Deploying Polycom® Unified Communications in RealPresence® Access Director™ System Environments
Trademark Information

POLYCOM® and the names and marks associated with Polycom's products are trademarks and/or service marks of Polycom, Inc., and are registered and/or common law marks in the United States and various other countries.

All other trademarks are the property of their respective owners.

Patent Information

The accompanying product may be protected by one or more U.S. and foreign patents and/or pending patent applications held by Polycom, Inc.
About This Guide

This guide describes the Polycom® RealPresence® Access Director™ system solution and the process of deploying the products in the solution. The solution provides firewall traversal for the connections required for the supported deployment architecture, model, and user scenarios.

Related Documentation

This guide is meant to supplement the associated product documentation, not replace it. When deploying the systems in this solution, please have the product documentation accessible, specifically.

- Polycom RealPresence Access Director System Release Notes
- Polycom RealPresence Access Director System Getting Started Guide
- Polycom RealPresence Access Director System Administrator’s Guide

In addition, you will need the product documentation for the other infrastructure products required for this solution, including:

- Polycom DMA System Operations Guide
- Polycom RealPresence Resource Manager System Operations Guide
- Polycom RealPresence Collaboration Server System Administrator’s Guide

Required Skills

Integrating Polycom infrastructure and endpoint systems with the RealPresence Access Director system requires planning and elementary knowledge of Polycom video conferencing and video conferencing administration.

This is not a training document. Polycom assumes those deploying this solution have a good understanding of networking, firewalls, DNS, H.323, and SIP concepts.
Contents

About This Guide ........................................ iii
   Related Documentation .................................. iii
   Required Skills ........................................ iii

1 Unified Communications with the Polycom® RealPresence®
   Access Director™ System Solutions .................... 1
   Overview of the Polycom RealPresence Access Director System Solution . 2
   RealPresence Access Director System Solution Deployment Models . . . . 3
      Call Scenarios Supported by this Architecture ................. 6
      Products Tested in this Solution .............................. 7

2 Deploying the Basic RealPresence Access Director System
   Solution to Support Remote and Guest Users ............. 9
   Configure the DNS Service .................................. 10
   Configure Firewalls and Ports ............................... 13
   Install the RealPresence Access Director System ............ 14
   Configure the RealPresence Resource Manager System .......... 14
   Configure the RealPresence Access Director System .......... 18
   Configure the Polycom DMA System ...................... 20
   Supporting Guests in a SIP Environment ..................... 21
   Configure Polycom Endpoint Systems ..................... 23
   Configure the Polycom RealPresence Collaboration Server .... 24
   Configure the Polycom RSSTM System .................... 24

3 Federation Between RealPresence Access Director Systems
   Only ...................................................... 27
   Federation in a SIP Environment ............................ 27
   Federation in an H.323 Environment ...................... 30
4 Federation Between RealPresence Access Director and Other Systems ........................................... 33
   Federation in an H.323 Environment with Polycom VBP-E Systems .................. 33
   Federation in a SIP Environment with Acme Packet ............................... 37

5 Verifying Deployment .................................................. 39
   Verifying Access Proxy .................................................. 39
   Verifying SBC ............................................................. 39
   Verifying Certificates ................................................... 40

A Required Ports .......................................................... 41
   Management Ports ......................................................... 41
      From the WAN to the RealPresence Access Director System ............. 41
      From the LAN to the RealPresence Access Director System ........... 42
      From the RealPresence Access Director System to the WAN ......... 42
      From the RealPresence Access Director System to the LAN ........ 43
   H.323 and WAN Support .................................................. 43
      From the WAN to the RealPresence Access Director System ........... 44
      From the WAN to the RealPresence Access Director System: H.323 B2B
      Calls ................................................................. 44
      From the RealPresence Access Director System to the WAN: H.323 B2B
      Calls ................................................................. 45
   H.323 and LAN Support .................................................. 46
      From the RealPresence Access Director System to the LAN ........... 46
      From the LAN to the RealPresence Access Director System ........... 47
      From the RealPresence Access Director System to the LAN: H.323 B2B
      Calls ................................................................. 47
      From the LAN to the RealPresence Access Director System: H.323 B2B
      Calls ................................................................. 48
   SIP and WAN Support .................................................... 49
      From the WAN to the RealPresence Access Director System ........... 49
      From the RealPresence Access Director System to the WAN ........... 50
   SIP and LAN Support .................................................... 51
      From the RealPresence Access Director System to the LAN ........... 51
      From the LAN to the RealPresence Access Director System ........... 52

B Network Interface Configurations ................................. 55
   Network Interface Configuration Summary ................................... 55
   Network Interface Configurations for Dynamic Routing .................... 56
      Two Firewalls—One Interface to the Outside Firewall .................. 56
Two Firewalls—Four Interfaces to the Outside Firewall .............. 56
Two Firewalls—One Interface to Inside Firewall .................... 57
Two Firewalls—Four Interfaces to Inside Firewall ................... 57
Single Firewall—One Interface .................................... 58
Single Firewall—Four Interfaces ................................. 58
Network Interface Configurations for Static Routing .......... 59
Two Firewalls—One Interface to the DMZ ......................... 59
Two Firewalls—Four Interfaces to the DMZ ......................... 59
Unified Communications with the Polycom® RealPresence® Access Director™ System Solutions

In this solution, Polycom’s integrated suite of video conferencing systems includes the RealPresence Access Director system, which:

• Secures the borders to the enterprise IP network, the private VPN, and the Internet.

• Enables high-quality and secure unified communications between divisions or enterprises, remote users, and guest users.

• Supports the Simple Network Management Protocol (SNMP) to enable communication between the RealPresence Access Director system SNMP agent and the SNMP management system.

The topics that follow describe the Polycom solution that includes the RealPresence Access Director system as the session border controller (SBC) for a site’s IP network.
Overview of the Polycom RealPresence Access Director System Solution

The Polycom video infrastructure integrates with the RealPresence Access Director system to provide video conferencing management for remote, guest, and federated users with secure firewall traversal for all the required connections. The following table describes the network traversal feature services this solution secures.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS Access Proxy</td>
<td>Enables remote and guest users via designated video endpoints to make HTTPS connections to the RealPresence Access Director system, which are then proxied to the internal RealPresence Resource Manager system or RealPresence Content Sharing Suite (the latter supports video sharing among Lync conference participants).</td>
</tr>
<tr>
<td>XMPP Access Proxy</td>
<td>Enables XMPP signaling from remote users via designated video endpoints to traverse the firewall to the internal XMPP server, and enables sending of outgoing XMPP signaling to other remote endpoints.</td>
</tr>
<tr>
<td>LDAP Access Proxy</td>
<td>Enables remote and guest users via designated video endpoints to make LDAP connections to the RealPresence Access Director system, which are then proxied to the internal LDAP server.</td>
</tr>
<tr>
<td>SIP Signaling</td>
<td>Enables:</td>
</tr>
<tr>
<td></td>
<td>• SIP signaling from remote users via designated video endpoints to traverse the firewall to the internal SIP server.</td>
</tr>
<tr>
<td></td>
<td>• Sending of outgoing SIP signaling to remote endpoints.</td>
</tr>
<tr>
<td></td>
<td>• Modifying SIP signaling to direct media through the media relay when required.</td>
</tr>
<tr>
<td>H.323 Signaling</td>
<td>Enables:</td>
</tr>
<tr>
<td></td>
<td>• H.323 signaling from and to remote users via designated video endpoints to traverse the firewall to the internal gatekeeper.</td>
</tr>
<tr>
<td></td>
<td>• Functionality to understand and manipulate all H.323 Annex O dialing messages.</td>
</tr>
<tr>
<td></td>
<td>• Functionality to route all H.323 messages from guest users to and from the internal gatekeeper.</td>
</tr>
<tr>
<td>Media Relay</td>
<td>Enables media from remote and guest users residing in federated sites to traverse the firewall. The media relay functions as an SBC-based relay.</td>
</tr>
</tbody>
</table>
In this solution, the RealPresence Access Director system uses access proxy to enable remote users to be provisioned and managed by setting up the HTTPS, LDAP, and XMPP connections with the RealPresence Resource Manager system. When access proxy receives an HTTPS, LDAP, or XMPP connection request from an external endpoint, the RealPresence Access Director system accepts the request and initializes a request to the internal HTTPS, LDAP, or XMPP server.

If your RealPresence Access Director system provides firewall traversal for a Polycom® RealPresence® Content Sharing Suite, HTTPS requests can be forwarded to the RealPresence Content Sharing Suite server.

If your system is deployed with both a RealPresence Resource Manager system and a RealPresence Content Sharing Suite server, the RealPresence Access Director system forwards requests to the correct server based on the access proxy HTTPS configuration settings. See the Polycom® RealPresence® Access Director™ System Administrator’s Guide for configuration details.

### RealPresence Access Director System Solution Deployment Models

In general, Polycom recommends that the RealPresence Access Director system be deployed in a corporate back-to-back DMZ; that is, deployed between an outside (also referred to as public or external) firewall and inside (also referred to as private or internal) firewall.

In this implementation:

- The outside firewall, which resides between the WAN (Untrust) and the RealPresence Access Director system in the DMZ, must be in Destination NAT mode. In this mode:
  - When inbound packets from the WAN pass through the firewall, it translates the destination IP address to that of the RealPresence Access Director system.
  - When outbound packets from the enterprise network pass through the firewall, it translates the source IP address to the outside IP address of the firewall system.
  - A static and direct 1:1 NAT mapping is recommended for the outside firewall.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Routing</td>
<td>Enables use of static routes to route traffic to the correct network destination. One or more static routes may be defined for each network interface</td>
</tr>
</tbody>
</table>

---

Polycom, Inc.
• The inside firewall, which resides between the RealPresence Access Director system in the DMZ and the LAN (Trust), must be in Route mode. In this mode, the firewall does not change the destination or source IP address, so no translation is required or supported.

This approach takes advantage of the firewall’s security functionality. However, because all media and signaling traffic flows through the firewall, performance can be affected.

The following figure illustrates two other ways in which the RealPresence Access Director system can be deployed in relationship to the outside firewall.

If you have a "three legged firewall" (one with at least three network interfaces), the same firewall can separate the RealPresence Access Director system in the DMZ from both the internal LAN and the Internet.

Note that in these configurations:
• Not all firewall traffic goes through the RealPresence Access Director system.
• All of these models can support the scenarios in this solution.
Avoiding Asymmetric Routing

Asymmetric routing issues may occur if the RealPresence Access Director system is deployed in the DMZ into the network topology shown in the figure below. To prevent asymmetric routing issues, static routes can be defined for each available network interface in your system. See the *Polycom® RealPresence® Access Director™ System Administrator’s Guide* for detailed information about configuring static routes.

The three-legged firewall configuration requires a static and direct 1:1 NAT mapping between the WAN (Untrust) and the DMZ and Route mode between the DMZ and the LAN (Trust).

Appendix B includes diagrams of the network interface configurations supported for this solution.
Call Scenarios Supported by this Architecture

This Polycom solution supports the following user scenarios:

• Connecting Remote Users to the Enterprise (SIP only)
• Connecting Guest Users to the Enterprise (H.323 and SIP)
• Connecting Trusted Divisions or Enterprises (H.323 and SIP)

Connecting Remote Users to the Enterprise (SIP only)

A remote user is an enterprise user with a managed Polycom SIP endpoint that lies outside of the enterprise network. In this user scenario:

• Remote users can participate in video calls with other enterprise users as if they were inside the enterprise network.
• Remote users can receive calls as if they were inside the network.
• Remote users can receive management services including endpoint provisioning, user directory, and XMPP contact list and presence services, as well as SIP calling, calendaring, and scheduling services.

The standard RealPresence Access Director system deployment as described in Chapter 2, “Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users,” supports this user scenario.

Connecting Guest Users to the Enterprise (H.323 and SIP)

A guest user is a user with a non-managed SIP or H.323 endpoint that lies outside of the enterprise network.

In this user scenario:

• Guest users can participate in video calls with division or enterprise users without being members of the site.
• Division or enterprise users cannot place video calls out to guest users. Until guest users initiate video calls, calls cannot be routed to them by the gatekeeper (H.323 endpoints) or SIP Proxy (SIP endpoints).
• Guest users do not have access to any management services such as endpoint provisioning, user directory, XMPP contact list and presence services, or SIP calling, calendaring, and scheduling services.

To support this user scenario, you must perform the standard RealPresence Access Director system deployment as described in Chapter 2, “Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users.”
Connecting Trusted Divisions or Enterprises (H.323 and SIP)

Enterprise users from one division or enterprise can call enterprise users from another division or enterprise when:

- Both division or enterprise users have supported and managed SIP or H.323 endpoints.
- Both division or enterprise sites have implemented a RealPresence Access Director system or other Access Solution for federation.
- The federated sites are connected by a mutually trusted connection. For SIP systems, this trust relationship is a SIP trunk. For H.323 systems, this trust relationship is mutually neighbored gatekeepers.
- The sites have established and supported dial plans.

In this user scenario, each user has access to their site’s provisioning, directory, presence, and calling services, as well as contact lists.

To support this user scenario, you must:

- Perform the standard RealPresence Access Director system deployment as described in Chapter 2, “Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users.”
- Perform the additional deployment processes described in the appropriate section for your deployment model:
  - Chapter 3, “Federation Between RealPresence Access Director Systems Only.”
  - Chapter 4, “Federation Between RealPresence Access Director and Other Systems.”

Products Tested in this Solution

The following products are supported in this RealPresence Access Director system solution.

<table>
<thead>
<tr>
<th>Polycom Product</th>
<th>Version</th>
<th>Function in Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polycom RealPresence Access Director</td>
<td>2.1</td>
<td>Secures access to H.323 and SIP video services for small- to medium-sized federated enterprises.</td>
</tr>
<tr>
<td>Polycom Distributed Media Application™ (DMA™) 7000</td>
<td>5.2, 6.0</td>
<td>Functions as SIP proxy/registrar, H.323 gatekeeper, SIP and H.323 gateway, and bridge virtualizer.</td>
</tr>
<tr>
<td>Polycom RealPresence Resource Manager</td>
<td>7.1, 7.2</td>
<td>Provisions and manages remote endpoints, and enables directory and presence services.</td>
</tr>
<tr>
<td>Polycom Product</td>
<td>Version</td>
<td>Function in Solution</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polycom RSS™ 4000</td>
<td>8.5, 8.6</td>
<td>Provides recording functionality for video, audio, and content.</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server 1500, 2000, and 4000</td>
<td>7.8</td>
<td>Provides bridge capability for SIP and H.323 conferences, including support for content over video.</td>
</tr>
<tr>
<td>Polycom RealPresence Collaboration Server 800s</td>
<td>8.0</td>
<td>Provides bridge capability for SIP and H.323 conferences, including support for content over video.</td>
</tr>
<tr>
<td>Polycom HDX Series</td>
<td>3.1.0</td>
<td>Video conferencing endpoint systems.</td>
</tr>
<tr>
<td>Polycom RealPresence Mobile</td>
<td>2.2, 2.3</td>
<td>Serves as client application for supported Apple® devices.</td>
</tr>
<tr>
<td>Acme Packet Net-Net ESD</td>
<td>6.3</td>
<td>Testing was carried out specifically with the Acme Packet Net-Net ESD-3820 platform running S-Cx6.3.MF-2 software. Other Acme Packet E-SBCs such as Net-Net ESD-4500, Net-Net ESD-SE and Net-Net ESD-VME also run the same line of C-series software. These other products can also be used in this Polycom RealPresence solution.</td>
</tr>
<tr>
<td>Polycom Video Border Proxy (VBP)</td>
<td>11.2.12</td>
<td>In some solution models, provides border control functionality for federated enterprises.</td>
</tr>
<tr>
<td>Polycom CMA system</td>
<td>6.2</td>
<td>In those solution models using a Polycom VBP-E border controller, the CMA system is behind the VBP system and provides management and H.323 gatekeeper functionality.</td>
</tr>
<tr>
<td>Polycom RealPresence Group 300 and Group 500</td>
<td>4.0.1, 4.0.2</td>
<td>Video conferencing endpoint systems.</td>
</tr>
</tbody>
</table>
Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users

This chapter describes the general configuration processes required for any RealPresence Access Director system deployment to support remote or guest users. The chapters that follow describe additional configuration processes required for the specific deployment models.

The following cross-functional flow chart identifies the tasks you must perform.

<table>
<thead>
<tr>
<th>General Preparation</th>
<th>On RealPresence Access Director System</th>
<th>On RealPresence Resource Manager System</th>
<th>On DNS System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure DNS Service</td>
<td>Perform basic installation</td>
<td>Create &quot;traversal&quot; data</td>
<td>Enable SIP Device Authentication</td>
</tr>
<tr>
<td>Configure firewall and ports</td>
<td>Configure Network &amp; Time settings</td>
<td>Add user account for IPAD provisioning</td>
<td>Add dial plan and dial rules (optional)</td>
</tr>
<tr>
<td>Configure certificates</td>
<td>Configure automatic provisioning</td>
<td>Add user account for resource provisioning</td>
<td>Configure SIP settings</td>
</tr>
<tr>
<td>Configure SIP settings</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
See these topics for detailed information about each of the tasks.

- “Configure the DNS Service” on page 10
- “Configure Firewalls and Ports” on page 13
- “Install the RealPresence Access Director System” on page 14
- “Configure the RealPresence Resource Manager System” on page 14
- “Configure the RealPresence Access Director System” on page 18
- “Configure the Polycom DMA System” on page 20
- “Supporting Guests in a SIP Environment” on page 21
- “Configure Polycom Endpoint Systems” on page 23
- “Configure the Polycom RealPresence Collaboration Server” on page 24
- “Configure the Polycom RSS™ System” on page 24

Configure the DNS Service

This section describes creating domain name system (DNS) service records to enable this solution.

If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.

**Task 1**

Create a DNS A record on the external DNS server

Create a DNS A (address) record on the external DNS server to map the FQDN of the RealPresence Access Director system to its public IP address.

So if the RealPresence Access Director system has the FQDN name `rpad.example.com`, add an A record as follows.

```
rpad.example.com IN A 192.168.11.175
```

Where:

- `FQDN` = `rpad.example.com`
- `Class` = `IN (Internet)`
- `A` = `Record type`
- `192.168.11.175` = `RealPresence Access Director system IP address`

**Task 2**

Create a DNS SRV record on the external DNS server

Create an SRV record on the external DNS server to map the SRV service address for endpoint provisioning to the FQDN of the RealPresence Access Director system. The SRV record is required by the Auto Find Provisioning Server feature of the RealPresence Mobile system.
So if the RealPresence Access Director system has the FQDN name `rpad.example.com`, add an SRV record as follows.

```plaintext
_cmaconfig._tcp.example.com. IN SRV 0 100 443 rpad.example.com
```

Where:
- `Service = _cmaconfig`
- `Protocol = _tcp`
- `Priority = 0`
- `Weight = 100`
- `Port = 443`
- `Host offering this service = rpad.example.com`

### Task 3  Create DNS A records on the internal DNS server

Create three DNS A records on the internal DNS server as identified in the following sections.

The RealPresence Resource Manager system and the DMA system in the internal network each need one A record to map their FQDNs to the IP address of the internal DNS server. In addition, the RealPresence Access Director system can use a specified FQDN as the provisioning server (access proxy configuration), SIP server, or gatekeeper (SBC setting). For example:

1. If the FQDN of RealPresence Resource Manager system is `rprm.example.com`, and its IP address is 10.22.202.134, create an A record:

   ```plaintext
   rprm.example.com IN A 10.22.202.134
   ```

2. If the FQDN of the DMA system is `dma.example.com`, and its IP address is 10.22.120.126, create an A record:

   ```plaintext
   dma.example.com IN A 10.22.120.126
   ```

3. If the FQDN of RealPresence Access Director system is `rpad.example.com`, and its IP address is 10.22.210.111, create an A record:

   ```plaintext
   rpad.example.com IN A 10.22.210.111
   ```

### Task 4  Create DNS SRV records on the internal DNS server

Create the required DNS SRV records on the internal DNS server as identified below.

The RealPresence Resource Manager system requires a DNS SRV record on the internal DNS server to map the SRV service address to the FQDN of the system. The DMA system requires several DNS SRV records on the internal DNS server to map the SRV service address for several services (SIP/UDP, SIP/TCP, SIP/TLS, H323) to the FQDN of the system.
If the FQDN of the RealPresence Resource Manager system is `rprm.example.com`, and its IP address is `10.22.202.134`, create an SRV record:

```plaintext
_rprmconfig._tcp.example.com. IN SRV 0 100 443 rprm.example.com
```

- If the FQDN of the DMA system is `dma.example.com`, and its IP address is `10.22.120.126`, create SRV records:

```plaintext
_sip._tcp.example.com. IN SRV 0 100 5060 dma.example.com
_sip._udp.example.com. IN SRV 0 100 5060 dma.example.com
_sip._tls.example.com. IN SRV 0 100 5061 dma.example.com
_sip._tcp.example.com. IN SRV 0 100 5061 dma.example.com.
```

### Task 5  Validate DNS settings on the external DNS server

The following steps use the Windows `nslookup` commands as an example. The procedure is similar on Mac and Linux.

1. From a Windows computer located on the Internet network, open a command line.
2. Type `nslookup rpad.example.com` to check the A record of the RealPresence Access Director system. The response should include the corresponding RealPresence Access Director system’s public IP address.
3. Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record. The response should include the FQDN of each RealPresence Access Director system.

### Task 6  Validate DNS settings on the internal DNS server

The following steps use the Windows `nslookup` commands as an example. The procedure is similar on Mac and Linux.

1. From a Windows computer located on the Internet network, open a command line.
2. Type `nslookup rprm.example.com` to check the A record of the RealPresence Resource Manager systems. The response should include the corresponding RealPresence Resource Manager system's IP address.
3. Type `nslookup dma.example.com` to check the A record of the DMA systems. The response should include the corresponding DMA system's IP address.
4 Type `nslookup rpad.example.com` to check the A record of the RealPresence Access Director systems. The response should include the corresponding RealPresence Access Director system’s internal IP address.

5 Type `nslookup -type=srv _cmaconfig._tcp.example.com` to check the SRV record. The response should include the FQDN of RealPresence Resource Manager system.

6 Type `nslookup -type=srv _sip._tcp.example.com` and `nslookup -type=srv _h323cs._tcp.example.com` to check the SRV record. The response should include the FQDN of DMA system.

Configure Firewalls and Ports

Follow these guidelines for configuring your firewalls.

- If you’re not familiar with firewall concepts and administration and your enterprise’s firewall implementation, please consult with someone who is.
- For greater security, Polycom recommends that you disable SSH and Web access connectivity from the Internet, and enable SSH and Web access connectivity from the LAN.

Outside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Configure 1:1 NAT
- Set interface mode to NAT
- Disable H.323 and SIP ALG
- Disable any H.323 helper services on the firewall (for example, Cisco® H323 Fixup).

Inside Firewall Configuration

- Implement a WAN (untrusted) and LAN (trusted) configuration
- Disable H.323 and SIP ALG
- Set interface mode to Route
- Disable the port NAT.
- Disable any H.323 helper services on the firewall (for example, Cisco® H323 Fixup).

For more information on port configuration, refer to Appendix A.
Install the RealPresence Access Director System

Task 1  Perform Basic Installation
Perform the basic installation as documented in the RealPresence Access Director System Getting Started Guide.

Task 2  Configure Network Settings
You must edit the network settings for the RealPresence Access Director system based upon the deployment model you are implementing. For more information about the deployment models, see “RealPresence Access Director System Solution Deployment Models” on page 3. For more information about RealPresence Access Director system network settings, see the Polycom RealPresence Access Director Administrator’s Guide.

To configure the Network Settings

1  See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about the Configuration Wizard. Then go to Admin > Network Settings.

   The General Network Settings that display are the settings configured during initial installation and first-time setup of the system.

2  Click Advanced network settings > Configuration Wizard and configure the network interface settings, binds, and static route settings for the different services (such as signaling, traffic, management).

3  Go to Admin > Time Settings > System time zone and select the time zone of your specific geographic location.

Configure the RealPresence Resource Manager System

The following tasks describe the configuration steps to perform on the RealPresence Resource Manager system to enable RealPresence Access Director system integration and provisioning. They include:

- Add a Site for the RealPresence Access Director System
- Add a Provisioning User Account for the RealPresence Access Director System
- Add a Provisioning User Account for Endpoints

It is assumed here that the RealPresence Resource Manager system is already installed and configured for use.
Add a Site for the RealPresence Access Director System

The RealPresence Access Director system secures a specific network segment or subnet. To accurately characterize and represent that network segment, you must create a site on the RealPresence Resource Manager system that is specifically enabled for the RealPresence Access Director system. Your remote users will be managed through this site.

**To add a site to the RealPresence Resource Manager system**

1. See the *Polycom RealPresence Resource Manager System Operations Guide* for detailed information about adding a site. Then go to Admin > Topology > Sites and add a site.

2. On the General Info tab of the Add Site dialog box, select Site with RPAD. Complete the other fields of the tab as required.

3. On the Subnets tab, add a subnet. Enter the RealPresence Access Director system internal signalling **IP address** and **Mask** (255.255.255.255).

4. Complete the other tabs and fields of the Add Site dialog box as required and finish adding the site.
   - The site is added to the system, and the Add Site Provisioning Details dialog box appears.

5. On the Directory Setting tab, enter the RealPresence Access Director system’s public IP address as **Directory Server**. Complete the other fields of the tab as required.

6. On the Presence Settings tab, enter the RealPresence Access Director system’s public IP address as **Presence Server**. Complete the other fields of the tab as required.

7. On the RPAD Settings tab, configure the general system values for the RealPresence Access Director system deployment.

8. On the RPAD Settings 2 tab, enter the required values.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable IP H.323</td>
<td>Select this if support for H.323 signalling is required for H.323 endpoints.</td>
</tr>
<tr>
<td>Gatekeeper Address</td>
<td>In this solution, the DMA system is the gatekeeper, so enter the DMA system IP address here.</td>
</tr>
<tr>
<td>Enable SIP</td>
<td>Select this if support for SIP signalling is required for SIP endpoints.</td>
</tr>
</tbody>
</table>
To enable remote users with H.323 endpoints:

a. On the H.323 Settings tab, select Enable IP H.323 and in the Gatekeeper Address field, enter the RealPresence Access Director system’s public IP signalling address.

b. Complete the other fields of the tab as required.
To enable remote users with SIP endpoints:

a. On the SIP Settings tab, select Enable SIP and in the Proxy Server and Registrar Server fields, enter the RealPresence Access Director system’s public signaling IP address.

b. Set the Transport Protocol to TLS.

c. Complete the other fields of the tab as required.

11 Complete the other fields of the dialog box as required.

Task 2 Add a Provisioning User Account for the RealPresence Access Director System

To provision a RealPresence Access Director system, the RealPresence Resource Manager system must have a user account dedicated for this purpose. This user account is the Login Name and Password that you enter on the RealPresence Access Director system to enable the integration and provisioning capability.

Because this user account is for system authentication only, the account:

• Should not be a real user account
• Needs only the minimum required user information

To add a provisioning user account to the RealPresence Resource Manager system for this purpose

1 See the Polycom RealPresence Resource Manager System Operations Guide for detailed information about adding a user account. Then go to User > Users > Add.

2 On the General Info tab of the Add New User dialog box, enter the minimum required information, as indicated by an asterisk and then click OK.

Task 3 Add a Provisioning User Account for Endpoints

To provision endpoint systems through the firewall, the RealPresence Resource Manager system must have a user account dedicated for this purpose. This user account is the username and password that you must enter on the endpoint system to enable the integration and provisioning capability.

IMPORTANT
If Device Authentication is enabled on the DMA system, disable Use Endpoint Provisioning Credentials and enter the Common SIP User Name and Common SIP Password, which are in the authentication list configured on the DMA system. For more information, refer to “Enable SIP Device Authentication” on page 20.
To add a user account to the RealPresence Resource Manager system for an endpoint

1. See the Polycom RealPresence Resource Manager System Operations Guide for detailed information about adding a user account. Then go to User > Users > Add.

2. On the General Info tab of the Add New User dialog box, enter the minimum required information, as indicated by an asterisk and then click OK.

3. On the Dial String Reservations tab, enter the SIP URI for the endpoint and then click OK.

Configure the RealPresence Access Director System

Once the RealPresence Resource Manager system has been configured to integrate with and provision the RealPresence Access Director system, you can finish configuring the RealPresence Access Director system.

The following sections describe the tasks to be performed. They include:

- Configure System Certificates
- Configure Automatic Provisioning (Recommended)

See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about each of these tasks. The following sections provide specific information as it relates to this solution.

Task 1 Configure System Certificates

The RealPresence Access Director system is delivered with a self-signed certificate at installation. You can replace the self-signed certificated with signed certificates issued by a certificate authority.

The RealPresence Access Director system certificate must be both a serverauth and clientauth certificate.

You should configure certificates before configuring automatic provisioning of the RealPresence Access Director system and before federating your RealPresence Access Director system with another enterprise. For more information about certificate signing requests and certificates, see the Polycom RealPresence Access Director Administrator’s Guide.

Task 2 Configure Automatic Provisioning (Recommended)

When integrated with a Polycom Management System, the RealPresence Access Director system connects to the RealPresence Resource Manager system to get some of the configuration information you entered when you configured the management system. (See “Configure the RealPresence
Configure the Polycom DMA System

Enable SIP Device Authentication

Device authentication enhances security by requiring devices registering with or calling through the DMA system to provide credentials that the system can authenticate. In turn, the DMA system may need to authenticate itself to an external SIP peer or neighbored gatekeeper.

If your DMA system is peered with other SIP devices, enabling SIP device authentication may cause inbound calls to the DMA system from those SIP peers to fail. Multiple solutions exist for resolving these issues with dial plan and network design. If necessary, please contact your Polycom field representative.

All authentication configurations are supercluster-wide, but note that the default realm for SIP device authentication is the cluster’s FQDN, enabling each cluster in a supercluster to have its own realm for challenges.
To enable SIP authentication for ALL internal and external endpoints:

1. See the Polycom DMA System Operations Guide for detailed information about enabling SIP device authentication. Then go to Admin > Local Cluster > Signaling Settings and in the SIP Settings section, select Enable authentication.

2. To add a device’s authentication credentials to the list of device credential entries that the Call Server checks, click Add and enter the user Name, Password, and Confirm Password credentials.

   These are the credentials you set up in “Add a Provisioning User Account for Endpoints” on page 17. They provide authentication of the endpoint’s provisioning request.

To disable SIP authentication for a specific endpoint:

1. Go to Network > Endpoints.

2. Select the endpoint for which you want to remove authentication.

3. Click Edit.


Supporting Guests in a SIP Environment

To support SIP guest calls, additional settings must be configured on the DMA system and on the RealPresence Access Director system. Polycom recommends the configurations described in the following sections:

- “Configure SIP settings for guests on the Polycom DMA system” on page 21
- “Configure SIP settings for guests on the RealPresence Access Director system” on page 22
- “Configure SIP settings for registered users on the RealPresence Access Director system” on page 23

Task 1 Configure SIP settings for guests on the Polycom DMA system

Your DMA system must be configured with a dial rule prefix that corresponds to the prefix used for guests on the RealPresence Access Director system.
To configure the DMA system to support SIP guest calls

1. See the Configure Signaling section of the Polycom DMA System Operations Guide for detailed information about this process. Then on the DMA system, go to Admin > Local Cluster > Signaling Settings.

2. Add a guest dial rule prefix (SIP Settings > Unauthorized prefixes > Add) and enable Strip prefix.

3. Configure the required information so that it matches the prefix for guest calls added in the RealPresence Access Director system.

4. Go to Admin > Call Server > Dial Rules and add three dial rules to handle the incoming unauthorized guest calls; one for each type of call resolution:
   - Resolve to conference room ID
   - Resolve to virtual entry queue
   - Resolve to external SIP peer

5. Go to Admin > Call Server > Domains and add a domain to the domain list for the host specified for guest port configuration.

Task 2  Configure SIP settings for guests on the RealPresence Access Director system

To configure the RealPresence Access Director system external SIP port 5060 for guests

1. See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring SIP settings. Then on the RealPresence Access Director system, go to Configuration > SIP and H.323 Settings.

2. Enable SIP signaling and then configure external port 5060 for SIP guest users (External Port Settings > Edit) with the required information. In this case:
   - Port name: Defaults to Unencrypted port.
   - Transport: UDP/TCP.
   - Enable Dial string policy and enter a dial string prefix (Prefix of Userinfo) that does not interfere with your dial plan and will be stripped by the DMA system.
   - The host is a domain name change the system can implement. For example, if a SIP guest user calls 8222@polycom.com, but the host is configured as example.com and the prefix is 77, the system will change the users dial string to 778222@example.com.
   - Enable Forbid registration.
To configure the RealPresence Access Director system external SIP port 5061 for guests

1. See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring SIP settings. Then on the RealPresence Access Director system, go to Configuration > SIP and H.323 Settings.

2. Enable SIP signaling and then configure external port 5061 for SIP guest users (External Port Settings > Edit) with the required information. In this case:
   - **Port name**: Defaults to Encrypted port.
   - **Transport**: TLS.
   - Enable **Dial string policy** and enter a dial string prefix (Prefix of Userinfo) that does not interfere with your dial plan and will be stripped by the DMA system.
   - The host is a domain name change the system can implement. For example, if a SIP guest user calls 8222@polycom.com, but the host is configured as example.com and the prefix is 77, the system will change the users dial string to 778222@example.com.
   - Enable **Forbid registration**.

**Task 3** Configure SIP settings for registered users on the RealPresence Access Director system

If you configure the external SIP ports 5060 and 5061 for guest users, you must also add an external SIP port for registered users.

To configure a RealPresence Access Director system non-standard external SIP port to support registered user calls

1. On the RealPresence Access Director system, go to Configuration > SIP and H.323 Settings.

2. Enable SIP signaling and then configure a port for SIP registered users (External Port Settings > Add) with the required information. In this case:
   - **Port number**: Any non-standard port number that is not already in use.
   - **Port name**: RegisteredUser (for example).
   - **Transport**: Polycom suggests using TCP but UDP, UDP/TCP, or TLS may also be used. The transport protocol entered here must match the transport protocol for the RealPresence Access Director system site in the RealPresence Resource Manager system. See “To add a site to the RealPresence Resource Manager system” on page 15.
   - Disable **Forbid registration**.
Configure Polycom Endpoint Systems

This solution supports the Polycom endpoint systems identified in “Products Tested in this Solution” on page 7.

Task 1  Configure Polycom HDX Series Endpoints

Polycom HDX series endpoints do not require any special set up for this solution. Polycom recommends automatic provisioning because it enables easy setup and access to advanced features.

See the Polycom HDX system documentation available at support.polycom.com for more information about configuring the system for automatic provisioning.

Task 2  Configure the Polycom Group Series System

See the RealPresence Group Series 300 or 500 user documentation at support.polycom.com for configuration information.

Task 3  Configure Polycom RealPresence Mobile or Desktop Endpoints

This section includes some specific information for configuring RealPresence Mobile software in this solution. It assumes you have already installed the software on your device.

For more detailed RealPresence Mobile product information, refer to the Help and the Release Notes for the software version you are using, available at support.polycom.com.

Professional Mode Sign-In Settings

Users can choose to use their RealPresence Mobile or Desktop system in Professional Mode. In this mode, the system is automatically provisioned/configured by the RealPresence Resource Manager system. Polycom recommends automatic provisioning because it enables easy setup and access to advanced features.

The product Help describes how users configure their systems for professional mode. When setting up professional mode, the user will need to enter the user name and password configured in “Add a Provisioning User Account for Endpoints” on page 17.
Configure the Polycom RealPresence Collaboration Server

To ensure that a RealPresence Mobile client can send content to a conference, on the RealPresence Collaboration Server, go to Setup > System Configuration > System Flags and set the value of the NUM_OF_INITIATE_HELLO_MESSAGE_IN_CALL_ESTABLISHMENT system flag to at least 3.

For information about adding system flags, see "Manually Adding and Deleting System Flags" in the Polycom RMX System Administrator Guide. After the change, you must restart the RMX system.

Configure the Polycom RSS™ System

Ensure that the Polycom RSS 4000 system is in normal mode, not maximum security mode.

Refer to the Polycom RSS 4000 User Guide for more information about Polycom RSS working modes.
Federation Between RealPresence Access Director Systems Only

This chapter describes how to configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises. In the deployment solution described in this chapter, each division or enterprise must have a RealPresence Access Director system.

In this chapter, we assume you have already performed the standard deployment as documented in Chapter 2, “Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users.”

Federation in a SIP Environment

To configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises in a SIP environment, each division or enterprise must have a RealPresence Access Director system that is configured:

- To trust the other’s certificate
- With mutual TLS enabled
- With a default route to the other’s Real Presence Access Director system.

In addition, the federated enterprises must:

- Have a dial plan to route traffic to and from specific ports using specified protocols
- Directed to the designated port

To support SIP calls from federated divisions or enterprises, perform the following deployment tasks:

- **Create additional DNS SRV records on the external DNS server**
- **Configure the RealPresence Access Director systems to support federated SIP calls**
Configure the Polycom DMA systems to support federated SIP calls

**Task 1**

**Create additional DNS SRV records on the external DNS server**

“Configure the DNS Service” on page 10 describes the basic DNS setup required for this solution. Federating sites requires additional DNS configuration as described here.

- Complete this process on the DNS systems for the two sites being federated.
- If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.

Create an SRV record on the external DNS server (the DNS server configured on the Network Setting page of the RealPresence Access Director system) to map the SRV service address to the FQDN of the RealPresence Access Director system. The SRV record is required by the Auto Find Provisioning Server feature of the RealPresence Mobile system.

So if the RealPresence Access Director system has the FQDN name _rpad.example.com_, add an SRV record as follows.

```
_sips._tcp.example.com. IN SRV 0 0 5080 rpad.example.com.
```

**Task 2**

**Configure the RealPresence Access Director systems to support federated SIP calls**

To configure the federated sites’ RealPresence Access Director systems to support SIP calls

1. See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring SIP settings. Then go to Configuration > SIP and H.323 Settings.

2. Enable SIP signaling and add a port for SIP users (External Port Settings > Add) and configure the required information.
   - Transport protocol must be TLS (mutual TLS)
   - Require certificate from remote endpoint must be selected
   - Enable Forbid registration

Complete this process on the RealPresence Access Director systems for the two sites being federated.
3 Go to Configuration > Federation Settings > Add and configure the required information for the federated sites.
   - Enter the FQDN or IP address of the federated site’s RealPresence Access Director system.

4 Go to Admin > Certificates and verify that the federated site’s certificate is in the Trusted Store.

**Task 3** Configure the Polycom DMA systems to support federated SIP calls

To configure the federated sites’ DMA systems to support federated SIP calls

1 See the Polycom DMA System Operations Guide for detailed information about adding an external SIP peer. Then go to Network > External SIP Peer > Add.

Complete this process on the RealPresence Access Director systems for the two sites being federated.

2 On the External SIP Peer tab, enter the internal signaling IP address of the RealPresence Access Director system as the Next hop address.

3 On the Preliminary tab, set Request URI options to Use original request URI (RR).

4 On the Authentication tab, click Add and add the federated site’s authentication information.

5 Go to Admin > Call Server > Device Authentication and add the federated site’s authentication credentials to the list of device credential entries that your call server should check.

6 Select the Inbound Authentication tab, click Add and add the local system’s authentication information for inbound messages.

7 Select the Shared Outbound Authentication tab, click Add and add the federated site’s authentication information for outbound messages.

8 Go to Admin > Local Cluster > Signaling Settings and in the SIP Settings section, select Enable SIP signaling and Enable authentication.

9 Go to Admin > Call Server > Dial Rules and add a dial rule for federated site’s RealPresence Access Director system that resolves to external SIP peer, so the DMA system can send the INVITE message out to the RealPresence Access Director system.

10 Go to Admin > Call Server > Domains and add the local RealPresence Access Director system to the domain list.
Federation in an H.323 Environment

To configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises in an H.323 environment, each division or enterprise must have a RealPresence Access Director system that is configured:

• With a dial plan to route E.164 aliases properly between the enterprises
• To be directed to the designated port

To support H.323 calls from federated divisions or enterprises, perform the following deployment tasks:

• Configure the RealPresence Access Director systems to support federated H.323 calls
• Configure the Polycom DMA Systems to support federated H.323 calls

Task 1 Configure the RealPresence Access Director systems to support federated H.323 calls

To configure the federated enterprises’ RealPresence Access Director systems to support H.323 calls

1 See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring H.323 settings. Then go to Configuration > SIP and H.323 Settings.

2 Enable H.323 signaling and configure the required information.
   – Gatekeeper (next hop) address is the DMA system IP address
   – CIDR should only include the subnet of internal gatekeeper

3 Go to Configuration > Federation Settings > Add and configure the required information for the federated enterprise.
   – Enter the IP address of the federated site’s RealPresence Access Director system

Generally, you will not need to configure the remote RAS port and H.225 signaling ports. The port used during the call will be returned by the DNS SRV search.
**Task 2**

**Configure the Polycom DMA Systems to support federated H.323 calls**

To configure the federated enterprises’ DMA systems to support H.323 calls

1. See the *Polycom DMA System Operations Guide* for detailed information about adding a neighbored gatekeeper. Then go to **Network > External Gatekeeper > Add** and add the local RealPresence Access Director system as a neighbored gatekeeper identified by its internal signaling address.

2. Go to **Admin > Call Server > Dial Rules** and add a “resolve to external gatekeeper” dial rule for the local RealPresence Access Director system that has been identified as the gatekeeper.

3. Go to **Admin > Call Server > Domains** and add the local RealPresence Access Director system to the domain list.

Complete this process on the RealPresence Access Director systems for both of the enterprises being federated.
Federation Between RealPresence Access Director and Other Systems

This chapter describes how to configure this solution to support calls between endpoint users in two separate but federated (trusted) divisions or enterprises.

In this deployment solution, one of the federated sites has a RealPresence Access Director. The other site has a different session border controller. Supported solutions include:

• Federation in an H.323 Environment with Polycom VBP-E Systems
• Federation in a SIP Environment with Acme Packet

In this chapter, we assume you have already performed the standard deployment for the applicable systems as documented in Chapter 2, “Deploying the Basic RealPresence Access Director System Solution to Support Remote and Guest Users.”

Federation in an H.323 Environment with Polycom VBP-E Systems

In this solution deployment model, two enterprises or divisions are federated. One of the federated enterprise has a RealPresence Access Director system as its access controller along with a DMA system as gatekeeper. The other federated enterprise has a Polycom VBP 5300E as its access controller and either uses an embedded or Polycom CMA system v6.2 gatekeeper.

To support calls between these federated divisions or enterprises, perform the following deployment tasks:

• “Create an additional DNS A record on the external DNS server” on page 34
• “Create additional DNS SRV records on the external DNS server” on page 34
• “Configure the RealPresence Access Director systems to support federated H.323 calls” on page 35
• “Configure the Polycom DMA System to support federated calls” on page 35
• “Configure the CMA system to support federated H.323 calls” on page 36
• “Configure the VBP-5300E system to support federated H.323 calls” on page 36.

Task 1  
Create an additional DNS A record on the external DNS server

“Configure the DNS Service” on page 10 describes the basic DNS setup required for the RealPresence Access Director system in this solution. Federation requires additional DNS configuration as described here.

If you’re not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise’s DNS implementation, please consult with someone who is.

Create a DNS A (address) record on the external DNS server to map the FQDN of the VBP 5300E system to its public (WAN side) IP address.

So if the VBP-E system has the FQDN name `vbp_e.example2.com`, add an A record as follows.

```
vbpe_e.example2.com IN A 192.168.11.100
```

Task 2  
Create additional DNS SRV records on the external DNS server

Each access controller—the RealPresence Access Director system and the VBP 5300E system must have an SRV record on the external DNS server to map the SRV service address to its FQDN.

- Create an SRV record on the external DNS server to map the SRV service address to the FQDN of the RealPresence Access Director system.

  The SRV record is required by the Auto Find Provisioning Server feature of the RealPresence Mobile system.

  So if the RealPresence Access Director system has the FQDN name `rpad.example.com`, add SRV records as follows.

  `._h323ls._udp.example.com. IN SRV 0 0 1719 rpad.example.com.
  _h323cs._tcp.example.com. IN SRV 0 0 1720 rpad.example.com.`

- Create an SRV record on the external DNS server to map the SRV service address to the public IP address of the Polycom VBP-5300E system.

  So if the VBP-E system has the FQDN name `vbpe_e.example2.com`, add SRV records as follows.

  `._h323ls._udp.example2.com. IN SRV 0 0 1719 vbpe_e.example2.com
  _h323cs._tcp.example2.com. IN SRV 0 0 1720 vbpe_e.example2.com`

If you're not familiar with DNS administration, the creation of various kinds of DNS resource records, and your enterprise's DNS implementation, please consult with someone who is.
Task 3 Configure the RealPresence Access Director systems to support federated H.323 calls

To configure the federated enterprises’ RealPresence Access Director systems to support federated H.323 calls

1 See the Polycom RealPresence Access Director Administrator’s Guide for detailed information about configuring H.323 settings. Then go to Configuration > SIP and H.323 Settings.

2 Enable H.323 signaling and configure the following gatekeeper and network settings (External Port Settings > Add).
   - Gatekeeper (next hop) address is the DMA system IP address
   - CIDR should only include the subnet of the internal gatekeeper

The CIDR is used by the RealPresence Access Director system to determine the origin of a call, the internal network or external network. The value of CIDR depends on the local DMA system mode (Routed or Direct).
   * If the local DMA is configured in Routed mode, the CIDR should only include the subnet of the DMA system.
   * If the local DMA system is configured in Direct mode, then the CIDR should include the subnet of the DMA system and local enterprise endpoints.

3 Go to Configuration > Federation Settings > Add and configure the required information for the federated enterprise.
   - Enter the FQDN or IP address of the federated site’s VBP-E system.
   - Complete the other tabs and fields of the dialog box as required

Generally, you will not need to configure the remote RAS port and H.225 signaling ports. The port used during the call will be returned by the DNS SRV search.

Task 4 Configure the Polycom DMA System to support federated calls

To configure the federated enterprises’ DMA system to support federated calls

1 See the Polycom DMA System Operations Guide for detailed information about adding neighbored gatekeeper. Then go to Network > External Gatekeeper > Add and add the local RealPresence Access Director system as a neighbored gatekeeper identified by its internal signaling address.
2 Go to Admin > Call Server > Dial Rules and add a “resolve to external gatekeeper” dial rule for the local RealPresence Access Director system that has been identified as the gatekeeper.

**Task 5  (Conditional)**

**Configure the CMA system to support federated H.323 calls**

If a CMA system v6.2 is the gatekeeper for the federated enterprise using the VBP-E access controller, perform this task. Otherwise, skip to “Task 7 (Conditional)” on page 37.

**To configure the federated enterprises’ CMA system to support federated H.323 calls**

1 See the Polycom CMA System Operations Guide for detailed information about adding neighboring gatekeeper. Then go to Admin > Gatekeeper Settings > Neighboring Gatekeepers and add the RealPresence Access Director system as neighboring gatekeeper.

2 Go to Admin > Server Settings > Network and enter the VBP-E’s LAN interface address as the IPv4 Default Gateway address.

3 Go to Admin > Dial Plan and Sites > Dial Rules and add a Prefix dial rule. Assign it a Routing Action of Route to a trusted neighbor.

4 Go to Trusted Neighbors and select the RealPresence Access Director system as a trusted neighbor.

**Task 6  (Conditional)**

**Configure the VBP-5300E system to support federated H.323 calls**

If a CMA system is the gatekeeper for the federated enterprise using the VBP-E access controller, perform this task. Otherwise, skip to “Task 7 (Conditional)” on page 37.

**To configure the federated enterprises’ VBP-5300E systems to support federated calls when the CMA system is the gatekeeper**

1 See the Polycom VBP System Configuration Guide for detailed information about specifying H.323 settings. Then go to Configuration Menu> VoIP ALG > H.323.

2 Select Gatekeeper mode > LAN/Subscriber-side gatekeeper mode and enter the CMA system’s IP address as the LAN/Subscriber-side GK address.
Task 7
(Conditional)

Configure the VBP-5300E system in Embedded gatekeeper mode to support federated H.323 calls

If the VBP-E is both the access controller and gatekeeper for the federated enterprise or division, perform this task. Otherwise, skip to

To configure the federated enterprises' VBP-5300E systems to support federated calls when the CMA system is the gatekeeper

1. See the Polycom VBP System Configuration Guide for detailed information about specifying H.323 settings. Then go to Configuration Menu> VoIP ALG > H.323.

2. Select Gatekeeper mode > LAN/Subscriber-side gatekeeper mode and enter the CMA system's IP address as the LAN/Subscriber-side GK address.

Federation in a SIP Environment with Acme Packet

To support calls from federated divisions or enterprises when an Acme Packet® Net-Net Enterprise Session Director (ESD) system is in the environment, perform the following configuration.

It is assumed here that the Acme Packet Net-Net ESD system is already installed and configured for standard use.

To configure the Acme Packet Net-Net ESD for federation

1. See the Acme Packet documentation at https://support.acmepacket.com/documentation.asp. Then add two realms (configure terminal; media-manager; realm-config). Configure the following mandatory parameters:

   identifier = B2B-Access
description = For External Connection(Optional)
network-interfaces = s0p0:0

identifier = B2B-Core
description = For Internal Connection(Optional)
network-interfaces = 1p0:0

2. Add two SIP interfaces (configure terminal; session-router; sip-interface). Configure the following parameters:

   state enabled
realm-id B2B-Access
sip-port
   address 192.168.203.2 ACME Server External IP
3 Add two steering pools (configure terminal; media-manager; steering-pool). Configure the following parameters:

```
ip-address 192.168.203.2 ACME Server External IP
start-port 60000
end-port 61999
realm-id B2B-Access

ip-address 192.168.204.2 ACME Server Internal IP
start-port 62000
end-port 63999
realm-id B2B-Core
```

4 Add two local policies (configure terminal; session-router; local-policy). Configure the following parameters:

```
local-policy
from-address *
to-address *
source-realm B2B-Access
state enabled
policy-attribute
    next-hop 192.168.12.4-----DMA IP
    realm B2B-Core

local-policy
from-address *
to-address *
source-realm B2B-Core
state enabled
policy-attribute
    next-hop 10.220.211.112----Another Enterprise IP
    realm B2B-Access
```

5 Save the configuration.
Verifying Deployment

Verifying Access Proxy

To verify functionality and connectivity between the RealPresence Access Director system and the RealPresence Mobile system, and between the RealPresence Access Director system and the RealPresence Resource Manager system:

1. On the RealPresence Mobile device, configure a WiFi network.
   For example, if the RealPresence Access Director public IP address is 192.168.11.175, make sure that the RealPresence Mobile system can access this address.

2. On the RealPresence Mobile device, configure this sign-in setting.
   **Provision Server**: FQDN or public IP address of the RealPresence Access Director system.
   **User Name**: User account login managed by the RealPresence Resource Manager system.
   **Password**: Correct password associated with User Name.

3. Click **Sign in**, and verify that sign-in was successful.

4. On the RealPresence Resource Manager system, go to **ENDPOINT > Monitor view** to check the status of the user.

Verifying SBC

To verify SIP service and H.323 service:

1. Have a user sign into the DMA system and verify that the user registered to the DMA system successfully.

2. Place a call, and verify that the call was established successfully.
3 Place a long call, and verify that the call remained connected.
4 Have the user sign out, and verify that the user was unregistered from the DMA system successfully.

Verifying Certificates

To verify that the administrator installed correct certificates on the RealPresence Resource Manager, RealPresence Access Director, and RealPresence Mobile systems:

1 In the access proxy configuration, select these settings:
   – Require client certificate from the remote endpoint
   – Verify certificate from internal server

2 Have a user sign on to the RealPresence Mobile device, and verify that the user signed on successfully.

3 In SIP settings, select TLS transport, and verify that the user can register and place a call successfully.
Required Ports

Management Ports

The following tables describe the management ports on which the RealPresence Access Director system (RPAD) can listen.

For greater security, Polycom recommends that you disable SSH and Web access connectivity from the WAN, and enable SSH and Web access connectivity from the LAN. If you require the ability to manage the RealPresence Access Director system from the WAN, refer to the following tables for specific requirements.

From the WAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the host managing the RPAD system via HTTPS</td>
<td>Any</td>
<td>TCP</td>
<td>* The RPAD system public management IP address</td>
<td>8443</td>
<td>HTTPS Web connectivity from the WAN client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host managing the Access Director system via SSH</td>
<td>Any</td>
<td>TCP</td>
<td>The RPAD system public management IP address</td>
<td>22</td>
<td>SSH connectivity from the WAN client to RPAD system</td>
</tr>
</tbody>
</table>

* The RPAD system public management IP address refers to the public IP address mapped in the firewall located between the WAN and the RealPresence Access Director system.
## From the LAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the host managing the RPAD system via HTTPS</td>
<td>Any</td>
<td>TCP</td>
<td>* The RPAD system public management IP address</td>
<td>8443</td>
<td>HTTPS Web connectivity from internal client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host managing the RPAD system via SSH</td>
<td>Any</td>
<td>TCP</td>
<td>The RPAD system public management IP address</td>
<td>22</td>
<td>SSH connectivity from internal client to the RPAD system</td>
</tr>
<tr>
<td>IP address of the host sending and SNMP request to the RPAD system</td>
<td>Any</td>
<td>** UDP or TCP</td>
<td>* The RPAD system public management IP address</td>
<td>** 161</td>
<td>SNMP connection from internal server to the RPAD system</td>
</tr>
</tbody>
</table>

* The RPAD system public management IP address refers to the public IP address mapped in the firewall located between the WAN and the RealPresence Access Director system.

** The protocol and DST port depend on the SNMP settings you configure in the RealPresence Access Director system user interface. See the *Polycom RealPresence Access Director System Administrator’s Guide* for details.

## From the RealPresence Access Director System to the WAN

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD system management IP address</td>
<td>123</td>
<td>UDP</td>
<td>IP address of external NTP, if in use</td>
<td>123</td>
<td>NTP service from the RPAD system to the public NTP server</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>30001-64000</td>
<td>TCP</td>
<td>IP address of external OCSP responder, if in use</td>
<td>8080</td>
<td>TCP connectivity from the RPAD system to the public OCSP responder</td>
</tr>
</tbody>
</table>
## Required Ports

### From the RealPresence Access Director System to the LAN

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD system management IP address</td>
<td>30001-64000</td>
<td>UDP</td>
<td>IP address of external DNS, if in use</td>
<td>53</td>
<td>DNS service from the RPAD system to the internal DNS server</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>30001-64000</td>
<td>TCP</td>
<td>IP address of internal OCSP responder, if in use</td>
<td>8080</td>
<td>TCP connectivity from the RPAD system to the internal OCSP responder</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>30001-64000</td>
<td>* UDP or TCP</td>
<td>IP address of internal syslog server, if in use</td>
<td></td>
<td>Syslog service from the RPAD system to the internal syslog server</td>
</tr>
<tr>
<td>RPAD system management IP address</td>
<td>30001-64000</td>
<td>** UDP or TCP</td>
<td>IP address of internal SNMP server, if in use</td>
<td>**162</td>
<td>SNMP connection from the internal server to the RPAD system</td>
</tr>
</tbody>
</table>

* The protocol for syslog service depends on the remote syslog settings you configure in the RealPresence Access Director system user interface. See the Polycom RealPresence Access Director System Administrator’s Guide.

** The protocol and DST port depend on the SNMP settings you configure in the RealPresence Access Director system user interface. See the Polycom RealPresence Access Director System Administrator’s Guide for details.

---

### H.323 and WAN Support

The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s public IP address and the WAN for H.323 support.

If your firewall has an H.323 function that enables it to intercept and alter H.323 messaging, for example, H.323 ALG, you must disable the service. If not disabled, the service may cause call failures due to re-writing of port or IP address information.
From the WAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP of external H.323 devices</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>* RPAD public signaling IP</td>
<td>* 1720</td>
<td>H.225 TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external H.323 devices</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>10001-13000</td>
<td>H.245 TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external H.323 devices</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>* RPAD public media IP</td>
<td>20001-40000</td>
<td>Inbound RTP traffic transport from the WAN to the RPAD system</td>
</tr>
</tbody>
</table>

* RPAD public signaling IP refers to the mapping public signaling IP address in the firewall located between the WAN and the RealPresence Access Director system.

* Port 1720 is the default H.225 TCP port in the RealPresence Access Director system. If you change the port in the RealPresence Access Director system, you must also change it accordingly on the firewall.

* RPAD public media IP refers to the mapping public media IP address in the firewall located between the WAN and the RealPresence Access Director system.

From the WAN to the RealPresence Access Director System: H.323 B2B Calls

If you use the RealPresence Access Director system for H.323 enterprise-to-enterprise calls, the ports listed in the tables below are required in addition to those listed in the preceding table.

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public signaling IP of RPAD or VBP-E in the other enterprise</td>
<td>* 1719</td>
<td>UDP</td>
<td>RPAD public signaling IP</td>
<td>** 1719</td>
<td>Inbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td>Public signaling IP of RPAD or VBP-E in the other enterprise</td>
<td>10001-13000(RPAD-RPAD) 14085-15084(VBP-E-RPAD)</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>** 1720</td>
<td>Inbound H.225 TCP connectivity for B2B call scenarios</td>
</tr>
</tbody>
</table>
### From the RealPresence Access Director System to the WAN: H.323 B2B Calls

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD signaling IP</td>
<td>* 1719</td>
<td>UDP</td>
<td>Public signaling IP of RPAD or VBP-E in the other enterprise</td>
<td>** 1719</td>
<td>Outbound H.225 UDP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td>10001-13000</td>
<td>TCP</td>
<td>Public signaling IP of RPAD or VBP-E in the other enterprise</td>
<td>** 1720</td>
<td>Outbound H.225 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td>10001-13000</td>
<td>TCP</td>
<td>Public signaling IP of RPAD or VBP-E in the other enterprise</td>
<td>10001-13000(RPAD-RPAD) 14085-15084(VBP-E-RPAD)</td>
<td>Outbound H.245 TCP connectivity for B2B call scenarios</td>
</tr>
<tr>
<td></td>
<td>20001-40000</td>
<td>UDP</td>
<td>Public media IP of RPAD or VBP-E in the other enterprise</td>
<td>20001-40000</td>
<td>Outbound RTP traffic transport from RPAD to WAN for B2B call scenarios</td>
</tr>
</tbody>
</table>
The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s internal IP address and the LAN for H.323 support.

**Note:** If your firewall has an H.323 function that enables it to intercept and alter H.323 messaging, for example, H.323 ALG, you must disable the service. If not disabled, the service may cause call failures due to re-writing of port or IP address information.

### From the RealPresence Access Director System to the LAN

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD signaling IP</td>
<td>10001-13000</td>
<td>TCP</td>
<td>IP Address of LAN-based H.323 Gatekeeper(DMA)</td>
<td>* 1720</td>
<td>H.225 TCP connectivity from the RPAD system to the LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
<tr>
<td>RPAD signaling IP</td>
<td>10001-13000</td>
<td>TCP</td>
<td>IP Address of LAN-based H.323 Gatekeeper(DMA)</td>
<td>** 36000-61000</td>
<td>H.245 TCP connectivity from RPAD to LAN-based H.323 gatekeeper (DMA system)</td>
</tr>
</tbody>
</table>

* 1720 is the default H.225 TCP port on a DMA system, so this port must be the same on the RealPresence Access Director system.  
** 36000-61000 is the H.245 port range on a DMA system.
## From the LAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of LAN-based H.323</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD internal</td>
<td>40001-60000</td>
<td>Outbound RTP traffic from the LAN H.323 clients to the RPAD system</td>
</tr>
<tr>
<td>endpoints or MCUs</td>
<td></td>
<td></td>
<td>media IP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* 1720 is the default H.225 TCP port on a DMA system, so this port must be the same on the RealPresence Access Director system.

** 36000-61000 is the H.245 port range on a DMA system.

## From the RealPresence Access Director System to the LAN: H.323 B2B Calls

If you use the RealPresence Access Director system for H.323 enterprise-to-enterprise calls, the ports listed in the tables below are required in addition to those listed in the preceding tables.

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPAD signaling IP</td>
<td>* 1719</td>
<td>UDP</td>
<td>IP address of</td>
<td>** 1719</td>
<td>Inbound H.225 UDP connectivity for B2B scenarios</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the LAN-based</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>H.323 gatekeeper</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(DMA system)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on the local RealPresence Access Director system. If you change it on the local system, you must also change it accordingly on the firewall.

** DST Port 1719 is the default H.225 UDP port on a DMA system, so this port must be the same on the RealPresence Access Director system.
**From the LAN to the RealPresence Access Director System: H.323 B2B Calls**

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>*1719</td>
<td>UDP</td>
<td>RPAD signaling IP address</td>
<td>**1719</td>
<td>Outbound H.225 UDP connectivity for B2B scenarios</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>36000-61000</td>
<td>TCP</td>
<td>RPAD signaling IP address</td>
<td>**1720</td>
<td>Outbound H.225 TCP connectivity for B2B scenarios</td>
</tr>
<tr>
<td>IP address of the LAN-based H.323 gatekeeper (DMA system)</td>
<td>36000-61000</td>
<td>TCP</td>
<td>RPAD signaling IP address</td>
<td>10001-13000</td>
<td>Outbound H.245 connectivity for B2B scenarios</td>
</tr>
</tbody>
</table>

* SRC Port 1719 is the default H.225 UDP port on a DMA system, so this port must be the same on the RealPresence Access Director system.

** DST Ports 1719 and 1720 are the default H.225 ports on the local RealPresence Access Director system. If you change the ports on the local system, you must also change them accordingly on the firewall.
# SIP and WAN Support

The following table describes the required ports for DMZ port-filtering policies between the RealPresence Access Director system’s public IP address and the WAN for SIP support with Access Proxy.

If your firewall has a SIP function that enables it to intercept and alter SIP messaging, for example, SIP ALG, you must disable the service. If not disabled, the service may cause call failures due to re-writing of port or IP address information.

## From the WAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>389</td>
<td>LDAP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>443</td>
<td>HTTPS connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>*5060</td>
<td>SIP TCP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD public signaling IP</td>
<td>*5060</td>
<td>SIP UDP connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>*5061</td>
<td>SIP TLS connectivity from the WAN to the RPAD system</td>
</tr>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD public signaling IP</td>
<td>5222</td>
<td>XMPP connectivity from the WAN to the RPAD system</td>
</tr>
</tbody>
</table>
From the RealPresence Access Director System to the WAN

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP of external SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD public media IP</td>
<td>20001-40000</td>
<td>Inbound RTP traffic transport from the WAN to the RPAD system</td>
</tr>
</tbody>
</table>

*5060 is the default SIP external listening port on RPAD. If you change these external ports or you have other SIP external listening ports on RPAD, these ports must be changed or added accordingly on firewall.*
SIP and LAN Support

The following table describes the required ports for DMZ port-filtering policies between RealPresence Access Director’s internal IP address and the LAN for SIP support with Access Proxy.

If your firewall has an SIP function that enables it to intercept and alter SIP messaging, for example, SIP ALG, you must disable the service. Failure to disable the service may cause call failures due to re-writing of port or IP address information.

From the RealPresence Access Director System to the LAN

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The RPAD system signaling IP address</td>
<td>13001-15000</td>
<td>TCP</td>
<td>IP of LAN-based SIP registrar(DMA)</td>
<td>*5060-5061</td>
<td>SIP TCP (5060) and SIP TLS (5061) connectivity from the RPAD system to the LAN-based SIP registrar (DMA system)</td>
</tr>
<tr>
<td>The RPAD system signaling IP address</td>
<td>**5070</td>
<td>UDP</td>
<td>IP of LAN-based SIP registrar(DMA)</td>
<td>*5060</td>
<td>SIP UDP connectivity from the RPAD system to the LAN-based SIP registrar (DMA system)</td>
</tr>
<tr>
<td>The RPAD system signaling IP address</td>
<td>30001-64000</td>
<td>TCP</td>
<td>IP of LAN-based provisioning server</td>
<td>443</td>
<td>HTTPS connectivity from the RPAD system to the LAN-based provisioning server</td>
</tr>
</tbody>
</table>
From the LAN to the RealPresence Access Director System

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The RPAD system signaling IP address</td>
<td>30001-64000</td>
<td>TCP</td>
<td>IP of LAN-based LDAP server</td>
<td>389</td>
<td>LDAP connectivity from the RPAD system to the LAN-based LDAP server</td>
</tr>
<tr>
<td>The RPAD system signaling IP address</td>
<td>30001-64000</td>
<td>TCP</td>
<td>IP of LAN-based XMPP server</td>
<td>5222</td>
<td>XMPP connectivity from the RPAD system to the LAN-based XMPP server</td>
</tr>
</tbody>
</table>

*5060, 5061 are the default SIP listening ports on DMA, so these ports must be the same as DMA.
**5070 is the default SIP internal ports on RPAD. If you change this internal port on RPAD, this port must be changed accordingly on firewall.

<table>
<thead>
<tr>
<th>SRC IP</th>
<th>SRC Port</th>
<th>Protocol</th>
<th>DST IP</th>
<th>DST Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>*5060</td>
<td>UDP</td>
<td>RPAD signaling IP</td>
<td>**5070</td>
<td>SIP UDP connectivity from the LAN-based SIP registrar (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of the LAN-based SIP registrar (DMA system)</td>
<td>&gt;1023</td>
<td>TCP</td>
<td>RPAD signaling IP</td>
<td>**5070-5071</td>
<td>SIP TCP connectivity from the LAN-based SIP registrar (DMA system) to the RPAD system</td>
</tr>
<tr>
<td>IP address of LAN SIP clients</td>
<td>&gt;1023</td>
<td>UDP</td>
<td>RPAD internal media IP</td>
<td>40001-60000</td>
<td>Outbound RTP traffic from LAN SIP clients to the RPAD system</td>
</tr>
</tbody>
</table>

*5060 is the default SIP listening ports on DMA, so these ports must be the same as DMA.
**5070, 5071 are the default SIP internal ports on RPAD. If you change these internal ports on RPAD, this port must be changed accordingly on firewall.
Network Interface Configurations

The illustrations in this chapter show the RealPresence Access Director system network interface configurations supported in this solution.

Network Interface Configuration Summary

The table below distinguishes which network interface configurations require use of static routes.

<table>
<thead>
<tr>
<th>Network Interface Configuration</th>
<th>Static Routing Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two firewalls—one interface to the outside firewall</td>
<td>No</td>
</tr>
<tr>
<td>Two firewalls—four interfaces to the outside firewall</td>
<td>No</td>
</tr>
<tr>
<td>Two firewalls—one interface to the inside firewall</td>
<td>No</td>
</tr>
<tr>
<td>Two firewalls—four interfaces to the inside firewall</td>
<td>No</td>
</tr>
<tr>
<td>Two firewalls—one interface to the DMZ</td>
<td>Yes</td>
</tr>
<tr>
<td>Two firewalls—four interfaces to the DMZ</td>
<td>Yes</td>
</tr>
<tr>
<td>Single firewall—one interface</td>
<td>No</td>
</tr>
<tr>
<td>Single firewall—four interfaces</td>
<td>No</td>
</tr>
</tbody>
</table>

Legend for Network Interface Configuration Diagrams

- Numbers inside blue circles specify the number of network interfaces required for the specific configuration.
- Network interface names, e.g., eth0 and eth2, indicate the interface being used and serve as examples only.
Network Interface Configurations for Dynamic Routing

Two Firewalls—One Interface to the Outside Firewall

Two Firewalls—Four Interfaces to the Outside Firewall
Two Firewalls—One Interface to Inside Firewall

Two Firewalls—Four Interfaces to Inside Firewall
Single Firewall—One Interface

Single Firewall—Four Interfaces
Network Interface Configurations for Static Routing

Two Firewalls—One Interface to the DMZ

Two Firewalls—Four Interfaces to the DMZ