Helping you piece IT together

An Overview of Firewalls

Disclaimer:
BH Consulting has made every reasonable effort to ensure that information contained within this document is accurate. However no representation or warranty, expressed or implied, is given by BH Consulting as to the accuracy or completeness of the contents of this document or any information supplied. Recommendations outlined in this document are based on accepted industry best practises.

The information contained in this document has been provided by BH Consulting for information purposes only. This information does not constitute legal, professional or commercial advice. While every care has been taken to ensure that the content is useful and accurate BH Consulting gives no guarantees, undertakings or warranties in this regard, and does not accept any legal liability or responsibility for the content or the accuracy of the information so provided, or, for any loss or damage caused arising directly or indirectly in connection with reliance on the use of such information. Any errors or omissions brought to the attention of BH Consulting will be corrected as soon as possible.

Any views, opinions and guidance set out in this document are provided for information purposes only, and do not purport to be legal and/or professional advice or a definitive interpretation of any law. Anyone contemplating action in respect of matters set out in this document should obtain advice from a suitably qualified professional adviser based on their unique requirements.

The information in this document may contain technical inaccuracies and typographical errors. The information in this document may be updated from time to time and may at times be out of date. BH Consulting accepts no responsibility for keeping the information in this document up to date or any liability whatsoever for any failure to do so.

BH Consulting are under no obligation to update this document or correct any inaccuracies or omissions in it which may exist or become apparent.

Table of Contents

1. Overview of Firewalls

As more and more companies attach their networks onto the Internet, many are considering how best to protect their computing assets from unauthorised access from the Internet. One of the methodologies used is the implementation of a network firewall. A firewall is located at the outer limit of the corporate network where it connects onto the Internet. All incoming and outgoing traffic is then filtered through this firewall. Therefore a firewall in many ways is similar to a security guard on duty at the front door of a company's building. The security guard ensures that people entering the building have permission to enter the building and those leaving the building are not taking corporate assets with them.

1.1 Security Guard Analogy

Like a firewall, a security guard's duty is to control traffic into and out of a building. For this control to be effective there must be only a single entrance through which all traffic passes. Security guards may function at different levels depending as to how secure the building should be. For some buildings a name badge attached to an employee's person's pocket is sufficient authentication. More rigorous authentication might require a combination of the name badge and an entry code or PIN, and include a computerised recording of the badge number and time. The most rigorous authentication could involve a gateway with two doors, and each person subjected to a biometrics authentication method such as fingerprint recognition, before being allowed entering the inner door. The security guard might also be directed to examine the contents of large purses, briefcases or packages, looking for items such as recording devices, explosives and weapons

A firewall provides the security at the entranceway to a network, for example a connection to an external network such as the Internet. The firewall should function at the level required by the organisation's policy for authenticating traffic, collecting sufficiently detailed logging, and perhaps inspection of data which passes through the firewall for computer viruses and harmful code such as malicious applets, Java and ActiveX scripts.

Just as there are many different types of security guards, some are more thorough than others; there are many different firewall products available.

As with all security products the firewall should be a tool used to enforce the company's security policy. The company's security policy should define what assets are essential to the organisation and what protection is required for these assets. The firewall solution should then fit in with the security policy for the company.

Most firewalls use one of four architectures:

1. Packet Filtering Gateway
2. Circuit Level Gateway
3. Application Proxy
4. Stateful Inspection

These four firewall architectures pose different configuration challenges for passing the Internet traffic. Some of the firewalls have built-in abilities to allow services and protocols to be passed, while others require specific workarounds.

1.2 Packet Filtering Gateways

Packet filtering gateways are the easiest to configure for Internet access but provide the least security. A packet filter analyses each IP packet at the network layer and determines whether to pass or block it based on a set of rules. A packet-filtering gateway is not really a firewall but more of an intelligent router. If the packet filter has a rule specified in its rule base that allows communication between two specific addresses, packets are allowed to travel through the firewall to the specified address. If no rule is available for a given address, the packet is rejected and not allowed to pass through the firewall.

1.3 Circuit Level Gateways

Circuit level gateways operate at the session level used by TCP/IP and UDP. A *circuit* is a logical connection that is maintained for a period of time, then torn down or disconnected. The firewall verifies the circuit when it is first created. Once the circuit is verified, subsequent data transferred over the circuit is not checked. Circuit level gateways can limit which connections can be made through the gateway. They provide a moderate level of security.

1.4 Application Proxies

Application proxies are probably the most secure firewalls but a special proxy must be written for a given protocol. Proxy servers provide in-depth knowledge of IP protocols and allow application level analysis. They examine each packet of information as it passes through the gateway. Proxy servers are not designed to allow for new types of protocols. To pass a new protocol through a proxy server, you must develop a workaround.

The most common workaround for proxy servers is a service called SOCKS. This service is loaded on the proxy server and allows new protocols to be passed through the proxy server without writing a full application proxy for the new protocol. While this is a workable solution, not all proxy servers support the SOCKS services. Some vendors are currently working on transparent interfaces that could allow proxy servers to pass new protocols.

1.5 Stateful Inspection

Stateful Inspection (SI) is a firewall technology that lends itself to the configuration of new protocols. Stateful inspection expands on packet filtering by adding state information derived from past communications and other applications. Some of the new Stateful Inspection firewalls allow new protocol definitions to be added to the firewall with minimal work. Much like a packet-filtering gateway, Stateful Inspection firewalls can be easily configured to allow new protocols to be passed through the firewall over defined ports. In addition to this ease of configuration, Stateful Inspection firewalls can provide added security to these new protocols by performing packet inspection as the packets move through the firewall. Some Stateful Inspection firewalls have a scripting language that allows custom scripts to be written for packet inspection. This adds an extra layer of security above packet filtering while keeping ease of configuration. Stateful Inspection firewalls have the ability to inspect all levels of the TCP/IP packets allowing inspection scripts to be as simple or complex as required.

Most Stateful Inspection firewalls do perform some level of packet inspection even without a custom inspection script. This provides an extra level of security above packet filtering; however, it is an issue that should be researched depending on the model of firewall used.

2. Network Topologies for Using Firewalls

There are three basic network topologies for using firewalls with Internet services:

- Clients can connect to servers on the Internet from their local area networks through a firewall
- Internet users can access a server that is behind a corporate firewall
- Virtual Private Network (VPN) architecture

2.1 Allowing Connections to a Server on the Internet

For local users to access external hosts on the Internet, packets must be passed through the firewall in an outbound direction to the Internet. Depending on the type of firewall being used, this could involve opening up port 80 and 25 on the firewall to allow outbound access to the Internet. In this configuration, a client behind the firewall can initiate a HTTP session to a server anywhere on the Internet.

2.2 Allowing Connections to a Server Behind the Firewall

For Internet users to access a server behind the corporate firewall, packets must be passed in an inbound direction through the firewall. In this configuration, users on the Internet are able to connect to a server behind the corporate firewall.

2.3 Allowing Connections in a Virtual Private Network

Modern firewall technologies allow the extension of the corporate network through the firewall to remote sites. In a situation like this, two office networks in different parts of the world can be linked together over a secure channel on the Internet. By implementing a firewall solution that supports Virtual Private Networking at both sites, a secure connection can be created that encrypts data as it passes over the Internet from one site to the other.

3. Contact Us

Helping you piece IT together

If you wish to contact us or provide any feedback on this whitepaper you may do so using the following contact details.

Telephone : **+353-(0)1- 4404065**
Website : **http://www.bhconsulting.ie**
Email : **info@bhconsulting.ie**