

Comparison between Horizon and Common Alternative Solutions

<i>Solution</i>	<i>Issues</i>	<i>Horizon Solution</i>
Virtual Private Network (VPN)	<p>VPN is primarily designed for intra-enterprise, mainly for branch offices and remote employees.</p> <p>VPN is a not suitable for inter-enterprise communication since it's not feasible to allow suppliers and distributor to have company's VPN access.</p>	<p>Lets you seamlessly and securely communicate across enterprises with AES based encryption.</p> <p>Dedicates to for IP voice and video communication, reduces the load of VPN by multiplexing visual communication traffic to a single fixed port.</p>
No Firewall No NAT	<p>Each video endpoint must have its own public IP address, it raises the network cost.</p> <p>By placing video endpoints on public internet, they are exposed to threats without protection.</p> <p>Endpoints' IP addresses are published during communication to all callers.</p>	<p>Let you leverage the security and protection of your enterprise firewall and NAT by placing them in the company's network.</p> <p>Video endpoints only need to use private addresses behind NAT.</p> <p>Horizon hides the enterprise network topology, callers never sees IP address of endpoints, only the Horizon server.</p> <p>Horizon is able to traverse any number of firewall and NAT of all types.</p>
Application Level Gateway (ALG)	<p>Implementation is difficult when there are multiple router, firewall & NAT along with path since boundary needs to be traversed separately.</p> <p>Requires access to every network boundary.</p> <p>Network Administrator needs to allow permanent inbound connection for callers outside of networks to initialize call session. This configuration is not recommended for most enterprise security policies.</p>	<p>Once Horizon server is deployed, securely traversal of multiple router, firewall and NAT can easily be accomplished.</p> <p>Horizon users need no access or understanding to any router, firewall or NAT.</p> <p>Horizon never requires or allows an inbound connection through your firewall.</p>
Stand-alone or Gatekeeper Proxy	<p>Implementation is difficult when there are multiple router, firewall & NAT along the communication path since each boundary needs to be traversed separately.</p> <p>Endpoints' IP addresses are published during communication to all callers.</p> <p>Needs to allow permanent inbound connection to proxy.</p>	<p>Once Horizon server is deployed, securely traversal of multiple router, firewall and NAT can easily be accomplished.</p> <p>Horizon never requires or allows an inbound connection through your firewall.</p> <p>Prevents IP advertising – Topology hiding.</p>