

Red Hat Network

Security Overview

Red Hat understands that security is a top priority for your company. Red Hat Network is designed with that in mind - allowing you to take advantage of Red Hat Network functionality while protecting your systems from outside risks.

This document is an overview of security practices used by Red Hat Network and demonstrates the differences between the three available Red Hat Network architectures (Hosted, Proxy, and Satellite).

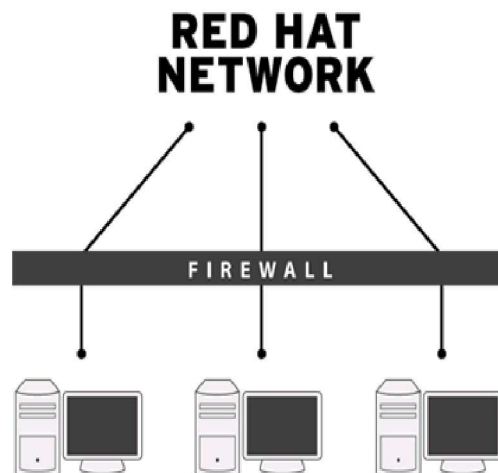
For more information on Red Hat Network functionality and product offerings please visit our web site: www.redhat.com/software/rhn/management/

Hosted Architecture

The customer's individual systems connect with Red Hat Network via the Internet and exchange packages and information from the central RHN servers.

Key security facts:

- **Authentication.** When your client connects to Red Hat, it uses an SSL certificate to verify that the certificate presented by Red Hat servers matches its internal copy. If the certificates do not match, the client will drop the connection. This ensures that your machines can not communicate with anyone other than Red Hat's official servers.
- **Encryption.** All data transferred between Red Hat and your hosts is encrypted end-to-end using standard 128-bit SSL and TLS protocols. This ensures that data is never revealed to unauthorized third parties when in transit.
- **Package Verification.** Every software package and update from Red Hat is cryptographically signed by the Red Hat GPG key, and then verified using MD5 and SHA1 checksum. Only intact packages that contain the correct signature will be installed. This ensures that only packages that have been built and tested by Red Hat will be installed on your machines.
- **Outbound connections only.** Your hosts make an outbound connection to the Red Hat servers. This connection is made on a single TCP port, HTTPS port 443. No inbound connections are used. This allows you to protect your hosts with strict firewall rules. Your hosts may even be placed behind a web proxy that controls standard HTTPS traffic that passes through it.



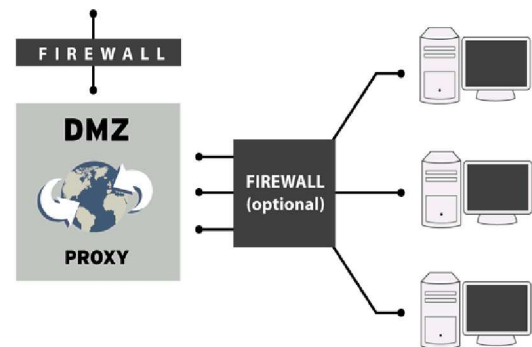
Proxy Architecture

The Proxy architecture allows caching and distribution of RPMs on your local network.

Key security facts:

- Under the Proxy architecture, your hosts use the same security standards outlined in the Hosted architecture, except that with Proxy, your clients are connecting to the Proxy Server rather than the Red Hat central servers.
- Only the Proxy Server needs to connect to the Internet. The remainder of your hosts may be restricted (optional).
- Connections to the central Red Hat servers are initiated only from your Proxy, protected by your firewall.
- Because the Proxy Server uses only HTTPS (tcp port 443) to communicate to Red Hat, all other ports can be restricted.
- Installing the Proxy server inside a DMZ will allow you to easily monitor and restrict all the traffic to and from the Proxy server over the public Internet.

RED HAT NETWORK



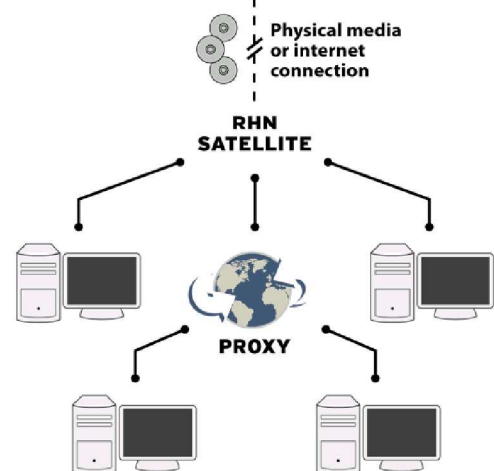
Satellite Architecture

The Satellite architecture allows you to place an entire Red Hat Network operation within your local area network.

Key security facts:

- Because the entire Red Hat Network functionality resides on your network, the update process is up to you. You can receive updates either through physical media (disks) or connect to the Red Hat servers over the Internet.
- If you obtain content directly from Red Hat over the Internet, key security facts from the Proxy Architecture apply.
- Your hosts do not need to be connected to the Internet. All communications can be internal within your local area network.
- You can determine your own security policy and decide who can connect to the server, what information about your hosts you wish to store, and when and how those communications take place.
- You can decide which updates from Red Hat you wish to include on your Satellite Server, allowing you to do internal QA on updates before releasing them to your hosts.
- Because all of the Red Hat Network functionality resides on your local area network, none of the information from your servers will ever leave your network.

RED HAT NETWORK



For more information, visit www.redhat.com/software/rhn