max Allowed 'Content-Length'
- Block SIP Messages with Invalid Header Value
- Block SIP Messages with Invalid Format in Start Line
- Block SIP Messages with Invalid Format in Via Header
- Block SIP Messages with Invalid Formats in Headers with Usernames
- Block SIP Messages with Invalid IP Address in SDP Header
- Block SIP Messages with Invalid Port in SDP Header
- Block SIP Messages with Invalid Format in CSeq Header

These protections are available on the: IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SIP > Protocol Anomaly > Specific Header Security.

**IPS Engine Settings for SIP**

Generals settings are configured on the IPS tab > Protections > By Type > Engine Settings > SIP - General Settings.

Configure these fields:

- **Timeout Configuration**

  Default registration expiration time period determines how long endpoint registration information is kept in the database if a timeout is not specified in registration messages. The time period must be greater than or equal to the registration time period of the endpoint or the proxy. The default registration...
expiration period is 3600 seconds. If the endpoint does not send a user registration message in this period, registration information is deleted from the database.

**SIP signaling idle timeout when RTP/RTCP traffic does not pass via the gateway** determines the maximal allowed time period between one SIP signaling message and the next. This includes scenarios where Dynamic Pinholing (see below) is disabled, or for calls between two external endpoints or two internal endpoints. The default idle period is 3600 seconds.

- **NAT Configuration**
  - **Hide NAT changes source port for SIP over UDP.** Selecting this option configures the gateway, when doing Hide NAT, to translate the IP address and source port of SIP endpoints.

    **Note** - This applies to SIP over UDP traffic. For SIP over TCP, the source port is always translated if Hide NAT is enabled.

    With this option cleared, the gateway does Hide NAT only on the IP address of the SIP endpoint phones. This option must be enabled in environments where:
    - The gateway is configured to do Hide NAT on the internal endpoint IP addresses and:
    - The SIP server can register only one endpoint with a given IP address and port combination. For example, if the server is a *Cisco Unified communications Manager*.

    **Note** - For all internal phones to be registered successfully on the server, the source port of the REGISTER message sent by the phone must be the same as the port in the Contact header of the REGISTER message. In Cisco IP Phones, for example, this is done by selecting the "NAT Enabled" option.

    For more, see the section on Hide NAT and SIP.

- **Extension Length**
  - **Assume VoIP network uses extension length.** The gateway can be configured to support short extension numbers for SIP. Endpoints register with the SIP server using their full name (usually a number). The gateway can be configured to identify a shortened name as belonging to an already registered endpoint. Calls to and from endpoints are made using a short extension name: a suffix of the full name.

    The length of the extension name is configurable. For example, if the full name of an endpoint registered with the SIP server is 987654321@example.com, and the configured extension length is 4. The gateway can associate calls to or from 4321@example.com with the registered endpoint.

- **Dynamic Pinholing**
  - **Block dynamic opening of ports for SIP media channel.** Selecting this option prevents SIP media channels from opening. A Security Gateway dynamically opens ports for the VoIP media channel according to data in the signaling connection. Do not select this option if SIP media channel passes through the gateway.

### H.323 IPS Protections

IPS protects against attacks by identifying attacks, identifying packets with protocol anomalies, and ensuring standards compliance.

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

- The Security Gateway supports these H.323 IPS protections:
  - H.323 Media Admission Control
  - Block H.323 Multicast Connections
  - Block Unrecoverable H.323 Inspections Errors

These protections can be found at:

**IPS tab > Protections > By Protocol > IPS > Software Blade > Application Intelligence > VoIP > H.323**
IPS protections can be configured for each profile. The protection can be **Prevent**, **Inactive**, or **Detect**. Logging settings for each protection are configured for each profile.

**H.323 Application Policy**

Specified VoIP services can be blocked if the services
- Consume more bandwidth than the IP infrastructure
- Do not comply with the organization’s security policy

Application policy options are not intended to protect against attacks.

These Application Policy options are available:
- Block H.245 Tunneling
- Block T.120 over H.323

H.323 application policy options are available on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > H.323 > Application Policy**

**H.323 Protocol Anomaly**

A protocol anomaly is a field value or a message in the protocol that is standards compliant but deviates from correct use. For example a field value with 100 bytes, where much less is usual, is a protocol anomaly. A message with 1400 bytes where 800 bytes is usual is a protocol anomaly. A message that is sent "out of protocol state" (the message does not match the definition of the protocol) is also a protocol anomaly.

A protocol anomaly in a VoIP packet is a good indication that the VoIP network is being attacked. To protect against H.323 protocol anomalies, these options are available:
- Max Allowed H.245 Message Length
- Block H.323 Messages with Illegal ASN.1 Encoding
- H.323 Max Allowed Phone's Extension Length
- Max Allowed Q.931 Message Length
- Max Allowed RAS Message Length
- Verify H.323 State
- Verify H.323 Message Content
- Block H.323 Sessions that Do Not Start with Setup Message

H.323 Protocol Anomaly Protections are available on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > H.323 > Protocol Anomaly**

**IPS Engine Settings for H.323**

General settings are configured on the **IPS tab > Protections > By Type > Engine Settings > H.323 - General Settings**.

Configure these settings:
- **T.120 Timeout**
  A timeout for a dynamically opened T.120 connection.
- **Block dynamic opening of ports for H.323 media channel**
  A Security Gateway dynamically opens ports for the VoIP media channel according to data in the H.323 signaling connection. Selecting this option prevents the opening of H.323 media channels. **Do not select this option if a H.323 media channel passes through the gateway.**
• **Block dynamic opening of H.323 connections from RAS messages**
  
  If the H323_ras service is allowed in the Rule Base, this option configures if control connections will be dynamically opened by the firewall from RAS messages. (Control connections are required by all H.323 connections.)

  This option applies only to connections that start with RAS (that are allowed and inspected by the H323_ras service). If you select this setting, make sure that the H323 service is allowed in the Rule Base.

• **Allow an initiation of H.323 connections from server to endpoints**

  The endpoint usually initiates the H.323 (H.225) TCP connection to the Gatekeeper or server. In scenarios where the Gatekeeper initiates the TCP connection to the endpoint, this setting must be selected.

  **Note** - In this scenario, Hide NAT on the internal network is not supported.

### MGCP IPS Protections

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

IPS protections can be configured for each profile. For each profile, the protection can be **Prevent**, **Inactive**, or **Detect**. Logging options for each protection can also be configured for each profile.

**Supported MGCP IPS protections:**

- Block Unrecoverable MGCP Inspection Errors
- MGCP Media Admission Control
- Block MGCP Multicast Connections
- Block MGCP Messages with Binary characters
- MGCP - General Settings

MGCP Protections are available at:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > MGCP**

### MGCP Protocol Anomaly Protections

- MGCP Max Allowed Call-ID Length
- MGCP Max Allowed Connection Mode Length
- MGCP Max Allowed Domain Name Length
- MGCP Max Allowed EndpointID Length
- MGCP Max Length of Header Value
- MGCP Max Allowed TransactionsID Length

MGCP Protocol Anomaly Protections are available at:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > MGCP > Protocol Anomaly**

### MGCP Application Policy

Specified VoIP services can be blocked if the services consume more bandwidth than the IP infrastructure can support (or if the services simply do not comply with the organization’s security policy).

These Application Policy options limit the VoIP services available to users.
MGCP Command Filtering

This option blocks MGCP commands that must not be processed. MGCP command filtering makes it possible to block commands that the MGCP server does not support, or that you do not want the server to handle.

Supported MGCP Commands

There are nine MGCP commands. They are defined in RFC 3435 section 2.3. Commands can be sent by the MGCP server to the endpoint or from the endpoint to the MGCP server.

The Nine supported MGCP commands are:

- AuditConnection (AUCX)
- AuditEndpoint (AUEP)
- CreateConnection (CRCX)
- DeleteConnection (DLCX)
- EndpointConfiguration (EPCF)
- ModifyConnection (MDCX)
- NotificationRequest (RQNT)
- Notify (NTFY)
- RestartInProgress (RSIP)

**Important** - If an MGCP server is flooded with requests that use commands the server does not support, the server might experience an overload. An overloaded MGCP server will affect customer service levels.

User Defined MGCP Commands

RFC 3435 section 3.2.1.1 states: *New verbs may be defined in further versions of the protocol. It may be necessary, for experimentation purposes, to use new verbs before they are sanctioned in a published version of this protocol. Experimental verbs MUST be identified by a four letter code starting with the letter X, such as for example XPER.*

It is possible to define new commands, and configure the MGCP Command filtering option to allow these commands.

Block Unknown Commands

Unknown commands are commands that do not show in the Blocked commands or Allowed commands lists. By default, all unknown commands are blocked.

User Defined Commands have SDP Header

This option specifies if user-defined commands include an SDP header. If the option is selected, the gateway inspects the SDP header attached to the command. If this option is not selected, the SDP header is ignored.

When defining an MGCP command, you can specify if the command contains an SDP header. This VoIP security option parses the header and checks that it has the correct syntax. If the destination address and port in the header are allowed, the media connection is allowed through the Gateway.
Block Unsupported MGCP Commands: Configuration Details

To block commands unsupported by the MGCP server:

1. Open **SmartDashboard > IPS tab > VoIP > MGCP > Application Policy > MGCP Command Filtering**.
2. On the **Protection Details** page, double-click the related IPS profile. The **Protection Settings** window opens.

![Protection Settings window](image)

3. In the **Supported Commands** area, clear from the list the MGCP commands you want to block.

**Fax**

When an MGCP call is made, a number of connections are set up, one of which is intended for fax. The Fax option blocks all applications that use MGCP to transmit fax. The default is not to block.

**IPS Engine Settings for MGCP**

Generals settings are configured on the **IPS tab > Protections > By Type > Engine Settings > MGCP - General Settings**.

Configure these options:

- **Hide NAT changes source port for MGCP**
  Enabling the **Hide NAT changes source port for MGCP** option configures the gateway to do Hide NAT on the:
  - IP address
  - Source port of the MGCP endpoint phones.
  With this option disabled, the gateway does Hide NAT only on the IP address of the MGCP endpoint phones. This option must be enabled in environments where:
  - The gateway is configured for Hide NAT on the internal IP addresses of the endpoints.
  - The MGCP server can register only one endpoint with a given IP address and port combination.

- **Block dynamic opening of ports for MGCP media channel**
  A Security Gateway dynamically opens ports for VoIP media channel, according to the information in the MGCP signaling connection. This option prevents opening of MGCP media channels. **Do not select this option if an MGCP media channel passes through the gateway.**
SCCP (Skinny) IPS Protections

IPS protects by identifying attacks, identifying packets with protocol anomalies, and ensuring standards compliance.

The Security Gateway has a number of IPS protections for SCCP. IPS protections are configured for each profile. For each profile, the protection can be Prevent, Inactive, or Detect. Logging settings for each protection are configured for each profile.

**SCCP IPS Protections**

- Block Unrecoverable SCCP Inspection Error
- SCCP Media Admission Control
- Block SCCP Multicast Connections

SCCP Protections are available on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SCCP**

**SCCP Application Policy**

Specified VoIP services can be blocked if the services:

- Consume more bandwidth than the IP infrastructure can support
- Do not comply with the organization's security policy

One SCCP Application Policy option is available: Block Unknown SCCP Messages. The option is available on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SCCP > Application Policy**

**SCCP Protocol Anomaly Protections**

Three SCCP anomaly protections are available on the:

**IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP > SCCP > Protocol Anomaly**

The protections are:

- Max Allowed SCCP Message Length
- Verify SCCP State
- Verify SCCP Header Content

**IPS Engine Settings for SCCP**

General settings are configured on the **IPS tab > Protections > By Type > Engine Settings > SCCP - General Settings**.

Block dynamic opening of ports for SCCP media channel prevents opening of the SCCP media channel. Based on information in the SCCP signaling connection, a Security Gateway dynamically opens ports for the VoIP media channel. Do not select this option if a SCCP media channel passes through the gateway.

**VoIP Media Admission Control**

Media admission control refers to how a VoIP Server lets one endpoint to 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.

1. **Endpoint A** initiates with **endpoint B**, using **VoIP server C**.
2. **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 (as shown in the diagram, if it knows its physical location), 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.
3. **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.
4. **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 possibly 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**

1. Create Host object for the VoIP Server
2. Create Host or Network objects for VoIP endpoints.
3. Create a Group for VoIP endpoints:
   
   **Network Objects > New > Groups > Simple Group.**
4. Create 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 Rulebase.

6. Enable the related IPS protection according to the VoIP protocol:

   **IPS tab > Protections > By Protocol > IPS Software Blade > Application Intelligence > VoIP >**

   • SIP > SIP Media Admission Control
   • H.323 > H.323 Media Admission Control
   • MGCP > MGCP Media Admission Control
   • SCCP > SCCP Media Admission Control
Chapter 9

VoIP Logging and Queries in SmartView Tracker

In This Section:

VoIP logging......................................................................................................................... 64
VoIP Queries.......................................................................................................................... 64

VoIP logging
SmartView Tracker:

- Shows detailed, protocol-specific logs for VoIP traffic.
  - There are also a number of predefined SmartView Tracker VoIP log queries. These logs supply enhanced troubleshooting capabilities.
  - SmartView Tracker logs are Accept, Drop, or Detect.

<table>
<thead>
<tr>
<th>To enable VoIP logging of...</th>
<th>Configure the Track option to Log in the...</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP calls</td>
<td>Security Rule Base VoIP rule</td>
</tr>
<tr>
<td>IPS protections</td>
<td>IPS protection</td>
</tr>
</tbody>
</table>

- If VoIP logging is disabled, then only standard logging takes place, showing the source, destination and protocol information.
- Logs SIP, H.323, MGCP and SCCP.

VoIP Queries
In SmartView Tracker, there are predefined Voice Over IP log queries.

<table>
<thead>
<tr>
<th>Predefined Query</th>
<th>Type</th>
<th>When Sent</th>
<th>Shows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registration Session</td>
<td>Accept logs</td>
<td>After successful registration.</td>
<td>Registration IP address, phone number, port, and transport protocol (TCP/UDP). Registration period (seconds). IP address of the registrar server.</td>
</tr>
<tr>
<td>Other Session</td>
<td>Accept logs</td>
<td>After response to SIP requests (such as MESSAGE or UPDATE) or response to MGCP commands (such as AUEP, AUCX, or EPCF).</td>
<td>Source IP address, port, and phone number. Destination IP address, port and phone number. SIP method or MGCP command type.</td>
</tr>
<tr>
<td>Security Events</td>
<td>Drop or Detect logs</td>
<td>IPS VoIP protection has detected a violation.</td>
<td>Source IP address, port and phone number. Destination IP address, port and phone number. Reason for log (Attack and Attack Information fields).</td>
</tr>
<tr>
<td>Predefined Query</td>
<td>Type</td>
<td>When Sent</td>
<td>Shows</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Session</td>
<td>Accept logs</td>
<td>After a call is established, and updated after the call is closed.</td>
<td>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.)</td>
</tr>
<tr>
<td>Policy Events</td>
<td>Drop or Detect logs</td>
<td>VoIP policy has detected a violation.</td>
<td>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.</td>
</tr>
</tbody>
</table>

Queries can be found under:

**Network and Endpoint Queries > Predefined > Network Security blades > Firewall Blade > Voice over IP**