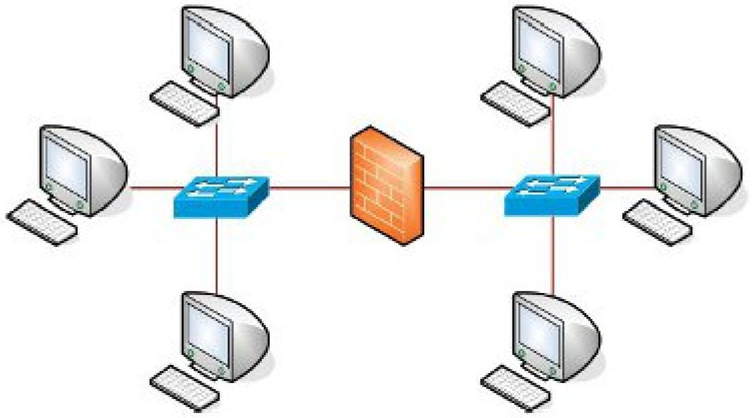
Published on *Jisc community* (https://community.jisc.ac.uk)

Technical consideration

Testing

Before any system is introduced into the production environment, it must undergo a period of testing and evaluation. This is usually done in a test environment away from the production infrastructure.

Once the firewall has been configured according to the security policy, testing under load should be the next stage. Multiple test computers can be connected on the inside and outside interfaces of the firewall, and then load testing tools can be used to transfer large quantities of data. Netcat, Deluge, Siege and Diesel are examples of open source tools, and there are also ame task.



[1]

Figure 16: Firewall testing using multiple PCs

Once wirespeed throughput testing has been completed, it is important to test the firewall functionality using penetration testing. Both a simple port scan and a more complex penetration test of the services protected behind the firewall will show how the configuration of the firewall reacts to malicious threats. For example, it is useful to monitor the difference between dropping and resetting unwanted connections.

As a further test, PCs on the inside interface can be configured to reflect the operating systems and configurations of standard computers inside the organisation, so that streaming and other services can be tested, and the best rules for protecting the internal infrastructure designed.

Finally, load balancing and failover should be tested, to observe the results before it happens for real. Issues with tailoring heartbeat timeouts and other failover aspects can then be addressed before implementation.

Problematic Protocols

With any firewall implementation there will be problems with functionality of some protocols. There are technical solutions provided in the software by some vendors, but it is important to consider the monitoring of these protocols during installation.

These issues include:

- H.322 and related videoconferencing software: videoconferencing is often the most difficult application to implement across a firewall
- UDP: a lot of streaming services rely on a TCP connection to initiate the stream, which is then formed of UDP packets with the destination of the host. The filtering of incoming UDP is becoming easier as the intelligence of firewalls becomes more sophisticated.

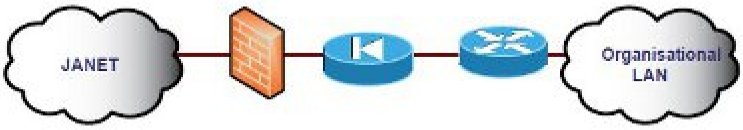
Pre-screening or Clean Feed

The increasing number of Internet threats and the demands of network traffic are proving difficult for some existing firewalls to manage successfully. An alternative to procuring a new firewall is to investigate a clean feed style technology.

Clean feed technology provides a pre-screened subset of the Internet traffic destined for the organisation. All the traffic initially passes through a first tier firewall which screens the traffic for threats and drops malicious traffic before providing a cleaner feed to the existing firewall.

Depending on the technology deployed, the first tier firewall may screen out most DoS attacks and port scans, restrict ICMP and use DPI to remove threats from the protocols that it can analyse.

The existing firewall therefore only has to manage the cleaner feed, which will have considerably lower bandwidth requirements. The firewall rules for granular control will still be applied at the existing firewall.



[2]

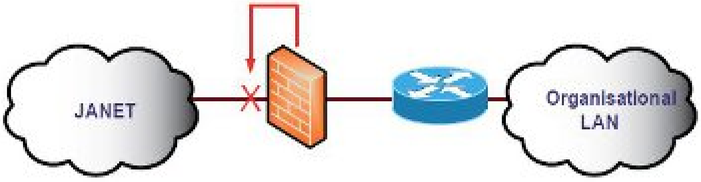
Figure 17: A first tier firewall providing a cleaner feed for an existing Cisco PIX

Integration with IDS and IPS

IDS and IPS are well established technologies that monitor network traffic for malicious content. The key difference between the two is how they react to a detected threat. An IDS will provide alerts when malicious content is identified, but human intervention is required to manage the issue. An IPS automates the mitigation to actively prevent malicious content compromising the network infrastructure.

Firewalls increasingly include IDS or IPS to complement the firewall code. They can be provided as additional software, additional hardware or fully integrated and configured by default.

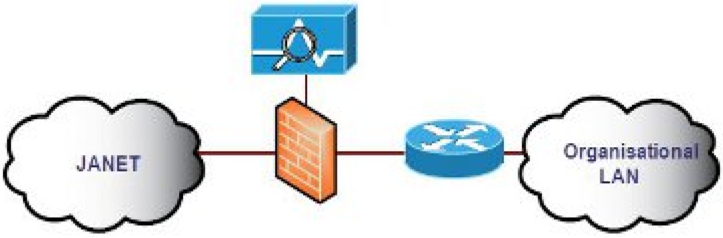
There are several different modes of operation. The system can be deployed inline so all traffic passing through the firewall is seen by the IDS/IPS and mitigated as appropriate before it is forwarded across the firewall.



[3]

Figure 18: Mitigation of malicious traffic using an IPS in inline mode on the firewall

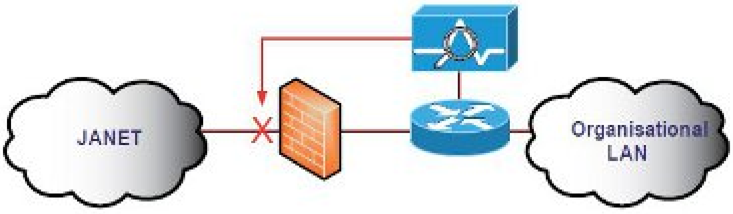
Some firewalls send all traffic received at the outside interface to the IDS/IPS as well as forwarding it according to the firewall rules. Alternatively, the IDS/IPS data can be sent to an external device for reporting.



[4]

Figure 19: Monitoring traffic using an IDS in promiscuous mode on the firewall

Often IPS-enabled firewalls can mitigate malicious traffic detected by systems elsewhere on the network. This is achieved by a secure connection that allows the firewall to issue a command or dynamically add a firewall rule. For example, on Cisco devices the **shun** command is used to mitigate traffic for a predetermined length of time.



[5]

Figure 20: An external IDS/IPS mitigating malicious traffic on the firewall

Source URL: https://community.jisc.ac.uk/library/advisory-services/technical-consideration

Links
[1] http://community.ja.net/system/files/images/firewalls-tg-16.jpg
[2] http://community.ja.net/system/files/images/firewalls-tg-17.jpg
[3] http://community.ja.net/system/files/images/firewalls-tg-18.jpg
[4] http://community.ja.net/system/files/images/firewalls-tg-19.jpg
[5] http://community.ja.net/system/files/images/firewalls-tg-20.jpg