



# Secure Remote Access for the Distributed Business

Challenges, trends, and considerations

# Contents

- Overview ..... 3
- Remote access trends ..... 3
- Increasing security threats ..... 4
- Popular remote access methods ..... 4
- Remote access management considerations ..... 5
- Endpoint security considerations ..... 5
- Easy and continuous connectivity ..... 6
- Flexible deployment options ..... 6
- Conclusion ..... 7
- More information ..... 7

## Overview

Businesses today are defined by a wide variety of distributed work locations, and a diversity of worker types with differing information requirements. At the same time, a number of new information security and privacy regulations—such as PCI, Sarbanes-Oxley, Gramm Leach Bliley and HIPAA—are being phased in and toughened. These new realities present organizations with a new set of challenges that have begun to pose a serious dilemma. To stay competitive, an organization must provide workers and partners with remote access to sensitive information and applications around the clock. However, many of these new access locations and devices are unsecure and unmanaged. How can an organization satisfy worker and partner needs while keeping sensitive and proprietary information safe? Business requirements have come into direct conflict with security requirements. Providing convenient, secure remote access to a diverse workforce has become a serious problem.

Remote access needs are typically determined by remote user type. For example, some employees require the ability to access information from company-owned and managed laptops, Smartphones, and PDAs—while others must be able to connect from unmanaged devices such as airport kiosks, home PCs and partner computers. At the same time, malware and malicious attacks are presenting an ever greater threat to the confidentiality, integrity, and availability of business information. Distributed businesses need a unified solution that provides flexible and secure access to information resources and applications. In addition, businesses need to keep an eye on the bottom line and are aggressively seeking opportunities to reduce total cost of ownership (TCO).

## Remote access trends

It is a formidable challenge to provide remote users and business partners with convenient access to enterprise resources while maintaining absolute security of information and infrastructure. Temporary work locations—such as airport Internet kiosks, WiFi hot spots, and unmanaged home computers—put information at even greater risk. Devices owned by the enterprise can be managed and controlled to ensure they have the latest software patches and up-to-date security software installed, while other devices are beyond the scope of enterprise control and may be using out-of-date, limited, or no security software at all. Therefore, a remote access solution must consider both managed and unmanaged devices to protect enterprise information and resources from malware and malicious attacks.

The ability of an organization to grant or restrict access rights to specific information and applications—depending not only on user needs and level of trust, but also on device type and security status—has become a highly desirable management feature on remote access gateways. A recent report on the global SSL VPN marketplace states that "One of the most dynamic forces in today's SSL VPN market is the increased buyer expectations of customizable and granular access control features."<sup>1</sup>

<sup>1</sup> Frost & Sullivan, World SSL VPN Products Market, 2008

### Increasing security threats

In the past, workers accessed information using virtual private network (VPN) client software installed on their company laptops and PCs. Computers and information were kept secure by the personal firewall and policy-verification software that often came bundled with the VPN client software. Clientless SSL VPNs, which are becoming increasingly popular, afford many advantages such as the ability to access information via a standard Web browser.

Clientless access, however, has some serious limitations. For example, IT administrators do not know as much about any given endpoint as they would like, and a lack of bundled security software leaves endpoints vulnerable. Adding to this challenge, there has been a dramatic rise in spyware—including keystroke loggers, Trojan horses, and a new category called crimeware, which has been defined as “a type of computer program or suite of computer programs that are designed specifically to automate financial crime.” Crimeware enables cyber criminals to target specific businesses. This new strain of malicious software threatens information confidentiality, endangers system passwords, and increases risk of data loss and compromise. More than ever before, businesses as well as their partners are at serious risk.

### Popular remote access methods

A remote access solution must make it as easy and as seamless as possible for users to connect and stay connected to needed applications without placing undue administrative burden on IT staff. Today there are two primary technologies—IPSec and SSL—which are used to create secure remote access VPNs. When choosing a technology to deploy, an organization must consider a mix of end user requirements and security priorities. For example:

- Remote access IPSec VPNs perform well for users who need to access information from a managed device, such as a company-owned PC. IPSec VPNs provide a LAN-like connection with support for a wide range of applications
- Remote access SSL VPNs are good for users who remotely access information part time, from the road or from a home PC. They give access to the most common business applications in a user-friendly environment. SSL VPNs are also suitable for extranet access

Therefore, in order to satisfy the most requirements, a secure remote access solution should include both IPSec and SSL VPN capabilities. Additionally, deployment of a single unified gateway instead of two is much easier to manage, saving money and providing lower TCO.

## Remote access management considerations

Management is a critical consideration when selecting a secure remote access solution. A good management plan should take into account:

- Configuration and maintenance—Most companies have a formal security policy in place that outlines their overall security policy and risk strategies. A good remote access solution will enable easy realization of that policy. A management infrastructure that centralizes configuration and maintenance will increase consistency and visibility, while minimizing deployment and maintenance efforts
- Policy enforcement—Similarly, an organization can ensure more consistent management and enforcement of such policies if they are unified and centrally managed. Policies can be invoked, updated and monitored more efficiently
- Reporting and auditing—A good security practice, and one required by several regulations, is to keep an audit trail of system performance and events. This provides information needed to spot security threats and aids capacity and performance planning. A good remote access solution stores event data centrally and offers real-time visibility and reporting on system health
- Security analysis—Network attacks are increasingly complex and involve blended threats. Hackers see no boundary between remote access solutions, and neither should a security solution. A good remote access solution should correlate security threats across all products and solutions to quickly identify potential attacks. For example, the capability to spot a user attempting to login from different locations is an easy way to flag a potential login violation

## Endpoint security considerations

A secure remote access solution should offer comprehensive endpoint security to ensure that only compliant devices are granted access and to protect the network from outside threats. A good endpoint security strategy will take into account the following:

- Policy enforcement—A remote access gateway should be able to scan an endpoint prior to granting access, and enforce access policies according to the results. This enables matching of access rights with endpoint trust level. Policy enforcement solutions should also be able to verify whether security software like antivirus and firewall applications are installed and running. There are two ways to provide these policy enforcement options:
  - Client-based IPSec VPNs can provide endpoint security as part of the VPN package and either include a personal firewall or verify that one is installed.
  - Clientless SSL VPNs typically enable endpoint security using on-demand ActiveX or Java controls, providing host checking and spyware detection.

- Guest computer security—This is a special concern for SSL VPNs and necessitates specific safeguards for endpoint security. A good solution should provide a way for users to access information securely from an unmanaged device as well as explicit controls to erase session data when the remote access session ends. There are three main approaches:
  - Malware checking identifies malicious software including keystroke loggers, Trojan horses, crimeware, and more.
  - Session encryption encrypts information on the hard drive, eliminating the possibility that usable information will remain on endpoints.
  - Cache cleaning is a best practice for SSL VPN security, but does not guarantee that all data will be erased or directories cleansed. Best when used in combination with encryption.
- Real-time security updates—Ensures that endpoints are scanned for the latest security threats, operating system patches and anti-virus program versions

Malicious software can easily enter the network from remote access points. Integrated intrusion prevention systems actively protect against threats injected at the application layer or through any type of network-level tunneling. It must also be able to receive real-time security updates regarding the latest security threats and protections.

### **Easy and continuous connectivity**

Remote workers need to use their time productively, not waste it on unnecessary re-authentication or connection issues. A good remote access solution should contain built-in intelligence to know when a user is on the move, and should be able to quickly adjust to the changing environment and location. Remote users want to connect quickly and easily and stay connected, even when roaming from an office-based LAN to a mobile GPRS network. An intelligent VPN client can solve these problems, and can even initiate connections on behalf of a user when in the presence of a desired wireless network.

### **Flexible deployment options**

Choice is king when considering deployment of a secure remote access solution. Efficiency and TCO goals can be achieved through consideration of different deployment options. For example, a business with limited IT resources may prefer a turnkey appliance in order to minimize installation and maintenance efforts, while a company wishing to standardize computer hardware may prefer installing software on an open server. An ISP or Telco offering remote access to a large and diverse customer base may realize the most benefit through deployment of remote access gateway software as a virtual appliance.

## Conclusion

Providing convenient and secure remote access to a diverse and growing remote workforce has clearly become a pressing challenge for organizations today. The dilemma created when new business requirements conflict with security requirements has sharply increased demand for a unified, flexible, scalable and easily manageable secure remote access gateway solution. The bar has been permanently raised for remote access gateway vendors. When choosing a solution, businesses should consider a vendor that provides not only remote access gateways, but also has a strong track record of developing and providing security solutions for the total spectrum of enterprise security needs.

## More information

Whether you're actively comparing secure remote access solutions, or just browsing for now, we invite you to visit us at [www.checkpoint.com](http://www.checkpoint.com) and discover a solution that fits your needs.



## About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. ([www.checkpoint.com](http://www.checkpoint.com)) is a leader in securing the Internet. The company is a market leader in the worldwide enterprise firewall, personal firewall, data security and VPN markets. Check Point's PURE focus is on IT security with its extensive portfolio of network security, data security and security management solutions. Through its NGX platform, Check Point delivers a unified security architecture for a broad range of security solutions to protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company also offers market leading data security solutions through the Pointsec product line, protecting and encrypting sensitive corporate information stored on PCs and other mobile computing devices. Check Point's award-winning ZoneAlarm Internet Security Suite and additional consumer security solutions protect millions of consumer 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 hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

### CHECK POINT OFFICES

#### Worldwide Headquarters

5 Ha'Solelim Street  
Tel Aviv 67897, Israel  
Tel: 972-3-753 4555  
Fax: 972-3-624-1100  
email: [info@checkpoint.com](mailto: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>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMSecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Power-1, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartProvisioning, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, Total Security, the totalsecurity logo, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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, 5,987,611, 6,496,935, 6,873,988, 6,850,943, and 7,165,076 and may be protected by other U.S. Patents, foreign patents, or pending applications.