Global Knowledge®

Expert Reference Series of White Papers

Do You Need a VPN, Firewall or Both?

Do You Need a VPN, Firewall or Both?

James Michael Stewart, CISSP, CEHv3-8, CHFIv3-8, Security+, Global Knowledge Instructor

Introduction

Protecting your IT assets from threats is an essential part of business and personal digital activities. VPNs and firewalls are two commonly used security tools to help reduce risk while maintaining usability. When used in concert, IT communications are filtered and encrypted. This white paper defines what these tools are, describes when you would want to use them, and offers suggestions for deployment.

Overview of the State of Internet Security

The online world is no longer a safe place to play or do business without being properly prepared. Gone are the days of being anonymous by default and an unlikely target for hackers and attackers. Today, every communication, every website visit, every file transfer, every email, and every e-commerce transaction puts you at risk of interception, spoofing, impersonation, hijacking, man-in-the-middle, account takeover, malicious code infection, and much more.

Our daily personal activities and work tasks often mandate the use of the Internet. Whether from a smartphone or a personal computer, many of us are online for most of the day. We perform personal tasks, like shopping and banking; social tasks, such as planning dinner or a rendezvous; and work tasks, such as communicating with customers or participating in video conferences and document collaboration over the Internet. It is these very tasks that put our information, our businesses, and us at risk for attack.

Fortunately, there are options for large organizations, small office/home office (SOHO) environments, and individuals that can reduce online risks considerably. Those options are to consider deploying a VPN and/or a firewall.

What Is a VPN?

A virtual private network (VPN), is a secure remote network or Internet connection that encrypts your communications between your local device and a remote trusted device or service. A VPN is a digital or electronic re-creation of a physical world concept; specifically, the idea of a dedicated isolated physical network cable that only you can use and access. A VPN creates a virtual or electronic version of a physical cable by wrapping up or containing a normal or standard insecure network communications in a tunneling protocol that encrypts the content being transported. Communications protected by a VPN still traverse the same, shared network pathways as normal traffic, but because the payload is encrypted, the result is the equivalent of a dedicated isolated physical cable.

The Different Types of VPNs

There are three main types of VPNs. They are:

- **Transport mode host-to-host** – A transport mode host-to-host VPN creates a secure connection between two individual systems. In such a VPN, only the payload is encrypted. The headers of the protocol packets, which guide the communication across the intermediary network, remain in their original plain-text form. Thus, the contents of a communication are protected, but the identity of those communicating is exposed.

This type of VPN is commonly used inside private network environments where there is a general level of modest trust of the network, but when additional protection is needed for specific host-to-host communications, such as database replication or periodic backups.

- **Tunnel mode site-to-site** — A tunnel-mode site-to-site VPN creates a secure connection between two different networks or physical locations. In such a VPN, both the payload and the original packet headers are encrypted. An additional tunnel header is added to the encrypted content to direct the communication from one endpoint of the VPN to the other. Communications between two systems are only encrypted while in the tunnel itself. Thus, if a client in Network A sends data to a server in Network B, the initial communication would cross Network A in plain text; then become encrypted as it entered the VPN on the border of Network A; remain encrypted across the Internet until it reached the border of Network B; and then the communication would be decrypted and sent across Network B to the server in plain text. This type of VPN is commonly used to connect remote networks.
- **Tunnel mode host-to-site** — A tunnel-mode host-to-site VPN creates a secure connection between a single computer and a remote network. In such a VPN, both the payload and the original packet headers are encrypted. An additional tunnel header is added to the encrypted content to direct the communication from one endpoint of the VPN to the other. Communications between two systems are only encrypted while in the tunnel itself, which starts on the single computer and ends on the boundary of the remote network. This type of VPN is commonly called a remote access VPN and is used for telecommuting or general remote activities.

When Would a VPN Be Useful?

Whenever communications may be exposed to interception, eavesdropping, spoofing, hijacking, or man-in-the-middle attacks – basically, any time traffic crosses the Internet or an insecure and unfamiliar network connection — a VPN would provide security through communication encryption.

VPNs should be implemented by organizations for securing communications between locations, such as branch offices, and whenever a worker needs to operate from a remote location. VPNs should be implemented by individuals for all of their transactions with any Internet service or resource. This includes using a trusted Internet link at home or at work. It is most important to use a VPN when accessing a public wireless network.

There are hardware and software self-deployment options for VPNS, as well as third-party services. Hardware and software solutions can be implemented into an organization of any size, including home or SOHO environments. These often are single-purchase implementations, without ongoing usage fees. But the implementation, ongoing management, and technical support may be on your shoulders as well. A third-party VPN service would provide secure communications through its servers rather than just through on-site equipment. Such services offer management and technical support, but also have a use fee. Many services also have a throughput and bandwidth consumption cap as well, so it is important to review the details of any VPN service carefully. Some hardware, software, and third-party VPN solutions may offer mobile-device support in addition to standard PC and network VPN connections.

Many VPN solutions, especially those designed for deployment by a large organization, may provide support for multiple types of VPN connections, such as both site-to-site and host-to-site. This would enable a single VPN product to be used to provide secure communications between business locations, while also providing security for remote-access links for telecommuters or other workers who simply need remote access.

What Are the Benefits of a VPN?

Benefits of a VPN include:

- improved communication security through encryption
- secure remote access and/or remote control
- anonymity services, in some instances

- masked client or origin IP address
- blocked attacks from local (physical and logical) attackers

There are other potential benefits as well. Some organizations experience network throughput improvement with the use of VPNs. This may be due to the streamlining of communications and the elimination of ancillary protocols and resource wasting communications. Some organizations also may experience cost savings, mostly from the reduction of recovery and repair costs due to compromises caused by plain-text communications.

When Is a VPN Not the Right Solution?

A VPN is unlikely something an organization should support for its individual employees from company network client systems. Such client-based remote-access VPNs are often used to hide or mask user activities from company filtering and monitoring. If client-based VPN connections are allowed to be established with external Internet providers, then the content of that communications would be encrypted. This enables users to bypass filters, access blocked content, and avoid being monitored. Thus, organizations should provide network-level VPNs for use, but block use of personal client-level VPNs.

However, personal VPNs are exactly what an individual needs when using a public network connection, whether wired or wireless, such as those offered by hotels, restaurants, coffee shops, and conference centers. In these situations, bypassing local attacks or over burdensome operator-monitoring is desired.

There are very few circumstances where a VPN will not provide improved security. However, in certain situations a VPN may cause some inconveniences. For example, if a VPN service provider offers exit nodes in other countries, your traffic may be labeled as “non-domestic” to sites or services that choose to offer their resources to local customers only. This could be true of online banks, many shopping sites, and most streaming entertainment services.

For those sites that do allow international communications and customers, a VPN may still cause some hassle. If the VPN exit node changes from one country to another, a service might assume that your account is under attack due to the change in country of origin, and lock your account. This may require contacting technical support or working through account recovery procedures to access the site. If your account is not locked, a sensitive online service might require additional steps of authentication, such as answering security questions or receiving an email or text message that includes click links or codes that must be responded to in order to prove you are the correct entity connecting to an account.

Thus, in most situations, I would choose to use a VPN, whether for organizational or personal-level use, except where such use is strictly prohibited by company security policy in order to prevent bypassing of monitoring and security controls.

What Is a Firewall?

A firewall is a security product that filters communications. Filtering may be done by blocking or opening ports, blocking or allowing by IP address, or controlling communications using content filtering. The goal of a firewall is to support authorized and legitimate communications while preventing unauthorized or malicious communications. Firewalls can also provide additional services or features, including proxying, NATing (e.g., translating internal IP addresses into public external IP addresses, malware filtering, spam filtering, etc.)

The Different Types of Firewalls

Many kinds of firewalls exist. Most modern or current firewalls are a mixture of types rather than being of a single type. The most commonly described kinds of firewalls are described below:

- A **packet-filtering** firewall is a fairly basic type of firewall that grants or denies communication solely on an IP address and/or port number. Any time a firewall supports communications for all visitors at all times, such as when offering an open port to access a website, a packet filtering rule is in use.

- A **circuit-level** firewall makes an allow/deny decision based on several potential parameters, including IP address, port, user account, and time. This type of firewall determines whether to allow a connection to exist or not. If allowed, no future filtering is applied to the connection.
- An **application-level** firewall focuses on a single application or protocol. Such a firewall is able to perform content inspection in order to allow or deny communications based on the content. If disallowed content is discovered, the packets are dropped, and the connection might be terminated.
- A **stateful-inspection** firewall is designed around filtering based on valid communications. It is aware of proper content and context of communications. If a valid request for content is received, it is allowed through; if an invalid request or a malformed request is received, it is blocked.

In addition to these types of firewalls, there are also hardware and software firewalls. A hardware firewall is a dedicated computer configured to exclusively provide firewall services. A software firewall is an application installed onto an existing OS that adds firewall services to the existing programs and services on that system.

When Would a Firewall Be Useful?

A firewall should be used whenever there is a change in trust level between one network segment and another. A firewall should also be used between a network connection and a local system (whether standalone, client, or server). There is always a risk of invalid communications reaching your system across a network link; thus, blocking and filtering traffic reduces the risk of being compromised by such communications.

What Are The Benefits Of A Firewall?

The benefits of a firewall include: filtering communications; blocking unauthorized or malicious transmissions; isolating a private network from a public or untrusted network; reducing hacking events; blocking spoofed traffic; and technical enforcement of network security policy. Depending upon the features provided in a specific firewall, the list of benefits could be greatly expanded.

Is a UTM Available That Can Provide Both VPN and Firewall Functions?

A unified threat management (UTM) solution can combine multiple-network communications, management services, and security features into a single product. There are several UTMs, which may be marketed as firewalls with extra features that can provide both firewall and VPN services. Such a UTM may be a good choice for smaller environments with minimal IT staff and budget.

However, larger organizations should consider implementing separate solutions for firewall and VPN in order to obtain best-of-breed products in each category rather than settling for whatever service or feature happens to be present on a UTM. Implementing a hardware firewall along with a software VPN solution, or vice versa, is also possible. When considering deploying separate firewall and VPN products, evaluate the best implementation architecture for your needs. If you want the VPN to provide direct access in and out of the private network with minimal interruption, then deploying the VPN inside the firewall would be the optimal arrangement. However, if you need to filter all traffic, whether over a public open link or a VPN link, then deploying the VPN device outside of your firewall would be the required deployment configuration.

Hardware vs. Software Solution: Which Is the Better Choice?

A hardware solution for a firewall or VPN will provide dedicated hardware resources to that specific function and service. Such appliance devices are designed to provide high-performance operations for their specific tasks. However, hardware devices can be quite expensive. Hardware devices can often be improved through firmware updates. But at some point, the next generation of a product will provide features that the old hardware cannot support. Dedicated hardware cannot be repurposed for other uses if the product becomes obsolete or gets replaced in the future.

A software solution for a firewall or VPN will depend upon the available system resources on the host system. Other applications and services will be competing for resources. If there is significant contention for resources, the security services may be unable to provide reliable or consistent operation. A software solution can often be a less expensive alternative to a hardware solution, but reliability and stability may be sacrificed for those savings. As the product is improved over time, updates can bring new features and capabilities to bear. However, significant updates might require purchase of a newer version or a license extension.

General Deployment Recommendations and Security-Policy Crafting

When deploying a firewall and/or VPN, it is important to plan out the deployment and the security policy before starting the actual implementation. When deploying a firewall, a good starting point is to inventory the communications that are required for business tasks or personal activities. This would include a list of protocols, ports, and applications. Then, review the documentation of the firewall. This should this help in drafting a step-by-step procedure on how to use the specific firewalls management interfaces to implement the filtering and security service settings in order to support your communications.

When deploying a VPN, a good starting point is to craft a list of the circumstances where VPN services are required, recommended, or may interfere. This should help determine which of the three types of VPN are needed to provide secure communications. While crafting the security policy for the VPN, be sure to define requirements for using a VPN, as well as configuration and settings specifics. This should include an acceptable-use policy.

Once a firewall or VPN has been implemented, thoroughly test that all intended configurations are operational. Confirm through testing that all forms of authorized communications are possible and forms of unauthorized communications or connections are blocked. On a regular schedule, review the security policy and configuration settings of your firewall and VPN. Make adjustments as technology changes, as your business tasks evolve, and as new attacks are discovered.

Conclusion

VPNs and firewalls are highly recommended security solutions that can be used to protect your IT assets from threats, and they are essential elements of both business networks and personal device connections. Communication filtering and encryption are foundational components of a secure network infrastructure.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Network Security, Firewalls, and VPNs

JNCIS Security Certification Boot Camp

Palo Alto Networks: Essentials 1

Palo Alto Networks: Essentials 2

SASAC - Implementing Core Cisco ASA Security v1.0

More courses are available through Global Knowledge’s Cybersecurity Skills Development portfolio under the

Cybersecurity VPN, Firewalls and Intrusion Prevention section. Visit www.globalknowledge.com or call 1-800-COURSES (1-800-268-7737) to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of CISSP Study Guide, 6th Edition; CompTIA Security+ Review Guide: SY0-401; Security+ Review Guide, 2nd Edition (SY0-301); CompTIA Security+ Training Kit (Exam SY0-301); and Network Security, Firewalls, and VPNs.

Michael has also contributed to many other security-focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.