Juniper Networks Secure Application Manager and Network Connect

Client-server and network-layer access functionality for Juniper Networks SSL VPN appliances

All the access methods the enterprise needs, in one package

The SAMNC upgrade, which combines Secure Application Manager (SAM) with Network Connect (NC), is a companion to Juniper Networks Core Clientless access for SSL VPNs. SAM and NC provide cross platform support for client/server applications using SAM, as well as full network-layer access using the adaptive dual transport methods found in NC. The combination of SAM and NC with Core Clientless access will provide secure access to virtually any audience, from remote/mobile workers to partners or customers, using a wide range of devices, from any network. Although SAM and NC deliver two different access methods, administrators can specify exactly which access method, or combination of access methods, they wish to assign for each user in every deployment scenario. This allows administrators to provision by purpose, balancing security concerns with access requirements, while dynamic access controls enable the access to change as the user, endpoint, and network criteria change.

The Lowest Total Cost of Ownership

SAM and NC both require just a standard Web browser. Both SAM and NC agents are dynamically delivered via a lightweight agent, which eliminates the need for IT to install, configure and maintain client software. End users get all the advantages of client/server and full network-layer access while administrators are freed from the supportability issues of IPSec VPNS, like NAT or firewall/proxy traversal. No changes to the network infrastructure are required. Both SAM and NC support Windows, MAC and Linux, lowering operational costs even further.

Secure Application Manager in Detail

- SAM intermediates remote communication with internal client/server applications over SSL, with options for either Java or Windows-based implementations. This complete support significantly reduces desktop support calls and administration while providing access to all client/server applications, including dynamic TCP apps. Administrators can easily enable native Citrix integration by dynamically provisioning Win32 Citrix clients from the Secure Access gateway, as well as provide native support for Microsoft Terminal Services without the need for a pre-installed Terminal Services client. All that the user needs is the application client (i.e., the Outlook Exchange client) and a standard Web browser.

Network Connect in Details

- Network Connect's innovative adaptive dual mode transport ensures that the user gets the best connection possible from any network environment. When the user is authenticated, Network Connect will initially create a high performance IPSec-like network tunnel. If the underlying network configuration does not support that type of connection, Network Connect will automatically fall back to SSL. This function is transparent to the end user and ensures the highest performance from any connection, enabling power users to take full advantage of powerful, resource-intensive applications like VoIP or streaming media from a standard Web browser.

Complete Access From a Single Platform

Enterprises can now meet all their remote access and extranet access needs with a single SSL VPN platform. Using SAM, administrators can provide the full functionality of client-server applications when and where required. Using NC, administrators can also provide all of the functionality of an IPSec VPN and an SSL VPN from one platform, reducing overall cost and simplifying day-to-day management.

Built-in Security

Deploying any type of access requires robust security enforcement. With Juniper Networks, security is built into the platform. Like all of Juniper's SSL VPN access methods, SAM and NC are supported by Juniper's Endpoint Defense Initiative (J.E.D.I), which combines native endpoint assessment with third-party best-in-class security applications. This ensures that the endpoint is compliant with corporate security policy before any connection is allowed, and compliance is checked throughout the session. Advanced remediation functionality extends ease of use, by giving non-compliant users the information that they need to correct security issues.

SAM and NC Features At-a-Glance

Deliver complete remote access from a single platform

- Cross platform support for MAC, Linux and Windows
- Eliminates the need to support both an IPSec and an SSL VPN.

Lowest Total Cost of Ownership

- Dynamically provisioned by a lightweight download
- No client software to deploy, install, configure or maintain
- Only one management platform to deal with

Complete Security and Control

- Hardened platform leverages Juniper's Instant Virtual Extranet, which has been verified by numerous third party experts.
- Native endpoint assessment before a connection is allowed and throughout the session at administrator-specified intervals
- Endpoints can also be checked for the presence and operation of 3rd party, best-in-class security applications, delivered via J.E.D.I.
- Enhanced remediation capabilities instruct non-compliant end users how to correct their security posture, easing management headaches and speeding productivity
- Integrates with the most commonly used security and authentication protocols
- Strong security and encryption protocols
- MD5 checksum for application validation
- Client-side and server-side Access Control Lists (ACL's)
- Powerful monitoring and reporting capabilities to track access requests and usage

Enhanced productivity

- Allows administrators to provision access to applications inside the LAN with reduced expense and administration
- Enables corporations to realize increased productivity from the remote and mobile work force, and to gain efficiencies with partners
- Enables users to access client/server applications and other key enterprise resources from a central location

Ease of Management and Support

- Enhanced client side logging capability with a friendly user interface enables users to identify problems easily and administrators to troubleshoot issues more quickly
- No alterations or customization to existing infrastructure required, speeding deployment and reducing maintenance and migration costs
- Leverages centralized Secure Access infrastructure
- Adaptive delivery of Secure Application Manager for deployment in connection environments where ActiveX has been blocked
- Network Connect is fully cross platform

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

100128-001 July 2005