

# Decentralized Branch Office VPN Architecture (Full Mesh)

*Example configuration files created with — WSM v11.4.1*

*Revised — 6/28/2011*

---

## Use Case

---

In this configuration example, an organization has multiple sites of different sizes and wants to establish secure VPN connections between all the sites. The organization wants the connection between any two sites to be independent of connectivity to a third site. They could have resources distributed among multiple sites, or business processes that are a good match for a decentralized architecture.

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

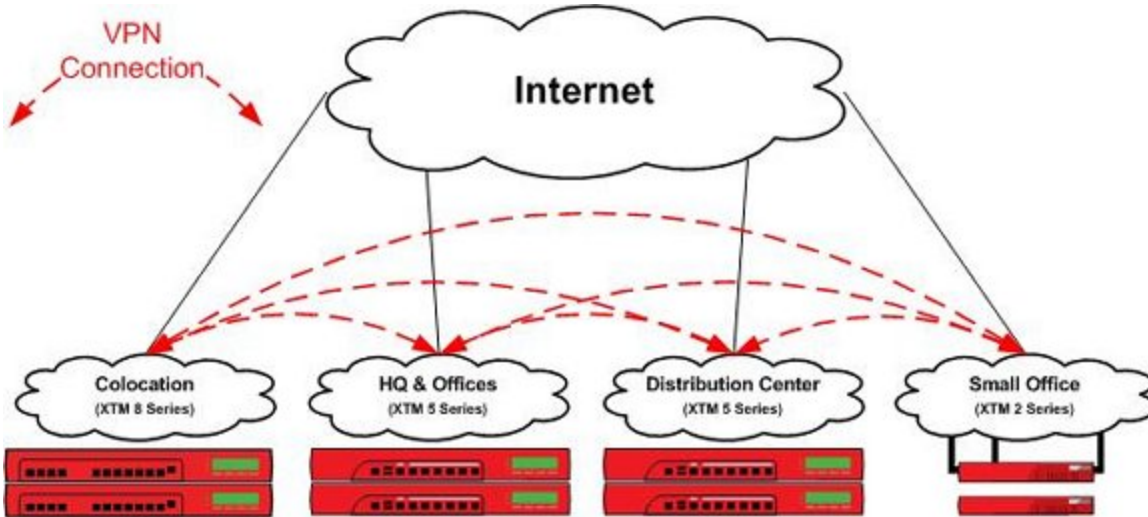
## Solution Overview

---

In a decentralized VPN configuration, also referred to as full mesh, each site has VPN tunnels established to all other sites. This configuration offers resiliency, because a failure at a single site impacts only the services directly dependent on it.

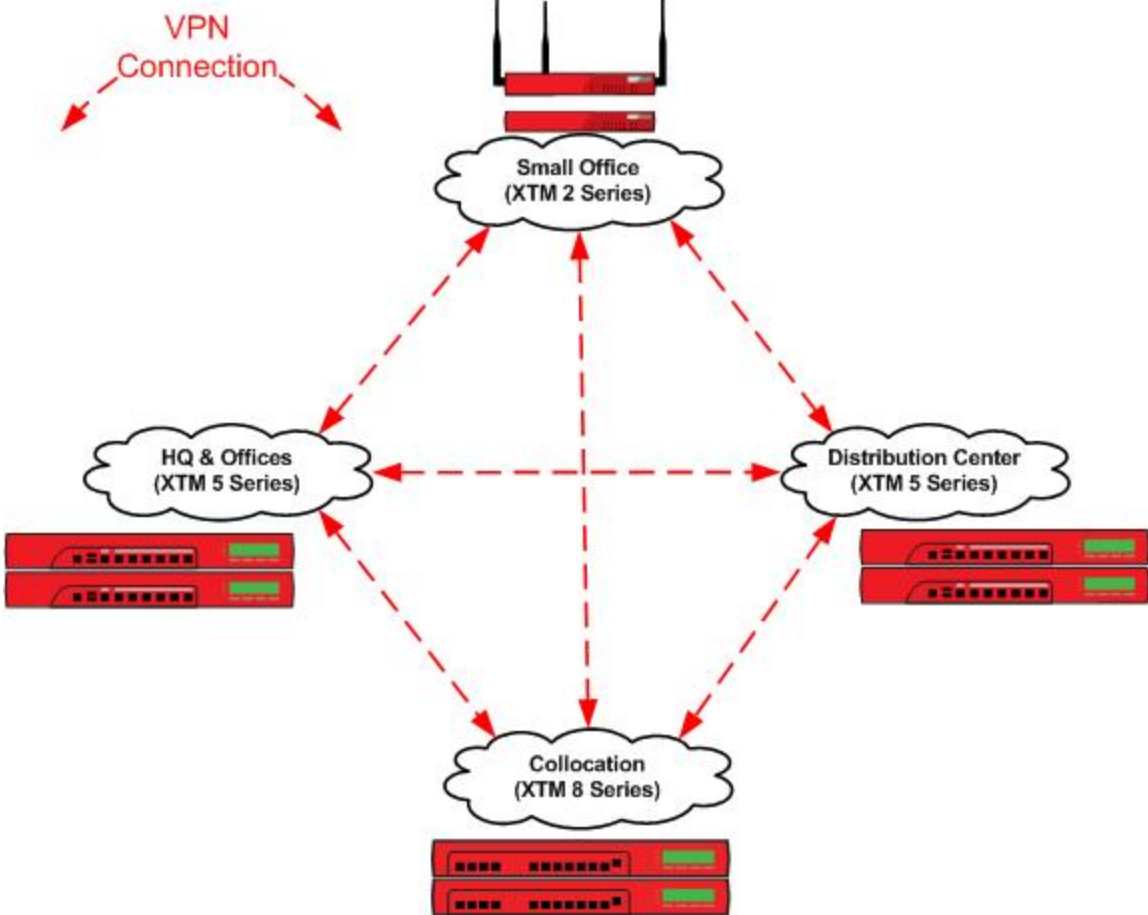
Heavy reliance is put on any location with a unique resource, which creates a need for reliable connectivity at any such site. As additional remote locations are established, the capacity of any site with a unique resource may also need to expand. If resources are located at a single site, a centralized architecture could be a better solution.

---



**How It Works**

The XTM device at each site establishes a VPN connection to the XTM device at every other site.



---

## Requirements

---

### *Reliable connectivity*

While this is a fault-tolerant design, sites that host resources unique to their location should have reliable connectivity appropriate for the resources they host.

### *Sufficient bandwidth*

Due to encryption and encapsulation overhead, VPN bandwidth is measured at less than line speed.

### *An XTM device appropriate for each location*

XTM device capabilities vary by model. For VPN configurations, you must consider the VPN throughput and tunnel capacity of each model. Network environment, configuration options, and other factors can also help you determine the most appropriate model for each site.

VPN throughput is the amount of data passed over the VPN per second.

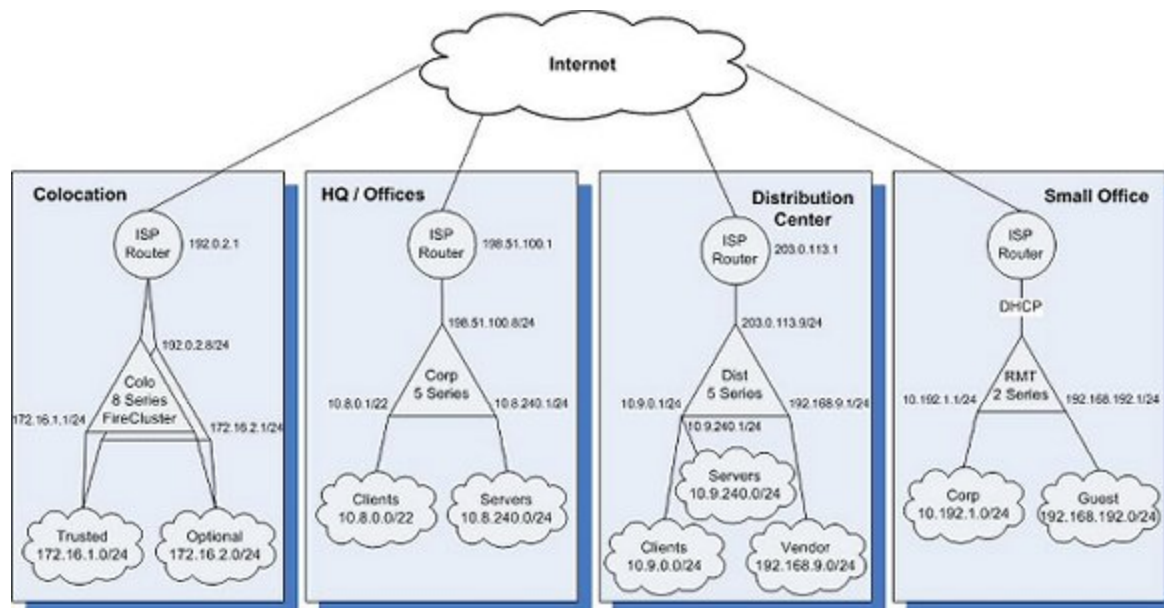
VPN tunnel count is determined by the number of connected networks (as configured in tunnel routes). For offices, this is generally the number of local networks multiplied by the number of remote networks.

For more information about VPN throughput and branch office VPN tunnel capacity available for each XTM model, refer to the product datasheets: <http://www.watchguard.com/products/resources/datasheets.asp>.

## Configuration Example

To illustrate this use case we present an example of an organization that has four locations: a colocation facility (Colo), a corporate office (Corp), a distribution center (Dist), and a small office (RMT). You can also scale up this solution to support additional offices, distribution centers, and small offices.

### Topology



The IP addresses for the sites in this configuration:

	Colo	Corp	Dist	RMT
External interface IP address	192.0.2.8/24	198.51.100.8/24	203.0.113.9/24	DHCP
Default gateway IP address	192.0.2.1	198.51.100.1	203.0.113.1	DHCP
Private network allocated to site	172.16.0.0/16	10.8.0.0/16	10.9.0.0/16	10.192.1.0/24
Un-routed network allocated to site	N/A	N/A	192.168.9.0/24	192.168.192.0/24

## Example Configuration Files

For your reference, we have included example configuration files with this document. To examine the details of the example configuration files, you can open them with Policy Manager. There are four example configuration files, one for each location in the example.

Configuration Filename	Description
De-Centralized-Colo.xml	Central location for the VPNs (the colocation facility)
De-Centralized-Corp.xml	A corporate office
De-Centralized-Dist.xml	A distribution center
De-Centralized-RMT.xml	A small office

The details of each configuration file are described in the next section.

## Configuration Explained

### Branch Office VPN Gateways and Tunnels

The example configurations contain branch office gateways and branch office tunnels defined for VPN connections between each site. Each site has three branch office VPN gateways and three branch office VPN tunnels configured.

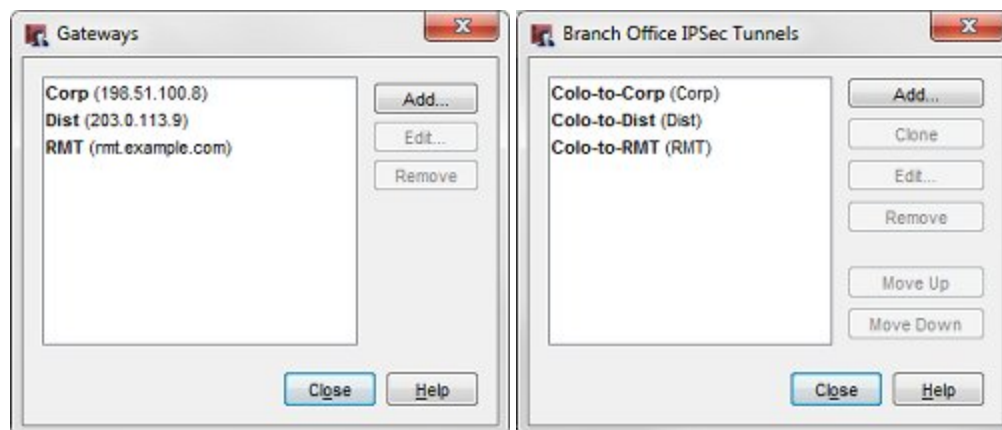
To see the branch office VPN gateways:

1. Start Policy Manager for the XTM device.
2. Select **VPN > Branch Office Gateways**.

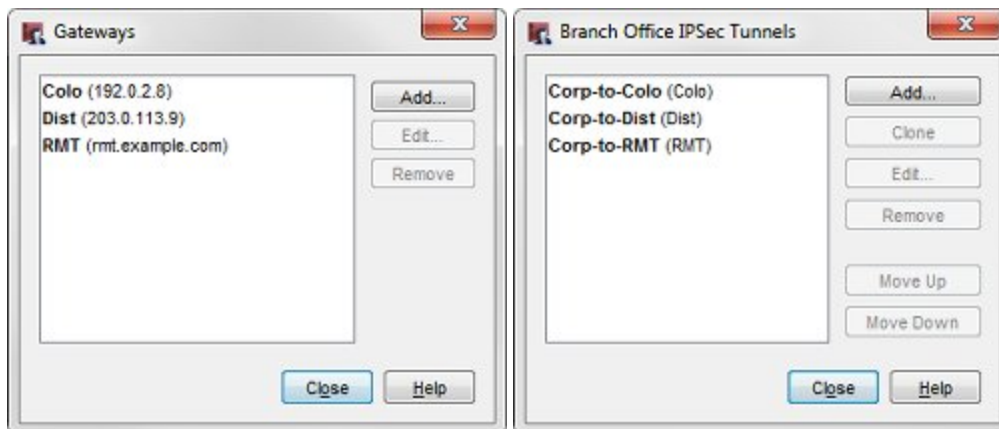
To see the branch office VPN tunnels:

1. Start in Policy Manager for the XTM device.
2. Select **VPN > Branch Office Tunnels**.

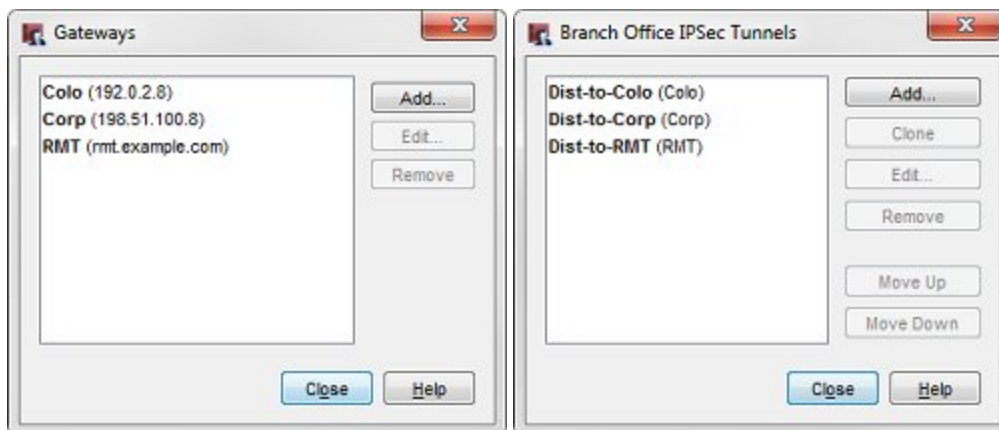
### Configuration at the Colocation Site (Colo)



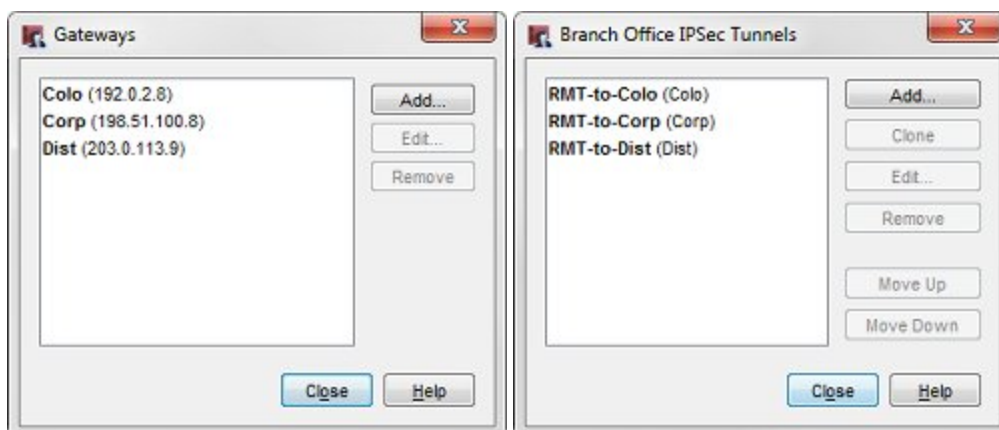
### Configuration at the HQ Corporate Network (Corp)



### Configuration at the Distribution Center (Dist)

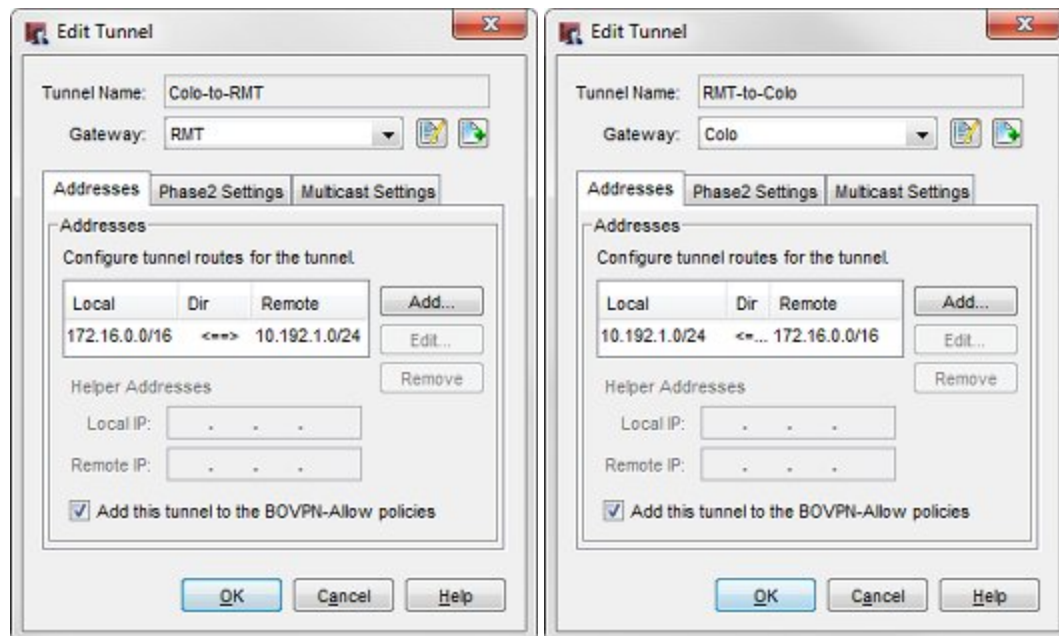


### Configuration at the Small Office (RMT)



In the example configuration files, each tunnel is named to represent the local and remote networks it manages. The identifier in parentheses is the gateway used by the tunnel.

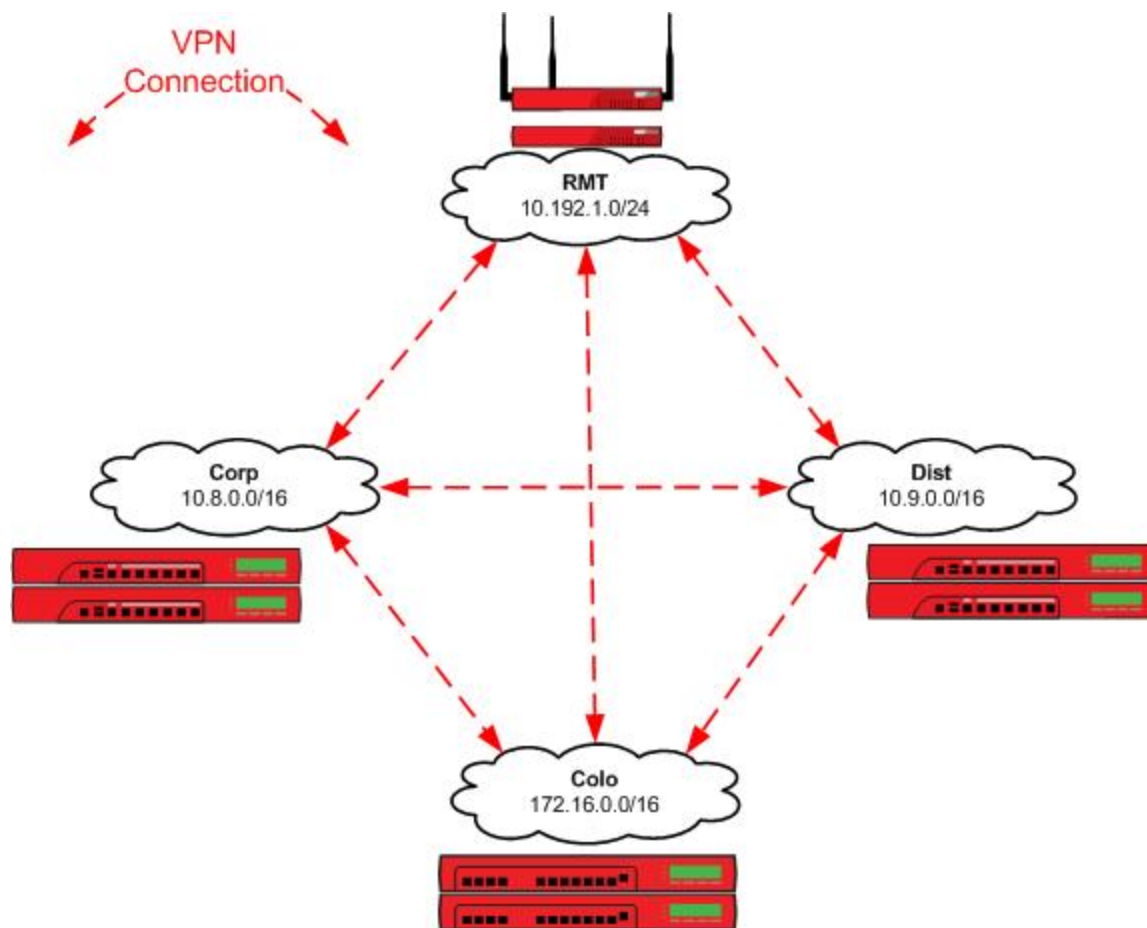
The tunnel routes have been defined to use the subnets allocated to each site, not the individual networks defined in the site. In this configuration, the small office (RMT) only requires three tunnel routes (not six tunnel routes) to reach the trusted and optional networks at each of the other sites. Any new networks in this allocation that is established at each site are routed over the existing Branch Office VPN. For more granular control of VPN tunnels, you can define each individual network at a cost of additional tunnel routes and administration time.



For example, the tunnel routes **Colo-to-RMT** and **RMT-to-Colo** use the subnet IP address 172.16.0.0/16 as the address of the Colo network. This enables these tunnels to manage all traffic between the small office (RMT) network and the Colo trusted (172.16.1.0) and optional (172.16.2.0) networks.

When you configure tunnel routes, it is important to remember that the local-remote pairs are defined relative to the tunnel being configured, not necessarily the network as a whole.

The subsequent figure represents the tunnel routes configured for each VPN connection.



## Conclusion

---

This configuration example demonstrates how to configure tunnel switching in full mesh network topology, to send VPN traffic between sites that are directly connected to each other. The VPN connection between any two sites does not rely on connectivity to a third site. This type of configuration can be a good fit for an organization that has resources distributed among multiple sites, or business processes that fit a decentralized architecture. The configuration described here can scale up to support additional sites.

This configuration example also shows how to use subnet IP addresses in the tunnel route configuration to reduce the number of tunnels you must configure to connect private networks at each site.

For more information about how to configure branch office VPNs, see the *Fireware XTM WatchGuard System Manager Help*.

## 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 XTM WatchGuard System Manager Help* or *Fireware XTM Web UI Help* on the WatchGuard web site 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 © 1998-2011 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 XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new 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](http://www.watchguard.com).

### Address

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### Support

[www.watchguard.com/support](http://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

