Cisco BroadCloud for Carriers

Firewall, Security and Network Considerations

Requirements

Last Updated 07/01/2021

Cisco BroadCloud™ Firewall, Security and Network Considerations Requirements

Notification

The BroadSoft BroadCloud has been renamed to Cisco BroadCloud. Beginning in September 2018, you will begin to see the Cisco name and company logo, along with the new product name on the software, documentation and packaging. During this transition process, you may see both BroadSoft and Cisco brands and former product names. These products meet the same high standards and quality that both BroadSoft and Cisco are known for in the industry.

Copyright Notice

Trademarks

Any product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

This document is printed in the United States of America.

Document Revision History

Release	Version	Reason for Change	Date	Author
Draft	0.1	Created document.	*March 9, 2017*	BroadCloud Engineering
Draft	0.2	Added DNS/NTP Addresses	June 9, 2017	BroadCloud Engineering
1	1.0	Document Released	July 17, 2017	BroadCloud Engineering
1	1.1	Added SIP Session Audit and NAT Info	March 7, 2018	Cisco BroadCloud Engineering
1	1.2	Updated Section 4 - NA Commercial with the additional IP Addresses for CH & DA and new IP Addresses for LA & NY for Hosted, SIPConnect & Apps Updated Section 4 - NA FedRAMP with the additional IP Addresses for CH & DA for Hosted, SIPConnect & Apps	April 24, 2018	Cisco BroadCloud Engineering
1	1.3	Reissued document with minor update to Section 4 - NA FedRAMP for Apps	June 22, 2018	Cisco BroadCloud Engineering
1	1.4	Added SY3 addresses in AU + panasonic.broadcloud.com.au	September 7, 2018	Cisco BroadCloud Engineering
1	1.5	Expanded detail on NAT/PAT	October 2, 2018	Cisco BroadCloud Engineering
1	1.6	Expanded Section 4 for NA, EMEA and APAC by including the SBC IP Address and Port details for SIP Signaling and Media for encryption based service Updated Section 4 - NA FedRAMP by deleting the obsolete IP Addresses	October 8, 2018	Cisco BroadCloud Engineering
1	1.7	Added UC-SaaS for US/EMEA under Applications	October 22, 2018	Cisco BroadCloud Engineering
1	1.8	Further detail on recommended NAT timers	November 22, 2018	Cisco BroadCloud Engineering
1	1.9	Added Webex Calling information	February 20, 2019	Cisco BroadCloud Engineering
2	2.0	Added FedRAMP PIV Card destination details Changed US Carrier UCaaS Address from incorrect FedRAMP reference	February 28, 2019	Cisco BroadCloud Engineering
2	2.1	Added new provisioning URL for specific Cisco device on BroadCloud Carrier	March 7th, 2019	Cisco BroadCloud Engineering

2	2.2	Changed **SBC Traffic** IP Addresses to IP subnet for BroadCloud Carrier Changed **SBC Traffic** IP Addresses to IP subnet for FedRAMP	March 20, 2019	Cisco BroadCloud Engineering
2	2.3	Expanded NA Product Offerings with additional subnet for Chicago and Dallas	July 17, 2019	Cisco BroadCloud Engineering
2	2.4	Added Webex Calling Japan Region	July 30, 2019	Cisco BroadCloud Engineering
2	2.5	Moved Cisco SPA122 from spa.sipflash.com to cisco.sipflash.com for US provisioning	September 16, 2019	Cisco BroadCloud Engineering
2	2.6	Removed erroneous statement on custom NTP support	October 17, 2019	Cisco BroadCloud Engineering
2	2.7	Added Canada region plus new Dallas and Chicago subnets	April 20, 2020	Cisco BroadCloud Engineering
2	2.8	Added Gigaset/Panasonic/Obihai/Mediatrix to EU region, added Obihai/Mediatrix/Patton/Vtech to US region, added Gigaset/Obihai/Mediatrix to AU region	May 19, 2020	Cisco BroadCloud Engineering
2	2.9	Added DNS for Canada DMS URL's and acodes specific URL	May 20, 2020	Cisco BroadCloud Engineering
2	2.10	Added Guest Client Desktop Sharing IPs/Ports for CA	September 1, 2020	Cisco BroadCloud Engineering
3	3.0	Update DMZ IPs used by FED, to FED DMZ	January 20, 2021	Cisco BroadCloud Engineering
3	3.1	Add new WxC public ranges	February 2, 2021	Cisco BroadCloud Engineering
3	3.2	Modify page breaks, update Examinet and Client IP's in AU	February 22, 2021	Cisco BroadCloud Engineering
3	3.3	Add public subnets for EU-N environment – Amsterdam 170.72.29.0/24 and Frankfurt 170.72.17.128/25. Removed Packetsmart as EOL. Removed Webex Calling as has help guide on Cisco website	September 16, 2021	Cisco BroadCloud Engineering
3	3.4	Added AudioCodes and Patton ATA provisioning URLs to FedRamp section	January 7, 2022	Cisco BroadCloud Engineering

Table of Contents

1 Introduction

This document provides an overview of the required protocols for service on the platform including the ports that are used.

It is our Partner's responsibility to ensure their customer's CPE in configured securely in accordance with industry best practices.

Identifying the protocols and ports that are to be used is the first step in designing a security policy using firewalls and/or access control lists (ACL) to restrict access to only the required services.

As part of successful Customer Premises Equipment (CPE) deployment and operation, all required devices, features, portals and applications located in *Section 4, Port Requirements* should have the corresponding LAN/WAN requirements for service implemented and tested before live customer calls are made.

2 Firewall and Security Best Practices

A correctly configured firewall is ***essential for all*** customer deployments.

Not all firewall configurations need ports to be opened. If the customer is running inside to outside rules, then ports should be opened to allow the protocols required for service out.

There should be no reason for the customer to open ports inbound on the firewall where NAT is employed, if reasonable binding periods are defined and there no SIP manipulation ("SIP aware") performed on the NAT device.

3 Customer Deployment Best Practice

Password Policy Best Practice

Manually configured CPE, including but not limited to routers and firewalls should always be configured with passwords that adhere to industry best practices for password policies.

Passwords should:-

- Be lengthy
  - A minimum of 8 characters
- Be complex
  - Containing:-
    - Upper and lower case letters
    - Numbers
    - Symbols where the CPE can support this
- Not contain dictionary words
  - Not contain the customer name
- Not contain the customer's the phone number
- Be encrypted and kept in a secure location
  - Only be accessible by authorized personnel
  - Changed regularly
- Not be shared by email

Deployment Access Requirements

The *Port Requirements* section of this document defines the ports and protocols required for correct operation of the service for the different customer deployments available.

If your customer deployment is a '*mixed estate'* deployment encompassing both IP endpoints and SIP Trunking endpoints, more than one section may need to be considered.

Select the section that applies to your customer's deployment region.

If your customer operates a Corporate Network with strict policies on internet access for its employees and operates an Access Control List (ACL) for websites, please ensure you refer to the Portals section.

SIP Trunk Deployments

As SIP Trunk deployments may require manual configuration of the CPE and include requirements or remote access for maintenance and support there are additional considerations.

This is extremely important for any IP PBX or Media Gateway that is accessible over the internet via an IP address. Other protocols such as, but not limited to, Telnet and FTP/TFTP are commonly used for upgrades and configuration backups so will also need to be considered.

Please ensure that all the manufacturers' recommendations and best practices for securing CPE are implemented.

Firewall

Particularly when using standard Internet Access for reaching Cisco BroadCloud, all IP PBXs and Media Gateways should be behind a firewall that is appropriately configured to prevent access to the CPE from unknown sources.

Remote Access

Where remote access to the IP PBX or Media Gateway is required for support and maintenance please refer to the manufacturer's best practice security recommendations.
If not already recommended as best practice by the manufacturer you may wish to consider configuring VPN access to allow access to the CPE from your authorized IP addresses only.

CPE Password Policies

On installation of CPE, change any access password from the manufacturers' default **IMMEDIATELY.**
This may include administrator access and extends to any authorised end user access to the CPE.

Please refer to the manufacturer's documentation to ensure ALL access passwords are updated from the default.

All manually configured passwords on CPE should adhere to industry standards for passwords, described in *Section 3.1, Password Policy Best Practice.*

Additionally please ensure:-

- The access passwords for each device in your customer estate is unique to that customer deployment only
- Passwords are kept in secure encrypted files and locations
    - Passwords should not be kept
        - In non-password protected files
        - On smartphones
- Passwords are only accessible by authorized and fully trained personnel
    - Passwords should not be openly shared with
        - end users
        - contractors
        - untrained personnel
- Passwords in use across your customer estate should be changed
    - At regular intervals
    - When personnel move on

SIP ALG

If a router and/or firewall is "SIP Aware", that is, it has SIP ALG or similar enabled, we recommend that this functionality be turned OFF for correct operation of the service

See the relevant manufacturer's documentation for more information on how to disable SIP ALG on specific devices.

SIP Session Audit

To help protect against potential fraud for longer calls, the platform performs a Session Audit every 15 minutes. The Session Audit will deliver either an UPDATE or re-INVITE SIP message depending on what the device can support and a 200 OK is expected in response. If a 200 OK is not received, the UPDATE or re-INVITE will be retried and if no response is received the call will be deemed to be invalid and will be gracefully ceased.

NAT/PAT

For certain Enterprise and Service Provider network designs, it is common to hide an entire client IP address space, usually consisting of private IP addresses (rfc 1918), behind a single IP address (or in some cases a small group of IP addresses) in another usually public IP address space. The PAT function gets deployed on either a customer CPE router/firewall or within the Service Provider network that translates multiple customer/client Source IP addresses to a single mapped IP address by translating the client source IP address and source TCP/UDP port to the mapped "outside" source IP address and a unique source TCP/UDP port.

Typically, each TCP or UDP client connection requires a separate PAT translation to be setup in the router/firewall because the client connection source port differs for each outgoing connection. Such PAT translation or a dynamic entry stays in the router/firewall NAT/PAT table as long as traffic flows between the client application and the server destination. Once the client/server communication stops the dynamic translations have a timeout period after which they are purged from the translation table.

The customer router/firewall must allow for a configurable Network Address Translation (NAT) bind timer, the value of the timer is dependent on the specific network configuration.

Cisco BroadCloud recommends that the minimum NAT timer for UDP is set to 300 seconds. Generally standard TCP timers are much higher and therefore sufficient however in cases where this may be an issue it is recommended that this is set to 300 seconds or more also, Please note that we do not recommend reducing default timers to align to these values as this may have a negative impact on other applications.

Operational Impacts of Source IP PAT/Dynamic NAT:

- Dynamic NAT introduces additional network operational and administrative overhead (in the routing appliances i.e. routers, firewalls, etc.) because it introduces a connection translation state table in to the network routing/firewall elements:
    - The new PAT connections may be rejected if the Outside IP port pool is exhausted
    - The operational state of the router (memory, CPU) must be closely monitored in high traffic customer deployments
    - The NAT/PAT pool of IP addresses must be augmented if the number of client sessions start to reach the number of available outside TCP/UDP ports. Typically the PAT pool consists of 1024-65535 available ports per single outside IP address
- There should never be two Source IP PAT or Dynamic NAT operations performed on the customer traffic within a single end-to-end connection. Due to existence of NAT/PAT timers and the overall ephemeral port allocations during the translation the double source PAT will introduce unexpected negative behavior to client application.
- Assurance that the propagation of any QoS markings (DSCP) is maintained within the IP packet after the PAT translation is necessary. In certain router/firewall PAT implementations the DCSP markings can be stripped off the IP packets and hence affecting the voice quality of service on the network.

DHCP, DNS and NTP

It is expected that when deploying devices, in particular IP Phones to a site that DHCP will be supplied locally which will also define DNS and possibly NTP servers for the LAN.

NTP

Cisco BroadCloud will define NTP sources as part of standard IP Phone configuration.

IP Phones will not be able to complete their initial or ongoing configuration refresh cycle without an accurate NTP resource being defined.

4 IP/Port Requirements

This section identifies the IP address and TCP/UDP ports that are required for proper operation of the service. The next sections are be broken down to different Products, Network elements and required protocols, please refer to the region applicable to your customer deployment.

IMPORTANT

The following does not apply to **Enterprise SIP/Carrier PSTN** deployments, as these can be subject to change and are bespoke in nature, the information required will be provided during the setup process.

Should you choose to restrict connectivity beyond the guidance given then this may impact upon future service operation and require remediation to the firewall configuration.

North America - NA - Cisco BroadCloud Carrier

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Device	Protocol	Destination/DNS	IP	Destination Port
IP Phone / ATA / IAD	**NTP** Endpoint clock synchronization	ntp.broadcloudpbx.net	199.59.65.181 199.59.66.181	UDP 123
IP Phone / ATA / IAD	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally		UDP/TCP 53
SBC Traffic **IP Endpoints**	**SIP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP / TCP 8933
SBC Traffic **IP Endpoints**	**RTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535
SBC Traffic **IP Endpoints**	**SIP/TLS**	Dallas Chicago	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24	TCP 8934

		New York Los Angeles	199.59.71.0/25 199.59.70.0/25	
SBC Traffic IP Endpoints	**SRTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535
Cisco SPA IP Phones & SPA8000, SPA2102 ATAs	**HTTPS**	spa.sipflash.com	128.177.36.192 128.177.14.192	TCP 443
Cisco 3PCC Phones with MPP firmware, Cisco SPA122, 191 and 192 ATAs, Cisco DECT	**HTTPS**	cisco.sipflash.com	199.59.65.228 199.59.66.228	TCP 443
Polycom IP Phone	**HTTP/HTTPS**	plcm.sipflash.com	128.177.36.191 128.177.14.191	TCP 80 443
Snom IP Phone	**HTTPS**	snom.sipflash.com	128.177.36.193 128.177.14.193	TCP 443
Yealink IP Phone	**HTTPS**	yealink.sipflash.com	128.177.36.213 128.177.14.213	TCP 443
Audiocodes IP Phone	**HTTPS**	acodes.sipflash.com	128.177.36.189 128.177.14.194	TCP 443
Aastra/Mitel IP Phone	**HTTPS**	aastra.sipflash.com	128.177.36.190 128.177.14.195	TCP 443
Panasonic IP Phone	**HTTPS**	panasonic.sipflash.com	128.177.36.218 128.177.14.218	TCP 443
Gigaset IP Phone	**HTTPS**	mediatrix.sipflash.com	199.59.65.173 199.59.66.173	TCP 443
Obihai IP Phone	**HTTPS**	obihai.sipflash.com	199.59.65.241 199.59.66.241	TCP 443

Patton IP Phone	**HTTPS**	patton.sipflash.com	199.59.65.240 199.59.66.240	TCP 443
vtech IP Phone	**HTTPS**	vtech.sipflash.com	199.59.65.171 199.59.66.171	TCP 443

Registering SIP Trunking IP PBXs and Gateways

Device	Protocol	Destination/DNS	IP	Destination Port
SIP-T Endpoint	**NTP** Endpoint clock synchronization	Supplied Locally	Supplied Locally	UDP 123
SIP-T Endpoint	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53
SBC Traffic SIP-T Endpoint	**SIP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 8933
SBC Traffic SIP-T Endpoint	**RTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535
SBC Traffic SIP-T Endpoint	**SIP/TLS**	Dallas	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24	TCP 8934

		Chicago New York Los Angeles	128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	
SBC Traffic **SIP-T** **Endpoint**	**SRTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535

Applications

Device	Protocol	Destination/DNS	IP	Destination Port
UC Endpoints (Clients)	**HTTP / HTTPS** **CAP** **XMPP** Cisco BroadCloud Applications, IM&P, file transfer and desktop sharing	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 80 443 1081 2208 8443 5222 5280 to 5281 52644 to 52645
SBC Traffic **UC Endpoints**	**SIP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP / TCP 8933

SBC Traffic **UC Endpoints**	**RTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535
SBC Traffic **UC Endpoints**	**SIP/TLS**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	TCP 8934
SBC Traffic **UC Endpoints**	**SRTP**	Dallas Chicago New York Los Angeles	128.177.36.0/26 199.59.65.0/25 135.84.171.0/25 199.19.197.0/24 128.177.14.0/25 199.59.66.0/25 135.84.172.0/25 199.19.199.0/24 199.59.71.0/25 199.59.70.0/25	UDP 19560 to 65535
UC-One SaaS	**XSI/CTI**	Customer Instance	35.239.73.31 35.224.174.163	TCP 8012
WebRTC **(Guest Client)**	**HTTPS** Desktop Sharing	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 8443
WebRTC **(Guest Client)**	**XMPP / TLS** IM&P	apps.broadcloudpbx.net	128.177.36.138 128.177.14.181	TCP 5222

WebRTC (Guest Client)	**SIP**	wrs.broadcloudpbx.net wrs02.broadcloudpbx.net	128.177.36.131 128.177.14.132 199.59.65.207 128.177.14.207	TCP 8060 8070
WebRTC (Guest Client)	**RTP**	wrs.broadcloudpbx.net wrs02.broadcloudpbx.net	128.177.36.131 128.177.14.132 199.59.65.207 128.177.14.207	UDP 16000 to 19000

Cisco BroadCloud DNS/NTP Service

Device	Protocol	Destination/DNS	IP	Destination Port
NTP	**NTP** Optional use of Cisco BroadCloud provided public NTP service	ntp.broadcloudpbx.net	199.59.65.181 199.59.66.181	UDP 123
DNS	**DNS** Optional use of Cisco BroadCloud provided DNS service for VPN customers	No DNS	199.59.65.181 199.59.66.181	UDP/TCP 53

North America - NA - Cisco BroadCloud Government FedRAMP

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Device	Protocol	Destination/DNS	IP	Destination Port
IP Phone / ATA / IAD	**NTP** Endpoint clock synchronization	ntp.broadcloudgov.us	139.177.94.5 139.177.95.5	UDP 123
IP Phone / ATA / IAD	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally		UDP/TCP 53
SBC Traffic IP Endpoints	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934
SBC Traffic IP Endpoints	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 to 65535
Cisco IP Phone & ATA	**HTTPS**	cisco.broadcloudgov.us	139.177.94.10 139.177.95.10	TCP 443
Polycom IP Phone	**HTTPS**	polycom.broadcloudgov.us	139.177.94.11 139.177.95.11	TCP 443
AudioCodes ATA	**HTTPS**	acodes.broadcloudgov.us	199.59.65.158 199.59.66.158	TCP 443
Patton ATA	**HTTPS**	patton.broadcloudgov.us	199.59.65.226 199.59.66.226	TCP 443

Registering SIP Trunking IP PBXs and Gateways

Device	Protocol	Destination/DNS	IP	Destination Port
SIP-T Endpoint	**NTP** Endpoint clock synchronization	Supplied Locally	Supplied Locally	UDP 123
SIP-T Endpoint	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53
SBC Traffic SIP-T Endpoint	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934

SBC Traffic SIP-T Endpoint	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 to 65535

Applications

Device	Protocol	Destination/DNS	IP	Destination Port
UC Endpoints (Clients)	**HTTP / HTTPS** **CAP** **XMPP** Cisco BroadCloud Applications, IM&P, file transfer and desktop sharing	apps.broadcloudgov.us	139.177.94.9 139.177.95.9	TCP 80 443 1081 2208 8443 5222 5280 to 5281 52644 to 52645
SBC Traffic UC Endpoints	**SIP/TLS**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	TCP 8934
SBC Traffic UC Endpoints	**SRTP**	Dallas Chicago	199.59.65.0/25 199.59.66.0/25	UDP 19560 to 65535
UC Endpoints (Clients)	**HTTPS** Personal Identity Verification (PIV) Card Authentication	ucone-piv.broadcloudgov.us	139.177.94.9 139.177.95.9	TCP 443

Cisco BroadCloud DNS/NTP Service

Device	Protocol	Destination/DNS	IP	Destination Port
NTP	**NTP** Optional use of Cisco BroadCloud provided public NTP service	ntp.broadcloudgov.us	139.177.94.5 139.177.95.5	UDP 123
DNS	**DNS** Optional use of Cisco BroadCloud provided DNS service for VPN Customers	No DNS	139.177.94.5 139.177.95.5	UDP/TCP 53

Canada - CA - Cisco BroadCloud Carrier

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Device	Protocol	Destination/DNS	IP	Destination Port
IP Phone / ATA / IAD	**NTP** Endpoint clock synchronization	ntp-ca.bcld.webex.com	135.84.173.152 135.84.174.152	UDP 123
IP Phone / ATA / IAD	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally		UDP/TCP 53
SBC Traffic IP Endpoints	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP / TCP 8933
SBC Traffic IP Endpoints	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535
SBC Traffic IP Endpoints	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
SBC Traffic IP Endpoints	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535
Phone Configs	**HTTPS**	dms-ca.bcld.webex.com polycom-ca.bcld.webex.com yealink-ca.bcld.webex.com cisco-ca.bcld.webex.com spa-ca.bcld.webex.com panasonic-ca.bcld.webex.com	135.84.173.155 135.84.174.155	TCP 443 80
Phone Configs	**HTTPS**	acodes-ca.bcld.webex.com	135.84.173.140 135.84.174.140	TCP 443 80

Registering SIP Trunking IP PBXs and Gateways

Device	Protocol	Destination/DNS	IP	Destination Port
SIP-T Endpoint	**NTP** Endpoint clock synchronization	Supplied Locally	Supplied Locally	UDP 123
SIP-T Endpoint	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53
SBC Traffic SIP-T Endpoint	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 8933
SBC Traffic SIP-T Endpoint	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535
SBC Traffic SIP-T Endpoint	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
SBC Traffic SIP-T Endpoint	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535

Applications

Device	Protocol	Destination/DNS	IP	Destination Port
UC Endpoints (Clients)	**HTTP / HTTPS** **CAP** **XMPP** Cisco BroadCloud Applications, IM&P, file transfer and desktop sharing	client-ca.bcld.webex.com	135.84.173.154 135.84.174.154	TCP 80 443 1081 2208 8443 5222 5280 to 5281 52644 to 52645
SBC Traffic UC Endpoints	**SIP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP / TCP 8933
SBC Traffic UC Endpoints	**RTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535

SBC Traffic UC Endpoints	**SIP/TLS**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	TCP 8934
SBC Traffic UC Endpoints	**SRTP**	Toronto Vancouver	135.84.173.0/25 135.84.174.0/25	UDP 19560 to 65535
WebRTC (Guest Client)	**HTTPS** Desktop Sharing	apps-ca.bcld.webex.com	135.84.173.154 135.84.174.154	TCP 8443
WebRTC (Guest Client)	**XMPP / TLS** IM&P	imp-ca.bcld.webex.com	135.84.173.158 135.84.174.158	TCP 5222
WebRTC (Guest Client)	**SIP**	wrscl01-ca.bcld.webex.com	135.84.173.132 135.84.173.133 135.84.174.132 135.84.174.133	TCP 8060 8070
WebRTC (Guest Client)	**RTP**	wrscl01-ca.bcld.webex.com	135.84.173.132 135.84.173.133 135.84.174.132 135.84.174.133	UDP 16000 to 19000

Cisco BroadCloud DNS/NTP Service

Device	Protocol	Destination/DNS	IP	Destination Port
NTP	**NTP** Optional use of Cisco BroadCloud provided public NTP service	ntp-ca.bcld.webex.com	135.84.173.152 135.84.174.152	UDP 123
DNS	**DNS** Optional use of Cisco BroadCloud provided DNS service for VPN customers	No DNS	135.84.173.152 135.84.174.152	UDP/TCP 53

Canada - CA – BroadCloud Carrier

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
NTP Time synchronization	Device IP	51494	UDP	135.84.173.152 135.84.174.152	123
DNS Name resolution	Device IP	Any	UDP / TCP	Customer defined	53
SIP Call Control Signalling	Device IP	5060 to 5080	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SRTP Call Media	Device IP	19560 to 19660	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 to 65535
Device Configuration and Firmware Management	Device IP	Any	TCP	135.84.173.155 135.84.174.155	443 80

Registering Gateways

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
NTP Time synchronization	Device IP	Any	UDP	Customer defined	123
DNS Name resolution	Device IP	Any	UDP / TCP	Customer defined	53
SIP Call Control Signalling	Device IP	8000 to 65535	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SRTP Call Media	Device IP	8000 to 48000 Can be reduced by the admin*	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 to 65535

* This is defined based on ***rtp-port range*** definition in the CUBE configuration.

Applications

Purpose	Src. IP	Src. Ports	Protocol	Dst. IP	Dst. Ports
NTP Time synchronization	Client Host IP	123	UDP	Host defined	123
DNS Name resolution	Client Host IP	Any	UDP / TCP	Host defined	53
SIP Call Control Signalling	Client Host IP	Any	TCP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	8934
SIP† Call Control Signalling	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	Any	TCP	Client Host IP	8934
SRTP Call Media	Client Host IP	Any	UDP	135.84.173.0/25 135.84.174.0/25 139.177.72.0/24 139.177.73.0/24	19560 to 65535
Client Configuration	Client Host IP	Any	TCP	135.84.173.154 135.84.174.154	80 443

† This flow is only required where there is no NAT between the Client and Webex Calling i.e. the Client Host is publicly addressed.

Europe - EMEA - Cisco BroadCloud Carrier

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Device	Protocol	Destination/DNS	IP	Destination Port
IP Phone / ATA / IAD	**NTP** Endpoint clock synchronization	ntp.broadcloud.eu ntp-eun.bcld.webex.com	85.119.57.218 85.119.56.218 170.72.0.146 23.89.76.146	UDP 123
IP Phone / ATA / IAD	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally		UDP/TCP 53
SBC Traffic IP Endpoints	**SIP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP / TCP 8933
SBC Traffic IP Endpoints	**RTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535
SBC Traffic IP Endpoints	**SIP/TLS**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	TCP 8934
SBC Traffic IP Endpoints	**SRTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535

Cisco SPA IP Phones & SPA122, SPA8000, SPA2102 ATAs	**HTTPS**	spa.broadcloud.eu	85.119.57.214 85.119.56.219	TCP 443
Cisco 3PCC Phones with MPP firmware, CIsco 191 and 192 ATAs, Cisco DECT	**HTTPS**	cisco.broadcloud.eu	85.119.56.198 85.119.57.198	TCP 443
Polycom IP Phone	**HTTPS**	polycom.broadcloud.eu	85.119.56.200 85.199.57.200	TCP 443
Snom IP Phone	**HTTPS**	snom.broadcloud.eu	85.119.56.201 85.119.57.201	TCP 443
Yealink IP Phone	**HTTP / HTTPS**	yealink.broadcloud.eu	85.119.56.205 85.119.57.205	TCP 80 443
Audiocodes IP Phone	**HTTPS**	acodes.broadcloud.eu acodes-eun.bcld.webex.com	85.119.56.211 85.119.57.211 170.72.0.141 23.89.76.141	TCP 443
Aastra/Mitel IP Phone	**HTTPS**	aastra.broadcloud.eu	85.119.56.199 85.119.57.199	TCP 443
Panasonic IP Phone	**HTTPS**	panasonic.broadcloud.eu	85.119.56.216 85.119.57.216	TCP 443
Gigaset IP Phone	**HTTPS**	gigaset.broadcloud.eu	85.119.56.219 85.119.57.219	TCP 443
Mediatrix IP Phone	**HTTPS**	mediatrix.broadcloud.eu	85.119.56.220 85.119.57.220	TCP 443
Obihai IP Phone	**HTTPS**	obihai.broadcloud.eu	85.119.56.227 85.119.57.	TCP 443
EUN Devices	**HTTPS**	dms-eun.bcld.webex.com cisco-eun.bcld.webex.com mediatrix- eun.bcld.webex.com patton-eun.bcld.webex.com polycom-eun.bcld.webex.com yealink-eun.bcld.webex.com	170.72.0.138 23.89.76.138	TCP 443

Registering SIP Trunking IP PBXs and Gateways

Device	Protocol	Destination/DNS	IP	Destination Port
SIP-T Endpoint	**NTP** Endpoint clock synchronization	Supplied Locally	Supplied Locally	UDP 123
SIP-T Endpoint	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53
SBC Traffic **SIP-T Endpoint**	**SIP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 8933
SBC Traffic **SIP-T Endpoint**	**RTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535
SBC Traffic **SIP-T Endpoint**	**SIP/TLS**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	TCP 8934
SBC Traffic **SIP-T Endpoint**	**SRTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535

Applications

Device	Protocol	Destination/DNS	IP	Destination Port
UC Endpoints (Clients)	**HTTP / HTTPS** **CAP** **XMPP** Cisco BroadCloud Applications, IM&P, file transfer and desktop sharing	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu umscl01-imp.broadcloud.eu client-eun.bcld.webex.com	85.119.56.197 85.119.57.197 85.119.56.197 85.119.57.197 23.89.76.137 170.72.0.137	TCP 80 443 1081 2208 8443 5222 5280 to 5281 52644 to 52645
SBC Traffic UC Endpoints	**SIP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP / TCP 8933
SBC Traffic UC Endpoints	**RTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535
SBC Traffic UC Endpoints	**SIP/TLS**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	TCP 8934
SBC Traffic UC Endpoints	**SRTP**	Amsterdam Frankfurt London	170.72.29.0/24 85.119.56.128/26 185.115.197.0/25 170.72.17.128/25 85.119.57.128/26 185.115.196.0/25	UDP 19560 to 65535

WebRTC (Guest Client)	**HTTPS** Desktop Sharing	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu	 85.119.56.197 85.119.57.197	TCP 8443
WebRTC (Guest Client)	**XMPP / TLS** IM&P	apps.broadcloud.eu apps2.broadcloud.eu apps1.broadcloud.eu	 85.119.56.197 85.119.57.197	TCP 5222
WebRTC (Guest Client)	**SIP**	wrs01.broadcloud.eu	85.119.57.231 85.119.56.231	TCP 8060 8070
WebRTC (Guest Client)	**RTP**	wrs01.broadcloud.eu	85.119.57.231 85.119.56.231	UDP 16000 to 19000
UC-One SaaS	**XSI/CTI**	Customer Instance	35.198.108.52 35.242.245.59	TCP 8012

Cisco BroadCloud DNS/NTP Service

Device	Protocol	Destination/DNS	IP	Destination Port
NTP	**NTP** Optional use of Cisco BroadCloud provided public NTP service	ntp.broadcloud.eu ntp-eun.bcld.webex.com	85.119.57.218 85.119.56.218 170.72.0.146 23.89.76.146	UDP 123
DNS	**DNS** Optional use of Cisco BroadCloud provided DNS service for VPN customers	No DNS	85.119.57.218 85.119.56.218 170.72.0.146 23.89.76.146	UDP/TCP 53

Australia - AU - Cisco BroadCloud Carrier

All destinations should be configured on the customer's firewall to ensure continuity of service.

IP Phones, ATAs and IADs

Device	Protocol	Destination/DNS	IP	Destination Port
IP Phone / ATA / IAD	**NTP** Endpoint clock synchronization	ntp.broadcloud.com.au	199.59.64.152 199.59.67.152	UDP 123
IP Phone / ATA / IAD	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally		UDP/TCP 53
SBC Traffic **IP Endpoints**	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP / TCP 8933
SBC Traffic **IP Endpoints**	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535
SBC Traffic **IP Endpoints**	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
SBC Traffic **IP Endpoints**	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535
Cisco SPA IP Phones & SPA122, SPA8000, SPA2102 ATAs	**HTTPS**	spa.broadcloud.com.au	199.59.64.155 199.59.67.155	TCP 443
Cisco 3PCC Phones with MPP firmware, CIsco 191 and 192 ATAs, Cisco DECT	**HTTPS**	cisco.broadcloud.com.au	199.59.64.143 199.59.67.143	TCP 443
Polycom IP Phone	**HTTPS**	polycom.broadcloud.com.au	199.59.64.144 199.59.67.144	TCP 443
Snom IP Phone	**HTTPS**	snom.broadcloud.com.au	199.59.64.148 199.59.67.148	TCP 443

Yealink IP Phone	**HTTP / HTTPS**	yealink.broadcloud.com.au	199.59.64.145 199.59.67.145	TCP 80 443
Audiocodes IP Phone	**HTTPS**	acodes.broadcloud.com.au	199.59.64.147 199.59.67.147	TCP 443
Aastra/Mitel IP Phone	**HTTPS**	aastra.broadcloud.com.au	199.59.64.146 199.59.67.146	TCP 443
Panasonic IP Phone	**HTTPS**	panasonic.broadcloud.com.au	199.59.64.151 199.59.67.151	TCP 443
Gigaset IP Phone	**HTTPS**	gigaset.broadcloud.com.au	199.59.64.215 199.59.67.215	TCP 443
Mediatrix IP Phone	**HTTPS**	mediatrix.broadcloud.com.au	199.59.64.211 199.59.67.211	TCP 443
Obihai IP Phone	**HTTPS**	obihai.broadcloud.com.au	199.59.64.216 199.59.67.216	TCP 443

Registering SIP Trunking IP PBXs and Gateways

Device	Protocol	Destination/DNS	IP	Destination Port
SIP-T Endpoint	**NTP** Endpoint clock synchronization	Supplied Locally	Supplied Locally	UDP 123
SIP-T Endpoint	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53
SBC Traffic **SIP-T Endpoint**	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 8933
SBC Traffic **SIP-T Endpoint**	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535
SBC Traffic **SIP-T Endpoint**	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
SBC Traffic **SIP-T Endpoint**	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535

Applications

Device	Protocol	Destination/DNS	IP	Destination Port
UC Endpoints (Clients)	**HTTP / HTTPS** **CAP** **XMPP** Cisco BroadCloud Applications, IM&P, file transfer and desktop sharing	apps.broadcloud.com.au apps1.broadcloud.com.au apps2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 80 443 1081 2208 8443 5222 5280 to 5281 52644 to 52645
SBC Traffic UC Endpoints	**SIP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP / TCP 8933
SBC Traffic UC Endpoints	**RTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535
SBC Traffic UC Endpoints	**SIP/TLS**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	TCP 8934
SBC Traffic UC Endpoints	**SRTP**	Melbourne Sydney	199.59.64.0/25 199.59.67.0/25	UDP 19560 to 65535
WebRTC (Guest Client)	**HTTPS** Desktop Sharing	apps.broadcloud.com.au apps1.broadcloud.com.au app2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 8443
WebRTC (Guest Client)	**XMPP / TLS** IM&P	apps.broadcloud.com.au apps1.broadcloud.com.au app2.broadcloud.com.au	199.59.64.140 199.59.67.140	TCP 5222
WebRTC (Guest Client)	**SIP**	wrs01.broadcloud.com.au	199.59.64.191 199.59.67.191	TCP 8060 8070
WebRTC (Guest Client)	**RTP**	wrs01.broadcloud.com.au	199.59.64.191 199.59.67.191	UDP 16000 to 19000

Cisco BroadCloud DNS/NTP Service

Device	Protocol	Destination/DNS	IP	Destination Port
NTP	**NTP** Optional use of Cisco BroadCloud provided public NTP service	ntp.broadcloud.com.au	199.59.64.152 199.59.67.152	UDP 123
DNS	**DNS** Optional use of Cisco BroadCloud provided DNS service for VPN customers	No DNS	199.59.64.152 199.59.67.152	UDP/TCP 53

Global

Web Portal Access

Device	Protocol	Destination/DNS	IP	Destination Port
All User Computers (includes ExamiNet)	**HTTP / HTTPS** Service Provider Portal Dashboards	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142 199.59.64.236 199.59.67.236	TCP 80 443
ExamiNet Computers	**HTTP** ExamiNet testing to validate bandwidth availability and network performance metrics	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au examinet-ca.bcld.webex.com	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142 135.84.173.157	TCP / UDP 1025
Examinet Computers	**HTTP** ExamiNet testing to verify port is accessible	examinet.adpt-tech.com examinetbeta.broadcloudpbx.com examinet.broadcloud.eu examinet.broadcloud.com.au	128.177.36.152 128.177.36.186 85.119.57.240 199.59.64.142 199.59.64.236 199.59.67.236	TCP 8933 to 8943 19560 to 65535
ExamiNet Computers	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53

Examinet - Packetsmart Access

Device	Protocol	Destination/DNS	IP	Destination Port
All User Computers (includes ExamiNet)	**HTTP / HTTPS** Service Provider Portal Dashboards	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com examinetpsde.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP 80 443

ExamiNet Computers	**HTTP** ExamiNet testing to validate bandwidth availability and network performance metrics	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com examinetpsde.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP / UDP 1025
Examinet Computers	**HTTP** ExamiNet testing to verify port is accessible	examinetpsusa.broadcloudpbx.com examinetpsuk.broadcloudpbx.com examinetpsde.broadcloudpbx.com	128.177.36.194 85.119.57.206 85.119.56.206	TCP 8933 to 8943 19560 to 65535
ExamiNet Computers	**DNS** For resolving configuration server A Records and call control SRV Records	Supplied Locally	Supplied Locally	UDP/TCP 53

Appendix A - Fraud

Fraud Prevention

Securing all aspects of our service against fraud is a key priority for BroadSoft, this section details prevention measures.

All customer premises equipment (CPE) that requires a configuration file from the service is centrally managed against fraud. All SIP authentication passwords are both complex and encrypted within the signaling to ensure no possibility for them to be intercepted. The administration of the password is managed by BroadSoft and is not accessible by end customers with the device web access portal also closed.

Where a password is required for a manually configured device, such as an IP PBX or Media gateway, the provisioning portal on the platform will randomly generate a complex password that should be used within the CPE.

Fraud Detection

BroadSoft operates a complex fraud detection tool which actively scans calling patterns on the system for suspicious activity. The system can take proactive steps to prevent fraud when calling patterns are detected as abnormal and block them.

The deployment of this tool should not be treated as a safety net allowing for deployment/use of a poorly protected CPE device.

IP PBX / Media Gateways and Fraud

As detailed within the previous sections rigorous steps have been taken to protect the core service and we would recommend that the same level of rigor is applied to customer endpoints, be they IP Phone, IP PBX or Media Gateways. Due to the requirement to manually configure and potentially allow remote access for support and maintenance purposes IP PBXs and Media Gateways can be exposed to unauthorized access.

To prevent this from occurring, our Partners should follow the best practice recommendations in *Section 2* and *Section 3* of this document.

Partner Actions in the case of Fraud detected

If unauthorized access occurs and we inform our Partner that their customer has been barred from making and forwarding high cost calls, as a minimum our Partner should:-

- Check the customer's network is secure
  - The firewall should only allow access to the IPs, ports and protocols required for service in the relevant part of Section 4, Port Requirements
- Remove the device from the public internet where applicable
- Change the CPE access credentials
  - Ensure that the access credentials adhere to the best practices for passwords in *Section 3.1* and *Section 3.3.3*
- Change the SIP authentication details