Firewall implementation

There are a number of issues that need to be considered before a new firewall is deployed or an existing one replaced on an organisation’s network.

Requirements Analysis

Defining a requirements specification will allow a successful evaluation of the various solutions available. There are many different elements involved in a firewall solution and the balance which needs to be achieved between these will differ significantly between organisations.

Interface

At a simple level, a firewall needs at least two network interfaces. Any firewall used to protect anything other than a small organisation will require more interfaces or the potential to expand the system. It should be established whether interfaces are generic and can be used for any firewall role or are specific to management of the device. The physical presentation of the interfaces will need to match those of the networking infrastructure into which the device is going to be placed. Most firewalls will have 10/100(/1000) copper Ethernet interfaces or fibre SC connectors.

DMZ

If the firewall is going to provide protection for computers within a DMZ it will need an additional interface for each DMZ network. Some firewalls will be able to support multiple DMZ interfaces and this is used increasingly to support wireless network configuration as well as traditional server farms.

Failover and load balancing

It is important to establish whether failover requires a dedicated interface, is managed by dedicated cable, or is managed inbound. As firewalls support load balancing and fault tolerance, they are one of the most critical devices in the organisation’s network infrastructure, and it is important to ensure appropriate facilities are available. The provision of basic requirements such as dual power supplies, redundant supervisors and removable fan trays can be established easily, but it is important to check if the firewall can operate in an Active/Passive or Active/Active mode of failover operation (see 3.4).

Operational Mode

Many devices will support different modes of operation (routed, NAT/PAT, bump-in-thewire),

which can be configured as part of the device setup. It is important to ensure there are no limitations in the method of operation to be used.

Speed

The wirespeed throughput will determine the traffic that can traverse the firewall before it becomes a bottleneck. It is important to base calculations on the speed of the device when it is performing DPI/IDS/IPS if you are going to use these functions. Vendors will often quote performance figures for a number of scenarios, so make sure you identify the correct figures.

Authentication

If users are going to be required to authenticate before packets are allowed to traverse the firewall, how does the firewall implement authentication? It could be web based or via a special client. It is also worth considering whether the device requires a local database of credentials, or if it can query another authentication service, such as AD, Radius or LDAP.

Content filtering

It is important to establish what functions you require the firewall to provide. Simple rule-based firewalling will almost certainly be included and, in the vast majority of cases, stateful inspection. Other additional features include DPI, Intrusion Detection, Intrusion Prevention, Anti-X and VPN termination.

Virtualisation

Virtual firewall facilities can be useful to partition firewalling into different areas for isolation or to better organise Active/Active failover. What is the maximum number of virtual firewalls that can be created?

Platform

Not all firewalls are appliance based: some run as an installation on top of an installed operating system. A decision will have to be made as to whether the necessary skills are available to support the operating system as well as the firewall. If this can be achieved, which operating systems and versions can be supported by the relevant staff?

Reporting and management

The provision for reporting and management is often investigated as secondary to the technical aspects, but these will be the facilities used to interact with the device on a day-today basis after installation.

Reports need to be available in a number of formats, preferably tailored to the requirements of the individual. The device may provide an overview, alerts when something occurs or just a daily report. The interface to the logs is also important: if one has invested resources in a syslog installation, it would be illogical to procure a firewall that cannot output logs to a syslog server. Conversely, can the operating systems used to manage the network infrastructure

support any applications required? Are they written in Java?

The firewall requires an interface for configuration of interfaces, rules and policies. Often the choice between GUI and CLI is a personal one, so the option of both will satisfy more staff. There may be additional requirements for the user interface. Almost certainly it needs to be secure: HTTPS instead of HTTP or SSH instead of telnet.

Documentation and support

A recent trend in the IT industry is to make product manuals available before purchase, either through pre-sales staff or the vendor website. This is an excellent way to find out about the product in more detail than is available in a datasheet. It is worth investigating training options for staff – are there vendor-run courses at different levels?

Support is essential for a mission-critical application like a firewall, so different options for maintenance will need to be discussed. Obtaining details about replacement times for parts and response times for human contact is critical, as when a fault occurs, this is the time you need to speak to someone, quickly.

If an additional operating system is involved, establish where the support burden lies, including operating system patching and maintenance.

Added value

Many firewalls offer ‘added value’ functionality: features that are included above and beyond the basic firewalling code. These may include VPN termination functions, which can be used for creating a tunnel between two firewalls or from an end user to the firewall. However, there is debate as to the security of terminating end user connections on the firewall or if they should be terminated on a dedicated VPN server within the firewall DMZ. It is important to check if these features are included in the purchase price or whether they require optional hardware upgrades or licensing.

Consultation

In any organisation there will be a number of individuals who will have concerns about any IT-related changes. A change in a firewall should include comprehensive consultation with all stakeholders.

The consultation will be different if the firewall policy is changing as opposed to a hardware or software change. If only the hardware and software are changing then the consultation will be internal, concentrating more on the technical issues like access to change rules, change control, reporting and logging and the networking implications.

If the firewall policy is to be changed then the consultation will need to be much wider. Stakeholders will come from all areas of the organisation and it is important to try to contact as many as possible during the consultation period. If the driver for change is clear and the benefit is obvious, the majority will be in support. This is all the more reason to get communication right. The one major problematic issue that is seen repeatedly is time frame: there is never a right time to change an IT system, but it has to be done some time.

Creation of Policy

The creation of a firewall policy should be carried out in conjunction with senior management within the organisation. The support of senior management is essential to ensure that IT staff can implement the policy and make decisions on firewall requests.

In the policy there should be answers to at least these key questions:

- Who is managing the policy?
- Which senior member of staff is sponsoring the policy?
- How often is the policy to be reviewed, and by whom?
- How are changes requested?
- How are disputes resolved?
- What is the Service Level Agreement?
- How is logging data managed and what is the data retention period?

As well as core decisions as to which rules will be approved and which will not, the policy may include technical elements. These may be an application version prerequisite, the location of a server on a specific netblock or a need for an individual to attend a training or briefing session.

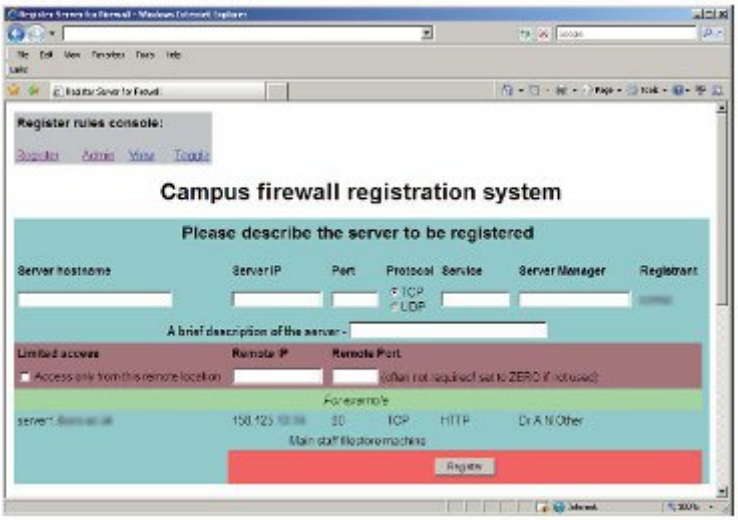
The policy should also contain details of in what circumstances rules will be removed, for example, to protect the organisation against compromised machines or in the event of an exploit being used against vulnerable services.

System Registration

For any system with more than a handful of rules, there needs to be some method to register systems for particular firewall rules. Most firewall implementations will be default deny, so the rules required will be holes in the firewall for particular services on specific hosts.

It is important to ensure that the firewall policy and guidance is available before any registration system is introduced. If no policy is in place then the registration procedure may get clogged with requests for NetBIOS ports to be opened, for example. A Frequently Asked Questions page is a useful method of communicating firewall policy, giving concrete examples of what will and will not be allowed.

The registration system could take a number of different guises, as some organisations have an open policy where IT administrators create their own rules. This might not be the most effective way of managing a firewall, as it may lead to unintentional security compromises. Other organisations have paper-form based systems or online web forms to request firewall changes.



[1]

Figure 15: Online firewall registration system

Auditing, Penetration Testing and Review

Once a new firewall system has been released into service, the protection offered will morph every time a firewall rule is changed. It would be impractical to audit the system every time a change is made, but it is prudent to periodically check the effectiveness of the firewall. Similar checks to those performed in the testing and evaluation stage (see 9.1) will ensure, as far as is possible, that the firewall is acting as an effective barrier against Internet-based attacks and threats.

Penetration testing is one way of auditing the technical aspects of the effectiveness of a firewall; however, it is worth remembering that it only tests one element of the system. Penetration tests can be performed in-house or through a commercial company. Results can vary greatly according to the technology and methodology used. A penetration test is not the only answer to the auditing issue and passing any test does not mean your organisation is secure.

Be careful to ensure when performing a penetration test that you have the permission of all necessary stakeholders for the infrastructure that you are using. It is usually best to conduct the testing on-site from a computer connected to the outside interface of the site firewall.

Conducting a penetration test across JANET or the public Internet will more than likely alert other organisations including JANET-CERT and result in wasted resources as they investigate the matter as a real attack against your organisation. However, there may be a policy that allows this within a Regional Network, so it is worth speaking with the managing agents first.

Any form of penetration testing needs to be more than just a port scan; therefore, it is recommended to seek the advice of a professional who has the knowledge not only to perform the tests but more importantly to interpret the output.

After auditing the technological aspects of the firewall system, it is worth investigating how well other procedures are working. This includes not only the monitoring of traffic problems but also whether requests for firewall changes are being actioned, recorded and checked

correctly.

While there is not a definitive set of auditing requirements for firewalls, a number of controls exist in BS ISO/IEC 27001:2005 which apply to the technology used for firewall implementation.

Links
[1] http://community.ja.net/system/files/images/firewalls-tg-15.jpg