Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

P/N 500205
July 2000

Check Point Software Technologies Ltd.

In this Document:

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Integrated VPN/firewall</td>
<td>2</td>
</tr>
<tr>
<td>VPN gateway placed in front of firewall</td>
<td>4</td>
</tr>
<tr>
<td>VPN gateway placed behind firewall</td>
<td>5</td>
</tr>
<tr>
<td>VPN gateway placed in parallel with the firewall</td>
<td>6</td>
</tr>
<tr>
<td>VPN gateway placed on the firewall side or in the DMZ</td>
<td>7</td>
</tr>
<tr>
<td>Summary</td>
<td>9</td>
</tr>
</tbody>
</table>
Introduction

Secure Internet communications have become critical to the success of today’s businesses. Organizations recognize that any plan to successfully leverage the Internet for business must include Virtual Private Networks (VPNs). A VPN is a network which dynamically links the sites and employees of an enterprise and allows them to privately share information over a public infrastructure, like the Internet. Deciding which VPN technology to implement can be confusing and intimidating; given what seems like a myriad of choices within a burgeoning VPN vendor landscape.

Today’s VPN product solutions generally fall into two main categories: 1) stand-alone VPN gateways and 2) integrated VPN/firewall solutions. Of these two, only integrated VPN/firewall solutions are designed to deliver complete Internet security. By contrast, VPN gateways deployed separately from the firewall burden network administrators with many needless complexities of security and management. In addition, with stand-alone VPNs, the placement of the VPN gateway with respect to the firewall becomes critical since firewalls cannot enforce access control of encrypted traffic.

This paper contrasts the advantages of integrated VPN/firewalls over stand-alone VPN gateways. Stand-alone VPNs necessitate the careful consideration of the placement of the VPN gateway with respect to the firewall since firewalls cannot enforce access control of encrypted traffic. For this reason, the discussion on stand-alone solutions and their architectural shortcomings is presented in the context of the various network placement options which security administrators must consider before implementing non-integrated approaches.
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

Virtual Private Networks provide a means for using a shared infrastructure like the Internet to establish secure information sharing among enterprise sites, business partners, and employees. A secure and effective VPN deployment should:

1. Enforce overall network security policy
2. Ensure that VPN traffic is subject to network access control
3. Protect the VPN gateway from security threats
4. Provide an overall architecture that optimizes VPN and firewall performance
5. Accommodate highly dynamic and growing network environments
6. Simplify network administration and management

Integrated VPN/firewall solutions meet all of the critical requirements for a sound VPN deployment by delivering:

- **Protection from Internet Threats.** With integrated VPN/firewall solutions, the VPN gateway, and therefore VPN connectivity, receives protection from the firewall. Common denial of service attacks that could compromise a stand-alone VPN gateway are detected and dealt with by the integrated firewall.

- **Access Control for all Traffic.** Placement of the VPN gateway within the access control device allows more granular security to be applied to VPN traffic. Since the firewall and VPN gateway share user information, individuals and pre-defined groups can use the resources and services to which they are entitled access and all VPN traffic is decrypted and inspected to ensure that only appropriate content is allowed through the firewall.

- **Centralized Management.** Integrated VPN implementations greatly simplify the administration of a security policy, particularly in environments where multiple firewalls and VPN gateways are required. Database updates and security policy changes can be simultaneously applied to all VPN/firewalls, minimizing the possibility of configuration errors. In addition, integrated VPN solutions allow critical user information to be shared among multiple network applications, including firewalls and VPN gateways, throughout the enterprise. In this way network managers do not have to maintain redundant user information across multiple proprietary user data stores.

- **Consolidated Logging.** It is only with integrated solutions that network, object, user, service and administrator data shared by the VPN gateway and firewall can be leveraged. This way, all of the auditing information, which is critical to network administrators, is available in unified log files.

- **Scaleable Architecture.** In order to extend the geography of networks to branch offices and customers, enterprises require VPN solutions that will scale. VPN/firewall solutions can be introduced into VPN networks seamlessly with virtually no disruption to network operations. This benefit becomes particularly compelling when considering environments with high availability requirements where the number of enforcement points to be deployed is doubled.
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

- **Simplified Routing.** As data travels through network devices, each possible path is reflected as a routing table entry. When resources are added to a network, routing tables must be augmented to direct traffic to the firewall and VPN gateway. Integrating the VPN and the firewall greatly simplifies this task by eliminating the need to maintain separate routes to these devices.

- **Performance.** Some critics of integrated VPN/firewall solutions maintain that stand-alone VPN devices deliver faster performance of VPN functions. This is simply not the case. Integrated VPN/firewalls can offer equivalent if not superior VPN performance including throughput, concurrent connections support and quality of service. Integrated VPN/firewalls can optimize performance through: 1. cryptographic acceleration 2. integrated bandwidth management. *Cryptographic acceleration* - many integrated VPN/firewall solutions support cryptographic accelerator cards, which offload processor intensive cryptographic operations from the host CPU to a dedicated processor on the card. Hardware-based VPN acceleration enables integrated VPN/firewall solutions to scale from T1 to T3 links while freeing gateway resources for other security tasks. *Integrated Bandwidth Management* – these solutions address network congestion issues by allowing enterprises to prioritize business critical traffic over discretionary traffic and thereby optimize use of available WAN links. Some integrated VPN solutions combine bandwidth management, VPN, firewall and Network Address Translation (NAT) policy editors into a single integrated application. As a result, network administrators can quickly and simply extend a firewall or VPN policy to include bandwidth management.

The table below summarizes the advantages of integrated VPN/firewall solutions. The pages that follow elaborate on this information by examining each of the possible implementations with stand-alone VPN gateways.

<table>
<thead>
<tr>
<th>Critical VPN Solution Requirements</th>
<th>Integrated VPN/firewall</th>
<th>VPN gateway in front of the firewall</th>
<th>VPN gateway behind the firewall</th>
<th>VPN gateway in parallel with the firewall</th>
<th>VPN gateway on the side of the firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection from internet security threats</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Access control of VPN traffic</td>
<td>✓</td>
<td>✓</td>
<td>Limited</td>
<td>Limited</td>
<td>✓</td>
</tr>
<tr>
<td>Centralized management</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low latency</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Simplified routing</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consolidated logging</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scalable architecture</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated user authentication</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

VPN gateway placed in front of firewall

A VPN gateway placed in front of the firewall may seem like a good idea at first. This configuration allows VPN traffic to be inspected by the firewall before it is forwarded to the trusted network. However, there are several problems with this layout.

Internet Security Threats. Since stand-alone VPN gateways have limited or simplistic means (i.e. packet filtering) of enforcing access control, VPN devices placed in front of the firewall are vulnerable to Internet threats. With this configuration, if a VPN gateway is compromised by such an attack, all VPN communications will cease, or worse yet, may be transmitted in the clear. This is a potentially disastrous scenario for customers and business partners relying on a corporation’s VPN technology for confidential communication.

Multiple Authentication Challenges. In the example above, remote access VPN users connect to the VPN gateway, which decrypts their traffic but does not provide access control. The decrypted connections instead, go back through the firewall where more granular security can be applied. As a result, a user may be forced to authenticate multiple times (once at the VPN gateway and once for every firewall rule requiring authentication). The reason this unnecessary burden is placed on remote access VPN users is that unlike integrated solutions, the firewall and stand-alone VPN device cannot share user information.

Unwieldy management. Second only to security, perhaps the most difficult aspect of implementing a firewall and a VPN separately is the cumbersome management architecture required to support them. Since there are two distinct devices, most often from different vendors (the majority of vendors that offer both solutions integrate firewall and VPN), the architecture requires separate:

- Security policies
- Management stations
- Logging facilities
- User databases (unless both solutions support industry standard directories)
- Object or resource databases
- Routing table entries

The topology shown in Figure 2 requires separate administration and management facilities for each device. Consequently, the amount of effort required to make updates to user databases, or add network resources is doubled. In addition to being more labor intensive, this approach is particularly error prone with security policy inconsistencies and routing table misconfigurations becoming much more likely. The complexity increases severely as VPN devices and firewalls are added to support high availability and site to site VPN connectivity.
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

VPN gateway placed behind the firewall

Placing the stand-alone VPN gateway behind the firewall is one alternative that mitigates the exposure to Internet security threats by allowing the firewall to protect the gateway. Although, this premise is reasonable, the fact remains that this configuration has serious security shortcomings.

**Limited Access Control.** In this configuration, the firewall must pass VPN traffic through to the gateway without conducting granular access control on that traffic. Since IPSec IKE VPN communications are encrypted, IP packets of type 50 and 51 (AH and ESP) must be allowed through the firewall. UDP packets on port 500 for IKE must also be allowed in. This type of configuration is not in keeping with the best practices for security. Access control ensures that VPN users including partners, employees and mobile workers have appropriate access to specific resources within a network. A VPN without sufficient access control only protects the security of the data in transit but cannot enforce secure access to resources on the network.

**Unwieldy management.** As with the VPN gateway placed in front of the firewall (Figure 2), the topology shown here in Figure 3 specifies distinct VPN and firewall system administration. This means that separate management stations are required as well as sufficient IT staff so that configuration updates, network upgrades and security policy edits can be supported within both architectures. Specifically, this network placement option requires separate:

- Security policies
- Management stations
- Logging facilities
- User databases (unless both solutions support industry standard directories)
- Object or resource databases
- Routing table entries

Although this configuration is particularly unwieldy with one set of devices, management of the firewalls and VPNs for multiple sites with this topology is nearly impossible. The most challenging administrative task within such a network is consistent security policy enforcement. Misconfiguration of VPN security here can be particularly disastrous since there is no access control applied to VPN data after decryption.
Many VPN vendors promote separate VPN and firewall connections to the Internet. In this setup the VPN device is configured to accept only encrypted traffic. The proposition here is that the dedicated VPN device can perform optimally while reducing disruption to network operation during installation and setup. Of all network placement options for a stand-alone VPN gateway, this configuration is perhaps the least sound in terms of security. There are several reasons for this:

**Internet Security Threats.** Since the VPN gateway has a direct connection to the Internet, it represents a visible target for malicious activity. The stand-alone VPN gateway is not equipped to adequately defend itself against sophisticated Internet-based attacks. A compromised VPN gateway in this scenario translates to a single point of failure for all VPN traffic or in more severe cases, an open doorway for unauthorized access to corporate resources.

**Limited Access Control.** A VPN gateway in parallel with the firewall has no direct connection to a device that is able to enforce granular access control. Such a configuration makes no distinction among mobile employees of the enterprise or business partners and customers. For instance, once remote VPN users are authenticated by the gateway, they have free access to any of the resources behind that gateway. Similarly, in the event that the VPN gateway becomes compromised, attackers will be able to reach all of the resources available to legitimate VPN users. Some stand-alone VPN implementations may incorporate rudimentary filtering. This functionality is not equivalent to granular access control. Since there is no application awareness, the stand-alone solution merely allows or denies access to a service by using IP header information. Content security services like URL filtering and virus scanning cannot be deployed using these stand-alone VPN devices.

Complex Routing Schemes Required. Placement of a stand-alone VPN gateway in parallel with the firewall is more complex than Figure 4 suggests. In order to make the configuration possible, the VPN gateway must provide integrated network address translation (NAT) as well as support for a pool of IP addresses that can be assigned dynamically to remote access VPN users. If the gateway does not support NAT then the scenario shown in Figure 4a takes place. In step one, a remote access VPN user has received a dynamically assigned IP address from the ISP, has been authenticated by the gateway and allowed to access the requested resource (step 2). The resource now needs to communicate with the remote access user through the VPN tunnel. Since the internal network does not recognize the source IP address of the remote VPN user, the device sends the response to its default gateway, which is the firewall (step 3). The firewall in turn has no knowledge of the initial communication request so the outbound connection with the client can never be established since the destination is unknown.
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

Figure 4b shows how this VPN communication is made possible through a feature called IP pools. Once a remote access VPN user has been authenticated, the VPN gateway translates the ISP assigned address to one that is recognizable by the internal network (step 1). The newly assigned address is selected from a predefined “pool” or range. Separate routing table entries for each network resource are required to ensure that responses destined for that pool of addresses are sent through the VPN gateway (steps 3,4). While IP pools make this configuration viable, the disparate solutions make it an error prone and labor-intensive way to provide VPN connectivity. Substantial administrative overhead will be incurred to ensure that routing tables are kept current with network updates.

Figure 4b: IP Pools

### Critical VPN Solution Requirements

- Protection from internet security threats
- Access control of VPN traffic
- Centralized management
- Low latency
- Simplified routing
- Consolidated logging
- Scalable architecture
- Integrated user authentication

<table>
<thead>
<tr>
<th>Critical VPN Solution Requirements</th>
<th>Integrated VPN/Firewall</th>
<th>VPN gateway on the side of the firewall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection from internet security threats</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Access control of VPN traffic</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Centralized management</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Low latency</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Simplified routing</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Consolidated logging</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Scalable architecture</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Integrated user authentication</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

VPN gateway placed on the firewall side or in the DMZ

One way to avoid the pitfalls of the “in parallel” configuration is to place the stand-alone VPN gateway on the firewall side. The VPN gateway is connected via a dedicated interface on the firewall or placed within the demilitarized zone (DMZ). In this way, VPN traffic can be forwarded to the firewall after decryption so that access control determinations can be made. The merits of this configuration are that it provides access control of VPN traffic while protecting the VPN gateway from Internet threats. These benefits are quickly diminished however, by network complexity.

**Unwieldy management.** As with any of the non-integrated solutions, the topology shown in Figure 5 requires separate VPN and firewall administration. Deploying two distinct management architectures poses many administrative challenges which affect scalability and network auditing. Specifically, the burden of maintaining and upgrading discrete VPN and firewall devices doubles once high availability is deployed. Potentially four or more devices will require multiple interconnections to ensure that VPN traffic is always properly forwarded to the firewall. Efficient network auditing and logging is also made difficult in this architecture. Since the firewall and VPN logs are not consolidated, administrators cannot track network access by user without manually merging and parsing through copious data.

**Latency.** With the configuration shown in Figure 5, the VPN gateway is placed within the firewall DMZ and given a routable IP address. All inbound VPN traffic destined for the gateway connects first through the firewall where the destination address is identified and then routed appropriately. Once the gateway has decrypted the traffic, it routes the data to the firewall for access control before being forwarded to the network resource for which it is destined. Outbound traffic (data which originates on the intranet and is bound for the Internet) gets processed by
the firewall and VPN gateway in a similar fashion. Effectively, this means that every VPN communication request requires two connections to the firewall. This needless overhead not only affects access control efficiency for the entire network, but also limits the performance of the VPN device to the throughput of the overburdened firewall.

**Multiple Authentication Challenges.** Just as in the configuration where the VPN gateway is placed in front of the firewall, both management and usability become more complex with the configuration shown in figure 5. Remote access VPN users connect to the VPN gateway by responding to an authentication challenge. The gateway decrypts the traffic but does not provide access control. For this functionality, the decrypted traffic must traverse back through the firewall where in order to provide user-based access into the network, the firewall will require each user to reauthenticate. This additional burden on remote access users exists because unlike integrated solutions, the stand-alone VPN device and the firewall do not share information.

**Complex networking.** As with the example in the previous page, the only way that this configuration is even possible is if the stand-alone gateway supports Network Address Translation (NAT). Even with this feature in place there is no guarantee that all applications to which VPN users will require access will be supported. Some interactive applications like NetMeeting and CUCME rely on the true IP address (rather than the translated one) in order to send responses to the requester. Since the stand-alone VPN gateway has no application awareness, there is no way to account for these specific cases in the gateway’s NAT processes. A possible scenario is that a VPN user requiring access to NetMeeting connects to the ISP and receives a dynamically assigned IP address. The user is routed to the VPN gateway where the “true” IP address is translated to one that is recognizable by internal network resources. The Netmeeting application, which requires the “true” IP, tries to return communication to this VPN user by sending packets whose destination is the user’s ISP assigned address. The default gateway, in this case the firewall, recognizes the destination as an Internet IP address and forwards it to the cloud without sending the data to the VPN gateway first for encryption.
Summary

This paper has outlined the unparalleled merit of integrated VPN/firewall solutions. It should be noted however, that some customers may need to maintain the VPN and firewall functions as separate implementations. For those customers, there is one main point to be garnered from this discussion; centralized management of the VPN gateway and the firewall is an absolute requirement in building architecturally sound network security. Whether a particular deployment involves an integrated VPN/firewall or separate devices placed according to the configurations shown above, the two functions must be unified by a single management architecture. In this way, network administrators can enforce security policies consistently across all network enforcement points while minimizing networking complexity and error-prone security configuration practices. Deploying the soundest Internet security architecture is only possible with solutions that integrate the VPN and firewall functionality within a single management paradigm.

About Check Point Software

Check Point Software Technologies is the worldwide leader in securing the Internet. The company's Secure Virtual Network (SVN) architecture provides the infrastructure that enables secure and reliable Internet communications. SVN secures business-to-business (B2B) communications between networks, systems, applications and users across the Internet, intranets and extranets. Check Point's Open Platform for Security (OPSEC) provides the framework for integration and interoperability with "best-of-breed" solutions from over 200 leading industry partners. 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.
Why Choose Integrated VPN/Firewall Solutions over Stand-alone VPNs

Check Point Software Technologies Ltd.

International Headquarters:
3A Jabotinsky Street
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@CheckPoint.com http://www.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