

How To Guide

XRoads Networks

Best Practices: Direct Network Address Translation
(NAT Mode)

EdgeXOS Deployment Scenario: Standard NAT

This document is designed to provide an example as to how the EdgeXOS appliance is configured based on a predefined scenario. The scenario is typical of many customers and is outlined below. If you have any questions about this document or how this scenario might differ from your actual deployment, please feel free to contact our support center.

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

Additional documentation is available on our website via our Support link, select the Documentation option. We also have a number of how-to videos online here:

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

Scenario Details:

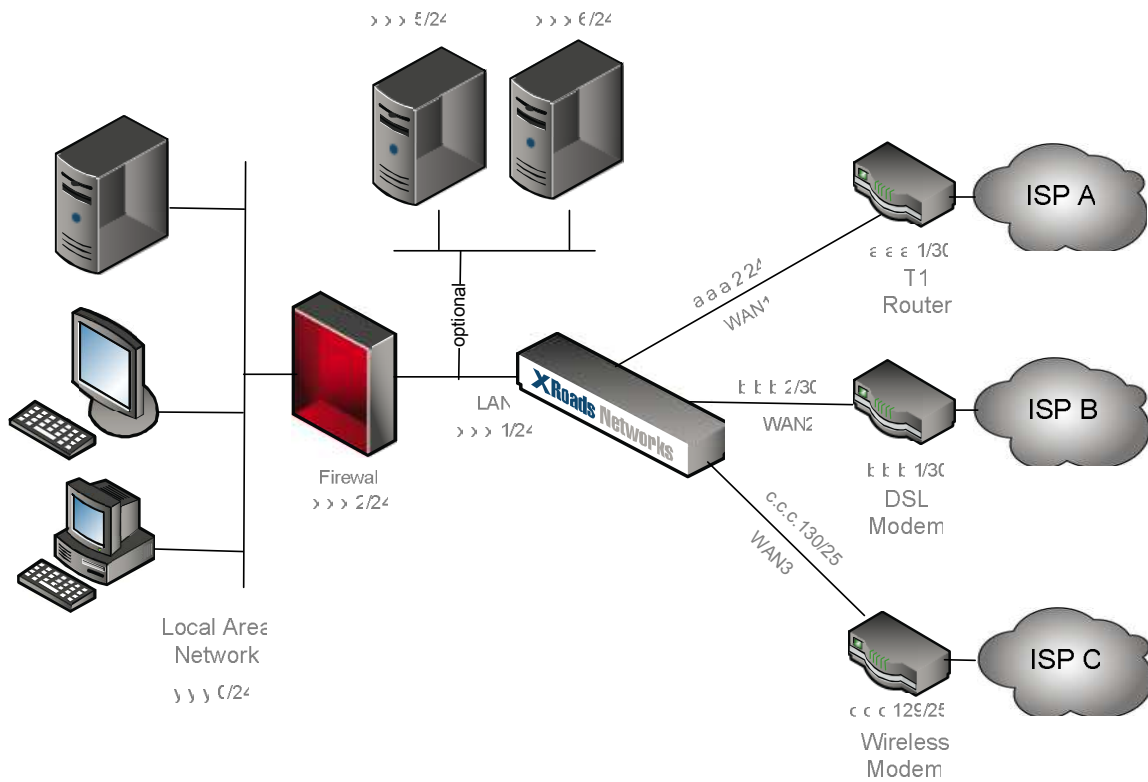
The following outline provides some predefined requirements for this scenario. Most of these requirements are taken from previous customer installs and real-world deployments.

- Must be able to load balance outbound end-user traffic across all three WAN links and provide automated failover in the event of an outage on any of the links.
- Must be able to assign a preference to WAN1 for most outbound traffic as it is a faster link than WAN2 or WAN3.
- Must be able to load balancing incoming web traffic to a dedicated onsite web server.
- Must be able to pass-through IPSec VPN tunnel to gateway firewall appliance.
- Must be able to pass-through inbound SMTP email connection to internal mail server and failover in the event of an outage on the primary WAN link.
- Must be able to maintain session persistence for critical CRM application.
- Must be able to offload non-critical web traffic over our WAN2 link.
- The customer has 120 end-users sitting behind an existing firewall.
- The customer has an existing Class C publicly routed network from WAN1.
- The customer has two additional links which each have 5 static addresses.

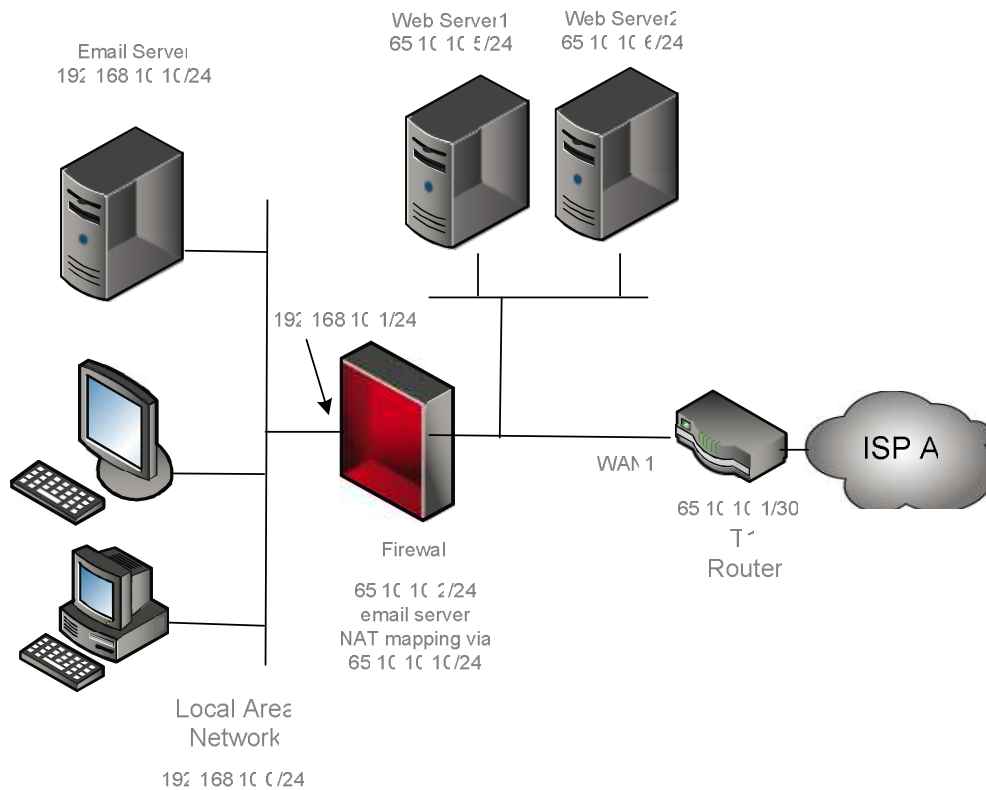
Deployment Method Selection

By utilizing the QuickStart Guide the method selected for this deployment is the Direct Network Address Translation (NAT Mode), which is the primary recommended method for installation as it provides the most flexibility and capabilities.

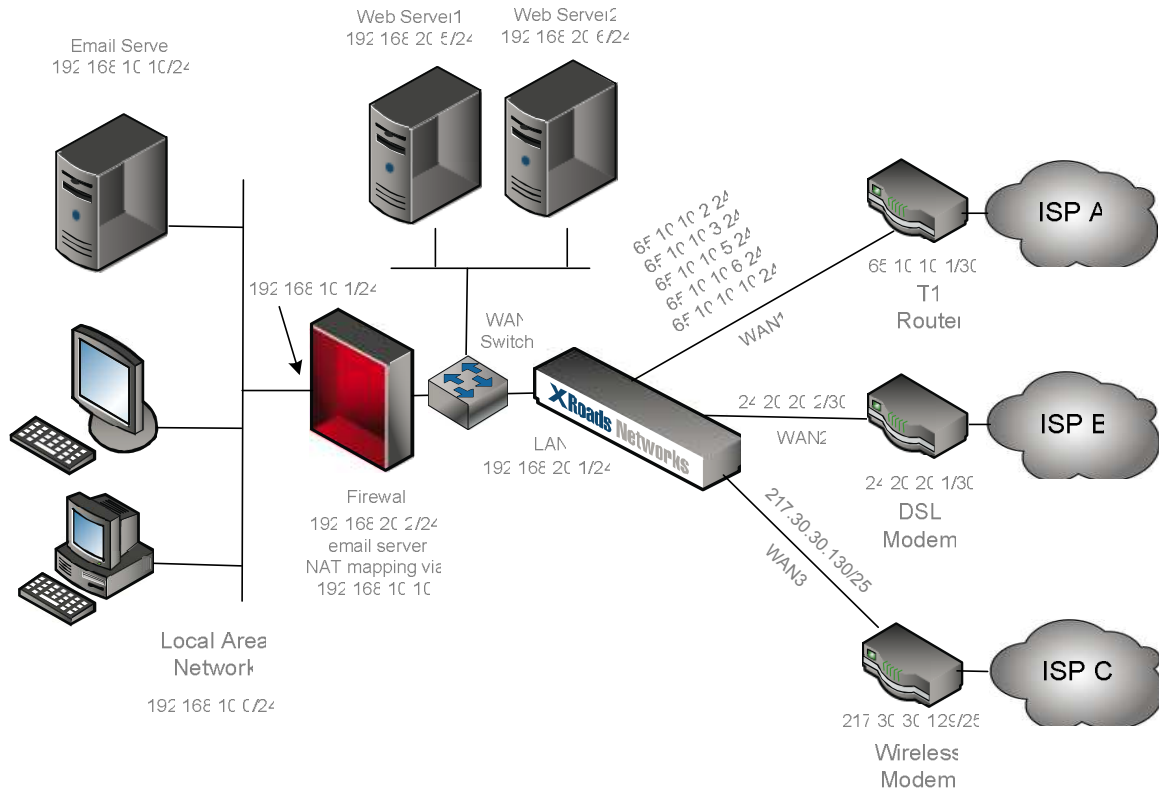
This is the default diagram provided by the QuickStart Guide:



This diagram show the configuration BEFORE the EdgeXOS appliance is put in place:



Here is the diagram based on our requirements AFTER the EdgeXOS appliance is in place:



Steps To Configure

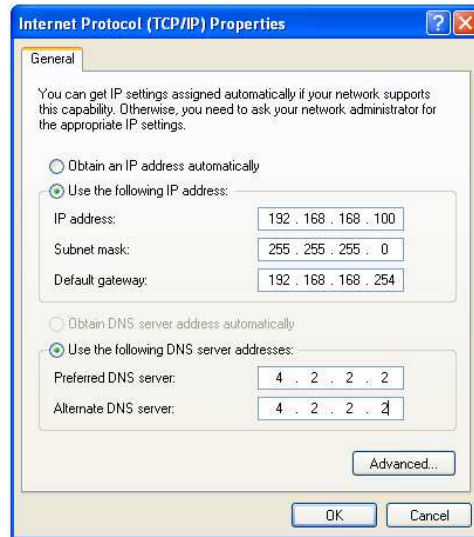
(This is a step-by-step implementation guide for the scenario detailed above)

The first step when installing the appliance once the method has been determined is to gain access to the web configuration interface. Given that you have already attempted to access the unit and gotten used to the web-GUI while the unit was offline, this document will show the actual installation procedure.

NOTE: It is also assumed that these steps will be taken during a schedule maintenance period or during a time when a short outage period has been approved.

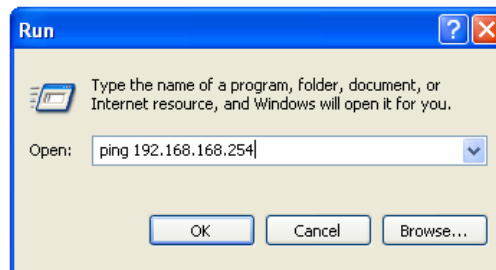
Step 1) Physically place the EdgeXOS appliance between the firewall and the WAN1 router. Connect the WAN1 Ethernet cable from the WAN1 router to the WAN1 interface of the appliance (note this may require a cross-over cable). Plug in the appliance and turn it on, the appliance takes approx 60 seconds to boot.

Step 2) Use a laptop or a PC to connect to the LAN interface of the appliance. Make sure to configure the laptop/PC's IP address to something in the 192.168.168.x/24 range. The screen shot below shows the settings we generally recommend.



Connect to the LAN interface from the NIC of the laptop/PC (note a cross-over cable may be required to do this). Make sure that you see a green light on the EdgeXOS appliance's LAN interface when it is plugged in. If a green light does not appear the cable may not be working correctly or the interface on the laptop/PC may not be enabled.

Step 3) Once connected 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



Step 4) Now that you have logged in to the appliance you should see the Home page. The first task is to configure the LAN and WAN interfaces. Click on the Interfaces tab and enter the LAN address information.



The LAN address is 192.168.20.1, the subnet is 255.255.255.0 (see diagram).

The DNS information is set to 4.2.2.2 and 4.2.2.2 (this can be changed to whatever DNS servers are provided by your ISPs).

The set the rate limit, which in this case is 10000, equal to a 10Mb connection.

Finally click the Apply button at the bottom of the page.

LAN Configuration: (MAC Address:)
192 . 168 . 20 . 1 (Interface IP Address)
255.255.255.0 (LAN Subnet Mask)

Link Rate: 10000 (kbit = thousands of bits per second, example: 1Mbps = 1000)
NOTE: Unless set to zero this will override the inbound rate settings.

External DNS Resolvers:
4 . 2 . 2 . 2 (WAN One ISP DNS Server)
4 . 2 . 2 . 2 (WAN Two ISP DNS Server)

Step 5) The next step is to configure the WAN1 interface. Select the 'WAN Interface One' menu option. Then enter the following information.

Set the Interface to 'Active', 'NAT', 'Static' with proxy mode disabled.

The WAN1 address is 65.10.10.3, the subnet is 255.255.255.0 (see diagram).

The WAN1 gateway is 65.10.10.1 (see diagram).

Leave the probe address blank as it will automatically fill in once the link is turned up.

The set the rate limit, which in this case is 1544, equal to a T1 connection.

Finally click the Apply button at the bottom of the page.

Interface Mode: ?

Active Inactive Select 'Active' to load balance or 'Inactive' to shutdown.

NAT Routed/Proxy DMZ

Static Dynamic Dynamic addresses require a DHCP server on the WAN network.

Proxy Disabled Proxy Enabled Enabling will make the LAN and WAN1 addresses the same.

Three Times Daily (Automatic Proxy Outage Checking) **Force Save**

65 . 10 . 10 . 3 (Interface IP Address)

255.255.255.0 (Subnet Mask)

65 . 10 . 10 . 1 (Interface Gateway IP Address)

WAN Testing: ?

Probe Address - will automatically populate if left blank

Link Rates: ?

10000 Outbound 10000 Inbound (kbit = thousands of bits per second; 1Mbps = 1000)

Weight: ?

80 (Ratio Of Link Utilization)

Step 6) The next step is to configure the WAN2 interface. Select the 'WAN Interface Two' menu option. Then enter the following information.

Set the Interface to 'Active', 'NAT', 'Static'.

The WAN2 address is 24.20.20.2, the subnet is 255.255.255.252 (see diagram).

The WAN2 gateway is 24.20.20.1 (see diagram).

Leave the probe address blank as it will automatically fill in once the link is turned up.

The set the rate limit, which in this case is 3000, equal to a 3Mb connection.

Finally click the Apply button at the bottom of the page.

Active Inactive Standby Select 'Active' to load balance or 'Standby' for failover mode.

NAT DMZ

Static Dynamic Do not enter WAN addresses if enabled.

Monthly Lease Request a DHCP lease time if available. (Interface IP Address)

(Subnet Mask)

(Interface Gateway IP Address)

(Probe Address - will automatically populate if left blank)

Link Rates: Outbound Inbound (kbit = thousands of bits per second; 1Mbps = 1000)

Weight: (Ratio Of Link Utilization)

Step 7) The next step is to configure the WAN3 interface. Select the 'WAN Interface Three' menu option. Then enter the following information.

Set the Interface to 'Active', 'NAT', 'Static'.

The WAN3 address is 217.30.30.130, the subnet is 255.255.255.128 (see diagram).

The WAN3 gateway is 217.30.30.129 (see diagram).

Leave the probe address blank as it will automatically fill in once the link is turned up.

The set the rate limit, which in this case is 768, equal to a 768K connection.

Finally click the Apply button at the bottom of the page.

Active Inactive Standby Select 'Active' to load balance or 'Standby' for failover mode.

NAT DMZ

Static Dynamic Do not enter WAN addresses if enabled.

Monthly Lease Request a DHCP lease time if available. (Interface IP Address)

(Subnet Mask)

(Interface IP Address)

(Interface Gateway IP Address)

(Probe Address - will automatically populate if left blank)

Link Rates: Outbound Inbound (kbit = thousands of bits per second; 1Mbps = 1000)

Weight: (Ratio Of Link Utilization)

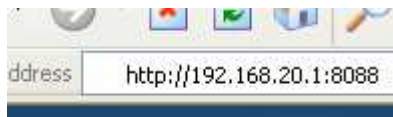
Step 8) The next step is to Commit all of the applied interface information. This is done by clicking the Commit button and the Commit To Interfaces button.

Once committed the interfaces on the EdgeXOS appliance will automatically be updated with the LAN and WAN interfaces changing to the new state.

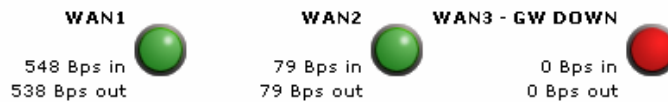
NOTE: At this point you will lose access to the web-GUI.

You now need to change the IP address of the laptop to be equal to the new subnet. In this case the laptop/PC needs to be changed to something like 192.168.20.100 with a 255.255.255.0 subnet and a gateway of 192.168.20.1.

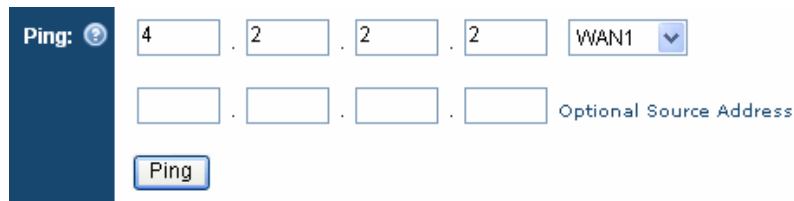
Once the address has been changes you should be able to reconnect using the new URL:



Step 9) Once you have confirmed that you are able to reconnect, take a look at the interface status on the Home page. It may take up to 30 seconds for the WAN links to become active. You may see that some interfaces are active but not all. It may take up to a minute or two for all of the interfaces to initially become active.



Once the links are all active attempt to perform a ping from the appliance out to the Internet via the Tools tab, under the Ping menu.

A screenshot of the 'Ping' configuration interface. It features a 'Ping:' label with a help icon, followed by four input fields containing the numbers '4', '2', '2', and '2'. To the right is a dropdown menu set to 'WAN1'. Below these is another set of four empty input fields labeled 'Optional Source Address'. At the bottom is a 'Ping' button.

You should get a positive result.

Host is ALIVE!
rtt min/avg/max/mdev = 15.173/18.057/20.942/2.887 ms

If this is the case, the next step is to perform a test from your laptop/PC. Assuming that you correctly configured the gateway on the laptop/PC.

```
Pinging 4.2.2.2 with 32 bytes of data:
Reply from 4.2.2.2: bytes=32 time=11ms TTL=53
Reply from 4.2.2.2: bytes=32 time=11ms TTL=53
Reply from 4.2.2.2: bytes=32 time=17ms TTL=53
Reply from 4.2.2.2: bytes=32 time=9ms TTL=53

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 17ms, Average = 12ms
```

You should also get a positive response.

Step 10) The next step is to make the required changes to the rest of the external network.

- a) Change the firewall's external WAN address to 192.168.20.2/24 with its gateway pointing to 192.168.20.1.
- b) Change the email servers NAT mapping on the firewall to use 192.168.20.10.
- c) Change the two web servers to use 192.168.20.5 and 192.168.20.6 with their default gateway pointing to 192.168.20.1.

Step 11) Once these changes have been made to the local network, the next step is to plug the EdgeXOS appliance into the WAN switch. Once connected the firewall and all of the ends behind the firewall should be able to access the Internet without any problems.

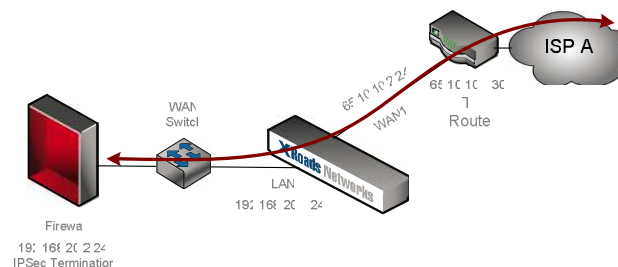
Test to make sure that the firewall and all end-users have access out to the Internet.

Next test to make sure that both servers connected to the WAN switch are able to access the Internet.

Step 12) With outbound access confirmed, it is time to configure inbound connectivity. There are three items which need to be configured.

- a) Inbound IPSec connection to the firewall via 65.10.10.2.
- b) Inbound email server connectivity via 65.10.10.10 port 25.
- c) Inbound web server access via 65.10.10.5 and 65.10.10.6.

A. We begin with setting up the inbound rule for the IPSec connection to the firewall. This is setup by using a One-to-One NAT rule with a Vector Map automatically created. This diagram shows what is being configured.



To enable this functionality we simply create a one-to-one NAT rule by going to the NetBalancing tab and selecting the One-To-One NAT menu.

We enter a name for this rule 'IPSec_Rule', select to create a reverse Vector Map (which is required to ensure bi-directional connectivity) and enter the external address 65.10.10.2 and the internal (internal to the EdgeXOS appliance) of 192.168.20.2. We also select the WAN1 interface which is the interface which the IPSec tunnel is coming in on.

IPSec_Rule (Must be different from One-To-Many)

(Check this to forced source NATing when the selected interface is in BACKUP mode)

(Check this to automatically create a reverse Vector Map)

External Address: 65 . 10 . 10 . 2 (Must be available via the WAN port selected below)

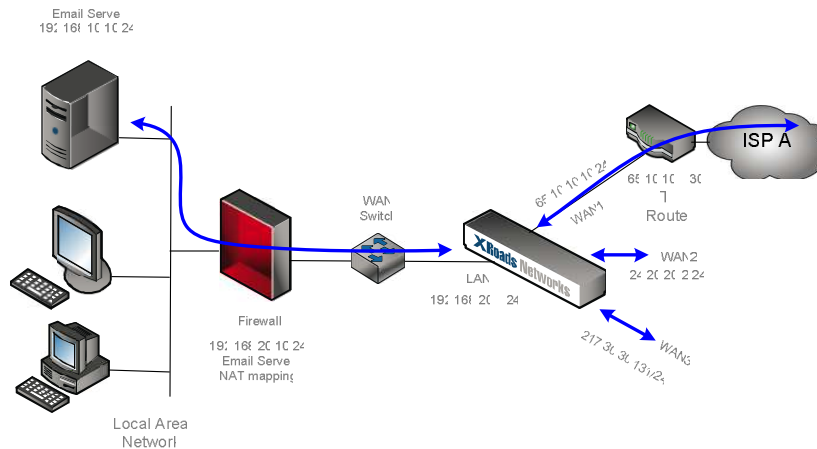
Inbound Interface: WAN1

Internal Address: 192.168.20.2 (Forward Address(es) Must be available via the LAN interface)

(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)

Apply Order: 1

- B. To enable this functionality we create a VirtualNAT rule using IP address 65.10.10.10, 24.20.20.2, and 217.30.30.131. This diagram shows what is being configured.



Using this method we are able to provide both load balancing and failover for the email server automatically. To enable this functionality we use a single VirtualNAT rule and use each of the above defined addresses.

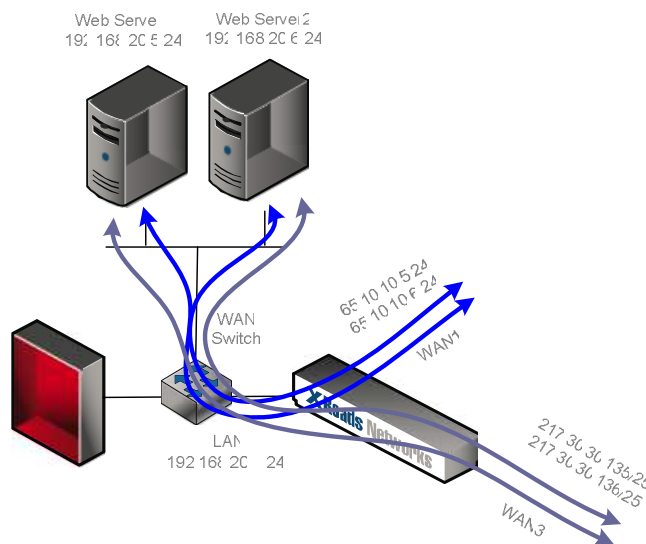
Create a VirtualNAT rule by going to the NetBalancing tab, then select the VirtualNAT menu. We enter a name for this rule 'Email_Server', select the service which will be VNAT'd, then enter the internal address (the address which is internal from the EdgeXOS point of view), then enter each of the external or WAN addresses which will be forwarded to the internal address.

Server Name: ?	<input type="text" value="Email_Server"/>
Server Service: ?	<input type="button" value="Mail Server (SMTP/POP3/IMAP)"/> ▼
	<input type="button" value="Create Server Service"/> (Create A New VirtualNAT Service)
Internal Address: ?	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="20"/> . <input type="text" value="10"/> (Internal Server Address)
WAN1 Address: ?	<input type="text" value="65"/> . <input type="text" value="10"/> . <input type="text" value="10"/> . <input type="text" value="10"/> (External Server Address for WAN1)
WAN2 Address: ?	<input type="text" value="24"/> . <input type="text" value="20"/> . <input type="text" value="20"/> . <input type="text" value="2"/> (External Server Address for WAN2)
WAN3 Address: ?	<input type="text" value="217"/> . <input type="text" value="30"/> . <input type="text" value="30"/> . <input type="text" value="131"/> (Forward Address - Must be available via an Edge interface)

You must now update your DNS information and add a secondary MX record for the WAN2 and WAN3 connections. The MX records should be set to 10, 20, and 30. The details of how to modify DNS records is beyond the scope of this document.

If you wish to utilize the EdgeXOS appliance to handle your MX records then you will need to delegate the MX records and utilize the ActiveDNS model. For details on delegation and ActiveDNS, please reference the HowToGuide for ActiveDNS and the Platform Notes on Delegation.

- C. Finally we will configure inbound link and server load balancing for two servers. Unlike server load balancers which can only balance traffic based on the server, the EdgeXOS appliance is able to perform both server and link balancing at the same time. This diagram shows what is being configured.



Using this method we are able to provide both load balancing and failover for the email server automatically. To enable this functionality we use two O2O NAT rules and ActiveDNS to perform the URL balancing.

The process used to create the four one-to-one NAT mappings is similar to section A, however in this case we specify multiple internal servers.

We enter a name for this rule 'Web_Server1', etc., select to create a reverse Vector Map (which is required to ensure bi-directional connectivity) and enter the external address and the internal (internal to the EdgeXOS appliance) addresses. We also select the WAN interface which the traffic is coming in on.

First Rule:

Service Name: ?	Web_Server1 (Must be different from One-To-Many)
	<input type="checkbox"/> (Check this to forced source NATing when the selected interface is in BACKUP mode)
	<input checked="" type="checkbox"/> (Check this to automatically create a reverse Vector Map)
External Address: ?	65 . 10 . 10 . 5 (Must be available via the WAN port selected below)
Inbound Interface: ?	WAN1
Internal Address: ?	192.168.20.5, 192.168.20.6 (Forward Address(es) Must be available via the LAN interface)
	(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)
Apply Order: ?	1

Second Rule:

Service Name: ?	Web_Server2 (Must be different from One-To-Many)
	<input type="checkbox"/> (Check this to forced source NATing when the selected interface is in BACKUP mode)
	<input checked="" type="checkbox"/> (Check this to automatically create a reverse Vector Map)
External Address: ?	65 . 10 . 10 . 6 (Must be available via the WAN port selected below)
Inbound Interface: ?	WAN1
Internal Address: ?	192.168.20.6, 192.168.20.5 (Forward Address(es) Must be available via the LAN interface)
	(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)
Apply Order: ?	1

Third Rule:

Service Name: ?	Web_Server3 (Must be different from One-To-Many)
	<input type="checkbox"/> (Check this to forced source NATing when the selected interface is in BACKUP mode)
	<input checked="" type="checkbox"/> (Check this to automatically create a reverse Vector Map)
External Address: ?	217 . 30 . 30 . 5 (Must be available via the WAN port selected below)
Inbound Interface: ?	WAN3
Internal Address: ?	192.168.20.5, 192.168.20.6 (Forward Address(es) Must be available via the LAN interface)
	(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)
Apply Order: ?	1

Forth Rule:

Service Name: ⓘ	Web_Server5 (Must be different from One-To-Many)
	<input type="checkbox"/> (Check this to forced source NATing when the selected interface is in BACKUP mode)
	<input checked="" type="checkbox"/> (Check this to automatically create a reverse Vector Map)
External Address: ⓘ	217 . 30 . 30 . 6 (Must be available via the WAN port selected below)
Inbound Interface: ⓘ	WAN3
Internal Address: ⓘ	192.168.20.6, 192.168.20.5 (Forward Address(es) Must be available via the LAN interface)
	(Server load balancing can be accomplished by entering the following xxx.xxx.xxx.yyy-xxx.xxx.xxx.zzz)
Apply Order: ⓘ	1

These four rules create a fully load balanced solution for inbound web connectivity. To complete this configuration, you must also configure ActiveDNS and delegate the web server URL to the EdgeXOS appliance.

Step 13) With inbound connectivity setup, you must now make sure that DNS works correctly. Since the IPSec tunnel uses a direct IP address, nothing needs to be done there. As we are simply adding to MX records to the existing zone record for inbound email redundancy, ActiveDNS is not required in that case either. However in the case of the web server load balancing, we do need to delegate the web servers DNS records to the EdgeXOS appliance and setup ActiveDNS for those records.

To understand how to setup delegation, please review the Platform Notes on Delegation. This must be done on your existing DNS server before DNS requests will be forwarded to the EdgeXOS.

Next we'll go through configuring the ActiveDNS service for load balancing the web server connections.

To configure the DNS services on the EdgeXOS appliance first go to the NetBalancing tab and select the ActiveDNS menu option. From there select the 'Domain Settings' option and create a new domain record. Since we are using delegation, the domain will be the full URL name, instead of simply the domain name.

Authoritative Domains: ⓘ	www.abc.com (Enter A Domain Name, Example: abc.com)
	NOTE: The root servers must be redirected to the Edge router in order to enable the DNS functionality.
Domain Parameters: ⓘ	30 (TTL - The number of seconds that this zone may be cached, '0' means no cache)
	30 (Refresh - The number of seconds after which nameservers should check to see if this zone has changed)
	1 (Serial - The incremental number assigned to this zone, used for zone transfers)
	86400 (Expire - If the Edge cannot be reached, all information is invalidated after 'expire' seconds)

As you can see in the example above, we create the fully qualified domain name, i.e. 'www.abc.com'. Once the domain is created we create the individual host records in order to direct the inbound connections. When new DNS requests are made, they are forwarded to the EdgeXOS appliance via delegation and then the EdgeXOS appliance will respond based on the load balancing algorithm and the status of each WAN link.

This screen shot demonstrates how a record can be created for this web service.

Authoritative Domain: (Domain name associated with the host)

Host Name: (Enter host name [example: www] and bound to an interface)

Host Address / URL: (Enter an ip address or a cname, TXT, or SRV record, see '?' help for more)
OR Click for dynamic WAN addressing

Internal Address: (Enter the LAN IP address for this record, 'A' records only)

Record Type: (Host Type)

Time-To-Live: (TTL determines how long this record is cached by DNS clients)

Load Balancing: (Used for load balancing server records, lower numbers are provided first more often [1 - 9999])
 Disabled Enabled (Enables SMART Load Balancing for this DNS entry, only enable for 'A' records)

(Host Status)

The Host Name and Internal Address are left blank when adding a delegation record.

We will add a record for each IP address for which we created a one-to-one NAT rule.

The following shows what the final listing of DNS records looks like.

Host Name	Type	Address	L.B.	Interface
.www.abc.com.	A	65.10.10.5	1	wan1
.www.abc.com.	A	65.10.10.6	100	wan1
.www.abc.com.	A	217.30.30.135	200	wan3
.www.abc.com.	A	217.30.30.136	300	wan3

You can see that we have added weights to each of the DNS rules, with 217.30.30.136 being the least likely address to be provided and 65.10.10.5 being the most likely address to be provided. As the administrator you are free to make any IP address more or less preferred based on your own requirements.

Step 14) Enforcing session persistence is important for anyone using web-based CRM systems. To that end in this scenario the customer is using a CRM system which requires a single sign-on multi-server connection.

In order to this to consistently work we add a Best Path Routing rule for the remote site. We might also want to add a BPR rule for critical FTP sites as well in order to ensure large file downloads utilize the same connection over long periods of time.

The process for setting up a BRP rule is simple, first enter the name of the rule, then enter the URL used when accessing the CRM portal (this is only an example, not real-world), then enter a high threshold level for latency, packet loss, and jitter.

Finally select the default interface to be used for outbound connections, and finally select the method to be used when performing the BPR testing. The default is to use 'When Threshold Exceeded' so that the only time the route is changed is if the high threshold you set is met.

Route Description: (Network Name)

(URL Address - example: www.xyz.com)
NOTE: Must be pingable, and should not be the same as a [link Control website](#).

Define Network: OR

. . . (Network Address Or Subnet)

(Subnet Mask)

. . . (This is the address that will be pinged)
NOTE: Created automatically if a URL is entered above.

Latency: ms (Round Trip Time Threshold - Default 80)

Packet Loss: % (Packet Loss Percentage - Default 3)

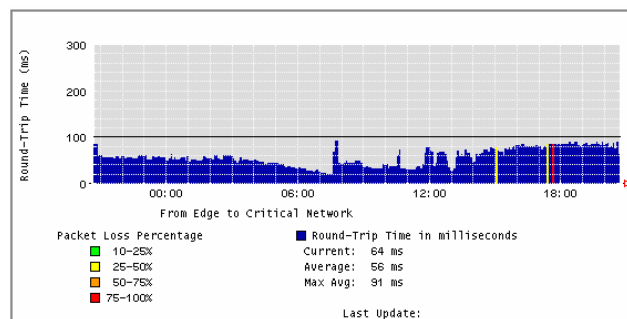
Jitter: ms (Latency Difference Between Tests - Default 50)

SLA Reporting: (Enable SLA Reports)

Route Method: (Select the default WAN interface)

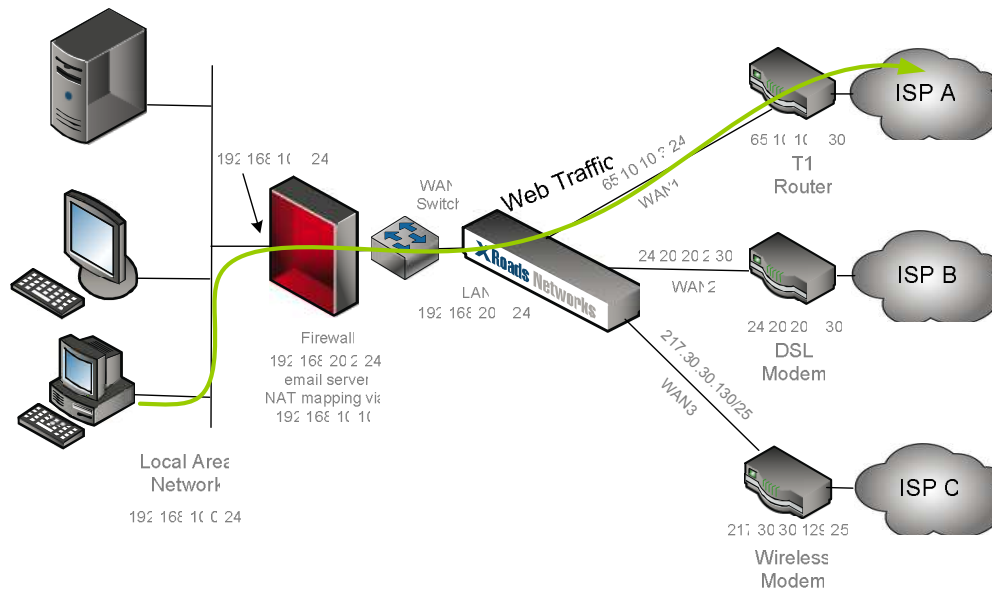
(How route selection will be applied)
NOTE: If persistence is an issue for this route, do not select best path.

This will ensure that all CRM traffic for this site will go through WAN1 unless the threshold is exceeded. It will also generate SLA reporting to this site so that each route path via each WAN link can be monitored. Below is an example of the reporting created:



It is also possible to setup email alerts when these thresholds are met so that you know when a link is not performing. These alerts are setup under the Tools tab.

Step 15) The final requirement for this deployment is to offload traffic from WAN1 by using forced application redirection on low priority web and email traffic. This is accomplished by setting up an application route. This diagram shows how this works:



To create an application route go to the NetBalancing tab and select the Application Routing menu. From here select the application to be directed, and the port this application should be direct out (optionally enter the source address to be forced, or leave blank to specify all).

Service: ?	WebHTTP----->80	<input type="button" value="New Service"/>
Source Address: ?	Optional - <input type="text"/> (Route Based On Address)	
Route Method: ?	WAN1 (During a WAN failure condition, the service will be automatically redirected)	

Deployment Summary

By reviewing this document and the example scenario provided, it should make deploying an EdgeXOS appliance in your environment easier. Please make sure to review the QuickStart Guide first to determine which installation method to use. Then make sure to review each of the HowToGuides and our online support videos for assistance.

If you need installation assistance, feel free to contract support. The support team is there to help. If you require an installation support call, please make sure to fill out the Live Configurator form first by using the QuickStart document as a guide.

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