NetXcom ICT / XRoads Solutions:

Solutions and Technology offerings:

Markets requirements – MEA region:

Customers required the next generation cost effective solutions for :

- "session bonding",
- "dynamic bandwidth management"
- MultiWAN technology,

We have to ensure the most cost efficient use of:

Customer WAN (wida-area network) connectivity and we have to provide significant advantages over traditional :

- load balancing,
- traffic shaping,
- WAN optimization solutions.

Our bandwidth management solutions include our Accelibond, Adaptiband, Site2Site, ApeXfilter and ActiveDNS technologies.
XRoads Networks developed the first Unified Bandwidth Management™ products based on these technologies. UBM by design provides an excellent platform for Internet and cloud connectivity which incorporates a number of core bandwidth management and network optimization capabilities. The following are some of the key functions built-in to the EdgeXOS platforms:

Accelibond™ Internet Session Bonding (MSA)
Bond multiple ISP connections

Adaptiband™ Dynamic Bandwidth Management (DBM)
Equalize bandwidth distribution

Site2Site™ VPN Virtualization (S2S)
Bond multiple tunnels to increase speed and reliability

NetXcom ICT / XRoads Solutions:

ApeXfilter™ NextGen Application Filter (MWF)
Next generation filtering & caching technology

ActiveDNS™ Inbound Load Balancing
Server link balancing w/redundancy

XFlow™ Real-Time Network Reporting (XRE)
Detailed application reporting

Active Network Redundancy (ActiveHA™)
Route failover and network monitoring

Server Load Balancing (SLB)
Application distribution and failover

MultiWAN Link Load Balancing (MVP)
Advanced application routing

Application QoS/Throttling (ATS)
Policy-based application & end-user shaping

Comprehensive Cloud Firewall (CFW)
Network security services

Comprehensive LAN Router (CLR)
VLANs, Bridging, SNAT/PAT, Bypass

XRoads Networks has also partnered with a number of best of breed companies to deliver additional security, reporting, and acceleration features to ensure **reliable, secure, and responsive** connectivity to cloud (Internet/Intranet) applications like remote CRM, Email, SSL, VoIP and other mission critical systems. XRoads Networks utilizes a combination of both Open Source as well as custom developed firmware for its XRoads Operating System (XOS). We utilize unmodified versions of the Linux Kernel, OpenVPN, IPRoute and several other open source technologies to which we have been a donor and strong supporter of over the years. We have also built our own proxy technology used to perform our balance and bonding capabilities.

It is important to note that our methods are unique and unlike other competing solutions at no time does our technology modify SYN packets in a way that changes and/or includes a physical router address. It is equally important to note that at no time does XRoads Networks provide the ability to aggregate or bond two or more tunnels together which use different levels of security and/or encryption. This distinction means that our products provide more consistant latency and jitter across all available Site2Site tunnels.

Internet Bandwidth Bonding

XRoads Networks is the inventor of Multi-Session Acceleration Bandwidth Bonding or **Accelibond™**. MSA is the ability to bond multiple ISP connections and cache response content in order to accelerate web-based connectivity. This ability to bond connectivity across multiple WAN links and remote servers and then cache

NetXcom ICT / XRoads Solutions:

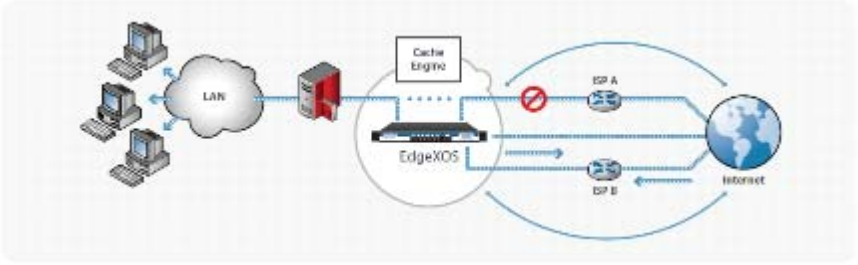
responses is unique in the industry.

Improving Application Performance

MSA is an application proxy which has built-in caching capabilities in order to increase network performance. These capabilities increase download speeds for commonly accessed websites or large data files. MSAs caching is built-in to the EdgeXOS platform (with larger systems having more caching memory). Optionally, customers can select solid state caching. What is unique about MSA is its ability to speed up first time access to files through link bonding.

Increasing Available Bandwidth

MSA actually increases network download speeds for first time access to files by utilizing multiple ISP connections and remote servers at the same time. Unlike most other "link balancing" solutions which can only utilize one ISP link at a time for each session, the EdgeXOS platform can actually utilize multiple links at the same time for the same session. This effectively makes a 3Mbps and 5Mbps link in to an 8Mbps link.



The diagram above demonstrates how the combined features of the MSA module can accelerate network downloads while increasing bandwidth through ISP link bonding and acceleration.

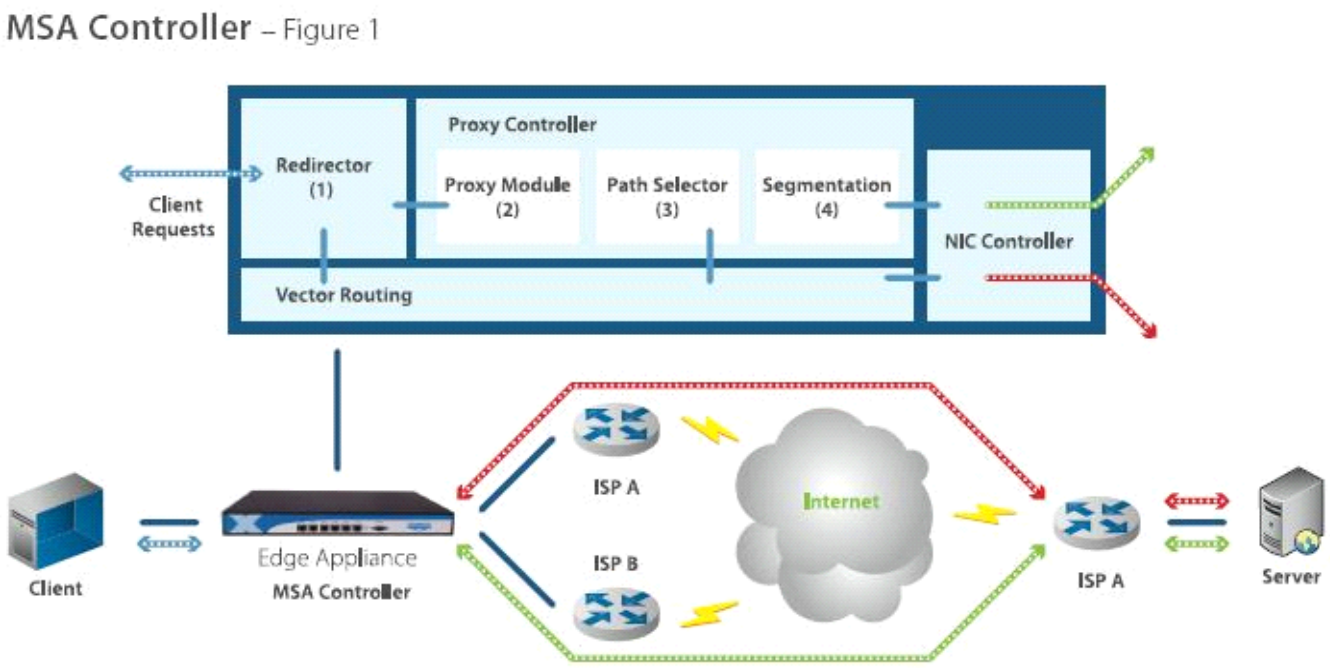
Accelerated Applications

The MSA module is typically used to improve responsiveness for network administrators which are looking to speed up connectivity for their end-users and/or dramatically speed up web-based downloads and large data files. The following are typical applications that are accelerated by MSA:

NetXcom ICT / XRoads Solutions:

How Does It Work?

This is a unique and patent pending technology developed by XRoads Networks. This technology enables our customers to effectively bind two diverse ISP links together to significantly improve web-based download speeds and reduce traffic congestion.

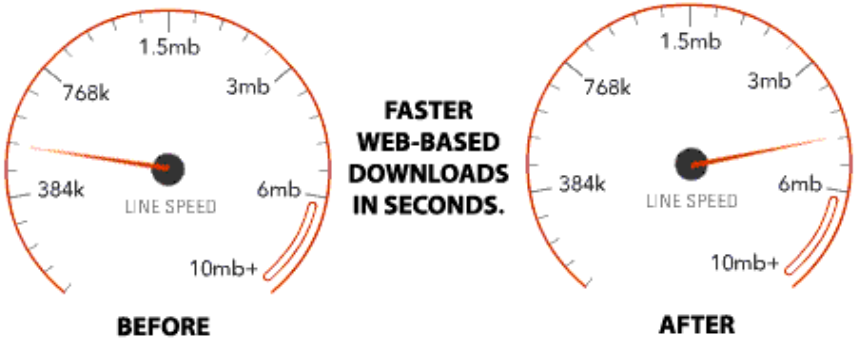


Data Segmentation

Unlike other solutions on the market which perform data object modification and packet forwarding, the EdgeXOS platform utilizes an advanced proxy service which is able to examine content on-the-fly and determine whether it is best to perform session-balancing or bonding.

If bonding is selected, the MSA module will attempt to download the remote data file across each of the available ISP links. When fully supported, the download speeds for these files can be much faster. Depending on the speed of your secondary WAN links, customers have realized up to 2100% faster download speeds.

NetXcom ICT / XRoads Solutions:

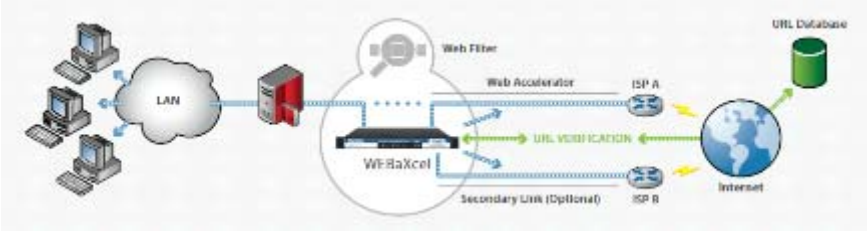


The following is an example of how download speeds can be dramatically improved for a customer after combining their existing ISP service with a secondary link using the EdgeXOS appliance.

ApeXfilter™ Cloud Threat Protection

XRoads Networks EdgeXOS platforms incorporate next generation application and web content filtering with built-in caching and acceleration technology. Our **web content filtering** is entirely appliance-based, meaning there is no external software required, simply connect the appliance to the network and all traffic traversing the appliance will be filtered.

This security solution is based on advanced machine learning (MED) techniques which scrubs new content in order to quickly and effectively categorize it. The EdgeXOS platform leverages Webroot's threat analysis system and database which has categorized nearly 10 billion URLs and hundreds of millions of top level domains.



Statistics:

- Nearly 10 Billion URLs Categoried
- Hundreds of Millions of Top Level Domains
- Over 40 Languages

NetXcom ICT / XRoads Solutions:

- Scan of over 500 Million Data Files
- 3.5+ Million Mobile Applications Scored
- Over 500 Million IP Addresses Analyzed
- New Phishing Page Detection In Less Than 10 Seconds
- 80+ Content Filtering Categories
- Forced Safe Search
- CIPA and HIPPA Complaint

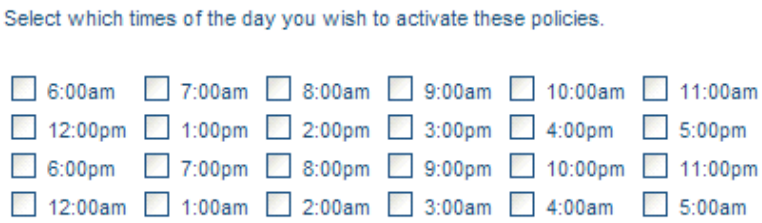
The ApeXfilter™ includes enhanced features and functionality not found in other web filtering appliances, including non-web ppplication filtering to lock down cloud-based services, IP reputation filtering to block malicious IP's instead of just URLs, and web threat protection services which prevent multiple types of Internet born threats, including **the blocking of Malware, Viruses, Spyware, and Phishing attacks**. When combined with XRoads Networks patented link bonding technology (Accelibond™) and caching capabilities, the ApeXfilter™ application filter is the pinnacle in content filtering.

The maximum entropy discrimination algorithm employed by the ApeXfilter™ is the most advanced categorization technology of its kind which has set new records in terms of reputation assignment with a less than 2% error rate.

In addition to the ApeXfilter's unique capabilities, it also includes a host of standard content filtering options, including Time of Day Controls, and Category-based filtering:

Time of Day Controls

Determine which filtering rules are apply at what times during the day or which days of the week. The network administrator has full control over how web access is granted.

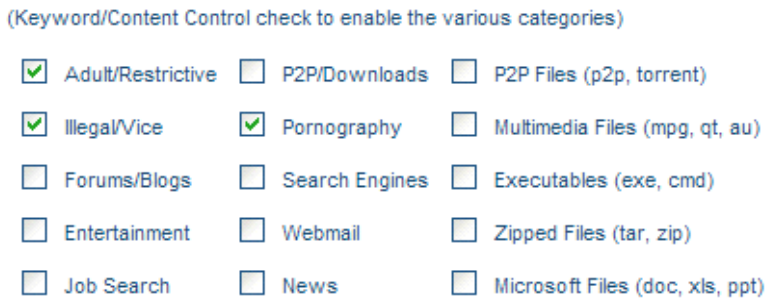


Category Controls

Determine which categories apply and which file types are blocked. Prevent end-users from accessing sites which to not comply with the organizations policies and/or block the download of

NetXcom ICT / XRoads Solutions:

files which may contain data which is not authorized or which may pose a risk.



XRoads Networks also has its own desktop web protection client which can be installed on end-users desktop, laptop and smartphone systems in order to provide per-user content access control and reporting. This is done via our WEBaXcel DWP client.

Adaptiband™ Bandwidth Management

XRoads Networks is the inventor of Adaptiband™ Dynamic Bandwidth Management. DBM is the ability to automatically and dynamically throttle end-user application traffic in order to ensure fair distribution of bandwidth and guarantee bandwidth for mission critical applications like VoIP, Citrix, RDP, and other real-time applications.

Guarantee Bandwidth for Critical Applications

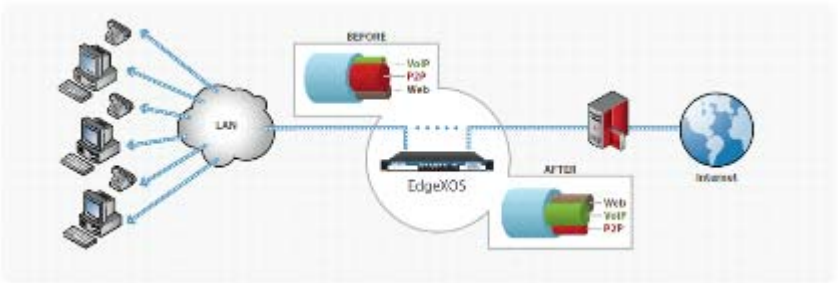
DBM allows network administrators to set pre-defined bandwidth levels to guarantee network resources for critical applications. This means that applications like VoIP will always have the bandwidth they need to complete calls without interruption or dropped packets. Additional prioritization can be assigned to these critical applications to ensure that they receive the fastest queuing even when the network is fully utilized.

Automatically Throttle Abusive Traffic

DBM will automatically throttle end-user traffic which exceeds pre-defined levels and ensure that mission critical applications always get the bandwidth they need. While other "traffic shaping" solutions must identify every possible application in order to shape it, DBM instead identifies traffic based on session flows. This means that unlike other "traffic shaping" solutions, the EdgeXOS platform can automatically throttle ANY application as soon as it comes

NetXcom ICT / XRoads Solutions:

out.



As demonstrated in this diagram, DBM works with our XRE (XFlow Reporting Engine) to collect packet data arriving on each of its interfaces and then determine whether each session flow traversing the EdgeXOS platform meets the pre-defined criteria, if it does not (like P2P in this example), it is throttled.

Optimized Application Delivery

The DBM module is able to effectively optimize the delivery of critical applications by ensuring that those applications receive the amount of bandwidth they need in order to provide end-users with real-time and responsive connectivity. Some of the applications DBM optimizes include:

How Does It Work?

As peer-to-peer and other applications become more sophisticated the ability to perform application matching has become more and more difficult. To improve the EdgeXOS platforms ability to control these applications XRoads Networks developed its DBM technology.

Session Monitoring & Prioritization

Automatically Prioritize Applications

- Secure Web Access
- E-Mail Access
- Peer-to-Perr / IM
- Remote Desktop Access
- CRM Access

Instead of attempting to constantly modifying our application database to match every change to each peer-to-peer and recreational application on the market, this new approach allows the

NetXcom ICT / XRoads Solutions:

EdgeXOS to dynamically manage any application based on session utilization information. DBM continuously monitors the usage of all sessions traversing the appliance and as overall utilization reaches over 80% it will begin prioritizing traffic based on utilization and administratively defined rules.
Unlike other traffic shaping equipment, the EdgeXOS appliance is able to analyze any application, regardless of whether it is in our database and prioritize that traffic based on pre-defined administrative preferences. The network administrator can determine which applications/end-users should receive higher priority and all other traffic will be prioritized based on session statistics and overall utilization, thus reducing high traffic users, smoothly overall bandwidth usage, and ensuring equal bandwidth distribution for mission critical applications.

Indestructible VPN Site2Site™

XRoads Networks is the inventor of the "indestructible" VPN Virtualization™ technology. Utilizing our Site2Site™ technology, our ability to virtualize VPN connections through multi-WAN link is unique in that it can combine multiple secure VPN tunnels at the same time in order to increase total available bandwidth and significantly improve redundancy and reliability between sites and/or remote offices.

VPN Virtualization™ - Virtualized VPN Tunnels

VPN Virtualization enables network administrators to combine multiple VPN tunnels across two or more WAN links in order speed up communications between sites, reduce congestion, mitigate network delays, and improve redundancy and reliability of existing connectivity.
VPN Virtualization includes integrated security features not found in other solutions on the market today. VPN Virtualization is designed to reduce cost through the use of inexpensive broadband connections, like DSL, cable, wireless, for transferring data between sites.
VPN Virtualization can also be used in conjunction with MPLS by offloading streaming applications like VoIP across a separate non-parallel and unbound network path. This

NetXcom ICT / XRoads Solutions:

functionality enables the best of both connection methods while reducing costs and improving performance which increases productivity.

VPN Virtualization works in conjunction with various WAN Optimization technologies which are designed to accelerate data between sites, when WAN Optimization is combined with VPN Virtualization the benefits are multiplied.

Optimize Branch Office / Remote Office Application Delivery

Organizations with branch offices are constantly looking for more effective methods for providing remote users with access to centralized applications and network resources. XRoads Networks' Site2Site tunnels can be used to improve performance between two or more sites by leveraging multiple WAN links in order to cost effectively increase the available bandwidth between sites. Site2Site also provides the ability for customers to achieve 99.999% reliability through automated link failover, something other optimization solutions don't offer.

Improved Responsiveness (Caching & QoS)

The Site2Site tunnel module includes built-in application caching and works with our DBM module to provide end-to-end QoS for mission critical applications. The caching module speeds up file transfers and improves the performance of large downloads by compressing data in real-time as it is sent over the Site2Site tunnel, then the data is decompressed on the remote end. Additionally, our Site2Site tunnels automatically adjust TCP windowing in order to improve performance across slower and/or high latency links.

Automated MPLS / Branch Office Redundancy

Many organizations have moved to an MPLS infrastructure for their wide-area network deployments. MPLS is expensive but provides exceptional network connectivity with built-in QoS, however it lacks redundancy at the edge. If an outage occurs at either end of the MPLS circuit, then potentially all of the remote sites could be down. XRoads Networks' Site2Site solutions enable our customers to setup a secure and inexpensive Internet-based redundancy solution to ensure automated failover in the event of an MPLS outage.

MultiWAN Optimization = WAN Optimization + Link Bonding / Automated Failover

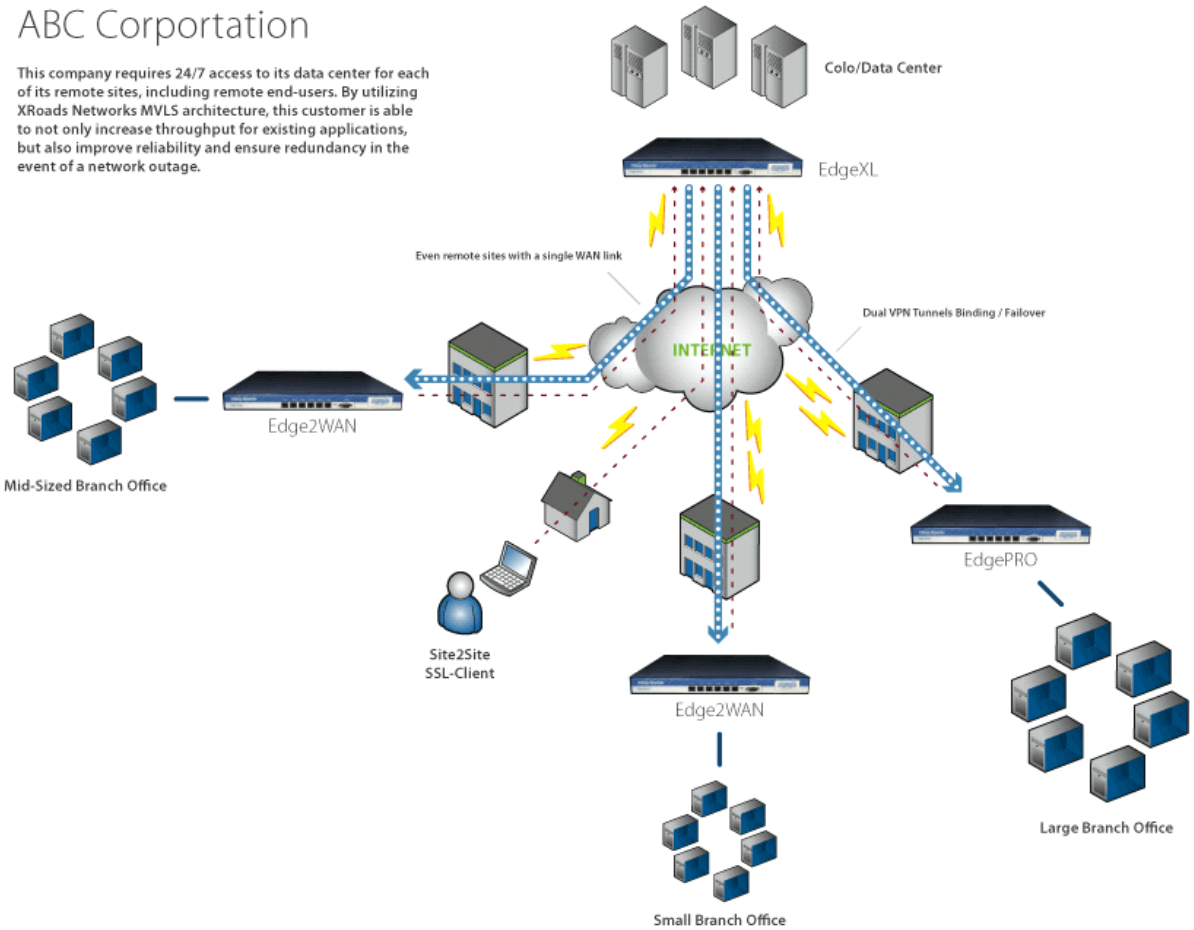
Our unique VPN virtualization technology includes built-in QoS and automated Internet-based

NetXcom ICT / XRoads Solutions:

failover capabilities. Additionally, customers can combine multiple inexpensive broadband links (DSL, cable, wireless, etc.) in order to increase bandwidth between sites, as an alternative to using more expensive private T1, Frame Relay or MPLS connectivity. XRoads Networks' MultiWAN Optimization reduces remote office connectivity costs by up to 50% (through lower bandwidth costs and improved productivity), increases application responsiveness vs. a single T1 Internet connection, and provides 99.999% redundancy in the event of a network outage. No other remote office connectivity solution can produce the ROI delivered by the EdgeXOS platform.

How Does It Work?

Our Site2Site module can combine multiple sites together via one or more SSL tunnels. Tunnels can be placed in an automated failover manner so that upon a link outage, the tunnel will automatically re-establish over the secondary connection. Further, when two or more tunnels are configured the appliance can selectively route traffic in a manner which optimizes the bandwidth available via each tunnel connection.



NetXcom ICT / XRoads Solutions:

The Problem: Connecting two or more offices can be done via most VPN technologies, however ensuring that they stay connected and are optimized is a challenge for most security appliances.

With the ability to connect two or more tunnels between offices, the EdgeXOS platform can also optimize the bandwidth by setting up specific application routes which brake-up the network traffic and thus provide faster overall throughput between the offices. The data between offices can be further segmented based on destination network.

The Solution:

With the ability to connect two or more tunnels between offices, the EdgeXOS platform, will automatically provide 99.999% uptime between offices in the event of a network failure. Additionally our appliances can also optimize the bandwidth by setting up specific application routes which brake-up the network traffic and thus provide faster overall throughput between the offices. The data between offices can be further segmented based on destination network.

- **Layer 3 Tunnel**
- **Standard 3DES Encryption**
- **Built-In Compression**
- **Automated Tunnel Failover**
- **Application Tunnel Routing**

Instantly add fault tolerance for remote users and enhance the responsiveness for critical remote applications.

XFlow™ Real-Time Reporting

When looking to manage network resources it is critical to understand how the network is being utilized in order to optimize it. XRoads Networks' XFlow Reporting Engine (XRE) was designed to do just that, with its built-in real-time packet analyzer and backend database, the reporting engine can collect, summarize, and display detailed network information.

Collects and records traffic flows in real-time

Analyzes and summarizes collected packet data

Produces easy to read tables and 3D graphics

How Real-Time Reporting Works

The XRE module actually captures the packet data which comes in to each of the active interfaces of the EdgeXOS platform. This packet data is then summarized and recorded to a backend database which is built-in to the EdgeXOS platform. Additional analysis of the data is then performed by various components of the XRE module. This analysis creates additional data which is used to generate various graphical displays of the data. Finally, the data is displayed to the network administrator via tabular and 3D graphical format.

EdgeXOS Reporting Capabilities

The EdgeXOS platform includes a number of reporting capabilities. Some of these include the

ability to report on the service level (packet loss, latency) for each connected ISP link, the ability to see how much traffic a specific user/server or application is using as compared with the rest of the network, the ability to see total bandwidth utilization and per application bandwidth utilization in real-time (updated every five seconds). When enabled, the XFlow packet collector can also determine which users and applications are using the most network bandwidth (and automatically throttle when combined with DBM).

How Does It Work?
XFlow™ is the name of XRoads Networks' built-in packet analyzer. This technology collects usage statistics on a per user / per application basis which allows the EdgeXOS appliance to produce a number of reports, including top users and top applications.
Packet Collection
XFlow Reports
Top Users
Top Applications
Top Sessions
Applications Per User
IP/Host Usage
The XFlow (XRoads Flow Collector) module examines each packet going through the EdgeXOS appliance. Packets are examined for their source/destination address/port, protocol, size, and session information. All of this information is then captured in statistical format and summarized for reporting purposes. The reports are dynamically created and are generated using a 3D graphics engine.
Typically customers will use these reports to identify top network users and applications and then create bandwidth prioritization and shaping rules in order to meet their organizations usage requirements, i.e. placing rate-limits on certain applications and/or end-users or prioritizing certain application servers.
Packet Streaming
One of extra features of the XFlow technology is the ability to output the packet data collected to an external collection server. This information can then be saved on a large drive array for future reporting purposes. The data is dumped via the OpenSource standard 'sFlow'.

ActiveDNS™ Load Balancing

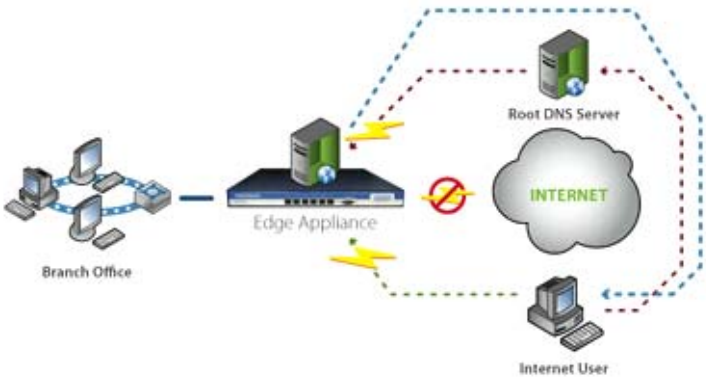
Server load balancing and failover requires the instant modification of DNS records

NetXcom ICT / XRoads Solutions:

in order to re-direct inbound sessions to the correct network interface. Our ActiveDNS & ISP Load Balancing module provide this capability along with advanced DNS balancing capabilities.

Intelligent DNS Management

The XRoads Networks' EdgeXOS appliance includes a fully functional DNS server which enables intelligent DNS responses based on the current status of the available WAN links, remote sites, internal servers, and other administratively defined criteria. The XRoads Networks solution also enables something called "delegation" which allows only those critical URLs, i.e. www.xyz.com to be handled by the EdgeXOS appliance, this way the entire domain does not have to be transfered, save time reducing complexity.



The EdgeXOS appliance has full support for NS, MX, A, PTR, CNAME, SVR, and TXT records. Records can be created to test both local and external paths for uptime. Weights can be assigned to each record for load balancing purposes. Complex rules can be created to support single or multiple geographically dispersed data centers.

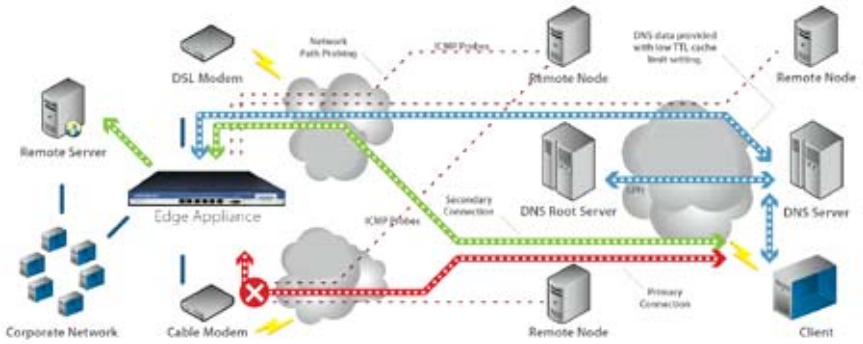
How Does It Work?

The ActiveDNS and ISP Load Balancer incorporates a complete DNS server. This DNS server is dynamically updated with the latest IP address and active interface information. While ActiveDNS does support load balancing requests to an internal server**ActiveDNS does not support "over-loading"**, or the ability to send an uneven amount of traffic to a specific server when multiple internal servers are available. The weighting functionality of the ActiveDNS module is designed to spread the traffic across the network interfaces, not multiple servers. If that functionality is required XRoads Networks recommends placing a server load balancer between the EdgeXOS appliance and the internal server farm, we work with a number of server load balancer partners that we can recommend.

The DNS server's purpose is to respond to remote clients inbound requests for IP address

information based on the queried domain. By changing how responses to these requests are handled, the Vector Routing module can determine on which interface the inbound traffic is received from the remote client. This is a very effective method for load balancing and redirecting inbound traffic during a network outage.

In order for this method of "inbound routing" to work, the EdgeXOS appliance, and the ActiveDNS module, must be configured as the domain primary DNS server.



The method used determine how the DNS responds to remote clients is based on the interface address information, active path status (as determined by the Vector Routing module), and changes made to the dynamic DNS database based on those methods.

As the DNS responses are made to the remote clients, they have a limited TTL (time to live) value and include all of the IP addresses of the network interfaces which are associated with the active network paths. These addresses are provided in an order defined in RFC 1034 / 1035 / 1794 and BIND 4.9, September 1998. An example of how ActiveDNS has implemented these standards is given below:

Equal Round-Robin Response

www IN A 10 10.0.0.100 5 1

www IN A 10 10.0.0.101 5 1

www IN A 10 10.1.1.100 5 1

(where 5 is the TTL specified in seconds)

Dynamically Weighted Response

www IN A 10 10.0.0.100 1 WAN1 (the lower the weighting the more preferred)

www IN A 20 10.0.0.102 1 WAN1 (where the "20" is less preferred)

www IN A 10 10.1.1.100 0 WAN2 (where the "0" represents a DOWN interface and is not provided in the DNS response)

Some BIND servers considers any TTL under 300 seconds as "irrational", and substitutes in the value of 300 instead. This greatly hampers the functionality of volatile zones. In the fastest of all cases - a 0 TTL - information would be used once, and then thrown away. Many the new server

NetXcom ICT / XRoads Solutions:

allow for the RR information to be calculated every 5 seconds, and the RRs handed out with a TTL of 0. It must be considered that one limitation of the speed of a zone is going to be the ability of a machine to calculate new information fast enough.

Weighted Route Selection

As seen in the above example, weighted route selection is performed for both outgoing and incoming connections.

Outbound connections can be routed directly, or load balanced between two or more interfaces and their gateways. The method used by the ActiveDNS and ISP Load Balancer is to increase the weight of each default route, and thus increase the likelihood that the route will be used.

Inbound connections are similarly load balanced using the ActiveDNS module's dynamic DNS server. In this case the IP addresses provided in response to DNS requests are similarly weighted so that the more highly weighted addresses are provided as the first address in the response.

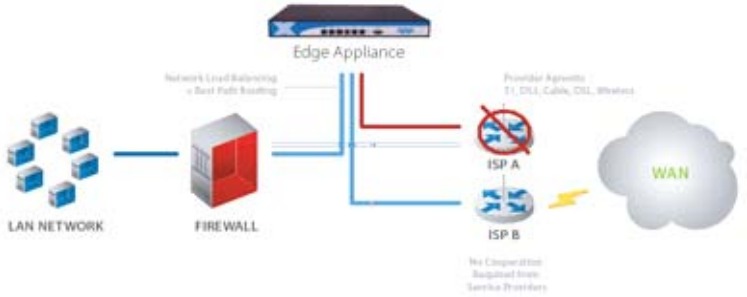
The ActiveDNS module is based on open source technology which has been available for over ten years. XRoads Networks has been developing and implementing these solutions for over a decade.

ActiveHA™ Network Redundancy

False outages and undiscovered outages are a major potential problem when implementing a network load balancer. Many network load balancers simply do not perform enough testing to know when an outage has actually occurred, or they may trigger an outage simply when a high latency event has occurred.

Automated Network Failover / Failback

XRoads Networks can help ensure that your network stays up and running by automatically detecting a network outage and failover application traffic from failed links to the remaining active connections. This failover occurs seamlessly and (depending on the type and timeout of the application) occurs without having to reset your existing connection.



NetXcom ICT / XRoads Solutions:

When an outage occurs the EdgeXOS platform automatically re-routes application traffic across the remaining available connections. Typically this is a secondary wide-area network connection, however it would also be a secondary route available via different VLANs and/or redundant switching clusters.

Deep Path Inspection™

To protect against these potential pitfalls the Edge appliance implements multi-level outage detection which performs various network tests in order to determine the true status of each link.

False Outages

Generally occur when a device is probing a network connection and due to some form of high latency, created either from normal high traffic usage or a potential hacking attempt, will cause the device to trigger an outage.

The problem with this is that it generally means that existing sessions are dropped (worst case) or delayed while the device turns down the "bad" link.

Undiscovered Outages

A potentially worst scenario is one in which the device does not perform enough testing, perhaps it only tests the local gateway connection, if the actual WAN link itself failed, or the local ISP was having problems with its connectivity to the Internet, the device would not see this problem and continue to forward traffic over the bad link.

How Does It Work

Using a patent-pending method for performing **Deep Network Probing** the Edge appliance not only tests the local connectivity, but continues to test out to the various points on the Internet to ensure that full connectivity is available.

When private networks are being balanced, the Edge appliance can be configured to only test the local and remote gateways thus ensuring full site-to-site connectivity.

Using multiple level testing the Edge appliance also ensures against temporary high-latency events from causing a link failure event. Only a sustained high latency event will trigger such

NetXcom ICT / XRoads Solutions:

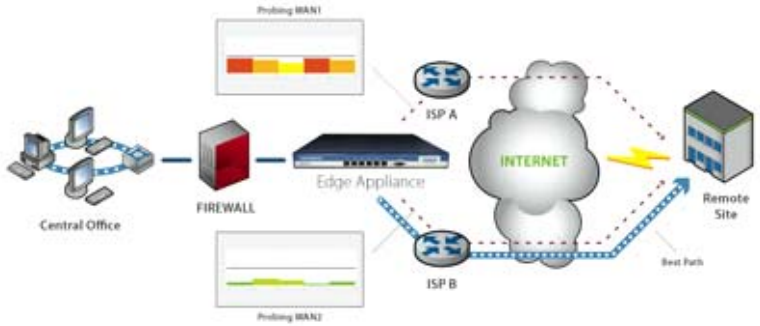
action, thus preventing any session breakdowns from re-routing traffic.

Multi Vector Priority Routing™

Only the EdgeXOS platform incorporates eleven (11) sophisticated algorithms for determining how to route traffic between multiple network paths. Using MVP Routing™ customers can combine multiple broadband links for more throughput and faster speeds for high bandwidth applications.

Best Path Routing

XRoads Networks solutions incorporate our MVP Routing™ technology which includes our Best Path Routing™ module. MVP Routing™ ensures that network traffic uses the most appropriate network path through a latency and packet loss testing performed across the available WAN links. Once the best path is determined all session traffic associated with that path traverses the chosen link. In the event of a network failure all traffic will be routed across the next best path.



XRoads Networks best path routing can help your network applications by reducing latency and providing improved response times for end-users, thus increasing productivity. The EdgeXOS appliance also reduces downtime for these critical applications by providing automated network failover.

Application Routing

MVP Routing™ also allows you to quickly force specific types of application and/or source traffic through a specific WAN interface. This means that end-user traffic will always take the most appropriate traffic based on either Best Path Routing™ or your specific application routing policies.

Routing Methods

Algorithm Metrics

- Available Link Rate

NetXcom ICT / XRoads Solutions:

- Current Utilization (per path)
- Current Latency (per path)
- Last Path Used (per path)
- Administrative Weighting (per path)

The Multi Vector Priority Routing algorithm is designed to provide two fundamental services, dynamic network load balancing across multiple paths and reliability assurance in the event that one or more of those paths should fail.

Vector Routing uses various metrics (below) to determine how new network sessions should be routed over the various active links. Unlike other load balancing solutions, it does not use simple Robin-Robin balancing. The EdgeXOS platform uses a combination of**11 different network aggregation algorithms** which are continuously fed metric information that is used to determine the best next hop for outbound connections. Some of the routing options include:

- **Intelligent Vector Routing Algorithm Includes:**
- **Least Used Adaptive Weighting**
- **BPR Latency Based**
- **BPR Packet Loss Based**
- **BPR Jitter Based**
- **Persistence Based**
- **Application Based**
- **Prioritization Based**
- **Multi-Session Based**
- **Active Spill-Over**
- **Standard Weighted**
- **Basic Round Robin**

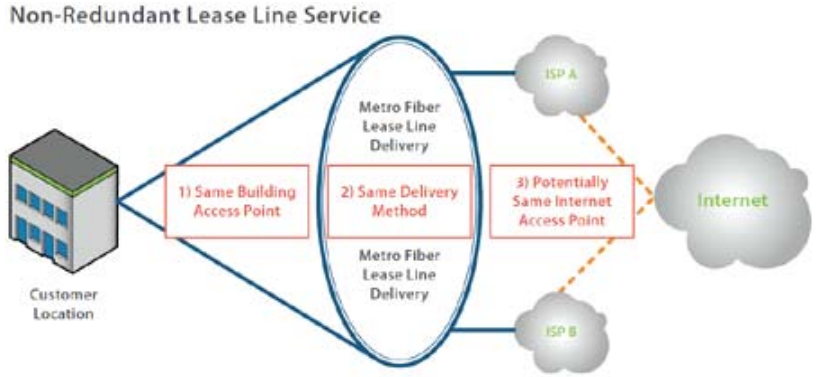
Intelligent Vector Routing Algorithm

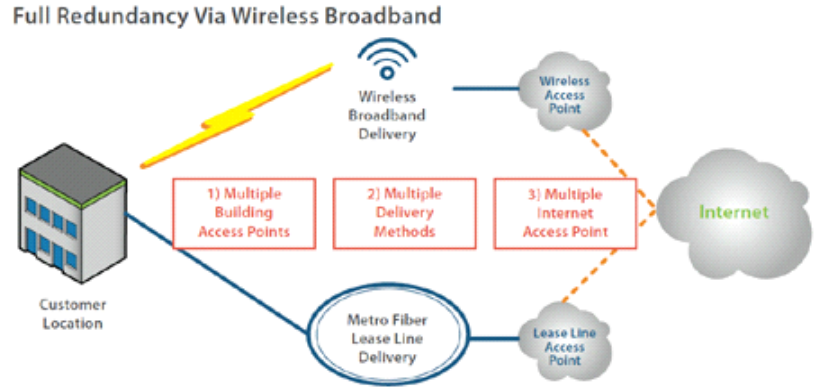
The default and recommended method for determining path balancing is our IVRA option. This option is the most dynamic and uses real-time metric information to determine how to best route new session traffic.

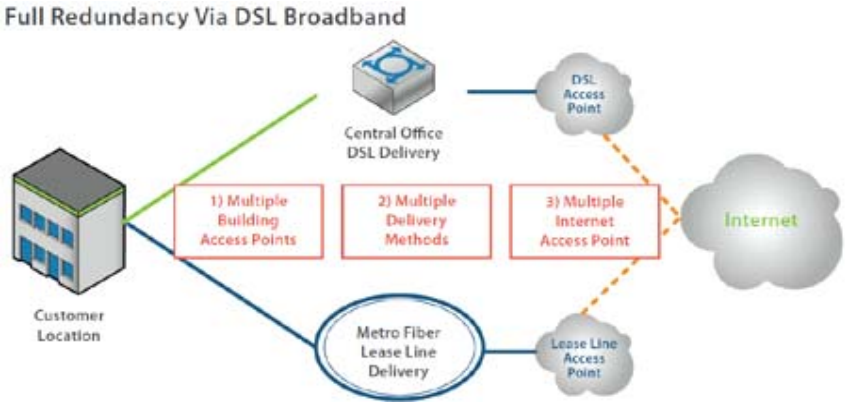
Deployment Scenarios

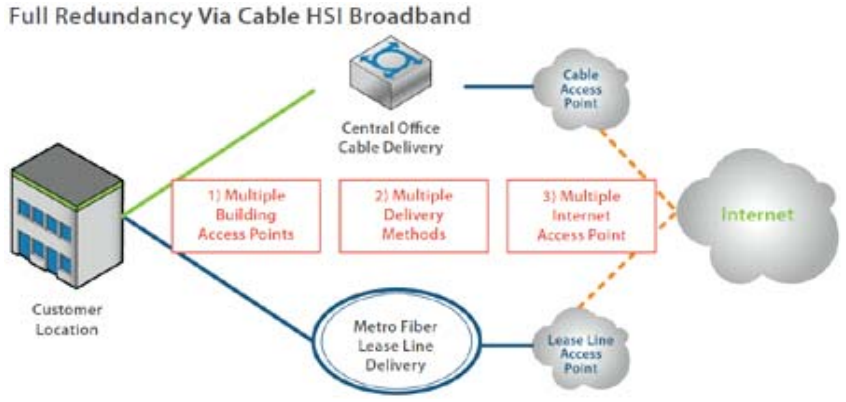
The following examples demonstrate the flexability in the EdgeXOS platforms design. These appliances can be deployed in a number of different environments based on the requirements of the customer and the existing infrastrucutre.

NetXcom ICT / XRoads Solutions:









NetXcom ICT / XRoads Solutions:

Application QoS/Throttling

The EdgeXOS appliance is one of the few bandwidth management appliances on the market that provides the level of granular shaping as our policy-based shaping rules provide.

Bandwidth Appropriation

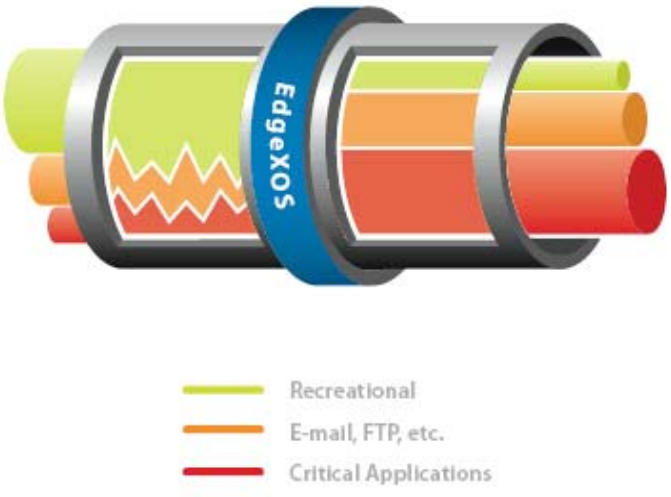
Network resources are a limited commodity and there is a constant battle for bandwidth by both critical and non-critical applications. XRoads Networks helps you better allocate these limited resources to those applications which your organization depends on. The EdgeXOS's shaping options include the ability to instantly prioritize critical applications and URLs and set lower priorities for non-critical applications.

Policy-Based Shaping

Give network administrators the ability to set specific limits for certain applications, users, and/or groups of users. The shaping policies enable a great deal of flexability in how bandwidth is allocated and reserved. Additionally, ppolicy-based shaping can be controlled based on network utilization, i.e. if utilization reaches 'x' policies can be applied to limit certain application which may be allowed to use more bandwidth when overall utilization is low.

Granular Policy-Based Control

Using the policy-based shaping a network administrator can set specific and exact (down to 10Kbps) bandwidth usage rules. What this means is that the administrator has complete control to allocate bandwidth as they choose and guarantee that certain servers, end-users, applications get the bandwidth they need.



Bandwidth Groups & Policies

NetXcom ICT / XRoads Solutions:

When creating a new policy, the first step is to initially define a bandwidth group to which the policy will be bound. Bandwidth groups can be defined based on shared or single group delegation. Within a group the administrator can set the **Max Bandwidth, Min Bandwidth, and Burst Bandwidth** for a given group. Additionally the administrator has the ability to also set the queuing rules for a specific group with up to 12 levels of priority.

Once a group is defined a policy must be assigned to the group. Policies can be defined using the following criteria:

- Name
- URL Address
- IP Address / Network
- Application Type
- Port / Protocol
- Source / Destination
- Layer 7 String
- QoS Level
- and MAC

Each policy will automatically generate usage statistics which can also be used for end-user or department billing purposes.

Without The Edge Platform

Slow screen loads, delayed responsiveness, high latency. All characteristic is poor network performance. What are the costs involved when end-users can't access business-critical applications due to poor network performance?

Opportunity Costs

When a network is performing poorly how does that effect the bottom line? If sales transactions can not be submitted in a timely fashion or follow-ups can not done on time how does that translate to lost revenue?

Reduced Productivity

While end-users may try to be as productive as possible, when network slowdowns cause applications to become unresponsive there is not much that can get accomplished. How much time is wasted each day by end-users attempting to access a business-critical application, timing out do to traffic spikes, or getting screen refreshes so slow that multiple button clicks cause duplicate entries?

MPLS End-to-End QoS

When connecting to an MPLS network, packets coming in and out of the network must keep the Diffserv marking throughout the process or shaping could be lost as it enters or leaves the local

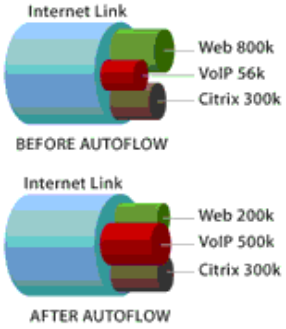
NetXcom ICT / XRoads Solutions:

network.

Application Prioritization

The EdgeXOS appliance supports several methods for prioritizing traffic, including session limiting (where only so many sessions are allowed per second), URL shaping (where traffic can be prioritized based on the destination), and application shaping (where the traffic can be prioritized based on a defined application classification).

Administrative Shaping



These methods for controlling bandwidth are called administrative shaping controls. They do not provide the granularity that policy-based shaping provides but do allow the administrator to set more general rules for which traffic is preferred and which traffic has lower important for the organization.

Download our **solution overview**

Application Classification

The EdgeXOS includes a number of pre-defined applications from which to choose from **Application Listing** however the network administrator can also define their own applications based on:

- Name
- Protocol
- Port (Source / Destination)
- and String Identifier

Application Prioritization

Once define an application can be set to one of 5 levels of prioritization within the shaping engine. By changing the queuing for each level the EdgeXOS platform is able to effect application responsiveness and smooth packet streams.

URL Prioritization

Similar to application shaping the EdgeXOS is also able to prioritize bandwidth based on the

destination URL. This is useful if end-users go to a specific website and/or SaaS service. It can also be used for prioritizing certain FTP sites, or for Citrix and RDP users. Simply define the remote URL/network and assign the level of priority.

Session Limiting

One of the many problems which peer-to-peer clients create is that when they start they launch many if not hundreds of sessions in order to speed up the download of recreation audio, video, and software files. These large session counts have the effect of slowing down networks. With session limiting enabled, peer-to-peer applications are limited to the number of sessions they can use, and this in turns ensures more equal distribution of bandwidth.

Application Auto-Classification

Listing (continuously updated)

Category Application Definition Category Application Definition

Backup Veritas Backup Exec Messaging SMTP (Simple Mail Transport Protocol) [top]

Backup Retrospect Backup Software Messaging IMAP (Internet Message Access Protocol)

Backup RepliStor Backup Software Messaging POP3 (Post Office Protocol) [top]

Backup Availl Backup Software Messaging Mircosoft Exchange Support [top]

Backup Veritas Utility Messaging Lotus Notes IBM Database

Client-Server Citrix Services [top] Messaging Yahoo Messaging Service

Client-Server SNA IBM Gateway Services Messaging AOL AIM Service

Client-Server SNA Microsoft Gateway Server Messaging SNPP (Simple Network Paging Protocol)

Client-Server WebSphere IBM Everyplace Software Messaging T120 Data Communications

Client-Server Microsoft Terminal Server Service Multimedia RTSP (Real Time Streaming Protocol)

Client-Server Microsoft DynamicCRM Software Multimedia IRC (Internet Relay Chat)

Client-Server Microsoft ASP.net Services Multimedia Microsoft Live Meeting Service

Client-Server AOL Instant Messaging Service Multimedia Microsoft Media Player Software

Client-Server RPC (Remote Procedure Call) Multimedia RTP Video Support

Client-Server Timbuktu Service Multimedia QuickTime Streaming Server

Client-Server SAP Access Control Multimedia Apple iTunes Radio Streams

Client-Server Apple NetAssistant Service Multimedia Microsoft NetMeeting Service

Client-Server PCAnywhere Service Multimedia Talk Service

Client-Server VNC Service Multimedia Real Networks G2 Server

Client-Server XWindows Service Multimedia Shoutcast Server

Client-Server Palm Network Service Printing RLP (Remote Line Printer) Service

NetXcom ICT / XRoads Solutions:

Client-Server IBM SNA Access Server Printing IPP (Internet Printing Protocol)
Client-Server IBM SNA Extender Service Printing Printer Spooler Service
Client-Server Edge Remote Admin Printing Print Server
Client-Server SAP R3 Application Routing NetBIOS Microsoft Local Network Services
Client-Server SAP R3 Utility Routing Micosoft RPC Service
Client-Server BootStrap Server Routing Microsoft NETBIOS Service
Client-Server Sun RPC Server Routing Microsfot DGM Service
Client-Server MSN Microsoft Network Routing NetBIOS Service
Database Oracle Database Protocol Suite Routing BGP (Border Gateway Protocol)
Database Microsft SQL Database [top] Routing RSVP (Resource Reservation Protocol)
Database MySQL Linux-based Database Routing L2TP (Layer 2 Tunneling Protocol)
Database DB2 IBM Document Management Software Routing X400 Service
Directory LDAP (Light Weight Directory) Routing RIP (Routing Internet Protocol)
Directory DNS (Domain Name Server) Service Security SSH (Secure Shell)
Directory DHCP (Dynamic Host Control Protocol) Security PPTP (Point-to-Point Tunnel Protocol) VPN Services
File System Microsoft SMS (Systems Management Server) Security TACACS Remote Access Service
File System TFTP (Trivial File Transfer Protocol) Security Kereros Authentication Service
File System NFS (Network File System) Security RDP Remote Desktop [top]
File System Netware Service Security ISAKMP Key Exchange Service
File System RemoteFS Service Security RADIUS Remote Access Control
Internet HTTPS Web SSL (Secure Sockets Layer) [top] Security RAD-ACCT Radius Accounting
Internet HTTP Web Browser Service [top] Security PGP (Pretty Good Privacy)
Internet Telnet Service Security VPN IPSec ESP Tunnel
Internet FTP (File Transfer Protocol) [top] VoIP H323 Discover Protocol Support
Internet NNTP (Network News Transfer Protocol) VoIP H323 Gatekeeper Protocol Support
Internet Netstat Service VoIP H323 Setup Protocol Support
Internet Telnet Service VoIP H323 Control Protocol Support
Internet NNTP (Network News Transfer Protocol) VoIP SIP Protocol Support [top]
Internet UUCP (Unix-Unix Copy Protocol) VoIP Cisco VoIP Skinny
Internet NTP (Network Time Protocol) VoIP Swyx VoIP Support
Internet SNMP (Simple Network Management Protocol) VoIP RTP (Real Time Protocol) [top]
Internet Syslog Service VoIP Asterisk VoIP IAX Support
Internet SOCKS Service VoIP Asterisk VoIP IAX2 Support

NetXcom ICT / XRoads Solutions:

Internet WebObjects Service VoIP VoIP Vonage Service

Internet SFTP (Simple FTP) VoIP VoIP Packet8 Service

Secure End-Point Solutions

XRoads Networks EdgeXOS provided a layered security solution, where security can be deployed at the networks edge and on the organizations end-point devices for even greater overall secuurity. The XOS end-point security solutions are supported on desktop, mobile and tablet platforms.

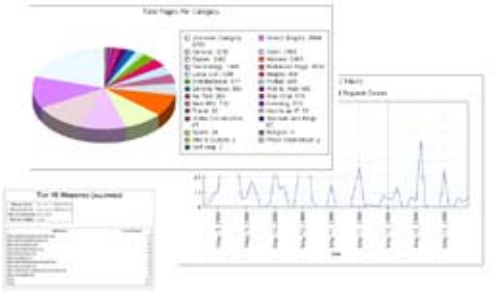
What Is The XOS Endpoint Client?

End-point client is a small software client which is loaded on to each end-users computer which will employ web content filtering. The client enables user-based reporting and filtering of Internet content, including preventing malware, spyware and other Internet born viruses.

During this time the Internet content requested is filtered through up to eight layers of checking, including URL checking, anti-virus, anti-phishing, anti-spyware/malware, custom rules and reporting, all while the EdgeXOS platform is ensuring **accelerated connectivity** through WAN bonding and 99.999% uptime through automated multi-link redundancy.

Global Web Filtering & Reporting

With the EdgeXOS platform scanning and redirecting new website requests in real-time our customers can be assured that access to unauthorized websites will be reported and blocked.



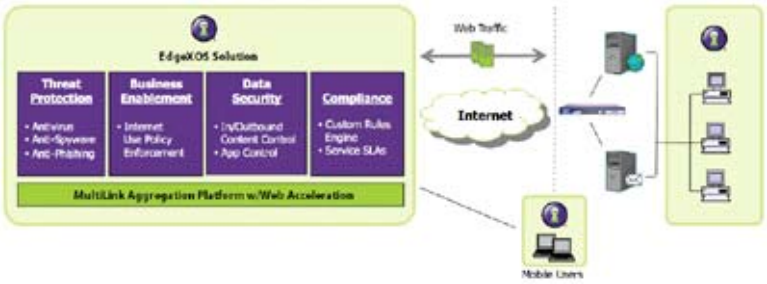
Our global web filtering solution is easy to implement, requires no changes to desktop systems or installation of client software, users simply login via login page presented when they go to initiate web connectivity. Some of the specs on our web filtering services include:

- Instantly allow/deny sites
- Bypass Specific Users
- Real-Time Web Usage Reporting
- PreDefined Category Blocking
- Capable of handling over 200,000 RPS

End-Point Web Threat Protection

NetXcom ICT / XRoads Solutions:

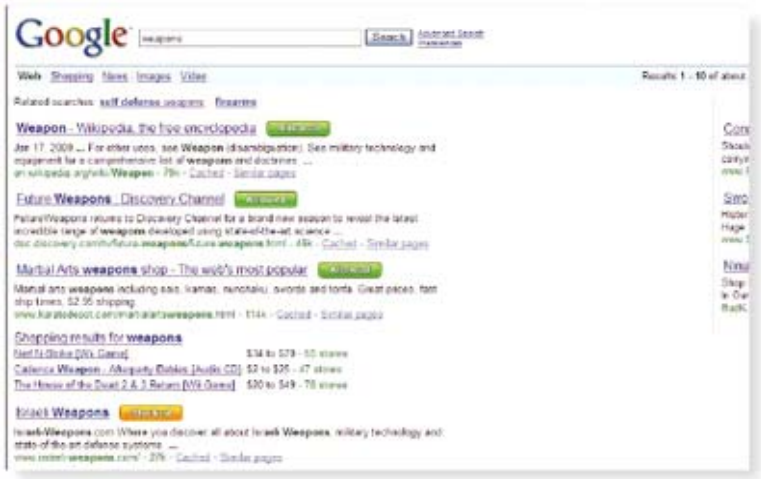
powered by Webroot



By integrating with the end-point client the EdgeXOS platform provides a unique combination of enhanced threat protection with real-time security acceleration for organizations of all shapes and sizes. The advantages delivered by this integration include:

- Desktop-Based Security Audits
- Local Site Caching & System Scanning
- Accelerated Real-Time Protection
- Multiple Reporting Layers
- Enhanced Traffic Shaping & Prioritization

With the EdgeXOS platform accelerating and redirecting the end-point client requests customers are guaranteed faster web downloads, improved prioritization, centralized network administration, and greater network reporting.
Some of the additional benefits of the end-point solution include:



Search Response Modification

Search that come back can be modified in real-time so that the end-user can see which sites would be blocked and which "might" be blocked and are placed in the "coached" category for further checking, all traffic is logged.

NetXcom ICT / XRoads Solutions:

Service Management / Keyword Tracking

Manage company Internet use and security policies via an intuitive web-based management console. Administrators can securely access a powerful rules engine to facilitate user, group and account level access policies. A real-time Web traffic summary dashboard displays company Web site access by category (12 main and 96 sub-categories) and popular search terms. The desktop Web proxy allows for seamless authentication into the service for mobile and on-site users, and it can be automatically updated to the latest version.

Real-Time Logging & Reporting

Real-time logs display which sites and downloads users have attempted to access and whether or not they were allowed. With logs accessible for 90 days, administrators can access the historical information they need to generate key metrics.

Detailed reports can be run ad-hoc or scheduled, allowing companies to accurately monitor Internet use by viewing graphs on Web traffic trends, top blocked URLs, blocked malware, bandwidth use and more. Scheduled reports can be set up to be distributed via email to a user, or a list of users, and can contain up to 100 separate charts for maximum visibility into company and user Internet use.

NetXcom ICT / XRoads Solutions:

Comprehensive Cloud Firewall

XRoads Networks incorporates a fully function firewall module within all of its appliances, along with our unique ApeXfilter™ which leverages our appliance link bonding capabilities and delivers both a next generation application filter AND a anti-spyware, anti-virus, anti-malware and anti-phishing solution.

Every EdgeXOS appliance includes our application firewall feature set, which incorporates a stateful firewall, simple rules-based application blocking, VLAN control, subnet firewalling, port and protcol based blocking, along with a comprehensive set of DoS protection and SYN flood prevention options.

The EdgeXOS also incoprorates advanced firewall logging features which capture full packet header information in order to assist in troubleshooting problems and/or network security issues. This logging can also be exported to a syslog server for long-term storage and examination.

With full NAT (Network Address Translation) and application proxy support, the EdgeXOS appliances also provide a flexible configuration environment. Support for port address translation and one-to-one address translation is included. The EdgeXOS appliances also feature DMZ and secure routed subnet capabilities by utilizing the DMZ interface options within the appliance.

Stateful Firewall

Each EdgeXOS appliance includes our PCI-compliant stateful rules-based firewall. Network administrators can quickly and easily create firewall rules to allow and deny traffic based on traffic type, source, destination IP address/network, port, protocol, etc. You can also create rules specifically to log certain types of traffic. This is extremely useful for troubleshoot network related issues to see where traffic is going and which ports it is using.

NetXcom ICT / XRoads Solutions:

Our WEBaXcel DWP thin-clients deliver **real-time databases** lookups which receive new web requests, instantly categorize the site, and response to the request. The entire express forwarding, scanning, and response takes less than several msecs.
During this time the Internet content requested is filtered through up to eight layers of checking, including URL checking, anti-virus, anti-phishing, anti-spyware/malware, custom rules and reporting, all while the EdgeXOS platform is ensuring **accelerated connectivity** through WAN bonding and 99.999% uptime through automated multi-link redundancy.

Comprehensive LAN Router

The Edge platform is a fully functional Later-3 router. It has the ability to handle static routing, RIPv2, and OSPFv2. The Edge Router also support VLAN tagging for switched networks.

Managing The Local Network

XRoads Networks' EdgeXOS appliances are hybrid bridge/router systems which enable localized routing across the LAN and DMZ interfaces. Hundreds of custom routes can be added to the EdgeXOS appliance along with the ability to connect the appliance to various switches in order to manage separate VLAN traffic and shape and accelerate applications across those separate network within your organization.

Routing Protocols

XOS PREVIEW

When the Edge platform is acting as the network gateway it is sometimes required to re-route traffic to other devices/routers which act as gateways for other departments, branches, etc. In these cases the administrator can setup static routes to forward data destine for the networks defined in those routes to be forwarded to the provided gateway.
The Edge platform also support dynamic routing using RIPv2 and OSPFv2. Both of these routing protocols can available via our command line interface, which is accessible via SSHv2 and the console port.

VLAN Tagging

XOS PREVIEW

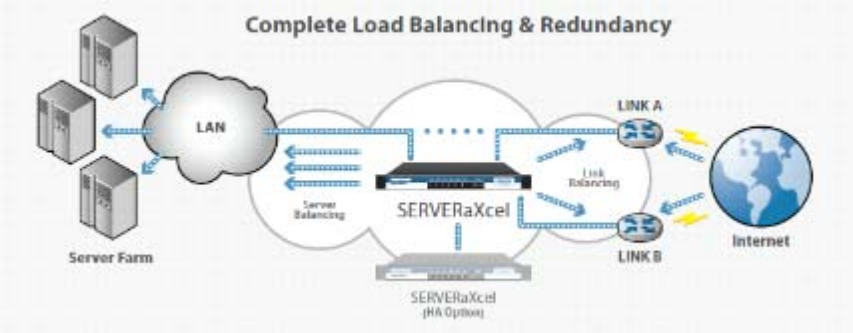
The Edge supports VLAN tagging for each of its interfaces, however it is recommended that only the LAN interface or a DMZ interface be used in conjunction with VLANs.
WAN ports can not be used with VLANs and still be able to test for network outages and thus can only be defined using VLAN tagging when the WAN interfaces are nailed up.

NetXcom ICT / XRoads Solutions:

Server Load Balancing - Scaling Application Services

XRoads Networks' EdgeXOS platform allows our customers to quickly and easily improve connectivity to critical applications by spreading inbound connection requests across two or more

application servers. Any TCP-based application can be balanced across up to 10 different servers. Servers are monitored in real-time for potential outages which would automaitcally bring that server out of production.



SVLB Methods

SVLB Features

- Easy Setup
- Round-Robin Balancing
- Weighted Balancing
- Session Persistance
- Multiple ISP Support

Server **Vector** Load Balancing is the ability to balance connectivity across multiple WAN links and multiple servers at the same time, thus increasing throughput and reliability for inbound network sessions. By combining these features into a single appliance, the EdgeXOS platform does so at a lower overall cost and delivers a faster return on investment.

Our server load balancing techniques are designed to be simplistic, i.e. easy to configure and manage. While the EdgeXOS may not include all of the capabilities as some other server load balancing solutions, we do have capabilities not found in other solutions, including:

- **ISP Link Balancing**
- **ActiveDNS Manipulation**
- **WAN Redundancy / Failover**
- **Built-In Traffic Shaping**
- **Full Network Usage Reporting**

NetXcom ICT / XRoads Solutions:

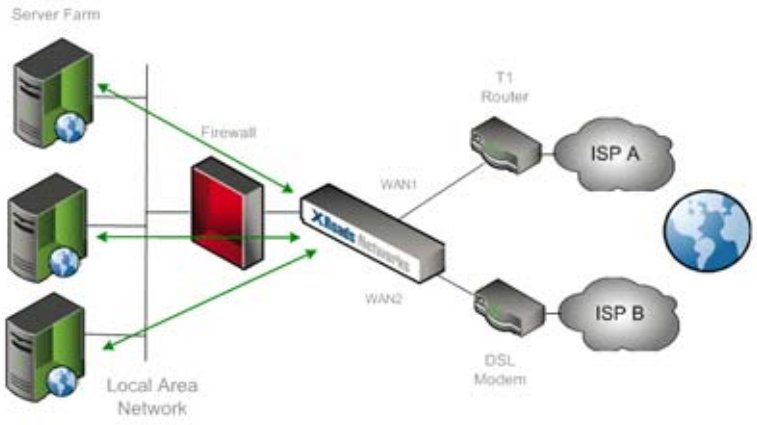
How Does It Work

Our server load balancing solutions work by excepting inbound server requests on one or more WAN links and then balancing those requests across the various defined servers. Servers are

monitored for uptime and removed automatically from the balancing algorithm if an outage is detected.

Servers are balanced in a round-robin order or can be weighted by the administrator.

Inbound connections can also be distributed across the various WAN links as needed.



Inbound connections are balanced between WAN links via our ActiveDNS technology and then load balanced across various servers based on pre-defined administrative weights.