TelePacific COMMUNICATIONS

UCx Local Area Network (LAN) Deployment Guide

Introduction

Customers wishing to deploy TelePacific's UCx service are required have a solid knowledge and understanding of their IP infrastructure. To ensure a successful UCx deployment, customers must inspect and properly configure each network service and component which makes up their LAN. This guide serves to identify those network services and components which should be considered.

Top 10 UCx Deployment Challenges

Here is a Top 10 list of challenges customers typically face during an UCx deployment. This short list illustrates how important it is for customers to review their network topologies. Each of these problem areas is discussed throughout this guide in more detail. Administrators can glance at this list to get an understanding of the types of configuration details contained in this guide.

#10 – Incorrect Firewall Settings (One Way Audio)
#9 – DHCP Address Pool Exhausted (Unable to Obtain an IP Address)
#8 – Uncertified Cat5 Cable (Static Heard on Calls)
#7 – Un-terminated Cat5 Network Jack (Unable to Plug in Phone)
#6 – Incorrect QOS Settings (Garbled Voice during Large Downloads)
#5 – Firewall License Restrictions (Unable to Place Call or Register)
#4 – IP Address Conflict (DHCP Address Statically configured on PC)
#3 – Incorrect Amplified Headset Settings (Static/Echo Heard on all Calls)
#2 – Incorrect FTP Server Settings (Failure to Register)
#1 – Speed/Duplex Mismatches (Voice Audio fades in/out)

IP Addressing

UCx phones are nothing more than specialized computers which process analog speech to Voice Over IP (VoIP). An UCx phone deployment of 30 phones is similar to deploying 30 additional computers on a customer's network; each UCx device requires an IP address. By default, UCx phones will request an IP address assignment using DHCP.

DHCP

Most customers use DHCP to assign IP addresses to their UCx phones. The phone will request a DHCP lease upon boot-up and will follow the lease timeout set by the DHCP server. The UCx phones require a minimum DHCP configuration to operation normally. The following are required to provide the phones with a working network configuration:

Option 3 – Router
Option 4 – Time Server
Option 5 – DNS Servers
Option 15 – DNS Domain Name

DHCP Reservations

Customers may statically assign IP Addresses to each UCx phone by using a DHCP reservation. This is a good idea for network administrators who want to assign all VoIP devices a specific IP Addresses of the DHCP scope (192.168.1.0/24 is the DHCP scope, but 192.168.1.128-196 contains the DHCP reservations for all VoIP devices). DHCP reservations are configured by the customer on their DHCP server by assigning an IP address within the DHCP scope to the MAC address of the phone. The MAC address of an UCx phone is also the serial number.

Statically Assigned IP Address

Customers who cannot support IP address assignment via DHCP have the option to statically assign IP address information on each UCx phone. An instructional guide may be requested on this procedure if required.

Option 66 – Boot Server

Customers who use Option 66 or "Boot Server" on their network will require a special configuration on each phone to ignore this DHCP option. Customers typically use Option 66 when they have Thin-Clients or WYSE terminals deployed on their network. Option 66 is used to identify a server which DHCP clients can obtain configuration and/or application information from. By default, UCx phones will attempt to use the Option 66 Boot Server; this will cause the phones to fail their initial setup. Customers who utilize Option 66 should notify their Account Executive during the ordering process so the phones will be configured to disregard the Option 66 setting.

LAN Cabling

Customers wishing to deploy VoIP should ensure their networks are wired with at least certified Cat5 wiring and adaptors. Cat5 terminations (4 pairs) is the minimum required to support Power over Ethernet (PoE). Some legacy networks are wired with Cat3 (2 pair) which will support a 10BaseT and possibly VoIP at 10MB but will not support PoE nor speeds greater than 10MB. Each location a customer wishes to deploy an UCx phone must have a readily accessible network jack to accept an RJ-45 male adaptor.

Customers wishing to run Gigabit speed networks required at least Cat5E wiring and adaptors. The use of Cat6 is required for 10GIG networks and greater.

Configuration Management

TelePacific has deployed two different platforms to manage device configuration: DMS and FTP. DMS is used for all new customers moving forward. FTP is used by existing customers who have not yet converted to DMS.

Phones are required to access TelePacific's configuration management servers periodically. During the startup process, phones will download configurations and software. Periodically going forward, the phones will upload log files used to assist in troubleshooting. Phones will also push localized changes made by the end user.

If Internet access will not be available to the phones from the customer network, the customer must notify their Account Executive during the order stages to identify the network limitations. A

secured gateway IP address may be configured to allow the phones to access the public server through an MPLS WAN IP address.

DMS Server

TelePacific utilizes a new secured public DMS set of servers which supports HTTP/HTTPS/TFTP/FTP protocols. Which protocol is used depends on the device and how it is configured to access the server. TelePacific UCx phones are programmed and tested during the shipping process to access DMS to retrieve their configurations.

Each phone on the customer's network must be able to HTTP/HTTPS file transfer (TCP/80 & TCP/443) with voice.dsci-net.com and voice2.dsci-net.com; each FQND can resolve to multiple servers. Customers who use a TelePacific MPLS product should make arrangements to ensure the phones are not restricted from accessing the HTTP/HTTPS servers using the customer's internet gateway.

FTP Server

TelePacific utilizes a secured public FTP server to maintain UCx configuration files. Each phone is provisioned to login to the FTP server using a username and password which is unique to each customer. Once logged into the FTP server, the phone will have access to download newer software, applications, and configuration files. The FTP server is also used by the phone to upload user customizations as well as various log files to assist troubleshooting.

Each phone on the Customer's network must be able to FTP file transfer (TCP/20 & TCP/21) with ftp.dsci-net.com. Customers who use a TelePacific MPLS product should make arrangements to ensure the phones are not restricted from accessing the FTP server using the customer's internet gateway.

Powering Phones

Each UCx phone may be powered in two methods; by an AC power supply or through Power over Ethernet (PoE) enabled network.

An AC power supply may be used to provide the phone power from a nearby wall outlet. Phones which use a power supply are dependant upon the power supply for operation.
PoE is typically made available to the phone by a PoE enabled network switch or through a PoE injector cable. Customers may wish to consider the use of PoE to centrally manage power required to support the UCx deployment.

Uninterrupted Power Supplies (UPS) are highly recommended for all customer network and VoIP devices. TelePacific customers are highly encouraged to use UPSs to protect network investments and provide business continuity during a power outage. In the event of a power outage, distributed PoE devices may be centrally supported by UPS protected PoE network switches. The UPS can be sized to supply power to the network switches and phones throughout the outage. Customer should also verify their DMARC equipment is also UPS protected (firewalls and routers).

As each UCx model consumes a differently amount of power, network administrators should ensure their PoE enabled switches have the capacity to support the number of phones the customer wishes to deploy. Some switch manufacturers enable PoE on each switch port but

restrict the total power available to all ports. Power requirements for Polycom phones are included in the Polycom Technical Bulletin TB48152 – Polycom Power Consumption.pdf

http://support.polycom.com/global/documents/support/setup_maintenance/products/voice/Power_Consumption_and_Management.pdf

Polycom phones support both PoE standards: Cisco and IEEE 802.3af. Optional PoE adaptor cables are required for the Polycom 300/301 and 500/501 phones to use switch based PoE. Polycom 601 phones are not supported on Cisco switches.

Customers wishing to deploy ATAs (analog terminal adapters) to support analog phones over a VoIP network are required to provide a power source near where the ATA is to be placed. TelePacific's ATAs do not currently support PoE.

Quality of Service (QoS)

QOS is a feature supported on most managed network switches and routers to ensure priority is given to specific network traffic. For a successful UCx deployment, Voice traffic must be identified, classified, and given priority through bottleneck segments.

Polycom UCx Phones will mark all VoIP traffic with an IP Precedence bit of 5 by default. All non-VoIP traffic from the phone or from the PC port on the back of the phone will be marked with an IP Precedence bit of 3. Network administrators can configure their LAN switches to look at the Precedence bit, and give the highest priority to traffic marked with a 5.

Once network traffic reaches the TelePacific Managed Router, TelePacific will reclassify all traffic based on destination network. All traffic going to the TelePacific outbound proxy will be marked with an IP Precedence bit of 5, all other traffic will be marked with a 3.

TelePacific uses strict priority queuing on TelePacificI managed routers. This means that traffic marked with a 5 is given the highest priority over a T1, or NxT1 solution across TelePacific's Backbone. Likewise, VoIP traffic destined for the customer's network is reclassified based on source network. Any traffic originating from T's outbound proxy is given strict priority queuing over the customer's T1 or NxT1 solution.

Priority queuing is configured to give up to 85% of the outbound bandwidth to VoIP traffic. If there is limited VoIP traffic at any time, all unused bandwidth is available for normal data traffic. TelePacific does not use Committed Access Rate (CAR) or Rate-Limits. These technologies effectively dedicate a portion of bandwidth to a specific traffic type.

Bring Your Own Broadband (BYOB)

TelePacific supports BYOB customers who have broadband based Internet service. BYOB customers typically have access to higher bandwidth than a business class T1/Ethernet product from TelePacific. The difference between BYOB and TelePacific services is the availability of QOS. TelePacific can apply QOS on both sides if its data products to ensure phone calls receive the highest priority over web and email.

Customers who access TelePacific using BYOB and perform basic tests to see what their network access is like. TelePacific has documented some basic windows tool to help identify bottlenecks which can affect any type of traffic (including VOIP).

KB Troubleshooting Slow Internet with Tools:
https://dash.dscicorp.com/#page=Kb&kbId=1065

Tools like pingpath can show where latency is being introduced. Customers can test to the following two endpoints to test against:

pingpath 204.11.148.254 (Charlestown)
pingpath 209.104.247.254 (Waltham)

Reviewing the results should show zero (0) packet loss.
Final RTT should be less than 100ms to support voip.
The final number of hops should be less than 25.

BYOB customers are bound to the configuration requirements within this document and must be aware there are benefits no longer available to them as TelePacific cannot control QOS and bandwidth dedication over the Internet.

Network Capacity

Customers should ensure they will have adequate network capacity to support the number of simultaneous phone calls desired as well as the bandwidth over their LAN. Capacity is typically only a factor when ordering T1s but attention to the LAN is also required.

TelePacific's converged products allow for VoIP and Data to traverse a shared T1 configured with QOS. As VoIP and Internet traffic are considered data, T1 channelization is not required, so there is no requirement to isolate 64K channels to data and 64K channels to VoIP.

TelePacific has selected G.722 HD as the primary VoIP codec as it offers High-Definition fidelity and consumes 80 kilobits of bandwidth in each direction. Alternatively, when G.722 is not available, phones can utilized G.729 which offers compression to reduce bandwidth requirements to 40 kilobits of bandwidth in each direction.

If a customer orders a TelePacific T1 which is configured with QOS, the customer can expect to simultaneously have 16 G.722 calls, 30 G.729 calls, or 22 G.711 calls without degradation.

Depending on the type of traffic which traverses the Customer's LAN and the speed of switch interconnections, customers should monitor their switch ports to ensure unlink interfaces have enough capacity to support VoIP.

Network Topology

There are a few general rules regarding network topology that customer network administrators should be aware of. Each of these important factors should be considered when determining if a network is VoIP capable.

Uplink ports are those ports which interconnect network devices together. Uplink ports should always be statically set for speed and duplex to ensure auto negotiation is never a cause of a speed/duplex mismatch. Devices which only support 10baseT are acceptable as long as they

can be set for Full Duplex. Speed/Duplex mismatches account for 90% of VoIP call quality issues.

Hubs are not supported with VoIP deployments and must be replaced with switches (preferably managed switches). Hubs broadcast traffic by design and will ultimately cause network congestion which will degrade call quality. Hubs are typically unmanaged which means there is no way to hard code speed/duplex settings.

Network switches should be deployed in a tree (or hub/spoke) topology versus in a cascade topology. This will ensure that all network traffic originating from one switch has the same number of Ethernet hops to reach the network gateway as any other switch. Care should be taken to avoid any Ethernet device from being more than three hops away from a network gateway.

Spanning-Tree portfast (on Cisco switches) and Spanning-Tree edgeport (on Adtran switches) should be enabled on each port a phone will be connected to. These commands allow the network port to turn on quickly and begin passing traffic faster than normal. As the UCx phones boot fairly quickly, if the network port does not unblock fast enough, the phone may try to obtain a DHCP lease prior to being able to pass network traffic. The phone will display an "Unable to obtain IP Address" if this happens.

NOTE: Spanning-Tree portfast / edgeport commands should not be enabled on uplink ports, nor ports used for mutli-link connections which may create a network loop.

Downlink ports are considered switch ports which phones plug into. Downlink ports should be configured for auto speed and auto duplex. Polycom phones currently support a maximum speed of 100 Mb. PCs plugged into the back of the Polycom phone should also be set for auto speed and auto duplex. This will ensure proper network negotiation during bootup.

Customer sites with multiple gateways require special attention as a customer may wish all network traffic to go to one router, and all VoIP traffic to go through another router. For these deployments, it is desirable to give the shortest path to the most critical traffic. This is accomplished by making the default route for the LAN to be the router closest to the VoIP network, and let that router direct the less critical traffic to the WAN router or out the internet router. Customers who support a WAN and an Internet connection at a single site typically use this to strip off VoIP to TelePacific and then route everything else over the WAN route.

Analog Terminal Adaptors

ATAs are devices which convert SIP based phone service into an Analog signal which can be used to support existing FAX machines, cordless phones, or any other legacy phone technology.

Types of ATA

There are many types of ATAs TelePacific can use to support a Customer with analog services. The main difference between the various devices is the number of analog ports each device supports and the customer handoff. Here are the three main ATAs TelePacific uses today:

Linksys PAP2T Supports:

- DHCP Client

- 2FXS analog ports
- 2 RJ-11 ports

Linksys SPA3000 supports:

- DHCP Client & Server
- 2FXS analog ports
- 1FXO analog ports
- 3 RJ-11 ports

Adtran TA900 series supports

- Full AOS Router
- 4-24 FXS analog ports
- 4 FXO analog ports
- Up to 4 RJ-11 ports
- Up to 2 RJ-45 Ethernet ports
- Amphenol connector, requires a cable and 66 Block for punch-down termination

Choosing an ATA

The ATA selection process is based on the Customer's physical building layout and how their phone plant is run. Customers who have existing phones wired back to a central closet may have the ATA installed in the closet. A Customer who has fax machines on opposite sides of the building may require two separate ATA. Customers who require a large number of Analog ports may have the ATAs stacked on top of each other, to provide multiples of 24 lines.

Remote Access

Unlike Polycom phones, ATAs are not centrally managed by TelePacific which means the ATA is pre-configured and installed on the customer premise. Once installed, TelePacific will require remote access to make configuration changes and to troubleshoot any Customer reported issues.

Customers are required to provide network connectivity and power to each ATA. Customers are also required to provide TelePacific with remote network access for the purposes of remotely managing the ATA configurations. To achieve remote access, ATAs should be:

1. Static IP Addressed or assigned a DHCP reservation
2. Firewalls must have a static port mapping created to each ATA

A single public IP address may be mapped to up to 65,000 ATAs, here is an example of how the public IP address 204.1.2.3 may be mapped to 3 internal ATAs:

Public IP	Public Port	Private IP	Private Port
204.1.2.3	TCP/8001	192.168.1.1	TCP/80
204.1.2.3	TCP/8002	192.168.1.2	TCP/80
204.1.2.3	TCP/8003	192.168.1.3	TCP/80

The firewall port mapping is critical to allow TelePacific remote technical access to troubleshoot each ATA. Remote access is required before TelePacific will dispatch a Field Technician to

continue troubleshooting an issue. Applicable charges will be assessed if remote access is not provided and a Field Dispatch is required.

Supported Security Devices

Customers are ultimately responsible for the security of their networks. The introduction of TelePacific's VoIP service adds additional intricacies to a customer's network which require careful consideration.

Most customers utilize private IP Address assignments on their LAN and use Network Address Translation (NAT) or Port Address Translation (PAT) on a router or firewall. Manufacturers are adding features and functionalities to their devices which may hinder the proper operation of the VoIP deployment.

TelePacific maintains an internal list of supported and unsupported devices and known workarounds. Account Executives can access to this to verify a customer's device has been used before.

https://dash.dscicorp.com/#page=Kb&kbId=2025

Fully Supported Security Devices

TelePacific will support the following network device which have been tested and proven to work with UCx deployments.

- Cisco ASA/PIX Firewalls
- Cisco IOS Routers (Using NAT/PAT)
- Adtran Total Access Routers
- Adtran NetVanta Routers
- NetScreen 5GT/XT
- Juniper

Partially Supported Security Devices

TelePacific supports the following less expensive security devices which typically support VoIP deployments for Small Office Home Office (SOHO) deployments and BYOB customers.

- Linksys
- Netgear
- D-Link
- Belkin

Non-Supported Security Devices

TelePacific will not support customers who experience problems with one of the following devices in their Network Topology. Once the device has been removed or replaced, TelePacific will begin troubleshooting the problem if it persists.

- Network Everywhere NR041
- Devices which have reached their End-of-Life
- Devices which run software which has reached their End-of-Life

Connection Timeouts

TelePacific has deployed an ACME Packet Session Border Controller, which is used to manage the device behind the customer's security device. The ACME Packet maintains a pinhole

through the firewall which keeps the UDP connection alive. If an inbound call to the customer's phone is made, the ACME sends the call through the opened port to the phone. If the firewall closes the port prematurely, the call will die at the firewall and the phone will never ring.

License Considerations

As each UCx phone consumes an IP Address, customers must ensure they have adequate licensing if their firewall restricts the number of connections or hosts it will support. For example: If a customer's firewall has a 10 user license, and there are 3 UCx phones and 8 computers, the site requires a total of 11 licenses through a firewall. Firewalls will typically block one IP address until connections from another are closed.

Configuration Notes

The following section has been documented to help the customer network administrator facilitate the appropriate changes prior to an UCx demonstration or UCx deployment.

TelePacific deploys the UCx product in such a way to reduce the amount of time a customer must spend configuring their Security devices. Typically, a customer's network is UCx ready if the customer supports a security device (router or firewall) which performs basic NAT. General network connectivity must be established prior to installing phones on the customer LAN. This means that NAT/PAT should be functional and provide basic Internet browsing prior to installing VoIP phones.

If a customer has locked down their network using IP Access Lists (ACL) or firewall policies, the customer should verify the following ports are not restricted from making outbound connections from the Customer's LAN. The customer should not need to make any inbound allotments for the proper functionality of the UCx product.

FTP.dsci-net.com

FTP	TCP/20-21 outbound to host 204.11.148.130

Time.dsci-net.com

NTP	TCP/123 outbound to host 204.11.148.0/24
NTP	TCP/123 outbound to host 204.14.71.14

SBC Charlestown Public

SIP	TCP/5060 outbound to host 204.11.148.40
SIP	UDP/5060 outbound to host 204.11.148.40
RTP	UDP/60000-65535 to host 204.11.148.40
SIP	TCP/5060 outbound to host 209.104.255.30
SIP	UDP/5060 outbound to host 209.104.255.30
RTP	UDP/60000-65535 to host 209.104.255.30

SBC Somerville Public

SIP	TCP/5060 outbound to host 209.104.247.240
SIP	UDP/5060 outbound to host 209.104.247.240
RTP	UDP/60000-65535 to host 209.104.247.240

XSP-WEB1.dsci-net.com

HTTP	TCP/80 outbound to 204.11.148.46
HTTPS	TCP/443 outbound to 204.11.148.46
FTP	TCP/20-21 outbound to 204.11.148.46
OCI	TCP/2208 outbound to 204.11.148.46

XSP-WEB2.dsci-net.com

HTTP TCP/80 outbound to 204.11.148.142
HTTPS TCP/443 outbound to 204.11.148.142
FTP TCP/20-21 outbound to 204.11.148.142
OCI TCP/2208 outbound to 204.11.148.142

XSP-REC1.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.47
HTTPS TCP/443 outbound to 204.11.148.47

XSP-REC2.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.139
HTTPS TCP/443 outbound to 204.11.148.139

XSP-CC1.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.48
HTTPS TCP/443 outbound to 204.11.148.48

XSP-CC2.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.138
HTTPS TCP/443 outbound to 204.11.148.138

XSP-XSI1.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.45
HTTPS TCP/443 outbound to 204.11.148.45

XSP-XSI2.dsci-net.com
HTTP TCP/80 outbound to 204.11.148.141
HTTPS TCP/443 outbound to 204.11.148.141

UMS1.dsci-net.com
XMPP TCP/5222 outbound to 204.11.148.44
XMPP TCP/1081 outbound to 204.11.148.44
HTTPS TCP/443 outbound to 204.11.148.44

UMS2.dsci-net.com
XMPP TCP/5222 outbound to 204.11.148.143
XMPP TCP/1081 outbound to 204.11.148.143
HTTPS TCP/443 outbound to 204.11.148.143

USS1.dsci-net.com
HTTPS TCP/8443 outbound to 204.11.148.49

USS2.dsci-net.com
HTTPS TCP/8443 outbound to 204.11.148.145

WRS1.dsci-net.com
HTTPS TCP/8060 outbound to 204.11.148.4
HTTPS TCP/8070 outbound to 204.11.148.4
STUN TCP/3478 outbound to 204.11.148.4

WRS2.dsci-net.com
HTTPS TCP/8060 outbound to 204.11.148.150
HTTPS TCP/8070 outbound to 204.11.148.150
STUN TCP/3478 outbound to 204.11.148.150

CounterPath Bria
HTTP TCP/80 outbound to bria.dsci-net.com (currently 209.104.229.128)
HTTPS TCP/443 outbound to secure.counterpath.com (currently 69.90.51.170)

Manufacturers are adding features to their security devices which alter VoIP traffic as it traverses the firewall. These devices attempt to mask the internal IP information required by the

ACME Packet to properly communicate with the UCx phone. For this reason, it is required to disable all VoIP Application awareness features configurable on the firewall. Failure to do so will cause one way audio issues and call route failures.

Cisco PIX Firewalls

Cisco's Fixup performs application layer modifications which are not desirable for TelePacific's VoIP. There are two global Fixup commands which must be disabled to allow the SIP protocol to traverse the security device unchanged.

All other commands, to include session timers, should be left at their default. Administrators should note that if a "clear xlate" is performed, UCx phones will cease to function correctly, until they are rebooted or the phones re-register.

```
Config t
        no fixup protocol sip 5060
        no fixup protocol sip udp 5060
```

Cisco ASA Firewalls

Like Cisco's PIX Firewall, the ASA version needs to have SIP ALG services disabled.
To determine whether the Cisco PIX or Cisco ASA security appliance is configured to support inspection of sip packets, log in to the device and issue the CLI command show service-policy | include sip. If the output contains the text Inspect: sip and some statistics, then the device has SIP inspection enabled. The following example shows a Cisco ASA with SIP inspection enabled:

```
asa#show service-policy | include sip
    Inspect: sip, packet 123612, drop 23, reset-drop 0
```

```
Config t
        policy-map global_policy
                class inspection_default
                        no inspect sip
```

Cisco IOS Routers (Using NAT/PAT)

It is recommended that IP Reflexive ACLs are enabled to ensure valid two-way communication is not restricted. Reflexive ACLs will allow dynamic port mappings for SIP and RTP to occur when using PAT.

Newer IOSs have a NAT Service which performs packet modification much like fixup for Cisco Firewalls which needs to be disabled. Administrators should note that if a "clear ip nat translation *" is performed, UCx phones will cease to function correctly, until they are rebooted or re-register.

```
Config t
        No ip nat service sip udp port 5060
```

IP Inspect is part of Cisco's Firewall feature set and is not supported.

Adtran Total Access (Using NAT/PAT)

Adtran routers which have “ip firewall” enabled should have the following two global configuration entries disabled

```
Config t
        no ip firewall alg h323
        no ip firewall alg sip
```

Juniper Netscreen 5-GT

The Netscreens have a Denial of Service (DoS) feature for UDP traffic which should be disabled. If this feature triggers, VoIP traffic will be blocked, causing call termination. Netscreen v5.3.0r1.0 (Firewall+VPN) was tested and certified by TelePacific as a supported Security Device.

```
Security Mode:  trust-untrust
ALG SIP:  DISABLED
UDP Flood Protection:  DISABLED
```

SonicWall SonicOS

The following SonicWall settings should be set to allow for UCx Phones to properly communicate through the firewall.

```
Enable Consistent NAT:  DISABLED
Enable SIP Transformations:  DISABLED
Enable H.323 Transformations:  DISABLED
```

FortiGate Firewalls

The following FortiGate Firewall Session Helper must be removed to disable the firewall’s ability to manipulate SIP traffic.

```
show sys session-helper
        #find the SIP helper ID #
config sys session-help
        #delete #
end
```

More hardware configuration notes will be added as additional equipment is certified.