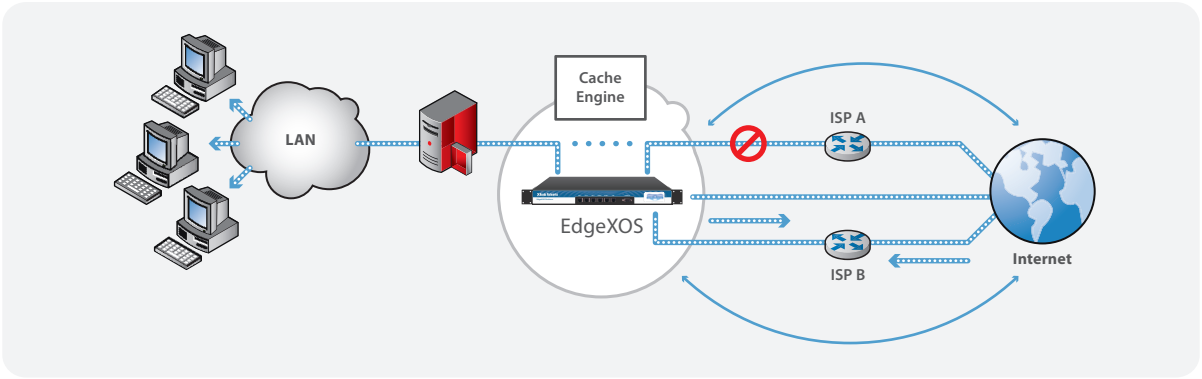
ZeroOutages

ZEROOUTAGES – WHITE PAPER

Private Cloud Solutions
Virtual Onsite Data Center

Single Side Internet Bonding / Balancing

The ZeroOutages solution makes for a perfect Internet link bonding/balancing device for customers that are simply looking to improve their Internet connectivity and reliability and do not yet have a remote data center facility, or utilize distributed hosted applications like NetSuite, Azure, or the Amazon Cloud.



A single sided ZeroOutages deployment includes a wide range of features and functionality designed to improve the customers overall Internet experience and dramatically improve network performance and reliability.

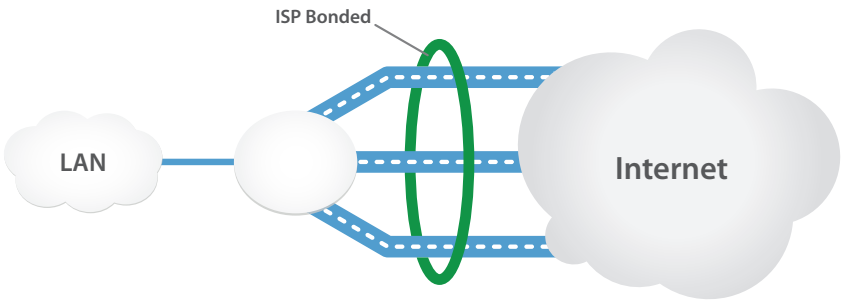
ISP Link Bonding/Balancing *(Scalability)*

Each ZeroOutages deployment includes our unqiue and patented single sided Internet bonding technology. This feature means that our customers can combine the speeds of each Internet connection WITHOUT the requirement of having a device at the opposite end, or having to "backhaul" the traffic to some remote data center.

This Internet bonding functionality can take a 3Mbps DSL link and a 7Mbps cable connection to obtain 10Mbps download speeds. Further the ZeroOutages' solution can ensure that all traffic can be balanced between the links in order to better utilize each Internet connection. As the customers' needs grow, they can simply add a new inexpensive broadband connection.

Automated ISP Failover

With built-in Deep Path Inspection, the ZeroOutages device can instantly update how it is route traffic based on the availability of each Internet link. DPI performs detailed testing to confirm the status of each connection which helps to eliminate any potential false outages that may occur with other standard firewall devices.



Automated ISP Failover
With built-in Deep Path Inspection, the ZeroOutages device can instantly update how it is route traffic based on the availability of each Internet link. DPI performs detailed testing to confirm the status of each connection which helps to eliminate any potential false outages that may occur with other standard firewall devices.

Application Routing
This feature enables the customer to route different applications out different Internet links, i.e. VoIP out ISP A and web/email traffic out ISP B. The application routing feature will automatically failover the traffic if their is an ISP link outage.

Best Path Routing
This service provides ZeroOutages' customers with the ability to optimize their Internet access to business critical applications. BRP will monitor remote application servers and re-route traffic based on the best possible path to that traffic, additionally BRP will produce reporting so that the customer can see how each of their Internet links are performing.

ActiveDNS Server Failover
The ZeroOutages solution incorporates a DNS server with the ability to automatically failover inbound server requests across each ISP connection. It does this by changing the DNS records in real-time based on the availability of each network connection.

Packet-Level Firewall w/ApeXfilter
As comprehensive WAN security appliance, the ZeroOutages device can replace an existing firewall and provide full NAT support, DoS protection, content filtering, and anti-virus/malware protection.

Real-Time Network Reporting
The ZeroOutages onsite device monitors traffic usage and provides detailed reporting on usage per ISP link, top users, top sites accessed, and top applications, all of which can be directly accessed by the customer or our partners.

Fully Managed Solution *No Hardware To Purchase*
ZeroOutages engineering team handles the setup, installation, and ongoing support. The customer can submit change requests that will be implemented by support. Best of all, there is never any equipment to purchase.

BPR (Best Path Routing)

The purpose of this paper is to provide an understanding of XRoads Networks' patent-pending BPR technology that is built into its XRoads Edge product line.

Background

In large computer networks, such as the Internet, the entire network is actually made up of many smaller networks. Each of those smaller networks use their own methods to route traffic, some better than others. Due to various adoptions of practices, it is very difficult to provide guarantees in terms of packet loss, latency, etc to every network and every node on this large network. There are simply too many smaller networks using too many different routing technologies to ensure that the data sent from one end of a network connection to the other is handled and/or treated the same.

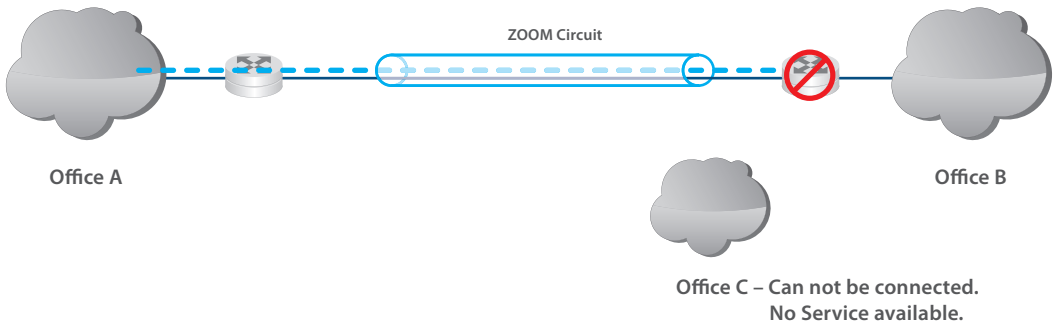
Many providers over the years have begun to implement standards within their own networks in an attempt to increase reliability and ensure that network traffic is handled the same from one end to the other.

The problem is that in most cases, the businesses that use the Internet have offices, and/or partners which do not use the same network provider and thus data traffic between these offices is not guaranteed.

This generally means that as the data leaves one office bound for a partner's office, the data must be exchanged from one service provider to another. Even if the first provider has a particular SLA (Service Level Agreement) with the customer sending the traffic, there is generally no agreement with the second service provider, and thus the data is delivered with minimal, if any, SLAs.

With most web and email traffic this is not a major problem, however when it comes to critical latency sensitive data, such as VPNs, VoIP, and Point of Sale systems, SLAs and quality of the service becomes critical.

BPR seeks to provide a novel method for optimizing network traffic by probing the critical remote networks via two or more diverse network paths, and then selecting the path that provides the overall best route, i.e. the lowest latency, lowest packet loss, and lowest calculated jitter. Using this method BPR effectively ensures that the network traffic stays on the same service provider as long as possible, in some cases from one side of the connection to the other.



Problem

How does one incorporate a ***universal solution***, with built-in ***automated redundancy***, that is ***inexpensive to deploy***, and provides added ***security above and beyond standard IPSec*** deployments?

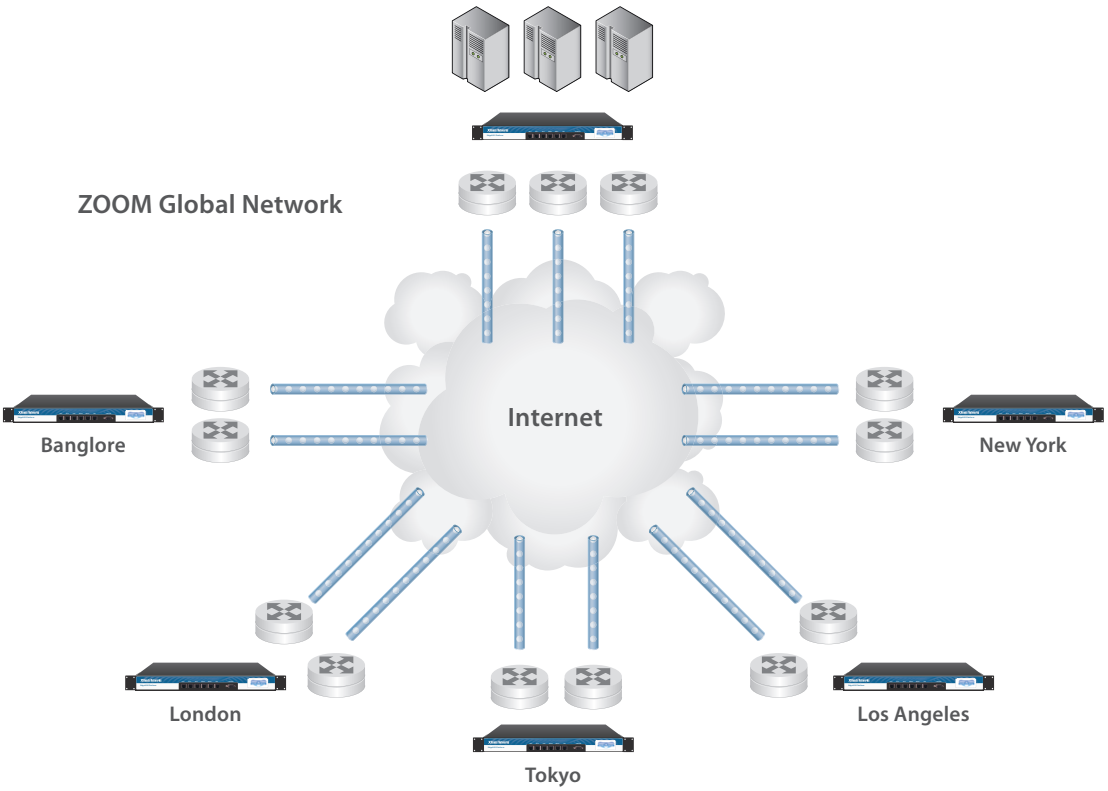
Solution

XRoads Networks' Private Cloud VPN connectivity technology provides the solution. Our Private Cloud VPN tunnels are inexpensive to deploy, include built-in redundancy capabilities which can failover automatically in the event of a network outage, can be deployed around the world using any type of broadband connection, provide end-to-end QoS and traffic shaping, and provide up to five times the security of standard IPSec deployments.

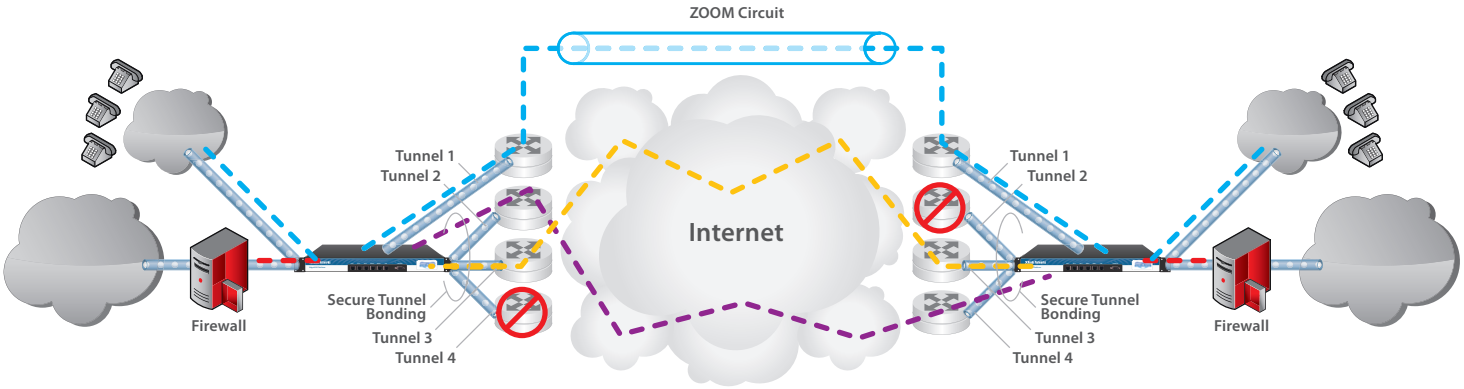
Private Cloud Delivers:

1. A single global deployment vehicle.
2. A fully meshed and fully redundant remote office connectivity solution.
3. A highly secure solution, similar to ZOOM and private lease line solutions.
4. A scalable solution with built-in end-to-end QoS and traffic shaping.
5. A solution that can provide improved performance through BPR tunnel routing.

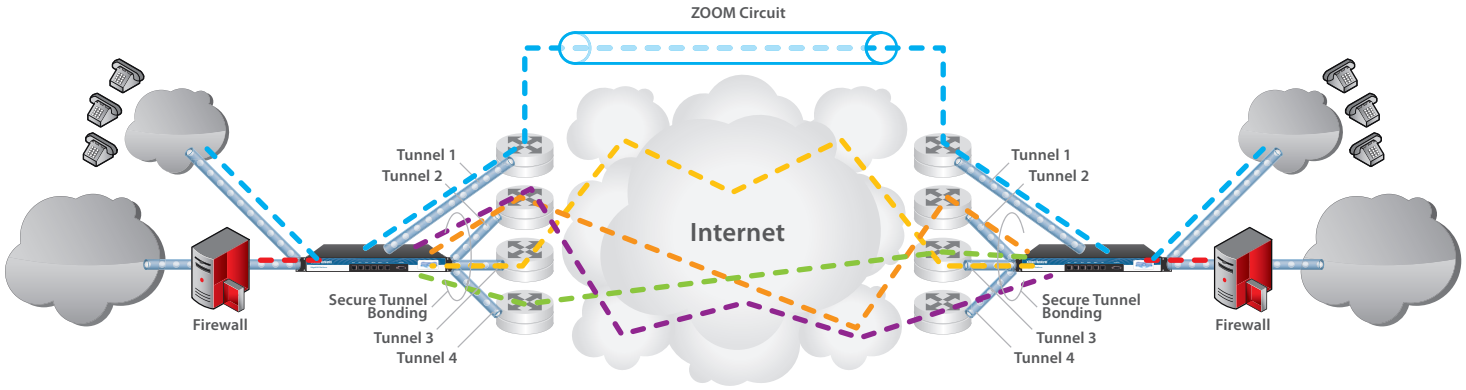
Our Private Cloud solutions provide a global reach that can not be achieved by any other solution which incorporates the same level of QoS, redundancy, and scalability.



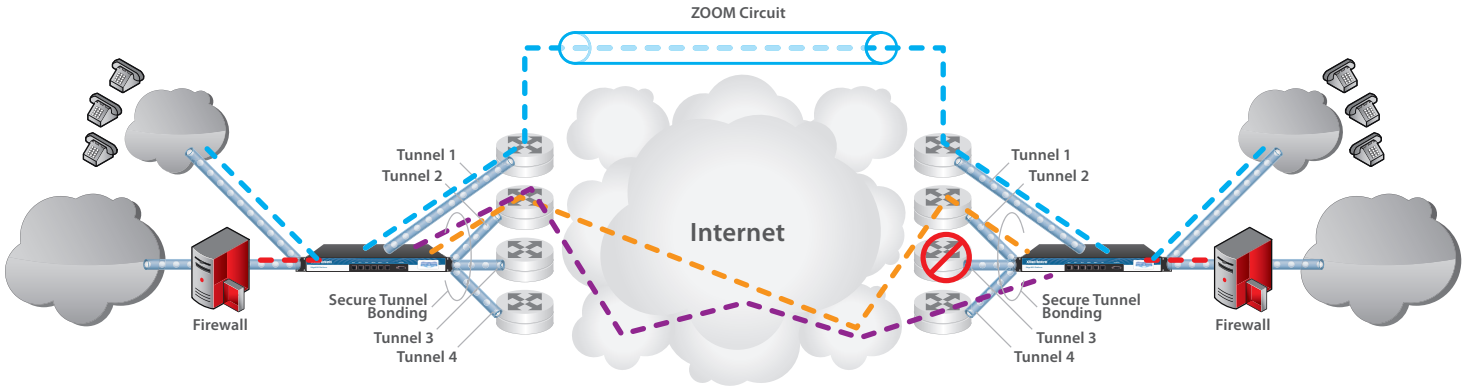
Private Cloud Fully Meshed Redundancy: With our Private Cloud tunnels a network administrator can configure a completely redundant and fully meshed remote office solution. Full meshing means that even in the event that two simultaneous network outages occur at both ends of the tunnels, that the remote sites stay up and running.



Private Cloud Security: Because our Private Cloud tunnels utilize multiple WAN links for passing traffic, link balancing improves security as no single link can be sniffed in order to obtain multi-session information. The balancing of session traffic by nature improves security across the tunnels.



Private Cloud Best Path Routing: Built-in to the routing mechanism for our Private Cloud tunnels is our Best Path Routing technology. Best Path Routing uses network thresholds to determine which tunnel path is the best one to use for sending each new session. This ability ensure that even when a link begin to perform badly that the Private Cloud tunnels are always leveraging the best possible connectivity provided via the available WAN links.



Private Cloud QoS: As packets traverse the Private Cloud tunnels, packet labeling is performed (as in ZOOM networks) with the label state remaining constant from end-to-end. This ToS/Diffserv labeling can be used to classify packets based on application type in order to prioritize critical applications. In addition, the EdgeXOS platform incorporate full rate-shaping and bandwidth partitioning at each end of the tunnel thus guaranteeing critical application priority between sites.