

At a Glance

Simplifies and centralizes encryption key rotation over a geographically dispersed network

Single console to view all security alarms and events

Allows the security of the network to be managed separately from the network itself

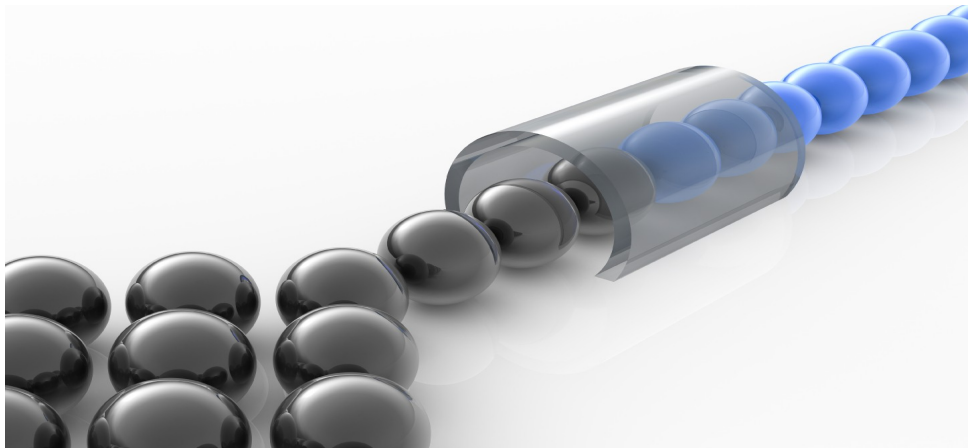
Assists with regulations compliance to audit network security

Allows service providers to sell security without being responsible for key management

Data Sheet: Network Security Portal

Abstract

The **Network Security Portal (NSP)** is designed to support automated key management for wide area network encryption devices. NSP is an Enterprise or Service Provider hosted software application that enables the separation of management tasks between Network Element management and encryption/security management. The application has been successfully deployed by large Enterprises and Service Providers to support packet and optical encryption devices.



Summary

NSP enables security demarcation for Enterprise and Service Providers that need data in-flight key management to comply with privacy regulations. It gives Enterprises control over the encryption of their network but allows them to purchase the equipment as part of a network service. It is deployable with a single server or distributed architecture. In the distributed deployment model, agents are deployed to allow isolated networks to be managed with a centralized web portal. Communications between all components are encrypted using industry standard AES256.

NSP is licensed per managed network element and currently supports the 2 leading optical transport vendors.

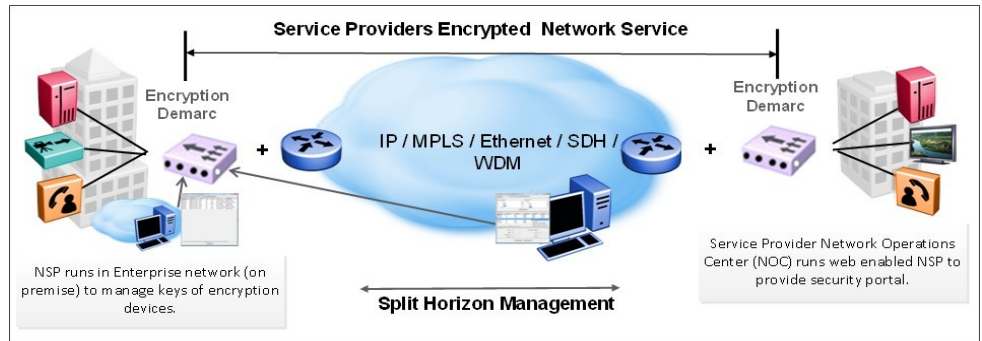
With an Encrypted Network Offering, Service

Providers can increase customer retention and differentiate their service offerings. NSP provides a complete solution for managing the security aspects of an Encrypted Network Service that is simple and cost effective.

Benefits

Simplifies and centralizes encryption key rotation over a network to view all security alarms and events

Assists with regulations compliance to audit network security

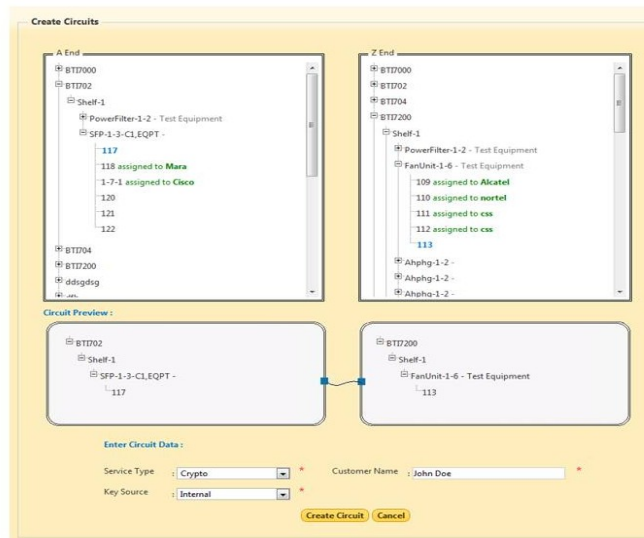


NSP Features

- ◆ A Google Maps web based console to monitor and manage all nodes and links across an enterprise or service provider network.
- ◆ A real-time dashboard display of security related alarms and performance metrics.
- ◆ Network-level automated key management and rotation.
- ◆ Scheduled and on-demand circuit authentication, key rotation, well-known answer test.
- ◆ Network Security Portal internal communications, passwords, encryption keys and authentication material secured by AES256.
- ◆ Network Element auto-discovery.
- ◆ User and Administrator audit log.
- ◆ Centralized or distributed deployment architecture.
- ◆ Software developer API based on web services.
- ◆ Support for communication over SSH, TL1, SNMP V3, SOAP.
- ◆ Designed based on Government standard FIPS 140-2.
- ◆ Integration with EMC RSA Data Protection Manager (previously RKM).
- ◆ Available as standalone Java server application and future web service hosted version.

Supported Operating Systems

*Windows 2008
VM Windows 7
VMware ESX*



NSP Application Example

Enabling Encryption as a Service for the Service Provider

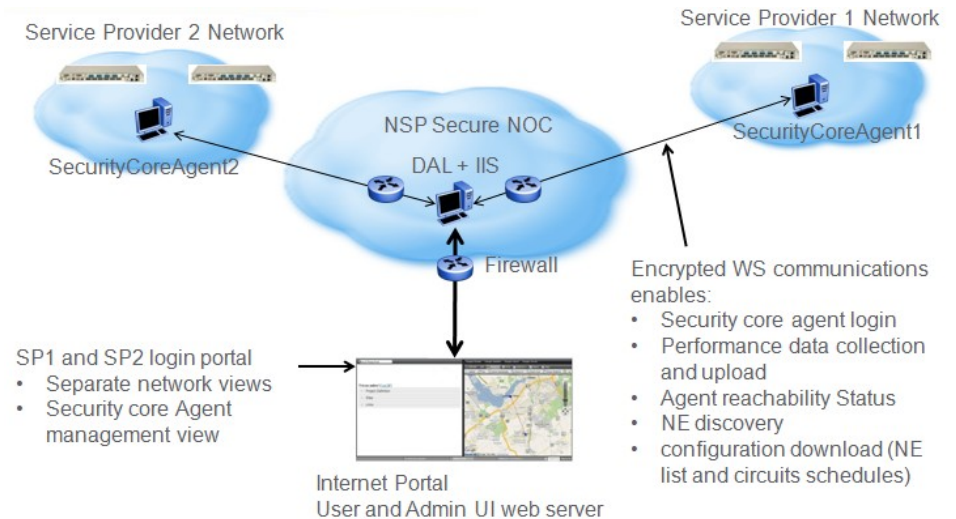
Key Management Encryption as a Service (EaaS)

Allows the security of the network to be managed separately from the network itself

Allows Service Providers to sell security without being responsible for key management

NSP can be used by Service Providers to provide encrypted carrier services and supports the separation of the Enterprise or Managed Service Provider management with a hosted software environment.

- ◆ Split Horizon Management separates cryptographic management and element management
- ◆ Enterprises retain encryption key management responsibilities with a single console to monitor and manage all of their devices and network virtual wires across wide area networks
- ◆ Provides real-time security related alarms dashboard
- ◆ Based on Government standard FIPS 140-2 Level 2 Crypto-officer user class of 'SECADMIN' to centralize security, encryption management and audit trail functions to a central console
- ◆ Operates over in-band or out-of-band management paths to Network Elements using SSH to secure the communications with the network devices
- ◆ Option for headless operation (no GUI) for continuous lights out network security monitoring.
- ◆ Operates as a background process on a Windows server
- ◆ Deployable as a single server or in a distributed environment



About Superna

Superna is focused on addressing network security, interoperability and management challenges faced by enterprise and telecommunications organizations. The company develops:

- ◆ Network based key management tools and security dashboard
- ◆ Storage over distance interoperability solutions
- ◆ Management mediation adaptors and applications for optical networks

In addition to the product portfolio, the Superna team has in-depth technical expertise in WAN based storage area networking, network security, WAN optimization, network modeling and large scale system implementation.

For more information please visit www.superna.net.