



Clustering & Queue Replication

## **Clustering and Queue Replication:**

### **How WatchGuard® XCS Provides Fully Redundant Messaging Security**

Technical Brief

WatchGuard® Technologies, Inc.

Published: March 2011

## Introduction

In the last decade, email has surpassed the telephone as the primary tool for business communications. Your messaging environment is no longer a matter of convenience, but one of necessity that must be protected with automated and native redundancy to ensure no messages are ever lost.

## A Totally Redundant Messaging Environment from WatchGuard

WatchGuard® XCS Extensible Content Security appliances include unique, native features and functionalities that support multiple levels of redundancy. To develop a totally redundant messaging infrastructure, four types of redundancy must be considered:

1. **Hardware redundancy**, in the event of a hardware failure of a single component such as a failed hard drive.
2. **Logical redundancy** or the ability to cluster multiple systems together, in the event of a single system failure, as well as for scalability. Logical redundancy must also allow administrators to manage the multiple systems acting as one logical unit easily and efficiently.
3. **Message redundancy**, to ensure no messages are ever lost or delayed due to the failure of a system that has unprocessed or undelivered queued messages at the time of failure. This becomes extremely important when deploying products that rely heavily on multiple delivery queues for processing their messages.
4. **Geographical redundancy** must include an easy way for administrators to manage systems that are deployed globally.

## Hardware Redundancy

WatchGuard XCS is available in seven appliance (hardware) models<sup>1</sup> that address the different scalability and throughput requirements of enterprise messaging environments. Hardware redundancy is available in higher end models (XCS 770R, 970, and 1170) to support the most resource-intensive messaging environments.

## Logical Redundancy

### *On-Demand Clustering*

Clustering provides a highly scalable, redundant messaging security infrastructure by interconnecting a number of cooperating nodes over a cluster bus in order to increase overall capacity and provide high availability. The cluster can be thought of as a single virtual gateway where all nodes are identically configured.

There is no theoretical limit to the size of the cluster, and you can add devices to the cluster to increase processing and high availability capabilities. By using clustering, message traffic flow is never interrupted because of individual device failures.

*“Clustering” —  
connecting two or more  
computers together so  
they behave like a single  
computer.*

*Clustering is used for  
parallel processing, load  
balancing, and fault  
tolerance.*

---

<sup>1</sup> WatchGuard XCS 170, 370, 570, 770, 770R, 970, and 1170

All of the nodes within a cluster are managed and configured as a single entity from the cluster Primary node, and all devices in the cluster can process messages. Any configuration changes, for example to Anti-Spam Settings, Policies, etc., are propagated to all cluster devices automatically, eliminating the need to manually replicate configurations on all units in the cluster, hence providing the ability to add systems quickly.

The WatchGuard XCS devices participating in the cluster communicate together through a network interface connected to a separate network called the cluster network. The cluster network is a dedicated, physically secure subnet, and the devices communicate clustering information with each other through this network. Devices can be removed or added from the cluster network without interruption to message processing.

### **Messaging Redundancy**

A cluster can be managed from any single system within the cluster without the need for a separate management console, and all systems in the cluster can process messages.

As seen in Figure 1, WatchGuard XCS operates in one of four modes in a cluster:

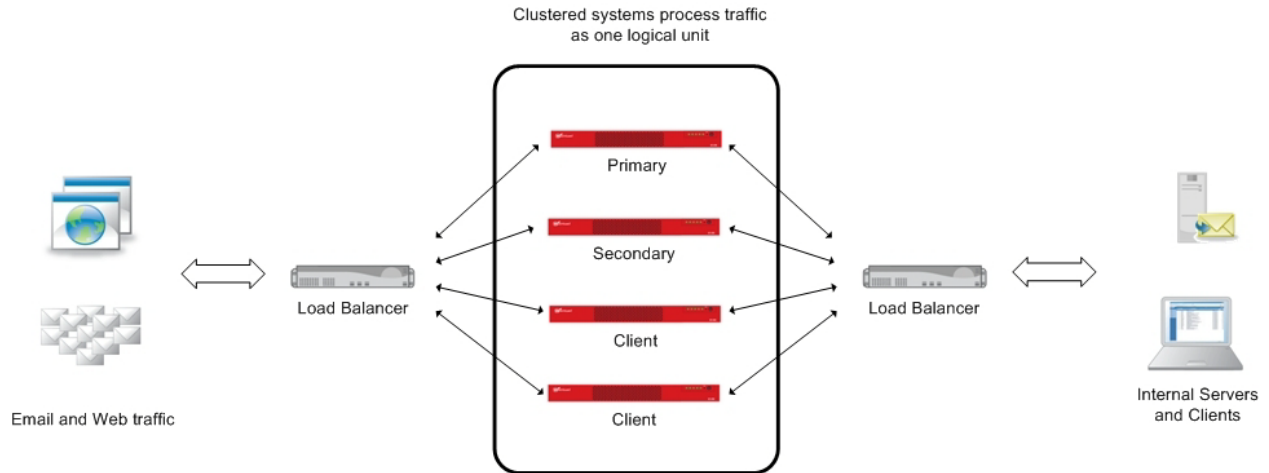
**Primary:** This device is a primary master system for the cluster. All configuration is performed on this device. Other devices in the cluster pull configuration changes from the Primary automatically when a new configuration is applied.

**Secondary:** A device running in Secondary mode operates the same way as a Client cluster device except that it retains a copy of the master database replicated from the Primary. If the Primary cluster device fails, the Secondary can be promoted to Primary status.

**Client:** A device that runs in Client mode pulls its configuration from the Primary. After the initial setup, no configuration is required on the Client. You can promote a Client to a Secondary. Unlike a Primary or Secondary, a Client does not contain a copy of the full configuration database.

**Standalone:** The device initially installs in Standalone mode. In this mode, the device still processes mail, but does not participate as part of the cluster and does not pull configuration updates. This mode is primarily used to remove a cluster device for offline maintenance or software updates.

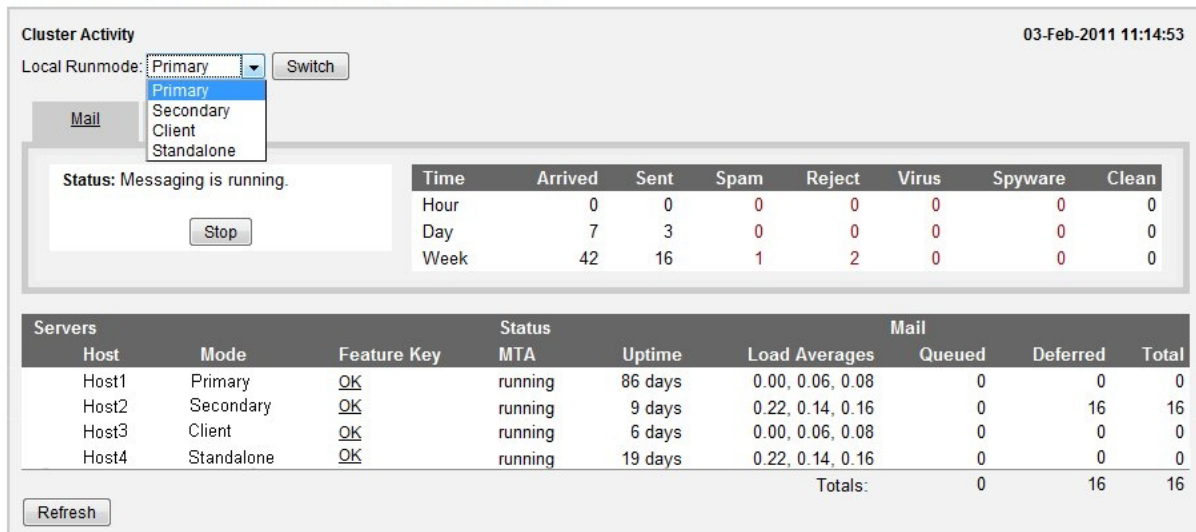
*There is no theoretical limit to the size of the cluster, and systems can easily be added to the cluster to increase processing and high-availability capabilities. Clustering ensures that the flow of traffic is not interrupted due to individual system failures.*



**Figure 1: WatchGuard XCS Clustering Architecture**

Cluster activity can be viewed at a glance in a display that provides processing statistics for the entire cluster as seen in Figure 2.

**WatchGuard Extensible Content Security - Cluster Activity**



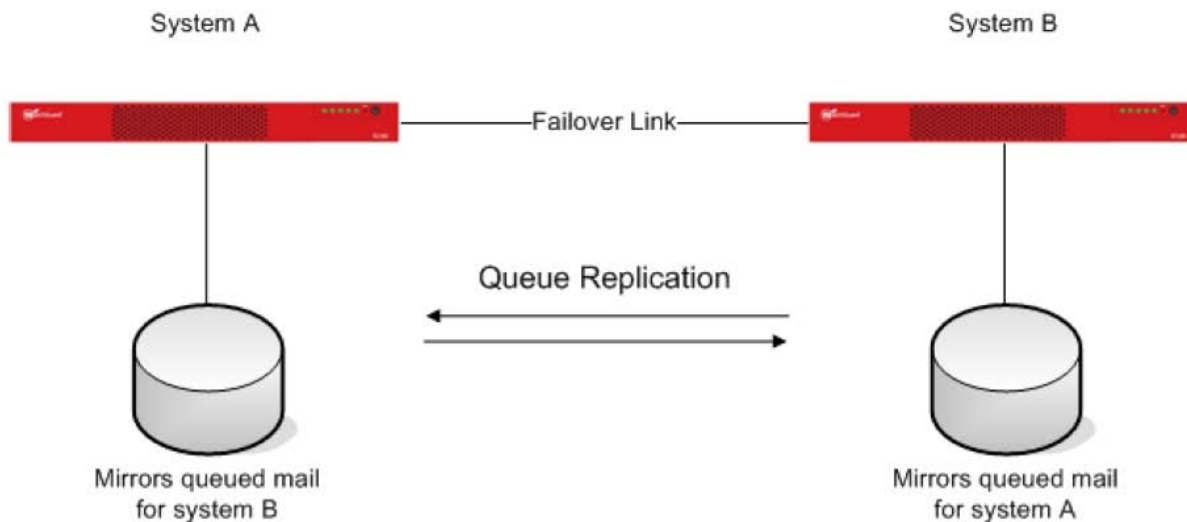
**Figure 2. Cluster Activity**

**Queue Replication**

*Ensures Zero Lost Messages*

Queue Replication, a patented technology integrated into all WatchGuard XCS appliances, actively copies any queued mail to a mirrored system, ensuring that if one system should fail or be taken offline, the mirror system can take ownership of the queued mail and deliver it. If the source system successfully delivers the message, the copy of the message on the mirror server is automatically removed. Without queue replication, if a system with received and queued messages that have not

been delivered suddenly fails, mail could be lost. In large environments, this could translate into hundreds or thousands of lost messages. As illustrated in Figure 3, System A and System B are configured to be mirrors of each other's mail queues.



**Figure 3. Queue Replication**

When a message is received by System A, it is queued locally and a copy of the message is also immediately sent over the failover connection to the mirror queue on System B. If System A fails, administrators can log into System B and take ownership of the queued mail to deliver it. Messages are exchanged between the systems to make sure that the mirrored mail queues are properly synchronized, which prevents duplicate messages from being delivered when a failed system comes back online.

### **Geographic Redundancy**

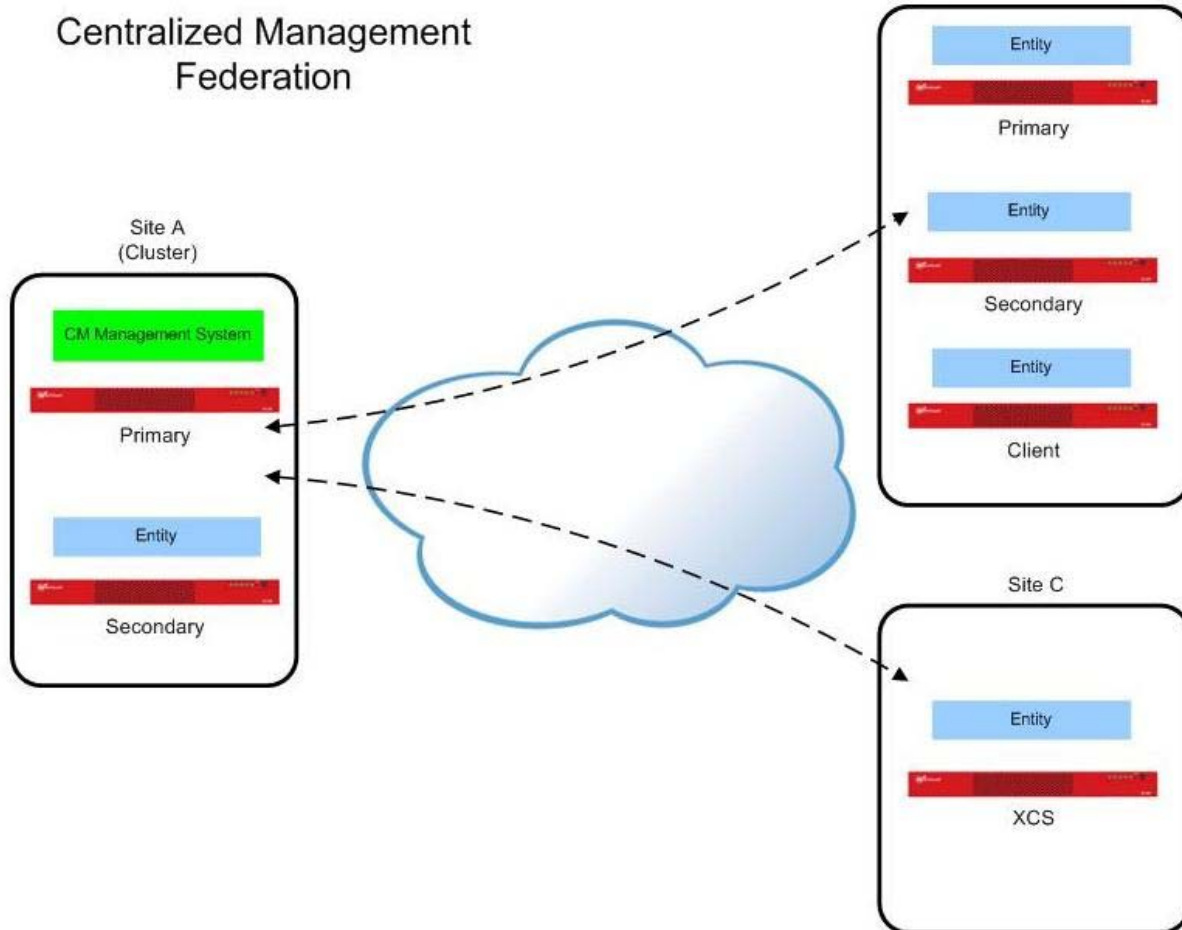
#### *Centralized Management of the System*

Centralized Management differs from clustering in that the intent is not to implement a “virtual gateway.” The intent is to manage a set of potentially heterogeneous and geographically dispersed clustered and non-clustered nodes. Centralized Management is therefore complementary to clustering, and used in deployments where multiple systems that require distinct configuration must be centrally managed. WatchGuard XCS Centralized Management, included with all appliance models, allows administrators to manage multiple local or remote security gateways (either standalone or clustered) from a single user interface (UI) without a dedicated system or additional management console. Using the Centralized Management capability, administrators can centrally monitor and configure a set of potentially heterogeneous and geographically dispersed clustered and non-clustered nodes.

All communication between the managed gateways and the Centralized Management node is encrypted using industry standard encryption techniques. Centralized Management allows administrators to efficiently monitor and manage several WatchGuard XCS appliances that are running independently or as part of a cluster, via a single management system. Also made possible by WatchGuard XCS appliances

is the operating of clustered or non-clustered systems that are located in geographically distant locations across the globe. Each of these systems may have several shared configuration parameters and also require unique configurations for each location.

A set of clustered or non-clustered systems that are monitored, secured, and managed by Centralized Management are called a Federation. Each system within the Federation is called an Entity. The Centralized Management system acts as the single point of management and provides the capability to add clustered and non-clustered Entities to the Federation.



**Figure 4. Centralized Management Federation**

The unique WatchGuard XCS Centralized Management feature provides the following capabilities:

- Allows you to group a Manager and Entity devices (this includes clustered and non-clustered devices) into a single Centralized Management Federation.
- Allows you to monitor the activity and status of all Entities in the Federation from the Manager device.

- Allows you to define a global configuration set that you can apply to all Entities in a Federation (this includes independent devices and clusters). Most aspects of the configuration are available for distribution, including message delivery settings, policies, policy mappings, and mail routes.
- You can modify the local configuration of Entity devices in the Federation for unique local requirements.
- You can view reports from all Entities in the Federation on the Manager system.
- You can search the Message History of all Entities in the Federation on the Manager system.

### **Advantages of WatchGuard XCS**

WatchGuard XCS offers multiple levels of redundancy available for a highly scalable, resilient, and always-on messaging security environment.

- Hardware redundancy to protect against a single component failure to an appliance such as hard drives and power supplies (only available with 770R, 970 and 1170 appliance models).
- Logical redundancy or clustering that protects against a single appliance failure as well as providing for scalability for increased message volumes as your business grows.
- Messaging redundancy to ensure a message is never lost or delayed in the event of an appliance failing when messages in the queue have not been processed.
- Geographical redundancy to prevent against a single data center failure. WatchGuard XCS also gives the administrator the capability to easily manage the entire enterprise including the ability to apply policies both for local clusters as well as across the entire Federation.

### **WatchGuard XCS: Always-On Email Security & Zero Downtime**

Today, email is used for transactions and communications that require multiple layers of redundancy, including message-level redundancy, since load balancing is not enough. For example, losing an important time-sensitive email such as a sales order or contract negotiation can cause an organization both lost productivity and lost revenue. WatchGuard XCS delivers multiple layers of redundancy for a fully redundant messaging security environment so you never lose a communication.

By implementing WatchGuard XCS advanced clustering and patented queue replication, XCS ensures that data is never lost as long as one device in the cluster remains operational. WatchGuard XCS eliminates content-security downtime – no lost messages, no re-transmissions, no dropped sessions. You benefit from unprecedented linear scalability and dramatic reduction in the time and effort administrators spend configuring and maintaining systems.

With XCS, you can increase throughput, maintain superior service levels and ensure resilience by simply configuring one appliance and distributing processes across multiple devices. This allows organizations of all sizes to scale to hundreds of devices, or start small with as few as two devices, as traffic requirements dictate. Ultimately, WatchGuard XCS allows you to scale your environment infinitely to address current and future demands to upwards of 100 million messages per hour, enabling you to quickly add systems in minutes. By clustering multiple units together, you remove a single point of failure and ensure that your network infrastructure is always up and running. WatchGuard XCS provides an unbeatable return-on-investment by reducing operational costs and guaranteeing the delivery of business-critical messages and communications for always-on network reliability.

## Next Steps

For more information on the powerful WatchGuard XCS family of extensible content security products, visit [www.watchguard.com/xcs](http://www.watchguard.com/xcs).

---

**ADDRESS:**

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

**WEB:**

[www.watchguard.com](http://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](http://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. ©2011 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard Logo 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. WGCE66733\_030811