



Technical Brief

Ensure Network Uptime: High Availability with XTM FireCluster

August 2010

DOWNTIME CAN SPELL DISASTER

Network downtime is expensive for businesses in today's 24/7 global economy. Any malfunctions in the company's IT network can lead to costly delays in mission-critical workflows, including production, communications, order processing, file transfers, accounts payable/receivable, and reporting.

Probably no single feature in the network's security topology does more to protect business continuity and prevent damaging delays than implementing a high availability pairing of security appliances, particularly when clustering capabilities are included.

THE WATCHGUARD® SOLUTION: FIRECLUSTER

High Availability – the ability to configure two firewalls to be installed and used in a failover configuration – provides the redundancy necessary to ensure maximum network uptime. Clustering refers to the linking of two devices that then function as a single logical unit for more processing power and greater ease of use.

WatchGuard's innovative high availability/clustering function, called FireCluster, is a component of the Pro version of the Fireware XTM operating system. FireCluster allows a business to add an additional, identical XTM network security appliance for scalability and redundancy. When you enable FireCluster, you manage and monitor the two devices in the cluster as a single device.

Active/Passive vs. Active/Active

As flexible as it is reliable, FireCluster allows IT administrators to choose to configure their high availability pair in active/passive mode or in active/active.

- To add redundancy, choose an active/passive cluster.
- To add both redundancy and load sharing to the network, select an active/active cluster.

The advantages of using active/passive are lower cost and a constant level of performance across failover events. An active/passive installation does not require subscriptions and upgrades to be purchased for both machines; active/active high availability does. Also, some business requirements demand that both devices not be active at the same time to ensure equivalent failover capacity.

WatchGuard products that support FireCluster

FireCluster functionality is one of the features of WatchGuard's powerful Fireware XTM Pro operating system. This Pro version of the Fireware XTM OS comes with all XTM 8 Series and 10 Series appliances, and is a simple license-key upgrade for XTM 5 Series appliances.*

*WatchGuard XTM 2 Series appliances do not support High Availability or FireCluster capabilities.

FIRECLUSTER OVERVIEW

About FireCluster

FireCluster is designed to deliver redundancy (active/passive) and load sharing and scalability (active/active) with as little additional administrative overhead as possible. Configuration, monitoring, and logging of FireCluster are all designed to give the administrator the necessary control and visibility to manage the cluster without imposing a burden on routine activities.

In a FireCluster, one device is the cluster master and the other device is the backup master. The backup master uses the primary cluster interface to synchronize connection and session information with the master. If the primary cluster interface fails or is disconnected, the backup master uses the backup cluster interface to communicate with the cluster master. Ideally, the IT administrator configures both a primary cluster interface and a backup cluster interface. This helps to make sure that if a failover occurs on the master, the backup has all the necessary information to become the new cluster master, and can transfer connections and sessions appropriately.

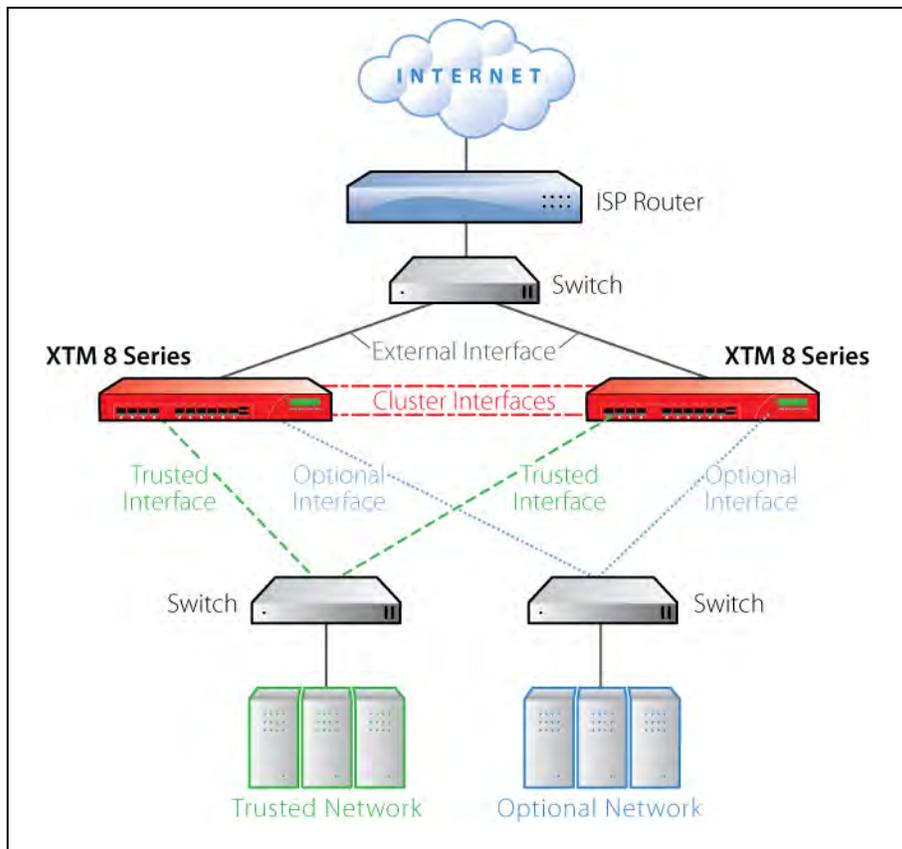


Figure 1: Sample FireCluster Interfaces

Events that trigger a failover

There are three types of events that can trigger a failover.

- **Monitored interface link down on the cluster master**
A failover starts if a monitored interface on the cluster master is unable to send or receive traffic. FireCluster monitors the link status of all enabled interfaces. You can see the list of monitored interfaces in the FireCluster configuration in Policy Manager, which is part of the WatchGuard XTM management console.
- **Cluster master device not fully functional**
A failover starts if a software malfunction or hardware failure is detected on the cluster master, or if a critical process fails on the cluster master.
- **Cluster receives the Failover Master command**
IT administrators can use a tool in the management console to force a failover from the cluster master to the backup master. This may be useful in order to test new software installations or configuration changes in a production environment.

What happens when a failover occurs

The FireCluster failover process is basically the same for an active/active cluster and active/passive cluster. When a failover of the cluster master occurs, the backup master becomes the cluster master. Then the original cluster master reboots and rejoins the cluster as the backup master. With both types of clusters, each cluster member maintains state and session information at all times. When failover occurs, the packet filter connections, BOVPN tunnels, and user sessions from the failed device fail over automatically to the other device in the cluster.

In an active/active cluster, the backup master shares the load of handling connections and user sessions. If the cluster master detects that the backup master has failed, either because a monitored interface link is down, or due to a software malfunction or hardware failure, the network traffic handled by the backup master automatically fails over to the cluster master.

- **In an active/active cluster**
If the backup master fails, proxy connections and Mobile VPN connections can be interrupted, as described in Table 1 at the end of the document.
- **In an active/passive cluster**
If the backup master fails, there is no interruption of connections or sessions because nothing is assigned to the backup master. (This is not technically a failover.)

When FireCluster is enabled, XTM devices continue to support:

- Secondary networks on external, trusted, or optional interfaces
- Multi-WAN connections (Limitation: a multi-WAN failover caused by a failed connection to a link monitor host does not trigger FireCluster failover. FireCluster failover occurs only when the physical interface is down or does not respond.)
- VLANs

When an active cluster member fails, the cluster seamlessly fails over and maintains:

- Packet filter connections
- BOVPN tunnels
- User sessions

These connections may be disconnected when a failover event occurs:

- Proxy connections
- Mobile VPN with PPTP

- Mobile VPN with IPsec
- Mobile VPN with SSL

Mobile VPN users may need to manually restart the VPN connection after a failover.

CONFIGURING AND MANAGING FIRECLUSTER

To use the FireCluster feature, you must install the same version of Fireware XTM Pro on each device that will be in the cluster. The FireCluster Setup wizard streamlines the configuration process, although IT administrators can also choose to configure FireCluster manually. See Table 2 for network configuration comparisons.

Note: XTM appliances come with multiple management tools, including scriptable command line interface, web UI, and centralized console. FireCluster is managed using the WatchGuard System Manager centralized console, which provides easy-to-use tools to set configurations, policies, and maintenance.

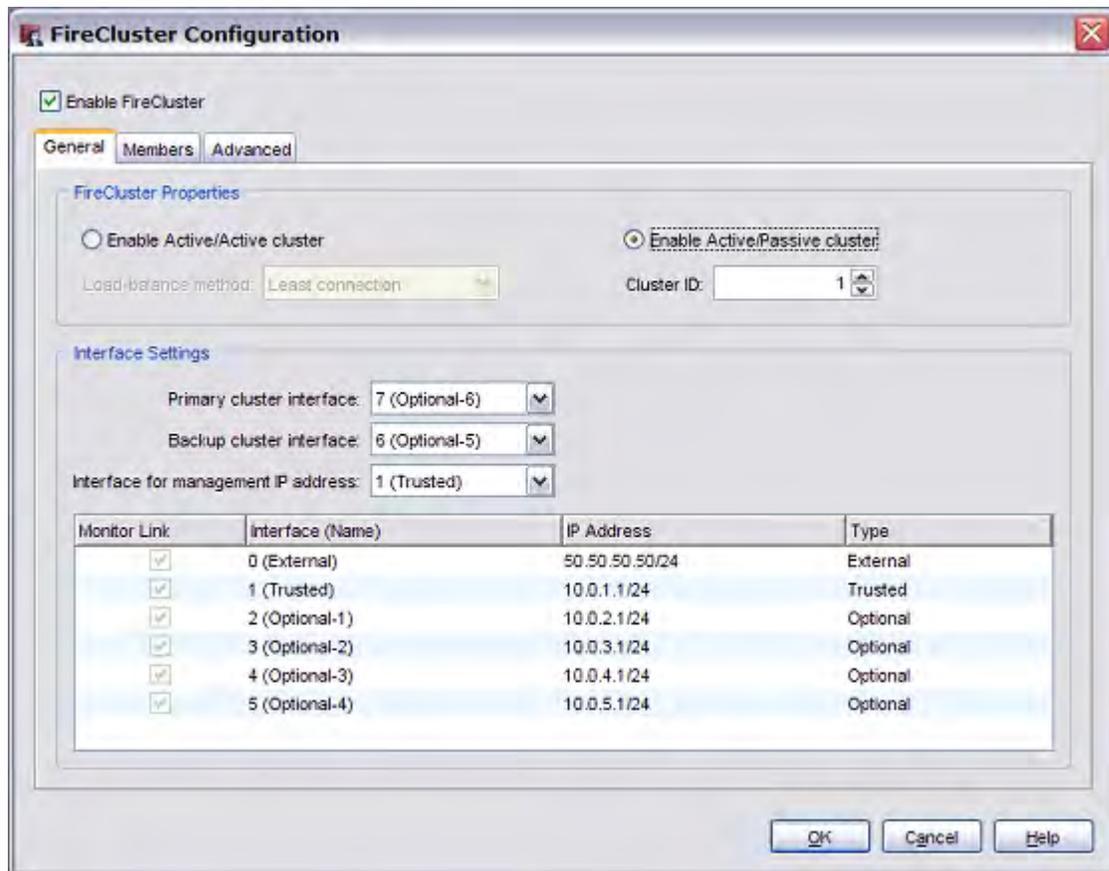


Figure 2: FireCluster Configuration dialog box

IT administrators use the IP address of the trusted interface to monitor and manage the cluster. When they monitor the cluster in the XTM device’s management console, they see an aggregated view of the devices in the cluster and view the status of the cluster members as if the cluster were one device.

Switch and router requirements

- **In an active/active FireCluster configuration**
Network interfaces for the cluster use multicast MAC addresses for all interfaces that send network traffic. Before enabling an active/active FireCluster, the IT administrator needs to make sure that network routers and other devices are configured to properly route traffic to and from the multicast MAC addresses.
- **In an active/passive FireCluster configuration**
The above step is not necessary because an active/passive cluster does not use multicast MAC addresses.

For information on network device interruption in active/active FireCluster, see www.watchguard.com/help and click the link for *Fireware XTM WSM Help*, then click the link in the left column for *FireCluster*.

WHAT FIRECLUSTER MEANS FOR SUBSCRIPTIONS AND UPGRADES

When you enable a FireCluster, the following subscription services and upgrades activated for cluster members must be considered.

- **BOVPN and Mobile VPN upgrades**
Active/Active mode — Licenses for Branch Office VPN and Mobile VPN are aggregated for devices configured as a FireCluster. If you purchase additional BOVPN or Mobile VPN licenses for each device in a cluster, that additional capacity is shared between the devices in the cluster.
Active/Passive mode — In this mode, licenses for Branch Office and Mobile VPN are *not* aggregated for devices configured as a FireCluster. The active device uses the highest capacity Branch Office and Mobile VPN activated for either device. If you purchase additional BOVPN or Mobile VPN licenses for either device in a cluster, the additional capacity is used by the active device.
- **LiveSecurity subscriptions for support and maintenance**
Each device in the configuration must have its own subscription to LiveSecurity Service and the subscriptions must be at the same level. (Example: two LiveSecurity Plus subscriptions).
- **Security service subscriptions**
Subscriptions include WebBlocker, Gateway AntiVirus, spamBlocker, Reputation Enabled Defense, and Intrusion Prevention Service. Subscriptions operate differently for an active/active cluster and an active/passive cluster.
Active/Active You must have the same subscription services enabled in the feature keys for both devices. Each cluster member applies the services from its own feature key.
Active/Passive You must enable the subscription services in the feature key for only one cluster member. The active cluster member uses the subscription services that are active in the feature key of either cluster member.

See Table 3 for a comparison of licensing requirements in active/active and active/passive FireCluster.

NEXT STEPS

WatchGuard's FireCluster can help companies that seek to ensure maximum network uptime and predictable performance and capacity. The flexibility of active/active or active/passive configuration allows the administrator to choose the configuration that best matches the needs of the business.

To learn more about WatchGuard's family of XTM security appliances and find the solution that is right for you, contact your authorized WatchGuard reseller, visit www.watchguard.com, or call us directly at 1.800.734.9905 (North America) or +1.206.613.0895 (international).

Table 1: Impact of a FireCluster failover event

Connection/session type	Impact of a failover event
Packet filter connections	Connections fail over to the other cluster member.
BOVPN tunnels	Tunnels fail over to the other cluster member.
User sessions	Sessions fail over to the other cluster member.
Proxy connections	Connections assigned to the failed device (master or backup master) must be restarted. Connections assigned to the other device are not interrupted.
Mobile VPN with IPSec	If the cluster master fails over, all sessions must be restarted. If the backup master fails, only the sessions assigned to the backup master must be restarted. Sessions assigned to the cluster master are not interrupted.
Mobile VPN with SSL	If either device fails over, all sessions must be restarted.
Mobile VPN with PPTP	All PPTP sessions are assigned to the cluster master, even for an active/active cluster. If the cluster master fails over, all sessions must be restarted. If the backup master fails, PPTP sessions are not interrupted.

Table 2: Comparison of network configuration in active/active and active/passive FireCluster

	FireCluster Active/Passive	FireCluster Active/Active
Device requirements	Both devices must be the same model	Both devices must be the same model
Devices active	Only one device is active at a time. Neither device is primary.	Both devices are active and traffic is load balanced between them.
MAC addresses	One virtual MAC address is shared between the pair.	One multicast MAC address is shared between the pair of devices.
Network configuration requirements	No special requirements	You must configure network switches, routers, and other devices to route network traffic that uses multicast MAC addresses.

Table 3: Comparison of licensing in active/active and active/passive FireCluster

	FireCluster Active/Passive	FireCluster Active/Active
OS	Fireware XTM with a Pro upgrade required for both devices*	Fireware XTM with a Pro upgrade required for both devices*
LiveSecurity subscription	Required for both devices	Required for both devices
Mobile VPN users	The active device uses the highest capacity Mobile VPN license activated for either device.	Licenses are aggregated. Each of the active devices use the combined capacity of the Mobile VPN licenses activated for both devices.
Branch Office VPN users	The active device uses the highest capacity BOVPN license activated for either device.	Licenses are aggregated. Each of the active devices use the combined capacity of the BOVPN licenses activated for both devices.
Subscription services: <ul style="list-style-type: none"> ▪ WebBlocker ▪ spamBlocker ▪ Gateway AntiVirus ▪ Reputation Enabled Defense ▪ Intrusion Prevention Service 	The active cluster member uses the subscription services that are active in the feature key of either cluster member.	You must have the same subscription services enabled in the feature key for both devices. Each cluster member uses the subscription services that are active in its own feature key.

*Fireware XTM Pro comes standard on all XTM 8 Series and 10 Series appliances, and is a simple license key upgrade for XTM 5 Series models. FireCluster is not available on XTM 2 Series appliances.

ADDRESS:
505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:
www.watchguard.com

NORTH AMERICA SALES:
+1.800.734.9905

INTERNATIONAL SALES:
+1.206.613.0895

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. WatchGuard’s award-winning extensible threat management (XTM) network security solutions combine firewall, VPN, and security services. The extensible content security (XCS) appliances offer content security across email and web, as well as data loss prevention. Both product lines help you meet regulatory compliance requirements including PCI DSS, HIPAA, SOX and GLBA. More than 15,000 partners represent WatchGuard in 120 countries. WatchGuard is headquartered in Seattle, Washington, with offices in North America, Latin America, Europe, and Asia Pacific. For more information, please visit www.watchguard.com.

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features, or functionality will be provided on an if and when available basis. ©2010 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, and WatchGuard ReputationAuthority are either registered trademarks or trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part.No. WGCE66709_081010