

High Availability

If a security device fails, connectivity goes down. To minimize the potential for a single point of failure, Juniper Network’s firewall and IPSec VPN solutions support device redundancy for high availability. This high availability is critical to maintaining network protection from an attack, even in the event of a device failure. Juniper Networks security solutions incorporate high availability capabilities based on a set of protocols, features and tools that are included as part of the overall solution.

The highly reliable nature of the hardware and redundant system designs means that Juniper Networks can provide some of the most comprehensive high availability security solutions available today. Bringing together redundancy features at the component, link and system level enables the solutions to survive multiple failures and ensure the connection can persist.

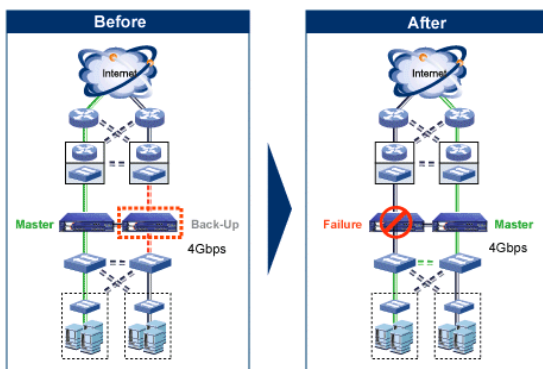
Juniper Networks high availability is centered around a redundancy protocol known as the NetScreen Redundancy Protocol (NSRP) that enables a redundant pair of security systems to be easily integrated into a high availability network architecture, with redundant physical connections between the systems and the adjacent network switches. With link redundancy, Juniper Networks can address many common causes of system failures, such as a physical port going bad or a cable getting disconnected, to ensure the connection is available, without having to fail over the entire system. Juniper Networks security devices also come with multiple fans and power supplies, to support device availability.

When deployed in redundant pairs, the operating system will automatically mirror the configuration between redundant systems to provide active firewall and VPN session maintenance. The devices synch both static information, such as the configuration, and dynamic run-time information. As a result, during failover synchronization the following information is shared: connection/session state information, IPSec security associations, NAT traffic, address book information, configurations changes, and more.

Juniper Networks solutions also employ a sophisticated fail-over algorithm to reroute network traffic to provide near-zero interruption, in the case of device failure. In a failover event, the backup unit already contains the necessary network configurations; session state and security associations to continue to process existing traffic in sub-second failover times. With built-in failover protocols and dynamic routing, enterprises and service providers can deploy Juniper Networks security systems in a fully-meshed network environment or in a load-sharing environment. The high availability functionality that has been built in to the Juniper Networks security products provides several configuration options including:

- Active/passive: One device acts as a master and the other as its backup. The master propagates all its network and configuration settings and the current session information to the backup. Should the master fail, the backup is promoted to master and takes over the traffic processing.

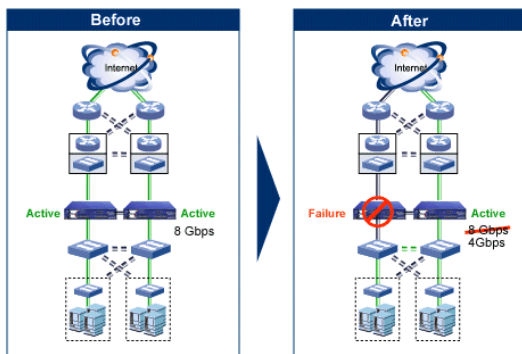
System Redundancy
Active / Passive



One device (Primary/Master) processes all traffic. Second device is passive (Back-up). In the event the master device fails, the back-up takes over, without session loss.

- Active/active: Both devices are configured to be active, sharing the traffic distributed between them by load-sharing. Each device receives approximately 50% of the network and VPN traffic. Should one device fail, the other device becomes the master and handles 100% of the traffic.

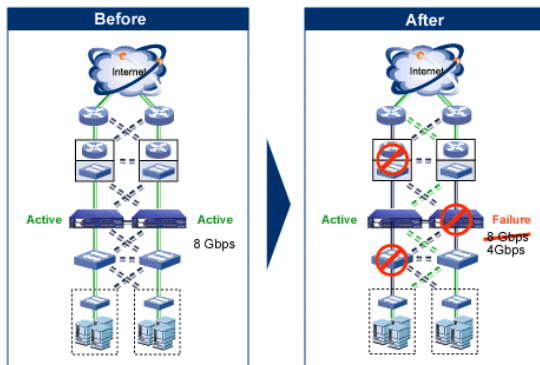
**System Redundancy
Active / Active**



Both NetScreen devices process traffic for a total of 8 Gbps. In the event of a failure up or down stream, the devices will be able to automatically route traffic around the failure to maintain availability.

- Active/active full mesh: Both devices are configured to be active with network and VPN traffic flowing through each. Should one device fail, the other device becomes the master and continues to handle 100% of the traffic. In full mesh mode, throughput adjustments must be made to ensure that if a failover occurs, the device performance is not hindered in any way.

**System Redundancy
Active / Active / Full Mesh**



Both devices process traffic. The solution is able to survive a failure at the device level and up and down stream to maintain availability.

In order to achieve maximum availability and ensure synchronization between two devices, the Juniper Networks higher-end security products have a pair of dedicated high availability interfaces. Should the connection to one interface be lost for some reason, synchronization information will fail over using the other interface. To determine if a failure has occurred and initiate a failover, heartbeat messages are sent on a configurable interval (minimum 200ms). Loss of heartbeat, loss of link on any interface or loss of access to a configured IP address or set of monitored IP addresses can be used to initiate a failover event. In addition to configurable failover, a rich toolset for customizing the HA environment to the network's requirements is available to the administrator. Juniper Networks provides a very available solution to ensure networks are protected.

Copyright © 2005 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, the NetScreen logo, NetScreen-Global Pro, ScreenOS, and GigaScreen are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

The following are trademarks of Juniper Networks, Inc.: ERX, ESP, E-series, Instant Virtual Extranet, Internet Processor, J2300, J4300, J6300, J-Protect, J-series, J-Web, JUNOS, JUNOScope, JUNOScript, JUNOSe, M5, M7i, M10, M10i, M20, M40, M40e, M160, M320, M-series, MMD, NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-SA 1000 Series, NetScreen-SA 3000 Series, NetScreen-SA 5000 Series, NetScreen-SA Central Manager, NetScreen Secure Access, NetScreen-SM 3000, NetScreen-Security Manager, NMC-RX, SDX, Stateful Signature, T320, T640, and T-series. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. All specifications are subject to change without notice.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.