



Configuration Example

Use a Branch Office VPN for Failover From a Private Network Link

Example configuration files created with — WSM v11.10.1

Revised — 7/22/2015

Use Case

In this configuration example, an organization has networks at two sites and uses a private network link to send traffic between the two networks. To make their network configuration more fault-tolerant, they want to set up a secondary route between the networks to use as a backup if the private network link fails, but they do not want to spend money on a second private network connection. To solve this problem, they can use a branch office VPN with dynamic routing.

This configuration example provides a model of how you could set up your network to automatically fail over to a branch office VPN if a primary private network connection between two sites becomes unavailable. To use the branch office VPN connection for automatic failover, you must enable dynamic routing on the Firebox at each site. You can use any supported dynamic routing protocol (RIP v1, RIP v2, OSPF, or BGP v4).



This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.

Solution Overview

A routing protocol is the method routers use to communicate with each other and share information about the status of network routing tables. On the Firebox, static routes are persistent and do not change, even if the link to the next hop goes down. When you enable dynamic routing, the Firebox automatically updates the routing table based on the status of the connection. When you configure dynamic routing for traffic sent through the private network connection, if the private network connection fails, the Firebox automatically removes that route from the routing table.

After you configure dynamic routing between the two sites, you then configure a branch office VPN tunnel between the two sites on another Firebox interface. As part of the VPN configuration, you enable the global VPN setting **Enable the use of non-default (static or dynamic) routes to determine if IPSec is used**.

How It Works

When the global VPN setting is enabled, the Firebox uses the status of the routing table to decide whether to send traffic through the branch office VPN tunnel.

With this configuration:

- When the private network connection is established between the two sites, the Firebox at each site adds the dynamic route to the routing table. Because the route is present in the routing table, each Firebox sends traffic to the other site over the private connection.
- If the private network connection fails, the Firebox at each site removes that route from the routing table. Because the route is not present in the routing table, each Firebox sends traffic to the other site through the encrypted IPSec branch office VPN tunnel.
- When the private network connection is restored, the dynamic route is added to the routing table at each site, and the two devices automatically begin to send traffic over the private network connection again.

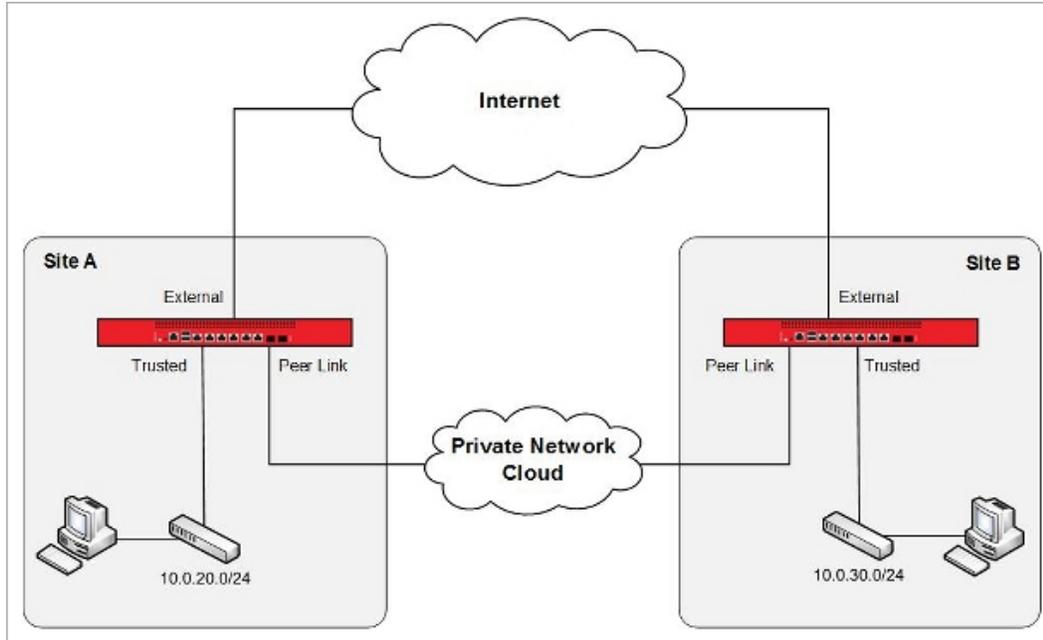
Requirements

For VPN failover to operate correctly, the configuration must meet these requirements:

- The Firebox at each site must use Fireware v11.3.1 or higher.
- The two sites must have a primary connection over a private network link, such as a leased line or MPLS network.
- The primary network connection between the two sites must terminate at the Firebox at each site.
- The trusted and optional networks at each site must use the Firebox as the default gateway.
- Dynamic routing (OSPF, BGP, or RIP) must be enabled on the Firebox devices for the primary private network link between sites. Fireware with a Pro upgrade is required to use OSPF or BGP v4.
- A branch office VPN must be configured between the Firebox devices at each site.
- The **Enable the use of non-default (static or dynamic) routes to determine if IPSec is used** global VPN setting must be enabled on the Firebox devices at both sites.

Network Topology

To configure automatic network failover, the private network link between the two sites must terminate at the Firebox devices at each site. At a high level, this generic network diagram shows the relationship between the networks at the two sites.



In this diagram, the *Private Network Cloud* could represent any one of several possible methods to connect the two sites over a private network. All of these connection types are supported for dynamic failover to a VPN connection.

Point-to-Point Link

In this type of connection, the Firebox devices at the two sites connect directly to each other. Typical examples of this type of connection are fiber optic connection, fiber-to-Ethernet converters, layer 2 VLAN connections, or a leased line with serial-to-Ethernet converters at each end.

Multi-Hop Link

In this type of connection, the Firebox at each site is connected to a router and the routers are connected by point-to-point links. The routers could be managed by the network administrators at each site, or by the service provider. A typical example of this type of connection is a leased line terminated on routers at each site.

MPLS Link

In this type of connection, the Firebox at each site connects to a router on an MPLS network. In this case, the routers are usually owned and managed by the service provider. A typical example of this type of connection is an MPLS or L2TP private network connection.

These connection types are explained more fully in the next section.

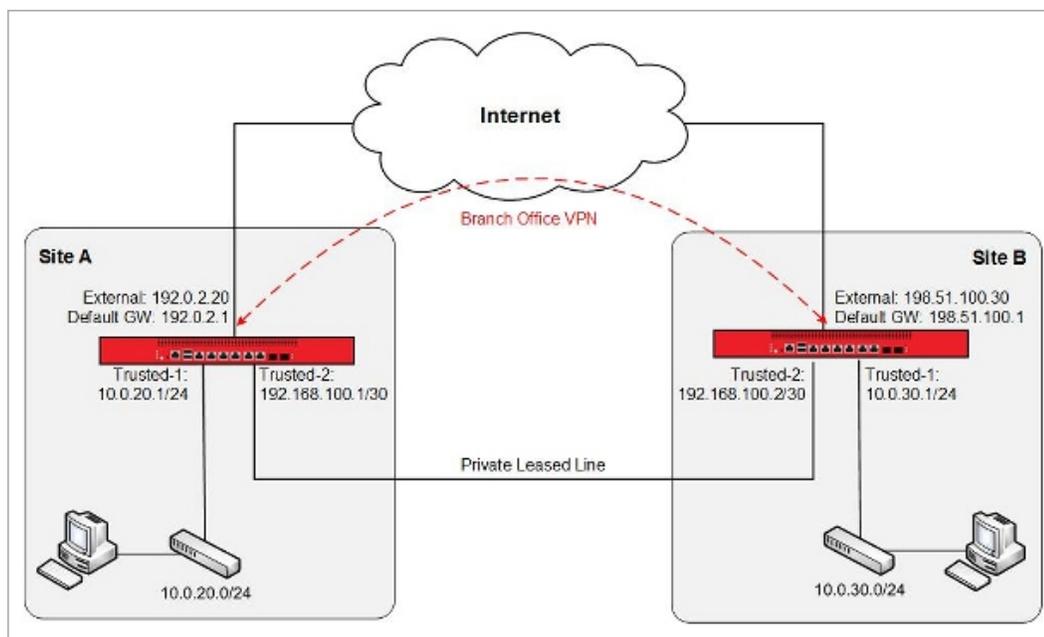
Example Network Topologies

For automatic failover to a VPN to operate correctly, the private network link between the two sites must terminate on a trusted or optional network interface on the Firebox at each site. This interface must be separate from the trusted network.

In this configuration example, we present two specific network topologies to illustrate the supported network connection types: *private network connection over point-to-point link* and *private network connection over multi-hop link or MPLS*. The example configuration files that accompany this document show configuration settings for each private network connection type. For similar topologies that are not supported, see the section [Appendix — Unsupported Network Topologies](#).

Private Network Connection Over Point-to-Point Link

In a point-to-point link, the private network connection between the two sites is a leased line, with a serial-to-Ethernet converter at each end. This point-to-point link connects directly to an interface on each Firebox.



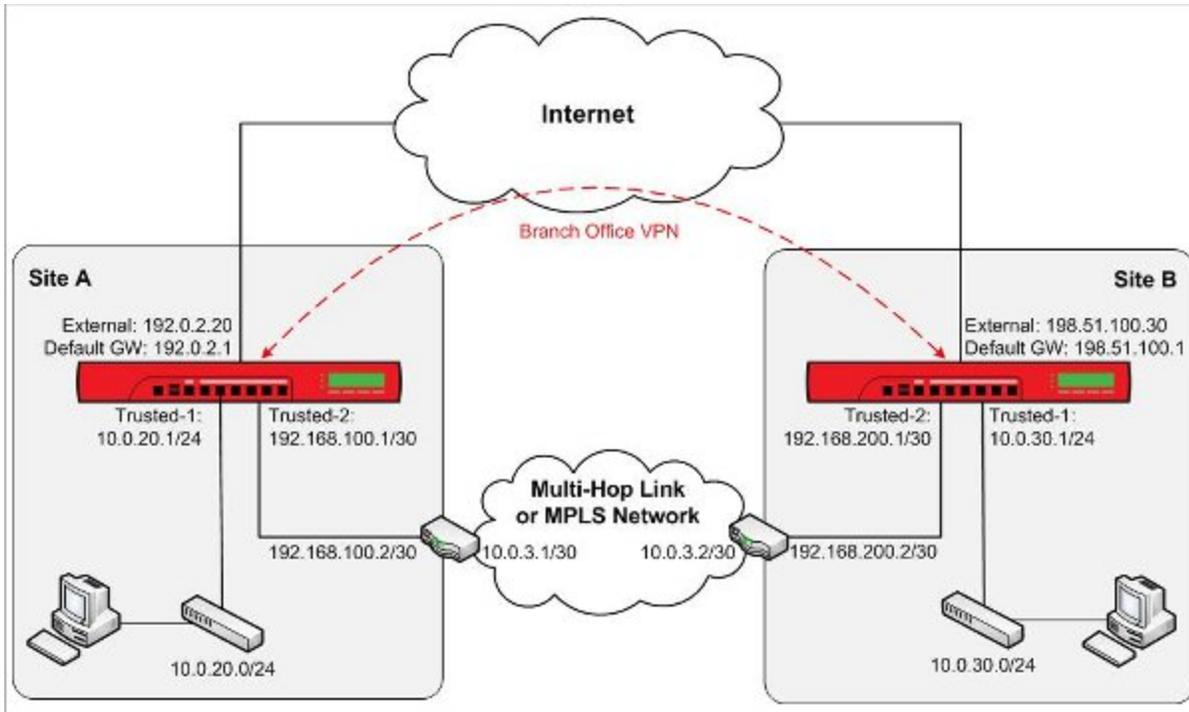
In this network diagram, the Firebox devices at the two sites use these IP addresses:

	Site A	Site B
External interface IP address	192.0.2.20/24	198.51.100.30/24
Default Gateway IP address	192.0.2.1	198.51.100.1
IP address of the Firebox interface connected to the trusted network	10.0.20.1/24	10.0.30.1/24
Trusted network IP address	10.0.20.0/24	10.0.30.0/24
IP address of the Firebox interface connected to the private leased line	192.168.100.1/30	192.168.100.2/30

With this type of connection, there are no routers to configure. Only these addresses are required to enable dynamic routing over the private leased line between the two sites. The recommended dynamic routing protocol for this type of private network topology is OSPF.

Private Network Connection Over Multi-Hop Link or MPLS

If the private network link is a multi-hop link or MPLS network, the Firebox at each site connects to a router configured at the edge of a leased line or MPLS network. In this topology, you must add a static route on each Firebox to define the IP address of the local router on the private network as the next hop to the other Firebox.



In this network diagram, the Firebox devices at the two sites use these IP addresses:

	Site A	Site B
External interface IP address	192.0.2.20/24	198.51.100.30/24
Default gateway IP address	192.0.2.1	198.51.100.1
IP address of the Firebox interface connected to the trusted network	10.0.20.1/24	10.0.30.1/24
Trusted network IP address	10.0.20.0/24	10.0.30.0/24
IP address of the Firebox interface connected to the router	192.168.100.1/30	192.168.200.1/30
LAN IP address of the router connected to the private network link	192.168.100.2/30	192.168.200.2/30
WAN IP address of the router connected to the private network link	10.0.3.1/30	10.0.3.2/30

At each end of the leased line or MPLS network between the two Firebox devices, are routers that can either be managed by the network administrator at each site, or managed by the network service provider. In this configuration, you must set up static routes on each Firebox and on each router to correctly direct the traffic between the two networks.

For the Firebox at Site A to be able to reach the interface of the Firebox at Site B (192.168.200.1/30), you must add static routes to the Firebox and to the router at Site A. For the Firebox at Site B to be able to reach the interface of the Firebox at Site A (192.168.100.1/30), you must add static routes to the Firebox and to the router at Site B. You must also configure static routes on the routers at each site to allow the traffic between the trusted networks at each site.



If you configure dynamic routing between each Firebox and the local MPLS router, you do not have to add static routes to the MPLS routers. For this configuration example, we assume you use static routing between the Firebox and the local router.

The static routes for the Firebox and the router at each site are:

Static Routes at Site A

	Firebox at Site A	Site A Router
Route to Site B Firebox	Network: 192.168.200.0/30 Next Hop: 192.168.100.2	Network: 192.168.200.0/30 Next Hop: 10.0.3.2
Route to Site A trusted network		Network: 10.0.20.0/24 Next Hop: 192.168.100.1
Route to Site B trusted network		Network: 10.0.30.0/24 Next Hop: 10.0.3.2

Static Routes at Site B

	Firebox at Site B	Site B Router
Route to Site A Firebox	Network: 192.168.100.0/30 Next Hop: 192.168.200.2	Network: 192.168.100.0/30 Next Hop: 10.0.3.1
Route to Site A trusted network		Network: 10.0.20.0/24 Next Hop: 10.0.3.1
Route to Site B trusted network		Network: 10.0.30.0/24 Next Hop: 192.168.200.1

After you configure the static routes and verify that the devices can contact each other, you can configure dynamic routing across the private network link. The recommended dynamic routing protocol for this configuration is BGP.

In this example configuration, dynamic routing occurs only between the Firebox devices. The routers connected to the private network link do not use dynamic routing.

Example Configuration Files

For your reference, we have included six example configuration files with this document. To examine the details of the example configuration files, you can open them with Policy Manager. Make sure to use Policy Manager v11.3.1 or higher, because the VPN failover option is not supported in earlier versions of Policy Manager.

The example configuration files show the configurations for Site A and Site B for each of the three dynamic routing configuration protocols. Only the BGP configuration files include the static routes required for a multi-hop link or an MPLS private network connection.

Description	Configuration Filename
BGP configuration	BGP-Site-A-multi-hop-with-VPN.xml BGP-Site-B-multi-hop-with-VPN.xml
OSPF configuration	OSPF-Site-A-with-VPN.xml OSPF-Site-B-with-VPN.xml
RIP configuration	RIP-Site-A-with-VPN.xml RIP-Site B-with-VPN.xml

The settings configured in the example configuration files are described in the subsequent sections.

Dynamic Routing Configuration

After you have established the primary connection between the two networks over the private network, you must enable dynamic routing between the Firebox devices at each site. You can use any supported dynamic routing protocol (RIP v1, RIP v2, OSPF, or BGP v4), but we recommend you use these dynamic routing protocols:

- For point-to-point link — OSPF
- For multi-hop link or MPLS connection — BGP

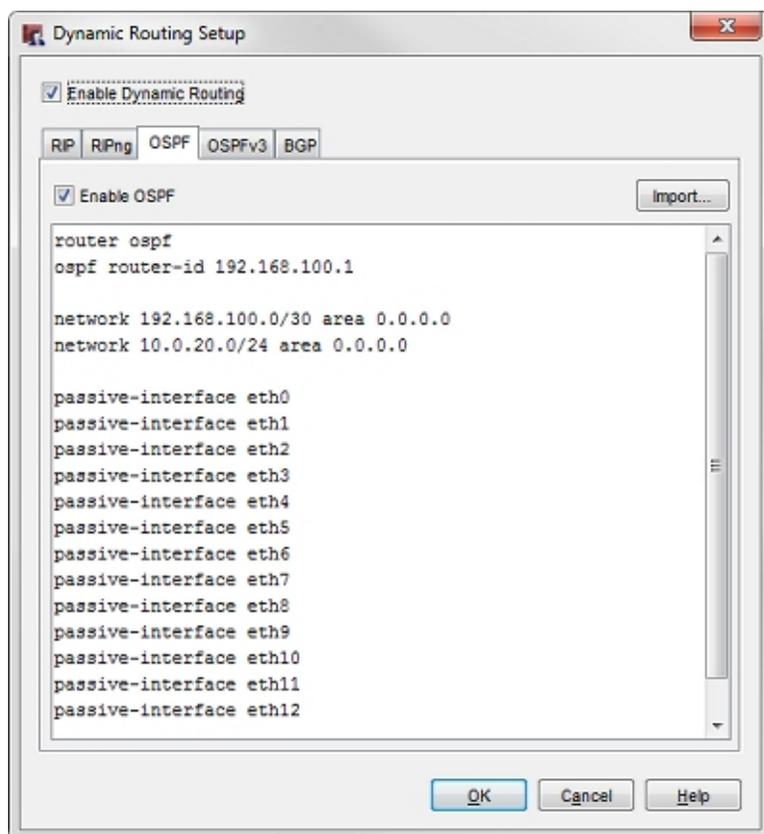
Each example configuration file contains a dynamic routing configuration that uses the IP addresses from the topology diagrams in this document. The dynamic routing configuration between the two Firebox devices is the same, regardless of the type of primary private network connection. To see the dynamic routing configuration for the two sites in this example, use Policy Manager to open the example files for the relevant dynamic routing protocols.

Dynamic Routing Settings

To see the settings for dynamic routing:

1. In Policy Manager, select **Network > Dynamic Routing**.
2. Select the **RIP**, **OSPF** or **BGP** tab.

For example, the dynamic routing settings in the Site A OSPF example configuration file look like this:



In the example configuration file, eth13 is the interface that connects to the private network connection.

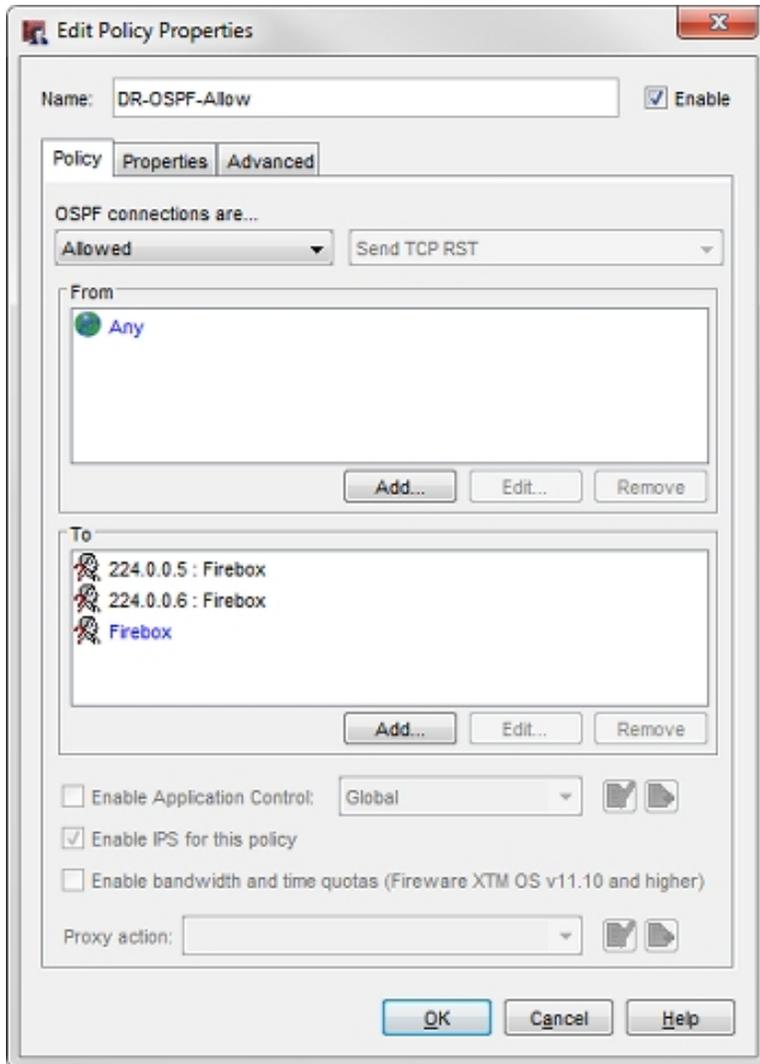
Dynamic Routing Policy

When you enable a dynamic routing protocol, a policy is required to allow the traffic. Policy Manager automatically creates the required policy.

To see the dynamic routing policy:

1. In Policy Manager, open one of the example configuration files.
2. Double-click the **DR-RIP-Allow**, **DR-OSPF-Allow**, or **DR-BGP-Allow** policy to edit it.

For example, the DR-OSPF-Allow policy in the Site A OSPF example configuration looks like this:



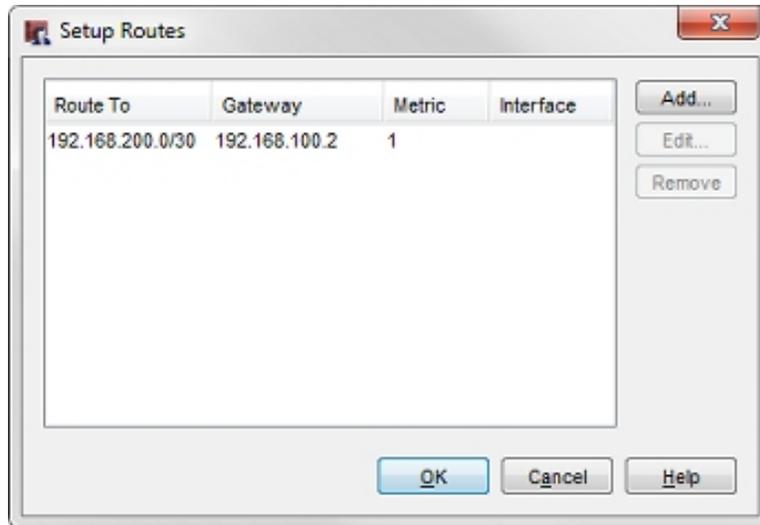
Static Routes

Because BGP is the recommended dynamic routing protocol to use with a multi-hop link or MPLS private network connection, the BGP example configuration files include the required static routes for the multi-hop link or MPLS topology.

To see the static route configuration:

1. In Policy Manager, open one of the BGP example configuration files.
2. Select **Network > Routes**.

For example, the static route in the BGP example configuration file for Site A looks like this:



VPN Configuration

Each of the example configuration files contains a branch office gateway and a branch office tunnel that are configured to match any of the network diagrams presented in this use case. The gateway and tunnel settings for each site are the same, regardless of the dynamic routing protocol, or the type of private network connection between the two sites. You can open any of the Site A or Site B example configuration files to see these settings.

VPN Settings at Site A

The VPN Gateway settings at Site A are available in any of the example configuration files for Site A.

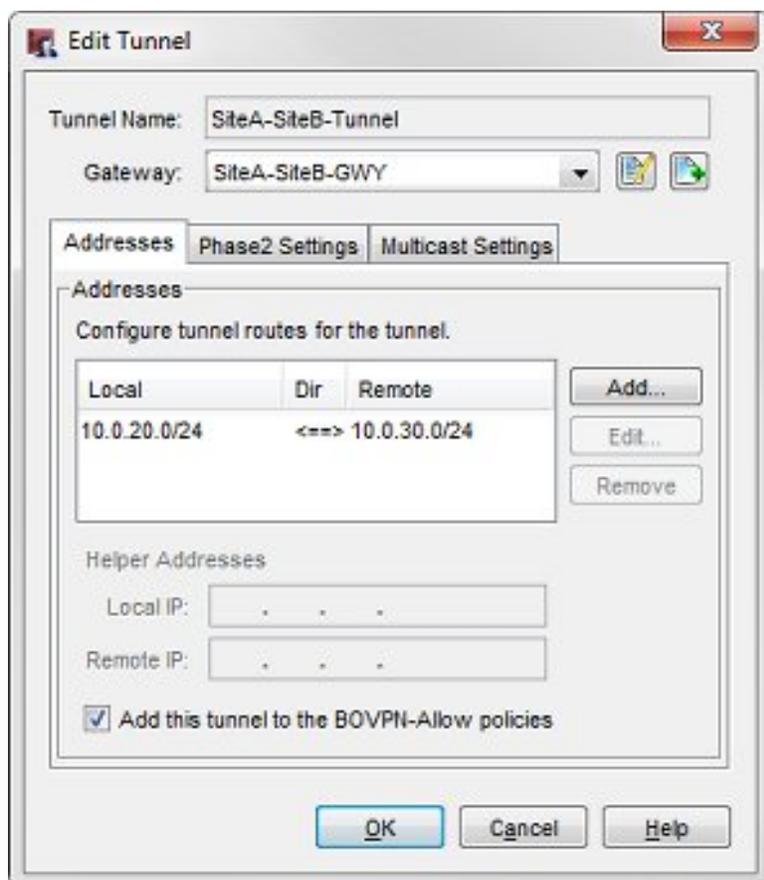
To see the gateway settings:

1. Select **VPN > Branch Office Gateways**.
2. Select the gateway name, **SiteA-SiteB-GWY**. Click **Edit**.

To see the tunnel settings:

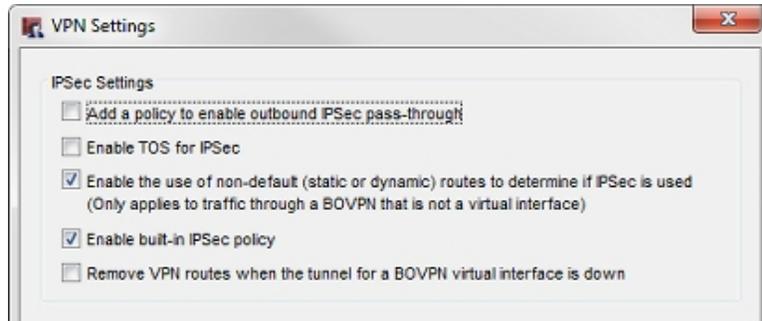
1. Select **VPN > Branch Office Tunnels**.
2. Select the tunnel name, **SiteA-SiteB-Tunnel**. Click **Edit**.

For example, the tunnel in the example configuration file for Site A looks like this:



To see the VPN failover setting:

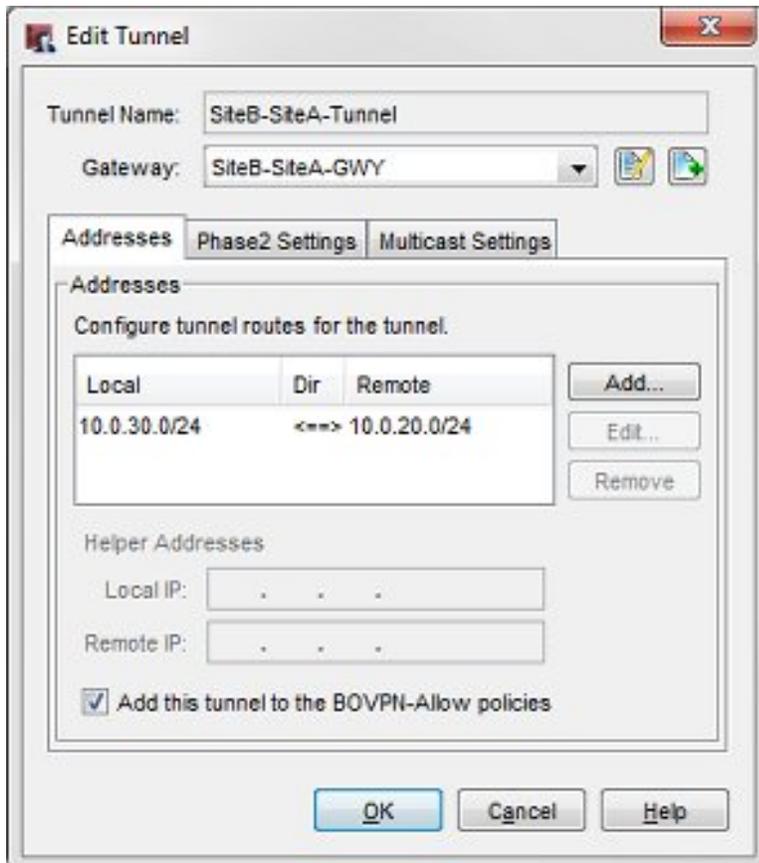
1. Select **VPN > VPN Settings**.
2. The **Enable the use of non-default (static or dynamic) routes to determine if IPSec is used** check box is selected.



This check box enables the automatic failover to the VPN based on dynamic changes to the routing table.

VPN Settings at Site B

The VPN Gateway settings at Site B are available in any of the example configuration files for Site B. To see the gateway, tunnel, and VPN failover settings for Site B, repeat the same steps you completed for Site A.



Conclusion

This configuration example demonstrates one method you can use to configure dynamic routing over a private link between two sites, and how to configure the Firebox devices at each site for automatic failover from the private network link to a branch office VPN. When you use this type of configuration, if the private network link route fails, a packet between the two networks can automatically use the VPN tunnel to get to its destination.

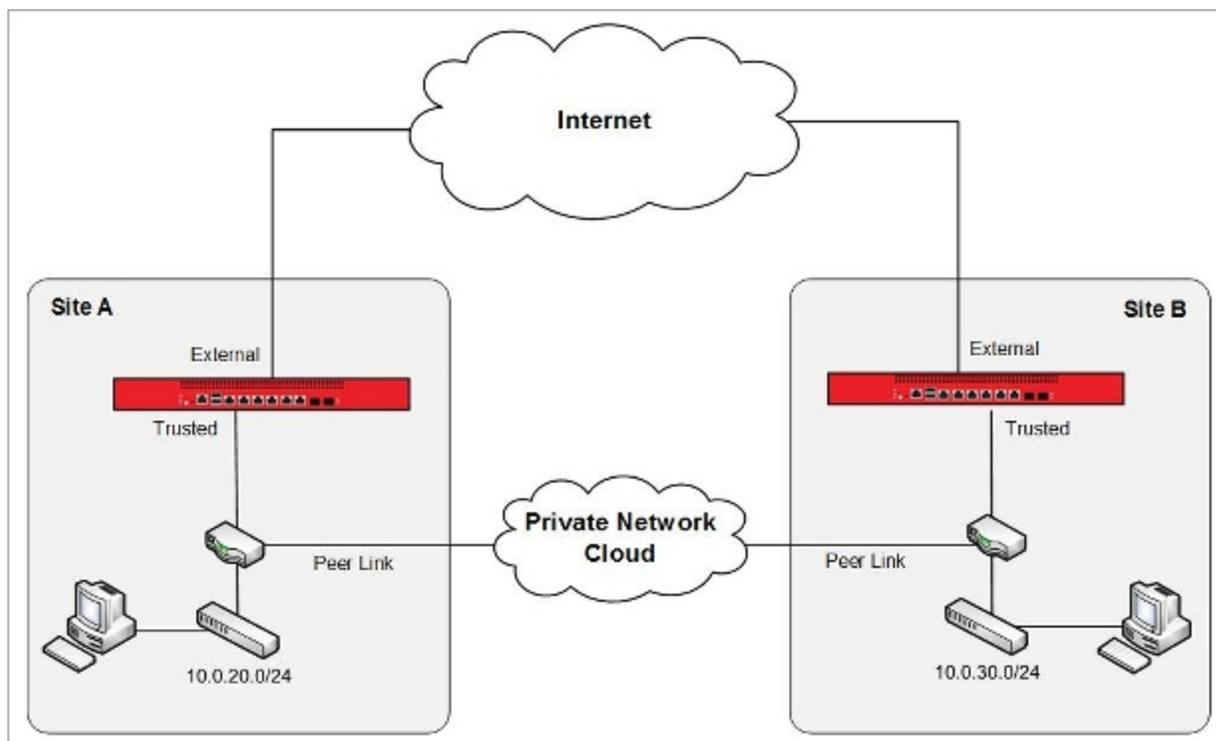
For more information about dynamic routing and branch office VPNs, see the *Fireware Help*.

Appendix — Unsupported Network Topologies

This section illustrates two network topologies that are not supported for this example.

Topology 1

The router that connects to the private network cloud is also the default gateway for the trusted network.

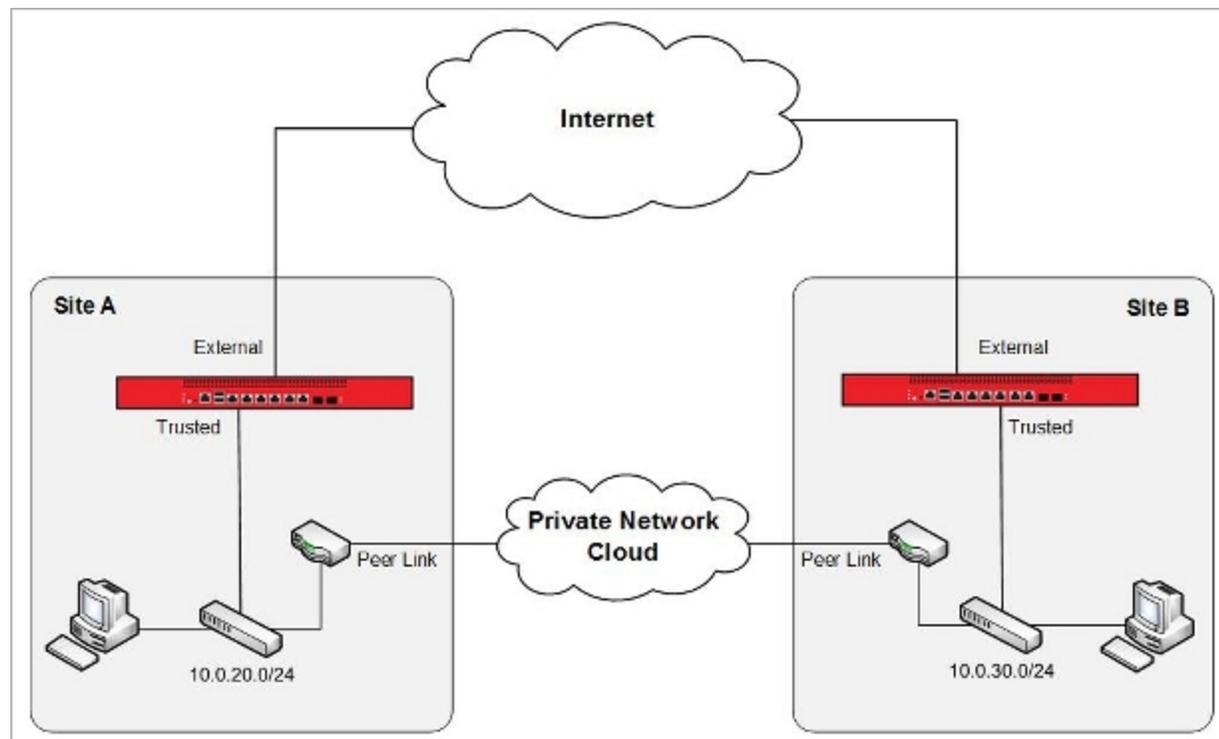


In this topology, the default gateway for the trusted network at each site is the router that connects each site. Because of this, the Firebox cannot control routing between the two networks. You can, however, configure the routers that connect the two sites for dynamic routing and to fail over to a route through the VPN tunnel on the Firebox. This network topology method is out of the scope of this configuration example because to do this you must configure that type of failover on the router.

There is also a possible security concern with this topology: because there is no firewall on the private network link between the two sites, any security compromise at one site can affect both sites.

Topology 2

The router that connects to the private network cloud connects directly to the trusted network, but is not the default gateway for the trusted network.



In this topology, the Firebox cannot control network failover between the two sites because there is not a single ingress and egress point at each site. We always recommend that you configure the Firebox as the single ingress and egress point on each network.

The larger problem with this topology is that it can create asymmetric routes between the two sites. Connections between the two sites can fail regardless of whether TCP SYN checking is enabled, because the firewall at each site might see only one side of the TCP handshake.

Asymmetric routing can occur because:

1. Packets sent from a computer at Site A to a computer at Site B are routed through the default gateway at Site A (the Site A Firebox). The packets are then routed over the peer link to the computer at Site B. These packets do not go through the Site B Firebox.
2. The returned packets from the computer at Site B are routed through the default gateway at Site B (the Site B Firebox). The packets are then routed over the peer link to the computer at Site A. These packets do not go through the Site A Firebox.

Even without dynamic routing or failover to a VPN, this network configuration can cause routing problems and is not recommended.

About this Configuration Example

This configuration example is provided as a guide. Additional configuration settings could be necessary, or more appropriate, for your network environment.

For complete product documentation, see the *Fireware Help* on the WatchGuard website at: <http://www.watchguard.com/help/documentation/>.

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Copyright, Trademark, and Patent Information

Copyright © 1998-2015 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at: <http://www.watchguard.com/help/documentation/>.

About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard Firebox line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit www.watchguard.com.

Address

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

Support

www.watchguard.com/support
U.S. and Canada +877.232.3531
All Other Countries +1.206.521.3575

Sales

U.S. and Canada +1.800.734.9905
All Other Countries +1.206.613.0895