

## Site-to-Site VPN Application

### Customer Problem

For a distributed enterprise, the recurring costs associated with enabling site-to-site connectivity on a wide area network (WAN) represents a significant portion of the IT budget. Companies are looking for a way to deploy new, higher bandwidth and performance intensive solutions, such as VoIP and streaming media, to their extended user base of employees, telecommuters and business partners.

The increased number of network users coupled with the high bandwidth demand applications make bandwidth increase out of the question, given the cost structures for legacy technologies, such as the Frame Relay. Cost-conscious companies are looking for a way to affordably replace their existing WAN to take advantage of low cost broadband services.

### Requirements for Site-to-Site VPNs

Most site-to-site communications will be traveling through the Internet and open to potential attacks, so any WAN solution needs to be secure. VPN provides a much more secure alternative to Frame Relay, without the exorbitant recurring cost infrastructure. By installing the right site-to-site VPN, the company can securely take advantage of less expensive, more flexible broadband connections.

First and foremost, the VPN must meet or exceed the performance and network resilience of the existing or alternative solutions in order for it to be a viable alternative and reduce the potential for costly downtime. Secondly, the content and user identity should be protected and verified through strong encryption and a range of authentication methods.

Other key requirements include robust, centralized management to simplify deployment, reliability to eliminate lost productivity in the event of a device failure and quality of service to fine tune bandwidth usage.

### The Juniper Networks Solution

The Juniper Networks NetScreen FW/VPN appliances combine a purpose-built platform with robust security applications and powerful centralized management to deliver a cost effective alternative to legacy connectivity alternatives, such as frame relay. With a Juniper Networks site-to-site IPSec VPN, customers can take full advantage of the Internet as an affordable and flexible communications medium.

Built on top of a security specific processing platform, the Juniper Network FW/VPN appliances IPSec VPN support includes various methods of encryption (DES, DES3, AES) and authentication along with additional security applications that include network and application level attack protection along with DoS protection. To address other key components such as ease of network integration, reliability and management, the FW/VPN appliances deliver an unmatched site-to-site VPN offering. Broad support for dynamic routing protocols along with NAT, transparent and route mode help simplify network integration while redundant paths and built-in Stateful high availability (FW and VPN) ensure traffic is uninterrupted at both the link and device layer.

With Multiple methods of management (CLI, WebUI and Juniper Networks NetScreen-Security Manager), these FW/VPN appliances can be easily installed and managed either locally or from a centralized, remote location. This intuitive approach makes site-to-site VPN management as easy as point and click, enabling changes, updates and the addition of new devices to be accomplished with minimal time and expense. Overall, Juniper Networks enables companies to lower their overall WAN costs, providing a secure, flexible and easy to manage solution.

- *Existing WAN too expensive; dial-up connection too slow*
- *Potential for disruption during deployment*

- *Must be secure*
- *Ability to use broadband*
- *Quality of Service capabilities*
- *Easily deployed and managed*
- *High performance and reliability*

- *IPSec encryption, integrated network and application level attack protection*
- *Enables broadband use*
- *Extensive network resilience features*
- *Point & click, drag & drop VPN management for simple deployment and management*
- *High performance (HW based VPN acceleration)*
- *Robust HA capabilities*

## Key Features, Benefits and Advantages

Feature	Function	Benefit	Competitive Advantage
High VPN throughput	Processing intensive VPN encryption is embedded in hardware to maximize throughput and minimize performance degradation of other applications	Consistent network performance without the need to "oversize" the system unnecessarily	Many competitive offerings do not embed VPN encryption in hardware, resulting in low VPN throughput
Dynamic Routing	Supports BGP, OSPF and RIPv1/2 and the ability to automatically learn network topology	Improves VPN tunnel resilience while minimizing downtime and management efforts	Other offerings do not support dynamic routing and require static routes thereby reducing resiliency
Redundant VPN Paths	Able to configure alternative VPN tunnels as backup	When combined with dynamic routing, improves network resilience and helps minimize downtime	Few, if any other, solutions provide VPN redundancy and dynamic routing to deliver automatic VPN route failover
Dial Backup VPN	Redundant VPN connection via dial-up modem/ISDN or DSL interface	Delivers network resilience for small sites	Dial back-up can be combined with redundant paths and dynamic routing to deliver an automatic failover
High Availability	Stateful FW and VPN-failover maintains session state during failover	Tunnels and sessions do not need to be rebuilt, so downtime is minimized if a device failure occurs	Many competitors deliver HA , but very few deliver Stateful HA for both FW and VPN
Transparent, NAT, Route Mode	Device can act as a "bump in the wire" (transparent), or can hide private IP address from publication across the Internet	Simplifies integration and deployment into almost any network	While many competitors will support one or two of these deployment options, none support all three, nor do they support them to the depth that Juniper Networks does
Policy-based Management	Juniper Networks NetScreen Security Manager (NSM) delivers centralized management of many devices in different locations with labor saving features, such as device and VPN templates and rapid deployment	Minimize or eliminate costly, on-site visits, resulting in lower overall operations costs	Most competitors deliver some rudimentary centralized management, but none have the depth of labor saving features that NSM has
Role-based administration	NSM provides the ability to delegate administrative tasks to specific people	With role-based administration, configuration errors can be minimized and greater levels of control exerted over who can/cannot change security policies	Only a handful of the competition has role based administration, and NSM delivers it down to the object level, eliminating editing conflicts that may occur in less robust offerings

## Qualifying Questions

- When does your frame relay contract end?
- Why haven't you rolled out a VPN solution already?
- Have you analyzed the cost savings of your current frame relay solution vs. a VPN solution?
- Is secure access for your remote users (remote offices, remote users, road warriors) an issue that your organization deals with?
- Do you rely on multiple service providers for Internet access?
- How dynamic is your organization? How often do you add/delete users? Change policies?

## For More Information

- J-Brief FW/VPN platform summaries
- Juniper Networks FW/VPN datasheets
- Juniper Networks NetScreen-Security Manager datasheet
- Dynamic, Route-based VPN whitepaper
- IPSec VPNs - Ready for Prime Time whitepaper