



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

IPSec and SSL VPN Deployment Considerations



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Contents

Introduction	2
IPsec VPNs	2
SSL VPN	3
IPsec VPNs or SSL VPN?	4
Remote Access Scenarios	5

Introduction

Over the last several years, the trend to utilize the Internet and encryption technologies for remote access connectivity has grown dramatically as organizations became more geographically dispersed and workers increasingly mobile. Two solutions have emerged for remote access over the Internet—IPSec VPN and SSL VPN. Choosing which one to deploy will be defined by the unique requirements of the organization, and in many both may be deployed as network-level access over SSL overlaps with IPSec in some deployments.

Inherently, remote access must support connectivity from a remote endpoint. Generally, these endpoints are end user computers, typically laptop or desktop computers but also personal digital assistants (PDAs), casual access via kiosks, as well as hardware devices. In the future, components such as mobile phones and application-specific devices (e.g. a handheld computer that checks in rented cars) will likely be used as remote access clients. The increased diversification of accessing devices is a major driver for new remote access technologies.

By definition, most remote access users are people accessing internal computing resources from endpoints outside an organization's security perimeter. These endpoints can be a target for hackers looking for a backdoor into an organization (i.e. the remote access client can effectively be turned into a router into the organization). As a result, organizations are deploying security to the remote access endpoint themselves. These solutions include checking for installed firewall, anti-virus, spyware checking, and configuration checking. The endpoint security checks can be used to allow, deny, or restrict access based on the trust level of the endpoint.

Relating to endpoint security are the access controls and security protections offered in the VPN gateway. Encryption techniques can provide strong data privacy and data integrity, but do not confer access rights. Just because a user can establish a VPN tunnel, whether IPSec or SSL, does not mean he or she should be able to access all resources. A remote access solution must allow administrators to limit access to those required and no others. In addition, as access is provided to more diverse endpoints, pro-active network and application level attacks can minimize the security risk to internal servers from potentially insecure endpoints.

This document will provide background information, relevant considerations for each technology, and deployment scenarios to help organizations pick the technology that fits their needs best.

Basic Technology Overview

Two popular technologies for providing remote access include IPSec VPN and SSL VPN (also referred to as "clientless" VPN).

IPSec VPNs

Typical deployment of IPSec (IP Security) VPNs consists of one or more VPN gateways providing VPN termination for the servers behind them, and VPN client software that must be installed on each remote access user's computer. The VPN client is configured — either manually or automatically depending on the specific solution — to define which packets it should encrypt and with which gateway it should build the VPN tunnel. For site-to-site VPNs, good interoperability between

vendors has been achieved. IPSec has also been adapted for use in remote access VPNs, although interoperability is not as good as with site-to-site VPNs, since many extensions to IPSec have been made to better support remote access scenarios (e.g., NAT traversal).

IPSec is a mature standard that is in production around the world with many vendors offering solutions in multiple modes: clients, servers, and gateways. IPSec supports a strong encryption and data integrity mechanisms. IPSec is a network layer VPN technology, meaning it operates independent of the application(s) that may use it. IPSec encapsulates the original IP data packet with its own packet, thus hiding all application protocol information. Once an IPSec tunnel is negotiated, any number of connections and types (web, email, file transfer, VoIP) can flow over it, each destined for different servers behind the VPN gateway.

IPSec VPNs Pros/Cons

Pros:

- All IP types and services are supported (e.g. ICMP, VoIP, SQL*Net, Citrix ICA)
- Same technology base works in client-to-site, site-to-site, and client-to-client
- IPSec client provides opportunity to embed other security features (e.g., personal firewall, configuration verification, etc.)
- VPN gateways are typically integrated with firewall functions for access control, content screening, attack protection, and other security controls

Cons:

- Typically requires a client software installation; not all required client operating systems may be supported
- Connectivity can be adversely affected by firewalls or other devices between the client and gateway (i.e. firewall or NAT devices)
- Interoperability between one vendor's IPSec clients to another vendor's IPSec servers/gateways is typically difficult

SSL VPN

SSL is the secure transport protocol commonly used today to ensure the confidentiality and security of transactions like online banking or e-commerce (e.g. links with HTTPS, like <https://www.example.com>). Often referred to as "clientless" because most Web browsers support SSL, the browser is used as the "client" for SSL VPN. This is in contrast to IPSec remote access scenarios where a vendor's IPSec client must be installed on each remote access user's computer. SSL VPNs typically refer to remote network access through an SSL VPN gateway, but can also include SSL-enabled applications such as email clients (e.g. Microsoft Outlook, or Eudora).

SSL is a protocol that operates over TCP. Like IPSec, it has an initial setup phase to negotiate and verify several parameters before a connection can be established:

- Authenticate the server to the client, via digital certificates
- Optionally authenticate the client to the server, via certificates or other means
- Securely generate session keys, which are used to encrypt the data and provide integrity checks

SSL can make use of various public key (e.g. RSA, DSA), symmetric key (DES, 3DES, RC4), and data integrity (MD5, SHA-1) algorithms.

SSL remote access can be deployed in two ways. First, individual servers can be enabled with SSL software to terminate individual remote access users. Alternatively, an SSL VPN gateway can be used to present an SSL interface for remote users while communicating to internal servers in their native format.

SSL VPN Browser Plug-ins

Recently, solutions have emerged in SSL VPN that allows a remote endpoint to tunnel client/server applications using a browser plug-in rather than installed remote access software. Users authenticate to a web portal, typically the SSL VPN Gateway, and download a small plug-in (i.e., ActiveX or Java agent). Transparent to the user, these plug-ins take client/server traffic and tunnel it over SSL. These plug-ins, however, vary in their application support. Some support only TCP traffic and many don't support dynamic applications like FTP or VoIP.

Pros:

- SSL (e.g. Internet Explorer, Netscape Communicator, Mozilla) is integrated with all leading Web browsers
- Popular applications such as mail clients/servers (e.g. Outlook and Eudora) support SSL
- Operates transparently across NAT, proxy, and most firewalls (most firewalls allow SSL traffic)
- Web plug-in may provide network-level connectivity over SSL for client/server applications

Cons:

- Only supports TCP services natively over SSL. These are typically only web (HTTP) or email (POP3/IMAP/SMTP) over SSL
- SSL typically requires more processing resources from the gateway than IPSec
- No native software installed in "clientless" scenarios. Limited ability to push security software to the endpoint (e.g., personal firewall, integrity checking, etc.)
- If sessions are not terminated at a firewall — this requires punching a hole through an organization's firewall(s), which precludes content inspection of the data within the HTTPS connection by firewalls
- Web plug-ins may have limited application support, or require administrator privileges on the PC to operate
- Not used for site-to-site VPNs. Typically IPSec is used, thus different technologies must be used for remote access VPN versus site-to-site VPNs

IPSec VPN or SSL VPN Remote Access?

The best choice of a given technology depends on the requirements and goals for a remote access project. Once a technology is decided upon, the next step is to find the best requirements fit amongst the vendors offering solutions based on that technology. Performance, manageability, acquisition cost, ease of integration with existing infrastructure, support, and other such criteria are used to drive the vendor implementation selection.

	IPsec VPN	SSL VPN
Application Accessibility	All IP Applications (Web applications, enterprise, e-mail, VoIP and multi-media)	Primarily Web applications
Software Required	IPSec client software	Standard Web browser
Information Exposure	Only designated people /computers are allowed access	Access from everywhere (e.g. internet kiosks). Information can be left behind (intentionally or unintentionally)
Level of Client Security	Medium-High (depending on client software being used)	Low-Medium (Medium can be achieved via dedicated software — non-clientless solution)
Scalability	Highly scaleable, proven in tens of thousands of customer deployments	Highly scaleable, easy to deploy
Authentication Methods	Supports multiple authentication methods; embedded PKI available from some vendors	Supports multiple authentication methods; use of strong authentication requires extra cost and limits access devices
Security Implications	Extends security infrastructure to remote access; enhances end-point security with integrated security (e.g., personal firewall)	Limited control over information access and client environment; good for accessing less-sensitive information
Ideal For	Secure employee access; site-to-site access	External Web customer access

Using the pros and cons listed above, for both IPsec and SSL, the following general observations can be made:

- IPsec is most likely the best-fit solution when one or more of the following are the primary project requirements:
 - Organization needs a general infrastructure to support a broad range of network protocols, not just Web or email access.
 - Organization has administrative control over the remote access user's computer.
 - Security controls (e.g. requiring personal firewall, etc.) over the remote access user's computer are required. For example, administrators may NOT want users to access sensitive data from public Internet kiosks, due to the unknown security state of these types of Internet access machines.
- SSL is, most likely, the best-fit solution when one or more of the following are the primary project requirements:
 - Remote users need access to mainly Web-based applications or email.
 - Universal information access (i.e. access from any Internet device such as laptops, home PCs, Internet kiosks) is required.
 - A firewall or ISP is preventing IPsec connections (i.e., not allowing IKE negotiation for IPsec) but allows SSL.
 - Organization does not have control over the remote access user's computer configuration.
 - Installation of software to provide remote access on the user's computer is not possible.

Remote Access Scenarios

While each organization has their own unique set of remote access requirements, there are several categories of remote access users that can be used to guide the choice of IPsec or SSL for a deployment.

The following scenarios can serve as an aid when choosing an appropriate technology for an organization. Two generalizations are made. First, the more diverse the endpoint becomes, from managed employee PC to public Internet kiosk, the more the scenario best-fit moves from IPsec to SSL. Secondly, as the scenario moves from purely client/server applications to purely Web applications the best-fit also moves from IPsec to SSL.

It is important to note that in a number of scenarios the best-fit may be to deploy both SSL and IPsec.

Heavy Remote Users: Examples include System Administrators and Engineers. These types of users are typically IPsec users. There are two important considerations that point to IPsec. First, the users are most likely using specific non-Web applications as part of their work. Secondly, the environment is probably owned and managed by the organization.

Light Remote Users: An example is a Day Extender accessing the network from a home computer. These types of users are a good fit for SSL VPN. A home computer is a partially managed environment and not publicly accessible to everyone, it is managed by the employee, not the organization. The remote PC may or may not have security software such as firewall or anti-virus. An organization may want to consider how much access to allow from these users. For example, allow more access if the request comes from a PC with a personal firewall, but provide only restricted access from a PC with no personal firewall. Because SSL VPN vendors provide different security measures in SSL VPN products, part of this decision will be made based on the security that can be ensured by the SSL VPN solution.

Mobile Employees: Examples include a sales person or manager. The choice of technology can be either IPSec or SSL, or both. For mobile workers using a laptop owned by the organization, IPSec is a good solution because it is a managed environment, and many IPSec clients include security software such as a personal firewall. However, in some cases SSL may be an additional access choice. For example, many mobile employees have access to a public computer like a hotel business center PC or Internet kiosk. These unmanaged environments make SSL a good fit for email and Intranet Web access, but will not allow client server applications because client software cannot and will not be installed on the unmanaged PC.

On-Site Workers: Examples include consultants and contractors. In these cases, SSL VPN may be a better fit. These workers often work from their own PC, but need access to the network. SSL VPN is a good way to provide secure access to information without requiring client software on the employee’s PC.

Extranet Partners: An example is a partner accessing a Web portal for information sharing or accessing a Web application. Partner extranet remote access has a strong attractiveness for SSL VPN because the partner is accessing information from a PC not controlled by the organization. SSL VPN products also commonly provide a user Web portal that provides a convenient place to aggregate partner information. This solution also provides the added benefit of eliminating the need for a separate extranet network for extranet resources. However, for organizations that require access to client/server applications, IPSec may be a better solution since the extranet environment will require installed software and the barrier to installing client software is lower.

Check Point IPSec and SSL Solutions

IPsec VPN	IPsec VPN & SSL VPN	SSL VPN
VPN-1 with SecureRemote or SecureClient	VPN-1 with SSL Network Extender	Connectra Web Security Gateway (includes SSL Network Extender)

VPN-1

Check Point offers the most comprehensive set of products and technologies for remote access, intranet, and extranet VPNs. VPN-1®/FireWall-1® security gateways protect the privacy of business communications over the Internet while securing critical network resources against unauthorized access. Select the right gateway product depending on the size or complexity of your network:

- VPN-1 Pro™ for the most comprehensive security for large, complex networks
- VPN-1 Express for worry-free security to businesses with up to 500 employees and multiple sites
- VPN-1 Edge™ for secure connectivity for remote sites and large-scale VPN deployments

The following IPSec and SSL solutions are available for VPN-1:

VPN-1 SecuRemote™ provides basic IPSec capabilities, including strong, flexible authentication and easy client-side configuration.

VPN-1 SecureClient™ is a superset of VPN-1 SecuRemote, and provides advanced remote access technologies including: personal firewall with a centrally managed policy, client security assurance, IP compression, automatic in-band software updating, and OfficeMode, which assigns a virtual IP address to the remote access client, which eliminates all known NAT issues (UDP encapsulation also helps in this regard) and makes users look like they are on the internal LAN.

SSL Network Extender™ provides secure network-level access over the web. SSL Network Extender enables remote users to connect client/server applications to VPN-1 using a Web browser.

Connectra

Check Point Connectra is a complete Web Security Gateway that provides SSL VPN access and integrated endpoint and application security in a single, unified security solution. By combining both connectivity and security in a single platform, Connectra allows organizations to deploy SSL VPNs safely and securely, with the peace of mind that comes from the industry's best security solutions. Integrating SSL VPN with Check Point's Application Intelligence,™ Web Intelligence,™ and Security Management Architecture (SMART), Connectra provides Web connectivity with unmatched security.

SSL Network Extender

Check Point SSL Network Extender provides secure network-level access over the Web for business partners and employees who need remote access to networked applications. Available for several Check Point security products, SSL Network Extender enables remote users to connect client/server applications using an Internet Web browser. As an integrated component of Check Point products, this network-level connectivity over the Web comes with the most comprehensive set of features available in the industry with a single management infrastructure. SSL Network Extender is included with Connectra and is an optional add-on for VPN-1.

About Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's Zone Labs (www.zonelabs.com) division is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,300 Check Point partners in 92 countries.

CHECK POINT OFFICES:

Worldwide Headquarters:

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@Checkpoint.com

U.S. Headquarters:

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2004-2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, HackerID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartL.S.M, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo, are trade-marks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

January 10, 2005 PN: 000000



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.