Horizon Network Configuration Guidelines

Contents

2.0 Configuration of Non Assured Access routers

2.1 Access Control

Network administrators must ensure that the following IP addresses and ports (both directions) are available and not blocked by firewalls. If these ports are not opened (i.e. a customer or network based firewall is blocking them), or IP addresses allowed, Horizon will not function correctly.

Assured recommends that only trusted IPs are allowed to send and receive traffic via port 5060

The requirements need to be checked by the Channel Partner with the customer / access provider as part of the Sales process to ensure that the solution will be fit for purpose for Horizon. This applies to all ISPs.

Domain Name	Record Type	IP Address	Ports	Function
xsp.unlimitedhorizon.co.uk	*A*	*88.215.61.171* *88.215.61.173*	*TCP 80, 443, 8011*	*Device provisioning*
xsi.unlimitedhorizon.co.uk	*A*	*88.215.60.155* *88.215.60.156*	*TCP 80, 443, 8011*	*Soft clients and Integrator*
clients.unlimitedhorizon.co.uk	*A*	*88.215.60.162* *88.215.60.163*	*TCP 443*	*Receptionist*
im.unlimitedhorizon.co.uk	*A*	*89.149.156.75*	*TCP 5222*	*Instant messaging and presence (for softphone clients)*
ntp.business-access.co.uk	*A*	*88.215.61.81* *88.215.63.145*	*UDP 123*	*NTP for time/date display*
europe.pool.ntp.org	*A*	*178.79.162.34* *78.47.138.42* *148.251.127.15* *46.165.212.205*	*UDP 123*	*NTP for time/date display* *Polycom*
ldap.unlimitedhorizon.co.uk	*A*	*88.215.60.129* *88.215.60.132*	*TCP 389*	*Corporate Directory Service*

sip.unlimitedhorizon.co.uk *sip0.unlimitedhorizon.co.uk* *sip1.unlimitedhorizon.co.uk* *sip2.unlimitedhorizon.co.uk* *sip3.unlimitedhorizon.co.uk* *sip4.unlimitedhorizon.co.uk* *sip5.unlimitedhorizon.co.uk* *sip6.unlimitedhorizon.co.uk* *sip7.unlimitedhorizon.co.uk* *sip8.unlimitedhorizon.co.uk*	*SRV*	*N/A*	*UDP 53*	*SRV Records for Horizon Voice Signalling & Media Traffic*
mobile-sip1.unlimitedhorizon.co.uk *mobile-sip2.unlimitedhorizon.co.uk*	*SRV*	*N/A*	*UDP 53*	*SRV Records for Horizon Mobile/PC Client Voice Signaling & Media Traffic*
node1.sip.unlimitedhorizon.co.uk	*A*	*88.215.63.171*	*UDP 5060, TCP 5080*	*SBC SIP signalling*
node2.sip.unlimitedhorizon.co.uk	*A*	*88.215.63.21*	*UDP 5060, TCP 5080*	*SBC SIP signalling*
node3.sip.unlimitedhorizon.co.uk	*A*	*88.215.58.1*	*UDP 5060, TCP 5080*	*SBC SIP signalling*
node4.sip.unlimitedhorizon.co.uk	*A*	*88.215.55.33*	*UDP 5060, TCP 5080*	*New SBC SIP signalling*
node5.sip.unlimitedhorizon.co.uk	*A*	*88.215.54.1*	*UDP 5060, TCP 5080*	*New SBC SIP signalling*
Domain Name	*Record Type*	*IP Address*	*Ports*	*Function*
N/A	*N/A*	*88.215.58.2*	*UDP 10000- 60000*	*SBC RTP Traffic*
N/A	*N/A*	*88.215.63.172*	*UDP 10000- 60000*	*SBC RTP Traffic*
N/A	*N/A*	*88.215.54.2*	*UDP 10000 - 60000*	*New SBC RTP Traffic*
N/A	*N/A*	*88.215.55.34*	*UDP 10000 - 60000*	*New SBC RTP Traffic*
N/A	*N/A*	*88.215.63.22*	*UDP 10000- 60000*	*SBC RTP Traffic*

2.2 UDP Fragmentation during Horizon communications.

In some instances the size of the UDP packets transmitted between the Horizon platform and customer handsets will exceed the default 1500 byte payload, when this happens packet fragmentation will occur. **It is the responsibility of the Channel Partner and/or End User to ensure that any in path CPE is able to support UDP fragmentation**. It is also advised that a check is made to confirm that any further applications/functions running on the CPE do not interfere with the reassembly of fragmented UDP packets.

If UDP fragmentation is not allowed on CPE network devices the following features may not function correctly.

- BLF (Busy Lamp Field)

- Feature Synchronisation (DND, Call Forward Busy, Call Forward Always & Call Forward Unreachable/No Answer)

2.3 SIP ALG

SIP Application Layer Gateway (ALG) is common in many of today's routers and in most cases enabled by default on enterprise, business and home broadband routers. Its primary use is to prevent problems associated to the router's firewalls by inspecting VOIP traffic packets, and if necessary modifying them to allow connection to the required protocols or ports.

On many business and home class routers Active SIP ALG will cause a mixture of problems by adjusting or terminating Horizon traffic packets in such a manner that they are corrupted and cause issues with the service, manifesting in a range of intermittent issues such as; one way audio, dropped calls, problems transferring calls, handset dropping registration and making or receiving internal calls.

SIP ALGs should be disabled on all CPE routers, we will not accept any faults or issues raised against Horizon if a SIP ALG is enabled.

For instructions on disabling this feature please refer to the specific router user guide. We have a limited selection of instructions for completing this via telnet which are available on the knowledge base under technical support > misc.

2.4 Keep Alives

Handsets are pre-configured to send UDP keep-alive messages towards the Horizon platform every 45 seconds using the SIP port. These messages keep the firewall pin-holes open which ensures the success of incoming calls.

2.5 NAT Port Translation

For Horizon handsets to register correctly, if using a router that requires setting up Dynamic Port Address Translation - Port Multiplexing option must be selected.

2.6 DNS

A public DNS service must be available to the Horizon handsets so that the domain names can be resolved to the associated IP addresses. SRV and A record types are used by the Horizon service. As best practice resilience of DNS needs to be considered hence both a primary and secondary DNS service should be configured as part of any deployment.

Assured's DNS servers are detailed below, please note these can only be used with Assured access.

Primary DNS Server	88.215.61.255
Secondary DNS Server	88.215.63.255

3.0 The LAN

3.1 Support for VLANS

Both Cisco and Polycom phones provided as part of the Horizon service have CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discover Protocol) enabled as default on delivery. These protocols, CDP (Cisco proprietary), and LLDP including LLDP-MED (vendor neutral), are link layer protocols used by network devices for advertising their identities and capabilities in order to assist with management of the local area network environment, specifically VLAN segregation.

If you wish to support either of these functions for VLAN configuration/selection on the customer LAN then you should enable the desired function on the customer's network equipment and disable the alternative option. For example if you wish to support CDP for a particular end user you should make sure LLDP is not configured as a live option on their network equipment and that CDP is enabled as a live option.

When using LLDP or CDP the Horizon phones will support and use any VLAN ID configured on the customer switching infrastructure (as part of the LLDP and CDP configuration) for both Voice and Data. If the customer wishes to daisy chain laptops or PC's using the switch port on the Horizon phones, any traffic from this port will be entered into the data VLAN.

Example VLAN set up (using CDP/LLP)

Data VLAN: 20

Voice VLAN: 30

What we do not support:

- Fixed VLAN ID's
- Static VLAN assignment either directly from the phone or from the core network.
- We cannot enable only **one** of the VLAN options (either CDP or LLDP). Both will always be enabled on Horizon phones and it is the customer's responsibility to enable/disable the required function on their network.

Please be aware Softphone Clients, ATA's and Wireless handsets (xxx) do not currently support VLAN

4.0 Firmware Upgrades

Horizon handsets are pre-configured to check for configuration and firmware updates every evening between 00:00 and 05:00.

Horizon handsets will only download new configuration or firmware files when they detect that a change has been made. Configuration files are typically ~70Kb or less, but firmware files are larger ranging between 3.5 to 57.5MB. Network administrators should consider these file downloads with regards to the bandwidth available on the access circuits the Horizon service runs over.

Device Type	Firmware file size
Cisco 122	10.0 MB
Cisco 232	11.3 MB
Cisco 501	4.2 MB
Cisco 502	4.2 MB

Device Type	**Firmware file size**
Cisco 504	4.2 MB
Cisco 509	4.2 MB
Cisco 525	11.6 MB
Polycom 331	3.5 MB
Polycom 335	3.5 MB
Polycom 450	4.1 MB
Polycom 650	3.5 MB
Polycom 5000	3.7 MB
Polycom 7000	11.3 MB
Polycom VVX 310	51.1 MB
Polycom VVX 410	51.1 MB
Polycom VVX 500	58.9 MB
Polycom VVX 600	57.5 MB

END