

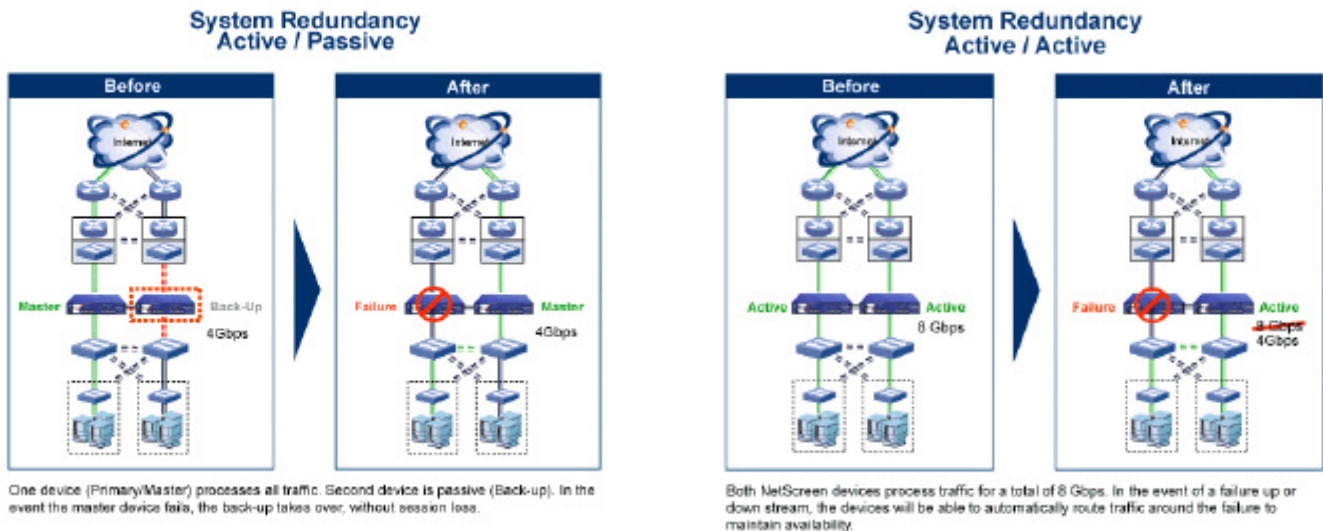
Juniper Networks high availability is centered around a redundancy protocol known as the **NetScreen Redundancy Protocol (NSRP)** that enables a redundant pair of security systems to be easily integrated into a high availability network architecture, with redundant physical connections between the systems 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. Juniper Networks low and mid-range security products provide two configuration options:

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.

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. [Active/active HA is only supported in ScreenOS 6.0 or greater releases for the SSG 5, 20, 140 & 520.](#)



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.

Active/passive and active/active High Availability requires the purchase of an Extended License on the SSG 5 & 20 but not on the 140 or 520/550. Active/active HA is only supported in ScreenOS 6.0 or greater releases for the SSG 5, 20, 140 or 520.