

EdgeXOS Platform Notes

XRoads Networks

Edge Network Appliance Platform Notes

EdgeXOS DMZ Ports

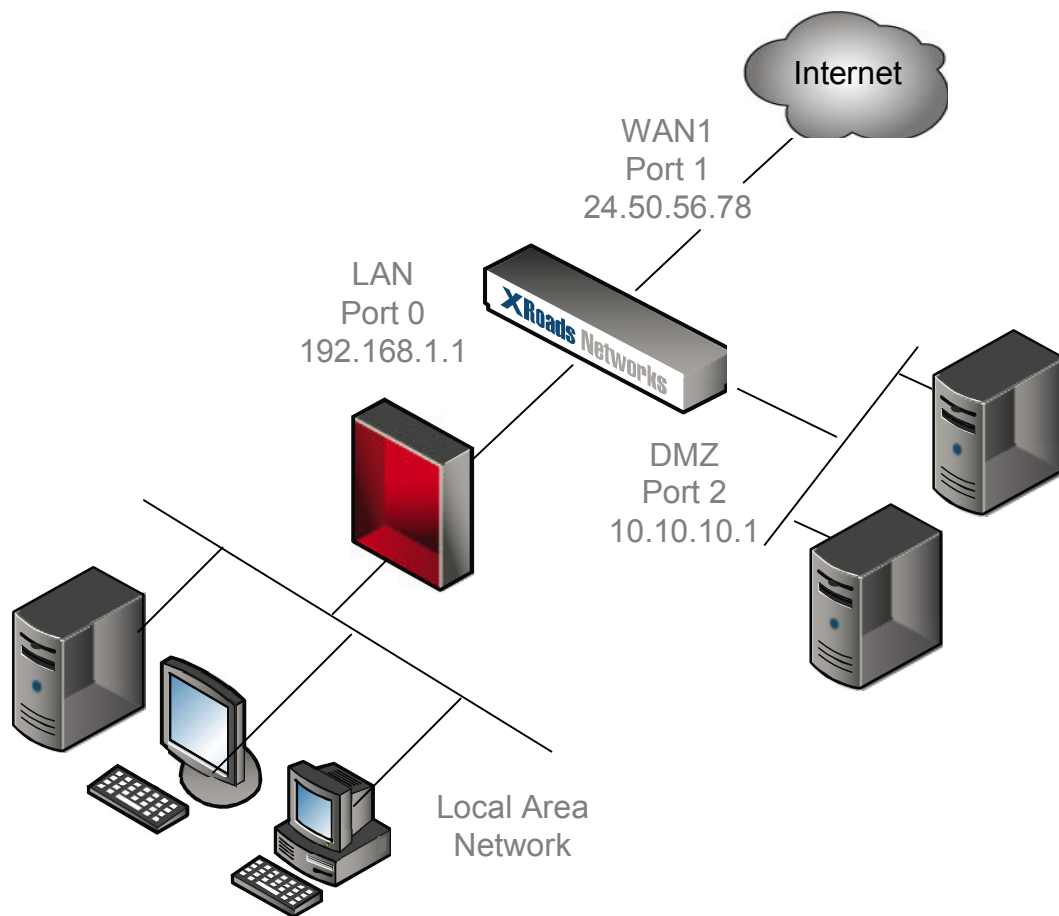
How To Configure DMZ Ports

This document provides an overview as to how DMZ interfaces may be configured. DMZ interfaces are typically used for several purposes: a) Creating a physically separate network for servers or other network connectivity, b) Terminate separate VLAN links, instead of using a trunk connection (this is useful for shaping multi-VLAN traffic, c) Connecting a point-to-point private circuit (like a P2P T1 or frame relay link).

NOTE: When set to DMZ mode an interface will not participate with active load balancing as do non-DMZ ports. DMZ ports do not have a default gateway assigned to them and thus will only route that traffic which is specifically configured to route over that port.

A) Creating A Separate Physical Network

As shown in the example network below, a physically separate network can be setup by setting one of the unused port on the EdgeXOS to DMZ mode. In this example a DMZ port is setup on the WAN2 interface. WAN2 is now acting as a DMZ port and thus will not be treated as a WAN port with a default gateway, but as a normal routed port, like the LAN interface.



How To Configure A Simple DMZ Port

In order to configure a DMZ port simply select the interface that you wish to make a DMZ port. This is done via the Interfaces tab and selecting the appropriate port. Then set the port to Active. Then enter the correct IP address for the interface, along with the subnet mask.

NOTE: No gateway or probe address is required, as this port will not participate in WAN load balancing.

In the example above the port address is set to 10.10.10.1, the subnet mask is 255.255.255.0 which means that any network device in the 10.10.10.2-254 range can be connected via this DMZ port and will be able to route to either the LAN interface or out the WAN interface(s)..

Additional firewall rules can be added to the DMZ port as an added layer of protection between the DMZ and the LAN network.

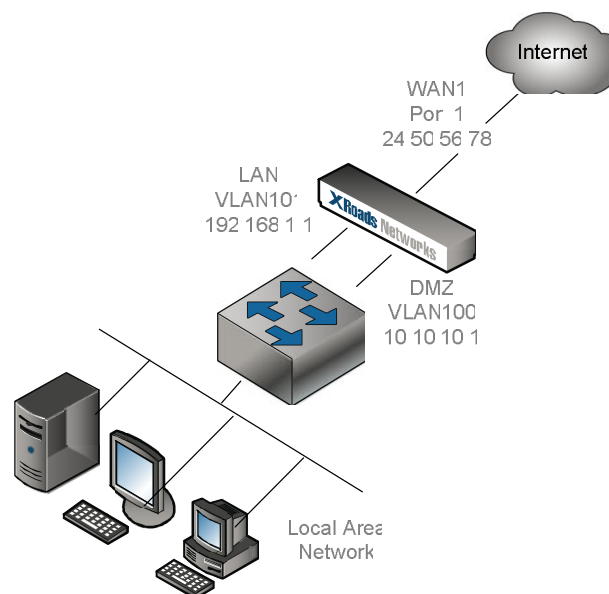
This feature is very useful for separating the LAN from your server network, test network, or other purpose.

How To Configure A Simple DMZ Port

Use the same process as used in option A where you simply turn up the port, make it Active and add the correct IP address and subnet. All VLAN control is handled by the switch.

B) Terminating Multiple VLANs

In this example a DMZ port can be used to terminate multiple VLANs without using a single trunk connection on the primary LAN interface. This is advantageous when attempting to perform policy-based shaping on VLAN connections, which can not be done using a trunked connection today.

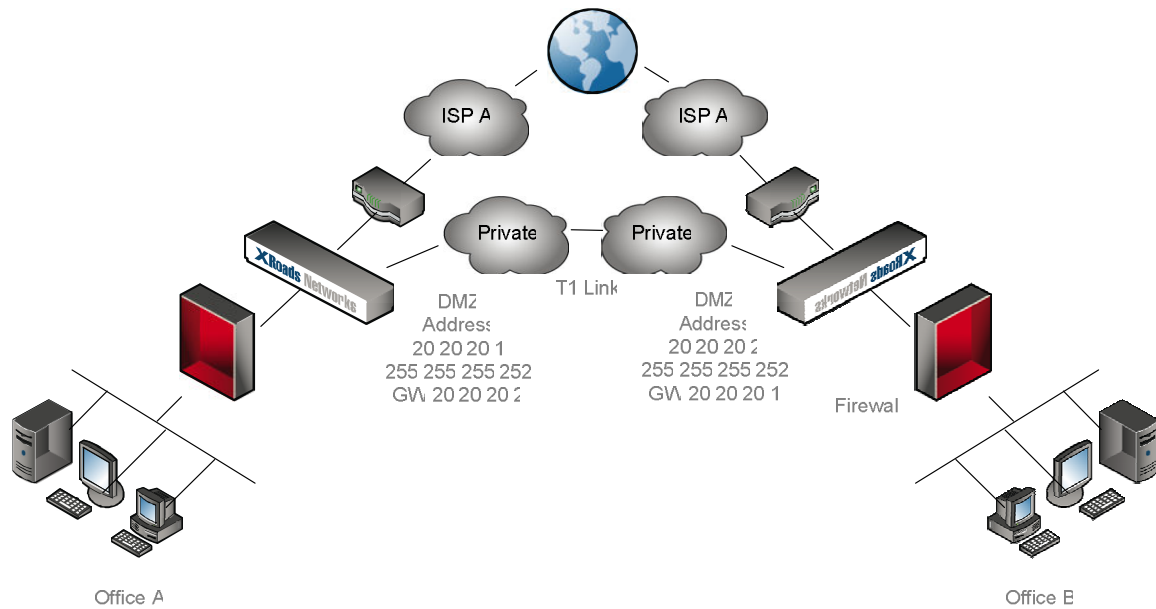


As shown in the example above a DMZ port is used to terminate a secondary VLAN switched port. This is highly effective when one needs to perform per-VLAN shaping, or simply to connect multiple VLANs when a trunked connection is not possible.

C) Connecting A Point-To-Point WAN Link Using DMZ Ports

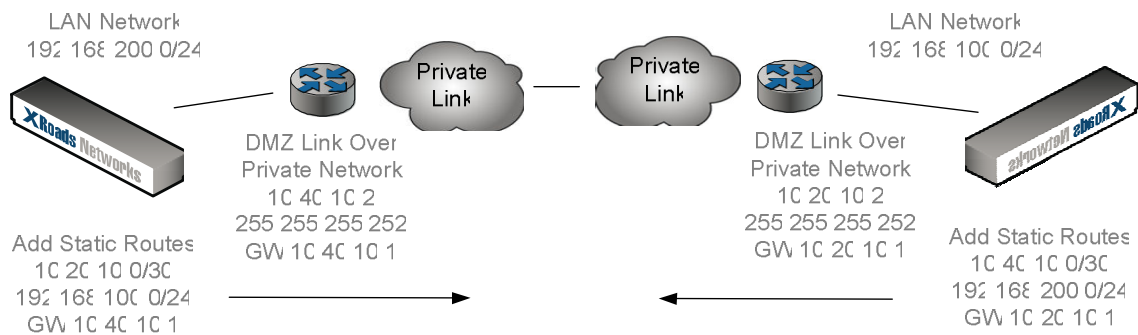
This method is used a great deal in conjunction with our Site2Site tunneling capabilities where one WAN port is connected over the Internet and the other is connected over a private link (T1, Frame Relay, MPLS, etc).

In the example below you can see that one can leverage DMZ interfaces to setup a private link between two sites. If additional networks need to be routed between two DMZ ports in this type of configuration static routing can be used.



Non-Site2Site Deployments

The following shows how a DMZ port would be configured when a simple end-to-end connection is required between two EdgeXOS appliances. In this example, no Site2Site tunnels are used. The only configuration required is the Interface being set to DMZ mode, and the static routes added to setup the routing between the two sites.



How To Configure A Simple DMZ Port

The following shows how a DMZ port would be configured when a Site2Site tunnel is being used. When a Site2Site tunnel is being used across a DMZ link, it is required that a gateway address be provided. The gateway address is either the local router gateway, or (as in the case above) the IP address of the remote EdgeXOS appliance.

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.

20 . 20 . 20 . 1 (Interface IP Address)

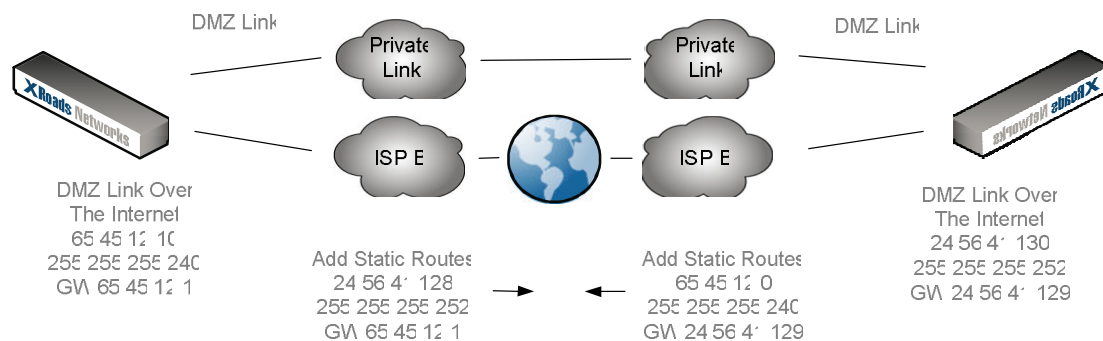
255.255.255.0 ▼ (Subnet Mask)

20 . 20 . 20 . 2 (Interface Gateway IP Address)

20 . 20 . 20 . 2 (Probe Address - will automatically populate if left blank)

The screen shot above shows how to configure a DMZ port to be used in conjunction with a Site2Site tunnel.

NOTE: It is also possible to use a DMZ interface with a non-private link (i.e. over the Internet). This may be required for an EdgeXOS deployment where a Site2Site tunnel is required, however the customer does NOT want to use the Internet connection attached to the EdgeXOS appliance as their default gateway.



The diagram shows how this can be accomplished by taking into consideration that no default gateway is provided (thus ensuring that the connection is not used for standard Internet access). When in this mode any and all access across the Internet connection must be added via static routes, this includes the network(s) of the remote EdgeXOS appliance, directing those routes to the local DMZ gateway router.

Once the connectivity between the two sites is working, and pingable you can then configure the Site2Site tunnels as normal. Please reference the Site2Site How To Guide for more details on configuring these tunnels.