

How To Guide

XRoads Networks

Edge Network Appliance How To Guide:
Site2Site

Edge Network Appliance How To Guide:
Site2Site

@2009 XRoads Networks

22642 Lambert St, Suite 403

888-9-XROADS

Table of Contents

Introduction

Site2Site Overview

Site2Site WAN Optimization

Example Network

Step-By-Step Tunnel Configuration

Starting The Tunnel(s)

Activation / Status Definitions

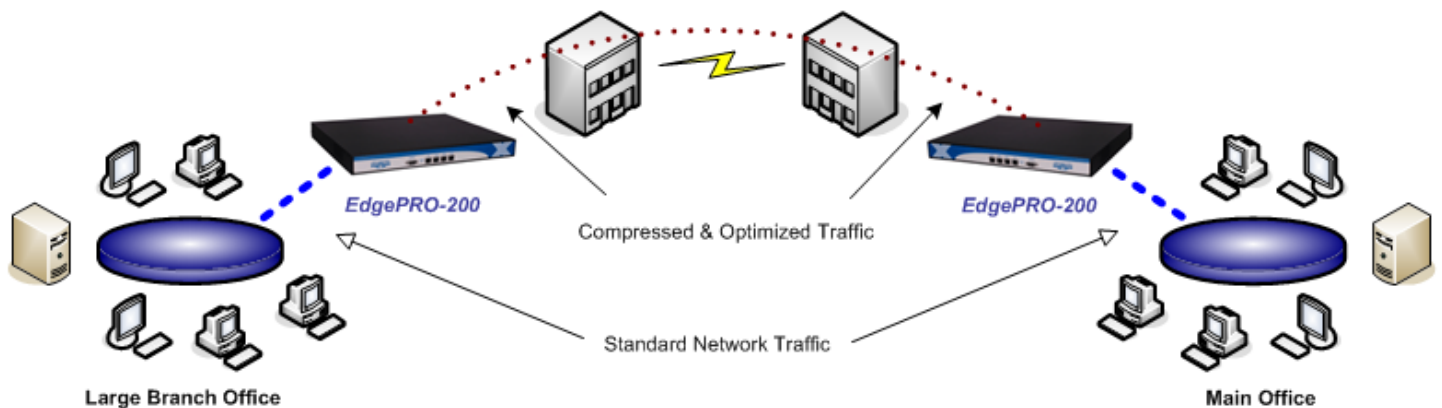
Encryption / Compression

Secondary Networks

Site2Site Parameters

Site2Site Introduction

Use this guide as a step-by-step manual for configuring the EdgeXOS platform for site-to-site connectivity between two EdgeXOS appliances. The examples provided herein are designed as a template which can translate to your organizations network environment. The three primary configuration steps are 1) Primary hub side tunnel configuration, 2) Primary client side tunnel configuration, and 3) Secondary hub and client side tunnel configuration (for failover and/or load balancing).



Edge Configuration Series Site2Site Overview

Our Site2Site technology is designed to provide improved connectivity between two or more offices where at least one office has two or more WAN connections. One of the core capabilities of the Site2Site technology is the ability to quickly failover connectivity between two sites when the primary connection is a point-to-point or MPLS connection. In these situations the EdgeXOS platform can provide instant and immediate failover for remote sites using an inexpensive broadband Internet connection via one or more secure encrypted tunnel(s)

XRoads Networks

[Home](#)

[Interfaces](#)

[Shaping](#)

[NetBalancing](#)

[Firewall](#)

[Site2Site](#)

[Tools](#)

[Reporting](#)

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.

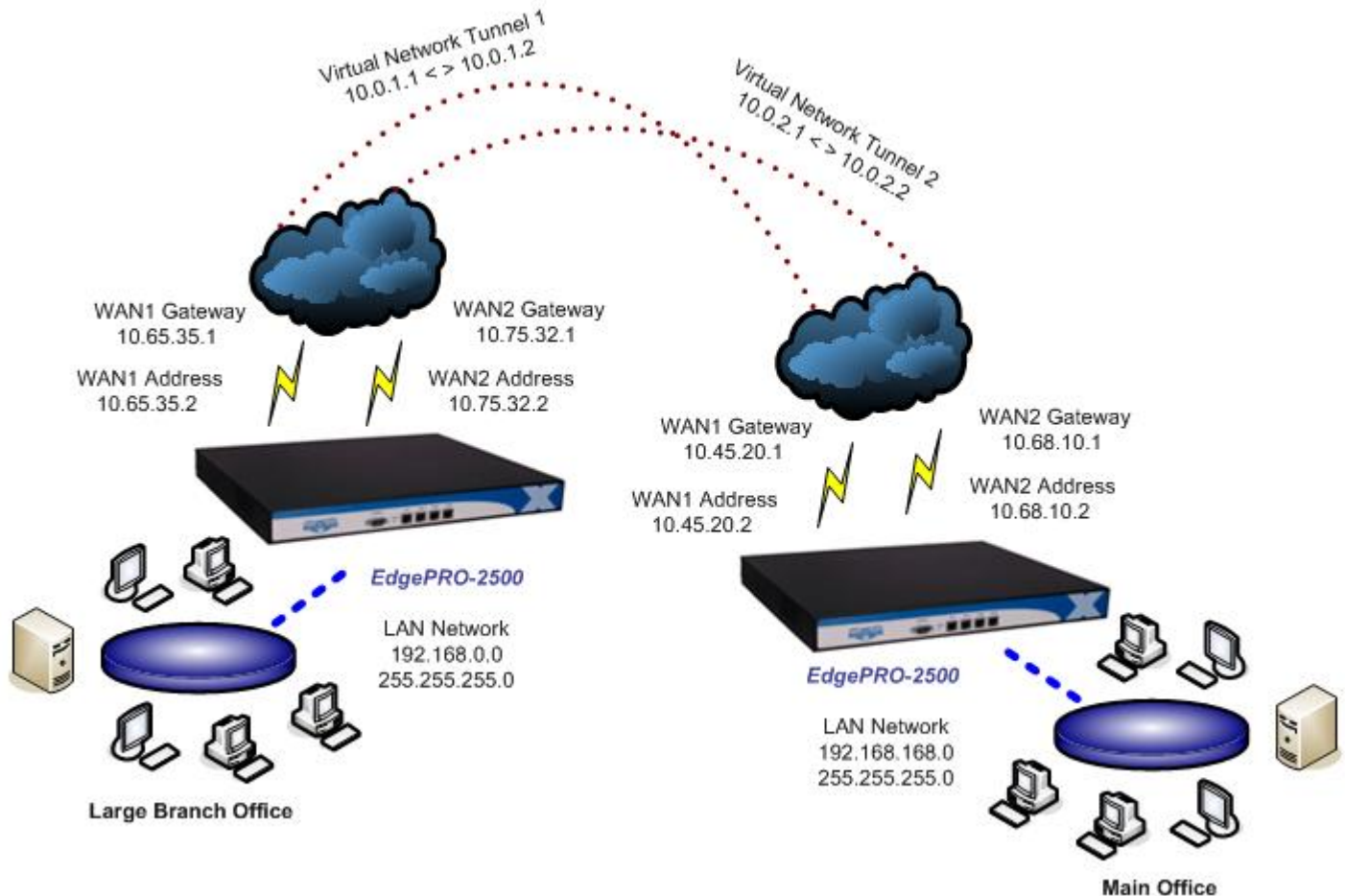
Site2Site Data Compression Statistics

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.

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.

| | |
|----------------------------|---|
| Tunnel Name: | <input type="text" value="m2b_tun1"/> (Used to define this site-to-site XOS tunnel) |
| Tunnel ID: | 1 . 1 (Select a unique tunnel ID) |
| Tunnel Type: | <input checked="" type="radio"/> Primary <input type="radio"/> Backup <input type="text"/> (Enter the primary tunnel name) <input type="radio"/> Bind To <input type="text" value="... none ..."/> (Select an existing tunnel for binding, see '?' for details) |
| Weight: | 100 (Ratio Of Tunnel Utilization) |
| Protocol Selection: | <input checked="" type="radio"/> TCP <input type="radio"/> UDP (Enable UDP to improve responsiveness for certain applications) |
| Data Compression: | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Enable file data compression for this tunnel) |
| | Level 1 (Compression Windowing Adjustment) |
| Shared Secret Key: | <input type="text" value="thisismykey12345"/> (This key must be 16 characters using only numbers and letters) |
| Encryption Type: | 3DES (Industry Standard) (Select an encryption type, if any) |
| WAN Interface: | WAN1 (Select the outbound interface) |
| Virtual Address: | 10 . 0 . 1 . 2 (Local Virtual Address) 10 . 0 . 1 . 1 (Remote Virtual Address) |
| Remote Edge Device: | <input checked="" type="radio"/> Static <input type="radio"/> Dynamic (Is the remote address dynamic or static?) 10 . 65 . 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: | <input type="radio"/> Client Side <input checked="" type="radio"/> Hub Side (Select this tunnel type) |
| On Failure: | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Select to enable tunnel only if failure detected - optional) |
| Fail Method: | <input checked="" type="radio"/> Probe Address <input type="radio"/> WAN1 (Select to either use WAN1 status or probe address below - optional) |

Step Two

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

| | |
|------------------------------|--|
| Tunnel Name: ⓘ | <input type="text" value="m2b_tun1"/> (Used to define this site-to-site XOS tunnel) |
| Tunnel ID: ⓘ | <input type="text" value="1"/> . <input type="text" value="1"/> (Select a unique tunnel ID) |
| Tunnel Type: ⓘ | <input checked="" type="radio"/> Primary <input type="radio"/> Backup <input type="text"/> (Enter the primary tunnel name) <input type="radio"/> Bind To <input type="text" value="--- none ---"/> (Select an existing tunnel for binding, see '?' for details) |
| Weight: ⓘ | <input type="text" value="100"/> (Ratio Of Tunnel Utilization) |
| Protocol Selection: ⓘ | <input checked="" type="radio"/> TCP <input type="radio"/> UDP (Enable UDP to improve responsiveness for certain applications) |
| Data Compression: ⓘ | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Enable file data compression for this tunnel) <input type="text" value="Level 1"/> (Compression Windowing Adjustment) |
| Shared Secret Key: ⓘ | <input type="text" value="thisismykey12345"/> (This key must be 16 characters using only numbers and letters) |
| Encryption Type: ⓘ | <input type="text" value="3DES (Industry Standard)"/> (Select an encryption type, if any) |
| WAN Interface: ⓘ | <input type="text" value="WAN1"/> (Select the outbound interface) |
| Virtual Address: ⓘ | <input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="1"/> . <input type="text" value="1"/> (Local Virtual Address) <input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="1"/> . <input type="text" value="2"/> (Remote Virtual Address) |
| Remote Edge Device: ⓘ | <input checked="" type="radio"/> Static <input type="radio"/> Dynamic (Is the remote address dynamic or static?) <input type="text" value="10"/> . <input type="text" value="45"/> . <input type="text" value="20"/> . <input type="text" value="2"/> (Enter the WAN address of the remote Edge device) |
| Remote Network: ⓘ | <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="168"/> . <input type="text" value="0"/> (Enter the network address of the remote network) <input type="text" value="255.255.255.0"/> (Remote network mask) |
| Client/Hub: ⓘ | <input checked="" type="radio"/> Client Side <input type="radio"/> Hub Side (Select this tunnel type) |
| On Failure: ⓘ | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Select to enable tunnel only if failure detected - optional) |
| Fail Method: ⓘ | <input checked="" type="radio"/> Probe Address <input type="radio"/> WAN1 (Select to either use WAN1 status or probe address below - optional) |

Step Three

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

| | |
|------------------------------|--|
| Tunnel Name: ⓘ | <input type="text" value="m2b_tun2"/> (Used to define this site-to-site XOS tunnel) |
| Tunnel ID: ⓘ | <input type="text" value="2"/> . <input type="text" value="2"/> (Select a unique tunnel ID) |
| Tunnel Type: ⓘ | <input type="radio"/> Primary <input type="radio"/> Backup <input type="text" value=""/> (Enter the primary tunnel name) <input checked="" type="radio"/> Bind To <input type="text" value="m2b_tun2"/> (Select an existing tunnel for binding, see '?' for details) |
| Weight: ⓘ | <input type="text" value="100"/> (Ratio Of Tunnel Utilization) |
| Protocol Selection: ⓘ | <input checked="" type="radio"/> TCP <input type="radio"/> UDP (Enable UDP to improve responsiveness for certain applications) |
| Data Compression: ⓘ | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Enable file data compression for this tunnel) |
| | <input type="text" value="Level 1"/> (Compression Windowing Adjustment) |
| Shared Secret Key: ⓘ | <input type="text" value="thisismykey12345"/> (This key must be 16 characters using only numbers and letters) |
| Encryption Type: ⓘ | <input type="text" value="3DES (Industry Standard)"/> (Select an encryption type, if any) |
| WAN Interface: ⓘ | <input type="text" value="WAN2"/> (Select the outbound interface) |
| Virtual Address: ⓘ | <input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="2"/> . <input type="text" value="2"/> (Local Virtual Address) <input type="text" value="10"/> . <input type="text" value="0"/> . <input type="text" value="2"/> . <input type="text" value="1"/> (Remote Virtual Address) |
| Remote Edge Device: ⓘ | <input checked="" type="radio"/> Static <input type="radio"/> Dynamic (Is the remote address dynamic or static?) <input type="text" value="10"/> . <input type="text" value="75"/> . <input type="text" value="32"/> . <input type="text" value="2"/> (Enter the WAN address of the remote Edge device) |
| Remote Network: ⓘ | <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="0"/> . <input type="text" value="0"/> (Enter the network address of the remote network) <input type="text" value="255.255.255.0"/> (Remote network mask) |
| Client/Hub: ⓘ | <input type="radio"/> Client Side <input checked="" type="radio"/> Hub Side (Select this tunnel type) |
| On Failure: ⓘ | <input checked="" type="radio"/> Disabled <input type="radio"/> Enabled (Select to enable tunnel only if failure detected - optional) |
| Fail Method: ⓘ | <input checked="" type="radio"/> Probe Address <input type="radio"/> WAN1 (Select to either use WAN1 status or probe address below - optional) |

Step Four

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

Tunnel Name: (Used to define this site-to-site XOS tunnel)

Tunnel ID: . (Select a unique tunnel ID)

Primary

Tunnel Type: Backup (Enter the primary tunnel name)

Bind To (Select an existing tunnel for binding, see '?' for details)

Weight: (Ratio Of Tunnel Utilization)

Protocol Selection: TCP UDP (Enable UDP to improve responsiveness for certain applications)

Disabled Enabled (Enable file data compression for this tunnel)

Data Compression: (Compression Windowing Adjustment)

Shared Secret Key: (This key must be 16 characters using only numbers and letters)

Encryption Type: (Select an encryption type, if any)

WAN Interface: (Select the outbound interface)

Virtual Address: . . . (Local Virtual Address) . . . (Remote Virtual Address)

Static Dynamic (Is the remote address dynamic or static?)

Remote Edge Device: . . . (Enter the WAN address of the remote Edge device)

Remote Network: . . . (Enter the network address of the remote network)

(Remote network mask)

Client/Hub: Client Side Hub Side (Select this tunnel type)

On Failure: Disabled Enabled (Select to enable tunnel only if failure detected - optional)

Fail Method: Probe Address WAN1 (Select to either use WAN1 status or probe address below - optional)

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="checkbox"/> | m2b_tun1 | wan1 168.0.0.0 | Client | 10.45.20.2 | 192.168.168.0/24 | None | 1 | Disabled | No | DOWN |
| <input type="checkbox"/> | 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

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 199.0.0.0 | 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 199.0.0.0 | Client | 10.45.20.2 | 192.168.168.0/24 | None | 1 | Enabled | Yes | DOWN |
| | m2b_tun2 | wan2 | Client | 10.68.10.2 | 192.168.168.0/24 | m2b_tun1 | 2 | Enabled | Yes | 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.

| Select | Connection | WAN Port | Client/Hub | Remote Device | Remote Addr/Mask | Binding | Session | State | Activated | Status |
|--------|------------|-------------------|------------|---------------|------------------|----------|---------|---------|-----------|--------|
| | m2b_tun1 | wan1 199.0.0.0 | Client | 10.45.20.2 | 192.168.168.0/24 | None | 1 | Enabled | Yes | UP |
| | m2b_tun2 | wan2 | Client | 10.68.10.2 | 192.168.168.0/24 | m2b_tun1 | 2 | Enabled | Yes | UP |

<< Add Tunnel Add Route Start Stop S2SLog Save

Select Delete Restart All Refresh View Params

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 |
|-----------|--------|
| Yes | UP |
| Yes | UP |

This state shows both tunnels UP in load balanced mode.

| Activated | Status |
|-----------|--------|
| Yes | UP |
| 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 |
|-----------|--------|
| Yes | UP |
| Yes | 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 called 3DES. 3DES encryption has long been a standard in the industry and is widely used by the government and banking sector. When setting up a tunnel which will traverse the Internet it is a good idea to enable 3DES encryption in order to provide for some level of protection for the site-to-site data. No encryption is required for tunnels established over a private point-to-point or MPLS connection.


Encryption Type:  (Select an encryption type, if any)

None
3DES (Industry Standard)

Site2Site Compression

If a majority of the data going through the tunnel is non-compressed, i.e. plain text or large database transfers then data compression could be used to increase the transfer rates across the tunnel(s). Data compression is ONLY useful if the data has not already been compressed as the compression aspect does add some latency and if the data is already compressed it actually increases transit times.

Data Compression:  Disabled Enabled (Enable file data compression for this tunnel)

Level 1  (Compression Windowing Adjustment)

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 | Sta |
|--------|------------|-------------------|------------|---------------|------------------|----------|---------|-----|
| | m2b_tun1 | wan1 188.0.0.0 | Client | 10.45.20.2 | 192.168.168.0/24 | None | 1 | |
| | m2b_tun2 | wan2 | Client | 10.88.10.2 | 192.168.168.0/24 | m2b_tun1 | 2 | |

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

Select Delete Restart All Refresh View Params

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: 200 . 200 . 10 . 0 / 24 (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.

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 [Mbits 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)