Juniper Networks **Advanced Feature Set**

Sophisticated features for complex deployments of Juniper Networks SSL VPN appliances

Juniper Networks SA 2000, SA 4000 and SA 6000 SSL VPN appliances are offered with either Baseline or Advanced Feature Sets, designed to create an affordable solution that meets the needs of every company, from small-to-mid-sized employee remote access deployments to the largest global enterprise extranet. The Baseline features that come with the appliance out of the box provide the functionality that an enterprise would need to deploy secure remote access, as well as a provision a basic customer/partner extranet or intranet. The Advanced feature set provides additional sophisticated capabilities that will meet the needs of more complex deployments with diverse audiences and use cases, including Secure Access Central Manager, which is described in detail below. Both feature sets provide remote access, extranet, and intranet capabilities with little to no need for client software, server changes, DMZ build-outs, or software agent deployments.

Baseline Feature Set

- Enable differentiated access with access privilege management
  - Dynamic authentication policies
  - Role definition and role mapping rules
  - Role- and resource-based authorization rules
  - Very granular auditing and logging capabilities
  - Flexible policy model
  - Hybrid role/resource based policy model
  - Re-usable, “copy-paste-edit” policy model
  - Extensive integration with existing directories for authentication and authorization
  - Native Web SSO
- Leverage security infrastructure
  - Comprehensive, end-to-end layered security
  - Enterprise-class AAA and seamless integration with third-party solutions
  - End-to-end security: Host Checker/Cache Cleaner, Data, and Server security

Advanced Product Feature Set (In addition to Baseline features)

- Advanced PKI support including ability to import multiple root and intermediate CAs, OCSP, and multiple server certificates
- User self-service
  - Password Management Integration
  - Header- and forms-based Web SSO
- Access Management Integration
  - SAML – Version 1.1 support for sending authentication assertions and querying for authorization assertions
  - SiteMinder – Custom Web Agent for SiteMinder Policy store for authentication and authorization.
  - Single Sign On – Ability to do SSO to access management products with Juniper Networks Secure Access SSO functionality and adhere to authentication and authorization policies
- Multiple hostname support
- Customizable User Interface
- Combine attributes using Boolean expressions, for flexible, dynamic, “per-session” policies
- Advanced role definition and role mapping rules combine attributes using Boolean expressions
- Advanced resource authorization policies combine attributes using Boolean expressions
- Role-based delegation, configurable at the individual task level
- Flexible role definition
- Juniper Networks Central Manager
  - Central management of a device or cluster
  - Real-time system/cluster use data via the system dashboard
  - Automated appliance software updates
  - Back-up and restore for rapid disaster recovery
  - Automated propagation of changes within a cluster
  - Push configuration technology dynamically sends information to other gateways or clusters
  - Detailed archives and log filtering capabilities

Central Manager Details

Central Manager is a robust product with an intuitive Web-based UI designed to facilitate the task of configuring, updating and monitoring Secure Access appliances whether within a single device/cluster or across a global cluster deployment. Enterprises can now employ all the benefits of Juniper's award-winning Secure Access appliances even more easily and cost-effectively, with scalable, centralized device configuration and maintenance.

Central Manager enables the enterprise to eliminate repetitive admin tasks while enforcing security policies by automating many repetitive tasks. Central Manager also uses sophisticated synchronization mechanisms between Secure Access appliances to propagate security access, authentication, and authorization policies as well as device configuration throughout the cluster. Software updates can also be conducted via an automated process that enables maximum system uptime. Central Manager can also assist with capacity planning and network utilization analysis with its graphical System Dashboard, which gives a real-time view of capacity utilization graphs as well as system-wide metrics. In the unlikely event of a failure, Central Manager provides another layer of recovery to the robust Secure Access appliances themselves with local backup and restore features that give administrators the ability to save configurations in whole or in part This same utility gives historical context to configuration changes and administrator access. The Deterministic Cluster Recovery feature optimizes system resilience by assigning ranks to the nodes within the cluster, ensuring that in the case of a disturbance the node with the highest assigned rank propagates the correct cluster state once connectivity is restored.

Juniper NETWORKS

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS
FOR NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737)
or 408-745-2000
Fax: 408-745-2100
www.juniper.net

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978-589-5800
Fax: 978-589-0800

ASIA PACIFIC REGIONAL
SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
Suite 2507-11, Asia Pacific Finance Tower
Citibank Plaza, 3 Garden Road
Central, Hong Kong
Phone: 852-2332-3636
Fax: 852-2574-7803

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Juniper House
Guildford Road
Leatherhead
Surrey, KT22 9JH, U. K.
Phone: 44(0)-1372-385500
Fax: 44(0)-1372-385501

100129-001 July 2005