



Rethinking Perimeter Security: New Threats Require Real-Time Protection

A DefensePro White Paper By Avi Chesla - VP, Security Products



Table of Content

Introduction..... 3

 Market History..... 3

 IPS Products and New Attack Trends..... 3

Technological Requirements of the Marketplace..... 4

 Network-Based Threats and Risks..... 4

 Server-Based Threats and Risks..... 5

 Client-Based Threats and Risks..... 8

APSolute Immunity with DefensePro..... 9

 Introducing Radware’s DefensePro..... 9

 Deploying DefensePro in Your Network..... 10

 Hardware Designed to Meet the Security Challenges..... 10

DefensePro Brain: A Technology Overview..... 11

 Automatic Real-time Signatures Technology..... 11

 Deterministic Security Technology Modules..... 14

APSolute Immunity: Solving the Emerging Threats..... 15

 Layers of Defense..... 15

 First Layer of Defense – Network-based Protection..... 16

 Second Layer of Defense –Server-based Protection..... 17

 Third Layer of Defense – Client-Based Protection..... 23

 Fourth Layer of Defense – Stateful Signature-Based Protection..... 25

Security Administration and Management..... 27

 Introducing APSolute ManagePro..... 27

 System Status and Operations Auditing..... 27

 Security Policies Configuration Tool..... 28

 Monitoring..... 28

 Real-time Dashboards..... 29

 Reporting Tool..... 29

 Attack Reporting of Real-time Signatures..... 30

 SLA Reports – Bandwidth Consuming Attack Reports..... 30

 Security Management Made Easy..... 31

Summary..... 31

Introduction

Market History

Over the last few years, networked resources have become increasingly available to a wide audience of customers, partners, suppliers, and the general public. As a result, more and more people have become reliant upon instantaneous access to information and services in order to do business. The importance of network availability has become paramount and it is therefore apparent that the network has become a target for attacks. Network infrastructure was designed to provide connectivity and not to limit connectivity.

A significant part of today's and tomorrow's threats are dynamic in nature – they are not addressable by static signature-based IPS devices.

Early developments in corporate network security included the firewall, which was intended to limit network traffic only to those users deemed necessary for its business to function. However, malicious hackers found ways to circumvent the firewall and attack the network, causing adverse and costly outages. The next important development was the intrusion detection system (IDS) that was designed to alert network administrators of attacks targeting known vulnerabilities in the network fabric. Difficulty in administration, high cost of maintenance, and the need for manual intervention rendered the IDS largely ineffective for addressing these network attacks. To address this last limitation, some IDS vendors began to not only flag network attacks, but also block them, and the in-line intrusion prevention system (IPS) was created.

IPS Products and New Attack Trends

First generation IPS devices match patterns (or “signatures”) of known attack vulnerabilities for incoming network traffic and block the traffic that is deemed undesirable. However, a significant amount of threats in network infrastructure – today and in the future - are dynamic in nature and cannot be addressed by static signature-based IPS devices.

These threats are generally not associated with unusually large traffic volumes, nor do they contain any non-legitimate application requests or exploit software vulnerabilities (they are usually defined as “non-vulnerability based attacks” which will be discussed later on in this paper).

This loophole allows hackers to integrate with legitimate forms of communications and comply with all application rules, so for traffic thresholds or known attack signatures, these hackers are below the radar of existing network security protections.

In the attempt to protect against and handle these new types of threats, administrators try to (reactively) sift through data logs and then manually set traffic filters and thresholds to mitigate attacks. Set the protection too high and legitimate users will be locked out; set the protection too low, and the organization is open to attack. It becomes a high-wire balancing act that few companies are willing to perform.

This latest wave of attacks introduces a whole new way for organizations to be extorted by cyber criminals. These threats need to be mitigated through new intrusion prevention technologies that complement existing signature-based IPS.

Technological Requirements of the Marketplace

For the reasons stated in the previous section, an effective IPS system must be able to detect and automatically repel a wide variety of attacks in real-time, without negatively impacting legitimate users. Because legitimate network traffic patterns change constantly, an effective IPS needs to quickly adapt to its surrounding, without human intervention.

An effective IPS system must be able to detect and automatically repel a wide variety of attacks in real-time, without negatively impacting legitimate users.

The automated detection mechanisms that are used by the IPS must be capable of distinguishing between normal and abnormal behavior, even though the differences between them may be subtle.

In case the IPS misidentifies traffic, it must also incorporate a self-correcting mechanism in order to minimize false positives.

Furthermore, the system must be able to select the optimal response method to stop the attack with minimum human intervention and the responses must be dynamically self-tuned and aligned with the changing conditions and developments of the attack's characteristics.

The following sections focus on emerging threats that impact the overall IP infrastructure, server applications as well as clients, putting most of today's organizations at high risk, including mid to large enterprises and carrier network environments such as ISP's and Telco's.

Network-Based Threats and Risks

The network-based layer of threats includes attacks that misuse network resources. One of the oldest - but still most effective - methods to exploit IP infrastructure weaknesses is the Distributed Denial of Service (DDoS) attack.

DDoS attacks typically involve breaking into hundreds or thousands of machines across the Internet. This break-in process can be performed "manually" or automatically by using, for example, worms and other malware that propagate on their own or can be downloaded by the unaware client, and infect every vulnerable host. After a successful break-in, the "attacker", or the malware acting on behalf of the attacker, installs specific DDoS tools or a specific bot, allowing the attacker to control all these "burgled" machines to launch coordinated attacks on victim sites.

In the 2007 CSI security survey¹, a new category of "bots within the organization" threats was added and ranked in 8th place among the 19 different threat categories in the survey. This emphasizes the fact that bots has become a major problem resulting in an increased amount of network DoS attacks.

All these network attacks typically exhaust network stack resources, router and switches processing capacity and/or misuse bandwidth resources, disrupting victims' network connectivity.

On top of the DoS flood threat, the network layer threats include the "traditional" exploit-based Operating System attack vectors. Each common network infrastructure product - such as routers, switches and firewalls - has a list of known vulnerabilities. If any of these vulnerabilities are being exploited, the product can be compromised, risking the entire IP infrastructure and putting business continuity at high risk.

¹The 12th Annual Computer Crime and Security Survey, Robert Richardson, Computer Security Institute (CSI)

Examples of such known vulnerabilities include:

- Cisco Catalyst vulnerability (CVE-1999-0430) – Cisco Catalyst switches are vulnerable to a denial of service attack that may affect the switches ability to forward traffic.
- 3COM router contains a design flaw that could result in authentication bypass and configuration modification (CVE-2004-0477). Exploitation of this vulnerability may result in configuration modification which may result in denial of service.

Server-Based Threats and Risks

The server-based threats can be clearly divided into two groups: TCP/IP stack weaknesses exploitation and application level attacks.

TCP/IP Stack Weaknesses

These types of threats include attack vectors that aim to misuse the resources of the transport layer in a way that can disturb, deny or bring down TCP connections, and of course the application transaction(s) that go along with them (e.g., HTTP transactions, FTP files downloads, MAIL messages, etc.). It's easy to exhaust the TCP resources of a server through several attack vectors, such as TCP Syn flood attacks and TCP established connection floods. The latter, although very easy to generate, cannot be effectively detected and prevented by most existing security products. This attack can bring down, or seriously damage, the operation of servers by consuming large amounts of server TCP resources. This misuse of TCP resource attacks are not necessarily large scale attacks, and are therefore difficult to detect and prevent by most security solutions.

As in the case of network based attacks, the TCP/IP stack threats also include the “traditional” Operating System attack vectors. Each of the common Operating Systems has a list of known vulnerabilities. If any of these vulnerabilities is exploited, the server can be compromised, risking the service as well. Examples of such known vulnerabilities include:

- Microsoft Windows is vulnerable to a denial of service attack (MS08-001). This vulnerability occurs due to improper Group IP Sources handling routines within the Windows networking stack.
- Microsoft Windows is vulnerable to a denial of service attack (MS08-001). This vulnerability may cause denial of service to the current session. This vulnerability occurs due to a flaw in the way MS Windows processes fragmented ICMP Packets.
- Linux SCTP conntrack module vulnerability (CVE-2006-2934).The vulnerability allows remote attackers to cause a denial of service (crash) via a packet without any chunks, which causes a variable to contain an invalid value that is later used to dereference a pointer.

Server Applications Level Attacks

The vulnerabilities that are associated with this layer of threats can be divided into two families:

- a. Vulnerability-based server application threats. This family includes both known and zero-minute attacks.
- b. “Non-vulnerability-based” server application threats.

Vulnerability-based Server Application Threats

Vulnerability-based server application threats are the more traditional types of attacks that are based on a previously known vulnerability of application software; they are defined as the known attacks. When a new vulnerability is discovered an attacker can exploit it before the security company or the software vendor is ready

with an attack signature protection, or alternatively with a software patch that “fixes” the newly discovered vulnerability. During this time of exposure in which the protection or the software patch is developed, the attack is defined as a “zero-minute²” attack.

New application vulnerabilities are discovered almost every day. According to IDC³ Key Forecast Assumptions for the Worldwide Threat Management Security Appliance Market, 2007–2011, “Software is becoming more rather than less vulnerable”. According to Cisco 2007 Annual Security Report, more than 6,000 new vulnerabilities and alerts were published during 2007, and the total number grows every year.

Representative categories of known and zero-minute server application attacks include:

- Buffer-overflow vulnerability types – a buffer overflow is a design flaw where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may result in erratic program behavior, a memory access exception, program termination (a crash), incorrect results or – especially if deliberately caused by a malicious user – a possible breach of system security.
- SQL injection vulnerabilities – an SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. A successful SQL Injection can result in information disclosure or even full database denial of service.
- XSS - Cross Site Scripting – is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Vulnerabilities of this kind have been exploited to craft powerful phishing attacks and browser exploits.
- Rootkits – a rootkit is a program designed to take fundamental control of a computer system, without authorization by the system’s owners and legitimate managers. Rootkits help intruders gain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Microsoft Windows, Mac OS X [2] [3], Linux and Solaris.
- Worms – a computer worm is a self-replicating computer program. It uses a network to send copies of itself to other computers and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer

² In the past these types of attacks were defined as “zero-day” attacks. Because today the time to exploit the newly discovered vulnerabilities has been shrinking-down to a less than a day, these attacks are now defined as “zero-minute” attacks.

³ IDC Market Analysis: World Wide Threat Management Security Appliances 2007-2001 Forecast and 2006 Vendor shares: Still Stacking the Rack, Charles J. Kolodgy, Jon Crotty

“Non-Vulnerability-based” Server Application Threats

Non-vulnerability based threats aim to exploit weaknesses in the servers’ application that cannot necessarily be defined as vulnerabilities. They can be typified by a sequence of “legitimate” events that are used to break authentication mechanisms (also referred to as “server cracking”), scan the application for existing vulnerabilities (e.g. vulnerability scanning) that are usually followed by a successful exploitation and could be used for taking control of the server’s application operations. More sophisticated non-vulnerability application attacks include well chosen repeated sets of legitimate application requests that misuse the server’s CPU and memory resources, creating a full or partial denial of service condition in the application.

Non-vulnerability based threats aim to exploit weaknesses in the servers’ application that cannot necessarily be defined as vulnerabilities.

According to IDC⁴, “Hackers and others continue to find ways to misuse other people’s software. Initially this was done by exploiting a vulnerability but they are now finding ways to just misappropriate software without a vulnerability”.

These emerging server application threats, which look like legitimate application requests, are generally not associated with unusually large traffic volumes. This allows hackers to integrate well with wholly legitimate forms of communications, comply with all application rules, so that in terms of traffic thresholds or known attack signatures they are below the radar of existing network security protections.

These non-vulnerability-based server application attack vectors include attack tools such as application scanners, brute-force and dictionary tools called crackers, application session-based flood tools and, last but not least, bots that are capable of integrating all of these attack tools into a legitimate infected client machine that will generate all of the above server-based threats.

The following illustration describes the relationships between threat types that were discussed:

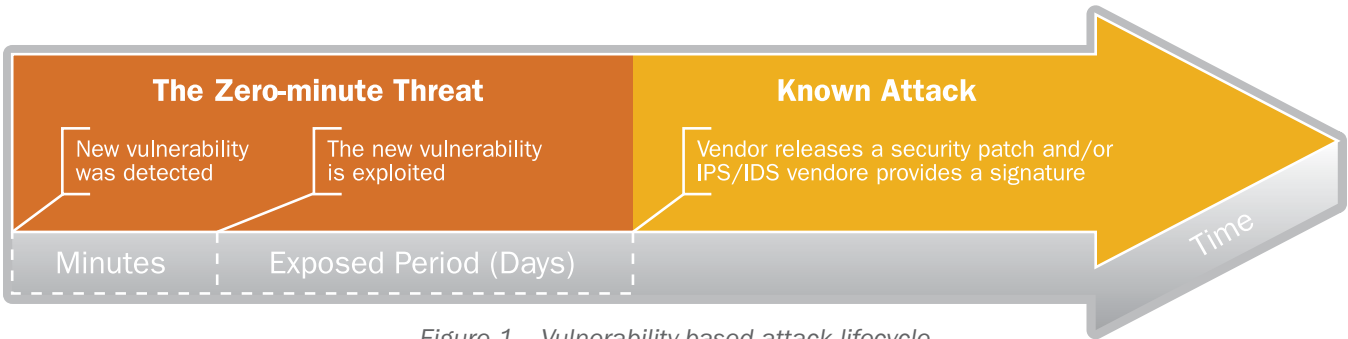


Figure 1 – Vulnerability-based attack lifecycle

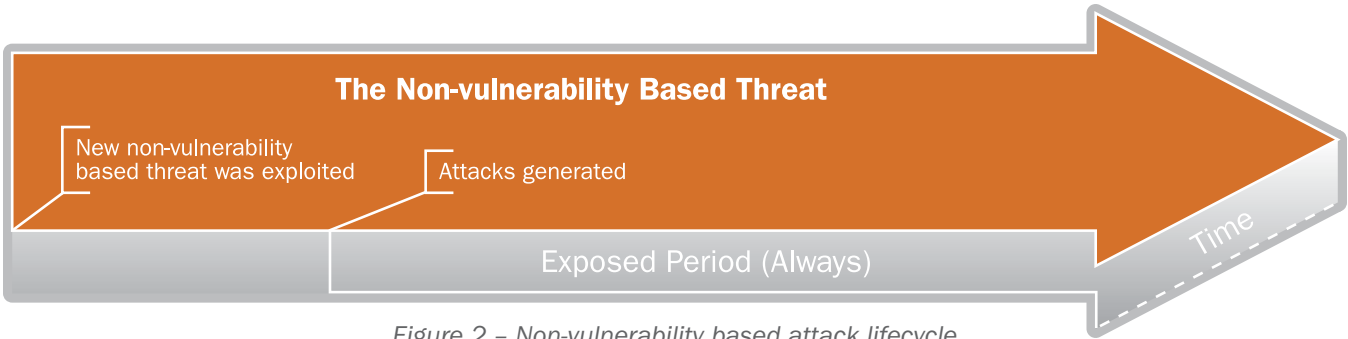


Figure 2 – Non-vulnerability based attack lifecycle

⁴ IDC, “Worldwide Threat Management Security Appliances 2007-20011 Forecast and 2006 Vendor Shares: Still Stacking the Racks,” Doc # 209303, November 2007

The vulnerability based attacks life cycle (Figure 1) focus is the early discovery stage: hackers try to exploit newly discovered application vulnerabilities while the security vendors scramble to provide a signature to protect against it. Hence the cat-n-mouse play between hackers and vendors.

The non-vulnerability threats define a new playground: security vendors cannot respond proactively by securing newly discovered vulnerabilities, nor can they use signature protection as the attack traffic interacts well into legitimate traffic patterns.

Client-Based Threats and Risks

Client-based attacks have been recognized for a long time. Client applications like Microsoft applications for Internet browsers, audio/video players and others include known vulnerabilities that can be exploited by known methods. In the last couple of years, we have seen that client applications have become more and more exposed to client-based exploits due to new mobility options for clients (i.e., the Mobile Users).

Mobility and the Disappearing of the Network's Perimeter

In recent years the mobility of companies in the global environment has caused the network perimeter, which is usually protected by gateway security devices, to “disappear”, making it more difficult to maintain a secured network. PDAs and “Smart” phones for example, use operating systems and applications that include client application vulnerabilities which can be exploited in a similar way to that of laptop computers and PCs. Therefore, employees who are frequently out of the office and use laptops and PDAs are often the unwitting malware carriers of bots, worms & Trojans. These malwares are carried into the organization by company employees who bring their infected laptops and PDAs into the office, or alternatively use their remote connection in order to access the internal network. This allows malware and other types of attacks to freely propagate in the “protected” network.

Once it is inside the network, the attack is unimpeded and can spread quickly attacking the network from within and *use the internal network computerized resources as part of a botnet for hire* in order to attack third party organizations.

As mentioned before, according to the 2007 CSI security survey, the “bots within the organization” category of threats was ranked in the eighth place among 19 different ranked threat categories. The reason for this high rank is the fact that infecting clients with bots has become easier. These botnets lay the foundation for different types of attacks, especially those attacks that were mentioned in the network and server-based threats section above.

Client Application Vulnerabilities

In general, client-based attacks aim to exploit known or new (zero-minute) vulnerabilities in the client's TCP/IP stack or application. Browsers such as Internet Explorer, Mozilla, Firefox, Microsoft Office applications, media players and other client-based applications have known vulnerabilities that can be exploited through several attack methods. The following are the main types of client based vulnerabilities:

- Microsoft vulnerabilities – Microsoft Windows operating system and Office Application Suite contain client vulnerabilities such as buffer overflows and other design flaws. These vulnerabilities are published through the Microsoft Patch Tuesday monthly bulletin. These vulnerabilities can lead from remote code execution, denial of service and up, to full system compromise.
- Active- X – ActiveX is a Microsoft technology used for developing reusable object-oriented software components. ActiveX control is similar to a Java applet. However, ActiveX controls have full access to the Windows operating system. This poses a risk that the ActiveX control may be exploited by hackers to damage software or data on victim machines.

- Spyware – spyware is computer software that is installed surreptitiously on a personal computer to intercept or take partial control over the user’s interaction with the computer, without the user’s informed consent.
- Phishing – phishing is an attempt to criminally and fraudulently acquire user identity through stealing sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. PayPal, eBay and online banks are common targets. Phishing is typically carried out by e-mail or instant messaging, and often directs users to enter details at malicious websites.
- Rootkits – a rootkit is a program designed to take fundamental control of a computer system, without authorization by the system’s owners and legitimate managers. Rootkits help intruders gain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Microsoft Windows, Mac OS X [2] [3], Linux and Solaris.
- Trojan – a Trojan horse program is a piece of software which appears to perform a certain action but in fact, performs another such action as a computer virus. Trojans are used to steal information, run applications or provide unauthorized access to the system.

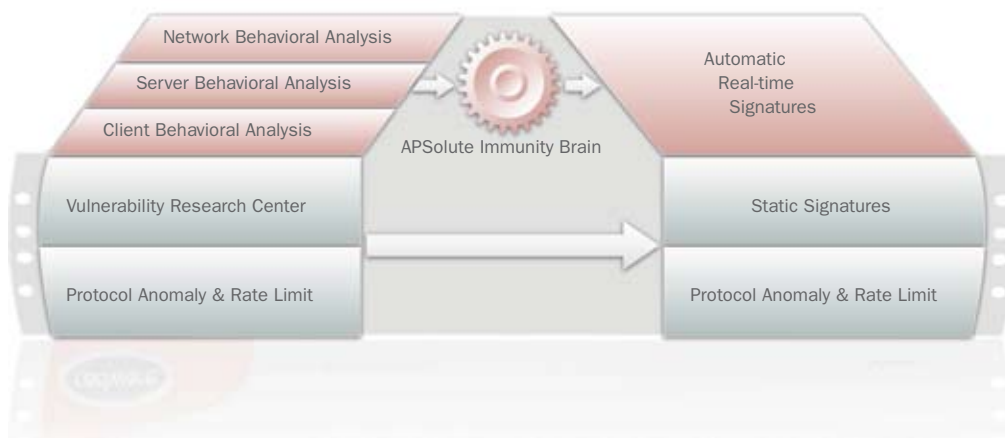
Evasion techniques – Recently we have seen that the methods of exploiting client-based vulnerabilities are getting more sophisticated in order to evade detection. Techniques such as anti-debugging and anti-virtualization can modify and compress an executable file by encrypting and changing its form from its original format and thus significantly raise the detection challenge for signature-based detection solutions.

APSoIute Immunity with DefensePro

Introducing Radware’s DefensePro

In order to meet the challenging demands of detecting and preventing today and tomorrow’s threats, Radware’s DefensePro features vulnerability-based protection through proactive signature updates with protocol anomaly and rate limit. This is a deterministic signature-based technology aimed at the prevention of already known attacks. *The Radware unique advantage is the real-time signatures that are generated automatically by DefensePro to prevent the non-vulnerability, zero-minute attacks without the need for human intervention.* The real-time signature “brain” is an adaptive multi-dimension Decision Engine that deploys Fuzzy Logic technology for accurate attack detection and mitigation. The brain is fed by three behavioral analysis modules performing analysis of client-, server- and network-based traffic, sending an alert once abnormal patterns are detected.

“With a range of innovative technologies under the hood, we found the DefensePro’s detection and mitigation capabilities to be excellent. We also found it to be very stable and reliable, coping with our extensive reliability tests with ease and without succumbing to most common evasion techniques.” NSS Labs, 2008.



Deploying DefensePro in Your Network

DefensePro can be deployed in multiple locations across the enterprise network, as shown in figure 3:

- At the Gateway, providing network perimeter protection against mass volume attacks such as worms, scanning, DoS/DDoS floods and more.
- At the Data Center or DMZ, protecting servers against application level attacks, application misuse and application vulnerability scanning.
- In the form of user segments, protecting and isolating the segments against worms, bots, Trojans, client vulnerabilities and more.

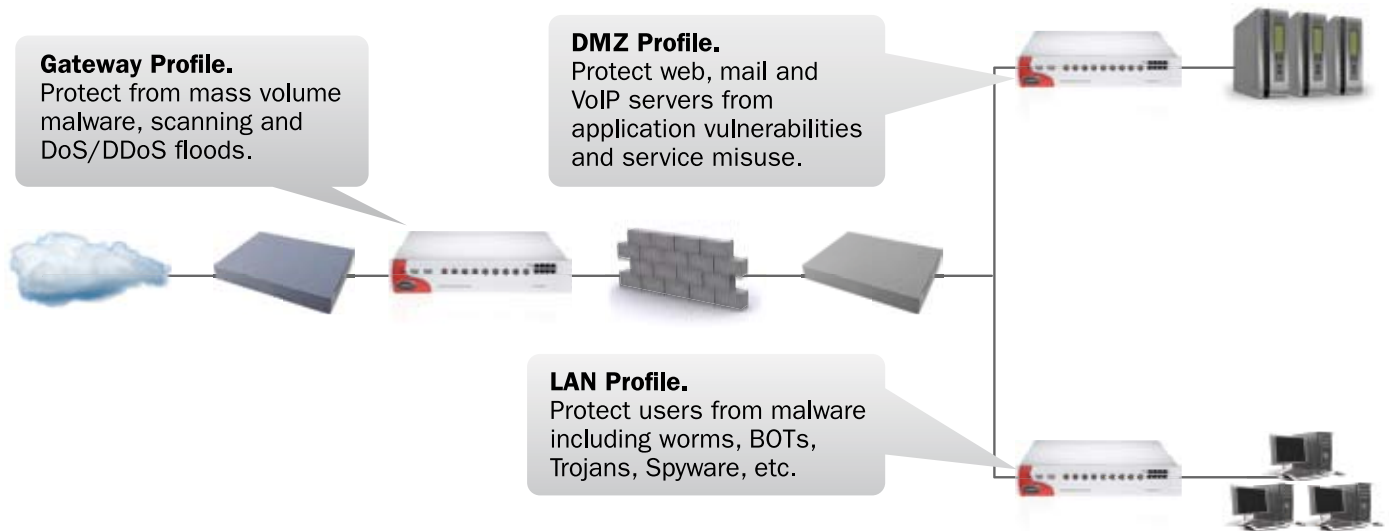


Figure 3 – Typical Deployment of DefensePro

Hardware Designed to Meet the Security Challenges

DefensePro's customized, ASIC-based hardware architecture ensures the highest levels of security, availability and performance. The DefensePro-x20 series supports multiple segments for monitoring enterprise core and perimeter environments. The DefensePro-x02 series for single segment monitoring offers the best price-to-performance for securing the enterprise perimeter remote branches.

Software-based performance upgrades maximize investment protection, allowing you to scale your solution easily and affordably by simply purchasing a software license for greater throughput. The DefensePro-x20 series scales from 600 Mbps up to 3 Gbps; the DefensePro-x02 series scales from 100 Mbps to 500 Mbps.

DefensePro Brain: A Technology Overview

As discussed in the previous section, the main security technologies deployed in DefensePro are:

- Automatic real-time signatures technology – Detects and prevents the non-vulnerability and zero-minute attacks without the need for human intervention.
- Deterministic signature-based technology – Detects and prevents known attack vulnerabilities.

Automatic Real-time Signatures Technology

The real-time signatures technology is an adaptive multi-dimension Decision Engine that deploys Fuzzy Logic technology for accurate attack detection and mitigation. This section reviews the following module building the Radware unique advantage in the IPS market:

- The Fuzzy Logic Module – A multi-dimension decision engine that detects attacks in real-time.
- Automatic Real-time Signature Generation module – Once an attack has been detected this module creates on-the-fly attack signatures.
- Closed-Feedback Modules – Responsible for optimizing the real-time signature during attack blocking stage, and remove the signature once attack is over.

Fuzzy Logic Module - Adaptive Multi-Dimension Decision Engine

When decisions about traffic, users and application behavior are to be made, Radware's Fuzzy Logic Module is the main decision engine. This engine collects traffic characteristics parameters and assigns them an anomaly weight according to an adaptive fuzzy membership function. It then correlates these parameter weights and produces real-time decisions represented by a "degree of attack" (or anomaly) value. Based on these degrees of attack figures, the system is able to introduce counter-measures that actively repel a perceived threat.

Radware's Fuzzy Logic algorithm overcomes traffic analysis difficulties that Internet communications usually present. The algorithm provides a remarkably simple way to draw definite conclusions from vague, ambiguous or imprecise information. Difficulties such as incomplete knowledge or noisy signals (something that usually happens when dealing with Internet traffic) are smoothly handled by the Fuzzy Logic algorithm. Radware has chosen Fuzzy Logic over other traditional analysis and approximation methods due to the large amount of CPU and memory resources that these methods consume.

The Fuzzy Logic algorithm can process a large amount of parameters, decide about their degree of anomaly, correlate between them and reach conclusions in real-time. The algorithm provides a methodology that does an excellent job of balancing significance and precision. Using Fuzzy Logic as a decision engine, Radware's Network IPS can perform more in-depth traffic analysis and come to conclusions quicker than any other traditional method.

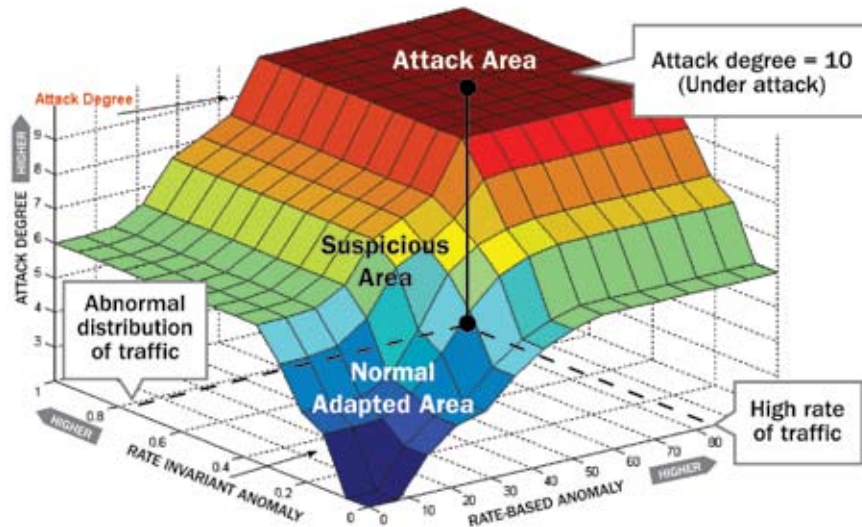
The Fuzzy Logic Module includes adaptive capabilities. As such, the sensitivity of the module is being continuously tuned in order to match the characteristics of the protected network. The adaptive algorithms include IIR (Infinite Impulse Response) filters that continually average traffic parameters and shape the Fuzzy Logic membership functions accordingly.

These capabilities allow the Radware's IPS to establish normal behavior baselines according to the date and the time of day.

For each required protection type, the Fuzzy Logic decision collects and learns traffic parameters that are needed in order to best characterize the threat that should be identified and mitigated. The "Full Spectrum Protection Technology Section" following this section, describes the traffic parameter types needed for the decision engine per each type of threat.

Typically, the Fuzzy Logic decision engine uses two categories of traffic behavioral parameters to generate a degree of attack:

- **Rate-based** behavioral parameters such as packet rate, Mbps, connection rate, application request rate, application response rate etc.
- **Rate-invariant** behavioral parameters such as protocol breakdown, TCP flag distributions, ratio between inbound and outbound traffic, application request/response ratio, connections distribution, URL hits probability functions and more.



The XY plane shows the fuzzy input rate-based input and rate-invariant inputs).
The z-axis represents the degree of attack (or anomaly).

Figure 4 - Fuzzy Logic Decision Surface

The Fuzzy Logic decision surface illustrated in the Figure 4 above shows a correlation between both rate-based and rate invariant behavioral parameters, before generating a degree of attack. Although, in reality, the Fuzzy Logic engine correlates between multiple behavioral parameters, for clarity the figure illustrates a two-dimensional decision surface.

Elimination of False Positives - In order to eliminate false positive decisions and misdetections, the Fuzzy Logic engine correlates between both rate and rate-invariant parameters. To illustrate this point, consider the frequent legitimate behavior of a mass crowd entering a news website in an unexpected manner. This behavior immediately causes rate-based behavioral parameters to significantly increase, thus making it look like an anomaly. If the detection engine relies only on rate-based behavioral parameters, this completely legitimate behavior will be flagged as an attack, and will be blocked. However, because rate-invariant parameters will remain unchanged (within certain boundaries) during such legitimate mass crowd behavior, an engine that intelligently correlates between both rate-based and rate-invariant parameters, such as Radware’s Fuzzy Logic engine, will not be susceptible to the aforementioned false positive decision.

“A major concern in deploying an in-line device is the blocking of legitimate traffic. ...DefensePro completed all our tests without raising a single false positive alert.” *NSS Labs, April 2008*

The Fuzzy Logic Module is an adaptive expert system that requires minimal human intervention to configure rules or thresholds. A system that relies upon manually-tuned thresholds and rules produces wildly disparate detection quality, depending mostly on the individual skill level of the system administrator.

Automatic Real-Time Signature Generation Module

In cases where the attack is unknown (zero-minute threat), it is always a great challenge to block the attack without blocking legitimate traffic at the same time.

The known attack is usually characterized by a well-defined content signature that can be used to remove the threat in a surgical manner. However, in the case of zero-minute or non-vulnerability based threats, no signature exists and therefore the security technology that detects the anomaly is based on behavioral analysis. In order to block the attack, the systems should also be capable of characterizing it in a very precise way. In other words, the behavioral-based technology should have the capability of automatically creating an attack signature.

In order to create an attack signature that characterizes the ongoing anomaly without the need for a human research vulnerability group, Radware utilizes probability analysis and closed-feedback loop technology. The below section describes how it works:

When the Fuzzy Logic decision module detects an anomaly, the system activates the automatic attack signature generation mechanism in order to find characteristic parameters of the ongoing anomaly. Working according to a Probability Theory (a unique patent-pending implementation method that was developed by Radware) that distinguishes between expected and unexpected repetition of parameters that were studied (statistically) according to the network environment, the automatic signature generation mechanism flags unexpected values as “possible” pieces of the attack signature that represents the ongoing detected anomaly.

The following parameter types as well as others are analyzed by the automatic signature creation module:

- Packet checksums
- Packet Identification number
- Fragment offset
- Source IP address
- Ports numbers
- TCP Flags
- SIP URL's (for VoIP anomalies)
- DNS query ID (identification number)
- Packet size
- TTL (Time to Live)
- ToS (Type of Service)
- Destination IP address
- TCP sequence numbers
- HTTP URL's
- DNS query
- DNS Qname (query count)

Once the values of these parameters are flagged as “abnormal”, the system transits into a signature optimization state that activates a closed-feedback loop mechanism.

Closed-Feedback Module

The closed-feedback module is responsible for creating the narrowest, but still effective, signature blocking rule. Each one of the above parameter types can include multiple values, detected by the automatic signature generation mechanism. The closed-feedback module “knows” how to tailor these values through AND/OR logical relationships. The more AND logical relationships are constructed between different values and parameter types, the more accurate and narrow the blocking signature rule is considered to be.

In order to create the logical relationship rules between the detected signature values, the closed-feedback module uses the following (but not limited to) feedback cases:

- **Positive feedback:** The traffic anomaly was reduced as a result of the decided blocking signature rules created by the module, the system continues to use the same action and tailors more attack characteristic parameters (i.e., signature types and values) through as many AND logical relationships as possible.

- **Negative feedback:** Meaning that the degree of traffic anomaly was not changed or was increased, the system stops using the last blocking signature rules and continues to search for more appropriate ones.
- **Attack stopped feedback:** If the attack stops, then the system will stop all countermeasures immediately, i.e., remove the signature rule.

The main advantage of the system described above is the ability to detect statistical traffic anomalies and create an accurate attack signature-based on heuristic protocol information analysis in real-time, mitigating the attack effect.

Deterministic Security Technology Modules

Even today, many threats simply violate stateful protocol rules, applications rules, or are exploiting application vulnerabilities that are already known. These threats can be precisely removed through a pre-defined attack signature that was developed by vulnerability research groups, or by enforcing deterministic protocol compliancy rules. For these purposes, the following deterministic security modules are deployed in DefensePro:

DefensePro's String Match Engine Module

For to the more deterministic types of threats, such as known application vulnerability exploitation attacks in which a signature is already available, DefensePro provides a proactive security update service that automatically downloads recent attack signatures to the system's attack database. DefensePro inspects incoming and outgoing traffic and compares each packet in real-time to the signatures in the database, while adding minimal latency. Radware's hardware accelerated String Match Engine is used for this purpose.

The String Match Engine is a hardware ASIC-based solution that is capable of multi-gig L7 (application layer), deep packet for full content inspection, including inspection of attack signatures that span across multiple packets (i.e., support cross packet inspection) or inspection attack signature that can only be written through regular expressions in order to avoid false positive or false negative events.

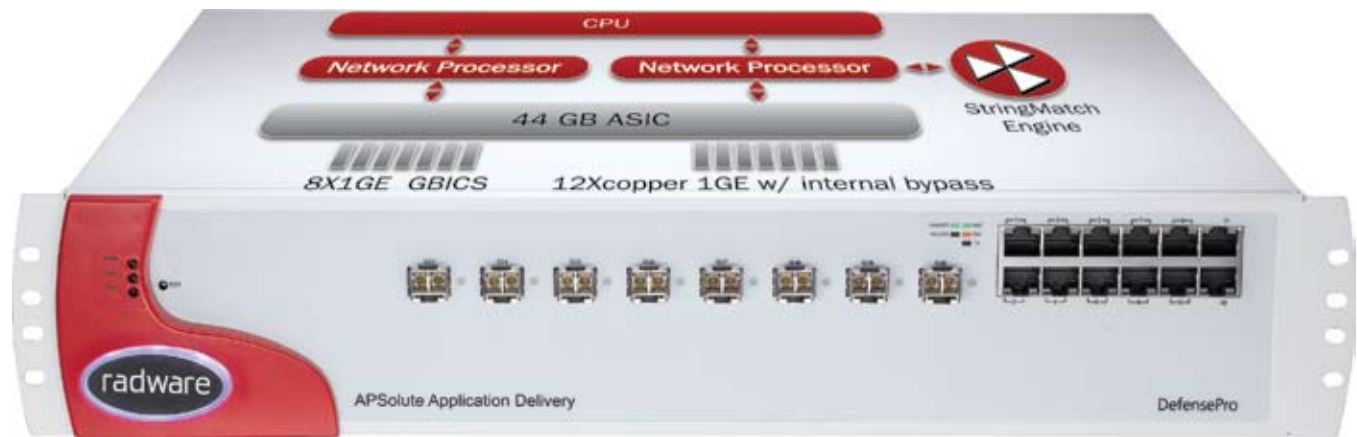


Figure 5 - DefensePro X20 Architecture

DefensePro uses a multi-layered hardware architecture comprising of the following parts:

- Master CPU – responsible for configuration management, monitoring and session management
- Network processors – offering up to 3Gbps of legitimate traffic forwarding and blocking attacks
- String Match Engine (SME) – performs in real-time deep packet lookup in each packet that matches a security policy.
- Switching fabric – a 44Gbps switching fabric designed for wire speed network traffic transfer with switch like latency

In the above described architecture, once the SME detects an attack signature within a packet, the network processors will block the whole session and the CPU will generate an event log with the attack information and details.

Radware’s Stateful Inspection Module

Stateful Inspection is a powerful tool designed to deal with a variety of attacks where the packets exchanged between a client and a server are legitimate, however the security threat is revealed only when inspecting a sequence of packets within a session, and not when inspecting individual packets. Most attacks, against which Stateful Inspection protects the network, are cases of protocol misuse where a session does not obey the state transition as defined by the specific protocol.

DefensePro Stateful Inspection module tracks new and existing sessions. Each packet is compared with its protocol state compliance according to the actual session state. Packets that disobey their protocol state machine are blocked and reported.

APSolute Immunity: Solving Emerging Threats

Based on the above technological modules, in this chapter we explain how DefensePro APSolute Immunity is uniquely suitable for the detection and prevention of each one of the major network, server and client threat types.

Layers of Defense

Threats can be categorized into different layers that typify different “natures” of attack behavior, and so the protection strategy must also be constructed with multi-layers of security technologies that will effectively analyze and repel each one of the threats. The following section describes DefensePro Layers of Defense that provide unparalleled network protection through the multiple protection modules.

The following diagram (Figure 6) describes the multi-layers of defense that form the APSolute Immunity in DefensePro:

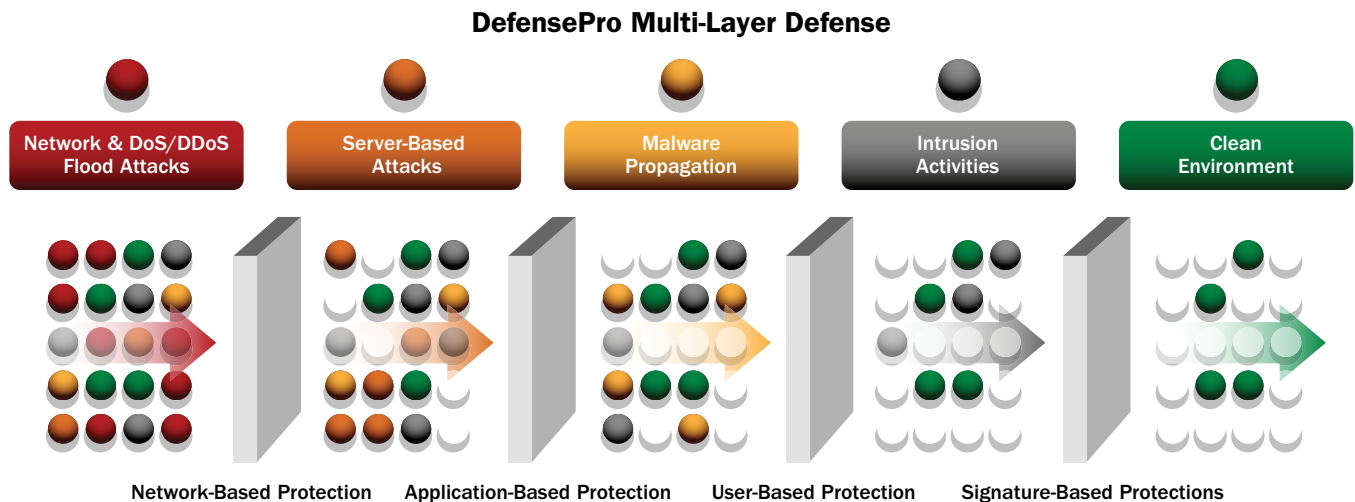


Figure 6: DefensePro Layers of Defense

DefensePro APSolute Immunity includes the following layers of defense:

- First layer: Network-based Protection – protects against DoS/DDoS flood attacks
- Second layer: Server-based Protection – protects against server resource misuse and server cracking
- Third Layer: Client-based Protection – detects already infected clients and prevents the spread of the client malware
- Fourth layer: Stateful Signature-based Protection – protects against known attack vulnerabilities

First Layer of Defense – Network-Based Protection

DoS/DDoS Flood Attacks Prevention

The first layer includes an innovative Network Behavioral DoS Analysis Technology which is called Behavioral DoS (BDoS). This technology is designed to process high volume threats such as DDoS and high rate worm propagations that significantly misuse the networks' bandwidth resources. This technology was designed to be the first layer of defense in the system in order to protect the system itself from attacks that will consume its own resources, thus causing "self DoS conditions".

The BDoS technology is particularly effective against the following high volume types of known and unknown (zero-minute) network attacks:

- TCP Floods (FIN, RESET, SYN+ACK, TCP fragment floods and more)
- UDP Floods (Including DNS, RTP, SIP and other UDP-based floods)
- Zero-minute high rate self-propagating worms
- Zero-minute high rate self-propagating network worms
- SYN Floods
- ICMP Floods
- IGMP Floods

Using the advanced statistical analysis and probability theory, Fuzzy Logic, and a novel closed-feedback filtering mechanism that were explained in the previous chapter, the Behavioral Network-based layer of defense automatically and proactively blocks known and zero-minute network flood DoS attacks and high rate self-propagating worms before they can cause harm.

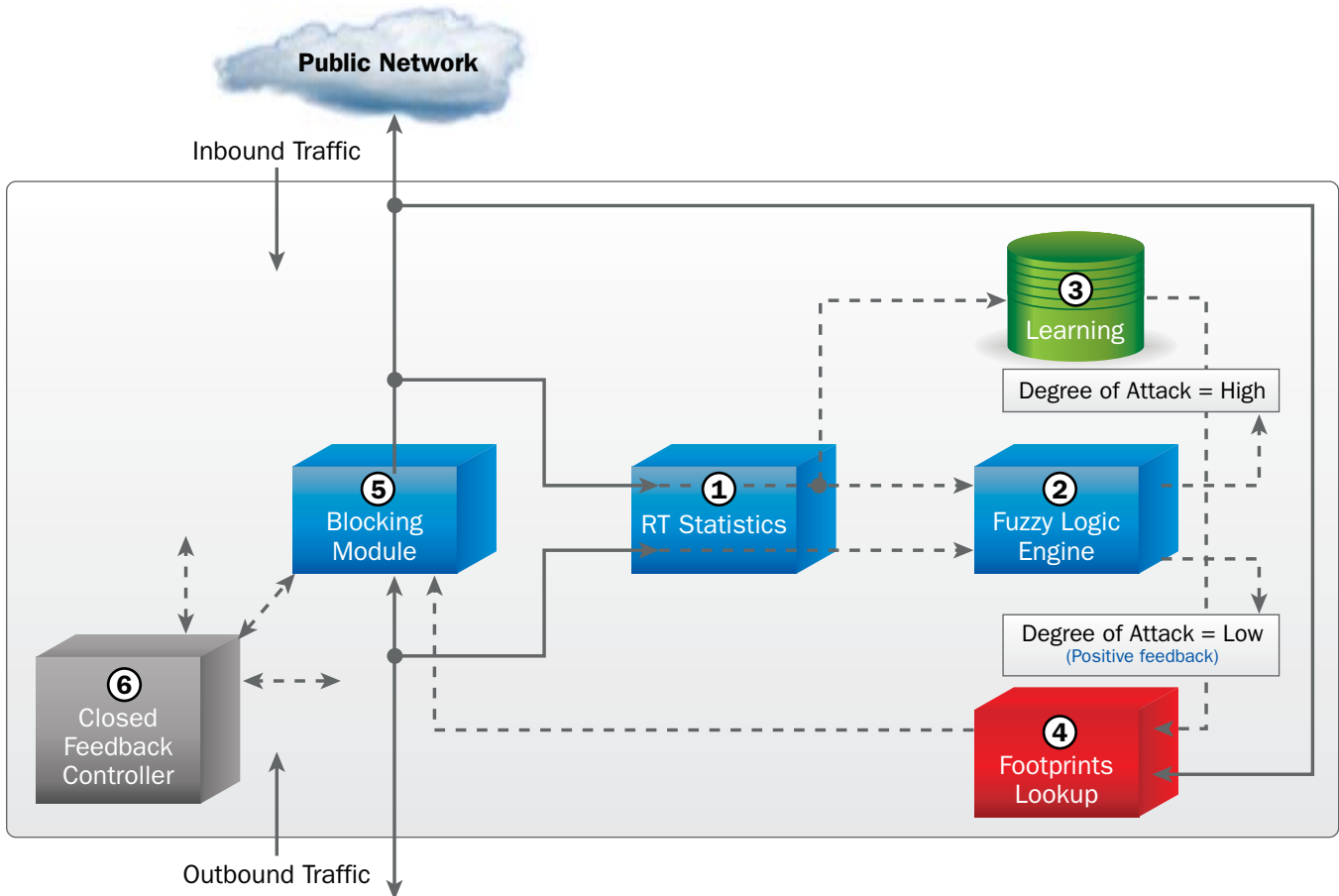


Figure 7 – Behavioral DoS Protection System

How Does It Work?

Figure 7 above represents the relationships between the major software modules that compose the Behavioral DoS protection system.

The protection system includes a **Real-time Statistics Module (1)** that takes measurements of the inbound and outbound traffic. The statistical operations are used to produce a comprehensive description of the communication (a multi-dimensional picture), thus a wide range of behavioral parameters are derived. Some of the rate-based and rate-invariant network traffic parameters that the BDoS protection collects in order to detect network based anomalies are specified below:

- Packet per second per protocol type
- TCP connections per second
- Protocol type distribution
- Kilo bit per second per protocol type
- Ratio of inbound versus outbound traffic
- Protocols' messages types' distribution ...

The RT statistics module constantly feeds the **Learning Module (3)** and the **Fuzzy Logic engine module (2)**, with the behavioral parameters. The Fuzzy Logic engine is the system's anomaly decision engine.

The Fuzzy Logic engine supports adaptive capabilities. This means that the sensitivity of the engine is being continually tuned by the **Learning Module (3)**, in order to fit the characteristics of the protected network environment.

The Fuzzy Logic algorithm correlates between the different network behavioral parameters, giving every parameter its suitable anomaly weight and, as a result, initiating the degree of attack in real-time. This degree of attack represents the intensity of the anomaly that reflects DoS and DDoS flood attacks.

Upon detection of an anomaly, the **Footprints Lookup Module (4)** which represent the system's Automatic Signature Generation Module, detects consistent patterns, called attack footprints, taken from the packet headers and payload fields. These attack characteristic parameters are used as filters by the **Blocking Module (5)**.

The ability of the protection system to measure the dynamics of the anomaly degree before and after the filtering operations is used for closed-feedback purposes.

In order to create an optimal blocking filter, the system uses a **Closed-feedback Loop Module (6)**, which compares between the desired and the existing degree of attack and tunes the blocking filter rules accordingly. The closed-feedback mechanism's aim is to create the "narrowest" possible filter rule against the ongoing attack. For more information about the automatic signature generation module and closed feedback operation refer to: Automatic Attack Signature Generation & Closed-Feedback Modules sections

Second Layer of Defense – Server-Based Protection

This layer of defense includes two main protections: Misuse of Web application resource protection and Server Cracking Protection. This layer of protection aims to detect and prevent both zero-minute attack and non-vulnerability based attacks – attacks which signature-based technologies or firewalls alone cannot fight.

Misuse of Web Application Resource Protection – HTTP Mitigator

The misuse of Web applications threat is perhaps the most advanced, non-vulnerability based threat that today and tomorrow's bots can generate against Web servers.

This attack is based on a completely legitimate, session-based set of HTTP GET or POST requests that are generated toward the victim Web server. These HTTP request are usually chosen with the main goal of utilizing significant amounts of the server's processing resources, thus creating denial of service conditions without necessarily having them typified as a high rate HTTP attack.

Today's network security technologies cannot differentiate between legitimate HTTP traffic and the aforementioned HTTP threat – resulting in very high rates false-positive detections. Rate-based engines also become insufficient as these HTTP floods may go under connection limit thresholds. Radware's adaptive behavioral server protection called HTTP Mitigator was designed to address both the detection and prevention challenge of these advanced Misuse of Web server attacks.

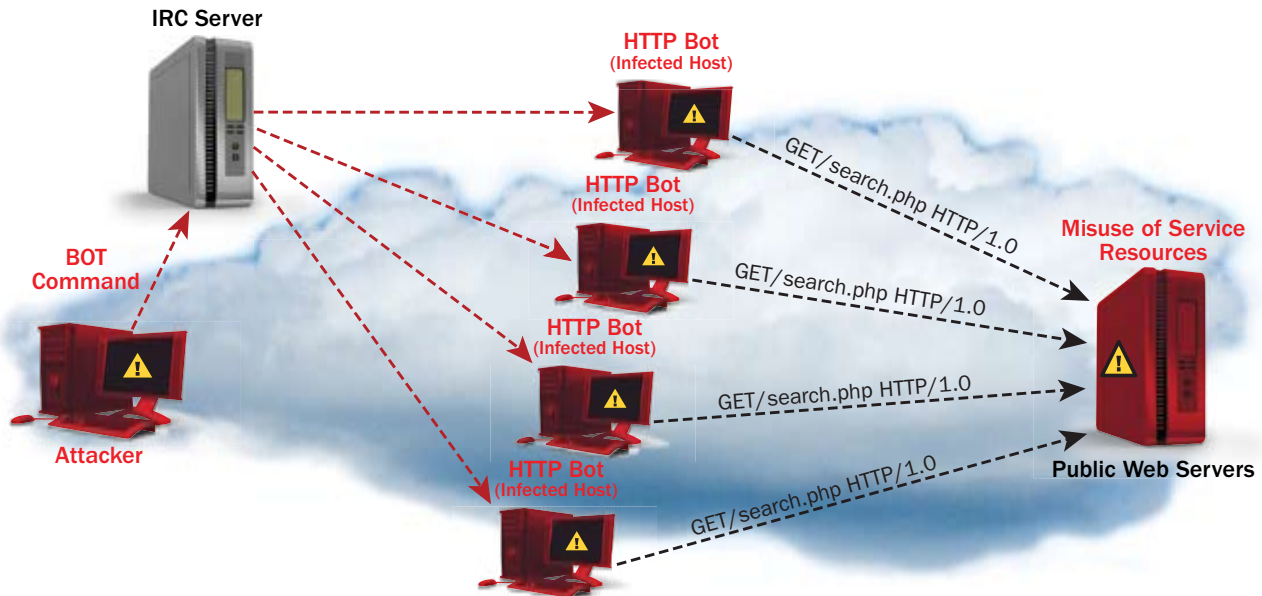


Figure 8 – HTTP Botnet Attack

A typical HTTP page flood is depicted in Figure 8. The attacker recruits an army of HTTP bot infected clients. Each bot usually connects to an IRC chat room and waits for the attacker command. The attacker issues a bot command indicating the victim site and the page to be downloaded, usually a Web page crafted with large images. Once the attack is launched, all HTTP bots start downloading the same page over and over, exhausting the victim web server's resources.

How Does It Work?

Detection Module

The attack detection is based on Radware's Statistical Based Module in conjunction with an adaptive Fuzzy Logic algorithm. The detection module classifies both network and application layer parameters such as:

- URL(s) hits probability distribution function
- HTTP GET request/sec
- HTTP POST request/sec
- HTTP "Other" methods/sec (e.g., HEAD, DELETE, PUT, etc)
- MAX HTTP GET & POST request per client
- MAX HTTP GET & POST requests per connection
- Download traffic [Mbps]
- Ratio between down loaded traffic and GET & POST requests toward the Web server

In order to accurately detect an HTTP flood attack, the Statistical Module collects both rate-based and rate-invariant HTTP traffic parameters. Both parameter types are analyzed and fed into the Adaptive (learning) Module and to the Fuzzy Logic decision engine.

It is important to emphasize the meaning of the rate-Invariant HTTP traffic parameters and their influence on the decision making, as these are crucial in order to prevent false-positive events. The rate-invariant parameters are:

- URL(s) hits probability distribution function
- Ratio between downloaded traffic and GET & POST requests to the Web server

URL(s) Hits Probability Distribution Function - The URL(s) hits probability function learns the normal usage of URL's (i.e., URL hits probability) for a given protected Web server. On the one hand, this parameter holds significant weight in the decision making about the detection of low-rate HTTP attacks which raise a major detection challenge. On the other hand, this parameter is responsible for eliminating false positive detection events in cases such as legitimate flash-crowds which enter the protected website unexpectedly.

The idea behind the URL's hits probability distribution function is that although the attack may use HTTP requests that are completely legitimate (as mentioned before, this attack is considered to be a non-vulnerability based threat), by using this distribution function it is possible to differentiate between legitimate and illegitimate usage of these HTTP requests. In other words, it differentiates between legitimate and illegitimate sequences of URL's hits without dependencies in traffic rate.



Figure 9 – URL hits probability distribution function

Download Ratio - Ratio between download traffic and GET & POST requests toward the Web server is part of the decision about attacks that use relatively low rate HTTP requests which result in a significant amount of bandwidth that is generated by the attacked Web server, thus misuse or saturate the outbound link. This type of attack behavior cannot be detected without the participation of this Download Ratio rate-invariant parameter.

Adaptive Module

The HTTP Mitigator includes a differential and continuous adaptive mechanisms that tune the sensitivity of the Fuzzy Logic decision engine.

The learning mechanism collects and aggregates the real-time traffic parameters through averaging and max procedure functions, and stores the aggregated values (“normal baselines”).

Two learning strategies are included in this protection system:

- Day-Time Differential Averaging (24×7 statistics) that groups data for aggregation according to hour of and day in the week.
- Continuous – Continuous moving window aggregation that groups data in recent history intervals based on IIR filtering averaging.

Both strategies are applied separately to each kind of statistical parameter. Choice of the proper learning strategy depends on the system history and its dynamics, i.e., stable HTTP traffic environments with a rather long history are likely to exploit the first strategy; otherwise, the second one is preferable. The system starts to learn the traffic through continuous IIR filtering; however, it has the capability to automatically choose which strategy is best according to the behavior of the protected network environment (i.e., protected Web servers).

Periodically (typically every one hour), the Learning Module updates the Fuzzy Logic decision engine with the associated normal baselines. In return, the decision engine tunes its detection sensitivity.

When a decision about an anomaly is made, the system stops all learning processes and starts a process which is responsible for characterizing the anomaly through the automatic attack signature generation module.

Automatic Attack Signature Generation Module

Upon anomaly detection, the system initiates its Automatic Attack Signature Generation mechanism. Because this threat is part of the “non-vulnerability” family of threats, it is not possible to create generic and static attack signatures through the traditional means. Therefore, it is crucial to find a dynamic signature that will fit each attack as it happens. The attack signature should be granular enough to mitigate the attack with no impact on legitimate Web transactions. Radware’s Automatic Signature Generation module analyzes all HTTP requests toward the protected server and identifies “abnormal” HTTP request (URL’s) patterns or a sequence of repeated patterns that are generated by the HTTP bots.

“Abnormal” HTTP requests, defined as URL’s that deviate from the adapted URL probability distribution function baselines (the same baselines that were established/learned by the detection module), thus violate the normal usage of the URL’s. The “abnormal” URL’s are flagged together with the source IP addresses that generate them. The system then generates mitigation patterns, i.e., dynamic attack signatures that include Source IP address(s) and one or more HTTP request URL checksums associated with them, and mitigates the attack.

Adaptive Traffic Normalization & Closed Feedback

Mitigation of the misuse of Web server resources attacks includes a few mechanisms.

One method uses an HTTP request rate-limit mechanism that limits the number of HTTP requests matching the detected attack signature in a gradual manner.

The rate limit factor is set according to the expected URL’s hits percentages, which is determined by the adapted URL’s probability distribution function, thus the HTTP traffic is normalized. According to a closed-feedback methodology, if the first rate limit factor that was determined is not sufficient to mitigate the attack, then a more “aggressive” rate limit factor is applied.

The idea is not necessarily to block all packets that participate in the HTTP flood, but rather to mitigate it to a level in which the protected Web server isn’t in a denial of service risk. These mitigation mechanisms are activated per one or many source IP addresses associated with the detected HTTP request URL’s that are used by the attackers or bots.

Behavioral Server Cracking Protection

Radware’s server cracking protection is a behavioral server-based technology that detects and prevents both known and unknown application scans, brute-force attacks and other application misuse activities.

The server cracking behavioral protection detects and prevents the following known and unknown (non-vulnerability based and zero-minute) threats:

- Web Authentication brute-force & dictionary attacks
- SMTP (Mail) brute-force & dictionary attacks
- POP3 (Mail) brute-force & dictionary attacks
- MSSQL brute-force & dictionary attacks
- SIP scans
- HTTP vulnerability scans attempts
- FTP brute-force & dictionary attacks
- MySQL brute-force & dictionary attacks
- SIP brute-force & dictionary attacks
- SIP DoS attacks

Scanner and Cracker Tools

There are many tools used to automate security tests. To simplify the description of these tools we can map them into two main categories: Network layer and application layer tools.

The server cracking protection focuses on the more challenging task of detecting and preventing scanners and crackers which fall into the application layer tools category, i.e., servers’ applications cracker and scanners.

We can recognize two main categories of non-vulnerability based server threats that the application layer tools fit into:

Cracking Attacks - Cracking attacks, being brute force or dictionary attacks, try to break into an application by guessing user names and passwords from known lists. The risk associated with these types of attacks is very clear. Once a useful username and password are obtained the attacker has free access to a service, information or even can get administration permissions to the server itself. Additional risks are denial of service by triggering built-in protections in the applications, locking out users or consuming system resources during authentication attempts.

Application Vulnerability Scanning - These scanners perform thousands of tests and provide a list of potential vulnerabilities that may be exploited. Typically, these scanners do not send an exploit to the server but a more legitimate request that only shows the existence of the vulnerability.

These application scanners generate thousands of application requests to the server and analyze the different behaviors of its responses. Through analysis of the application responses, the tools can identify the exact targeted application information (type, version etc.). According to the discovered application’s information the tool typically searches into a vulnerabilities database and selects a specific set of application requests that fit the application type and version and sends them to the probed application. Through this scheme the tool can automatically identify which vulnerabilities exist in the application.

The following figures show a typical HTTP vulnerability scanning:



Figure 10 – HTTP Vulnerability Scan Activities

After the vulnerability scanning phase the following results are achieved by the hacker:

- Information about the server application type and version is discovered.
- During the scanning activities the server resources (CPU and Memory) are misused and this can result in service disruption.
- Known potential application vulnerabilities are detected.
- In the second stage of the attack, a direct vulnerability exploitation attempt can be generated with a high probability of success.

The aforementioned application pre-attack probes, by definition, cloak themselves as legitimate traffic since they do not usually violate protocol rules or match pre-defined attack signatures that represent an exploitation attempt of known application vulnerabilities. Therefore, these server-based threats are defined as non-vulnerability based attacks. Network Intrusion Prevention Systems [NIPS] that support only signature-based detection capabilities are ineffective against these threats.

How Does It Work?

Detection Module

Radware’s server cracking behavioral-based mechanism uses statistical engine and an adaptive Fuzzy Logic decision engine in order to detect users that try to scan or brute force attack server applications. The engine classifies plurality of application response messages that are generated by the protected servers and extracts the user identifier from them.

The statistical engine then computes statistical characteristics such as frequency, quantity and distribution parameters of the plurality of response messages corresponding to each user.

The Fuzzy Logic decision engine assigns an anomaly weight to each characteristic parameter, correlates between these weights through expert rules, and generates a degree of anomaly corresponding to each user.

One of the challenges that every system administrator faces with protection systems is to define the time-out interval in which the system will monitor the user’s activities until a decision can be made (e.g., until a certain threshold is breached). Wrong time-out settings can lead immediately to false positive or false negative decisions. Monitor intervals that are too long increase the chances for false positive decisions, while intervals that are set too short increase the risk that the system will not detect the scan or brute force attack.

In order to solve this problem, Radware’s Server Cracking Decision engine automatically adjusts the user monitoring interval based upon the user’s degree of anomaly. This dynamic monitoring interval determines how much time the system will consider the user suspect and continue to analyze his activities until a decision can be made. This adaptation process increases the accuracy of the system’s decisions and reduces dramatically the configuration and maintenance operations that are required from the system administrator.

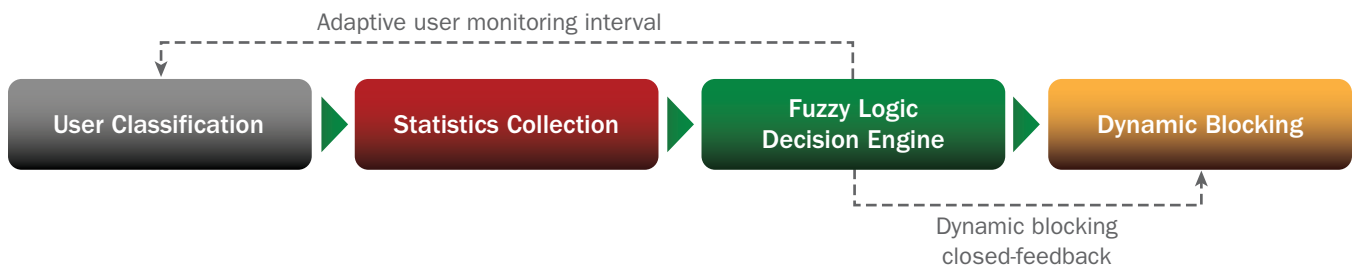


Figure 11 - Server Cracking Decision Making Process

Mitigation & Closed Feedback Module

Once a user has been identified as an attacker he is blocked, meaning no more connections from this source to the attack target server will be accepted. In case of attack, DefensePro inserts the source IP into a dynamic block list, or extends the blocking duration lest the source IP address had already been blocking during the same attack lifecycle.

Besides the dynamic user monitoring interval, Radware's DefensePro Closed Feedback Module is responsible for further minimizing false positive decisions. The closed-feedback methodology that the system supports is characterized by a dynamic blocking period. When the system discovers attacker activities, it will use a very short first blocking period against him. During this period, the system keeps tracing the blocked user and checks for consistency in his abnormal activities. If his activities are discovered as a one time case, the system will immediately reduce the blocking duration to zero and release the user. If the user's abnormal activities are consistent, then it will automatically increase the blocking duration. Figure 11 illustrates the server cracking decision making process.

Third Layer of Defense – Client-Based Protection

Most network intrusion prevention systems fail to prevent client-based attacks. This is due to the reasons mentioned before in the client-based threat section. The main reasons for this are:

- Mobility issues – the “disappearing of the perimeter” exposes the clients to more different types of attacks.
- The zero-minute threat – once an infected client enters the network, the malware is usually spread faster than security device vendors can “tag” them (i.e., the vendor will not be able to create a signature of the malware in time).
- Advanced evasion techniques that today's client-based malware uses.

The Already Infected Client

In order to effectively mitigate the risk of the client-based attack, there is a need for a system that will be able to detect abnormal activities that the already infected hosts are generating. The systems should identify these hosts and mitigate their activities.

For this purpose, Radware's DefensePro provides client-based behavioral analysis technology which detects unusual client based activities in the network and flags them. On top of this, in case the infected hosts become part of Botnet activities (which are the major threat organizations face today), any attack that is generated from these infected hosts is detected and mitigated by Radware's server-based and network-based security technology modules, which were described in the previous two sections.

How Does It Work?

The DefensePro employs three automatically synchronized processes to detect and prevent malware such as a network worm that is spread by the infected clients. These three processes are:

- **Detection** – Real-time discovery of malware propagation⁵
- **Characterization** – Classification of the malware's propagation profile by the automatic signature generation module.
- **Mitigation** – Activation of the automatic signatures that block the malware's evolving profile.

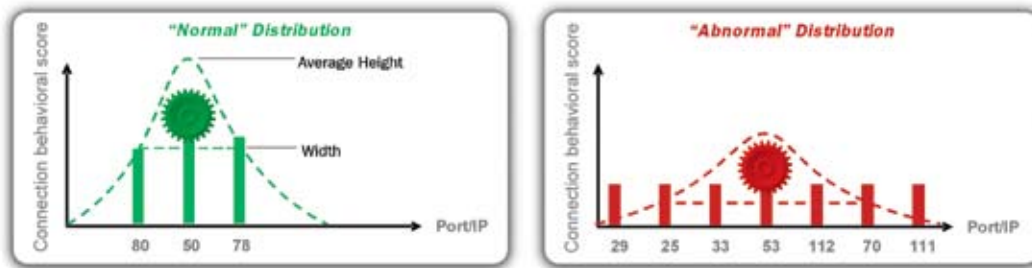
Each of these processes is described below.

⁵Propagation and spreading are used synonymously in the descriptions

Detection

Detection is based on an analysis of a host (i.e., user that connects into other hosts on or outside the network) payload distribution across its connections in the network. Analytical parameters, which represent this client's distribution curve, feed the decision engine (a Fuzzy Logic inference system) that calculates the likelihood that specific traffic constitutes malware propagation through worms. This system is time invariant, which means that low rate propagation activities will also be detected.

The figure below left, shows a normal traffic distribution curve, which represents normal client's traffic behavior patterns. The figure on the right represents traffic that indicates an attack (e.g. malware propagation). The distribution curves are generated by the decision engine using advanced statistical analysis of multiple clients' traffic parameters. The figures shown demonstrate the patterns derived from the statistical analysis.



Y-axis: Connection behavioral score; X-axis: Connections Identification (destination IP and port of each connection).

Figure 12 – Illustration of client distribution curves

The important task of the decision engine is to decide when the distribution curve represents normal, suspect or real attack propagation activities.

Automatic Real-Time Signature Generation Module

One of the most important capabilities that any IPS system needs to offer in order to detect the already infected client is the ability to accurately characterize malware propagation behavior. If the characterization is accurate, corresponding prevention measures can accurately target the spreading behavior, without interfering with legitimate network traffic.

DefensePro's automatic real-time signature generation module can characterize the ongoing (and potentially mutating) propagation methods used by malware.

The technology is based on novel implementation of statistical algorithms that characterize the spreading malware profile. The profiles include information such as where the malware originated, which vulnerable applications it is trying to exploit and additional traffic characteristic parameters that can be associated with the spreading malware.

The automatic signature generation module represents the spreading profile through the following traffic parameters:

- Packet size
- TTL (Time to Live)
- Destination IP address addresses
- TCP sequence numbers and more
- Packet Identification number
- Source IP address
- Ports numbers

Mitigation & Closed Feedback

One of the important tasks of network intrusion prevention systems is to be able to mitigate the impact that the malware spreading has on the network, allowing the system administrator to perform reactive procedures in order to contain all of the infected clients through system upgrades, patches and attack signature updates (if these are available).

The mitigation module is responsible for generating blocking filters, based on the detected spreading profile, that prevent the spreading activities and at the same time allow legitimate traffic to go through (even if it was generated from the infected clients themselves).

DefensePro incorporates closed-feedback technology that optimizes the prevention measures against the malware propagation activities, by continuously evaluating the effectiveness of the countermeasures and adjusting them accordingly.

The closed-feedback mechanism optimizes the prevention measures through the following steps:

- **First-Step** – initial prevention measures are constructed from the broadest criteria that categorize the malware’s spreading profile. For example, if the malware probes a few vulnerable application ports, the first prevention measure will block only the activities originating from the infected client and targeting the port(s) that are being probed most intensively.
- **Closed-Feedback Confirmation** – the closed-feedback mechanism evaluates the effectiveness of the initial counter-measure, i.e., whether the malware’s spreading activities were sufficiently filtered to a level at which the network can work “undisturbed.” If the initial counter-measure was successful, the filter is optimized with more granular filtering criteria such as typical packet size that represent the malware. The network administrator can then patch and upgrade the infected systems while reducing significantly the infection risk.
- **Closed-Feedback Optimization** – if the initial counter-measures were not effective enough, i.e., malware’s spreading activities are still disturbing network operation, the closed-feedback mechanism implements additional, less granular filters, on top of the previous one(s). This feedback process continues until the attack is under control.
- **Closed-Feedback Dynamic Signatures** – the closed-feedback mechanism works continuously. If a spreading profile is changed, the closed feedback mechanism will generate a new prevention profile that will best fit the new characteristics of the malware spreading profile.

Fourth Layer of Defense – Stateful Signature-Based Protection

Having said all of the above, for detection and prevention of **known network, server and client-based applications’ vulnerability** exploitation attempts, the signature based-approach is probably the best. An attack signature, when created effectively by the vulnerability research groups, reveals the known attacks very accurately and immediately. The level of reporting details about the type of attack and the exact impact/risk it imposes on the target application is also very high. This brings us to the conclusion that behavioral-based and signature-based technologies form a complementary solution. A security device that combines signature-based approaches with advanced behavioral technology will have an advantage over signature-based technology alone.

Security Update Service - Radware’s Security Operations Center (SOC)

For to the more deterministic types of threats, such as known application vulnerability exploitation attacks in which a signature is already available, DefensePro provides a proactive security updates service that automatically downloads recent attack signature to the system’s attack database.

Radware's 24x7 Security Operations Center (SOC) provides subscribers with an automated, weekly delivery of new attack signature filters as well as emergency and custom delivery of signatures. This helps ensure networks and applications are fully protected from current known vulnerabilities.

Radware SOC comprises of a group of network security experts that constantly monitor networks and applications for vulnerabilities, participate in security forums and discussion groups, and deploy honey pots to discover new attacks. Radware SOC performs research for the newly discovered vulnerabilities and attacks which result in a weekly signature database update. In the case of urgent attack situation, an update will be issued on the same day.

Each signature database update is fully tested on real customer's networks utilizing devices deployed as beta staging. The signatures are tested against real world traffic to eliminate false-positives.

Radware SOC has gained world recognition by the security industry and application vendors: SOC researchers present their latest findings in industry events such as BlackHat; Radware SOC was the first to discover application vulnerabilities in YATE IP telephony engine, Apple iPhone Safari Web browser, issue immediate protections for critical Microsoft vulnerabilities and the like.

For more information please refer to Radware Security Zone:
<http://www.radware.com/Customer/SecurityZone/default.aspx>

Radware's vulnerability based Attack Database includes the following attack categories:

- **Web servers** – Protection against attacks targeting common Web server application including IIS and Apache. The attack signatures protect against application level vulnerabilities, SQL injection and cross-site scripting.
- **Mail servers** – Protection against POP3, IMAP and SMTP protocol vulnerabilities and mail application vulnerabilities.
- **DNS** – Service protection against DNS protocol and DNS server applications vulnerabilities.
- **FTP** – Service protection against FTP vulnerabilities.
- **Databases** – Protection of DB servers such as Oracle and SQL.
- **Telnet and FTP – Protection against Remote access** protocol vulnerabilities and FTP/Telnet server implementation vulnerabilities.
- **SIP** – Protection for SIP servers, proxies and IP phones against SIP protocol violations preventing shut downs, denial of service and malicious takeovers.
- **Network Malware Protection** – Protection against worms, Trojan Horses, Spyware, and backdoor attacks.
- **Botnets protection** – This protection includes a solution to detect and block known communication control channel of the Botnets.
- **Infrastructure Vulnerabilities Protection** – Protection for routers and switches operating systems' vulnerabilities including Cisco, 3Com, Juniper and more.
- **Client Side Vulnerabilities**⁶ – Protection against vulnerabilities that are found on client machines and client side applications, including Microsoft Windows client side vulnerabilities and ActiveX vulnerabilities.
- **Anonymizers**⁷ – Prevention from users within a given network to use anonymizers
- **Phishing** – Detection and prevention of malicious attempts to redirect users into phishing dropping points for known and legitimate eCommerce and banking sites.
- **IPv6 attacks** – Protecting against IPv6 protocol vulnerabilities.
- **SSL-Based Attacks** – Protection against encrypted, SSL-based attacks⁸

⁶ Even though Microsoft releases a patch for these vulnerabilities, many systems are still vulnerable, especially critical Web servers which cannot be updated with a patch until their next scheduled maintenance window.

⁷ An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It accesses the Internet on the user's behalf, protecting personal information by hiding the source computer's identifying information. Sensitive and personal information may not be completely protected with an anonymizer.

⁸ In conjunction with Radware's AppXcel™ application accelerator appliance.

Security Administration and Management

Introducing APSolute ManagePro

APSolute ManagePro appliance allows the system administrator to manage remote Radware devices while reducing the amount of SNMP traffic flowing through the WAN. This is done by connecting the Appliance in the vicinity of the Radware devices, and connecting to the Appliance from a remote station using a Java applet. APSolute Insite Appliance is an application delivery management device that enables multiple users with centralized management to configure Radware’s application delivery devices, optimize network performance, anticipate problems before they occur, and reduce the total cost of ownership of Radware solutions. Using the Appliance it is possible to manage up to thousands of devices, with support for up to twenty simultaneous users and ten million security events.

The APSolute Insite Appliance works in a Client-Server mode, where the user opens a Web Browser to a predefined URL belonging to the Appliance. Once the user connects to the Appliance, it is authenticated by the Appliance by entering a Username and Password. If the user is authenticated then a Java Applet is downloaded to the user’s workstation browser on which APSolute Insite is then run. If the user is not authenticated then the connection is closed and the user is disconnected from the Appliance.

APSolute Insite main features:

- Multiuser management
- System status and operations auditing
- Configuration management of device characteristics, Security policies, BWM policies, reporting and more
- Monitoring, Alerting and Reporting
- SLA Reports

The following sections briefly highlight some of APSolute capabilities:

System Status and Operations Auditing

Status of managed devices can be monitored in real-time. A global view provides information about systems: status, uptime, system alerts and number of active attacks (see figure below).



Figure 13 - Global system status

Security Policies Configuration Tool

Policy definition is made simple by using a commonly known look and feel interface very similar to that of firewalls. Therefore, and although rules and policy can be very granular, the interface remain easy to use, as shown in the figure below.

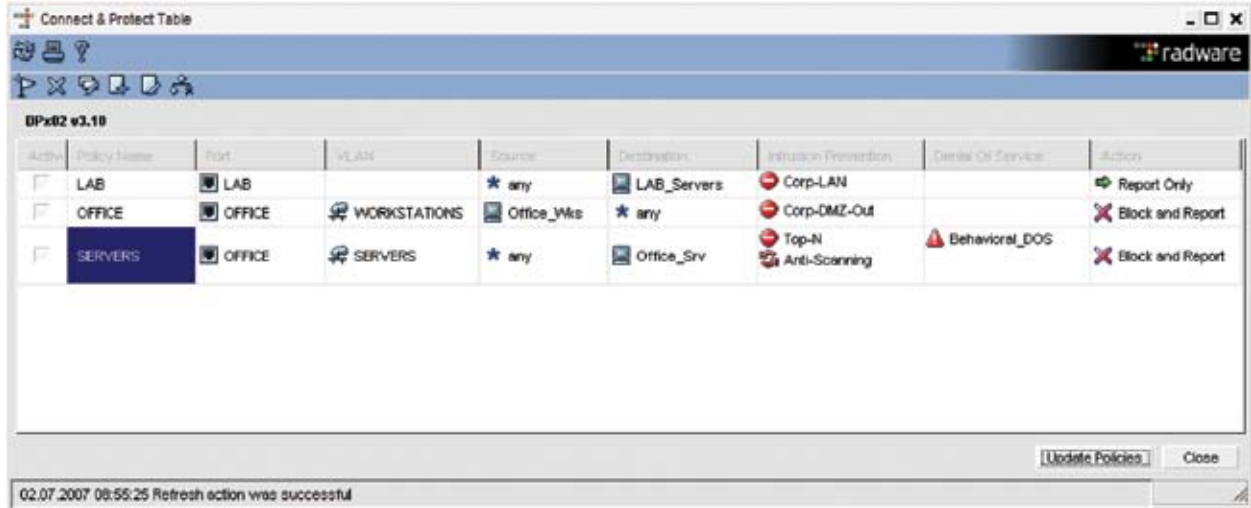


Figure 14 - APSolute Insite Connect & Protect Table

Monitoring

APSObsolute Insite facilitates operations by providing shortcuts through contextual menus, directly available via the right click. It is then possible to get packet traces of an attack, create a new network objects in rules or access an attack signature from a single click (see figure below).

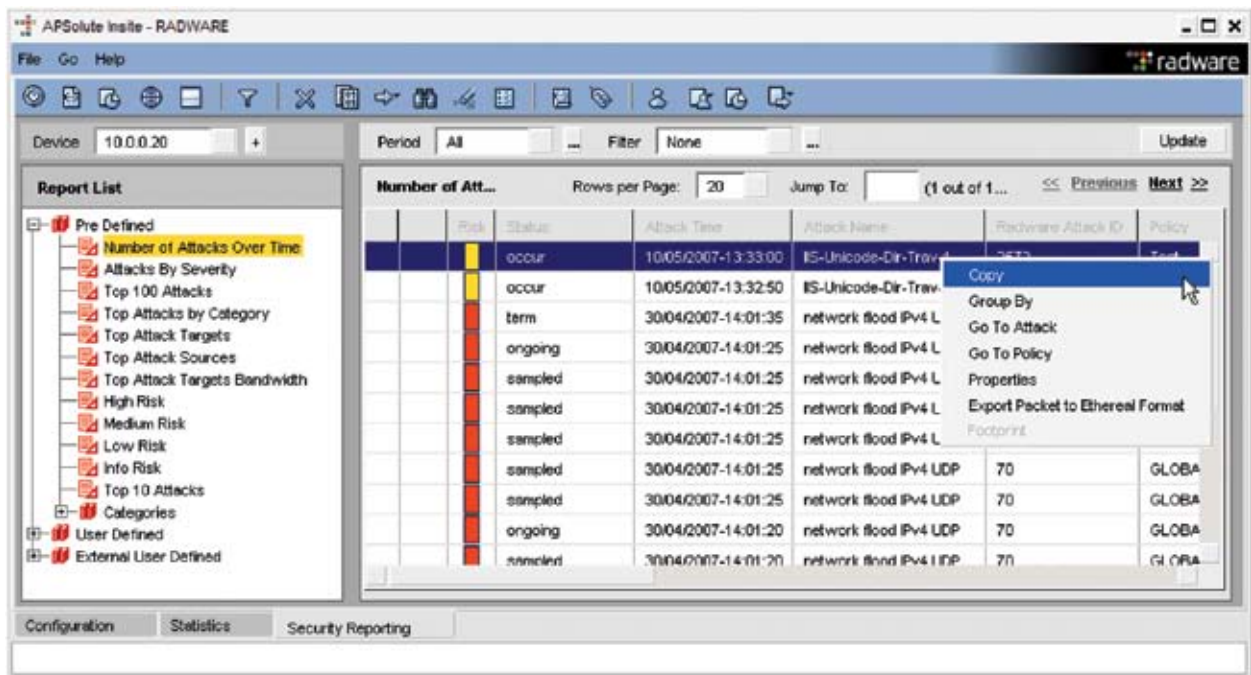


Figure 15 - Example of contextual menu in security logs

Real-time Dashboards

Insite ManagePro provides different interfaces to monitor and investigate security and system events.

“Real-time” interfaces include:

- A generic security dashboard that shows short-term statistics, and most recent attacks
- A top scans interface that shows top scanned IPs and ports as well as most active scanning sources
- A traffic monitoring interface that shows short-term statistics of traffic going through the DefensePro bandwidth, sessions (new and established) and discards
- A map of main attack sources locations around the world
- Web behavioral monitoring tools



Figure 16 - Real-time security interfaces

Reporting Tool

APSObsolute ManagePro provides a wide set of predefined reports and user defined reports in order to facilitate security event investigation and generation of activity reports.

An example of the reporting tools interface is depicted in Figure 17 below: Event logs can be aggregated into groups, filtered for relevant event and presented in graphical view.

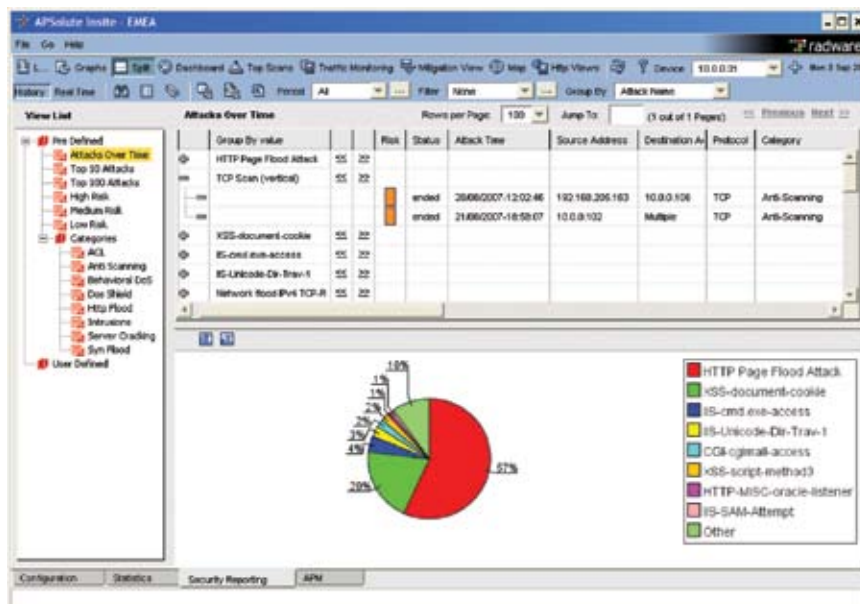


Figure 17 - Generic security reporting

Pre-defined views are available such as: Top attacks, attacks per category etc. However, custom views can be created in order to speed up incident analysis and provide operators with reports they are concerned with.

Attack Reporting of Real-time Signatures

Attack footprints created by the real-time signatures engine and attack traffic that has been blocked accordingly are reported through dedicated interfaces.

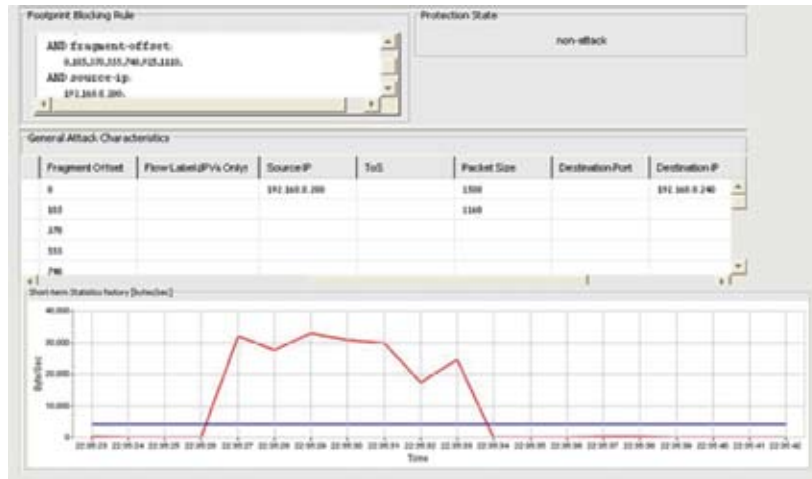


Figure 18 - Behavioral engine reporting

SLA Reports – Bandwidth Consuming Attack Reports

Radware’s Insite management system allows the user to see how much of the attack traffic was mitigated through Attack Mitigation View. This monitoring view is used for the bandwidth consuming attack, such as DoS, network scans, worm propagation and so on.

The graphical representation of the traffic statistics, as provided in the Mitigation view, enables you to see the ratio between all the traffic that passes through the DefensePro device and the traffic that was blocked by the security protections during the attack.

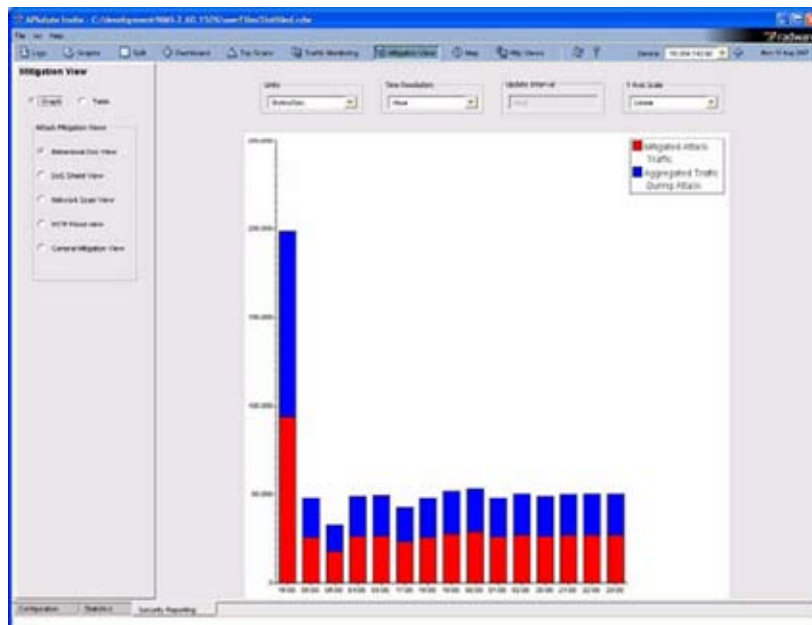


Figure 19 - Mitigation views

Security Management Made Easy

Radware's management system is simple and intuitive for the following reasons:

Real-time Signatures Engine – Radware's advanced algorithms translate human linguistic rules into mathematics. This means that when an administrator decides to intervene with the system's automated operation, it is not necessary to specify arcane thresholds or policies, but rather to select from easy to understand sensitivity levels. The Decision Engine does the rest.

Self-tuned System – an administrator's interaction with the system is usually limited to monitoring system performance and generating reports that detail the types of attacks that have been successfully blocked.

Summary

Signature-based and behavior-based security technologies form a complementary solution that covers more threats than each one is able to cover on its own. A network security product which includes signature, behavioral and automatic signature generation technologies and was designed to effectively divide detection and prevention 'responsibilities' between them, will achieve better security performance over a security product that implements just one technology.

An effective protection against today and tomorrow's network and application level attacks should include the following key capabilities:

Wide Security Coverage – protection should incorporate a multi-layer defense technology that includes network & application layer protections. Known, zero-minute and non-vulnerability based attacks should be confronted through both proactive behavioral-based and signature-based security technologies.

Scalability – the product should be able to work in a high-speed environment with minimal impact on traffic latency. This important capability should be supported through advanced hardware architecture accompanied by advanced security technologies.

Low TCO – maintaining low Total Cost of Ownership forces systems to be more independent of the human factor ("hands-off" system). Relying less on the human factor means that operations that were usually conducted by the security expert are now performed automatically by the systems themselves. This requires advanced expert systems that are integrated into the security systems to generate attack signatures in real-time.

Accuracy – the accuracy of both the detection and prevention technologies that the product has to offer, especially in real-time environments, is paramount. Even low percentages of false positive detections or false preventions render the security product useless.

Radware's DefensePro introduces a Network Intrusion Prevention System that was designed to fulfill all the aforementioned key capabilities. It includes both vulnerability based signature protection against the known attack and exploits, and automatic accurate real-time signature detection and prevention engine that offers a unique value to *automatically create an attack signature for the zero-minute and non-vulnerability based attacks*.

These capabilities position the DefensePro as the definitive solution to repeal the most emerging threats in the network today and in the future.

To read more about Radware's DefensePro, please refer to:

DefensePro x20 & x02 Datasheet and Technical Specifications

<http://www.radware.com/content/download.asp?document=7156>

DefensePro 6000 Datasheet

<http://www.radware.com/content/download.asp?document=6833>

Multi-Layered VoIP Security

http://www.radware.com/content/document.asp?_v=about&document=7490

Bandwidth Management Solution Brief

<http://www.radware.com/workarea/showcontent.aspx?ID=4818>

PCI Compliance Solution Brief

<http://www.radware.com/workarea/showcontent.aspx?ID=5257>

NSS Product Certification Report

<http://www.radware.com/workarea/showcontent.aspx?ID=5407>