

XRoads Networks

Edge Network Appliance How To Guide:
Site2Site

Edge Network Appliance How To Guide: Site2Site

©2007 XRoads Networks

17165 Von Karman, Suite 112
888-9-XROADS

Table of Contents

4 **Introduction**

Solution

- 5 Site2Site Overview
- 6 Site2Site WAN Optimization
- 7 Example Network

Step-by-Step

- 8 Tunnel Configuration
- 10 Starting The Tunnel(s)
- 12 Activation / Status Definitions
- 13 Encryption / Compression
- 14 Site2Site Parameters

Site2Site Introduction

Use this guide as a step-by-step manual for configuring your Edge appliance Site2Site. The Site2Site configuration is designed to enable site-to-site data compression, TCP tuning, and error checking to speed up application responsiveness.

About the “Screen Shots”

The included screen shots were taken from a working example configuration in the XRoads Networks lab. This configuration was running on XOS3.4.x. Some screen shots may be different depending on your version of XOS code.

Step-By-Step Method

Use this guide to assist in configuring your own Edge device. The examples provided herein are designed as a template which can translate to your organizations network environment. The three primary configuration steps are outlined below:

Primary Hub Configuration

This is setup of the Site2Site tunnel of the Edge device designated as the hub.

Primary Client Configuration

This is setup of the Site2Site tunnel of the Edge device designated as the client.

Secondary tunnel for binding at each site

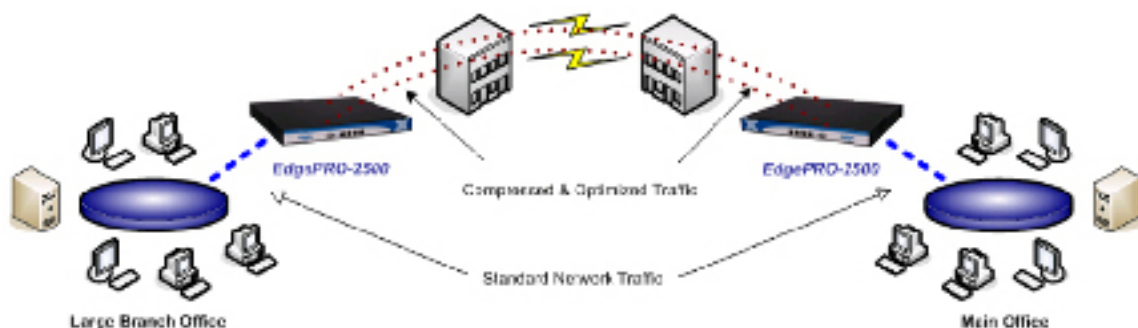
This is the configuration of a secondary tunnel on each Edge device for the purpose of binding the two tunnels together. Tunnel binding automatically provides failover in case one of the tunnels (i.e. WAN connections) should stop working.

Site2Site WAN Overview

Increase site-to-site application responsiveness and download times. This feature is designed to improve the performance of critical applications primarily between a central location and one or more branch offices.

Some of the advantages of the Site2Site solution include data compression (where data is compressed prior to being sent out the WAN interface), tunnel binding (the ability to bind multiple Site2Site tunnels through multiple WAN interfaces to increase overall throughput for the network), adaptive TCP tuning (automatic scaling of the TCP window to improve performance), and forward error checking (dynamically resetting a file download when errors occur to minimize the time to resend the file).

The example below shows a highly optimized solution between two sites. This example demonstrates how to Edge appliances (one at each location) in combination with multiple WAN connections, can greatly increase the overall performance and throughput of critical applications being access between the sites.



XRoads Networks

- Home
- Interfaces
- Shaping
- NetBalancing
- Firewall
- Site2Site**
- Tools
- Reporting

EdgeXL Traffic Manager

EdgeXL-20SXV
XOS Version 3.4.x Build Demo

This is our powerful Site2Site VPN solution with built-in data compression technology. The XOS site to site tunnel can provide instant tunnel failover for branch office/remote office 24x7 connectivity as well as tunnel load balancing between two or more sites for faster downloads and quicker response times for critical applications.

Use the Site2Site menu selection to create a new tunnel. When selecting this menu option the tunnel listing first appears. Select the "<< Add Tunnel" button to begin the configuration process.

Site2Site WAN Optimization

XRoads Networks offers a new method to deliver increased throughput between sites. Most WAN Optimization technologies utilize caching and various types of data compression to improve speeds.

Existing WAN Optimization Problems

The primary problems with existing WAN optimization techniques is that they are expensive to scale, and are lacking in their ability to optimize small packet bi-directional traffic (applications like Citrix, RDP, VoIP, etc). Most WAN optimization devices rely on two techniques, data caching, which only works for short-term retransmissions, and TCP window scaling, which is usually slow to adjust to small packet traffic.

Site2Site WAN Optimization Solution

XRoads Networks has chosen a “different path” in regards to WAN optimization. Instead of simply caching traffic and trying to guess what is in a packet the Edge appliance actually increases the amount of bandwidth available using inexpensive broadband links.

The advantages to using multiple broadband links are numerous, and the cost is still less than most scalable WAN optimization solutions. Most WAN optimization solutions become oversaturated within several years and become obsolete. The Edge continues its ROI beyond most WAN optimization appliances by allowing the connection of additional inexpensive broadband connections in order to easily increase throughput as needed, a step-up approach which works well with most IT budgets. The Edge’s scalability makes this process easy and affordable.

The most unique aspect of the Site2Site tunneling system developed by XRoads Networks is that unlike any other WAN optimization solution, the Site2Site tunnels are 100% network outage resistant. By connecting multiple WAN links on each end of the tunnel, the Edge can achieve over 99.9999% uptime between sites. No other independent WAN optimization solution can make this claim.

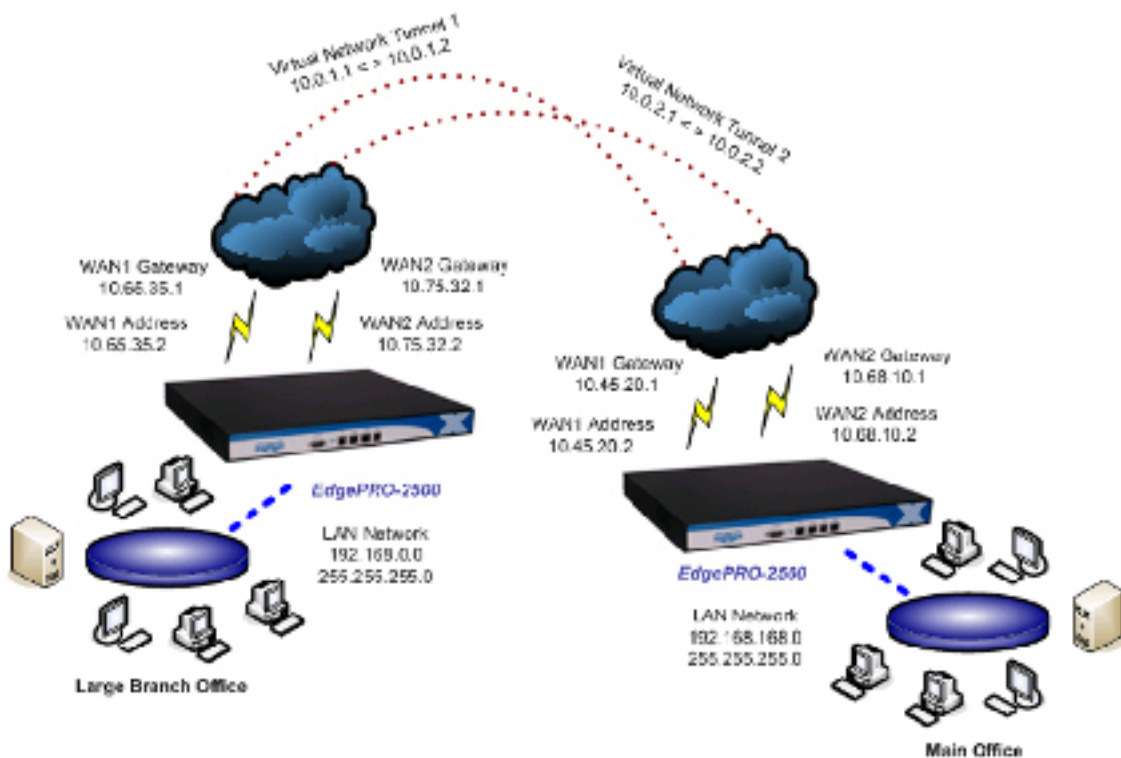
Site2Site Data Compression Statistics

Based on tunnel testing using un-compressed text files, the Edge platform was able to achieve a 5:1 increase on download speed and a 3:1 increase in overall download time. Example: A normal download over the Internet took 35 seconds and max’d out at 90Kbps, the same download over our XOS tunnel took 8-9 seconds and max’d out at 450Kbps.

If you multiply that across the multi-WAN capability of our Edge platform you get an overall network throughput increase of up to 30:1 (or 5:1 x 6 load balanced WAN ports). Based on real-world tests XRoads Networks has found a max increase in network throughput of over 2100% for un-compressed data files.

Example Network

This example network is provided as a template which can be used to determine how to best configure your Edge appliance. In the example network environment, each Edge appliance is connected to two WAN interfaces. The WAN interfaces are statically routed in this case, but the method of WAN connection does not matter when configuring the tunnels. The only requirement is that the interfaces being configured are active.



Network Overview

This example network shows two Edge devices connected via two WAN links at each site. The goal is to create two optimization tunnels between the sites and bind them for increase speed via tunnel load balancing with the ability to automatically failover in the event of a WAN outage.

The primary tunnel will be called m2b_tun1 (b2m_tun1), and the secondary tunnel will be called m2b_tun2 (b2m_tun2). The secondary tunnel will be bound to the primary tunnel.

The addressing information that will be used is located in the diagram above. The following steps show how to configure this scenario.

Site2Site Step-By-Step

The following pages show a step-by-step example of how to configure the Edge router based on the network environment in the example scenario.

The following screen will be displayed whenever changes are made to the tunnel rules.

Make sure to save your settings.
Please wait while the XOS policies are being updated...

Step One

The following screen demonstrates how TUNNEL 1 on the HUB device is configured.

The screenshot shows the configuration page for Tunnel 1. The interface is split into a dark blue sidebar on the left with labels and a main white area with input fields. The labels in the sidebar are: Tunnel Name, Tunnel ID, Tunnel Type, Weight, Data Compression, Shared Secret Key, Encryption Type, WAN Interface, Virtual Address, Remote Edge Device, Remote Network, Client/Hub, and On Failure. The main area contains the following configuration details:

- Tunnel Name:** m2b.tun1 (Used to define this rule as a Site2Site tunnel)
- Tunnel ID:** 1 (Selected as unique tunnel ID)
- Tunnel Type:** Primary (Selected), Backup (Empty field), Bind To: none (Selected as binding name for binding, see ? for details)
- Weight:** 100 (Ratio Of Tunnel Up/Down)
- Data Compression:** Disabled (Selected), Enabled (Unselected)
- Shared Secret Key:** thisismykey12345 (This key must be 16 characters using only numbers and letters)
- Encryption Type:** 3DES (Selected as encryption type, if any)
- WAN Interface:** WAN1 (Selected the outbound interface)
- Virtual Address:** 10.0.1.2 (Local Virtual Address), 10.0.1.1 (Remote Virtual Address)
- Remote Edge Device:** Static (Selected), Dynamic (Unselected) (Is the remote address dynamic or static?)
10.0.35.2 (Enter the WAN address of the remote Edge device)
- Remote Network:** 192.168.0.0 (Enter the network address of the remote network)
255.255.255.0 (Remote network mask)
- Client/Hub:** Client Side (Unselected), Hub Side (Selected as tunnel type)
- On Failure:** Disabled (Selected), Enabled (Unselected) (Selected to enable tunnel only if WAN fails)

Step Two

This screen demonstrates how TUNNEL 1 on the CLIENT device is configured.

NOTE: The tunnel ID prefix MUST match the prefix of the hub side tunnel configuration.

The screenshot shows the configuration interface for Tunnel 1 on a client device. The settings are as follows:

- Tunnel Name:** m2b_tun1 (Used to define the site-to-site IPSec tunnel)
- Tunnel ID:** 1 (Selected a unique tunnel ID)
- Tunnel Type:** Primary (Selected)
- Weight:** 100 (Ratio Of Tunnel Utilization)
- Data Compression:** Disabled (Enabled to enable file data compression for this tunnel)
- Shared Secret Key:** hixismykey12345 (This key must be 25 characters long, only numbers and letters)
- Encryption Type:** 3DES (Select an encryption type, if any)
- WAN Interface:** WAN1 (Select the outbound interface)
- Virtual Address:** 10.0.1.1 (Local Virtual Address) 10.0.1.2 (Remote Virtual Address)
- Remote Edge Device:** Static (Selected) (To use remote address dynamic or static?) 10.45.20.2 (Enter the WAN address of the remote Edge device)
- Remote Network:** 192.168.168.0 (Enter the network address of the remote network) 255.255.255.0 (Remote network mask)
- Client/Hub:** Client Side (Selected) (Select the tunnel type)
- On Failure:** Disabled (Selected) (Select to create tunnel only if WAN is Up)

Step Three

The following screen demonstrates how TUNNEL 2 on the HUB device is configured.

The screenshot shows the configuration interface for Tunnel 2 on a hub device. The settings are as follows:

- Tunnel Name:** m2b_tun2 (Used to define the site-to-site IPSec tunnel)
- Tunnel ID:** 2 (Selected a unique tunnel ID)
- Tunnel Type:** Primary (Selected)
- Weight:** 100 (Ratio Of Tunnel Utilization)
- Data Compression:** Disabled (Enabled to enable file data compression for this tunnel)
- Shared Secret Key:** hixismykey12345 (This key must be 25 characters long, only numbers and letters)
- Encryption Type:** 3DES (Select an encryption type, if any)
- WAN Interface:** WAN2 (Select the outbound interface)
- Virtual Address:** 10.0.2.2 (Local Virtual Address) 10.0.2.1 (Remote Virtual Address)
- Remote Edge Device:** Static (Selected) (To use remote address dynamic or static?) 10.75.12.2 (Enter the WAN address of the remote Edge device)
- Remote Network:** 192.168.168.0 (Enter the network address of the remote network) 255.255.255.0 (Remote network mask)
- Client/Hub:** Hub Side (Selected) (Select the tunnel type)
- On Failure:** Disabled (Selected) (Select to create tunnel only if WAN is Up)

Step Four

This screen demonstrates how TUNNEL 2 on the CLIENT device is configured.

The screenshot shows the configuration page for a tunnel named 'm2b_tun2'. The settings are as follows:

- Tunnel Name:** m2b_tun2
- Tunnel ID:** 2-2
- Tunnel Type:** Primary
- Bind To:** m2b_tun1
- Weight:** 100
- Data Compression:** Disabled
- Shared Secret Key:** thisismykey12345
- Encryption Type:** 3DES
- WAN Interface:** WAN2
- Virtual Address:** 10.0.2.1
- Remote Edge Device:** Static, 10.68.10.2
- Remote Network:** 192.168.168.0
- Clone/Hub:** Client Side
- On Failure:** Disabled

Step Five

Once the tunnels have been created they must be ENABLED. This is done by selecting a tunnel and clicking the “Start” button. This will change the State of the tunnel to ENABLED and the tunnel will attempt to make a connection to the remote Edge device.

XOS Tunnels are listed by Connection Name.

Select	Connection	WAN Port	Client/Hub	Remote Device	Remote Addr/Mask	Binding	Session	State	Activated	Status
<input checked="" type="radio"/>	m2b_tun1	wan1 169.0.0.0	Client	10.45.20.2	192.168.168.0/24	None	1	Disabled	No	DOWN
<input type="radio"/>	m2b_tun2	wan2	Client	10.68.10.2	192.168.168.0/24	m2b_tun1	2	Disabled	No	DOWN

Control buttons: << Add Tunnel | Add Route | **Start** | Stop | S2SLog | Save

Control buttons: Select | Delete | Restart All | Refresh View | Params

The following screen is displayed during the starting or stopping of a tunnel.

Please wait while the Edge attempts to start VPN Optimization Tunnel 'm2b_tun1'...

Both tunnels should be ENABLED to enable tunnel binding.

Select	Connection	WAN Port	Client/Hub	Remote Device	Remote Addr/Mask	Binding	Session	State	Activated	Status
	m2b_tun1	wan1 169.0.0.0	Client	10.45.20.2	192.168.168.0/24	None	1	Enabled	No	DOWN
	m2b_tun2	wan2	Client	10.68.10.2	192.168.168.0/24	m2b_tun1	2	Enabled	No	DOWN

<< Add Tunnel | Add Route | Start | Stop | S2SLog | Save

Select | Delete | Restart All | Refresh View | Params

Step Six

The client tunnels must also be started as the hub tunnels were in order to bring the tunnels to an UP and activated mode.

Select	Connection	WAN Port	Client/Hub	Remote Device	Remote Addr/Mask	Binding	Session	State	Activated	Status
	m2b_tun1	wan1 169.0.0.0	Client	10.45.20.2	192.168.168.0/24	None	1	Disabled	No	DOWN
	m2b_tun2	wan2	Client	10.68.10.2	192.168.168.0/24	m2b_tun1	2	Disabled	No	DOWN

<< Add Tunnel | Add Route | Start | Stop | S2SLog | Save

Select | Delete | Restart All | Refresh View | Params

Step Seven

This screen shows the tunnels UP and activated. Both tunnels are now in a load balanced state able to pass traffic between the two sites with full optimization, data compression, error checking, and redundancy.

Activation / Status Definitions

The "Status" column is used to provide information regarding the availability of the tunnel. If the tunnel is in a working state, the "Status" column will show as UP. If the tunnel is not in a working state, due to either a WAN failure, route failure, disabled or stopped tunnel the "Status" column will show the tunnel as DOWN.

The "Activated" column is used to determine whether the tunnel is being actively routed, meaning whether network traffic is actually being routed through that particular tunnel. If the "Activated" column equals -Yes- than traffic is being routed over this tunnel. If the "Activated" column equals -No- than traffic is not being routed over this tunnel.

Activated	Status
No	DOWN
No	DOWN

This state shows both tunnels UP in load balanced mode.

Activated	Status
No	DOWN
No	DOWN

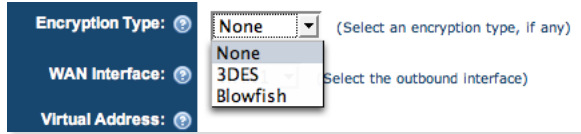
This state shows the primary tunnel UP and the secondary tunnel DOWN, most likely from a WAN failure or if the tunnel was disabled.

Activated	Status
No	DOWN
No	DOWN

This state show the primary tunnel UP and routing traffic. The secondary tunnel is also UP (meaning available) however it is not routing traffic. This is most likely because the tunnel is in Backup mode.

Site2Site Encryption

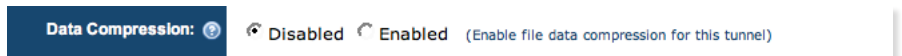
Built-in to each Site2Site tunnel is the ability to encapsulate data using a highly secure encryption algorithm. The two currently available algorithms include 3DES (a standard used by most government and financial institutions) and Blowfish (a slightly faster algorithm but less widely used). Future generations of the firmware will include support for AES (the next generation of government level encryption).



Simply select the encryption option desired. Make sure that both ends of the tunnel are configured with the same encryption type.

Site2Site Compression

Data compression enabled traffic traversing through Site2Site tunnels to be compressed when possible. Compression is only effective when the data has not been previously compressed, i.e. text files, non-compressed images, and other types of large data types which are not compressed prior to transit.



It is possible to disable compression when the processing cycles required to attempt compression outweighs the net gain due to the compression.

NOTE: Typically compression is disabled when small packet applications are used, such as Citrix, RDP, etc.

COMPRESSION SPECIFICATIONS: We have completed a number of site-to-site tests between multiple offices. Based on this testing we have confirmed the following compression ratios.

The EdgeXOS platform can achieve a 5:1 increase on download speed and a 3:1 increase in overall download time for non-compressed files. Example: A normal download over the Internet took 35 seconds and max'd out at 90Kbps, the same download over our Site2Site tunnel with compression enabled took 8-9 seconds and max'd out at 450Kbps.

However files that are PRE-compressed, meaning that it was zipped or compressed by another application prior to being downloaded, it will almost always take the same amount of time to download, i.e. no increase in speed or throughput. In fact, under some conditions it may take a bit longer due to the tunnels added overhead.

Tunnel compression is not recommended for use with database applications, Windows remote file access, or real-time streaming applications as it does not provide an increase in speed for those applications.

Site2Site Secondary Network Routing

Some customers may have multiple networks on each end of a Site2Site tunnel. When multiple subnets are required, the Site2Site routing table is used to setup balanced routing for secondary routes.

Select	Connection	WAN Port	Client/Hub	Remote Device	Remote Addr/Mask	Binding	Session	St
	m2b_tun1	wan1 169.0.0.0	Client	10.45.20.2	192.168.168.0/24	None	1	
	m2b_tun2	wan2	Client	10.68.10.2	192.168.168.0/24	m2b_tun1	2	

Simply enter the subnet and select which tunnel to use when routing this subnet. If this subnet should be balanced between multiple tunnels, simply enter the subnet for each tunnel which should be used for balancing.

Insert Route: / (Must Be A Network Address)

(Tunnel Name)

Administrators may also choose to use a specific tunnel for routing one subnet and using another tunnel for routing another subnet. This could be used for separating application traffic (VoIP, etc) based on subnets.

Site2Site Parameters

The parameters below can be used to adjust how the Edge platform automatically manipulates its TCP window sizing and performs tunnel testing. It is generally advised to not make changes to these settings.

NOTE: TCP Window Scaling may be reduced when it is known that most application traffic through the Site2Site tunnel is small data packets, i.e. for applications like Citrix, RDP, etc.

S2S Parameters: Caution: Do not change unless you are sure of what you are doing.

(TCP Window Scaling [latency ms] - default 80)

(TCP Window Scaling [Mbps per second] - default 100)

(TCP Retries - default 3)

(TCP Timeout - default 5)

(TCP MTU/MSS Size - default 1500)

(PMTU Discovery Threshold - default 1450)

(Tunnel Holdtime - default 30)

(Tunnel Test Timing - default 5)

NOTES