Stopping Internet Threats Before They Affect Your Business by Using the IBM Security Network Intrusion Prevention System

Redguides

for Business Leaders

Axel Buecker
Diogo Bulhoes
Matthew Dobbs

- Examination of today’s IT network perimeter security and its impact on business transactions
- Introduction of the IBM Security Network IPS components and deployment architecture
- Presentation of a typical customer scenario with a solution that meets the challenge

Executive overview

In this IBM® Redguide™ publication, we look closely at network-related security risks such as targeted attacks, worms, bots, intrusion attempts, phishing scams, and so on. These threats target vulnerabilities in IT systems, workstations, and applications and can have a crippling financial effect on all organizations, disrupting business processes, and causing loss of confidential and proprietary information.

To better understand how these threats are targeting your organization, we examine the composition of today's IT network perimeter, which has been diluted from a well-defined set of ingress and egress points to a mesh of undetectable flows from devices that are capable of accessing and penetrating every organization's resources. The days of keeping the attackers out by building a well-defined wall are definitely over. Businesses and organizations require collaboration with internal and external business partners, customers, and employees, which further removes walls and protective barriers.

After identifying these increasing threats, we describe how the IBM Security Network Intrusion Prevention System (IPS) can help you consolidate intrusion prevention with data and web application security into a single, optimized appliance for faster, more accurate security protection. The hardware appliance is preloaded and preconfigured with IBM security software and extends the capabilities of the IBM X-Force® research team, to address high-performance network security.

The audience for this guide includes business leaders, decision makers, network managers, IT security managers, and IT and business consultants.

IT network perimeter security: A primer

IT perimeter security is a broad term that has a diverse set of implications and meanings. Misunderstanding the nuances that are implied by the term is common.

At the beginning of the digital computer age, computer systems were single stand-alone entities, located in a physically secured room known as the *machine room*. Input and output media were hand-carried to and from the room or handled at the *remote job entry* (RJE) location. Both the machine room and the RJE were subject to the physical security and access controls in place at the given location. Because the computational centers were located in well-defined locations, identifying sources of entry was easy. Therefore, historically, the phases evolved as described in this section.

The perimeter was well-defined, and security could be enforced on a physical level.

The next phase of computing introduced terminals, where a keyboard and monitor were wired directly to the central computer system. With this approach, input could be submitted from various locations, no longer restricted to the physical location of the central computer system. However, a certain proximity to the central computer system was required. Access controls were needed as an integrated part of the computer. Physical constraints dictated the distance between the computer and its terminal and keyboard.

The perimeter continued to be well-defined, but, physical security was no longer sufficient.

The proximity clause changed when modems, or other means of single-point remote access, were introduced to enable computers or terminals to communicate directly with the central computer system. This new infrastructure layer also required an additional access control layer because access control enforced at the central system was no longer sufficient.

Although these systems were "remote," the perimeter was still defined. Security enforcement required additional access controls. Furthermore, because multiple users could access the same CPU, each user had to be monitored (authenticated) for this use.

The single-point remote access paradigm shifted dramatically with the dissemination of the Internet, which connected these large CPU systems, such as mainframes, *to each other*.

Authentication at the local system was lost as systems became *personal*. These personal computers (PCs) had no need for authentication; as the name implies, they were intended for personal and home use. These PCs also began to be networked together through the use of modems and eventually connected to the Internet through technical means such as high-speed broadband or DSL access devices. The connections today provide access lines even into private homes, and the bandwidth provided to the user community is growing every year.

As the systems grew and became more powerful, authentication was reintroduced into the personal computers as the PCs themselves could be remotely accessed.

This development is used by companies and employees alike to promote home working environments and past-office-hours work through connections to the corporate network. These connections use high-speed lines as a carrier into and over the Internet through a corporate virtual private network (VPN) entry point into the corporate network infrastructure. For example, the corporate network extends seamlessly to the employee's home.

The same technology is being used for customer and business-partner access to the corporate application and data resources also.

Devices that can use Internet technology are no longer bound to well-known personal computers; many sorts of wireless devices allow people to transparently gain access to the Internet and to a corporate IT environment. Because the systems and applications have become interdependent and connected, knowing where the application is hosted, or what computer the application is executing on is often difficult. Devices such as vending machines, telephones, medical equipment, manufacturing equipment, all have the ability to access the Internet and can even be accessed remotely.

The perimeter is now becoming fuzzy. Any sort of computing device may become the perimeter itself, and these devices in many cases are mobile.

This situation introduces us to a new concept. If the network perimeter has eroded, then what is the perimeter? The network perimeter has become a dynamic changing barrier that you must redefine and protect. The problem arises when you view the network perimeter as a static barrier because *it is not!* The systems that interact with the network perimeter make this network dynamic, and thus you must protect it by defining a *system perimeter* that understands and is capable of being a part of the network perimeter.

Another issue is that applications, introduced by a web browser and run on local machines, are difficult to control with traditional network perimeter tools. The systems do not even have to move to introduce unwanted access on the system itself.

We look more closely at how the perimeter relates to the real business world.

Challenges for secure business transactions beyond the network perimeter

Every successful organization today has to collaborate with customers, employees, and business partners and provide them access to business relevant assets. Those assets can be tangible goods, financial, community or health care services, or anything that is of value to both business partners.

This somewhat foundational business model is not new. It is the methods of collaboration that are constantly changing. Although business can still be conducted by human interaction, today's elaborate information technology presents us with more flexible ways of engaging in all sorts of business transactions.

To remain successful, an organization has to fully exploit the potentials of the IT network perimeter. Using the physical access layer alone will not secure continued business success. Employing a sophisticated web application infrastructure (Web 2.0) enables an organization to create a user-friendly web-facing layer that can provide access to almost every business asset. The combination of this user-interface layer and the ubiquitous IT network-perimeter access model is what most successful organizations are deploying today.

This business model capitalizes on extended reach, availability, and business hours. An organization can use it to capitalize on benefits that were almost impossible to achieve a few years ago, but it does not operate without risks.

Several benefits that are related to this business model are as follows:

- Reduced time to market

  Time to market is an external business driver that reflects the pressure to gain a competitive advantage by rapid implementation of the system. A short time to market can result in cutting corners, adding, or delaying some security controls to meet the deadline.

- User-friendly access to systems

  The user-friendly access reflects the need or desire for the system to be intuitive to the user community. This approach can be achieved by fully employing Web 2.0 and supporting technology to provide single sign-on or federated identity, which can help reduce the number of credentials that is required by users.

- Availability of services

  With the right IT infrastructure, the organization can provide access to its most valuable business assets for a multitude of devices 24 hours a day from almost anywhere in the world.

Besides enjoying powerful benefits, considering the following risks is important:

- New threat vectors

  Every single point-of-entry into the IT network perimeter can pose a threat that must be closely studied in a risk assessment.

- Additional protection for high-value assets

  High-value assets might require additional protection (encryption, step-up authentication, and so on).

- Legal and regulatory compliance

  Legal and regulatory compliance refers to externally imposed conditions on the transactions in the business system, and the organization. Rules and policies imposed by regulatory and government agencies are included. Ensuring compliance also includes privacy issues, the ability to prove the transaction initiator, and proving compliance.

No organization today can avoid the new technologies, but every organization has to consider the risks and threats and measure the level of acceptance of these risks in a proper *risk assessment*. The outcome of this risk assessment, combined with the regulatory and business policy compliance requirements, can help the organization to define the best defense available.

In the remainder of this section, we examine the ever-changing threat landscape and several compliance drivers that can all influence the organization in its quest for the best IT network perimeter protection.

The ever-changing threat landscape

In the context of our secure business transactions, *threats* can be defined as events, people, or forces that can pose a risk to our assets by exploiting a vulnerability. To help you better understand those risks, we examine the concepts of vulnerability and exploit:

- Regarding IT systems, a *vulnerability* can be considered a flaw in a system, for example application code, that can lead to an unexpected response of the system (such as a deadlock situation where the system stops working) or the susceptibility for malicious attacks.
- An *exploit* however can be a piece of software, such as an application, a sub-routine, a process, or a command, to take advantage of a particular vulnerability to gain access to or disrupt a system by evading its security measures and thereby potentially causing harm to an organization.

Where do typical threats originate from? Threats can come from *insiders*, *outsiders*, and a new source we call *accidental insiders*. A technical adversary can trick an insider, for example an employee, into doing something that can open a pathway into the internal network. That is, these techniques can allow an outsider access, from the inside.

Over the past years, the threats that we have come to know have evolved dramatically. What has motivated this change in the threat landscape? Beginning in 2005, methods for executing Internet attacks have quietly evolved. The shift has remained subtle to date, but organizations that ignore newer attack methods can experience significant losses. A hacker's motivation for launching attacks has changed, causing the current threat evolution. Today's attacks are motivated by profit and politics, and rarely motivated by glory and fame. The more organized attempts for financial gain are harnessing intellectual talent within the hacker community to devise new attack strategies and create malicious code (malcode) that can invade, without detection, even complex IT systems.

Information security solutions previously protected organizations from hackers intending to generate front page news about a successful denial-of-service attack or a website defacement. In the new era of Internet threats, attackers are motivated by profit or politics, and use cutting-edge technology to probe networks, undetected for as long as possible. The longer attacks go unnoticed, the more opportunity for success in data theft and other profit-generating activities.

Table 1 on page 6 compares attack characteristics, how the attacks occurred in the past and how the new era of attacks can occur.

The new attacks and motivations can help you better understand the need for a threat mitigation architecture.

Table 1 Characteristics of older attacks versus new era attacks

Attack characteristics	Older attacks	New era attacks
Motivation	Glory and fame	Profits and politics
Complexity	One-dimensional	Multifaceted attack
Scope	Widespread for maximum publicity (carpet bombing or shotgun approach)	Targeted attacks to go unnoticed (surgical strikes or sniper approach)
Primary risk	Network downtime to clean and repair	Direct financial loss; theft of trade secrets or corporate strategy; customer data breaches and disclosure
Targets of attack	High profile; widespread	Sharply focused on firms or individuals
Effective defense	AV signatures; reactive approach	Multi layer protection; preemptive and behavioral approach required
Recovery	Scan and remove	Removal not always possible; systems might require re-imaging
Types of attack	Virus, worms, spyware	Designer malware, rootkits, ransomware, spear phishing
Attack approach	Network traffic (purposely tell everyone the threat is here)	Malicious code (stealth-like operation to avoid discovery)

With the growing number of required techniques to gain access to systems and networks, many security researchers attempt to classify these threats. Unfortunately, the public in general and many sources to the media, tend to use the term *virus* for anything that is malicious to a computer. This term generates a false sense of security, and in many cases, administrators “believe” they are protected because they have antivirus protection, and network-based firewalls. However, this type of protection is no longer sufficient.

Antivirus software is good at identifying and stopping attacks that have already happened. Traditional antivirus software works by understanding what threat has occurred, identifying that threat, and then preventing the infection and spread of that threat onward. The problem that remains occurs when the threat is not identified. What if there is only one target or what if you are the first target? In these cases, the antivirus solution cannot protect you.

Traditional firewalls are only as good as the policy that is applied to the device. Firewalls are designed to reduce the threat-surface area by limiting exposure. Unfortunately, the technical adversaries have designed techniques to bypass the policies that are required to have networks be useful by legitimate users. Techniques such as allowing a user to view a web page can lead to an internal breach. Most firewalls do not have the ability to identify these types of threats.

Another significant problem is that many threats do not use malicious techniques to get into our systems and networks. They infect our computers through social engineering and deceptive software techniques. Traditional security solutions, such as antivirus, do not address these types of techniques, and a different approach is required.

Several of the most common and destructive types of malware are as follows:

- Malcode

  Malcode comes from programs, scripts, or macros that can execute on user machines, and are malicious in nature. This category of threat is often subdivided into viruses and trojan horses. A *virus* is attached to code, or contained within a legitimate program or document. A *trojan horse* is a program that has an external visible purpose, but also has covert malicious behavior that is unknown to the user. Malcode can contain many components, and categorization is subdivided according to the purpose of components (for example, *password stealers*, *keyboard loggers*, *botnets*, *droppers*). A variety of stealth technology can be deployed to keep malcode installed without detection (for example, *rootkits*). Self-propagating code is often designated as a *worm*.

- Vulnerabilities

  Vulnerabilities, although not considered malware in itself, come from *deficiencies in legitimate code* that is running on internal computer systems, or a *system misconfiguration* that can lead to an unexpected outcome (for example, if you allow your DNS servers to do transfers to any system, or if your FTP servers grant too much access by default). If an attacker can interact with the system's internal network, or provide data to the system that is examined by executing software, then the possibility exists for the attacker to use a vulnerability to compromise the system. As with malcode, the vulnerability threat has many subcategories:

  – *SQL injection* vulnerabilities are well known for being easily exploited to gain knowledge of internal database structure and contents.

  – *Cross-site scripting* vulnerabilities (XSS) are often used to execute script code within users' browsers.

  – However, the most devastating types of vulnerabilities are those that are designated as *remote code execution*. These vulnerabilities, when exploited, allow native code execution on the computer containing the vulnerable code. In 2006, a number of vulnerabilities were exploited to gain remote code execution on sensitive sites.

  – Perhaps the biggest remote code vector that has been used to compromise systems in the past years are vulnerabilities that are contained in browsers, or browser based plug-ins. If a user is enticed into visiting a malicious website that hosts a document containing an *exploit for a browser* vulnerability, the users machine can be *owned*.

  Vulnerabilities are often coupled together causing complexities to be introduced when describing attacks. An XSS vulnerability can be used to direct a user to a website that contains a browser exploit. After the browser exploit is used to gain code execution, malcode can be installed on the user's machine. Malcode can use one or more separate vulnerability vectors as a propagation strategy. The combination of malcode with multiple vulnerability vectors can lead to considerable confusion when describing various threats.

- Data leakage

  Data leakage often comes from unintentional insiders that transfer restricted information to external systems. However, it can also be the result of malcode that is installed on user machines. The problem is detecting and preventing the transfer of sensitive information from within the organization to an unauthorized external site.

- Denial-of-service

  Denial-of-service comes from external users or systems attacking a system infrastructure. The general idea is to disrupt the operation of the system. Various forms of denial-of-service attacks exist. One is the vulnerability denial-of-service. Certain vulnerabilities might not be able to exploit remote code execution, but can crash the system. An attacker can cause a computer to crash by sending a single packet to the vulnerable host.

More common are denial-of-service disruptions that come from generating a volume of traffic that overwhelms a network, or host computer in the network. DNS servers are particularly vulnerable when dealing with malformed DNS requests. If an attacker can find a packet that causes many cycles to be spent by the host computer, a flood of these packets to the host can cause a denial-of-service.

Bandwidth denial-of-service attacks seek to exhaust the network capacity by flooding the network with traffic. Often these attacks are mounted from thousands of separate host computers (*distributed denial-of-service*), and usually the computers that are attacking are compromised with botnet malcode that is installed on the machines.

- Human-related threats

  The human-related threats are not based on pure technology vulnerabilities, although technology can be used to achieve the attacker goals. The following techniques are the most common:

  - Phishing scam

    A fraudulent attempt to acquire information such as username, password, and credit card details by appearing as a trustworthy entity in an electronic communication is called a *phishing scam*. Communications purporting to be from popular social websites, auction sites, online payment processors, financial institutions, or IT administrators are commonly used to lure in the unsuspecting user. Phishing is typically carried out by email or instant messaging, and it often directs users to enter personal details at a fake website that looks and feels almost identical to the legitimate site.

  - Social engineering

    The manipulation of individuals to perform actions or divulging confidential information, rather than using technical hacking attacks, is called *social engineering*. Although similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information-gathering, fraud, or computer system access. In most cases, the attacker never comes face-to-face with the victim.

To better illustrate information about the threat landscape previously described, we review several statistics from the latest IBM X-force report.[1] For instance, the IBM X-Force analyzed and documented 4396 new vulnerabilities in the first half of 2010, a 36% increase compared to the first half of 2009 and the highest count of new disclosures in the first half of the year ever recorded. In 2007, the vulnerability count dropped for the first time, but in 2008 there was a new record high. Although 2009's lower vulnerability-disclosures rate appeared to indicate a plateau, the dramatic increase in the first half of the year puts that trend into question. It now looks like 2009 was only a short lull in the ongoing saga of increasing vulnerability disclosures. If the trend from 2010 continues, there might be a new record high.

What does this massive increase in vulnerability disclosures mean? One fact that we know for certain is that all vendors and other sources are reporting more vulnerabilities than ever before, as depicted in Figure 1 on page 9. For example, in 2009 the *milw0rm* group[2] disclosed over 2000 exploits. They closed late in that year when the *Offensive Security Exploit Database*[3] took over. At the time of this writing, Offensive Security had disclosed over 2000 exploits. That single source alone is trending to release 60% more exploits for the year 2010 than in previous years. The annual vulnerability disclosure rate now appears to be fluctuating in the range of 6000 - 8000 new disclosures each year.

[1] The latest IBM X-Force Trend and Risk Report is available at: http://www.ibm.com/services/us/iss/xforce/

[2] A general overview about milw0rm is at: http://en.wikipedia.org/wiki/Milw0rm

[3] The Offensive Security Exploit Database can be located at: http://www.exploit-db.com/

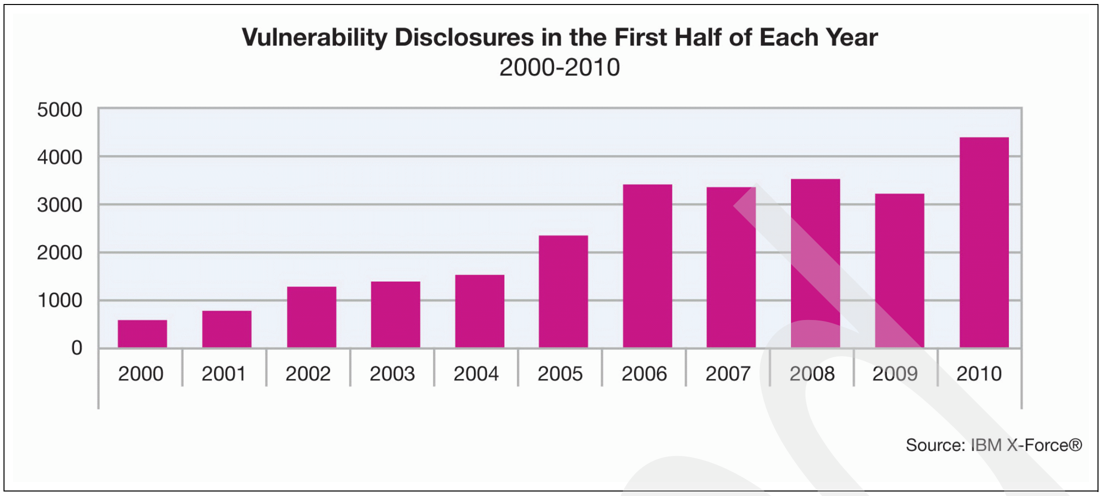


Figure 1 Vulnerability disclosures over the past ten years

Of even greater concern is that more than half of all vulnerabilities found in the first part of 2010 are yet without patches, and that is only for 2010; an enormous number of unpatched vulnerabilities still exist since 2006.

As mentioned earlier, the web is the main interface for business applications today, and so far, web application vulnerabilities continue to be the most prevalent type of vulnerability affecting organizations today. Web application vulnerabilities have moved up past the 55% mark, accounting for more than half of all vulnerability disclosures in the first half of 2010, as shown in Figure 2.

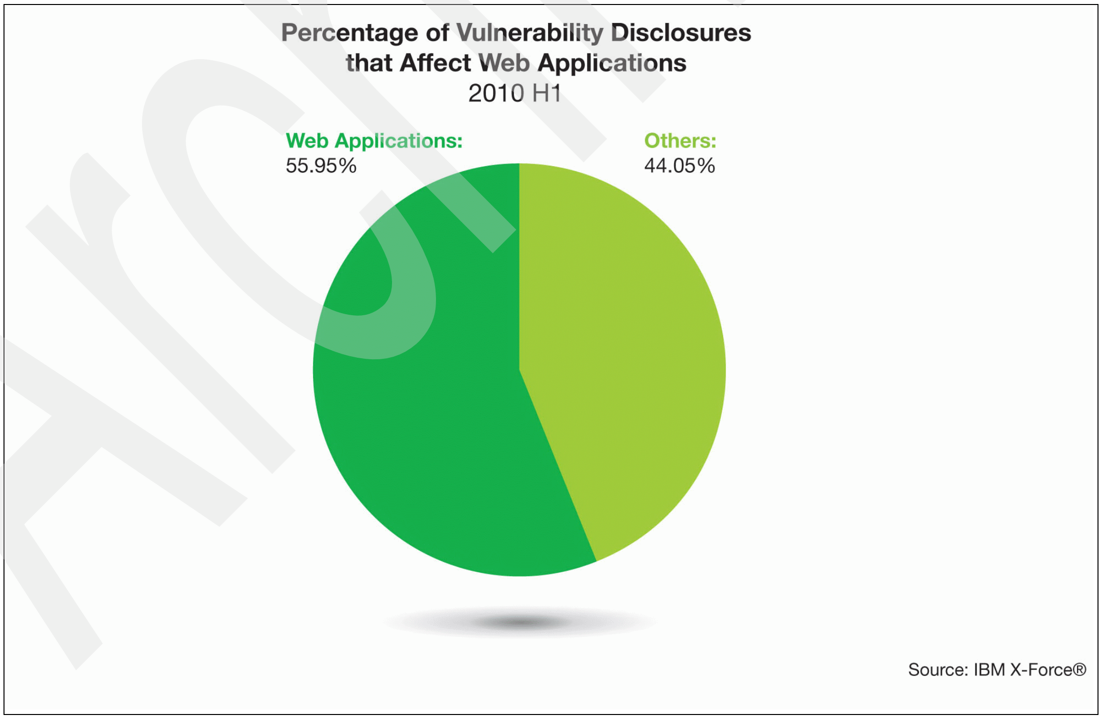
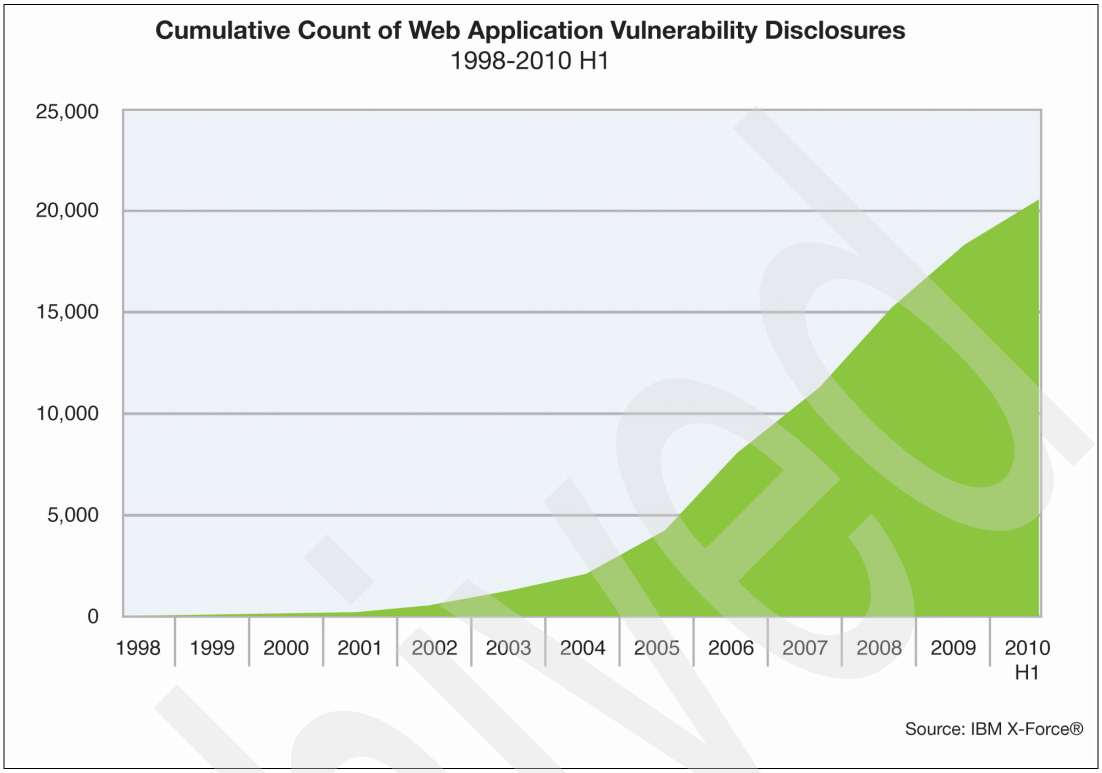


Figure 2 Web application vulnerability disclosure percentile

The number of web application vulnerabilities continues to climb at a moderately steady rate of 3000 - 4000 disclosures per year, as shown in Figure 3 on page 10. These figures do not include custom-developed web applications or customized versions of these standard packages, which also introduce vulnerabilities.



Source: IBM X-Force®

Figure 3 Cumulative count of web application vulnerability disclosures

The increasing attacks targeted at web applications, services, and data are driving organizations to address security enforcement across the organization. These attacks include SQL-injection attacks, cross-site scripting (XSS), denial-of-service attacks, and miscellaneous techniques such as directory traversal and others. Attackers use these types of attacks to view or obtain unauthorized information, or to change files, directories, user information, and other components of web applications.

The (Open Web Application Security Project (OWASP) Top 10 provides an awareness document for web application security and represents a broad consensus surrounding the most critical web application security flaws[4]. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

The list includes the following vulnerabilities, to name a few:

- Broken authentication and session management that allow attackers to compromise passwords
- Keys and session tokens that exploit implementation flaws to assume user's identities.
- Failure to restrict URL access, security misconfiguration, and unvalidated redirect and forward operations that expose business-sensitive data and information to unauthorized users

Organizations must assess the risks and vulnerabilities of externalized applications and services and implement appropriate security controls to manage user identity and access within and throughout the organization.

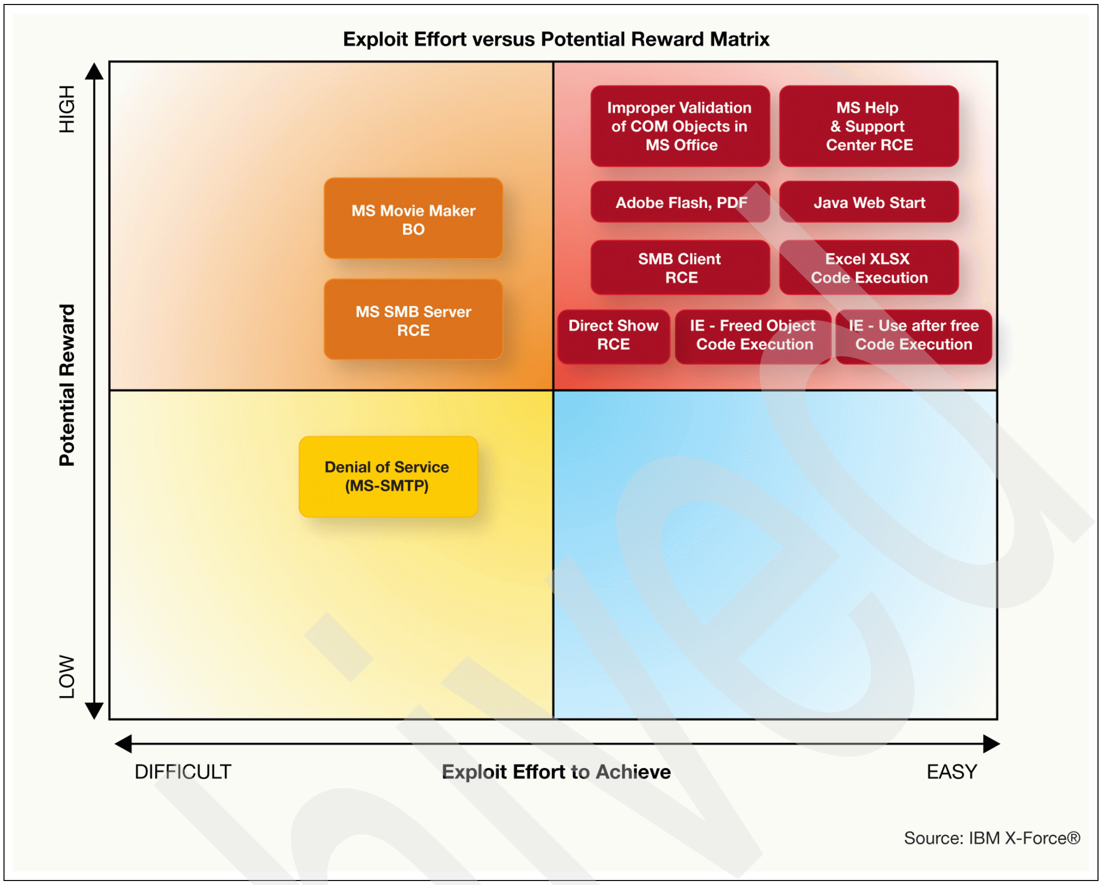
[4] http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Table 2 shows the Top 10 threats that were identified by OWASP for 2010. Be sure to consider the questions that we list in the “Key considerations” column.

Table 2 OWASP Awareness list

OWASP Top 10 threats in 2010	**Key considerations**
A1: Injection flaws	Separate the untrusted data from user-supplied application command or query. *Who can send data to systems?*
A2: Cross-site scripting (XSS)	Separate the untrusted data from active browsers. *Who can send data to systems?*
A3: Broken authentication and session management	Control access with the ability to invalidate session state at logout. No reuse of tokens or SSL state must be allowed.
A4: Insecure direct object reference	*Do any users have partial access to change system data?*
A5: Cross-site request forgery (CSRF)	Control access with ability to deny, “step-up,” or re-authenticate the user.
A6: Security misconfiguration	*Have you performed security hardening across the entire application stack?*
A7: Insecure cryptographic storage	Encrypt sensitive data. Use security tokens to protect cryptographic resources.
A8: Failure to restrict URL access	Control access to URLs on the portal. *Can anyone with network access send an application request?*
A9: Insufficient transport layer protection	Use SSL to protect all authenticated traffic. *Who monitors the network traffic of your users?*
A10: Unvalidated redirects and forwards	*Can anyone trick your users into submitting a request to your website?*

With the number of vulnerability announcements rising and vendors scrambling to provide patches and protection to the problem areas, how can organizations prioritize the efforts of IT administrators so that adequate coverage is provided? The Exploit Effort versus Potential Reward Matrix, as shown in Figure 4 on page 12, provides a simple model for thinking about vulnerability triage from the perspective of attackers. Many of the vulnerabilities represented by the X-Force alerts and advisories cluster toward the top right quadrant (shaded in red). This quadrant represents issues that provide high payoff for attackers and can be relatively easy to implement. These vulnerabilities tend to receive a large amount of exploitation activity on the Internet. In contrast, the one vulnerability that is represented in the lower left quadrant (shaded in yellow) states that this vulnerability is relatively difficult for the attacker to exploit, and provides a minimal potential reward.



Source: IBM X-Force®

Figure 4 Exploit Effort versus Potential Reward Matrix

What about compliance

Corporate scandals and breakdowns, such as the Enron case in 2001, have highlighted the need for stronger compliance and regulations for publicly listed organizations. The most significant regulation in this context is the Sarbanes-Oxley Act[5] (SOX), developed by Senator Paul Sarbanes and Representative Michael Oxley in 2002. It defined significant tighter personal responsibility of corporate top management for the accuracy of reported financial statements.

Extrapolating to the Internet business scenario, not only publicly listed organizations need to implement standards and comply to regulations. To participate in online business, adhering to regulatory compliance standards can be beneficial to your organization and will probably be mandatory in the near future, if it is not already. Regarding the computational systems, *compliance proves that systems operate according to security expectations, and operate to meet guidelines within a tolerance of acceptance.*

Compliance includes operating within the boundaries of *acceptable risk* and *business context*. The business context includes laws and regulations that can result in a potentially different definition of security and compliance for every organization. The differences result from both the methods and factors that are used in analyzing the business context. The commonality is that the security policy can be defined by determining an acceptable risk level, how to achieve (control, mitigate, or accept) that risk level, and how to verify that the security is implemented as specified (compliance).

[5] To learn more about the Sarbanes-Oxley Act visit: http://www.soxlaw.com/

Besides SOX, a number of additional regulations exist, such as GLBA[6], FISMA[7], and HIPAA[8]. In certain cases, other compliance frameworks (such as COBIT[9]) or standards (NIST[10], ISO[11], and so on) can inform how to comply with the regulations.

Conclusion

In this first section, we described business drivers and the threats and compliance requirements in relation to the IT network perimeter. To address a risk mitigation strategy that can be applied for every organization, we must examine the acceptable level of risk our organization is willing and capable to accept and understand what kind of threats jeopardize the continuity of the business and can potentially cause loss of revenue.

To implement an efficient risk mitigation posture, we must consider not only the technological infrastructure piece of compliance, but also the human part: implementing a security awareness program and a security policy document based on the organization's needs.

In regards to the infrastructure, we have to understand how our information is accessed through the IT network perimeter, what are the entry points setting our particular perimeter definition, and what security measures are best for this scenario.

The next section describes security architecture further, how network intrusion prevention systems can be placed, the importance of implementation, and how IBM Network IPS can help you stop Internet threats.

Addressing problems related to network intrusion

Now that you have a good understanding of the gravity of Internet threats, we focus on how to stop them. There are a variety of valid answers, and although it is possible that all of them are correct, only one of them is going to be the right choice for your organization.

Even if you are using the best security technologies, your organization might still be vulnerable, because, regardless of the quality of your security tools, without well designed security policies that consistently address your data protection, privacy, and security needs, your organization is still at risk.

We return to our discussion of how to truly stop security threats. There is no magical solution, nor is there one single product that can provide solutions for all of the potential threat scenarios. Rather, you have to approach the problem from an overall enterprise security architecture perspective. For more information, see *IBM Enterprise Security Architecture for Network, Server and Endpoint*, SG24-7581.

[6] Gramm-Leach-Bliley Act (GLBA): http://www.ftc.gov/privacy/glbact/glbsub1.htm
[7] Federal Information Security Management Act (FISMA): http://csrc.nist.gov/groups/SMA/fisma/index.html
[8] Health Insurance Portability and Accountability Act (HIPAA): http://www.hhs.gov/ocr/privacy/
[9] COBIT: http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
[10] National Institute of Standards and Technology (NIST): http://www.nist.gov/index.html
[11] International Organization for Standardization (ISO): http://www.iso.org/iso/home.html

The following components are the most important regarding IT perimeter security:

- Firewall

  A *firewall* is a software application or hardware appliance that filters traffic between networks based on source address, destination address, and protocols. When positioned on the perimeter of your network, it is your first line of security because it allows or denies IT traffic coming from or going in to your network. A firewall must reflect your security policy for external access to your resources and internal resources accessing external targets.

  For firewall applications, various technologies exist:

  – *Packet filters* filter only the traffic that is based on ingress or egress rules with no connection state awareness, meaning, without knowledge of the application session. The packet filter can leave many paths into your network unprotected.

  – *Stateful inspection* firewall also filters packets, but with session awareness. This technology enables an understanding of cohesion between ingress and egress packets that are part of the same communication context and therefore it can perform legitimacy checks on the opening and ending of sessions, without performing packet-by-packet checking. This approach makes traffic monitoring faster, easier, and more reliable.

- VPN

  A Virtual Private Network (VPN) virtually creates a private network inside an otherwise open network, for example, the Internet. It uses keys and cryptography to authenticate and transport the traffic, making it unreadable to any person who does not have the correct configuration, password, or digital certificate. VPNs are useful when communicating with branch offices or business partners across the Internet. A VPN can securely connect two networks, and it is often used to allow a remote user to have secure access into the organization’s network. The cryptographic technologies involved can be based on *IPSec*, which uses specific client and server applications, or *Secure Sockets Layer* (SSL). Both methods can render access to whole networks or simple applications and can use several forms of authentication and cryptographic algorithms. Although a VPN can use a separate hardware appliance or software, most commonly it is a feature implemented within the firewall.

- IPS

  An *intrusion prevention system* (IPS), the main topic of this document, can be implemented as a software application, but is currently used mostly in a hardware appliance form to block threats. An IPS is the second most important piece in the scope of security architecture, because it is the primary tool for stopping threats to the network, as we describe in this guide.

- Antivirus gateway

  An antivirus gateway operates the same way as a host antivirus software does, but the gateway scans files traversing the Internet through communication protocols such as FTP, HTTP, Telnet, rlogin, SMTP, POP3, IMAP, and news. It looks for virus signatures in files passed across these protocols. Because it has to disassemble the streams of data to look at the whole file as the traffic crosses the network, a slight delay can be sensed in the scanned streams.

- Proxy server and content filtering

  Proxy servers are generally software applications that act on behalf of the client. A proxy server acts as a network service preventing the direct connection from the user to an Internet application. It can help to enforce the security policies on what can be accessed from within, using authentication to control it by user ID or groups.

Another application that can be used for network traffic security is content filtering, which allows or denies access to websites, based on contents. Content filtering is designed to prevent users from accessing potentially harmful sites and also to increase productivity. It is not considered a protection by itself, but a way to enforce a security policy and control the content accessed by your employees, making sure the content is appropriate and necessary for business needs. Content filtering can also help to prevent phishing techniques when accessing potentially malicious or harmful websites.

- Anti-spam

  Anti-spam is considered another prevention tool rather than an active protection tool. It works in conjunction with your email server to ensure the email messages received and sent are proper and therefore eliminating the those that are not related to the business, or that can have harmful content.

Figure 5 illustrates each of these components as used in a typical organization.

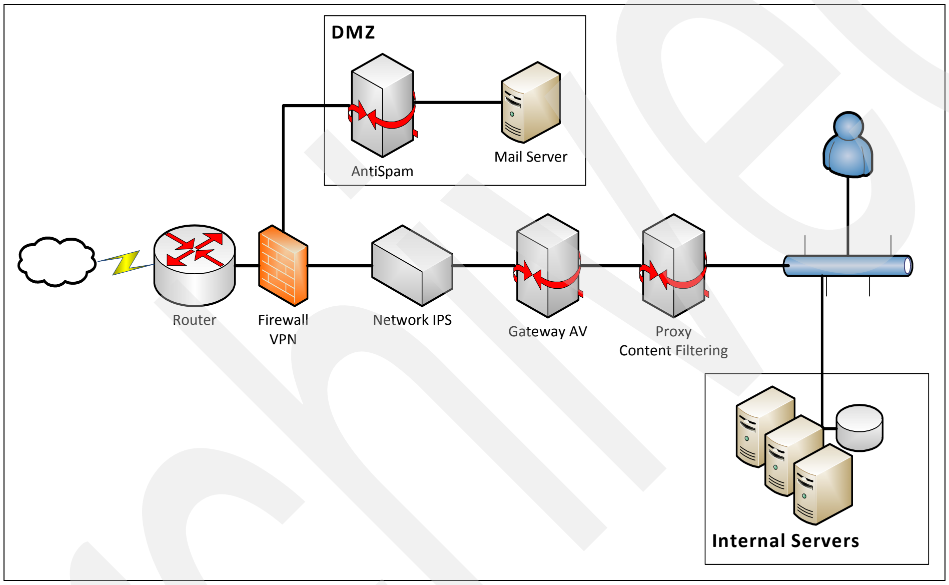


Figure 5 Perimeter security architecture

Although the network IPS is not the only piece of the security architecture, it is the most important piece when threats are the main concern. Also, when Internet-based business applications are at stake, IPS is the second only to the firewall in terms of protection.

To use an analogy, if we compare the technology to the physical world, the firewall can be considered the doorman of a building, who lets you in if you can provide the correct address and name of the person you are visiting. The doorman realizes whether you have had previous visits, whether the doorman knows you, whether the visit is an appropriate time, and so on. The IPS represents the armed security guard in the lobby watching the doorman and the people that the doorman lets in to further protect the residents of the building. This security guard’s role, beyond that of the doormans, is to check for forced entries, harassment of the doorman, any weapons or other malicious objects you may hide, and if you pose a threat by the way you act. Even after you enter the building, the guard watches you to double-check whether you pose a real threat. In case of a threat, the guard relies on training to stop the threat: calling the police, or even reacting with force if needed.

UTM: Security architecture in a system and determining where it fits

An emerging trend is the consolidation of multiple applications, servers, and sometimes network devices to better address cost, space, energy, and complexity issues. An example of this trend (in the security perspective), is the *Unified Threat Management* (UTM) appliance. A UTM appliance is basically a combination of a firewall, an IPS, and antivirus gateway. It can simplify the IT perimeter security architecture by combining all of these components and, in theory, is already integrated. We say in theory, because it is not always the case. Certain vendors include other security features such as content-filtering and antispam, and depending on the vendor, the appliance might contain even more embedded network and security capabilities.

Although this solution seems perfect, because everything an organization needs is in a single system, there is a catch. To run all those applications on a single system, massive processing power is needed, affecting the cost factor of the solution. In addition, the processing resources have to be shared by all applications.

To achieve a balance of the resources that are used versus application features, some functionality must be sacrificed. Several vendors have created a dedicated processor architecture to address this issue, but choices must still be made to address the achievement of a cost-effective solution. Choosing performance over functionality is the most common choice. This choice is only natural when the performance needs are also growing at a fast pace and having all applications available at the same time in a single system. The applications do not have the ability to be thorough and also achieve the performance needed at the same time. Another issue is the single point of failure that is inherent in such solutions. This problem might not be the primary problem, because any security architecture that is not designed to handle high availability has single points of failures. However, when all those functions are joined together in the same appliance, troubleshooting problems might be difficult, because one application can affect another in regards to performance, configuration, integration, and so on.

In summary, to achieve the most cost effective solution and have the expected performance, a feature trade-off is made. This way, the product should be less thorough and less complex, covering less threats and security enforcement necessities.

Therefore, we enforce our first thought that there is no such thing as a perfect solution. The security architecture in a system is useful for smaller and simpler networks such as branch offices, retail stores, and small business organizations. For other types of organizations, the better fit is to have a separate security architecture, choosing the best solutions for each piece, and to maintain a better security coverage in your network and mitigate the risk.

The risk and cost versus benefit calculation must be measured so that you can have the best solution for your needs. This means that depending on the importance of the data and the availability of your service and how it is accessed, you can choose a simpler or more complex, but inherently more capable, architecture. The selected architecture can provide all the components, described earlier, or a subset of them, and it can be designed to handle or not handle high availability.

The IDS to IPS evolution

Intrusion detection systems (IDS) were first used to complement the security architecture and to monitor inbound traffic that was allowed by the firewall, and searching for attacks into the payload of packets, where the data and application lies. It was typically implemented as a normal server, with a network interface, operating system, and the IDS application, which used the network interface card (NIC) in a promiscuous mode like a sniffer, but comparing what it saw to attack signatures or patterns. It was able to see all traffic of a subnet by taking a copy of every packet that crossed that part of the network.

At that time, the technology had not fully evolved and numerous problems existed. For instance, if the server did not have enough resources to process all packets received, parts of the traffic were not monitored. Also, because the IDS system worked like a sniffer, it did not have session awareness; with several simple evasion techniques, this protection could be circumvented and avoided. The basic design of an IDS system was to generate alerts based on signatures, and not stop the threat itself. To further analyze, tune, and monitor the generated alerts resulted in a lot of manual processing. In addition to this manual overhead the IDS also generated *false positives* (an alert is issued but there is no actual attack), and *false negatives* (an attack occurs but generates no alert). These problems reflected in a lack of confidence in this type of tool among security analysts and consultants.

By comparison, the IPS shares certain technological concepts with the IDS, but it is not simply a next generation of it. In fact, IPS technology completely changed the way the intrusion detection and prevention concept is positioned in the network, the way it captures and analyzes packets, the detection accuracy, and, most important, the final result and application of the tool.

The IPS is positioned, similar to the firewall, inline to the traffic, so all packets must traverse it. It can understand session state, is not limited to uni-direction flows, and can block traffic at near-real time when needed. Additionally, the false negatives and false positives are rare and the configuration and tuning are much simpler and effective. Because most IPS solutions are based on hardware appliances, they have low latency and low impact on the network performance, and they do not disrupt any communication in case of failure. This technique can be achieved because most IPS systems implement a *network bypass*, a hardware device that allows all traffic to flow if the sensor should fail to work.

The paradigm of reactive protection changed because the IPS is an inline device and it can stop threats on the wire. Because of its flexibility and adaptability, the expectation is that this technology can be proactive and prevent both known attacks and attacks that are still to come.

IPS technology basics

Typically, an intrusion prevention system (IPS) is implemented as a hardware appliance that sits inline to the network traffic as described previously. However, this appliance, which represents the actual sensor, is only a part of the overall implementation architecture. The IPS solution might also include a managing server, an administration console, and, in some cases, a database server to consolidate all the logs and configurations. The sensor is a device that is transparent to the network traffic. It allows or blocks packets based on IP address, protocol or service, and of course application-level analysis and verification by comparing the extracted data with attack signatures and patterns.

Although the IPS appliance is commonly placed behind the firewall to enforce perimeter security, it can also be helpful in other network segments, as depicted in Figure 6 on page 18.

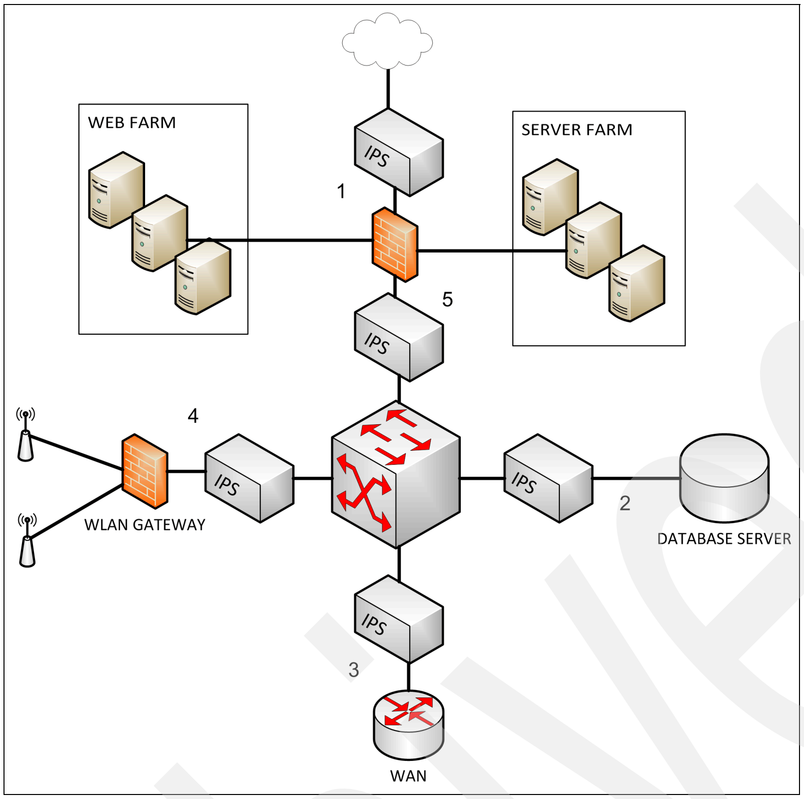


Figure 6 IPS positioning

Let us examine the placements in more detail, by referring to the numbers in Figure 6:

1. In front of the firewall

   Rather than looking into the allowed traffic, use this placement if the main concern is denial-of-service attacks that aim to disrupt service offerings or even as a way to evade the firewall protection by flooding it. This placement can protect the firewall and the DMZ at the same time.

2. In front of mission critical servers

   Because the IPS can view the entire network packet all the way to the application layer, it can be effective in protecting internal mission-critical servers and specific applications by being tuned to monitor specific attacks to databases, DNS servers, file servers, and so on.

3. Behind the WAN router

   If your network extends to remote offices or includes business partner segments, the network perimeter immediately expands, requiring that security measures also be expanded. Because remote servers rarely contain critical or sensitive information, they are frequently not covered by the stringent security measures that are used for the central IT environment, which is why they are often targeted by attackers. Ultimately, they are directly connected to the organization's core network and, therefore, to other mission-critical servers and resources. Placing the IPS behind the WAN router can protect against attacks coming from those remote networks.

4. Behind the wireless local area network (WLAN)

   Wireless networks are particularly attractive to attackers because they are more easily accessible, do not require a physical infrastructure to connect (cables and connections), and are built on evolving technology. However, wireless networks are attractive to the organization that wants to benefit from the flexibility, relatively low cost, and fast deployment options that the networks offer. Behind the WLAN is a good placement for the IPS to protect the wireless network perimeter.

5. Behind the firewall

   As we mentioned previously, this location is the most common placement for an IPS sensor because it can use its core capabilities. After the firewall filters grant access for the acceptable traffic, the IPS checks for threats on protocols and services that are going to be accessed and used.

Network-based IPS offers extensive detection capabilities. Most vendors combine signature-based techniques, protocol decoding, anomaly detection, stateful filtering, and deep-packet inspection to perform in-depth traffic and pattern analysis. The integration of these techniques, the number of protocols decoded, the types of signature checks, and the analysis methods are key to the effectiveness of the network-based IPS. As stated by NIST in its *Guide to Intrusion Detection and Prevention Systems*,[12] the most common event types that are detected by the IPS sensors are as follows:

- Application layer reconnaissance and attacks: For example, banner grabbing, buffer overflow, format string attacks, password guessing, and malware transmission
- Transport layer reconnaissance and attacks: For example, port scanning, unusual packet fragmentation, and SYN floods
- Network layer reconnaissance and attacks: For example, spoofed IP addresses and illegal IP header values
- Unexpected application services: For example, tunneled protocols, backdoors, and host that is running unauthorized application services
- Policy violations: For example, use of forbidden protocols, and the use of inappropriate websites

Detection accuracy is important and, as the technology has matured, the IPS has become a key factor in the security architecture. Many of today's IPS can provide a protection rate of greater than 90%. However, to be successful, the network IPS must provide a powerful, yet easy-to-use management platform that can generate alerts and reports, and can also integrate with other security tools, such as correlation engines, security information and event-management systems, and vulnerability assessment software.

Although network IPS technology is constantly evolving and adapting, it is still subject to various limitations. Several of the most important limitations include analyzing encrypted network traffic, dealing with high traffic loads, withstanding attacks against themselves, and focusing on the exploit rather than the vulnerability. To analyze encrypted traffic requires the IPS to either be the encryption endpoint or perform a *man-in-the-middle* technique to decrypt and encrypt the network traffic. This approach requires the encryption capability and access to the authentication certificates, and also the processing power necessary to handle this kind of workload. Having to deal with encrypted network traffic affects the appliance performance and affects the detection capabilities for ordinary, unencrypted traffic.

Handling constantly increasing network traffic loads is a typical trend, which involves better hardware and software optimization. Attacks against the network IPS is a technique of evading its security, and is a major concern to be addressed. The signature focus, although it

[12] http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

is still based on the exploit rather than the vulnerability, must be changed each time a variation of the same exploit appears. If the focus is on the vulnerability, all kinds of exploit variations can be covered.

Additionally, other threat prevention technologies are appearing and converging with the traditional IPS. These recent innovations are as follows:

- Web application protection

  As described previously, Web 2.0 technology has introduced new capabilities and services to the web, providing access to critical and existing systems and enabling the integration with other systems. Web 2.0-based access created a new kind of threat and a whole new category of attacks, such as SQL injection, cross-site scripting, cross-site request forgery, and others. Web application protection can provide protection against all these attacks by using protocol decoding methods, and application-specific signatures and access patterns.

- High speed networks

  Hardware and software integration and optimization is evolving to address the insatiable need for performance. Network speeds are increasing exponentially and the fast Ethernet of yesterday is now *gigabit Ethernet*, which is quickly becoming *10 gigabit Ethernet* with a potential of continuous growth.

- Data Loss Prevention (DLP)

  DLP is a new technology and still being adopted. It is similar to the way IPS monitors traffic (analyzing the payload of the packet). The main difference is that the DLP solution does not check for attacks, but for classified information, where it is going, and who is accessing it. Therefore, implementing a new set of signatures to look for specific information in the packets is not difficult. However, as part of the IPS, it typically has a simpler feature set because it shares resources with other important features.

Why we need an IPS

Today's network-based IPS is much more affordable, powerful, and accurate than ever before. Through its constant evolution, it can be considered one of the most complete security tools that aims to stop Internet threats. This function makes the network IPS indispensable for network protection.

An IPS can stop malicious traffic the instant IPS recognizes it. IPS can either terminate the network connection or the user session that is attacking your organization. It can block the dangerous user account, IP address, or other attacker attribute from accessing your targeted servers or other network assets. It can completely shut down all access to the host, service, application, or whatever network asset under siege.

One of the driving forces behind the deployment of an IPS in many organizations is to maintain compliance with regulations such as SOX and HIPAA. The IPS solution can help demonstrate those applications and network resources that are being accessed by malicious code, which is a key requirement to comply with SOX or HIPAA.

By analyzing reports from the IPS solution, a network administrator can better protect specific resources, such as finding those that lack adequate security measures, and better resolve the problems that inevitably occur. It can also be a good way to educate the executive staff about the threats that have targeted their organization.

An IPS system can ensure that a security breach to your network, such as a worm or virus, does not propagate out to the network of your partners. This business practice becomes crucial when your organization works with government agencies and financial institutions.

Conclusion

Although the IDS possesses limited and inefficient characteristics, the IPS has changed this paradigm by applying improved technology and placement. Today, the IPS solution is a key element for every security architecture, with the aim of stopping threats on the wire and preventing business from being affected. The wide interconnectivity throughout the web brings with it new concerns and business drivers. The use of IPS is a necessity because of compliance and application protection. Its placement is not limited to the perimeter concept we once had; its technology is now as adaptive as our environment. Regardless of the complexity of your security architecture and risk-mitigation strategy, the IPS is the current tool of choice.

IBM Security Network Intrusion Prevention System (IPS)

This section describes how IBM Security Network IPS technology can help protect your network from Internet threats.

The IBM Security Network IPS[13] is designed to deliver uncompromising protection for every layer of the network to protect your organization from internal and external threats by providing a proactive security solution to ever-changing security needs.

Overview

The IBM Network Intrusion Prevention System was developed to deliver the security that networks need and provides the uptime that organizations require. It provides the balance needed to allow business network traffic to flow, while keeping the intruders out. When evaluating intrusion prevention technology, organizations often struggle to balance and optimize the following six characteristics:

- Performance
- Security
- Reliability
- Deployment
- Management
- Confidence

IBM Security Network IPS delivers on all six characteristics. It offers performance, preemptive protection, high availability, simple deployment and management, advanced research and development, and excellent customer support.

Security measures should not degrade network performance. The IBM Security Network IPS solution offers high throughput, low latency, and quick uptime to maintain efficient network operations. With its modular product architecture, IBM Security Network IPS delivers security convergence by adding entirely new modules of protection as threats evolve and the IT network perimeter expands. From worms to botnets to data security to web applications, IBM Security Network IPS delivers the protection that is demanded for business continuity, data security, and compliance.

The IBM Security Network IPS uses the Protocol Analysis Module (PAM) to inspect, maintain state, and block traffic where needed. Multiple layers of protection are available throughout the seven layers of the OSI model. PAM provides deep packet inspection that identifies and analyzes more than 200 network and application layer protocols and data file formats.

[13] The IBM Security Network IPS was previously known as the IBM Proventia® Network IPS

The IBM X-Force[14] Research and Development team designed the PAM (Figure 7) and provides the content updates that help maintain “ahead of the threat” protection. PAM uses the following modular-extensible framework to provide coverage for the various needs of a network intrusion prevention solution:

- IBM Virtual Patch® technology: Shields vulnerabilities from exploitation, independent of a software patch.
- Client side application protection: Protects users against attacks that target applications that are used everyday, such as Microsoft® Office files, Adobe® PDF files, multimedia files, and web browsers.
- Advanced network protection: Provides advanced intrusion prevention including DNS protection.
- Data security: Provides monitoring and identification of unencrypted personally identifiable information (PII) and other confidential data.
- Web application security: Provides protection for web applications, Web 2.0 and databases (same protection as web application firewall).
- Application control: Reclaims bandwidth and blocks peer-to-peer applications and protocol tunneling that can violate an organization’s security policy.

Figure 7 IBM Protocol Analysis Module technology

With its modular-extensible framework, the Protocol Analysis Module is constantly evolving to block your most challenging security threats, eliminating the need to purchase additional point solutions. Backed by the IBM X-Force Research and Development team, the Protocol Analysis Module is regularly and automatically infused with new security intelligence to keep you ahead of the latest threats. Many other available IPS solutions try to match individual protection signatures with exploits, a process that is too slow to stop the evolving threats, and results in higher rates of false positives and false negatives.

Architecture

To provide you with more insight into the IBM Security Network IPS architecture, we more closely examine the main characteristics listed in “Overview” on page 21.

Performance

The various models of the IBM Security Network IPS provide the performance characteristics needed to protect various network environments: 10 Mb, 100 Mb, 1 Gb, and 10 Gb. The IBM Security Network IPS maintains a high level of overall network performance by providing an average latency of less than 150 - 200 microseconds and a configurable bounded maximum

[14] The IBM X-Force is a world-renowned security research organization that is dedicated to proactive examination of threats and the underlying software vulnerabilities the threats seek to exploit.

latency. IBM Security Network IPS performance metrics have been validated by third-party testing organizations. See Table 3.

Table 3 IBM Security Network IPS model comparison

Model	Inspected throughput	Interface
GX4004C-V2-200	200 Mbps	4 (2 network segments)
GX4004C-V2	800 Mbps	4 (2 network segments)
GX5008-V2	1.5 Gbps	8 (4 network segments)
GX5108-V2	2.5 Gbps	8 (4 network segments)
GX5208-V2	4 Gbps	8 (4 network segments)
GX6116	8 Gbps	16 (8 network segments)
Network Security Controller	16 Gbps	4 (2 10-Gbps network segments) 24 (1 Gbps port to various segments)
GV200	200 Mbps	2 (1 network segment)
GV1000	700 Mbps	2 (1 network segment)
Crossbeam	40 Gbps	8 (4 network segments)

Security

The security characteristic contains several technologies that we discuss:

- Virtual Patch
- Client-side application protection
- Threat detection and prevention
- Web application protection
- Data security
- Application Control

Virtual Patch

The *Virtual Patch* can shield vulnerabilities from exploitation, independent of a software patch. This characteristic enables a responsible patch management process that can be adhered to without fear of a breach. Virtual Patch technology is important because at the end of 2009, over half of all vulnerabilities disclosed during the year had no vendor-supplied patches to remedy the vulnerability.

Attackers use a wide variety of exploits that target vulnerabilities in software applications and operating systems. The traditional method of identifying and stopping these attacks was to create a signature that detected the exploit. The problem with this approach is that exploits that take advantage of these vulnerabilities often change, and when this change happens a new signature needs to be created. To create a new signature, however, a security vendor would need to know of the new exploit. This reactive approach allows the exploit to be successful as long as no new signature was deployed.

A more proactive approach is to protect the vulnerability rather than the exploit. This approach is used in the Virtual Patch module of the IBM Security Network IPS. The Virtual Patch protects against vulnerabilities and not the exploit that is trying to take advantage of this weakness. This proactive approach protects against all exploits for a vulnerability (old, new, discovered or undiscovered).

When vulnerabilities are discovered, software and hardware vendors sometimes provide patches to fix the vulnerability. Another advantage of the Virtual Patch module is that you can achieve protection until the software or system can be patched. Any IT professional who is security-oriented can agree that a well-planned and ongoing patch process is essential to any organization’s security posture. However, in certain circumstances, the appropriate patch cycle cannot be completed on affected systems in a timely manner.

Because many production systems require that patches be tested in test environments before going into production, maintenance windows must be scheduled; the vast numbers of systems that might require patching means that the time to complete the patch process can take days, weeks, or months. How much time and how many work hours are necessary to patch 80, 800, or even 8000 servers? Also, what happens when the discovery is made that the operating system patch breaks one of your key applications? How long would it take to identify the root cause of the problem, provide application changes, and implement the changes for a large amount of servers? With the Virtual Patch module, you need to update only a few IBM Security Network Intrusion Prevention Systems at key locations in the network to protect your overall IT infrastructure against threats that try to exploit the vulnerability. The process of applying the IBM Security Network IPS update and applying the appropriate security policy can take as little as five minutes.

Client-side application protection

The *Client-side Application Protection* module can protect users against attacks that target applications that are used every day, such as Microsoft Office files, Adobe PDF files multimedia files, and web browsers. The Client-side Application Protection module can also detect evasion techniques such as attacks to web browsers that use JavaScript obfuscation.

Threat detection and prevention

The *Threat Detection and Prevention* module protects against a wide array of threats including zero-day vulnerabilities, denial-of-service attacks, botnets, worms, trojans, and network reconnaissance.

The Threat Detection and Prevention module can detect and prevent entire classes of threats as opposed to a specific exploit or vulnerability. It eliminates the need for constant signature updates and includes the proprietary technology that has an unbeatable track record of protecting against zero-day vulnerabilities. This module identifies and stops malicious code based on behavior, rather than matching a particular attack signature or pattern. Heuristics can prevent evolving threats, which can change minor aspects of their signatures to bypass traditional Network IPS solutions.

Botnets, worms, and trojans can provide access to all areas of an internal network from infected systems within the organization. The IBM Security Network IPS provides the ability to identify the command, control, and back-door communications many of these malware technologies use to report back to and receive orders from their masters. The Threat Detection and Prevention module can stop these malware technologies.

Attackers often use various scanning techniques to gain an understanding of a network topology, such as the type of operating systems, the applications that run on these systems, and what vulnerabilities might exist. With this type of information, attackers can fine-tune the attack to better their chances of successfully exploiting a vulnerable system or application.

Many tools are currently available, some of which are free, that provide the ability for network and system reconnaissance. This availability potentially enables anyone to perform these types of scans, from script kiddies with limited skills to dedicated professionals who are focused on intruding on a particular organization. The Threat Detection and Prevention module can identify and prevent these types of activities by recognizing various scanning, probing, brute-force, and password-guessing techniques. This protection can help to identify an attacker and prevent any exploits from being successful. Because the attempt to obtain useful information about the network is blocked, the attacker will likely move on to another, easier target that does not have sufficient protection against this type of reconnaissance.

The Threat Detection and Prevention module also allows for the creation and use of customized signatures. *User-defined signatures* can provide a simple way to create custom security policies based upon pattern-matching HTTP URL requests, file transfers, DNS requests, email, SNMP, news group, and username data by using a wizard style configuration. For more advanced users, the OpenSignature policy can be used by security professionals to create customized signatures based upon SNORT[15] syntax.

Web application protection

Web application protection can protect web applications against sophisticated application-level attacks such as SQL injection, XSS, PHP file-includes, and CSRF. This technology expands security capabilities to meet both compliance requirements and threat evolution.

The *IBM X-Force 2009 Trend and Risk Report*[16] has the following statements:

- "During the last four years, we have seen a massive increase in web application vulnerabilities, so much so that these vulnerabilities make up more than half of the disclosed vulnerabilities since 2006."
- "The predominate types of vulnerabilities affecting web applications are Cross-Site Scripting (XSS), SQL Injection, and File Include vulnerabilities."

The IBM Security Network IPS provides excellent coverage for these web application vulnerabilities; when used in conjunction with other IBM applications the security posture of protecting these web applications can be greatly increased. When the IBM Security Network IPS is used in conjunction with the IBM Security SiteProtector System[17] and IBM Rational® AppScan®[18], customized web application protection policies can be created by using results from IBM Rational AppScan. The IBM Security SiteProtector System can convert IBM Rational AppScan results into a web application policy to provide the most accurate protection of your web applications.

Another major challenge with protecting web applications is how to implement protection for secure web applications that send and receive encrypted data. Most secure web applications use Secure Sockets Layer and Transport Layer Security (SSL/TLS), which prevents any third party from being able to see the transferred information, including a network IPS. Implementing SSL/TLS encryption/decryption technology is not always a viable option for a network IPS because there is increased overhead in data decryption that can drastically decrease the overall performance and the need to install and update the SSL/TLS certificates for each web server directly on the network IPS.

This dilemma can be solved by deploying the IBM Security Network IPS in conjunction with an IBM Tivoli® Access Manager for e-business solution. Along with many other benefits[19], the Tivoli Access Manager for e-business solution can provide the front-end data encryption for client and web application transactions, while the communication between the Tivoli Access Manager for e-business solution and the back-end web applications can be transferred in an unencrypted format. This solution provides both the advantages of

[15] Snort is an open source network intrusion prevention and detection system: http://www.snort.org/

[16] Obtain the IBM X-Force Trend and Risk Reports: http://www.ibm.com/services/us/iss/xforce/

[17] Learn more about IBM Security SiteProtector System in *IBM Enterprise Security Architecture for Network, Server and Endpoint*, SG24-7581.

[18] Learn more about IBM Rational AppScan in *Improving Your Web Application Software Development Life Cycle's Security Posture with IBM Rational AppScan*, REDP-4530.

[19] Learn more about IBM Tivoli Access Manager for e-business in *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

offloading the resources needed to encrypt and decrypt data from the web servers, and more important, allowing for the IBM Security Network IPS to provide protection against the threats that target the web application.

Data security

The *data security* module monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. You can configure the data security module to scan a multitude of document types sent through instant messenger programs, Internet chat relay (IRC) channels, HTTP, file shares, FTP, email, and IMAP protocols. The data security module has built in signatures to identify credit card numbers, names, dates, U.S. dollar amounts, email addresses, social security numbers, U.S. phone numbers, and U.S. postal addresses. It also has the ability to create custom signatures to identify any additional data deemed sensitive.

With the data security module, all individual signatures can be used in conjunction with one another. For example, you can create a signature that looks for names, email addresses, phone numbers, and addresses. A large block of this type of information being transferred out of the network might indicate that an internal employee is trying to misappropriate a list of customers.

Application Control

The *Application Control* module manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, peer-to-peer, instant messaging, and tunneling. It enforces network application and service access based on corporate policy and governance.

Peer-to-peer (P2P) networks account for a myriad of issues within a corporate network. Cisco Systems[20] reports that in 2009, P2P file-sharing networks accounted for 37% of all Internet traffic. By restricting P2P file-sharing using the IBM Security Network IPS, organizations can recoup this bandwidth and extend the lifetime of their existing network infrastructure. P2P file-sharing is notorious for transferring copyrighted materials, such as music and videos, that could have adverse and costly legal ramifications. These networks are also widely used to spread malicious software to unsuspecting users and update mechanisms for botnet infected systems. The IBM Security Network IPS provides detection and prevention of many of the most common P2P networks such as Gnutella, Napster, BearShare, and BitTorrents.

Protocol tunnelling is another aspect in which the network IPS can provide protection. Protocol tunneling is used by individuals who are trying to circumvent security policies that restrict access to various activities on the Internet.

Reliability

Devices placed in the flow of network traffic must be extremely reliable. The IBM Security Network IPS offers high availability (active/active or active/passive), hot-swappable redundant power supplies, and hot-swappable redundant hard drives to help maintain the flow of network traffic. The IBM Security Network IPS also provides network bypass functionality by using either internal or external bypass modules in case of system error or power failure.

The IBM Security Network IPS can be integrated into existing high availability networks that provide multiple network paths to protect against network outages. You may also integrate the IBM Security Network IPS into both active/active and active/passive high availability networks. In addition, the geographic high availability option can use the management port to

[20] Cisco Visual Networking Index: Forecast and Methodology, 2009-2014:
http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_Networking_Solutions_White_Paper.html

share quarantine-blocking decisions to ensure a secure failover to a geographically remote standby network IPS device. Figure 8 illustrates this concept.

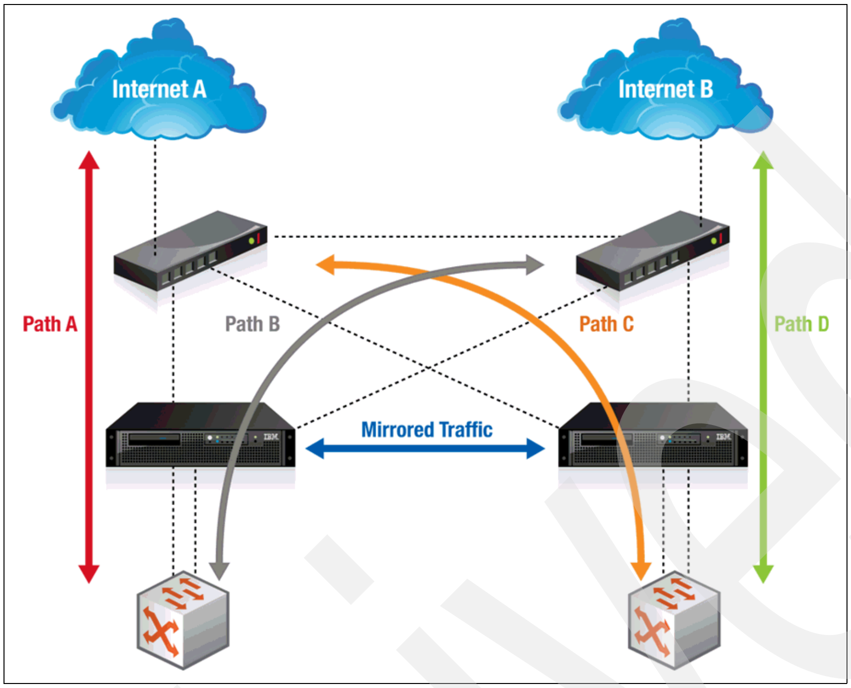


Figure 8 Logical diagram of high availability

Deployment

The IBM Security Network IPS features a Layer 2 architecture that does not require network reconfiguration. In addition, network and security administrators can become comfortable and familiar with the device's behavior by choosing one of three *operating modes* or any combination when using multi-segment models:

- Inline prevention
- Inline simulation
- Passive monitoring

When first deployed, the IBM Security Network IPS can be run in simulation mode to identify threats and network behavior without causing an impact to network traffic. You can use this data-gathering period to configure the security policy of the network IPS to provide the balance of business uptime and threat protection. After the security policy configuration has been completed, the IBM Security Network IPS can be placed in protection mode with a simple policy change to the device and without the need for any physical changes to the network.

Figure 9 shows an example of how to use the three operating modes.

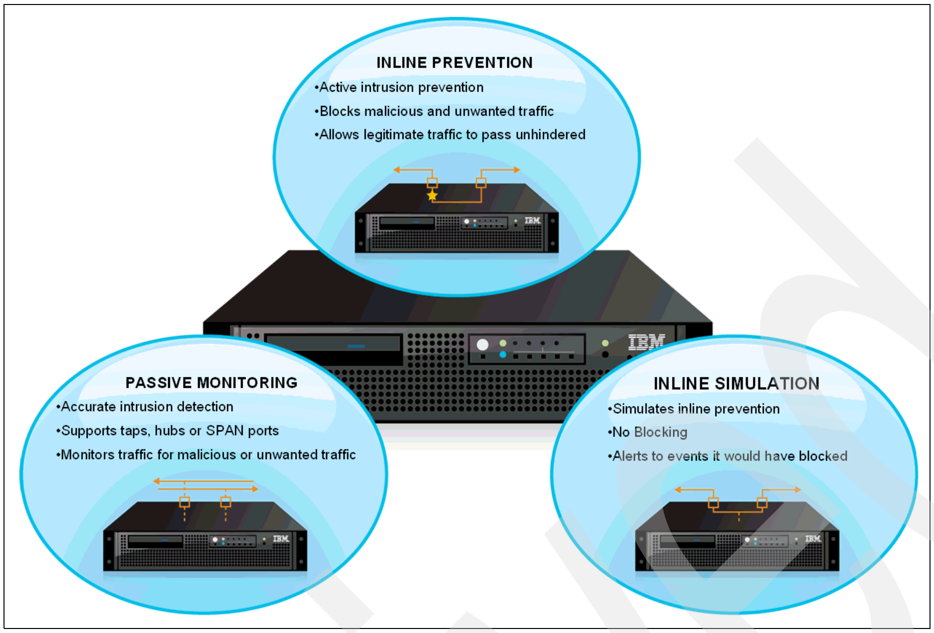

INLINE PREVENTION
•Active intrusion prevention
•Blocks malicious and unwanted traffic
•Allows legitimate traffic to pass unhindered
PASSIVE MONITORING
•Accurate intrusion detection
•Supports taps, hubs or SPAN ports
•Monitors traffic for malicious or unwanted traffic
INLINE SIMULATION
•Simulates inline prevention
•No Blocking
•Alerts to events it would have blocked
IBM

Figure 9 Security interface operating modes

The IPv4 protocol still dominates todays network infrastructure, but times are changing. As the capabilities of IPv4 are reaching their upper limits, networks are starting to migrate to IPv6 environments. During this migration, there is a need to mix both IPv4 and IPv6 traffic in the same network, or a mixed network. The IBM Security Network IPS works natively in IPv4, IPv6, and mixed networks for both managing the device and protecting data that flows through these networks.

The IBM Security Network IPS solution has the flexibility of being combined with other systems to be deployed in various environments, in addition to being integrated into the physical network. The IBM Security Network IPS virtual appliances can be deployed on VMWare ESX4 systems. The IBM Security Network IPS for Crossbeam can be deployed on the Crossbeam X-Series chassis.

Management

A key component to any network IPS is management of configuration and reporting. The IBM Security Network IPS provides both a customizable web user interface and a central management system known as the IBM Security SiteProtector System.

With the web user interface, you can fully configure all aspects of the IBM Security Network IPS, from policies to event reporting. It also provides for analysis and reporting for security events, firewall logs, analysis statistics, throughput utilization, and the overall health of the network IPS.

Organizations often have various people with various job functions to manage security products, which creates a need for multiple levels of access to a system. Certain employees who monitor for security events do not always need to apply changes. To accommodate this approach, organizations using the IBM Security Network IPS can define administrator or read-only access to the web user interface by using Active Directory, LDAP, or Radius authentication. By using a remote authentication method, removing the remote authentication access is much simpler than having to change passwords or revoke access on each individual system when an employee’s access is no longer allowed.

IBM Security Network IPS devices can be centrally managed by the IBM Security SiteProtector System. The IBM Security SiteProtector System can provide simple, powerful configuration and control of IBM agents, along with robust reporting, event correlation, and comprehensive alerting. SiteProtector allows for multiple layers of policy hierarchy, so an organization can apply policies at a group level to multiple agents, to individual agents, or any combination in between. This structure can reduce the overall complexity of security policy deployments and still provide the policy granularity that is needed within an organization.

Both the IBM Security Network IPS web user interface and the IBM Security SiteProtector System provide multiple ways of accessing event data through multiple transports, in addition to event analysis views within the respective management consoles. The use of SNMP and email capabilities provide additional methods of propagating data for event reporting. With these capabilities, reporting can be integrated with a multitude of other systems from multiple vendors when using centralized reporting systems.

Another requirement for any network IPS is the need to configure the security policy to best protect against threats. The IBM Security Network IPS allows for the use of an X-Force default policy, also known as *X-Force Virtual Patch Policy*. The X-Force policy is a set of default attack signatures that are preconfigured to protect against the most dangerous threats. For each new content update for the IBM Security Network IPS, X-Force makes changes to this policy as these threats evolve. The IBM Security Network IPS can be configured to always use the X-Force recommendations, up to but not past, a specific security release version, or to never use the recommendations. Security policies can be customized to use both the X-Force recommendations and any additions, changes, or removal of security signatures. No custom configuration are overridden if the X-Force recommendations change during a security update.

As previously described, the current state of networking consists mostly of either IPv4, IPv6, or a mix of both. The IBM Security Network IPS provides security policy management for each of these networks. The management of the IBM Security Network IPS can also be configured to work in each of these networks.

Confidence

The IBM Security Network IPS is backed by the IBM X-Force Research and Development team to provide updated content to continuously provide *ahead of the threat protection* as threats evolve. The IBM X-Force Research and Development team conducts original, primary research on vulnerabilities and threats, which is then applied to the IBM Security Network IPS in the form of security content updates. The X-Force team is credited with discovering and mitigating more major software vulnerabilities since 1998 than any other commercial security research organizations.

The IBM X-Force Research and Development team compiles and analyzes data from tens of thousands of sensors around the world that are under management of the IBM Managed Security Services group. This data allows the X-Force team to identify the ever changing trend patterns in Internet, protocol, and content usage and the threats that try to take advantage of these. The X-Force team also maintains a research network that is comprised of both internal IBM networks and external customer networks. The X-Force team can use this research network to proactively qualify security updates before being released. Because of this research, the IBM Security Network IPS does not have to rely on third-party research to provide up-to-date security content.

Retail chain scenario: Implementing an end-to-end network security solution

In this section, we provide a retail scenario as an example of using the IBM Security Network IPS to protect network transactions and secure data necessary for various aspects of the business.

Scenario description

In this scenario, a retail firm has 600 store locations throughout the United States and a website to sell the firm's products. The retail firm also has integrated dedicated application and network connections with multiple offices and the firm's various business partners. The corporate data center houses all the core application servers and databases to conduct business, including web servers, email servers, supply-chain management, and processing of credit card transactions for each store location.

The retail firm has identified the need to protect the various parts of the organization from both external and internal threats. The Chief Security Officer (CSO) has tasked the organization to provide a solution to protect the network on which the servers, workstations, and data storage resides. Because so many separate locations need access to the data center, and the Internet, the network perimeter has become blurred. The following networking zones have been defined as the key locations to provide protection:

- Public Internet access including online ordering
- Internet and intranet connections at all store locations and offices
- Connections to business partners
- Data center and intranet connections

Figure 10 on page 31 shows the various zones that need protection. Each zone has unique protection requirements and needs a customized protection solution that is based on the systems that are operating in each zone. Because of the large number of locations to protect, the solution must provide a centralized command and control system to allow for ease of deployment, management, and monitoring.

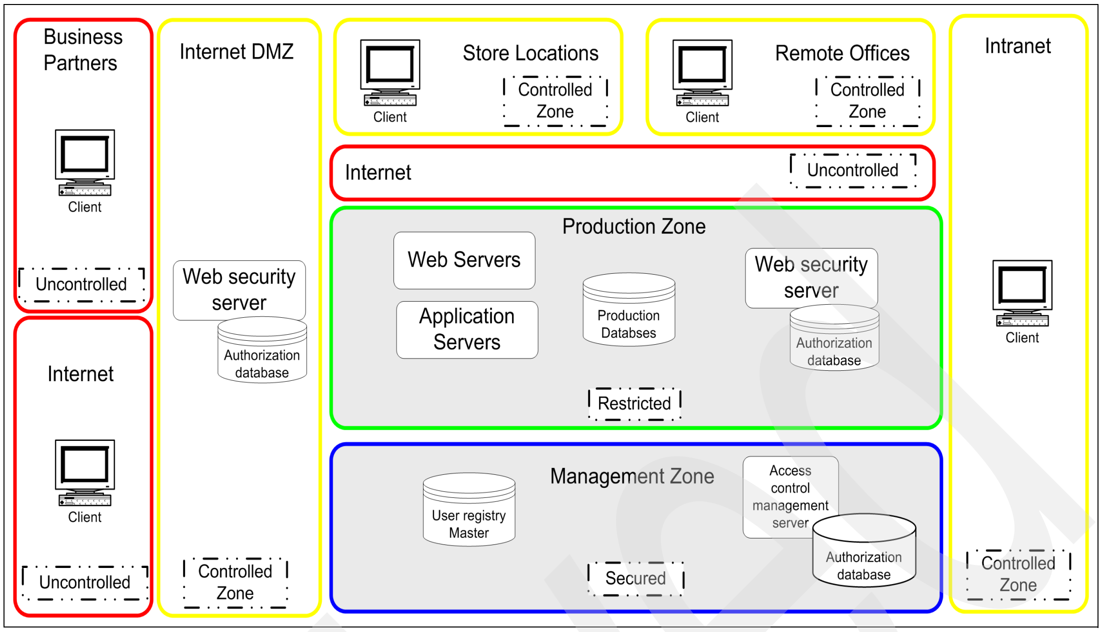


Figure 10 Diagram of the various network zones

Solution

To fulfill all these requirements, an IBM Security Network IPS provides the ability to protect the various needs set forth by the CSO. The IBM Security Network IPS appliances can be deployed throughout the various zones, where each appliance can be configured to match the needs of each area of deployment.

Public Internet access

Allowing access from the Internet is a requirement for many aspects of the business. Customers need to browse the organization's website and complete online orders. Emails need to be sent to and from customers and employees. By deploying the IBM Security Network IPS appliance, these transactions can be protected from various threats.

Figure 11 on page 32 outlines the layers of protection against the outsider threat:

- The network IPS in front of the Internet DMZ provides protection for unencrypted traffic such as email and web traffic.
- The Virtual Patch module protects against exploits that are targeted at the web server and application servers.
- The Threat Detection and Prevention module protects against reconnaissance scans that are designed to gain information about the systems within the network.
- The Web Application Protection module protects the web applications that handle unencrypted HTTP web traffic from various web based attacks such as SQL Injection and Cross Site Scripting.

To protect encrypted traffic that is used for online ordering and customer data housing, the network IPS is used in conjunction with the Tivoli Access Manger for e-business (abbreviated as TAMeb in Figure 11 on page 32) solution, which provides front-end data encryption for client and web application transactions, while the communication between the Tivoli Access Manager for e-business solution and the back-end web applications can be transferred in an unencrypted format. This approach allows the Web Application Protection module of the network IPS to inspect and protect the web servers from web-based attacks.

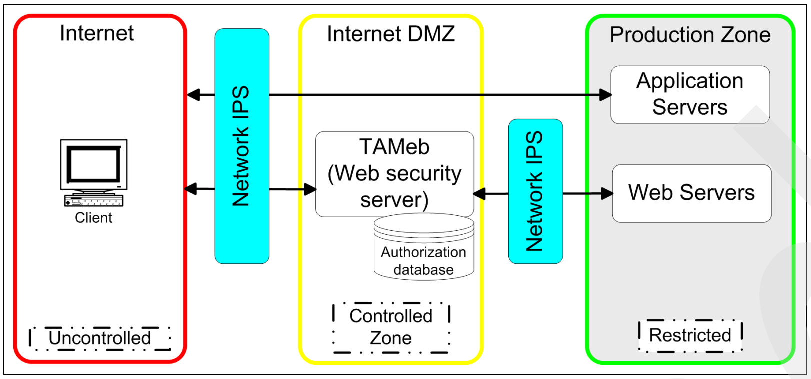


Figure 11 Protection diagram for Internet protection

Internet and intranet connections at all store locations and offices

The retail firm has hundreds of remote locations and offices that must all work together and share information. Protecting these multitudes of corporate locations is a vital part of a layered network security solution.

The organization has implemented dedicated connections from each remote location to the data center by using encryption endpoints to protect data being sent between each location, such as credit card transactions, employee records, and supply chain management data. The use of encryption endpoints protects this data from unintended parties that may intercept this data from being accessed. These dedicated connections from each location are an entry point to the core of the network and provide direct access to production servers and require protection. These locations are potential sources of compromise by both insider threats and external threats from the public Internet if one of these locations is compromised. Deploying the network IPS in a layered approach can protect against both the internal and external threats.

The Client-side Application Protection module can protect the employees' computers as they browse the web, send and receive emails, and other applications that use access to the Internet. The Application Control module can detect and prevent applications that are against the corporate security policy accessing the Internet. The Virtual Patch module can protect the systems in these remote locations against exploits targeted at the operating systems and applications. The Data Security Module can detect attempts to gather transmitted personally identifiable information (PII), such as a batch of customer credit card numbers that are sent through email by a store employee.

Deploying the IBM Network IPS at each location also provides for compartmentalized protection. If a store is compromised by an employee who is plugging in an infected USB thumbdrive to a workstation, the threat can be contained to that one location. This protection can prevent a widespread outbreak to other store and office locations and the data center. The Threat Detection Module can identify and protect against these outbreaks based on the network footprint that these pieces of malware propagate and communicate.

Figure 12 illustrates the protection strategy for store locations and offices.

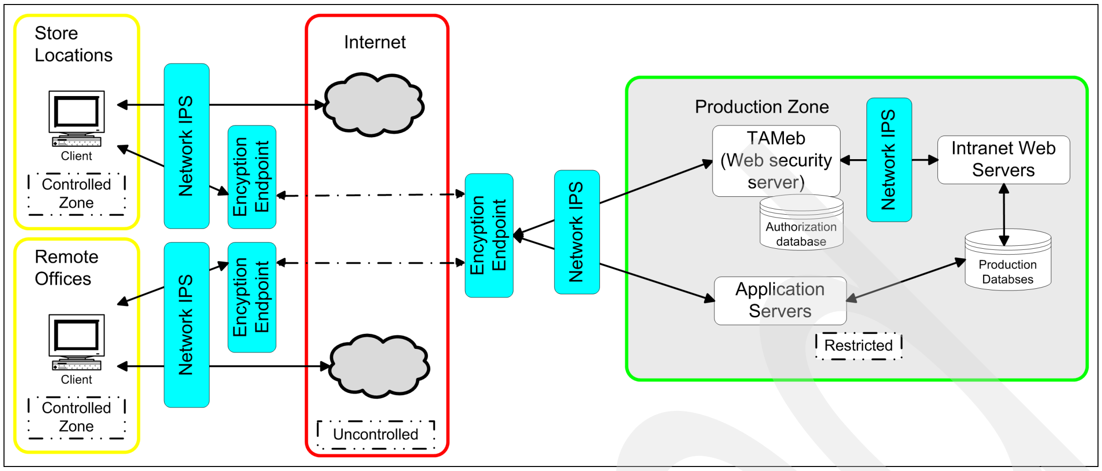


Figure 12 Protection diagram for remote stores and offices

Connection to business partners

In today’s business world, organizations are becoming more integrated with the partners that are needed to conduct business. Vendors, suppliers, and marketing companies play a major role in the retail firm’s ability to provide products to the customer, and each of these organizations must communicate efficiently. To accomplish this challenge, the retail firm has implemented encrypted connections between the organizations to protect their data as it traverses the Internet. Several business partners have dedicated encryption endpoints; other partners use encrypted HTTPS traffic to communicate with the retail firm.

Each connection to the business partners must be protected as a layered network security solution. Similar to the store locations and remote offices, the business partners require a higher level of access to the data center than to the Internet. Because of this level of access, the connection to the business partners can pose a greater threat than that of the Internet, because the retail firm has no control over the security solution implemented by each business partner. To remedy this, the IBM Security Network IPS is deployed at the different encryption endpoints to provide protection against the threats presented by this elevated threat by utilizing the different protection modules. The network IPS is also used in conjunction with the Tivoli Access Manger for e-business solution to provide protection for the connections that use encrypted HTTPS.

Figure 13 illustrates the protection strategy for business partners.

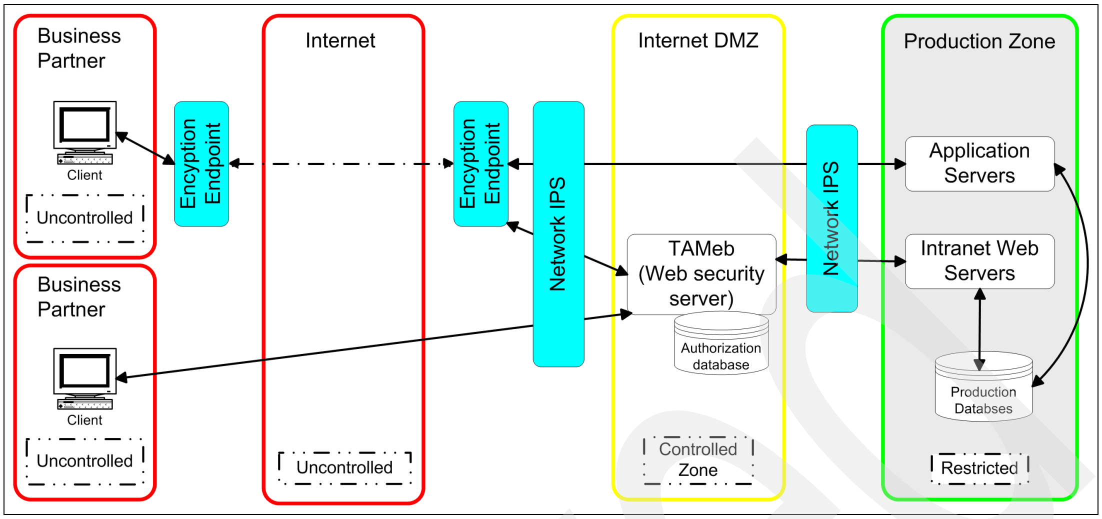


Figure 13 Protection diagram for business partners

Data center

At the heart of the retails firm's business network is the data center. The data center houses all the application servers, web servers, databases, and management systems. The data center also houses the intranet that is used by the employees to accomplish the daily needs to operate the business. Each area of the data center has a unique role to play in the organization's network operations.

The retail firm's data center is divided into three zones.

- The intranet is a controlled zone with access that is limited to employees who run the business, such as in human resources, supply chain, order fulfillment, and management.
- The production zone houses the application servers, web servers, and databases. This zone is restricted to a smaller set of employees who maintain these systems, such as web developers, system administrators, and database administrators.
- The management zone is a secured zone that controls key security systems such as user accounts and access management controls. This zone is restricted to senior system administrators and security professionals.

The IBM Security Network IPS is deployed between each zone to maintain this division of access. Figure 14 illustrates each of these zones for data center protection.

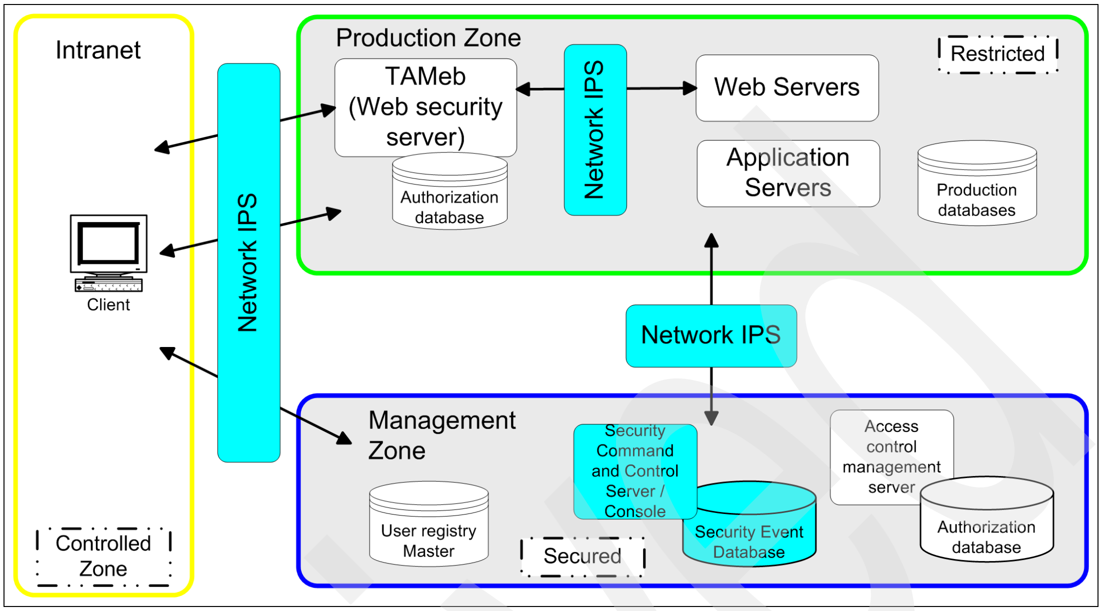


Figure 14   Protection diagram for the data center

Command and control system

The IBM Security SiteProtector System has been deployed in the Management Zone of the data center to manage and monitor the IBM Security Network IPS appliances. Because the IBM Security SiteProtector System allows for managing agents at group levels, the hundreds of Network IPS appliances that are deployed across the country can be centrally managed by using only a few security policies. Because each store shares the same network policy and application needs, all 600 network IPS appliances that are deployed at store locations can be managed by a single set of security policies. The office locations are controlled by another set of security policies, and the business partners by yet another set of policies. As changes in network policy and policy exceptions are made for any of these locations, the group structure can be changed to minimize the complexity of security policy management. The network IPS appliances in the data center have their own highly customized security policies to meet the security needs of each zone.

The retail firm has configured varying levels of access for the users of the organization’s security team to access the IBM Security SiteProtector System. The members of the security operations center have been given access to monitor the security events and create management and executive-level reports but without the ability to affect changes on the network IPS appliances. The ability of making changes, such as policy changes and content update, to the Network IPS appliances has been restricted to the senior level security professionals.

Summary

In this guide, we looked at the composition of today’s IT network perimeter, which has been diluted from a well-defined set of ingress and egress points to a mesh of undetectable flows from devices that are capable of accessing and penetrating every organization’s resources. We then examined the challenges for secure business transactions by looking at the threat landscape.

After we investigated these increasing threats and the various ways of addressing proper mitigation techniques, we described how the IBM Security Network IPS can help you consolidate intrusion prevention with data and web application security into a single, optimized appliance for faster, more accurate security protection.

Other resources for more information

The following publications are useful as a further source of information:

- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- *IBM Enterprise Security Architecture for Network, Server and Endpoint*, SG24-7581
- *Improving Your Web Application Software Development Life Cycle's Security Posture with IBM Rational AppScan*, REDP-4530

The team who wrote this guide

This guide was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO).

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of software security architecture and network computing technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 24 years of experience in a variety of areas that are related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Diogo Bulhoes is a security expert with over 15 years of experience. He works for IBM in Brazil as a Client Technical Specialist within the Tivoli Security group, specializing in the security products that are formerly known as ISS Proventia. Prior to joining IBM, he worked for several security vendors as a Security Engineer, supporting channels and developing new business in Latin America. He holds a variety of security certifications such as SANS GIAC Certified Firewall Analyst and Modulo Certified Security Officer.

Matthew Dobbs is a Technical Team Lead for the Level 2 Technical Support for IBM Security. He has worked with IBM Security for six years, with a technical specialization in IPS products. Prior to joining IBM, Matthew worked as a System Developer and Consultant in the telecommunications industry. He holds a Bachelor of Science in Computer Engineering degree from the Georgia Institute of Technology.

Thanks to the following people for their contributions to this project:

Diane Sherman
International Technical Support Organization, Austin Center

Greg Abelar, Brian Fitch, Jeremy Hatfield, Robert McEwin, Brian Moran
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Learn more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document, REDP-4683-00, was created or updated on January 21, 2011.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at
http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AppScan®
IBM®
Proventia®
Rational®
Redbooks®
Redguide™
Redbooks (logo) ®
Tivoli®
Virtual Patch®
X-Force®

The following terms are trademarks of other companies:

Adobe, the Adobe logo, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.