Internet Security for Small to Medium Sized Businesses

AN INTERNET SECURITY GUIDE FOR EVERY BUSINESS

DOCUMENT VERSION 1.2 - OCTOBER 2002

COMPLIMENTS OF POWERWALLZ NETWORK SECURITY INC.

WWW.POWERWALLZ.COM

Introduction

INTERNET ACCESS IS INDISPENSIBLE — AND INSECURE

The Internet has become an indispensable business tool. Broadband technologies such as ISDN, DSL and Cable have made it possible for more businesses to enjoy the benefits of always-on, always available Internet connectivity – improved and expanded communications between customers, partners and internal staff. Unfortunately, it also increases the potential for network security breaches.

This paper is a security primer for Internet security. It provides the information that a small to medium business would need to help understand their security needs:

> The risks associated with always-on, always available Internet connectivity
> Firewall technology
> Firewall deployment strategies
> Security needs
> PowerWallz security products

Risks

UNDERSTANDING THE RISKS HELPS YOU PROTECT YOUR BUSINESS

As Internet usage increases and becomes commonplace, so do the risks. It is no longer just large enterprises that need to worry about security issues. There are many types of risks that affect all computers connected to the Internet and with the increasing usage of broadband technologies, more computers are noew susceptible as targets.

HACKER ATTACKS

These can be described as direct attacks on an organization's computers. The perpetrator is looking to attack a company directly. They are after data or are trying to disable the organization's Internet access. In many cases, the web site or the Internet connection is being attacked with denial of service attacks.

TROJAN HORSES

Computers are now being hijacked and used as tools to deploy greater attacks. By implementing Trojan horse programs, computers become part of a network of computers that are used to implement distributed denial of service attacks such as: Smurf, Tribe Flood Network and Trinoo against other sites. It was this type of attack that disabled large sites such as Yahoo not that long ago.

VIRUSES

Viruses have always been a threat, but until recently, most viruses have needed some kind of human intervention to spread. Now viruses are able to replicate and spread throughout networks automatically. To stop viruses, a number of strategies must be used. This includes filtering at the firewall as well as at the desktop.

CONTENT FILTERING

A content filter allows businesses to implement policies that dictate what is acceptable for people to access using the company's computers. In many corporations, formal Acceptable Use Policies have been implemented. Abuse causes many problems, both technical and social. Inappropriate material may offend people and may lead to legal issues for a company. Widespread access of inappropriate material will affect bandwidth utilization and may affect usage for legitimate purposes.

INTERNAL

Security problems can also originate internally within an organization. This can be controlled by limiting access to the Internet or tracking usage and reporting on inappropriate usage.

The Firewall

PROTECTION FOR YOUR BUSINESS

Most firewall products — both software and hardware — are usually grouped into one of four major categories:

> Packet Filters
> Application Gateways
> Circuit Level Gateways
> Stateful Inspection Firewalls

The following sections describe each of these functions and the platform choices available.

PACKET FILTERING

A packet filtering firewall monitors the source and destination IP of any connection. It then verifies the destination port of the same connection and then matches it against it's configuration to allow or deny a connection. A packet filter does not check content. This means that no connection is monitored or protocol validated to a set of rules.

Can a packet filter be fooled? By spoofing an IP address (making it appear traffic is from an IP address that it isn't) one can already send unwanted packets into a network, but routing remains an obstacle seeing return traffic from such an attack. This may be over-come but requires further factors or access. Port re-writing is another popular method to fool packet filters.

The use of packet filtering in those routers can be a cost-effective mechanism to add firewall capability to an existing routing infrastructure. Generally speaking, packet filtering routers offer the highest performance firewall mechanism. However, they are harder to configure because they are configured at a lower level, requiring you to have a detailed understanding of protocols.

The biggest advantage of packet filtering firewalls is speed. Unfortunately, there are many known problems with packet filtering firewalls that hackers can use or exploit. Examples of packet filtering technology can be found in many of the lower-priced, home firewall products.

APPLICATION PROXY GATEWAYS

An application Gateway allows a connection to be made to the firewall and then initiates a connection on behalf of the user to the server. The host on which the proxy runs does not need to be acting as a router. When a client program establishes a connection "through" a proxy to a destination service, it first establishes a connection directly to the proxy server program. The client then negotiates with the proxy server to have the proxy establish a connection on behalf of the client between the proxy and the destination service. If successful, there are then two connections in place: one between the client and the proxy server and another between the proxy server and the destination service. Once established, the proxy then receives and forwards traffic bi-directionally between the client and service.

This means that inherently, connection state information is maintained and that content can be filtered if the application on the firewall (sometimes referred to as a proxy) is configured to expect only certain traffic. Because an application gateway connects on behalf of the user, this kind of firewall is inherently strong on logging and recording traffic and authentication. As one can gather from the fact that a process is run for each expected service, this type of firewall puts a great amount of load on a machine. The other drawback of this type of product is that it is not seamless to the user at all. Applications, routing, browsing and mail needs to point at the firewall or an aliased IP address on the firewall for connections. UDP connections are not handled with ease.

Generally speaking, application proxies are slower than packet filtering routers. However, application proxies are, in some ways, inherently more secure than packet filtering routers.

CIRCUIT LEVEL GATEWAYS

A circuit-level gateway is a firewall that runs an application that allows connections through it and copies the bytes across for any connection flowing through it, thus creating a circuit. This type of firewall has its own strengths in that it does not proxy a connection but rather just monitors a connection through it. This kind of firewall is more transparent to the user. The content checking is limited however for this kind of firewall. This means that a protocol could be further scrutinized and parsed (for instance http commands) to verify validity.

Some features of circuit level gateways are:

> More secure than packet filter, but not as secure as application proxies
> Relay TCP connections
> Permission granted by port address
> No application level checking
> Can understand what is in packet

STATEFUL PACKET INSPECTION

Many firewalls now have combined the concept of application proxy-based firewalls and circuit-level gateways with stateful inspection technology. This means that this kind of firewall is seamless to the user if you want it to be.

The principle motivation for stateful inspection is a compromise between performance and security. Stateful inspection provides much better performance than application proxies. It also provides more firewall functionality than simple packet filtering. Like proxies, more complex access control criteria can be specified and like packet filtering, stateful inspection depends on a high quality (i.e., correct) underlying routing implementation.

> It does content checking passing protocols through a validation exercise.
> It keeps a state-table of connections whereby it monitors the state of a TCP connection and allows traffic accordingly.
> It does address translation.
> It can authenticate connections.
> Parses UDP through a set of rules and expected responses. PowerWallz has utilized technology that allows the firewall to treat "stateless" protocols such as UDP as stateful packets.

Hardware vs. Software

Firewalls traditionally have been software implementations, but firewall appliances (turnkey hardware/software devices) have become very popular. Both products are designed to provide Internet and network security.

THE HARDWARE FIREWALL APPLIANCE

Firewall appliances come with software embedded and bundled with the hardware platform, making them faster to deploy and configure than pure software firewalls. If you are installing a firewall as a result of a security incident, speed of implementation may be critical to your selection. Appliance firewalls are not necessarily more secure – the real value is in their speed of implementation, cost savings, and ancillary features such as high availability and load balancing.

Main advantages of firewall appliances are:

> They offer the convenience of an all-in-one turnkey approach.
> Installations are much less complex, especially for those lacking security skills.
> Compatibility with software-only solutions.
> Appliances use hardened, embedded operating systems that are inaccessible to end users, thereby minimizing security threats and configuration needs.
> They don't require any additional hardware

THE SOFTWARE FIREWALL

The biggest advantage of software-based firewalls is that they offer more flexibility and scalability because of their configuration options. The biggest disadvantage is the added time they take to procure and implement. Because of their richer configuration options, software firewalls often take longer to deploy and therefore, cost more to implement. There is also a greater risk of configuration errors leading to security holes.

Because hardware firewalls don't require any installation – and carry lower prices – the startup costs both in real dollars and resources also are lower. This is a point that hardware firewall vendors love to tout, and it's a significant one for shops where the advanced server-administration skills required to successfully install and configure an OS and firewall software are in short supply. PowerWallz products are hardware-based with hardened operating systems.

Main advantages of software firewalls are:

> Can be easily integrated into enterprise-level platforms (i.e. must be Windows-based)
> They have a higher degree of performance scalability because the software can be deployed onto more powerful equipment as needed.
> Software-based firewalls can usually be installed on companies' existing hardware, thus reducing overall equipment costs and associated space requirements.

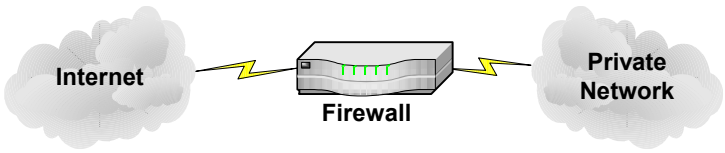
It is important to note that software-based firewalls and firewall appliances are not mutually exclusive. Because the two can be easily integrated, several companies have utilized both versions to construct a customized security platform.

Firewall Implementations

To get a better understanding of firewall technology and how it can be implemented, here are the main methods of setting up and deploying firewall protection.

BASIC

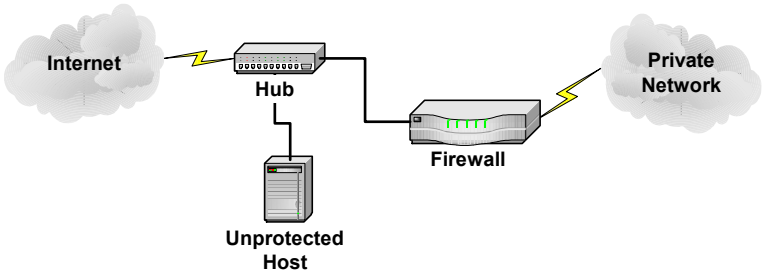
This is the starting point for all firewalls. A basic border firewall is a single host interconnecting an organization's internal network and some untrusted network, typically the Internet. In this configuration, the single host provides all firewall functions. This architecture is very easy and quick to deploy and is good for simple Internet connectivity, but offers limited functionality.



UNPROTECTED HOST

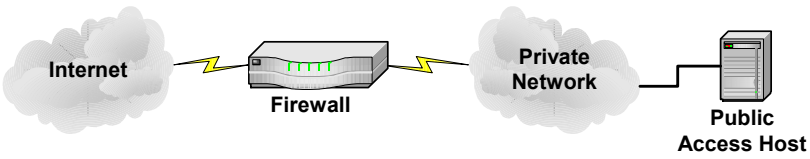
To the basic border firewall, add a host that resides on an untrusted network segment where the firewall cannot protect it. That host is minimally configured and carefully managed to be as secure as possible. The firewall is configured to carefully manage traffic

between the private network and the untrustworthy host. The host is referred to as untrustworthy because it cannot be protected by the firewall; therefore, hosts on the trusted networks can place only limited trust in it. This configuration allows a company to deploy public hosts (i.e. web and mail servers) without compromising internal network security. Unfortunately, without being protected, there is a high security risk on the hosts themselves.



PROTECTED HOST ON LAN

In this configuration, the untrusted host is brought inside the firewall onto the private network. The firewall is configured to carefully manage traffic between the Internet and the untrustworthy host. Only specific traffic is allowed between these two segments. This provides greater security protection for the public hosts, but a breach of these servers would compromise the security of the internal network.

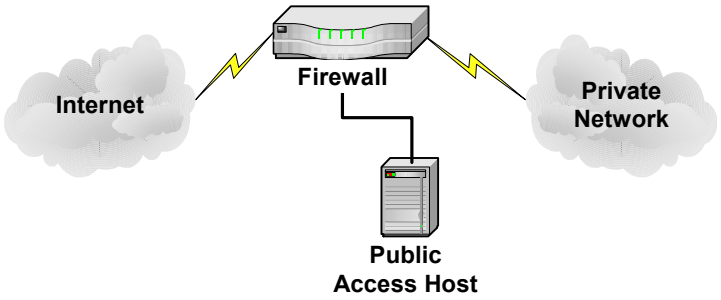


PowerWallz firewall products can easily be deployed using any of the above with little or no configuration. In many cases, the firewall can be dropped in using the pre-configured rules and stealth mode.

DEMILITARIZED ZONE (DMZ)

In a DMZ network, the untrusted host is brought "inside" the firewall, but placed on a network by itself (the firewall host then interconnects three networks). This increases the security, reliability, and availability of the untrusted host. Other hosts for other purposes (for example, a public web site or ftp server) can easily be placed on the DMZ network,

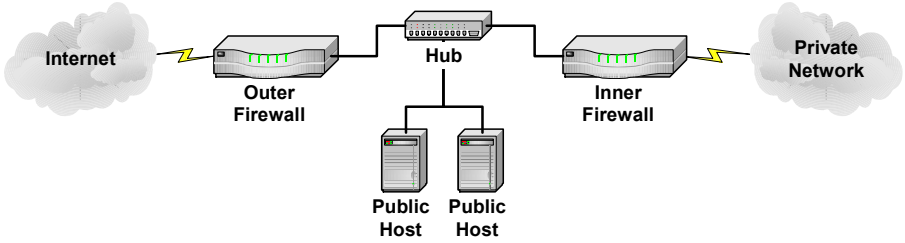
creating a public services network. Again, the firewall is configured to carefully manage traffic between the three distinct networks. Any breach of security on the DMZ network will not result compromise the internal private network.



PowerWallz firewall products can be easily deployed using this design because most of the products come with a built in DMZ port for adding a third network. This means no additional hardware costs or upgrades are required with the PowerWallz products.

DUAL FIREWALL

The organization's internal network is further isolated from the untrustworthy network by adding a second firewall host. By connecting the untrustworthy network to one firewall host, the organization's internal network to the other, and the DMZ between, traffic between the internal network and the Internet must traverse two firewalls and the DMZ. This design offers the greatest security protection for all hosts, both in the DMZ and the private network. This configuration is best utilizing a firewall with "stealth" technology as the outer firewall.



PowerWallz firewall products can be easily deployed using this design because the products utilize the "stealth" technology. This allows the Outer firewall to be completely transparent to the Internet, yet provides the full protection for the Public Hosts and Private Network. By utilizing the "stealth" technology, minimal configuration and management is required to deploy this network design.

Business Security Needs

The security needs of small to medium sized businesses will vary greatly, but will likely be very similar. In general, a small to medium sized business needs a security product to provide one or more of the following:

> Secure Internet connectivity to one or more computers securely
> Secure public hosts such as web servers and email servers
> Some content filtering
> Limited secure access to internal resources
> Flexibility to change with business needs
> Ease of deployment and manageability

The last point is a very important one as many businesses of this size will not have dedicated IT staff, let alone security specialists. Many will not have the resources to hire them either. The solution they select will need to be easy to deploy and manage. As well, it should be cost effective to use and flexible enough to grow with them as the company grows.

PowerWallz security products are developed to meet the needs of the small to medium business. They employ the best security features from higher-priced products, yet retain the ease of use and manageability of lower-priced, simpler products.

PowerWallz Security Products

FEATURES & BENEFITS

PowerWallz's ProShield X100DMZ and v1000 security appliances offer the best features and benefits for the small to medium sized business.

STEALTH MODE

The ProShield X100DMZ can be deployed without being visible to anyone on the Internet. It acts as a transparent device, thereby, making it impossible for potential hackers to identify and attack it. The ProShield X100DMZ surpasses other firewalls that offer this technology by being able to combine this feature with other advanced features such as stateful inspection.

STATEFUL INSPECTION

Originally developed by CheckPoint Software, this technology provides the best combination of security and performance. It intelligently analyzes network traffic and determines whether the packets should pass through the firewall or not. All PowerWallz ProShield security appliances deploy this technology. The ProShield X100DMZ security appliance has the unique ability to utilize stateful inspection while in stealth mode, therefore, offering greater flexibility and security.

NAT

Virtually all firewall devices utilize this technology. Network Address Translation protects internal networks by masking the internal network IP addresses with one or more external addresses. This gives the internal network greater security because a potential hacker cannot determine how the internal network is configured. All ProShield security appliances support NAT, multiple-IP NAT and masking, therefore, giving it more flexibility and security than all its competitors. This feature also allows a company with many computers to share an Internet connection.

PLUG & PLAY

Unlike other vendors that claim that their products are plug and play, PowerWallz firewalls can be truly plug and play. In some instances, deploying a PowerWallz firewall can be as easy as attaching the network cables (Internet and LAN) and plugging it in – with no configuration required. At the same time, the firewalls can be easily configured if needs change.

UNLIMITED USERS

The ProShield X100DMZ and v1000 appliances offer support for an unlimited number of users. This allows a company to grow without having to incur greater expenses and eliminates problems with confusing and complicated licensing schemes.

DOWNLOADABLE UPDATES

Firmware updates can be easily downloaded and installed. By utilizing the management client, users can easily download the latest firmware for their firewalls or be used for advanced functions such as: additional features, preset configurations, and even technical support fixes.

ALERTS

The ProShield X100DMZ will provide real-time alerts of any potential attacks on the firewall. By providing proactive alerts, it reduces the time required to manually monitor the firewall. It also gives companies time to react to potential attacks and to implement any security measures necessary to prevent the attacks or to gather information to help track the hacker. The v1000 provides alerts if there are unsuccessful attempts to access the administration tools.

VPN

Virtual private networking allows remote users to connect to internal resources. It also allows remote offices to create a private network using the Internet. The ProShield X100DMZ supports both site-to-site and remote user VPNs. This means that multi-office companies and companies with remote users will be able to allow access to important resources within the internal network, yet remain protected. The V1000 also offers vpnNOW, which simplifies the process of setting up and configuring VPN connections. Interoperability with other products such as Checkpoint Firewall-1 have been simplified as well. This makes the V1000 the ideal choice for branch offices where dedicated technical personnel may not be available. The V1000 has better VPN performance and will support a greater number of simultaneous VPN connections, including remote, mobile users.

IP BLOCKING

Specific IPs and machines can be blocked from accessing the internet completely. This helps manage the number of computers accessing the Internet and also helps reduce unauthorized traffic leaving the internal network.

MULTIPLE IP ADDRESSES AND MULTIPLE NAT

The ProShield X100DMZ and v1000 can be set up to "answer to multiple IP addresses". This is useful when NAT is being used and there are multiple internal servers that need to be accessed from the Internet.

PORT REDIRECTION

For companies that have more advanced needs, full port direction can be used. This allows traffic to be redirected based on IP ports. This helps increase security when allowing access to internal servers. Instead of using common well-known ports, the firewall can be set up to answer to customized port, but then redirect to internal server using normal port number.

DHCP

Full DHCP support gives the ProShield security appliances greater flexibility to be deployed in any situation. In new networks that need DHCP to assign IP addresses, the ProShield X100DMZ and v1000 hava a built-in DHCP server than can be configured to serve this function if required. As a DHCP Client, the ProShield security appliances can request an external IP address for itself from the ISP. Again, this reduces set up and configuration time needed to deploy the firewall. In Passthru mode, the ProShield security appliances provides firewall security, but allow DHCP requests to seamlessly pass between internal computers and the ISP.

FORM FACTOR

The ProShield X100DMZ is available as a 5" standalone unit. The v1000 is available in a 9" standalone case as well as a 19" rack mountable case. With this flexibility, the PowerWallz's ProShield security appliances can be easily deployed and used by home offices as well as large companies with dedicated computer rooms.

POWERWALLZ — SMART. SIMPLE. SECURE.

The Internet is a valuable business tool. It offers tremendous communications benefits, but also brings with it increased security risks. By taking the necessary precautions, such as deploying a PowerWallz firewall product, businesses can reduce their security risks at utilize the Internet for its full potential.

PowerWallz products are designed to offer network security solutions for any business. Our products are smart, simple, secure and affordable.

For more information about a PowerWallz network security solution for your business, contact us at:

PowerWallz Network Security Inc.
228 - 1027 Davie Street
Vancouver, BC, V6E 4L2

Phone: 604.233.2837
Fax: 604.233.2832

Email: sales@powerwallz.com
Web: www.powerwallz.com