Networking Changes Required For Your Deployment

This chapter provides a list of the changes you need to make for your system deployment:

- IP addresses required for your system
- DNS configuration changes
- Firewall configuration and port access
- Network routing changes

Networking Checklist For Your System

The networking checklist lists the networking changes required for your system, depending on your company's DNS configuration and whether or not you enable public access (users can host or attend meetings from the Internet or mobile devices).

Choose the appropriate checklist depending on whether you are using automatic system deployment (recommended for 50, 250, or 800 user deployments) or manual system deployment (required for a 2000 user deployment).

- All virtual machines, including the Internet Reverse Proxy, are in your internal network (easiest configuration for your system)
    - Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines, on page 3
    - Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines, on page 5
- Non-split-horizon DNS (the most common DNS configuration for companies)
    - Networking Checklist for an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS, on page 8
    - Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS, on page 11
- Split-horizon DNS
    - Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS, on page 14
    - Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS, on page 16
- Systems without public access
    - Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access, on page 19
    - Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access, on page 21

Networking Checklist for an Installation or Expansion With an Automatic Deployment, Public Access, and All Internal Virtual Machines

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your internal network.
- Ensure that the ESXi hosts for all your virtual machines (including the Internet Reverse Proxy) are managed from the same VMware vCenter.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	Internal (may be on the same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the public VIP address)	Internal (same subnet as the Internet Reverse Proxy) **Note** This IP address must be publicly routable.	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	Internal—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server with the hostnames and IP addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, if applicable) virtual machines.

Although it is not recommended, we do also support placing all of your virtual machines (Internet Reverse Proxy and internal) on the same subnet. See Port Access When All the Virtual Machines Are in the Internal Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24

Task	Compare These IP Addresses
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet. **Note** As you are deploying all your system virtual machines internally (the Internet Reverse Proxy is not in the DMZ), then this subnet must be in the internal network.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist for an Installation or Expansion With a Manual Deployment, Public Access, and All Internal Virtual Machines

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your internal network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	Internal (may be on the same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the public VIP address)	Internal (same subnet as the Internet Reverse Proxy) **Note** This IP address must be publicly routable.	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	Internal—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines.

Although it is not recommended, we do also support placing all of your virtual machines (Internet Reverse Proxy and internal) on the same subnet. See Port Access When All the Virtual Machines Are in the Internal Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet. **Note** As you are deploying all your system virtual machines internally (the Internet Reverse Proxy is not in the DMZ), then this subnet must be in the internal network.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist for an Installation or Expansion With Automatic Deployment, Public Access, and a Non-Split-Horizon DNS

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the public VIP address)	DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>

Task	Example
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist For an Installation or Expansion With Manual Deployment, Public Access, and a Non-Split Horizon DNS

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the public VIP address)	DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server with the hostname and IP address for the Internet Reverse Proxy virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server with Administration site URL and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address>
Update your DNS server with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist For an Installation or Expansion With Automatic Deployment, Public Access, and a Split-Horizon DNS

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to two VIP addresses) • internal users—private VIP address • external users—public VIP address	• Internal users—Internal (same subnet as Admin virtual machine) • External users—DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Update your DNS server (that enables internal lookup) with the hostname and IP address for the DMZ virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server (that enables internal lookup) with WebEx site URL, Administration site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Update your DNS server (that enables external lookup) with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin and Media, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks	• Internal Subnet <internal-subnet>/24 • DMZ Subnet <DMZ-subnet>/24

Task	Compare These IP Addresses
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist for an Installation or Expansion with Manual Deployment, Public Access, and a Split-Horizon DNS

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.
- Ensure that the Internet Reverse Proxy virtual machines are in your DMZ network.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Internet Reverse Proxy	DMZ (but may use NAT with a private IP address)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to two VIP addresses) • internal users—private VIP address • external users—public VIP address	• Internal users—Internal (same subnet as Admin virtual machine) • External users—DMZ (same subnet as the Internet Reverse Proxy)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Internet Reverse Proxy (if applicable)	DMZ—same subnet as the primary system's Internet Reverse Proxy (but may use NAT with a private IP address)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Update your DNS server (that enables internal lookup) with the hostname and IP address for the DMZ virtual machine.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Update your DNS server (that enables internal lookup) with WebEx site URL, Administration site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Update your DNS server (that enables external lookup) with WebEx site URL and Public VIP address information.	• <WebEx-site-URL> <Public-VIP-address>

Firewall Configuration

For security reasons, Cisco recommends that you place the Internet Reverse Proxy in a separate subnet from the internal (Admin, Media and Web, if applicable) virtual machines. See Port Access With an Internet Reverse Proxy in the DMZ Network, on page 25.

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Enable L3 (Layer 3) routing between the internal and DMZ networks for the following virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Ensure that the Public VIP address and the Internet Reverse Proxy virtual machines are on the same subnet.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Ensure that the Private VIP address and internal virtual machines (Admin virtual machine and if applicable, the Media and Web virtual machines) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Networking Checklist for an Installation or Expansion with Automatic Deployment and No Public Access

Virtual Machine Deployment

In an automatic deployment, we deploy all the virtual machines (other than the Admin virtual machine) for you. You may choose an automatic deployment if you are deploying a 50, 250, or 800 user system.

- Ensure that the Media virtual machine (if applicable) is on the same subnet as the Admin virtual machine.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media virtual machine.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Update your DNS server with Administration site URL, WebEx site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Firewall Configuration

Make the following changes to your firewalls.

Task	Example
Configure all the firewalls inside your internal network to permit web browsers to access the Private VIP address.	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Ensure that the Private VIP address and internal virtual machines (Admin virtual machine, and Media virtual machine, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Networking Checklist For an Installation or Expansion With Manual Deployment and No Public Access

Virtual Machine Deployment

In a manual deployment, you create all the virtual machines for your system using the OVA wizard from your vSphere client. You then install your system using a manual deployment.

You must choose a manual deployment if you are deploying a 2000 user system.

- Ensure that any additional internal virtual machines (Media and Web, if applicable) are on the same subnet as the Admin virtual machine.

Required IP Addresses

Description	Network Location	IP Address
Real IP address of the Admin virtual machine	Internal	
Real IP address of the Media virtual machine (if applicable)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	

Description	Network Location	IP Address
Real IP address of the third Media virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Real IP address of the second Web virtual machine (2000 user system only)	Internal (same subnet as Admin virtual machine)	
Administration URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
WebEx site URL (used exclusively by the system. Maps to the private VIP address)	Internal (same subnet as Admin virtual machine)	
Real IP address of the HA Admin virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Media virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	
Real IP address of the HA Web virtual machine (if applicable)	Internal (same subnet as primary system's Admin virtual machine)	

DNS Configuration

Make the following changes to your DNS configuration.

Note There are some limitations for the hostname portion of the WebEx site URL and the Administration site URL. For a list of the words that you may not use, see WebEx Site and WebEx Administration URLs, on page 23.

Task	Example
Update your DNS Server (that enables internal lookup) with the hostnames and IP Addresses for the internal virtual machines: Admin virtual machine and if applicable, the Media and Web virtual machines.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Task	Example
Update your DNS server with Administration site URL, WebEx site URL, and Private VIP address information.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

Firewall Configuration

Make the following changes to your firewalls.

Task	Example
Configure all the firewalls inside your internal network to permit web browsers to access the Private VIP address.	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

Network Routing Configuration

Make the following changes to your network routing.

Task	Compare These IP Addresses
Ensure that the Private VIP address and internal virtual machines (Admin, and Media and Web, if applicable) are on the same subnet.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

WebEx Site and WebEx Administration URLs

WebEx Site URL

End users access the WebEx site URL to host or attend meetings. This URL resolves to either the private VIP address or the public VIP address, depending on whether or not you are using a split-horizon DNS.

- Resolves to the public VIP address for all users, when you do not have “split-horizon” DNS.
- Resolves to the public VIP address for external users when you have split-horizon DNS.
- Resolves to the private VIP address for internal users when you have split-horizon DNS.

WebEx Administration URL

Administrators access the WebEx Administration URL to configure, manage, and monitor the system. This URL resolves to the private VIP address.

Names for the WebEx Site and WebEx Administration URLs

You may choose almost any names for these URLs, comprising all lowercase characters. However, you cannot use the following as the hostname in the site URLs:

- the same name as the hostnames for any of the virtual machines comprising the system
- authentication
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-client-services
- emails
- maintenance
- manager
- orion
- oriondata
- oriontemp
- nbr
- npp
- probe
- reminder
- ROOT
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- version

- WBXService
- webex

Port Access When All the Virtual Machines Are in the Internal Network

This section describes the port access required in the external firewall when all the system virtual machines (Admin, and if applicable, Media, Web, and Internet Reverse Proxy) are in the internal network. This is the Internal Internet Reverse Proxy network topology.

Note The Web node and Admin node send SMTP requests to the configured mail server. If there is a firewall between the internal Web and Admin virtual machines and the mail server, the SMTP traffic may be blocked. To ensure mail server configuration and mail notification work properly, port 25 or 465 (secure SMTP port number) must be open between the mail server and the Web and the Admin virtual machines.

Port Access in the External Firewall

If you have enabled public access, then the following ports are open inbound directly from the Internet to the Internet Reverse Proxy virtual machines in the internal network:

Important Ensure that the firewall or any load balancing solution redirects requests to the ports listed below to ensure end users can host and join meetings successfully.

- TCP Port 80 to the public virtual IP (VIP) address
- TCP Port 443 to the public virtual IP (VIP) address

Port Access With an Internet Reverse Proxy in the DMZ Network

This section describes the port access required in the internal and external firewalls when you have internal virtual machines (Admin, and if applicable, Media and Web) in the internal network, and the Internet Reverse Proxy in the DMZ network.

Configure access control lists (ACLs) on the switch that permits traffic to the ESXi hosts for the system's virtual machines.

Port Access in the External Firewall

If you have enabled public access, then the following ports are open inbound from the Internet to the Internet Reverse Proxy virtual machines in the DMZ:

Important Ensure that the firewall or any load balancing solution redirects requests to the ports listed below to ensure end users can host and join meetings successfully.

Note Cisco strongly recommends that you open port 80 (http) in addition to port 443 (https), to simplify the end user experience (in a browser, users enter the WebEx site URL without having to remember whether it is http or https. However, for this product, the actual network traffic always flows over port 443 (SSL encrypted https).

Restriction Configure TCP port 64700 on the Internet Reverse Proxy to deny any requests that come to the public VIP address. In the external firewall, you will limit access to this port for requests only from the Admin virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	443	Any external clients	Public VIP (Eth1) of the Internet Reverse Proxy	External clients accessing the WebEx site URL using https. TCP connections are initiated from the external client machines to the Internet Reverse Proxy virtual machines.
TCP	80	Any external clients	Public VIP (Eth1) of the Internet Reverse Proxy	External clients accessing the WebEx site URL using http. TCP connections are initiated from the external client machines to the Internet Reverse Proxy virtual machines.
UDP	53	Real IP (Eth0) of the Internet Reverse Proxy	DNS server	This is needed if you have a firewall between the virtual machines and the DNS server, for your system to deploy and operate successfully.

Port Access in the Internal Firewall

The following ports must be open when the Internet Reverse Proxy is in the DMZ network. If you have restrictions on connections from the internal network to the DMZ network, then the following table applies. Allow TCP connections *outbound* from the internal network to the DMZ network segment on the following ports.

Note No TCP connections need to be allowed from the DMZ segment in to the internal network for this product to work properly.

Note UDP port 10162 is the only port that is open inbound from the DMZ to the internal virtual machines. This port is required for monitoring of the Internet Reverse Proxy by the system.

Note Using iptables or access control lists (ACLs), configure the firewall so that connections to port 64616 only come from the Admin virtual machine.

Note The Web node and Admin node send SMTP requests to the configured mail server. If there is a firewall between the internal Web and Admin virtual machines and the mail server, the SMTP traffic may be blocked. To ensure mail server configuration and mail notification work properly, port 25 or 465 (secure SMTP port number) must be open between the mail server and the Web and the Admin virtual machines.

Note Especially when the Internet Reverse Proxy is in the DMZ network, allow Internet Control Message Protocol (ICMP) echo requests and replies. Otherwise, the Internet Reverse Proxy detect and the DNS server reachability validation may fail if the ICMP echo reply is not received.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64001	All internal virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed by the internal virtual machines for establishing reverse connections to the Internet Reverse Proxy. TCP connections are established from the internal virtual machines to the Internet Reverse Proxy virtual machines.
TCP	7001	All internal virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed by the internal virtual machines for establishing reverse connections to the Internet Reverse Proxy. TCP connections are initiated from the internal virtual machines to the Internet Reverse Proxy virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64616	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed for bootstrapping the Internet Reverse Proxy. TCP connections are initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines. **Note** Using iptables or access control lists (ACLs), configure the firewall so that connections to port 64616 only come from the Admin virtual machine.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	64700	Admin virtual machines (Eth0 IP)	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed to collect logs from the Internet Reverse Proxy. TCP connections are initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines. **Note** Limit access to this port on all Cisco WebEx Meetings Server virtual machines only to other Cisco WebEx Meetings Server virtual machines with firewall rules.
TCP	22	Any internal client machines	Real IP (Eth0) of the Internet Reverse Proxy virtual machines	This is needed for troubleshooting the Internet Reverse Proxy virtual machines using a Remote Support Account.
TCP	443	Any internal client machines	Private VIP (Eth1) of the Admin virtual machines	Internal users accessing the WebEx site URL using https. TCP connections are established from the internal client machine to the Admin virtual machine.

Protocol	Port	Source	Destination	Why It Is Needed
TCP	65002	Any internal client machines	Any internal client machines	Controls network traffic between internal virtual machines
TCP	65102	Any internal client machines	Any internal client machines	Controls network traffic between internal virtual machines
TCP	80	Any internal client machines	Private VIP (Eth1) of the Admin virtual machines	Internal users accessing the WebEx site URL using http. TCP connections are established from the internal client machine to the Admin virtual machine.
TCP	10200	Any internal client machines	Real IP (Eth0) of the Admin virtual machines	This is needed for the initial system deployment. TCP connections are established from the internal client machines to the Admin virtual machines.
UDP	161	Real IP (Eth0) of the Admin virtual machines	Real IP (Eth0) of the Internet Reverse Proxy	Needed to allow SNMP GET requests to be sent from the Admin virtual machines to the Internet Reverse Proxy virtual machines. The UDP connection is initiated from the Admin virtual machines to the Internet Reverse Proxy virtual machines.

Protocol	Port	Source	Destination	Why It Is Needed
UDP	10162	Real IP (Eth0) of the Internet Reverse Proxy	Real IP (Eth0) of the Admin virtual machines	Needed to allow SNMP traps and information to be sent from the Internet Reverse Proxy virtual machines to the Admin virtual machines. The UDP connection is initiated inbound from the Internet Reverse Proxy to the Admin virtual machines.
UDP	53	All internal virtual machines (Eth0 IP)	DNS server	This is needed if you have a firewall between the virtual machines and the DNS server, for your system to deploy and operate successfully.

VMware vCenter Ports

These are some of the ports that are used during the deployment of Cisco WebEx Meetings Server. Once the deployment completes, you may optionally close any ports that were opened solely for the deployment.

TCP Port 443 should be open, in both directions, between vCenter and the Admin virtual machine for secure https management during an automatic system deployment. The Admin virtual machine uses this port to provide vCenter credentials to deploy the virtual machines automatically in vCenter.

The ports listed below are used for communication between the ESXi host and vCenter. If the ESXi host and vCenter are connected to a *separate management network*, you may not need to open these ports through the firewall. For a complete list of ports used by vCenter and the ESXi host, see your VMware documentation.

- UDP/TCP Port 902 in both directions between vCenter and the ESXi hosts for vCenter management
- (Optional) TCP Port 22 from the vSphere client to the ESXi hosts for SSH management
- UDP Port 514 from the ESXi hosts for your system to the internal syslog
- TCP Port 5989 in both directions between vCenter and the ESXi hosts for XML management

Cisco WebEx Meeting Center Ports

These ports are used for communication between Cisco WebEx Meeting Center and Cisco WebEx Meetings Server.

- The UDP ports used for internal clients for audio and video data transmission between UDP and SSL include:
  - For 50 user systems, use UDP port 9000
  - For 250 user systems, use UDP ports 9000, 9001, 9002, 9003
  - For 800 user systems, use UDP ports 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009
  - For 2000 user systems, use UDP ports 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007
- With the appropriate network settings, internal media servers allow connections through any port used by Meeting Center.
- The Internet Reverse Proxy only accepts connections from Meeting Center through TCP Ports 80 and 443.

Using NAT With Your System

Cisco supports Network Address Translation (NAT) traversal with this product for virtual machine IP addresses and for the virtual IP addresses (Public and Private VIPs) that are used in your system.

Note For more information about NAT, see http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

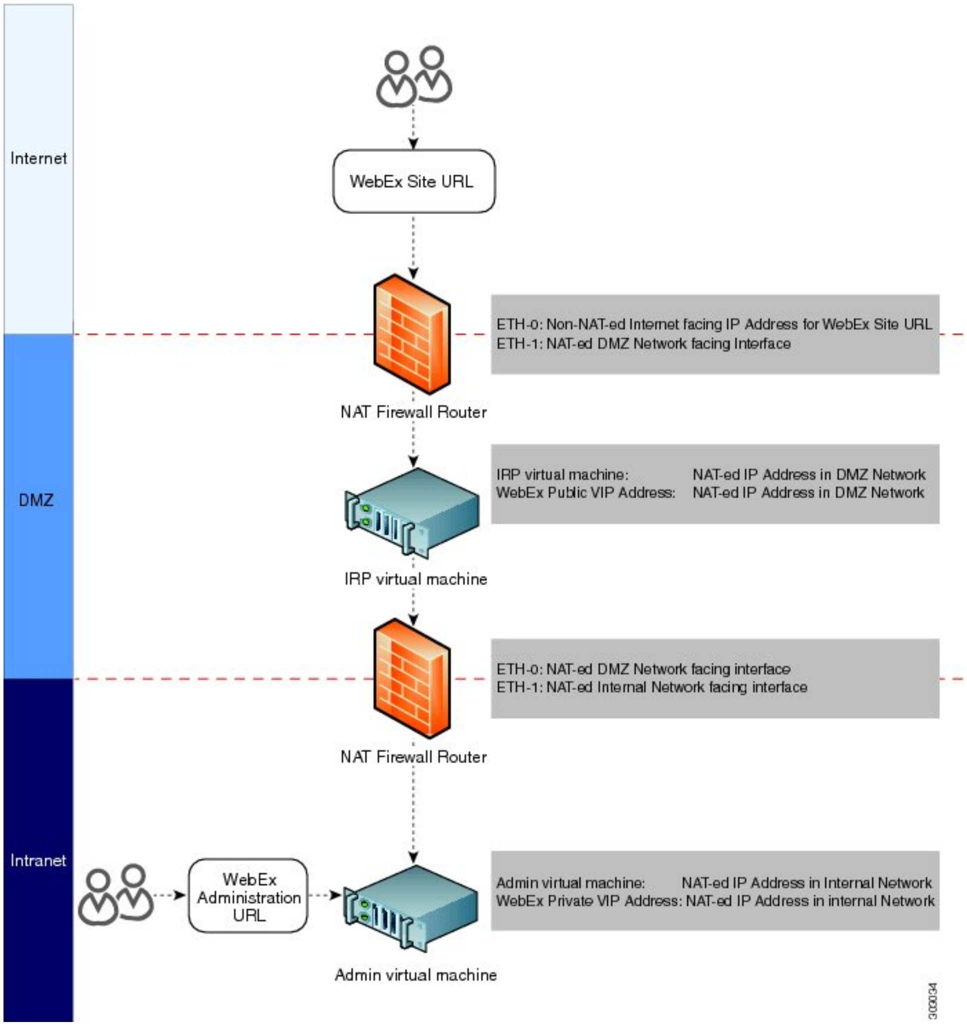
The following schematic diagram illustrates a typical NAT traversal for a 50 user system without HA. By using NAT, you can reduce the number of *public IP addresses* required for the product to just one IP address, instead of two (or three if you deploy HA). You may also deploy similar NAT deployments as long as these meet the overall system requirements.

Note The use of multiple NATs and firewalls tends to increase latency, affecting the quality of real time-traffic for users.

Important When using multiple NAT domains, then routing between these various NAT domains may be challenging. However, you may use NAT-ed IP addresses as long as the following requirements are met:

- All the virtual machines in the system may use NAT-ed IP addresses.
- The Internet Reverse Proxy virtual machine IP address must be reachable by the Admin virtual machine in the internal network.
- The public VIP address itself does not need to be publicly visible, but it must be translatable from the Internet.
- When deploying public access, the WebEx site URL must be mapped to an Internet-visible IP address. This Internet-visible IP address must be accessible by external users and *also* map to the public VIP address you configure during the system deployment.

  You may choose to make the public VIP address visible from the Internet. If you choose not to make it publicly visible, then it must be translatable from the Internet.


Internet
DMZ
Intranet
WebEx Site URL
NAT Firewall Router
ETH-0: Non-NAT-ed Internet facing IP Address for WebEx Site URL
ETH-1: NAT-ed DMZ Network facing Interface
IRP virtual machine: NAT-ed IP Address in DMZ Network
WebEx Public VIP Address: NAT-ed IP Address in DMZ Network
IRP virtual machine
NAT Firewall Router
ETH-0: NAT-ed DMZ Network facing interface
ETH-1: NAT-ed Internal Network facing interface
WebEx Administration URL
Admin virtual machine
Admin virtual machine: NAT-ed IP Address in Internal Network
WebEx Private VIP Address: NAT-ed IP Address in internal Network
303034

In the diagram, an external user accesses the WebEx site to join or host a meeting. Following a DNS lookup, the IP address for the WebEx site is the NAT public IP address (Eth0). This NAT public IP address is for the external NAT firewall router (Firewall and NAT router 1), between the external network and the DMZ network.

The firewall router receives this request from the external user, and internally routes the request to the NAT private IP address for the router (Eth1, exposed to the DMZ network). Eth1 then sends the request to the public VIP address (also a NAT IP address in the private networking segment for the WebEx site).

You may use NAT IP addresses for the public VIP address, and the Internet Reverse Proxy IP addresses. The only NAT public IP address is the Eth0 IP address for the NAT firewall router.

Note To ensure this NAT firewall router (between the Internet and DMZ network) routes the incoming packet correctly, set port mapping configuration on the NAT device, or apply other similar mechanisms to ensure the packet is routed correctly to the public VIP address and the Internet Reverse Proxy.

There is usually a second internal NAT firewall router between the DMZ network and the internal network. Similar to the external NAT firewall router, Eth0 is a DMZ NAT private IP address and is an interface to the DMZ network. Eth1 is also a NAT private IP address that is an interface to the internal network.

You may use NAT IP addresses for the private VIP address and the Admin virtual machine IP addresses.

Forward Proxies

If your network topology includes forward proxies, they *must meet specific requirements* for the Internet Reverse Proxy to work properly. See "Use of Forward Proxies in Your System" in the *Cisco WebEx Meetings Server Troubleshooting Guide* for complete details.