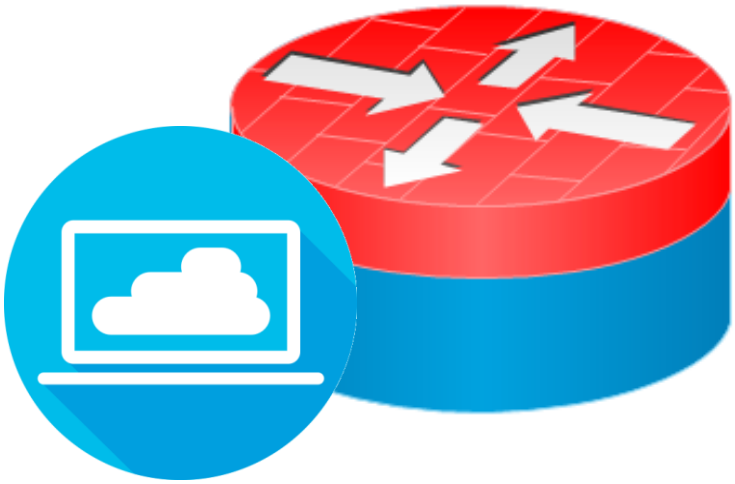
Webex Teams Firewall Traversal

Last Updated: September 6, 2018



Introduction

Webex Teams is a cloud collaboration platform that brings together all your people and communication tools in one secure and easy-to-use app. With the Webex Teams app, you can send messages, share files, and meet with different teams, all in one place. Webex Teams runs on various devices, such as your smartphones, laptops, Webex-registered room devices, and Webex Boards.

In this white paper, we discuss what is needed for a successful deployment of Webex Teams in a network behind a typical enterprise firewall.

You'll also learn how a customer journey with Webex Teams operates. This journey starts with early adopters who want to test Webex Teams. It's important that early adopters get Webex Teams to work without too much hassle. As early adopters go through trials, more official trial programs, and later to full deployment, we need to make sure that their enterprise network configuration is optimized for the best possible user experience with Webex Teams.

The examples in this white paper refer to real URLs, IP ranges, and port usage. To get the most accurate and current information, see the online Webex Teams firewall documentation.

Customer Journey

You don't need to host and maintain a large set of complicated services on-premises anymore. With the Webex Teams app, you can connect to the Webex Cloud to handle all your messaging, video conferencing, calling, interoperability with existing VoIP systems, and so on. The list of features that the Webex Cloud supports is rapidly growing.

The Webex Cloud offers meetings-focused services. What that means is that when the Webex Teams app connects to the cloud, you get features like gapless Wi-Fi/cellular handoffs and the ability to move calls from mobile to video units. This scenario is possible because all calls go through the Webex Cloud.

Webex Teams communicates with the Webex Cloud through HTTPS (including WebSockets) for messaging and signaling, and the Secure Real-Time Transport Protocol (SRTP) for media. To keep latency to a minimum, Webex Teams uses the User Datagram Protocol (UDP) as the preferred transport protocol for interactive media. With the Webex Cloud, new nodes can be geographically near customer locations, which helps to keep latency low.

Some enterprises might have restrictive security policies that prevent the Webex Teams app from connecting optimally to the Webex Cloud. For that reason, our "Get it working now, optimize later" strategy simplifies our trials process for our early adopters. See Figure 1.

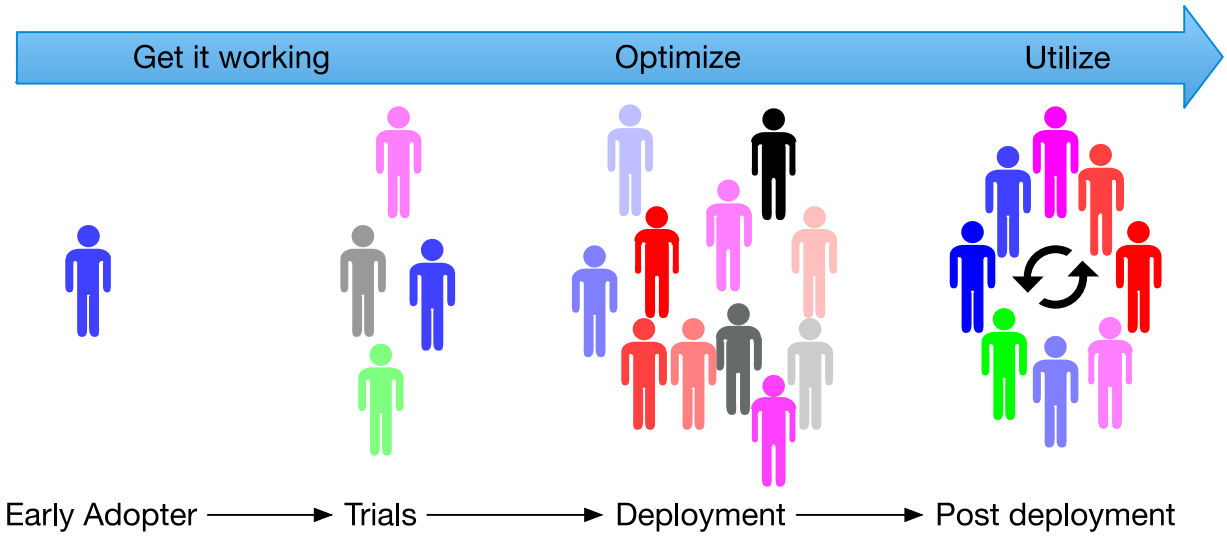


Figure 1 Early Adoption to Deployment

You can learn about a successful Webex Teams app customer journey, from early adoption to post deployment, in the next chapter.

Early Adoption

Some early adopters want to try Webex Teams but they find that their IT departments restrict connections to the Webex Cloud. How did we remove this obstacle so that early adopters can successfully try out Webex Teams? That's why we developed our "Get it working now, optimize later" strategy to simplify the trials process for our early adopters.

If early adopters can browse the Internet from their enterprise network, they can use the Webex Teams app, unless their enterprise actively blacklists any of the needed URLs that the Webex Teams app needs to connect to.

The Webex Teams app supports various options that allow early adopters to connect to the Webex Cloud. For the best possible media quality, we recommend that early adopters open up their firewall for inside-initiated UDP traffic. If that's not possible, the Webex Teams app supports TCP fallback or TLS fallback for media. As a last resort, it's also possible

that early adopters can send media through HTTP proxies.[1] Note that if you send media through a proxy, it often has a negative impact on audio/video quality, but this option allows for simple trials. Our goal for our early adopters is to help them get something up and running that can be optimized later.

Official Trials

At this stage, the early adopter's IT department is involved. Early adopters can make simple changes to the network infrastructure configuration such as configuring the firewall and making sure that enough bandwidth is available to satisfy the requirements for good quality media. More information is available in Webex Teams Bandwidth Requirements documentation.

Another option at this stage is to install a local Webex Video Mesh Node. This node is a virtual image that you can install in the local network. The media traffic from the Webex Teams app can terminate on the Webex Video Mesh nodes within your network instead of terminating on a media node in the Webex Cloud.

If early adopters open the firewall to permit inside-initiated UDP traffic on port 5004 (our recommended solution), they should also make sure that any Intrusion Detection Systems (IDS) installed in the network are aware of this change, because a sudden spike in UDP traffic can trigger alarms.

If early adopters can't allow UDP traffic through their firewall at this stage, we recommend that they don't send their media through an HTTP proxy. HTTP proxies can add latency and might not handle the required bandwidth needed for a successful official trial. If early adopters can't allow UDP through their firewall for media, we recommend that they use TCP fallback, TLS fallback or a local Webex Video Mesh Node so that the Webex Teams app can send media over UDP.

Deployment

In this phase, Webex Teams becomes an integral part of the early adopter's organization. At this stage, the early adopter's IT department actively helps to optimize the network by choosing deployment options that are based on their own network requirements and security policies. For example, the early adopter can benefit from low latency meetings media by opening inside-initiated UDP connections to ANY IP on port 5004. See Figure 2.

[1] Currently, Webex Board and Webex-registered room devices do not support media through HTTP proxies.

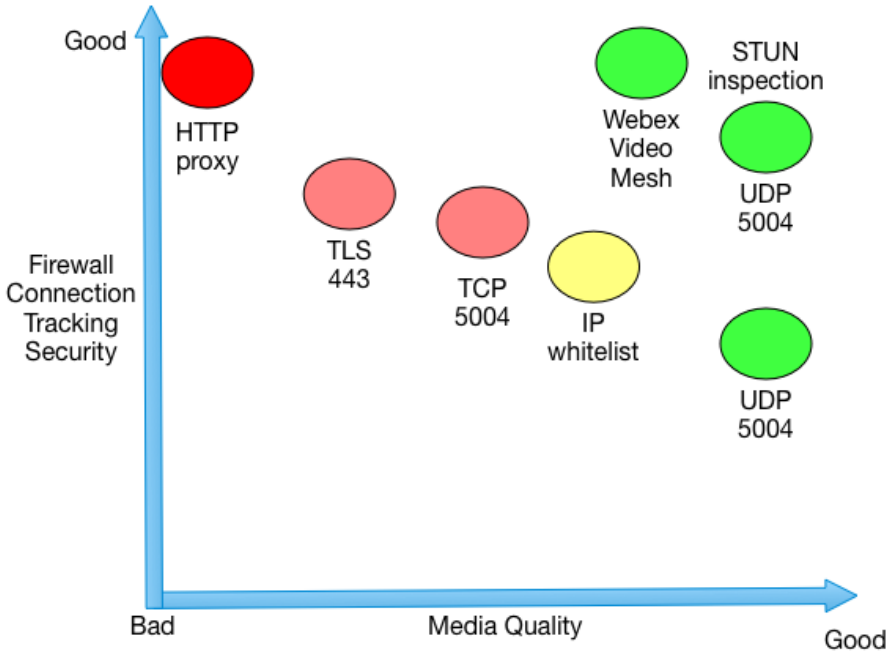


Figure 2: Security Versus Media Quality

Webex Teams always tries to reach a Webex Cloud or Webex Video Mesh media node that can provide the best media quality. If early adopters are concerned about opening inside-initiated UDP connections to ANY on port 5004, we recommend that they look into the Session Traversal Utilities for NAT (STUN) inspection capabilities of the installed firewall. STUN inspection adds TCP SYN/ACK-like properties in the initial packets. The Cisco Adaptive Security Appliance firewall supports STUN inspection.

Other options that an early adopter can consider is to include an IP range whitelist and install a local Webex Video Mesh Node to handle media.

Transport Layer Security (TLS) does not add any extra protection in securing the data in the media stream. The media stream payload is always encrypted with the Secure Real Time Transport Protocol (SRTP).

Post Deployment

We know that because technology changes and evolves, an early adopter's enterprise requirements and needs change as well. As an early adopter, your journey does not end after deployment; your post-deployment journey with Webex Teams is just beginning. For more information, contact your Cisco Partner or Cisco Customer Success representative.

Messages and Signaling

Messaging and meeting setup requires the Webex Teams app or endpoints to connect to the Webex Cloud. This chapter describes how you can configure a firewall to allow the Webex Teams app to connect to the Webex Cloud.

Ports and Protocols

Webex Cloud is deployed in data centers across the world. The Webex Teams app or endpoint can reach the cloud only if it can open a connection out on TLS port 443. The traffic on TLS port 443 is either HTTPS or WebSocket. In general, if your normal web browsing works, the Webex Teams app will also work.

URLs

Webex Teams connects to four categories of URLs:

- Messaging and signaling
- File and content storage
- Software upgrade images
- Metrics and analytics

The complete list of URLs used by Spark is available in the Network Requirements for Webex Teams Services document.

Messaging and Signaling

The Webex Teams app connects to Cisco-controlled URLs when the Webex Teams user authenticates to the Webex Cloud, send and receive messages, place and receive calls, share content, or share a whiteboard.

File and Content Storage

When a Webex Teams user uploads a file into a Webex Teams space, all Webex Teams user-generated content is encrypted end to end and is safe both in transit and rest. The content decryption keys are located at a Cisco-operated Key Management Server (KMS) in the Webex Cloud, or on a KMS installed on a Hybrid Data Security node within your Enterprise network. See the Webex Teams Security white paper for more details.

Software Upgrades

The Webex Teams app has a frequent update cycle. Security fixes and other continuous improvements are automatically updated by the Webex Teams app or endpoint. To ensure that you can download our upgrades easily, we rely on a Content Delivery Network (CDN). The Webex Teams app automatically downloads updates on most devices. Some devices require user action to install; other devices install the update automatically.

Metrics and Analytics

Collecting metrics and analytics is key for Webex Teams. This data collection adheres to the policies described in our Cisco Privacy Statement.

It's important that we collect this data because it helps us fine-tune our services. With this data, we can optimize data center locations and internal networks to make sure that latency is low.

Sending and Receiving Media

To enable audio and video with the best possible quality, we recommend that your firewall allows inside-initiated UDP connections to port 5004. If the Webex Teams app fails to connect on UDP, it can fall back to traverse a firewall using TCP port 5004 and TLS port 443 as well, but the media quality might suffer.

The Webex Teams app also supports a media tunnel through an HTTP proxy. This tunnel can help you to maintain connectivity in scenarios where an HTTP proxy is required and no other protocols succeed. The drawback is that it usually causes poor media quality.

All connections are initiated by the Webex Teams app. This requirement is important because it allows the Webex Teams app to work in Network Address Translation (NAT) environments. The Webex Teams app or endpoint expects the firewall's NAT table entry to expire after some time of inactivity and sends keepalives to maintain the connection if it's still needed. How long a firewall/NAT actually keeps the pinhole open varies, but Webex Teams requires at least a 30-second timeout. Media is always symmetric; the same source port is used to send and receive media.

Some Webex Teams apps probe for connectivity on port 33434 to send and receive media. While it can be used as a last resort, we suggest that you do not open port 33434 for media. This port is often referred to as the traceroute port and is rate limited by some ISPs. Using this port can cause bad media quality.

Media Node Discovery

Periodically, all Webex Teams apps perform a media node discovery probe to ensure that the best possible media node can handle a media flow to/from the Webex Teams app. During this probe, nodes in the Webex Cloud and local Webex Video Mesh Nodes, managed in your Webex Cloud organization, are discovered.

The Webex Teams app or endpoint receives a node list from the Webex Cloud, performs a ping by sending a STUN (RFC 5389) request, and listens for a response from all the nodes in the list.

The Webex Teams app or endpoint receives answers from the reachable media nodes. The Webex Teams app measures the packet's round-trip time (RTT) on UDP, TCP, and TLS based on the send requests and received responses.

The Webex Teams app reports back to the Webex Cloud. The Webex Teams app reports what media nodes it has connectivity to, which protocol it has connectivity to, and what the measured RTT is. Figure 3 shows an example of how media node discovery works. This figure is an example only; the real-world placement of these nodes might differ.

Figure 3 Media Node Discovery

After media node discovery occurs, the Webex Cloud knows which media nodes can be reached by that particular client or endpoint and on which protocols.

When a meeting starts, the Webex Cloud assigns a media node to the Webex Teams app or endpoint. The assignment is based on information from a previously completed media node discovery probe. Probing is not part of the meeting setup, but is performed when the Webex Teams app registers to the cloud and changes its network connection. The probing data cache expiry is set to 2 hours. The node assignment might not rely just on the RTT measurements, but also on where the other participants in the meeting are joining from.

Media Connectivity

Webex Teams offers five basic firewall traversal options (as shown in Figure 4):

1) Inside-initiated UDP to ANY IP address
2) STUN inspection
3) Webex Video Mesh (outbound 1: ANY)
4) IP range whitelisting
5) Fallback (TCP, TLS, HTTP proxy)

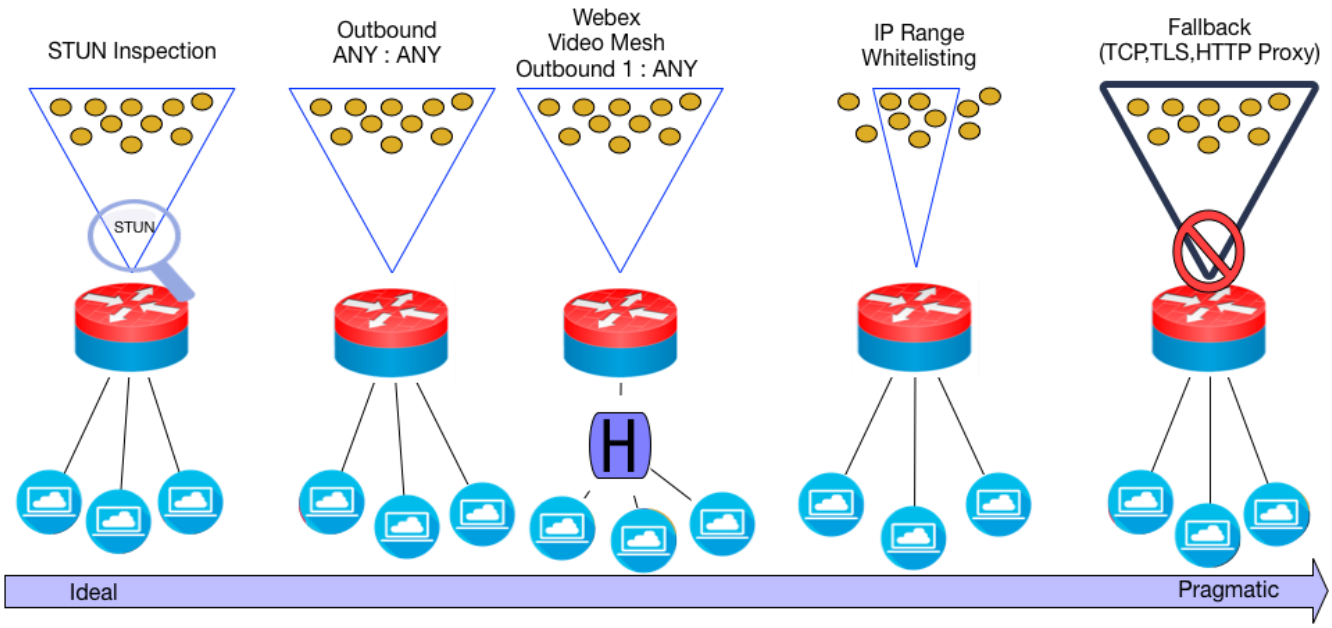


Figure 4 Firewall Traversal Options

The ideal solution is to allow inside-initiated STUN-inspected UDP traffic to ANY destination IP address. This allows the Webex Teams app to use the full range of dynamically available media nodes in the Webex Cloud. UDP is the preferred protocol for interactive media, because it has lower latency.

Inside-initiated UDP to ANY Destination IP Address

It's important to understand that the Webex Cloud never connects directly to any Webex Teams app. All needed connections are initiated from the Webex Teams app. Media flows in both directions using a symmetric inside-initiated,

5-tuple UDP stream outbound to the Webex Cloud.[2] The pinhole created in the firewall for this connection is usually closed after 30 seconds if no packets are sent from inside of the network to keep it open.

STUN Inspection

STUN packets are sent as part of the IETF firewall traversal standard, "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," RFC 5245. STUN packets are defined in the IETF standard, "Session Traversal Utilities for NAT (STUN)," RFC 5389.

STUN packets are sent during the call setup as probes. These probes can determine the best possible network path for the media. Those packets contain useful information for both upstream and downstream links. A firewall can use that information to validate any media flow that follows them.

The Cisco ASA Series of firewalls can be configured to perform STUN inspection.

Webex Video Mesh

Webex Video Mesh brings the cloud closer to your network. Using it is like hosting part of the Webex Cloud in your network that only you have access to.

Webex Video Mesh is delivered as a virtual machine (VM) image (VMware ESXi). See Figure 5. You can install this image anywhere in your network, even behind Network Address Translation (NAT), or in a data center of your choice. The Webex Video Mesh Node always initiates any needed connections.

A Webex Video Mesh Node adds hardware cost because physical CPUs are needed in the local network. For media streams that stay in the local network, this scenario has a significant positive impact on latency, and it also saves bandwidth on the public internet uplink.

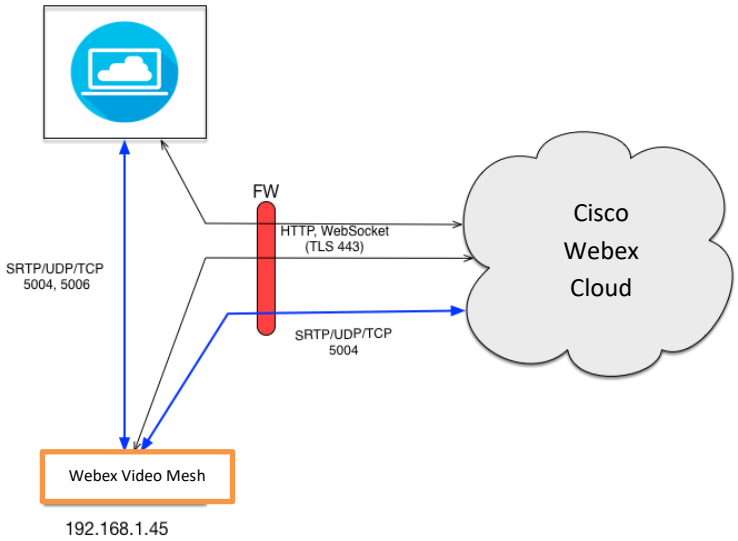


Figure 5 Webex Video Mesh Ports and Protocols

The Webex Video Mesh Node uses the same ports and protocols as the Webex Teams app when it talks to the cloud.

[2] Sending and receiving media on the same port

IP Range Whitelisting

A cloud service is dynamic; it can start up and tear down resources as needed. So that you can get the most benefit from this behavior, we encourage you to open up the firewall for inside-initiated UDP connections to ANY (any IP address) to port 5004 for the best possible media quality.

If you have a security policy that prevents you from opening up inside-initiated connections on UDP to ANY on port 5004, we recommend that you consider if your firewall can support STUN inspections and dynamically open traffic based on STUN packets. Doing so can increase your security while you still can take advantage of all available media nodes.

Another option is to whitelist an IP address range in which Webex Cloud operates media nodes. Bear in mind that whitelisting may reduce media quality, because you can't use an unlisted media node that may be closer to you.

Whitelisting specific IP ranges affects the media node discovery because the Webex Teams app can only reach the media nodes within the whitelisted IP range. This scenario might cause the Webex Teams app or endpoint to end up with a suboptimal media node.

IP ranges for Webex Teams are documented in Network Requirements for Webex Teams Services.

HTTP Proxy Traversal

The behavior of HTTP proxies can vary. Automatic discovery and configuration are usually done by the Web Proxy Auto-Discovery Protocol (WPAD). WPAD is a DHCP extension that points to a proxy auto-config (PAC) file. The PAC file contains JavaScript that must be executed by the application that wants to traverse the HTTP proxy. The Webex Teams app relies on the underlying operating system to support this scenario.

Note: Because Android doesn't have this feature, you must manually configure any HTTP proxy on an Android device.

If you configure the underlying operating system to use a proxy, the Webex Teams app or endpoint can use it when it establishes a connection out to Webex Cloud. Supported authentication methods can vary between devices and operating systems. See the Network Requirements for Webex Teams Services documentation for more detailed information.

HTTP Proxy in Split Signaling and Media Scenarios

If you configure the Webex Teams app to use an HTTP proxy, all signaling is sent to the configured proxy address and port. See *Figure 6*. The Webex Teams app uses the appropriate proxy signaling (HTTP Connect) to connect to the Webex Cloud. Signaling passes through the HTTP proxy and is inspected by the HTTP proxy. To allow the signaling traffic to reach Webex Cloud, it's important that you set the HTTP proxy to allow traffic to the appropriate URLs. See the Network Requirements for Webex Teams Services documentation and the section on URLs for details.

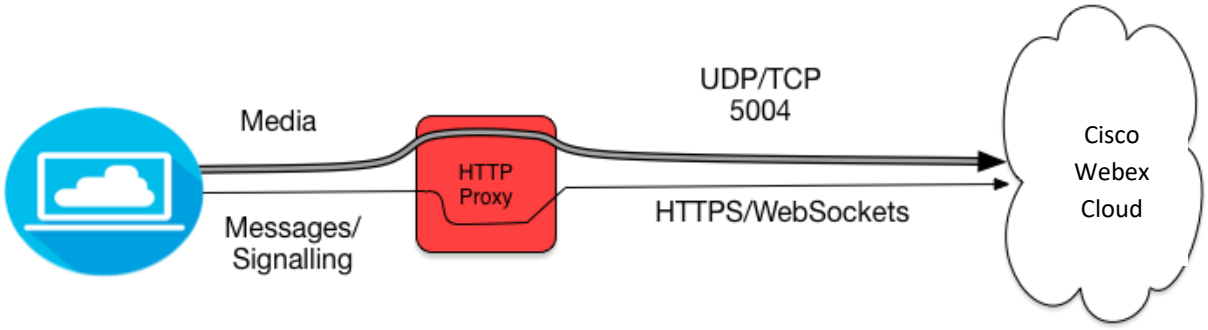


Figure 6 Signaling and/or Media Through an HTTP Proxy

If Webex Video Mesh is present in the local network, you can use it to handle media. See Figure 7. In this scenario, media no longer needs to traverse the HTTP proxy. This scenario significantly improves the media quality because you can use UDP as the transport protocol. If all the meeting participants are located on the same network, media is not sent to the Webex Cloud because the local Webex Video Mesh Node handles the media streams.

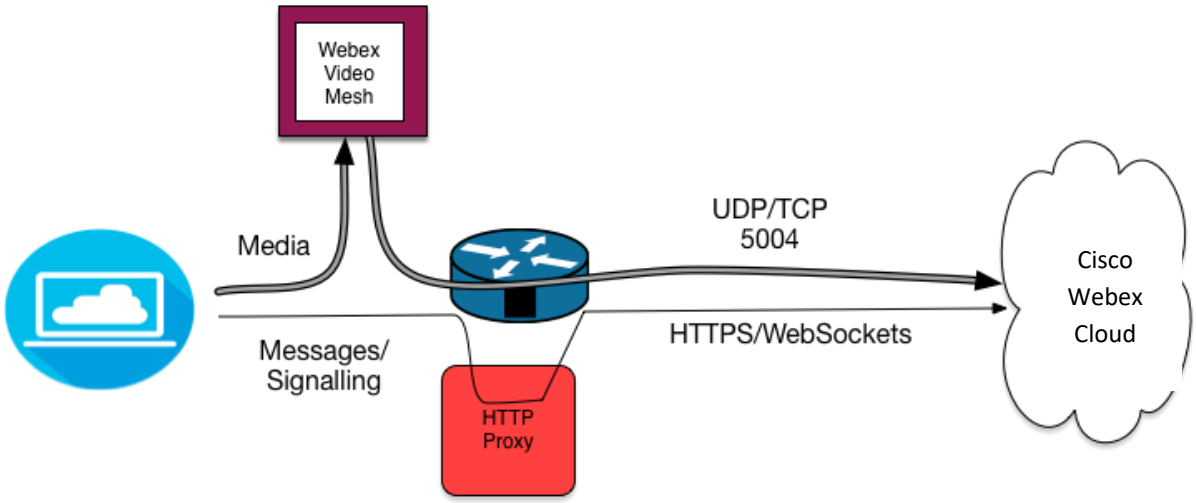


Figure 7 HTTP Proxy and Webex Video Mesh Node

If Webex Video Mesh is not present in the local network, media can also pass through the HTTP proxy itself. How this is handled by the HTTP proxy depends on the proxy configuration. We do not recommend that you send media through a HTTP proxy because excessive latency is added. An HTTP proxy is not designed to handle interactive audio and video.

We recommend that you consider any of the other firewall traversal alternatives that are described in this white paper. We realize that it might be a major shift in how the enterprise handles internet traffic, but that is the tradeoff using any cloud technology.

Summary

Dealing with enterprise firewall traversal is no easy task, especially when your goal is to ease the adoption of Webex Teams and minimize the workload for your IT department. Webex Teams can help you to do the following:

- Initiate outbound connections
  Note: The Webex Cloud never initiates any connections to the Webex Teams apps.

- Use documented ports and protocols to connect to the Webex Cloud
- Connect to Cisco controlled URLs for messaging, signaling, and identity management
- Use TCP fallback or TLS fallback for media as an alternate way to connect to the Webex Cloud
- Support HTTP proxies to allow the signaling traffic to reach the Webex Cloud
- Use IP range whitelisting to connect to Webex Cloud media nodes within the whitelisted IP range
- Use Webex Video Mesh to bring the cloud closer to your network