

# Juniper Networks Secure Access Series SSL VPN High Availability Clustering

## Features At a Glance

Provides mission-critical availability and redundancy

- Multi-Unit Clusters and Cluster Pairs for high availability and redundancy across the LAN
- Multi-Site Clusters for high availability and redundancy across the WAN
- No user session interruption or loss of productivity in the rare event of failure
- No loss of productivity of user downtime in the case of system maintenance
- Stateful peering synchronizes:
  - User settings
  - System settings
  - User session

## Best-in-class performance scalability

- Multiplies aggregate throughput
- Provides premium user experience with optimized response times
- Handles large volumes of users and resource-intensive applications
- Maintains performance in the case of burst traffic or exceptional usage patterns

## Easy to install and manage

- Centralized management for multiple Secure Access Series products with Secure Access Central Manager, now part of the Advanced feature set
- No administrative involvement required in the rare event of failure

## Meeting enterprise access infrastructure high availability requirements

Juniper Networks provides native high availability solutions, which are imperative for business-critical secure access infrastructure. Juniper Networks has designed a variety of high availability clustering options to support the SA (Secure Access) Series product lines, ensuring redundancy and seamless failover in the rare case of a system failure. These clustering options also provide performance scalability to handle the most demanding usage scenarios. Juniper Networks cluster options can be implemented for failover and performance scalability within a single site or across global deployments, offering enterprises a full range of options.

## Flexible configuration options

The Juniper Networks Secure Access 2000, 4000 or 6000 can be purchased in different cluster configurations, allowing enterprises the flexibility to choose the configuration that best addresses their high availability, performance scalability, and site deployment needs.

## Multi-unit clusters and cluster pairs

Secure Access 2000, 4000 or 6000 appliances can be purchased in a Multi-Unit Clusters or Cluster Pairs, to provide complete redundancy and expansive user scalability. Both Multi-Unit Clusters and Cluster Pairs feature stateful peering and failover across the LAN and WAN, so in the unlikely event that one unit fails, system configurations (including authentication server, authorization groups, bookmarks, etc.), user profile settings (including user-defined bookmarks, cookies,

etc.), and user sessions are preserved. Failover is seamless, so there is no interruption to user/enterprise productivity, no need for users to log in again, and no downtime. Multi-Unit Clusters are automatically deployed in Active/Active mode, while Cluster Pairs can be configured in either Active/Active or Active/Passive Mode. Secure Access Cluster configurations are centrally managed for efficiency. Multi-Unit Clusters also feature user license scalability making it easy to add more users by adding another appliance to the multi-unit cluster. Multi-Unit Clusters on the Secure Access 6000, for example, enable the enterprise to scale to over 10,000 simultaneous users. Juniper Networks' Secure Access 2000, 4000 and 6000 cluster configurations can work together to provide performance scalability, because the units in an Active/Active cluster configuration process requests in parallel at all times. This configuration, combined with an external load balancing switch, provides the exceptional aggregate throughput that is essential in the case of high user volume, exceptional usage patterns, or use of resource-intensive applications.

In addition, Multi-site clusters allow Secure Access 2000, 4000 and 6000 products to be deployed at different locations and even on different IP subnets, while maintaining state information by syncing over the Wide Access Network (WAN) and operating on a single usage license. Multi-Site Clusters feature stateful peering and failover, so in the case of failover or new system setup, gateway settings, user bookmarks and other key information is replicated across the cluster. Secure Access Series Multi-Site Clusters can be centrally managed, greatly simplifying administration for multi-site deployments, while providing broad access and fault tolerance throughout the campus or around the world.