NEXTEP *Broadband* **White Paper**

Firewall Architecture

Understanding the purpose of a firewall when connecting to ADSL network services.

A Nextep Broadband White Paper
June 2001

Firewall Architecture

WHAT IS A FIREWALL?

In order to keep a corporate network secure, companies protect and isolate their internal systems from the Internet with a network firewall. Simply put, a firewall prevents certain outside connections from entering your network. A firewall will trap inbound or outbound packets, analyse them, and then either permit access or discard them.

The firewall (sometimes referred to as a bastion host) is a sub-system of computer software and hardware that intercepts data packets before allowing them into or out of a Local Area Network (LAN). A firewall makes decisions on whether or not data is allowed to pass based upon a security policy. For each packet of data, the firewall compares known components of the packet to a security rule set and decides if the packet should be allowed to pass.

In addition, a firewall may have security rules that involve altering the packet in some basic ways before passing the data. With a sensible security policy and a security rule set designed to implement that policy, a firewall can protect a LAN from attacks.

FIREWALL TYPES

A true firewall is the hardware and software that intercepts the data between the Internet and your computer. All data traffic must pass through it, and the firewall allows only authorized data to pass into the corporate network.

Firewalls are typically implemented using one of four primary architectures:

- Packet Filters
- Circuit-level Gateways
- Application Proxies
- Network Address Translation

Packet Filters

The first line of defense in firewall protection, and most basic, is the packet filter firewall. Packet filters operate at the Network Layer to examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass.

The packet filter firewall is typically very fast because it does not examine any of the data in the packet. It simply examines the IP packet header, the source and destination IP addresses, and the port combinations, then it applies filtering rules.

For example, it is easy to filter out all packets destined for port 80, which might be the port for a web server. The administrator may decide that port 80 is off limits except for specific IP sub-nets, and a packet filter would suffice for this.

Packet filtering is fast, flexible, transparent (no changes are required at the client) and cheap. Most routers will provide packet filtering capabilities, and pure packet filter firewalls do not require powerful hardware.

This type of filter is commonly used in small to medium business that need to control where users can or cannot go. IP addresses can be spoofed so using this type of filter by itself is not enough to stop an intruder from gaining access to your network. Nevertheless, a packet filter is an important element of a complete firewall solution.

Circuit-level Gateways

One step above standard packet filtering firewalls, but still considered part of the same architecture, are circuit level gateways, otherwise known as “stateful packet inspection” firewalls. In the circuit-level firewall, all connections are monitored and only those connections that are found to be valid are allowed to pass through the firewall.

This generally means that a client behind the firewall can initiate any type of session, but clients outside the firewall cannot see or connect to a machine protected by the firewall.

Stateful inspections usually occur at the Network Layer, thus making it fast and preventing suspect packets from travelling up the protocol stack. Unlike static packet filtering, however, stateful inspection makes its decisions based on all the data in the packet (corresponding to all the levels of the OSI stack).

Using this information, the firewall builds dynamic state tables. It uses these tables to keep track of the connections that go through the firewall -- rather than allowing all packets that meet the rule set's requirements to pass, it allows only those packets which are part of a valid, established connection. Packet filtering

firewalls are popular because they tend to be inexpensive, fast, and relatively easy to configure and maintain.

Application Proxies

Working at the application of the OSI stack, a proxy firewall forces all client applications on workstations protected by the firewall to use the firewall itself as a gateway. The firewall then authorizes each packet for each protocol differently.

There are some disadvantages to using this type of firewall. Every client program needs to be set up to use a proxy, and not all can do so. Also, the firewall must have a proxy in it for each type of protocol that can be used. This can mean a delay in implementing new protocols if the firewall doesn't support it.

The penalties paid for this additional level of security are performance and flexibility. Proxy server firewalls have large processor and memory requirements in order to support many simultaneous users, and introduction of new Internet applications and protocols can often involve significant delays while new proxies are developed to support them.

True proxy servers are undoubtedly the safest, but impose an overhead in heavily loaded networks. Dynamic packet filtering is definitely faster, though most of the high-end firewalls are hybrids these days, incorporating elements of all architectures.

Network Address Translation (NAT)

Firewalls using NAT and/or Port Address Translation (PAT) completely hide the network protected by the firewall by using many-to-one address translation.

In most NAT implementations there is a single public IP address used for the entire network. All packets going outside the network have their internal IP addresses hidden for security, so any incoming packets are delivered to the network's public IP address. To handle ensuing port conflicts, PAT needs to be added to NAT.

A disadvantage of NAT is that it can't properly pass protocols containing IP address information in the data portion of the packet.

DEMILITARIZED ZONES

A demilitarized zone (DMZ) isolates hosts which are accessible from outside the network (e.g. a web server or FTP server) from internal servers. The external hosts are placed in a separate network zone, on a separate adapter, connected to the firewall. This creates the DMZ. This is easily achieved with a firewall with three or more interfaces.

Each subnetwork is also configured with its own security zone (e.g. the Finance network, the Sales network, etc.) by connecting it to a separate firewall adapter. All traffic between zones, and all traffic from the Internet to all zones, is checked by the firewall.

In this way, each zone is isolated, and the systems in each zone only trust other systems within the same zone. Therefore, if a hacker succeeds in breeching an accessible host, the other hosts within the network are still safe.

DMZs are often used for special servers, such as web servers, which must be accessible from two separate networks. Usually an organization has one Internet connection, one local network and one DMZ with servers that must be both internally and externally accessible. This is shown in the following diagram.

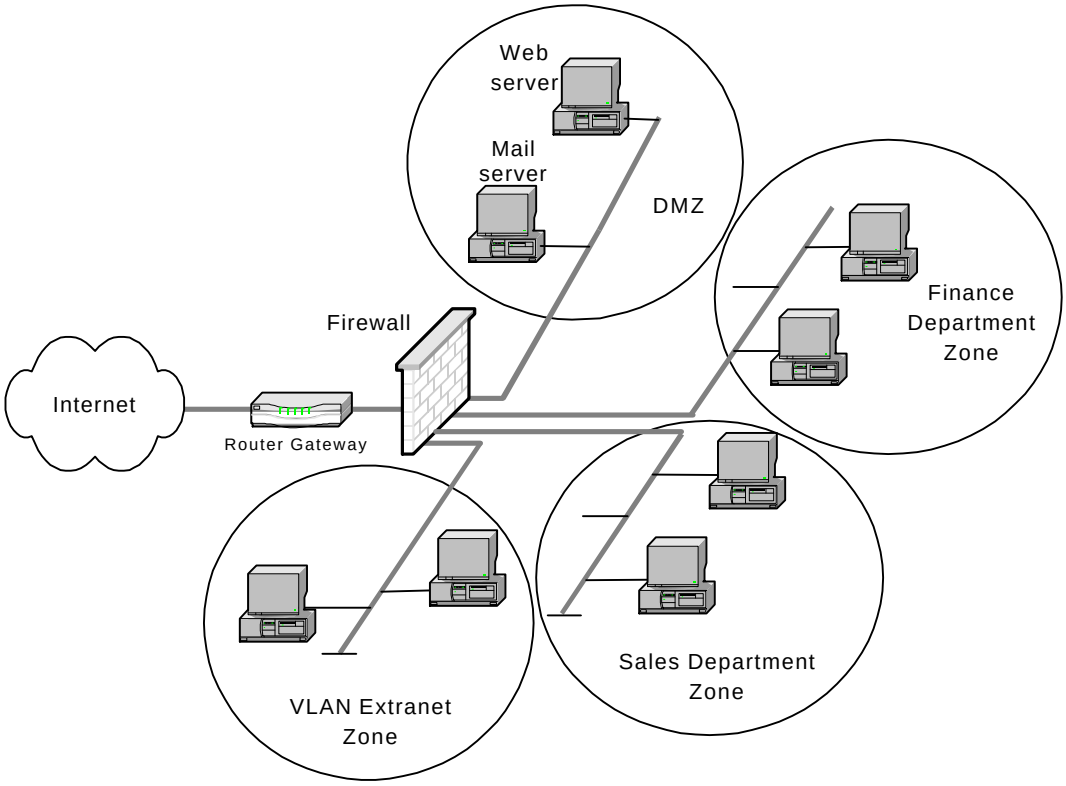

Figure 1 – Demilitarized Zone Configuration

FIREWALLS WITH VPNS AND VLANS

If you are using or considering an IP virtual private network (VPN) you need to consider where to place the VPN device in relation to the firewall, as a firewall cannot enforce access of encrypted traffic.

- **Inside the firewall:** If a Windows-based VPN server is placed inside the firewall, you will probably have to upgrade the firewall firmware or hardware to enable passthrough of encrypted IPSec or PPTP packets.
- **Outside the firewall:** To avoid upgrading or replacing your firewall, especially if you are using NAT or PAT, you can place your VPN server outside the firewall. The danger here is that traffic between the VPN device and the firewall does not have full security.
- **Integrated with the firewall:** To place the VPN termination at the firewall will require routing equipment or software that will perform both the VPN and firewall function. This is the most efficient and secure mode of operating a VPN and firewall.
- **Inside the DMZ:** In this configuration, VPN traffic is delivered to the firewall both when it arrives and after it is encrypted or decrypted by the VPN device. This provides high security, but can slow down the VPN.
- **In parallel with the firewall:** Of all options, this is the least secure because a standalone VPN server is not equipped to defend itself against attacks and presents an open doorway to your corporate resources.

Note: A virtual local area network (VLAN) type of VPN is a bridged connection between two or more LANs. This is different from an IP VPN because it uses virtual circuits, which means no firewalls or VPN devices are needed because the VLAN is shielded from other traffic.

FIREWALL POLICIES

If an intruder can find a hole in your firewall, then the firewall has failed. Once a hacker is in, your internal network is severely compromised.

No firewall can protect against inadequate or mismanaged policies. If a password gets out because a user did not properly protect it, your security is at risk. If an internal user dials out through an unauthorized connection, an attacker could subvert

your network through this backdoor. Therefore, you must implement a firewall policy.

Policy vs. Users

Obviously, the firewall and the firewall policy are two distinct things that require their own planning and implementation. A weakness in the policy or the inability to enforce the policy will weaken any protection provided by even the best firewalls.

If internal users find your policies too restrictive, they may go around them by connecting to the Internet through a personal modem. The firewall in this case is useless. You may not even know your systems are under attack because the firewall is guarding the wrong entrance.

The most basic firewall policy is:

Block all traffic, then allow specific services on a case-by-case basis.

This policy is restrictive but secure. However, it may be so restrictive that users circumvent it. In addition, the more restrictive your policy, the harder it will be to manage connections that are to be allowed.

Contents of a Firewall Policy

Security policies must be outlined in advance so administrators and users know what type of activities are allowed on the network. Your policy statement should address:

- internal and external access
- remote user access
- virus protection and avoidance
- encryption requirements
- program usage

Ensure your policy includes the following considerations:

- All incoming and outgoing network traffic must go through the firewall (i.e., that no traffic which bypasses the firewall is permitted, for example, by using modems). The traffic must be filtered to allow only authorised packets to pass.
- Never use a firewall for general-purpose file storage or to run programs, except for those required by the firewall. Do not run any services on the firewall except those specifically required to provide firewall services. Consider the firewall expendable in case of an attack.

- Do not allow any passwords or internal addresses to cross the firewall.
- All access to the firewall itself is blocked from the Internet. Almost all access to the firewall is blocked from inside the network. The only people with access to the firewall should be the firewall administrators.
- If you need to provide services to the public, put them on the outside of the firewall and implement internal settings that protect the server from attacks that would deny service.
- Accept the fact that you might need to completely restore public systems from backup in the event of an attack.

Before the security policy is converted to the firewall rule set, ensure that the policy is not overly complex and that the firewall rule set is kept to a minimum. Implementing a relatively simple policy/rule set combination can actually enhance security and greatly assists with ongoing operational maintenance.

CONTRIBUTING COMPANIES

For over a year, two of Australia's leaders in DSL technology have worked together to perfect a cost-effective high speed broadband service for small and medium enterprises (SMEs).

The result is a new business enterprise, Nextep Broadband, bringing together the expertise of NEC Australia and xDSL Limited.

NEC Australia

NEC Australia has more than 7 years experience with broadband deployments in Australia, New Zealand, Spain, Hong Kong and Venezuela, and is the DSL Global Design Centre for NEC Corporation.

NEC's DSL-based system is a standards-based, fully managed, multi-service access platform designed for carrier and enterprise applications. System interoperability has been tested and confirmed with more than 20 major CPE vendors and a range of backend server, switch and transmission equipment.

xDSL Limited

xDSL Limited was established in 1999 to explore the commercialisation of DSL as a broadband technology in Australia. Its major shareholders include ASX-listed Sirocco Resources N.L., RMB, and AIB investments.

xDSL has a 26.7% interest in VOD Pty Limited, a joint venture with the Sirocco group and Civic Video. VOD is currently deploying video-on-demand over the TransACT network in Canberra.

xDSL has considerable experience in deploying content and other broadband services in commercial environments. The success of xDSL is due in large measure to its highly focused and skilled team assembled from a broad mix of backgrounds and disciplines.

"Firewall Architecture" Rev 1.0
Written by Robert Slemp for NEXTEP Broadband

This document is printed for informational purposes only and the information herein is subject to change without notice.

This document is written for installations where all items are supplied by Nextep Broadband and the system integration has been completed by Nextep Broadband personnel. Nextep Broadband is not responsible for overall system performance, thermal characteristics, EMC and safety issues where the customer uses third party equipment and the system integration has been completed by parties other than Nextep Broadband.

649-655 Springvale Road
Mulgrave, Victoria 3170 Australia

Phone: (03) 9271 4240
Fax: (03) 9271 4249