

EdgeXOS Platform Notes

XRoads Networks

Edge Network Appliance Platform Notes

EdgeXOS Vector Maps 101

Vector Mappings Overview

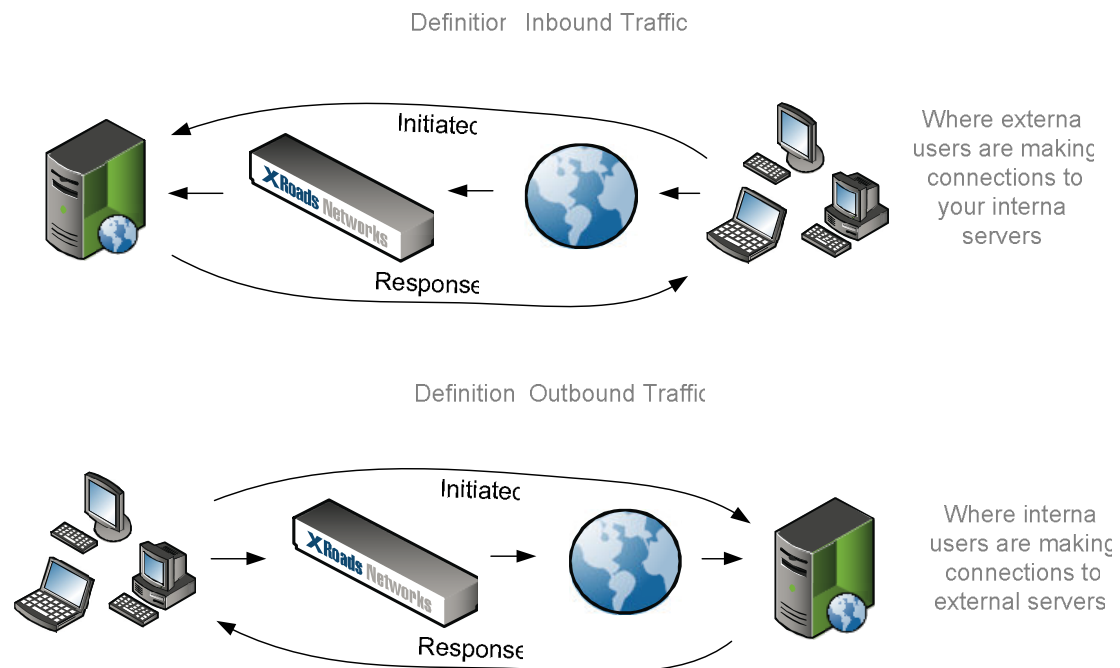
This document provides an overview of how Vector Maps work within the EdgeXOS platform and when you would use them to direct outbound traffic.

First let's review how the EdgeXOS appliance defines inbound and outbound traffic.

- Inbound traffic are those connections which are initiated from the outside inward to the local network, i.e. from the WAN to the LAN interfaces of the EdgeXOS appliance.
- Outbound traffic are those connections which are initiated from the inside outward to the wide-area network, i.e. from the LAN to the WAN interfaces of the EdgeXOS appliance.

NOTE: The responses from these initiated connections should not be considered when attempting to define the type of connection, it is entirely defined based on who initiates the connection.

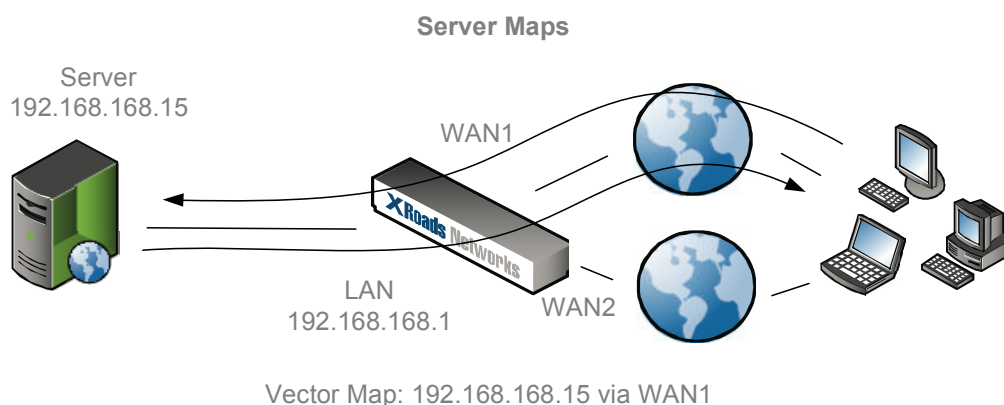
This diagram show how inbound and outbound connections are defined:



Now that we have defined how connections are viewed by the EdgeXOS platform, let's discuss when Vector Maps are used to ensure proper WAN link routing depending on whether the connection is inbound or outbound traffic.

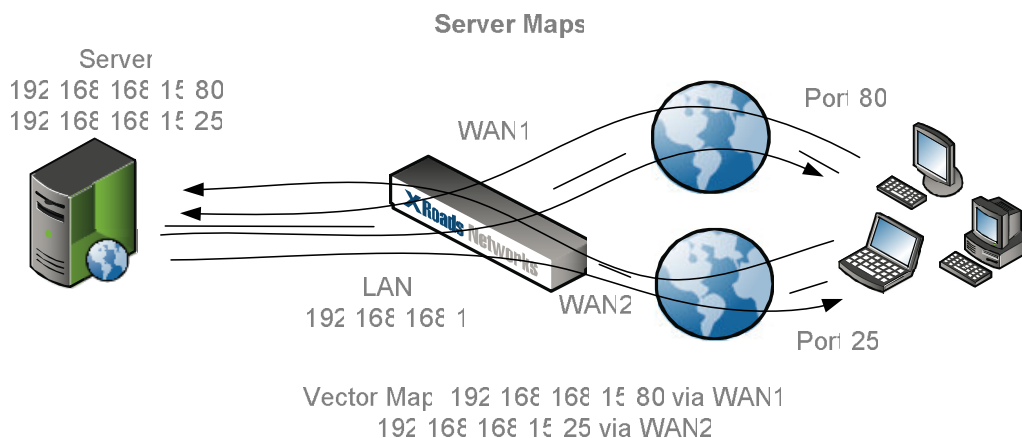
The two most common reasons for using a Vector Map is 1) to ensure that response traffic from inbound initiated connections go back out the same WAN interface that they came in on, i.e. server maps, 2) to force a specific LAN side address to always use the same WAN connection for any and all outbound connections, i.e. local maps.

Server Mappings: When ever an inbound connection is made through an EdgeXOS appliance that has multiple active WAN interfaces in load balancing mode it is possible that the response from the device to which the inbound connection was made could go out the wrong WAN interface. This is a problem as any inbound connection **MUST** go back out the same link that it came in on. If it does not, most Internet routers and/or firewalls will drop the response traffic as it would think that the response is invalid or a potential spoofing attack. Therefore, it is required that this traffic be sent out the correct WAN link. While the EdgeXOS does have several features which will automatically do this, it is important to also add Vector Maps to ensure that the response traffic always goes out the correct WAN link.



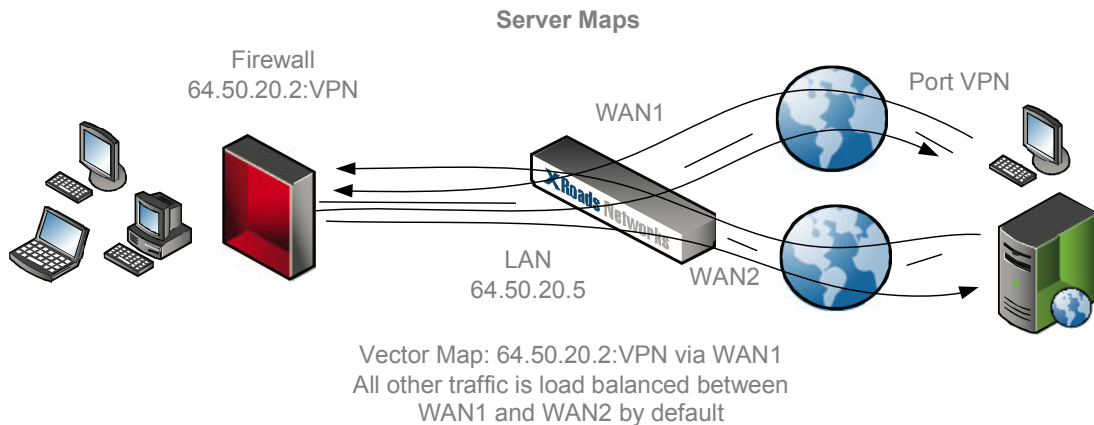
In this diagram we see how a server map is applied to ensure that any response traffic from the inbound connection coming in over the WAN1 connection to the server at 192.168.168.15 goes back out via the WAN1 connection.

Port-based vector maps are also possible, so that the same server IP address can be used for different types of traffic coming in over both WAN1 and WAN2.

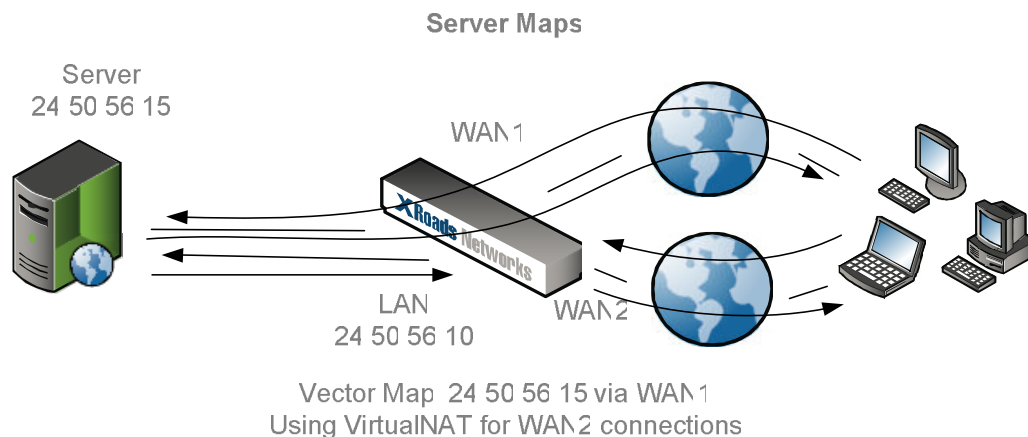


What if I have a firewall? The ability to do port specification is very useful when there is a firewall involved. Most firewalls perform NATing to a single primary outside address. This same address is often used for inbound IPsec tunnel termination or perhaps for inbound one-to-one NAT mappings, etc.

In these cases defining a specific port ensures that only that ports is forced back out the same connection, in this case WAN1. All other ports continue to be load balanced as they go out. So while inbound VPN traffic goes back out WAN1, outbound web, email, and all other traffic is still load balanced across both interfaces.



So you might ask at this point, how does one load balance server traffic if all response traffic is forced out the same WAN port? There are two primary methods for setting up load balancing across a single server. These methods include: 1) VirtualNAT (application proxy) which essentially proxies inbound connections to the server on the LAN side of the EdgeXOS appliance. VirtualNAT is commonly used for both load balancing and failover scenarios.

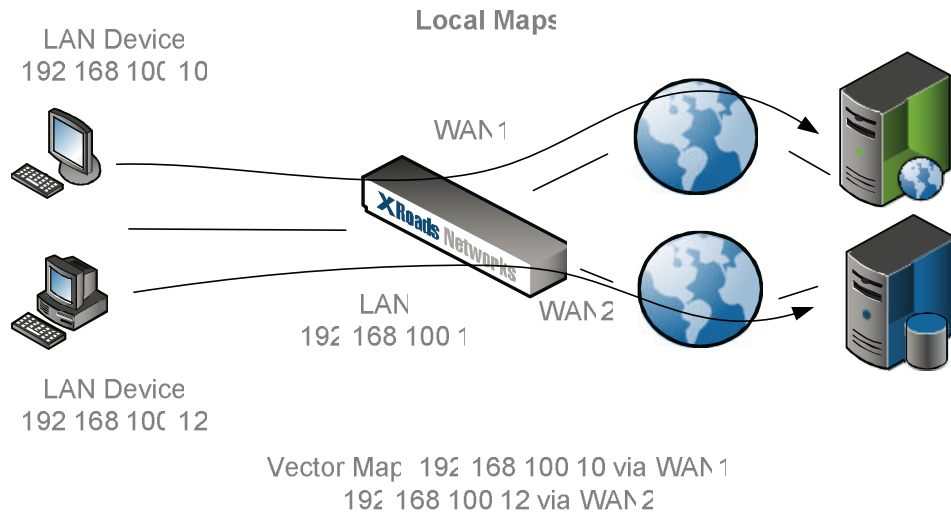


In this example the WAN1 link is in proxy/bridge mode, and all inbound traffic for WAN1 simply passed right through the EdgeXOS appliance. A Vector Map is used to ensure that inbound WAN1 traffic goes back out WAN1. However WAN2 traffic also works, as we are using the VirtualNAT (application proxy) which takes inbound connections requests and makes a direct request to the server (24.50.56.15), the server then responds directly to the EdgeXOS appliance, even though by default all traffic should be

routed out WAN1, because the EdgeXOS appliance is making a direct request, the response is handled by the VirtualNAT proxy and thus is forwarded out the WAN2 link.

NOTE: Additional details on how VirtualNAT works can be found in the NetBalancing HowToGuide, and other Platform Notes.

Local Mappings: Local maps are used to simply force a directly connected LAN address out a specific WAN interface. Local maps can also be port specific, so you could force all web traffic (port 80) out the WAN1 interface, while all other traffic from 192.168.100.10 would be load balanced.



In this example we show how to easily add a Vector Map rule to force a specific LAN device out one WAN link while another Vector Map rule forces a different LAN device out the other WAN link.

Vector Map Configuration: Adding a new Vector map is easy, simply click the NetBalancing tab and select the Vector Mappings menu. Click the add button...

Device Name:	<input type="text" value="Firewall_VPN"/>
Map Address:	<input type="text" value="64"/> . <input type="text" value="50"/> . <input type="text" value="20"/> . <input type="text" value="2"/> . <input type="text" value=""/> (Forward Address or Range - Available via the LAN interface)
	Optional - <input type="text" value=""/> OR <input type="text" value="VPN"/> (Enter a source port or port range x:x, if any)
Map Interface:	<input type="text" value="WAN1"/>
Apply Order:	<input type="text" value="1"/>

- Step 1) Enter the name of the server/device or "rule name" to identify the rule.
- Step 2) Enter the IP address of the device (must be a device on the LAN)
- Step 3) Optionally enter a port or select from the drop-down (VPN covers most types)
- Step 4) Select the WAN interface to which this outbound traffic will be directed
- Step 5) Select the Apply order for this rule. Apply order determines when a rule is applied and is covered in more detail in the Platform Notes guide for Apply Policies.

NOTE: It is recommended that all devices with inbound connections initially be setup with a Vector Map rule tied to the primary/existing WAN link.