

EdgeXOS Platform Notes

XRoads Networks

Edge Network Appliance Platform Notes

EdgeXOS VirtualNAT 101

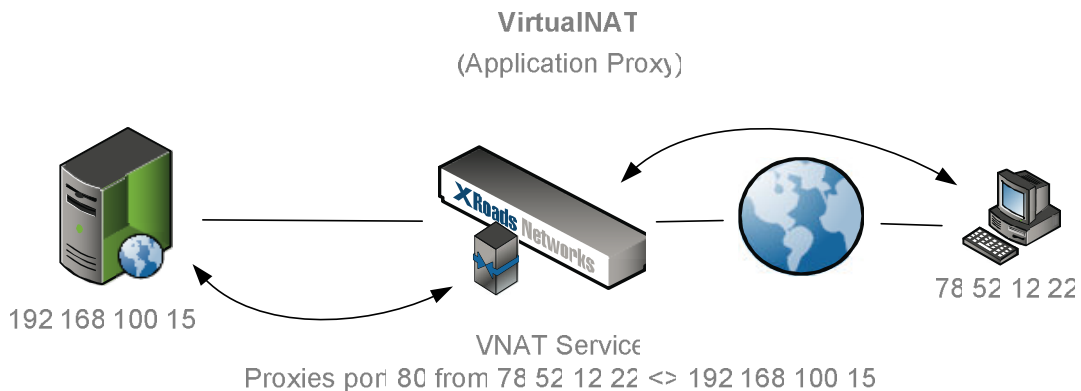
VirtualNAT (application proxy) Overview

This document provides an overview of how VirtualNAT works and what application proxy means. It is called VirtualNAT (or VNAT) as it achieves the same objectives as NAT, however it does not actually forward the inbound connection, it proxies it.

VirtualNAT is the default method which is recommended for handling inbound connections. It is generally used for providing failover and load balancing support for web servers, email servers, and most other TCP-based inbound connections.

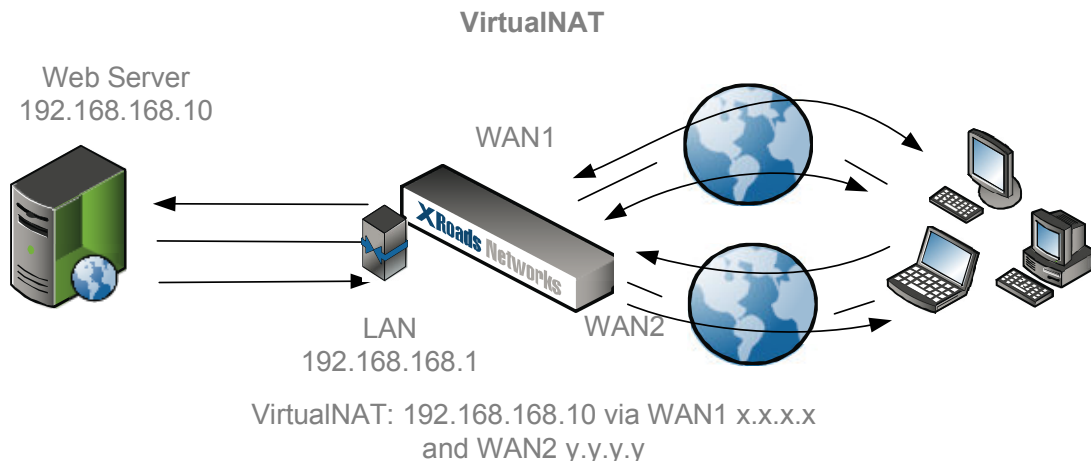
So, what is an application proxy? Application proxies work by receiving a connection and establishing a new connection to another device and then acting as a middle man between the two devices.

The example below shows how in general application proxy works. This is very similar to how an outbound web proxy works, except that in this case it happens in reverse.



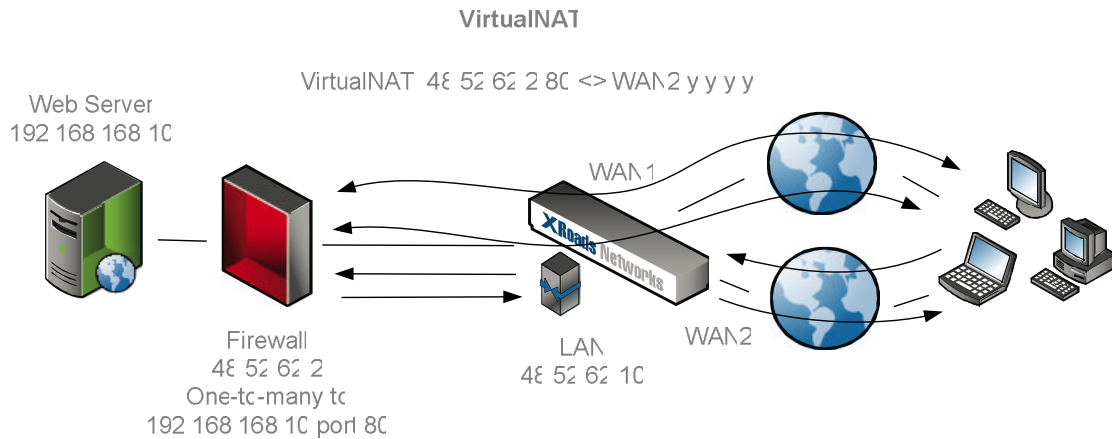
NOTE: There are several limitations to VNAT which must be taken into consideration. VirtualNAT ONLY works with TCP-based applications, so UDP applications like DNS, VoIP, and real-time streaming applications will not work. Additionally, any application which uses non-IP based protocols, like ICMP, IPSec, etc. can not be VNAT'd.

Load Balancing (NAT/NAT Mode): When the EdgeXOS appliance is NATing multiple WAN ports then you can use VirtualNAT to load balance inbound server connections across the two links. This is very easy to setup and simply requires that you add a secondary A record for the WAN2,3,etc addresses to your DNS records.



This example shows how two links can be balanced using a single VirtualNAT rule. All inbound web traffic going to the WAN1 x.x.x.x address and WAN2 y.y.y.y address will be balanced to the web server located at 192.168.168.10.

Load Balancing or Failover (Proxy/NAT Mode): When the EdgeXOS appliance is allowing WAN1 addresses to pass-through to the LAN, i.e. when there is an existing public network for WAN1 which needs to connect to an internal firewall device, etc. then VirtualNAT can be easily used to provide load balancing or failover for inbound server connections.



In this example the WAN1 link is operating in proxy/bridge mode and thus the WAN1 address space is passed directly to the firewall as before the EdgeXOS appliance was inserted into the network. Vector map rules (see Vector Maps 101) are added to ensure that WAN1 address space goes out via the WAN1 link.

Now, in order to get WAN2 working, we add a VirtualNAT rule which creates an application proxy for web traffic from the WAN2 y.y.y.y interface to the WAN1 firewall address of 48.52.62.2, which is the address used to forward web traffic to the web server.

With the Vector Map for WAN1 and the VirtualNAT rule for WAN2, full inbound and outbound load balancing and/or failover will work for the web server.

NOTE: If the firewall is enabled you will also need to make sure that rules are created to allow traffic to both the 48.52.62.2 address and the WAN2 address on port 80.

NOTE: Even though connectivity has been setup, this does not mean that the URL will immediately work for both WAN ports. This requires that your DNS records be modified to include the WAN2 address. This can easily be done by adding a second A record which will provide round-robin load balancing. Additionally, and for more control, you could have the EdgeXOS appliance handle the DNS for this server and thus dynamically adjust the load balancing and failover the DNS if an outage occurs. This is something that normal DNS can not do. For more information on our ActiveDNS, please refer to the appropriate HowToGuide.

VirtualNAT Configuration: Adding a new VirtualNAT rule is easy, simply click the NetBalancing tab and select the VirtualNAT menu. Click the add button...

The screenshot shows a configuration form for a VirtualNAT rule. On the left is a dark blue sidebar with labels: 'Server Name: ?', 'Server Service: ?', 'Internal Address: ?', 'WAN1 Address: ?', and 'WAN2 Address: ?'. The main area contains input fields and a button. The 'Server Name' field contains 'Web Server'. The 'Server Service' is a dropdown menu showing 'Web Server (HTTP/HTTPS)'. Below it is a button labeled 'Create Server Service' with a tooltip that says '(Create A New VirtualNAT Service)'. The 'Internal Address' is a dotted IP field with values 192, 168, 168, and 10, with a tooltip '(Internal Server Address)'. The 'WAN1 Address' is a dotted IP field with values 65, 56, 89, and 12, with a tooltip '(External Server Address for WAN1)'. The 'WAN2 Address' is a dotted IP field with values 66, 23, 56, and 59, with a tooltip '(External Server Address for WAN2)'.

As in the NAT/NAT example above, this screen shot shows how a VNAT rule can be created for two WAN ports which are in load balancing mode. The WAN1 link is 65.56.89.12 and the WAN2 link is 66.23.56.59. Any inbound connections to either of the addresses will be forwarded to 192.168.168.10.

Step 1) Enter the name of the server/device or "rule name" to identify the rule.

Step 2) Select the service for which you wish to create an application proxy

Step 3) Enter the internal address

NOTE: The internal address is the address of the server which is directly connected on the LAN side of the EdgeXOS appliance. If there is a firewall which is between the EdgeXOS and the server, then it is the firewalls NAT address for the server that we are looking for here.

Step 4) Enter the WAN1 address which will be used for this rule

NOTE: If the unit is in proxy/bridge mode then no WAN1 address is used, instead the WAN1 address is simply passed-through to the LAN side of the EdgeXOS appliance.

Step 5) Enter the additional WAN addresses to be forwarded to the internal address

Add the rule and confirm that the rule has been added properly.