McAfee Botnet Protection:
Correlation, Context and Intelligence

REV: 0.1.3 - (July 2011)
Contents

1. Overview ....................................................................................................................................... 4
  1.1 The Problem .................................................................................................................................. 4
  1.2 The Solution .................................................................................................................................. 4

2. Viruses, Spam, Malware, What’s Next? Botnets! ........................................................................ 5
  2.1 What is a Botnet? .......................................................................................................................... 5
  2.2 Anatomy of a Botnet ..................................................................................................................... 5
  2.3 Botnet Size .................................................................................................................................... 6
  2.4 Protecting Your Computer from a Botnet ..................................................................................... 6
  2.5 How Do Botnets Work? ................................................................................................................. 6

3. McAfee Network Security Platform ................................................................................................ 7

4. McAfee Host Intrusion Prevention for Server ................................................................................ 8

5. Security with Three Layers of Protection ..................................................................................... 9
  5.1 Securing the Mission-Critical Network ......................................................................................... 9
    Network IPS ......................................................................................................................................... 9
  5.2 Network Threat Behavior Analysis ................................................................................................ 9
    Network Behavioral Analysis ............................................................................................................. 9
  5.3 Dynamic Stateful Firewall with Global Reputation Technology .................................................. 10
    Firewall ............................................................................................................................................... 10

6. Context Aware Network Security .................................................................................................. 12
  6.1 Workload-Aware Intrusion Detection ........................................................................................... 12
  6.2 Network-aware Honeynet configuration ......................................................................................... 12
  6.3 Context-Aware Blacklist Generation ............................................................................................. 12
    Two Techniques of Context-Aware Models .................................................................................... 12

7. Next-Generation Intrusion Prevention System (NGIPS) ............................................................... 14
  7.1 Automate Security with Contextual Awareness ............................................................................ 14
  7.2 IPS and NGIPS Hardware and Technology .................................................................................. 14
    How the NGIPS Uses Contextual Awareness to Fuel Intelligent Automation ................................ 14
  7.3 Contextually Aware Engine .......................................................................................................... 15

8. McAfee Global Threat Intelligence Technology ............................................................................ 16
  8.1 McAfee’s Six Principles that make Global Threat Intelligence Effective ....................................... 17
  8.2 McAfee GTI Cloud-Based Services ............................................................................................. 17
9. McAfee Web Gateway - Providing Increased Protection against Malware and Botnets .......... 18
9.1 McAfee’s Web Gateway Offers the Following Capabilities ............................................. 18
10. Network Intrusion Prevention .................................................................................. 19
10.1 McAfee Network Security Manager ........................................................................ 19
10.2 McAfee Network Security Platform ....................................................................... 19
10.3 McAfee Network Threat Response ........................................................................ 19
11. Keywords .................................................................................................................. 20
1. **OVERVIEW**

1.1 **The Problem**

The Internet has drastically improved personal and business communications and has made available an ever increasing range of possible online activities (including online banking, filing taxes, selling products or performing other routine financial transactions).

Most, if not all, of these activities mandate that you divulge some amount of personal information, which is then processed by the host and permanently written to a database system somewhere.

And as the Internet becomes more and more accessible everywhere we go these days, the software we use to interact with it becomes increasingly obsolete and unwieldy and rife with vulnerabilities that can be used to exploit and outright steal your company’s critical information.

1.2 **The Solution**

To combat tomorrow’s threats, McAfee develops a number of network-based security solutions to defend your critical systems, hosted apps, database servers, client desktops, and more.

You will be able to view file system processes and network access on networked machines at a precise and granular level.

Backed by McAfee’s 24/7 Global Threat Intelligence and integrated into a single management platform, McAfee’s solutions deliver a strong yet streamlined package.
2. **VIRUSES, SPAM, MALWARE, WHAT’S NEXT? BOTNETS!**

Today’s threats are more sophisticated than ever, and they are growing at an unprecedented rate. Both malicious Websites and malware have increased nearly six-fold in the last two years, and 2010 alone saw more new malware than all prior years combined. With the increased threat of criminals mining for consumer and corporate data, the efficiency of your security must be a priority.

### 2.1 What is a Botnet?

A Botnet, or robot network of infected computers, commonly called a “Botnet,” is a distributed group of computers that have been infected by some type of malware (virus, Trojan horse or worm) under the control of the botnets’ originator or creator (called the “Botmaster” or “Herder.” When the infected software is installed on a local computer, one or more hidden programs are also installed which use particular ports to provide a back door which allows a remote attacker to gain control of the compromised system.

Because infected systems are secretly controlled without their owners’ knowledge, individual computers within a botnet are sometimes called drones or “Zombies.”

### 2.2 Anatomy of a Botnet

Remotely controlled Botnet computers are typically used to perform malicious and/or illegitimate activities such as:

- Launching large-scale distributed denial-of-service (DoS) attacks
- Sending spam and phishing emails
- Proliferating Trojans and infecting other computers with viruses.
- Distributing pirated media
- Stealing personal information.
2.3 Botnet Size

To support their criminal activities, cyber criminals take control of (or “Herd”) Zombie drones in astonishingly large numbers. And due to their sheer numbers, Botnets are often hard to defeat.

The largest botnets in history have been estimated to consist of as many as 30 million machines. Below are some of the largest Botnets ever unleashed.

<table>
<thead>
<tr>
<th>Botnet Name</th>
<th>Number of Infected Machines</th>
</tr>
</thead>
<tbody>
<tr>
<td>TDL-4</td>
<td>4.5 Million</td>
</tr>
<tr>
<td>Conficker</td>
<td>10.5 Million</td>
</tr>
<tr>
<td>Mariposa</td>
<td>12 Million</td>
</tr>
<tr>
<td>BredoLab</td>
<td>30 million</td>
</tr>
</tbody>
</table>

NOTE: At its peak, the BredoLab botnet was capable of sending 3.6 billion spam emails every day. The masterminds sent billions of fake Facebook password-reset emails in an attempt to trick PC users into downloading and opening an attached dangerous piece of malware. A large number of the zombies a large-scale spam attack that uses fake Facebook password-reset messages to trick PC users into

2.4 Protecting Your Computer from a Botnet

It is important to have active security software scan all downloads and incoming files. Astonishingly, most people who get a botnet virus, do so by downloading and installing (and thereby executing) a botnet virus-ridden piece of software. The culprit piece of code was likely “smuggled” into your system by means of a larger Trojan horse piece of software used to package and deliver the infection. You can unwittingly infect your computer and perhaps many thousands more.

The Infection Spreads

Some victims will be oblivious to the initial infection. Others may sense something’s wrong, but won’t be able to recall what they did (or tried to install) that landed them with the virus. All will hopefully soon realize that their systems have been hijacked by the perpetrator of a botnet.

2.5 How Do Botnets Work?

Individual Botnet Zombies run a series of scripts, commands and/or programs that are designed to secretly establish a connection to a remote server or servers. Even when an infected machine is rebooted, the harmful code is re-executed upon startup and the series of commands is run.
3. **McAfee Network Security Platform**

The *McAfee Network Security Platform* includes enhanced botnet control through reputation intelligence, virtual network inspection and a traffic analysis port for network monitoring, forensics and other advanced analysis engines. McAfee surpasses traditional **Network Intrusion Prevention Systems (NIPS)** by providing a greater level of network intelligence across both physical and virtual environments.

Real-time, reputation-based intelligence supplied through **McAfee Global Threat Intelligence** provides McAfee Network Security Platform users with additional context for enforcing network security policies, not to mention faster, more accurate threat detection.

**McAfee Network Security Platform includes:**

- **Enhanced botnet control:** File and network connection reputation feeds from cloud-based McAfee Global Threat Intelligence allows Network Security Platform to perform in-line botnet prevention based on over 60 million malware samples and the reputation of hundreds of millions of network connections based on over two billion IP reputation queries each month. This external intelligence provides vital context for faster, more accurate detection and prevention.

- **Traffic analysis port:** Traffic redirect capabilities allow arbitrary network traffic to be subjected to additional inspection by McAfee and third party products, including data loss prevention, network forensics and advanced malware analysis tools.

- **Virtual network inspection:** Enables the Network Security Platform sensors to examine inter-virtual machine traffic on virtual environments and provide attack detection for virtual data center environments. Network Security Platform can inspect traffic both within virtual environments and between virtual and physical environments, giving organizations the same level of visibility regardless of where the traffic flows.
4. **McAfee Host Intrusion Prevention for Server**

Your corporate servers house your organization’s most valuable assets and information. They literally must be up and running to keep your business up and running. One of the major IT challenges you face is to successfully protect your servers and their hosted applications from known and unknown attacks that threaten to disrupt your business.

*McAfee Host Intrusion Prevention for Server* delivers specialized web and database server protection to maintain system uptime and business continuity. This technology provides the industry’s only dynamic and stateful firewall to shield against advanced threats and malicious traffic.

In addition, it also provides signature and behavioral intrusion prevention system protection. McAfee Host Intrusion Prevention for Server reduces patching frequency and urgency, preserves business continuity and employee productivity, protects data confidentiality, and simplifies regulatory compliance.

Enforce the broadest IPS and zero-day threat protection coverage across all levels: network, application, and system execution.

*McAfee Host Intrusion Prevention for Desktops* safeguards your business against complex security threats that may otherwise be unintentionally introduced or allowed by desktops and laptops. Host Intrusion Prevention for Desktops is easy to deploy, configure, and manage.
5. Security with Three Layers of Protection

5.1 Securing the Mission-Critical Network

Protecting the Network from the latest malware, unsecured and unprotected devices, unauthorized users—it’s what we do with network access control to intrusion prevention, network behavioral analysis to protection for your web and email gateways.

Network IPS

- Proactive protection for unpatched systems
- Proactive protection for zero day attacks
- System-aware IPS with ePO integration
- Real-time host IPS integration and visibility
- Next-gen 10-Gigabit Ethernet
- Adaptive rate limiting
- Built-in host quarantine

GOAL: Prevent malicious intrusions by the most advanced threats on the Internet, such as botnets, distributed denial-of-service (DDoS) and zero-day attacks. Protect your company and defend your assets against known and emerging exploits.

SOLUTION: Three primary layers are essential to complete protection:

Security in three layers of protection:

1. The first layer examines your network traffic for known botnet signatures (Signature Analysis).
2. The second layer analyzes your network for threats and inspects it for behavior associated with attacks, behavior blocker (Network Threat Behavior Analysis).
3. The third layer implements a thorough, dynamic and stateful desktop firewall to secure servers, desktops and laptops against advanced threats.

5.2 Network Threat Behavior Analysis

Network Behavioral Analysis

- Associate all network traffic with its initiating identity and/or user group.
- Based on this correlation, discover gaps and enable policy controls at the network layer: an identity-aware network.
- Ensure network access and behavior comply with intended usage and policies.

McAfee’s set of threat analysis appliances provide comprehensive inspection of your entire network for threats and associated network behaviors.
Additionally, McAfee is the only vendor to provide Layer-7 flow export. This, when coupled with network flow data, empowers security analysts to ‘turn on the lights’ across the network with visibility into users, data, and applications.

McAfee Network Threat Behavior Analysis maintains a comprehensive and efficient network security infrastructure. A single sensor effectively collects traffic, and analyzes host and application behavior to detect worms, zero-day threats, botnets, and reconnaissance attacks.

Network Threat Behavior Analysis monitors and reports unusual network behavior by analyzing traffic from switches and routers from vendors such as Cisco, Juniper Networks, and Extreme Networks. It comes fully equipped with quad-core processors, a RAID array, distinct flow capacity, gigabit Ethernet connectivity, and offline storage area network connectivity.

Network Threat Behavior Analysis collects and analyzes traffic from the entire network — host and applications — to detect worms, botnets, zero-day threats, spam, and reconnaissance attacks. It reports any unusual behavior to help you maintain a comprehensive and efficient network security infrastructure.

Network Threat Behavior Analysis seamlessly integrates with the McAfee Network Security Platform intrusion prevention system to build a comprehensive and robust security infrastructure.

Integrate Network Threat Behavior Analysis into your existing security infrastructure.

Use Network Threat Behavior Analysis with your current network defenses. Seamlessly integrate Network Threat Behavior Analysis with the McAfee Network Security Platform intrusion prevention system to correlate unusual network behavior caused by intrusions.

5.3 Dynamic Stateful Firewall with Global Reputation Technology

Firewall

- Control inbound and outbound
- Granular app filtering
- Decrypt traffic for inspection
- Transparently authenticate users for outbound access
- Inspect internet usage for malicious content and apps
- Securely control VoIP traffic
- Provide virtualization support

Delivering advanced threat protection through our dynamic, stateful desktop firewall. Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Desktop has integrated McAfee Global Threat Intelligence™ network connection reputation to secure desktops and laptops against advanced threats such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic before attacks can occur. With the increase in advanced threats, McAfee Global Threat Intelligence offers the most sophisticated protection you can deploy.

Additional firewall features, such as application and location policies, further safeguard laptops and desktops especially when they are not on the corporate network.
Get advanced threat protection through our dynamic, stateful system firewall.

Unlike traditional system firewalls that rely on specific rules, McAfee Host Intrusion Prevention for Server has integrated McAfee Global Threat Intelligence—network connection reputation to protect servers against advanced threats such as botnets, distributed denial-of-service (DDoS), and emerging malicious traffic before attacks can occur. With the increase in advanced threats, McAfee Global Threat Intelligence offers the most sophisticated protection you can deploy.
6. **CONTEXT AWARE NETWORK SECURITY**

The rapid growth in malicious Internet activity and the rise of semi-automated threats (like botnets) has driven the development of advanced tools designed to protect host and network resources.

One approach that has obtained significant recognition is the use of network based security systems, where certain system components are strategically deployed across the network and which are tasked to identify, distinguish and alleviate both new and existing threats.

### 6.1 Workload-Aware Intrusion Detection

McAfee’s adaptive Intrusion Detection and Prevention System (IDS/IPS) takes a set of input signatures and network traffic characteristics and identifies intrusions by matching them with network traffic.

Adjusted according to workload, IDS and IPS systems include the set of input signatures and network traffic characteristics.

McAfee’s adaptive algorithm systematically profiles attack signatures and network traffic to generate a high performance and memory-efficient packet inspection strategy.

Two distinct components: a profiler that analyzes the input rules and the observed network traffic to produce a packet inspection strategy, and an evaluation engine that pre-processes rules according to the strategy and evaluates incoming packets to determine the set of applicable signatures.

### 6.2 Network-aware Honeynet configuration

A Honeynet is a collection of sacrificial decoy hosts that are relatively easy for attackers to discover which are specifically deployed to be compromised and used in Botnet attacks. Honeynets have recently become a popular means to detect and characterize malware threats such as worms, viruses and botnets.

Honeynets must represent the security environment of the networks they are trying to protect. Thus, a honeynet configuration should imitate the network in which it is deployed to provide visibility into attacks and resistance to fingerprinting.

### 6.3 Context-Aware Blacklist Generation

Blacklisting allows the IT community to filter or block unwanted traffic from the Internet. Blacklists generated by firewall log files are used to obstruct nefarious hosts and block spam bots.

**Two Techniques of Context-Aware Models**

*Ratio-Based Blacklisting*

In ratio-based blacklisting, traffic on the live network is compared to traffic on the spamtraps to determine if it is safe to blacklist an IP address. We call this approach the ratio-based approach as
the ratio of email messages on the live network to the email messages on the spamtrap is used as a measure to blacklist an IP address.

**Speculative Aggregation**

In the speculative aggregation approach, we use local reachability information as well as application history to predict where new spam messages will come while limiting the chance that these predicted hosts or networks are of use to the local network.

A deployment of context-aware blacklists for over a month in a large academic network demonstrated significant improvement in blacklist accuracy.

The core component of popular IDSs (Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), like Snort [67], is a deep packet inspection engine that checks incoming packets against a database of known signatures (also called rules).
7. **Next-Generation Intrusion Prevention System (NGIPS)**

7.1 **Automate Security with Contextual Awareness**

Today’s networks are highly dynamic, where new technologies cause ever-increasing complications.

As the number and type of applications and systems on your network continues to grow, information security risks also develop rapidly in quantity and extent as attackers become more sophisticated and crafty.

Sourcefire Next-Generation IPS raises the bar for IPS technology by integrating real-time contextual awareness into its inspection. The system gathers information about network and host configurations, applications and operating systems, user identity, and network behavior and traffic baselines. By having the utmost visibility into what’s running on your network, NGIPS offers event impact assessment, automated IPS tuning, and user identification to significantly lower the total cost of ownership.

7.2 **IPS and NGIPS Hardware and Technology**

Sourcefire IPS and NGIPS solutions take advantage of the best hardware technology in the industry, providing IPS inspected throughput options ranging from 20Gbps down to 5Mbps. Upgrading Sourcefire IPS to NGIPS is as easy as adding a license to your software.

The new Sourcefire 3D8000 Series appliances offer interface modularity, expandability, and scalability. Modularity provides a low entry-price and enables you to choose the number of ports and media type for your network and swap out interface types as needed. Expandability gives you the option to pay for network interfaces as you grow. Scalability enables you to add additional processing power through appliance stacking.

**How the NGIPS Uses Contextual Awareness to Fuel Intelligent Automation**

<table>
<thead>
<tr>
<th>Network Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continual network visibility, including new hosts entering the network, network and host configuration changes, and IT policy compliance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify application traffic that is traversing the network to define application policies and management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve audit controls and regulatory compliance by linking events directly to individual users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Behavior Awareness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect and quarantine internal threats by establishing &quot;normal&quot; traffic baselines and detecting network anomalies.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Automated Tuning &amp; Impact Assessment Reduces Costs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically determine threat relevance, threat severity, and self-cure to defend against attacks; increasing security, maximizing throughput, and reducing operational costs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application Policy Management Improves Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control your acceptable use policy (AUP) by automatically identifying the types of applications on your network and recognizing policy violations.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Identity Tracking Speeds Incident Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatically link Active Directory and LDAP users to events so you know exactly who to contact when time is of the essence.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Behavior Analysis Increases Network Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor bandwidth consumption, troubleshoot network performance degradation, and automatically quarantine internal hosts with malware before it spreads.</td>
</tr>
</tbody>
</table>
7.3 Contextually Aware Engine

Sourcefire is moving toward allowing RNA Recommended Rules to operate fully dynamically. Sensor rule sets will be dynamically modified in real time to correspond to the network and host profiles that are seen in a customer’s environment. The contextually aware engine feature will include:

- The RNA-driven automated population/definition of variables (e.g., $HTTP_SERVERS) that control the invocation of various 3D Sensor preprocessors.
- The ability to recommend rules and dynamically adjust 3D Sensor configurations based on data and attributes obtained from external tools (e.g., vulnerability scanners, patch management systems) via the Sourcefire Host Input API.
- Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. With help from the Open Source community, Snort has developed to be the most widely deployed intrusion detection and prevention technology worldwide, becoming the de facto standard for the industry.
8. **McAfee Global Threat Intelligence Technology**

McAfee Global Threat Intelligence (GTI) is a comprehensive cloud-based threat intelligence service. Already integrated into McAfee security products, it works in real time, 24 hours a day, to protect customers against cyberthreats across all vectors — file, web, message, and network. McAfee GTI offers the broadest threat data, most robust data correlation, and most complete product integration in the industry.

McAfee’s GTI network allows enabled products to evaluate threats on multiple vectors in real time, leading to faster identification of threats and higher capture rates. Host Intrusion Prevention for Desktop uses the McAfee GTI file reputation service and network connection reputation service to find suspicious files before they are identified as carrying malicious payloads, as well as domains/IP addresses that are infected or hosting malware attacks, and block those attacks.

**McAfee Global Threat Intelligence** delivers the most comprehensive protection solution on the market. With visibility across all major threat vectors (file, web, email, and network), GTI collects real-world data from millions of sensors across the IT industry and around the globe, determines the latest vulnerabilities and delivers real-time protection via McAfee’s advanced security products.

McAfee Global Threat Intelligence (GTI) is a system that monitors the Web for malicious sites. When a malicious Website is identified by the site’s anomalous behavior:

- GTI adjusts the website’s reputation so McAfee web security products can block access and protect customers.
- GTI looks out across its broad network of sensors and connects the dots between the website and associated malware, email messages, IP addresses, and other associations
- GTI adjusts the reputation of each related entity so McAfee’s security products, from user to gateway to network, can protect users from cyber threats at every angle.
McAfee GTI offers the most comprehensive threat intelligence in the market. With visibility across all threat vectors — file, web, message, and network — and a view into the latest vulnerabilities across the IT industry, McAfee correlates real-world data collected from millions of sensors around the globe and delivers real-time, and often predictive, protection via its security products.

### 8.1 McAfee’s Six Principles that make Global Threat Intelligence Effective

1. Maintain a footprint that spans the Internet, including millions of sensors gathering real-world threat information.
2. Gather and correlate data from and across all threat vectors, including file, web, message, and network.
3. Ensure that data collection and threat intelligence distribution are cloud-based and performed in real time.
5. Integrate threat intelligence into a complete suite of security products.
6. Support the entire process with a global research team dedicated solely to threat intelligence.

McAfee Web Gateway uses a bi-directional hybrid security approach that includes an intent-based anti-malware scanning engine, along with several cloud-based technologies.

### 8.2 McAfee GTI Cloud-Based Services

- McAfee GTI file reputation
- McAfee GTI web reputation
- McAfee GTI web categorization
- McAfee GTI message reputation
- McAfee GTI network connection reputation
9. **McAfee Web Gateway - Providing Increased Protection against Malware and Botnets**

Through integration with McAfee Labs’ cloud-based global threat intelligence, McAfee provides a scalable platform that delivers proactive malware scanning and unmatched protection for enterprises and service providers.

The use of targeted attacks via Web-borne malware is becoming more sophisticated and widespread. A majority of these attacks are used to capture resources for ever-expanding botnets or to steal business information including personal or customer information, records, financial transactions and intellectual property.

McAfee Web Gateway platform enables user access to authorized Web 2.0 applications, while significantly reducing risk by combining local and cloud-based protection. McAfee provides protection at every stage for today’s most prevalent threats to enterprises. Reputation management is an essential element of complete protection.

Integration with real-time technology protects organizations against viruses, provides mobile filtering for remote users and expands Web reputation capabilities. Through Web reputation and Global Threat Intelligence, the platform obstructs access to infected websites, stops malicious content from downloading and thwarts back-channel communication of tainted machines.

McAfee Web Gateway allows flexibility and granular control over security policies. Ultimately, you will notice enhanced performance from fine tuning your existing infrastructure.

9.1 **McAfee’s Web Gateway Offers the Following Capabilities**

- **Advanced Security**: A patent-pending approach to behavior analysis inspects content in real-time to expose embedded code, buffer overflows or exploits. Cloud-based technology delivers mobile filtering for remote users, and expanded Web reputation capabilities including geo-location and URL categorization.

- **Enhanced Performance and Scalability**: Highly scalable and functionally robust, deployment capabilities include VMware support and transparent proxy options for added flexibility and control.

- **Full Content Security**: Grasp increased security and financial savings through the integration of McAfee’s Web and Email Gateways, Network Data Loss Prevention and ePolicy Orchestrator platform. Leverage the benefits of Web 2.0 enabled applications and achieve a significant return on your investment by implementing this integrated security solution.
10. **NETWORK INTRUSION PREVENTION**

McAfee’s *Network Intrusion Prevention* products are designed to keep your business running and secure with industry-leading defense against hackers, malware, and other exploits. With comprehensive coverage and robust protection, configuration is easy via McAfee’s simplified, centralized, web-based management console.

**10.1 McAfee Network Security Manager**

With the McAfee *Network Security Manager* you can configure, deploy, and administer multiple McAfee intrusion prevention system (IPS) and Network Access Control appliances through a single, straightforward management console.

**10.2 McAfee Network Security Platform**

McAfee *Network Security Platform* is the industry’s most secure network IPS. Backed by McAfee Labs, it protects customers on average 80 days ahead of the threat. It blocks attacks in real time, before they can cause damage, and protects every network-connected device. With Network Security Platform, you can automatically manage risk and enforce compliance — while improving operational efficiency and reducing IT efforts.

**10.3 McAfee Network Threat Response**

McAfee’s *Network Threat Response* is used by top security analysts to uncover threats and perform forensic investigations that can successfully distinguish and effectively counter malware.
11. **Keywords**

**backdoor**
A feature of a program that gives an attacker access to and remote control of another computer. Programmers build this feature into applications so they can fix bugs. However, if hackers learn about backdoor access, it may pose a security risk. Backdoors, also known as trapdoors, are commonly utilized by Trojans, which can be detected by most anti-virus products and Network Intrusion Prevention Systems (NIPS).

**bot**
This program automatically searches for information and performs repetitive tasks. A bot can also generate generic traffic over the network. While bots are not always malicious, the most common are Internet relay chat (IRC) bots that can install malware or potentially unwanted programs, distribute compromised machine lists, and organize zombies for distributed denial of service (DDoS) attacks.

**botnet**
A collection of zombie PCs. Botnet is short for robot network. A botnet can consist of tens or even hundreds of thousands of zombie computers. A single PC in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers.

**distributed denial of service (DDoS)**
A type of denial-of-service (DoS) attack in which more than one traffic generator directs traffic to a targeted URL. Traffic-generating programs are called agents, and the controlling program is the master. DDoS agents receive instruction from a master to carry out an attack, which is designed to disable or shut down the targeted URL.

**denial of service (DoS)**
This attack targets a computer, server, or network and is either an intentional or accidental byproduct of instruction code that is either launched from a separate network or Internet-connected system, or directly from the host. A DoS attack is designed to disable or shut down the target, and disrupt the system’s ability to respond to legitimate connection requests. A denial-of-service attack overwhelms its target with false connection requests, so the target ignores legitimate requests.

**exploit**
To use the defects found in software code or function on a system to elevate privileges, execute code remotely, cause denial of service, or prompt other attacks. A buffer overflow is one example of an exploit.

**heuristic analysis**
A method of scanning that looks for virus-like behavior patterns or activities. Most leading anti-virus packages have a heuristic scanning method to detect new or not-yet-known viruses in the field.

**in-the-cloud detection**
This type of detection is derived by querying remote servers using the Internet.
Intrusion prevention system (IPS)
A preemptive approach to host and network security used to identify and quickly respond to potential threats. An IPS monitors individual host and network traffic. An attacker might carry out an attack immediately after gaining access, so an IPS can take immediate action as preset by the network administrator.

Host Intrusion Prevention System (HIPS)
A system that defends desktops and servers with combined signature, behavioral, and firewall protections.

Network intrusion prevention system, network IPS, NIPS
Software or a device that monitors network traffic and prevents attacks on a network or system. McAfee Network Security Platform is one example.

reputation filtering
A type of filtering that scores Internet senders based on global messaging and communications behavior to block transmission of content to or from risky sources and sites.

Trojan, Trojan horse
A malicious program that pretends to be a benign application. It does not replicate but causes damage or compromises the security of your computer. Typically, an individual emails a Trojan horse to you; it does not email itself. You can also download a Trojan from a website or via peer-to-peer networking. Trojans are not considered viruses because they do not replicate.

zero-day threats, zero-day vulnerabilities
Also known as zero-hour threats and vulnerabilities, they include threats that immediately exploit a newly discovered vulnerability.