A Primer on the need for Next Generation Firewalls

Cost and lost business associated with data breaches and lawsuits continue to increase every year. As long as valuable information exists, criminals will attempt to steal it using a wealth of traditional, as well as ever more sophisticated attacks.

To stay ahead of new threats, businesses need a security platform that can provide protection against both known and new threats, while scaling to accommodate business growth and new services.

Introduction

The term 'next-generation firewall' (NGFW) became popular in 2009 when the research firm Gartner published a report titled "Defining the Next Generation Firewall". The report refers to a firewall that offers specific features to address changes in both the way business processes use IT and the ways attacks try to compromise business systems. [1]

Unfortunately, some Next Generation Firewalls not only fail to provide these advanced next-generation features to guard against new attacks; they also fail to provide a mature platform of core network protection features to block existing attacks. This is why industry analysts still caution that NGFW features are most effective when used in conjunction with other layers of security controls.

In order to block all threats, Next Generation Firewalls must also include traditional packet filtering, network address translation, stateful protocol inspection, and virtual private network (VPN) capabilities.[1]

Next Generation Firewalls must be built on a solid, field-proven base of traditional or core network protection features before attempting to add next-generation security features such as application control and deep packet inspection.

1. Gartner, Inc., Defining the Next-generation Firewall, October 2009

Existing security threats that will never go away

Once in the wild, viruses, malware and traditional methods of attacking networks and users never go away. In fact, many exploits enjoy prolonged lives simply because vendors of widely used applications are reluctant to add or enforce user protections, such as strong passwords or SSL encryption, for fear of slowing user acquisition and feature development. This has the effect of placing responsibility for security entirely upon the enterprises and service providers whose employees and customers use these popular web-based applications.

Many businesses and end users remain susceptible to a myriad of known attacks due to a simple failure to patch known vulnerabilities, out-dated equipment and malware signatures, or a failure to properly setup and deploy security devices.

Since many of these vulnerabilities have been known for years, they are well documented, and any limited experience hackers can easily learn to exploit them to attack unpatched systems.

When developing a security strategy, businesses must plan to protect against not just current threats, but all threats, known and unknown.

The evolution of new threats are accelerating

Web-based Attacks Increase Data Breach Costs

The Internet's standards-based web interface and incredible number of applications have made it the primary choice for hackers and thieves looking for new ways to steal information, disrupt services and perform other malicious activities for financial gain.

Corrupting computers and networks, and stealing personal data through web-borne viruses, worms and Trojan applications is now commonplace.

Ever increasing sophisticated attacks leverage technology and social engineering to trick users into executing malicious activity that harvest confidential information. The most prevalent threat types include spyware, phishing, instant messaging, peer-to-peer file sharing, streaming media and social media.

The resulting number of data breaches, including identity theft, credit card information theft, fraud, etc. increase every year and cause real damage.

According to a report by the Phenon Institute, in 2010, 31% of data breaches were based from web-based attacks. They also reported the average cost of a data break was $214 per compromised record and averaged $7.2 million per data break event.

Web 2.0 Applications

Both consumers and business are adopting social media applications including Twitter feeds, Facebook pages, and YouTube videos into their everyday business practices at a rapid pace. These Web 2.0 applications enable instantaneous, always-on communications between employees, business partners and even temporary contractors, bringing the opportunity for great leaps in productivity and increasing profits.

As might be expected, allowing these consumer-oriented applications with user-generated content into the enterprise raises a myriad of security concerns.

Technically speaking, Web 2.0 applications can be very intelligent and crafty. They can tunnel through trusted ports, use proprietary encryption algorithms and even masquerade as other applications to evade detection and blocking by traditional firewalls. This makes it much easier to transmit content undetected and unimpeded from inside of a 'secure' network to the outside world and vice versa.

Web 2.0 applications also create a green-field opportunity for a new generation of viruses and threats to breach traditional network security firewalls.

Traditional firewalls are no longer effective

Traditional stateful firewalls with packet filtering capabilities used to be highly successful at blocking unwanted applications simply because most applications communicated over networks by using specific and unchanging computer ports and protocols.

Traditional port-based protection is no longer practical. For example, blocking port-80 would block access to the web entirely, and this is simply not an option for businesses today.

Next-Generation Networks

For many businesses, their existing networks are not adequate to support their long-term and sometimes even short-term growth plans.

These next-generation networks are being tasked with demanding needs; from providing large branch offices or mobile workers with secure access to critical corporate information, to powering virtualised data centres and low-latency cloud-based applications, to delivering reliable high-quality business and security services to multiple globally dispersed customers.

Next-generation networks must be flexible enough to simultaneously support high volumes of traffic as well as rich media protocols without slowing down.

In order to maintain high throughput and reliability, these complex networks must have security devices that won't become chokepoints as they inspect and filter traffic for threats and malware.

The Next Step in Security Evolution: Next-Generation Security Platforms

As enterprises and service providers migrate to more complex multi-protocol network architectures with higher data rates and traffic volumes, they require highly flexible security platforms that can evolve and scale. Organizations need next-generation security platforms and related devices that are flexible enough to provide protection against both known and unknown threats, while scaling to accommodate business growth and new services.

Next-Generation Security Technologies

Traditional security solutions such as firewalls, intrusion detection systems and host-based antivirus are no longer adequate to protect against new, sophisticated attacks. The potential for data loss and damage to corporate networks increases every year as criminals find new ways to penetrate defence mechanisms.

In addition, as government regulations and legal requirements[2] such as PCI DSS, HIPAA and the HITECH Act begin to hold company executives accountable for their employee's actions, corporate executives and IT professionals are becoming more concerned about what their employees are viewing and downloading from the Internet.

2. Note: Government regulations may not be Australia specific, however, Australian businesses (especially those who deal directly or indirectly with international businesses) generally adopt these regulations and legal requirements (in order to sell to, buy from, partner with or compete against).

Next-Generation Security Technologies must, in addition to protecting against traditional threats incorporate additional key protection and defence mechanisms. These new protection mechanisms are discussed below:

- ✓ **Application Control**

  In order to prevent data loss and mitigate new threats, organizations must be able to effectively control traditional applications as well as the new breed of Internet-based applications. Application control must be able to detect, monitor, and control the usage of applications and any associated network traffic flows at gateways and at endpoints, regardless of network ports and protocols used.

  Association must be made between the application and the end user before the proper access rights and security policy can be assigned.

- ✓ **Intrusion Prevention System (IPS)**

  Deploying updates and patches is a complex and time-consuming process. Following a patch release, it can take businesses weeks or even months to deploy the fix to all affected systems. IPS protects networks from both known and zero-day vulnerabilities, blocking attacks that take advantage of unpatched systems.

- ✓ **Data Loss Prevention (DLP)**

  Trusted employees frequently send sensitive data into untrusted zones, either intentionally or by accident. DLP features include fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching, and data archiving.

Numerous communication protocols - including HTTP, HTTPS, FTP, FTPS, email (POP3, POP3S, IMAP, IMAPS, SMTP, and SMTPS), NNTP and instant messaging (AIM, ICQ, MSN, and Yahoo!) – may need to be monitored for sensitive data.

- ✓ **Web Content Filtering**

Web content filtering technology enables a wide variety of actions to inspect, rate, and control perimeter web traffic at a granular level. Web content can be classified and filtered according to organisational policy.

Web Content Filtering can be an expensive exercise on compute resources and the technology vendor should provide mechanisms to accelerate web content filtering. Acceleration of web content filtering allows the filtering to occur without disrupting end-user quality of service expectations.

- ✓ **Dual Stack IPv4 and IPv6 Support**

The IPv4 network address schema prevalent on the internet has been exchausted (i.e., there are no additional addresses left). As a result many businesses are migrating towards IPv6, the next generation Internet communication protocol.

As more content and service providers begin to transition to IPv6, it's essential that organizations deploy network security devices that can deliver the same level of protection for IPv6 content as IPv4. The two most common are dual-stack and tunnelling. Dual-stack is preferable because it allows the security device to process each network packet in either IPv4 or IPv6.

Checklist: traditional security technologies are still needed

- ✓ **Firewall - Stateful Traffic Inspection and Packet Filtering**

  One of the most fundamental protections for networks of any size is a stateful firewall with packet filtering capabilities, which can selectively allow or block outsiders from accessing private data resources. A firewall, working closely with other networking infrastructure, examines each network packet to determine whether or not to forward it toward its destination according to policy.

- ✓ **Virtual Private Network (VPN)**

  With the number of threats accelerating, secure communications between enterprise networks, businesses and partners, and corporations and mobile workers is now more important than ever. Data breaches, information leaks, and infected networks and systems are costing corporations and government agencies billions of dollars every year.

  VPN technology allows organizations to establish secure communications and data privacy between multiple networks and hosts using IPsec and secure sockets layer (SSL) VPN protocols.

- ✓ **URL Filtering**

  URL filtering is typically deployed to prevent users form visiting dangerous or inappropriate web sites.

- ✓ **Antivirus/ Antispyware**

  Malware infections in networks, servers and endpoint devices cost billions of dollars every year. Ensure your antivirus technology combines advanced signature and heuristic detection engines to provide multi-layered, real-time protection against both new and evolving virus, spyware, and other types of malware attacks in web, email, and file transfer traffic.

- ✓ **Antispam**

  Just like viruses and spyware, unsolicited email in the form of spam costs businesses billions of dollars every year. Employees spend time sorting and deleting spam from their regular email while servers and networks have to contend with the extra traffic generated. In addition, spam emails are the most common means with which bots propagate, and often contain malware and links to inappropriate sites.

  A large amount of spam is sent everyday by improperly configured or virus-infected host email servers. Ensure your Antispam Service maintains an IP reputation database where the reputation of each IP address is updated based on information gathered from multiple sources. IP address reputation properties can include 'whois' information, geographical location, service provider, host server information, and more.