radware

Smart Network. **Smart** Business.

Attack Mitigation Solution

Technology Overview - Whitepaper

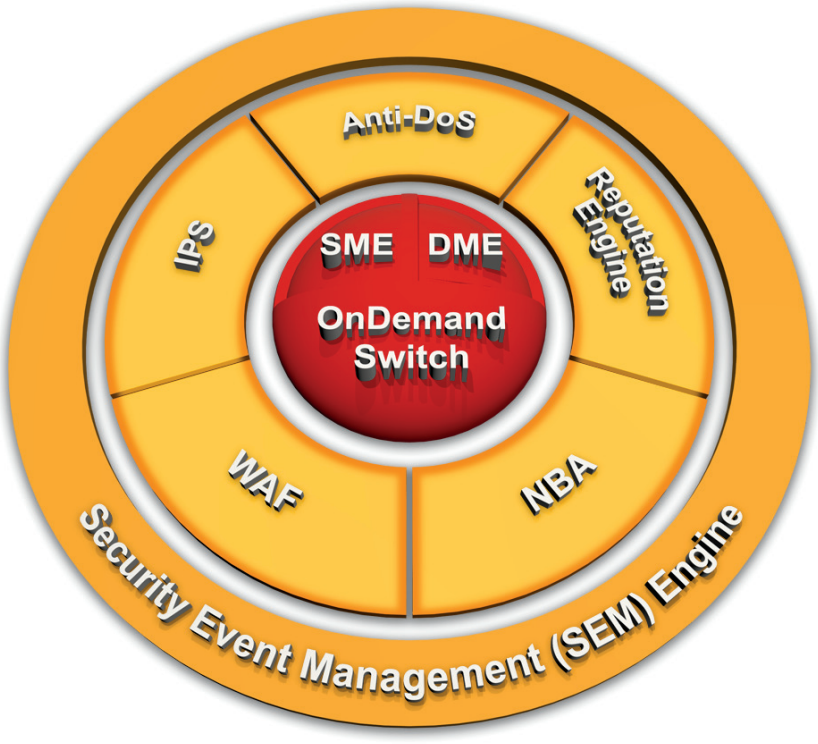


Table of Contents

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 people rely upon instant 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.

Today's threats are dynamic, and not addressed by static signature-based IP 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.

Recent Attack Trends

Recent attacks show that attackers are using new techniques known as multi-vulnerability attack campaigns. During this, the attackers set the Botnet, or instruct their fans (as in the case of Anonymous group operations), to launch several attack types in parallel, targeting multiple vulnerability points of the victim's IT infrastructure such as the network, servers and the application layers. Multi-vulnerability attack campaigns are highly destructive even though each attack vector is well known. For example, UDP flood targets the network bandwidth resources, SYN flood targets the server resources, and HTTP Get flood targets the web application resources. The victim is at high risk — if one attack vector hits the target. The result is destructive. The attackers' assumption is that even if their victims deploy multiple protections tools, there are blind spots in their perimeter network security architecture that expose them to a few of the attack vectors.

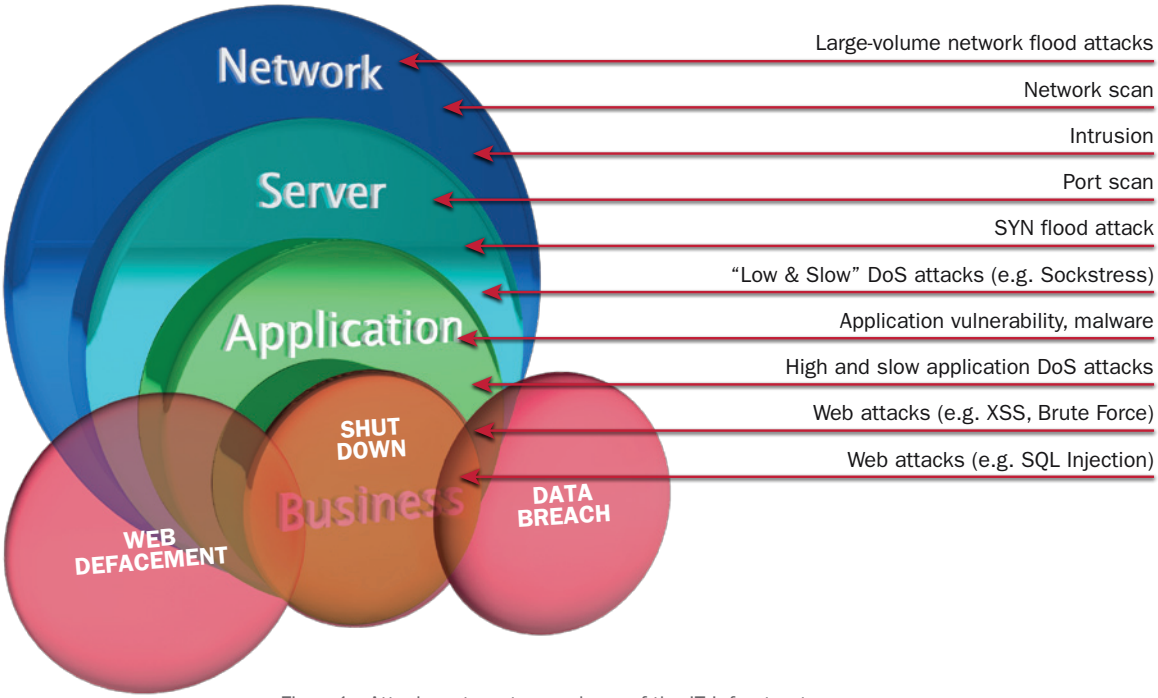


Figure1 : Attackers target every layer of the IT infrastructure

We can split the recent attacks into two main groups of threats: vulnerability based attacks and non-vulnerability based attacks. Vulnerability based attacks are the more traditional types of attacks that are based on previously known vulnerability. If the vulnerability is known, the attack can be blocked using static signatures on the security devices, mainly IPS devices. Non-vulnerability based attacks exploit weaknesses in the victim's infrastructure that cannot necessarily be defined as vulnerabilities. For example, they can be typified by a sequence of "legitimate" events that break authentication mechanisms or misuse the infrastructure resources that lead to resources becoming exhausted, which then stops the service. In recent attacks, we noticed that DDoS attacks are becoming more sophisticated and more persistent. Attack planning has improved, the attack timing is carefully selected, and during the attack period, multiple attack vectors are launched (network, application, and slow rate), until the most destructive one is found. This highlights the need for an attack mitigation solution that can offer both static signature based mitigation and real time signature based mitigation that can respond to dynamic changes in the attacks behavior.

Technological Requirements of the Marketplace

To successfully protect organizations from recent attacks, an effective attack mitigation 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 attack mitigation system needs to quickly adapt to its surrounding, without human intervention.

An effective attack mitigation solution 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 mitigation system must be capable of distinguishing between normal and abnormal behavior, even though the differences between them may be subtle.

In case the attack mitigation system 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. In addition, 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 network 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 ISPs and Telcos).

Network-Based Threats and Risks

The network-based layer of threats includes attacks that misuse network resources. One of the 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 worms and other malware that propagate on their own or can be downloaded by the unaware client, then 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 2011 CSI security survey[1], "bots within the organization" threat was ranked in the fourth place among the 22 different threat categories in the survey. This emphasizes the fact that bots has become a major problem resulting in an increased amount of network DDoS attacks.

[1] The 15th Annual Computer Crime and Security Survey, Computer Security Institute (CSI)

Network attacks typically exhaust network stack resources, router and switches processing capacity, and/or misuse bandwidth resources, all which disrupt the victims' network connectivity.

In addition to the DDoS flood threat, the network layer threats include the "traditional" exploit-based operating system attack vectors. Each common network infrastructure product—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.

Server-Based Threats and Risks

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 misuse the resources of the transport layer in a way that can disturb, deny, or bring down TCP connections, and the application transaction(s) that go with them (for example, 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, which risks the service as well.

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 type 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. While the protection or the software patch is developed, the system is exposed, and any attack during this time period is defined as a "zero-minute"[2] attack. New application vulnerabilities are discovered every day, which adds up to thousands of new vulnerabilities every year.

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

- Buffer-overflow vulnerability types – 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.

[2] In the past these types of attacks were defined as "zero-day" attacks, but now that 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.

- SQL injection vulnerabilities – 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 – 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 by powerful phishing attacks and browser exploits.

- Rootkits – 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 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.

"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.

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, and 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 bots that integrate all of these attack tools into a legitimate infected client machine that will generate all of the previously mentioned server-based threats.

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

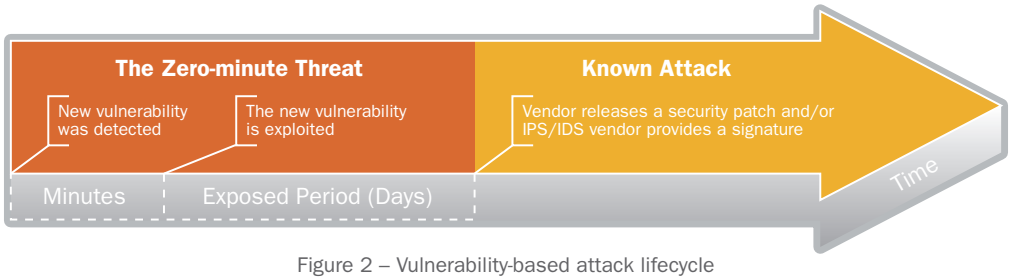


Figure 2 – Vulnerability-based attack lifecycle

Figure 3 – Non-vulnerability based attack lifecycle

The focus of the vulnerability-based attacks life cycle (Figure 2) 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, or 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 exposed to client-based exploits due to new mobility options for clients (for example, the mobile users).

Mobility and the Disappearance of the Network's Perimeter

In recent years, companies' mobility in the global environment has caused the network perimeter, which is usually protected by gateway security devices, to "disappear" and it is more difficult to maintain a secured network. Phones and tablets for example, use operating systems and applications that include client application vulnerabilities which can be exploited in a similar way to laptop computers and PCs. Therefore, employees who are frequently out of the office and use laptops and phones are often the unwitting malware carriers of bots, worms, and Trojans. These malwares are carried into the organization by company employees who bring their infected laptops 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 using the internal network computerized resources as part of a botnet for hire in order to attack third party organizations. As mentioned earlier, according to the 2011 CSI security survey, the "bots within the organization" category of threats was ranked in the fourth place among 22 different ranked threat categories. The reason for this high rank is that it has become easier to infect clients with bots. 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, 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 and denial of service 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 victims' 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 – Rootkits are programs 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 action (for example, a computer virus). Trojans are used to steal information, run applications, or provide unauthorized access to the system.

- Financial fraud attacks – Attackers are using social engineering tools and malware spread in order to trick users to disclose sensitive financial information (phishing), or perform man-in-the-browser attacks (such as Zeus Trojan), that result with keystroke logging and form grabbing. The malware spread is performed by tricking users to access infected sites (also referred as "bad reputation" sites), that scan the user hosts for known application vulnerabilities and then exploit them to install unwanted malware such as Trojan horses.

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. This significantly raises the detection challenge for signature-based detection solutions.

Radware's Attack Mitigation System

Introduction

Protecting the application infrastructure requires deployment of multiple prevention tools. Radware's Attack Mitigation System (AMS) is a real time network and application attack mitigation solution that protects the application infrastructure against network and application downtime, application vulnerability exploitation, malware spread, information theft, web service attacks, and web defacement.

Radware's Attack Mitigation System contains three layers:

- **Protections layer** – A set of security modules including: Denial-of-service (DoS) protection, Network Behavioral Analysis (NBA), Intrusion Prevention System (IPS), Reputation Engine and Web Application Firewall (WAF), which fully safeguard networks, servers, and applications against known and emerging network security threats
- **Security risk management** - Built-in Security Event Information Management (SEIM) collects and analyzes events from all modules to provide enterprise-view situational awareness
- **Emergency Response Team (ERT)** - Consists of knowledgeable and specialized security experts who provide 24x7 instantaneous services for customers facing a denial-of-service (DoS) attack in order to restore network and service operational status

When compared to stand-alone solutions deployment, the synergy of multiple protection modules at part of one system enables more effective protection against attackers who seek to systematically compromise business assets. Multiple protection modules also provide unified reporting and compliance.

AMS Protection Modules

AMS is comprised of five protection modules that are well optimized for online business and data centre protection as well as carrier environments:

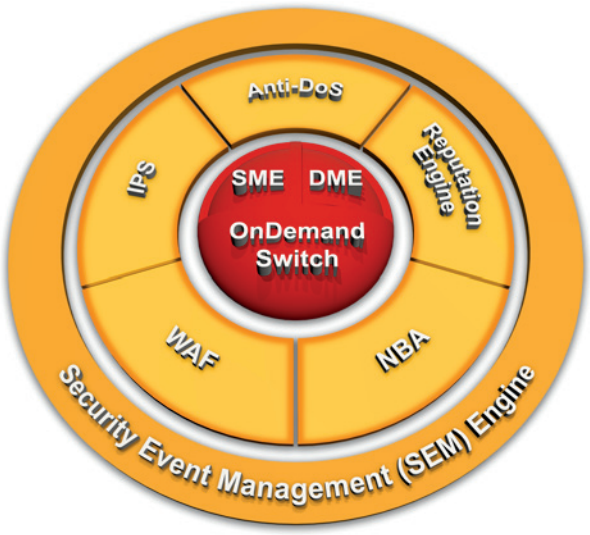


Figure 4 – Radware Attack Mitigation System

DoS Protection – Prevent all type of network DDoS attacks including UDP flood attacks, SYN flood attacks, TCP flood attacks, ICMP flood attacks, IGMP flood attacks, and Out-of-state flood attacks.

NBA – The network behavioral analysis module prevents application resource misuse and zero-minute malware spread. Users are protected against the following attacks: HTTP page flood attacks, DNS flood attacks, SIP flood attacks, brute force attacks, network and port scanning, as well as malware propagation.

IPS – This module protects against application vulnerabilities and exploits, OS vulnerabilities and exploits, network infrastructure vulnerabilities, malware (worms, bots, Trojans and drop-points, and spyware), anonymizers, IPv6 attacks, and protocol anomalies.

Reputation Engine – Protects against financial fraud, Trojan, and phishing attack campaigns. This feature is based on third party real time IP reputation feeds.

WAF – Radware's WAF module secures web applications and enables PCI compliance by mitigating web application security threats and vulnerabilities. It prevents data theft and manipulation of sensitive corporate and customer information.

Cutting-edge Security Technologies

Radware AMS uses multiple technologies to provide complete attack protection for online businesses, data centers and networks:

- The **DoS Protection** module is based on several technologies: signature detection, behavioral based real time signatures, and a SYN cookies mechanism that challenge new connections prior to establishing a new session with the servers.

- The **Network Behavioral Analysis (NBA)** module employs patented behavioral-based real time signature technology. It creates baselines of normal network, application, and user behavior. When an anomalous behavior is detected as an attack, the NBA module creates a real time signature that uses the attack characteristics and starts blocking the attack immediately. In case of DDoS attacks, it injects the real time signature into the DME hardware, offloading the main CPUs from the excessive unwanted traffic.

- The **Intrusion Prevention System (IPS)** module is based on stateful static signature detection technology with periodic signature updates, and emergency updates in cases of newly discovered high risk attacks.

- The **Reputation Engine** offers real time anti-Trojan and anti-phishing service, targeted to fight against financial fraud, information theft, and malware spread.

- The **Web Application Firewall (WAF)** offers patent-protected technology to create and maintain security policies for the widest security coverage with the lowest false positives and the lowest operational effort. The WAF auto policy generation module analyzes the security related attributes of the protected web application and derives the potential threats in the application. The web application is mapped into an application zone, each with its own common potential threats. It then generates granular protection rules per each zone, and sets a policy in blocking mode once it has completed an optimization process that minimizes false-positives while maintaining the best security coverage.

Security Risk Management Best-of-breed Reporting, Forensics, and SIEM Engine

The built-in Security Information Event Management (SIEM) system provides an enterprise-wide view of security and compliance status from a single console. Data from multiple sources is collected and evaluated in a consolidated view of dashboards and reports. These views provide extensive, yet simple, drilldown capabilities that allow users to easily drill into information to speed incident identification and provide root cause analysis, which improves collaboration between NOC and SOC teams, and accelerates the resolution of security incidents.

The SIEM provides complete alignment with the enterprise's compliance, regulations, and business processes, providing compliance and audit professionals with a comprehensive picture of compliance across the enterprise. It ensures the appropriate separation of duties, collection of information, configuration, and operation auditing mandated by business processes, regulations, and information security standards (PCI-DSS, SOX, HIPAA, etc).

Full Alert Lifecycle Management

The SIEM provides IT managers with a rich set of tools to manage all the alerts (availability, performance, security, and more) within their infrastructure. Alerts are managed from the moment they surface (identification stage), through ticket opening, analysis, resolution, and verification until the problem is resolved and summarized.

Deploying AMS in Your Network

Security attacks are a risk to all types of organizations. Online businesses must secure their service data center to guarantee their business. Medium to large enterprises must protect their headquarters and regional centers to guarantee ongoing enterprise IT services. Service providers and hosting providers must protect their customers'

hosted services, their customers' network access pipes, and their own peering and core pipes to guarantee their service level agreements with their customers.

Figure 5 below describes a typical deployment model of AMS protecting the business infrastructure within enterprises, online businesses, and service providers who wish to protect their own infrastructure.

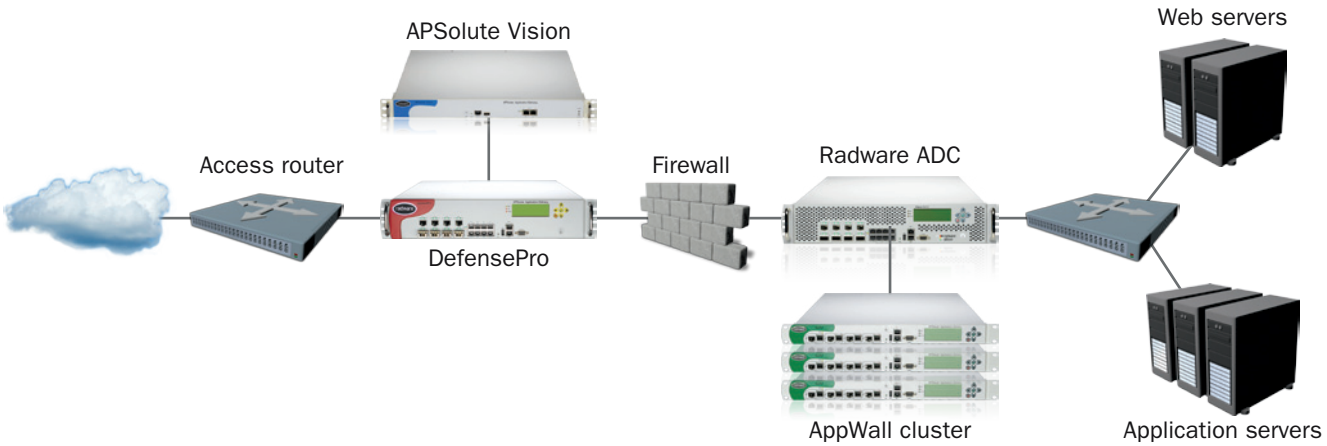


Figure 5: Typical Deployment of AMS protecting the business infrastructure

Figure 6 below describes a typical deployment of AMS as a service provider who wishes to offer security-as-a-service for its customers.

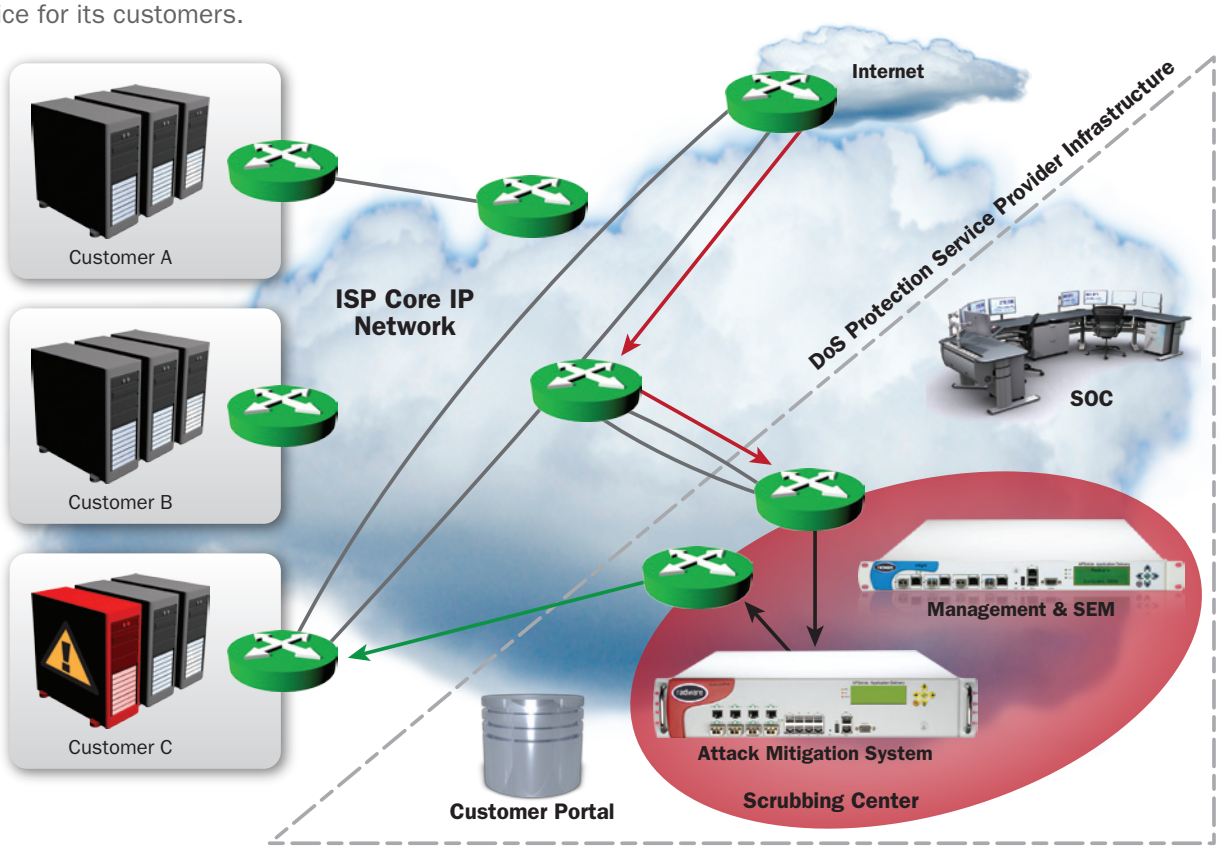


Figure 6: Typical deployment of AMS at service providers offering security-as-a-service

Intelligently Embedding Radware's 'On Demand' Strategy

By embracing Radware's "pay-as-you-grow" approach, customers only pay for the exact capacity currently required. This prevents over-spending on the initial solution, while benefiting from top performance of a high-end platform. Additional throughput capacity can be added on demand to meet new business requirements, with no forklift upgrade of the device, and without even restarting it. The pay-as-you-grow approach enables organizations to overcome capacity planning challenges, and reduces the risk associated with business growth for best investment protection. Additionally, Radware provides an exclusive five-year platform longevity guarantee, which results in extended project lifetime and accelerated ROI.

The AMS Brain: A Technology Overview

As discussed in the previous section, the main security technologies deployed in AMS 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.

NBA & Anti DoS Modules Technology Overview

Two main patented technologies are responsible for AMS's network and application behavior analysis, and for the Anti-DoS modules:

- Fuzzy Logic expert detection and real time signature generation technology
- Advanced action escalation technology

Fuzzy Logic and real time signature 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 the attack-blocking stage, and removing the signature once attack is over.

Advanced Action Escalation Technology

This mechanism works in conjunction with the real time signature and closed feedback modules.

The main idea behind this escalation approach is to first detect suspicious users (through the real time signature generation module) and second, to start and activate a set of actions beginning with the most "gentle" one that will have negligible, if any, impact on the legitimate user. Based on a closed-feedback loop, the system will decide if escalating to a more aggressive action is required.

The approach aims to minimize the impact on the human user experience while presenting a more accurate and adaptive response to the artificial users (for example, a bot). This automatic process allows the system to automatically tune the countermeasure's actions based on the detected level of risk. This dynamic action per level of risk also improves the protection system resistance against reverse engineers.

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 characteristic 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 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 processes many parameters, decides about their degree of anomaly, and correlates between them to reach conclusions in real time. Using Fuzzy Logic as a decision engine, Radware's AMScan perform more in-depth traffic analysis and come to conclusions quicker than any other traditional method.

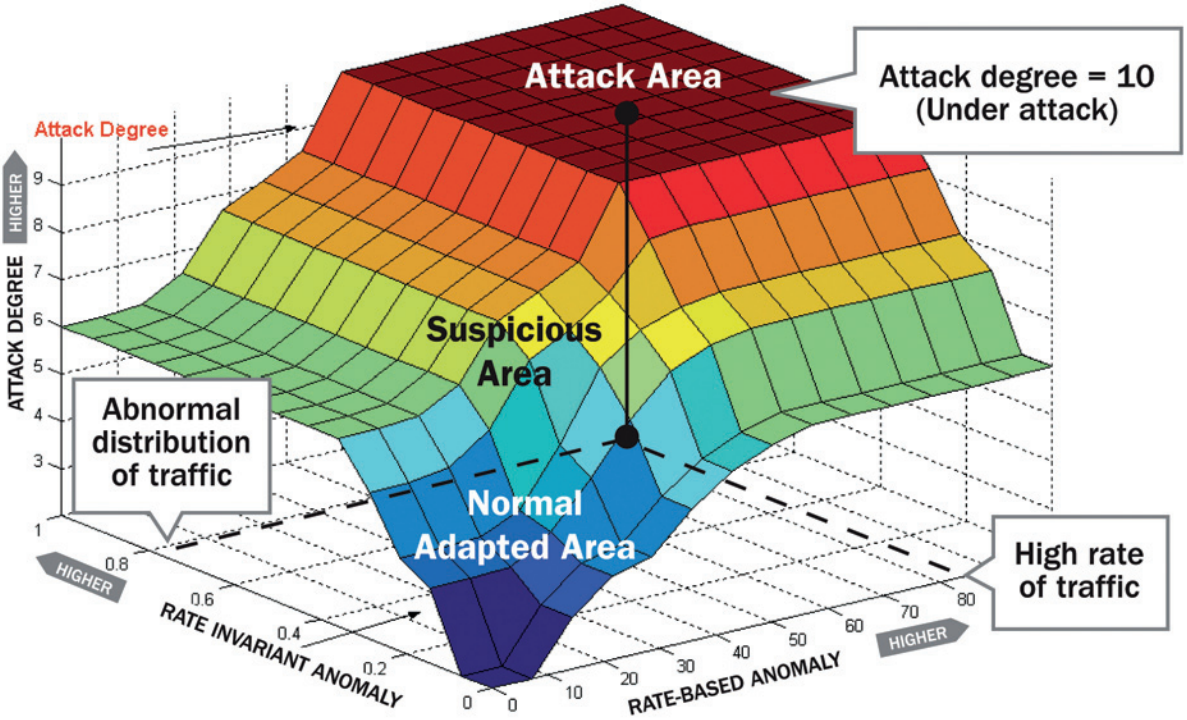
The Fuzzy Logic module includes adaptive capabilities and the sensitivity of the module is being continuously tuned to match the characteristics of the protected network. The adaptive algorithms include IIR (Infinite Impulse Response) filters that continually average traffic parameters and shape the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

These capabilities allow the Radware's IPS to continuously establish normal behavior baselines according to the date and the time of day, and depending on the behavior of the protected site.

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" follows this section and 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 7: Fuzzy Logic Decision Surface

The Fuzzy Logic decision surface (illustrated in the Figure 7), 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.

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 a challenge to block the attack without simultaneously blocking legitimate traffic.

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. Radware developed a probability theory, a unique patent-pending implementation method, that distinguishes between expected and unexpected repetition of parameters. These parameters were studied (statistically) according to the network environment, and the automatic signature generation mechanism flags unexpected values as "possible" pieces of the attack signature that represents the ongoing detected anomaly.

"A major concern in deploying an in-line device is the blocking of legitimate traffic. Once we had configured the appropriate trusted hosts and the device had finished its learning process, the DefensePro completed all our tests without raising a single false positive alert."

NSS Labs, 2010

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 Qcount
- DNS Qname

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 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 by using the 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***: 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.

Advanced Action Escalation Mechanism
The AMS's action escalation allows the system to adapt its action to the ongoing risk, which provides automatic risk management as intended by the network and application security expert (an expert system that emulates the human security experts decision process in real time).

Detection and real time signature creation:
At this stage, the AMS uses its adaptive fuzzy logic engine to detect the attack and creates a real time signature using the real time signature generation module. The real time signature is a pattern that characterizes the ongoing attack activities.

Advanced action escalation process:
At this stage, the system starts to enforce counter measure actions in order to accurately mitigate the attack. Actions apply to the suspicious users only (those that match the RT signature).

As mentioned before, the advanced action escalation technology is designed to minimize the impact on the human user experience, while presenting a more accurate and adaptive response to the uses behind the detected threat.

The action escalation mechanism will initiate a set of actions, beginning with the most "gentle" one (e.g., a syn cookie) that will have negligible, if any, impact on the legitimate user (in case the user was accidently matched to the RT signature). Based on the closed-feedback loop mechanism, the system will decide if an escalation into a "stronger" action is required. The following is a more specific example for this mechanism:

a. The mitigation engine only intercepts the sessions which originate at the suspicious source and replies back with a "weak" challenge option. A weak challenge can be considered a redirect HTTP command that forces real browsers to re-initiate their requests automatically. A simple bot will fail to respond correctly.

b. If the suspicious source responds correctly but continues to generate suspicious activities, it means a more advanced tool is behind the operation (if not, then the suspicious flags that were raised were probably false alarms and the human user will be able to continue his activity on the site);

c. The mitigation engine raises the level of the challenge to include some customized JavaScript that forces the suspicious user to download and process the object. Most of the advanced bot tools will fail to respond correctly, and will be blocked;

d. In case the user responds correctly and suspicious activities are still identified, then the system can either generate a rate limit rule or a full blocking rule. In any case, the action will apply only to users who match the RT signature.

The main benefit of this process is that it allows an accurate mitigation process with minimal impact on the user experience. It also presents an adaptive response aimed at dealing with the dynamic nature of behavior types that today's and tomorrow's attackers may choose to use. Lastly, most actions described above do not require the human user to go through any disruptive tests.

An illustration of the closed-feedback loop mitigation process can be seen in Figure 8 below:

Figure 8

The above actions show how AMS is used against HTTP based attacks. Other mitigation options will be used in case other types of attack are detected (e.g., UDP based attacks, DNS attacks etc), but the main idea is to follow the closed-feedback loop and action escalation mechanism, ensuring minimal impact on the user experience, while maintaining a high level of effectiveness in mitigating the emerging threats.

Deterministic Security Technology Modules – IPS Module Technology Overview

Up until now, we have described Radware's behavioral based engine however, even today, many threats simply violate stateful protocol rules, applications rules, or are exploiting known application vulnerabilities. These threats can be precisely removed through a pre-defined attack signature that was the developed by vulnerability research groups, or by enforcing deterministic protocol compliancy rules. For these purposes, the following deterministic security modules are deployed in DefensePro:

A security device that combines IPS signature-based approaches with advanced behavioral technology will have an advantage over signature-based technology alone.

For the more deterministic threat types, such as known application vulnerability exploitation attacks in which a signature is already available, AMS provides a proactive security update service that automatically downloads recent attack signatures to the system's attack database. DefensePro inspects the traffic and compares each packet in real time to the signatures in the database. Radware's hardware accelerated string match engine is used for this purpose.

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

To support the IPS module, the AMS provides a proactive security updates service that automatically downloads recent attack signature to the IPS module 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 ensures that 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 customers' 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 evens such as BlackHat. Radware SOC was the first to discover application vulnerabilities in SIP applications and the Apple iPhone Safari web browser, and issued immediate protections for critical Microsoft vulnerabilities, and more.

For more information on Radware's SOC, please visit the Radware security zone site:
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 for database 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 e-commerce and banking sites.
- **IPv6 attacks** – Protecting against IPv6 protocol vulnerabilities.
- **SSL-Based Attacks** – Protection against encrypted, SSL-based attacks.

The Web Application Firewall Module

Radware's WAF module secures web applications and enables PCI compliance by mitigating web application security threats and vulnerabilities. It prevents data theft and manipulation of sensitive corporate and customer information.

The WAF module provides protection against the following web application attacks:

- **Full coverage out-of-the-box of OWASP top-10 threats** – Including injections, cross site scripting (XSS), cross site request forgery (CSRF), broken authentication and session management, and security mis-configuration.
- **Data leak prevention** – Identifying and blocking sensitive information transmission, such as credit card numbers (CCN) and social security numbers (SSN).
- **Zero-day attacks prevention** – AppWall positive security profiles limiting the user input only to the level required by the application to properly function, thus blocking also zero day attacks. The positive security profiles are a proven protection against zero-day attacks.
- **Protocol validation** – AppWall enables HTTP standards compliance to prevent evasion techniques and protocol exploits.

---

[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.

- **XML and Web services protection** – AppWall offers a rich set of XML and web services security protections, including XML validity check web services method restrictions, XML structure validation to enforce legitimate SOAP messages, and XML payloads.
- **Web application vulnerabilities** – Signature protection offers the most accurate detection and blocking technology of web application vulnerability exploits. AppWall negative security profiles offers comprehensive attack protection.

The WAF module is based on positive and negative security policies:

- Positive security policies are based on behavioural analysis technology. The security technology learns what the possible inputs per each web page are and what the typical values per each input field are. It then locks the policy to the allowed ranges of values.
- Negative security policies are based on static signature detection technology. The WAF module stores a signature file that covers thousands of known application vulnerabilities and exploits that are checked against every user transaction. Once a signature match is found – the session is terminated and the attack is blocked.

The WAF module offers patent-protected technology to create and maintain security policies for the widest security coverage with the lowest false positives and lowest operational effort. The WAF module uses a four step flow to create and maintain security policies:

Step 1 – Application mapping

The WAF model learns the web application and maps the application pages into application zones or paths. For example, admin pages are allocated into an admin application path, dynamic content pages are allocated into another application path, registration pages into a third application path, etc. The application mapping is performed passively or actively using an embedded web crawler.

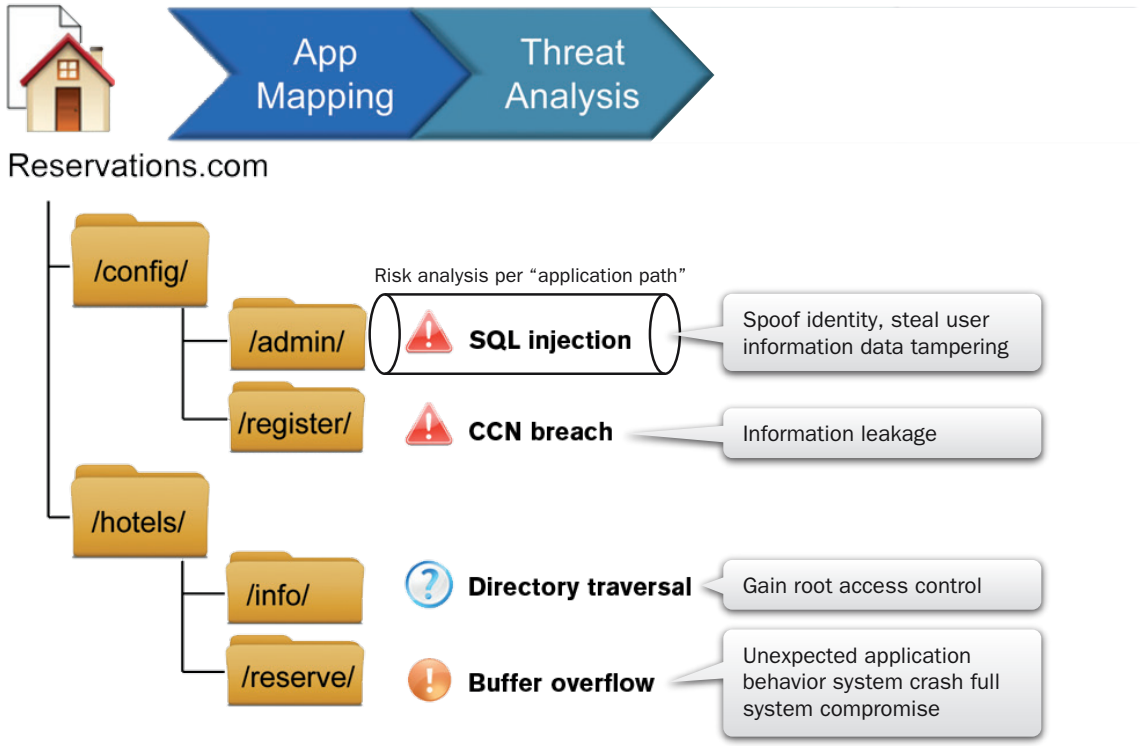


Figure 9

Step 2 – Threat Analysis

Once the WAF module has completed the application learning and mapping, it performs a risk analysis per each application path. The result of the risk analysis is an association of relevant web threats per path. For example, an admin path should be protected against attacks that aim to steal user information, create false user accounts or tamper with user account data; the dynamic application-path should be protected against buffer overflow attacks that could lead to remote code execution, unexpected application behavior, and full system compromise.

Step 3 – Policy Generation

In this step, the WAF module automatically generates granular security policies per each application path. Typically, admin paths and static pages paths will be assigned with negative security policies, while dynamic content application-paths will be assigned with positive security policies.

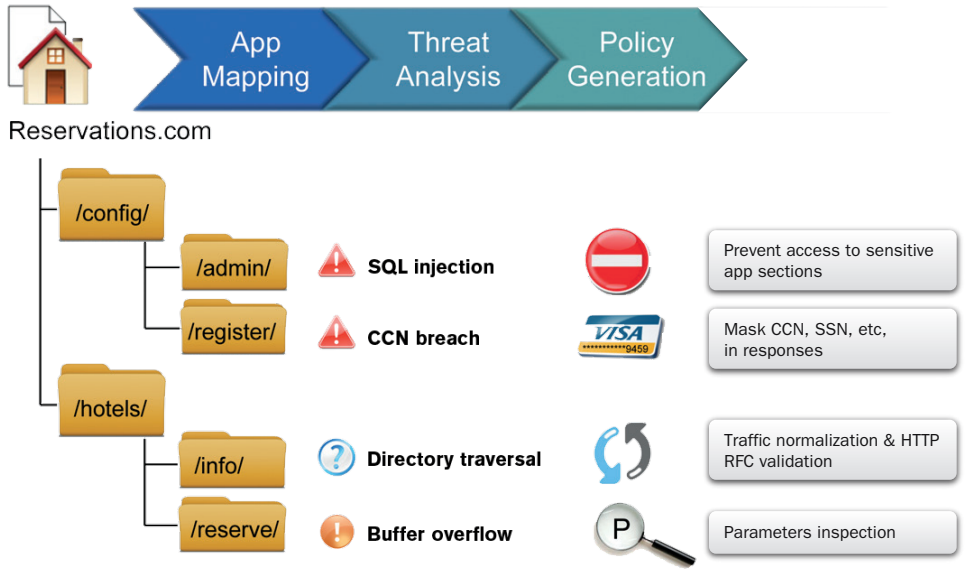


Figure 10

Step 4 – Policy Activation

The last step is used to optimize the security policies to maintain maximum coverage while reducing false-positives and improve the system performance. The WAF module optimizes the negative security policies (based on application vulnerability signature detection technology), by learning what attacks the application-path is vulnerable to, and removes unnecessary signatures. The result is full-attack coverage while reducing false-positives due to non-relevant signatures. For the positive security policies, the WAF module performs the parameter inspection and learning per field in every application page. Once learning is completed, it locks the learned values and any parameter value exceeding the learned ranges will be detected as an attempt to attack the application.

Benefits of the Adaptive Policy Generation Technology:

- Best security coverage
  - Auto detection of potential threats
  - Other WAFs require admins intervention and knowledge to protect
- Lowest false-positives
  - Adaptive security protections optimized per application resource (“app- path”)
  - Other WAFs auto generate global policies
- Shortest time to protect
  - Highly granular policy creation and activation (“app-path”)
  - Immediate policy modification upon application change
  - Other WAFs wait upon global policy activation
- Reduced cost of ownership
  - Automatic real time attack mitigation with no need for human intervention

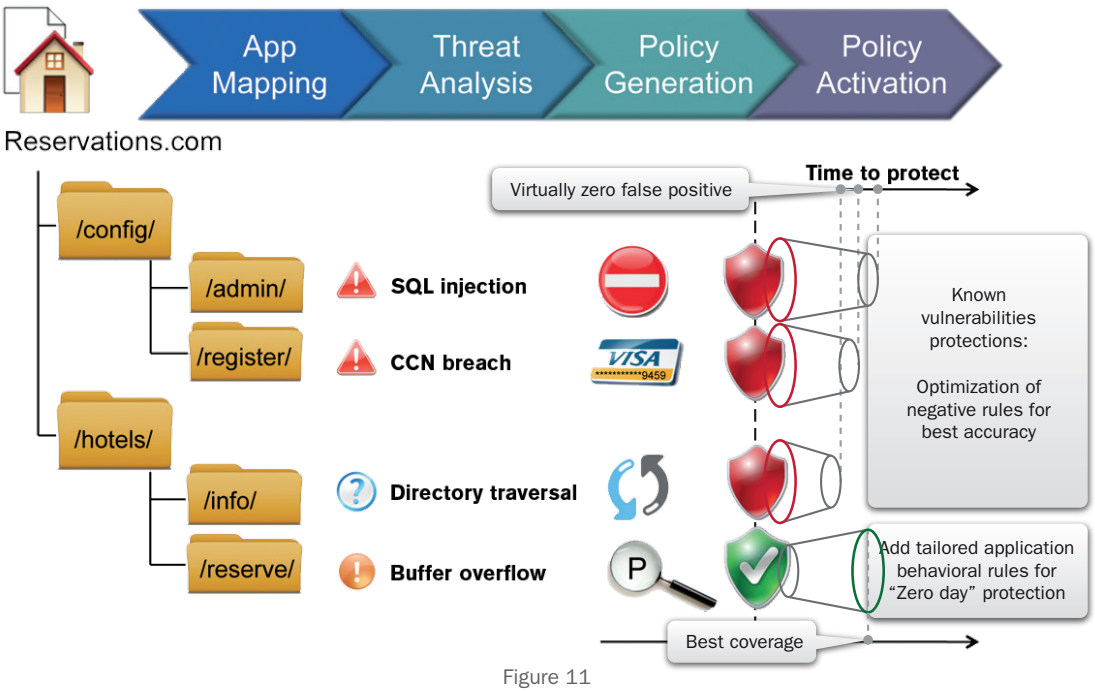


Figure 11

Reputation Engine

The reputation engine is a module that receives external feeds and translates them into real time signatures which are then injected to the AMS systems in real time. The reputation engine has been integrated with the RSA FraudAction service.

RSA FraudAction is a proven service that stops online phishing, pharming, and Trojan attacks. With its 24x7 monitoring and detection using real time signature feeds, FraudAction protects organizations and users by preventing and blocking access from online threats including:

- Identified phishing sites
- Identified infected sites and sites that have been compromised and may therefore spread unwanted malware
- Identified Trojan dropping points

For more information about the RSA FraudAction service, please visit:
http://www.emc.com/security/rsa-identity-protection-and-verification/rsa-fraudaction.htm.

Hardware Architecture That was "Tailored" for Attack Mitigation

Each layer and module of defense in the AMS is supported by hardware architecture that was designed to maximize the protection performance.

DME – DoS mitigation engine

The DME is a dedicated network processor that was optimized to perform L3 and L4 filtering operation at a rate of 12 Million PPS.

SME – String Match Engine

The string match engine is a hardware ASIC-based component that supports the IPS module. The solution is capable of multi-gig L7 (application layer), and deep packets for full content inspection. This includes inspection of attack signatures that span across multiple packets (i.e., support cross packet inspection), or inspection attack signatures that can only be written through regular expressions in order to avoid false positive or false negative events.

Multi-purpose CPU's
The other protection layers and network based operations are done by mutli-purpose CPUs which provide the required flexibility and scalability for the more standard operations, such as stateful and statistical analysis which are part of the behavioral analysis modules.

Hardware Architecture That was "Tailored" for Attack Mitigation
The main advantage of AMS's hardware architecture is its ability to completely separate the mitigation tasks, each one in a different dedicated hardware component, thus preventing internal resource "cannibalization" that typifies other attack mitigation products.

Repelling the multi-million PPS L3-4 DDoS attack is done solely by the DME hardware component while attacks that need to be mitigated through DPI (Deep Packet Inspection) utilizes the L7 Regex acceleration ASIC. At the same time, legitimate traffic that should continue to be processed by the stateful analysis modules and to feed the statistical analysis modules in the system is being processed by the multi-purpose (multi-cores) CPU's.

This hardware architecture provides higher and more predictable performance figures than other attack mitigation systems.

Security Management, Monitoring, Reporting, and SIEM Engine

Introducing APSolute Vision

Radware APSolute Vision provides a highly available, single point of access for network and security administrators to centrally manage distributed Radware devices and monitor the health, real-time status, performance and security of enterprise-wide application delivery infrastructures.

APSolute Vision consolidates the monitoring and configuration of several Radware devices across multiple data centers. By removing the need for deploying management appliances in multiple data centers, it reduces IT CAPEX and OPEX, and simplifies data center management.

APSolute Vision continuously monitors the system and will send an alert if there is any degradation of business continuity or performance in the entire infrastructure. It provides the following benefits:

- Up-to-date information, and improved business continuity service.
- Effective application delivery and security capacity planning.
- Shorter time frame required to resolve business continuity issues.
- Minimized impact of service downtime on the enterprise's business.

APSolute Vision is a specifically tailored unified management and monitoring application for application delivery and network security devices. It supports all aspects of management: initial device setup, ongoing maintenance, SSL certificate management, reporting, forensics, and more. It also provides central storage of vital device information, allowing IT managers to easily find hardware platform details, software versions, serial numbers, etc. This eliminates manual tracking of critical device information, and reduces errors.

Real-Time Threat Identification, Prioritization, and Response

APSolute Vision provides an enterprise-wide view of security and compliance status from a single console.

Data from multiple devices is collected and evaluated in a consolidated view of dashboards and reports. These reports—viewable from a secure portal or exported in HTML, PDF, CSV, etc.—provide extensive yet simple drilldown capabilities that allow users to easily access information in order to expedite incident identification and provide root cause analysis. This improves collaboration between NOC and SOC teams, and accelerates the resolution of security incidents.

APSolute Vision provides real-time monitoring and alerts on policy violations, non-standard processes, rogue applications, potential financial fraud, identity theft and cyber-attacks.

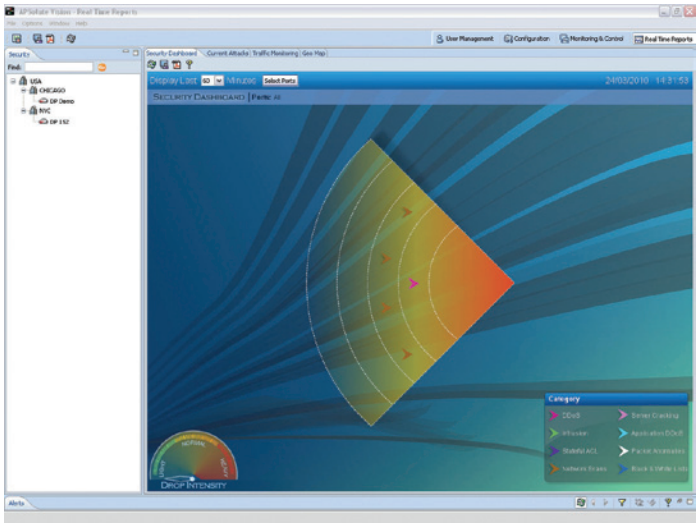


Figure 12: The real-time sonar view allows you to see current attacks in your network. High risk attacks are located closer to the sonar transmitter. The side meter indicates the drop intensity of attack traffic.

Per User Dashboards and Report Customization

APSolute Vision allows users to fully customize real-time security dashboards and historical security reports. This ensures a complete network security view at a glance, which provides the specific information needed to take action, and reduces the amount of drill-downs required to access information.

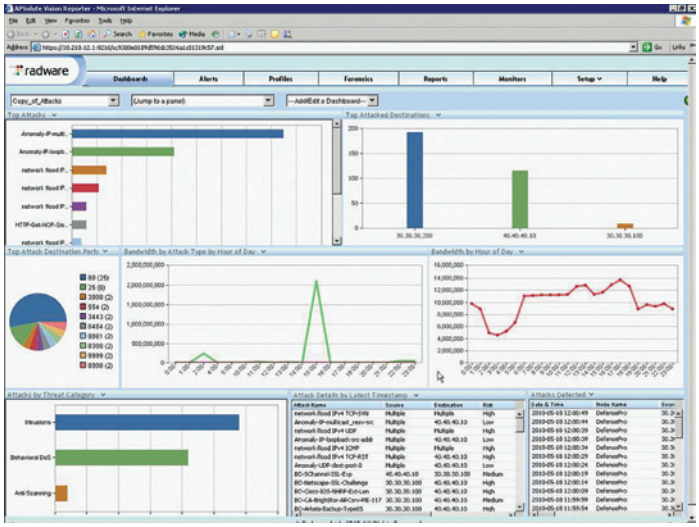


Figure 13: The security dashboard displays multiple attack reports in a single view, customizable per user.

Advanced Security Forensics Engine

APSolute Vision provides an easy-to-use search engine that allows users to quickly sort through large volumes of archived log, vulnerability, and attack data. Forensics analysis helps users isolate attack vectors, investigate security breaches and position appropriate defenses in place by detecting anomalies, identifying policy violations, and displaying a chronological order of malicious activity.

Complete Alignment with Enterprise Compliance Requirements and Regulations

APSolute Vision provides complete alignment with the enterprise's compliance, regulations, and business processes, providing compliance and audit professionals with a complete picture across the enterprise. It ensures the appropriate separation of duties, collection of information, and operation auditing mandated by many regulations and information security standards (PCI-DSS, SOX, HIPAA, etc).

Through enhanced role-based access and logging capabilities, APSolute Vision ensures all actions across the application delivery and security infrastructure are logged and performed only by authorized personnel.

In addition, APSolute Vision segregates statistical and performance data to support job-specific views, dashboards, analysis, and reporting. While executives may desire to view high-level summary reports, IT professionals can easily drill into more complex monitoring, reporting, and forensics detail.

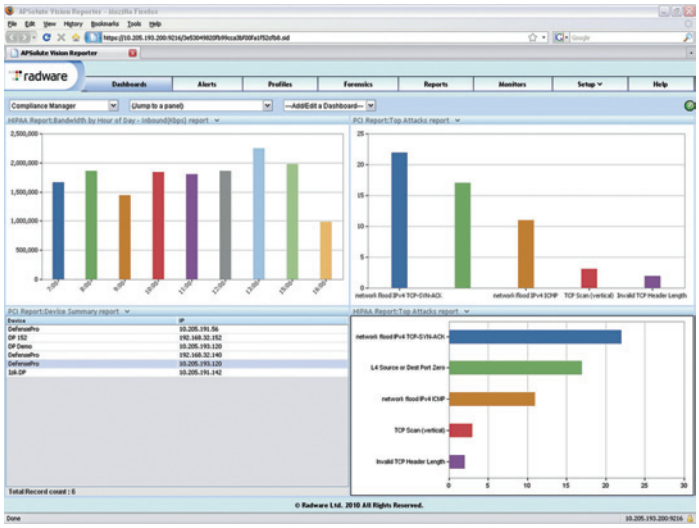


Figure 14: Create job specific dashboards, such as a compliance manager dashboard containing compliancy information on different regulations.

Summary

Cyber activists and motivated attackers are getting more sophisticated, initiating multi-vulnerability attack campaigns that make mitigation very difficult. No single protection tool is effective against the broad range of attacks that target every layer of the IT infrastructure – the network layer, the servers' layer, and the applications' layer. With the Radware Attack Mitigation System, online businesses, data centers, and service providers can ensure the security of their online presence, and maintain productivity thanks to the following solution benefits:

- Radware AMS is the only solution that can truly defend against emerging cyber attack campaigns that target all IT infrastructure layers.
- The Emergency Response Team (ERT) offers rapid assistance to customers under attack, and ensures their business is up at all times.
- AMS offers the lowest cost OpEx and CapEx solution in the industry.

© 2012 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.