Networking Topology For Your System

End user experience with Cisco WebEx Meetings Server is of a web site, that users access to schedule and join meetings. A special aspect of this web site is real-time conferencing elements that facilitate online meetings.

This chapter describes the different networking topologies supported for this product, including the advantages and disadvantages of each. Select the one that best meets your needs and your network deployment. However, if you want mobile users to attend meetings, then select a network topology that includes the Internet Reverse Proxy virtual machine that enables public access.

Recommended Network Topology

Cisco WebEx Meetings Server comprises two groups of virtual machines: the internal virtual machines and the Internet Reverse Proxy virtual machines. All systems must comprise one or more internal virtual machines. The Internet Reverse Proxy is required only for systems where external users can host or attend meetings from the Internet and mobile devices. Without an Internet Reverse Proxy, only internal and VPN users can host or join meetings.

Internal Virtual Machines

Internal virtual machines refer to the Admin virtual machine, and if applicable, the Media and Web virtual machines.

- The internal virtual machines *must* be on a single, common VLAN or subnet. During the system deployment, you will see error messages if your IP address assignments violate this rule. The system design assumes that all the internal virtual machines, including any HA virtual machines, are connected

together on a local LAN, offering high bandwidth, negligible packet loss, and latency under 1 ms, between these virtual machines. The Cisco WebEx Meetings Server system is not designed to be split between multiple data centers.

- Cisco recommends placing all the internal virtual machines on the same Ethernet switch (usually on the same rack as the virtual machines) with a minimum throughput of
  - 1 Gbps for 50 user and 250 user systems
  - 10 Gbps for 800 user and 2000 user systems

  for links between the edge and core switches. Network latency must be less than 1 ms.

  Note On the Internet Reverse Proxy, the NIC sees double the network traffic of other devices because the connections go through it twice, inbound and outbound.

  Voice, data, video and the SAN all rely on the network bandwidth. It is critical to deploy a network that is capable of handling the required load.
- If you decide instead to place the virtual machines on different Ethernet switches within the same datacenter, then your network *must meet* the requirements listed in this section. In this situation, the switch-to-switch trunk must meet the same networking characteristics as the L3 latency and throughput for a single physical switch.

For additional information on systems with HA, see Redundant Network in HA Deployments, on page 2.

Internet Reverse Proxy Virtual Machines

- The Internet Reverse Proxy virtual machines share the same general networking requirements as the internal virtual machines. For the non-split-horizon and split-horizon DNS configuration, the Internet Reverse Proxy virtual machines are deployed in your DMZ network and not the internal network.
- Because it is common to separate the internal virtual machines from the Internet Reverse Proxy virtual machines on different racks, servers, and ESXi hosts, Cisco recommends:
  - 50 and 250 user systems—dual redundant 1 Gigabit Ethernet links between the DMZ switches and the switches used by the internal virtual machines.
  - 800 and 2000 user systems—dual redundant 10 Gigabit Ethernet links between the DMZ switches and the switches used by the internal virtual machines.

Redundant Network in HA Deployments

- The redundant (HA) virtual machines must be co-located in the same data center with the primary virtual machines. All these virtual machines must be on the same VLAN or subnet. The speed and latency requirements for connectivity between the primary and HA components are the same as defined previously for the primary virtual machines.

Important Cisco does not recommend splitting the primary and redundant (HA) components of the system between data centers.

- Connectivity between all the internal virtual machines, both primary and HA, must be fully redundant, so that the failure of a switch or network link will not sever the connectivity between the primary and HA components. To achieve this redundancy, each host server should have dual redundant connections to a pair of Ethernet switches (that is, a connection to switch A plus a connection to switch B).
- The primary and redundant (HA) Internet Reverse Proxy virtual machines must be on a common VLAN or subnet (typically not the same subnet as the internal virtual machines). Connectivity between these two Internet Reverse Proxy virtual machines should be fully redundant, in the same manner as the internal virtual machines.

Different Types of Network Topology For Your System

This product supports the following network topologies:

- Internal Internet Reverse Proxy Network Topology, on page 3
- Non-Split-Horizon Network Topology, on page 4
- All Internal Network Topology, on page 5
- Split-Horizon Network Topology, on page 6

Note If your network topology includes forward proxies, they must meet specific requirements for the Internet Reverse Proxy to work properly. See the *Cisco WebEx Meetings Server Troubleshooting Guide* for complete details.

Internal Internet Reverse Proxy Network Topology

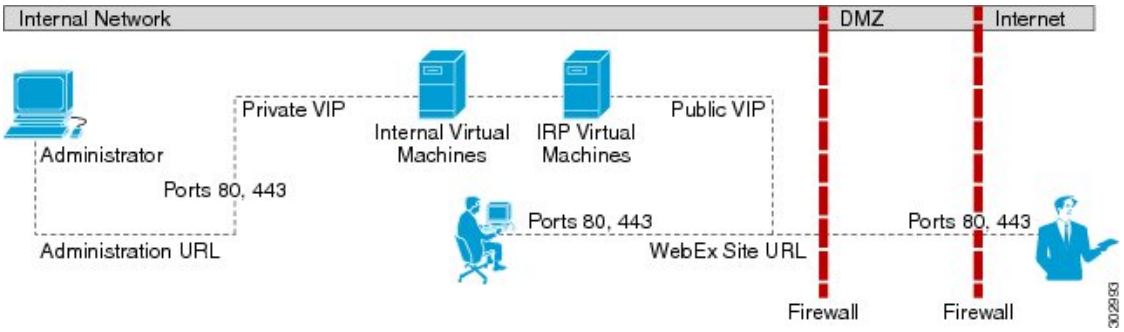
This section describes the network topology when all the virtual machines in your system, including the Internet Reverse Proxy, are in the same internal network.

Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

Note If you are using automatic deployment, then the ESXi hosts for all your virtual machines (including the Internet Reverse Proxy) must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of an all internal Internet Reverse Proxy network topology.



Note For a complete list of the port access required for this deployment, see Port Access When All the Virtual Machines Are in the Internal Network.

Advantages of an All Internal Internet Reverse Proxy Network Topology

- Provides lower latency as there are fewer network hops between the virtual machines.
- Compared with the non-split-horizon network topology, there are no virtual machines in the DMZ.
- Compared with the non-split-horizon network topology, the network traffic for internal users will not connect through the DMZ to host or attend meetings.

Disadvantages of an All Internal Internet Reverse Proxy Network Topology

- Public access (allowing external users to access the system) requires opening inbound ports (80 and 443) directly from the Internet to the internal network.

Non-Split-Horizon Network Topology

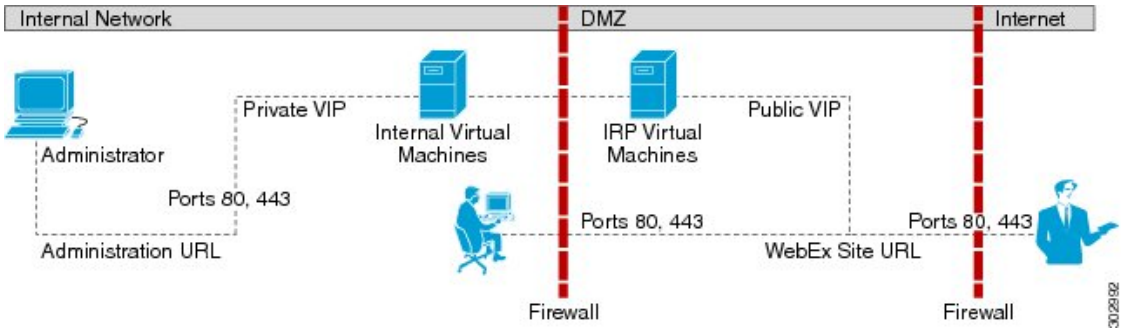
This section describes the network topology when you have a non-split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the WebEx site URL using the private VIP address. External users (outside the firewall) access the WebEx site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the WebEx site URL using the public VIP address.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of a non-split-horizon network topology.



Note For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network.

Advantages of a Non-Split-Horizon Network Topology

- Tight control on the traffic that comes in and goes out of a network.
- Addresses more common, simple DNS network requirements.

Disadvantages of a Non-Split-Horizon Topology

- Complex setup, but not as complex as the split-horizon network topology.
- Internal traffic is directed to the DMZ network. All network traffic from the Internet as well as from the internal (private network) will go to the Internet Reverse Proxy in the DMZ network, then come back to the internal virtual machines.
- Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.
- Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.
- Of the three network topologies, this configuration most affects network performance, since all of the meetings load is through the Internet Reverse Proxy. Because there are multiple hops, network latency is affected as well.

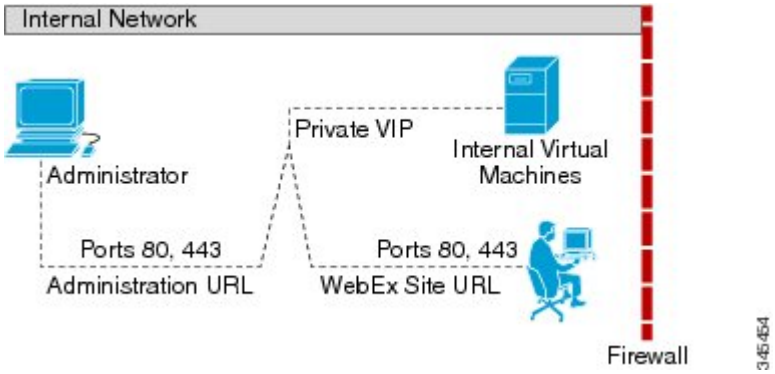
All Internal Network Topology

This section describes the network topology when all the virtual machines in your system are in the same internal network. There is no public access; only internal and VPN users can host or join meetings.

Note If you are using automatic deployment, then the ESXi hosts for all your virtual machines must be managed from the same VMware vCenter. This vCenter information is required during an automatic system deployment.

You will define the Administration URL, the WebEx Site URL and the private VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of an all internal network topology.



Advantages of an All Internal Network Topology

- Provides lower latency as there are fewer network hops between the virtual machines.

Disadvantages of an All Internal Network Topology

- There is no public access (allowing external users to access the system) and no access for mobile users.

Split-Horizon Network Topology

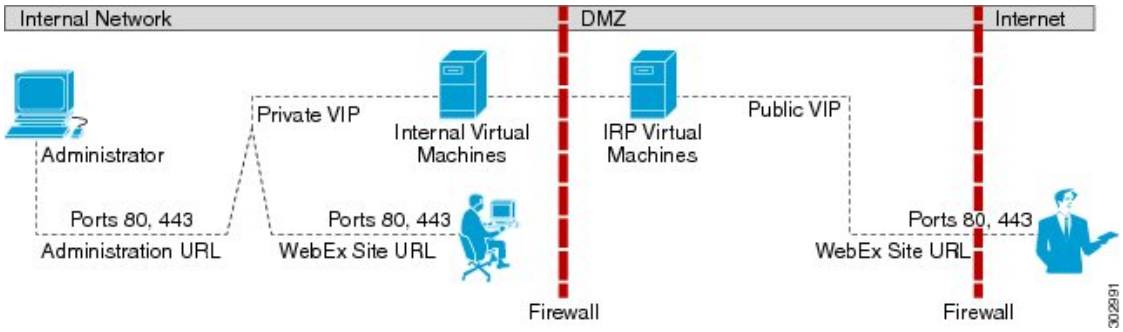
This section describes the network topology when you have a split-horizon DNS. The internal virtual machines (Admin, and if applicable, Media and Web) are in the internal network, and the Internet Reverse Proxy is in the DMZ network.

Note This configuration permits users to sign in and join meetings securely from the Internet without a VPN connection.

For this product, the primary difference between a split-horizon and a non-split-horizon network topology is that for a split-horizon system, internal users access the WebEx site URL using the private VIP address. External users (outside the firewall) access the WebEx site URL using the public VIP address. For a non-split-horizon network, all users (internal and external) access the WebEx site URL using the public VIP address.

You will define the Administration URL, the WebEx Site URL, the private VIP address, and the public VIP address during the deployment of your system. For more information about these terms, and when you provide them, see the Installation section of the *Cisco WebEx Meetings Server Administration Guide*.

This is a schematic diagram of a split-horizon network topology.



Note For a complete list of the port access required for this deployment, see Port Access With an Internet Reverse Proxy in the DMZ Network.

Advantages of a Split-Horizon Network Topology

- Tight control on the traffic that comes in and goes out of a network.
- There is a separation of network traffic hitting the system, enabling a more distributed spread of the load.

  The traffic coming in from the Internet will go to the Internet Reverse Proxy. The traffic coming from the internal (private network) will go directly to the internal virtual machines (Admin, and if applicable, Media and Web).
- Performance and network latency is better than a non-split-horizon DNS, but worse than an all internal network topology.

Disadvantages of a Split-Horizon Topology

- Of the three different network topologies, this is the most complex setup.
- Requires sophisticated DNS mapping.
- Requires more ports to be opened in the firewall between the DMZ and internal network than the all internal network topology.
- Automatic system deployment (for 50, 250, or 800 concurrent user systems only) requires a more detailed setup in vCenter.
- Because of web redirection, for internal users, the WebEx site URL is replaced with the URL exposing the hostname of the virtual machine containing the web services as well as the Media virtual machines.