NODE4

Empowering business to do more

Protecting the Business Boundary From Cyber Threats

IT Security Considerations for Today & Tomorrow

Public

Node4 Limited

28/01/2016

Introduction

Packet-filtering firewalls have come a very long way from the simple allow/deny packet gateways, to the ability to recognise and mitigate the threats and risks against which businesses of today are having to protect themselves. Over recent years perimeter security technology has blossomed in the wake of extensive research and constant vigilance against the rapidly evolving threats and sources of exploit.

The firewall (that often misused all-encompassing term) still forms the cornerstone of a business' security policy. As most enterprises now integrate their own private networks with public Internet connectivity, the emphasis on robust security policies and current technology has never been greater. The complexity of protecting networks, systems, and the transit of data between them has become even more complicated as cloud services integrate closely with on premise and co-located systems. The types of threat and their delivery mechanisms have morphed into sophisticated and automated tools, and the threat landscape is in a continuing state of evolution.

Businesses need to be aware of the complexities of cybersecurity and compliance as it now impacts business strategy as much as industry trends and global markets. Companies affected by security breaches – even in the supply chain- quickly come to understand this fact when the breach becomes a major discussion point in the boardroom.

The National Institute of Standards and Technology (NIST) has published guidelines which recommend that organisations implement a security policy that supports a firewall's performance; but surely firewall selection should be based on security requirements, and then factor in growth and future feature expansion? This document is intended to give the reader some insight into the type of technology features required for a comprehensive security foundation, guidelines on how to implement them, and to highlight future threats on the horizon.

History

As early as 1988 our networks were discovered to be vulnerable when the Morris Worm was unleashed as a bad experiment in "discovering" the size of the Internet. This "rabbit" virus exploited the Unix Sendmail application and brought down most of the Internet. DARPA was prompted to establish the Computer Emergency Response Team (CERT). Another consequence of the Morris Worm was the development of the first firewall technologies which examined the network address and port mapping of the incoming packet and either allowed or denied access based on simple rules. This packet filtering type of firewall is now known as first-generation firewall technology.

Second-generation firewalls dug a little deeper into the packets to identify the packet's state in conjunction to other packets. Thus, "stateful packet inspection" (SPI) evolved. Third-generation firewalls delve deeper still into the application layer of the packet to understand how certain applications and protocols behave and their purpose. Although specific Web Application Firewall (WAF) technology has been around since 1999 the full depth of application aware firewalls did not arrive until the advent of Next Generation Firewalls (NGFW) in 2012.

Today

Long gone are the days of simple packet filtering, the types of threat have increased proportionally with the increased complexity and diversity of connectivity. Now, advanced threat mitigation such as is required for DDoS is achieved through heuristics, benchmarking the traffic profile and blocking anomalies. The 90s goal of mobility is now a reality, but riding alongside the nightmare of fending off malicious code, are the threats posed by unauthorised intrusion/exfiltration, criminal organisations and hacktivists.

Firewalls are still the foundation of our security suite of tools, along with the inclusion of anti-virus, anti-malware, spam protection, email filtering, intrusion protection, phishing protection, secure encrypted remote access, data leaking prevention, web access firewalls, secure authentication, application control, sandboxing, load balancing, QoS and too many others to mention. There are so many elements that managing and monitoring them all consistently with a single security policy is hard work. Many companies are only able to cover the basics and many of these use default security settings as “good enough” policy. Whatever security tools are to hand, they need to be wielded with experience in the context of stringent corporate policy and a sound network design – a locked front door is of no use when the side window is left open.

The harsh truth is that every business should assume that at some time it will be a target; whether specifically or arbitrarily. It is recognised that many small and medium companies are prime targets for hackers and the reason for this is as stated in the previous paragraph; they have very basic protection and usually know no better than to select the default settings. There are not very many companies (they tend to be the larger enterprise ones), who have their own IT security experts who implement their corporate security policy in line with their environment; closing ports, scanning relevant open ports and producing scheduled reports on user web access and virus exclusions. Most companies’ IT staff manage broad aspects of IT, spreading their experience very thinly across a plethora of IT topics.

NGFW technology has allowed for the expansion of capabilities at the perimeter to incorporate a complete Unified Threat Management (UTM) system. This is the inclusion on a single platform of an array of comprehensive tools which mitigate a wider range of threats and intrusion methodologies, and is a huge advance in collating the various security threads and unifying the control and policies under a single canopy for reporting and auditing purposes.

Considerations

Firewall technology has learned some painful lessons over the years. Chief amongst these is the need to have a secure operating system underlying the firewall application. In the early days, Checkpoint delivered its Firewall on a Microsoft Windows server, but thankfully we learnt that lesson quickly. A bespoke, secure hardened OS should be the foundation upon which all firewall technology is built.

The outdated idea that provisioning security solutions from multiple vendors to allow businesses to “cover all the bases” by dispersing risk across multiple security vendors is now regarded as ill-conceived. Focus is around implementing and controlling a common security policy which can be managed and maintained across the enterprise, usually via a single pane of glass. This makes both logical and economic sense, and the better firewall vendors can reliably provide integrated threat management across a unified management system,

As NGFW technology is based around “deep inspection”, analysing application specific traffic, it is important that all effort is placed in processing the traffic as quickly as possible. Application-specific integrated circuits (ASIC) process the traffic in the fastest way possible, and by offloading processor tasks traffic bottlenecks within the hardware are avoided and throughput maximised. This is a serious consideration for scalability; today’s trickle is tomorrow’s torrent.

To support mobility secure remote access is a fairly standard offering in firewall technology; the ability to provide VPN tunnels between multiple endpoints and also [free] VPN clients for end users will make the solution cost effective. Single sign-on through integration of LDAP will greatly improve the user experience.

Intrusion Prevention Systems (IPS), which monitor, log, identify and (more importantly) stop malicious inbound network activity use a constantly updated blacklist/whitelist database of signatures. The Intrusion Detection System (IDS) is a reactive tool which provide baseline for security and reports on packets that have broken the chalk-lines, and a journal of the potential resulting intrusion. Where orchestrated attacks appear quickly, attack and as quickly disappear it is important to have a dynamic solution which can address these evasion techniques. IP Reputation services aggregates data from locations around the world and provide up to date information on threatening sources which allows for proactive protection against malicious sources.

The ability to shape traffic on priority applications is an important factor wherever application traffic is linked to revenues. Similarly, load balancing is the ability to intercept incoming traffic with a virtual server and share it among one or more backend real servers, enabling multiple real servers to respond as if they were a single device, which in turn means that more simultaneous requests can be handled and improves the availability of on-line services. The provision of multiple zones (DMZ) can also be an important factor in firewall selection, allowing extranet, corporate infrastructure and web facing services to co-exist behind a high-availability appliance.

Managing outgoing web access with full granular control and comprehensive reporting such as the top ten web sites accessed and most prolific web users is essential information for managing the internal acceptable usage policy. Application control is another valuable tool which can identify and control specific application types and providing relevant enforcement is essential in the current Web 2.0 and cloud environments. This type of feature can identify thousands of applications, even those on encrypted channels and can also mitigate against sophisticated botnet activities that easily evade traditional firewalls. When used together Web and App' control can exercise policing of the web use in way that staff will co-operate with.

For organisations as diverse as medical, legal and retail industries preventing valuable data from exfiltration is a key deliverable. Data can be sent outbound by accident, by attaching the wrong files, or deliberately by synchronising corporate data to cloud stores like Dropbox, or by deliberate exfiltration methods such as DDoS application attacks. Data Leak Prevention (DLP) is the ability to watermark, track and prevent this type of data from unauthorised export and forms a substantial tool in border security compliance and data governance.

The most visible security protection which users see is Anti-Virus protection. AV on the end-point client in order to protect this as a point of entry can often be managed from the Firewall. As the main public front door for many organisations, email and subsequent filtering of Spam is an essential feature for businesses. This form of gateway management allows for key word exclusion, important in managing litigious or distasteful content.

In a recent survey provided by Cisco, (*Data Leakage Worldwide: Common Risks and Mistakes Employees Make*), over 50% of employees altered their endpoint security settings from those set by their employers citing; "*Because I wanted to visit that Web site regardless of the company's policy*". Over 60% used their company computers at least once per day for personal use, potentially opening up the network to threats. Clearly companies need to secure users' endpoints, but more importantly extend the company security policy and have visibility across the enterprise via a single-pane-of-glass in order to manage the risks.

All of the above features are important as part of an overall security structure, which should include employee awareness, policy enforcement and regular penetration testing in a managed and reportable context. Selecting a firewall which will provide the required throughput for the various features isn't easy; the more features enabled the more processing power is required. Enterprises should also factor in anticipated growth of users, throughput and features throughout the life of the appliance. Fortunately with cloud technology and advances in NGFW technology and UTM systems, OPEX-based fully managed security has arrived.

Tomorrow

Although predicting the future is fraught with risk, emerging technologies continue to raise interesting questions as to their vulnerability and predilection to threats.

The rise of Machine to Machine (M2M) technology, an area in which Node4 are providing solutions, is expected to increase as the Internet of Things (IoT) explodes to over 6.4 billion devices in 2016, according to Gartner. We have already seen interest in attacking PoS devices and researchers Miller and Valasek demonstrated flaws in the compromise and control of connected vehicles in 2015. Gartner also predicts that 20 billion devices will be connected by 2020 and as well as the bulk of industrial engineering end points and a multitude of medical devices such as heart monitors connected into various reporting systems. The scope and availability of many more devices for the average hacker to exploit are huge.

Hackers are not the elite group of IT experts we might have thought they were in the past. With the vast publication of generic exploitation toolkits which have been used it is now a field open to virtually anyone who can download, install and run via a wizard control program with a menu of exploitation choices and subsequent payloads. There are currently over 70 different exploitation kits out “in the wild”, each taking advantage of hundreds of vulnerabilities on various operating systems and applications. One might think that “knowing” of a vulnerability is enough to protect against it but clearly not all businesses are learning; in 2015 TalkTalk fell foul of an SQL Injection vulnerability which has been known since 1998, apparently wielded by a teenager. This is just one reason why a policy of patching both OS and applications in the infrastructure as well the perimeter forms such a vital part of protection.

So what are the future threats on the horizon? Fortinet predicts a “Land & Expand” tactic in which hackers look to exploit further away from the defensive core by first targeting employees’ personal technology. Security policies which incorporate end point protection for BYOD - extending the protected perimeter outwards - will be well placed for the future. Fortinet also predicts that headless devices such as smartwatches may well be targeted by worm attacks like the virus codes which were seen in the early 00’s.

The Data Centre is not exempt from vulnerability, a form of Jailbreaking of the hypervisor has already been exploited. *Venom* used floppy disk drivers to break out of the hypervisor and gain access to host operating systems. There may well be more of this type of exploitation as the continual expansion of virtual platforms proceeds.

Fortinet foresees the rise of **Ghostware** which follows in the footprint of identity protection services such as Snapchat. Malware which can perform a function and then delete and trace itself has already been proved as viable when researchers saw *Rombertik* as the first **Blastware** which once installed determines if it has been detected or reverse-engineered, then self-destructs, permanently crashing the host system to avoid detection.

As Sandboxing technology becomes more prevalent in “testing” the intentions of applications entering the enterprise, Fortinet predicts the growth of Two-Faced Malware. This Malware is designed be appear to be benign to avoid detection but then executes a malicious process once it passes security scrutiny. Even worse; on passing through a sandbox successfully the malware may get awarded a “safe” category which proliferates throughout the organisation or even globally.

CONCLUSION

There are enough concerns in the future to safely predict that as threats morph and increase, the platform on which business security resides will need to scale up and adapt to meet them. It is vital that investment now forms a sound foundation and is not lost in the near requirements of the future.

The following summarizes the major recommendations from this whitepaper:

- An organisation's security policy should be based on a comprehensive and continuous risk analysis.
- A Firewall is only one part of an overall secure Network design.
- Comprehensive perimeter security has to incorporate all threats in a unified solution which can be organised from a single management platform.
- Perimeter security is a two-way flow. Due diligence should be given on North-South as much as South- North.
- Firewall policies should be based on blocking all inbound and outbound traffic, with exceptions made for desired traffic.
- Firewall selection should reflect the requirements of the organisation and it's infrastructure
- Managed security services are preferable in many organisations because of the broad skill sets necessary to implement, manage and maintain a comprehensive security platform across the enterprise.
- The network perimeter includes user end-points, and security mitigation needs to incorporate these.
- Solutions should be adaptable to incorporate future threats and policy adjustments.

Please contact Node4 for any questions relating to this whitepaper or enquiries regarding N4Protect services; please email sales@node4.co.uk or call 0845 1232222.