

# Intrusion Detection & Response - Leveraging Next Generation Firewall Technology


Ahmed Abdel-Aziz

# Intrusion Detection & Response Leveraging Next Generation Firewall Technology

*GCIA Gold Certification - Practical Assignment*

**Author:** Ahmed Abdel-Aziz, CISSP

**Advisor:** Joel Esler

Accepted: February 19th, 2009

# Table of Contents

## 1. Abstract

This paper will address a recent trend in network security, which is leveraging next-generation firewalls (**NGFW**) at the network perimeter. The paper will demonstrate how this relatively new type of firewall technology can be used in intrusion detection, analysis and response. The focus will mainly be on Fortinet technology as one of the leading vendors in that space. By writing this paper, I wish to benefit the security community by sharing useful knowledge and techniques related to NGFWs. Not only will this information help others in the field make optimum use of Fortinet NGFWs, it will also enable the use of other vendors' NGFW products as well.

## 2. Background

Online and data security threats continue to increase in number and sophistication (Cisco, 2008). In the UK, overall cybercrime increased by 9% from 2006 to 2007 according to the Garlik UK Cybercrime Report (Falinski, Minassian, 2008); financial motivation is fueling the attacks. As indicated by the McAfee Virtual Criminology Report, trojans increased from 40,000 variants in 2007 to nearly 120,000 in 2008 and the global recession will only increase cybercrime (McAfee, 2008). This makes the near future state of the global economy a catalyst to an already increasing trend in cybercrime activity. Therefore, making optimum use of any security technology, process, or knowledge is logically a step in the right direction. By writing this paper, I hope to make a significant contribution in that right direction.

## 3. Network Firewalls

In the business environment, information security is about supporting the business to achieve its goals. Security mechanisms work together in a concerted effort attempting to reduce risk and enable the business. One key security mechanism that has been around since the 20th century is the network firewall.

### 3.1 The Firewall Role

If we wanted to summarize the role of a firewall by answering one simple question: **"What does the firewall do?"** The simple answer would be: **"The firewall controls data flow."** Whether the firewall is a personal firewall used by an end-user to control data flow to and from the computer, or a network firewall controlling data flow to and from different security zones (DMZ, Internet, LAN, etc.); the firewall is basically controlling what data is allowed, or not allowed, to flow according to predefined firewall rules that enforce the organization's security policy.

As noted earlier, firewall technology has been around for some time, as early as the 1980s (Wikipedia, 2008); therefore researchers have had ample time to advance the technology. The next section briefly discusses firewall types.

### 3.2 Main Firewall Types

This paper is not about the various firewall types and architectures available; such a detailed focus on these topics has been the subject of various published books and papers in the technical and commercial literature. However, we will briefly address the main firewall types for the sake of elaborating how Next-Generation Firewalls fit into the firewall picture.

| *Firewall Type* | Packet-Filter | Stateful Packet Inspection (SPI) | Application Proxy | Deep Packet Inspection (DPI) |
|---|---|---|---|---|
| *OSI Layer* | Transport Layer | Transport Layer | Application Layer | Application Layer |
| *Generation* | First Generation | Second Generation | Third Generation | Fourth Generation |
| *Main Characteristics* | Looks at destination and source addresses, ports, and services requested. Routers using ACLs dictate acceptable access to a network. | Looks at the state and context of packets. Keeps track of each conversation using a state table. | Acts as a middleman between communicating systems by breaking the session and reestablishing a new session to each system. Different proxy required for each service allowed. | Looks deep into packets and makes granular access control decisions based on packet header and payload. Excels in managing application and data driven threats. Incorporates intrusion detection and prevention technology features. |
| *Resource Requirement* | Low | Low-Medium | High | Medium |
| *Firewall Design* | Initial Design | Design Considered Evolution of Packet-Filter | Alternative Design | Design Considered Evolution of Stateful Packet Inspection |

The table above briefly compares the four main firewall types from different perspectives. Although the four types vary greatly in features and capabilities, each one of the firewall types can play a role in securing the organization. For example, a packet filter firewall would be good for high performance egress filtering, whereas an application proxy firewall would excel as a web application firewall to prevent SQL injection attacks. The focus of this paper is on the Deep Packet Inspection (DPI) firewall type, which is discussed in more detail in the following section.

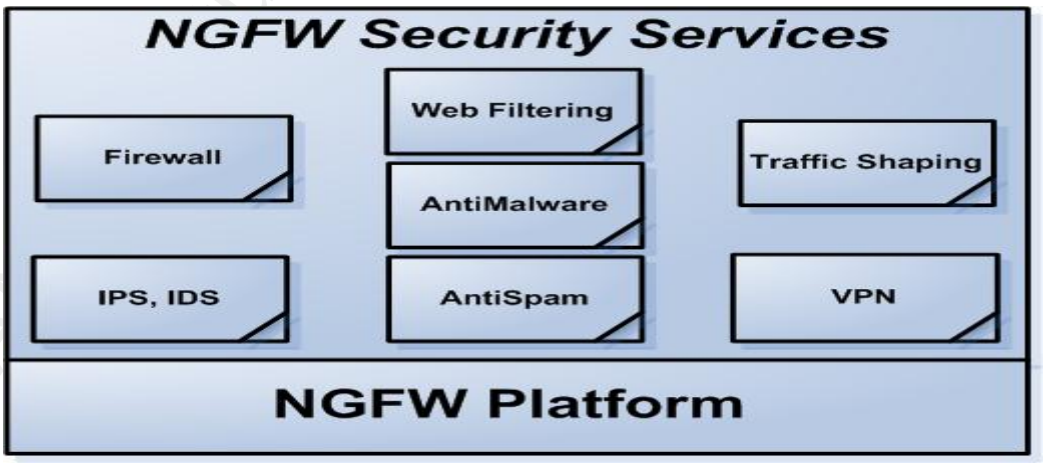
## 4. Next-Generation Firewalls (NGFWs) – The Evolution

Next-generation firewalls use deep packet inspection (DPI) as a core technology (Young, 2008). It is important to note that I have not yet found a constant and detailed definition of a NGFW, although attempts have been made to define what a NGFW can include (Young, Pescatore, 2008). In the context of this paper, a next-generation firewall is a term used to represent the new generation of stateful firewalls that integrate intrusion prevention, malware filtering, as

well as other security functions to allow more advanced control of data flow. As indicated in the Main Firewall Types table above, these new firewalls look deep into the packet's payload before making a decision on whether to allow or deny the traffic flow. Essentially, they are performing the main firewall role of **"controlling data flow"** but at a much finer and more granular level than was possible with stateful firewalls. Since these firewalls perform application level inspection and intrusion prevention, and are gaining momentum, Gartner predicts that the NGFW market will overtake the stand-alone IPS appliance market at the enterprise perimeter (Young, 2008). The subsections below present the current main security services of a NGFW, as well as new and future security services expected in this advancing firewall type.

### *4.1* Current NGFW Security Services

The different security services of the NGFW work together to provide a higher level of security than stateful packet inspection (SPI) firewalls, due to deep packet inspection (DPI) capability. The security services below are based on Fortinet technology but represent more or less the current state of next-generation firewalls.



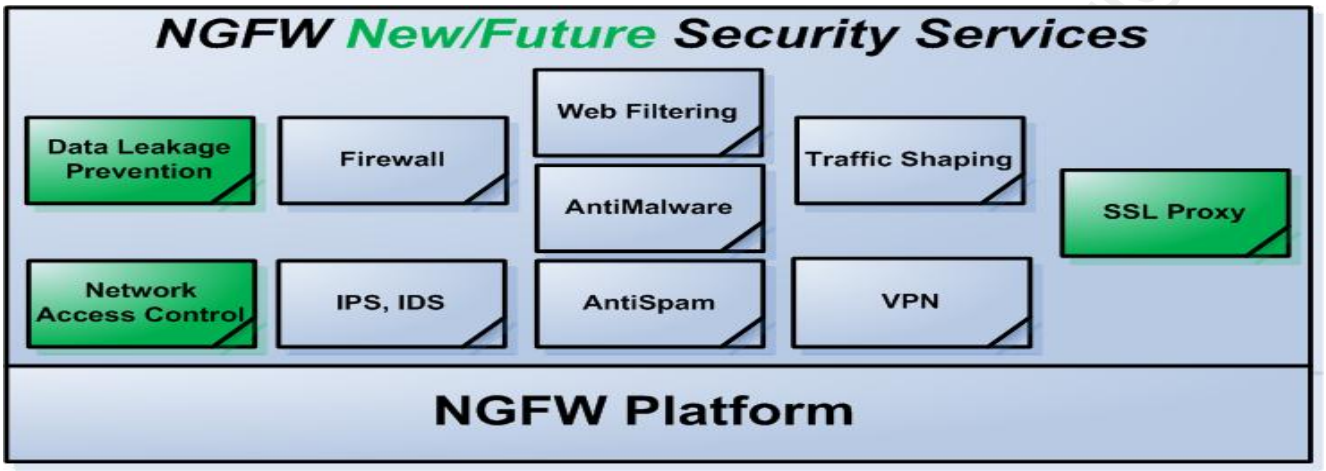

- **Firewall:** Providing multi-layer and protocol inspection, network segmentation, and access control.

- **Intrusion Detection & Prevention:** Featuring wide range of detection techniques (ex: header-based, pattern matching, protocol-based, heuristic-based, anomaly-based), and rich customization capabilities.
- **Anti-Malware:** Providing malware protection on all web, mail, and file transfer traffic.
- **Web Filtering:** Enforcing access to allowed web content and filtering high risk URLs such as anonymizers and known hostile addresses.
- **Anti-Spam:** Mitigating directory harvesting attacks, spam, and enforcing email policy.
- **Traffic Shaping:** Apply quality-of-service (QoS) to various applications' traffic such as: instant messaging (IM), web, streaming video and audio, or Peer to Peer (P2P) if allowed.
- **Virtual Private Network (VPN):** Provide remote access and secure site-to-site interconnection over untrusted networks. Support protocols such as IPSec, SSL.

### *4.2* New & Future NGFW Security Services

To provide finer and more granular control on network traffic flow to cope with changing business requirements and blended threats, new security services are being integrated into NGFWs. Stateful firewalls focused on network ports and protocols, while NGFWs focus deeper on the applications and data. The new security services address current blind spots (caused by encryption), and allow decisions to be made based on content and context (Higgins, 2007); for example, decisions such as allowing credit card numbers and intellectual property to move only from one security zone to another, otherwise traffic is denied; or being able to detect and prevent SSL encrypted threats. The following represents a sample of new or future security services offered by NGFWs; Palo Alto Networks, a new vendor

in that space supports a number of these services (Palo Alto Networks, 2008).




- **SSL Proxy:** Manage encrypted threats by selectively terminating SSL connections, decrypting, analyzing traffic, and re-establishing encrypted connections transparently.
- **Data Leakage Prevention (DLP):** Control flow of intellectual property, credit card numbers and other sensitive information.
- **Network Access Control (NAC):** Integrate with Network Access Control (NAC) solutions in provisioning appropriate network access.

### *4.3* Benefits & Drawbacks

In this imperfect world, NGFWs are not an exception. This subsection will highlight some of the pros and cons of NGFWs.

**Benefits:**

- The tight coupling of the various security services in the NGFW, especially latency-sensitive services -IPS and Firewall- has the potential of providing basic level and tested integration between the various services. This introduces operational advantages over many point products offering the same security services. With the right integration, higher security effectiveness can be achieved. For instance, a web-filtering component detecting a compromised host connecting to a known malicious IP can quickly make the

firewall component block communication, leading to better intrusion detection and response. Better intrusion detection and response is crucial when most compromises are within days, most discoveries of compromises take months, and 82% of compromised cases already had the data to prove compromise (Baker, Hylender, Valentine, 2008).

- Complexity in architecture and self-management of many point products works against security, when the needed high level security skills are not available.
- Integration of security services in one appliance can also provide economic advantages.

**Drawbacks:**

- On the other hand, best-of-breed point products are multi-vendor. The combination of multiple security services in one box has the tradeoff of missing out on best-of-breed products.
- Relying on one vendor for firewall, IPS, Web filtering, Antimalware, and other security services represents a single point of failure, especially if no high availability features are put in place.
- Performance can become an issue due to the high resources required to simultaneously fulfill the many security requirements of a large number of sites, users and connections.

**Best of Both Worlds Strategy:**

The Next-generation firewall provides many benefits and like its predecessor, the stateful firewall, is a cornerstone of an organization's security program. By leveraging the defense-in-depth principle, a NGFW could be used as a key security mechanism at the perimeter which can be augmented with other mechanisms. These other mechanisms would be best-of-breed point products employed when there is high risk exposure to information or information systems. The idea basically is to make more security investments when there is a high

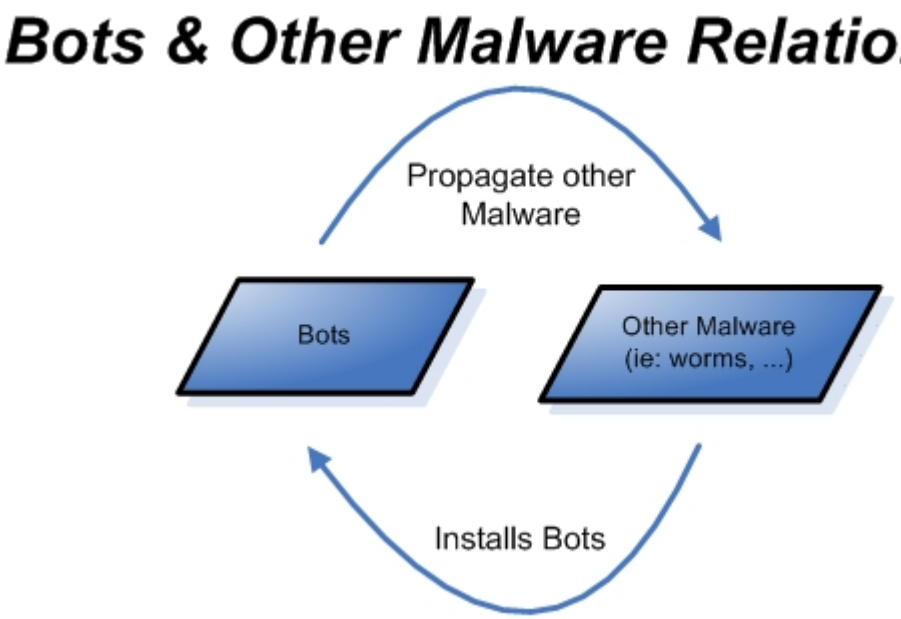
level of risk; this strategy could be one option in trying to make the best of both worlds.

## 5. Detecting & Analyzing Bots on the Network

This section addresses the following problem which many organizations have to deal with; bots on their networks. We will address this problem mainly from a NGFW perspective, since thorough coverage on bot detection and analysis requires complete papers. When examples are given to elaborate, they will be related to Fortinet technology.

### *5.1* Botnets on the Rise

As defined on WhatIs.com, a bot "short for robot" is a program that operates as an agent for a user or another program or simulates human activity." A botnet is a collection of bots that are commonly controlled. Bots and botnets are not necessarily malicious. For example, a web crawler bot, or a network of computers using distributed computing software are not necessarily malicious. But the terms are often associated with malicious software. Botnets are growing more powerful and destructive and some believe that botnets have grown into the largest threat facing the Internet (GreenGard, 2008). Two botnets that have gained notoriety over the last few years are Kraken and Storm. The rise of trojan variants to nearly 120,000 in 2008 from 40,000 in 2007, as indicated by the McAfee Virtual Criminology Report, is one indication of malicious bots on the rise since these bots are one form of trojans. Botnets help cyber criminals make serious money (Skoudis, 2007), no wonder they are on the rise! There is a mutual benefit win-win relationship between bots and other malicious software; the figure below illustrates the relationship.




In addition to propagating other malware, bots perform a variety of tasks with some examples below:

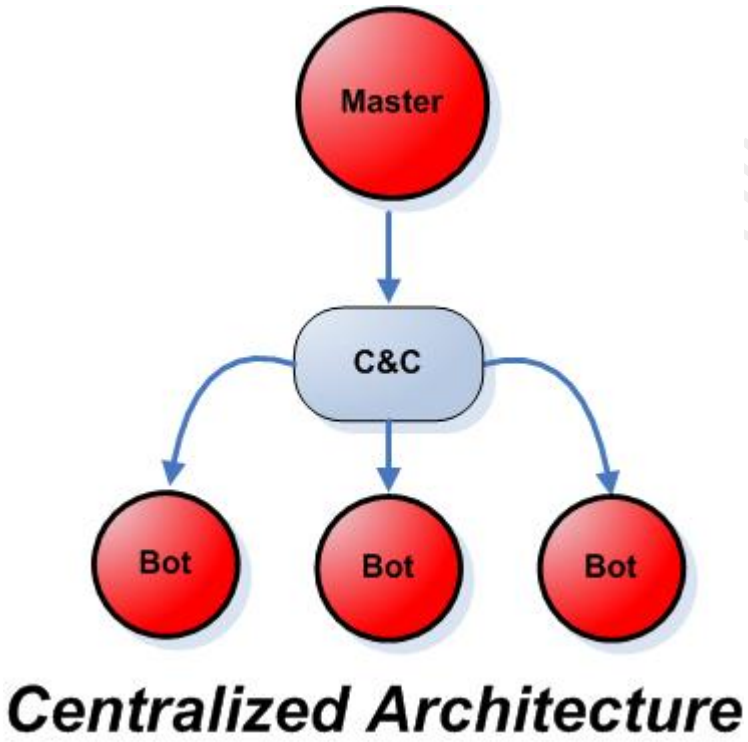
- Steal passwords, identities, intellectual property, and other sensitive information.
- Send spam, produce adware, act as proxy, and perform click frauds.
- Execute distributed denial of service attacks (DDOS) on a target.

## 5.2 Botnet Architectures (Centralized vs Decentralized)

Botnets can be classified according to their architecture; currently there are two main types of architectures: **Centralized** and **Decentralized**.

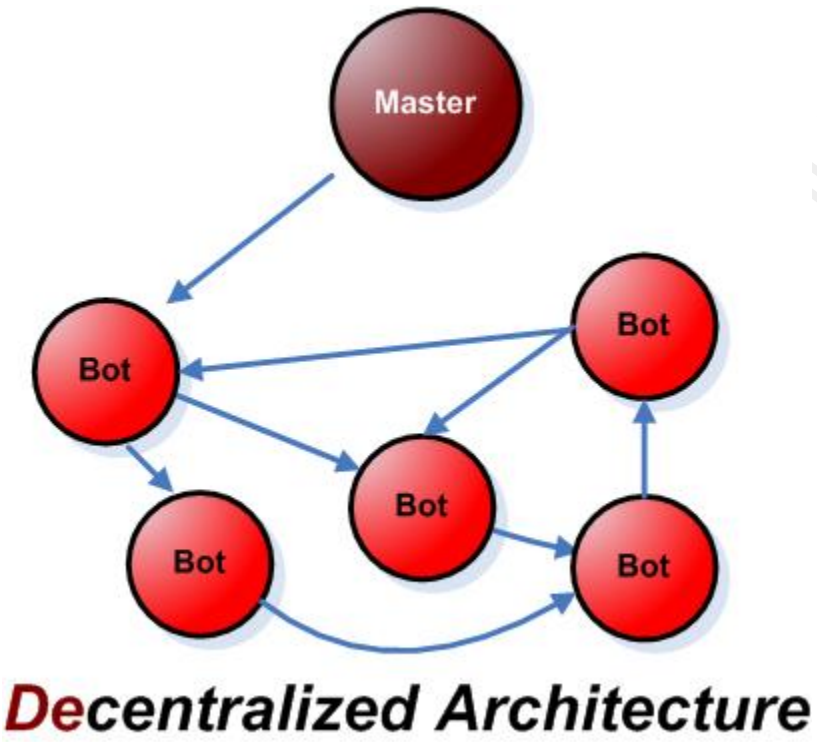
**Centralized Botnets:**

In centralized botnets, all the bots are connected to a single command-and-control or C&C. The bots connect to C&C and register in its database, their status is tracked and they are sent selected commands from the botnet owner. All the bots are visible to the C&C, from which the owner manages the botnet. Centralized botnets have historically preceded decentralized botnets and are easier to take down due to their single point of failure, the C&C.




**Decentralized Botnets:**

In decentralized botnets, the bots connect to other infected machines rather than to a single command-and-control. Each bot has a list of neighbors; commands are transferred from one bot to another until the command is distributed across the whole botnet. Therefore, the bot owner needs to have access to at least one bot on the zombie network to be able to manage the entire botnet. In practice, decentralized botnets can start off as centralized with a C&C to receive a list of neighbors, and then revert to decentralized afterwards (Kamluk, 2008). Taking down decentralized botnets is much more difficult because there is no single point of failure, contrary to centralized botnets where the C&C is a single point of failure.




Now that we have covered botnet architectures, we move to bot detection techniques.

## 5.3 Bot Detection Techniques

Bots are clearly a problem; their detection is also a challenge since many bots, like Storm, mutate every 30 minutes (Fortinet, 2007). Antimalware vendors have a hard time catching up with these continuous changes, which makes signature-based detection very difficult for mutating bots. Bot detection and defense techniques fall into two broad categories: **host-based** and **network-based**. Our focus will be more on the network-based techniques since that is where the NGFW is. This analysis is from a technology perspective only since people's security awareness and sound policies go a long way in protecting organizations from bot threats.

### 5.3.1 Host-Based Techniques:

- Antivirus and antispyware software using signature and heuristic detection techniques for bot detection and removal. Some vendors are now offering specialized Antibot software for the same purpose. In addition, a strong patch management system will

quickly fix known software vulnerabilities, which can limit malware propagation.

- Host intrusion detection/prevention systems (HIDS/HIPS) limiting the various applications that can run on a system.
- Host based firewalls to limit network communication.
- Techniques based on common OS tools such as netstat, reg, dir, tasklist, and others, example here.

### 5.3.2 Network-Based Techniques:

#### *5.3.2.1 NIPS Component in NGFW*

Network intrusion prevention systems (NIPS) defend against bot infection by blocking known network attacks that precede malware infection. They can also block attacks originating from internal bot infected hosts, allowing the detection of compromised hosts. In addition, command-and-control traffic of popular bots can be blocked using IPS signatures. By cutting communication between the bot and its command-and-control server, the host is still infected with the bot, but is unable to perform its duties or update itself. For the NIPS to be able to block bot's command-and-control traffic, it is necessary that the traffic not be encrypted. Unfortunately many bots, such as Storm and Nugache, use encrypted command-and-control communication; this makes the NIPS unable to block the communication.

#### *5.3.2.2 Block Protocol used for Command-and-Control*

In the first technique, the protocol used for command-and-control was allowed, but the command-and-control traffic itself was blocked. This is equivalent to allowing IRC traffic, but blocking known IRC command-and-control traffic. In this second technique, the protocol used for command-and-control is blocked altogether. For example, Fortinet suggests a procedure to use on Fortinet's NGFW to prevent the storm worm from updating itself. This will eventually allow the antivirus signatures to catch up and eliminate the worm. Quoting from Fortinet's website:

*"The worm uses the P2P eDonkey protocol to communicate with its Command and Control servers to get updates to be able to mutate. Therefore, if any of the PCs in your network is affected by this worm, you can use a FortiGate protection profile and firewall policy to block the eDonkey application and allow the AV signatures to catch up and eliminate the worm.*

*To block eDonkey*

1. *Go to **Firewall** > **Protection Profile.***
2. *Edit a protection profile or add a new protection profile.*
3. *Select the blue arrow for IM/P2P.*
4. *Select Block for eDonkey.*
5. *Save the protection profile.*
6. *Go to **Firewall > Policy***
7. *Make sure the eDonkey-blocking protection profile is added to firewall policies that allow Internet access through your FortiGate unit."*

For people unfamiliar with Fortinet technology, the meaning of a "**Protection Profile**" listed in the above procedure may not be clear. A protection profile is a group of settings that can be applied to firewall rules to allow finer granularity in controlling data flow. In this procedure, the protection profile created states that the eDonkey P2P protocol is not allowed. The protection profile is then attached to a specific firewall rule to enforce the blocking of eDonkey P2P traffic matching that rule. For more information about Protection Profiles, the FortiGate administration guide is an excellent reference (Fortinet, 2009).

#### *5.3.2.3 Reviewing Firewall Logs & the Network Audit Trail*

Logging firewall policy violations and setting up a network audit trail can be invaluable for malware detection even without a perimeter antivirus. For example, a NGFW policy that does not allow outgoing IRC & Peer-to-Peer (P2P) protocols, and logs the violations, will detect bots on the internal network attempting to communicate with C&C or other bots through these protocols. This does not mean that all logged violations are due to bots on the network, since a user may be running an application that is generating the traffic; however it is an indication that these violating machines need further investigation. In Fortinet NGFW technology, there is an

implicit deny at the end of the firewall policy, but violations are not logged by default. I have found that by adding an explicit deny rule that logs violations, at the end of the outgoing firewall policy, some bots on the internal network are easily detected. These are the bots that generated policy violating traffic, which demonstrates the importance of having a strict outgoing firewall policy. Unfortunately, the outgoing firewall policy is very often too relaxed. The figure below shows how the explicit deny rule is configured.


Another useful technique is to review the network audit trail. This can be done using a sniffer such as Wireshark on the network perimeter. Returning to Fortinet NGFW technology, a network audit trail *(up to the application layer)* can easily be setup. By choosing to log allowed traffic for each firewall rule configured in the firewall policy as in below figure, in addition to enabling all application layer logging in the associated protection profile, a traffic log for network sessions is available. This type of logging will require a dedicated log collection and reporting appliance referred to by Fortinet as the Forti-Analyzer.

**Note:** Both figures above and below have a title of "New Policy"; I personally found this a bit misleading at first as the graphical interface is actually used to configure a new firewall rule which is only part of the firewall policy. This is mentioned just to clear any confusion.

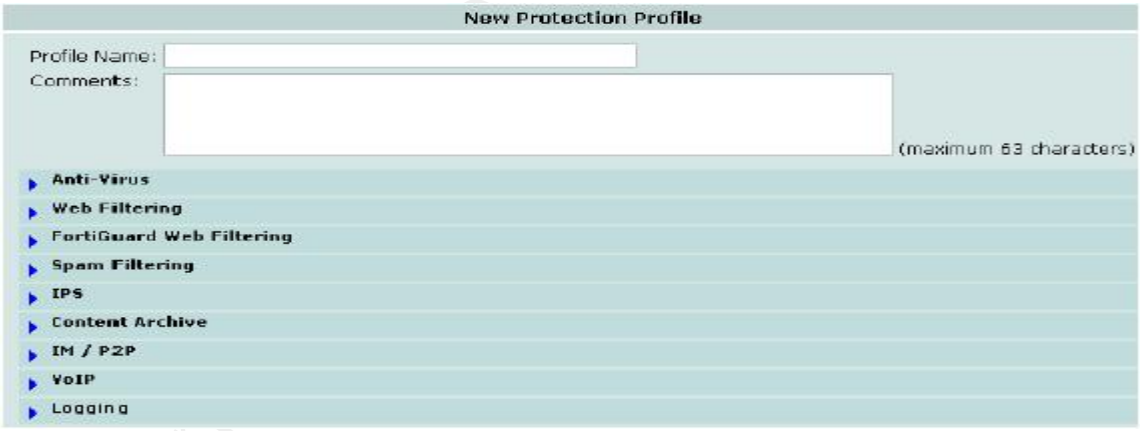

Since the network sessions log is a high level log created mostly from the protocol headers, the log is handy in performing traffic flow analysis. For example, the traffic log can indicate that there is unusual high web/DNS activity between an internal host and an uncommon web/DNS server. This may make a Security Analyst suspicious and cause the Analyst to decide to perform some passive reconnaissance on the web/DNS server using a Whois lookup service such as Samspade - only to find that the web/DNS server is associated with an organization in a distant country the host has no business with. This may well indicate a bot infection and would require further investigation from the Security Analyst.

#### *5.3.2.4 Filtering Malicious Content in Web & Email Traffic*

This technique is more of a bot defensive technique than a bot detection one, although it plays a role in detection as well. Social engineering plays a key role in bot infection; the following are examples of infection vectors (IPA, 2007):

- User is tricked into opening a file attached to a malicious email or instant messaging (IM) message.
- User is tricked into downloading and running software from a malicious web site.
- Infected due to client-side exploit from infected or malicious web site during normal user activity.
- Infected by clicking a link (URL) contained in a spam mail or instant messaging (IM) service, which takes the user to a malicious web site.

By filtering malicious content in web traffic through perimeter antimalware, perimeter web site filtering, and perimeter antispam, bot infection from the above threat vectors can be effectively mitigated. All these safeguards can be configured in a Fortinet NGFW protection profile as illustrated below.




#### *5.3.2.5 DNS Based Techniques*

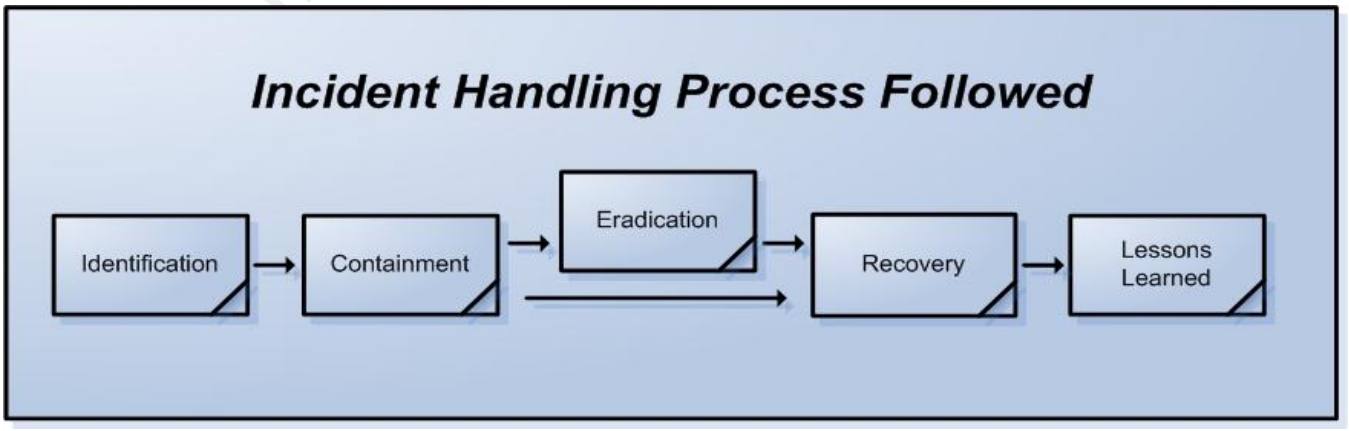
DNS allows mobility, which is an essential design goal for attackers (Dagon, 2005). One DNS technique, called **fastflux,** is used by attackers to hide phishing and malware delivery sites behind an ever changing network of compromised hosts. Multiple hosts, using a very short TTL *(time-to-live)* value, register and deregister their DNS A record for the same DNS name. The same can be done for DNS NS records. Both DNS record types can constantly be changing thus

serving the attackers' mobility design goal. Recent bots such as Storm make use of the fastflux technique (Wikipedia, 2008).

DNS based techniques can also be used in bot detection and defense. For example, hosts sending their DNS requests to an unknown DNS server, rather than to their internal or ISP DNS servers, could be infected. Hosts that are not SMTP servers, and are making a high number of MX DNS requests are most likely spam sending bots. Also, same DNS requests coming from many different internal sources at the same time would be suspicious (Shadowserver Foundation, 2007). Fastflux countermeasures such as blocking DNS replies with very small TTL values can be used (ICANN SSAC, 2008). The DNS based techniques in bot detection and defense are more or less detecting or defending against anomalous DNS traffic. I have not yet come across point-and-click functionality in current NGFW technology, specifically Fortinet, which can make use of these or similar DNS based techniques.

## 6. Security Incident Handling Using NGFW for Spam Sending Host

While performing some work at a site, a security incident took place. I was asked to help out in quickly mitigating the impact of the security incident, and I was happy to do so. This section discusses how the incident was handled at the site, which happened to be using Fortinet technology. The incident was handled using the below incident handling process.



The process followed in detecting and responding to the incident consists of five main phases. An explanation of each phase and what actions were taken in each of the phases are included in the later subsections. The five phases are as follows:

**1- Identification Phase**

**2- Containment Phase**

**3- Eradication Phase**

**4- Recovery Phase**

**5- Lessons Learned Phase**

## 6.1 Incident Handling Process – Identification Phase

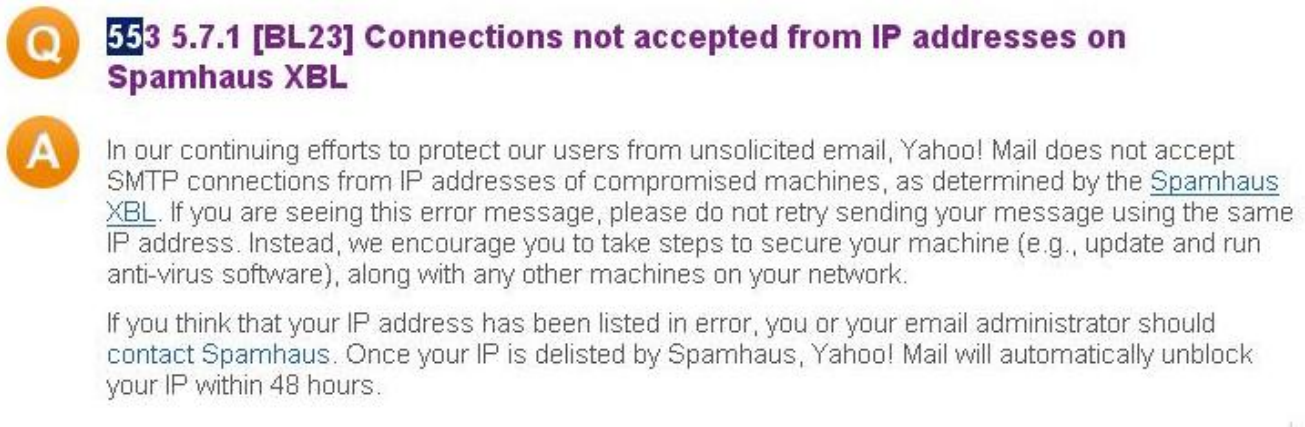
This phase of the process is where the security incident actually is detected. The initial symptom of this security incident was that users were not able to send any email to any destination on November 2nd, 3:30 PM. To further investigate, a simulation of email sending was carried out using the telnet application for sending SMTP commands to a destination mail server. The destination mail server used in the test was a Yahoo! mail server; however any mail server can be used. In order to perform the test, the mail server hostname is needed, which can be retrieved by requesting the MX records for a domain. The below commands are an example of how to carry out this task by using the Windows command-line.

```
 C:\>nslookup -query=mx example.com
Server:
Address:  192.168.1.1

Non-authoritative answer:
example.com     MX preference = 1, mail exchanger = c.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = d.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = e.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = f.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = g.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = a.mx.mail.example.com
example.com     MX preference = 1, mail exchanger = b.mx.mail.example.com

C:\>telnet c.mx.mail.example.com 25 (first listed mail server was chosen)
Destination Server Response: 220 smtp.example.com ESMTP Postfix
 SMTP Command Entered through Telnet Client: HELO relay.domain.org
Destination Server Response: 250 Hello relay.domain.org, I am glad to meet you
SMTP Command Entered through Telnet Client: MAIL FROM:<user@domain.org>
Destination Server Response: 250 Ok
```

```
SMTP Command Entered through Telnet Client: RCPT TO:<anotheruser@example.com>
Destination Server Response: 250 Ok
SMTP Command Entered through Telnet Client: RCPT TO:<thirduser@example.com>
Destination Server Response: 250 Ok
SMTP Command Entered through Telnet Client: DATA
Destination Server Response: 354 End data with <CR><LF>.<CR><LF>
SMTP Command Entered through Telnet Client: From: "User Example" <user@domain.org>
SMTP Command Entered through Telnet Client: To: Anotheruser Example
<anotheruser@example.com>
SMTP Command Entered through Telnet Client: Cc: thirduser@example.com
SMTP Command Entered through Telnet Client: Date: 2 Nov 2008 15:40:43 +0200
SMTP Command Entered through Telnet Client: Subject: Test message
SMTP Command Entered through Telnet Client:
SMTP Command Entered through Telnet Client: Hello,
SMTP Command Entered through Telnet Client: This is a test message with 5 headers
and 4 lines in the body.
SMTP Command Entered through Telnet Client: Your friend,
SMTP Command Entered through Telnet Client: User
SMTP Command Entered through Telnet Client: .
Destination Server Response: 250 Ok: queued as 12345
SMTP Command Entered through Telnet Client: QUIT
Destination Server Response: 221 Bye
```

*(The server then closes the connection)*

This would be a normal SMTP session; however what actually happened was the Yahoo mail server rejected the SMTP connection giving an error message and an associated URL for more information. The URL was visited using a web browser and a snapshot of the web page is included below.

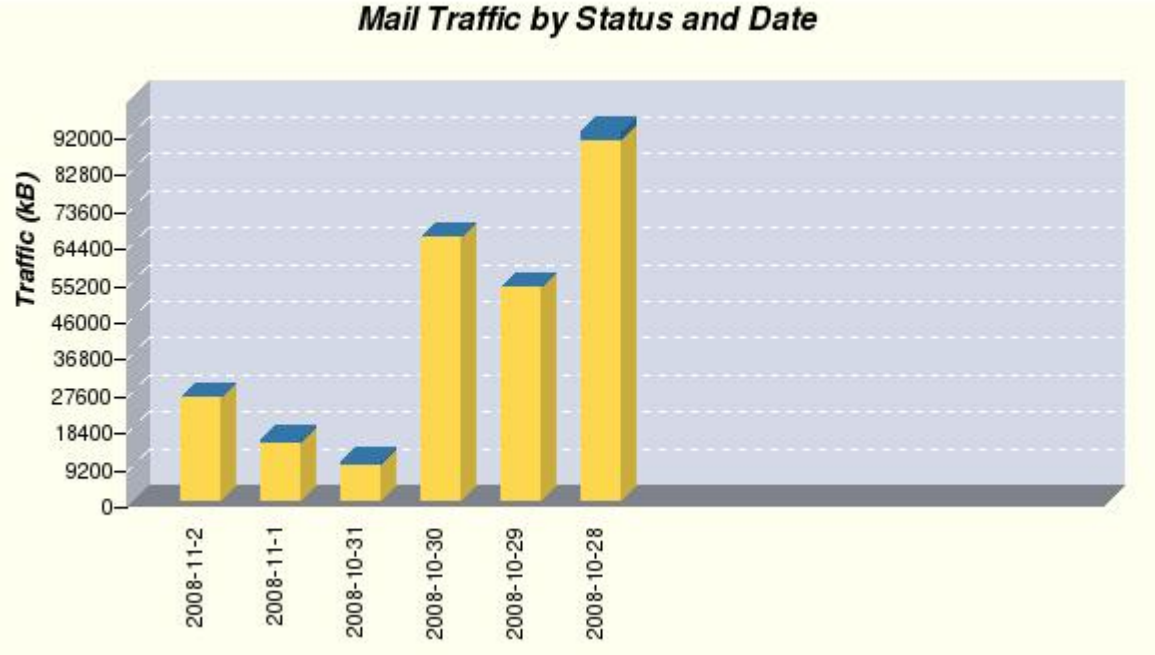


**553 5.7.1 [BL23] Connections not accepted from IP addresses on Spamhaus XBL**

In our continuing efforts to protect our users from unsolicited email, Yahoo! Mail does not accept SMTP connections from IP addresses of compromised machines, as determined by the Spamhaus XBL. If you are seeing this error message, please do not retry sending your message using the same IP address. Instead, we encourage you to take steps to secure your machine (e.g., update and run anti-virus software), along with any other machines on your network.

If you think that your IP address has been listed in error, you or your email administrator should contact Spamhaus. Once your IP is delisted by Spamhaus, Yahoo! Mail will automatically unblock your IP within 48 hours.

This message, along with users being unable to send email, indicates that the site's public IP address is sending SPAM. To confirm, the NGFW traffic logs were inspected for recent high activity in email traffic. The following is a snapshot from the FortiAnalyzer logs for recent SMTP activity.




The diagram confirms that there has been relatively high email activity in the recent past, which stopped by October 31st 2008. The publicly available black lists were checked through MXToolbox to confirm whether the public IP is blacklisted as spam sender. The IP address was indeed found on several blacklists, which explains why other mail servers refuse to accept email from the site. This indicates the presence of a compromised machine – most likely a spambot - that is sending large amounts of spam.

## 6.2 Incident Handling Process – Containment Phase

The goal of this phase is to quickly stop any more damage from occurring. The first action taken was blocking outgoing SMTP traffic *(TCP/25)* from all internal machines except for the mail server. This prevented any internal compromised machine from being able to continue sending spam. Although this corrective measure was taken and no more spam could be sent, the damage had already been done in previous days and the site's public IP address had already been blacklisted.

## 6.3 Incident Handling Process – Eradication Phase

The eradication phase is probably the most difficult phase of the incident handling process (Skoudis 2007). The main goals of this phase are to remove the attacker's artifacts, as well as determine the cause & symptoms of the incident. The symptom *(inability to send mail)* is already known, the incident cause in this case is also known *(internal machines sending spam)*. The main target of this phase is to identify the compromised machine**(s)** and remove the malware. In order to detect most of these compromised machines network wide, the NGFW was setup to log all policy violating traffic, which now includes any attempt from internal machines to connect to an external mail server through **TCP/25** port. Following this firewall change, the logs were then inspected for detection of the policy violating machines. These machines have bots installed which are attempting to send spam. In addition to spam sending, the machines could also be attempting to attack other machines, spread malicious software, or perform other unwanted activities.

The initial source of the infection was found to be an infected flash drive a user had used, which the host antivirus was not able to detect. The firewall logs indicated 12 infected hosts that were attempting to send spam. The machines were to be disconnected from the network, formatted and have their operating system reinstalled. This is to ensure that the malicious software has been removed from these compromised machines. The eradication phase will not be completed quickly, therefore the recovery phase started right after the containment phase.

## 6.4 Incident Handling Process – Recovery Phase

The objective of the recovery phase is to safely return all attack-related systems in the site back into production. There were several actions taken to recover the mail delivery service.

**Action 1:**

A public IP address was dedicated for the mail server that is different than the public IP address that was blacklisted. This

allowed mail traffic sent from the site to use a public IP as a source address that was not blacklisted. The two diagrams below compare a black listed IP address for sending spam, versus a non-blacklisted IP address as captured from MXToolbox.

*Blacklisted IP Address*

| Blacklist Name | Status | Reason | TTL | Response Time (ms) |
|---|---|---|---|---|
| AHBL | OK | | 172 | 47 |
| BGISOCBL | OK | | 172 | 172 |
| CASA-CBL | OK | | 172 | 94 |
| CASA-CBL+ | OK | | 172 | 78 |
| CASA-CDL | OK | | 172 | 78 |
| CBL | OK | | 0 | 78 |
| CLUECENTRAL | OK | | 0 | 172 |
| CYBERLOGIC | OK | | 0 | 156 |
| DEADBEEF | OK | | 0 | 156 |
| DNSBLINFO | OK | | 0 | 156 |

*Non-Blacklisted IP Address*

| Blacklist Name | Status | Reason | TTL | Response Time (ms) |
|---|---|---|---|---|
| AHBL | OK | | 0 | 47 |
| BGISOCBL | OK | | 0 | 172 |
| CASA-CBL | OK | | 0 | 94 |
| CASA-CBL+ | OK | | 0 | 78 |
| CASA-CDL | OK | | 0 | 78 |
| CBL | OK | | 0 | 78 |
| CLUECENTRAL | OK | | 0 | 172 |
| CYBERLOGIC | OK | | 0 | 156 |
| DEADBEEF | OK | | 0 | 156 |
| DNSBLINFO | OK | | 0 | 156 |

In Fortinet NGFW, the feature by which we can enforce specific traffic to originate from an IP address different than the physical network interface is called **IP Pools**. By creating a new IP pool containing an unused public IP address for the site, and attaching that IP pool to a new firewall rule matching outgoing mail server traffic, it becomes possible to use a non-blacklisted IP address for email sending. Since SMTP sessions originating from the site no longer use a blacklisted IP address when sending email, remote mail

servers started accepting emails from the site once more. The procedure below explains how to configure an IP pool.

***How to Configure IP Pool for Mail Traffic***
*1. Go to **Firewall > Virtual IP > IP** Pool and select Create New.*
*2. Enter Mail_Server_Address in the name field.*
*3. From the interface drop down, select external.*
*4. In the IP Range/Subnet field, enter the unused public IP for site.*
*5. Select OK.*
*The IP pool named Mail_Server_Address will now be available for selection in*
*any policy (firewall rule) where the destination interface is set to external, NAT is enabled, and*
*Dynamic IP Pool is enabled.*

**Action 2:**

Some of the blacklists allow removal of the public IP address from the blacklist. It is important that this be done after containment only since the public IP address can be blacklisted again if malicious activity is detected from the IP address. After a few removals without proper containment, the blacklist will prevent the removal of the public IP.

## 6.5 Incident Handling Process – Lessons Learned Phase

The goal of the lessons learned phase is process improvement and documenting what happened for future reference. The duration from identification to recovery was **only one hour**. This demonstrates the importance of following a known incident handling process when an incident takes place, in addition to being acquainted with technical security controls present on site. The persons at the site learned a few lessons from this incident and they are summarized below.

- The importance of having a network audit trail for both allowed and denied traffic was clear; the first made spotting network anomalies possible, while the second helped identify network-wide infected hosts.
- The site outgoing firewall policy needed improvement since it was too relaxed, which allowed internally compromised hosts to send spam.

- Security controls were needed to mitigate the removable media threat vector.
- The site's network traffic on the Internet should not be using one public IP address. One approach could be to group network traffic according to importance or type, and have each group use a dedicated public IP address. This would prevent malicious activity from one group type from affecting other more important traffic in other group types.

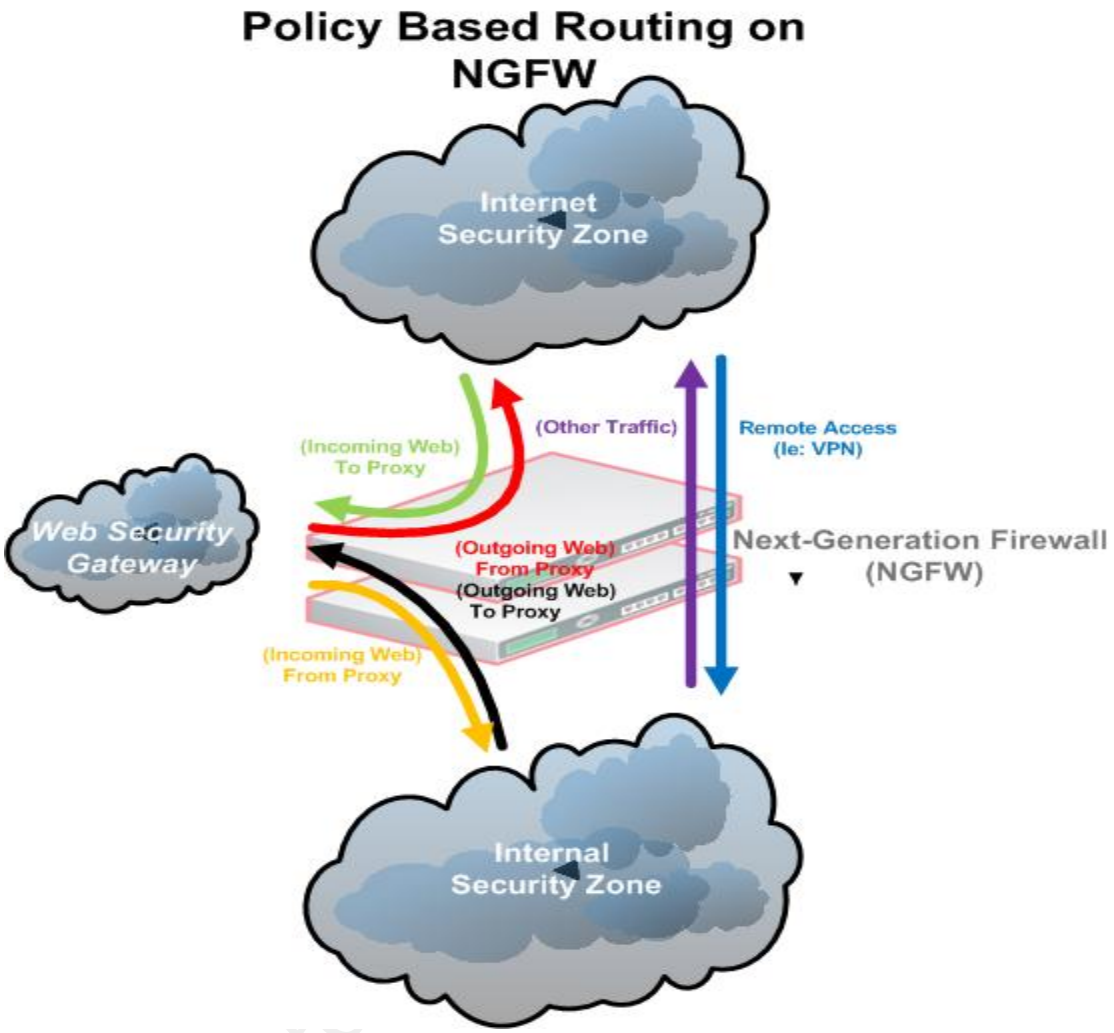
Finally the incident handling process is not complete without the preparation phase. Since I was only a site visitor, I had little preparation to do. However, the site made use of the lessons learned to be better prepared for the next security incident.

## 7. Useful Tips & Techniques – Applied to NGFW Technology

This section addresses some useful tips and techniques applied to NGFWs. When specific examples are given, they will be focused on Fortinet technology.

### 7.1 Policy-based Routing for Web Traffic Inspection & Caching

Policy-based routing provides the freedom to route packets based on the organization's needs, instead of routing packets based solely on their destination IP address and the local routing table. There are many benefits to policy-based routing; however this subsection addresses using policy-based routing to implement a transparent web proxy. The main benefit of this technique is leveraging a separate web security gateway appliance in a ***transparent*** manner; the policy-based routing is configured to redirect HTTP, HTTPS and FTP traffic to the web security gateway, which listens for the traffic and acts as a **transparent/implicit** proxy. This would allow use of additional specialized network and security services not commonly present in NGFWs, such as web caching and HTTPS traffic inspection. The figure below illustrates policy-based routing taking place on a NGFW.




Detailed configuration for the NGFW to perform policy-based routing can be found on the Fortinet Knowledge Center (Fortinet, 2005).

## 7.2 Firewall Considerations & Firewall Policy Violations

Logging firewall policy violations was covered previously in subsection 5.3.2.3. It is included here to emphasize its importance in intrusion detection, especially outgoing firewall policy violations. For easier firewall audits, better performance, and proper firewall policy implementation, a few actions are suggested:

- Adding proper firewall rules for traffic flows enforced by policy-based routing, which are different than normal traffic flows and are often forgotten.
- Using unique public IP addresses based on traffic importance or type when NATing, to allow traffic source identification on the Internet. Issues resulting from ignoring this action are similar to the accountability issues faced when a shared user account *(or public IP)* is used on a computer *(or Internet)*.
- Minimizing the number of firewall rules for easier firewall auditing.
- Ordering firewall rules to match specific cases before generic ones.
- Ordering firewall rules to match more frequent cases before less frequent ones.

## 7.3 Providing Granular Remote Access Privileges

NGFWs commonly provide remote access functionality through a virtual private network (VPN) such as IPSEC or SSL. Both IPSEC and SSL VPNs provide privacy through encryption, however the SSL VPN adds a level of security that is difficult to obtain with traditional network level VPNs such as IPSEC (Mircrosoft, 2005). The Fortinet NGFW provides two SSL VPN modes that allow granular remote access privileges:

- **An agent-less** reverse web proxy for web enabled applications
- **An agent-based** network extension using a browser plugin such as: ActiveX control for Internet Explorer or Java Applet for Firfox

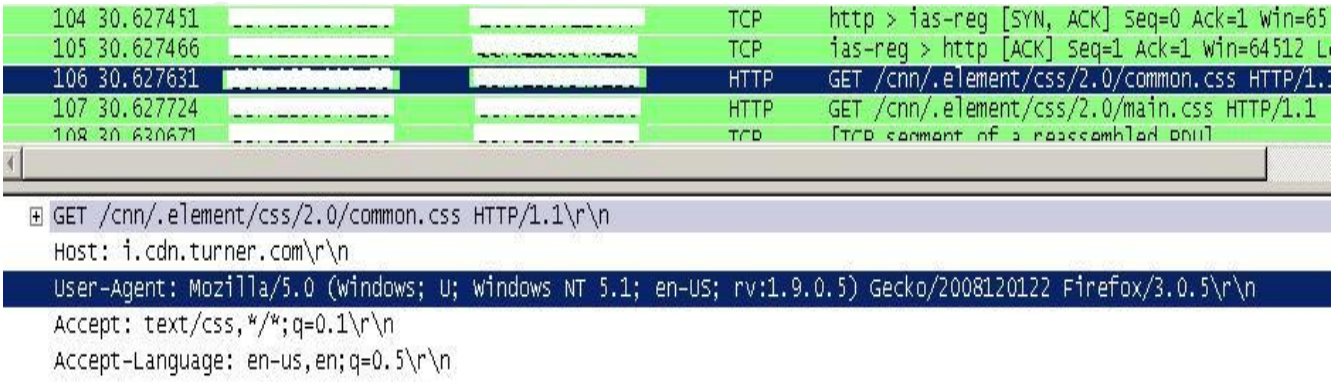
SSL VPN would be a good choice to use for remote access to provide granular remote access privileges to remote users, from any thin client computer connecting from a restricted network, which may be blocking IPSEC protocols. The FortiGate SSL VPN User Guide can be used to configure SSL VPN (Fortinet, 2008). Some web applications

require multiport communication sessions with the client to function. In this case, the agent-based network extension mode is necessary for the web application to function. It essentially creates a SSL tunnel through which the multiport communication traffic flows.

## 7.4 Applying Application Use Enforcement

An Intrusion Prevention System (**IPS**) normally implements a negative security model. Meaning what is not expressly prohibited is permitted. In a NGFW, application use enforcement is possible using the firewall's integrated IPS features but implemented in a positive security manner. To further explain, instead of configuring a "what is prohibited" signature, a "what is allowed" signature is configured, and the inverse of that signature is used in the IPS rule. The resulting IPS rule will then block whatever is not allowed, and what is allowed is specified in the signature, effectively creating a positive security model.

As an applied example, we will use a Fortinet NGFW to enforce web browsing using only a specific version of the Firfox web browser running on Windows. This is achieved by blocking any **HTTP Get request** that does not have the proper **User-Agent** field. The User-Agent field of an HTTP Get Request is populated differently by each web browser. We will create an IPS rule that matches and blocks any HTTP Get request except for our specified HTTP Get request, which happens to include the rightly populated User-Agent field. The figure below is a packet capture showing the User-Agent field of the allowed Firefox application.



A custom IPS signature with the name of *NotFirefoxBrowswerOnWindows* is then created as follows: (the "!" is critical in this signature)

```
config ips custom
edit NotFirefoxBrowserOnWindows
set signature 'F-SBID(--service HTTP; --default_action DROP; --flow
established; --pattern "GET"; --context header; --pattern !"User-
Agent: Mozilla/5.0 (Windows: U: Windows NT 5.1: en-us: rv:1.9.0.5)
Gecko/2008120123 Firefox/3.0.5\r\n"; --context header; )'
end
```

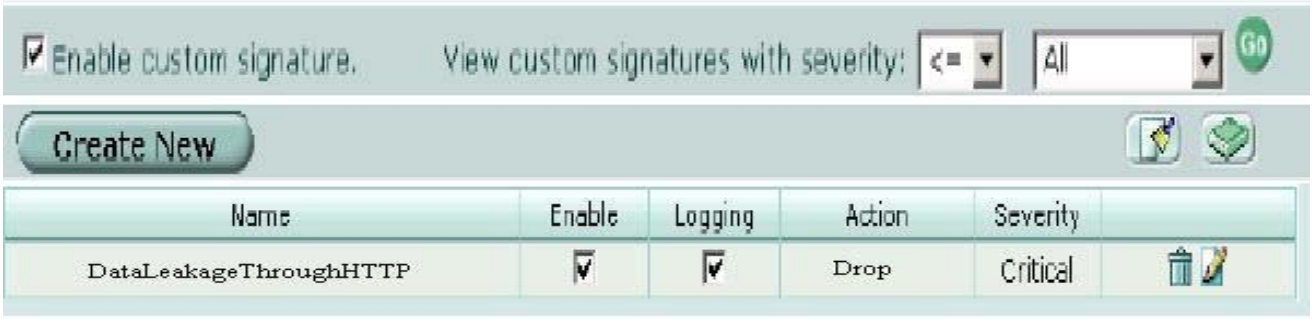
The custom IPS rule is then specified in an IPS sensor, which is attached to a Protection Profile, which is then attached to the firewall rule that allows outgoing HTTP traffic. This enforces web browsing using only a specific version of the Firefox browser running on Windows; it will prevent other web browsers from successfully browsing the web and block bot communication using HTTP Get requests. By using the same methodology, other application use enforcements can be configured to control unauthorized application use on the network.

## 7.5 Applying Basic Data Leakage Prevention (DLP) Controls

Basic data leakage prevention controls (DLP) can be configured on the NGFW. On a Fortinet NGFW, FTP uploads can be denied altogether or restricted based on the user by using the **FTP_PUT** service in a firewall rule. This would still allow FTP downloads but controls FTP uploads. By using a specially defined watermark in documents such as "Organization Confidential", the deep packet inspection engine can be configured to drop & log any connection with the watermark included in the network traffic. This would control events such as outgoing emails (SMTP) with confidential attachments, web-based emails with confidential data being uploaded as an attachment, as well as other data leakage scenarios. For this to be effective, the traffic needs to be unencrypted and the watermark needs to be uncommon to reduce false positives. Rather than using "**Organization Confidential**" as the watermark, "Organization **Confidential x!kltsrodm*(&!sldrk4#dk-+**" can be used. An example custom IPS signature to use for controlling data leakage through the HTTP protocol is:

```
config ips custom
edit DataLeakageThroughHTTP
set signature 'F-SBID(--dst_port 80; --flow bi-direction; --
default_action DROP; --protocol tcp; --pattern "Organization
Confidential X!kltsrodm*(&!sldrk4#dk-+"; )'
end
```

The signature can be put into effect using the same method described in subsection 7.4 Applying Application Use Enforcement. To enable logging and to edit the custom signature, go to **Intrusion Protection > Signature > Custom** on the web-based management interface, which display the following:




## 7.6 High Availability Clustering Considerations

The next-generation firewall placed at the network perimeter is a key security control. Therefore, two next-generation firewalls are often setup as a high availability cluster to prevent it from becoming a single point of failure on the network. In Fortinet technology, the cluster can work in either active-active or active-passive modes. Based on my experience, two issues are worth noting to save others time and effort when working with an active-active high-availability Fortigate cluster:

- When managing the cluster, the two units act as one virtual unit with one single configuration. It is easy to forget *(when troubleshooting complex problems using the built-in sniffer)* that the command-line session is for one box only. Although the packets traverse both boxes in an active-active setup, the built-in sniffer used in a command-line session will capture packets on only one of the boxes; this is the box the sniffer command is executed on.

- Policy-based routing used in an active-active cluster gave strange results. Policy-based routed packets directed to a web proxy led to corrupted HTML pages, which often made the web proxy crash. Policy-based routing using an active-passive cluster worked fine and was stable in the same environment.

## 8. Conclusion

Next-generation firewalls (NGFW), like almost any type of technology, are as useful as you make them. The more knowledge and effort put into understanding and deploying NGFWs, the more effective they are in mitigating risk and enforcing security policy. The information in this paper has demonstrated how NGFWs can be used in intrusion detection, analysis and response. Specifically, the paper demonstrated how NGFWs use deep packet inspection to manage application and data driven threats, the pros and cons of NGFWs, how they can be used to control bot threats, how they can be leveraged in incident handling, and finally useful tips and techniques were demonstrated to make even better use of NGFW technology. All this should help in making optimum use of Fortinet NGFWs, in addition to enabling the use of other vendors' NGFWs.

In the end, NGFWs are only one of many security technologies forming a subset of an organization's **ISMS** (Information Security Management System). Technology, people and process should all work together to create a mature security posture for an organization. It will be interesting to see how next-generation firewalls will evolve, and what type of security services they will become capable of in the future.

## 9. Glossary & Abbreviations

**ActiveX:** ActiveX is Microsoft technology used for developing reusable object oriented software components. (Wikipedia, 2007)

**Antivirus (AV):** Is software used to detect and eliminate malicious software.

**Demilitarized Zone (DMZ):** A network area (a subnetwork) that sits between an organization's internal network and an external network, usually the Internet.

**HTML (Hyper Text Markup Language):** Is the predominant markup language for web pages, it provides a means to describe the structure of text based information in a document supplementing it with embedded images and other objects, it can also embed scripting language code affecting the behavior of web browsers.

**HTTP (Hyper Text Transfer Protocol):** Is a communications protocol used to transfer information *(very often HTML)* on the Internet or Intranet between a client making an HTTP request, and a server providing an HTTP response. HTTP is a protocol that resides in the application layer of both the ISO and TCP/IP network models; it commonly relies on the TCP protocol as the transport layer protocol.

**IDS (Intrusion Detection System):** Software employed to monitor and detect possible attacks and behaviors that vary from the normal and expected activity. The IDS can be network based, which monitors network traffic, or host based, which monitors activities of a specific system and protects system files and control mechanisms. (Harris, 2005)

**IPS (Intrusion Prevention System):** Is a preventative and proactive technology that not only detects a malicious activity as an IDS does, but prevents the activity as well.

**IP (Internet Protocol):** The protocol that specifies the format of packets and the addressing scheme. Most networks combine IP with a higher-level protocol called Transmission Control Protocol (TCP),

which establishes a virtual connection between a destination and a source.

**IPSEC (IP Secure):** A set of protocols that support secure exchange of packets at the IP layer. The sending and receiving devices must share a secret key. IPSEC supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion of each packet; Tunnel mode encrypts both the header and the data.

**NAT (Network Address Translation):** The process of modifying network address information in datagram packet headers while in transit across a traffic routing device for the purpose of remapping a given address space into another. (Wikipedia, 2009)

**Post Office Protocol (POP):** An application layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection.

**SMTP (Simple Mail Transfer Protocol):** A communication protocol that sends e-mail messages from one server to another. The messages can then be retrieved from a server with generally either POP or Internet Message Access Protocol (IMAP).

**SSL (Secure Socket Layer):** A protocol developed by Netscape to transmit data in encrypted form, using a public/private key pair.

**TCP (Transmission Control Protocol):** A set of rules used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data called packets that a message is divided into for efficient routing through the Internet.

**Tunnel:** An encrypted connection that securely carries traffic across a public network.

**UDP (User Datagram Protocol):** A communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is

an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP.

**Virtual Private Network (VPN):** A way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network.

## 10. References

[1] Harris, Shon (2005). *CISSP All-in-One Exam Guide, Third Edition (All-in-One)*.McGraw-Hill Osborne Media.

[2] Firewall. (2008, December 28). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved January 3, 2009, from http://en.wikipedia.org/wiki/Firewall_(networking)

[3] Dubrawsky, Ido (2003, July, 29). Firewall Evolution - Deep Packet Inspection. *SecurityFocus*, Retrieved January 3, 2009, from http://www.securityfocus.com/infocus/1716

[4] Ranum, M. What is "Deep Inspection"?. Retrieved January 3, 2009, from Editorials Web site: http://www.ranum.com/security/computer_security/editorials/deepinspect/

[5] Cisco Systems, (2002). Evolution of the Firewall Industry. Retrieved January 3,2009, from Cisco Documentation Web site: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch3.htm

[6] Young, Greg (2008, September 22). Next-Generation Firewalls. *Hype Cycle for Infrastructure Protection, 2008*, G00161383, 26. Retrieved January 7, 2009, from Gartner.

[7] Fortinet. (2006). *Multi-Layer Security Platforms - The New Definition for Best of Breed* [Whitepaper]. Sunnyvale, CA: Mark Bouchard, Freddy Mangum.

[8] Higgins, K. (2007, November 28). Firewalls Ready for Evolutionary Shift. Retrieved January 7, 2009, from Dark Reading Web site: http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208804838

[9] Palo Alto Networks, (2008). Firewall Feature Overview. Retrieved January 7, 2009, from Palo Alto Networks Web site: http://www.paloaltonetworks.com/literature/datasheets/PAN_OS_Feature_ds.pdf

[10] Young, Pescatore, Greg, John (2008, November 21). Next-Generation Firewalls. *Magic Quadrant for Enterprise Network Firewalls, 2008*, G00162592, Inclusive -- 4-5. Retrieved January 7, 2009, from Gartner.

[11] Lucas, Rothschild, S.,M. (2008, September 30). [Podcast] Anti-X and the Mob: Addressing Content-Borne Threats with Unified Threat Management. *Information Security Research Library. Retrieved December 31, 2008, from* *http://searchsecurity.bitpipe.com/detail/RES/1222108104_896.html?src=pc_ssec_dayof_11_06_08&li=151301&asrc=EM_DWPC_4953517&uid=1078573*

[12] McAfee. (2008). *McAfee Virtual Criminology Report – Cybercrime Versus Cyberlaw* [Report]. Santa Clara, CA

[13] Cisco. (2008). *Cisco 2008 Annual Security Report* [Report]. San Jose, CA

[14] Falinski, Minassian, Stefan, Neshan (2008, September). *UK Cybercrime Report 2008, 2008*, Retrieved January 8, 2009, from garlik.

[15] Baker, Hylender, Valentine, W., C., J. (2008). 2008 Data Breach Investigations Report. *Study Conducted by Verizon Business RISK Team*, Inclusive -- 23-24. Retrieved January 8, 2009, from Verizon Business.

[16] GreenGard, S. (2008, Autumn). Battling Botnets. *InfoSecurity Professional – An (ISC)2 Digital Publication, Autumn*, Retrieved December, 2008.

[17] Skoudis, E. (2007, July, 24). Q&A - What are the Risks of Logging into a Botnet Control Channel?. *Information Security Threats Questions & Answers*, Retrieved January, 2009, from http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1274217,00.html

[18] Skoudis, E. (2007, June, 22). Q&A – Is it Possible to Detect Today's Peer-to-Peer (P2P Botnets?. *Information Security Threats Questions & Answers*, Retrieved January, 2009, from http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1265784,00.html

[19] Fortinet, (2007, October 22). Blocking Storm Worm by Blocking eDonkey. Retrieved January 10, 2009, from Fortinet Knowledge Center Web site: http://kc.forticare.com/default.asp?id=3537&Lang=1&SID=

[20] Kamluk, V. (2008, May 13). The Botnet Business. Retrieved January 16, 2009, from VirusList.com Web site: http://www.viruslist.com/en/analysis?pubid=204792003#l2

[21] Fortinet, (2009, January 12). FortiGate Administration Guide. *Technical Documentation*, Version 3.0 MR7, 365. Retrieved January 16, 2009, from FortiCare.

[22] IPA, (2007, September 25). Countermeasures Against Bots. Retrieved January 17, 2009, from IPA CounterMeasure Guide Series Web site: http://www.ipa.go.jp/security/english/virus/antivirus/pdf/Bot_measures_eng.pdf

[23] Shadowserver Foundation, (2007, November 12). Botnet Detection. Retrieved January 17, 2009, from Shadowserver Knowledge Base Web site: http://www.shadowserver.org/wiki/pmwiki.php?n=Information.BotnetDetection

[24] Dagon, D. (2005). Botnet Detection and Response - The Network is the Infection. Retrieved January 17, 2009, from CAIDA: The Cooperative Association for Internet Data Analysis Web site: http://www.caida.org/workshops/dns-oarc/200507/slides/oarc0507-Dagon.pdf

[25] Fast Flux. (2008, October 6). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved January 16, 2009, from http://en.wikipedia.org/wiki/Fast_flux

[26] ICANN SSAC, (2008, October 23). Fast Flux Hosting and DNS. Retrieved January 17, 2009, from SSAC Presentation on Fast Flux Hosting Web site: http://www.docstoc.com/docs/2032178/SSAC-Presentation-on-Fast-Flux-Hosting

[27] Skoudis, Ed (2007). Incident Handling Step-by-Step and Computer Crime Investigation. *Hacker Techniques, Exploits & Incident Handling* SANS.

[28] Fortinet, (2005, July 17). Policy Based Routing Example. Retrieved January 10, 2009, from Fortinet Knowledge Center Web site:

http://kc.forticare.com/default.asp?id=781&Lang=1&SID=

[29] Microsoft, (2005, April 13). How ISA Server 2004 Provides SSL VPN Functionality for Outlook Web Access and RPC over HTTP. Retrieved January 24, 2009, from Microsoft Technet Web site: http://technet.microsoft.com/en-us/library/cc512659.aspx

[30] Fortinet, (2008, April 4). SSL VPN User Guide. *Technical Documentation*, Version 3.0 MR6, 19. Retrieved January 16, 2009, from FortiCare.

[31] Network Address Translation. (2009, January 22). In *Wikipedia* [Web]. Wikimedia Foundation. Retrieved January 28, 2009, from http://en.wikipeida.org/wiki/network_address_translation

[32] Fortinet, (2008, April 22). IPS User Guide. *Technical Documentation*, Version 3.0 MR6. Retrieved January 16, 2009, from FortiCare.

[33] SonicWALL. (2008). *10 Cool Things Your Firewall Should Do* [Whitepaper].

Last Updated: January 22nd, 2020

# Upcoming SANS Training

**Click here to view a list of all SANS Courses**

| | | | |
|---|---|---|---|
| SANS Las Vegas 2020 | Las Vegas, NVUS | Jan 27, 2020 - Feb 01, 2020 | Live Event |
| SANS Vienna January 2020 | Vienna, AT | Jan 27, 2020 - Feb 01, 2020 | Live Event |
| SANS Security East 2020 | New Orleans, LAUS | Feb 01, 2020 - Feb 08, 2020 | Live Event |
| SANS New York City Winter 2020 | New York City, NYUS | Feb 10, 2020 - Feb 15, 2020 | Live Event |
| SANS Northern VA - Fairfax 2020 | Fairfax, VAUS | Feb 10, 2020 - Feb 15, 2020 | Live Event |
| SANS London February 2020 | London, GB | Feb 10, 2020 - Feb 15, 2020 | Live Event |
| SANS Dubai February 2020 | Dubai, AE | Feb 15, 2020 - Feb 20, 2020 | Live Event |
| SANS Cairo February 2020 | Cairo, EG | Feb 15, 2020 - Feb 20, 2020 | Live Event |
| SANS San Diego 2020 | San Diego, CAUS | Feb 17, 2020 - Feb 22, 2020 | Live Event |
| SANS Scottsdale 2020 | Scottsdale, AZUS | Feb 17, 2020 - Feb 22, 2020 | Live Event |
| SANS Brussels February 2020 | Brussels, BE | Feb 17, 2020 - Feb 22, 2020 | Live Event |
| Open-Source Intelligence Summit & Training 2020 | Alexandria, VAUS | Feb 18, 2020 - Feb 24, 2020 | Live Event |
| SANS Training at RSA Conference 2020 | San Francisco, CAUS | Feb 23, 2020 - Feb 24, 2020 | Live Event |
| SANS Jacksonville 2020 | Jacksonville, FLUS | Feb 24, 2020 - Feb 29, 2020 | Live Event |
| SANS Secure India 2020 | Bangalore, IN | Feb 24, 2020 - Feb 29, 2020 | Live Event |
| SANS Manchester February 2020 | Manchester, GB | Feb 24, 2020 - Feb 29, 2020 | Live Event |
| SANS Zurich February 2020 | Zurich, CH | Feb 24, 2020 - Feb 29, 2020 | Live Event |
| SANS Northern VA - Reston Spring 2020 | Reston, VAUS | Mar 02, 2020 - Mar 07, 2020 | Live Event |
| SANS Munich March 2020 | Munich, DE | Mar 02, 2020 - Mar 07, 2020 | Live Event |
| SANS Secure Japan 2020 | Tokyo, JP | Mar 02, 2020 - Mar 14, 2020 | Live Event |
| ICS Security Summit & Training 2020 | Orlando, FLUS | Mar 02, 2020 - Mar 09, 2020 | Live Event |
| Blue Team Summit & Training 2020 | Louisville, KYUS | Mar 02, 2020 - Mar 09, 2020 | Live Event |
| SANS Jeddah March 2020 | Jeddah, SA | Mar 07, 2020 - Mar 12, 2020 | Live Event |
| SANS St. Louis 2020 | St. Louis, MOUS | Mar 08, 2020 - Mar 13, 2020 | Live Event |
| SANS Dallas 2020 | Dallas, TXUS | Mar 09, 2020 - Mar 14, 2020 | Live Event |
| SANS Paris March 2020 | Paris, FR | Mar 09, 2020 - Mar 14, 2020 | Live Event |
| SANS Prague March 2020 | Prague, CZ | Mar 09, 2020 - Mar 14, 2020 | Live Event |
| Wild West Hackin Fest 2020 | San Diego, CAUS | Mar 10, 2020 - Mar 11, 2020 | Live Event |
| SANS Doha March 2020 | Doha, QA | Mar 14, 2020 - Mar 19, 2020 | Live Event |
| SANS Secure Singapore 2020 | Singapore, SG | Mar 16, 2020 - Mar 28, 2020 | Live Event |
| SANS Norfolk 2020 | Norfolk, VAUS | Mar 16, 2020 - Mar 21, 2020 | Live Event |
| SANS SEC401 Lille March 2020 (in French) | Lille, FR | Mar 16, 2020 - Mar 21, 2020 | Live Event |
| SANS San Francisco East Bay 2020 | OnlineCAUS | Jan 27, 2020 - Feb 01, 2020 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |