

# Next Generation Firewalls

Graham McLean

Managing Director

---

# Contents

Introduction	3
What the Industry says	5
In the News	7
New breed of attack	8
Advanced evasion techniques	10
Intrusion protection system	11
Ring fence your network	12
Summary	13

## Distribution List

Name	Title	Company

Author: Graham McLean  
Version: V1.1

---

## Introduction

“Keeping your network, IT systems and data secure is high on the agenda of all businesses”.

There is nothing new in this statement. In fact most have been aware of the threat for almost two decades and everyone understands the benefits of a Firewall. Here lies the heart of a real problem that many individuals and businesses have not yet woken up to. The firewalls that have served us well for the last 20 years are now rendered helpless against a new breed of attack. Too many companies are being complacent about the real risk of being a victim of, or being used as a launch pad for, a new wave of advanced cyber-attacks.

When we say a new breed there are four important things to be aware of:

1. This new breed of attack is carried out by criminals for gain. In the past the virus was more about notoriety and caused hindrance, but this new kind of attack is serious crime. ‘They’ are after personal details, banking records, credit card data. Information that can be used for illegal monetary gain.
2. ‘They’ use sophisticated Anti Evasion Techniques embedded in application traffic to gain access into your network. This works because the application being used is considered to be safe by your existing firewall.
3. Whilst many people assume that the companies at risk of such attacks are within specific industries, such as finance, the reality is that all companies are potential targets. It is simply not sufficient to undermine the risk based on your industry type and the perceived value of your data in the public domain.
4. There is the additional threat of commissioned attacks, where some networks are specifically targeted to order, be it for competitive gain or exploitation by the media.

---

In this white paper we will:

- Explore how the new breed of attack works.
- Explain why first generation firewalls are no match for these attacks.
- Discuss the use of web 2.0 applications, which are the main carriers for the new wave of attacks.
- Explain how a next generation firewall will help.
- Consider the need for the next level of security - a fully blown Intrusion Prevention System.
- Talk about the advantages of having distributed firewalls at all endpoints as part of a unified security platform.
- Advise on the next steps.

Before we get into the details let's take a look at what the IT security industry and analysts are saying and review some recent news stories.

## What the industry says

The need for enhancing your security capabilities is not something Link-Connect, as a Managed Security Service Provider, is on a lone crusader for. The whole security industry is aware of the dangers and are all working on their own next generation solutions. The following are extracts from information readily available from major security industry players.

### **Stonesoft**

The first generation of firewall technology was developed for first generation networks. With the proliferation of sophisticated network threats, many of which are a by-product of advances in Web 2.0 and cloud computing, enterprises have been challenged to secure their networks within the limits of their budgets, staff and available technology.

The rise of Next Generation Firewall technology is quickly giving enterprises the ability to more effectively secure their networks at the perimeter level – as well as address several other formidable network concerns like availability and lack of centralized management. Through its long history of developing market leading high availability and centralized management technologies that are built in with its firewall solutions – not to mention advanced security performance – the StoneGate NextGen Firewall is uniquely qualified to lead the Next Generation Firewall evolution.

### **Palo Alto**

The firewall is a cornerstone of most organization's information security strategy. However, the effectiveness of this security stalwart is steadily diminishing as threats continue to migrate up the computing stack and as applications of all types are engineered to take advantage of web technologies and other services that are typically allowed by enterprise policies. Furthermore, attempts to counteract this trend by bolting capabilities such as deep packet inspection on to conventional firewall products are not sufficient. Too much unwanted traffic, some of it potentially laden with threats, is still able to get through. What organizations need instead is a next-generation firewall system – one that incorporates application awareness at the core of its design, has fully integrated threat protection, and also includes a customized hardware architecture to deliver a suitable balance between security and performance.

## **Juniper**

Today's enterprise and public sector networks are more geographically distributed than ever before. Enterprise applications are more centrally located and must be flawlessly and securely delivered to all locations. This evolution offers many new opportunities but also has spawned a new generation of network threats.

## **Check Point**

New endpoint vulnerabilities such as Web-based malware are increasing information security risk in the enterprise. Traditional point solutions compound administrative overhead and management complexities. In response, organizations are demanding a new strategy that includes a broad set of technologies for endpoint security unified into a single agent with central control.

## **Gartner (extract from Cisco White Paper)**

Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware.

Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network.

Next-generation firewalls, according to Gartner, integrate firewalls and IPSs such that traffic is inspected just once for both functions. By contrast, having to inspect traffic once for connection layer access information and then again for malware would significantly slow down system throughput.

---

## In the News

In addition to the industry players there are numerous national news stories that talk about how major corporations' security is being breached. These are the ones we hear about, just like an iceberg there are many more such stories below the surface that do not hit the headlines.

BBC News 3 June 2011

### Sony investigating another hack

Sony is investigating another hacking attack on one of its websites.

A group called Lulz Security claims to have broken into Sonypictures.com and accessed details of a million users.

Passwords, home addresses and other personal information relating to several thousand of the accounts was released online.

It is the third major hack to hit Sony since April when the PlayStation Network was targeted and the details of 77 million users compromised....

<http://www.bbc.co.uk/news/business-13636704>

BBC News 25 November 2011

### Exposing Russia's murky trade in exploit hack packs

Russian computer programmers have created an industry supplying criminals with easy-to-use automated hacking software which can take control of a home PC in seconds.

This type of software, called an exploit pack, takes advantage of known flaws in commonly used programs, such as Adobe Reader and Internet Explorer, to hack computers without the need for human intervention.

Criminals are then able to install viruses or steal online banking details without the need for any technical expertise.

The exploit pack market mimics the market for legal software, with vendors offering criminals trial periods, regular updates and even 24-hour technical support.....

<http://www.bbc.co.uk/news/technology-15877751>

---

## New breed of attack

Let's take a quick look at the history of cyber attacks.

**Phase 1:** In the very early days the attacks were a direct hit on an unprotected PC or exploiting a known flaw in an operating system or application. This was particularly true for Microsoft; hence it was imperative to apply the patches as they were released to stay safe from the latest exploit.

**Phase 2:** As we all became aware of the need for a firewall and to stay current on patching, the attacks moved to a slightly more sophisticated process of delivering the payload (virus, trojan, bot...) via files that had to be opened. These would be via email attachments, instant messaging attachments or files that we were encouraged to download from web sites. Because these attacks entered via email or web browsing, vendors improved firewalls and anti-virus capabilities by focusing on a small number of ports and protocols. At a human level we all got wise to not opening attachments from any unknown source. In this phase the end user was downloading or receiving a file as a discrete action. As we look at the next phase we will see how the door is opened and the download is an automated ongoing background activity.

**Phase 3:** With the explosion of the use of 2.0 web applications the security door has once again been well and truly opened. Examples of Web 2.0 applications include Facebook Twitter, Skype, YouTube, MSN, Google Apps, LinkedIn and Yousendit – there are thousands more...

Unlike an email or download which is a one off activity web 2.0 applications are like a permanent online connection between your client and the web server. Once the application is active, your client will poll for updates on a constant basis and will receive anything that is sent. This is a feature of the way the client server architecture works. All the effort has gone into making sure the client is asking for legitimate content, once the connection is active the server can send pretty much anything and the client will receive it and try to interpret it.

In a similar way to Phase 1, some payloads are placed into legitimate web content that has been hacked at its source, i.e. on the web server. A good example of this is Spotify where an advert played between the music content had been hacked and a payload incorporated into the video stream in the advertisement.

The other common way to deliver a payload is to include it into content that is then published onto the web site and wait/encourage visitors to access such content. First generation firewalls will not spot such attacks because they see the communication between the client and the server as legitimate and are not capable of checking the contents as it flows through the firewall.

One way to stop this kind of attack is to 'switch off' these applications, but this is becoming more and more difficult as the line between web 2.0 applications being social network or business critical tools is now blurred.

The only real way to stop such attacks is to inspect the content, not just the envelope, in real time as the data is passing through the firewall. This is exactly what a next generation firewall is designed to do. The deep packet inspection of the NGF is looking for known signatures or data patterns matching those held in its library of known attacks.

This is further complicated by the explosion in the number and variety of client devices. Once a single client device is infected then the corporate network is exposed, unless you deploy a ring fence at all edge points on your network.

The good news about some NGF is that they will watch both inbound and outbound traffic. In the event that a botnet is deployed and starts to pass data to its control and command centre the NGF will spot unusual traffic being sent and can prevent the activity or at least alert it before the problem is too serious.

---

## Advanced Evasion Techniques

NGF will protect against the most common payloads embedded in the most common applications, which is a big step forward for most companies and will probably be sufficient protection. However for some more targeted companies a full blown IPS is the only way to really secure your network.

TCP/IP, the protocol suite used on the Internet and the vast majority of all computer networks, is based on the requirements from RFC 791 that was written in 1981. Among other things, the RFC says, “In general, an implementation must be conservative in its sending behavior, and liberal in its receiving behavior. That is, it must be careful to send well-formed datagrams, but must accept any datagram that it can interpret (e.g., not object to technical errors where the meaning is still clear)” (Postel, 1981, p. 23). That means there will be multiple ways to form messages that will be interpreted identically by the receiving host. While this permissive stance was intended to make interoperability between systems as reliable as possible, it at the same time paved the way for a number of attacks and ways to hide those and other attacks from detection.

As different operating systems and applications behave in different ways when receiving packets, the destination host’s application may see something quite different than what was in the network traffic. Also, the network itself between the detection system and the host may alter the traffic. By carefully exploiting these differences, in many cases, it is possible to construct packets in a way that looks normal and safe, but when interpreted by the end host, forms an exploit against it. In general, these techniques are called evasions.

---

## Intrusion Protection System

Here is a classic example of Pareto's Law. A good NGF will protect you from around 20% of the known attacks but this will equate to 80% of the criminal activity. An IPS will protect you from the additional 80% of known attacks but this represents about 20% of the activity and is typically aimed at specific targets.

To really address Advanced Evasion Techniques a NGF alone is insufficient and IPS needs to be deployed.

Like all technology some IPS systems are stronger than others. Because of the way the known payloads can be transformed and thus hidden from even some of the most popular IPSs we selected StoneGate as our preferred solution as it can detect the payloads even in their disguised forms.

Whilst a NGF will be a great help in preventing malicious code entering your network it is no guarantee, even adding IPS will not be a guarantee. Those who want to perpetrate such malicious activities will work on the next attack to bypass the security systems as we have seen with the advanced evasion techniques.

---

## Ring-fence your network

Managed Network providers create a private cloud with a central breakout to the Internet either from head office or from within the Service Providers core network. Traditionally all the security effort is focused at the interface with the public world and all traffic on the private cloud is considered safe. As we have seen above this is not necessarily the case as there are advanced (and ever advancing) new techniques designed to breach whatever security system is put in place. It is not just PC clients accessing the internet for browsing, email or applications, it is that USB stick or mobile devices that can be the entry into the corporate network.

The fact is that all nodes on the network have some form of CPE to receive whatever link is deployed to that particular site. Link-Connect recommends that all these routers also be Next Generation Firewalls in an active mode. This way you will significantly increase your chances of spotting any unusual traffic or application usage inside your network before the attack even attempts to send the data to the outside world. In order to manage this configuration effectively it is necessary that these distributed Firewalls can be managed from a central management centre otherwise the task of updating 10s or even 100s of firewalls is too big a workload and is too prone to error if managed manually.

---

## Summary

Cyber attack has moved from being a real nuisance to being really malicious. First generation firewalls are effectively redundant as cyber criminals up their efforts to penetrate corporate networks. No organization is immune to these attacks – every organization owns data that is valuable to someone else. As the business use of web 2.0 applications grows the potential for attack increases.

The first step towards understanding the vulnerability of your network is to subject it to independent review or penetration test. With these data in hand you will be better placed to understand where your weaknesses lie and how at risk your corporate data and systems are.

Leading experts across the industry recommend next generation firewall technology.

In Gartner's research note, "Defining the Next-Generation Firewall" they find that the stateful protocol filtering and limited application awareness offered by first-generation firewalls are not effective in dealing with current and emerging threats and recommend that if you have not yet deployed network intrusion prevention, you require NGF capabilities at your next firewall refresh point. Link-Connect fully agrees with these findings and recommendations.