

How To Guide

XRoads Networks

EdgeXOS Platform QuickStart Guide

EdgeXOS Functionality Overview

The EdgeXOS platform is a Unified Bandwidth Management device, meaning that it has the ability to support multiple bandwidth management functions, including: WAN Link Load Balancing & Failover, Web Aggregation & Acceleration, Traffic Shaping & QoS, Network Monitoring & Reporting, and Site2Site Link Bonding w/Automated Redundancy.

Beyond these various capabilities, the EdgeXOS platform is also highly flexible when it comes to setup and installation. This guide is designed to assist new customers with planning their installation so that it meets their unique requirements. Use the examples provided below to determine which installation method is best for your environment based on your specific requirements.

We hope that you enjoy the capabilities that the EdgeXOS platform provides, thank you for your purchase of our products, and please provide us with feedback by going to:

<http://www.xroadsnetworks.com/ubm/products/survey.xrn>

Obtaining Installation Support & Assistance

XRoads Networks provides a host of support services for our end-users, including free and unlimited online web-based support, email and chat support, along with phone and remote configuration support provided by our support center (with the purchase of a support contract). Access support by going to our dedicated online support web site...

Video (Step-by-Step Support) URL: <http://videos.xroadsnetworks.com>

Support URL: <http://www.myxroads.com>

The screenshot displays the XRoads Networks Support Center website. At the top, the XRoads Networks logo is visible. Below the logo is a navigation bar with buttons for Home, Knowledgebase, Submit Ticket, Troubleshooter, and Login. The main content area features a large banner with a woman working at a computer, labeled "SUPPORTCENTER". Below the banner, there is a section titled "XOS Support Center" with a welcome message. A prominent button says "Chat with a Live Service Representative". The page is organized into a grid of service tiles:

- Submit a Ticket:** Submit a help desk trouble ticket to our service representatives.
- Live Chat:** Chat with a customer service representative directly.
- Knowledge Base:** Search our knowledgebase of information to find resolutions to common issues.
- Troubleshooter:** Find the resolution to issues by taking a step by step tour based on your responses to questions.
- Schedule Install Support:** Submit an installation support call request, please submit 24 hours in advance.
- Live Configurator:** Configuration wizard, automatically builds config files for your Edge device.
- Documentation:** Access online Manuals, HowToGuides, and configuration examples.
- Firmware Downloads:** Obtain the latest XOS firmware revisions and patches (requires support contract).

The MYXROADS site provides 24/7 access to:

- Our frequently asked questions via our Knowledge database which includes hundreds of answers to the most asked questions regarding the EdgeXOS platform
- Technical support documentation, including HowToGuides, Best Practices & Installation Guides, and Platform Notes (which provide specific feature details and step-by-step examples)
- Our Troubleshooter which guides administrators step-by-step through problems in an attempt to find a solution
- Live Chat support which provides users with online access to our support team.
- The ability to open and view the status of support tickets. All phone-based support is driven through our ticketing system, so if you require installation phone support, please make sure to open a ticket at least 24 hours before the time that you wish to actually install the appliance.
- Access to the latest EdgeXOS firmware (requires platform maintenance and a valid username/password)
- Our Live Configurator which is what you will need to use when requesting installation support from an XRoads Network support engineer. All installation support is predicated on the requirement that the Configurator be filled out ahead of time and that our engineering team has a chance to review what has been submitted.

Live Configurator

All installation support is driven by the information submitted to this system. The information submitted via the 'Live Configurator' is saved and can be retrieved by our support team 24/7 for review and comment. When submitting information to the Live Configurator you will be assigned a configuration ID. You may use this ID to edit the configuration information in the future, and you should provide this ID when requesting support via the ticket system.

The Configurator can be accessed via the MYXROADS website, or by going to:

<http://configurator.myxroads.com/configurator.html>



XOS Configurator

XRoads Networks has developed this configuration file generator to simplify the initial configuration of your Edge platform. If you have any questions about how to use this form, please refer to your QuickStart Guide or contact the support center.

Configuration ID:

Enter a registered configuration ID to make changes.

Steps To Obtain Phone-Based / Remote Installation Support

(IMPORTANT SUPPORT INFORMATION)

The following steps MUST be followed in order to obtain phone-based, remote installation support for your EdgeXOS appliance.

Step 1) Review the rest of this QuickStart manual and determine the best method for installing your appliance. If you are unable to determine this then you may wish to consider purchasing our 360 Consultation Support services. These services provide full network consultation for your EdgeXOS installation and include all of the support you would need to install this device.

Step 2) Once you determined the correct method to install your EdgeXOS appliance, utilizing the example within this guide. The next step is to login to the www.myxroads.com support site and fill out the Live Configurator with the information that matches the example you selected below (i.e. in the examples below you will find numbered fields, these fields match the information requested by the Live Configurator, simply match up these fields when filling out the Live Configurator.

Step 3) Upon generating the Live Configurator file you will receive a unique ID for your configuration. Make sure that the serial number you enter is correct or the ID will not be correct. The serial number can be found either on the bottom of the appliance itself, or by viewing the serial number on the Home page of the web interface for the appliance. You can use the README 1ST document included with your appliance to find out how to access the Home page of the appliance.

NOTE: The configuration file MUST be filled out at least 24 hours before a scheduled installation call can occur. Phone-based installation support requires this amount of time in order to review your configuration, ask additional questions, etc. in order to make your installation quick and successful.

Step 4) Now that you have a configuration ID you can request phone-based installation support. You can request installation support via one of two methods: a) call our support center at 888-997-6237 and schedule your installation support time (make sure to have your configuration ID available when you call), b) go to our support website www.myxroads.com and click on the Schedule Install Support icon to create your own installation ticket. Tickets are based on your email address.

Step 5) Installation support times are setup in 90-minute intervals so we can only accommodate a finite number of requests per day. Installation times are assigned on a first come, first serve basis. Upon scheduling your installation a technician will email confirmation of the scheduled time, or ask if we can schedule it for a different time/day. Once scheduled an engineer will respond to the ticket (via email) confirming the installation time and request any additional information which might be required by the install engineer.

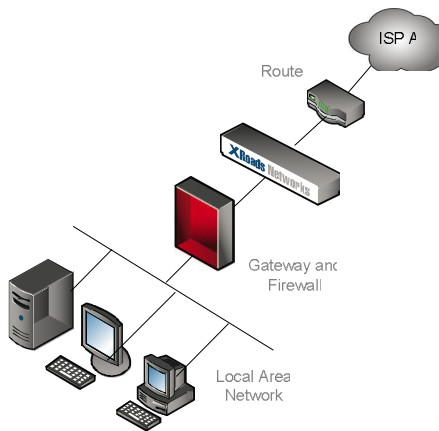
Live Configurator: Example Configurations

Use these example configurations to determine the best installation method for your deployment. If you are unable to determine the correct method you may wish to purchase our 360 Consultation Support service in which we assign a dedicated network engineer to assist you with your implementation.

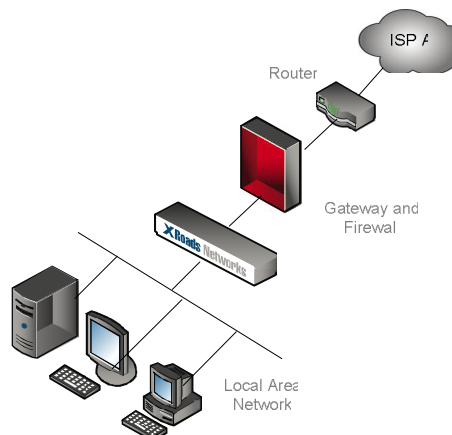
The following examples are broken down into three different categories. These categories are based on where the appliance will be placed, either a) in front of the firewall (i.e. between the firewall and the WAN), b) behind the firewall (i.e. between the LAN and the firewall), c) where the EdgeXOS replaces the existing firewall.

So in general, when would you implement a specific category?

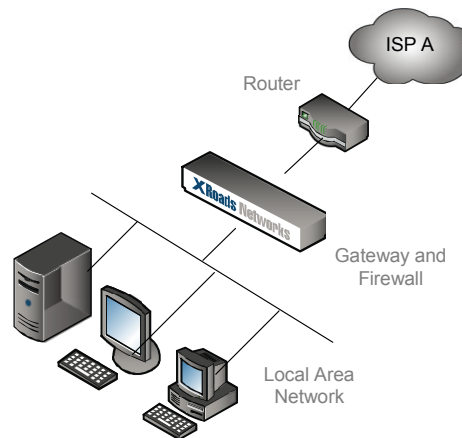
- Pre-Firewall (In Front of the Firewall) – If you have an existing firewall and wish to fully utilize your firewalls capabilities for any inbound or outbound connectivity then typically the EdgeXOS is placed using one of these examples.



- Post-Firewall (Behind the Firewall) – If you have an existing firewall but wish to fully utilize the traffic shaping capabilities and reporting capabilities of the EdgeXOS appliance then typically the EdgeXOS is placed using one of these examples.



- Replace the Firewall – If you have an existing firewall but believe that the EdgeXOS firewall will be able to handle most of your security requirements as it does have a fully stateful Layer-7 firewall built-in, then you can use one of these examples.



NOTE: The 'Pre' or 'Post' firewall designation is determined from the WAN perspective. So when we say "Pre-Firewall" we are looking at it from the WAN or Internet side of the network configuration, so the EdgeXOS appliance is sitting in front of or before the firewall, i.e. a "Pre-Firewall" deployment.

Pre-Firewall Installation Examples

The following network diagrams can be used when placing the EdgeXOS appliance in front of an existing firewall. The examples are provided in order with the most typical network scenarios provided first.

Pass-Through w/Bridge (Bridge Mode)

This is the easiest method for installing the EdgeXOS appliance; however it does have some requirements and some limitations.

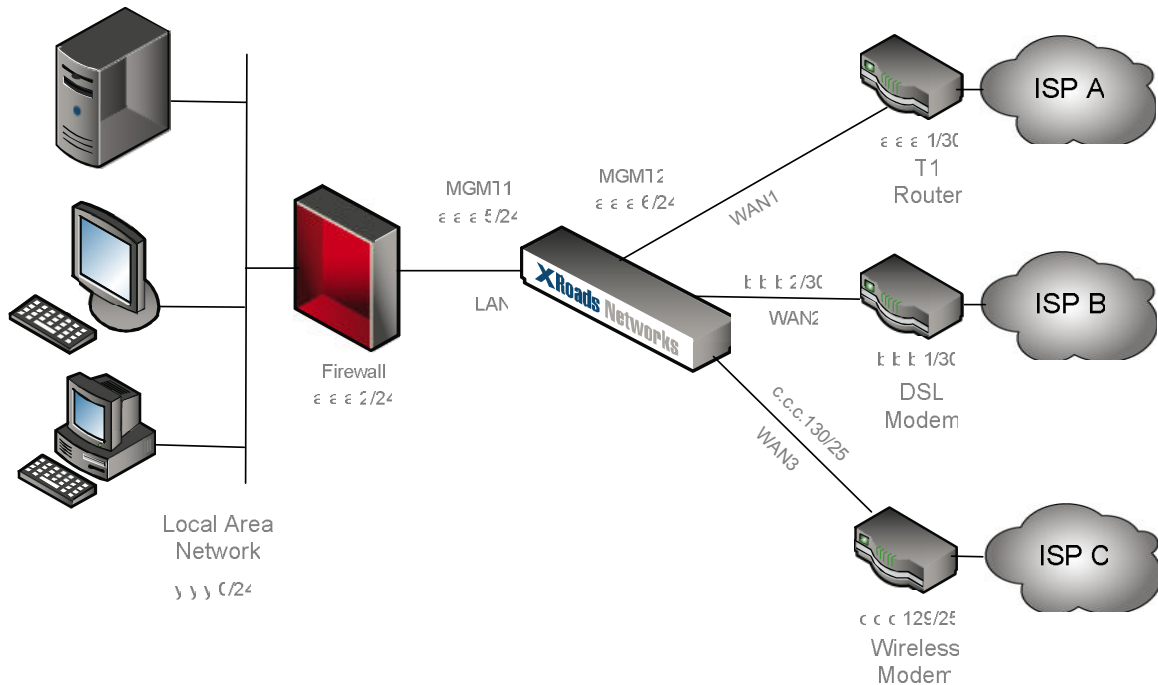
Requirements: When in bridge mode, it is required that you have two available IP addresses within the bridged network range, i.e. if you have 32 available addresses, 2 must be allocated for the management of the EdgeXOS appliance.

Limitations: When using bridge mode the appliance can not be configured to use multiple WAN subnets, i.e. there can only be a single network which is managed by the EdgeXOS platform. You can have additional subnets on the WAN; however they can not be controlled and/or monitored by the EdgeXOS appliance.

Steps To Install: The first step when installing this example is to pre-configure the appliance offline using a laptop or other similar method. Once bridge mode is configured, committed, and saved, you can then physically place the appliance between the LAN and WAN devices of the network. This will create a momentary outage while you are booting the appliance.

When initially configuring the appliance, set the laptop to use the IP address 192.168.168.100/24. Then connect to the LAN address (default 192.168.168.254/24 via a

web browser). Next configure the LAN interface to use the first management IP address (example a.a.a.5/24), then configure the WAN1 interface to use bridge mode and configure the second management IP address (example a.a.a.6/24). Make sure to Apply both changes and then commit the changes (the LAN port will use the same address). Change the laptop to use an address on the LAN address/subnet. You should now be able to access the EdgeXOS appliance via the LAN address you assigned. Make sure to SAVE the configuration once you are back into the appliance, then shutdown and prepare for installation into the network, as detailed in the diagram below:



Once installed between the LAN and WAN gateway devices you should be able to access the EdgeXOS appliance through the firewall using the management IP address you assigned to the LAN interface.

If you have any problems at this point, you can console into the appliance in order to perform ping tests to the LAN and WAN side IP addresses. If you continue to have problems it might be a configuration issue, default the configuration via the console CLI using the standard default method (see Platform Notes) and repeat the previous steps.

Once you are back into the web GUI, continue the configuration by bring up the additional WAN interfaces, one at a time. Once all of the WAN connectivity is up and active you can move forward with setting up traffic shaping rules and any inbound server balancing via Virtual, O2O, or O2M NAT. See our HowToGuides and Platform Notes documentation for details on this configuration.

Direct Network Address Translation (NAT Mode)

This method requires some changes to your existing network; however when configured in this mode all of the features and capabilities of the appliance can be fully enabled.

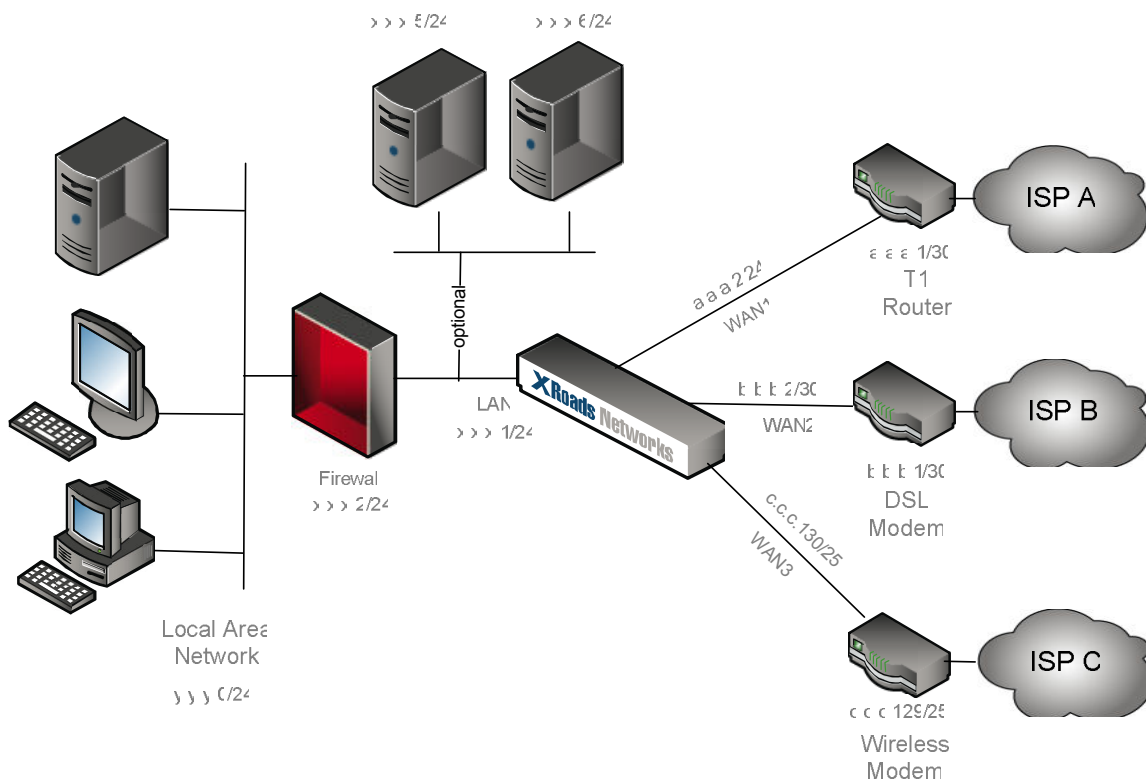
NOTE: If possible this is the recommended method for pre-firewall configurations.

Requirements: This method does require changes to your existing network architecture, including changing any LAN side network addresses to use private space (any private space will work). If all of your existing network traffic is behind a firewall, then only the firewall needs to be changed, which makes the configuration much easier.

Limitations: No feature limitations, however the hardware bypass features can not be fully utilized if there is an appliance failure, however this can be offset by using two appliances in HA (high-availability) mode.

Steps To Install: The first step when installing this example is to physically place the appliance between the LAN and WAN devices. This will create a momentary outage while you are configuring the appliance. The WAN1 interface must be connected to the WAN1 router/modem device.

Once the WAN1 interface is connected, connect the LAN into a laptop to begin the configuration process using 192.168.1.100/24 on the laptop. Configure the WAN1 interface to use NAT mode, use the old firewall address for the WAN1 interface. Configure the LAN address with a private address (which will become the gateway address for all devices on the LAN side of the appliance). Now Apply and Commit the changes.



Make sure to change the IP address on the laptop to use the same network/subnet as the newly configured LAN interface. Now log back into the appliance via the new IP address (if you have any problems change the laptop back to the old address and make sure that the changes were committed). The WAN1 link will take 10-30 seconds to come up. Now test connectivity and (very important) SAVE the changes via the Save button on the Home page. Once the configuration has been saved connect the LAN interface directly to the LAN device (i.e. the firewall in most cases).

Make any changes to the firewall, servers, etc. that are on the LAN side of the EdgeXOS appliance so that they are now in the same subnet as the LAN interface. Also make sure that the gateway address of these devices now points to the LAN address of the EdgeXOS appliance.

You should now be able to test connectivity to the EdgeXOS appliance through the firewall and from anywhere on the LAN side of the appliance. Once you have re-established access to the appliance you can begin configuring the rest of the WAN interfaces, inbound server connectivity, NAT mappings, Vector Maps, etc. See our HowToGuides and Platform Notes documentation for details on this configuration.

Pass-Through w/Proxy (Proxy Mode)

This is probably one of the easiest methods for installing the EdgeXOS appliance; however it does have some requirements and some limitations.

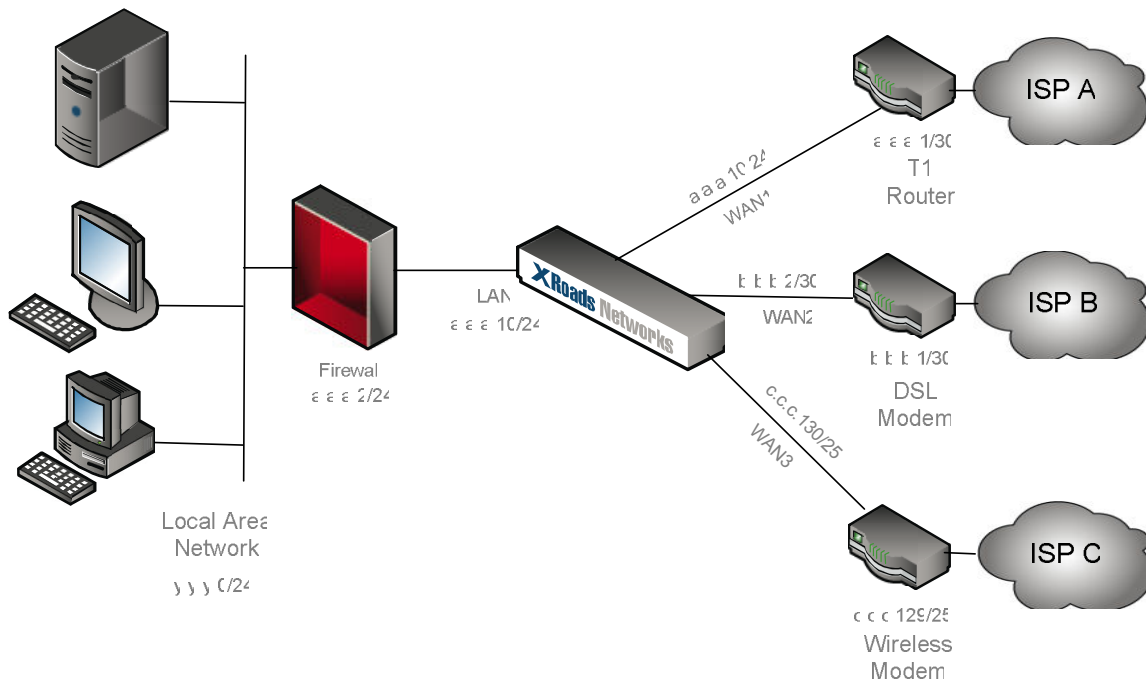
Requirements: In order to use proxy mode, the EdgeXOS appliance must sit between a local WAN router and a local firewall appliance, i.e. it must sit between two routing devices. Also, both devices must be local to the appliance, i.e. directly physically connected, no switches, no hubs, no extended Ethernet drops, etc.

Limitations: When using proxy mode the appliance can not be connected directly to any other appliance which is already in a proxy mode (i.e. no proxy firewalls or other ARP proxy devices). Proxy mode also prevents some traffic shaping functionality from working, specifically policy-based shaping. In some versions of the EdgeXOS firmware proxy mode also requires that the appliance switch its LAN to the WAN1 address when a failure occurs, thus requiring failback testing several times throughout the day, so immediate WAN1 failback is not possible.

Steps To Install: The first step when installing this example is to physically place the appliance between the LAN and WAN devices. This will create a momentary outage while you are configuring the appliance. WAN1 must be directly connected to the WAN1 router; no switches, hubs, etc are allowed.

Once the WAN1 interface is connected to the WAN1 router, connect the LAN into a laptop to begin the configuration process using 192.168.168.100/24 on the laptop. Configure the WAN1 interface to use proxy mode, use an available IP address from the WAN1 network. Apply and then commit the changes (the LAN port will use the same address). Change the

laptop to use an address on the WAN1 address/subnet. You should now be able to access the EdgeXOS appliance via the WAN1 address you assigned to the WAN1 link.



Now test connectivity and (very important) SAVE the changes via the Save button on the Home page. Once the configuration has been saved connect the LAN interface directly to the LAN device (i.e. the firewall in most cases).

Now reboot the firewall, the EdgeXOS appliance, and the WAN1 router all at the same time. This will clear all ARP cache and should allow the firewall to ping through to the Internet once everything comes back online, make sure to allow for up to 120 seconds after reboot.

You should now be able to access the EdgeXOS appliance through the firewall using the management IP address you assigned to the WAN1 interface.

If you have any problems at this point, repeat these steps and make sure that you have followed the steps correctly. Also, make sure that no other devices are connected to the WAN1 interface and that the ARP cache has been cleared.

Once you are back into the web GUI, continue the configuration by bring up the additional WAN interfaces, one at a time. Once all of the WAN connectivity is up and active you can move forward with setting up traffic shaping rules and any inbound server balancing via Virtual, O2O, or O2M NAT. See our HowToGuides and Platform Notes documentation for details on this configuration.

Post-Firewall Installation Examples

The following network diagrams can be used when placing the EdgeXOS appliance in front of an existing firewall. Typically placing the appliance in front of the firewall is useful when you wish to perform IP-based traffic shaping and/or obtain specific end-user information.

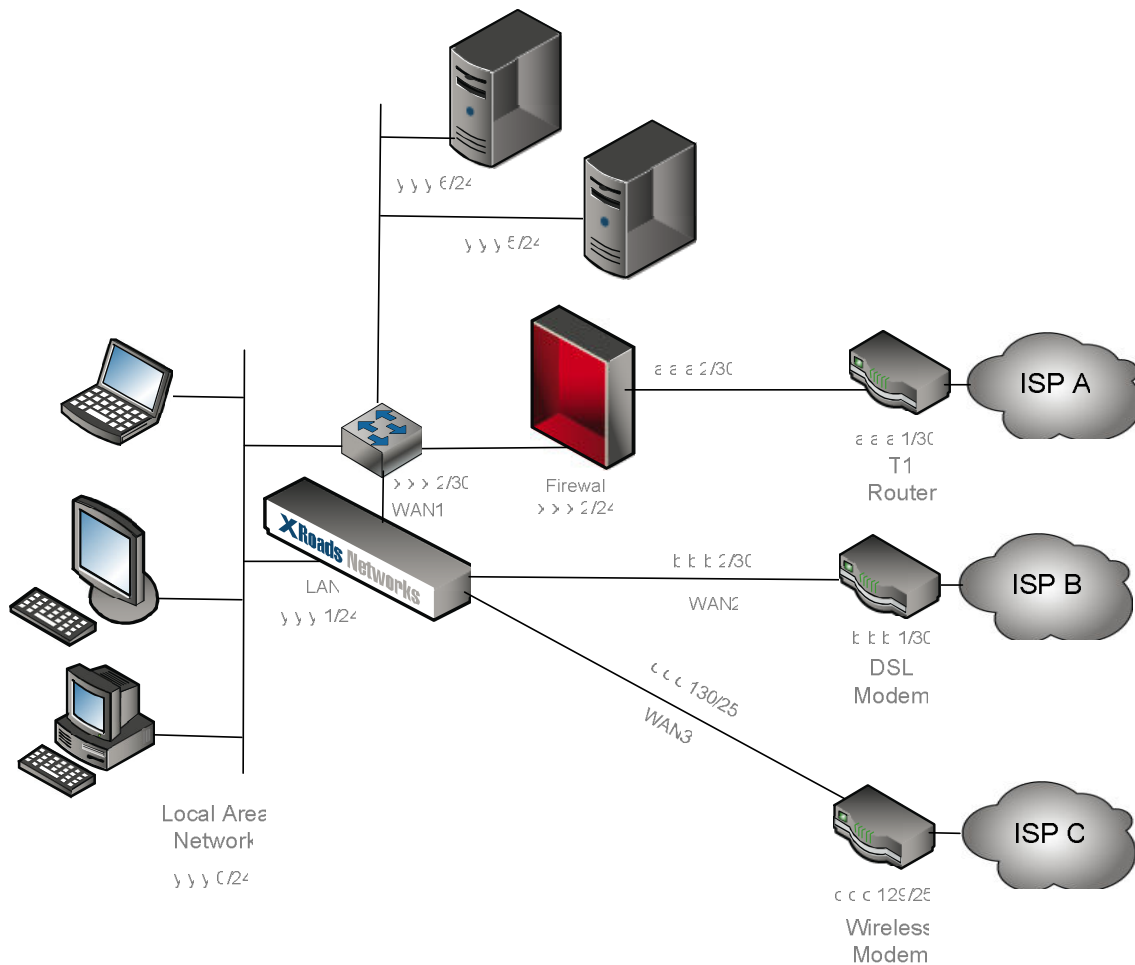
Direct Static Routing (Static Mode)

This method provides the most functionality and is generally the easiest to configure; however it does have some requirements.

Requirements: This method does require several to your existing network architecture, including placing a subnet between the firewall and the EdgeXOS appliance.

Limitations: No feature limitations, however the hardware bypass features can not be fully utilized if there is an appliance failure, however this can be offset by using two appliances in HA (high-availability) mode.

Steps To Install: The first step when configuring this scenario is to setup a new subnet between the EdgeXOS appliance and the existing gateway (typically a firewall). To do this the appliance is placed on the LAN network, both the LAN and WAN ports will need to be connected to the LAN switch.



Prior to connecting the LAN port use this interface to connect a laptop to begin the configuration process using 192.168.168.100/24 on the laptop. The LAN interface of the EdgeXOS will become the new LAN gateway address (typically whatever the firewall was using). The WAN1 interface uses the newly created subnet to communicate with the firewall. Routes are added to the firewall to send all incoming traffic bound for the LAN to the WAN1 interface of the EdgeXOS appliance.

Once the changes are made Apply and Commit the changes. Then change the laptop address to match the LAN network subnet.

Now test connectivity and (very important) SAVE the changes via the Save button on the Home page. Once the configuration has been saved connect the LAN interface directly to the LAN switch.

You should now be able to access the EdgeXOS appliance from any address on the LAN network. If you have any problems at this point, repeat these steps and make sure that you have followed the steps correctly.

Once you are back into the web GUI, continue the configuration by adding inbound server connectivity through the appliance via Virtual, O2O, or O2M NAT Vector Maps for all inbound services, and configure the other WAN interfaces, one at a time to make sure that everything comes up correctly.

Direct Network Address Translation (NAT Mode)

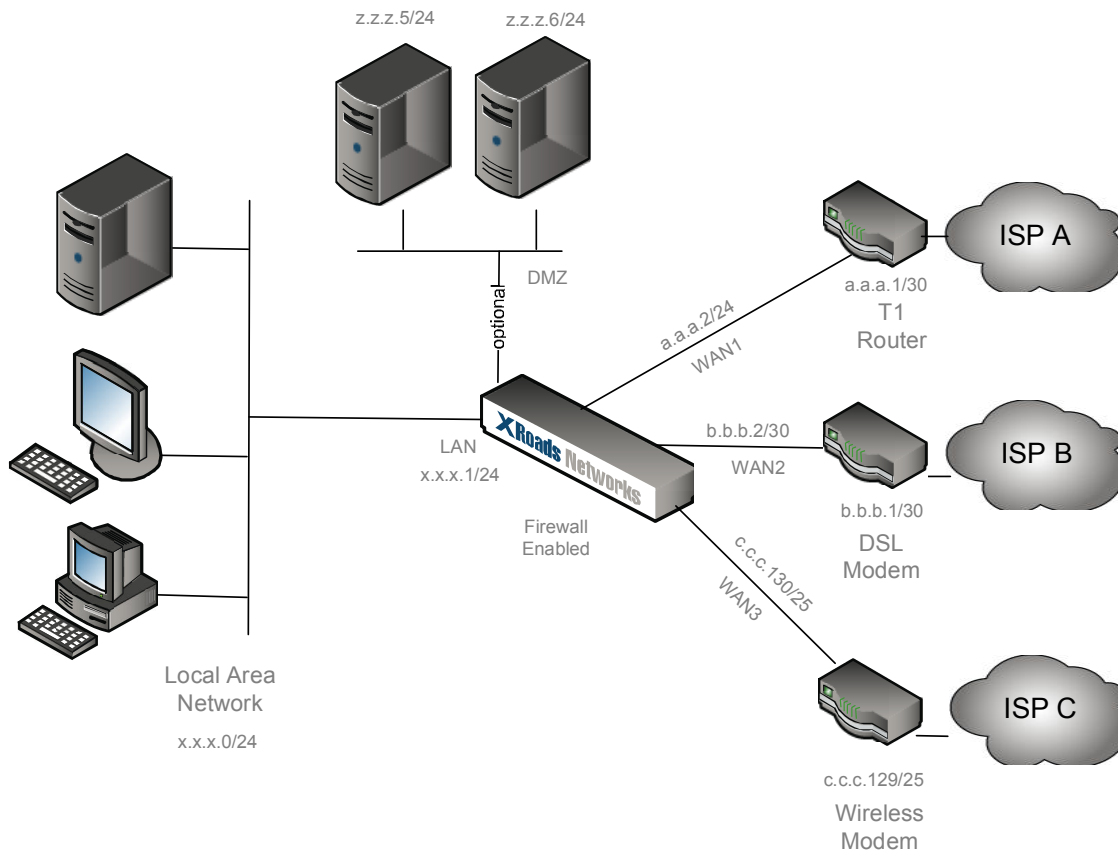
Replacing the firewall simply requires setting the EdgeXOS interfaces to duplicate the old firewall. The firewall rules, NAT rules, etc must also be converted over.

Requirements: This method requires that the administrator converts the existing firewall rules over to the EdgeXOS appliance.

Limitations: No feature limitations, however the hardware bypass features can not be fully utilized if there is an appliance failure, however this can be offset by using two appliances in HA (high-availability) mode.

Steps To Install: The first step when installing this scenario is to obtain the rules from the old firewall including all of the interface information. Once this information has been pulled off the old firewall, replace it with the EdgeXOS appliance. This will create a momentary outage while you are configuring the appliance. The WAN1 interface must be connected to the WAN1 router/modem device.

Once the WAN1 interface is connected, connect the LAN into a laptop to begin the configuration process using 192.168.168.100/24 on the laptop. Configure the WAN1 interface to use NAT mode, use the old firewall address for the WAN1 interface. Configure the old firewalls LAN address (which will become the gateway address for all devices on the LAN side of the appliance). Now Apply and Commit the changes.



Make sure to change the IP address on the laptop to use the same network/subnet as the newly configured LAN interface. Now log back into the appliance via the new IP address (if you have any problems change the laptop back to the old address and make sure that the changes were committed). The WAN1 link will take 10-30 seconds to come up. Now test connectivity and (very important) SAVE the changes via the Save button on the Home page. Once the configuration has been saved connect the LAN interface directly to the LAN device (i.e. the firewall in most cases).

Continue making any changes necessary based on the old firewall, including any NAT rules, and firewall rules.

You should now be able to test connectivity to and through EdgeXOS appliance from anywhere on the LAN side of the appliance. Once you have re-established access to the appliance you can begin configuring the rest of the WAN interfaces, inbound server connectivity, NAT mappings, Vector Maps, etc. See our HowToGuides and Platform Notes documentation for details on this configuration.

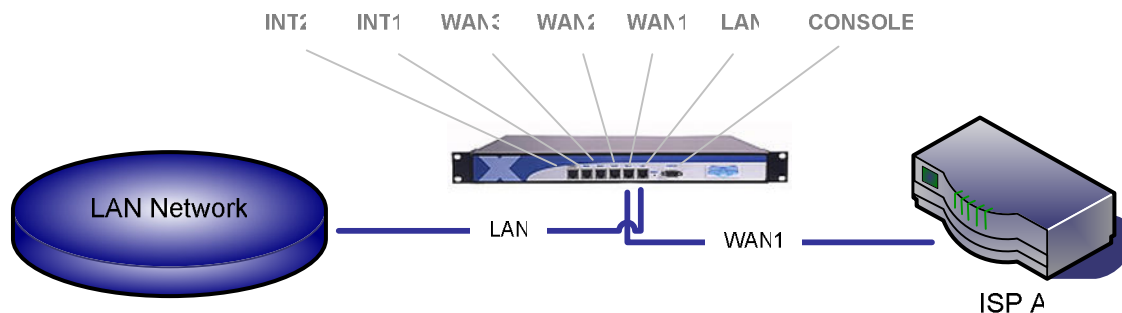
Physically Connecting the EdgeXOS Appliance

By default the EdgeXOS appliance is configurable from either the LAN Ethernet interface or the console port. In order to access the web-based GUI, you must first connect a PC running a web browser to the appliance via an IP network connection.

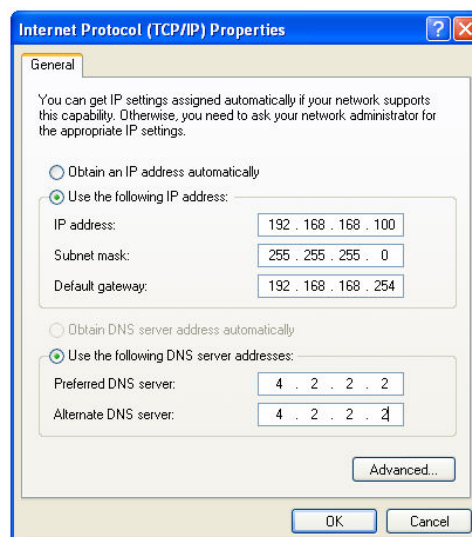
The EdgeXOS uses standard Ethernet ports (either 10/100 or 10/100/1000 depending on the model) and can be connected directly to a PC via a standard crossover cable, or to any standard Ethernet switch or hub.

Use the link lights on the Ethernet interface to verify that you have Layer 1 connectivity. When properly connected the interface should show a **green light**. A flashing yellow or orange light may also appear, this designates that traffic is coming in or going out of the interface.

Interfaces Overview: The LAN (local area network) interface is used to connect the internal network. The WAN (wide-area network) interfaces are used to connect to the external networks or Internet. The INT interfaces can be used as either WAN or DMZ interfaces. When used as DMZ interfaces they do not perform connectivity testing or participate in load balancing, they are simply routed ports. The console port is used for local CLI access.

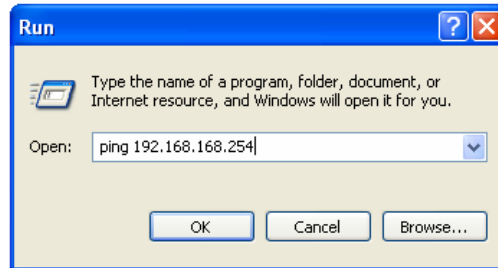


Once you have a green light on the LAN interface, change your computers network settings so that it will reside on the same network as the EdgeXOS appliance, see example:



Administrative Access - Web GUI

When connecting to the EdgeXOS appliance you should first perform a PING operation to make sure that your computer is able to access the appliance over the network. This operation can be conducted on a Windows system via the Start menu. The image below shows how to run this test:



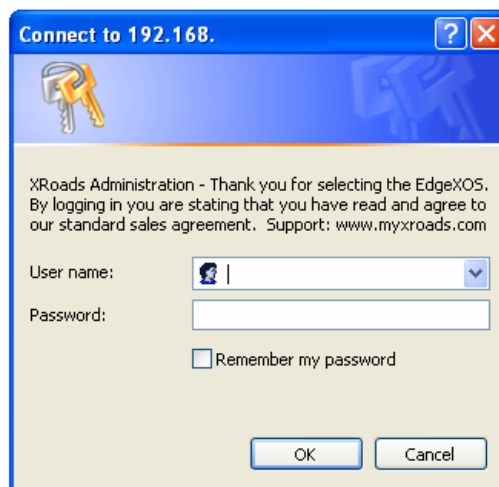
You should get back a reply response from the ping test. If you do not, then your computer is not setup on the correct network, or the appliance is not properly connected to the network.

Once you are able to ping the appliance the next step is to open a web browser and enter the URL **http://192.168.168.254:8088**. This is the default IP address of the LAN interface for the EdgeXOS appliance. The 8088 is the default administrator web port.



You must include the http:// portion any time you use a direct IP address in your URL or the connection will not work.

Next you will be prompted for a login and password. The default login username is '**admin**', the default login password is '**password**'. Enter these in the popup window in order to log in to the appliance. This will grant you access to the Home page of the device



Accessing the CLI

The CLI or command line interface is actually a menu driven system which is accessible via either SSH or through a console port connection and provides access to many common troubleshooting tools like ping and traceroute, the ability to view route and interface information, the ability to add secondary interface IP addresses, and the ability to modify the text configuration file via the command line.

SSH access can be made by connecting to port 2022 via the LAN interface. Access is also available via the WAN interfaces when remote access is enabled. This must be initially configured via the web GUI.

Console access can be obtained via the console port:



By using a terminal application (like HyperTerminal in Windows) you can connect to the console port via a console cable (one is provided with the appliance packaging). The standard settings for the console connection are 9600bps, Data bits 8, Parity none, Stop bits 1, Flow Control Hardware.

Note: Flow Control must be set to 'none' for the smaller Edge2WAN models.

```
XRoads Edge Router (Console Access)
Version 3.5+
xroads login: _
```

Once connected a login prompt will appear, simply enter the current login and password information as you would use for the web GUI. The default login is **'admin'**, the default password is **'password'**.

Terms & Definitions

XRoads Networks provides a host of support services for our end-users, including free and unlimited online web-based support, email and chat support, along with phone and

BPR (Best Path Routing) – This is XRoads Networks next generation, patent pending method for network load balancing and optimizing application routing. More specifically, BPR allows customers to optimize critical routes between two or more offices with full path reporting which show the latency, packet loss, and calculated jitter between each location. Only XRoads Networks has this capability.

Vector Routing – This is the algorithm that is used to determine through which WAN connection network traffic is routed. This algorithm is affected by the utilization of each link, the previous DNS responses, WAN weighting (as determined by the administrator), specific application routing rules, and the current condition of each WAN connection.

ActiveDNS – This is the module responsible for editing and configuring the dynamic DNS system. All adjustments to the inbound (server) connections are handled via this module. This module is required for any inbound DNS based connectivity, redundancy and/or load balancing.

Traffic Shaping – A core feature of the EdgeXOS appliance, intelligent traffic shaping enables a network administrator to rate-limit traffic based on IP address, TCP/UDP port, network subnet, and URL. Bandwidth usage can be designated with a max and min bandwidth setting per policy. Additionally various priorities can be established to create very granular allocation of network bandwidth to specific applications.

Multi-WAN Aggregation & Network Load Balancing – The ability to balance network traffic over multiple connections. Balancing is session based, which means that each network session is balanced across the various active WAN connections. The balancing can be weighted and is adjusted based on utilization and critical path definitions.

Example: When connecting to a web site, multiple sessions are opened to download the text, and images of the site. Each session is balanced over the active WAN connections, thus decreasing the wait time for a site to be downloaded.

Multi-Level Outage Detection – This is the process in which we determine whether a WAN connection is up or down. Our patent pending method includes two phases, first we ping the gateway and the remote probe address (or the remote side of the WAN connection), then we further probe various core routers and core websites on the Internet to determine if an outage has occurred.

Inbound vs Outbound Load Balancing – Outbound load balancing is when LAN traffic is balanced across the various WAN connections. Inbound load balancing is when inbound server based connections are balanced via the ActiveDNS module. Each time an inbound request is made, the ActiveDNS module determines which WAN interface address to provide based on the current usage, and administrative preferences.

Site2Site Auto-Failover – There are many appliances on the market that provide secure virtual private networks (VPN) capabilities. A VPN is generally used to connect two or more locations via a secure tunnel so that the data passing between the two or more connections is highly secure. The problem with normal VPN appliances is that they are incapable of automatically failing over to a secondary VPN tunnel and WAN interface in the event that the primary VPN fails.

Virtual Technician – This trademarked feature provides the ability to actively and automatically troubleshoot a network failure. When a failure is detected by the WAN testing module, the Virtual Technician begins a series of tests in an attempt to determine the cause of the problem in order to assist with its resolution. Only XRoads Networks has this capability.

VirtualNAT – This is the XRoads Networks name for a Virtual Server (when a device proxies connections for another device). VirtualNAT is essentially a TCP proxy for LAN based servers and makes setting up inbound services a snap. The limitations of VirtualNAT are that all logging will appear to come from the Edge appliance.

Vector Mapping – The process by which the Edge appliance ensures that inbound and outbound traffic flows are bonded to the correct WAN connection. If an inbound connection, destined for a server, does not go out the WAN interface which it came in on, the session could be dropped by either the ISP routers or firewall.

One-To-One vs. One-To-Many NAT – Network Address Translation (NAT) is designed to essentially translate an address on the WAN to an address on the LAN. For example NAT is commonly used to translate private space on the LAN to public space on the WAN.

These two specific forms of NAT are designed to allow inbound connections, destined for a WAN address, to be forwarded to internal LAN addresses. One-To-One is designed to translate all the ports of a WAN address to all of the ports of a LAN address, where One-To-Many only translates a single port on a WAN address to a single port on a LAN address.

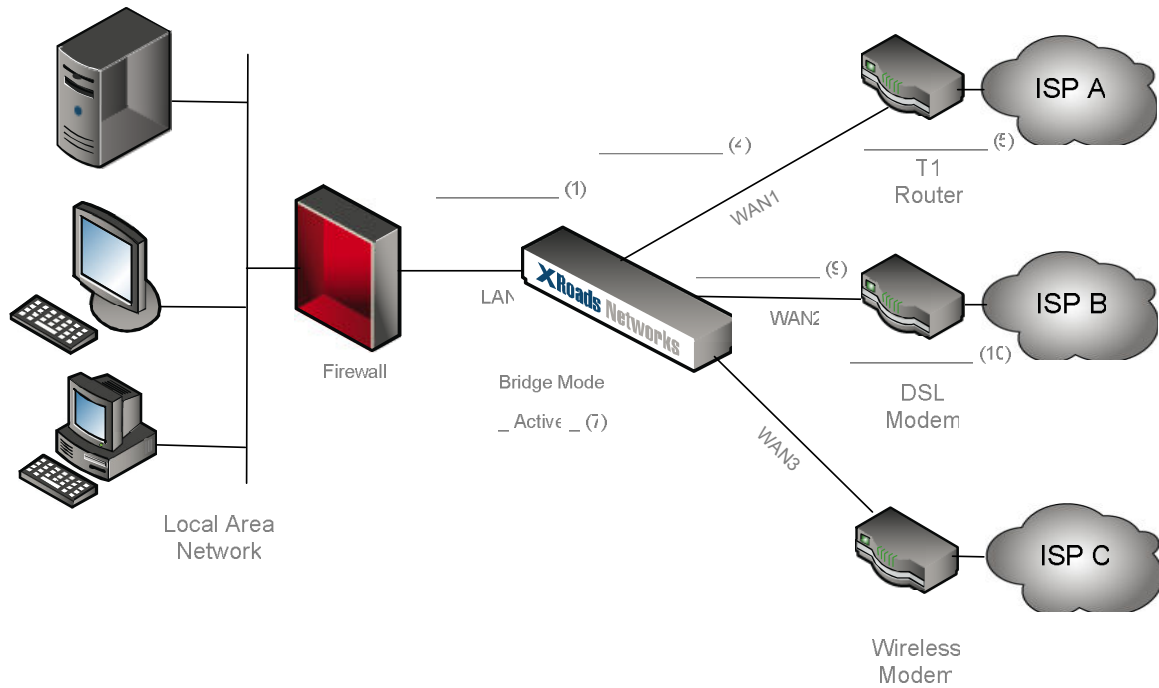
Notes

This page left blank for configuration notes, etc.

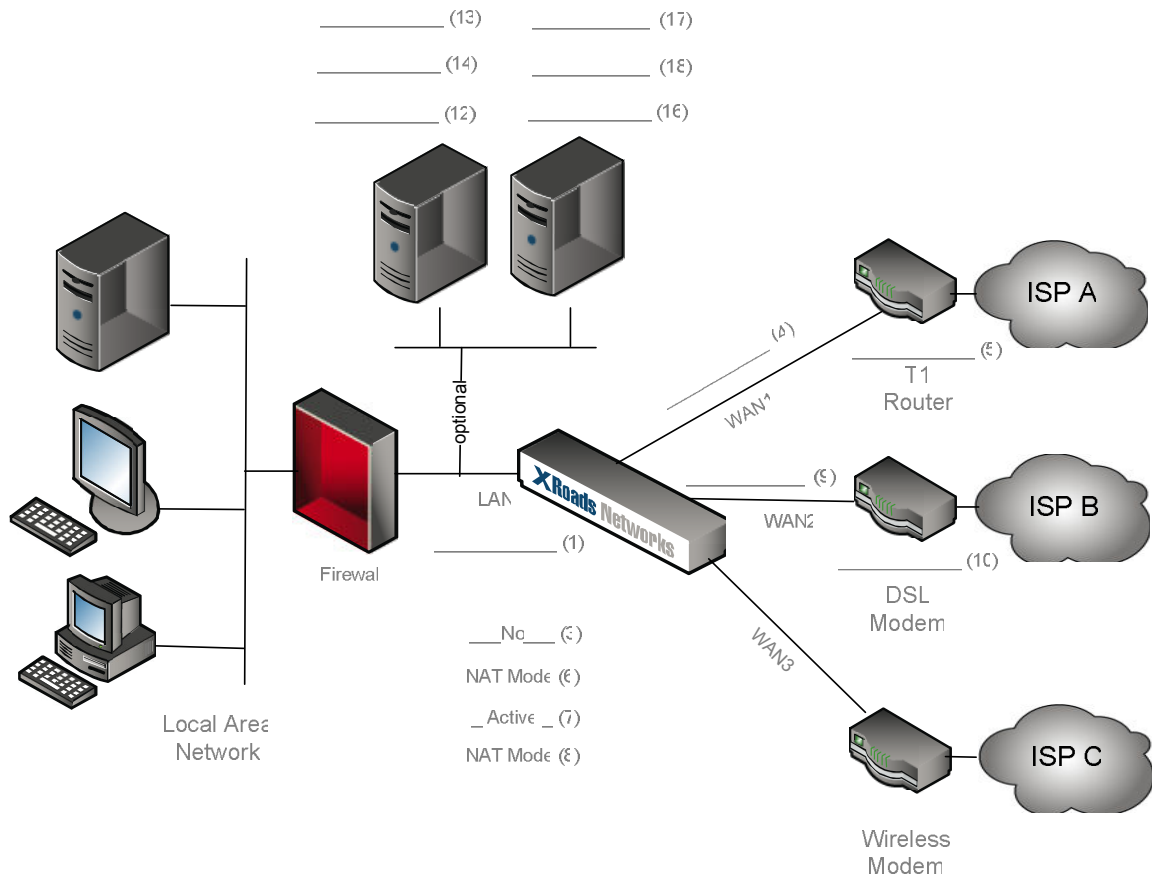
Configurator Worksheets

These worksheets were developed to assist you in determining what information you will need to enter in to the Live Configurator via the MYXROADS support site. Use these worksheets to determine what information belongs in which fields. Feel free to contact support via www.myxroads.com to answer any questions regarding these worksheets.

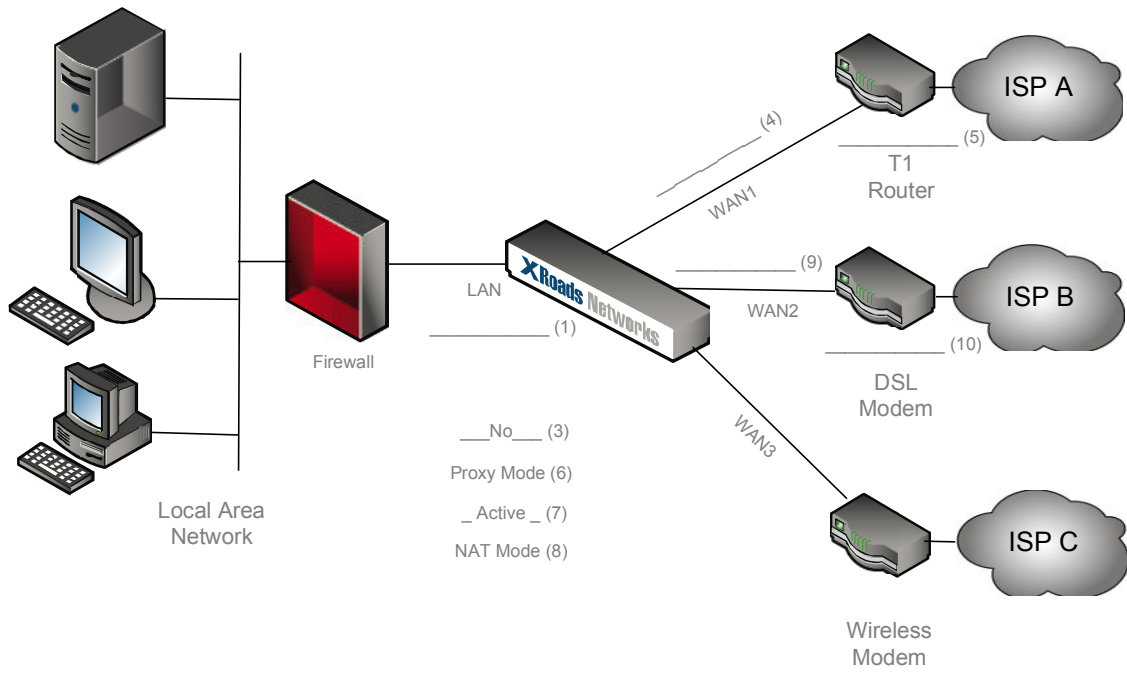
WORKSHEET: Transparent Bridge Connectivity (Bridge Mode)



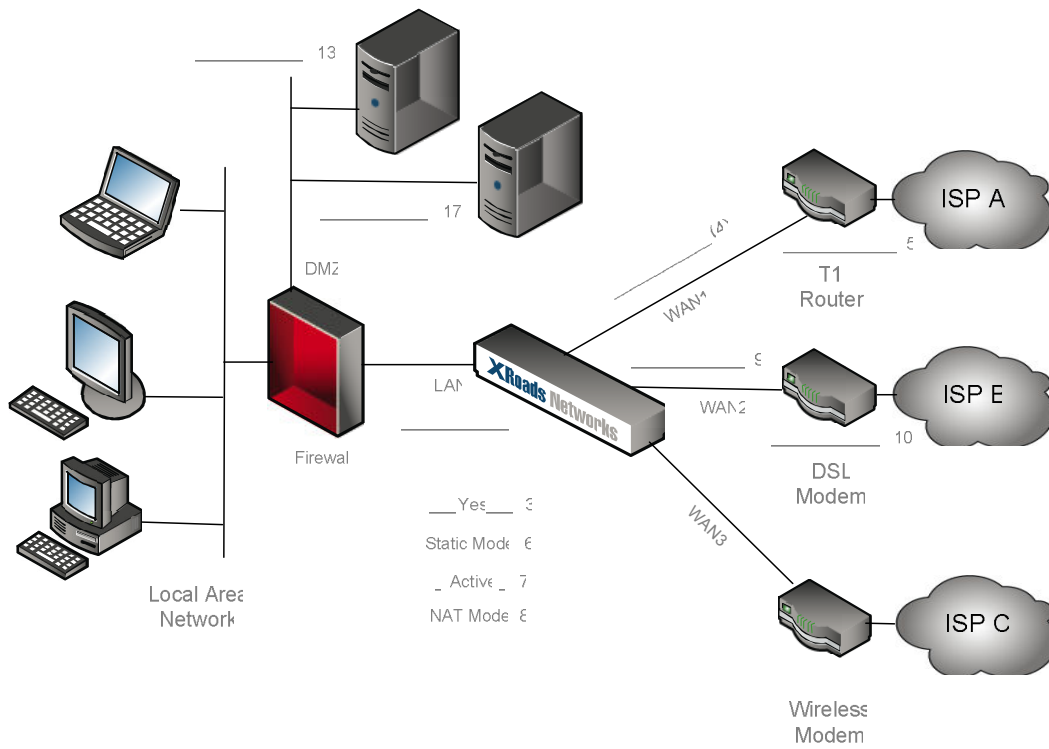
WORKSHEET: Direct Network Address Translation (NAT Mode)



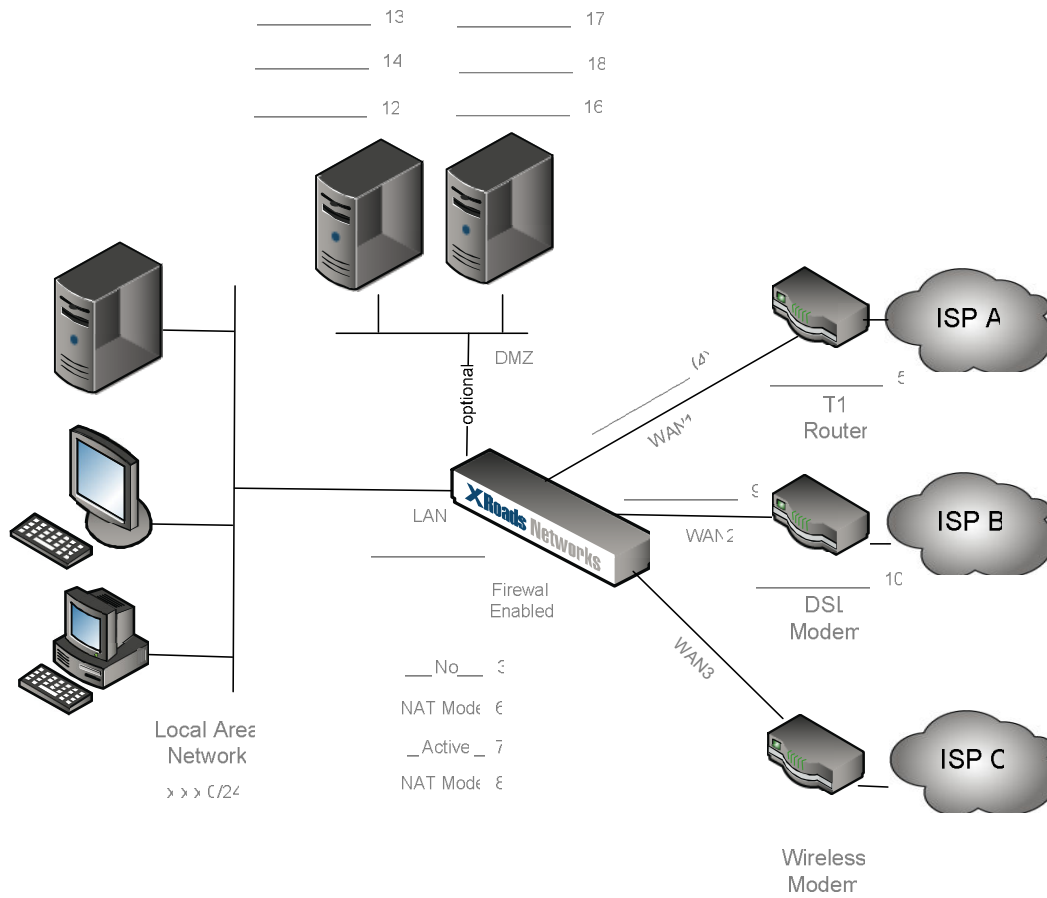
WORKSHEET: Pass-Through w/Proxy (Proxy Mode)



WORKSHEET: Direct Static Routing (Static Mode)



WORKSHEET: Direct Network Address Translation (NAT Mode)



Inbound Server Balancing

Please use this form to configure inbound service rules. This worksheet is to be used to determine what information belongs in which fields within the Live Configurator. Feel free to contact support via www.myxroads.com to answer any questions regarding these worksheets.

