

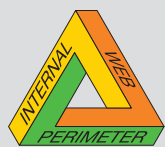
End-to-End Security for Remote VPN Sessions

In this Document

- 1 Introduction
- 2 Recognizing the Risk
- 3 Patching Security Holes
- 4 An Integrated Approach
- 5 Improving Security through Management
- 6 Summary

Features:

- The security risks of remote access
- The need for personal firewalls
- Ensuring end-to-end security for remote users



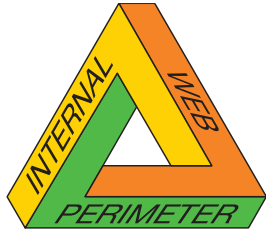
Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

INTRODUCTION



Intelligent Security

Today, increasing numbers of remote workers are using VPN technology to access internal corporate network resources via Internet access technologies such as cable modems and DSL. However, the “always on” nature of these broadband Internet services can leave individual machines open to intrusion—ultimately putting both the client and the reliability of the corporate network at risk. In order to prevent hackers from potentially hijacking a VPN session for use as an entryway to internal corporate resources, it is critical that enterprises deploy an end-to-end security solution for VPN clients. Corporate security managers may take different approaches to securing these remote users’ systems, ranging from a light-handed “mandate” to a restrictive policy which may hamper users’ ability to fully realize the benefit of high-speed connections. The best approach, however, is the thoughtful deployment of a comprehensive solution that ensures Perimeter, Internal and Web security while enabling users to truly leverage broadband Internet service.

Recognizing the Risks

Remote access VPNs pose risks to corporate security in several ways. First, any machine used for business purposes is likely to contain corporate data worth protecting, thereby meriting the use of access control measures such as those provided by firewalls. Second, the data being transmitted to and from an employee’s machine must also be protected. While this is indeed the purpose of a VPN, the adoption of always-on broadband services makes this risk both more serious and more widespread, as these long-running sessions are more prone to attack. The third and perhaps most serious reason to protect worker’s PCs is to prevent them from being infiltrated on a longer-term basis, such as by Trojan Horse programs. As an example, imagine that a hacker places a program on a fellow Internet user’s unprotected PC that captures and reports all of that user’s keystrokes. If the hacker can thus obtain the user’s passwords for his company’s VPN, then the purpose of that VPN is certainly defeated. Another dangerous type of Trojan Horse program registers an unprotected PC for use as an unwitting attacker, or “zombie”, in a Distributed Denial of Service (DDoS) attack.

As network security managers grow increasingly aware of these risks, the need for end-to-end enterprise security solutions becomes apparent. But what’s the best approach?

Patching Security Holes

One approach to securing VPN clients is to institute a corporate policy requesting that users deploy an individually managed personal firewall solution — many brands of which exist on the market today. However, this approach places the burden of personal firewall installation, configuration, and management squarely on the shoulders of end users. The difficulty of providing the required support and training for this approach — let alone ensuring its success — makes it an unrealistic one.

Another solution is to purchase a centrally managed personal firewall solution to secure individual machines. However, this method includes no measures to ensure that users do not disable or change their personal firewall configurations before establishing a VPN session. If the VPN client and firewall products are not integrated, there is no method of guaranteeing that the personal firewall is actually running on a client machine. A VPN tunnel can be compromised without the knowledge of security management or the end user — with the end result that the entire network is compromised.



Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

In addition, when deploying two separate products for remote access VPN connectivity and desktop security, organizations must weigh the cost of the associated administrative burden. Compatibility testing must be done with every new release of either the VPN client or the desktop firewall. Network security administrators should also consider issues such as scalability and management when using multiple independent client security products — what will be involved to add a new user, or to update a corporate security policy on both solutions for all VPN users?

An Integrated Approach

There are, however, solutions available today that tightly integrate desktop security features within a VPN client solution, an approach that delivers many tangible benefits. For example, an integrated firewall/VPN client can automatically enforce security on every end user's machine. While VPNs provide standard connectivity with client-side encryption and user authentication, these solutions add powerful client security features such as access control and client security assurance control. These features allow administrators to enforce centrally managed client security policies, implement rule-based access control on clients, specify different policies for different user groups and more. Organizations with different types of remote access VPN users — such as salespeople and IT staff — can tailor desktop security policies to the varying needs of their users.

Another advantage of such solutions is their ability to extend network security to include customized security checks — Windows “.dll” files that can verify a variety of conditions on the client machines, such as the installation of a particular application on the client, or a value in the Windows registry. The success of those checks may be used as a condition for allowing the client to establish a VPN connection as is illustrated in Figure 1. For example, such a solution can be configured to ensure that a client machine's anti-virus solution is up-to-date before establishing a VPN session with that machine — thereby protecting the client and the corporate network from potentially harmful viruses.

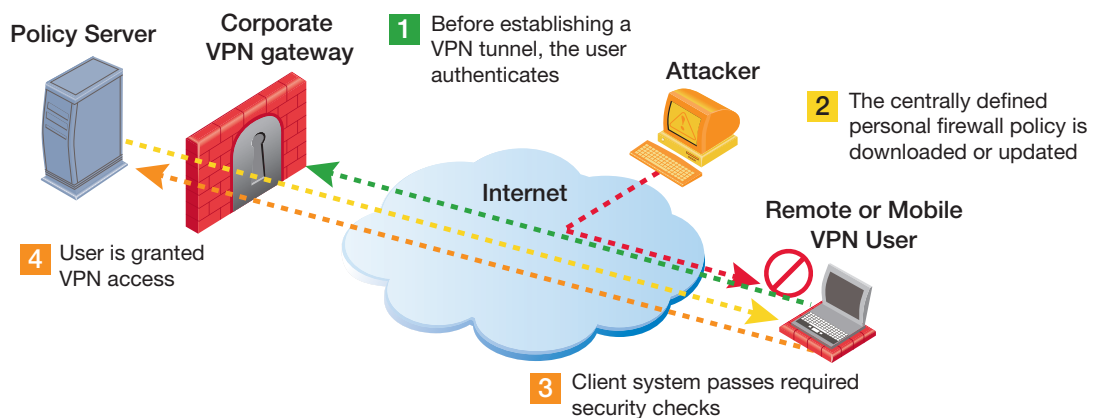


Figure 1: Comprehensive Security for VPN clients

Improving Security through Management

Client security solutions that are difficult to maintain will not provide the required level of security, therefore it's important to look for products that offer features to assist administrators with deploying and maintaining large numbers of remote users. For example, if client software is difficult to set up, then the chances are high that many users will have misconfigured systems



Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

that are not as secure as they think. Some VPN vendors deliver tools that enable the creation of self-extracting, self-executing software packages that install silently on client systems. No expertise or interaction is required on the part of the end user, which not only minimizes corporate help-desk support costs but ensures that the software will be correctly set up.

Similarly, organizations should look for products that automatically update client software if any piece is not current — greatly improving client security by ensuring that all necessary software is always up-to-date. New software components should be transparently pushed down to the client, applied, and any necessary restarting of services or of the machine itself done automatically.

Summary

In order to realize the true benefits of a remote access VPN, organizations must ensure that the chosen technology offers comprehensive security for VPN clients. While standard VPN features such as encryption and authentication secure communications to and from VPN users, securing the machines of end users is also a critical component of overall enterprise security. Client systems must be protected with personal firewall technologies that are tightly integrated with the VPN itself. And the overall VPN solution must provide the capability to enforce security requirements on VPN clients as a condition of VPN connectivity. Only when VPN clients are protected can organizations trust that the security of their networks is intact.

About Check Point Software Technologies

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Check Point provides Intelligent Security Solutions for Perimeter, Internal and Web Security. Based on INSPECT, the most adaptive and intelligent inspection technology and, SMART Management, which provides the lowest TCO for managing a security infrastructure, Check Point's solutions are the most reliable and widely deployed worldwide. Check Point solutions are sold, integrated and serviced by a network of 1,900 certified partners in 86 countries. For more information, please call us at (800) 429-4391 or (650) 628-2000 or visit us on the Web at <http://www.checkpoint.com> or at <http://www.opsec.com>.

CHECK POINT OFFICES:

International Headquarters:

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

U.S. Headquarters:

Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233
URL: <http://www.checkpoint.com>

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, 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, and VPN-1 VSX are trademarks 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 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

P/N 000000

