ION Networks

White Paper

Examining New Options in Remote Connectivity for Managed Service Providers:

Services SSL VPN™ vs. Traditional SSL VPN and IPSec VPN

Written by:
Tara Flynn Condon
Steve Scrace
Bill Whitney, CTO

Produced by:
ION Networks, Inc.
www.ion-networks.com
info@ion-networks.com
+1 908.546.3900 (Office)
+1 908.546.3901 (FAX)

The Service Delivery Challenge: An Overview

When service providers and remote administrators require secure, remote IP access to a network, they generally use one of two connectivity alternatives: Secure Sockets Layer Virtual Private Network (SSL VPN) or Internet Protocol Security Virtual Private Network (IPSec VPN). Either seems a logical choice, as they both provide secure access as well as encryption. However, both solutions can prove complicated for service providers. Coordinating the opening of ports, reconfiguration of firewalls, and the sharing of IP addresses and multiple passwords often requires the coordination of multiple departments within each customer. This process can prove time and resource intensive.

Also, in order to offer consistently high service levels, a service provider needs to receive pertinent site data in real time. Traditional SSL VPN's one-directional connectivity (outside → in) hinders a service provider's ability to offer management and monitoring services. IPSec connections, on the other hand, offer the desired two-way connectivity but, due to the costs associated with custom configuration management, are highly difficult to scale. This limits a service provider's ability to manage multiple sites for many different customers.

ION recently released Services SSL VPN™, a feature of its SA5600 site appliance and PRIISMS management software. Services SSL VPN™ offers new, remote connectivity, monitoring, and management options for service providers. Now, service providers can leverage the Internet to deliver enhanced, proactive managed services to customers of all sizes. With its uncomplicated set-up and bi-directional connectivity, Services SSL VPN™ marries service providers' need for always-on, scalable access with customers' desire for security compliance and predictable costs.

How IPSec VPNs Inhibit Service Providers

IPSec VPNs are Not Designed for Service Provider Access: IPSec VPNs were originally designed to provide connectivity between two offices, typically a corporate headquarters and a branch office. Essentially, the IPSec VPN served an extension of the corporate Wide Area Network (WAN), which helped companies reduce costs by centralizing technology resources. In today's highly collaborative business environment, companies must open their networks to all types of outside parties, from service providers, to vendor technicians, to consultants. Because IPSec was originally conceived to enable one-to-one connectivity between two trusted parties, opening up the network to outsiders creates both connectivity and security challenges.

Costly Configurations Limit Scalability: One key requirement of IPSec VPNs is that compatible equipment is required at both ends of the tunnel. This can prove costly, as customers and services providers often have varied technical environments and would need to purchase and configure complementary hardware and software.

Unfettered Network Access Opens Customers to Risk: IPSec VPNs were designed for site-to-site connectivity, often within a single corporate entity. As such, remote administrators using IPSec VPN for connectivity often have unlimited access to system resources. Due to heightened security concerns, customers are often required to have a role-based or permissions-based architecture to restrict access by service providers and remote administrators to designated systems only. Additionally, many customers require

a detailed audit report of all system activity. At worst, these security risks can inhibit a customer from working with a service provider. At best, these risks can translate into incremental and unwelcome equipment costs.

How Traditional SSL VPNs Inhibit Service Providers

Traditional SSL VPNs Meet Customers' Security Requirements, But Not Service Providers' Monitoring Needs: Traditional SSL VPN connections offer service providers sporadic access to a customer's network, typically for troubleshooting and repairs. However, because service providers cannot receive outbound traffic and alarms from a customer's network, service providers are unable to remotely monitor and manage customer devices. Traditional SSL VPN connectivity limits the service provider to reactive, break/fix services, rather than proactive, revenue-generating managed services.

Scalability is Hindered by Custom Configurations: Each customer's network and security requirements are different. As such, setting up a traditional SSL VPN connection requires in-depth knowledge of each customer's unique operating environment. Considering the service provider has to manage thousands of customer sites worldwide, creating a custom configuration for each individual customer simply does not scale.

Services SSL VPN™ Improves Service Delivery

In August 2006, ION Networks released Services SSL VPN™, a new element in its overall solution for secure, remote administration, management and monitoring. The original inspiration for the product came from one of ION's clients, a large, international service provider. This service provider sought a highly scalable way to boost revenue and simplify operations by delivering managed services to customers via the Internet.

Services SSL VPN™ Simplifies Connectivity by Harnessing HTTPS to Easily Traverse Complex Enterprise Networks: Because the Services SSL VPN™ uses standard HTTPS ports to initiate a secure tunnel between the enterprise customer and service provider, there is no need to reconfigure firewalls or navigate through complex IT environments. As soon as ION's SA5600 appliance is placed on the customer site, it automatically establishes a connection from inside the network to the service provider's Network Operations Center (NOC). The customer sees and treats the connection just as it would an employee browsing the Internet. This makes it easy for service providers to connect to customer premise equipment using a variety of connectivity methods, including (but not limited to): broadband (ADSL/DSL/Cable modems) or leverage existing customer's Internet connectivity.

Bi-Directional Connectivity via the Internet Enables Delivery of Revenue-Generating, Proactive Managed Services: Services SSL VPN™ is the first of its kind to create bi-directional, encrypted tunnels, which originate within the customer's network. This means service providers can have always-on, Internet connectivity to customer devices, enabling the delivery of key site data (for example, alarms and traps) in real time. As a result, the service provider can consistently monitor equipment and conduct proactive maintenance, a service option previously unavailable with traditional SSL VPN connectivity. Customers benefit from higher service levels, while service providers benefit from the additional, revenue-generating service options they can provide.

A Single Platform Means Scalability and Ease of Administration: With Services SSL VPN™, there is no need for custom configurations. ION technology fits seamlessly into each customer's unique technology environment.

Customers are in Control of Access, a Key Factor in Enabling Security-related Compliance: With ION's SA5600 site appliance (the host device for Services SSL VPN™), the customer can designate who may access the network, when they can access system resources, where they may access, and what they can do. A detailed audit log is dynamically produced for each session. This level of customer control (unavailable in IPSec VPNs and traditional SSL VPNs) is an essential component of a secure, compliant solution.

In the competitive managed services marketplace, having awareness of, and a solution for customers' security and compliance requirements can be the key differentiator between service providers and their competitors.

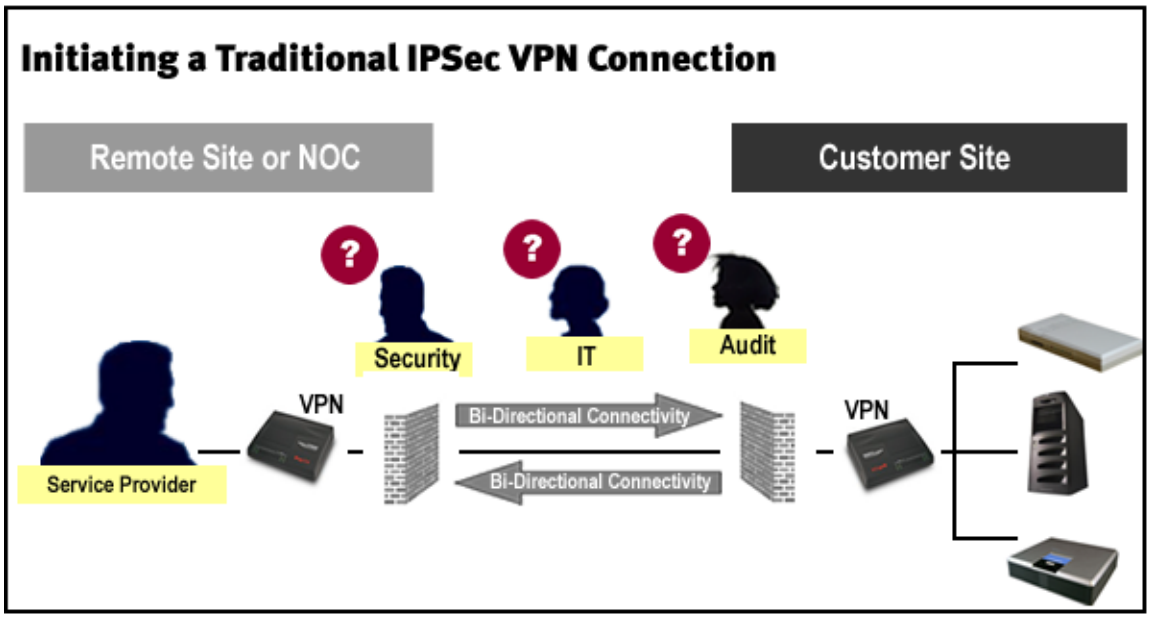
Connectivity Method Comparison

Comparing IPSec VPNs, Traditional VPNs and Services SSL VPN™

Feature	IPSec VPN	Traditional SSL VPN	Services SSL VPN™
Bi-directional connectivity	X		X
Site data (ex: alarms, traps)	X		X
Strong authentication	Proprietary	X	X
Secure connectivity to customer network via ADSL, DSL, xDSL, Cable modem, Internet	X	X	X
Customer device access from any Internet connection		X	X
Flexible equipment choices		X	X
Ability to limit network access permissions		X	X
Automatic NATing		Vendor Dependent	X
Unlimited concurrent sessions			X
Quick to deploy with no custom configurations			X
Scalability to thousands of sites			X

How it Works: IPSec VPN

IPSec VPNs serve as a secure, point-to-point connection between two entities. The following illustrates the complexities associated with this approach:

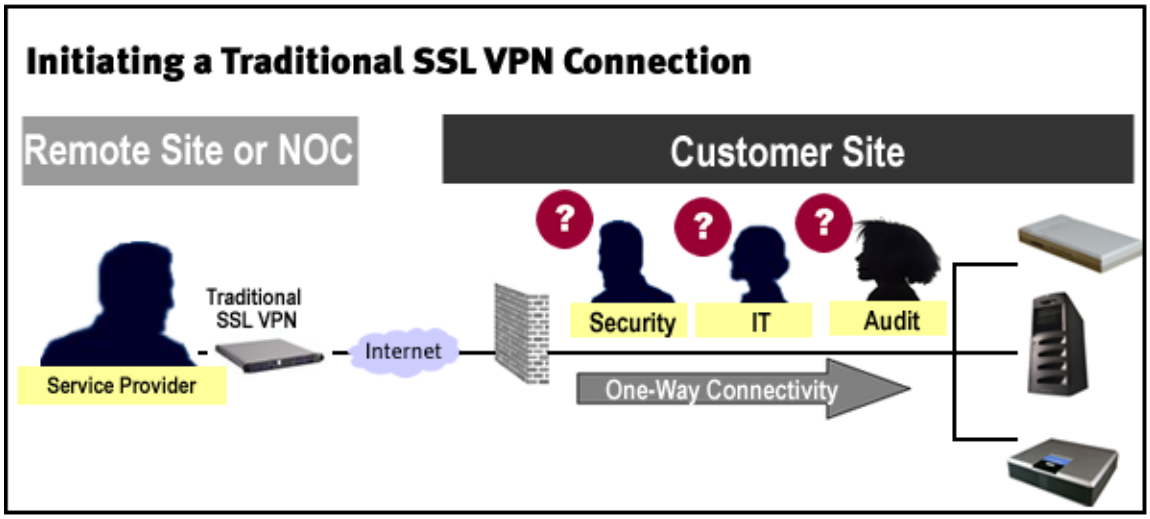


In order to set up an IPSec connection, the service provider must first coordinate with the customer's security, IT and, audit departments to outline customer-specific access and security protocols. Additionally, all parties must agree on which equipment will be used to make the IPSec connection and decide who will bear the respective costs. Due to a lack of role-based permissions, the customer may need to reconfigure its systems architecture. This would give the service provider access to designated systems, a requirement of many enterprise security policies.

While IPSec offers always on, bi-directional connectivity, it requires custom configurations, as well as additional hardware and software costs. Additionally, the lack of visibility into service providers' activities (audit / reporting) is likely to present security compliance issues for customers.

How it Works: Traditional SSL VPN Connection

Because a traditional SSL VPN connection is initiated by the service provider (outside → in), collaboration is required on both the part of the service provider and the customer. The following illustrates the complexities associated with this approach:



First, the service provider must collaborate with the customer's security team to agree on access protocols. Then, the service provider must coordinate with the customer's information technology team to open the appropriate ports. Finally, this connection must be evaluated by a team of auditors to ensure compliance with security policies.

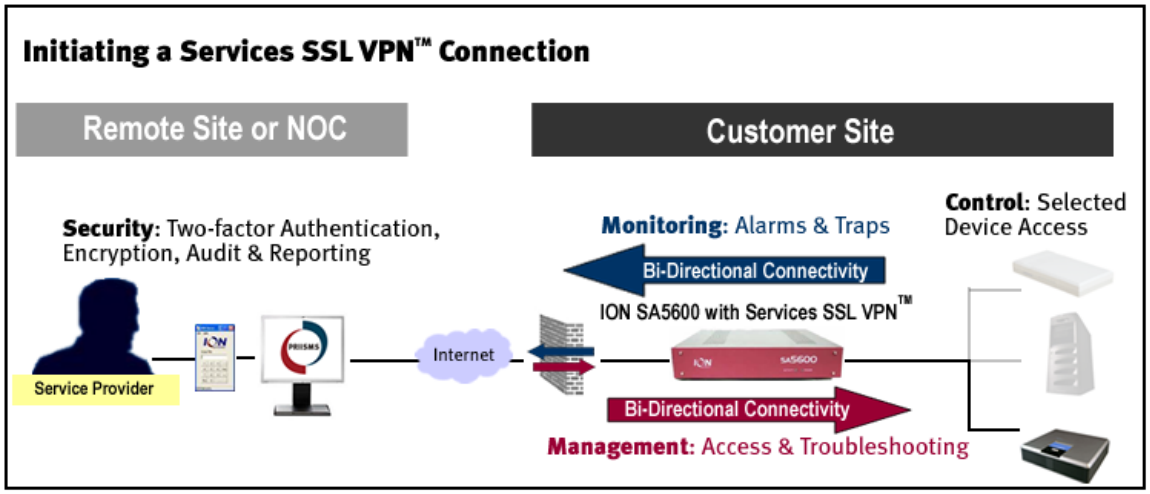
This process slows the installation and taxes both service provider and customer resources. Additionally, the reconfiguration of security systems (for example, firewalls) will most likely be in direct conflict with customers' security policies.

At the end of the set-up process, the service provider only has one-way connectivity. This means that, despite the investment in time and resources, the service provider only has the ability to offer break/fix services, not real-time monitoring of customer devices.

How it Works: Services SSL VPN™ Connection

With Services SSL VPN™, connections initiate within the customer network (inside → out). These connections are controlled and monitored by the customer via an ION SA5600 site appliance, which is located at the customer site.

Once the ION appliance is installed at the customer site, it automatically generates a Services SSL VPN™ tunnel from inside the customer's network to the service provider's NOC. Now the service provider has instantaneous, bi-directional connectivity via the Internet without having to navigate through the network or change security policies. The customer views this new connection just as it would an employee browsing the Internet. The illustration below demonstrates the solution elements and benefits:



Service providers can connect to the customer site via a variety of connectivity methods, including (but not limited to): ADSL/DSL, Internet, IP, or dial-up. After signing in by using an embedded, two-factor authentication token, the service provider is directed to the select device(s) via an encrypted Services SSL VPN™ tunnel.

Meeting Customers' Security Requirements: Key Services SSL VPN Differentiators™

Control
Using the management features available in the SA5600 site appliance, the customer can precisely control:

- Who may access network devices
- Where they can go in the network
- When they are able to access network resources
- What they can do with each device

Audit & Visibility
With the SA5600 site appliance's built-in reporting function, customers have complete, real-time visibility into all activities on the network. This helps customers to meet stringent security and compliance requirements.

Key Services SSL VPN™ Solution Elements

Required

Administrative Access Point

ION SA5600 – Site Appliance
The ION SA5600 is an administrative site appliance used by service providers and owners of distributed networks for both in-band and out-of-band secure access to a variety of devices.

Management Software

ION PRIISMS - Secure Administrative Gateway
ION PRIISMS is a secure web-based application that provides centralized control over the security and administrative access policies of distributed and complex network device environments. Network administrators can configure, troubleshoot and manage consolidated or geographically dispersed critical infrastructure devices, in-band or out-of-band, remotely or from a central NOC.

Recommended

Tokens

ION ST520 Soft Token
ION's free, single-use tokens with multi-factor authentication eliminate the use of passwords, which can be easily compromised. The ION ST520 employs strong two-factor, triple-DES, challenge/response authentication and is compatible with Microsoft Windows® platforms, RIM Blackberry® devices, and PalmOS® PDAs.

Services SSL VPN™: Benefits

Service Providers

- **Offer more revenue-generating services** by expanding services portfolio to include proactive monitoring and management services via the Internet using ION's bi-directional Services SSL VPN™.
- **Manage thousands of sites worldwide**, each with highly varying security and connectivity requirements.
- **Get customers up and running quickly** by offering a scalable, easy-to-install connectivity solution.
- **Easily access customer premise equipment** in sites all over the world via the Internet without having to navigate through customer networks or change security policies.
- **Receive instant problem notification** via real-time alarm delivery.
- **Meet customer security policies** by offering a solution that complies with security regulations and offers full audit capabilities.
- **Differentiate yourself from competitors** by proactively addressing customers' security requirements and offering an easy, cost-effective solution.

Customers

- **Easily enable and control access for all service providers and remote administrators**, using a single device.
- **Comply with security requirements** by having complete control of, and visibility into, a service provider's activities. At any given time, see who logged in, when they logged in, where they went, and what they did.
- **Protect information assets** via strong authentication and AES encryption.

About ION Networks, Inc.

ION Networks, Inc. (OTCBB: IONN.OB) is the most trusted name in remote administrative management and secure access technology. ION's suite of tools enables service providers, government and military agencies, and corporate IT resources to remotely manage, monitor, and secure critical voice and data networks. More than half of the world's top telecommunications firms rely on ION technology to ensure quality service for their customers. With over 50,000 devices deployed worldwide, ION's products are currently in use in over 35 countries. For more information, visit or call 800.722.8986 (US), +1 908.546.3900 (International).