# Remote-Access VPNs: Business Productivity, Deployment, and Security Considerations

Choosing Remote-Access VPN Technologies, Securing the VPN Deployment

## Defining Remote-Access VPNs

Remote-access VPNs allow secure access to corporate resources by establishing an encrypted tunnel across the Internet. The ubiquity of the Internet, combined with today's VPN technologies, allows organizations to cost-effectively and securely extend the reach of their networks to anyone, anyplace, anytime.

VPNs have become the logical solution for remote-access connectivity for the following reasons:

- Provides secure communications with access rights tailored to individual users, such as employees, contractors, or partners
- Enhances productivity by extending corporate network and applications
- Reduces communications costs and increases flexibility

## Using Remote-Access VPNs to Improve Business Productivity

Anytime, anyplace network access gives employees great flexibility regarding when and where they perform their job functions. VPNs accommodate "day extenders", employees who desire network access from home after hours and weekends to perform business functions such as answering e-mail or using networked applications. Using VPN technology, employees can essentially take their office wherever they go, thus improving response times and enabling work without interruptions present in an office environment.

VPNs also provide a secure solution for providing limited network access to non-employees, such as contractors or business partners. With VPNs, contractor and partner network access can be limited to the specific servers, Webpages, or files they are allowed access to, thus extending them the network access they need to contribute to business productivity without compromising network security.

## Technology Options: IPsec and SSL VPNs

There are two primary methods for deploying remote-access VPNs: IP Security (IPsec) and Secure Sockets Layer (SSL). Each method has its advantages based on the access requirements of your users and your organization's IT processes. While many solutions only offer either IPsec or SSL, Cisco® remote-access VPN solutions offer both technologies integrated on a single platform with unified management. Offering both IPsec and SSL technologies enables organizations to customize their remote-access VPN without any additional hardware or management complexity.

SSL-based VPNs provide remote-access connectivity from almost any Internet-enabled location using a Web browser and its native SSL encryption. It does not require any special-purpose client software to be pre-installed on the system; this makes SSL VPNs capable of "anywhere" connectivity from company-managed desktops and non-company-managed desktops, such as employee-owned PCs, contractor or business partner desktops, and Internet kiosks. Any software

required for application access across the SSL VPN connection is dynamically downloaded on an as-needed basis, thereby minimizing desktop software maintenance.

SSL VPNs provide two different types of access: clientless and full network access. Clientless access requires no specialized VPN software on the user desktop. All VPN traffic is transmitted and delivered through a standard Web browser; no other software is required or downloaded. Since all applications and network resources are accessed through a Web browser, only Web-enabled and some client-server applications—such as intranets, applications with Web interfaces, e-mail, calendaring, and file servers—can be accessed using a clientless connection. This limited access, however, is often a perfect fit for business partners or contractors who should only have access to a very limited set of resources on the organization's network. Furthermore, delivering all connectivity through a Web browser eliminates provisioning and support issues since no special-purpose VPN software has to be delivered to the user desktop.

SSL VPN full network access enables access to virtually any application, server, or resource available on the network. Full network access is delivered through a lightweight VPN client that is dynamically downloaded to the user desktop (through a Web browser connection) upon connection to the SSL VPN gateway. This VPN client, because it is dynamically downloaded and updated without any manual software distribution or interaction from the end user, requires little or no desktop support by IT organizations, thereby minimizing deployment and operations costs. Like clientless access, full network access offers full access control customization based on the access privileges of the end user. Full network access is a natural choice for employees who need remote access to the same applications and network resources they use when in the office or for any client-server application that cannot be delivered across a Web-based clientless connection.

IPsec-based VPNs are the deployment-proven remote-access technology used by most organizations today. IPsec VPN connections are established using pre-installed VPN client software on the user desktop, thus focusing it primarily on company-managed desktops. IPSec-based remote access also offers tremendous versatility and customizability through modification of the VPN client software. Using APIs in IPsec client software, organizations can control the appearance and function of the VPN client for use in applications such as unattended kiosks, integration with other desktop applications, and other special use cases.

Both IPsec and SSL VPN technologies offer access to virtually any network application or resource. SSL VPNs offer additional features such as easy connectivity from non-company-managed desktops, little or no desktop software maintenance, and user-customized Web portals upon login. Table 1 compares the two technologies.

**Table 1.** Comparing IPsec and SSL VPN Technologies

| | Characteristics |
|---|---|
| **Application and Network Resource Access** | • SSL (using full network access) and IPsec VPNs offer broad access to virtually any application or network resource |
| **End-User Access Method** | • SSL VPNs are initiated using a Web browser<br>• IPsec VPNs are initiated using pre-installed VPN client software |
| **End-User Access Device Options** | • SSL VPN enables access from company-managed, employee-owned, contractor and business partner desktops, as well as Internet kiosks<br>• IPsec VPN enables access primarily from company-managed desktops |
| **Desktop Software Requirements** | • Only a Web browser is required for SSL VPN<br>• IPsec VPN requires proprietary pre-installed client software |

| | Characteristics |
|---|---|
| **Desktop Software Updates** | • Basic SSL VPN access can operate without any special-purpose desktop software, thus no updates are required. Full network application access is provided using software that automatically installs and updates without any user knowledge or intervention.<br>• IPsec VPNs can automatically update, but is more intrusive and requires user input |
| **Customized User Access** | • SSL VPNs offer granular access policies to define what network resources a user has access to, as well as user-customized Web portals<br>• IPsec offers granular access policies, but no Web portals |

## Which To Deploy: Choosing Between IPsec and SSL VPNs

IPsec is a widely deployed technology that is well-understood by end users and has established IT deployment support processes. Many organizations find that IPsec meets the requirements of users already using the technology. But the advantages of dynamic, self-updating desktop software, ease of access for non-company-managed desktops, and highly customizable user access make SSL VPNs a compelling choice for reducing remote-access VPN operations costs and extending network access to hard-to-serve users like contractors and business partners. As such, organizations often deploy a combination of SSL and IPsec approaches. IPsec is commonly left in place for the existing installed base. SSL is deployed for new users, users with “anywhere” access requirements, contractors, and extranet business partners. By offering both technologies on a single platform, Cisco remote-access VPN solutions make the choice simple—deploy the technology that is optimized for your deployment and operating environment. Table 2 summarizes the issues to consider when evaluating which VPN technology best fits your operating environment.

**Table 2.** Choosing a Remote-Access VPN Technology

| | SSL VPN | IPsec VPN |
|---|---|---|
| **“Anywhere” Access from Non-Company-Managed Devices, such as Employee-Owned Desktops and Internet Kiosks** | X | |
| **Business Partner Access** | X | |
| **User-Customized Access Portals** | X | |
| **Minimized Desktop Support and Software Distribution** | X | |
| **Greatest Flexibility to the End-Users** | X | X |
| **Greatest VPN Client Customizability** | | X |
| **Ability to Maintain Existing IT Deployment and Support Processes** | | X |

## Remote-Access VPN Security Considerations

Worms, viruses, spyware, hacking, data theft, and application abuse are considered among the greatest security challenges in today’s networks. Remote-access and remote-office VPN connectivity are common points of entry for such threats, due to how VPNs are designed and deployed. For both new and existing IPsec and SSL VPN installations, VPNs are often deployed without proper endpoint and network security. Unprotected or incomplete VPN security can lead to the following network threats:

- Allows remote-user VPN sessions to bring malware into the main office network, causing virus outbreaks that infect other users and network servers
- Allows users to generate unwanted application traffic, such as peer-to-peer file sharing, into the main office network causing slow network traffic conditions and unnecessary consumption of expensive WAN bandwidth

- Enables theft of sensitive information, such as downloaded customer data, from a VPN user desktop
- Enables hackers to hijack remote-access VPN sessions, providing the hacker access to the network as if they were a legitimate user

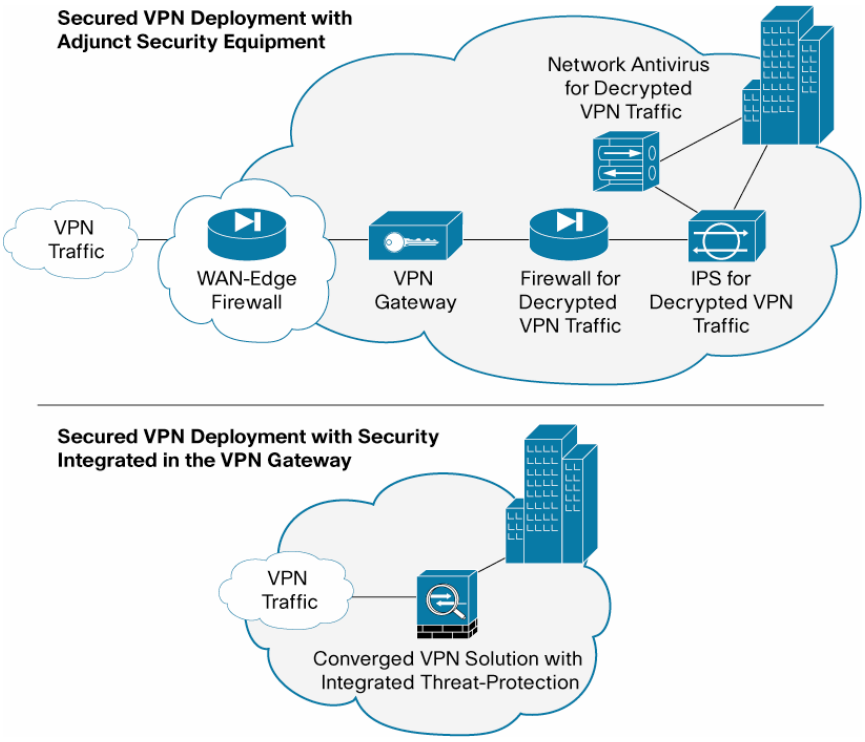
To combat these threats, the user desktop and the VPN gateway that the user connects to must be properly secured as part of the VPN deployment. User desktops should have endpoint security measures such as data security for data and files generated or downloaded during the VPN session, anti-spyware, antivirus, and personal firewall. The VPN gateway should offer integrated firewall, antivirus, anti-spyware, and intrusion prevention. Alternatively, if the VPN gateway does not provide these security functions, separate security equipment can be deployed adjacent to the VPN gateway to provide appropriate protection.

Cisco remote-access VPN solutions offer threat-protected VPN services with full firewall, antivirus, anti-spyware, intrusion prevention, application control, and full endpoint security capabilities. These security services are integrated into the VPN platform, delivering a threat-protected VPN solution without any additional equipment, design, deployment, or operational complexity.

### Steps to Securing the Remote-Access VPN

Technologies required for mitigating malware such as worms, viruses, and spyware and for preventing application abuse, data theft, and hacking exist in the security infrastructure of many organizations' networks. In most cases, however, they are not deployed in such a way that they can protect the remote-access VPN, due to the native encryption of VPN traffic. While additional security equipment may be purchased and installed to protect the VPN, the most cost-effective and operationally efficient method of securing remote-access VPN traffic is to look for VPN gateways that offer native malware mitigation and application firewall services as an integrated part of the product (Figure 1).

**Figure 1.** Securing the Remote-Access VPN—External Security Equipment or Security Services Integrated on the VPN Gateway




## Cisco Remote-Access VPN Solutions

Cisco Systems® offers a variety of remote-access VPN solutions customized for small, medium-sized, and large organizations. Available on the Cisco ASA 5500 Series VPN Edition and Cisco integrated services routers, Cisco remote-access solution features include Web-based clientless access and full network access without pre-installed desktop VPN software, threat-protected VPN to guard against malware and hackers, cost-effective pricing with no hidden "per-feature" licenses, and single-device solutions for both SSL and IPSec-based VPNs that deliver robust remote access and site-to-site VPN services from a single platform.

The Cisco ASA 5500 Series Security Appliance is Cisco's most advanced SSL VPN solution, delivering concurrent user scalability from 10 to 10,000 sessions per device and tens of thousands of sessions per cluster through integrated load balancing. Converging VPN services with comprehensive threat defense technologies, the ASA 5500 Series delivers highly customizable remote network access while providing fully secured connectivity.

Cisco Integrated Services Routers enable organizations to use their existing router deployment to provide full tunnel SSL VPN capabilities to as many as 200 concurrent users. Integrating security, industry-leading routing, and converged data, voice, and wireless with Cisco IOS® SSL VPN provides a highly manageable and cost-effective network solution for small and medium-sized businesses and organizations.

## Acknowledgements

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

## Next Steps

To learn more about remote-access VPNs or to find the solution that best fits your organizational processes and access requirements, please visit http://www.cisco.com/go/sslvpn, contact Cisco at

800 553-NETS or 408 526-4000, or locate a Cisco VPN/Security Specialized Partner at http://tools.cisco.com/wwchannels/locatr/jsp/partner_locator.jsp?page=partner_withincountry_content.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



Printed in USA C11-360982-02 02/08