WHITEPAPER

The Firewall Market

Choosing The Right Product

Author SecureData

May 2012

CONTENTS

Introduction

Firewalls have evolved exponentially since the original days of the port 80 filter, to state full firewalls and modern firewalls that include next generation firewall (NGFW) or unified threat management (UTM) functionality, remote access capability, intrusion prevention and other advanced functionality. This paper discusses the firewall market and considers offerings from Check Point, Cisco, Juniper and Palo Alto and discusses factors that should be taken into account when selecting the right firewall for your business.

With global sales in the firewall market rising to more than $6.3 billion in 2011 there are a lot of vendors attempting to lead or break into the market with new and innovative features. Whilst many of these features are useful and help increase the security posture of a network, which is ultimately the task of a firewall, there are also features that do not necessarily increase protection of the business assets, but may deliver a cost benefit to the business by enabling the removal of other technologies and are therefore interesting to consider. A prime example of this may be an intrusion prevention system (IPS) where a standalone IPS could be migrated to a firewall service, reducing hardware and therefore heating, cooling, space, support costs and management costs. However, as will be discussed, this is not always to the benefit of the security of the network.

Much is stated about the NGFW, and the capabilities thereof. An NGFW can be considered one in which the IPS, firewall, application identification and control technologies are tightly integrated. In addition rules are configured via one interface and not a standalone device (or piece of software) bolted on to the site of a traditional firewall, which means that traffic must take the same path through the device. A UTM can be defined as a firewall platform that includes IPS, antivirus, antispam and web filtering capabilities. There are however no hard and fast rules as to what constitutes a firewall, NGFW or UTM device. It is more important to consider the capabilities of a platform and whether there is a business need.

Firewall technology

When considering the firewall platform, it is difficult to differentiate between vendors on the security capabilities of just firewalling alone. That is to say taking into account the basic stateful firewall functionality and the propensity to be hacked of the platform, or how many vulnerabilities are discovered on that vendor platform. During 2011, the Security Tracker website, securitytracker.com, listed ten vulnerabilities discovered against firewalls during that year, five for Cisco products, two for Barracuda, two for Trustwave and one for ZyWall. Discovered vulnerabilities do not necessarily lead to an exploit (that is a piece of usually malicious software which takes advantage of a vulnerability) being written, and are quite often very theoretical due to the levels of access required to take advantage of the vulnerability. For instance, one of the Cisco vulnerabilities takes advantage of a vulnerability in the web management interface. This management interface should never be available from an external interface and so the majority of the other vulnerabilities create a denial of service (DoS) attack. Whilst DoS attacks can of course be damaging to a business, the target of the modern hacker is not to disrupt business but to gain access to privileged resources and data, in order to take advantage of that data. In fact, the vulnerabilities listed on the Security Tracker website for 2011 have all had fixes or workarounds issued by the vendor, emphasising the necessity of keeping security platform software up to date. Of course, there may well be vulnerabilities or even exploits that have been discovered by less scrupulous parties, who do not necessarily inform the vendor, and these vulnerabilities could be taken advantage of. However, it is more likely that the hacker would take advantage of either security misconfiguration (such as the case above of allowing managed web port access via an insecure network) or an application vulnerability, such as a Windows or application bug.

Multi-layer firewalling

The reality is that many vendors use shared libraries to build their firewalls on, and as such vulnerabilities that are discovered on one platform often exist on other vendor's platforms where the same libraries are used.

This was the case in the so called TCP Split Handshake discovery. In this attack a little known way of establishing a network session was utilised to bypass firewall security. Many firewalls allowed this attack via a default configuration with extra configuration being required to block the attack, although it could be considered that this wasn't a vulnerability, but either a misinterpretation of the rules of TCP, or a lack of documentation or understanding. Interestingly enough, many vendors with vulnerable products detected and blocked this attack via their IPS offering, helping to prove the need for multiple layers of differing security.

Many companies have an information security policy that dictates that external (or even internal) facing firewall infrastructures should be built from two firewalls from two different vendors. As stated, the main threat to firewall infrastructure comes, not from the firewalls themselves, but from applications internally on the network, as well as from the misconfiguration of those firewalls. Adding a second firewall vendor, within one infrastructure, does not automatically increase the security posture of the network. In some cases it may actually decrease security due to the increased risk of misconfiguration. This could be the case as in dual layer infrastructures where it may be assumed that one layer of the firewall infrastructure is blocking a threat, and therefore the second layer is less of a risk, being subsequently less tightly controlled, when in fact that firewall is incorrectly configured giving a false sense of security. The addition of two management platforms also increases the risk of misconfiguration as the engineer is expected to be familiar with two technologies, or the management of these two technologies may well be split across the team, where each member may assume the other is blocking a threat.

In the majority of cases it is a better policy to consider deploying two different types of technology, for instance, a stateful firewall deployed alongside IPS, or a stateful firewall with application identification technology. Often that technology can be deployed on a single firewall, although that is not always the case as will be discussed below.

NGFW / UTM funcitonality

Notwithstanding vendor claims, when implementing additional technology on any firewall, the performance of that firewall will be affected. This effect may be greater or less on differing vendor platforms, but if this effect were not there then clearly the customer would be paying for performance that is not required when it should be used for the base requirement of that platform, i.e. basic firewalling.

IPS

IPS has been integrated with many vendors' firewalls for some years, and as such is a mature technology. In some cases, such as with Cisco firewalls, additional hardware is required whereas with Check Point, Juniper and Palo Alto this is achieved with software, utilising on board hardware. Whilst integrated IPS is part of the firewall, and traffic may follow the same path internally to be scanned by IPS as that to be firewalled, when considering integrated IPS it is possible to evaluate it in the same way as an external standalone IPS. In fact, as stated above when discussing TCP Split Handshakes, integrated IPS can detect threats that the firewall alone cannot detect or prevent.

It can certainly be cost effective to integrate IPS with the firewall from a management and hardware perspective. However, the traffic to be scanned must be taken into account. Some businesses may wish to scan traffic destined for particular services that are not protected by a firewall. In this case it may be necessary to deploy a firewall to gain advantage of IPS, or alternatively deploy a standalone IPS solution. If a standalone solution and an integrated solution is deployed, then there are two IPS platforms to manage. When this is considered preferable to a complete standalone solution, then consideration should be given to a security information and event monitoring (SIEM) deployment.

The SIEM will take the logs from multiple locations and IPS devices in the network to present a single view of the security posture of the network, and is highly recommended even in the case of a single vendor IPS to correlate logs. In some cases this SIEM can be built into the firewall management platform, as in the case of Check Point, or be a standalone solution.

UTM

UTM capability such as antivirus, antispam and web filtering is best suited to the branch office. Where a business has a firewall deployment in the head office or data centre, it is beneficial to deploy similar technology to the branch to allow direct access to predefined, or all, internet services via a local ISP connection rather than have access via the data centre. Using the same vendor in the HQ and branch office ensures that management is not an issue.

Application/user control

Application control is the ability of the NGFW to identify the specific application that is being accessed by the end user, and filter traffic accordingly. Similarly, user control allows the NGFW to identify the end user and filter accordingly. For instance, in the case of Facebook, rather than just create a rule to deny all staff, marketing staff could access Facebook based on active directory group membership, but the application awareness of the NGFW could prevent access to games inherent within Facebook. There are downsides to this approach. Firstly, whilst there are signatures for common applications, where the application being protected is a bespoke application or not on the signature list, these signatures will have to be created. Add to this the fact that many businesses do not know which applications are being used on the desktop and as identifying these applications could be an enormous task, many businesses are not willing to invest in making full use of application awareness. Secondly, user identification is not 100% reliable, and there will be instances where it is not possible to identify a user, such as a user machine that is not logged into a domain, or a Linux or Macintosh workstation. In these cases allowances have to be made to give these devices access, either via a captive portal where a user must enter their credentials, or control has to be carried out via traditional firewall rules.

Selecting a vendor

When selecting a vendor it is all too easy to get blinded by technology, and not focus on the functionality that is important to your business and the protection of your resources. Any function of a firewall that does not address a business need is not a worthwhile option. For instance, if you have a standalone secure web gateway (SWG) to scan files downloaded from the Internet for threats, then the claimed throughput of antivirus scanning on a UTM firewall is irrelevant. Similarly if the need is for a firewall to protect a 10 megabit link, then a vendor boast of multigigabit throughput is not important unless one is considering short term future requirements for that platform.

When considering NGFW and UTM functionality, it is not always possible for one vendor to be considered best in breed. In this case it may be necessary to consider two platforms from different vendors, one for firewalling and one for IPS or SWG. Certainly in the short to medium term it is recommended that businesses do not retire their SWG and look instead at keeping this functionality separate from the firewall to allow better control and monitoring. There are also considerations around redundancy and the ability to change systems. In a single platform solution there will be more changes required on what is possibly an internet facing firewall in order to grant access to a specific application. When this control is carried out via the SWG, the important security device does not have to have as many changes made, where changes increase the risk of a security misconfiguration. In the event of a failure, with standalone devices, it is possible to create workarounds and to better balance traffic. When considering user identification, if this is a business requirement then consideration should be given to a network access control (NAC) product, which allows control of network access across the network, not just at the security perimeter, and allows control of access to critical business resources. It may also be necessary to consider the integration of the firewall platform with other products from that vendor, for instance, as already stated Juniper integrated IPS is managed via the same platform as a standalone IPS, or Check Point offer data leakage protection (DLP) or SIEM functionality on their firewall and management platforms.

Below is an overview of four firewall vendors, along with detail about some deployment considerations. However, no two networks are the same and it is not possible to select a product from a table alone. Business needs may outweigh technology requirements. Comment has only been made where it is considered that platform is particularly suited to that requirement, in the case where it is neutral no comment has been made.

Cisco Systems Ltd

Cisco has a 32% share of the security market via their diverse offerings including firewalls and SWG products, and has the highest market share worldwide for firewall appliances. Cisco also has offerings in other technology sectors such as network and routing, wireless, telephony and servers. Their firewall offerings are based around the adaptive security appliances (ASA) firewall platform, and the integrated services router (ISR) platform. The primary firewall product is the ASA, the ISR is considered a secure router offering all the functionality of a router, including multiple interface types, along with traditional firewall functionality.

Deployment considerations

- Standalone firewalling
- Integration with Cisco network
- Remote access virtual private network (VPN)
- Advanced routing
- No advanced centralised management
- No NGFW functionality
- No hardware or IPS or deep inspection (UTM functionality)
- No branch office functionality with UTM
- No high end data centre firewalling

Check Point

Check Point is a pure security company, founded in 1993 and is credited with many innovations including patenting the stateful firewall. They are second to Cisco in market share for firewall appliances. Check Point offers a UTM model for branch functionality through to the newly announced high end platforms including the 61000 model that is capable of delivering 200 megabit / second of firewall functionality. Additional functionality includes SIEM, endpoint encryption via firewall management platform and advanced management of multiple devices.

Deployment considerations

- High end high performance firewalling with growth by adding additional processors / interface cards
- Remote access VPN
- Branch office UTM
- Integration with Juniper NAC and IPS, standalone and integrated
- Single managment platform for multiple products via network and security manager (NSM) although NSM is not the most capable management platform
- Advanced routing

Palo Alto

Palo Alto is a newcomer to the security market, having been founded in 2007 by ex-Check Point employees. They are a pure firewall company with a small market share. However, their disruption to the market, forcing other vendors to look at application and user identity, has ensured rapid growth. Their platforms range from the PA-200 to the PA-5040, with up to 20 gigabit of throughput.

Deployment considerations

- Application or user identification requirment
- All in one appliance for smaller business
- No Common Criteria EAL4+ requirement
- No high end data firewalling

Conclusion

The selection of a firewall, and other security products, is not a simple task. Consideration has to be made regarding functionality, management, throughput and additional functionality. There is no single vendor that is suitable for every network, every network is different. Vendors will always push their product to the detriment of others, and not necessarily mention functionality that is poor on their platform, even to the point of attempting to displace already deployed platforms to replace with an inferior (in that deployment) device.

It is essential when considering this to partner with a company that has the knowledge and experience to assist in this decision making, and to take a vendor agnostic approach to selection to ensure that what is finally implemented is the platform best suited to meet business requirements at the right price with the minimum of disruption. For instance, it can be difficult to migrate from one vendor platform to another, due to the upheaval of training, rule migration etc. In many cases historical firewall rules are not documented and it can be difficult to ascertain whether that rule is still needed.

We are ideally suited to help you meet this challenge with our Presales team assisting in identifying the best vendor or vendors to meet that requirement along with initially designing the solution for implementation by our Professional Services staff, alongside your technical staff with our project management. Finally we can assist in the migration by offering levels of service from telephone technical support up to a fully managed service including monitoring and reporting on the solution, 24 hours a day from our UK-based Security Operations Centre (SOC) where staff are on site 365 days a year monitoring your security infrastructure and reporting on anomalies via our in-house created

Affinity service. Alongside this service management ensures that service level agreements (SLAs) are met and you are kept informed of any security vulnerabilities or incidents that may affect your platform.