UltraBand DPI/PBR Pre-Installation Information and Requirements

Remote Access and Firewall Requirements

1. PeerApp requires four (3) public or VPN-accessible IPv4 and/or IPv6 addresses:
   a. iDRAC (lights-out management)
   b. Management access to the CentOS host
   c. Normal management access to the PA Cache VM guest (management GUI, PeerApp command-line, Linux command-line).

2. The physical connection for this is normally presented on a single Gigabit Ethernet circuit on the PeerApp cache, with four MAC addresses.
   a. Either enable RSTP (Rapid Spanning Tree Protocol, preferred) or disable STP (Spanning Tree Protocol) on the switch port facing the shared PeerApp management port
   b. Some customers prefer to provide inbound one-to-one NAT mapping and use addressing from RFC 1918 (v4) or RFC 4193 (v6) inside, and this is perfectly acceptable.
   c. Some customers prefer to connect the separate iDRAC NIC to its own switch port. In that case, please also observe the STP request above for this switch port, and please let your PeerApp SE know of this choice.
   d. Some customers prefer to use one-to-N NAT mapping. This works fine for everything other than the iDRAC address, which needs either a one-to-one NAT or its own public address.

3. On each of those four addresses, we'll need the following inbound ports mapped and permitted:
   a. TCP 22 (SSH)
   b. TCP 49 (TACACS, optional)
   c. TCP 443 (HTTPS)
   d. TCP 5800-5801 (Java software download for VNC)
   e. TCP 5900-5901 (VNC and Java Console)
   f. UDP 123 (NTP)
   g. UDP 161-162 (SNMP)
   h. ICMP ping

4. The address ranges from which PeerApp requests access are:
   a. 35.153.171.203
   b. 52.44.115.17

5. You should also permit access to whatever subnets there are from which you will be accessing the management functionality, using the same ports.

6. Please also assure that you can permit the following destination ports outbound from the management IP addresses toward your own equipment, and ours in the subnets in section C, for monitoring and management purposes:
   a. TCP 25 (SMTP for system alerts)
   b. TCP 49 (TACACS, optional)
   c. UDP 53 and TCP 53 (DNS queries)
   d. UDP 123 (NTP)

   e. UDP 161-162 (SNMP for optional traps)

   f. UDP 514 (syslog for optional logging)

   g. UDP and TCP high ports related to return traffic for protocols in #3 above.

7. If firewall or ACL protection and access are not available, then we can provide limited firewall functionality on the server itself. Please notify PeerApp Technical Services through your System Engineer if this is required.

8. Please provide one or more email addresses for automatic email notification of critical system events.

9. Please also provide the IP addresses of:

   a. Your DNS server(s)*

   b. Your NTP server(s)*

   c. Your SNMP trap server(s) (optional)

   d. Your SNMP community strings (optional)

   e. Your Syslog server(s) (optional)

  *In the absence of your own servers, public servers will be used.

For Policy-Based Routing (PBR) or DPI insertions:

2. Please provide us with the subnet ranges of all your subscriber networks so that we can recognize which IP addresses are those of your subscribers.

3. Please provide the type and model of the Layer 3 equipment you are planning to use, and we will send you examples of PBR configurations, if we have any on hand, and work with you to adjust them as necessary.

4. To help with the configuration example, please tell us how many circuits you plan to use.

5. For each interface used for PBR between your router(s) and the UltraBand:

   a. Please assign an IPv4 address assignment of /30 in size, or IPv6 address assignment of /126 (two usable addresses) and provide these addresses to us.

     i. These can (probably should) be from RFC-1918 / RFC-4193 (private) address space, but this is not a requirement.

     ii. We will typically use the second usable address. (E.g., if you assign 10.1.1.0/30, we would use .2, and you would use .1.

Thank you!