



# WebEx Communications

## Network Trace Confirmation for On-Demand Web Collaboration Service

Executive Summary



**iSEC Partners, LLC**

<https://www.isecpartners.com>

**iSEC**  
PARTNER

# EXECUTIVE SUMMARY

## INTRODUCTION

Information Security Partners, LLC (iSEC) was engaged by WebEx Communications (WebEx) to enumerate and confirm the network communication routes used for WebEx meetings. The primary objective of the project was to understand what networks are used when a WebEx user creates, joins, or initiates a meeting, for both external communications on the Internet as well as internal communication inside the WebEx MediaTone Network.

## ANALYSIS AND CONCLUSION:

iSEC used the following scenarios to confirm the route for network communications:

- **Scenario:** Trace network route when a WebEx user creates, initiates, hosts or joins a meeting
  - o **Conclusion:** WebEx San Jose and Santa Clara, California are the valid routes paths.
- **Scenario:** Trace routing configuration from WebEx production border routers/firewalls to determine where gateway routes to public resources are directed
  - o **Conclusion:** United States locations are the valid route paths.
- **Scenario:** Trace network route and office locations used for internal routing to production servers
  - o **Conclusion:** United States locations, including San Jose, California, are the valid route paths.

Production WebEx sites and servers were used for the testing. All tests were conducted using the WebEx data center in San Jose, CA.

iSEC completed at least 11 tests for each scenario. Based on the testing, iSEC was able to confirm the following locations are used externally for network communication, which includes WebEx networks and Internet Services Providers (ISPs) of WebEx:

- Santa Clara, California
- San Jose, California

Furthermore, iSEC was able to confirm the following locations are used internally for network communication to the WebEx San Jose Data Center, which only includes WebEx networks:

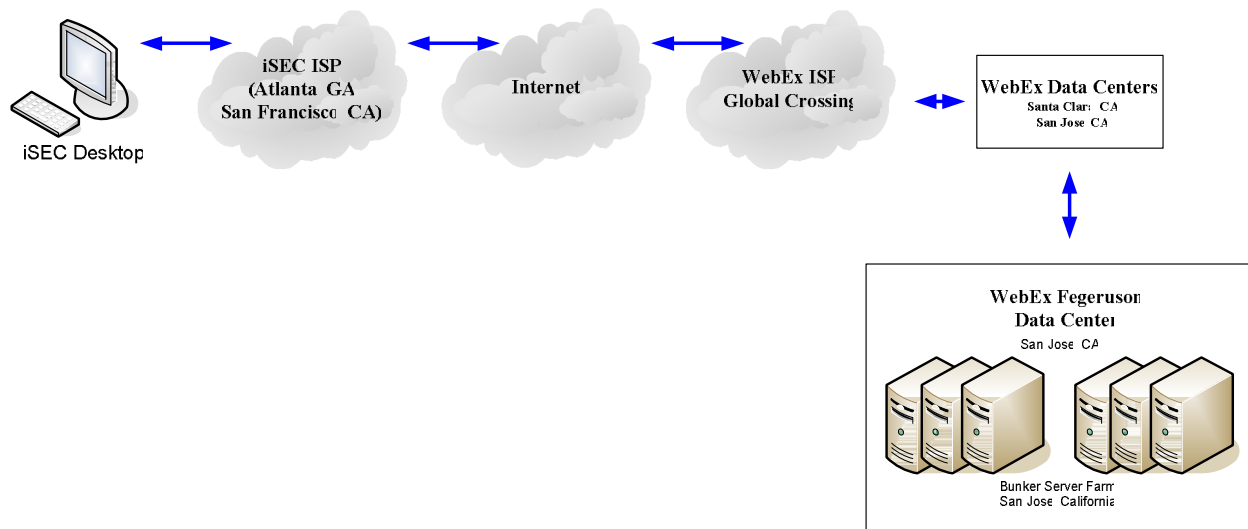
- Santa Clara, California
- San Jose, California

# TECHNICAL SUMMARY

## OVERVIEW OF NETWORK PATH

iSEC created and joined several WebEx meetings to complete the testing. A typical communication path for the meetings routed from iSEC's network, to iSEC's ISP's network, to the ISP of WebEx (e.g. Global Crossing), and then finally to WebEx's network. The communication route enumerated by iSEC to and from the WebEx San Jose Data Center, which is the location of the WebEx servers, is shown in figure 1.1.

**Figure 1.1**



## NETWORK TESTING AND CONCLUSIONS

The following tables summarize iSEC's test, analysis, and conclusions for the testing. The tables below summarize the following network communication paths:

- External to Internal Communication
- Internal to External Communication
- Network Routes for Border Network Devices
- Network Routes for Internal Network Devices
- Servers used by perimeter Load Balancers

### TECHICAL FINDINGS SUMMARY – EXTERNAL TO INTERNAL COMMUNICATION

**Description:** Verify the routing between any end user who creates initiates, or hosts a meeting to the production WebEx servers. This test will determine where and what networks the routing uses until it arrives in the WebEx domain.

TEST	ANALYSIS
1. Execute a trace route between an end user machine that is initiating a meeting and the WebEx meeting site, which is delivering the meeting.	The analysis shows that all packets routed from the end user initiating the meeting to the server delivering the meeting went through San Francisco, CA, Atlanta, Georgia, San Jose, CA and then to Chicago, IL before the packets were ultimately dropped. <b>Note</b> , while the ICMP packets were terminated in Chicago, the WebEx communication packets continue after Chicago, IL. Test 1 confirms the routing to the Global Crossing network, but later in test 3 we will be able to confirm the communication after the Chicago, IL location.
2. Execute a visual route to wbxsecurity.webex.com	Test 2 visually confirms the trace route in test 1.
<b>CONCLUSION:</b> SAN JOSE, CA AND CHICAGO, IL (GLOBAL CROSSING) ARE VALID ROUTES PATHS.	

### TECHICAL FINDINGS SUMMARY – INTERNAL TO EXTERNAL COMMUNICATION

**Description:** Verify the routing between the Global Crossing network in Chicago, IL to the WebEx Servers delivering the meeting.

TEST	ANALYSIS
3. Since the ICMP packets dropped at the GLX cloud, network traces should be performed from the internal WebEx servers out to the public internet. This will confirm if internal routing takes packets to other network locations besides San Jose, CA. Since wbxsecurity.webex.com is a virtual IP address on the load balancer, verification of the server's hostname must occur to ensure it is the actual server that is delivering a WebEx meeting.	The nslookup command confirms the real address and hostname of the WebEx web server. In test 4, dhweb1 will be shown as the source for internal to external testing.
4. Verification of the internal routing from WebEx servers in production domains to external end user locations (specifically where the ICMP packets were dropped in test 1 and 2). This test will confirm if any packets are routed to other networks before it is presented to the publicly accessible (non-WebEx domain) network. A trace route from a production WebEx Server to the location where the packets were dropped in test 1 and 2 should be executed.	The test confirms the first hop from the WebEx server. The trace route shows the time it took to get to its first hop was less than 2 ms, indicating the network device is very close to the WebEx server in San Jose, CA. The location of the network device is also confirmed by the Ferguson Data Center network map, which shows the IP address as a HSRP IP address on the router.
5. Verify hops 2 and 3 route from the Ferguson Data Center in San Jose, to the Tasman Data Center in San Jose, and then to the outside public Internet.	The test confirms the second and third hop from the WebEx server delivering the meeting is located in the Tasman data center in San Jose, CA (routed from the Ferguson data center in San Jose, CA). The trace route shows the time it took to get to its both hops was less than 2 ms, indicating the network devices are very close to the WebEx Server in San Jose, CA. The location of the network device is also confirmed by the Tasman Data Center network map.
<b>CONCLUSION:</b> SAN JOSE, CA, AND SANTA CLARA,, CA ARE VALID ROUTES PATHS.	

### TECHICAL FINDINGS SUMMARY –NETWORK ROUTES FOR BORDER NETWORK DEVICES

**Description:** Verify the default outbound route on border routing devices, which are used by the WebEx servers delivering meetings, to public end users.

TEST	ANALYSIS
6. Review the default route of the border router in the San Jose	No default route listed outbound. BGP route reflectors are

Data Center.	used with no China location included. An internal default route is used and is located in the US.
7. Review the default route of the border router in the Denver Data Center.	No default route listed outbound. BGP route reflectors are used with no China location included.
8. Review the default route of the border router in the Ashburn, VA Data Center.	No default route listed outbound. BGP route reflectors are used with no China location included.
<b>CONCLUSION:</b> UNITED STATES LOCATIONS ARE THE VALID ROUTE PATHS.	

#### TECHICAL FINDINGS SUMMARY – NETWORK ROUTES FOR INTERNAL NETWORK DEVICES

**Description:** Verify the default outbound route on internal routing devices, which are used by the WebEx servers delivering meetings, to public end users.

TEST	ANALYSIS
9. Review the default route of the internal router in the San Jose, CA Data Center.	The default route is shown to be an IP address on WebEx's internal network, which is located in the San Jose, CA.
10. Review the default route of a firewall in the San Jose Data Center.	The default route is shown to be a network device inside the WebEx datacenter in San Jose, CA.
<b>CONCLUSION:</b> UNITED STATES LOCATIONS, INCLUDING SAN JOSE, CA, ARE THE VALID ROUTE PATHS.	

#### TECHICAL FINDINGS SUMMARY – SERVERS USED BY PERIMTER LOAD BALANCERS

**Description:** Verify the location of servers used by perimeter load balancers, which are used to route traffic from external end points to internal servers for WebEx meetings.

TEST	ANALYSIS
11. Review the configuration of load balancers in the San Jose Data Center, specifically the servers listed to deliver WebEx meetings.	All servers used for the test WebEx meetings contain IP addresses within a set range. Enumerating the location of the IP addresses can be approximated using a public website, such as IP2Location.com, which shows the locations to be in Santa Clara, CA.
<b>CONCLUSION:</b> UNITED STATES LOCATIONS, INCLUDING SANTA CLARA, CA, ARE THE VALID ROUTE PATHS.	