VegaStream Information Note

Considerations for a VoIP installation

To get the best out of a VoIP system, there are a number of items that need to be considered before and during installation. This document identifies a number of these:

1. Firewalls – Firewalls are designed to prevent unlawful viewers being able to read or retrieve data from a network. They work by preventing certain connections and data paths being made across the firewall. Firewalls have to examine each packet of data to decide whether to allow it across the firewall or not.

   Often Firewalls support NAT (Network Address Translation) functionality that enables multiple end point devices with local IP addresses to be "hidden" behind a single real routable IP address. This provides additional security, and also makes better use of real IP addresses – only one real IP address is required to support multiple endpoints.

   VoIP protocols were not written with firewall and especially NAT traversal in mind, they pass end-point IP addresses from one end point to the other, even though the address may be a local (non routable) address.

   To get VoIP gateways to work across NAT firewalls, either

   a) the firewall must understand the VoIP protocol and over stamp IP addresses in the protocol with their address translated values, or
   b) the VoIP gateway must be given a real (routable) IP address and sufficient "holes" must be made in the firewall to allow the VoIP protocols to operate.
   c) The NAT must have static translation configuration and a Vega, running Release 6 or above firmware must be configured with appropriate parameters to allow it to pre-convert the in-protocol IP information (see information note IN14-NAT_handling for further details)

If the Vega is to be placed behind a firewall it will require the following “holes” to be punched through the firewall:

inbound:

UDP (RTP) traffic to IP address lan.ip on port numbers 10,000 to 20,000
ping responses
telnet to IP address lan.ip (port number 23)
TFTP and TCP connections to IP address lan.ip on ports 2,130 to 3,000
H.323 to IP address lan.ip on port 1720
(SIP to IP address lan.ip on port 5060)
RAS to IP address lan.ip on port 1718
SNMP to IP address lan.ip on ports 161 to 162
TFTP initiation to IP address lan.ip on port 69
FTP to IP address lan.ip on ports 20 and 21
HTTP to IP address lan.ip on port 80

outbound:

ping traffic
TFTP and TCP connections on port numbers 2,130 to 3,000
H.323 on port 1720
(SIP on port number 5060)
RAS on port 1718
SNMP on ports 161 to 162
TFTP initiation on port 69
FTP on ports 20 and 21
HTTP on port 80

Where existing – non VoIP aware firewalls are to be used, the Vega supports some special features, i.e.:

1. the ability to reduce the number of ports that need to be opened up to pass rtp (media) traffic – see the section “Working with Firewalls” in the Vega Primer.
2. the ability to tunnel H.245 messages through an already opened IP path rather than having to open an additional channel – see the section “H.245 Tunnelling” in the Vega Primer.

Another consideration with firewalls is the data bandwidth that they can handle – voice data provides a heavy loading on firewalls as it is continuous data and also it is data that cannot afford to be delayed or dropped – check the capabilities of the firewall, a more modern, faster one may be required.

How secure is a Vega outside the firewall? -- A VoIP gateway like the Vega is different from typical IT devices. A typical IT device receives data from one place and relays it to another. Therefore, if someone "breaks" into it, potentially they have access to any data that that device can access. With a VoIP gateway the data is modified from IP data to telephony traffic. If someone "breaks" into the Vega it will not become a doorway into back end systems, because "the other side" of the Vega is a telephony connection. The only concern with someone breaking into the Vega is that they may corrupt, or purposefully alter parameters within the Vega. The Vega uses password protection to restrict entry, and there is no backdoor password (if the password is forgotten the Vega has to be factory reset locally to initialize it, and only then can the Vega be re-configured).

For additional security which does not disrupt the existing customer firewall – the Vega can be placed outside the existing firewall, and then a small VoIP aware firewall can be placed in between the Vega and the data network – this gives additional security protection to the Vega.

Another method of providing security and allowing NAT traversal is to use a VPN between the VoIP gateways.

Ideally the Vega should be behind a VoIP aware firewall that has sufficient bandwidth capability notto introduce delay or jitter to the voice packets it is passing.

2. Data bandwidths – Vegas support a number of different audio encoding schemes. The different encoding schemes require different amounts of bandwidth to pass the voice data.

   G711Alaw64k = 64kbps
   G711Ulaw64k = 64kbps
   G729AnnexA = 8kbps
   G723.1 = 6.4kbps

   To pass the audio across the LAN / WAN network, it is packetised – a short duration of audio is collected and encoded using the appropriate coding scheme. To deliver this audio payload to the correct destination it needs to be enveloped wit other information in order to provide the appropriate addressing capabilities across the LAN / WAN network. Standard IP over Ethernet uses the following "envelopes":

Ethernet header 14 bytes	IP header 20 bytes	UDP header 8 bytes	RTP header 12 bytes	Payload XX bytes	Ethernet CRC 4 bytes

   i.e. there are 58 bytes overhead for each packet of audio sent.

   For G723.1 a 30ms audio packet has a payload of 24 bytes

   With header compression, the IP,UDP and RTP headers can be compressed from 40 bytes down to 3..5 bytes.

   Check that the data network has sufficient bandwidth to carry the audio data; for network bandwidth efficiency header compression should be implemented within the WAN.

3. Latency – this is the delay between the time the audio enters the system and the time that the audio is played from the system. Transatlantic 'phone conversations often have as much as 800ms latency, and it is at this level of delay that conversations become uncomfortable due to the delays.

   Within the Vega itself the latency is dependent on the audio coding scheme in use, the amount of audio sent in each LAN packet and whether out of bound DTMF is enabled. There are very few other delays inherent in the Vega due to its design, with hardware rather than software being used to route the audio internally. Latency through the Vega is therefore close to the "ideal" latency for the coding scheme – around 135ms for G723.1, and around 50ms for G729AnnexA.

   The duration of audio passed in the LAN packets can be adjusted for the coding schemes. Increasing the duration beyond its default value will increase the latency (i.e. it will add to the delay before the audio can be sent out of the Vega).

   Latency is also introduced by delays in the data network. Each hop through a router or firewall will add delays. The data network must be designed so as to minimise the number of hops (delays).

   Minimise the latency of the WAN and keep audio packets short to improve perceived quality.

4. Jitter – this is the difference in delays of the audio packets through the network. For a VoIP system to provide high quality audio it must not allow any gaps in the played audio. In a VoIP system the audio data is packetised (cut up into short segments) and sent through the data network, the receiving unit collects the incoming audio packets and plays them to the listener. Different packets may be delayed through the LAN / WAN network by different amounts (jitter). To overcome the effects of this jitter, the receiver therefore has to delay the playing of the audio such that under worst-case jitter situations, it never runs out of audio to play. Vegas do this by having a delay buffer that collects audio packets and then passes them on to the rest of the system for processing and playing to the listener. For this to operate correctly, the delay buffer size must be set such that there is always audio available to pass on for processing, even under the worst case jitter conditions.

   Jitter tends to be introduced by devices that have to process the information, e.g. routers – which need to look at headers to see how to route the packets, and firewalls which need to look at packets to decide whether to allow them through or not.

   Ensure that the Vega buffer (VP_FIFO_nom_delay) is configured to handle the maximum jitter.

5. Packet Priority – Within the IP protocol it is possible to define priorities of packets using the TOS (Type Of Service) bits in layer 3 and 802.1p bits in layer 2. It is important that if contention is ever encountered within the data network that the routers will keep and pass on real time data, like VoIP audio in preference to TCP and other less time-critical traffic (less time-critical traffic can be re-sent, either by the protocol (TCP) or by the application, and will just result in a slowing of the delivery of the data, where-as if audio data is discarded then the audio will be corrupted at the receiver). Audio data should therefore be allocated a high priority – least likelihood of being discarded. See the Vega primer for details on how to configure QoS (Quality of Service) values.

   Configure audio RTP packets to have a high priority.

6. Using the Vega on the Internet. A number of things need to be considered when connecting a Vega to the Internet, especially, for example, intentional LAN attacks, including ping attacks and port 80, web browser, ping attacks. Also other gateways, IP phones or other VoIP endpoints making calls through your gateway.

   Because the Vega handles management, signalling and audio data across the LAN, it must look at and review all data being sent to it, to see if it is needed. This does make the Vega a possible target for Ping and other LAN attacks. Consider using a firewall, or better still a VPN to limit who can web browse to the Vega, and even who can ping the Vega. It will then be the firewall, and not the Vega gateway that will have to have the bandwidth to discard unwanted communications.

   To protect against 3rd parties making calls through your gateway, use dial-plan whitelists to define the list of IP addresses of gateways / proxies that are allowed to communicate through your gateway. Again firewalls can be helpful here, limiting which IP addresses may have access to your Vega.

Contact Details
Email: support@vegastream.com
Web: http://www.vegastream.com

EMEA Office
VegaStream Limited
Berkshire Court
Western Road
Bracknell
Berks RG12 1RE
UK

+44 (0) 1344 784900

USA Office
VegaStream Inc.
3701 FAU Boulevard
Suite 200
Boca Raton
FL 33431
USA

+1 561 995 2300