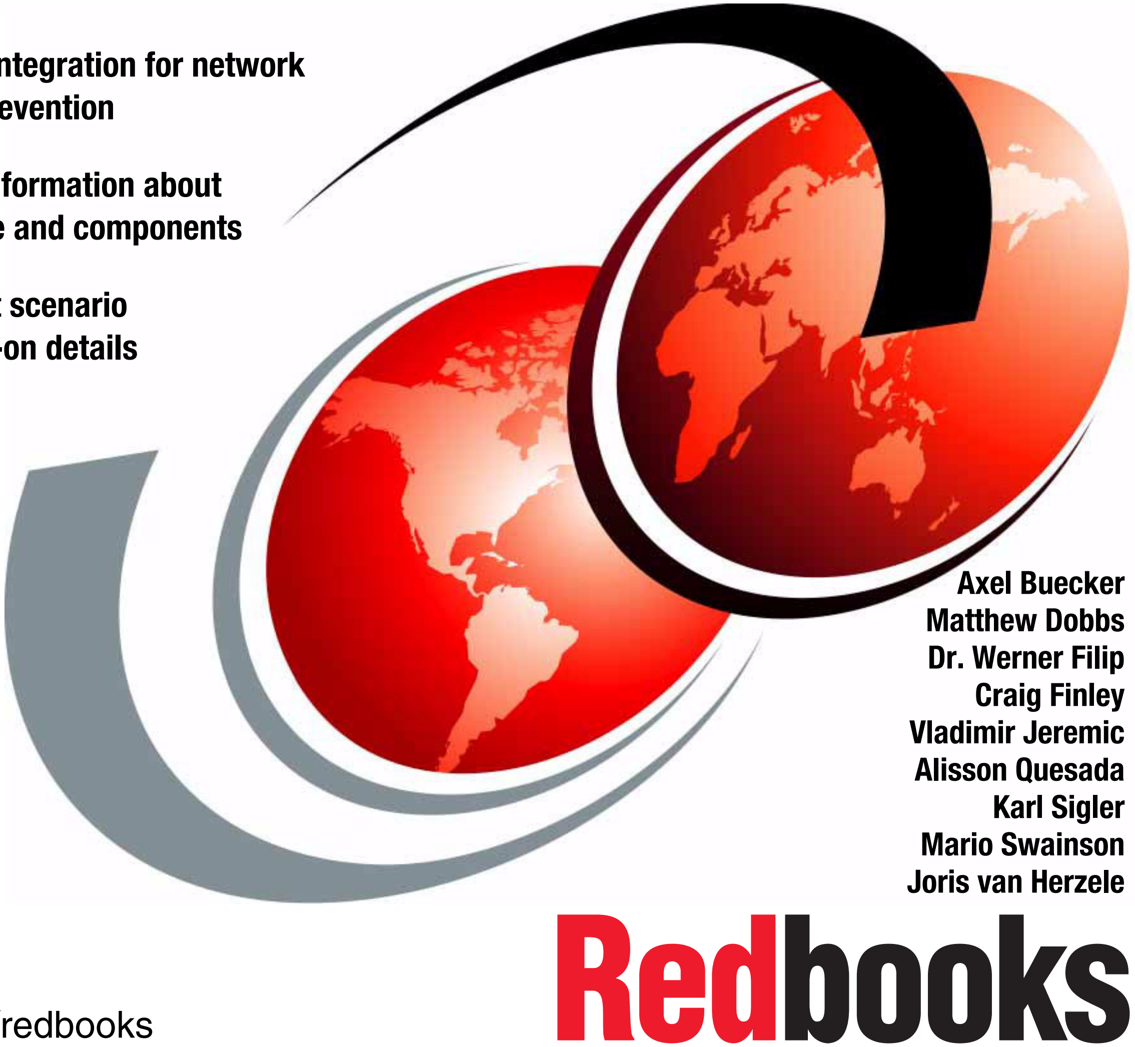
Network Intrusion Prevention Design Guide

Using IBM Security Network IPS

- Enterprise integration for network intrusion prevention
- Complete information about architecture and components
- Deployment scenario with hands-on details



Axel Buecker
Matthew Dobbs
Dr. Werner Filip
Craig Finley
Vladimir Jeremic
Alisson Quesada
Karl Sigler
Mario Swainson
Joris van Herzele

Redbooks

ibm.com/redbooks

International Technical Support Organization

Network Intrusion Prevention Design Guide: Using IBM Security Network IPS

December 2011

SG24-7979-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (December 2011)

This edition applies to IBM Security Network Intrusion Prevention System physical appliances (GX7x, GX5x, and GX4x) and virtual appliances (GVx) based on a Version 4.x firmware.

Contents

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 websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites 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.

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:

AIX®
AppScan®
developerWorks®
Guardium®
IBM®
InfoSphere®
OpenPages®
Proventia®
Rational®
Real Secure®
Redbooks®
Redguide™
Redpaper™
Redbooks (logo) ®
Service Request Manager®
Tivoli®
Virtual Patch®
WebSphere®

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.

Intel Xeon, Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

Preface

Every organization today needs to manage the risk of exposing business-critical data, improve business continuity, and minimize the cost of managing IT security. Most all IT assets of an organization share a common network infrastructure. Therefore, the first line of defense is to establish proper network security. This security is a prerequisite for a logical set of technical countermeasures to protect from many different attack vectors that use the network to infiltrate the backbone of an organization.

The IBM® Security Network Intrusion Prevention System (IPS) stops network-based threats before they can impact the business operations of an organization. *Preemptive protection*, which is protection that works ahead of a threat, is available by means of a combination of line-speed performance, security intelligence, and a modular protection engine that enables security convergence. By consolidating network security demands for data security and protection for web applications, the IBM Security Network IPS serves as the security platform that can reduce the costs and complexity of deploying and managing point solutions.

This IBM Redbooks® publication provides IT architects and security specialists a better understanding of the challenging topic of blocking network threats. This book highlights security convergence of IBM Virtual Patch® technology, data security, and web application protection. In addition, this book explores the technical foundation of the IBM Security Network IPS. It explains how to set up, configure, and maintain proper network perimeter protection within a real-world business scenario.

The team who wrote this book

This book 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 in Austin, Texas. He writes extensively and teaches IBM classes worldwide about software security architecture and network computing technologies. He has 25 years of experience in various areas 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. He has a degree in Computer Science from the University of Bremen in Germany.

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

Dr. Werner Filip is a professor for the Department for Computer Science and Engineering at the University of Applied Sciences, Frankfurt am Main, Germany, and a Consultant in IT Security. His primary research interests are systems and network management and applied security. Before joining the Frankfurt University of Applied Sciences, he worked 25 years for IBM in various positions. During his last 10 years with IBM, he was a Consultant in Systems and Network Management at the former IBM European Networking Center in Germany. Dr. Filip received a Diploma in Mathematics and a Doctorate in Computer Science from the Technical University Darmstadt in Germany.

Craig Finley, a Certified Information Systems Security Professional (CISSP), has over 10 years of LAN and WAN management experience with a focus on network security. He joined IBM six years ago as a Technical Support Analyst on the Global Customer Support Team for IBM Security Solutions. In his role, he developed and delivered new-hire training and new-release update training for Customer Support. He delivered training to audiences in multiple theaters, including the Americas, EMEA, and APAC. During this time, Craig also served as the lead trainer for third-party products in data loss prevention, disk encryption, and intrusion prevention. Recently he joined the IBM Tivoli® Technical Enablement team. His training audiences include IBM Sales and Technical Sales, Services, Business Partners, Support, and Customers worldwide. Currently Craig is a member of the Technology Associates of Georgia and the Information Systems Security Association of Metro-Atlanta.

Vladimir Jeremic is a Security Enablement Instructor for the IBM Security Systems portfolio. He primarily focuses on IBM Security Solutions for Network, Server and Endpoint (formerly known as the *IBM Internet Security Systems (IBM ISS) portfolio*). He has experience in designing, developing, and delivering learning materials. Vladimir also worked for many years as a Certified Security Managing Consultant with the IBM Global Services team, where he focused on architecture and implementation of the IBM Tivoli Security portfolio. He has over ten years of experience in the IT field related to security, networking, and programming. Vladimir is a Tivoli Certified Professional and IBM Certified Consultant. He holds a Bachelor of Science degree in Electrical Engineering from the University of Novi Sad in Serbia.

Alisson Quesada is an IBM Security IT Specialist and he works with government and banking customers in Brazil. He has broad experience with Security Information and Event Management (SIEM) and Identity and Access Management solutions. He started working with IBM Intrusion Prevention solutions one year ago. Alisson has over 7 years of experience in IT Service Management and IT Security. He has a degree in Network Communications Engineering from the University of Brasilia and a Master of Business Administration degree in IT Governance from the Catholic University of Brasilia.

Karl Sigler is a Senior Security Instructor for IBM Security Systems. He joined IBM in 2006 as part of its acquisition of Internet Security Systems. Karl has had a life-long interest in information security, which he has been doing professionally since 1996. He has led product-oriented classes, such as CheckPoint, RSA, and ISS, and vendor-neutral classes, such as intrusion analysis, incident handling, vulnerability assessment, and ethical hacking. He is a published author and is responsible for the creation of the first Live Linux CD dedicated to security, *Knoppix Security Tools Distribution*.

Mario Swainson is a Certified Information Security Professional. His skills include designing and implementing secure networks; training and consulting security best practices; and reviewing policies, procedures, and standards. Mario was part of the IBM Security Solutions team, serving the initial and ongoing sales education needs of the Security Sales force and technical support community. Before joining IBM, Mario was a level 3 NetBackup support engineer with Veritas Software (now *Symantec Software*). He holds Associate in Science degrees in Network Services and Cisco Internetworking from Seminole State College. He is completing a Bachelor of Science degree in Information Technology from Southern Polytechnic State University.

Joris van Herzele is an IT Specialist based in Brussels, Belgium. He provides research, design, and evaluation analysis for IBM Managed Security Services. He is a Certified Information Systems Security Professional with 10 years of experience in the network and security field and is a subject matter expert on threat management. Before his current role, Joris taught classes in the EMEA region through IBM X-Force education services. He was also a technical presales engineer advocating the comprehensive product portfolio of IBM Security Systems.

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

Gregory Abelar
Lamar Bailey
James Bowerman
John Brown
Carlos Caballero
Brian Fitch
Don Hall
Duncan Hoopes
Leandro Jordino Pereira Marques
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.

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

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 78758

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

Part 1

Architecture and design

Part 1 highlights the overall business context for network intrusion prevention systems (IPSs). It explains the general business requirements for a network IPS and describes a framework for providing network intrusion prevention functionality throughout an organization. This part introduces the high-level components and concepts for the design of a network IPS using the IBM Security Network IPS. In addition, this part provides an understanding of the high-level product architecture of the IBM Security Network IPS.

This part includes the following chapters:

- Chapter 1, “Business context for threat and vulnerability management” on page 3
- Chapter 2, “Introducing the IBM Security Network IPS solution” on page 35
- Chapter 3, “IBM Security Network IPS architecture” on page 73
- Chapter 4, “IBM Security Network IPS solution design and management” on page 103

1

Business context for threat and vulnerability management

Security is a major consideration in the way that business and information technology (IT) systems are designed, built, operated, and managed. The need to integrate security into discussions about business functions and operations exists more than ever.

This chapter explores some of the concerns that characterize security requirements of, and threats to, business and IT systems. It identifies several of the business drivers that illustrate these concerns, including managing risk and cost, and compliance to business policies and external regulations, showing how they can be translated into frameworks to enable enterprise security.

To help with security challenges, IBM has created a bridge to address the communication gap between the business and technical perspectives of security to enable simplification of thought and process. The *IBM Security Framework* can help translate the business view, and the *IBM Security Blueprint* describes the technology landscape view. In concert, they can help unite the experiences that we have gained from working with many clients to build a comprehensive solution view.

The last section of this chapter focuses on threat and vulnerability management for networks, servers, and endpoints by exploring the current landscape of malware and the important concept of the *Advanced Persistent Threat*. It also looks closely at how to deal with threat and vulnerability management in an organized way.

This chapter includes the following sections:

- Drivers that influence security
- IBM Security Framework
- IBM Security Blueprint
- Threat and vulnerability management
- Conclusion

1.1 Drivers that influence security

Most projects today are driven by both business and IT drivers, although business drivers are almost always the initiating factor. Let us take a closer look at these influencing factors:

- *Business drivers* measure value, risk, and economic costs that influence their approach to IT security. Value drivers determine the worth of assets of the system to the business and of the business itself.

  Risk drivers involve compliance, corporate structure, corporate image, and the risk tolerance of the company. Economic drivers determine productivity impact, competitive advantage, and system cost.
- *IT drivers* represent operational constraints in the general IT environment. For example, the complexity of a system, including its environment, that is exposed to internal and external threats presents risks that the organization must address.

Business drivers also represent issues and consequences of significance to the stakeholders of the managed business system. This set of drivers might vary from industry to industry, from organization to organization in the same industry, and from different business applications in an organization.

IT drivers represent technical considerations that affect the trustworthiness of the IT environment and likely the managed business systems as a whole. IT drivers are universal and must be considered within the context of the business drivers in all efforts. The combination of business and IT drivers represents the key initiatives for security management.

1.1.1 Business drivers that influence security

Business drivers represent a relationship between the IT organization and the rest of the business. They refer to business values that must be supported by the IT security infrastructure.

Correct and reliable operation

Correct and reliable operation is the degree to which the business must be accurate and consistent in its operation. *Correct operation* means that the operations perform the proper response or function with no errors. *Reliable* means that the same result occurs all the time. Any IT system must consistently provide stakeholders with the expected results.

Security events and incidents might affect the correct and reliable operation of these business processes. It might also affect the underlying IT infrastructure or upstream and downstream business processes. The consequences of a defective service (incorrect or varying results over time) might be significant to the consumer of the service, and therefore, to the provider of the service.

Service level agreements

The service level agreements (SLA) driver applies to circumstances where security threats and threat agents can affect the ability of an organization to conduct business. SLAs incorporate acceptable conditions of operation within an organization. SLAs might vary from business system to business system or application to application. Availability of systems, data, and processes is a condition commonly referenced within SLAs.

IT asset value

From a business perspective, the IT asset value is directly related to the value of the business transactions that it supports. These assets might be tangible (machines) or intangible (data). For an e-retailer, these assets are tangible. For a financial services company, the asset might be the client information or other data used in transactions of the system.

Protection of the business asset value or brand image

The protection of business asset value of brand image driver captures the desire of the firm to protect its image. The loss of good will from a security incident or attack has a direct consequence to the business. Therefore, the security measures are likely to be proportional to the consequence. When the desire to avoid negative publicity increases, upon encountering a security breach, the stipulation for this driver becomes stronger.

Legal and regulatory compliance

Legal and regulatory compliance refers to externally imposed conditions on transactions in both the business system and the company. These conditions include the rules and policies imposed by regulatory and government agencies. Civil, criminal liability, or regulatory penalty from a security incident or attack can have a negative impact on the business. Therefore, the amount of regulation and steps ensure that compliance must be factored in this driver. The regulation includes privacy issues, the ability to prove the transaction initiator, and proving compliance.

An implemented log management system can identify who does what, where, and when. Log management, therefore, is part of an IT security compliance management system. For the log retention period, it ensures that the necessary information is available and can be analyzed or interpreted to a level that can help management to better investigate security incidents or comply with external regulation or laws.

Compliance is a key business driver today, and log management must be a part of every IT security compliance management solution. Log management can even be implemented alone as an initial step toward a larger IT security compliance initiative. As mentioned already, many international standards and regulatory controls require logging to be enabled and implemented. Also, these logs must be analyzed periodically and stored for a specific time, depending on the particular standard or regulatory control.

Contractual obligation

Security measures for an IT system are likely to be proportional to the consequences encountered when the business encounters contractual liability from a security attack. Depending on the structure and terms of the contract, the consequence might lead to financial loss or liability. For example, when security incidents are encountered, the business might be unable to fulfill its contractual obligations of providing goods or services.

Financial loss and liability

Direct or indirect financial loss is a consequence to the business as a result of a security incident. Direct loss might include theft of an asset, theft of a service, or fraud. Indirect loss might include loss based on civil or criminal judgment, loss of good will, or reprioritized budget allocation. This driver identifies the fact that security measures for an IT system are likely to be in proportion to these consequences.

Critical infrastructure

The critical infrastructure driver applies where security threats or threat agents can have a major impact on services or resources that are common to, or shared among, a community of businesses, the population at large, or both. Examples include telecommunications, electrical power, transportation systems, and computing. The loss of critical infrastructure by its provider might have a ripple effect, causing secondary losses and driving security decisions for those who are affected. An important part of risk analysis is identifying critical infrastructure.

Safety and survival

The safety and survival driver applies where security threats and threat agents can have a major impact on aspects of human life, government function, and socio-economic systems. Examples of processes to be considered for safety and survival impact include continuity of critical infrastructure, medical system, life support, or other high-impact or time-dependent process.

1.1.2 IT drivers that influence security

IT drivers make up the second group of key security initiatives. These drivers are considered universal. They must be considered in every modern IT solution in a manner commensurate with the risks and consequences of a related failure or incident.

Internal threats and threat agents

Security-related failures and incidents are caused by threats or threat agents in the physical and logical boundaries of the organization or enterprise that operates and controls the IT system. These threats and threat agents might be associated with technology or people.

An example of an internal threat is a poorly designed system that does not have the appropriate controls. An example of an internal threat agent is a person who accesses the IT system or influences the business or management processes to carry out malicious activity.

External threats and threat agents

Security-related failures and incidents are caused by threats or threat agents outside of the physical and logical boundaries of the organization or enterprise that operates and controls the IT system. These threats and threat agents are also associated with technology or people. They seek to penetrate the logical or physical boundary to become internal threats or threat agents or to influence business or management processes from outside the logical or physical boundary.

External threats are single points of failure for one or more business or management processes that are outside the enterprise boundary. Examples include a power system grid or a network connection, or a computer virus or worm that penetrates the physical or logical network boundary. An example of an external threat agent is a hacker or someone who has gained the ability to act as an insider, using personal electronic credentials or identifying information.

IT service management commitments

The IT service management commitments driver identifies the fact that failure to manage the operation of the IT system might result in security exposures to the business. This driver can be divided into two categories, IT service delivery and IT service support:

- Service delivery commitments

  The failure of the IT system to meet its metrics for managing itself can be viewed as a security exposure to both business or management processes.

  An example of security exposure for service delivery is when IT operations processes cannot respond to critical events in a timely manner. Another example is when IT resilience processes cannot recover from a denial-of-service attack (DoS) in a timely manner, resulting in a loss of capacity or response time for business processes.

- Service support commitments

  The failure of the business or IT management system to meet its SLAs can be viewed as a security exposure to business or management processes.

  An example of security exposure for service support is a situation in which the customer relationship processes do not add, modify, or remove users from access control lists in a timely manner.

IT environment complexity

The complexity of the IT environment might contribute to the security or insecurity of the IT system. The IT environment reflects the infrastructure on which the business system will be placed.

For example, any IT environment that is connected to the intranet or extranet is exposed to internal or external threats or threat agents and requires specific security responses. A stand-alone facility for our system represents the lowest complexity. A hosting facility with other systems and other firms represents a more complex environment. An environment with a larger number of systems, varied network access paths, or a complex architecture is a complex IT environment.

Business environment complexity

Because most businesses rely on IT, most business environments are an interconnected set of businesses, each with its own complex IT environment, business processes, and IT management processes. This complexity might contribute to the security or insecurity of the IT system.

Audit and traceability

Audit and traceability identify the need for the IT system to support an audit of information in the system, whether it is associated with management data or business data.

IT configuration vulnerabilities

Configuration vulnerabilities are potentially present in every IT system. They provide an opening to a potential attack based on the system and how it is designed and set up.

IT flaw vulnerabilities

Software flaws potentially exist in every IT system. These flaws represent vulnerabilities that were not detected and are not evident in the design documents. As such, they are an unexpected deviation from what was designed. An example is a defect in an operating system or application that is discovered after implementation.

IT exploit vulnerabilities

The basic design of software in any IT system might be exploited by threats or threat agents as a part of an attack on the IT system, the business, or the management processes. This exploit might include the use of a function within a system in a way to compromise the system or underlying data. Although some people might define an exploit as both the flaw and the method, we treat them separately because an exploit might involve using normal functions as designed in an unusual manner to attack the system. The exploits can also be viewed as the openings or avenues that an attacker can use.

The following section introduces the IBM Security Framework, which can help translate an organization’s requirements into coarse-grained business solutions, not into specific IT components or IT services.

1.2 IBM Security Framework

Business leaders today are expected to manage risk in their areas of responsibility in the same way that CFOs manage risks in their domains. Security risks and the potential impact on IT need to be communicated to executive peers in business terms. Additionally, they need to align IT security controls with their business processes, monitor and quantify IT risk in business terms, and dynamically drive business-level insight at the executive level. Finally, business leaders need to manage risk and orchestrate security operations in a way that enforces compliance and optimizes business results.

As an organization secures its business processes, a business-driven approach needs to become the guiding influence for ensuring that all the security domains work together in a holistic and synergistic manner. They must be in alignment with the overarching business objectives. Otherwise, the risk stance of an organization becomes vulnerable due to misalignment of priorities between IT and the business strategy. Using a standards-based approach to map business drivers to IT security domains is often difficult and is often an afterthought.

IBM created a comprehensive IT security framework (Figure 1-1 on page 11) that can help ensure that every necessary IT security domain is properly addressed when using a holistic approach to business-driven security.

IBM provides the full breadth and depth of solutions and services that can enable organizations to take this business-driven, secure-by-design approach to security in alignment with the IBM Security Framework. Comprehensive professional services, managed services, and hardware and software offerings are available from IBM to support an organization’s efforts in addressing the different security domains covered by the IBM Security Framework.

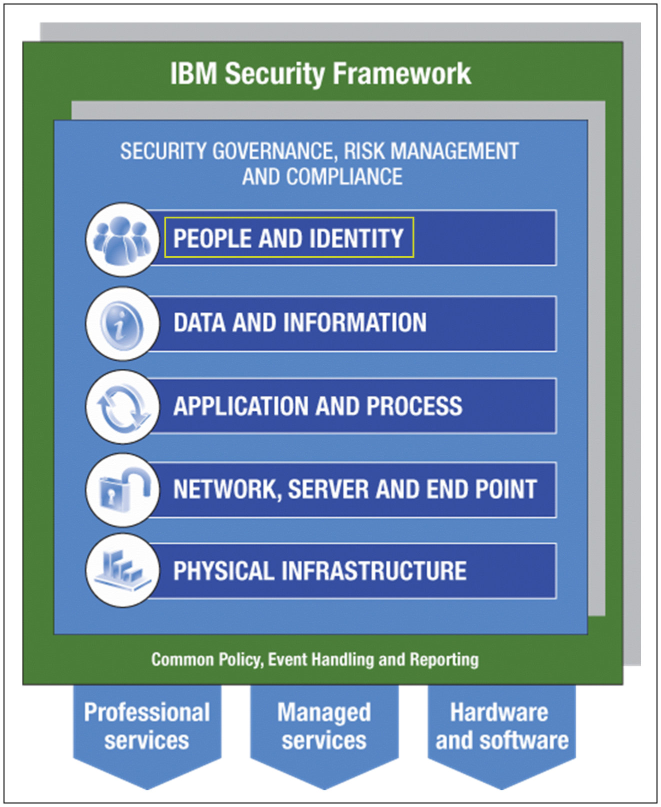


Figure 1-1 The IBM Security Framework

1.2.1 Security Governance, Risk Management, and Compliance model

Every organization needs to define and communicate the principles and policies that guide business strategy and business operation. In addition, every organization must evaluate its business and operational risks. Every organization must also develop an enterprise security plan to serve as a benchmark for the execution and validation of the security management activities that are appropriate for their organization.

These principles and policies, the enterprise security plan, and the surrounding quality improvement process represent the enterprise *Security Governance, Risk Management and Compliance model*. This model includes the following security domains, for which each has their own requirements and compliance criteria:

People and Identity Covers aspects about how to ensure that the correct people have access to the correct assets at the correct time.

Data and Information Covers aspects about how to protect critical data in transit or at rest across the organization.

Application and Process
Covers aspects about how to ensure the security of applications and business services.

Network, Server, and Endpoint (IT infrastructure)
Covers aspects about how to stay ahead of emerging threats across IT system components.

Physical Infrastructure
Covers aspects about how to use the capability for digital controls to secure events (on people or things) in the physical space.

The following section examines the Network, Server, and Endpoint domain. This domain is *the* driving factor for implementing a network intrusion prevention system (IPS) solution. To learn more about the other IBM Security Framework domains, see the IBM Redpaper™ publication *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, REDP-4528.

1.2.2 Network, Server, and Endpoint domain

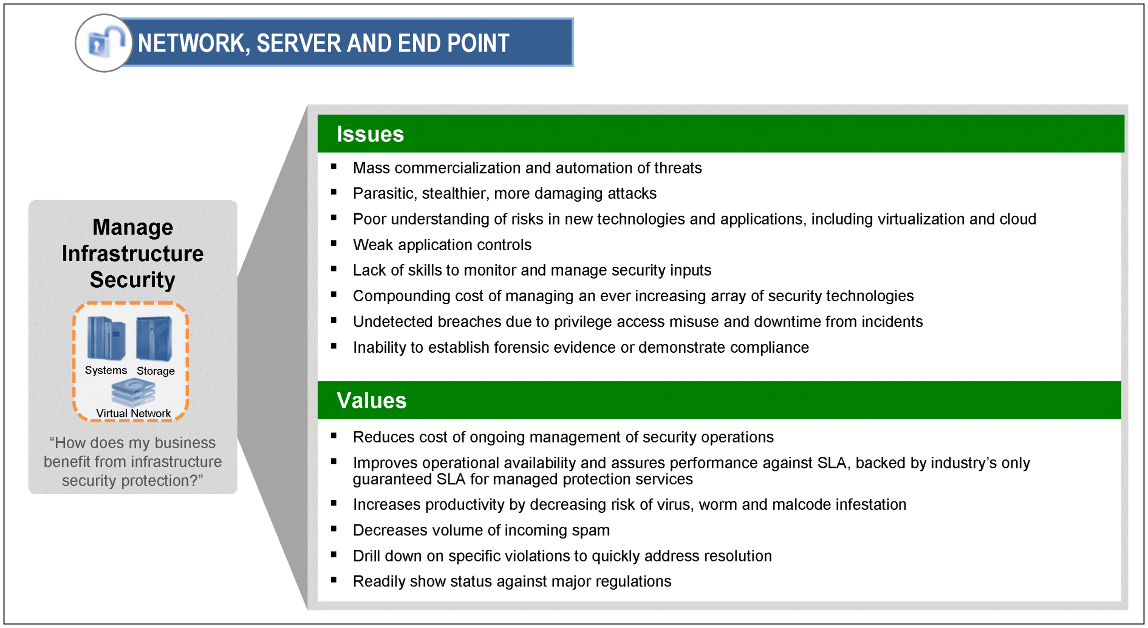
Organizations need to *preemptively* and *proactively monitor* the operation of the business and the IT infrastructure for *threats* and *vulnerabilities* to avoid or reduce breaches.

The Security Governance, Risk Management, and Compliance model can provide guidance on the business implications of technology-based risks. In practice, the definition, deployment, and management of technology-based threats, in addition to the technical aspects of incident response, can be delegated to operational management and staff or outsourced to a service provider.

The security monitoring and management of the Network, Server, and Endpoint domain of an organization is critical to staying ahead of emerging threats that can adversely affect system components and the people and business processes that they support. The need to identify and protect the infrastructure against emerging threats has dramatically increased with the rise in organized and financially motivated network infiltrations. Although no technology is perfect, the focus and intensity of security, monitoring, and management can be affected by the type of network, server, and endpoints deployed in the IT infrastructure. They can also be affected by how those components are built, integrated, tested, and maintained.

Organizations use *virtualization technology* to support their goals of delivering services in less time and with greater agility. By building a structure of security controls within this environment, organizations can reap the goals of virtualization and gain peace of mind that the virtual systems are secured with the same rigor as the physical systems. Examples of the goals of virtualization include improved physical resource utilization, improved hardware efficiency, and reduced power costs.

Figure 1-2 shows a summary and additional aspects to be addressed within the Network, Server, and Endpoint domain.



NETWORK, SERVER AND END POINT

Manage Infrastructure Security

“How does my business benefit from infrastructure security protection?”

Issues

- Mass commercialization and automation of threats
- Parasitic, stealthier, more damaging attacks
- Poor understanding of risks in new technologies and applications, including virtualization and cloud
- Weak application controls
- Lack of skills to monitor and manage security inputs
- Compounding cost of managing an ever increasing array of security technologies
- Undetected breaches due to privilege access misuse and downtime from incidents
- Inability to establish forensic evidence or demonstrate compliance

Values

- Reduces cost of ongoing management of security operations
- Improves operational availability and assures performance against SLA, backed by industry’s only guaranteed SLA for managed protection services
- Increases productivity by decreasing risk of virus, worm and malcode infestation
- Decreases volume of incoming spam
- Drill down on specific violations to quickly address resolution
- Readily show status against major regulations

Figure 1-2 Network, Server, and Endpoint domain

After addressing and mapping the IT security domain, Network, Server, and Endpoint, into business solutions, it is time to look at the component-oriented view of IT security in the IT Security Blueprint.

1.3 IBM Security Blueprint

The IBM Security Framework divides the area of business-oriented IT security into six domains. The next step is to break down these domains into further detail to work toward a common set of core security capabilities needed to help organizations securely achieve their business goals. These core security capabilities are called the *IBM Security Blueprint*.

The IBM Security Blueprint uses a product-agnostic and solution-agnostic approach to categorize and define security capabilities and services that are required to answer the business concerns in the IBM Security Framework. The IBM Security Blueprint was created after researching many customer-related scenarios, focusing on how to build IT solutions. The blueprint supports and assists in designing and deploying security solutions in your organization.

Building a specific solution requires a specific architecture, design, and implementation. The IBM Security Blueprint can help evaluate these areas, but does not replace them. Using the IBM Security Blueprint in this way can provide a solid approach to considering the security capabilities in a particular architecture or solution.

IBM has chosen to use a high-level service-oriented perspective for the blueprint, based on the IBM service-oriented architecture (SOA) approach. Services use and refine other services. For example, policy and access control components affect almost every other infrastructure component. Figure 1-3 helps you to better understand and position the IBM Security Blueprint.

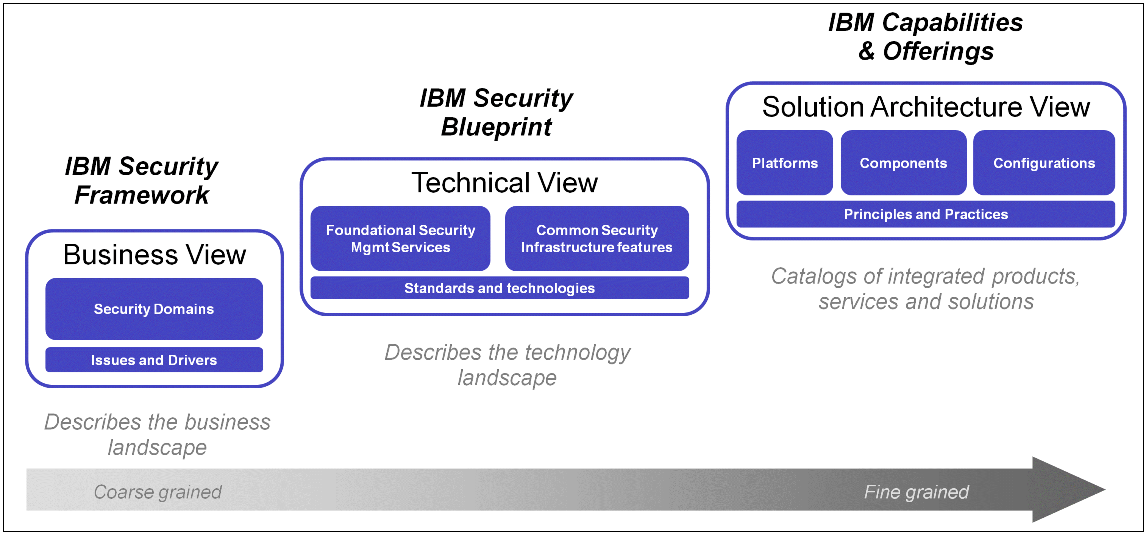

IBM Capabilities & Offerings
IBM Security Blueprint
IBM Security Framework
Business View
Security Domains
Issues and Drivers
Technical View
Foundational Security Mgmt Services
Common Security Infrastructure features
Standards and technologies
Solution Architecture View
Platforms
Components
Configurations
Principles and Practices
Describes the business landscape
Describes the technology landscape
Catalogs of integrated products, services and solutions
Coarse grained
Fine grained

Figure 1-3 IBM Security Blueprint positioning

The left portion of Figure 1-3 on page 14 represents the IBM Security Framework, which describes and defines the security domains from a business perspective.

The middle portion in Figure 1-3 on page 14 represents the IBM Security Blueprint, which describes the IT security management and IT security infrastructure capabilities needed in an organization. As explained earlier, the IBM Security Blueprint describes these capabilities in product and vendor-neutral terms.

The right portion of Figure 1-3 on page 14 represents the solution architecture views, which describe specific deployment guidance particular to a given IT environment. Solution architecture views provide details about specific products, solutions, and their interactions.

Figure 1-4 on page 16 highlights the components and subcomponents of the IBM Security Blueprint that you, as the administrator for your organization, must examine for every solution in the Network, Server, and Endpoint security domain. Besides the Foundational Security Management, with the IBM Security Blueprint, you can determine the Security Services and Infrastructure components by reviewing the component catalogs for these Foundational Security Management services. You can then assess each of these components by determining whether they are required to make a Foundational Security Management service functional. With this approach, the service can address the issues or provide a prospected value associated with the business security domain, which in this case is the Network, Server and Endpoint domain.

Figure 1-4 on page 16 shows that almost all infrastructure components can be required for a Network, Server, and Endpoint security solution apart from the Application Security, Storage Security, and Physical Security components. These components are not included because they are mostly covered by other domains of the IBM Security Framework.

The Application Security component is covered by the Application and Process domain. The Storage Security component is covered by the Data and Information domain. The Physical Security component is covered by the Physical Infrastructure domain.

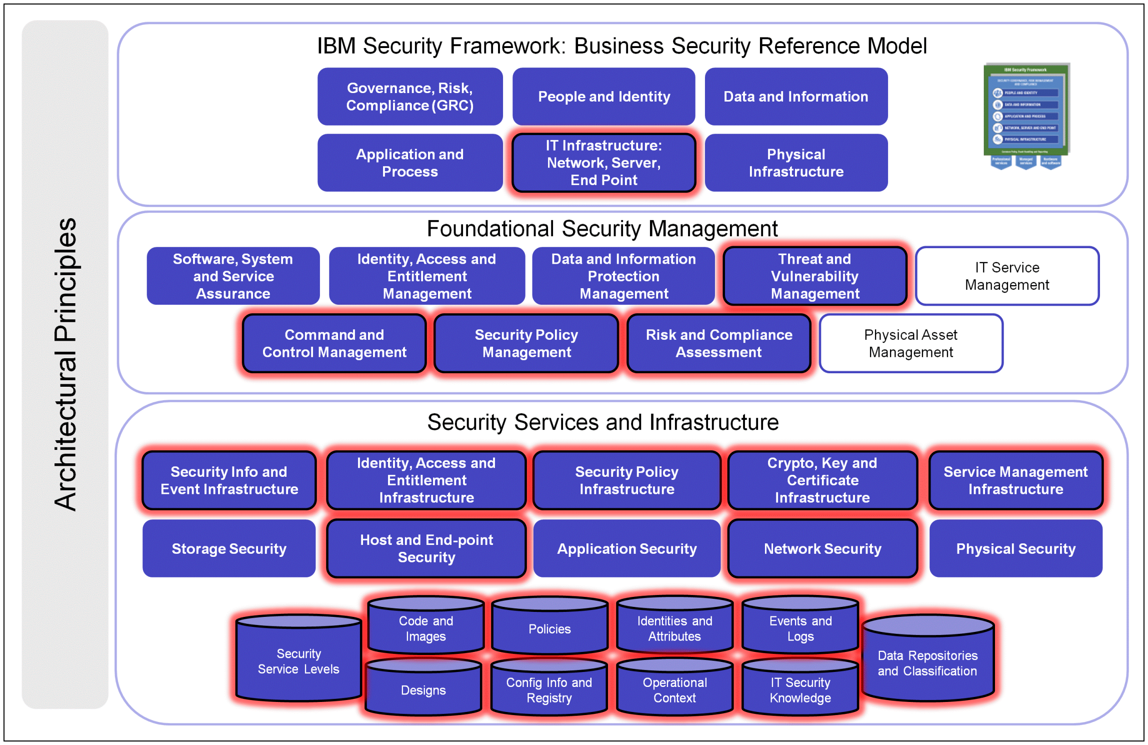

Architectural Principles
IBM Security Framework: Business Security Reference Model
Governance, Risk, Compliance (GRC)
People and Identity
Data and Information
Application and Process
IT Infrastructure: Network, Server, End Point
Physical Infrastructure
Foundational Security Management
Software, System and Service Assurance
Identity, Access and Entitlement Management
Data and Information Protection Management
Threat and Vulnerability Management
IT Service Management
Command and Control Management
Security Policy Management
Risk and Compliance Assessment
Physical Asset Management
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 1-4 IBM Security Blueprint components for the Network, Server, and Endpoint solution pattern

The next section focuses on threat and vulnerability management for networks, servers, and endpoints.

1.4 Threat and vulnerability management

In the world of IT security today, in the Network, Server, and Endpoint domain, organizations are facing the following major challenges among others:

- The number and sophistication of threats are increasing.

  Organizations now face more than just viruses and worms. They must be able to defend against and stay ahead of various threats rather than respond to intrusions.

- IT security resources are stretched thin.

  Today, threats seem to evolve faster than IT budgets and resources can keep up with. Every organization needs an efficient, integrated approach to threat and vulnerability management.

- Intrusions and malicious disruptions affect the bottom line for organizations in both customer confidence and business productivity.

  Security breaches can destroy the brand image of an organization and affect its critical business processes, both of which can cost significant dollars.

At the bottom line, effective threat and vulnerability management processes need to be proactive rather than reactive, preventing problems rather than responding to them. To be efficient and effective, organizations need to address prevention, detection, and compliance in an integrated way.

1.4.1 Security concepts and terminology

The term *security* has many definitions and is used in many situations. This section focuses on defining the major terms that are used throughout this book.

Security represents almost an industry in itself that is focused on the confidentiality, integrity, and availability of information. *Information security* stands for a broader spectrum than pure IT security. It can include aspects that do not have a direct relationship with technology, such as physical security, or the security policies of an organization at the business level.

Information security has to deal with *vulnerabilities* and *exploits* to properly address threats to the organization and its information, assets, and networks.

A *threat* can be defined as events, people, or forces (*threat agents*) that can pose a risk to the assets of an organization by exploiting a vulnerability.

A *vulnerability* represents a weakness in the systems. Vulnerabilities come from deficiencies in legitimate code that is running on internal computer systems or from a system misconfiguration that can lead to an unexpected outcome. For example, SQL injection vulnerabilities are known for being easily exploited to gain knowledge of internal database structure and contents.

Another well-known vulnerability category is a *software bug*, which is a name for an application that malfunctions due to a programming mistake or error. Other common vulnerabilities in relation to applications are the misconfiguration or lack of properly implemented access control.

An *exploit* is the result of a vulnerability. It can be a piece of software or a command that takes advantage of the vulnerability. Based on an exploit, an organization experiences different attacks, such as buffer overflows (BOFs), DoS, and worms. An exploit can be revealed by using a *signature*, and it can be prevented from propagating by blocking. As an administrator, you can also apply a proper software patch at the target system to remediate the vulnerability.

Thus, a *signature* is a piece of information that describes a specific attack pattern. Signatures are used in IT security devices, such as network intrusion prevention or detection systems, to detect and hopefully block an attack.

Exploits that do not yet have defined signatures or cannot be remediated by a software patch are called *zero-day exploits*. They typically attack undisclosed or unknown vulnerabilities.

> **Fast attack patterns:** Most antivirus vendors require a 7 – 30 hour window after revealing an exploit to reverse-engineer it, create a signature to stop the attack, and send out the update to their customers. However, exploits, such as Slammer, are known to propagate worldwide in just 15 minutes. The damage is already done before an antivirus signature can be constructed. This example is typical of a reactive approach to security that does not help with new and undisclosed vulnerabilities and the zero-day effect.
>
> To learn more about the Slammer worm, see “Slammed! An inside view of the worm that crashed the Internet in 15 minutes” from Wired at:
>
> `http://www.wired.com/wired/archive/11.07/slammer.html`

Malware

Many IT-related attacks today are implemented by developing and using malicious software, which is also called *malware*. Malware stems from programs, scripts, or macros that can run on almost any computer and are malicious in nature. This category of threat is often subdivided into viruses, worms, and trojan horses.

A *virus* is code attached to or contained within a legitimate program or document. Self-propagating code is often designated as a *worm*.

Trojan horses (also called *trojans*) are old threats now returning to the forefront of IT. A *trojan* is a piece of code that uses *trickery* to get people to run it for a visibly legitimate purpose. However, in reality, the code hides its intended malicious behavior, which is unknown to the user. A trojan might perform key logging or password stealing activities. Because the motives for hacking have shifted from fame and satisfaction to financial or political profit, trojans are becoming a more significant threat vector. As of 2006, trojans represent the vast majority (75%) of malicious code. Stealthy trojans might not even replicate; they are intended to steal data or gain access to systems for future exploitation. Examples include keyloggers and password stealers that can enable financial profit through inappropriate access to accounts.

Malware can contain many components, and its categorization is subdivided according to the purpose of a component (such as password stealers, keyboard loggers, botnets, and droppers). Various stealth technologies can be deployed to keep malware installed without detection (for example, rootkits). The following examples are some of the common and destructive types of malware:

Designer malware

Designer malware is a piece of malcode written to infect or compromise either one or a few organizations with similar profiles. For example, designer malware can be a trojan horse written specifically for a single bank.

Threats that use designer malware are targeted and specific. Targeted attacks and designer malware take a laser-focused approach on which organization to infect. At the most simplistic level, they might target a single company or user population. In the past, antivirus vendors prioritized threats by the *total number of infected systems*. As a more targeted attack mode, designer malware takes advantage of the old view of risk and stays under the radar of antivirus systems.

It is possible to develop antivirus signatures for designer attacks. However, attackers have come to understand the traditional responses to virus outbreaks and have crafted attacks that carefully avoid the trigger points that start the typical response. When the attack does not propagate beyond a small user community, it greatly decreases its chance of being detected at all.

Although most modern hackers eschew headlines in favor of profits, designer malware is responsible for several notable attacks. For example, in Israel, a trojan horse attack conducted industrial espionage and remained undetected for 18 months. This attack directly mirrors the trend of new attacks to fly under the radar of existing protection and steal data for as long as possible before being found. In the Israeli incident, intellectual property was stolen during 18 months of infection.

Another more recent example is *Stuxnet*, which is a trojan that was discovered in June 2010 by the antivirus company VirusBlokAda. It is one of the most sophisticated malware programs ever written. It targets industrial control systems and can modify code on programmable logic controllers (reprogram PLCs) that drive industrial processes. It is also the first malware that included a PLC rootkit. This example again demonstrates that traditional antivirus software can be ineffective against malware that exploits undisclosed vulnerabilities until a sample is discovered and a signature can be developed and distributed.

With millions of dollars invested in proprietary research, the biotech industry is another target of designer malware. Imagine the value of stealing the recipe for the next wonder drug. Two biotech firms have been infected with designer malware targeted to steal research secrets for new projects. Designer malware has the potential to steal research findings and trade secrets, undetected and in a relatively short period.

Ransomware

Ransomware is malcode that executes on an infiltrated computer system. It packs important files into an encrypted archive and deletes the original files, making access to the source information impossible unless a ransom is paid. More advanced ransomware scenarios now use multiple forms of user manipulation and extortion.

Ransomware is a growing and significant trend dealing with data, file, and user manipulation. With ransomware, attackers encrypt a user's documents and force the user to pay a ransom to regain access to the files. After paying the ransom, the user is given the password to unlock the files. Typically, users pay the ransom by visiting a website devised by the hacker and *purchasing* a high-priced product.

Ransomware attacks also employ fear and embarrassment by telling victims that the ransomware is caused by visiting inappropriate websites or from storing pornography on their computers. Whether these accusations are true or false, such ransomware tactics can prevent users from working with security teams to cure the problem.

New threats like ransomware employ technology and engage the user, which escalates damage beyond traditional Internet worm outbreaks. Certain ransomware uses stealth tactics that can cause code to self destruct after encrypting a user's files. Therefore, unlocking the files becomes even more difficult without dealing with the attacker.

Rootkits

With the ability to make malcode invisible to operating system and antivirus signature scans, rootkits can be combined with multiple types of malicious code to enter enterprise systems undetected and launch multifaceted attacks.

The *rootkit* is one of the most significant threats in practice today due to its stealthy nature and its ability to work with other malware. Rootkits help make malcode invisible to signature antivirus scans. A rootkit is *shielding technology* that can be used by any type of malcode. By insinuating itself into the operating system of the compromised system, it can effectively prevent detection of any elements of the attack it wants to hide. Basic requests, such as asking for a list of all files in a directory, might be unreliable because the rootkit might hide files in the directory.

Dealing with rootkits can be similar to a game of hide-and-seek. If you watch someone hide, you have a much better chance of finding the person. If the person hides and you did not see where, you might never find the person. Using behavior-based protection technology can help to identify rootkits before they can establish themselves. After the rootkit hides, it might be too late, and damage can be irreversible.

Many firms attempt to clean up the rootkit after infection. However, best practices suggest that re-imaging is preferable to restoring the system. Even if the time is taken to restore the system, the real damage to the enterprise is already done. If the rootkit enabled the theft of strategic corporate data or intellectual property, the enterprise cannot retrieve information that becomes public or is revealed to their competition.

Besides malware, computer crime is focused on other types of attacks, such as DoS, social engineering, phishing, and spear phishing. Let us look a bit closer at one of the most prominent of these types of attacks.

Denial-of-service attacks

DoS originates from external users or systems attacking the infrastructure of a system with the general idea to disrupt the operation of the system. Various forms of DoS are possible such as the vulnerability denial of service. Vulnerabilities are possible that might not be able to exploit remote code execution, but that can crash the system. An attacker can crash a computer 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. Domain name servers (DNSs) are 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 DoS seek to exhaust the network capacity by flooding the network with traffic. Often these attacks are mounted from thousands of host computers (distributed denial-of-service), and usually the computers that are attacking are compromised with botnet malcode installed on the machines.

Advanced Persistent Threat

The term *Advanced Persistent Threat* (APT) originated in US Government circles. It refers to groups from various nation states that attack computer networks to steal intelligence information, as opposed to groups with a more direct financial motivation, such as those who target caches of credit card numbers.

The word *advanced* is used because APT groups use exploits for unreported vulnerabilities (zero-day). The tools are advanced, custom malware that is not detected by antivirus products, and they coordinate attacks by using various vectors.

The word *persistent* characterizes the capacity that APT groups have for maintaining access to, and control of, computer networks, even when the network operators are aware of their presence and are taking active steps to combat them. Also, APT groups are patient, as they slowly develop access to the information they want while staying below an activity threshold that might attract attention. Therefore, the attack can potentially last for months or years.

In addition, APT is a *threat*, because APT groups are dedicated to the target. The attacks are not random. These groups are “out to get you”, targeting specific individuals and groups within an organization with an aim at compromising confidential information.

APT has the following concepts:

Reconnaissance Includes identification of a target and method of compromise. APT groups use a lot of investigation and information collection about the target before they execute the attack.

Social engineering Comes in the form of *spear-phishing* (email or instant messaging that appears to come from a known trusted source). The message typically contains a malicious payload or a link to a web page that has malicious code.

Use of zero-day tools Attacks involve exploitation of never-before-seen vulnerabilities discovered by the attackers. Not all malware in APT cases is undetectable, but most malware used during the initial compromise is custom.

Covert The attackers remain patient and attempt to conceal their activity by masquerading as normal users. Attackers attempt to cover their actions by using legitimate accounts and protocols when possible.

Privilege escalation and lateralization
Most often the attackers attempt to use a current account and obtain any information they can with those privileges. Some APT cases have involved the creation of new accounts with administrative privilege.

Adaptive The attackers observe remedial actions and adjust accordingly. They use their least sophisticated attacks first.

Persistence Attackers are patient and watch targets for long periods of time. Attackers install multiple back doors to ensure continued access to the target network.

The level of sophistication of attack techniques seen in APT cases is often directly proportional to the level of sophistication of the capabilities of the people defending a particular network. What all sophisticated, targeted attacks have in common is that the first step for the attackers is *reconnaissance*. Often, an initial target is not always the true target. Although this target might include the traditional network probing and scanning activities that we associate with computer intrusions, sophisticated attackers think outside of that box.

A wealth of information is available on the Internet regarding many people working in the business world. For example, we publish profiles on personal and professional social networking sites, we send out status updates that indicate where we are traveling, and we engage in online forums relevant to our jobs. We also speak at public conferences, write articles and papers, and take news media interviews. In doing these activities, we leave many bread crumbs that malicious persons can use to reconstruct a picture of our personal lives and the organizations that we work for and how we fit into them.

Sophisticated attackers use this public information to develop a complete picture of a targeted organization, including who works there, what they do, and who they report to within the organization. With this picture, they can identify the particular individuals who might have access to the information that they seek. Those individuals are targeted with various kinds of *social engineering attacks* that are intended to trick them into running a malicious exploit.

We can say that social engineering exploits the “bugs” in the human brain and behavior that will help the attacker gain control of the victim’s workstation. From that point, all of the victim’s work and communications become an open book. These attacks often involve malformed documents or web pages that target zero-day vulnerabilities with obfuscated exploits.

Spear phishing is a combination of phishing and social engineering that targets a single person or a single group of people. Spear phishing is hyper-focused to lend added credibility to the attack. Spear phishing combines the standard phishing attack with additional social engineering techniques to build super targeted attacks. Spear phishing is used heavily in state sponsored attacks and attacks against financial institutions. The attacker takes advantage of personal or public information about individuals to customize an email message that appears to come from a legitimate source. This message tricks people into responding with personal information such as user names and passwords.

For example, John Smith’s name and professional contact information are published in an industry magazine based on his recent promotion. A spear phishing attacker uses John’s information to send a spoofed, but official looking, email message to John. The attacker poses as a professional service and requests that he activate his new complimentary account. In responding, John inadvertently allows the attacker to install a trojan horse or back door on his computer.

This example illustrates one of the reasons why Adobe PDF and Microsoft office product exploits and attacks are rising. The focus is always on the weakest link in the security chain, which is the users. By exploiting the vulnerabilities of those vastly used tools in combination with phishing, the attackers can insert different malware on the employee's workstations and use them for further attacks.

The attack might come as an email message, addressed from a business partner or colleague, with a malicious attachment that sounds directly relevant to the victim's job function. For example, it might be a link to an interesting document that is hosted on a competitor's website or a USB token given to the victim at a trade show with an interesting presentation.

The custom malware that is installed by the exploit uses covert channels to communicate over the network without being noticed. After the attackers have their malware running on one victim's machine, they often try to spread their control to other systems in the targeted network. They also try to exploit business relationships to use their control over one company's network to break into others. For network security professionals in the private sector, the line between intelligence-related APT activity and financially motivated attacks is blurry at best.

Power plants have been attacked by state-sponsored cyber warriors and criminal groups who are simply interested in blackmail. The same sophisticated spear phishing attacks that have been used to target government strategists have also been directed at executives in financial institutions who have access to funds transfer systems.

Preventing Advanced Persistent Threat attacks

Deploying proper sophisticated security protection mechanisms (such as state-of-the-art identity and access management (IAM) systems, email antispam filters, or the latest IPS) is just half of the story. Education of employees is the other important factor.

One of the most effective countermeasures that you, as the administrator for your organization can employ to combat these threats is to enlist your people. If you can identify the people who are most at risk for this type or attack in your organization, you can explain to them the nature of the threat and how it works. Then, they can become your first line of defense. They can report suspicious email messages to you. After you receive a sample of an exploit being used by these attackers, you have a foothold on the problem. You might be able to identify other targeted victims, identify malware command and control patterns, and begin to unravel the infestation.

1.4.2 Threat management

Threat management is the process of identifying, understanding, and fighting threats to network infrastructure (including wireless networks), hosts, and end points. With increased market focus on cloud computing and virtualization, those security issues are also prevalent in virtual environments.

The threat management discipline consists of the following categories:

- Threat identification
- Threat analysis
- Threat mitigation

Threat identification embraces activities that help to discover actors and actions in the IT environment that might have a harmful effect on IT assets and the information stored and processed on them. Threat identification can be performed manually. However, today it can usually be based on the automated recognition of deviations from the usual operations in an IT environment. Any discovered anomalies can then be examined for their threat potential.

Threat analysis is the continuous examination of available information related to threat agents, often called *attackers*, and their possible threat actions, that is the actual attack, to evaluate the severity of an identified threat. For example, the severity might be based on the potential occurrence of an attack due to the general awareness of the attack vector. It might also be based on the presumed attractiveness of an organization as an attack target in the view of an attacker.

Threat mitigation describes the ability to reduce risk by identifying and preventing malicious attacks from being successful in the network of an organization, on its hosts, and compromising the entire IT environment. In many cases, threat mitigation is often overlooked as part of the necessary security infrastructure. One reason it is overlooked is because many people assume that the security, which is included in applications, operating systems, and traditional network infrastructure (such as firewalls) includes the ability to mitigate complex threats. Attacks are created by *technical adversaries* to take advantage of these assumptions, which is why so many attacks go unnoticed.

It is not that traditional protection techniques are not good. Rather, they simply cannot cover the complete spectrum of the threat mitigation problem space. Threats can come from insiders, outsiders, and now a new source, what we call an *accidental insider*. A technical adversary can trick an employee into doing something that can open a pathway into the network. These techniques can allow an outsider access from the inside.

The threat landscape has been evolving quickly over the past few years. A hacker's motivation for launching attacks has changed, causing the current threat evolution. Today, attacks are profit or politically driven; a real hacker is no longer after glory and fame.

The IBM Security X-Force Research and Development Organization (X-Force) studies and monitors the latest threat trends (including vulnerabilities, exploits, and active attacks), viruses, and other malware (such as spam, phishing, and malicious web content). The results from the X-Force analysis efforts are posted on the X-Force website.

The *IBM X-Force Trend and Risk Report* is produced twice each year (once at mid-year and once at year end). This report provides statistical information about all aspects of threats that affect Internet security. It includes software vulnerabilities, public exploitation, malware, spam, phishing, web-based threats, and general cyber criminal activity. These reports are intended to help any organization, fellow researchers, and the public at large to better understand the changing nature of the threat landscape and what can be done to mitigate it.

For more information about The IBM X-Force Trend and Risk Report, see the IBM X-Force Threat Reports website at:

http://www.ibm.com/services/us/iss/xforce/trendreports

The *IBM X-Force Threat Insight Report* is another publication from IBM that highlights some of the most significant threats and challenges that security professionals are facing today. This report is produced by the IBM Managed Security Services (MSS) team and is compiled by the X-Force. Each issue focuses on a specific challenge and provides a recap of the most significant recent online threats. In addition to advising organizations and the general public on how to respond to emerging and critical threats, the X-Force delivers security content to protect IBM customers from these threats.

For more information about the X-Force, see Chapter 6, “Security intelligence, research, and technology” of the IBM Redbooks publication *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581.

Threat mitigation architecture

The constant, new, and improved attacks and motivations drive the need for an overall threat mitigation architecture.

With the growing number of techniques required to gain access to systems and networks, many security researchers attempt to classify threats. Unfortunately, the public and many sources, including the media, tend to call anything malicious a computer a *virus*. As a result, a false sense of security is generated. In many cases, administrators *feel* 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 the threat that has already 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? What if you are the first target (zero-day attack)? 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 reduce the threat surface area by limiting exposure. Unfortunately, the technical adversaries have designed techniques to bypass the policies that are required so that networks are useful to legitimate users. Allowing a user to view a web page can lead to an internal breach. Most firewalls are unable to identify these types of threats, and according to the latest X-Force reports, over 50% of the current attacks are web-based, and the number is rising.

Another significant problem is that many threats do not use malicious techniques to get into systems and networks. They infect computers through social engineering and deceptive software techniques. Traditional security solutions, such as antivirus solutions, do not address these types of techniques, and a different approach is required. No “one fits all” solution can ensure that you have the right protection to cover these new types of sophisticated and complex threats. IBM Security Systems provide a holistic approach to address end-to-end security across a whole organization. Standard security tools, such as firewalls and antivirus software, must still be in the place and used.

IBM is constantly attempting to look one step ahead and blend research experience with leading-edge technology and services with developed intelligence. Figure 1-5 illustrates this blended attempt.

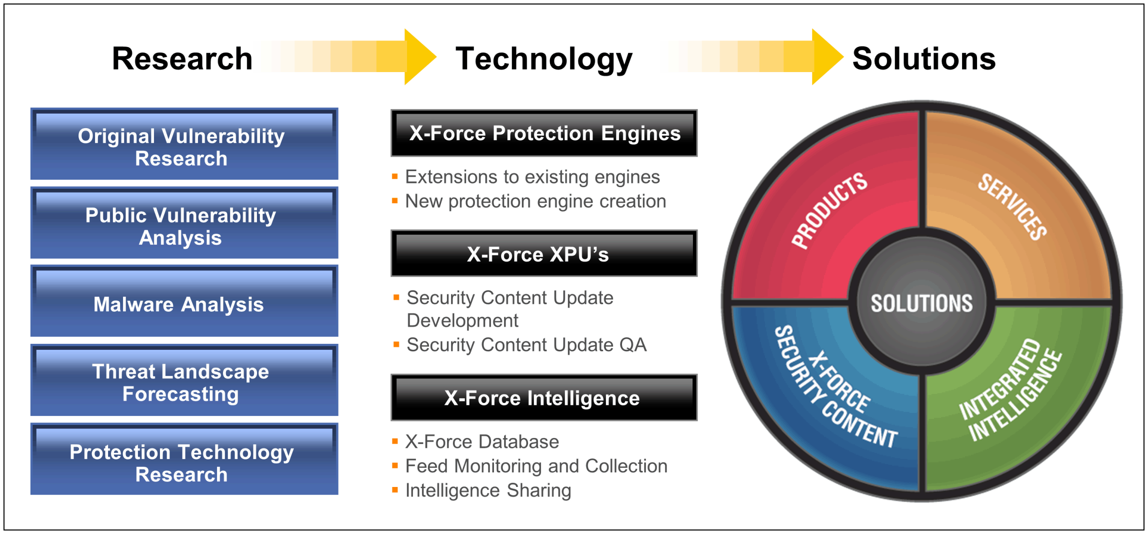

Research
Technology
Solutions
Original Vulnerability Research
Public Vulnerability Analysis
Malware Analysis
Threat Landscape Forecasting
Protection Technology Research
X-Force Protection Engines
Extensions to existing engines
New protection engine creation
X-Force XPU's
Security Content Update Development
Security Content Update QA
X-Force Intelligence
X-Force Database
Feed Monitoring and Collection
Intelligence Sharing
PRODUCTS
SERVICES
SOLUTIONS
X-FORCE SECURITY CONTENT
INTEGRATED INTELLIGENCE

Figure 1-5 IBM Security Systems: Blended approach of research, technology, solutions, and services

IBM provides a powerful portfolio of products and services focused on threat mitigation in the network, on the host, and at endpoint levels.

1.4.3 Vulnerability management

Besides threat management, vulnerability management is another vital component in the security operations portfolio of an organization. Vulnerability management consists of the following major functional areas:

- Vulnerability discovery
- Vulnerability analysis
- Vulnerability remediation

Vulnerabilities in a system can be the results of an array of reasons. Computer users might use weak passwords that can be discovered by *brute force* guessing. Alternatively, they might use the same password in many applications where the exposure of one of these applications can lead to a potential compromise of many systems.

Vulnerabilities can also be caused by fundamental operating system design flaws where designers choose to enforce suboptimal policies on user or application management. For example, operating systems with a *default permit* policy grant every program and every user full access to the entire computer. Such an operating system flaw can allow malware to run commands at an administrator level.

When talking about vulnerabilities, most people immediately think about a *programming bug* that might get used. The software bug might allow an attacker to misuse an application by bypassing access control checks or running privileged commands on the system that is hosting the application. Another common programming error is the failure to check the size of data buffers. This error can lead to a buffer overflow, causing corruption of the stack, or heap areas of memory. In turn, they can cause the computer to run malicious code injected by the attacker.

One more type of vulnerability exists when an application falsely assumes that all user input is safe and fails to perform adequate *input validation*. Programs that do not check user input can allow unintended direct execution of injected malicious code. A few of the most well-known forms of injecting malicious statements are *SQL injection* targeting databases and *cross-site scripting*, where a malicious client-side script gets inserted in the code of a trusted web application.

These vulnerabilities have in common that they can pose a risk to the organization. As the administrator for your organization, you want to reduce this risk by mitigating the threat they pose.

A need for vulnerability management

New vulnerabilities are discovered every day in all sorts of operating systems, software, and web applications. Databases can be compromised, networking devices can be attacked, and web applications can have vulnerabilities coded in them. In a world where exploit code for the latest vulnerabilities is sold on the black market and conveniently packaged in malware toolkits, the amount of threats continues to increase.

You can significantly reduce the number of vulnerabilities that can creep into applications that you create yourself. For example, you can use source code checking tools, such as IBM Rational® AppScan® Source Edition, and use IBM experts to analyze your preproduction web applications with Rational AppScan OnDemand.

Reference information: For more information about the Rational AppScan family of products, see the IBM Redguide™ publication *Improving Your Web Application Software Development Life Cycle's Security Posture with IBM Rational AppScan*, REDP-4530. See also the Rational AppScan Product line page at:

http://www.ibm.com/software/awdtools/appscan/

Additionally, IBM Security Services can provide consulting services for more in-depth Application Security Assessments, which offers assistance in evaluating the security of applications used in an organization. IBM Security Services can conduct application assessments on applications that were developed in-house or by a third party, including commercial applications.

However, the threat landscape is continually evolving, and many or most applications contain unintended vulnerabilities that can be successfully exploited. For these reasons, all organizations must have a process in place that allows them to manage these vulnerabilities.

When talking about vulnerability management, focus efforts on the following items:

- Make sure you can continuously *identify* the vulnerabilities that exist in your organization.
- *Prioritize* the vulnerabilities according to the threat that they pose.
- Start to *remediate* vulnerabilities to reduce the risk exposure of the organization and remain compliant with governing regulations.

Comparing vulnerability assessment methods

Many scanning tools exist that can aid in the discovery, prioritization, and remediation of vulnerabilities in IT systems. Although these tools can provide an auditor with a good overview of possible vulnerabilities present, they cannot replace human judgment. Relying solely on scanners can yield false positives and a limited-scope view of the problems present in the system. A high level of expertise is required to interpret the raw data that scanners provide.

Additionally, it is important to highlight the vital significance of keeping your vulnerability infrastructure current. Maintaining an acceptable risk level starts with determining what you are protecting and what threats your assets are facing. Based on this information, you put in place or modify additional security controls, such as firewalls or IPSs. Not all organizations have the resources available to provide this level of expertise and maintenance themselves. They might much rather focus on their core business and call on external experts to provide these critical tasks of keeping everything current for them.

When comparing scanning tools, take into account the following factors:

- Accuracy of the vulnerability scanning results
- Speed and flexibility of the scanning process
- Cost and scalability of the scanning solution
- Vulnerability tracking and reporting options
- Vulnerability descriptions and remediation information

Accuracy of the vulnerability scanning results

The first step in vulnerability scanning is to create an accurate list of the vulnerabilities that currently exist throughout your organization. These vulnerabilities are mapped to your assets and applications. One principle way to differentiate between several scanning tools or services is the completeness of the discovered vulnerabilities and the number of false positives they generate.

> **False positive:** A *false positive* in this context occurs when a scanning tool indicates that an asset has a vulnerability, although in reality, this vulnerability is not present.

The number of false positives can affect your organization negatively for two reasons. False positives can distort your view of the most critical vulnerabilities that need to be addressed. You can waste time investigating non-existing flaws when other more critical weaknesses remain present and exploitable.

Additionally it is self evident that the remediation process is resource-consuming. A system needs to be checked, a change request needs to be created, a patch might need installing, or another preventive or detective control might have to be put in place. You clearly want to minimize resource spending on checking false positive vulnerability alerts.

When talking about the completeness of scanning results, we primarily refer to the breadth and depth of the scanning process. Some tools focus on network devices and servers. Others add authenticated scanning where the scanner logs in to assets (using securely provided credentials) for a more accurate view of the services running or to accurately check the patch levels of the system. The latest generation of scanning tools and services also increasingly uses the capability to scan your *databases* and *web applications*. A clear need exists for this capability, because we see an increase in the number of vulnerabilities and compromising exploits at the application level.

Speed and flexibility of the scanning process

An organization can ask several questions about itself when selecting a scanning solution. Some of them are related to performance, the ease of deployment, and the ease of use.

Most organizations will put forward quantifiable requirements for their scanning solution. They want to ensure that the solution they select can, for example, guarantee that their entire network and all the assets on it can be scanned within a predefined time frame.

Additionally, most organizations will insist on a certain degree of flexibility. A common type of functionality request is to have the option to mix scheduled and *ad hoc* scanning. If a need exists to assess whether a critical, newly disclosed vulnerability is present within the organization, it must be possible to run a scan immediately that checks all assets for that one type of vulnerability. Such a process must not require any change to the regular scheduled scans.

Cost and scalability of the scanning solution

When putting several scanning solutions side-by-side, cost is a key factor. Capital expenditure might be required when you need to purchase scanning equipment, or you can choose to rely on a vendor's scanning infrastructure. In that case, you pay them a fee for the usage of their infrastructure so that you are not bothered by doing maintenance yourself.

Additionally, it is worth considering the effort it takes to deploy additional scanners as the network expands. Not all scanning options require the same steps and levels of complexity to roll out.

Vulnerability tracking and reporting options

One of the key drivers for implementing a vulnerability assessment solution is the need to demonstrate compliance with one or several standards and regulations. It is obvious that the tracking and reporting options that the tool or service offers are important selection criteria.

When comparing vulnerability management solutions, see how the solution offers a comprehensive view of the vulnerability status of your organization. Most organizations require the option to provide trending reports that enable them to show value. A vulnerability management solution must include ways to keep track of the efficiency of the remediation process.

Additionally, a key differentiating element between several vulnerability management solutions is their predefined scanning scenarios or templates. It can be useful to have predefined scanning templates for checking database and web servers, for example. It is also just as important to be able to run compliancy-standard specific scans.

Vulnerability descriptions and remediation information

Rather than getting a list of vulnerabilities from your vulnerability assessment service or tool, you need sufficiently detailed information readily bundled with it. This type of information can help you tweak the prioritization of your list of vulnerabilities. With it, you can correctly assess your risk exposure by determining the real threats you are facing. In addition to concise and accurate descriptions of the vulnerability, you must check whether the solution offers remediation steps detailing the actions to take to mitigate the threat. You must also check whether it provides an estimate about how long it takes on average to implement these changes.

1.5 Conclusion

This chapter highlighted the business context for threat and vulnerability management. After a short description of different factors that influence security, this chapter introduced the concepts of the IBM Security Framework and the IBM Blueprint. Finally, after definition of the necessary terms, this chapter described the threat and vulnerability management disciplines for the Network, Server, and Endpoint domain.

See Chapter 2, “Introducing the IBM Security Network IPS solution” on page 35, which introduces the IBM Security Network IPS solution.

2

Introducing the IBM Security Network IPS solution

This chapter provides an overview of the key tasks that IBM Security Network IPS appliances can perform in an organized approach to threat and vulnerability management. These tasks include the accurate detection of protocols, the identification and blocking of attacks, and the collection of security event data.

This chapter lists some characteristics of the available physical and virtual appliances including the IBM solution for securing 10 GbE core networks. It describes how IBM Security Network IPS can deliver zero-day threat protection with Data Loss Prevention (DLP) and Web Application Protection (WAP) services.

In addition, this chapter explains how IBM Security Network IPS appliances can be centrally managed and monitored using IBM Security SiteProtector. It also explains how further integration with IBM Rational AppScan can enable enhanced security event analysis.

This chapter includes the following sections:

- Intrusion prevention
- Physical and virtual appliances
- IBM Security Network IPS functionality
- Enforcing intrusion prevention policies
- Centralized management in IBM Security SiteProtector
- Conclusion

2.1 Intrusion prevention

To threat and vulnerability management, a proactive approach is needed as explained in 1.4, “Threat and vulnerability management” on page 16. One of the key aspects of this process is preventing intrusions from occurring in the first place.

An intrusion is defined by any or all of the following definitions:

- An unauthorized act of bypassing the security mechanisms of a computer system to gain access to it or to cause a denial-of-service condition
- Attacks that are attempted from outside the network security perimeter in attempts to access a secured computer system
- An uninvited and unwelcome entry into a computer system by an unauthorized source
- An entrance by force or without permission
- An attempt to compromise the integrity, confidentiality, or availability of a system

Intrusion prevention implies the ability to prevent or deny an attempt to access an unauthorized portion of data, computer system, or network service. The goal is to prevent the alleged intrusion or to at least report on it.

Another way to think about intrusion prevention is that it is a preemptive approach to network security that is used to identify potential threats and respond to them swiftly.

An exploit might be carried out quickly after the attacker gains the knowledge or ability to bypass traditional security precautions. Therefore, intrusion prevention systems (IPSs) can also take immediate action, based on a set of rules established by the administrator of the IPS. For example, an IPS might drop a packet that it determines to be malicious and then block all further traffic from that IP address or port. Legitimate traffic is forwarded to the recipient with no apparent disruption or delay of service.

An effective IPS must be able to perform more complex monitoring and analysis. For example, it might be able to track and identify protocols based on content and behavior (instead of port numbers) and to watch and respond to traffic patterns and individual packets.

Network-based IPSs are critical components when deploying network segments. Most firewalls do not have a sophisticated ability to identify the threats in the data portion of the packet stream.

As shown in Figure 2-1, a firewall typically only inspects the header of the packet and compares the information in a firewall policy to determine if the packet is allowed to pass through the firewall.

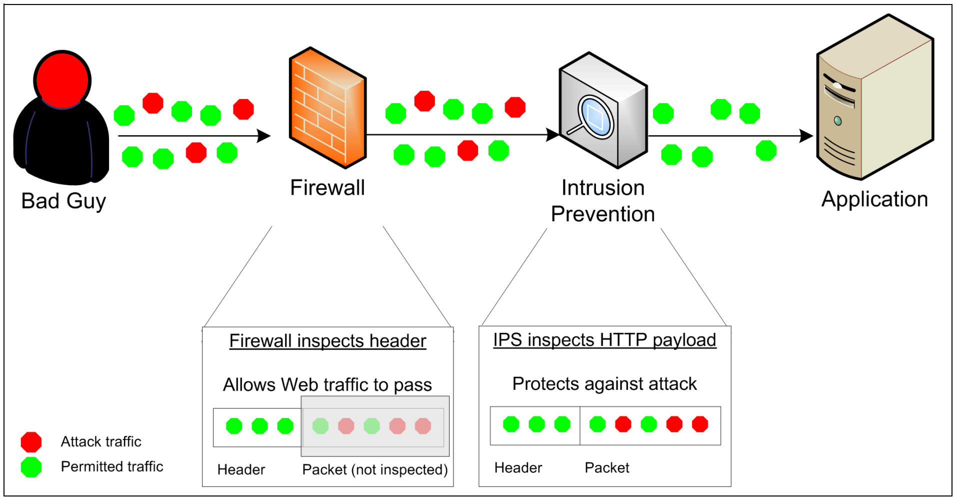


Figure 2-1 Firewalls inspecting the header and an IPS inspecting the entire stream

The Network IPS examines the complete stream, analyzing the data that is destined for the application host. Today, most threats are being transported in the actual data-portion of the traffic, which is difficult for a firewall to inspect. For this reason, a network IPS is crucial to prevent a threat from penetrating your networks.

This IBM Redbooks publication only focuses on Network IPS solutions. For more information about other IPSs, such as host-based IPS solutions, see the Redbooks publication *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581.

2.2 Physical and virtual appliances

The latest generation of IBM Security Network IPS hardware delivers a significant gain in performance compared to previous hardware models.

Performance was optimized by deploying the following items:

- Upgrading x86 technology to support multicore processors
- Increasing memory bandwidth and faster bus speeds
- Providing native 10 GbE connectivity

Architectural design: For information about the architectural design and components of the IBM Security Network IPS, see Chapter 3, “IBM Security Network IPS architecture” on page 73.

The IBM Security Network IPS has the following major hardware and software component releases:

- GX appliance first released in 2006.
- GX V2 appliances released in first quarter of 2010 for all GX4000 and GX5000 models. The hardware refresh across all models led to an increase of 2 – 4 times in performance.
- GX 7000 series appliances released in March 2011. The GX7800 model offers inspected throughput of up to 23 Gbps and supports eight 10 GbE interfaces. GX7412 models are available to cover inspected throughput rates of 5 Gbps, 10 Gbps, and 15 Gbps for each model and support 10 GbE and 1 GbE interfaces.

Table 2-1 shows the 2011 IBM Security Network IPS product range and some associated performance figures.

Table 2-1 IBM Security Network IPS throughput metrics

	Remote	**Perimeter**			**Core**				
Model	GX4004 -200	GX4004	GX5008	GX5108	GX5208	GX7412 -5	GX7412 -10	GX7412 -15	GX7800
Inspected throughput	200 Mbps	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps+
Inspection interfaces	4x1 Gbe	4x1 Gbe	8x1 Gbe	8x1 Gbe	8x1 Gbe	4x10 GbE 12x1 GbE	4x10 GbE 12x1 GbE	4x10 GbE 12x1 GbE	8x10 GbE
Form factor	1U	1U	2U	2U	2U	3U	3U	3U	3U

Figure 2-2 shows the front of a GX7800 appliance. Starting in the lower left corner, you can see the two management interfaces, a console port to the right of them, then a couple of USB ports, and finally the eight inspection interfaces.

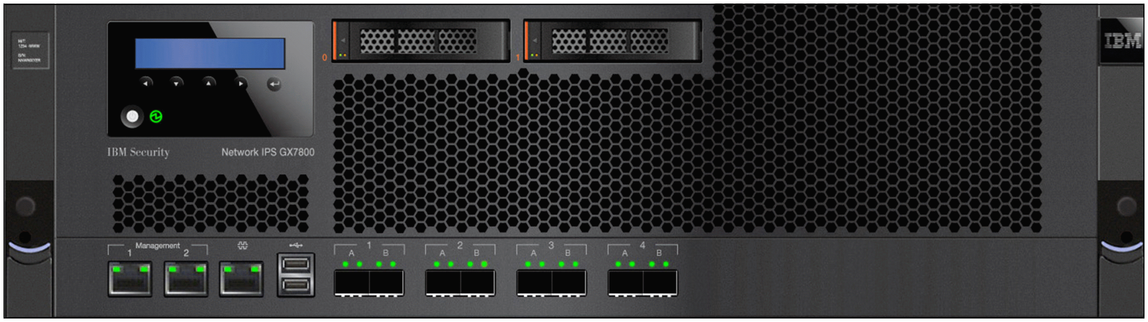


Figure 2-2 IBM Security Network IPS GX7800 model

The number on the inspection or monitoring interfaces corresponds to the *network segment* that is being protected. The letter corresponds to the physical interface.

Current generation Network IPS appliances can be upgraded by using a USB flash drive. For information about the procedure to do this upgrade, see the *IBM Network Security Network Intrusion Prevention System Installation Guide* at:

http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.ips.doc/pdfs/ProventiaIPS_InstallGuide.pdf

IBM Security Network IPS for 10 GbE core networks

The GX7800 is the IBM flagship intrusion prevention appliance. It can handle more than 23 Gbps of security inspection throughput. It includes 10 GbE network interfaces for the high-speed core networks available today. It consists of a newly redesigned hardware platform and is the first IBM Security Network IPS appliance to feature PAM 2.0. PAM 2.0 is the next generation of the Protocol Analysis Module (PAM) that can run in multiple instances on a single appliance, amounting to dramatic improvements in overall throughput and performance. For a more detailed explanation of PAM, see 3.3, “Protocol Analysis Module” on page 82.

Similar to the GX7800, the GX7412 supports 10 GbE network interfaces. It uses the same hardware architecture as the GX7800. However, it is available in three models that support up to 5 bps, 10 Gbps, or 15 Gbps of security inspection throughput. In addition to the 10 GbE, it supports several 1 GbE interfaces.

Remote segment Network IPS

With the GX4004C-200, IBM can serve the low-end IPS market at a competitive price. The GX4004C-200 is a 4-port appliance that can protect two network segments. It is licensed for up to 200 Mbps.

The GX4004C-200 uses the same hardware as the GX4004C. However, the client is limited by the license agreement to deploy this product only on networks with a maximum of 200 Mbps of traffic.

2.2.1 Version 4.x generation firmware

The Version 4.x firmware releases provide the following functions and benefits among others:

- Improved, faster, and easier to use navigation in the dashboard (see 2.2.2, “Local management interface” on page 40)
- IPv6 support
- Simple Network Management Protocol (SNMP) version 3 support
- Support for a Radius authentication server
- Support for geographic high availability (HA; see 3.4, “High availability” on page 97)
- Simplified and more intuitive editors for Data Loss Prevention and Web Application Protection policies

2.2.2 Local management interface

In firmware release 4.1, a major redesign of the local management interface (LMI) was made. This new release provides an improved user experience when managing individual IBM Security Network IPS appliances from a secure web browser session. The interface is organized in two main sections:

- Drop-down menus for navigation at the top of the page
- The page itself, where the content of menu selections is shown

The menu items shown in Figure 2-3 divide the appliance management into five areas with corresponding subtasks:

- Home: Appliance Dashboard
- Monitor: Health and Statistics
- Secure: Protection Settings
- Manage: System Settings
- Review: Analysis and Diagnostics

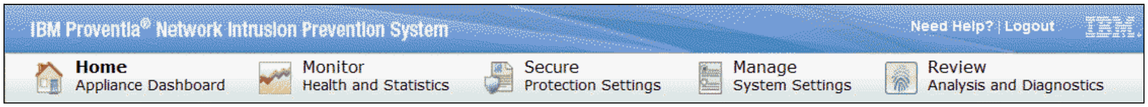
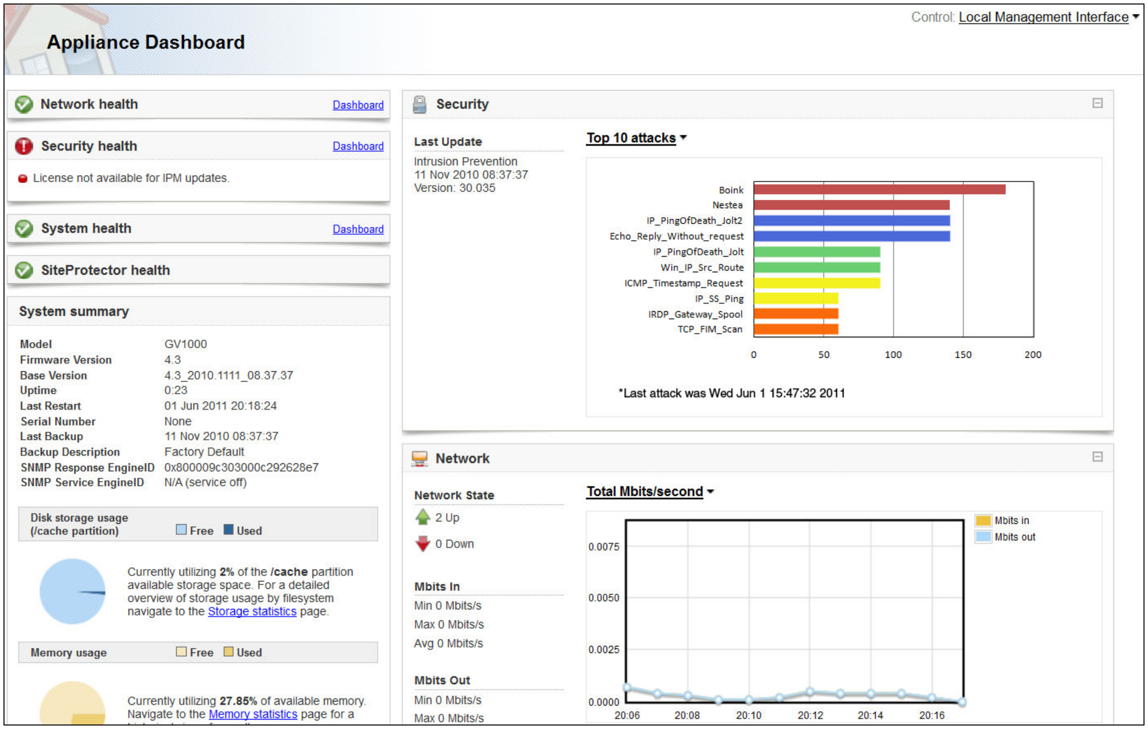


Figure 2-3 Menu options on the LMI

Home (first menu option)

The Home page is the first menu option on the left in the dashboard. It provides a single action selection called the *Appliance Dashboard* (Figure 2-4).



License not available for IPM updates.

System summary

Model	GV1000
Firmware Version	4.3
Base Version	4.3_2010.1111_08.37.37
Uptime	0:23
Last Restart	01 Jun 2011 20:18:24
Serial Number	None
Last Backup	11 Nov 2010 08:37:37
Backup Description	Factory Default
SNMP Response EngineID	0x800009c303000c292628e7
SNMP Service EngineID	N/A (service off)

Disk storage usage (/cache partition) □ Free ■ Used

Currently utilizing **2%** of the **/cache** partition available storage space. For a detailed overview of storage usage by filesystem navigate to the Storage statistics page.

Memory usage □ Free ■ Used

Currently utilizing **27.85%** of available memory. Navigate to the Memory statistics page for a

Last Update
Intrusion Prevention
11 Nov 2010 08:37:37
Version: 30.035

*Last attack was Wed Jun 1 15:47:32 2011

Network State
2 Up
0 Down

Mbits In
Min 0 Mbits/s
Max 0 Mbits/s
Avg 0 Mbits/s

Mbits Out
Min 0 Mbits/s
Max 0 Mbits/s

Figure 2-4 Home page (Appliance Dashboard) of the LMI

The dashboard provides an at-a-glance view of the health status of the key components of the solution:

- The upper left section provides an overall picture of the current posture of the system.
- The Network section shows the network health status for each segment and throughput charts.
- The Security section shows health notifications and graphs of the last 10 IPS events, top 10 intruders, top 10 victims, blocked attacks, and blocked packets.
- The System summary section provides an overview of memory and hard disk storage utilization graphs and a table of significant events.

Users can navigate to explore more detailed data by clicking through the dashboard summary information.

Monitor (second menu option)

The Monitor page (Figure 2-5) is the second menu option from the left in the dashboard. It contains a convenient set of tools for viewing the health, status, and performance of your appliance in one place. You use this page to analyze trends in your security network or to navigate to specific pages to troubleshoot and research security events. You can also use this page to view general information, such as the model, firmware version, available memory, uptime, or the current backup version.

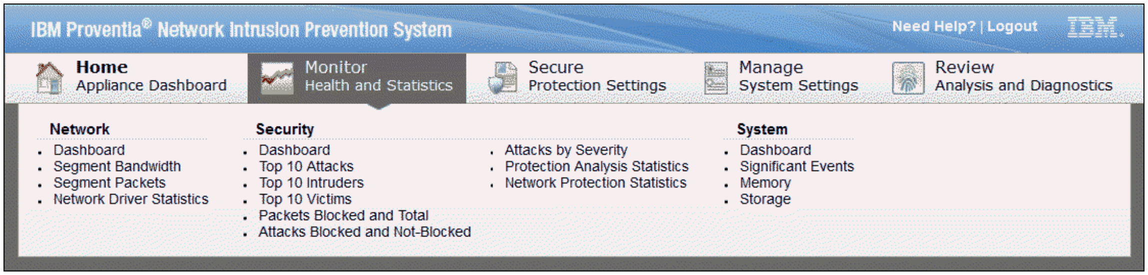


Figure 2-5 Monitor page (Health and Statistics) of the LMI

The Monitor page provides multiple actions that are divided in three major areas:

- Network
- Security
- System

Network

The tools under the Network section provide a pictorial view of the health of your network. The Network section delivers the following views:

- Network Dashboard

  You use the Network Dashboard for general health information concerning interfaces and the speed and time at which network packets are entering and exiting the network.

- Segment Bandwidth

  You use the Segment Bandwidth page for detailed information about network segment traffic over time. You can also view summaries of specific segments and check interface settings.

- Segment Packets

  You use the Segment Packets page to view detailed information about blocked, forwarded, injected, and unanalyzed packets over time. You can also view summaries of specific segments and check interface settings.

- Network Driver Statistics

  You use the Network Driver Statistics page to view network activity on each adapter used on the appliance. You can also view information about packet counts (such as packets injected, forwarded, or dropped) or any unanalyzed packets that have passed through the network.

Security

With the tools in the Security section, you can view the health of your security settings. You can also find information about attackers, intruders, and victims, and view which attacks and packets the appliance blocked over time. The Security section includes the Security Dashboard, which you use for general security health information about your Network IPS. On the dashboard, you can find consolidated information about the following security options:

- Overall security health
- Top 10 Attacks

  You can inspect the name of the attack and when it occurred.

- Top 10 Intruders

  This option helps you to find the IP address of an intruder and the time of the attack.

- Top 10 Victims

  The information from this option helps you determine which IP address is being attacked and when.

- Last 10 IPS Events

  This option provides information about intrusion prevention events, such as when they occurred, the names, severity, and status.

- Blocked Attacks

  This option provides information about the number of attacks that the appliance blocked. You can compare this number to the number of attacks it did not block.

- Blocked Packets

  This option provides information about the number of packets the appliance blocked. You can compare this number to the volume of traffic in the network.

  You can examine the information in these options in more detail by going to the specific menu items under the **Security** menu option.

In addition to the graphical representations, the following options show results in a table:

- Protection Analysis Statistics

  Use the Protection Analysis Statistics page to view all the statistics output of the Protocol Analysis Module. You can use this information to track protocol counts and protocol processing.

- Network Protection Statistics

  Use the Network Protection Statistics page to view information about the current appliance configuration and behavior that occurred as a result of the configuration. You can find statistics about enabled event checks and details about attack and blocking actions that the appliance has taken.

System

By using the tools in the System section, you can review the health of your system. You can find detailed information about the appliance, memory and storage usage, and system events, such as recent firmware updates, IBM Security SiteProtector communication, and license availability.

Beside the Dashboard view, you have other options to review some of the system settings in more detail. One set of information that is not visible from the dashboard is the Significant Events page to view system events that the appliance processes and when the events occur.

Secure (third menu option)

The Secure page is the third menu option from the left in the dashboard. It helps you to monitor network traffic and block attacks by applying different protection settings. Figure 2-6 shows that the Secure section page classifies security settings into four major areas:

- Security Modules
- Advanced IPS
- Response Tuning
- Firewall

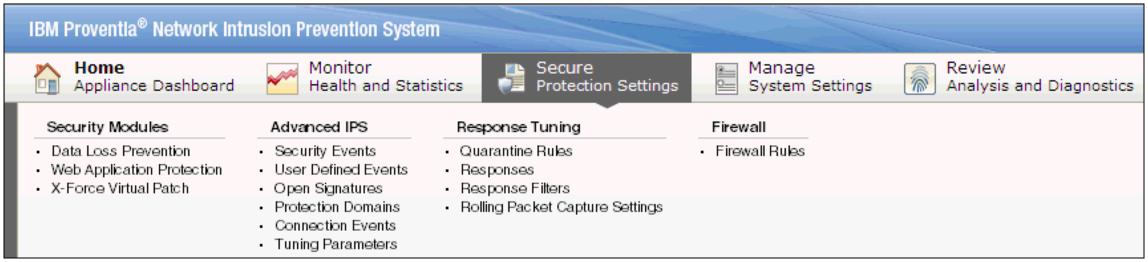


Figure 2-6 Secure page (protection settings) of the LMI

Security Modules

You use the Security Modules options on your Network IPS appliance to configure features for analyzing suspect content, protecting web applications, and enabling X-Force Virtual Patch functions. For more information about these settings, see 2.3.2, “Security modules” on page 56.

Advanced IPS

You use the Advanced IPS options on your Network IPS appliance to configure IPS settings specifically to meet the security requirements of your network. You configure options such as protection domains, security events, user-defined events, open signatures, and connection events. You also set global and local tuning parameters. For more information about these settings, see 2.3.3, “Advanced IPS” on page 62.

Response Tuning

You use Response Tuning on your Network IPS appliance to configure quarantine rules, set responses to events, tune responses in your security policies with response filters, and configure rolling packet capture settings. For more information about these settings, see 2.3.4, “Response Tuning” on page 63.

Firewall

You use Firewall rules on your Network IPS appliance to configure rules to drop or block attacks based on various source and target information in the packet before they enter your network. For more information about these settings, see 2.3.5, “Firewall” on page 64.

Manage (fourth menu option)

The Manage page is the fourth menu option from the left in the dashboard. It contains a set of tools to use for managing different appliance settings, such as HA, user accounts and passwords, authentication methods, updates, and licensing.

Figure 2-7 shows that the Manage page provides multiple actions that are divided in four subsections.

- Network
- Appliance Access
- Appliance
- Updates and Licensing

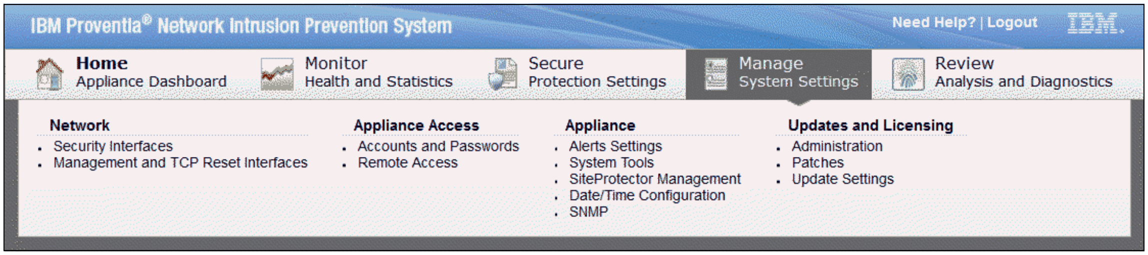


Figure 2-7 Manage page (system settings) of the LMI

Network

The Network settings provide two separate sections for security and management interfaces:

- Security Interfaces that you can use to perform the following actions:
  - Configure the adapter list, which is used to view and manage the network security interfaces of the appliance.
  - Configure HA, which is used to configure the high availability mode of the appliance.
- Management and TCP Reset Interfaces

  You use the Management and TCP Reset Interfaces page on your Network IPS appliance to set network configuration options, such as a host name, the DNS search path, and speed and duplex settings.

Appliance Access

The Appliance Access menu offers options regarding access management. These options include, for example, resetting default accounts passwords, adding authentication servers (LDAP, Microsoft Active Directory, or Radius), and managing additional (non-default) users. Users of this menu can have one of two roles: Admin or Read-only.

> **Read-only users:** Read-only users can access the IBM Security Network IPS only through the web-based LMI. SSH and local console access are disabled for them.

You can also configure the password policy to manage password complexity, expiration dates, allowable characters, and other options for user accounts. The appliance does not apply password policies to the root account or to remote user accounts.

Appliance

In the Appliance area of system settings, you can configure alerts, IBM Security SiteProtector management, date and time, and SNMP and SNMP traps. You can also restart or shut down your Network IPS appliance.

Updates and Licensing

With the Updates and Licensing page, you can administer licenses and system updates. This page also provides information about whether the IBM Security Network IPS is current with the latest firmware and intrusion prevention (security) updates. It also lists any updates you installed on the appliance.

Review (fifth menu option)

The Review page is the fifth menu option from the left in the dashboard. It contains a set of tools to help in diagnostic testing and troubleshooting. Figure 2-8 shows the Review page actions divided into three subsections.

- Logs
- Diagnostics
- Downloads

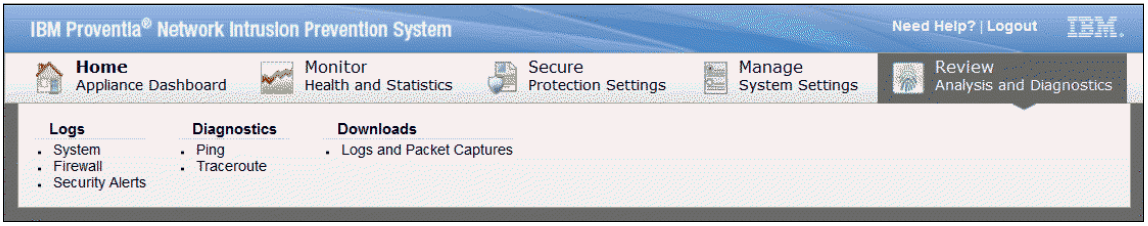


Figure 2-8 Review page (analysis and diagnostics) of the LMI

Logs

You use the Logs area of the dashboard of your Network IPS appliance to view system, firewall, and security alert logs. You can filter these lists for specific keywords and network characteristics and then save your searches for future use.

Diagnostics tools

You use the Diagnostics area of your Network IPS appliance to test communications and trace IP packets.

Downloads

In the Downloads section, you can view and download log files and packet captures that are associated with your Network IPS appliance and translate log file timestamps.

2.2.3 Deployment options

The IBM Security Network IPS appliances can be cabled and configured in several types of deployment scenarios. For a more detailed description of these options, including HA scenarios, see Chapter 3, “IBM Security Network IPS architecture” on page 73. This chapter focuses on introducing some of the available options.

Inline or passive mode

The IBM Security Network IPS supports three modes of operation:

- Passive monitoring

  Passive monitoring mode is similar to a traditional intrusion detection system (IDS). It sits on a side channel of the actual production-network and passively listening in on and analyzes the traffic using a promiscuous interface. In this mode, responding to TCP attacks is done manually by sending TCP reset packets to both source and destination hosts to prevent certain attacks.

- Inline simulation

  Inline simulation mode acts as a learning mode for the appliance sitting inline in the network, alerting you about traffic that might otherwise have been blocked (in inline prevention mode). This mode is often used by organizations to ensure that no false positives are blocking valid traffic before converting to inline protection mode.

- Inline protection

  Inline protection mode also sits inline on the wire. However, it actively blocks malicious and unwanted traffic according to the security policy that has been applied, without user intervention being required. The malicious packets are not allowed to traverse the IBM Security Network IPS and are unable to reach their target.

Figure 2-9 illustrates these three modes of operation.

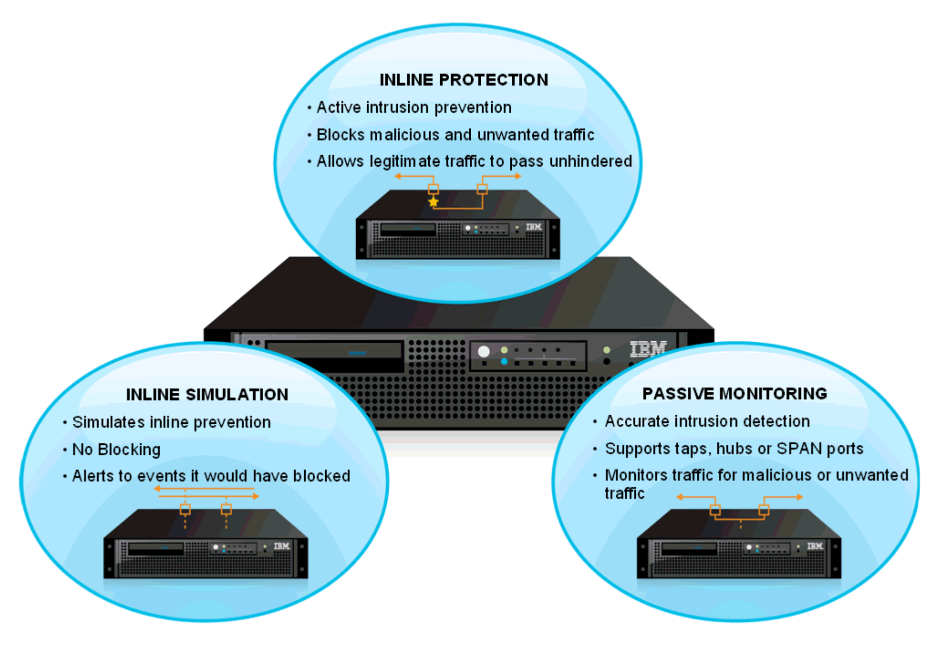

INLINE PROTECTION
• Active intrusion prevention
• Blocks malicious and unwanted traffic
• Allows legitimate traffic to pass unhindered
INLINE SIMULATION
• Simulates inline prevention
• No Blocking
• Alerts to events it would have blocked
PASSIVE MONITORING
• Accurate intrusion detection
• Supports taps,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

Figure 2-9   Three modes of operation for the IBM Security Network IPS

Passive monitoring mode can be used with the *TCP_Reset* port on the IBM Security Network IPS appliances. Together they block certain types of attacks that use TCP as the transport layer protocol and when it is not physically possible to place a network IPS appliance between two devices. An example is a TCP session between two hosts on the same Layer 2 switch.

Figure 2-10 shows a cabling diagram that illustrates this type of passive deployment scenario.

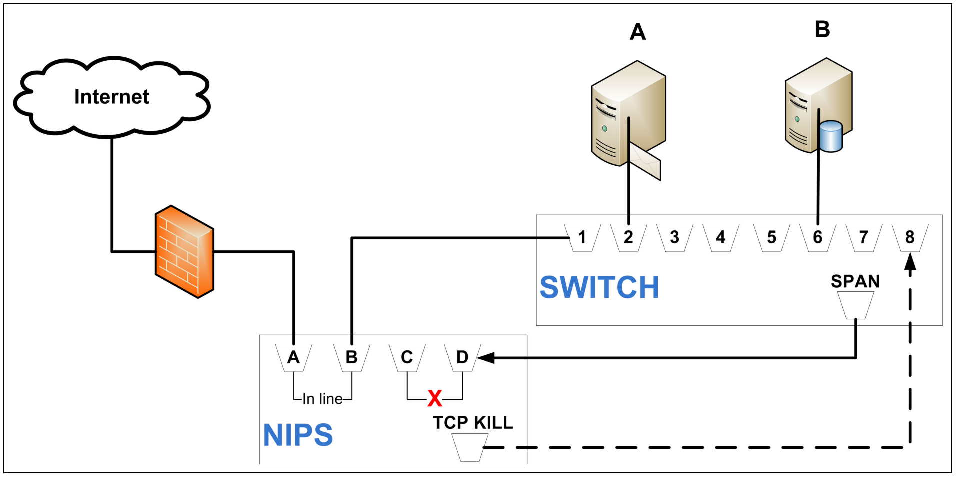


Figure 2-10 Cabling overview of a network IPS in passive monitoring mode

You can use *passive monitoring* mode and connect one of the available monitoring ports on the IBM Security Network IPS to a SPAN port on that switch and the TCP_Reset port to another available port on the same switch. This way, TCP sessions between the two hosts that are deemed to be malicious can be reset.

The IBM Security Network IPS is a preconfigured appliance. It operates effectively by using an easily integrated configuration, whether it is deployed in passive monitoring, inline simulation, or inline protection mode.

High availability

IBM Security Network IPS models GX5008 and later support several types of HA network setups. They can operate in active/active or active/passive networks. Since the release of firmware 4.1, they also work in geographically dispersed HA setups. For more information about possible HA deployment models, see 3.4, “High availability” on page 97.

The IBM Security Network IPS appliances rely on existing networking equipment to determine when to fail over and how to orchestrate failover. They do not participate in the Virtual Router Redundancy Protocol (VRRP) or Hot Standby Router Protocol (HSRP).

Most networks sense failure by a lack of link state. To support this capability, the IBM Security Network IPS has link state propagation enabled by default. If the link goes down on one side of the appliance, the link on the other side is automatically taken down. This behavior can be changed through configuration options.

IBM Security Network Active Bypass

IBM offers external bypass units that can be used with its Network IPS devices. These bypass units ensure that the network remains functional and users have unimpeded access to important applications if the IBM Security Network IPS appliance fails for any reason. The bypass units make sure that the network traffic is only sent through the IBM Security Network IPS as long as the IBM Security Network IPS is operating normally. If a failure is detected, then the IBM Security Network IPS is bypassed.

2.2.4 Virtual Network IPS appliances

As part of the overall IBM Security Network IPS portfolio, two virtual appliances are available, the GV200 and GV1000. They are provided as preconfigured virtual machine (VM) packages.

Deploying an IBM Security Network IPS Virtual Appliance provides the following benefits:

- Inheritance of the lower total cost of ownership (TCO) realized in a virtual environment

  For more information about why to use virtual solutions, see the white paper *Why Choose VMware* at:

  http://www.vmware.com/files/pdf/vmware_advantage.pdf
- IBM Security X-Force powered protection in a virtual environment
- Lowered complexity with centralized operations
- Protection of web applications, web server, and browsing clients

The following virtual interfaces are automatically created during the installation process:

- TCP reset port, which is optionally used for resetting TCP connections when the VM is configured in passive mode
- Management port, which is used for connection to IBM Security SiteProtector and the LMI
- Two inspection or monitoring ports

To understand the system requirements of the server onto which you are deploying these products, see the *System Requirements for IBM Security Network IPS Virtual Appliances* guide in the IBM Security Network Intrusion Prevention System Information Center at:

http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=/com.ibm.ips.doc/IBMSecNetIPS_landing_page.html

Monitoring limits: Unlike the physical appliances, the virtual appliances have only *two* monitoring (sensor) ports.

Figure 2-11 shows a deployment in which the virtual appliance provides protection to the cluster of VMs. Other deployment scenarios, such as bridging two physical networks, are also possible.

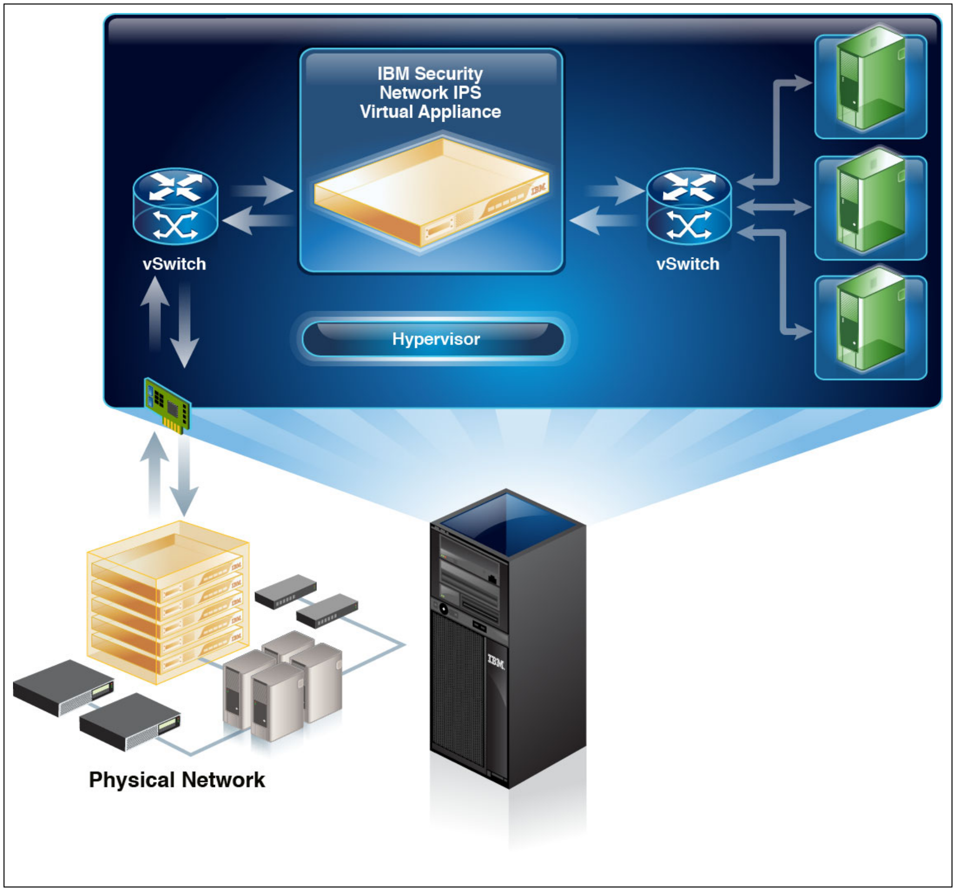


Figure 2-11 Single virtual appliance on a physical server protecting a virtual server farm

IBM also offers a more advanced solution for providing intrusion prevention in virtual environments. The IBM Security Virtual Server Protection for VMware offers integrated threat protection for VMware ESX and VMware ESXi. It provides protection for *multiple layers* of the virtual infrastructure, including the protection on the virtual network (which the IBM Security Network IPS Virtual Appliance can also provide). Virtual Server Protection for VMware also protects the VMs and traffic between the VMs.

The transparent intrusion prevention and firewall in Virtual Server Protection for VMware provides multilayered IPS and firewall technology. They protect the virtual data center in a solution that is purpose-built to protect the virtual environment at the core of the infrastructure. For more information about Virtual Server Protection for VMware, see the Redbooks publication *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581.

2.3 IBM Security Network IPS functionality

The IBM Security Network IPS delivers preemptive network protection through its combination of line-speed performance, security intelligence, and a modular protection engine that delivers security convergence. This section highlights several security capabilities that the IBM Security Network IPS product offers.

Figure 2-12 on page 54 illustrates how the security capabilities of the IBM Security Network IPS can be mapped to the IBM Security Blueprint. This diagram shows the functional components of the Threat and Vulnerability Management solution pattern. The darker highlighted elements indicate the functional components that can be fulfilled or implemented by using IBM Security Network IPS. This functional highlighting is also applicable for the infrastructure service components. For more information about the IBM Security Blueprint, see the IBM Redpaper publication *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, REDP-4528.

In addition to the fully highlighted elements, Figure 2-12 on page 54 also shows medium highlighted elements. Although the IBM Security Network IPS can be used to address such components to some degree, the respective area of coverage is not considered a core function of the product and thus is considered to be limited.

You might determine the desired function of a solution by using the Threat and Vulnerability Management solution pattern. In this case, you can use the mapping shown in Figure 2-12 on page 54 as a quick reference of the functional security management aspects of the IBM Security Network IPS. This reference can help you determine which functions of a solution can be covered by selecting this product.

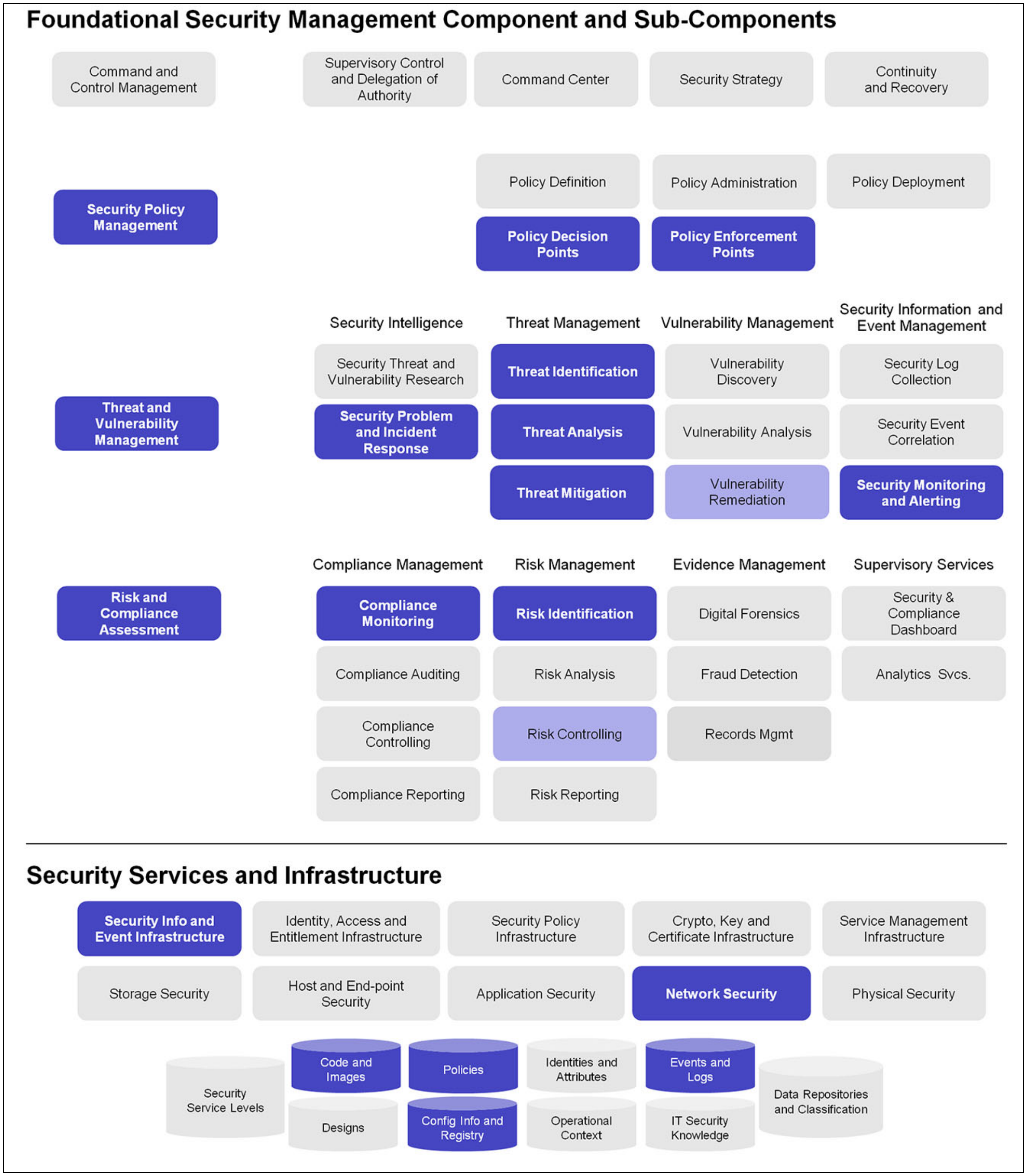

Foundational Security Management Component and Sub-Components
Command and Control Management
Supervisory Control and Delegation of Authority
Command Center
Security Strategy
Continuity and Recovery
Security Policy Management
Policy Definition
Policy Administration
Policy Deployment
Policy Decision Points
Policy Enforcement Points
Threat and Vulnerability Management
Security Intelligence
Threat Management
Vulnerability Management
Security Information and Event Management
Security Threat and Vulnerability Research
Threat Identification
Vulnerability Discovery
Security Log Collection
Security Problem and Incident Response
Threat Analysis
Vulnerability Analysis
Security Event Correlation
Threat Mitigation
Vulnerability Remediation
Security Monitoring and Alerting
Risk and Compliance Assessment
Compliance Management
Risk Management
Evidence Management
Supervisory Services
Compliance Monitoring
Risk Identification
Digital Forensics
Security & Compliance Dashboard
Compliance Auditing
Risk Analysis
Fraud Detection
Analytics Svcs.
Compliance Controlling
Risk Controlling
Records Mgmt
Compliance Reporting
Risk Reporting
Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Policies
Identities and Attributes
Events and Logs
Data Repositories and Classification
Designs
Config Info and Registry
Operational Context
IT Security Knowledge

Figure 2-12 Mapping of the IBM Security Network IPS to the IBM Security Blueprint

The IBM Security Network IPS delivers network protection with the following functions:

- Stops threats before they impact network assets without sacrificing high-speed network performance
- Provides a platform for security convergence that eliminates the costs of deploying and managing point solutions for web application and data security
- Protects networks, servers, desktops, and revenue-generating applications from malicious threats
- Conserves network bandwidth and prevent network misuse or abuse from instant messaging (IM)and peer-to-peer file sharing
- Prevents data loss and aids compliance efforts

The IBM Security Network IPS can stop Internet threats before they affect your organization. It delivers protection to all three layers of the network: core, perimeter, and remote segments.

The IBM Security X-Force research and development organization enables *ahead of the threat* protection for an IT infrastructure before vulnerabilities are made public and before exploits against those vulnerabilities become available.

By consolidating network security demands for Data Loss Prevention and Web Application Protection, IBM Security Network IPS serves as the security platform that helps reduce the costs of deploying and managing point solutions.

When evaluating intrusion prevention technology, organizations often struggle to balance and optimize the following six areas:

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

The IBM Security Network IPS delivers on all six areas, with performance, preemptive protection, HA, simple deployment and management, and excellent customer support. Organizations can manage the IBM Security Network IPS products themselves. Alternatively, they can transfer the risk of protecting their network to a trusted security partner such as the IBM Security Services division, which you can learn more about at:

http://www.ibm.com/services/us/en/it-services/security-services.html

Working with IBM organizations provides benefits from a range of complementary consulting services for assessment, design, deployment, management, and education. To learn more about the IBM Security Services offerings in this space, see the Redbooks publication *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581.

2.3.1 Zero-day threat protection

IBM Security Network IPS delivers zero-day threat protection through the X-Force Virtual Patch technology. By providing the X-Force Virtual Patch, with the IBM Security Network IPS, organizations can avoid emergency patching. The X-Force Virtual Patch blocks attacks against vulnerabilities at the network level before they can reach their targeted system, application, or network resource.

IBM Security X-Force research and the IBM Security Network IPS PAM identify and block attacks based on the vulnerability. Therefore, IBM Security Network IPS does *not* require a new signature for every new exploit that is created. The PAM engine employs multiple intrusion prevention technologies in tandem to monitor, detect, or block these classes of network threats, such as cross-site scripting, drive-by downloads, and web browser attacks.

PAM adapts its algorithms to the network traffic and the available resources. However, in some environments, you can benefit from fine-tuning the PAM algorithms using various advanced tuning parameters. IBM Security Systems also changes the algorithms regularly by using security content updates and through extensive use of beta programs, customer feedback, and close cooperation with IBM Managed Security Services.

For more information about PAM engine, see Chapter 3, “IBM Security Network IPS architecture” on page 73.

2.3.2 Security modules

To simplify the configuration of the most important protection aspects of the IBM Security Network IPS, a separate option, *Security Modules*, is available in the appliances web-based management dashboard (Figure 2-13 on page 57). This menu option simplifies the configuration of the following items:

- Data Loss Prevention
- Web Application Protection
- X-Force Virtual Patch

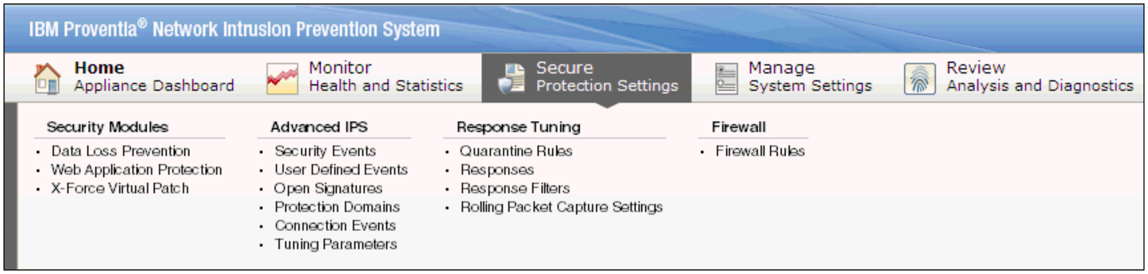


Figure 2-13 IBM Security Network IPS management dashboard showing the Security Modules

The following sections explain these Security Modules.

Data Loss Prevention

Data loss can be costly for any organization, and it can occur in many ways. For example, data can leak purposely from an insider who intentionally takes information from the network, or data loss can happen accidentally. In keeping with the scope of this book, this section addresses how threat mitigation techniques can complement DLP techniques.

Information can be digitally stored in various ways. It can be structured, unstructured, images, video, voice, or many other types of formats. To make matters more complex, data can be stored on many types of devices, such as cell phones, laptops, USB drives, portable media players, or personal digital assistants (PDAs), and in briefcases.

However, the access and changes to the data introduce the risk. If someone accesses the data, that person has many opportunities to move the data across the digital network (over voice, audio channels, or both), cut and paste the data into an email message, print or fax the data, and so on.

The process of outlining the risk of data leakage entails the following actions:

- Assess

  Regarding the access of data at rest, you might want to ask: “Do I have intellectual property, confidential records, or personally identifiable information (PII) that potentially violates policy or government regulations, is on the verge of being compromised, or both?” You can only adequately protect your data when you know how it is classified.

- Protect

  When you identify the need to protect the data usage at the endpoint, consider methods to categorize the data, standardize policies, manage data protection issues at the point of use, and keep those policies manageable.

- Defend

  Regarding data in transit, guarding the data while it is at rest might not be an issue. However, you must manage policies that can help protect the data while sharing it and note the issue surrounding the internal threats to the organization.

- Monitor

  The number of integrated solutions keeps growing, and the ability to report and track information about multiple consoles can be a daunting task. It is as though you have so much control, yet you are out of control.

- Control and respond

  The amount of data you must respond to can create additional problems. With false positives, and the amount of data to sort through, the real violations can be lost. Data leakage strategies typically do not begin with protection technologies.

  However, threat mitigation technologies can assist with identifying data leakage problems in the environment. They can also provide insight to where the data leakage problem might exist, and therefore, provide a complement to address the problems listed previously.

  Although data leakage is typically addressed at the point where the data resides, two key technologies help complement a data leakage network architecture: network IPSs and mail security systems.

  By understanding the communication between hosts, you can get a visual representation of the data movement in your network. Many times, this representation can lead you to detect areas of concern that previously went unnoticed.

  The IBM Security Network IPS can also help you gain insight into improving the protection of data movement. In this case, the data must be unencrypted and available for the IPS to see, which allows it to locate misuse and abuse from an insider.

  Modern IPSs can examine files and content within the data stream that passes through the appliance. By looking for keywords and information associated with important business aspects, you can use an existing IPS infrastructure to watch for data leakage. For example, you can look for data signatures, inspection of the use of common and uncommon protocols, and the content that can be carried within the protocol.

- Content types

  Typically, the data content that is being searched for includes PII, where someone is trying to gain access to steal another person’s identity. Examples include credit card numbers, Social Security numbers, and email or postal addresses.

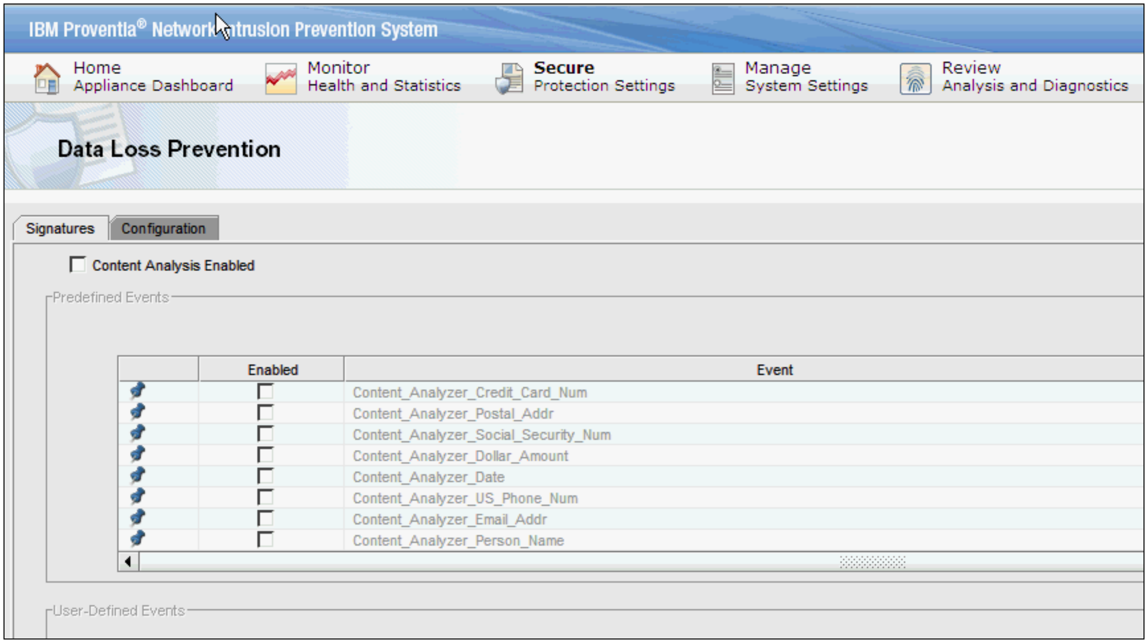
- Protocols

  The protocols that are inspected include HTTP, FTP, SMB, IMAP, POP3, SMTP, and IRC. They also include peer-to-peer protocols, such as Yahoo! Messenger, Microsoft Messenger, and AOL IM.

- File types

  The types of files that are being inspected include Microsoft Office documents, PDF files, HTML files, and compressed files.

The Data Loss Prevention policy editor (Figure 2-14) shows that a DLP policy can be made up of a combination of predefined events and user-defined events.



□ Content Analysis Enabled

Predefined Events

	Enabled	Event
	□	Content_Analyzer_Credit_Card_Num
	□	Content_Analyzer_Postal_Addr
	□	Content_Analyzer_Social_Security_Num
	□	Content_Analyzer_Dollar_Amount
	□	Content_Analyzer_Date
	□	Content_Analyzer_US_Phone_Num
	□	Content_Analyzer_Email_Addr
	□	Content_Analyzer_Person_Name

User-Defined Events

Figure 2-14 Data Loss Prevention policy editor

Web Application Protection

The security communities behind the Web Application Security Consortium (WASC) and the Open Web Application Security Project (OWASP) continue to develop and refine a common testing and evaluation standard for web applications. In line with this refined testing methodology, IBM introduced *Web Application Protection* as a new threat category.

> **More information:** For more information about WASC, see the WASC website at:
>
> `http://www.webappsec.org/`
>
> For more information about OWASP, see the OWASP website at:
>
> `http://www.owasp.org/`

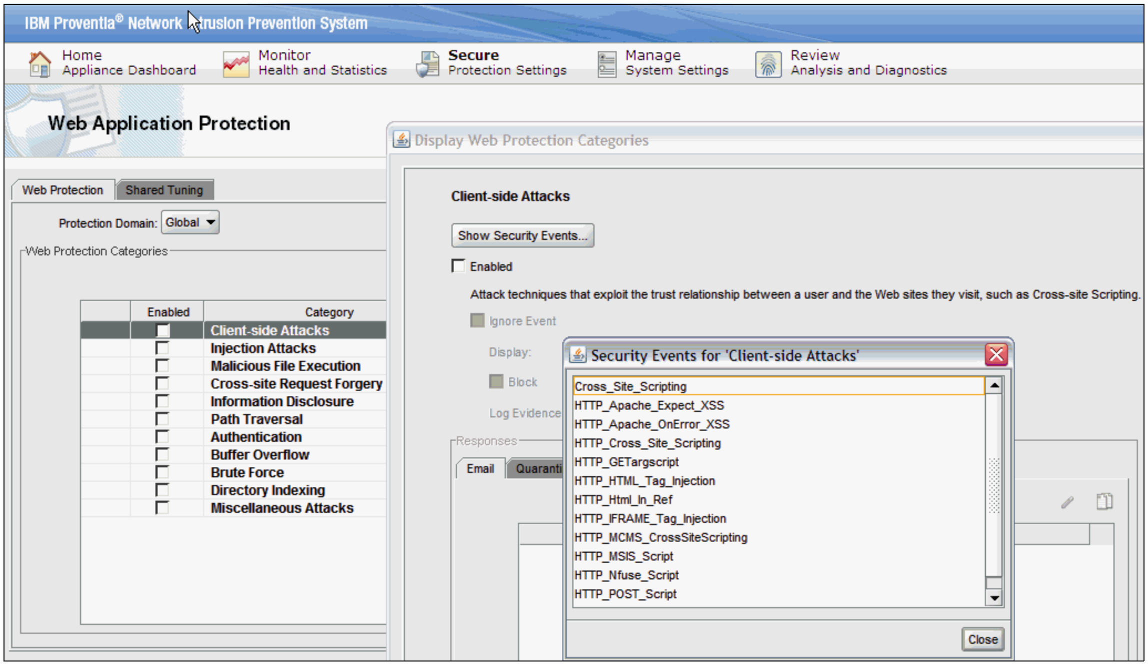
This introduction has the following goals:

- Group together the web application attack signatures into a single category.
- Simplify the policy management of these signatures.

This new threat category includes the following attack types:

- Client-side attacks
- Injection attacks
- Malicious file execution
- Cross-site request forgery (CSRF)
- Path traversal
- Buffer overflow
- Directory indexing

Figure 2-15 shows the Web Application Protection policy editor that is available in the IBM Security Network IPS management dashboard.



Protection Domain: Global

Web Protection Categories

Enabled	Category
☐	Client-side Attacks
☐	Injection Attacks
☐	Malicious File Execution
☐	Cross-site Request Forgery
☐	Information Disclosure
☐	Path Traversal
☐	Authentication
☐	Buffer Overflow
☐	Brute Force
☐	Directory Indexing
☐	Miscellaneous Attacks

Client-side Attacks

Show Security Events...

☐ Enabled

Attack techniques that exploit the trust relationship between a user and the Web sites they visit, such as Cross-site Scripting.

☐ Ignore Event

Display:

☐ Block

Log Evidence

Responses

Email | Quaranti

Security Events for 'Client-side Attacks'

Cross_Site_Scripting
HTTP_Apache_Expect_XSS
HTTP_Apache_OnError_XSS
HTTP_Cross_Site_Scripting
HTTP_GETargscript
HTTP_HTML_Tag_Injection
HTTP_Html_In_Ref
HTTP_IFRAME_Tag_Injection
HTTP_MCMS_CrossSiteScripting
HTTP_MSIS_Script
HTTP_Nfuse_Script
HTTP_POST_Script

Close

Figure 2-15 Web Application Protection policy editor showing some of the client-side attack signatures

To see how closely the Web Application Protection categories match OWASP Top Ten Web Application Security Risks or for more information about this WAP component, see the following resources:

- OWASP Top Ten Project

  `http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project`

- *OWASP Testing Guide*

  `http://www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf`

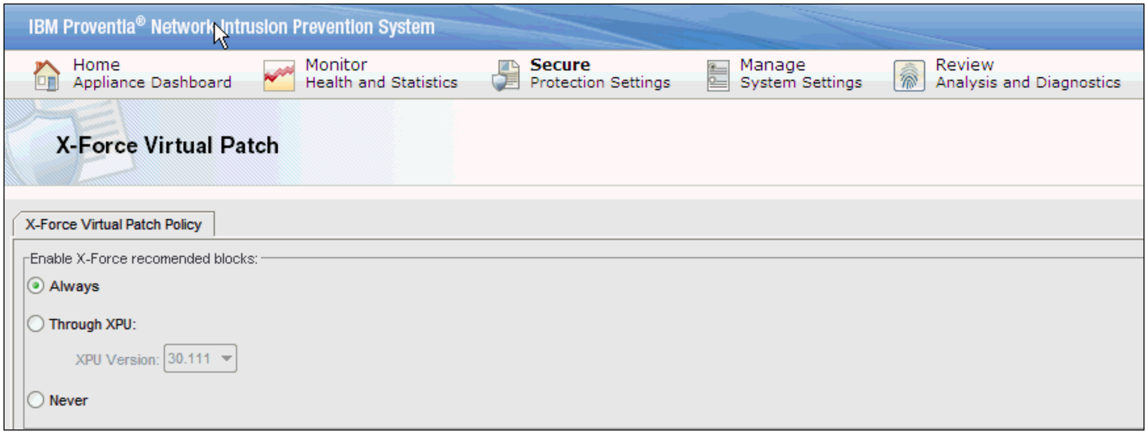
> **Where to look:** The attack signatures in the Web Application Protection policy editor are not present in the general *Security Events* policy editor.

X-Force Virtual Patch

The third security module is the X-Force Virtual Patch module. Within this menu option, the user can define whether the default *block responses* as defined and recommended by IBM Security X-Force are turned on or off.

In order for a specific signature to detect an attack and to block it, it must have the associated *block response* enabled. To simplify the deployment of the products in real-life environments, the IBM Security X-Force team specifies default block responses for those signatures in each X-Press Update (XPU) where they recommend blocking to be enabled. Administrators can then decide whether they want to trust the X-Force default block responses. For more information about this option, see Chapter 4, “IBM Security Network IPS solution design and management” on page 103.

By using the X-Force Virtual Patch menu option, an administrator can change this setting, as shown in Figure 2-16.



Enable X-Force recomended blocks:

● Always

○ Through XPU:

XPU Version: 30.111

○ Never

Figure 2-16 X-Force Virtual Patch policy editor

Individual block responses for specific signatures can still be modified by using the policy editor in the *Security Events* menu option as explained in 2.4, “Enforcing intrusion prevention policies” on page 64.

2.3.3 Advanced IPS

With the Advanced IPS options on the IBM Security Network IPS appliance, you can configure settings that tune IPS settings specifically to meet the security requirements of your organization. The configuration options are available for protection domains, security events, user-defined events, open signatures, and connection events. They also enable the setting of global and local tuning parameters.

The following options are available:

- *Security Events*. You can use the Security Events page on your IBM Security Network IPS appliance to view attacks and audits and to configure security events.
- *User Defined Events*. You can configure user-defined events to specify the type and part of a network packet that your Network IPS appliance scans for events. User-defined events can be created by using specific contexts for use globally with the global protection domain or locally with the custom protection domains.
- *Open Signatures*. On the Open Signatures events page of the IBM Security Network IPS appliance, you can write customized, pattern-matching signatures using a flexible rules language.
- *Protection Domains*. You can use protection domains on your Network IPS appliance to configure domains where you can apply policies to deploy across groups of network assets or globally across your organization.
- *Connection Events*. Connection events are user-defined notifications of open connections to or from particular addresses or ports. They are generated when the appliance detects network activity at a designated port, regardless of the type of activity, the type of network packets, or the content of network packets exchanged.
- *Tuning Parameters*. You can use the Tuning Parameters page to configure certain parameters. Then you can apply them globally to a group of Network IPS appliances to better meet your security needs or to enhance the performance of your hardware.

2.3.4 Response Tuning

You can use Response Tuning on your IBM Security Network IPS appliance to configure quarantine rules, set responses to events, tune responses in your security policies with response filters, and configure rolling packet capture settings.

The following options are available:

- *Quarantine Rules*. On the Quarantine Rules page on your IBM Security Network IPS appliance, you can modify rules dynamically generated in response to detected intruder events. These rules can prevent worms from spreading and deny access to systems that are infected with back doors or Trojan horses.
- *Responses*. The responses in this section determine how you want the appliance to notify you when it detects an intrusion or other important events

in your system. You can create different types of responses and then apply them to events as necessary.

- *Response Filters*. You can use response filters on your Network IPS appliance to refine your security policies. They can control the number of events to which the appliance responds and the number of events reported to the management console.
- *Rolling Packet Capture*. On the Rolling Packet Capture Settings page on the IBM Security Network IPS appliance, you can configure how the appliance captures and stores network packet information for troubleshooting or general network analysis.

2.3.5 Firewall

You can use *firewall rules* on your IBM Security Network IPS appliance to configure rules which drop or block attacks based on various source and target information in the packet before they enter your network. Alternatively as explained in “Whitelisting or blocking traffic through the firewall module” on page 132, the firewall rules can also change the way the IBM Security Network IPS inspects or ignores network traffic.

Firewall rules work only when you set the appliance to inline protection mode. An appliance in passive mode works similar to a traditional sensor and is not in the direct path of the packets. In simulation mode, packets still pass through the appliance, and the appliance describes what it might have done to the traffic in protection mode.

> **Firewall rule order:** The IBM Security Network IPS reads the list of firewall rules from top to bottom in the order in which they are listed and applies corresponding actions.

2.4 Enforcing intrusion prevention policies

The need to enforce a policy with the goal of preventing intrusions is readily understood and accepted. A granular intrusion prevention policy must be defined, enforced, audited, revised, and re-enforced. Due to the impact of managing a granular policy, many system owners opt to outsource these types of burdens to a trusted security partner such as IBM Managed Security Services, which you can learn more about at:

http://www.ibm.com/services/us/en/it-services/managed-security-services.html

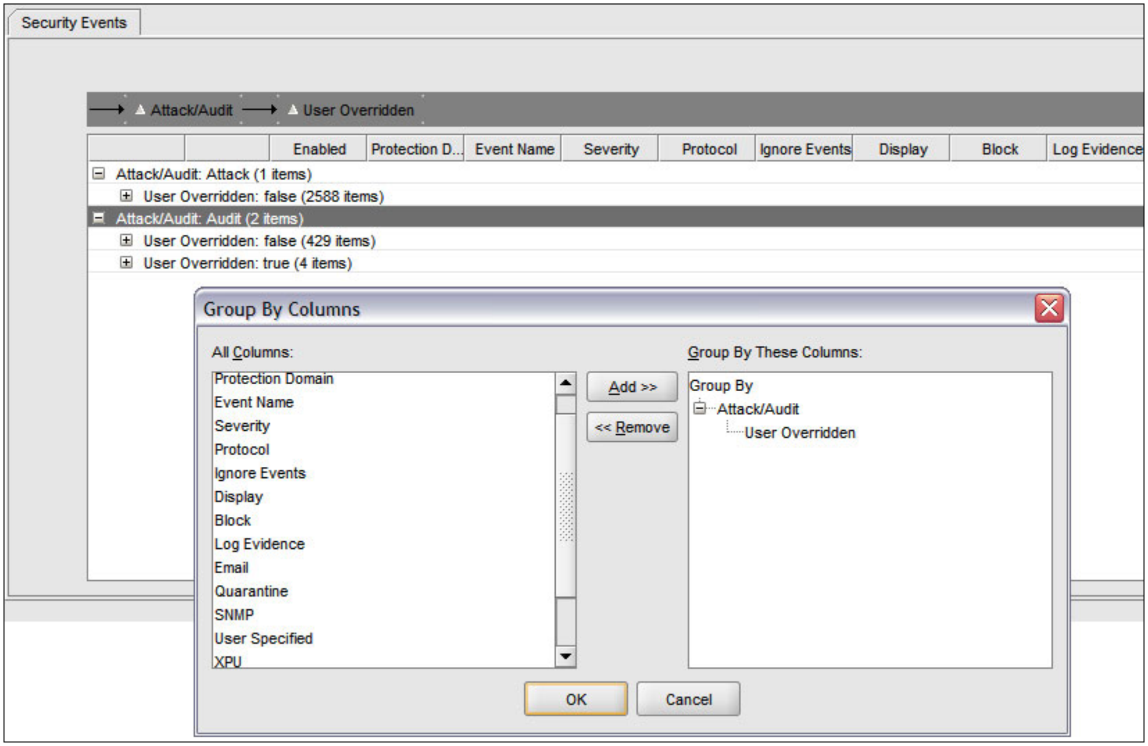
However, you must still take responsibility for evaluating and updating the policy at specific intervals. Organizations expect their security technologies to protect them against each new threat with the same efficiency and level of performance as the day the solution is first purchased and installed.

New threats are not the only unauthorized activity that protection technology must combat. Older threats still plague the Internet. They must continually be prevented, whether they are old login bypass vulnerabilities, web browser exploits, worm infestations, or new vectors for previously incorrectly classified vulnerabilities. Many of these threats are in the eradicated phase of the vulnerability life cycle for many years. However, they continue to find avenues of success if the diligence to continue to prevent them is not present. Therefore, older threats must continue to be monitored and prevented.

To provide organizations with granular policy management capabilities, IBM Security Network IPS uses the concept of *protection domains*. By default, each IBM Security Network IPS has its own global protection domain. Organizations can specify their own specific protection domains, for example, for a specific set of servers. Then they can apply a specific subset of signatures to that *protection domain*. Protection domains can be defined according to the following parameters (including combinations thereof):

- Specific interface (port) on the IPS
- VLAN tag or range
- IP address or range

After one or more *protection domains* are configured, you can then allocate specific signatures to each one. To simplify this process, with the policy editor, signatures can be grouped, for example, by X-Press Update (XPU) version number or by protocol (Figure 2-17 on page 66).



Attack/Audit: Attack (1 items)
User Overridden: false (2588 items)
Attack/Audit: Audit (2 items)
User Overridden: false (429 items)
User Overridden: true (4 items)

Figure 2-17 Signature grouping on the Security Events page

In addition, the following intrusion responses (and combinations thereof) are configurable within the policy editor:

- Block
- Ignore
- Log and log evidence
- Email
- Quarantine
- SNMP
- User-defined

When it comes to logging data that might be necessary for auditing purposes, the following log options are available:

- Attack packet logging
- Pcap file

Log files can be accessed from the web-based interface of the appliance by using the *Logs and Packet Captures* menu item (Figure 2-18).

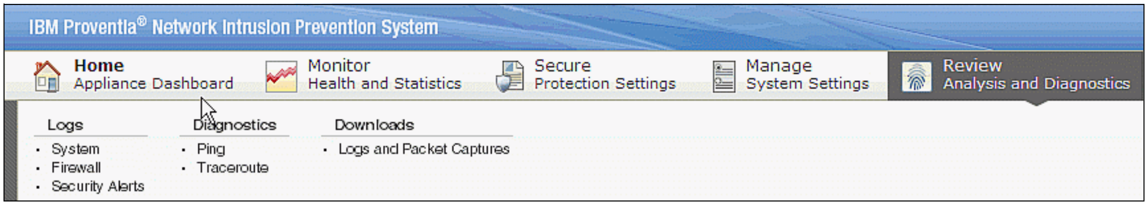


Figure 2-18 Logs and Packet Captures menu Item

2.5 Centralized management in IBM Security SiteProtector

Managing your security infrastructure is never an easy task. However, when you are trying to manage multiple devices from security vendors and you have to answer to a list of compliance regulations, it might seem impossible. Over time, the cost and complexity of securing your organization can rise substantially, without a corresponding decrease in your exposure to security risks and noncompliance. Valuable resources are continually diverted from revenue-gathering projects, while your IT staff spends hours on day-to-day administration.

A centralized management system can offer a flexible way to command and control a broad array of network security agents and appliances. With such a centralized system, you can monitor and measure your exposure to vulnerabilities and demonstrate regulatory compliance, all from one single interface. This centralized approach can reduce the burden of your IT security team by unifying the management of security platform offerings across gateways, networks, servers, desktops, and select third-party security solutions.

The centralized management system can help reduce operational costs by automating and simplifying tasks, such as setting policies, applying updates, and enabling protection.

2.5.1 Managing policies

IBM Security SiteProtector provides an array of functionality. For information about the full spectrum of functionality, including asset management, event analysis, and reporting, see *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581. This Redbooks publication focuses on centrally managing IBM Security Network IPS policies.

This section addresses the hierarchical model that IBM Security SiteProtector uses to assign policies and policy elements. It explains how IBM Security SiteProtector keeps track of policy changes, how you can compare policies, and how you can manage, deploy, and roll back several versions of a given policy.

Hierarchical policy model

IBM Security SiteProtector uses a *hierarchical inheritance model* to manage policies across all of the asset groups in a site. In this environment, you can apply a single, distributed policy element to multiple agents and groups.

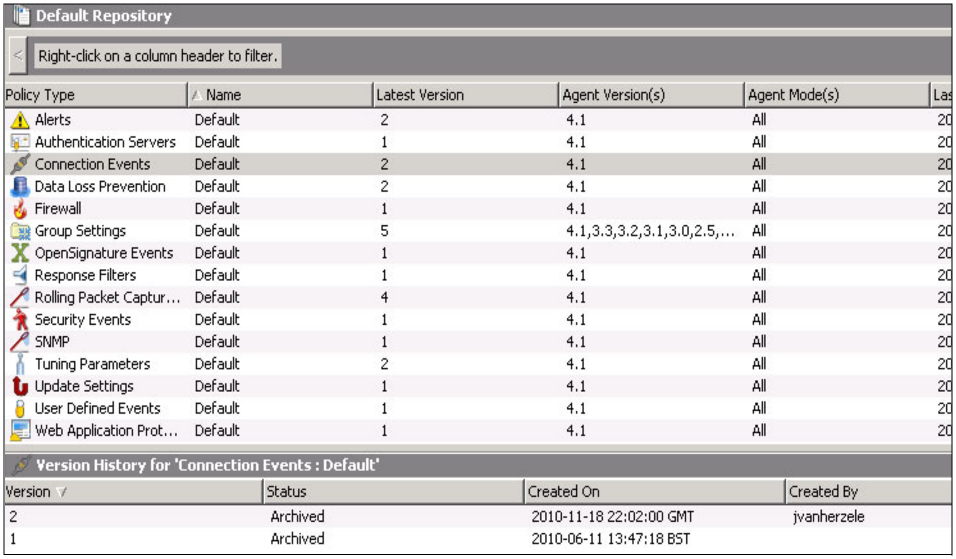
The main advantage of using *policy inheritance* is the fact that you can share policies among several appliances while maintaining sufficient flexibility to tailor individual appliances or software agents.

Often you find that many configuration elements are the same throughout your organization. You can use the same type of update settings for all your IBM Security Network IPS appliances, but give them a different type of response to attacks depending on their location in the network.

> **Remember:** You can also assign policies to specific agents and not just to groups. Agent-specific policies are not shared among appliances.

2.5.2 Policy repositories

A *policy repository* (Figure 2-19 on page 69) is a workspace that you can use to store, modify, and deploy the hierarchical agent policies used in your organization. To maximize your control over hierarchical policies, with IBM Security SiteProtector, you can create a separate *repository* for any group you want to create.



Default Repository

Right-click on a column header to filter.

Policy Type	Name	Latest Version	Agent Version(s)	Agent Mode(s)	Las
Alerts	Default	2	4.1	All	20
Authentication Servers	Default	1	4.1	All	20
Connection Events	Default	2	4.1	All	20
Data Loss Prevention	Default	2	4.1	All	20
Firewall	Default	1	4.1	All	20
Group Settings	Default	5	4.1,3.3,3.2,3.1,3.0,2.5,...	All	20
OpenSignature Events	Default	1	4.1	All	20
Response Filters	Default	1	4.1	All	20
Rolling Packet Captur...	Default	4	4.1	All	20
Security Events	Default	1	4.1	All	20
SNMP	Default	1	4.1	All	20
Tuning Parameters	Default	2	4.1	All	20
Update Settings	Default	1	4.1	All	20
User Defined Events	Default	1	4.1	All	20
Web Application Prot...	Default	1	4.1	All	20

Version History for 'Connection Events : Default'

Version	Status	Created On	Created By
2	Archived	2010-11-18 22:02:00 GMT	jvanherzele
1	Archived	2010-06-11 13:47:18 BST	

Figure 2-19 View of a default repository showing two versions of a policy

Repositories facilitate policy management in several ways. For example, you can use repositories to create and safely modify new versions of active production policies, without directly configuring your active policies. Then after thoroughly reviewing the revised policies, you can *deploy* them to your production environment.

Policy repositories also help you in the following ways:

- The track the deployment of your policies.
- The archive previously deployed policies.
- They reapply previously deployed policies, if necessary.

2.5.3 Policy versioning

You can open and edit a policy at any time, even if the policy is deployed. Whenever you edit and save a policy, IBM Security SiteProtector saves a new version of the policy. The original policy version is unaffected by your changes. If you want to apply your changes to an agent, you must deploy the new version of the policy.

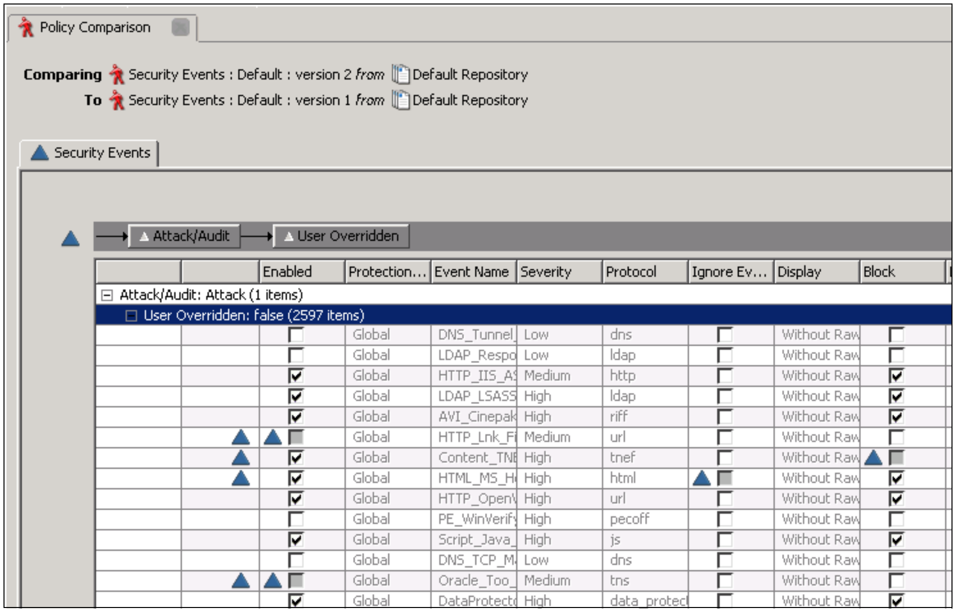
After you modify a policy in a repository, you might want to deploy the policy. IBM Security SiteProtector gives you the option to automatically deploy a policy when you save the policy, or you can deploy the policy at a later (scheduled) time.

Important: When deploying policies from a repository, you can only deploy the policies to the group associated with the repository and to its child groups.

2.5.4 Comparing policies

IBM Security SiteProtector also offers the option to run a line-by-line comparison of two policies. This feature and the policy reporting capability offer a way to quickly map the differences between policies that might contain thousands of security event signatures, each with a dozen parameters.

Figure 2-20 shows the result of such a policy comparison, where changes are marked by triangles.



Policy Comparison

Comparing Security Events : Default : version 2 *from* Default Repository
To Security Events : Default : version 1 *from* Default Repository

▲ Security Events

▲ → ▲ Attack/Audit → ▲ User Overridden

⊟ Attack/Audit: Attack (1 items)
⊟ User Overridden: false (2597 items)

		Enabled	Protection...	Event Name	Severity	Protocol	Ignore Ev...	Display	Block
		□	Global	DNS_Tunnel_	Low	dns	□	Without Raw	□
		□	Global	LDAP_Respo	Low	ldap	□	Without Raw	□
		☑	Global	HTTP_IIS_AS	Medium	http	□	Without Raw	☑
		☑	Global	LDAP_LSASS	High	ldap	□	Without Raw	☑
		☑	Global	AVI_Cinepak	High	riff	□	Without Raw	☑
	▲	▲ ▨	Global	HTTP_Lnk_Fi	Medium	url	□	Without Raw	□
	▲	☑	Global	Content_TNE	High	tnef	□	Without Raw	▲ ▨
	▲	☑	Global	HTML_MS_H	High	html	▲ ▨	Without Raw	☑
		☑	Global	HTTP_OpenV	High	url	□	Without Raw	☑
		□	Global	PE_WinVerify	High	pecoff	□	Without Raw	□
		☑	Global	Script_Java_	High	js	□	Without Raw	☑
		□	Global	DNS_TCP_M	Low	dns	□	Without Raw	□
	▲	▲ ▨	Global	Oracle_Too_	Medium	tns	□	Without Raw	□
		☑	Global	DataProtect	High	data_protect	□	Without Raw	☑

Figure 2-20 Comparison between two policy versions

2.5.5 Integrating IBM Rational AppScan data

IBM Rational AppScan can automate vulnerability testing to help protect against the threat of cyber-attack with a scanning solution that combines dynamic analysis, static JavaScript analysis, and ease of use. You can also use the scan information to mitigate risk for applications already deployed. To achieve this goal, you feed IBM Rational AppScan data to IBM Security SiteProtector.

IBM Rational AppScan can upload vulnerability data to IBM Security SiteProtector by using an extension that is available for download at no charge from IBM developerWorks® at:

http://www.ibm.com/developerworks/rational/downloads/08/appscan_siteprotectorpublish/index.html

IBM Security SiteProtector includes several analysis views that are specific to IBM Rational AppScan vulnerability data within the reporting and analysis modules. With this broader view, you get a complete understanding of your security position, so that you can better understand the risks that your organization faces and can set priorities accordingly.

2.6 Conclusion

This chapter introduced the overall IBM Security Network IPS solution. It started by explaining the base concepts of intrusion prevention and why every organization must focus effort on implementing these concepts. Then this chapter introduced the IBM Security Network IPS physical and virtual appliances, their functions, and their deployment models. This chapter also looked into the centralized management capability that IBM Security SiteProtector offers when it comes to centrally managing a hierarchical policy model for the entire network intrusion prevention deployment.

Now continue with Chapter 3, “IBM Security Network IPS architecture” on page 73, to take a closer look into the IBM Security Network IPS component architecture.

3

IBM Security Network IPS architecture

This chapter focuses on the following architectural aspects in regard to the IBM Security Network Intrusion Prevention System (IPS):

- Software components and logical design
- Hardware architecture
- Protocol Analysis Module
- High availability
- File system architecture
- Default users

3.1 Software components and logical design

The IBM Security Network IPS appliance is developed based on a modular Linux kernel architecture. The software (firmware) architecture relies on years of continuous IBM development efforts in this technology.

Along with major appliance releases, IBM made significant improvements in the appliance firmware, hardware, and user interface. This chapter focuses on the latest architecture of the IBM Security Network IPS GX7800 model. To begin, It begins by examining the high-level software components of the Linux kernel-based OS that are shown in Figure 3-1 on page 75.

The first daemon (process) that starts when the appliance boots is *issDaemon*. This process routes communication between the two types of management interfaces, the IBM Security SiteProtector and the local management interface (LMI), and the other software modules.

The issDaemon also starts the *issCSF* process, which loads the *Common Response Module* (CRM). The CRM is responsible for core configuration and response processing functionality with other internal processes, especially the *iss-secmgr* and *iss-netengine*. The responsibilities of the CRM include policy processing and notification response invocation.

The Security Manager (*iss-secmgr*) is the core component responsible for management and configuration of the appliance. The Security Manager process is started during boot time, and it manages the Adapter Manager subprocess.

The primary function of the Network Engine process (*iss-netengine*) is high performance deep packet inspection. This module handles the core of the code known as the *Protocol Analysis Module Version 2* (*PAM2*). The Network Engine process sends security (attack) events to the Security Manager, while all other events are communicated back to the CRM. For more information about PAM, see 3.3, “Protocol Analysis Module” on page 82.

The Policy Processing daemon (*issppd*) is responsible for translating policies from a user readable format into process readable configurations. The CRM sends the user readable policy to the Policy Processing daemon and receives a response that is distributed to the Security Manager, Network Engine, and other involved processes.

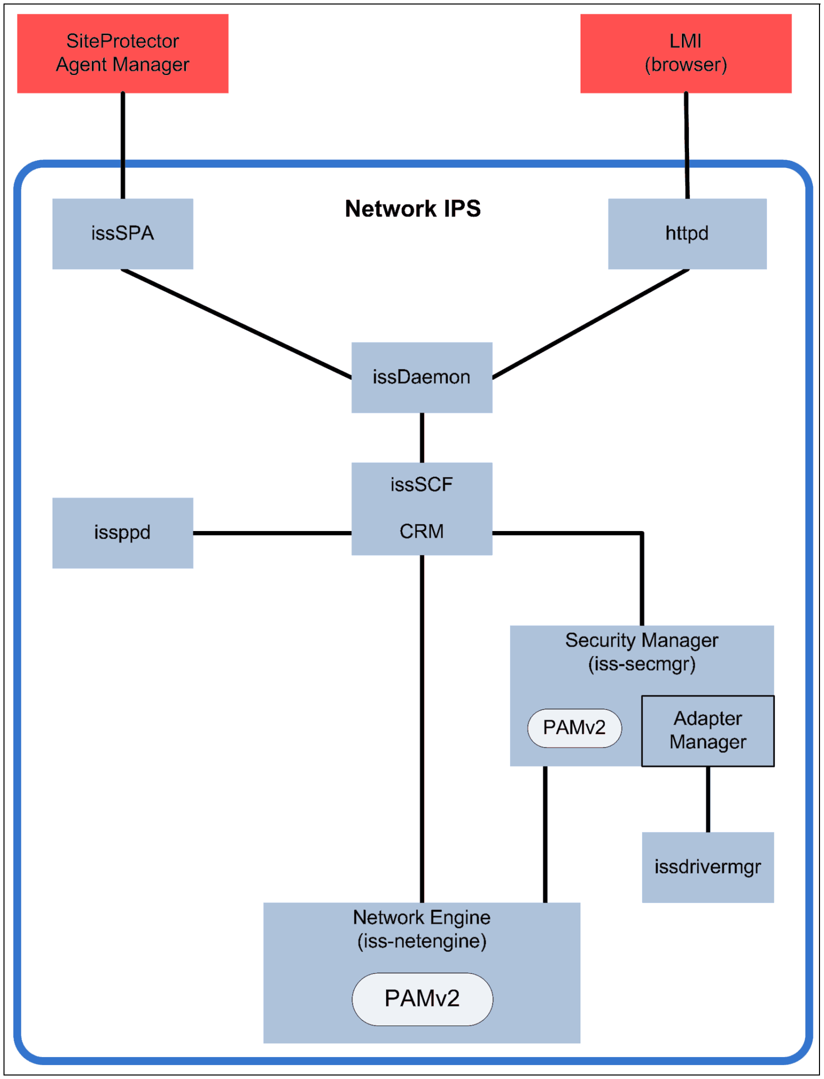


Figure 3-1 High-level software component architecture of the GX7800 model

The following sections look closely at the communication between the IBM Security Network IPS and its management interfaces. They also address the other daemons shown in Figure 3-1 and the policy process communication flow.

3.1.1 Communication between Network IPS and management interfaces

The communication between IBM Security SiteProtector and the IBM Security Network IPS appliance is handled by the SiteProtector Agent daemon called *issSPA*, which routes requests to the issDaemon. The process communicates with the SiteProtector Agent Manager component over the default TCP port 3995. The communication is always initiated by the issSPA and flows to the Agent Manager.

Figure 3-2 illustrates the communication paths between the Agent Manager and Network IPS.

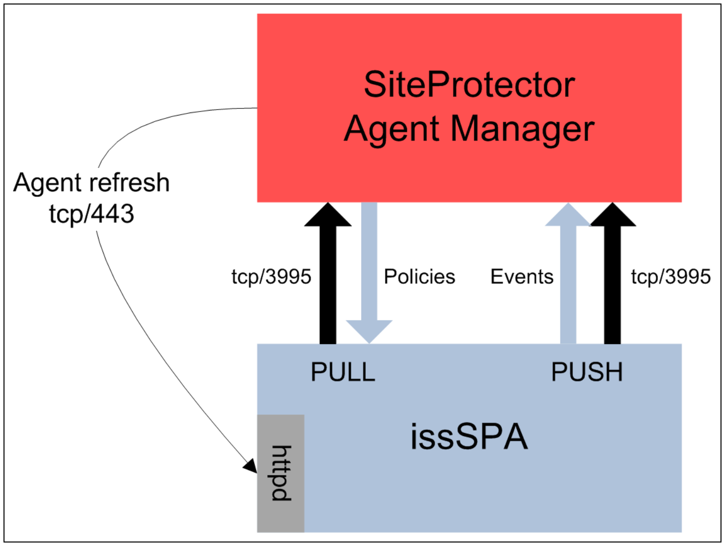


Figure 3-2 SiteProtector Agent Manager and IBM Security Network IPS communication

This communication channel carries two types of traffic:

- Event data, which is *pushed to* the Agent Manager
- Policy updates (commands), which are *pulled from* the Agent Manager

On regular intervals (known as a *heartbeat*), the issSPA checks with the Agent Manager for any policy updates. Again, the communication is *initiated by the issSPA*. The policies are pulled from IBM Security SiteProtector.

In addition, every IBM Security SiteProtector action that requires an immediate response on the agent side is implemented so that the Agent Manager sends an *agent refresh* request over https port 433 to the issSPA. Then, the issSPA connects to the Agent Manager to pull the policies.

Troubleshooting tip: For the quickest response in *troubleshooting situations*, an agent refresh can be initiated from the appliance by using the following command as root user:

```
service iss-spa doheartbeat
```

If a firewall is in place between the Agent Manager and the Security Network IPS that blocks port 443, the appliance still receives the policy update in the configured heartbeat interval (instead of immediately) initiated by the IBM Security Network IPS.

Use the root user account, for example, by using the previous command, only in troubleshooting scenarios. Refrain from using root user access in everyday activities. For more information, see 3.6.1, “Root user considerations” on page 102.

3.1.2 Policy process communication flow

Figure 3-3 on page 78 helps to better understand how policies are being used and transformed in our Network IPS architecture.

An administrator, who is granted the necessary permissions, can create new or update existing policies by using the IBM Security SiteProtector console or the LMI. In both cases, the policy is routed to the issDaemon process. The issDaemon receives the user coded policy (XML file) and routes it to the CRM. The CRM forwards the policy to the issppd process.

Next, the issppd process converts the XML file into a specific set of instructions that control the behavior of the other involved Network IPS processes to reflect the updates in policy settings dictated by the user. The instructions are sent back to the CRM, which in turn forwards them to the Security Manager (iss-secmgr), which manages the Network Engine (iss-netengine).

The command channel that is used between the CRM, the Security Manager, and the Network Engine is separate from the event or data channel. Security Events that are detected by the Network Engine are routed to the Security Manager. All other events are communicated directly to the CRM. The events are routed back to the management console by using the CRM.

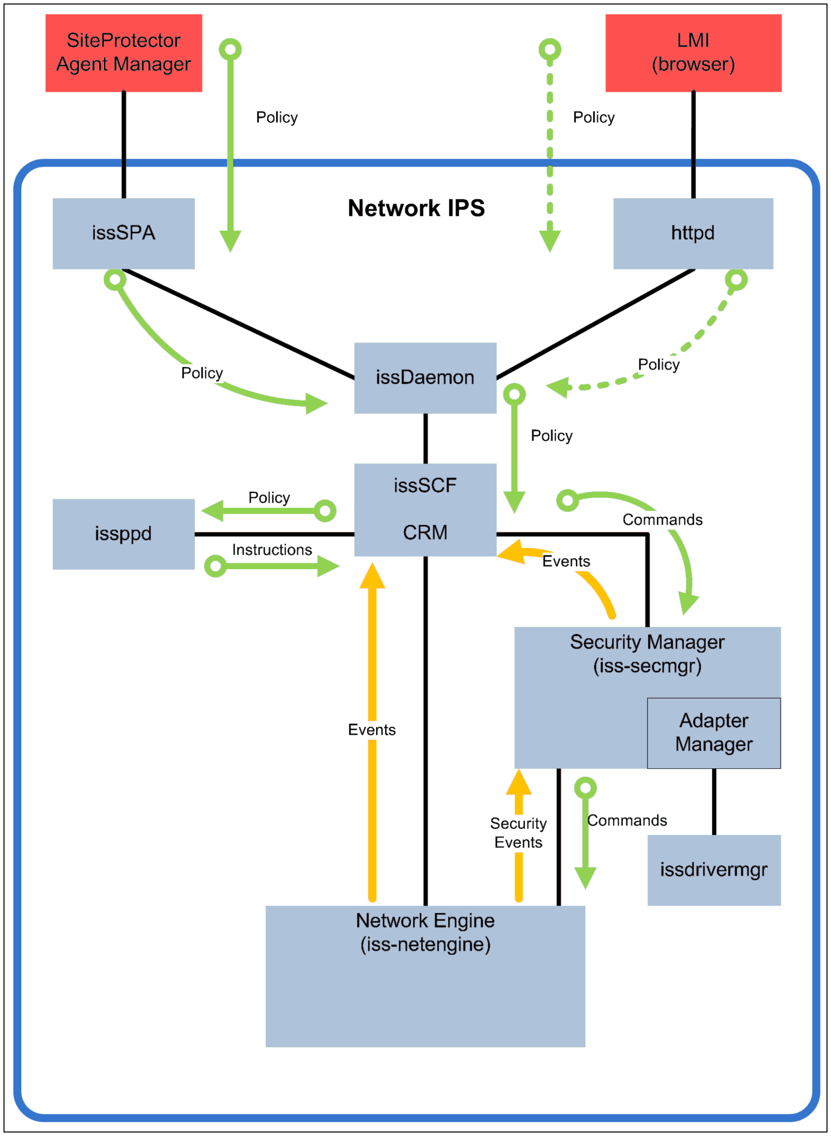


Figure 3-3 Communication flow for policy processing

The following section looks at the hardware architecture of the IBM Security Network IPS.

3.2 Hardware architecture

Figure 3-4 illustrates the hardware architecture that complements the software architecture described in 3.1, “Software components and logical design” on page 74.

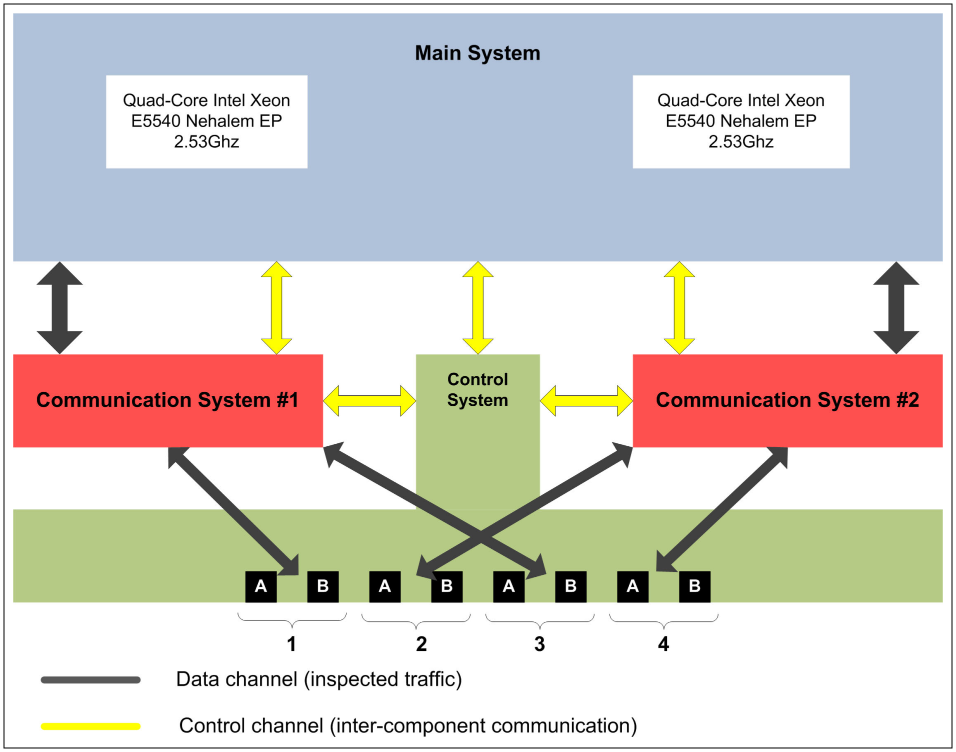


Figure 3-4 Network IPS hardware architecture (GX7800 model)

The hardware architecture has the following major components:

- Main System

  The Main System uses double Quad-Core Intel Xeon processors, which have access to 24 GB of DDR3 memory. Besides redundant hot-swappable power supplies and hot-swappable fans, the Main System uses redundant RAID-1 storage and a system health monitoring and alert system that communicates health information back to IBM Security SiteProtector. The Main System operates based on a Linux kernel and Network IPS software components described in 3.1, “Software components and logical design”.

- Communication System

  Network-related communication is handled by a separate subsystem that employs dual communication-related processors. This system handles the network traffic and routes the traffic to the Main System for deep packet inspection. The Communication System uses its own proprietary operating system and drivers.

- Control System

  The Control System uses its own processor to manage the front panel and the data ports.

The GX7800 appliance operates eight ports that provide four protection segments. Each segment can support various connectors:

- 10G SFP+; short range (SR) and long range (LR)
- 1G SFP; copper (TX), short range (SX), and long range (SLX)
- Direct-attach copper

Consider the fixed mapping between the front monitoring ports and the two individual communication systems where the odd and even port pairs (segments) are connected to opposite communication systems. This mapping will be different if the IBM Security Network IPS is configured for standard high availability mode as described in 3.4, “High availability” on page 97.

10G or 1G: It is important for the installation process to understand the port architecture, especially if you have a mixed type of network environment (10G and 1G). You must properly load balance the traffic among the communication processors and avoid routing all 10G traffic to a single communication system.

Figure 3-4 on page 79 also shows that the data path (inspected traffic) uses separate communication channels form the control path, which routes control information between the different components.

The following section examines the packet inspection process flow to help you better understand the different configuration options.

3.2.1 Packet inspection process flow

Figure 3-5 illustrates how the inspected traffic flows within the IBM Security Network IPS.

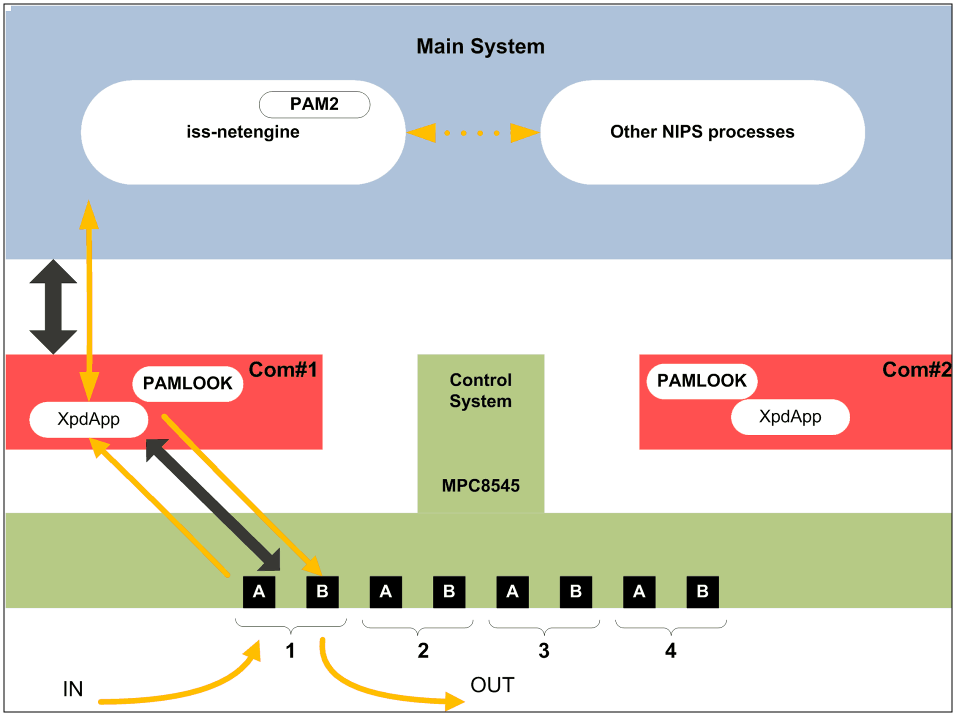


Figure 3-5 Example of inspected traffic flow

The traffic flow has the following major steps:

1. A network packet is received by the switch at the front-panel port (for example, port 1A).
2. The switch routes the packet to Com#1.
3. The packed driver application (XpdApp) of the communication system receives the packet and uses an algorithm (PAMLOOK) to decide if the packet requires deep packet inspection.

   This preinspection is vital to help preserve high network bandwidth while preserving network security in situations with high network traffic load. PAMLOOK is used to determine *if* the packet must be routed to the Network Engine (iss-netengine). If network traffic is low and the IBM Security Network IPS can consume all packets, the complete network traffic is routed to the Network Engine.

4. The XpdApp forwards the network packet to the Main System for further inspection. The transfer uses the data channel.
5. The packet is received and is placed in a queue for the Network Engine, which runs Protocol Analysis Module v2 code.
6. The Network Engine performs its deep packet inspection and communicates, if necessary, with other Network IPS software components.
7. The Network Engine returns a *forward* or *drop* decision to the XpdApp.
8. If the packet is flagged as forward, XpdApp transmits the packet back to switch.
9. The switch routes the packet to port 1B to continue its way back into the network for further regular processing.

To help you better understand the process for deep packet inspection, the following section look into the Protocol Analysis Module.

3.3 Protocol Analysis Module

The key security technology built into Network IPS device is called *IBM Security Protocol Analysis Module*. PAM is the major threat detection engine behind the preemptive protection that is available in the IBM Security Network IPS and in many IBM Security Systems products.

This book refers to Version 2 of the IBM Security PAM. PAM identifies and analyzes 170 different network protocols and 77 data file formats. These numbers are constantly growing because the IBM X-Force research team is investing more time to discover new threats and vulnerabilities and to build new detection mechanisms into the PAM code.

More information: For the latest PAM document that references the number of protocols and data formats, in addition to the features of PAM, see the PAM help file, which you can download from:

http://www.iss.net/security_center/reference/help/pam

As PAM parses the protocols and monitors the traffic, it employs various techniques to accurately detect attacks while allowing legitimate traffic to pass. X-Force security expertise includes the vulnerability modeling that is necessary to incorporate vulnerability signatures for proactive and preemptive protection rather than to use signatures for reactive protection.

PAM consists of several key security technologies, as shown in Figure 3-6:

- Virtual Patch
- Client-side Application Protection
- Web Application Protection
- Threat Detection and Prevention
- Data Security
- Application Control

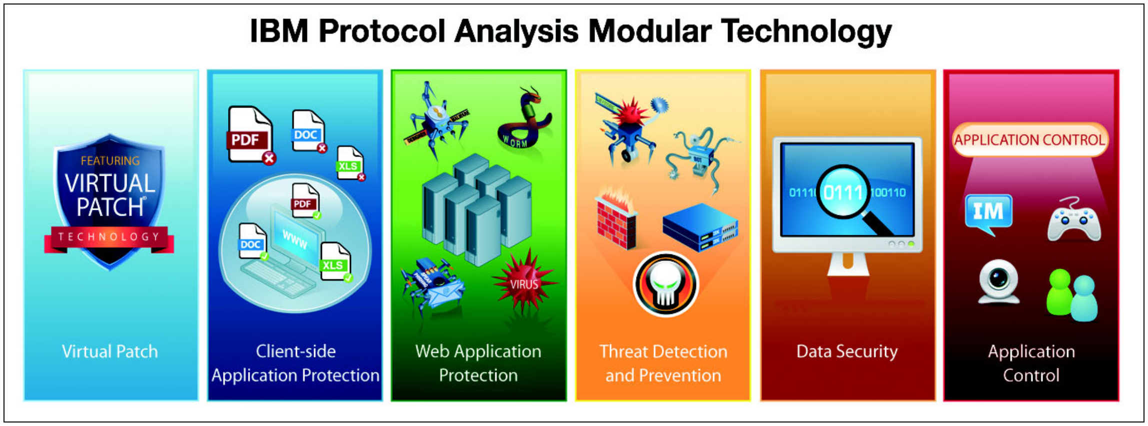


Figure 3-6 PAM technology

PAM adapts its algorithms to the network traffic and the available resources. However, in some environments, you can benefit from fine-tuning the PAM algorithms by using various advanced tuning parameters. IBM Security Systems also changes the algorithms regularly by using security content updates, through extensive use of beta programs, customer feedback, and close cooperation with Managed Security Services.

Virtual Patch

The Virtual Patch technology shields vulnerabilities on your infrastructure from exploitation independent of the software patch that is available or installed. This action enables a responsible patch management process that can be implemented without fear of a breach or causing issues with production systems.

With patches being released on a weekly or daily basis, operations personnel who maintain production systems are often faced with a dilemma: Install the patch or be susceptible to a vulnerability. With the Virtual Patch capability of PAM, the IBM Security Network IPS infrastructure can prevent any exploits while the new software patches are put through the configuration and change management cycle.

Client-side Application Protection

The Client-side Application Protection module protects users against attacks that target applications used everyday, such as Microsoft Office files, Adobe PDF files, multimedia files, and web browsers.

Web Application Protection

The Web Application Protection module protects web applications against sophisticated application-level attacks such as SQL-injection, cross-site scripting (XSS), PHP file includes, and cross-site request forgery (CSRF). This capability is implemented as part of the IBM patented *injection logic engine*. This capability expands security to meet both compliance requirements and threat evolution.

Threat Detection and Prevention

The Threat Detection and Prevention module detects and prevents entire classes of threats as opposed to a specific threat or vulnerability. This capability eliminates the need for constant signature updates. IBM Shellcode Heuristics and JavaScript Obfuscation Detection technologies are part of this capability.

Data Security

The Data Security module monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. This module helps to explore data flow through the network to determine if any potential risks exist.

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 (IM), and tunneling.

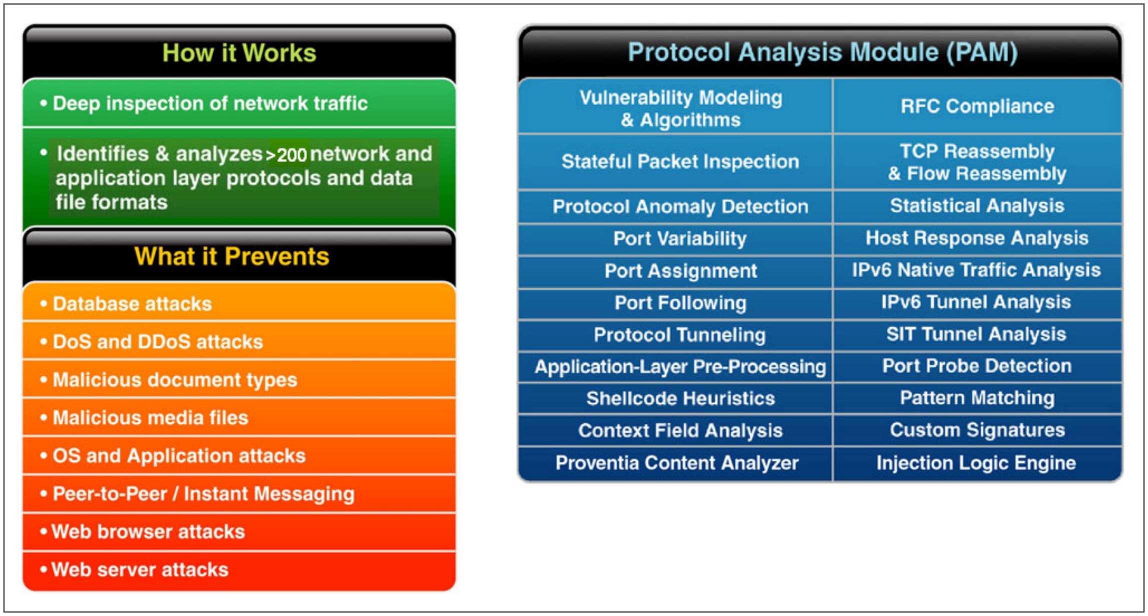
3.3.1 Protocol Analysis Module techniques

Every skilled craftsperson uses a collection of tools to deliver a quality product. Unfortunately, hackers are no different and often use collections of unique purpose-built tools so that they can gain easier access into computer systems.

Therefore, IPS devices must rely on their own diverse set of tools to combat attacks. The individual tools in a robust IPS toolkit fall into two high-level categories: *identification* and *analysis*.

The identification category consists of tools that help the IPS accurately identify the protocol encountered within the network traffic. In the analysis category, tools analyze identified protocol traffic for malicious behavior, indicating what is blocked or allowed.

The collection of tools and detection techniques used in the IBM Security Systems products are in the Protocol Analysis Module. Figure 3-7 shows how PAM works, what it prevents, and the detection techniques that are used.



How it Works

- Deep inspection of network traffic
- Identifies & analyzes >200 network and application layer protocols and data file formats

What it Prevents

- Database attacks
- DoS and DDoS attacks
- Malicious document types
- Malicious media files
- OS and Application attacks
- Peer-to-Peer / Instant Messaging
- Web browser attacks
- Web server attacks

Protocol Analysis Module (PAM)

Vulnerability Modeling & Algorithms	RFC Compliance
Stateful Packet Inspection	TCP Reassembly & Flow Reassembly
Protocol Anomaly Detection	Statistical Analysis
Port Variability	Host Response Analysis
Port Assignment	IPv6 Native Traffic Analysis
Port Following	IPv6 Tunnel Analysis
Protocol Tunneling	SIT Tunnel Analysis
Application-Layer Pre-Processing	Port Probe Detection
Shellcode Heuristics	Pattern Matching
Context Field Analysis	Custom Signatures
Proventia Content Analyzer	Injection Logic Engine

Figure 3-7 IBM Security Protocol Analysis Module

Before analysis of protocol traffic can begin, the traffic must be accurately identified. All remaining steps of traffic inspection hinge on the accuracy of this initial process. Traffic parsed incorrectly can render false positives at best and false negatives at worst. Using multiple techniques, protocols can be accurately identified with a high degree of confidence. The following sections describe the main detection techniques used in PAM.

Port assignment

Port assignment is the most elementary method of identifying application protocol types. The technique of port assignment assumes the application protocol type based on the TCP/IP port that is being used for the connection.

Port assignment can be used as a preliminary protocol identification technique. However, because protocols are not bound to particular ports, using port assignment alone poses significant problems. An IPS that assumes protocols are always bound to particular ports provides intruders with an elementary way to evade the system, possibly resulting in an unnoticed successful attack. To reduce false negatives, traffic identified by port assignment is always double-checked with another recognition technique to ensure that attacks are blocked. In fact, more modern network IPSs only use port assignments as a last method of identifying protocols types.

Heuristics

In the context of protocol identification and recognition, heuristics involve developing algorithms that are used to positively identify traffic. The algorithms are based on sets of rules that uniquely identify the protocols behavior. For example, IM applications often purposely avoid using specific ports so that they can take advantage of any ports that remain accessible through the firewall.

Heuristics are often the only method to correctly identify certain protocols. Heuristic techniques assume that unique identifiers in the traffic always exist. However, due to some protocol designs, unique traffic identifiers are not always present. The next technique, port following, is sometimes used as an additional method to accurately identify protocols and their traffic flows.

Port following

The port following technique monitors previously identified communication sessions for additional connections on random ports. Some application protocols use an initial port to control a connection. However, then they negotiate and open a random port to transfer data between the client and the server endpoints of the connection.

Protocol tunneling recognition

Protocol tunneling is the practice of *embedding* one application protocol within another protocol, which is a common occurrence in modern network communication. In some cases, hackers might use protocol tunneling to disguise their attacks. Therefore, the ability to recognize this evasion technique is critical to preemptive protection.

Traffic analysis techniques

Traffic analysis occurs after traffic is correctly identified. Further analysis beyond basic identification helps the IPS to determine the intent of the traffic and to take appropriate steps to block malicious traffic.

As with identification techniques, no single method is effective enough on its own. Therefore, an IPS with multiple analysis techniques working in tandem provides additional protection.

Protocol analysis

Protocol analysis is a popular technique used by IPS devices to stop known and unknown threats. Known threats consist of attacks and use code that is already released. Unknown threats are yet to be released and have the potential to target known and unknown vulnerabilities.

Protocol analysis can be performed on protocols down to level 2 of layer 3 of the Open Systems Interface (OSI) Model. Using protocol analysis techniques, the IPS double-checks the communication of a a connection against the generally accepted behavior for the protocol. If a network transaction does not follow the accepted behavior, the traffic is blocked, or an alert is generated, depending on the configuration of the IPS engine.

RFC compliance checking

Request for Comments (RFC) compliance checking, also commonly called *protocol validation* or *protocol anomaly detection*, triggers when network traffic does not conform to the RFC standard. This technique produces a high rate of false positives because developers are not required to adhere to the application protocols of RFC. RFC compliance checking also tends to produce many false negatives because most attacks are considered legal, according to the application protocols RFC standard. Therefore, RFC compliance checking is rarely used by itself and is most effective when combined with another technique.

TCP reassembly

Packet fragmentation, which is the splitting of one original packet of information in the network into two or more packets, is a normal networking operation due to varying transport protocols. Hackers also employ fragmentation as a method for evading elementary detection systems. Such tools as Fragroute make it easy to break malicious attack packets into smaller fragments before sending them across the network.

To handle the normal conditions that exist in a network environment, and the abnormal attempts to stop an attack, IPS devices must be able to reconnect pieces of traffic that belong together. This preprocessing is called *TCP reassembly* and is always used to analyze traffic for hidden signs of malicious intent.

Flow reassembly or simulation

Flow reassembly or simulation is similar to TCP reassembly. However, flow reassembly requires IPS to keep up with a connection in its entirety, as opposed to a packet or a portion of the data flow. Flow reassembly must analyze the connection as a whole rather than inspect individual portions of the traffic as they are encountered. Several modern threats use fragmentation techniques to avoid detection by security devices. By reconstructing the traffic flow of the connection, the IPS can identify threats that have evaded the system.

Statistical threshold analysis

Statistical threshold analysis is based on detection and blocking of network anomalies. This technique is also sometimes called *statistical anomaly* or *threshold analysis*. It usually involves monitoring the network for some time to create a *baseline* of what normal traffic patterns look like. After the baseline is established, patterns that exceed the threshold of the baseline are suppressed. Establishing baselines and using other statistical anomaly techniques can effectively stop threats that generate obvious deviations from normal traffic. Other, more subtle threats might go undetected by IPS devices relying solely on statistical threshold analysis.

Many vendors might claim that statistical analysis stops all unknown threats, but this theory is flawed due to the dynamic nature of most modern computer networks. In a dynamic environment, establishing baselines is difficult, cost-prohibitive, and limited in scalability as a stand-alone component of an IPS.

Pattern matching

Pattern matching is the most popular methods of analyzing threats, but has a reputation as one of the weakest IPS technologies. Pattern matching is also called *regular expression (regex) matching*.

In lieu of using regular expressions, some security vendors have implemented a custom pattern matching language that simulates the effect of using regular expressions. Pattern matching involves scanning network traffic as it passes through the IPS for patterns that are predefined to signal malicious behavior. Pattern matching remains a useful tool in the detection of security threats.

All IPS vendors use a form of pattern matching to some degree in their traffic analysis. The reputation of pattern matching as a weak IPS technology results from its history as the first method of detecting threats. In its infancy, pattern matching was elementary, effectively triggering on any traffic that matched the pattern of bad behavior. This basic technique is commonly referred to as *packet-grepping* or *blind pattern matching*.

The packet-grepping name is derived from the popular **grep** tool for UNIX technology-based systems, which is a utility that finds patterns in strings. Initially, pattern matching triggered a high volume of false positives, resulting in a higher cost of ownership for organizations who use IDS.

The pattern matching analysis technique has evolved. Current solutions use algorithms that trigger a match only if the pattern matches in a portion of the traffic that can result in successful vulnerability exploitation. This technique is sometimes called *stateful pattern matching*. As the name implies, the IPS signals a match only if the attack appears in the portion of traffic where an attack exists.

Today, pattern matching remains useful, but only as a tactical, reactive approach to threat mitigation.

Protocol anomaly detection

A *protocol anomaly* is a deviation from a protocol format or protocol behavior. Protocol format and behavior are defined in the various protocol definitions, many of which are on the Internet Engineering Task Force (IETF) website, under the Request for Comment (RFC) section. You can learn more about RFCs at the IETF website at:

http://www.ietf.org/rfc.html

Figure 3-8 shows the network protocols and data file formats that are recognized by PAM.

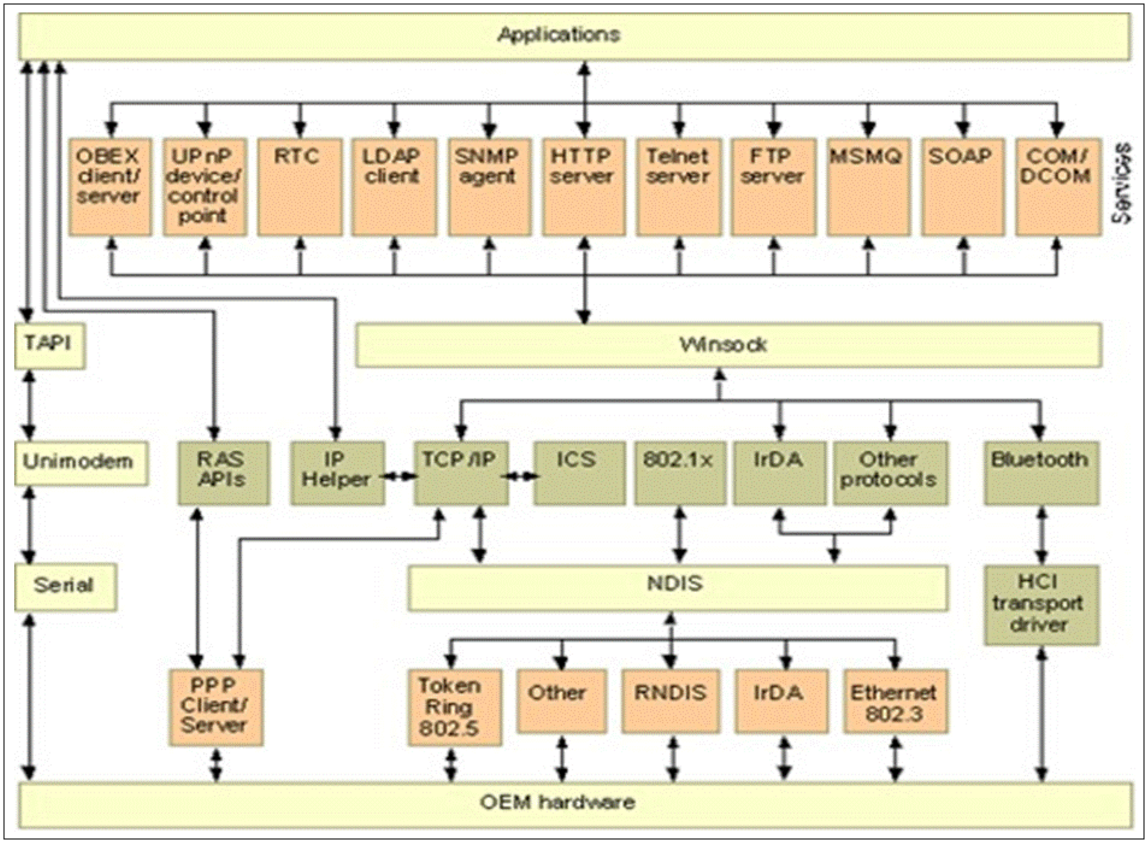


Figure 3-8 Network protocols and data file formats

3.3.2 Protocol Analysis Module example

To help you understand how a detection algorithm works inside of PAM, consider this example. Example 3-1 defines the algorithm for SQL_SSRP_StackBo.

Example 3-1 SQL_SSRP_StackBo

```
udp.dst == 1434
ssrp.type == 4
ssrp.name.length > ssrp.threshold
where ssrp.type is first-byte of packet
where ssrp.name is nul-terminated string starting at second byte
where ssrp.threshold defaults to 96
```

The signature first ensures that the destination port is UDP port 1434, which is a requirement for the SQL Server listener.

The next criteria to meet is that the SQL Server Resolution Protocol Type (`ssrp.type`) must contain the value of 4. If the `ssrp.type` is not 4, the vulnerability is not affected by this code, and we allow it to pass.

Next, we ensure that `ssrp.name.length` is greater than `ssrp.threshold`, which is set to 96 bytes. The unchecked length of this variable is the root cause of the vulnerability in the SQL Server application. Security researchers found what is required for this particular buffer overflow to occur. They can determine that the buffer is not bounds checked and that 96 bytes overflow the buffer. Therefore, if we see more than 96 bytes in the variable `ssrp.name`, we know that, 100% of the time, the SQL Server service crashes.

In effect, the PAM signature examines the network flow for the *criteria necessary to exploit the vulnerability*. You can think of this security algorithm as a patch to the bug in the actual application. The benefit of creating a security algorithm, rather than a signature, is that no variant of an attack can pass through this security algorithm. This reason is because the buffer overflow of the variable *name* (ssrp.name in our example) must exceed 96 bytes. If it exceeds this length, all variants are stopped. We have created a single method to prevent all forms of exploits to this vulnerability.

This technique might seem easy to implement on the surface, but the analysis engine has much work to do. It must understand the protocol and how the application at the destination processes these packets. Also, hackers typically use so many techniques to try to hide their attacks from threat analysis engines. PAM employs many techniques to ensure that hackers have a difficult time bypassing these types of signatures.

Let us look at a real-world example where we can contrast this technique with a traditional pattern matching signature engine. A signature attack analyzer looks for a pattern that is already seen in the world and provides a pattern to look for. In this case, a researcher notices an attack, such as Slammer, and develops a signature that matches this pattern, as shown in bold text in Example 3-2.

Example 3-2 Packet capture of an SQL Slammer attack

```
0000 04 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0010 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0020 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0030 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0040 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0050 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 ................
0060 01 DC C9 B0 42 EB 0E 01 01 01 01 01 01 01 70 AE ....B.........p.
0070 42 01 70 AE 42 90 90 90 90 90 90 90 90 68 DC C9 B.p.B........h..
0080 B0 42 B8 01 01 01 01 31 C9 B1 18 50 E2 FD 35 01 .B.....1...P..5.
0090 01 01 05 50 89 E5 51 68 2E 64 6C 6C 68 65 6C 33 ...P..Qh.dllhel3
00A0 32 68 6B 65 72 6E 51 68 6F 75 6E 74 68 69 63 6B 2hkernQhounthick
00B0 43 68 47 65 74 54 66 B9 6C 6C 51 68 33 32 2E 64 ChGetTf.llQh32.d
00C0 68 77 73 32 5F 66 B9 65 74 51 68 73 6F 63 6B 66 hws2_f.etQhsockf
00D0 B9 74 6F 51 68 73 65 6E 64 BE 18 10 AE 42 8D 45 .toQhsend....B.E
00E0 D4 50 FF 16 50 8D 45 E0 50 8D 45 F0 50 FF 16 50 .P..P.E.P.E.P..P
00F0 BE 10 10 AE 42 8B 1E 8B 03 3D 55 8B EC 51 74 05 ....B....=U..Qt.
0100 BE 1C 10 AE 42 FF 16 FF D0 31 C9 51 51 50 81 F1 ....B....1.QQP..
0110 03 01 04 9B 81 F1 01 01 01 01 51 8D 45 CC 50 8B ..........Q.E.P.
0120 45 C0 50 FF 16 6A 11 6A 02 6A 02 FF D0 50 8D 45 E.P..j.j.j...P.E
0130 C4 50 8B 45 C0 50 FF 16 89 C6 09 DB 81 F3 3C 61 .P.E.P........<a
0140 D9 FF 8B 45 B4 8D 0C 40 8D 14 88 C1 E2 04 01 C2 ...E...@........
0150 C1 E2 08 29 C2 8D 04 90 01 D8 89 45 B4 6A 10 8D ...).......E.j..
0160 45 B0 50 31 C9 51 66 81 F1 78 01 51 8D 45 03 50 E.P1.Qf..x.Q.E.P
0170 8B 45 AC 50 FF D6 EB CA                         .E.P....
```

While many public domain and proprietary engines also look for specific protocols, and the SQL Server Protocol type variable, in the end, they look for bytes that match a specific pattern. Therefore, while the signature is accurate for the SQL Slammer event, it is unable to see attacks against the same vulnerability that do not have the same pattern match. Therefore, you need many signatures to stop all threats from attacking the Microsoft MS 02-039 vulnerability.

3.3.3 IBM Shellcode Heuristics

Users have come to view `.exe`, `.cmd`, and other file types delivered by email as suspicious and have been trained not to trust such attachments. However, Microsoft Office documents and PDFs have not traditionally presented a threat to users. Malcode writers are now exploiting this trust and embedding shellcode in seemingly innocuous file types to exploit vulnerabilities in document parsing programs such as Microsoft Office and Adobe Acrobat. The mix of social engineering with profit-inspired malware makes document format attacks attractive for botnet operators, cyber criminals, and insiders targeting organizations.

IBM takes a behavioral approach to identifying and blocking the shellcode that attempts to exploit file format vulnerabilities. Historically, shellcode referred to the payload associated with an exploit, which often resulted in shell or command-prompt access. The term has retained popularity even as payloads increasingly do other actions, such as downloading malware. In essence, *shellcode* is code that exists where it does not belong, although attackers might think otherwise.

IBM Shellcode Heuristics technology works ahead of the threat

IBM Shellcode Heuristics technology affords powerful protection against zero-day threats. Attackers typically include shellcode as a payload for buffer overflow and memory corruption bugs regardless of whether the targeted vulnerability is known.

For this reason, the behavior-based approach used by IBM Security Systems can detect exploit attempts against known and zero-day vulnerabilities. The Shellcode Heuristics technology in PAM includes a list of heuristic-based decodes that detect shellcode in the most commonly used file and network protocols. All of these decodes or signatures detect payloads that are used by, but not limited to, Metasploit tools and other well-known patterns that are used to attack and exploit multiple operating systems. Such operating systems include Windows and various UNIX platforms, such as IRIX, Solaris, and SCO.

The IBM Shellcode Heuristics technology that is available in all IBM PAM-based offerings detects shellcode in the following files:

- Microsoft Office Compound Document files, such as `.doc`, `.xls`, and `.ppt`
- Microsoft .NET intermediate Language DLL files
- The SOCKS protocol stream
- JavaScript
- Adobe Portable Document (PDF) files

- Other areas, such as HTTP POST Form Data, DNS UDP Traffic, Finger requests, FTP requests, Ident Requests and Responses, IRC Requests, POP3 requests, SNTP requests, and WINS requests

Reactive security technologies, such as antivirus, are not as equipped to protect against document format attacks. The type of exploit and the use of serial variants make it especially difficult for antivirus vendors to create signatures effectively. Eventually, after enough time has passed, antivirus vendors can create specific signatures to block this form of malware, but it does nothing to prevent zero-day attacks.

X-Force developed its Shellcode Heuristics technology in early 2006 and has only needed to update it once since that time. Embedded in all IBM PAM-based solutions, IBM Shellcode Heuristics focuses on behavior. Therefore, IBM does not have to create new protection or new pattern matching schemes to detect and block threats even as attackers morph their exploits.

3.3.4 IBM Injection Logic Engine

In the X-Force 2010 mid-term report, more than half of all new vulnerabilities occur in web applications, creating one of the largest attack surfaces for cyber criminals. Attacks targeting web servers by using SQL injection and cross-site scripting are nothing new, but they continue to be creatively concealed to bypass many security products.

A pattern-matching approach to blocking SQL and shell command injection attacks is not effective. Such technologies require the development of a new signature after the vulnerability is discovered. In addition, these types of signatures can only identify attack patterns, making it easy for attackers to evade detection by using capitalization, white space, code comments, and URL encoding methods.

IBM has developed a behavioral approach to identifying and blocking injection-related attempts to exploit web application vulnerabilities. A heuristic examination of the entire data stream sent to the web server makes evasion more difficult, resulting in fewer false negatives and fewer false positives. [1]

The IBM Injection Logic Engine (ILE) affords protection against zero-day threats. The ILE helps preempt injection attacks by detecting unique patterns that are not usually seen in valid web requests. By applying scores for specific keywords and symbols and their resulting logical constructions, ILE can detect and then block SQL injection and other injection-related attacks without requiring new signature updates.

[1] Source: IBM 2010 X-Force Mid-Year Trend and Risk Report

Instead of reacting to security breaches, vulnerabilities, and new exploits after they are discovered, the ILE can instead assume an attack posture toward the web application vulnerability landscape. Through its comprehensive heuristic understanding of SQL syntactic cues, the ILE helps protect systems in the following ways:

- Evaluating and scoring parameter URL query and POST data values
- Blocking requests that exceed the scoring threshold
- Flagging particular keyword combinations to identify the type of SQL injection that is occurring

A proactive approach to web application security is atypical of many web protection solutions, which merely audit attacks and react to them. Instead, the ILE is a patent-pending algorithm that uses behavior analysis and heuristics to score and rank name-value pairs in multiple file or network protocols, including the following examples:

- SQL
- JavaScript
- Shell-command
- PHP scripts
- LDAP
- XPATH

X-Force developed the Injection Logic Engine in 2007 by using heuristic and behavior analysis that theoretically results in protecting against injection-related vulnerabilities before the exploit is developed. Since its deployment in the IBM Protocol Analysis Module, X-Force has not added an attack signature to the ILE, but it has made customer-driven improvements to the technology.

3.3.5 JavaScript obfuscation detection

According to the X-Force midyear 2010 report, IBM detected a 52% increase in obfuscated attacks during the first half of 2010 versus the same period in 2009. JavaScript obfuscation is difficult to detect and prevent. Malware authors evade detection by security products such as antivirus and intrusion prevention hardware and software by obfuscating their code.

Before looking at the definition of JavaScript obfuscation is, you must understand the meaning of term individually:

JavaScript *JavaScript* is a scripting language that is primarily used to write web browser extensions that are downloaded from websites when the browser reads a page from that site.

The extensions are then run on a user’s workstation, mobile computer, or mobile device.

Obfuscation *Obfuscation* is a technique used for the concealment of intended meaning in communication, making communication confusing, intentionally ambiguous, and more difficult to interpret.

JavaScript obfuscation is the intended concealment of the actual script code that might be run within a user’s web browser or other environment, such as PDF files. Programmers often obfuscate their code to protect intellectual property, prevent their code from being reused without permission, or compress it for performance purposes. Attackers use these same techniques to make their malicious code unreadable and, therefore, hard to detect by traditional signature-based detection engines.

One technique that security engineers use to protect their network is to block certain websites that might have malicious JavaScript code present. This technique, while still important, does not protect against legitimate sites that are compromised because of SQL injection or cross-site scripting issues.

The obfuscated code in Example 3-3 is a subsection of a malicious JavaScript program. Trying to determine what this program is doing is a challenge even for a person who is trying to parse it by hand. Traditional methods of looking for known patterns of text and characters does not work because of the multitude of permutations that can exist.

Example 3-3 Malicious obfuscated JavaScript code example from sans.org[2]

```
<script language =JavaScript>
var J=funkyon(m){return
String.fromCharCode(m^66)};eval(J(52)+J(35)+J(48)+J(98)+J(55)+J(48)+J(46)+J(1
10)+J(50)+J(35)+J(54)+J(42)+J(121)+J(55)+J(48)+J(46)+J(127)+J(96)+J(42)+J(54)
+J(54)+J(50)+J(120)+J(109)+J(109)+J(33)+J(45)+J(45)+J(46)+J(108)+J(118)+J(117
)+J(119)+J(119)+J(119)+J(108)+J(45)+J(47)+J(109)+J(115)+J(58)+J(58)+J(58)+J(5
8)+J(108)+J(39)+J(58)+J(39)+J(96)+J(121)+J(50)+J(35)+J(54)+J(42)+J(127)+J(96)
+J(1)+J(120)+J(30)+J(30)+J(32)+J(45)+J(45)+J(54)+J(108)+J(39)+J(58)+J(39)+J(9
6)+J(121)+J(54)+J(48)+J(59)+J(57)+J(52)+J(35)+J(48)+J(98)+J(35)+J(38)+J(45)+J
(127)+J(106)+J(38)+J(45)+J(33)+J(55)+J(47)+J(39)+J(44)+J(54)+J(108)+J(33)+J(4
8)+J(39)+J(35)+J(54)+J(39)+J(7)+J(46)+J(39)+J(47)+J(39)+J(44)+J(54)+J(106)+J(
96)+J(45)+J(32)+J(40)+J(39)+J(33)+J(54)+J(96)+J(107)+J(107)+J(121)+J(52)+J(35
)+J(48)+J(98)+J(38)+J(127)+J(115)+J(121)+J(35)+J(38)+J(45)+J(108)+J(49)+J(39)
+J(54)+J(3)+J(54)+J(54)+J(48)+J(43)+J(32)+J(55)+J(54)+J(39)+J(106)+J(96)+J(33
)+J(46)+J(35)+J(49)+J(49)+J(43)+J(38)+J(96)+J(110)+J(96)+J(33)+J(46)+J(49)+J(
43)+J(38)+J(120)+J(0)+J(6)+J(123)+J(116)+J(1)+J(117)+J(117)+J(116)+J(111)+J(1
```

[2] Source: SANS Technology Institute, Internet Storm Center (http://isc.sans.edu)

```
16)+J(119)+J(3)+J(113)+J(111)+J(115)+J(115)+J(6)+J(114)+J(111)+J(123)+J(122)+
J(113)+J(3)+J(111)+J(114)+J(114)+J(1)+J(114)+J(118)+J(4)+J(1)+J(112)+J(123)+J
(7)+J(113)+J(116)+J(96)+J(107)+J(121)+J(52)+J(35)+J(48)+J(98)+J(39)+J(127)+J(
115)+J(121)+J(52)+J(35)+J(48)+J(98)+J(58)+J(47)+J(46)+J(127)+J(35)+J(38)+J(45
)+J(108)+J(1)+J(48)+J(39)+J(35)+J(54)+J(39)+J(13)+J(32)+J(40)+J(39)+J(33)+J(5
4)J(107)+J(57)+J(63)+J(121)+'');
</script>
```

The IBM Protocol Analysis Module supports detection of obfuscated JavaScript attacks by using multiple techniques within its modular approach to protection. PAM skims over the input. It tokenizes sections of code that appear interesting and analyzes the structure of how these tokens are put together. In certain well-known compression functions, PAM applies knowledge of the compression scheme to distinguish items of potential interest inside. PAM can search for suspicious looking indicators inside the obfuscated code to make an intelligent determination about whether it is a threat or a legitimate program. PAM uses a scoring mechanism that can determine a level of maliciousness.

PAM is efficient in recognizing techniques because it does not attempt to completely analyze everything in the obfuscated code. Based on certain markers, PAM analyzes only small sections of the JavaScript more closely to look for possible exploits. PAM is optimized to look only at the minimal portions of the code necessary to make a determination in an attempt to not sacrifice performance of the network or the application.

PAM uses its Shellcode Heuristics technology to detect shellcode within JavaScript. The PAM threat detection and prevention module uses technology to prevent an attack from reaching a vulnerable target. This module also blocks many types of back doors and rootkits from installing or communicating over the network. Because PAM works at the vulnerability level, this technique works regardless of whether the JavaScript code is obfuscated.

In most cases where there is obfuscated JavaScript, the coverage of JavaScript exploits is exploit specific or obfuscation specific and not vulnerability specific. When there is not any JavaScript obfuscation, the coverage skews more toward vulnerability detection. The Virtual Patch technology built into PAM provides protection against zero-day vulnerabilities that the obfuscated JavaScript might try to exploit. These techniques together provide a comprehensive solution to preventing JavaScript obfuscation from affecting the enterprise.

The next section continues to highlight the IBM Security Network IPS management interfaces.

3.3.6 PAM 2.0

With the latest GX7000 hardware, IBM introduces a new 64-bit PAM 2.0 that uses new 64-bit hardware to create multiple threads of PAM for more parallel and more efficient packet analysis. It is important to understand that PAM 2.0 does not introduce multiple instances of the PAM module. It operates as a single instance that can monitor separate network threads and connections in parallel.

3.4 High availability

As mentioned in Chapter 2, “Introducing the IBM Security Network IPS solution” on page 35, the IBM Security Network IPS supports the following high availability modes:

- Standard high availability (HA)
  - Active/active mode
  - Active/passive mode
- Geographically dispersed HA (geographical HA)

High availability modes can be configured for one pair of appliances. More devices are not supported for HA configuration.

Different models and firmware versions of the IBM Security Network IPS support different high availability modes. Geographically dispersed high availability mode is supported in all models (including virtual GV appliance) that run firmware 4.1 and later.

However, standard HA is available only for GX5000, GX6000, and GX7000 appliances on firmware 4.1 and later.

> **Important**: You cannot mix models in an HA environment. For example, you cannot configure an HA setup for a GX5208 and a GX7412 appliance.

Based on the high availability mode that has been selected, the supported security features and the cabling requirements are changing. For example, in HA mode, you cannot define protection domains based on interfaces, and passive monitoring mode is not supported in HA mode.

In addition, each high availability mode has an impact on the cost and security of the overall solution. The following sections examine the individual HA modes.

3.4.1 Standard HA: Active/active configuration

In standard HA *active/active mode*, both Network IPS appliances are inspecting live traffic at the same time. As a result, *asymmetrically routed traffic is supported* in this configuration, as long as the traffic passing through the monitoring interfaces is *mirrored* to the second Network IPS appliance in the HA cluster. Therefore, this solution is the most secure because both appliances inspect all traffic.

Figure 3-9 shows two GX7800 appliances configured for standard active/active HA where both appliances are configured to monitor two network segments (1 and 3). Segments 2 and 4 are used to mirror the traffic from one appliance to the other.

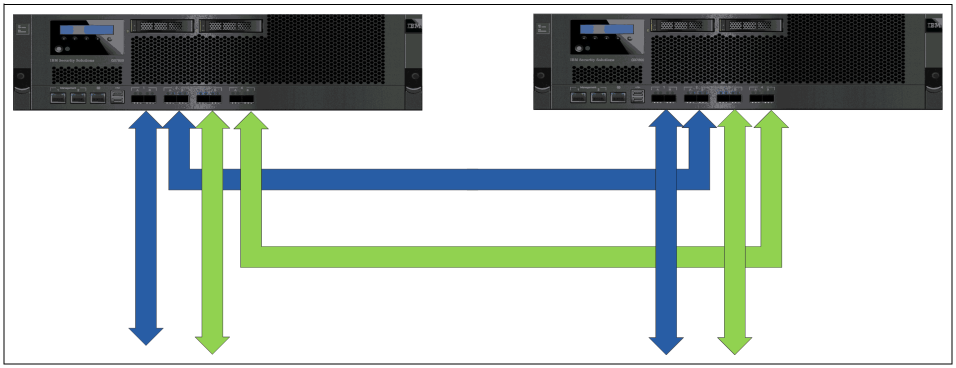


Figure 3-9 Active/active standard HA for GX7800 with two protection segments

Port mapping in HA mode: The port configuration shown in Figure 3-9 is opposite from the recommendation in 3.2, "Hardware architecture" on page 79, because Network IPS behavior is different if configured in HA mode.

In active/active mode, the PAM on both appliances is active, monitoring and blocking traffic as needed. Both network IPSs report events to the central Site Protector by using unique IDs (IP addresses). Thus, it is important that traffic is mirrored between appliances to allow the PAMs to effectively detect attacks.

Mirrored ports: Appliances process, but do not block or report, events that are generated by traffic that arrive on mirrored ports. The blocking happens for traffic generated at the inline ports.

3.4.2 Standard HA: Active/passive configuration

Network traffic flows on the primary (active) network segment, and the devices in that segment handle all of the network traffic. If one of these devices fails, the network traffic fails over to the secondary (passive) network segment, and the secondary devices take over all the traffic. The network IPSs rely on routing and switching equipment to determine when to fail over and to orchestrate failover to a secondary (passive) network segment.

In this scenario, both PAM engines are active and can analyze the traffic. However, the secondary PAM does not provide blocking until failover occurs, because there is no traffic over the passive link.

It is important to mirror the traffic, so that the secondary Network IPS can detect an attack in case the primary appliance fails during an attack.

3.4.3 Geographical HA

Where standard HA requires the use of dedicated mirroring ports on each Network IPS, geographical HA uses the IBM Security Network IPS management interfaces to exchange the information needed for the HA cluster to operate correctly.

Geographical HA has the following characteristics:

- It does not support asymmetric traffic.
- It does not mirror the complete traffic. It exchanges Dynamic Blocking Tables by using the IBM Security Network IPS management interfaces.
- It exchanges quarantine information between the active and standby devices.
- It does not support network address translation (NAT) between the geographically separated devices.

Due to its design, geographical HA is less secure overall. However, this configuration provides advantages over standard HA in certain situations:

- The data exchange can take place over a routed network. All communication between the partner appliances is encrypted. You need certificates to enable communications.
- The solution can help manage two remote data centers that mirror the entire operations.
- The monitoring ports are not used up as mirroring ports.
- The solution can help manage additional network segments without the need to purchase additional appliances.

3.5 File system architecture

As mentioned earlier, the IBM Security Network IPS is a Linux kernel-based appliance. This section provides a rudimentary overview of the file system and highlights some of the key files and directories.

> **Limitations:** Access and manipulation of the files and processes on the appliance using root user access and Linux commands are unsupported and are strictly limited for *troubleshooting and support* purposes.

For everyday activities, all appliance management tasks must be managed by using IBM Security SiteProtector, the browser-based LMI, or both.

The following directories are important to understand:

/boot Contains the current boot images.

/etc Contains standard Linux configuration files and multiple Network IPS configuration files for different types of processes (for example iss-spa, iss-netengine, and issCRM).

/bin and **/sbin** Standard system binary directories. All Network IPS process binary files are in these two directory paths.

/var/www Contains configuration files and web pages for the LMI application.

/restore Contains factory (unconfigured) images and the image created by performing a backup of the current configuration.

/var/spool/updates Use to manually store updates on the appliance. This path is used in troubleshooting and supports scenarios where an appliance does not have access to the Internet.

/cache Contains various log files that are necessary for troubleshooting the appliance. However, these files are accessible through the LMI. By using LMI, these files can also be downloaded to a local workstation for further detailed analysis.

/var/iss A symbolic link to `/cache/iss` where most log files for troubleshooting purposes are located.

3.6 Default users

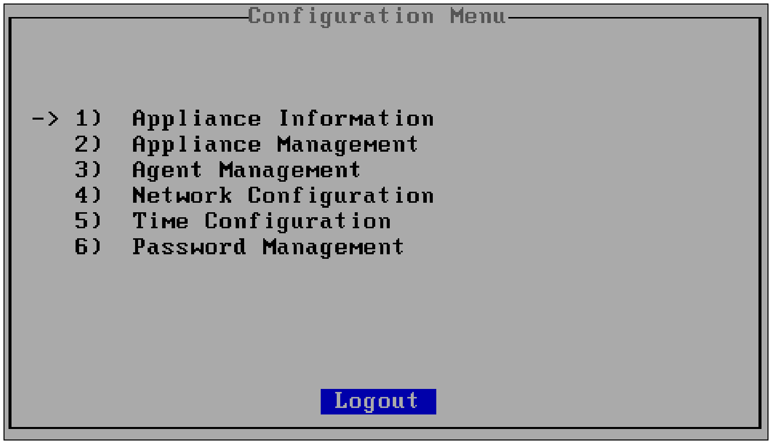
The IBM Security Network IPS can be managed by using multiple interfaces:

- IPS Setup wizard by using terminal access to an appliance or over a Secure Shell (SSH) connection
- LMI by using a remote web browser-based connection
- IBM Security SiteProtector management console by using a remote SiteProtector connection

The default user ID that is used for running the IPS Setup wizard (SSH console access) and the LMI is *admin*.

After the user logs in to the appliance by using the admin account, the shell automatically prompts the user for the default IPS Setup wizard panel (Figure 3-10).

Recording your initial admin password: If the appliance is configured to use the LCD panel-based setup process after the first boot, the randomly generated password is displayed on the LCD panel after the setup is completed. If you turn off or reboot the appliance without recording the password, access to the management interface is impossible. The only way to recover from this situation is to reimage the appliance to the factory default.



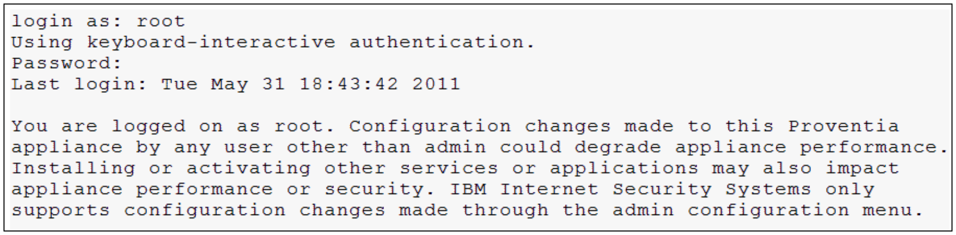
```
                    Configuration Menu

-> 1)  Appliance Information
   2)  Appliance Management
   3)  Agent Management
   4)  Network Configuration
   5)  Time Configuration
   6)  Password Management

                         Logout
```

Figure 3-10 IPS Setup wizard

If users are accessing the IBM Security Network IPS by using the IBM Security SiteProtector console, account management (access level and password) is done by using the *Users Management* console menu in IBM Security SiteProtector.

3.6.1 Root user considerations

Even though the appliance provides valid root user credentials, the usage of this account must be restricted from everyday administration activities because it is not supported to manage the device. This fact is emphasized in the login SSH banner shown in Figure 3-11. The purpose of the root account is to help in troubleshooting situations and in rare situations where administration is not possible by using the regular management interfaces.



```
login as: root
Using keyboard-interactive authentication.
Password:
Last login: Tue May 31 18:43:42 2011

You are logged on as root. Configuration changes made to this Proventia
appliance by any user other than admin could degrade appliance performance.
Installing or activating other services or applications may also impact
appliance performance or security. IBM Internet Security Systems only
supports configuration changes made through the admin configuration menu.
```

Figure 3-11 Login prompt for root user

3.7 Conclusion

This chapter focused on the various aspects of the IBM Security Network IPS architecture. It provided an overview of the key software and hardware components of the IBM Security Network IPS. It also addressed file system organization, appliance management tools, and user accounts and their usage. Chapter 4, “IBM Security Network IPS solution design and management” on page 103, focuses on deployment considerations and explains how to properly deploy the appliance in real-life environments.

4

IBM Security Network IPS solution design and management

This chapter highlights some of the important aspects involved when designing an IBM Security Network Intrusion Prevention System (IPS) solution. These aspects include determining in which strategic network locations the appliances can best be deployed and how to select the right hardware models based on a scaling exercise. They also include assessing the impact of the preferred high availability (HA) solution and selecting the preferred way for the network IPS to behave when it encounters a threat.

This chapter explains how an organization can use the IBM Security X-Force recommended policies as a base for their own customized policies. It also explains how you can use a single IBM Security Network IPS appliance to protect multiple network segments that might all have separate protection needs.

This chapter concludes by providing a possible methodology that you can use when dealing with fine-tuning intrusion prevention policies and when scheduling updates. It briefly touches on some of the most important policy elements that you can use to map the behavior of the IBM Security Network IPS to different network environments.

This chapter includes the following sections:

- Deployment locations
- Scaling considerations
- High availability and external bypass options
- Setup, licensing, and updating before deployment
- Tuning the policy before moving to blocking mode
- Conclusion

4.1 Deployment locations

For threat and vulnerability management, organizations need a proactive approach as explained in 2.1, “Intrusion prevention” on page 36. This section also explained how one of the key aspects of this process is preventing intrusions from occurring.

4.1.1 Concept of network zones

To illustrate how a network IPS fits within the broader spectrum of network security, this section looks at a network model for IT deployment architectures. It introduces different *network zones* to allow the placement of IT components according to their risk and security classifications.

By using a natural language, you can classify these zones (shown in Figure 4-1 on page 105) as *uncontrolled*, *controlled*, *restricted*, *secured*, and *external controlled*. A client (for example, an application, a human being, or another intelligent system) uses the network to access information hosted within your network. This client can come from within your organization or from an external source.

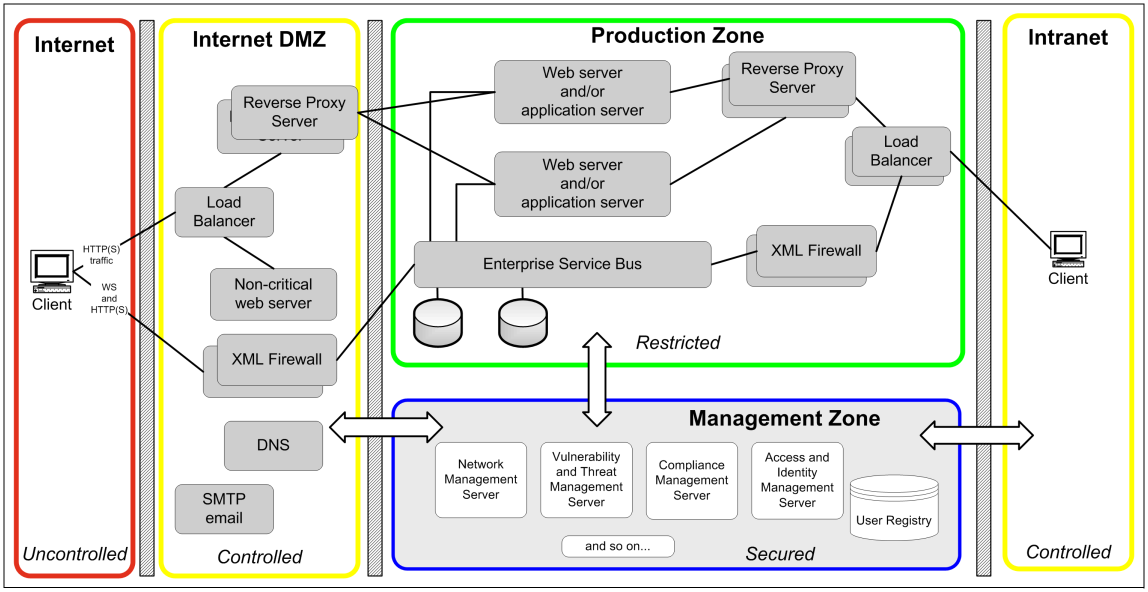


Figure 4-1 Network zones used within an organization

The organization diagram in Figure 4-1 has the following domain categories:

Uncontrolled Refers to anything outside the control of an organization. Access from the uncontrolled environment to systems in the controlled zone can be through a large number of channels.

Controlled Restricts access between uncontrolled and restricted zones (for example, a traditional demilitarized zone (DMZ)).

Restricted Access is restricted and controlled. Only authorized individuals gain entrance, and no direct communication is made with external sources (Internet).

Secured Access is available only to a small group of highly trusted users. Access to one secured area does not give access to another.

External controlled An external zone in which data is stored by business partners who are external to the systems within an organization. In this zone, which is not shown in Figure 4-1, there is limited trust in the protection of data (for example, credit reporting agencies, banks, and government agencies). An external zone typically connects to an organization like any other system in the Internet using, for example, VPN technology.

By designing your IT environment in this manner, internal users can see out, but external users cannot see anything inside your premises. Access to external users is restricted. Constructing security domains this way has the following benefits:

- They are clear and efficient.
- They are easy to explain.
- They are easy to work with.
- They provide a complete design and implementation view, so that you can avoid errors.
- Fewer errors mean a lower risk of exposure and loss.
- Each network deployment model can use any number of network zones.

In addition to security assurance, a proper risk management strategy plays a big part in designing a secure solution. If you assess the risks for your systems, you must also ensure that you assign countermeasures for those risks providing assurance for the correctness and effectiveness of the security solution.

4.1.2 Selecting network segments for inspection

Chapter 6, “Phase 1: Design and implementation of IBM Security Network IPS” on page 161, shows the development of a realistic design and implementation approach to address the security requirements of a fictional organization. It explains how you can use the IBM Security Blueprint to map the functional requirements of the organization.

For example, an organization can have a functional need to protect their sensitive data against information leakage due to intrusions and zero-day attacks. It might have a need to protect critical infrastructure servers with additional layers of protection. In addition, compliance requirements can be a driving force behind the decision to deploy network IPSs.

The decision can be made to deploy policy enforcement points (PEP) and policy decision points (PDP) for intrusion prevention on all network segments, but often a selection must be made. A risk analysis will be performed to determine where the risks are too high to accept and where IPSs must be deployed.

The following elements can help influence this type of deployment location selection:

- Determining where in the network sensitive data is stored and is it vital to deploy a Data Loss Prevention solution
- Listing critical systems that are not easily patched that need additional layers of protection, such as the X-Force Virtual Patch
- Identifying web applications that need more fine-grained inspection for exploit attempts
- Checking which network zones are most likely to be compromised and ensuring that malware cannot easily propagate but is contained within that zone

Based on these types of elements, a subset of network segments can be identified where deploying a network IPS is warranted. For example, this subset can include a network segment that links the Internet Zone to the Internet DMZ Zone. Alternatively it might include a network segment that segregates the databases from the rest of the Production Zone.

Network IPS also within internal networks: If you use a network IPS between the intranet and the Production Zone, a threat can be contained in the zone that it initially affected. Therefore, if a worm infects systems in the intranet, the Production Zone is not affected because the worm cannot pass through the network IPS. This deployment approach also provides the added benefit of requiring far fewer policy rules to manage.

4.1.3 Inside or outside the network address translation environment

Because a network IPS is often deployed in combination with a firewall, it is prudent to consider the impact of *network address translation* (NAT) when deploying a network IPS. More specifically, the question often arises whether it is best to put the network IPS before or after the firewall or NAT device.

Figure 4-2 illustrates how a network IPS is deployed *outside* the NAT environment. This type of deployment, while capable of stopping malicious packets, can complicate log analysis and policy fine-tuning.

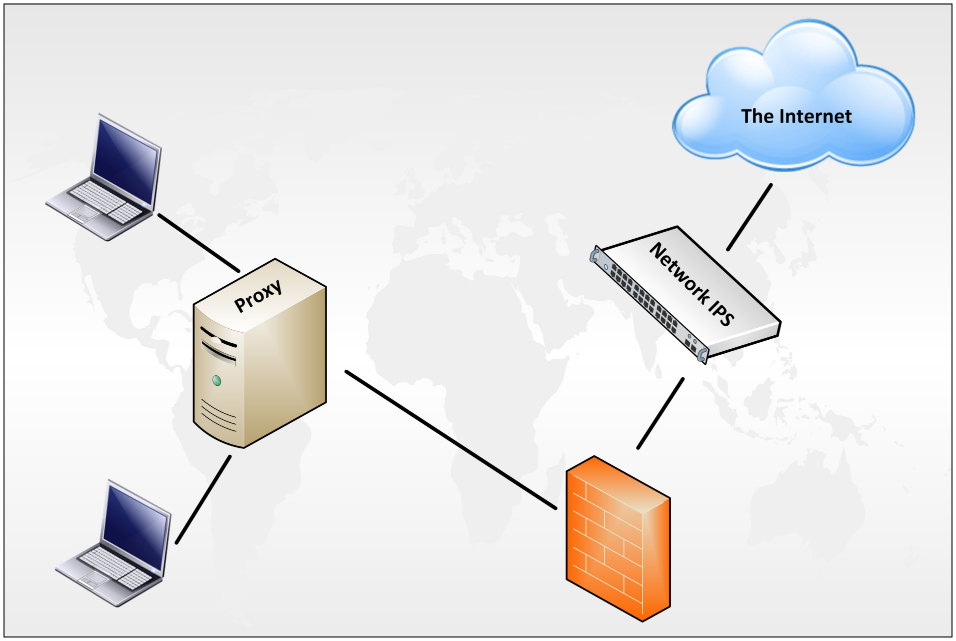


Figure 4-2 A network IPS deployed outside or behind the firewall or NAT device

When the IBM Security Network IPS detects a possible threat to the machine of an internal user connecting to a malicious website, it generates an alert that contains various details about the attack it stopped. This alert includes the IP addresses of both the victim and attacker.

With the IBM Security Network IPS deployed *outside* the NAT environment of the organization, the IBM Security Network IPS reports the public IP address of the web server that is hosting the malicious content and the public IP address behind which the proxy server of the organization is network address translated by the firewall. This report can complicate matters when it comes to analysis. To determine which specific client was under attack, the firewall, proxy server logs, or both must be checked to see which host inside the organization made the request.

Taking this scenario one step further, we can include the commonly used proxy servers for this type of traffic. By placing the network IPS behind the proxy server (from the client perspective), a condition is created where the proxy logs must be analyzed for each alert that is generated. The reason is that a network IPS does not necessarily log information about the client for which the traffic was forwarded by the proxy server. The packets that traverse the IBM Security Network IPS show the IP address of the proxy server.

Even if we leave the concept of a proxy server out of the equation, in this scenario the IBM Security Network IPS only displays the NAT IP addresses and not the private IP address of the internal machine.

We can compare this scenario to one where the IBM Security Network IPS appliance is deployed *inside* the NAT environment. For most situations, this deployment option, where the IBM Security Network IPS is kept in the NAT environment as shown in Figure 4-3, is the best choice.

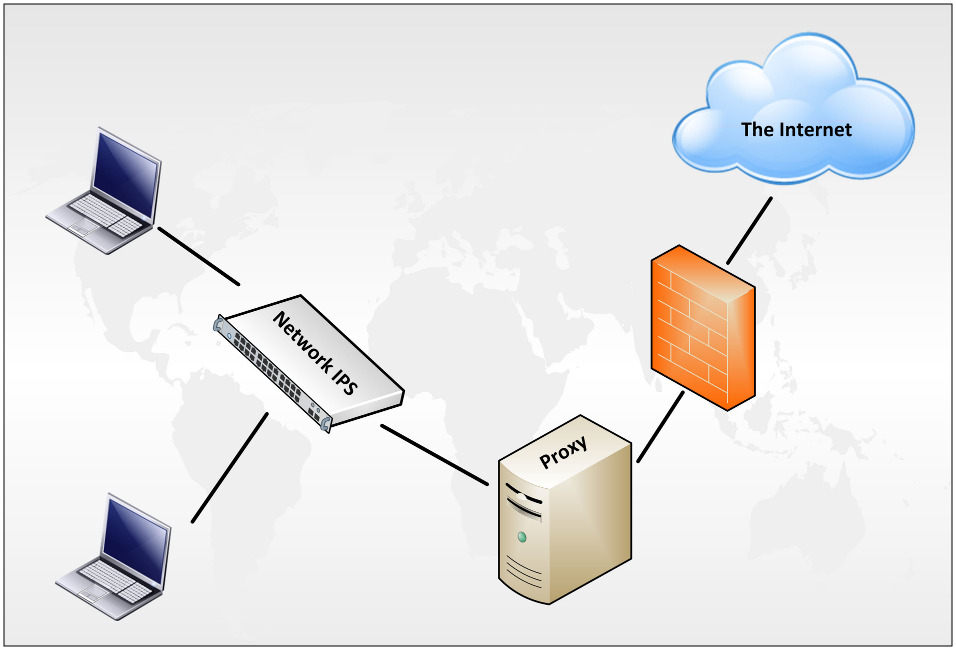


Figure 4-3 A network IPS deployed inside or before the firewall or NAT device

By deploying the network IPS *inside* the NAT environment, all the events are reported with actual client IP addresses of the machines that are facing threats from the Internet.

Additionally, with this type of deployment, an organization can define more specific custom blocking or exception rules. When you create a custom filter or exception (as explained in 4.5.3, “Tuning options” on page 127), you can instruct the IBM Security Network IPS to apply only that rule when a specific client IP is involved. This method is not possible with the previous deployment option shown in Figure 4-2 on page 108. In that scenario, the IBM Security Network IPS always sees the NAT public IP address of the proxy server regardless of the client from which the request originated.

4.2 Scaling considerations

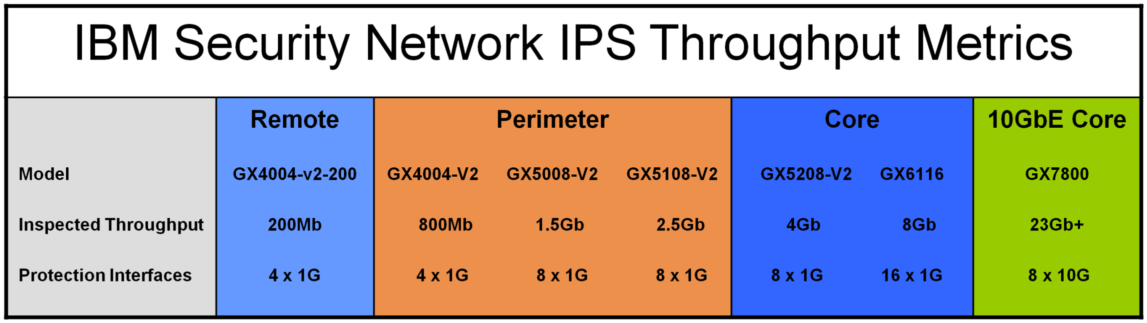
After the locations are determined for installing an IBM Security Network IPS appliance and the network segments that need to be inspected for malicious or anomalous activity are identified, the organization must perform a scaling exercise. This exercise determines the number of IBM Security Network IPS appliances that are needed and the amount of traffic that the solution can inspect.

The following important factors determine the outcome of this scaling exercise:

- The number of segments to protect
- The amount of network bandwidth the traffic consumes
- The type of physical interfaces that are needed (copper, fiber, 1G, 10G)

A first determining factor is the *number of segments* that need to be inspected. Various models of IBM Security Network IPS appliances have a different number of protection or monitoring interfaces, varying in the range 4 – 16 interfaces per device. When an IBM Security Network IPS appliance is run in inline mode, you need two interfaces for each inspected segment. This approach is the default way of operating an IBM Security Network IPS device. When the device is running in passive mode, the cabling is different, and only one interface is needed for each monitored switch.

Figure 4-4 shows the number of protection interfaces listed for each hardware model.



IBM Security Network IPS Throughput Metrics

	Remote	Perimeter			Core		10GbE Core
Model	GX4004-v2-200	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116	GX7800
Inspected Throughput	200Mb	800Mb	1.5Gb	2.5Gb	4Gb	8Gb	23Gb+
Protection Interfaces	4 x 1G	4 x 1G	8 x 1G	8 x 1G	8 x 1G	16 x 1G	8 x 10G

Figure 4-4 IBM Security Network IPS throughput metrics for 2011

Virtual appliances: Unlike the physical appliances, the IBM Security Network IPS Virtual Appliance only has *two* monitoring (sensor) ports.

A second factor that determines the type and number of IBM Security Network IPS equipment that is needed is the amount of bandwidth of network traffic that must be inspected for intrusions. The overview in Figure 4-4 shows the maximum amount of inspected throughput for each device. These values are measured by using industry standard types of mixed traffic, which give a good indication of what most network administrators can expect.

The combined raw network throughput of the interfaces on IBM Security Network IPS appliances is generally higher than the amount of traffic that they can fully inspect. When more network traffic is sent through an IBM Security Network IPS appliance than it is specified to inspect, by default, the excess amount of data is intelligently allowed to traverse the IPS uninspected.

In this case, the IBM Security Network IPS looks at the first part of a communication stream. If it finds no intrusions, it forwards the remainder of the traffic stream without processing it, or rather it fails open to traffic. When traffic levels return to normal, the agent resumes normal operation. This method guarantees that even during peak-moments, the IBM Security Network IPS does not interrupt the network flow or cause additional latency in the network.

This behavior can be changed through configuration of the IBM Security Network IPS at the interface level. For network segments where security is more important than availability, the IBM Security Network IPS can be instructed to not allow any traffic to pass uninspected. When the appliance is configured to behave this way, an excess amount of traffic (more than it can inspect) results in the IBM Security Network IPS blocking some of the traffic without processing it, or rather, it fails closed to traffic. When traffic levels return to normal, the agent returns to normal operation.

Unanalyzed packets: The IBM Security Network IPS generates logging alerts when it encounters unanalyzed packets due to a surplus in network traffic.

A final element that can help determine which IBM Security Network IPS models to select is the type of interface that is required. The entry-level models, such as the GX4004, support Gigabit Ethernet interfaces. Higher-end models allow the choice between copper or fiber connectivity. The GX7800 model supports 10G SPF+ (SR, LR) modules.

An accurate decision can be made on the types of IBM Security Network IPS that are best suited for the solution design of the organization based on the following information:

- The number of interfaces needed to inspect network segments
- The amount of network traffic that needs to be inspected
- The physical interface connections desired

4.3 High availability and external bypass options

HA is a standard non-functional, or operational, requirement in many deployment scenarios. HA is also often mixed, and sometimes confused, with load balancing. *High availability* can be defined as a network design approach that accommodates the ability of a system to overcome hardware and software failure. *Load balancing* is a network design that distributes the workload evenly across two or more resources to achieve some of the following goals:

- Get optimal resource utilization.
- Maximize throughput.
- Minimize response time.
- Avoid overload.
- Reduce the cost of not using the secondary appliance in a HA cluster.

You might say that load balancing increases reliability through system redundancy.

Depending on the availability requirements and the architectural model selected to accomplish HA within an organization, there can be an impact on the IBM Security Network IPS solution that will be designed. The supported security features and the cabling requirements differ, for example, based on the type of high availability model that was selected as explained in 3.4, “High availability” on page 97.

4.3.1 General considerations for HA deployment

When deploying IBM Security Network IPS appliances in HA environments, keep in mind the following important elements among others:

- Port mirroring

  In an HA setup, both appliances process packets that are received from all redundant segments, but they only need to block attack traffic that arrives on their inline ports when appropriate. Both appliances report events to the management console at all times. However, responses are processed only for events that are generated by packets that arrive on inline ports. Appliances process, but do not block or report, events that are generated by traffic that arrive on mirroring ports. Because both appliances see all the traffic at all times, the failover time for response processing is eliminated. Both appliances maintain a current state. Therefore, if one HA network segment fails, the other appliance receives all the packets on its inline ports, resulting in events generating as soon as the network fails over.

- Supported operations modes

  In an HA configuration, the appliance can operate in only inline simulation or inline protection modes:

  - Passive monitoring mode does not need to be supported because a passive configuration is not an inline deployment. Adapter-level operation modes supported in normal mode are not supported in an HA configuration.
  - If HA simulation mode is selected, all monitoring adapters are placed in inline simulation mode automatically.
  - If HA protection mode is selected, all monitoring adapters are placed in inline protection mode automatically. In normal mode, each adapter can be configured to run in a different operational mode.

- Using port mirroring for standard HA

  Port mirroring provides the fully secured HA solution, because the Protocol Analysis Module (PAM) needs to view all the data to make a decision about whether traffic is malicious. If a failover scenario occurs, the IBM Security Network IPS that remains functioning in the network fabric contains all the data necessary to prevent attacks.

- Not using port mirroring for standard HA

  - Less cabling is needed, and the appliances can be separated over a longer geographical distance.
  - The solution is acceptable solution if there is no asymmetric traffic.
  - It might be considered for active/passive HA, because the attack might be missed only during the failover transition process, which is unlikely.

- Active/passive traffic converging

  - It might drop some Transmission Control Protocol (TCP) packets while network protocols converge.
  - It might drop some User Datagram Protocol (UDP) packets while network protocols converge.

VoIP information: A Voice over Internet Protocol (VoIP) environment might have some loss of voice quality while the network protocols converge and when UDP packets are dropped.

- IBM Security Network Active Bypass unit

  The IBM Security Network Active Bypass unit is another option for configuring HA. Do not use this method in any Network IPS HA mode. However, you can use it on passive (backup) links of an active/passive configuration because it can protect against dual failures.

- Licensing considerations

  Licensing for an HA configuration is identical to licensing for a non-HA appliance. Each individual appliance requests a single license from IBM Security SiteProtector (if you are using IBM Security SiteProtector to manage the appliance).

- Configuration limitations

  In HA mode, you cannot use adapter parameters as part of the firewall rules, and you cannot define protection domains. Because the same traffic can flow on different adapters in an HA environment, using adapter parameters can cause the two HA partner appliances to become out of sync.

- Synchronization

  - You cannot mix different hardware models in a single HA environment. For example, you cannot use a GX5208 appliance and a GX7412 appliance as an HA pair.
  - Ensure that the firmware level and X-Press Update (XPU) level on appliances in an HA pair match.
  - Manage appliances in an HA pair in the same IBM Security SiteProtector group so that you can easily apply the same policies to both appliances.

4.3.2 Asymmetrically routed traffic

By having the IBM Security Network IPS HA configuration mirror the inspected traffic between both appliances, the PAM engines on both appliances can view the complete protocol and recognize any attack. Attacks can be missed if the traffic is not mirrored (fully visible on the both appliances) in the following two cases:

- Traffic flows in a loop. Therefore, initiated traffic goes over one route and a response returns using an alternate route. Figure 4-5 illustrates this type of attack.

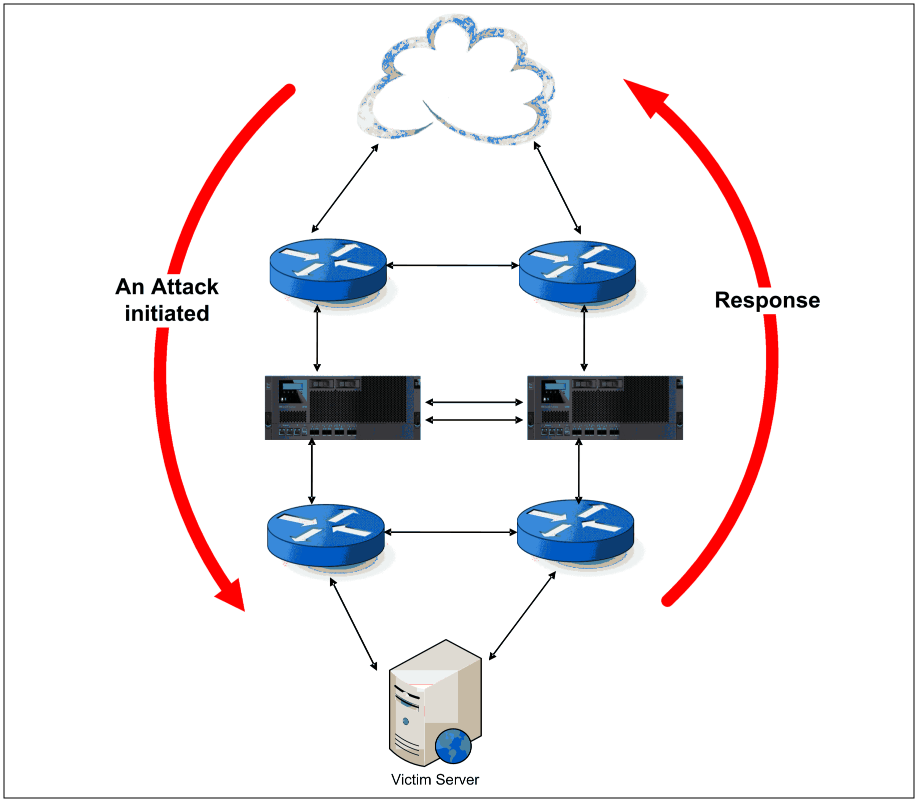


Figure 4-5 Network traffic loop

- The attack starts over one route and then continues over a second route. For example, the first appliance fails, or a routing metric changes. Figure 4-6 illustrates this type of scenario.

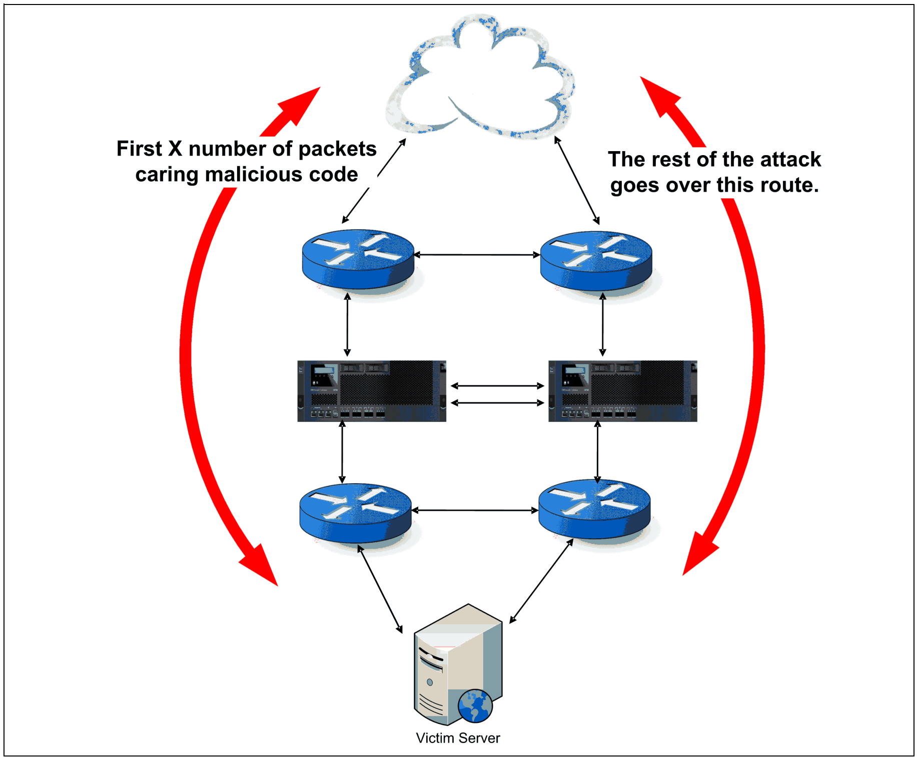

First X number of packets caring malicious code
The rest of the attack goes over this route.
Victim Server

Figure 4-6 Network traffic route changing

In both scenarios, if traffic is not mirrored, the PAM engines on both IBM Security Network IPS appliances might not see the complete conversation. Also PAM might not be able to understand or analyze the protocol. As a result, the security signature might fail to detect the attack.

Even though these types of scenario are rare, the approach to mirror over the traffic between both HA network IPS appliances ensures no risk of having a gap in the organization’s protection during failover.

4.3.3 Active/passive HA deployments

Because the passive link does not have any traffic flowing across it during normal operation mode, there is no asymmetric traffic. That is, port mirroring is not a necessity to avoid that type of scenario. However, an attack can take place during the failover process. An attack can start over the active link and continue over the secondary link during failover. This scenario is similar to the active/active scenario illustrated in Figure 4-6 on page 116.

If active/passive configuration is not using port mirroring, there is no need for both IBM Security Network IPS devices to be deployed in close physical proximity.

4.3.4 Geographical HA deployments

When considering the use of the geographical HA type, which is supported by the IBM Security Network IPS since firmware version 4.x, an organization must be aware of limitations that can entail the following details:

- When Geographic HA is invoked, the policy must be adjusted by the operational security team. Standard block responses do not work across IPS devices deployed in geographical HA mode. Change *block* responses on the signatures to *quarantine blocks*.
- Additional quarantine responses might be needed.
- Trusting the X-Force recommended settings does *not* provide blocking on future signature updates, because block responses must be converted to quarantine responses manually.
- NAT traffic and geographical HA blocks, by address, port, or both, come with a limitation. Consider the case where an organization has NAT traffic and a malware infected machine inside. With geographical HA blocking, *all* traffic on a port from that business partner might be blocked, both good and bad traffic.

4.3.5 External bypass units

The IBM Security Network Active Bypass intelligently provides maximum flexibility and delivers an uninterrupted communications session. The active bypass units can be configured to go from *inline* or active mode to bypass mode if a number (1 – 10) of heartbeats between the bypass unit and the IBM Security Network IPS get lost. The fastest way to switch to bypass mode is to configure `heartbeat=1`. In addition, you can configure the maximum time allowed between heartbeat acceptance in the range 100 – 25500 ms.

For the bypass unit to switch back to *inline* or active mode, you can configure the same threshold as a number (1 –10) of heartbeats. When you set `heartbeat=1`, the bypass unit switches back to active mode after only one heartbeat is accepted from the IPS appliance.

If the IPS appliance fails for any reason, the bypass ensures that the network remains functional and users have unimpeded access to important applications.

IBM Security Network Active Bypass in HA deployments: In active/passive network setups, install an external bypass unit on the passive/backup link, and not on the active/primary link. Not having a bypass unit on the primary link ensures that a failure on the primary link triggers a failover to the secondary link. This secondary link must also have a network IPS deployed. The external bypass unit on the secondary link then can be used only in case of dual failure.

For more information about the IBM Security Network Active Bypass, see the web page at:

`http://www.ibm.com/software/tivoli/products/network-active-bypass/`

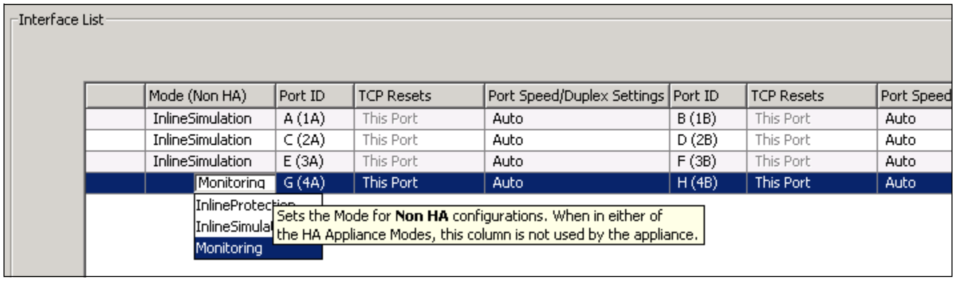
4.4 Setup, licensing, and updating before deployment

Your organization decides which IBM Security Network IPS models to deploy, where to deploy them, and how they will fit in the existing HA setup. Next it must consider performing basic setup steps before physically cabling the IBM Security Network IPS into the network. Although the IBM Security Network IPS works immediately when powered on without any configuration, as a best practice, your organization must follow the approach documented in this section before the actual roll-out.

You can perform the basic setup of an IBM Security Network IPS in several ways. For example, you can use the local management interface (LMI), which is a web server (HTTPS) running on the IPS that can be discovered by using Bonjour or by using the LCD display on the physical appliance. However, most users typically prefer to use a serial console connected to the IBM Security Network IPS.

When connecting to an IBM Security Network IPS by using a serial console and logging in using the administrative user for the first time, the appliance automatically prompts a setup wizard. This wizard asks for basic configuration options. These options include, for example, which IP address to assign to the management interface of the IBM Security Network IPS and the speed and duplex settings of the inspection interfaces.

One of the most important steps during the initial configuration is selecting the desired operational mode for the inspection ports of the IBM Security Network IPS. As explained in “Inline or passive mode” on page 48, you can have these port-pairs run in *inline simulation* mode, *inline protection* mode, or *passive* mode, as shown in Figure 4-7. For most initial deployments, an organization selects inline simulation mode. The goal remains to eventually move to inline protection mode, but to start with a fail-safe test phase.



	Mode (Non HA)	Port ID	TCP Resets	Port Speed/Duplex Settings	Port ID	TCP Resets	Port Speed
	InlineSimulation	A (1A)	This Port	Auto	B (1B)	This Port	Auto
	InlineSimulation	C (2A)	This Port	Auto	D (2B)	This Port	Auto
	InlineSimulation	E (3A)	This Port	Auto	F (3B)	This Port	Auto
	Monitoring	G (4A)	This Port	Auto	H (4B)	This Port	Auto

Sets the Mode for **Non HA** configurations. When in either of the HA Appliance Modes, this column is not used by the appliance.

Figure 4-7 Available operating modes per interface pair

In inline simulation mode, the appliance is immediately cabled inline, meaning the network traffic that needs to be inspected already traverses the IBM Security Network IPS. However, in inline simulation mode, the IBM Security Network IPS does not yet intervene in any way in the network flow. The appliance inspects and generates log events including those events where it might have stopped a packet or connection if it was already running in inline protection mode.

After the initial configuration setup is completed, you must consider one more recommended step before placing the IBM Security Network IPS in the network. That is, you must ensure that it has the latest X-Press Updates (XPU) installed.

X-Press Updates include the latest X-Force vulnerability and threat information that is researched by the IBM Security X-Force team. Each XPU adds valuable content that is searchable by using the online help. This content describes each event, affected platform, corrective action, and active hyperlinks with additional details. The XPU are available on a regularly scheduled basis and in an immediate fashion when late-breaking threat emergencies occur.

To download and install the XPU packages, a valid license must be installed on the IBM Security Network IPS. You can upload this license through the LMI web interface of the appliance. Alternatively, you can obtain it by registering the IPS with IBM Security SiteProtector if sufficient licenses are still available. After a valid license is active on the IBM Security Network IPS, you can apply the updates.

Obtaining XPU files: You can download XPU packages by using the IBM Security Network IPS directly from IBM web servers or from the IBM Security SiteProtector system for your organization.

Because an IBM Security Network IPS is usually initially deployed in *inline simulation* mode, where blocking attacks are not yet enabled, enable the X-Force recommended settings regarding the security checks or signatures. IBM Security X-Force offers suggestions for which signatures to enable and for which of these signatures (simulated) blocking is prudent.

Nearly all organizations benefit from starting with the X-Force recommended settings as a base for their environment. For information about the steps to take to address possible false negatives and false positives before switching the IBM Security Network IPS to *inline protection* mode, see 4.5, “Tuning the policy before moving to blocking mode” on page 120.

Many organizations continue to rely on the X-Force recommended blocks for all new XPU updates that are released, even when the IBM Security Network IPS is already running in *inline protection* mode. The extensive research performed by IBM Security X-Force yields a low occurrence of false positive alerts and blocks.

For organizations with more strict change management processes, an option is available to trust only the IBM Security X-Force recommendations through a specific XPU release. This way, new XPU releases can be tested first by the organization in a separate environment before accepting the recommendations.

Also, some organizations with sufficient in-house knowledge and resources might opt to never rely on the X-Force recommended settings. Instead, they will determine completely independently which checks they want to enable and when to enable blocking on a per signature basis.

4.5 Tuning the policy before moving to blocking mode

The final step that an organization typically must take when deploying a network IPS solution is to enable the blocking functionality. As explained in 2.2.3, “Deployment options” on page 48, only in *inline protection* mode can the IBM Security Network IPS provide true intrusion prevention and not just intrusion detection functionality. In inline protection mode, the IPS stops the threats before they can reach their intended targets. In inline simulation mode, the IPS logs only the blocks that it might have issued in inline protection mode.

As soon as the operational security team can verify the accuracy of the detected attacks and simulated blocks, it must schedule a change window to move the IBM Security Network IPS from *inline simulation* mode to *inline protection* mode.

Reminder: Every adapter pair on an IBM Security Network IPS can independently be configured to run in *inline simulation*, *inline protection*, or *passive monitoring* mode. An IBM Security Network IPS can combine these modes into one appliance.

After the IBM Security Network IPS is operating in *inline protection* mode, it blocks malicious or anomalous packets. Therefore, most organizations want to validate the simulated blocks that an IBM Security Network IPS has generated over a period of around 14 days. Where necessary, they also want to make policy changes or define exceptions, before enabling the blocking responses. Before trusting the IBM Security Network IPS to perform this blocking task and to intervene in the network traffic of the organization, the organization must perform analysis on the logged event data. It must look for *false positive*s and then tune the IBM Security Network IPS policy where necessary.

False positives: A false positive in this context occurs when valid, benign network traffic is incorrectly identified as malicious.

4.5.1 Reasons for policy tuning

An organization might want to tune their policy for the following main reasons among other reasons:

- To reduce the number of events that are being generated and that need to be analyzed by operational teams. This way, the available human resources can focus on more critical events or tasks.

  An organization can create response filters to reduce the amount of unnecessary alerts generated in the following situations:

  - When it wants to improve the performance of its IBM Security Network IPS
  - When it wants to reduce the workload on its operational security team that follows up on all generated security alerts

If the IBM Security Network IPS is protecting a network segment that does not hold any Microsoft Internet Information Services (IIS) for Windows Server web services, consider disabling the signatures related to IIS web server vulnerabilities. Consider a case where large amounts of backup data are sent across the inspected network to the same backup host every day. In some cases, you might tell the IBM Security Network IPS to ignore this type of network data and use its resources better to inspect other traffic instead.

- To reduce the number of false positive alerts that might cause unwarranted blocking in inline protection mode.

  The prime reason to perform a tuning of the policy is to ensure that switching from inline simulation to inline protection does not cause any interruptions in the regular benign network flow. To verify this situation, the organization must analyze all the simulated block events for accuracy before making the change to *inline protection* mode.

  In some occasions, an organization will notice that regular valid traffic in their network is being identified as malicious or anomalous and that the IBM Security Network IPS triggers a simulated block. For example, this situation can occur when a custom in-house developed application is not respecting all expected protocol standards. A policy change might be warranted in these cases to remove the false positive alerts that might fire in the network traffic of such a custom application.

- A concern about malicious activity not being detected in the most critical applications of the organization.

  An organization must consider which applications are most critical in their environment. If an organization has custom-built applications or can determine which type of applications and protocols are most important to them, it can match the available signatures in the PAM engine to them and enable some additional signatures.

  Not all malicious and anomalous activity will result in a (simulated) block response. The type of responses can be configured separately for each of the thousands of attack and audit signatures. A simple example might be changing the way that the IBM Security Network IPS reacts to detecting the `NICK` command in the Internet Relay Chat (IRC) protocol. By default, the IBM Security Network IPS is not configured to block this command. However, an organization might change this behavior if it learns that this type of communication occurs for no valid reason in their network and that all occurrences that it investigated were related to botnet activity.

- Acceptance testing of new XPU content releases.

  As explained in 4.4, “Setup, licensing, and updating before deployment” on page 118, an organization can hold back in accepting the X-Force recommended blocking responses for the newest XPU content releases until it verifies their impact. Some organizations run these tests in a separate network environment, where others use the new signatures directly in their production networks. They can have their IBM Security Network IPS operate in inline protection mode and apply the X-Force recommended settings, except for the latest XPU release signature changes. Although these settings have been tested thoroughly by IBM Security X-Force, an organization can consider their custom environment to be too prone to false positives to blindly accept these suggestions.

  An organization can choose to enable the latest signatures according to IBM Security X-Force suggestions, but not enable the blocking response associated with them at first. After only a week of testing and reviewing the log data, it can decide whether the new signatures will pose any risk in blocking valid traffic and then enable the blocking response.

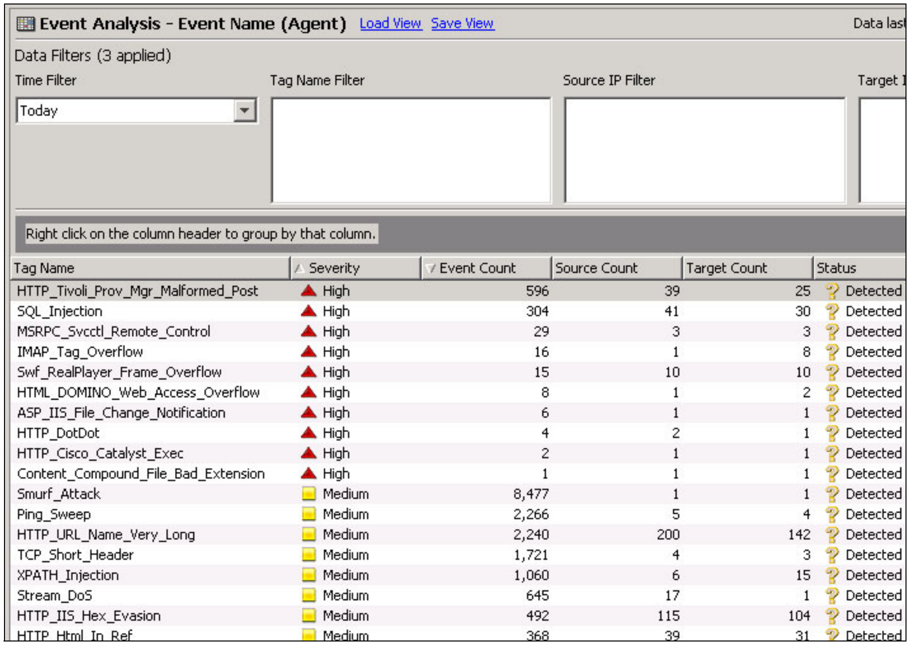
4.5.2 Analysis methods

Because organizations must address a large number of security events each day, security administrators must use the right tools and strategies to analyze these events. IBM Security SiteProtector provides event analysis functions that support a straightforward methodology to help your organization perform security analysis more efficiently.

When using IBM Security SiteProtector, as the analyst for your organization, you can use the following analysis strategy:

1. View summary event information.

   IBM Security SiteProtector includes predefined Analysis views with summary counts of important data points. As shown in Figure 4-8, the Event Analysis - Event Name view shows all events, with aggregated counts of sources, targets, and target objects (usually a port number). This view provides a broad look at the events that are affecting the network.



Data Filters (3 applied)

Time Filter: Today

Tag Name Filter

Source IP Filter

Target I

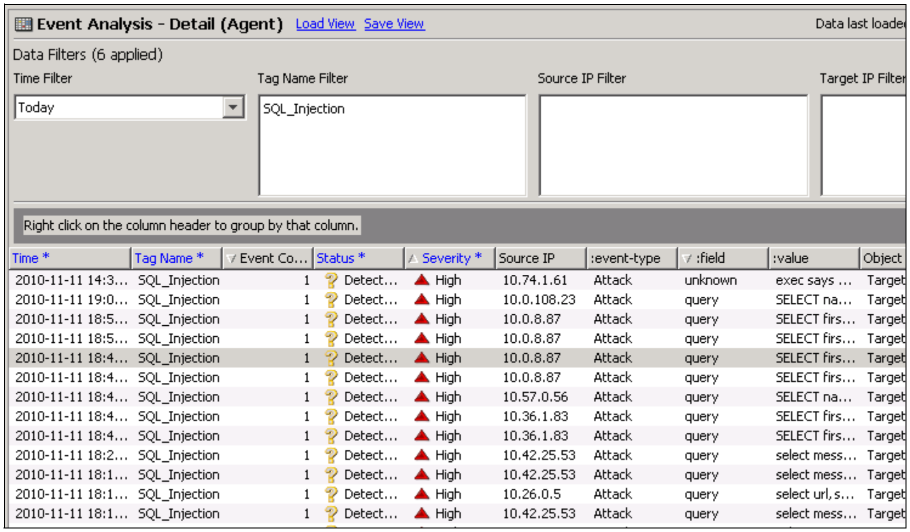
Right click on the column header to group by that column.

Tag Name	Severity	Event Count	Source Count	Target Count	Status
HTTP_Tivoli_Prov_Mgr_Malformed_Post	▲ High	596	39	25	? Detected
SQL_Injection	▲ High	304	41	30	? Detected
MSRPC_Svcctl_Remote_Control	▲ High	29	3	3	? Detected
IMAP_Tag_Overflow	▲ High	16	1	8	? Detected
Swf_RealPlayer_Frame_Overflow	▲ High	15	10	10	? Detected
HTML_DOMINO_Web_Access_Overflow	▲ High	8	1	2	? Detected
ASP_IIS_File_Change_Notification	▲ High	6	1	1	? Detected
HTTP_DotDot	▲ High	4	2	1	? Detected
HTTP_Cisco_Catalyst_Exec	▲ High	2	1	1	? Detected
Content_Compound_File_Bad_Extension	▲ High	1	1	1	? Detected
Smurf_Attack	🟨 Medium	8,477	1	1	? Detected
Ping_Sweep	🟨 Medium	2,266	5	4	? Detected
HTTP_URL_Name_Very_Long	🟨 Medium	2,240	200	142	? Detected
TCP_Short_Header	🟨 Medium	1,721	4	3	? Detected
XPATH_Injection	🟨 Medium	1,060	6	15	? Detected
Stream_DoS	🟨 Medium	645	17	1	? Detected
HTTP_IIS_Hex_Evasion	🟨 Medium	492	115	104	? Detected
HTTP_Html_In_Ref	🟨 Medium	368	39	31	? Detected

Figure 4-8   Event analysis overview in the IBM Security SiteProtector console

2. View high-level event details to determine their importance. These details can be blocked attacks, simulated blocks, or detected events with a high severity rating.

   To facilitate analysis, IBM Security SiteProtector provides predefined Analysis views with detailed information, such as the Event Analysis - Details view, as shown in Figure 4-9. By using such views, as the analyst, you can look more selectively at detailed event information. This information includes sources, targets, target objects, other events directed at a target, vulnerabilities on a target, and the agents that detected an event.



Event Analysis - Detail (Agent) Load View Save View Data last loade

Data Filters (6 applied)

Time Filter

Today

Tag Name Filter

SQL_Injection

Source IP Filter

Target IP Filter

Right click on the column header to group by that column.

Time *	Tag Name *	Event Co...	Status *	Severity *	Source IP	:event-type	:field	:value	Object
2010-11-11 14:3...	SQL_Injection	1	? Detect...	▲ High	10.74.1.61	Attack	unknown	exec says ...	Target
2010-11-11 19:0...	SQL_Injection	1	? Detect...	▲ High	10.0.108.23	Attack	query	SELECT na...	Target
2010-11-11 18:5...	SQL_Injection	1	? Detect...	▲ High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:5...	SQL_Injection	1	? Detect...	▲ High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	? Detect...	▲ High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	? Detect...	▲ High	10.0.8.87	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	? Detect...	▲ High	10.57.0.56	Attack	query	SELECT na...	Target
2010-11-11 18:4...	SQL_Injection	1	? Detect...	▲ High	10.36.1.83	Attack	query	SELECT firs...	Target
2010-11-11 18:4...	SQL_Injection	1	? Detect...	▲ High	10.36.1.83	Attack	query	SELECT firs...	Target
2010-11-11 18:2...	SQL_Injection	1	? Detect...	▲ High	10.42.25.53	Attack	query	select mess...	Target
2010-11-11 18:1...	SQL_Injection	1	? Detect...	▲ High	10.42.25.53	Attack	query	select mess...	Target
2010-11-11 18:1...	SQL_Injection	1	? Detect...	▲ High	10.26.0.5	Attack	query	select url, s...	Target
2010-11-11 18:1...	SQL_Injection	1	? Detect...	▲ High	10.42.25.53	Attack	query	select mess...	Target

Figure 4-9 Detailed view of a single type of security event

3. Create a prioritized subset of the event data.

   Sort and filter the event data to focus on critical and high value assets first.

4. Perform additional filtering on the events that are prioritized.

   Use *guided analysis* and other filtering options to focus on the most critical events.

5. Manually correlate events of undetermined importance.

   If you cannot make a final determination about the importance of an event, leave the event in the list so that you can manually correlate it with future events.

6. Check *raw details* of a security event where necessary. The raw details of an event can often help you determine the specific element or string in the network stream that the IBM Security Network IPS reacted on.

Guided analysis

The IBM Security SiteProtector console provides context-sensitive event data that can help you, the analyst for your organization, to access the detailed information required in your event analysis strategy. This event data is accessible through the pop-up menu of an event, which includes a view-specific set of options in the form of *guided* questions.

When you access detail information through the pop-up menu, as shown in Figure 4-10, the information is not displayed in a separate window. Instead, it is displayed as a new data view within the current Analysis view. After you review the detail information, you can return to the previous parent view by clicking the **Back** toolbar button.

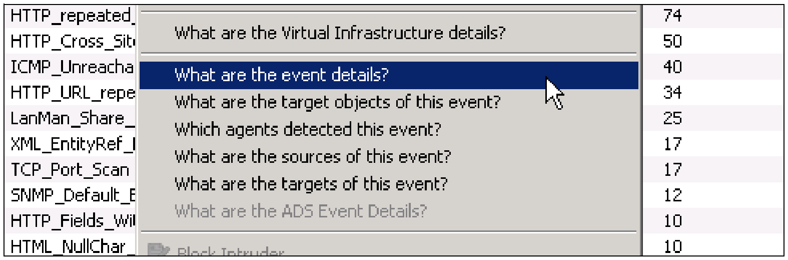

HTTP_repeated_
HTTP_Cross_Sit
ICMP_Unreacha
HTTP_URL_repe
LanMan_Share_
XML_EntityRef_I
TCP_Port_Scan
SNMP_Default_E
HTTP_Fields_Wi
HTML_NullChar_
What are the Virtual Infrastructure details?
What are the event details?
What are the target objects of this event?
Which agents detected this event?
What are the sources of this event?
What are the targets of this event?
What are the ADS Event Details?
Block Intruder
74
50
40
34
25
17
17
12
10
10

Figure 4-10 Guided analysis options in the IBM Security SiteProtector console

Analysis views

The IBM Security SiteProtector console includes several predefined Analysis views that you, as the analyst for your organization, can use to examine data from various perspectives and at different levels of detail. These views can help you perform the first two steps of the event analysis strategy to review summary and detail information. You can access predefined views from the drop-down list in the Analysis view.

PAM help file: A valuable resource when performing analysis on security event data generated by the IBM Security Network IPS appliances is the PAM help file. This file lists all relevant data (descriptions, references, tuning parameters and so on) for all available signatures. To download this file, got to:

http://www.iss.net/security_center/reference/help/pam

4.5.3 Tuning options

To deal with any false positives or other unwarranted security events as explained in 4.5.1, “Reasons for policy tuning” on page 121, an organization can make changes to the security policy of their IBM Security Network IPS appliances.

These types of policy changes are complementary to each other. They affect which network traffic is inspected, which security checks are used to inspect that traffic, and how the IBM Security Network IPS will respond when it detects malicious activity.

The information about the policy elements in this section is not exhaustive. Many more policy options exist and offer different functions. For a more complete discussion of all policy elements, see the *IBM Security Network IPS User Guide* in the IBM Security product Information Center at:

http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp

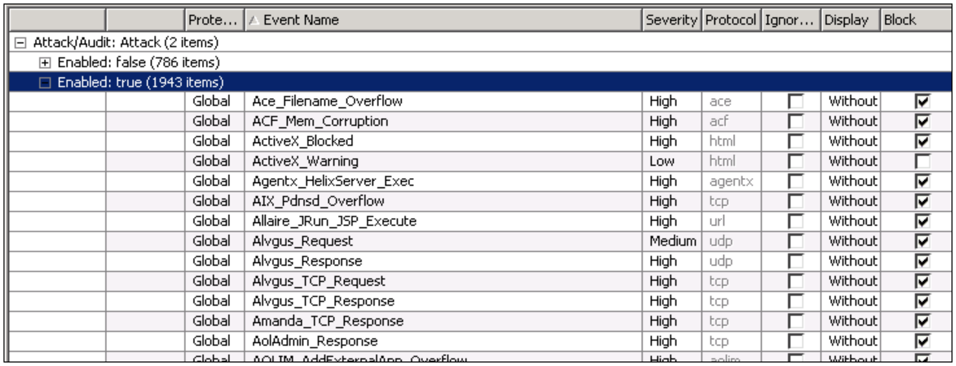
The policy elements listed in this book are the most commonly used when dealing with false positive alerts.

Enabling or disabling attack and audit signatures

One of the most straightforward methods for reducing the number of irrelevant security alerts is disabling a security signature altogether.

By using the *security events* policy editor (Figure 4-11), as the analyst for your organization, you can control security policy at the signature level. By default, all of the preconfigured event signatures are grouped under the following two nodes:

- Attack/Audit: *attacks*
- Attack/Audit: *audit*



		Prote…	△ Event Name	Severity	Protocol	Ignor…	Display	Block
⊟ Attack/Audit: Attack (2 items)								
⊞ Enabled: false (786 items)								
⊟ Enabled: true (1943 items)								
		Global	Ace_Filename_Overflow	High	ace	□	Without	☑
		Global	ACF_Mem_Corruption	High	acf	□	Without	☑
		Global	ActiveX_Blocked	High	html	□	Without	☑
		Global	ActiveX_Warning	Low	html	□	Without	□
		Global	Agentx_HelixServer_Exec	High	agentx	□	Without	☑
		Global	AIX_Pdnsd_Overflow	High	tcp	□	Without	☑
		Global	Allaire_JRun_JSP_Execute	High	url	□	Without	☑
		Global	Alvgus_Request	Medium	udp	□	Without	☑
		Global	Alvgus_Response	High	udp	□	Without	☑
		Global	Alvgus_TCP_Request	High	tcp	□	Without	☑
		Global	Alvgus_TCP_Response	High	tcp	□	Without	☑
		Global	Amanda_TCP_Response	High	tcp	□	Without	☑
		Global	AolAdmin_Response	High	tcp	□	Without	☑
		Global	AOLIM_AddExternalApp_Overflow	High	aolim	□	Without	☑

Figure 4-11 Security events policy configuration organized by default grouping

You can enable or disable specific event signatures and configure the following settings:

- Severity
- Blocking
- Event throttling
- Display
- Logging evidence

To help you manage the large number of security events supported by the appliance, the *security events* editor includes tools that you can use to change how events are displayed. These tools are especially useful when you need to configure multiple events, because you can quickly group, filter, and sort events to display just the events that you want to configure.

If an organization determines that, for example, it has no need to be alerted on IIS for Windows Server related attacks, it can select all the signatures related to it and disable them.

Enabling or disabling a blocking response

The *Security Events* tab lists hundreds of attacks and security events. As the analyst for your organization, you can configure security events that make up a security policy for your network. When the appliance detects network traffic with content indicating an attack or other suspicious activity that matches an event in the active policy, the appliance responds to the event as you specify.

While many more response options exist, the following options are the two most important ones:

- *alert only*
- *alert and block*

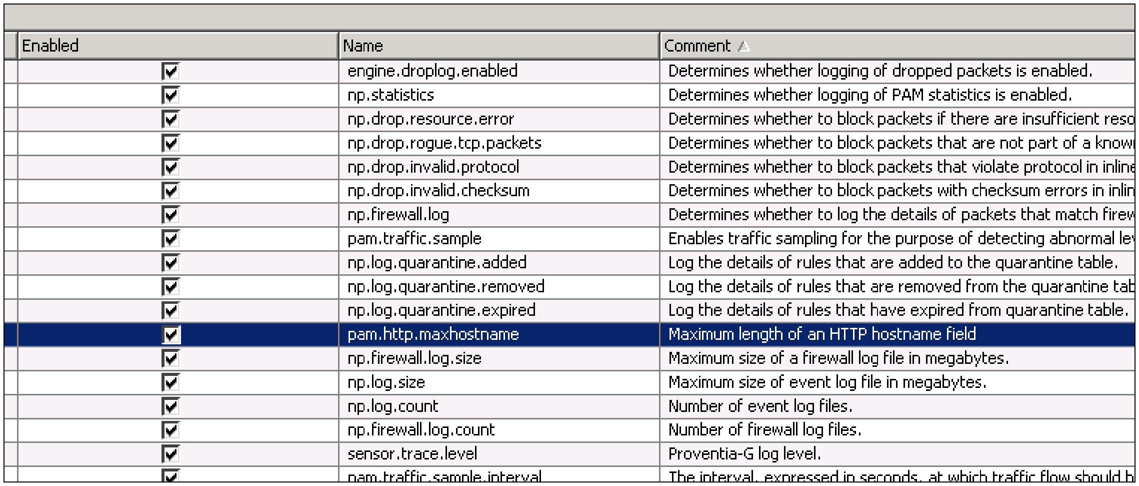
When tuning a policy before switching the IBM Security Network IPS to *inline protection* mode, the people doing the analysis will most likely focus on all the simulated blocks generated in inline simulation mode with highest priority. They want to verify that the packets that triggered a simulated block were malicious or at least unwanted in the network traffic.

However, if these people find a signature that consistently triggers a simulated block response on valid benign traffic, they need to take action. They can disable that signature, or they can keep it enabled but remove the block response. When they switch the IPS to inline protection, they might still see the logs coming in when the IPS detects the offending packets but can be assured that they do not block valid traffic.

Additionally it makes a lot of sense to enable various audit signatures, but often there is no need to enable blocking for them. An organization might want to detect a range of Instant Messaging protocols but not deem them malicious, and therefore, not choose to enable the blocking response.

Changing signature behavior with tuning parameters

Another way to deal with possible false positives is to deal with the way that the security event signature operates in the PAM engine. This task can be accomplished by using *tuning parameters* as shown in Figure 4-12.



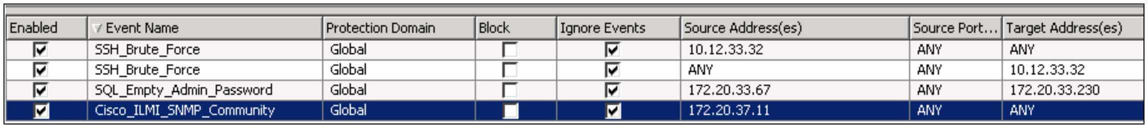
Enabled	Name	Comment
☑	engine.droplog.enabled	Determines whether logging of dropped packets is enabled.
☑	np.statistics	Determines whether logging of PAM statistics is enabled.
☑	np.drop.resource.error	Determines whether to block packets if there are insufficient reso
☑	np.drop.rogue.tcp.packets	Determines whether to block packets that are not part of a know
☑	np.drop.invalid.protocol	Determines whether to block packets that violate protocol in inline
☑	np.drop.invalid.checksum	Determines whether to block packets with checksum errors in inlin
☑	np.firewall.log	Determines whether to log the details of packets that match firew
☑	pam.traffic.sample	Enables traffic sampling for the purpose of detecting abnormal le
☑	np.log.quarantine.added	Log the details of rules that are added to the quarantine table.
☑	np.log.quarantine.removed	Log the details of rules that are removed from the quarantine tab
☑	np.log.quarantine.expired	Log the details of rules that have expired from quarantine table.
☑	pam.http.maxhostname	Maximum length of an HTTP hostname field
☑	np.firewall.log.size	Maximum size of a firewall log file in megabytes.
☑	np.log.size	Maximum size of event log file in megabytes.
☑	np.log.count	Number of event log files.
☑	np.firewall.log.count	Number of firewall log files.
☑	sensor.trace.level	Proventia-G log level.
☑	pam.traffic.sample.interval	The interval, expressed in seconds, at which traffic flow should b

Figure 4-12 Tuning parameter changing the maximum length of an HTTP hostname field

Tuning parameters can affect the overall behavior of the IBM Security Network IPS, but many parameters simply change the behavior of individual signatures. An example is changing the number of occurrences in a given time that are needed for a specific flooding signature to trigger. Many false positive alerts can easily be resolved by adapting these types of values to the needs of an organization.

Creating exceptions through response filters

The most frequently used policy element to reduce the number of unwarranted security alerts and (simulated) blocks is the *response filters* element. Figure 4-13 shows an example of the response filters policy editor.



Enabled	Event Name	Protection Domain	Block	Ignore Events	Source Address(es)	Source Port...	Target Address(es)
☑	SSH_Brute_Force	Global	☐	☑	10.12.33.32	ANY	ANY
☑	SSH_Brute_Force	Global	☐	☑	ANY	ANY	10.12.33.32
☑	SQL_Empty_Admin_Password	Global	☐	☑	172.20.33.67	ANY	172.20.33.230
☑	Cisco_ILMI_SNMP_Community	Global	☐	☑	172.20.37.11	ANY	ANY

Figure 4-13 Response filters used to ignore specific events based on IP addresses

The response filters element always take three basic elements into account when defining exceptions to the default policy rules:

- Specific event types or security events
- Affected hosts
- Action that the IBM Security Network IPS must take as a response

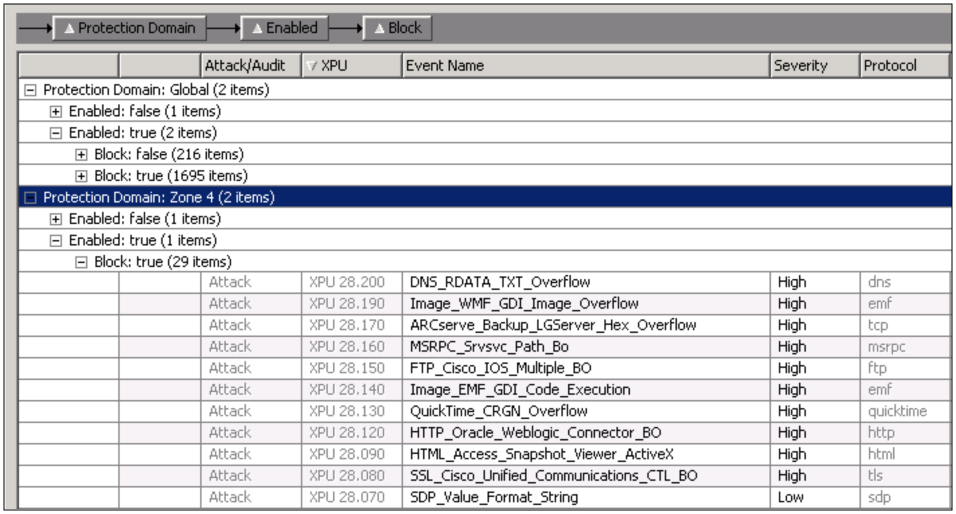
The response filter might be an ideal method to tune the policy when the analysts conclude that a specific signature is triggering false positive alerts on traffic originating from one specific host.

For example, an organization might conclude that, although the alerts generated by the PDF_Shellcode_Detected signature are generally accurate in indicating malicious activity, it has noticed one exception. It might have noticed that this signature is also triggering on benign network traffic from a network printer that uses an unusual way to encode scanned documents in the PDF file format. In this case, the organization can plan to create a response filter that states that this signature must not issue a block response only if the source IP of the connection belongs to that printer. In all other cases, the default policy might still be enforced.

Creating multiple virtual policies through protection domains

As mentioned in 2.2, “Physical and virtual appliances” on page 37, the IBM Security Network IPS appliances have multiple protection or monitoring interfaces. With this feature, an organization can use a single IBM Security Network IPS to protect multiple network segments. These segments might also be diverse. One might include user-initiated HTTP traffic to the Internet, and another segment might contain connections between middleware and databases.

Both segments can use the same policy, but it is not a necessity. By defining *protection domains*, the organization can run separate virtual policies in parallel on one IPS appliance as shown in Figure 4-14 on page 131.



Protection Domain → Enabled → Block

		Attack/Audit	XPU	Event Name	Severity	Protocol
⊟ Protection Domain: Global (2 items)						
⊞ Enabled: false (1 items)						
⊟ Enabled: true (2 items)						
⊞ Block: false (216 items)						
⊞ Block: true (1695 items)						
⊟ Protection Domain: Zone 4 (2 items)						
⊞ Enabled: false (1 items)						
⊟ Enabled: true (1 items)						
⊟ Block: true (29 items)						
		Attack	XPU 28.200	DNS_RDATA_TXT_Overflow	High	dns
		Attack	XPU 28.190	Image_WMF_GDI_Image_Overflow	High	emf
		Attack	XPU 28.170	ARCserve_Backup_LGServer_Hex_Overflow	High	tcp
		Attack	XPU 28.160	MSRPC_Srvsvc_Path_Bo	High	msrpc
		Attack	XPU 28.150	FTP_Cisco_IOS_Multiple_BO	High	ftp
		Attack	XPU 28.140	Image_EMF_GDI_Code_Execution	High	emf
		Attack	XPU 28.130	QuickTime_CRGN_Overflow	High	quicktime
		Attack	XPU 28.120	HTTP_Oracle_Weblogic_Connector_BO	High	http
		Attack	XPU 28.090	HTML_Access_Snapshot_Viewer_ActiveX	High	html
		Attack	XPU 28.080	SSL_Cisco_Unified_Communications_CTL_BO	High	tls
		Attack	XPU 28.070	SDP_Value_Format_String	Low	sdp

Figure 4-14   A couple of virtual policies configured through protection domains

Protection domains act similar to virtual sensors, as though several appliances are monitoring the network. As the analyst for your organization, you can define protection domains by using any combination of the following criteria:

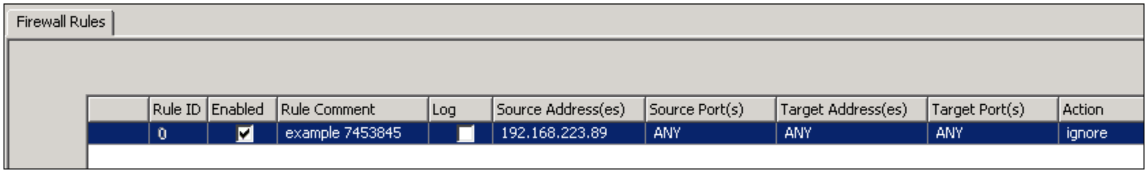
- Appliance adapters
- VLAN range
- Source and target IP address ranges

All events are listed under the global protection domain. The appliance always uses a global security policy. It handles security events in the same manner for all areas of your network unless you define protection domains and edit security event policies to suit each domain.

After you configure protection domains, you use them in conjunction with security policies that handle security events that occur on your network. You can create security policies for specific protection domains, or you can tweak the global policy for specific domains as necessary. With these policies, the appliance can detect which properties signal an event and how to respond if the event occurs.

Whitelisting or blocking traffic through the firewall module

A final policy element that proves to be a useful tool in tuning the security policy of the IBM Security Network IPS is the Firewall component (Figure 4-15).



	Rule ID	Enabled	Rule Comment	Log	Source Address(es)	Source Port(s)	Target Address(es)	Target Port(s)	Action
	0	☑	example 7453845	□	192.168.223.89	ANY	ANY	ANY	ignore

Figure 4-15 A firewall rule used to ignore all network traffic originating from a specific IP

With IBM Security Network IPS appliances, as the analyst for your organization, you can add firewall rules to drop or block unwanted packets before they enter your network. Alternatively, you can also create firewall rules to ignore specific traffic that you do not want to have inspected for intrusions. You can define firewall rules by using any combination of the following criteria:

- Adapter
- VLAN range
- Protocol
- Source or target IP address and port ranges

Consider the following guidelines, among others, when configuring firewall rules:

- Firewall rules only block and drop events when the appliance is set to the *inline protection* mode.
- Firewall rules are triggered on the ingress port.
- When working with firewall rules, pay attention to the order of your rules. Similar to other firewall products, the appliance processes firewall rules in the order in which they are listed.

When creating firewall rules, you can specify which type of action you want the IPS to take when traffic matches the firewall rule. The following actions are available:

Drop Drops packets as they pass through the firewall. To the user whose packet is dropped, it appears as though the target system does not respond.

Drop-and-reset Functions the same as the Drop action, but sends a TCP reset to the source. This connection terminates more quickly than the drop action because of the automatic reset.

Protect Passes traffic to the appliance, which logs, blocks, and quarantines as configured on the event signature.

Monitor (whitelist) Passes traffic to the appliance and logs traffic if there is a signature match. It does not block or quarantine traffic even if it is enabled on the signature.

Ignore Enables the matching packet to pass through the firewall and appliance without further inspection by the PAM engine.

As a rule of thumb, an organization must check the logged security events, especially the simulated blocks that were generated during a 14 – 30 day period of regular network traffic, for accuracy. Where necessary, it must make modifications to tune the policy to the custom environment of the organization as explained in this section.

Caveat: The time it takes for the full spectrum of generated security event logs to be generated differs from one organization to another. The time needed depends on the number of applications that are running on the inspected network segments and the frequency by which they are used.

After the organization tests the reliability of the initial policy in detecting and stopping the threats without blocking any valid network traffic, it must move the IBM Security Network IPS in *inline protection* mode. It does this task by changing the appropriate adapter mode setting as explained in "Inline or passive mode" on page 48.

4.6 Conclusion

This chapter explained some aspects of designing an IBM Security Network IPS solution. It explained where to deploy and how to select the right hardware models based on a scaling exercise. It also explained how to assess the impact of the preferred HA solution and how to select the preferred way for the IBM Security Network IPS act when it encounters a threat.

In addition, this chapter showed how an organization can use the IBM Security X-Force recommended policies as a base for their own customized policies. It addressed how you can use a single IBM Security Network IPS appliance to protect multiple network segments that might all have separate protection needs.

Finally this chapter outlined a possible methodology to fine-tune intrusion prevention policies and schedule updates. It touched on some of the important policy elements that can be used to map the behavior of the IBM Security Network IPS to different network environments.

Part 2

Customer scenario

Part 2 introduces a typical business scenario involving a healthcare company. It explains how the company can use the IBM Security Network IPS to help protect its servers and network from various security threats.

This part includes the following chapters:

5

Overview of scenario, requirements, and approach

This chapter introduces a typical business scenario of a fictional cardio healthcare company, referred to as *the cardio healthcare company* or the *company*. It shows how the company can use the IBM Security Framework and IBM Security Blueprint to help protect its servers and network from various security threats.

This chapter includes the following sections:

- Company overview
- Business vision
- Business requirements
- Functional requirements
- Design approach
- Implementation approach
- Conclusion

5.1 Company overview

The cardio healthcare company is a healthcare provider that focuses on providing specialized cardiovascular-related healthcare services in the US. The company was founded in California and then expanded across the country. It operates stand-alone clinics in several states, where each clinic occupies its own building and provides preventive care and outpatient services. For surgery and other inpatient services, the cardio healthcare company uses operating environments in partner hospitals. The cardio healthcare company also participates in research programs.

The cardio healthcare company maintains financial and confidential health information about its customers (patients, research partners, and affiliated hospitals). All records are kept in electronic form. One of the key applications is the *Patient Web Portal*, where, by using a personal portal page, patients can access their personal health records, payment information, and so on. In addition, email communication is available between patients and service providers.

Because the cardio healthcare company works closely with a few pharmaceutical companies on the latest drugs for heart disease, the exchange of confidential research-related information is extensive. Research information is also kept in an electronic form and shared over the network.

The cardio healthcare company has built a strong and long-term reputation and financial stability over the past 15 years in the US. The company's plan is to expand its operations within the US and to open healthcare centers in international markets.

The following section provides an overview of the information technology (IT) infrastructure that supports this business.

> **Staying focused:** The following sections describe company information that is relevant to the security solutions of the Network, Server, and Endpoint domain. It does not provide a complete description of the company nor address all the necessary activities related to information security.

5.1.1 Current IT infrastructure

The cardio healthcare company relies on two data centers: a *primary site* (in Phoenix, AZ) and a *backup site* (in Raleigh, NC). All production-related operations are performed in the primary data center. In terms of production, the backup data center is used for disaster recovery only.

The backup data center is also used for development and quality assurance (QA) tests on the applications and the infrastructure. Most of the business applications are web-based. All clinics are considered to have isolated internal networks that communicate with the production servers at the primary site. The endpoint systems in the intranet networks are primarily workstations running Microsoft Windows. In addition, most of the clinic's modern healthcare appliances (such as electrocardiogram (ECG) and nuclear diagnostic imaging systems) are also connected to its network and generate patient-related data, which is considered part of a patient's data record.

Figure 5-1 shows the geographical distribution of the provider.

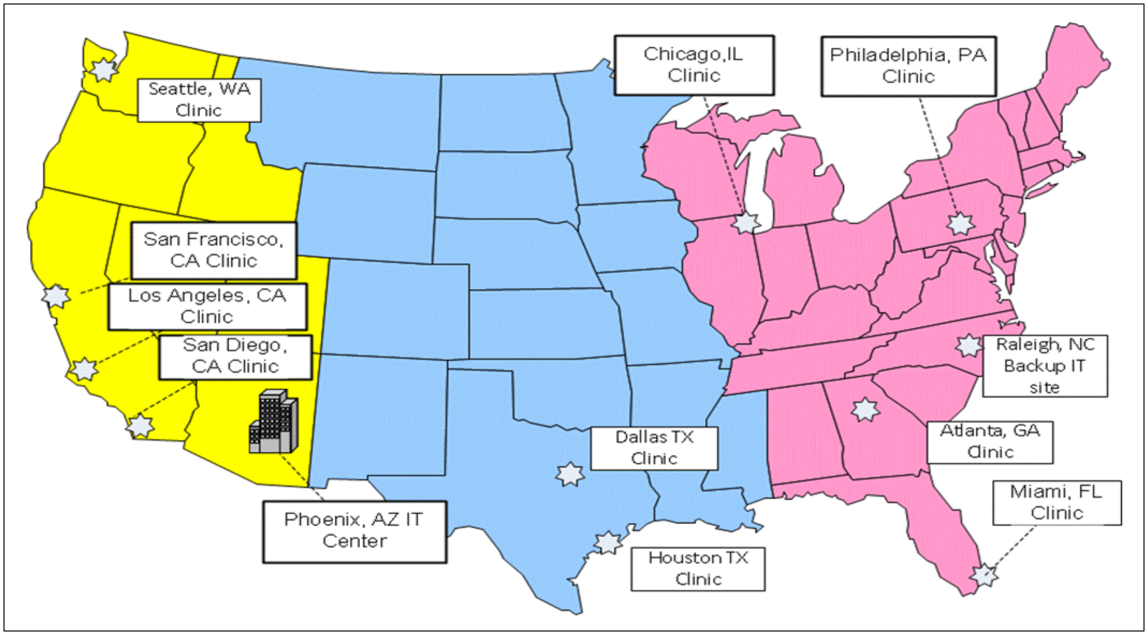


Figure 5-1 Geographical distribution of the cardio healthcare company

Clinics

The cardio healthcare company runs clinics in multiple US states. Each clinic operates its own network, with multiple zones, and communicates with the primary data center.

Primary data center

All customer-related information is stored on separate database entities that are clustered to fulfill high availability (HA) requirements. Most business critical web applications are deployed in a highly available configuration by using IBM WebSphere® Application Server Network Deployment.

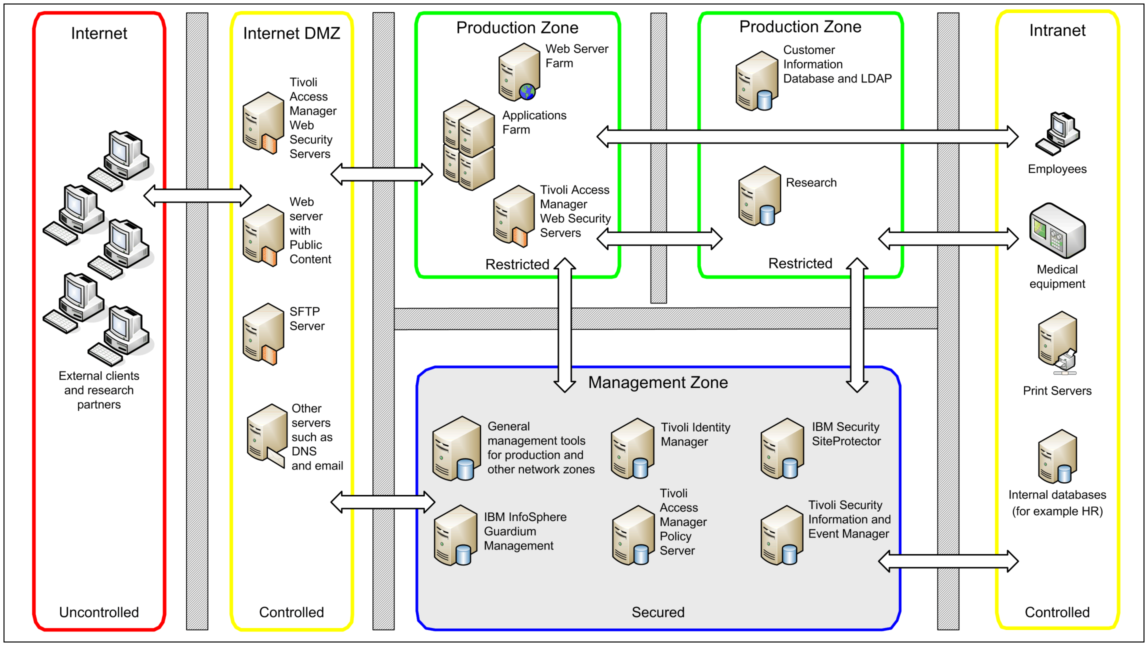
Web Security Servers (built on IBM Tivoli Access Manager technology) are in the Internet demilitarized zone (DMZ) to manage access to the applications from the Internet. The Web Security Servers help consolidate access management for the external users who are accessing web applications. The Web Security Servers perform centralized authentication and authorization before allowing access to the web applications. Public web content is isolated on separate web servers and is not protected with Secure Sockets Layer (SSL). All existing network infrastructure components (such as firewalls, switches, and routers) are designed and implemented in an HA (redundancy) configuration.

Application servers and database servers are in separate network zones and are isolated from each other by using firewalls.

The IT standards of the cardio healthcare company require all servers to use a UNIX or Linux technology-based operating system, with the following configuration:

- Application and database servers operate on IBM AIX®.
- Tivoli Access Manager Web Security Servers operate on Linux.
- The secure File Transfer Protocol (SFTP) server operates on Linux.
- Domain name servers (DNSs) and email servers operate on Linux.
- The server components deployed in the Management Zone operate on AIX.

Figure 5-2 shows several security components that are deployed in different network zones, which are separated by firewalls.



Internet
External clients and research partners
Uncontrolled
Internet DMZ
Tivoli Access Manager Web Security Servers
Web server with Public Content
SFTP Server
Other servers such as DNS and email
Controlled
Production Zone
Web Server Farm
Applications Farm
Tivoli Access Manager Web Security Servers
Restricted
Production Zone
Customer Information Database and LDAP
Research
Restricted
Intranet
Employees
Medical equipment
Print Servers
Internal databases (for example HR)
Controlled
Management Zone
General management tools for production and other network zones
Tivoli Identity Manager
IBM Security SiteProtector
IBM InfoSphere Guardium Management
Tivoli Access Manager Policy Server
Tivoli Security Information and Event Manager
Secured

Figure 5-2 Network zones in the current IT architecture of the cardio healthcare company

Figure 5-2 on page 140 shows the following security components, among others:

- A centralized identity management solution is based on IBM Tivoli Identity Manager. This system manages the full identity life cycle for internal and external users. Tivoli Identity Manager workflows are used to implement business processes for onboarding new users, for role changes, and when termination of access is required. The company also implements a role-based access control (RBAC) model that ties into the user management processes with Tivoli Identity Manager. The self-service password reset functionality provided by Tivoli Identity Manager helps lower IT help desk costs.
- Centralized access control management is implemented based on IBM Tivoli Access Manager software. All web-based access is controlled by using Web Security Servers. In addition, operating system-level access is enforced on critical servers using Tivoli Access Manager for Operating Systems agents. The following critical servers are identified:
  - The secure FTP server (Linux) containing confidential research reports
  - Application and database servers in the Production Zone (AIX)
- Centralized log collection, analysis, and reporting on compliance for Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), and ISO/IEC 27002:2005 is enforced by using Security Information and Event Management (SIEM) technology. This technology is implemented by using IBM Tivoli Security Information and Event Manager, which integrates with the Tivoli Identity Manager and Tivoli Access Manager infrastructure. It also offers operating system-level actuators (agents) that can collect logs from critical AIX and Linux servers.
- A distributed database real-time monitoring system is implemented by using IBM InfoSphere® Guardium® Database Monitoring and Protection. This system monitors all database activities in real time, including privileged user access, without the performance impact and separation-of-duties issues of native database logging. This solution also provides capabilities such as blocking, workflow management, and vulnerability assessments for the databases. The solution can be integrated with the Tivoli Security Information and Event Manager enterprise dashboard. The resulting compliance reports include IBM InfoSphere Guardium Database Monitoring and Protection events.

Minimized complexity: To minimize complexity, Figure 5-2 on page 140 does not contain the following agents that are deployed on various servers:

- Tivoli Identity Manager
- Tivoli Security Information and Event Manager
- Tivoli Access Manager for Operating System
- InfoSphere Guardium

Figure 5-2 on page 140 shows an overview of the current IT infrastructure of the cardio healthcare company using the network zone representation:

- Internet DMZ Zone

  The Internet DMZ Zone hosts Web Security Servers for Tivoli Access Manager that enforce access control policies for clients and research partners who access the applications and servers from the Internet. The architecture diagram also shows standard application servers in the Internet DMZ, such as an email and DNS and a web server with public content. The SFTP server, which is used to exchange research data and reports with the business partners in the pharmaceutical industry, is also in the DMZ. It operates over a secure connection.

  Design consideration: You often find that storing production data on any server in the Internet DMZ is unacceptable due to compliance and policy issues in many customer environments. In such case, an SFTP server can be replaced with a Secure FTP proxy server, and data can be placed on a server hosted in the Production Zone. In the scenario in this book, the cardio healthcare company used a Linux server with IBM Tivoli Access Manager for Operating Systems to enforce tight access control on the SFTP server.

- Intranet Zone

  In Figure 5-2 on page 140, the intranet, which depicts the IT resource location for a single clinic, is represented as a single network zone. Each clinic operates its own network with local print servers, human resource (HR) servers for that clinic, various workstations, and clinic devices.

  Design consideration: For the overall scenario, Figure 5-2 on page 140 might need multiple Intranet Zones, with each one representing a separate clinic, and each clinic having multiple zones for its own network. To simplify this scenario, we omit this complexity.

- Production Zone

  The Production Zone is split into two segments. One segment is used to host the production web and application servers, and the second segment shows that the database servers are securely isolated by another firewall. This setup helps enforce strong control of data access, which is often implemented in the healthcare industry. In addition, the Production Zone hosts Tivoli Access Manager Web Security Servers, which enforce access control policies for employees who access servers from the internal network.

- Management Zone

  The Management Zone shows that the cardio healthcare company has implemented an IBM Tivoli Security Information and Event Manager solution for centralized log and event management. Many Tivoli Security Information and Event Manager agents are deployed throughout the IT infrastructure, but for the sake of simplicity, we do not show those agents.

  Identity and access management solutions are also in place. The centralized Tivoli Access Manager and Tivoli Identity Manager components are securely deployed in the Management Zone to restrict access to security administrative personnel only.

  Database access controls and logging are strictly enforced by using an IBM InfoSphere Guardium Database Monitoring and Protection solution and collector component. The Guardium solution offloads the tasks from the database server (continuous analysis, reporting, and storage of audit data) to avoid any negative impact on database performance.

  In addition, this zone hosts other centralized management components, such as an incident and problem management solution based on IBM Tivoli Service Request Manager®.

The core applications used by external users (patients and business partners, such as pharmaceutical and research partners) are hosted on the applications farm:

- The Patient Web Portal, which provides the single web interface where patients can look up their health record, check and provide payments, and appointment management
- The Secure FTP server, which is used for information exchange with pharmaceutical companies

In addition to the applications mentioned previously, internal users have access to more applications, such as the following examples:

- HR database and applications that are locally deployed in each clinic
- Research information shared with pharmaceutical business partners, for example

After discussing the logical network zone layout, the cardio healthcare company determines it needs a more operational architecture diagram of the current IT infrastructure, with a focus on the network security devices. This type of diagram can vary in design and provides a more specific angle on functional design.

Figure 5-3 shows the operational architecture diagram of the cardio healthcare company, which involves firewalls, network switches, and major communication lines between the separate zones.

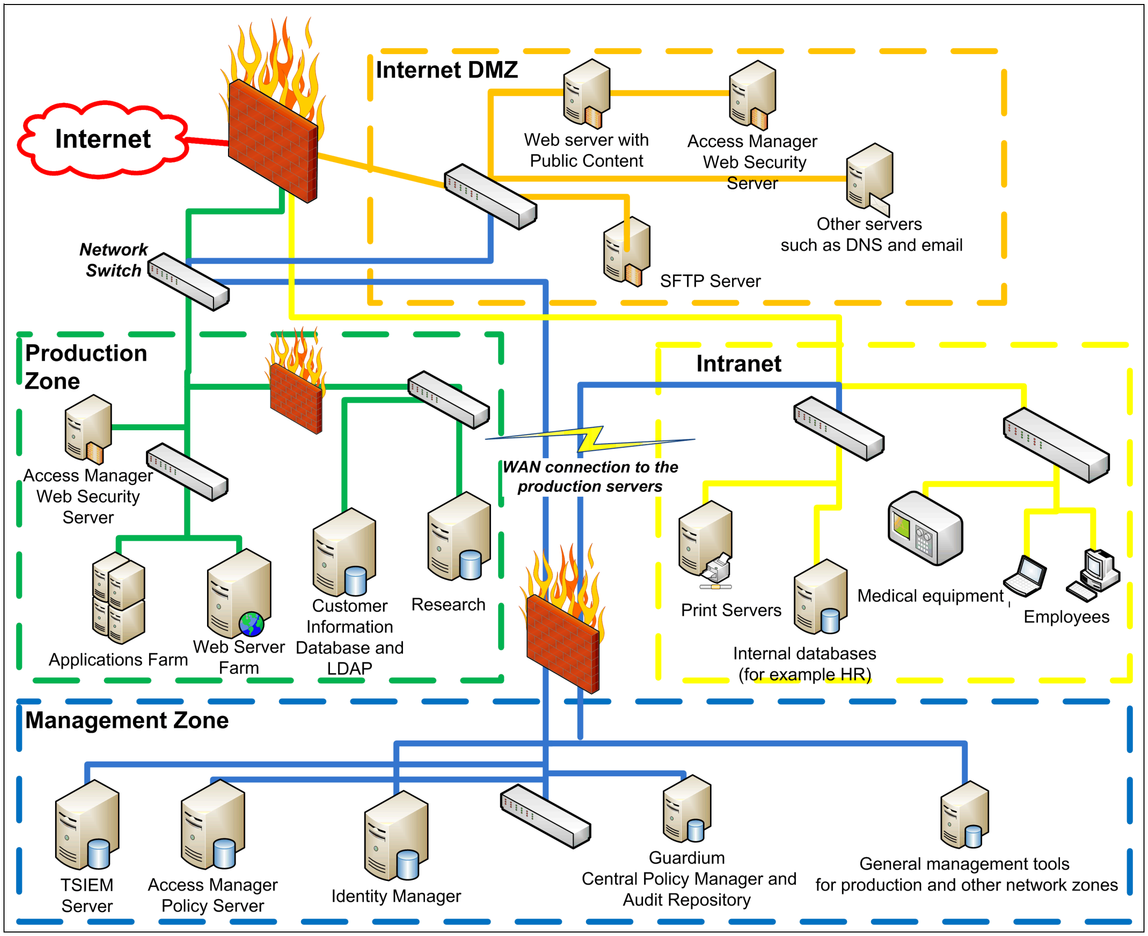


Figure 5-3 Current architecture overview of the cardio healthcare company

> **High availability capability:** To simplify the diagram in Figure 5-3, we did not include any HA aspects of the current architecture. However, all IBM security products in this scenario can be implemented in an HA infrastructure design.

Backup site

The backup site is not designed with high availability capabilities. The disaster recovery plan target is to recover the primary data center within one day. All system snapshots from the primary site are taken nightly and transferred to the backup site. In addition to this main purpose, the backup site is used as a test and integration environment for various application development and other IT projects. As a part of application development cycles, IBM Rational AppScan is used to perform web application scanning and testing to various security vulnerabilities.

Security at the primary site and beyond: In this book, we focus only on the security of the primary site. However, all security aspects and diagrams can be applied to the backup site and to the local networks at clinic locations.

5.1.2 Security issues within the current infrastructure

The cardio healthcare company has several other security-related issues in the current IT environment. Most web applications are running on different versions of IBM WebSphere Application Servers and web servers that require regular patching and maintenance. However, change management processes are usually slow and can take time to approve specific patch implementation in the production environment, which can expose systems to security risks.

In addition, IT management is aware that the current threat management approach is passive because it only involves antivirus software, intrusion detection devices, and firewalls. This type of threat management does not address zero-day attacks. The cardio healthcare company is looking to enhance security threat management with a more active approach, such as intrusion prevention devices.

A constantly increasing number of medical devices is connected to the internal IT network. These devices operate on different versions of embedded operating systems that are in the firmware of those devices, and the firmware is usally difficult to patch. Because these devices run the same or similar code as the regular operating systems (and, to some extent, providing the same system service), the devices are exposed to the same threats.

Due to increased electronic communication (email) between doctors and patients, a higher risk of worms and other malicious code is introduced into this environment. Although the cardio healthcare company has antivirus software in place, it does not provide increased protection against zero-day attacks or more focused and advanced attacks that can target a patient's information.

Besides the web applications, several other systems (including some healthcare devices) rely on non-encrypted Java Database Connectivity (JDBC) and Open Database Connectivity (ODBC) to the patient record database. This requirement poses a constant threat for possible information leakage over those types of connections.

5.2 Business vision

This section highlights the future direction that the cardio healthcare company plans to move its business development toward in the next five years:

- Expand business to the European Union (EU) by opening a clinic in Munich, Germany.

  By collaborating with some pharmaceutical companies on research in the EU, the cardio healthcare company wants to expand its business related to heart diseases by opening a clinic in Europe. The project is scheduled to begin in two years, and the opening is planned in the next four years.

- Reduce costs by reusing the solutions and using the lessons learned from the current IT infrastructure.

  The cardio healthcare company wants to reuse its architectural and implementation approach wherever possible. While copying the general infrastructure design, it tries to improve challenges found during operations and remediate them at an early phase.

- Respond to changing business needs and technology directions that can help improve customer experience by using new technologies.

  Business goals are always reassessed and are constantly changing depending of the organization’s needs. More often, the Internet is becoming a part of everyone’s life. An increasing number of patients are using email as a communication tool with their doctors. In addition, patients are using the web applications for reviewing their own medical records and to manage appointments online.

  Long term, the cardio healthcare company is looking to interconnect with other healthcare providers through the Smart Healthcare System. This system involves other aspects of health business, such as pharmaceutical and insurance.

  The myriad of constant changes requires a greater flexibility in IT technology. However, new technologies and means of communication open the possibility for new threats and vulnerabilities.

- Manage the budget by avoiding penalties due to non-compliance with major regulations, such as HIPAA, SOX, and PCI-DSS.

  In the healthcare industry, as in many others, non-compliance with regulations and standards can lead to significant financial fines and other types of penalties. The cardio healthcare company is successful in managing compliance with major regulations and is looking to maintain this good practice while expanding the business.

- Protect the company image and reputation by avoiding patient information leakage, preventing security attacks, and practicing security due care and due diligence.

  Any security intrusions, or leakage of any type of patient information (health, financial, or personal type), can lead to a loss of trust and damage to the reputation of the cardio healthcare company. The bottom line is that, besides losing money on penalties, it leads to a loss of customers and missed revenue opportunities.

5.3 Business requirements

Based on the visionary aspects highlighted in 5.2, “Business vision” on page 146, and the information in 5.1.2, “Security issues within the current infrastructure” on page 145, the cardio healthcare company wants to achieve the following short-term business goals:

- Improve the quality and availability of patient care and satisfaction by delivering an excellent, individualized healthcare experience.
- Increase the protection of all patient-related information, and then address the diverse security risks that are driven by eHealth initiatives, emerging technologies, data explosion, and so on.
- Facilitate the management of the overall compliance posture with data privacy laws and industry regulations, such as HIPAA and PCI-DSS.

Overall, the cardio healthcare company wants mature security solutions that can prevent information leaks, and that stay ahead of constantly evolving threats.

By addressing these pressing business requirements, the cardio healthcare company is trying to achieve the following goals:

- Continue to manage an acceptable balance between preventing security risks and adversely affecting the business.
- Constantly look for new and innovative solutions in all areas of the business, and always take security aspects into account.
- Be more proactive in security measures.
- Raise security awareness throughout the company by practicing corporate security education.

5.3.1 IBM Security Framework mapping to business requirements

Based on the following information, the administrator can engage in a discussion with the cardio healthcare company to better articulate its needs:

- The IBM Security Framework definitions for business-driven security
- The administrator's knowledge of the business requirements, which are outlined in 5.3, "Business requirements" on page 147
- The current organizational infrastructure, which is explained in 5.2, "Business vision" on page 146

Through this discussion, the administrator can derive the functional requirements using the underlying IBM Security Blueprint:

- People and Identity

  The cardio healthcare company uses mature identity and access management processes and tools that help lower the costs related to this domain. Many processes are automated, such as password reset and onboarding and terminating users. The implementation uses IBM Tivoli Identity Manager and IBM Tivoli Access Manager software.

- Data and Information

  The cardio healthcare company uses a granular information asset classification scheme paired with a least privilege principle. Access to the database servers is strictly real-time monitored and enforced, including privileged users, without the performance impact and separation of duties issues of existing database logging by using IBM InfoSphere Guardium Database Monitoring and Protection. The solution is integrated with the Tivoli Security Information and Event Manager enterprise dashboard.

- Application and Process

  Application development focuses on the *secure by design* principle. The cardio healthcare company follows a rigorous release management process with a granular promotion-to-production path that specifies security testing criteria. The cardio healthcare company uses IBM Rational AppScan software for testing during early development stages through to applications running in the production environment. This approach helps with practicing security during the application development phase and helps to discover any application vulnerabilities.

  The processes of the cardio healthcare company have achieved a high level of automation and embrace security controls, such as separation of duties and creation of auditable records.

For more information about a secure by design development approach, see the IBM Redguide publication *Security in Development: The IBM Secure Engineering Framework*, REDP-4641.

- Physical Infrastructure

  Physical Infrastructure controls are also embraced in the security program of the cardio healthcare company. Respective controls for physical access controls to facilities and systems are also present in all locations.

- Governance, Risk Management, and Compliance (GRC)

  The cardio healthcare company practices strong compliance enforcement by managing a security controls framework and strict audit and security awareness program. From a security monitoring perspective, running a Security Information and Event Management solution with compliance reporting modules for HIPPA and with other custom reports addresses important regulations for the operations of the cardio healthcare company in the healthcare industry.

  The cardio healthcare company designed and implemented a security policy framework and supporting processes for security governance. In this process, the company gained better insight into their GRC initiatives and could make better decisions about the following tasks by using the IBM OpenPages® solutions:

  – Where to allocate resources
  – How to mitigate risks effectively
  – How to respond quickly to the evolving compliance landscape

  On the technical side, the cardio healthcare company proactively works on identifying and eliminating security threats that enable attacks against systems, applications, and devices. The approach involves using various products, such as IBM Rational AppScan and IBM InfoSphere Guardium Database Monitoring and Protection, and integrating them with IBM Tivoli Security Information and Event Manager for compliance reporting purposes.

Based on the business requirements (5.3, “Business requirements” on page 147) and security issues (5.1.2, “Security issues within the current infrastructure” on page 145), the main requirements indicate a solution in the Network, Server, and Endpoint domain of IBM Security Framework.

We now take the next step in understanding the functional requirements and mapping them to the IBM Security Blueprint, followed by high-level look at the implementation approach.

5.4 Functional requirements

As mentioned in 5.1.1, “Current IT infrastructure” on page 138, the cardio healthcare company has a mature security infrastructure in place to address compliance needs by using Tivoli Security Information and Event Manager. The cardio healthcare company also deployed a strong identity and access control management solution using Tivoli Identity Manager and Tivoli Access Manager. Governance, change management, and separation of duties are strictly enforced across the organization.

However, to properly address the new business requirements, the cardio healthcare company must enhance its security solution infrastructure. The cardio healthcare company defines the following high-level functional requirements:

- To better manage its compliance posture with data privacy laws and industry regulations, the company must employ a cost-effective centralized management solution for security configuration polices and audit data. It must also integrate the proposed new security solution to the existing incident and problem management solution.
- To better protect all patient-related information and to address the diverse security risks driven by, for example, eHealth initiatives, emerging technologies, and data explosion, the company must protect against information leakage. Such leakage might be due to intrusions and zero-day attacks. The company must also protect its critical servers with additional layers of intrusion prevention.
- To improve the quality and availability of patient care and satisfaction by delivering an excellent, individualized healthcare experience, and to increase caregiver productivity and reduce administrative costs, the company must address unavoidable delays in the IT change management processes. This requirement will help to improve the security posture of the servers of the company and of all nonstandard (embedded) operating systems of medical appliances that are connected to the network.

In addition to these distinct functional requirements, which are in line with the business requirements, the cardio healthcare company has more, generally valid functional requirements that require examination:

- Respond more in real time to intrusion detection and prevention (blocking) events.
- Detect and, if possible, automatically counteract detected attacks.
- Provide a solution that is more proactive to security threats.

The cardio healthcare company already uses some solutions to identify and eliminate security threats that enable attacks against systems, applications, and devices. However, the level of automation and the speed of these activities, in addition to the information available for Threat and Vulnerability Management, can be improved.

5.4.1 IBM Security Blueprint mapping to functional requirements

We now understand the functional requirements for the additional security measures that the cardio healthcare company needs to implement. Yet we still must determine which specific solutions can potentially fulfill the functional requirements. By using the IBM Security Blueprint, we can better explain and map the functional requirements into specific blueprint areas, identifying the appropriate solutions to implement within the IT environment of the company.

Figure 5-4 shows the mapping of the functional requirements to the IBM Security Blueprint.

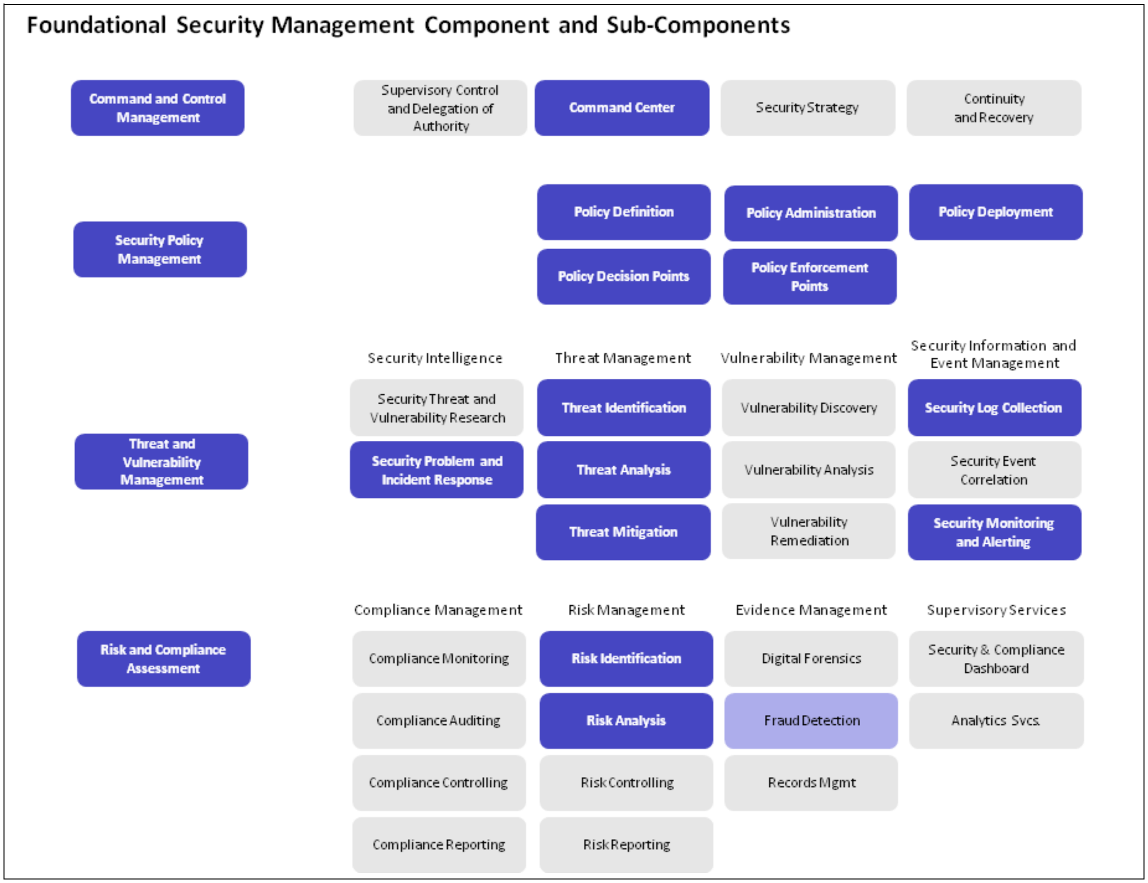


Figure 5-4 IBM Security Blueprint: Foundational components for functional requirements

Let us look closer at each of the functional requirements derived from the IBM Security Blueprint and map them to each of the required Foundational Security Management Components and Subcomponents:

- Continue good management practices by adding a centralized management platform (command center) for intrusion prevention system (IPS) components.
- Centralize lifecycle management of security configuration polices (definitions, administration, deployment, and archiving) for the IBM Security Network IPS infrastructure.
- Better understand the ability of the actual threat posture (identification) to perform attack (threat) analysis and threat mitigation.
- Continue to comply with HIPAA regulations. Have the ability to integrate with the current SIEM infrastructure by collecting security logs from different security tools deployed with the new solution, and have the ability to perform more frequent and efficient monitoring and alerting.
- Report all security-related tickets and incidents using a standard company enterprise ticketing system (IBM Tivoli Service Request Manager).
- Use policy enforcement points (PEP) and policy decision points (PDP) for intrusion prevention on all network segments and strategic (production) servers. The following strategic servers are identified:
  - Secure FTP server containing confidential research reports
  - Application and database servers in the Production Zone
- Capture and block information leakage of customer-sensitive information, and research data from the production databases.
- Protect financial and health records information on all systems, and prevent any leakage of that information to the public web pages.
- Continue practicing strict governance, change management, and separation of duties rules.
- Rely on multiple levels of security protection by using network zoning.

Although business and functional requirements are the main parts of the security design objectives, we also must consider other non-functional requirements and constraints. These non-functional requirements and constraints might include objectives that are necessary to meet general business requirements, service level agreements (SLAs), or practical constraints about constructing security subsystems.

The architectural team performed analyses of non-functional requirements and identified the following key non-functional requirements and constraints:

- Provide 99.99% (“four nines”) availability (access to the system) that translates into 52.56 minutes of downtime per year.
- Provide a scalable solution that can be replicated to any other data center.

Product mapping: Because this book focuses on the security architecture of the Network, Server, and Endpoint domain, it does not look in detail at these non-functional requirements. However, all IBM products mapped to this IBM Security Framework component can satisfy the non-functional requirements and constraints mentioned previously.

The following sections show how to further use the IBM Security Framework and IBM Security Blueprint in both the design and implementation of new security solutions.

5.5 Design approach

The administrator for the cardio healthcare company determined the areas of the IBM Security Blueprint that the new solutions must fulfill to adequately address all of its requirements. As the administrator for the company, you can now map the technical requirements to the Security Services and Infrastructure components of the IBM Security Blueprint. The purpose of this exercise is to help determine which security solutions ultimately best satisfy all of our requirements, whether they are business, functional, non-functional, or technical.

Figure 5-5 shows how the mapping was done for the cardio healthcare company using the functional requirements and existing architecture.

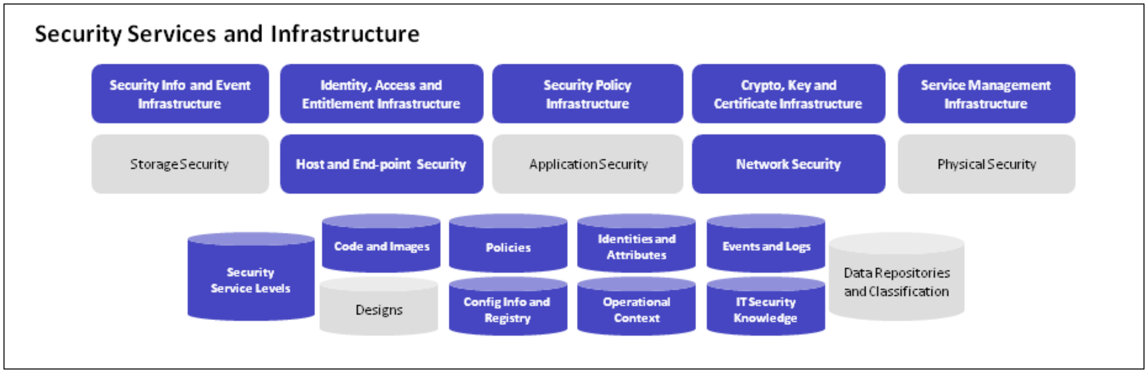

Security Services and Infrastructure
Security Info and Event Infrastructure
Identity, Access and Entitlement Infrastructure
Security Policy Infrastructure
Crypto, Key and Certificate Infrastructure
Service Management Infrastructure
Storage Security
Host and End-point Security
Application Security
Network Security
Physical Security
Security Service Levels
Code and Images
Designs
Policies
Config Info and Registry
Identities and Attributes
Operational Context
Events and Logs
IT Security Knowledge
Data Repositories and Classification

Figure 5-5 IBM Security Blueprint: Technical components for design

As part of the design, you can produce an implementation plan for the deployment that involves following steps:

1. Prioritize the requirements.
2. Map the requirements to IBM product features.
3. Define the tasks involved in using those features to satisfy the requirements, and estimate the effort required for each task.
4. Divide the tasks into phases.

Therefore, you can now focus on the technical components of the IBM Security Blueprint and how they can be mapped into technical and operational requirements.

Based on the mapping, you now know that the solutions must provide the following Security Services and Infrastructure components:

- Integrate log and intrusion events with the existing Security Information and Event Infrastructure.
- Define network access control infrastructure and mechanisms (network traffic security access polices) to allow proper communication between the components.
- Centralize management of technical level security polices with a single location to design, update, change, and roll back the policies.
- Secure communication between key components using certificate infrastructure or some type of public/private key infrastructure.
- Integrate event, incident, and problem handling with existing services management procedures.
- Integrate the ticketing mechanism of the existing service management infrastructure (Tivoli Service Request Manager).
- Support the existing operating systems (hosts), identified as key components, for UNIX (AIX) and Linux.
- Support the existing network infrastructure, and facilitate the deployment of network security mechanisms (tools) with a minimal disruption of the current network design and address schema. At the same time, the components must be deployed into key network communications paths.
- Implement proactive protection against security threats to help stop attacks against known vulnerabilities at network zone borders.
- Mitigate the security risk from delays in change management for operating systems and middleware by stopping the threats at the network level before they reach vulnerable targets.

Physical and storage security: Physical security and storage security are also an important part of the overall solution. However, they are treated as a separate project that is not in scope of this book.

- Meet SLAs that are in line with the policies, standards, and procedures (for example, the 99.99% availability target) of the organization.
- Use a central repository for code updates and new release of agents.
- Provide policy lifecycle management. The solution must store, maintain, and provide versioning of security polices.
- Store the credential (identities and attributes) for communication between components; for interactive login, the credentials must be stored in accordance with company security polices.
- Create and map events and logs by all agents, and integrate them with the overall event management solution and allow for near real-time alerting.
- Provide an efficient mechanism for keeping a record of the actual configuration.
- Consider the criticality, the layout, and the structure of communication patterns (operational context) to determine the threat landscape of observed vulnerabilities.
- Establish educated resources that possess the appropriate security knowledge and analytic skills and that have support from the vendor.

After completing the mapping, you can use the output to determine which solutions are needed and ultimately produce an implementation plan for the selected solutions. To accomplish this task, you map all of the stated requirements into product features using the IBM Security Blueprint diagrams.

5.6 Implementation approach

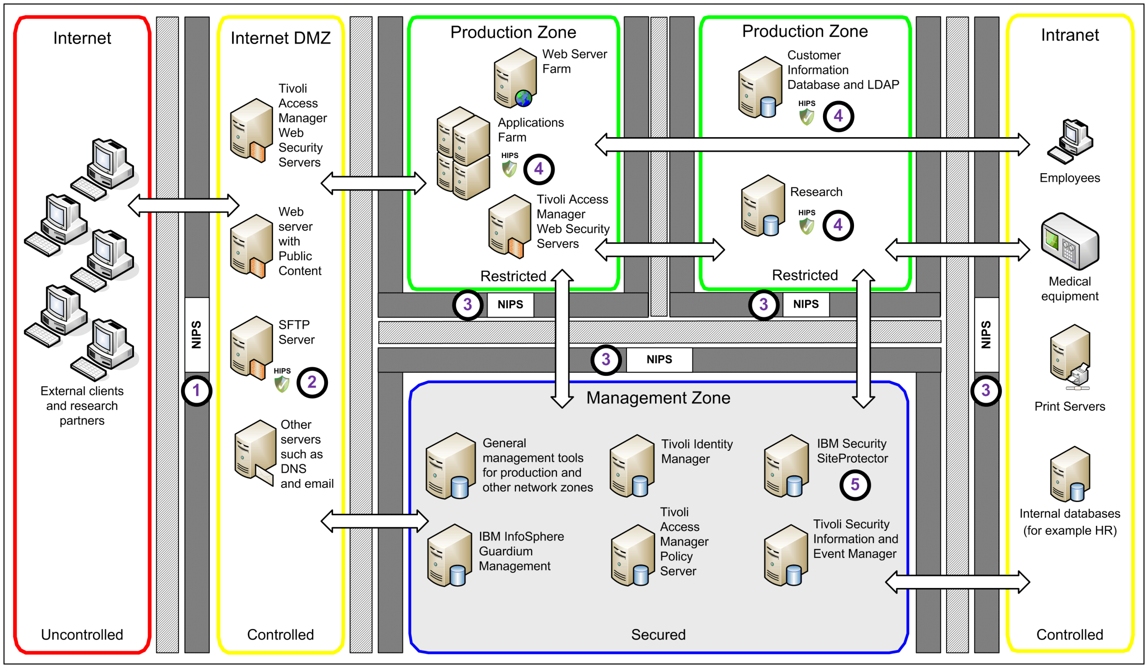
You now understand all of the requirements and how they map into the IBM Security Framework and IBM Security Blueprint. As the administrator for the cardio healthcare company, you can apply this knowledge to select the appropriate solutions to satisfy all of the requirements.

Based on the design approach (see 5.5, “Design approach” on page 153), you can build the following implementation plan:

1. IBM Security Network Intrusion Prevention System as the robust, proactive IPS for the networks
2. IBM Security SiteProtector as the centralized management platform for IPSs (network and hosts)
3. IBM Security Server Protection for Linux as the host-based IPS for Linux
4. IBM Security Real Secure® Server Sensor as the host-based IPS for the AIX platform
5. IBM Tivoli Security Information and Event Manager as an extension of the centralized management platform for IPSs

   It can manage and monitor logs from various technology platforms and provide analytics that help the security manager to protect intellectual property and privacy and to support compliance mandates.

By using the components mentioned previously, you can position them in the new solution using a network zone diagram, as shown in Figure 5-6.



Internet
External clients and research partners
Uncontrolled
NIPS
1
Internet DMZ
Tivoli Access Manager Web Security Servers
Web server with Public Content
SFTP Server
HIPS
2
Other servers such as DNS and email
Controlled
Production Zone
Web Server Farm
Applications Farm
HIPS
4
Tivoli Access Manager Web Security Servers
Restricted
3
NIPS
Production Zone
Customer Information Database and LDAP
HIPS
4
Research
HIPS
4
Restricted
3
NIPS
3
NIPS
Management Zone
General management tools for production and other network zones
Tivoli Identity Manager
IBM Security SiteProtector
5
IBM InfoSphere Guardium Management
Tivoli Access Manager Policy Server
Tivoli Security Information and Event Manager
Secured
Intranet
Employees
Medical equipment
NIPS
3
Print Servers
Internal databases (for example HR)
Controlled

Figure 5-6 New proposed solution using a network zone

The selected solutions that address the requirements for the cardio healthcare company have the following key features provided among other features:

1. An IBM Security Network IPS device, configured in the area marked with ❶ in Figure 5-6, applies a *virtual patch* to all the systems behind the Internet DMZ firewall. As the admininstrator for the company, you can apply policies that stop sensitive data transfers (such as email and email attachments) that contain, for example, private patient information (such as credit card data and social security numbers). This device can help protect against zero-day attacks and the propagation of known and unknown viruses, worms, and other types of malware.
2. IBM Security Server Protection for Linux implemented on the SFTP server adds a layer of protection to a server. This layer stores reports and data on drugs and other research-related information that are exchanged with pharmaceutical companies. Because the Network IPS device deployed in ❶ in Figure 5-6 on page 156 is unable to block encrypted FTP traffic, adding host-based IPS protection adds significant value. This host-based protection layer can also potentially be deployed to other Linux technology-based servers at a later time.
3. IBM Security Network IPS devices in other zones help satisfy the layered protection requirement. These devices can contain attacks within one network zone. In addition, the devices in the database zone can be configured with Information and Data Leakage Protection policies to prevent uncontrolled use of patient sensitive information across ODBC and JDBC connections.
4. Host IPS agents deployed on servers in the Production Zone can also provide an additional security layer. With these agents, you can apply policies that are specific to hosts, such as a Buffer Overflow Exploit Prevention (BOEP) policy.

   All previously mentioned devices provide the Virtual Patch technology to all critical and non-critical assets.
5. IBM Security SiteProtector helps deliver centralized management of intrusion prevention agents (host and network). It can analyze intrusions, handle real-time discovery, and monitor subsequent attacks. Integration with the Tivoli Security Information and Event Manager can help maintain further compliance to critical regulations.

   In addition, IBM Security SiteProtector has an API that can integrate the ticketing solution and incident management system of the organization based on Tivoli Service Request Manager. Going a step beyond, you can integrate IBM Security SiteProtector with IBM Rational AppScan and discover any new vulnerabilities, which can help create new signatures (policies) in IBM Security SiteProtector. IBM Security SiteProtector can then again push such policies to all deployed IBM Security Network IPSs.

The final architecture overview diagram in Figure 5-7 shows more details about how you place the IBM Security Network IPSs with inline protection mode, showing the position of firewalls and network switches in the architecture.

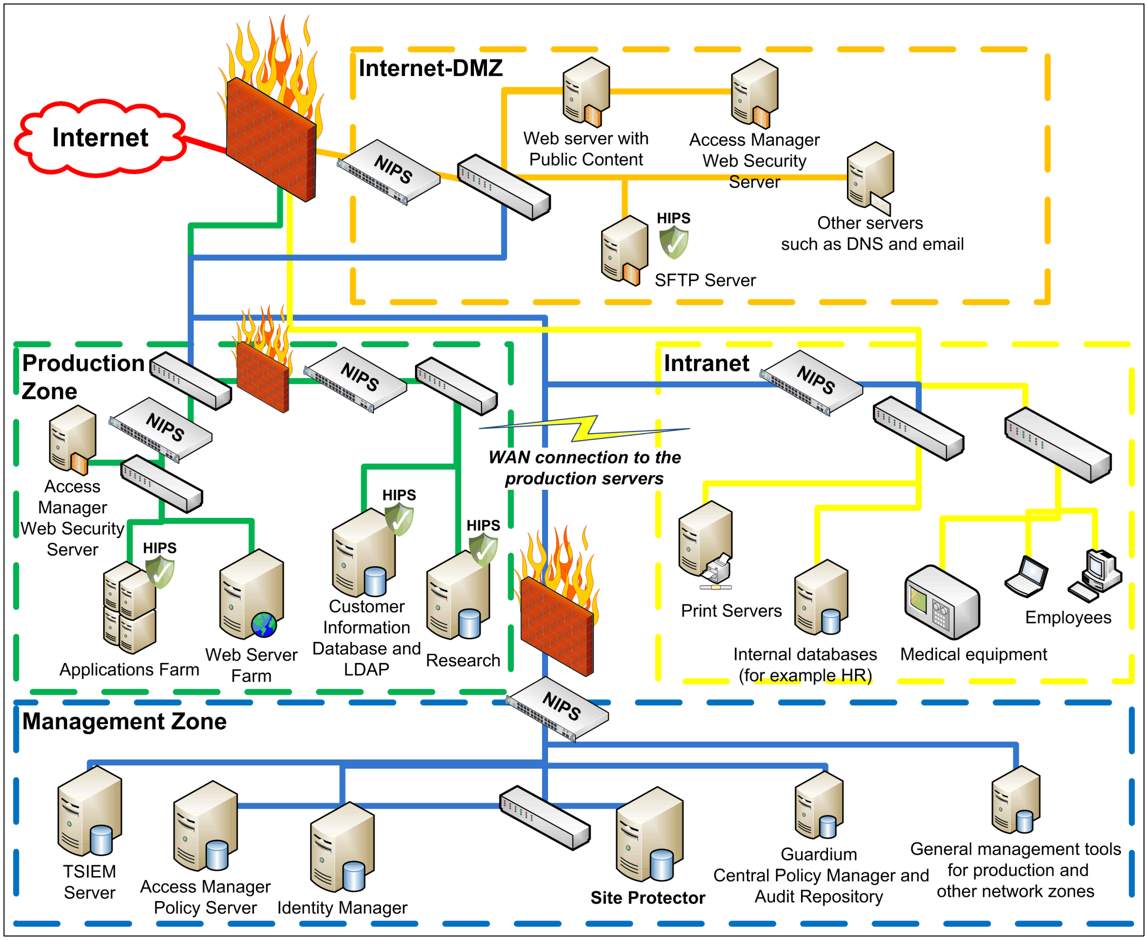

Internet
Internet-DMZ
NIPS
Web server with Public Content
Access Manager Web Security Server
HIPS
SFTP Server
Other servers such as DNS and email
Production Zone
NIPS
NIPS
Access Manager Web Security Server
HIPS
Applications Farm
Web Server Farm
HIPS
Customer Information Database and LDAP
HIPS
Research
WAN connection to the production servers
Intranet
NIPS
Print Servers
Internal databases (for example HR)
Medical equipment
Employees
NIPS
Management Zone
TSIEM Server
Access Manager Policy Server
Identity Manager
Site Protector
Guardium Central Policy Manager and Audit Repository
General management tools for production and other network zones

Figure 5-7 Architecture overview of the new proposed solution

The remainder of this book focuses on the implementation plan steps to set up the IBM Security Network IPSs along with the centralized IBM Security SiteProtector. This approach results in two distinct deployment phases:

- “Phase 1: Design and implementation of IBM Security Network IPS” on page 161
- “Phase 2: Policy tuning for IBM Security Network IPS” on page 211

5.7 Conclusion

This chapter combined several IBM Security Systems products to help an organization fulfill the requirements for Threat and Vulnerability Management. It showed how the IBM Security Framework and the IBM Security Blueprint can provide a structure to derive the IT functional and technical requirements from the business vision, goals, and requirements.

First, this chapter introduced the cardio healthcare company. It began with a company profile, its current IT infrastructure, and its issues with networks, servers, and endpoints. Then it explained the business requirements and the associated functional requirements, including refining them to a more detailed technical level.

Next, this chapter described the design approach that the cardio healthcare company took for its solution, following the IBM Security Framework and the Threat and Vulnerability Management Solution Pattern of the IBM Security Blueprint. When applied to the company's unique IT environment, this process of analysis and design helped the cardio healthcare company define an implementation plan.

6

Phase 1: Design and implementation of IBM Security Network IPS

This chapter examines the network design and implementation of the IBM Security Network Intrusion Prevention System (IPS) device for the cardio healthcare company (or the *company*). The cardio healthcare company is responsible to many regulatory authorities. Examples include the Health Insurance Portability and Accountability Act (HIPPA), Electronic Protected Health Information (ePHI), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), and International Organization for Standardization/International Electro Technical Commission (ISO/IEC) 27002.

All of these authorities require high security and auditing standards that influence business requirements. The business requirements map to the functional requirements that are derived from the IBM Security Blueprint. The concepts of the IBM Security Blueprint are mapped to the required Foundational Security Management Subcomponents in 5.4.1, "IBM Security Blueprint mapping to functional requirements" on page 151.

The security management solution for the cardio healthcare company is derived from meeting the business requirements with the mix of IBM Security products. The solution consists of IBM Security Network IPS and IBM Security

SiteProtector. IBM Security SiteProtector provides real-time event aggregation and policy management. This chapter highlights the design and implementation of IBM Security SiteProtector and the various IBM Security Network IPS models to be managed.

This chapter includes the following sections:

- Design
- Implementation
- Conclusion

6.1 Design

An IBM Security Network IPS appliance monitors the network for malicious attacks while preserving network bandwidth and availability. These appliances are purpose-built, Layer 2 network security appliances. They can be deployed at the gateway or the network to monitor intrusion attempts, denial of service (DoS) attacks, malicious code, back doors, and spyware. They can also monitor peer-to-peer applications and a growing list of threats without requiring extensive network reconfiguration. The IBM Security Network IPS appliance must be deployed where it complements the existing network architecture of firewalls and switches. When placed properly, the advanced features of the IBM Security Network IPS appliance can provide an additional layer of protection for network environments.

The cardio healthcare company employs the following steps to design its IBM Security Network IPS solution:

1. Define *network zones*.

   Figure 4-1 on page 105 illustrates the network zones where each zone represents a logical boundary separated by a firewall. The firewalls are strategically placed in areas where the cardio healthcare company wants to inspect and control the flow of network traffic. The company complements its firewall infrastructure with IBM Security Network IPS appliances. All network information is examined and protected as it flows between the defined network zones (uncontrolled, controlled, restricted, secured, and external controlled; see 4.1.1, “Concept of network zones” on page 104).

2. Define *information zones*.

   In some instances, zones must be further divided to segregate functional differences. Functional division considerations allow more granular implementation of the IBM Security Network IPS capabilities. A review of logical criteria can lead to proper implementation of technical controls and definition of policy elements in the implementation phase.

3. Define *protection mode*.

   The IBM Security Network IPS can operate in three modes of protection as defined in 2.2.3, “Deployment options” on page 48. The cardio healthcare company selected to do a staged implementation of the IBM Security Network IPS technology. After the final stages of design are complete, the company selects a protection mode.

4. Examine the boundaries of communication, the communication flow as it ingresses and egresses zones, and functional considerations.

   The cardio healthcare company looks at the recommended IBM Security Network IPS policy and appliance models for network zones.

6.1.1 Network zones

The network for the cardio healthcare company is logically divided into separate zones that are protected by the IBM Security Network IPS appliances. This section examines the characteristics of the zone that influence the policy and the types of protection delivered to the zone.

Production Zone

The Production Zone for the cardio healthcare company is based out of the primary site IT data center in Phoenix, Arizona. The site has two high-speed redundant links to the carrier network of the Internet service provider and hosts the main connection to the Internet. Both the primary and secondary 10 GbE links are terminated at the demarcation point of the company in the data center. The connections terminate as a MiniGBIC fiber. The circuit is then connected to the core routing and switching 10 GbE infrastructure of the cardio healthcare company.

These network segments provide the following benefits:

- High-speed access to the *warm backup* site
- VPN encryption endpoints for each Intranet Zone branch office
- Snapshot replication of the database to the backup site in Raleigh, NC

The high-speed links are required to maintain the snapshot data replication to the backup site. The high availability (HA) network links of the cardio healthcare company are configured as primary and secondary connections (see Figure 6-1 on page 164). The company integrates the IBM Security Network IPS appliances into the existing HA solution. With the high availability mode, two comparable IBM Security Network IPS appliances can integrate into an existing HA environment and benefit from added protection during convergence if a failover occurs.

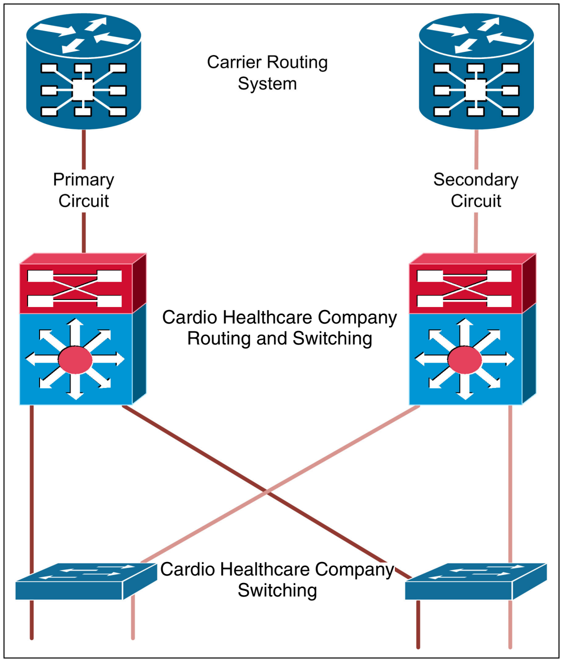

Carrier Routing System
Primary Circuit
Secondary Circuit
Cardio Healthcare Company Routing and Switching
Cardio Healthcare Company Switching

Figure 6-1 Existing infrastructure of the cardio healthcare company

HA-paired IBM Security Network IPS appliances have interfaces configured to mirror traffic to the peer IBM Security Network IPS appliance. This way, each IBM Security Network IPS appliance can have accurate entries in its state tables. The devices share state tables, so that both devices in the pair can be aware of each cleared, blocked, or quarantined connection. The information exchange minimizes disruption and allows for faster convergence, if a failover occurs while all established inspected sessions continue to exchange data.

The Production Zone also encompasses the backup site in Raleigh, NC. The backup site data center has no HA network structure. The backup site is used as a test and integration environment for application code development, quality assurance (QA) unit testing, and other IT projects. As a part of the software life cycle and as a preemptive or proactive security measure, the cardio healthcare company uses IBM Rational AppScan to perform web application scanning and testing to discover security vulnerabilities.

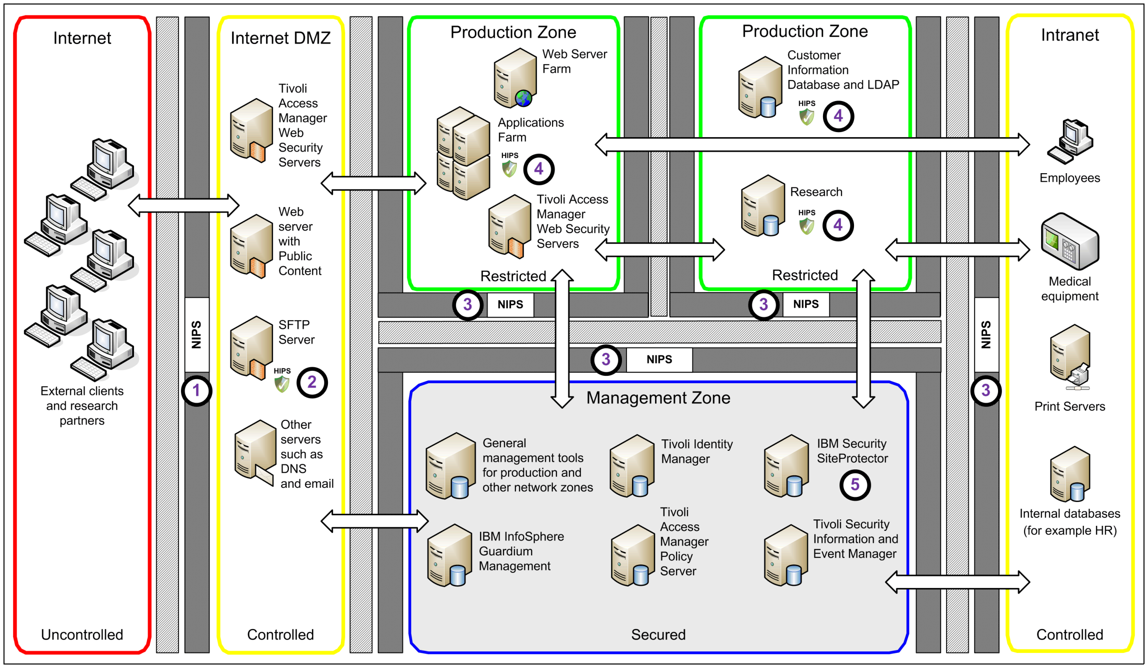
For more information about IBM Rational AppScan, see the IBM Redpaper publication *Improving Your Web Application Software Development Life Cycle's Security Posture with IBM Rational AppScan*, REDP-4530.

Management Zone

The Management Zone hosts the servers that provide command and control services to the various network agents deployed throughout the organization. The communication between the management systems and their agents occurs on a separate virtual local area network (VLAN; only routed internally) that is defined for management traffic. In this zone, the cardio healthcare company placed management servers for the following products:

- IBM Tivoli Identity Manager
- IBM InfoSphere Guardium
- IBM Tivoli Access Manager Policy Server
- IBM Tivoli Security Information and Event Manager
- IBM Security SiteProtector

This section focuses on only IBM Security SiteProtector and the IBM Security Network IPS appliances. IBM Security SiteProtector uses Agent Managers to ensure that policies are delivered to remote sites. For more information about Agent Managers and their deployment, see the IBM Redbooks publication, *IBM Security Solutions Architecture for Network, Server and Endpoint*, SG24-7581. The management systems listed previously are placed in the Management Zone as shown in Figure 6-2.



Internet
External clients and research partners
Uncontrolled
NIPS
1
Internet DMZ
Tivoli Access Manager Web Security Servers
Web server with Public Content
SFTP Server
HIPS
2
Other servers such as DNS and email
Controlled
Production Zone
Web Server Farm
Applications Farm
HIPS
4
Tivoli Access Manager Web Security Servers
Restricted
3
NIPS
Production Zone
Customer Information Database and LDAP
HIPS
4
Research
HIPS
4
Restricted
3
NIPS
3
NIPS
Management Zone
General management tools for production and other network zones
Tivoli Identity Manager
IBM Security SiteProtector
5
IBM InfoSphere Guardium Management
Tivoli Access Manager Policy Server
Tivoli Security Information and Event Manager
Secured
Intranet
Employees
Medical equipment
NIPS
3
Print Servers
Internal databases (for example HR)
Controlled

Figure 6-2 Management components in the Management Zone

Agent Manager deployment: To minimize complexity, Figure 6-2 on page 165 does not reflect the SiteProtector Agent Manager deployment in the controlled, secure, and restricted zones. Agent Manager is deployed at each physical location for policy management and event collection.

The solution for the cardio healthcare company defines which machines have access to the secured Management Zone. It also defines the firewall and policy rules that are implemented to restrict access for other devices or users.

Internet DMZ Zone

The Internet DMZ Zone serves as the entry point for all connections coming from the uncontrolled networks to the controlled networks of the cardio healthcare company. The management team divided this zone into two logical information zones:

- The DMZ web zone, which hosts the web-based servers for patients of the cardio healthcare company to access their own personal information
- The DMZ secured information zone, which hosts the host the secure File Transfer Protocol (SFTP) file transfer server

All network traffic originating from an external segment is initially intercepted by the network firewall, which has the responsibility of forwarding traffic to the proper IP address and port number. The Internet DMZ is the first line of defense against zero-day attacks and the propagation of known and unknown viruses, worms, and other types of malware. The IBM Security Network IPS appliance is deployed behind the firewall with a complementary set of firewall rules.

Government regulatory authorities require that the cardio healthcare company ensures that no personally identifiable information (PII) is stored on any server in the DMZ. The cardio healthcare company requires Data Loss Prevention (DLP) policies to always check for PII information. The company constantly updates and tunes these policies.

Intranet Zone

The cardio healthcare company has 10 remote medical clinics that connect to the headquarters by using a virtual private network (VPN). These segments connect to the production network to exchange, for example, confidential patient data. Each clinic operates its own network with local file and print servers, workstations, and clinic devices.

The cardio healthcare company implements the IBM Security Network IPS solution at the individual clinics with the following goals in mind:

- Protect against viruses, worms, and malware.
- Ensure that all patient information is encrypted and transmitted to the primary data center.
- Ensure that access to the human resource file server is restricted to authorized workstations.

6.1.2 Information zones

Some of the network zones (see Chapter 5, “Overview of scenario, requirements, and approach” on page 137) can be further segregated, for example, by the types of business functions that they provide. The cardio healthcare company groups its servers into information zones according to the types of business services they provide. Then it classifies the business services into broad categories of common characteristics. Policy management elements can then be derived from these categories and characteristics.

Production Zones

The Production Zone of the cardio healthcare company is functionally divided into two subzones:

- The Production Web Zone
- The Production Customer Database Zone

Technical controls are in place to control access to these critical systems. Access to these systems is strictly controlled by Tivoli Access Manager. Intrusion prevention protection is provided by the IBM Security Network IPS. The IBM Security Network IPS firewall verifies the network traffic configurations from the existing firewall of the cardio healthcare company.

The two subdomains require the company to define custom-based Web Application Protection (WAP) policies for the Production Web Zone. The Production Customer Database Zone contains the PII that must be protected. Access to this information is protected by IBM InfoSphere Guardium real-time database activity monitoring. The cardio healthcare company is adding a DLP solution to examine PII data as it traverses the different zones.

Production Web Zone

The Production Web Zone hosts the web application servers with the production application code. The backup site is used to test and develop new web-based applications or updates. The cardio healthcare company performs scheduled IBM Rational AppScan scans at both the primary and backup sites to identify vulnerabilities present in production and preproduction code. The events from Rational AppScan are sent to IBM Security SiteProtector. These events are used in the implementation phase to secure the web-based products. With this input, the company can better prepare web-based application protection policies for existing code vulnerabilities.

A network administrator at the cardio healthcare company can generate reports from IBM Security SiteProtector for the development team, quality assurance (QA) team, and the network security team. All of these groups can then take the input from these scans and create a comprehensive security policy. This policy can preemptively protect against current coding flaws and potential future production coding flaws that are not corrected in QA unit testing.

> **SiteProtector support for Rational AppScan:** The events from Rational AppScan can be propagated to SiteProtector by using the *SiteProtector Publisher Extension*. To download the extension, go to:
>
> `http://www.ibm.com/developerworks/rational/downloads/08/appscan_siteprotectorpublish/index.html`

The IBM Security Network IPS Web Application Security can provide preemptive protection against the following threats:

- Buffer overflow exploits
- CGI-BIN parameter manipulation
- Form/hidden field manipulation
- Forceful browsing
- Cross-site scripting (XSS)
- Command injection
- SQL injection
- Website defacement
- Well-known platform vulnerabilities
- Zero-day exploits

In the first implementation phase, the security administrator of the cardio healthcare company configures the base protection. Later the development, QA, and security team of the cardio healthcare company meets and generates recommendations for a more tuned policy.

For more information about implementing tuning input, see Chapter 7, “Phase 2: Policy tuning for IBM Security Network IPS” on page 211.

Production Customer Database Zone

The Production Customer Database Zone is the hub of communication for all of the other zones. The following communication flows influence design:

- The primary database sends snapshot replication data to the secondary database in the backup site.
- Each intranet site can add and retrieve information in the production database from Intranet Zone branch offices.
- Customers have access to their own personal information from the Internet DMZ Zone.
- Research personnel have access to research data from the Internet DMZ Secured Information Zone and Web Services Zone.

Special consideration must be taken at the ingress and egress points across the network. The steps to protect customer information for the cardio healthcare company affects other zones.

Internet DMZ Zone

The Internet DMZ Zone is divided into two information zones *DMZ Web Services* and *DMZ Secured Information*. The cardio healthcare company places technical controls within this zone that complement policies and policy elements in the Production Zone.

DMZ Web Services Zone

Three Internet-facing web services are provided in the Internet DMZ:

- The external facing website
- The external facing DNS server
- The email server

These services must all be considered attack vectors and represent high-risk areas for intrusion for the cardio healthcare company. The security administrator enables security signatures and firewalls on the IBM Security Network IPS appliances to mitigate these risks. The external facing resources have limited access to resources within the Production Web Zone. They do not need to make any inbound connections. Firewall rules are constructed to enforce these policies.

DMZ Secured Information Zone

The DMZ Secured Information Zone provides access to information that the cardio healthcare company must protect. Patient connections to the DMZ Secured Information Zone are authenticated by Tivoli Access Manager Web Security Servers. These servers enforce access control policies for clients and research partners accessing the applications and servers from the Internet.

The SFTP server, which is used to exchange research data and reports with the business partners in the pharmaceutical industry, is also located in the DMZ Secured Information Zone. No PII can be stored on servers in the DMZ. All PII data must be transmitted over a secure and encrypted connection.

The management team for the cardio healthcare company elected to place DLP policies to block any PII information from being sent to the research partners. The DLP policy for the company is also used to ensure that patient PII is properly encrypted by the servers that host the external connection. The DLP policies are complementary to the policies in the Production Zone.

6.1.3 Network protection mode selection

The cardio healthcare company selected to initially use *inline simulation* as the protection mode. Inline simulation mode allows monitoring of the network using the appliance without affecting traffic patterns. In addition to the traditional *block response*, the appliance uses a *quarantine response*. Packets are not dropped when these responses are started, and the appliance does not reset Transmission Control Protocol (TCP) connections by default. Events that might have been blocked are reported with the status *Simulated Block*. This mode is helpful for baselining and testing the security policy without affecting network traffic.

The implementation plan for the cardio healthcare company has three phases:

1. Define and implement policy elements in inline simulation mode.
2. Use input from detected network events to further tune the IBM Security Network IPS policies. For more information about the tuning of policies, see Chapter 7, “Phase 2: Policy tuning for IBM Security Network IPS” on page 211.
3. After the policy tuning phase is completed, switch to *inline protection* mode.

Not a one-time event: Policy tuning represents an ongoing task that should occur at regular intervals.

6.2 Implementation

The implementation phase begins by configuring IBM Security SiteProtector with groups for policy storage and management. The first step is to configure *Protection domains* based on the group structure. The cardio healthcare company team configures policies at the group level. Each IBM Security Network IPS appliance is deployed between network zones. The security team at the cardio healthcare company evaluates the criteria of the segments to be protected. It then selects an IBM Security Network IPS model based on matching the capabilities of the device to the business needs as discussed in the design phase.

After the model is selected, the policies are configured regarding five functional considerations:

- Installation
- Protection domains
- Configuring default policies
- Web application protection
- Data leakage protection

Policies are configured in IBM Security SiteProtector. After the IBM Security Network IPS appliances are registered on the IBM Security SiteProtector system, the IBM Security Network IPS inherits policies and configurations from the IBM Security SiteProtector groups.

6.2.1 Group definitions

The security team decided to manage the network zones of the cardio healthcare company by creating IBM Security SiteProtector groups that reflect the network zones. Figure 6-3 shows the IBM Security SiteProtector groups created by the security administrator.

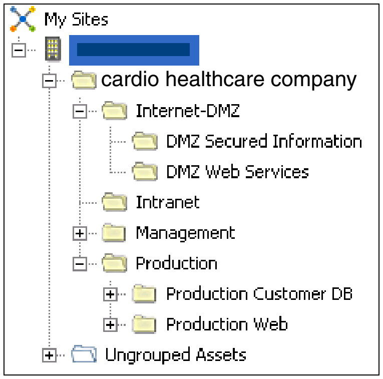


Figure 6-3 Group structure based on network zones

Each group serves the cardio healthcare company as policy repositories, which serve as versioning and change control. For more information about policy repositories, see 2.5.2, “Policy repositories” on page 68. For information about version controls, see 2.5.3, “Policy versioning” on page 69.

6.2.2 GX7800 implementation

The cardio healthcare company selected the GX7800 series appliance for its high-speed inspection speeds in 10G networks. The GX7800 is placed in the Production Zone backbone and uses the HA solution provided by the cardio healthcare company as illustrated in Figure 6-1 on page 164.

Installation of the GX7800

The security administrator at the cardio healthcare company unpacks the appliance and sees a device with a configuration similar to the example in Figure 6-4.

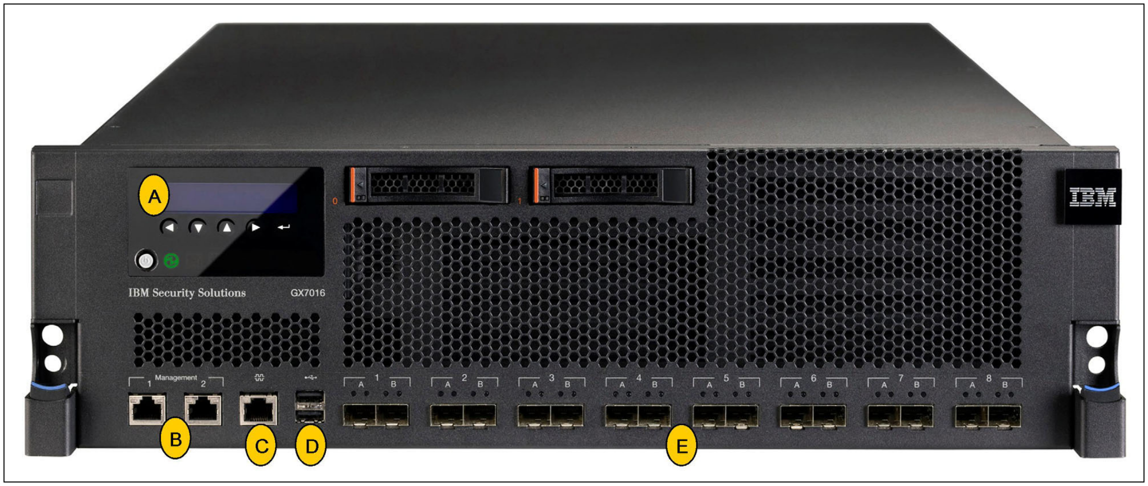


Figure 6-4 The GX7000 series appliance common configuration modules and ports

In the following detailed explanation of the different ports, the letters correspond to the items shown in Figure 6-4:

A LCD Controller Module

The LCD Controller Module is used for configuring the initial network, restarting or shutting down the appliance, and obtaining IPS version information. It is also used to inspect the serial number of the appliance, if desired.

B Management ports

The appliance offers two management ports. Management port 1 is used to communicate with the IPS local management interface (LMI) and IBM Security SiteProtector Management. This interface is placed in the Management Zone (and management VLAN) of the cardio healthcare company. Management port 2 is used exclusively for sending TCP Reset responses.

C Serial Console port

The Serial Console port is used for terminal-based setup and recovery.

D USB ports

The USB ports are used to retrieve data and to install firmware.

E Protected ports

The protected ports are used for either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention uses a pair of ports for each segment, and passive detection uses a single port for each segment.

Deviations on the front panel: The exterior appliance form can vary from the image shown in Figure 6-4 on page 172 depending on the model.

Requirements

As the administrator, you gather the necessary materials to install the appliance physically within a secure premise closet. The following peripheral devices are required to set up the GX7800:

- Power cables
- Serial console cable
- Ethernet crossover cable
- For each inline segment:
  - A pair of Ethernet cables (copper or fiber), straight-through or crossover, depending on the network type
  - A crossover adapter
- Additional Ethernet cables, as needed
- PC with a web browser and a network connection

Cabling the appliance

Best practice suggests that the cardio healthcare company keeps management and monitoring communication separate, so that network traffic can pass uninterrupted through the network interface card (NIC) of the appliance. First, the administrator connects the power cables to the appliance. The GX7800 series appliances have two power cords; both must be connected. Next, the management ports are assigned IP addresses in the management VLAN. Then the administrator connects the network cables to the protected ports.

The GX7800 series is chosen for this segment because of the HA requirement as explained in 6.1.1, “Network zones” on page 163. The segments provided by the ISP are 10 GbE links terminated as a MiniGBIC fiber. The core routing or switching layer has redundant links to the core switching layer of the cardio healthcare company as shown in Figure 6-1 on page 164.

The IBM Security Network IPS appliances are integrated into the existing network to provide protection within the existing network configuration. The GX7800 appliances forward traffic across to the redundant segments. Traffic connections are allowed to pass. Blocked connections are stored in both appliance state tables and cannot continue through the redundant link when convergence occurs. Figure 6-5 shows the implementation of the GX7800 devices into the existing configuration for the cardio healthcare company.

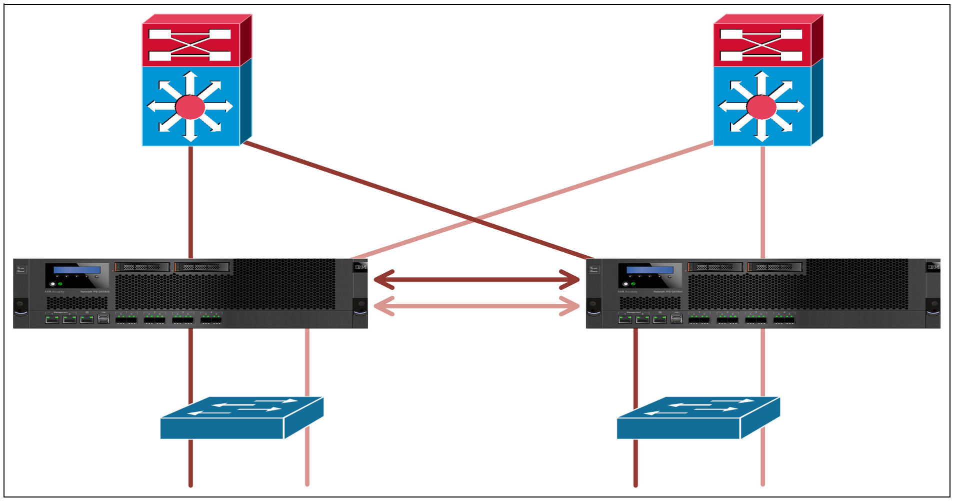


Figure 6-5 Cabling or redundant links and sharing of HA information

The appliances are connected by mirror links that consist of multiple connections over multiple ports. These mirror links pass all traffic that an appliance receives on its inline ports to the peer appliance, ensuring that the protocol analysis module on each appliance processes all of the network traffic. In addition, the appliances process asymmetrically routed traffic. This approach ensures that there is no gap in protection during failover.

Appliances in an HA pair process all packets received from inline ports and mirror ports. The appliances block attacks, report events, and generate responses for events occurring on their inline ports. They do not block, report, or generate responses for traffic occurring on mirror ports. The appliances process only mirror port traffic.

Figure 6-6 illustrates the port configuration of this setup.

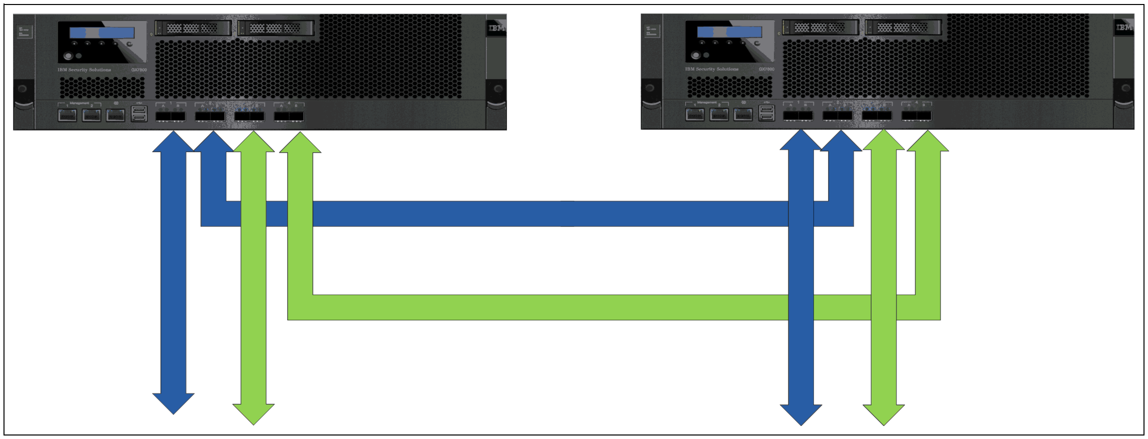


Figure 6-6 The second set of paired ports forwarding mirrored traffic over the links to the partner appliance

Both appliances see all traffic at all times. There is no lapse in security if a failover occurs. Both appliances maintain the current state. Therefore, if one HA network segment fails, the other appliance receives all packets on its inline ports. The network remains protected without interruption.

Configuring the initial network setup

As the network administrator, you can choose from three methods for the initial setup and configuration:

- Zero configuration networking
- Serial console
- LCD panel

After supplying the basic IP address information, you use the web-based configuration wizard to configure network settings for the IPS system.

Installation approach for the cardio healthcare company: For simplicity, only configuration by serial console and LCD only are addressed. For more information about *zero configuration network* setup, see "Configuring network settings for the Network IPS system" in the *Installation Guide*. This guide is available in the IBM Security Network IPS section of the IBM Security product Information Center at:

http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp

Configuring a network connection using a serial console

To configure a network connection using a serial console, as the administrator for the cardio healthcare company, complete the following steps:

1. Connect the serial console cable to the appliance and a computer to complete the initial configuration.
2. Connect to the appliance using hyperterminal or another terminal emulation program. Follow the instructions listed in the documentation for the chosen program.
3. Use the following settings to make the connection:
   - For Communication Port, select **(Typically) COM1**.
   - For Emulation, select **VT100**.
   - For Bits per second, enter `9600`.
   - For Data bits, enter `8`.
   - For Parity, select **None**.
   - For Stop bits, enter `1`.
   - For Flow control, select **None**.
4. At the unconfigured login prompt, complete the following actions:
   a. For Username, enter `admin`.
   b. For Password, enter `admin`.
   c. Press Enter.
5. Follow the instructions on the panel to complete the setup after logging in as admin.

Configuring a network connection using the LCD panel

To configure a network connection using the LCD panel, as the administrator for the cardio healthcare company, complete the following steps:

1. Using the LCD panel, enter the predetermined IP address for initial configuration when starting the appliance. The appliance has an address assigned to it. The administrator can use this IP address for setup or change it to a desired address.
2. On the LCD panel, press Enter.
3. On the LCD panel, when prompted to set up the network, click **OK**, and then press Enter.
4. Press Enter again.
5. On the IP address panel, change the IP address and then record the address (for configuration in a later step). Press Enter.
6. On the subnet mask panel, if the subnet mask and the default gateway need to be changed, change it here by using similar steps.

Tip: Press the Up and Down keys to select the numbers, and then press the right arrow key to move to the next field.

7. After all the fields are complete, press Enter.
8. Click **OK**, and then press Enter to confirm the selection.
9. After entering all of the network information, in the final confirmation panel, click **OK** to save all network information and to enable the Management port. Alternatively, click **Cancel** to discard any information.
10. After confirming the settings, record the temporary, case-sensitive password that the appliance generates. Recording this password is mandatory. The administrator must use this generated password to log in to the appliance.
11. Connect to the appliance by using a secure network connection and the IP address of the appliance to complete the initial configuration. At the unconfigured login prompt, complete the following steps:
    a. For Username, type `admin`.
    b. For Password, enter the case-sensitive password that the appliance generated
    c. Press Enter.
12. Follow the instructions on the panel to complete the setup.

IPv6 restrictions for LCD panel setup: IPv6 addresses cannot be used when using the LCD panel for setup. If you are using an IPv6 address, connect to the network by using a serial console.

Configuring the network settings

You configure the appliance by using a version of IBM Security Network IPS Setup (either web-based or on the appliance). You do this task after using zero configuration networking or after configuring a network connection by using a serial console or the LCD panel.

Completing the setup and connecting to the local management interface

As the administrator for the cardio healthcare company, depending on the method used to connect the appliance to the network, use the following procedures to access IBM Security Network IPS Setup:

> **License required:** IBM Security Network IPS Setup offers the option to upload a license. The appliance needs a license file to receive updates and run at full capability. For more information about how to upload the license, see “Installing the product license” on page 178.

1. Connect to the appliance using a secure network connection and the IP address of the appliance.
2. At the unconfigured login prompt, complete the following actions:
   a. For Username, enter `admin`.
   b. For Password, enter the case-sensitive password that the appliance generated in the LCD setup.
   c. Press Enter.
3. Follow the instructions on the panel to complete the setup.

Connecting to the IPS local management interface

The IPS LMI is the web-based utility used to monitor appliance status, to configure and manage settings, and to review and manage appliance activities.

As the administrator of the cardio healthcare company, you connect to the LMI by using the following steps:

1. Open a web browser and enter either of the following addresses:

   ```
   https://appliance IP address
   https://appliance host name
   ```

2. Log in with the user name `admin` and the applicable IBM Security Network IPS LMI password.

Installing the product license

To run at full capability, the IBM Security Network IPS requires a properly configured license file. As the administrator, you use the Licensing page in IPS LMI to view information about the status of the license file, including expiration dates. On the Licensing page, you can also access the License Information page, which includes information about how to acquire a current license.

Additional license setup information: For more information about acquiring and installing a product license and applying initial updates, see “Installing licenses and applying updates” in the *IBM Security Network Intrusion Prevention System Installation Guide*. You can find this guide in the IBM Security Network IPS section of the IBM Security product Information Center at:

`http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp`

The security team at the cardio healthcare company saved the license file to a secure location for uploading to the LMI and SiteProtector. As the administrator for the cardio healthcare company, you can install the license in the LMI or in IBM Security SiteProtector.

Installing a product license using the LMI

To install the license using the LMI, select **Manage System Settings** → **Updates and Licensing** → **Administration** (Figure 6-7).

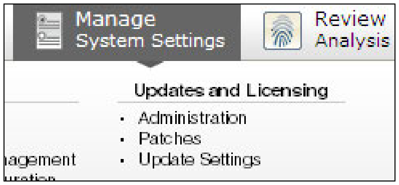


Figure 6-7 Updates and Licensing from the LMI

Installing a product license using IBM Security SiteProtector

To install licenses from IBM Security SiteProtector, select **Tools** → **Licenses** → **Agent/Module** (Figure 6-8).

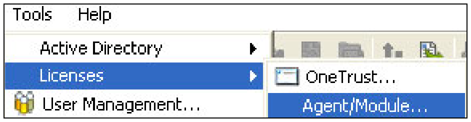


Figure 6-8 Updating the licenses from IBM Security SiteProtector

Installing an update policy

The IBM Security Network IPS appliance must be updated regularly to maximize performance, and ensure that it runs the most current security content, firmware, and data leakage signatures.

As the administrator for the cardio healthcare company, you can configure the policy in the LMI or in IBM Security SiteProtector.

Accessing the update settings in the LMI

To ensure that the appliance is always running the latest firmware and intrusion prevention updates, as the administrator, you can configure the IBM Security Network IPS to install updates automatically by using the LMI.

Go to the LMI, and then select **Manage System Settings** → **Updates and Licensing** → **Update Settings** (Figure 6-9).

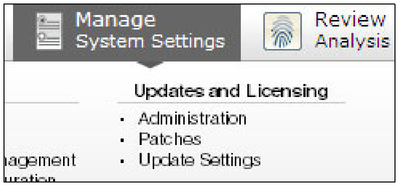
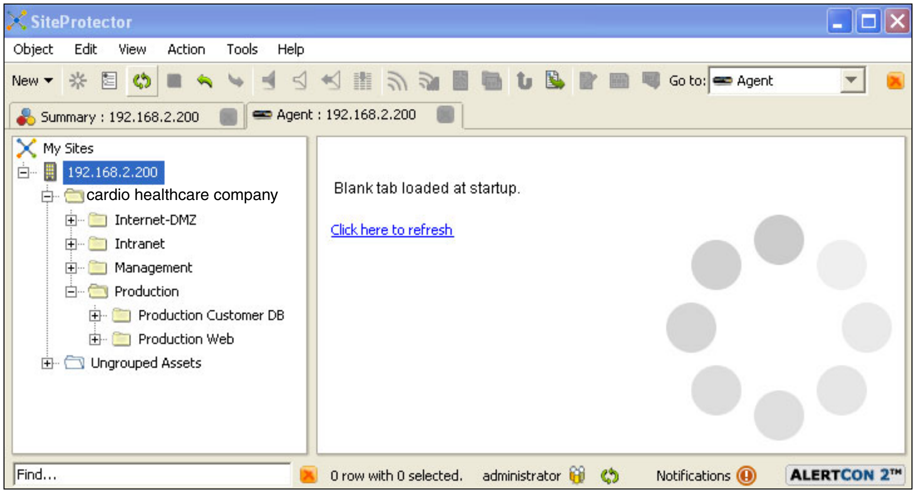


Figure 6-9 Configuring Update Settings

Accessing the update settings in IBM Security SiteProtector

After the policy is configured, it can be inherited by each IBM Security Network IPS appliance registered in IBM Security SiteProtector. Figure 6-10 shows the SiteProtector console.



Blank tab loaded at startup.

Click here to refresh

0 row with 0 selected.

Figure 6-10 SiteProtector console

Configuring the policy settings

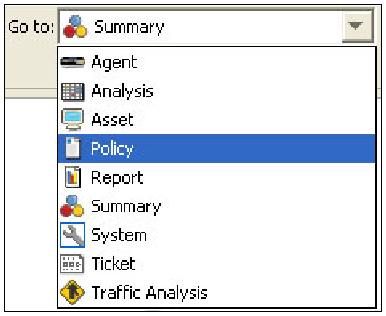
The change control policy of the cardio healthcare company specifies that updates must occur during a controlled window that begins at 3:00 a.m. (The time is relative to the physical location of the IBM Security Network IPS.)

The management team for the cardio healthcare company approved the automatic installation of security and content updates. The SiteProtector management system will download and installs security content updates at 3:00 a.m. without additional user intervention.

IBM Security Network IPS firmware updates occur during a more specific and scheduled change control window. The management team at the cardio healthcare company mandates the automatic download of firmware, but not automatic installation. Installing firmware updates causes the appliance to reboot. The management team for the cardio healthcare company requires a physical person to be present during the firmware installation. The policy mandates that manual firmware updates must be scheduled in the maintenance window of the organization.

As the administrator, you navigate to the SiteProtector console (Figure 6-10 on page 180), and then complete the following steps:

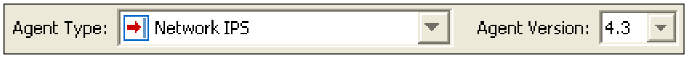
1. In the upper right corner of the console, in the **Go to** drop-down list (Figure 6-11), select **Policy**.



Go to: Summary

Figure 6-11 Selecting Policy from the Go to drop-down list

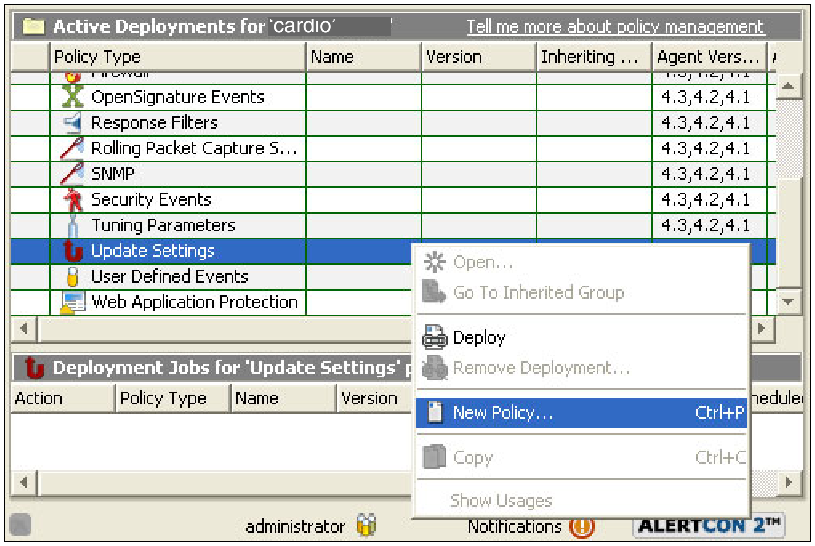
2. Select the agent version and type. In this scenario, the Agent Type is **Network IPS**, and the Agent Version (firmware) is **4.3**. Figure 6-12 shows the properly selected options from the drop-down lists.



Agent Type: Network IPS Agent Version: 4.3

Figure 6-12 Selecting the Agent Type

3. In the policy repository, right-click **Update Settings** (under Policy Type), and select **New Policy** (Figure 6-13).



Active Deployments for 'cardio'
Tell me more about policy management

Policy Type	Name	Version	Inheriting ...	Agent Vers...
OpenSignature Events				4.3,4.2,4.1
Response Filters				4.3,4.2,4.1
Rolling Packet Capture S...				4.3,4.2,4.1
SNMP				4.3,4.2,4.1
Security Events				4.3,4.2,4.1
Tuning Parameters				4.3,4.2,4.1
Update Settings				
User Defined Events				
Web Application Protection				

Figure 6-13 Creating a policy

4. On the **Update Settings** tab, configure the update policy based on the requirements set by the management team for the cardio healthcare company described in “Configuring the policy settings” on page 180.

> **Policy dialog boxes:** The policy dialog boxes are the same in the LMI and in IBM Security SiteProtector. In this example, consider storing policies in SiteProtector for centralized management, backups, and rapid policy deployments to the entire cardio healthcare company enterprise.

In this example, the administrator completes the following steps:

a. Select the **Check for Updates daily or weekly option**.

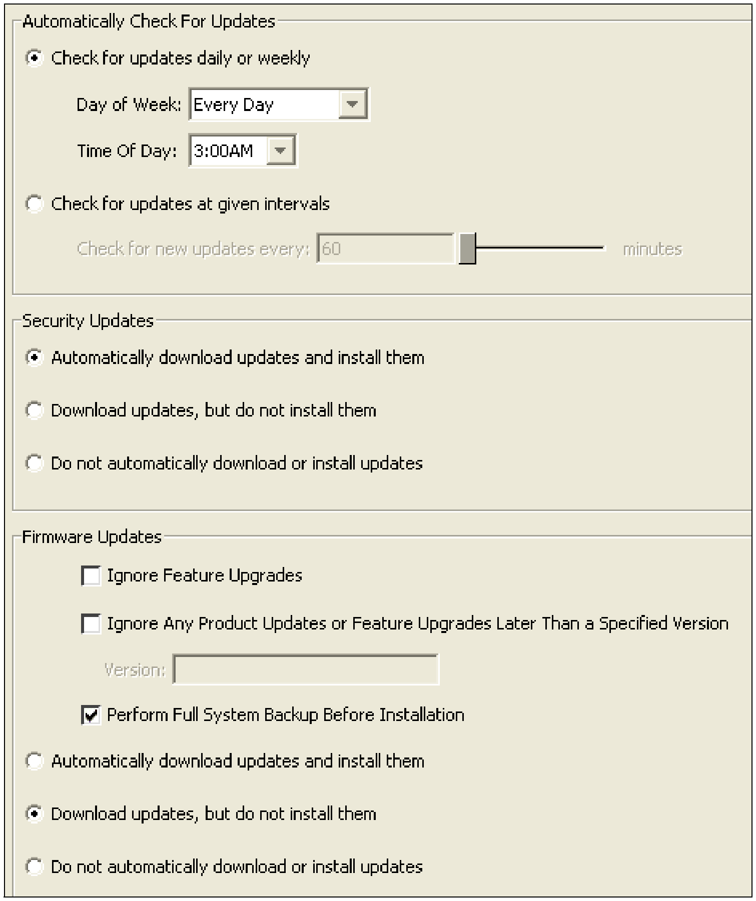
b. For Day of Week, select **Every Day**.

c. For Time Of Day, select **3:00AM**.

d. Under Security Updates, select **Automatically download updates, but do not install them**.

e. Under Firmware Updates, select the **Perform Full System Backup Before Installation** check box. Then select **Download updates, but do not install them**.

Figure 6-14 shows the resulting policy.



Automatically Check For Updates

● Check for updates daily or weekly

Day of Week: Every Day

Time Of Day: 3:00AM

○ Check for updates at given intervals

Check for new updates every: 60 minutes

Security Updates

● Automatically download updates and install them

○ Download updates, but do not install them

○ Do not automatically download or install updates

Firmware Updates

□ Ignore Feature Upgrades

□ Ignore Any Product Updates or Feature Upgrades Later Than a Specified Version

Version:

☑ Perform Full System Backup Before Installation

○ Automatically download updates and install them

● Download updates, but do not install them

○ Do not automatically download or install updates

Figure 6-14 Configure update policy

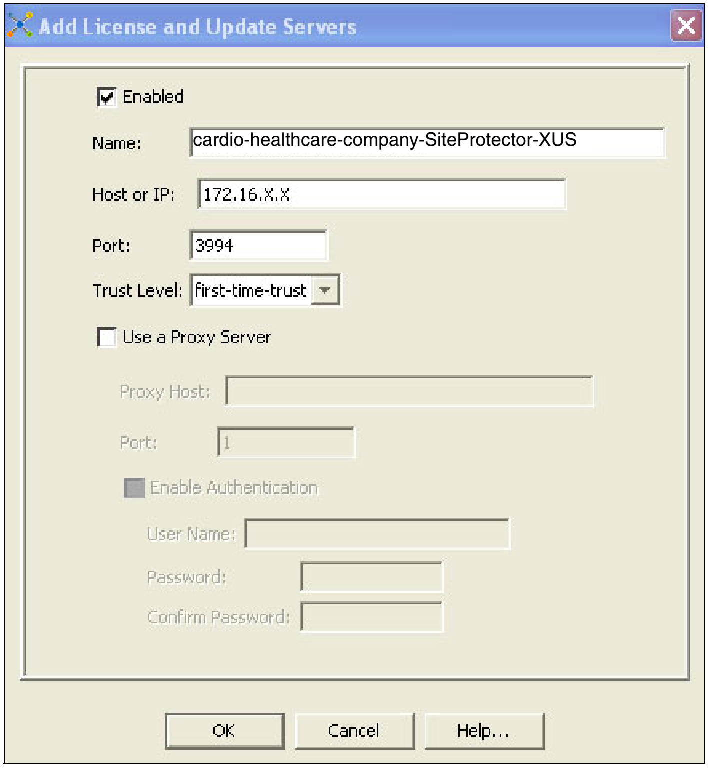
5. On the **Update Settings** tab, complete or change the settings. Select **Update Settings Policy** → **License and Update Servers**.
6. Click the **Add** icon (green plus sign).

7. Configure the address of an upstream update server. In this example, we choose to have all of the agents retrieve updates from the update server that is embedded into the SiteProtector management system.

   The administrator completes the following steps in the Add License and Update Servers dialog box:

   a. Select the **Enabled** check box.
   b. For Name, enter `cardio-healthcare-company-SiteProtector-XUS`.
   c. For Host or IP, enter `172.16.x.x` (make sure to use a valid IP address for your organization).
   d. For Port, enter `3994`.
   e. For Trust Level, select **first-time-trust**.
   f. Click **OK** to finalize the update policy configuration.

   Figure 6-15 shows the resulting configuration.



Add License and Update Servers

☑ Enabled

Name: cardio-healthcare-company-SiteProtector-XUS

Host or IP: 172.16.X.X

Port: 3994

Trust Level: first-time-trust

☐ Use a Proxy Server

Proxy Host:

Port: 1

☐ Enable Authentication

User Name:

Password:

Confirm Password:

Figure 6-15 Redirecting updates to the SiteProtector update server

Creating protection domains

With protection domains, the cardio healthcare company can create and apply security or user-defined policies for different network segments to a single appliance. Protection domains act similar to virtual sensors, as though several appliances are monitoring the network. The cardio healthcare company defines protection domains by interfaces, VLANs, or IP addresses. Protection domains are used to monitor groups of network segments from a single IBM Security Network IPS appliance, using global security or user-defined policies that centralize intrusion prevention.

The cardio healthcare company uses protection domains on the IBM Security Network IPS appliance to configure and apply policies to deploy across groups of network assets or globally across the organization. As the administrator of the company, follow these steps:

1. Navigate through the SiteProtector menu to the **Policy Management** tab. Select the agent type and firmware.
2. Navigate to the site-level group. Expand **cardio healthcare company** → **Default Repository** → **Shared Objects**, and then select **Protection Domains** (Figure 6-16).

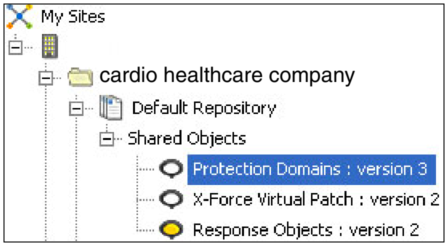

My Sites
cardio healthcare company
Default Repository
Shared Objects
Protection Domains : version 3
X-Force Virtual Patch : version 2
Response Objects : version 2

Figure 6-16 Navigating to Protection Domains

3. Right-click **Protection Domains**, and then select **Open**.
4. Click the **Add** icon (green plus sign).

5. In the Edit Protection Domains dialog box, configure the protection domain options:

   a. Select the **Enabled** check box to enable the protection domain.

   b. Add a unique and descriptive comment for the domain, such as `Cardio-Internet_DMZ-SEC-Info` (Figure 6-26 on page 197).

   c. Select the physical adapters on the device to assign to the protection domain.

   > **Number of available ports:** The appliance dialog box might show more ports than are available on the physical device. The IBM Security Network IPS device that subscribes to the policy ignores port configurations that do not apply to the specific appliance. For example, the appliance might allow configuration of eight adapter ports, even though only four ports are available on the appliance.

   d. Bind the adapter to the monitored traffic. To configure the monitored traffic, use assign any combination of the following criteria to a protection domain interface:

      - 802.1q VLAN tags
      - IPv4 addresses
      - IPv6 address ranges

   e. Click **OK**.

6. Deploy the settings to a group when configuring through SiteProtector.

The GX7800 installations are in the backbone of the Production Zone for the cardio healthcare company. The production protection domain is assigned to the monitoring adapters. These settings apply to all interfaces on any VLANs and on any IPv4 addresses, IPv6 addresses, or both.

Configuring the X-Force Virtual Patch settings

The cardio healthcare company uses the X-Force Virtual Patch settings to preemptively shield vulnerabilities from exploitation regardless of a software patch on the target system.

As the administrator, you can configure the policy to apply the block response to the latest exploits and threats across the enterprise:

1. Navigate through the SiteProtector menu to the **Policy Management** tab, and then select agent type and firmware.

2. Navigate to the site-level group. Expand **cardio healthcare company** → **Default Repository** → **Shared Objects**, and then select **X-Force Virtual Patch** (Figure 6-17 on page 187).

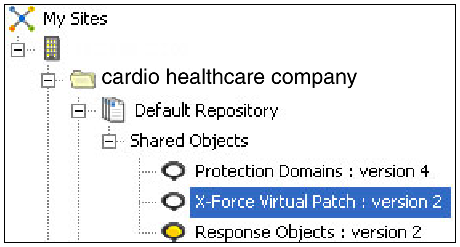
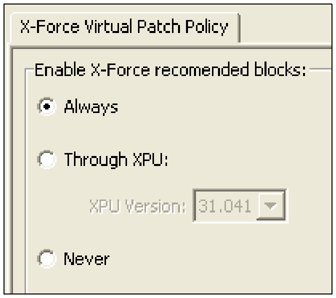

My Sites
cardio healthcare company
Default Repository
Shared Objects
Protection Domains : version 4
X-Force Virtual Patch : version 2
Response Objects : version 2

Figure 6-17 Selecting the X-Force Virtual Patch configuration

3. Right click **X-Force Virtual Patch**, and then select **Open**.
4. Configure the default block response using one of the following blocking options:
   - Always
   - Through XPU
   - Never

   Figure 6-18 shows that the **Always** radio button selected from the recommended block settings.



X-Force Virtual Patch Policy

Enable X-Force recomended blocks:

● Always

○ Through XPU:

XPU Version: 31.041

○ Never

Figure 6-18 The three options for X-Force Virtual Patch settings

By using the *Through XPU* option, an organization can test new signatures in a controlled lab environment before placing a block response in production. The cardio healthcare company elected to use inline simulation as the initial protection mode for the IBM Security Network IPS appliances.

The inline simulation mode issues alerts on triggers for a block based on the policies that are configured. These alerts give the cardio healthcare company insight into how the security policy affects the networking environment before switching to protection mode.

For a description of the types of tuning activities that the administrator of the company takes before switching to inline protection mode, see Chapter 7, “Phase 2: Policy tuning for IBM Security Network IPS” on page 211.

Configuring the high availability policy in IBM Security SiteProtector

To configure the high availability mode, the administrator of the cardio healthcare company selects the Security Interfaces policy by locating the registered agent within the SiteProtector management console. In the following example, the host name of the appliance is *GX7800-Cardio*.

The cardio healthcare company uses the Sensor High Availability Mode area to configure the IBM Security Network IPS appliance for HA support:

1. Locate the Security Interfaces policy under a registered agent in SiteProtector. Figure 6-19 shows **Security Interfaces** selected for one of the GX7800s in the HA pair.
2. Right-click **Security Interfaces**, and select **Open**.

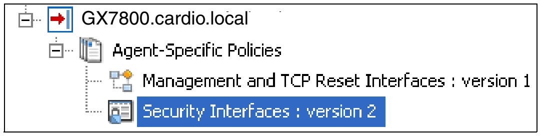

GX7800.cardio.local
Agent-Specific Policies
Management and TCP Reset Interfaces : version 1
Security Interfaces : version 2

Figure 6-19 Selecting Security Interfaces to configure HA policies

3. In the Sensor High Availability Mode area (at the bottom of the policy page), select **HA Simulation mode**. This setting places all monitoring adapters into inline simulation mode.

> **HA synchronization for updates:** Both appliances in an HA configuration must be registered to the same SiteProtector group. IBM Security SiteProtector can then synchronize appliance updates, including XPUs and policy updates.

4. Save and deploy the settings to the agent after configuration in SiteProtector.

Configuring a Web Application Protection policy

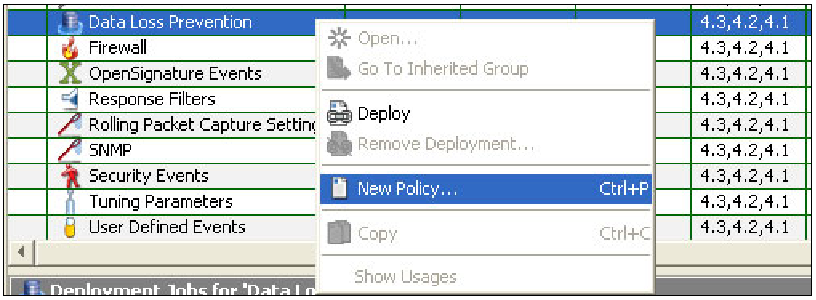
The Web Application Protection policy is enabled within this zone to detect attacks and suspicious traffic in the Production Web domain. The policies that are enabled here can alert the security staff for the cardio healthcare company about vulnerabilities in production code and threat vectors used to access protected information. The input from the Web Application Protection policy provides the necessary feedback for the cardio healthcare company to have an improved security posture. The policy is configured by taking the following steps:

1. In the LMI, select **Secure Protection Settings**. Then select **Security Modules → Web Application Protection**.
2. On the Web Application Protection policy page, in the Web Protection Categories table, enable all of the Web Protection Categories.
3. Deploy settings to a group when configuring through SiteProtector.

Configuring a Data Loss Prevention policy

As the administrator for the cardio healthcare company, configure the Data Loss Prevention policy by using the following steps:

1. From the policy repository, highlight and then right-click the **Data Loss Prevention policy**. Select **New Policy** (Figure 6-20).



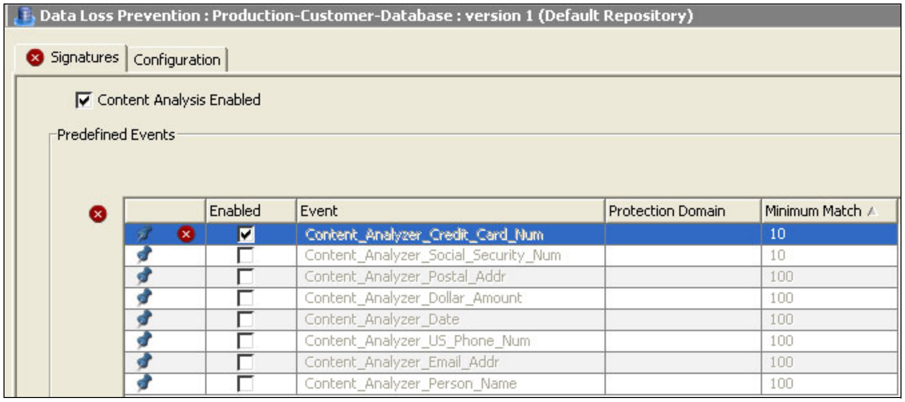
Data Loss Prevention	4.3,4.2,4.1
Firewall	4.3,4.2,4.1
OpenSignature Events	4.3,4.2,4.1
Response Filters	4.3,4.2,4.1
Rolling Packet Capture Settinç	4.3,4.2,4.1
SNMP	4.3,4.2,4.1
Security Events	4.3,4.2,4.1
Tuning Parameters	4.3,4.2,4.1
User Defined Events	4.3,4.2,4.1

Figure 6-20 Creating a DLP policy object

2. On the Data Loss Prevention policy page, complete the following steps on the **Signatures** tab (Figure 6-21):

   a. Select the **Content Analysis Enabled** option.

   b. In the Predefined Events table, select **Content_Analyzer_Credit_Card_Num**.



Data Loss Prevention : Production-Customer-Database : version 1 (Default Repository)

☑ Content Analysis Enabled

Predefined Events

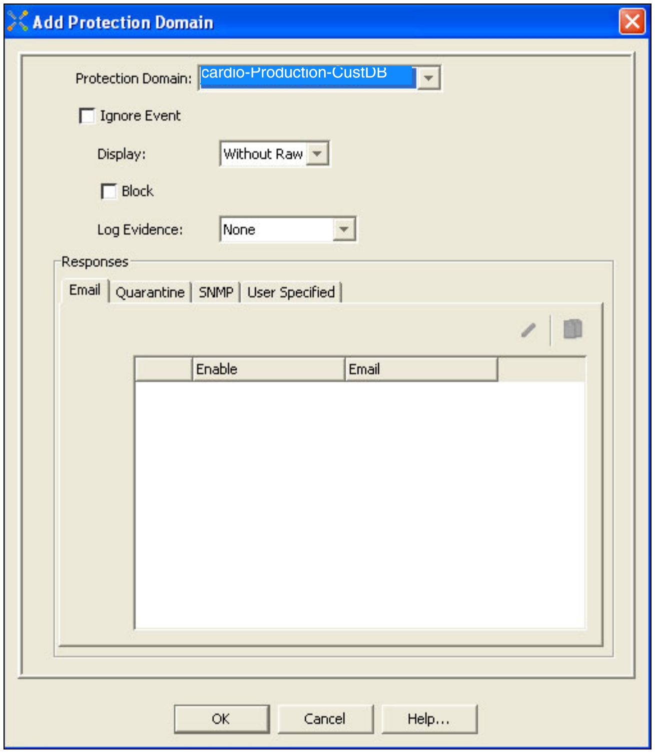
	Enabled	Event	Protection Domain	Minimum Match
	☑	Content_Analyzer_Credit_Card_Num		10
	□	Content_Analyzer_Social_Security_Num		10
	□	Content_Analyzer_Postal_Addr		100
	□	Content_Analyzer_Dollar_Amount		100
	□	Content_Analyzer_Date		100
	□	Content_Analyzer_US_Phone_Num		100
	□	Content_Analyzer_Email_Addr		100
	□	Content_Analyzer_Person_Name		100

Figure 6-21 Assigning each policy element to a protection domain

3. Click the **Edit** icon.

4. Click the **Add new row** icon.

5. In the Add Protection Domain dialog box (Figure 6-22), from the **Protection Domain** drop-down list, select **cardio-Production-CustDB**. Then click **OK**.



Add Protection Domain

Protection Domain: cardio-Production-CustDB

□ Ignore Event

Display: Without Raw

□ Block

Log Evidence: None

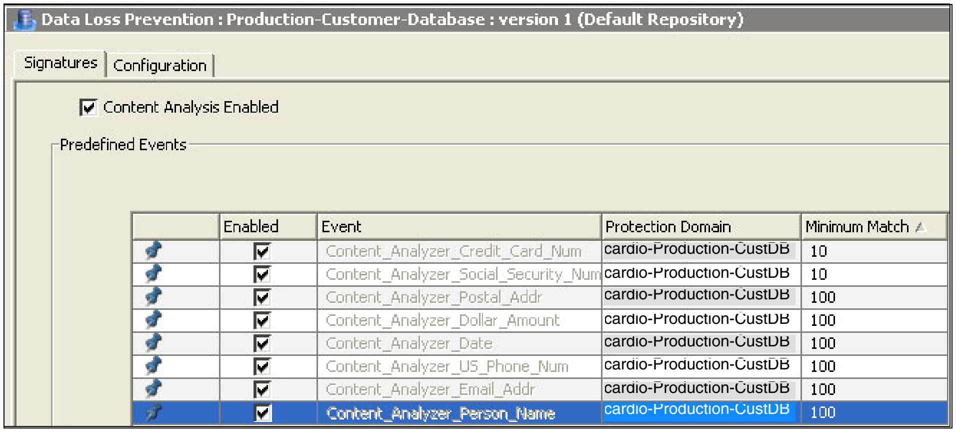
Responses

Enable	Email

Figure 6-22 Add Protection Domain dialog box

6. In the Edit Predefined Events dialog box, click **OK**.
7. Verify that the Content_Analzyer_Credit_Card_Num event is **Enabled** and assigned to the cardio-Production-CustDB protection domain.

8. Repeat these steps for all other types of PII (Figure 6-23).



Data Loss Prevention : Production-Customer-Database : version 1 (Default Repository)

☑ Content Analysis Enabled

Predefined Events

	Enabled	Event	Protection Domain	Minimum Match
	☑	Content_Analyzer_Credit_Card_Num	cardio-Production-CustDB	10
	☑	Content_Analyzer_Social_Security_Num	cardio-Production-CustDB	10
	☑	Content_Analyzer_Postal_Addr	cardio-Production-CustDB	100
	☑	Content_Analyzer_Dollar_Amount	cardio-Production-CustDB	100
	☑	Content_Analyzer_Date	cardio-Production-CustDB	100
	☑	Content_Analyzer_US_Phone_Num	cardio-Production-CustDB	100
	☑	Content_Analyzer_Email_Addr	cardio-Production-CustDB	100
	☑	Content_Analyzer_Person_Name	cardio-Production-CustDB	100

Figure 6-23 All enabled DLP policies

6.2.3 GX5208 with Active Bypass implementation

The GX5208 series appliances are deployed between the Internet DMZ Zone and the Production Zone. The GX5200 series appliances are places in simulation mode between the zones and configured with an external active bypass unit. This section provides an overview of the installation and base configuration instructions for the IBM Security Network IPS and the external bypass unit.

Installation of the GX5208

The security administrator at the cardio healthcare company unpacks the appliance and sees a device with a configuration similar to the example in Figure 6-24.

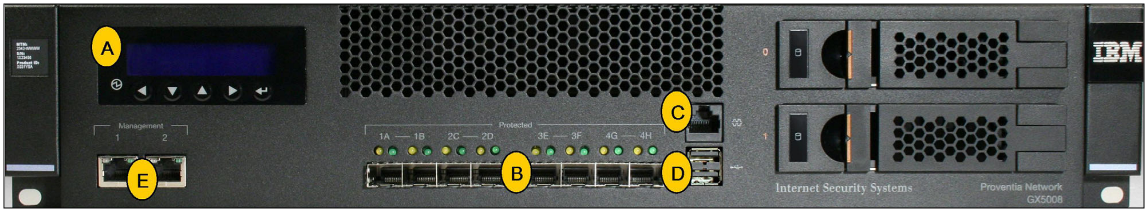


Figure 6-24 The GX5208 series appliance common configuration modules and ports

In the following detailed explanation of the different ports, the letters correspond to the items shown in Figure 6-24 on page 192:

A LCD Controller Module

This module is used for initially configuring the network, restarting or shutting down the appliance, and obtaining IPS version information.

B Protected ports

The protected ports are used for inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention always uses a pair of ports for each segment.

> **Deviations on the front panel:** The port configuration might look slightly different depending on the combination of fiber and copper interfaces selected.

C Serial Console port

The Serial Console port is used for terminal-based setup and recovery.

D USB ports

The USB ports are used to retrieve data and to install firmware.

E Management ports

- Management port 1 is used to communicate with IBM Security SiteProtector.
- Management port 2 is used exclusively for sending TCP Reset responses.

Cabling the appliance

To properly cable the appliance, as the administrator, follow these steps:

1. Connect the power cable or cables to the appliance. If the appliance has two power cords, you must connect both of them.
2. Connect Management port 1 to the management VLAN.

   The use of the management VLAN separates management traffic from the network (allows regular network traffic to pass on the monitored interfaces). Management port 2 is the TCP Reset port. This port must be on the same network or VLAN as the regular traffic.
3. For an SFP-capable appliance: Populate the protected ports with SFP modules as necessary. For each port pair, SFP modules must be the same media type. For example, if port 1A is copper (TX), port 1B must also be copper (TX).
4. Connect the network cables to the protected ports. To run the appliance in passive mode, connect only the first protected port in the pair to the network.

5. From the appliance, ping to a computer on the other side to verify that traffic passes.
6. Turn on the appliance.

The IBM Security Network Active Bypass unit

The IBM Security Network Active Bypass unit is an external device that uses active bypass functions to ensure that network traffic continues to flow if the appliance fails or loses power. The Network Active Bypass unit provides seamless failover and extensive management capabilities. It also provides four independent gigabit Ethernet interface segments with various media combinations. The cardio healthcare company selected to install the active bypass unit with the GX5208 Series Network IPS appliances.

Figure 6-25 shows the IBM Security Systems Active Bypass Unit with both copper and fiber interfaces.

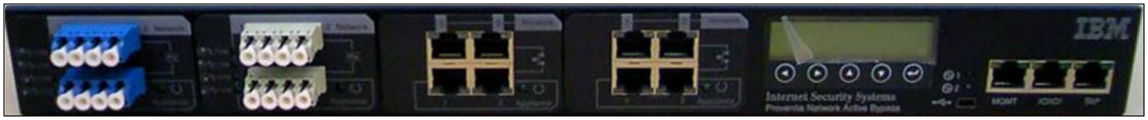


Figure 6-25 The IBM Security Network Active Bypass unit

For more information about the IBM Security Network Bypass unit, see the web page at:

http://www.ibm.com/software/tivoli/products/network-active-bypass/

Configuring and deploying the Network Active Bypass unit

As the administrator for the cardio healthcare company, you place the Network Active Bypass unit and the IBM Security Network IPS appliances in the rack and then connect the cables to the IBM Security Network IPS appliances. Then you provide redundant power by following these steps:

1. Connect the power cables to the Network Active Bypass unit and to two different power sources (for added redundancy).
   a. Plug the dc connector of each ac adapter into the Network Active Bypass unit.
   b. Plug one of the power cables into an ac outlet. Plug the other power cable into an ac outlet serviced by a different ac feed.
   c. Check the power LEDs to confirm that the Network Active Bypass unit is receiving power.

2. Use a browser to access the LMI of the bypass unit, and then log in.

> **Local management interface:** The IBM Security Network Active Bypass unit has an LMI that allows for further configuration of the unit. For information about the advanced configurations and capabilities, see the following Network Active Bypass guides:
>
> - *IBM Security Network Active Bypass User Guide*
>
>   http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.ips.doc/pdfs/ProvNetworkActiveBypassUG.pdf
>
> - *IBM Security 10G Network Active Bypass User Guide*
>
>   http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.ips.doc/pdfs/IBMSec_10G_NAB_UG.pdf

3. Verify that the Network Active Bypass unit is passing traffic.
4. Use the management interface to set the segment configuration. (This process maps the ports on the appliance and sets bypass tolerances.)

Unique policies to the Internet DMZ Zone

This section highlights the policies that are unique for the deployment of the GX5208 appliance.

Complementary firewall rules for the Internet DMZ Zone

The cardio healthcare company chose to implement a complementary base of firewall rules in the Internet DMZ Web Services Zone. The rule base is complementary to the existing firewall that is already deployed in this zone. It is also a part of the layered defense in depth from external threats.

The administrator identified the need to create two sets of firewall rules that are complementary to the border firewall. The first set of rules monitor for implicitly allowed traffic. Any traffic originating from the untrusted Internet Zone that enters the Internet DMZ Zone (from VLAN or any network segment that includes the firewalls internal interface) flows through this IBM Security Network IPS appliance. The administrator selects **Protect** as the response for these firewall rules. Packets that match the firewall rule are processed by the Protocol Analysis Module (PAM).

Firewall rules and protection domains: Firewall rules have many policy elements in common with protection domains. Both firewall rules and protection domains use VLAN tags and interface ports to configure what to protect. Use care when creating firewall rules to ensure that they complement protection domains. Firewall responses, such as *Monitor* and *Protect*, can affect protection domain coverage.

This configuration enables matching packets to be processed by normal responses, such as (but not limited to) logging, the block response, and quarantine responses. After policy tuning occurs, the protection mode is switched from *inline simulation* to *inline protection*. The second rule set contains the explicit *deny* rules. These rules block any traffic originating from the untrusted Internet Zone that attempts to enter the Internet DMZ Zone (from any VLAN or any network segment that includes the firewalls internal interface). This configuration alerts the administrator for the cardio healthcare company of any traffic that can traverse a poorly written border firewall rule.

Auditing the firewall: A rule base that is complementary to the firewall rule provides the management team for the cardio healthcare company a means to audit the success and failure of the security rule base of a firewall appliance. By using the triggered events, the management team can create audit reports in IBM Security SiteProtector.

Internet DMZ protection domain

The DMZ secured information zone (within the Internet DMZ) has a protection domain created. This protection domain is used within the definition of the DLP policy. This definition assists in the protection of PII.

As the administrator of the cardio healthcare company, create the protection domain by using the following steps:

1. Right-click the protection domains, and then select **Open**.
2. Click the **Add** icon (green plus sign).
3. In the Edit Protection Domains dialog box (Figure 6-26 on page 197), configure the protection domain options:
   a. Select the **Enabled** check box to enable the protection domain.
   b. Add a unique and descriptive comment for the domain.
   c. Select the physical adapters on the device to assign to the protection domain.

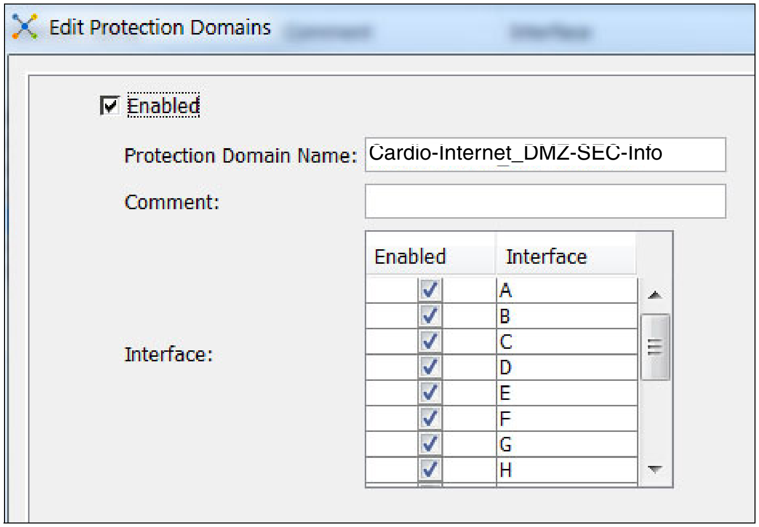
Available ports: The appliance dialog box might show more ports than are available on the physical device. The IBM Security Network IPS device that subscribes to the policy ignores the port configurations that do not apply to the specific appliance. For example, the dialog box might allow the configuration of eight adapter ports although only four ports are available on the appliance.

d. Bind the adapter to the monitored traffic. To configure the monitored traffic, use assign any combination of the following criteria to a protection domain interface:

- 802.1q VLAN tags
- IPv4 addresses
- IPv6 address ranges

e. Click **OK**.

Figure 6-26 shows the creation of the protection domain.



☑ Enabled

Protection Domain Name: Cardio-Internet_DMZ-SEC-Info

Comment:

Interface:

Enabled	Interface
☑	A
☑	B
☑	C
☑	D
☑	E
☑	F
☑	G
☑	H

Figure 6-26 Edit Protection Domains dialog box

Internet DMZ update policy

The security administrator configured the update policy to perform updates every day at 3:00 a.m. The IBM Security Network IPS appliance downloads and installs security content updates automatically. Firmware updates are downloaded only. The management team for the cardio healthcare company dictated that firmware updates cannot be automatically installed because they can cause the appliance to restart.

The IBM Security Network IPS update policy is the same for GX5208 appliances (deployed in the Internet DMZ Zone) as it is for the GX7800 appliances (deployed in the Production Zone). The update policy is applied to the top-level SiteProtector group and can be inherited by the IBM Security Network IPS agents by using group membership.

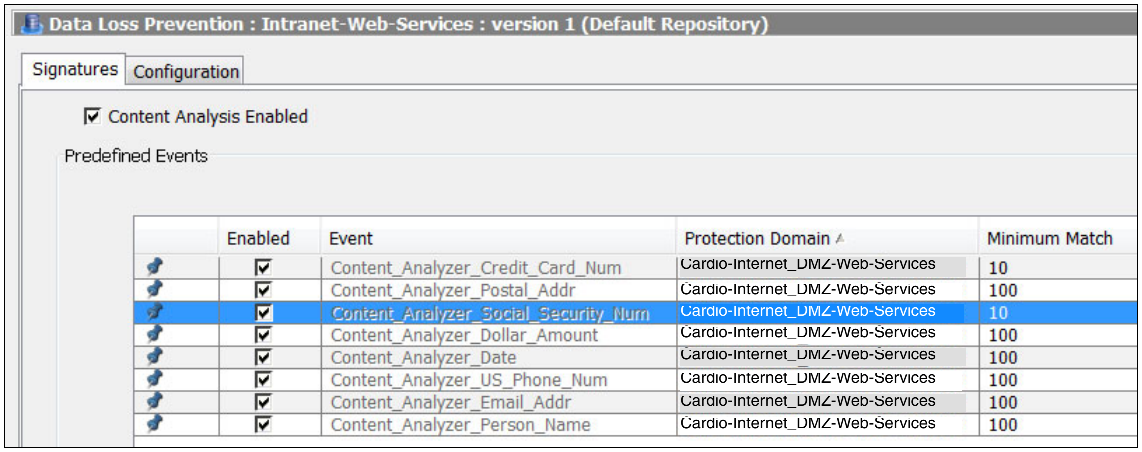
Internet-DMZ Web Application Protection

WAP uses attack signatures, audit signatures, and parameter names (keywords) from the PAM engine to provide overall protection against web application-based security attacks. The WAP policy is applied to the Cardio-Internet_DMZ-Web-Services protection domain, and all of the signatures are enabled, except the client-side attacks. Client-side attacks can exploit the trust relationship between a user and the websites they visit. In this zone, the focus is on *code vulnerabilities* from the production and preproduction environments.

> **Protection domain and WAP:** You can apply a WAP policy, and it can be active, only on one protection domain at a time.

Intranet DMZ Data Loss Prevention

As the administrator of the cardio healthcare company, you create the Data Loss Prevention policies on the **Signatures** tab. This tab binds the signatures to a protection domain (Figure 6-27).



Data Loss Prevention : Intranet-Web-Services : version 1 (Default Repository)

☑ Content Analysis Enabled

Predefined Events

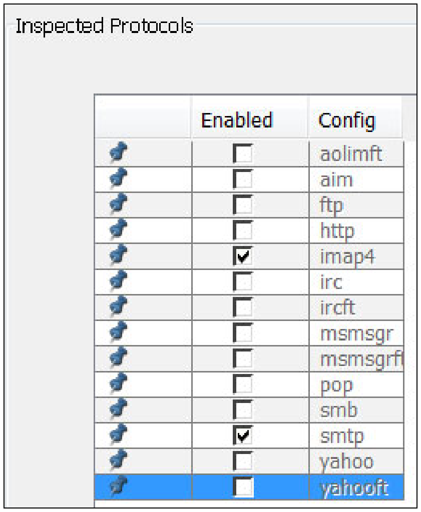
	Enabled	Event	Protection Domain	Minimum Match
	☑	Content_Analyzer_Credit_Card_Num	Cardio-Internet_DMZ-Web-Services	10
	☑	Content_Analyzer_Postal_Addr	Cardio-Internet_DMZ-Web-Services	100
	☑	Content_Analyzer_Social_Security_Num	Cardio-Internet_DMZ-Web-Services	10
	☑	Content_Analyzer_Dollar_Amount	Cardio-Internet_DMZ-Web-Services	100
	☑	Content_Analyzer_Date	Cardio-Internet_DMZ-Web-Services	100
	☑	Content_Analyzer_US_Phone_Num	Cardio-Internet_DMZ-Web-Services	100
	☑	Content_Analyzer_Email_Addr	Cardio-Internet_DMZ-Web-Services	100
	☑	Content_Analyzer_Person_Name	Cardio-Internet_DMZ-Web-Services	100

Figure 6-27 The DLP signatures bound to the Cardio-Internet_DMZ-Web-Services protection domain

Then you select the **Configuration** tab to bind the individual signatures to protocols.

Two sets of DLP policies are defined on the two different protection domains. The first DLP policy binds to the DMZ web services information zone. This policy is configured to protect any PII that flows to the external facing web or email servers in the Internet DMZ.

These signatures are specifically configured to examine the Internet Message Access Protocol (IMAP) and Simple Mail Transfer Protocol (SMTP) as shown in Figure 6-28.



Inspected Protocols

	Enabled	Config
📌	□	aolimft
📌	□	aim
📌	□	ftp
📌	□	http
📌	☑	imap4
📌	□	irc
📌	□	ircft
📌	□	msmsgr
📌	□	msmsgrf
📌	□	pop
📌	□	smb
📌	☑	smtp
📌	□	yahoo
📌	□	yahooft

Figure 6-28 IMAP and SMTP inspected for DLP

The second set of DLP policies is defined to prevent PII from flowing to the research partners by inspecting traffic before it is encrypted at the SFTP server. If PII is detected in the transmission, the connection is blocked. The administrator for the cardio healthcare company verifies that the paired ports in the protection domain are in line between the Production Customer Database zone and that the SFTP Server is in the Internet DMZ. These signatures are configured to examine the Server Message Block (SMB) protocol.

6.2.4 GX4004 implementation

The cardio healthcare company has 10 remote medical clinics that connect to the headquarters by using a VPN connection. Each of the remote medical clinics is tied into the Intranet Zone. These segments connect to the Production Zone to upload confidential patient data over the VPN connections. Each clinic operates its own network with local file and print servers, workstations, and clinic devices. The GX4004 series appliances are deployed between the Intranet and the Production Zones.

The GX4004-v2 Security Network IPS model offers 200 Mbps of throughput across two protected network segments. It can deliver comprehensive security, performance, and reliability in a solution that is simple to deploy and manage. Figure 6-29 shows the physical makeup of the GX4004 appliances.

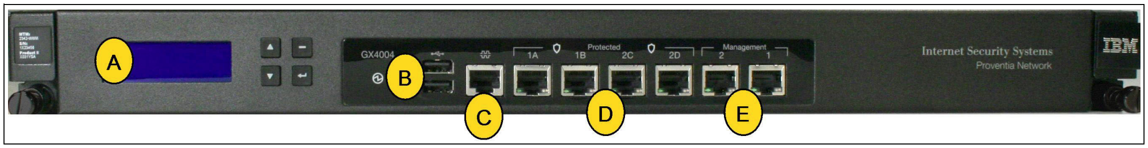


Figure 6-29 Common configuration modules and ports of the GX4004-v2 series appliance

In the following detailed explanation of the different ports, the letters correspond to the items shown in Figure 6-29:

A LCD Controller Module

The LCD Controller Module is used for initially configuring the network, restarting or shutting down the appliance, and obtaining IPS version information.

B USB ports

The USB ports are used for retrieving data and installing firmware.

C Serial console port

The Serial console port is used for terminal-based setup and recovery.

D Protected ports

The Protected ports are used for either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention uses a pair of ports for each segment. Passive detection uses a single port for each segment.

> **Deviations on the front panel:** Port configuration might look slightly different depending on the number of ports.

E Management ports

- Management port 1 is used to communicate with IBM Security SiteProtector.
- Management port 2 is used exclusively to send TCP Reset responses.

Cabling the appliance

To cable the appliance, as the administrator for the cardio healthcare company, follow these steps:

1. Connect the power cable to the appliance.
2. Connect Management port 1 to the management VLAN. The use of the management VLAN separates management traffic from the network (allows regular network traffic to pass on the monitored interfaces). Management port 2 is the TCP Reset port. This port must be on the same network or VLAN with the regular traffic.
3. Connect the network cables to the protected ports. To run the appliance in passive mode, connect only the first protected port in the pair to the network.
4. From the appliance, ping to a computer on the other side to verify that traffic passes.
5. Turn on the appliance.

Configuring the default policies

This section explains how to set up the default policies for the GX4004 appliance in the medical centers.

Firewall rules for the Intranet Zone

The Intranet Zone firewall rules are complementary to the existing firewall that is already deployed. The GX4004 appliance is placed in inline simulation mode with monitoring ports on the switched backplane. With this configuration, the monitored ports on the GX4004 series can detect VLAN tags and trunked segments. As the administrator for the cardio healthcare company, you configure a firewall policy. This policy prevents local file and print servers, workstations, and clinic devices from accessing the local HR VLAN where the local company information is contained.

Protection domains

The Intranet Zone has a protection domain defined. This protection domain is used to define the network security policy and assists in protection against unknown viruses, worms, and other types of malware.

As the administrator of the cardio healthcare company, create a protection domain by following these steps:

1. Right-click **Protection Domains**, and the select **Open**.
2. Click the **Add** icon (green plus sign).

3. In the Edit Protection Domains dialog box (Figure 6-30), configure the following protection domain options:

   a. Select the **Enabled** check box to enable the protection domain.

   b. Add a unique and descriptive comment for the domain.

   c. Select the physical adapters on the device to assign them to the protection domain.

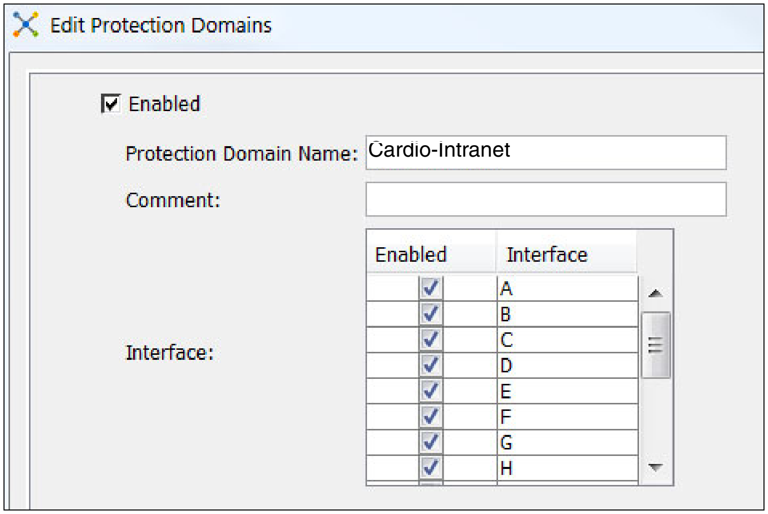
   > **Available ports:** The appliance dialog box might show more ports than are available on the physical device. The IBM Security Network IPS device that subscribes to the policy ignores the port configurations that do not apply to the specific appliance. For example, the dialog box might allow the configuration of eight adapter ports although only four ports are available on the appliance.

   d. Bind the adapter to the monitored traffic. To configure the monitored traffic, use assign any combination of the following criteria to a protection domain interface:

   - 802.1q VLAN tags
   - IPv4 addresses
   - IPv6 address ranges

   e. Click **OK**.

   Figure 6-30 shows the protection domain created for the Intranet Zone.



Edit Protection Domains

☑ Enabled

Protection Domain Name: Cardio-Intranet

Comment:

Interface:

Enabled	Interface
✓	A
✓	B
✓	C
✓	D
✓	E
✓	F
✓	G
✓	H

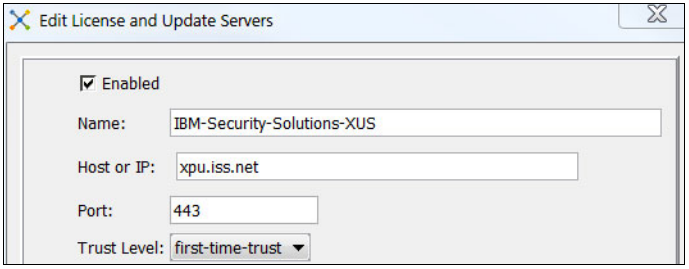
Figure 6-30 The Intranet Zone protection domain

Update policy

The administrator configured the update policy to perform updates every day at 3:00 a.m. The IBM Security Network IPS appliance downloads and installs security content updates automatically. Firmware updates are downloaded only. The management team for the cardio healthcare company mandated that firmware updates cannot be automatically installed because they can cause the appliance to restart. The machines in this zone have two entries for retrieving updates. The first choice is to download directly from `xpu.iss.net`.

> **Port configuration for updates:** When downloading from the IBM Security X-Press Update Server (XUS), the port number must be 443. The license used for updates must be installed on the GX4004 and IBM Security SiteProtector. To download any security and feature updates, the appliance submits credentials to the website.

Figure 6-31 shows the resulting policy.



Edit License and Update Servers

☑ Enabled

Name: IBM-Security-Solutions-XUS

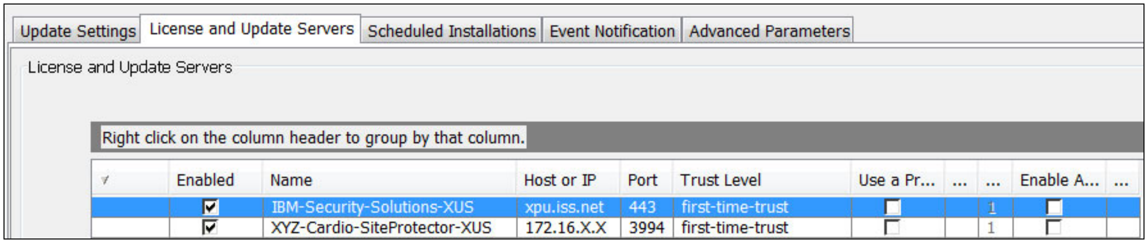
Host or IP: xpu.iss.net

Port: 443

Trust Level: first-time-trust

Figure 6-31 Edit License and Update Servers dialog box

The second choice is to use the XUS in the Management Zone. Connections to the Management Zone traverse the VPN connection and the management network. This policy ensures that the remote offices have current protection and a redundant means to obtain updates if the headquarter site is unavailable. Figure 6-32 shows the resulting policy.



License and Update Servers

Right click on the column header to group by that column.

	Enabled	Name	Host or IP	Port	Trust Level	Use a Pr...	...	...	Enable A...	...
	☑	IBM-Security-Solutions-XUS	xpu.iss.net	443	first-time-trust	□		1	□	
	☑	XYZ-Cardio-SiteProtector-XUS	172.16.X.X	3994	first-time-trust	□		1	□	

Figure 6-32 Both configured update sites

This policy is deployed to the Intranet group. All GX4004-v2 appliances will inherit this setting.

DLP policy

The administrator for the cardio healthcare company creates a comprehensive DLP policy that blocks any PII from being transmitted over the Internet connections for the medical clinics. The IBM Security Network IPS is configured to block DLP on all outbound connections.

As the administrator for the cardio healthcare company, configure the Data Loss Prevention policy in the network by using the following steps:

1. From the policy repository, select and right-click the **Data Loss Prevention policy**. Then select **New Policy** (Figure 6-20 on page 189).
2. On the Data Loss Prevention policy page, complete the following steps on the **Signatures** tab (Figure 6-21):
   a. Select the **Content Analysis Enabled** option.
   b. In the Predefined Events table, select **Content_Analyzer_Credit_Card_Num**.
3. Click the **Edit** icon.
4. Click the **Add new row** icon.
5. In the Protection Domain field, select **XYZC-Production-CustDB**. Then click **OK**.
6. In the Edit Predefined Events dialog box, click **OK**.
7. Verify that the Content_Analzyer_Credit_Card_Num event is Enabled and is assigned to the XYZC-Production-CustDB protection domain.
8. Repeat these steps for all other PII types.

The basic configuration of the GX4004 appliance in the medical centers is now completed.

6.2.5 Registration with IBM Security SiteProtector

This section explains what you, as the administrator for the cardio healthcare company, must do to register the appliances with the central IBM Security SiteProtector management console. First you see how to access the LMIs on the individual appliances.

Accessing the local management interface

Each IBM Security Network IPS appliance has a web-based LMI that is used to configure individual appliance settings. To access the LMI, perform the following steps:

1. From the desktop, open a web browser.
2. In the Address field, type the following address, which represents the IP address of the appliance:

   ```
   https://IP_ADDRESS
   ```

3. On the page that opens, complete the following actions:
   a. In the User name field, type `admin`.
   b. In the Password field, type the password for that particular appliance.
   c. Click **OK**.

LMI required: Some appliance settings, including the following settings, are exclusive to the LMI:

- Assign or revoke management of the appliance to SiteProtector
- Use the appliance diagnostic tools
- View and interact with appliance event logs
- View the quarantine rules and intrusions
- Manage and change the appliance passwords
- Test appliance connectivity to SiteProtector
- Manage network interfaces

The cardio healthcare company manages individual appliances by using IBM Security SiteProtector as the preferred solution for centralized administration of multiple appliances.

Configuring client authentication on the Agent Manager

The Agent Manager facilitates command and control between the SiteProtector console and the IBM Security Network IPS appliance. The appliance submits heartbeats to the Agent Manager on a configurable schedule to obtain policy and configuration changes. By default, communication between the appliance and the Agent Manager is encrypted by using SSL. The administrator for the cardio healthcare company creates a user account and password combination that is shared with the IBM Security Network IPS agents and the Agent Managers.

As the administrator for the company, configure client authentication on the Agent Manager by using these steps:

1. Log in to the SiteProtector console, and select the cardio healthcare company site.
2. From the **Go to** drop-down list in the upper right corner of the SiteProtector console, select **Agent**.
3. Right-click the Agent Manager, and then select **Properties**.
4. On the **Properties** tab, click the **Agent Properties** icon.
5. Click the **Edit Agent Properties** link.
6. In the Agent Manager Properties - Policy Editor window, complete the following steps:
   a. In the Agent Manager Properties tree, select **Accounts**.
   b. Click the **Add new row** icon.
   c. Create a user name and password credentials.

      > **Login credentials for this scenario:** In this example, the user name is `nipsadmin`, and the password is `XYZC4rd10`.

   d. In the Agent Manager Properties tree, select **Communications Settings**.
   e. In the IBM Proventia® Client Authentication field, select **Account/Password**.
   f. Click the **Save** toolbar button. SiteProtector adds the account to the Agent Manager.
   g. Close the Agent Manager Properties window.
7. In IBM Security SiteProtector, close the **Properties** tab.

The **`issdaemon`** service on the Agent Manager machine is restarted to apply the changes on the Agent Manager. To restart the service, open a command prompt and enter the **`net stop issdaemon`** command.

Registering the appliance with IBM Security SiteProtector

IBM Security Network IPS appliances are registered with IBM Security SiteProtector for long-term policy storage and version control of policies. IBM Security Network IPS appliances must be registered with IBM Security SiteProtector before they are displayed in the console.

To register an appliance in IBM Security SiteProtector, as the administrator, perform the following steps:

1. In the LMI, select **Manage System Settings**. Then select **Appliance** → **SiteProtector Management** (Figure 6-33).

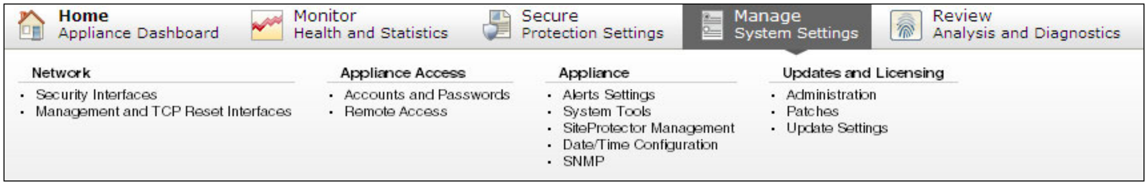
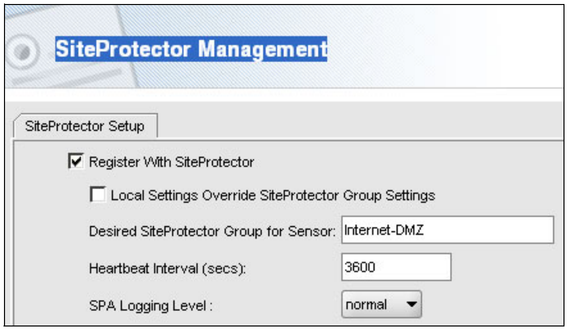


Figure 6-33 Accessing the Appliance Menu

2. On the **SiteProtector Setup** tab, complete these actions;

   a. Select the **Register With SiteProtector** check box.

   b. In the Desired SiteProtector Group for Sensor field, enter the name of the group for registration. In this example, the IBM Security Network IPS is registered to the group Internet-DMZ as shown in Figure 6-34.



SiteProtector Management

SiteProtector Setup

☑ Register With SiteProtector

□ Local Settings Override SiteProtector Group Settings

Desired SiteProtector Group for Sensor: Internet-DMZ

Heartbeat Interval (secs): 3600

SPA Logging Level : normal

Figure 6-34 Register with SiteProtector

3. In the Agent Manager Configuration area, select the **Add new row** icon (green plus sign).

4. In the Add Agent Manager Configuration dialog box (Figure 6-35), complete these steps:

   a. For the Authentication Level, accept the default setting **first-time-trust**.

   b. In the Agent Manager Name field, type `AgentManager_XYZCARDI001`.

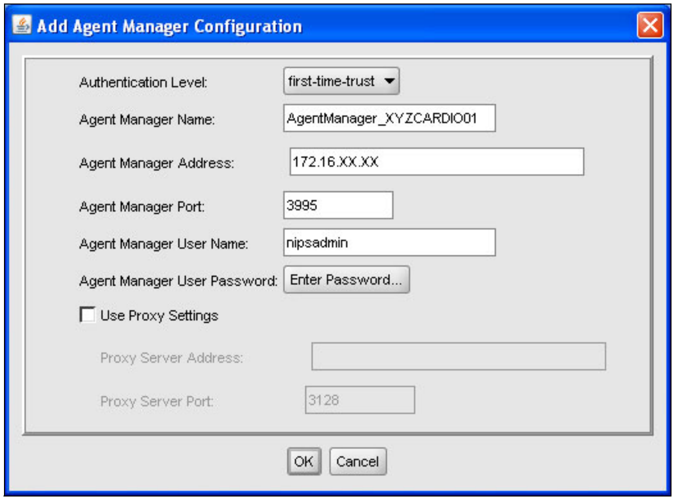
   c. In the Agent Manager Address field, enter the (resolvable) host name or IP address of the Agent Manager.

   d. In the Agent Manager Port field, accept the default value of `3995`.

e. In the Agent Manager User Name field, enter `nipsadmin`.

f. In the Agent Manager User Password field, type `XYZC4rd10`.

Figure 6-35 shows the completed dialog box.



Add Agent Manager Configuration

Authentication Level: first-time-trust

Agent Manager Name: AgentManager_XYZCARDIO01

Agent Manager Address: 172.16.XX.XX

Agent Manager Port: 3995

Agent Manager User Name: nipsadmin

Agent Manager User Password: Enter Password...

□ Use Proxy Settings

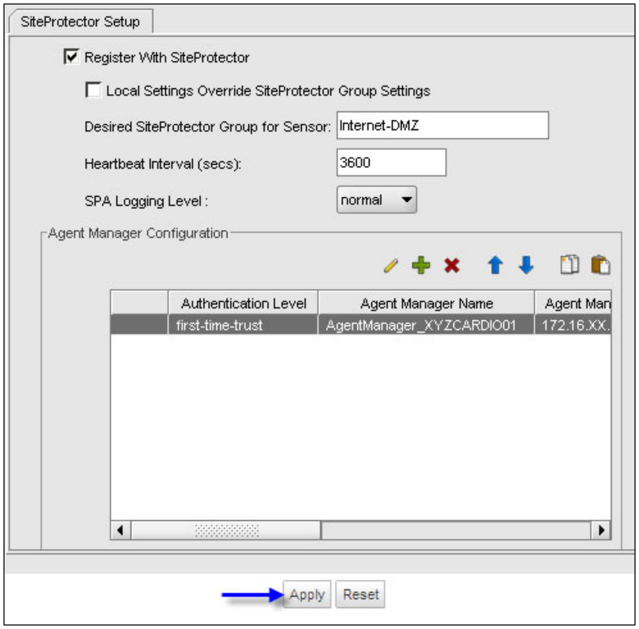
Proxy Server Address:

Proxy Server Port: 3128

Figure 6-35 Add Agent Manager Configuration

The Agent Manager is now added to the Agent Manager Configuration list.

5. Click **Apply** to apply the changes (Figure 6-36) to initiate the registration process with SiteProtector.



SiteProtector Setup

☑ Register With SiteProtector

□ Local Settings Override SiteProtector Group Settings

Desired SiteProtector Group for Sensor: Internet-DMZ

Heartbeat Interval (secs): 3600

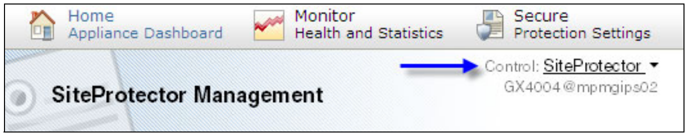
SPA Logging Level : normal

Agent Manager Configuration

	Authentication Level	Agent Manager Name	Agent Man
	first-time-trust	AgentManager_XYZCARDIO01	172.16.XX.

Figure 6-36 Clicking the Apply button to save your configuration

6. Verify registration on both the IBM Security Network IPS appliance and the SiteProtector console. In the upper-right corner of the LMI, verify that the Control field indicates `SiteProtector` (Figure 6-37).



SiteProtector Management

Control: SiteProtector
GX4004@mpmgips02

Figure 6-37 Confirming Agent Registration with SiteProtector

7. Log in to the SiteProtector console, select the **Agent** view, and verify the agent registration.

Wait time: It might take up to 5 minutes for the appliance to contact the Agent Manager.

6.3 Conclusion

This chapter examined the network design and implementation of the IBM Security Network IPS device for the cardio healthcare company. It explained the type of IBM Security Network IPS appliances that are needed to protect the individual network zones. It highlighted the different network protection modes and an implementation strategy for the cardio healthcare company about how to use them.

Then this chapter guided you through the steps that the administrator must follow to prepare for and install every IBM Security Network IPS appliance. It also showed how to configure basic policies and general setup parameters. In addition, it showed how to register the appliances with the central management console IBM Security SiteProtector.

Chapter 7, “Phase 2: Policy tuning for IBM Security Network IPS” on page 211, looks more closely at tuning the base policies and eventually taking all appliances into inline protection mode.

7

Phase 2: Policy tuning for IBM Security Network IPS

To use the IBM Security Network IPS efficiently as a security control, security policy tuning is essential to the cardio healthcare company (also called the *company*). This chapter explains how the cardio healthcare company tunes the IBM Security Network IPS enforcement policy to their production environment.

This chapter includes the following sections:

- Policy tuning objectives
- Overview of the IBM Security Network IPS policy
- False positives versus false alarms
- False negatives
- Modifying default settings
- Conclusion

7.1 Policy tuning objectives

The IBM Security Network IPS can act as two separate security controls. It can provide accountability controls through its intrusion detection system (IDS) functions in passive monitor mode. It can also provide authorization controls through its Network IPS functions in inline protection mode.

After initial implementation at the cardio healthcare company, the IBM Security Network IPS appliances are in simulation mode, as explained in Chapter 6, “Phase 1: Design and implementation of IBM Security Network IPS” on page 161. To provide full efficiency of an IPS appliance, the appliance must block malicious network traffic when identified, which requires moving from simulation mode to prevention mode.

The simulation mode allows tuning of a security policy in production. The concern about prevention mode is that you might accidentally block data that is valid for the network. Tuning a policy allows the transition to prevention mode.

7.2 Overview of the IBM Security Network IPS policy

To help you better understand how to tune the IBM Security Network IPS policy, you must understand how policy is implemented by the IBM Security Network IPS appliance. The following policies are available for enforcement:

- Firewall policy

  The firewall policy is similar to any standard firewall policy. A packet match is made that is typically based on network and transport packet headers (ports and IP addresses). An action is then taken on the packet such as *drop* or *ignore*.

- IPS policy

  The IPS policy is an amalgam of several individual policies:

  Security Events The primary IPS policy for the Network IPS.

  Response Filters Helps to create exceptions to the security events policy.

  Protection Domains By defining a protection domain, you can create bulk exceptions to the security events policy.

  Connection Events Help you to define IPS signatures based on firewall-type rules. This policy is deprecated by the Network IPS Firewall policy.

WAP Helps you to manage IPS signatures that are meant to protect vulnerable web applications from attacks such as cross-site scripting.

DLP Helps you to configure IPS signatures that can monitor for the leakage of personally identifiable information (PII), such as credit card information.

- Custom signatures

  The IBM Network IPS has two policies that allow for custom IDS or IPS signatures:

  OpenSignatures Custom signatures using a Snort syntax.

  User Defined Events Custom signatures using regular expressions.

7.3 False positives versus false alarms

By default, the IPS or IDS policies are set up with X-Force recommended signatures turned on. Over the course of deployment and implementation, the cardio healthcare company will change these default settings to match its environment and security threat posture. One of the primary changes that will be made to this default policy is the elimination of false positives.

An IDS or IPS system is put in place to audit for the presence of malicious network activity or, in the case of IPS, block it altogether. Such systems are not interested in traffic that is considered valid for the network, such as an employee browsing the web or sending an email. When security alerts trigger on valid traffic, this noise makes it harder to identify real security incidents.

Two types of security alert triggers are generally considered *noise* by the security analysts who must monitor such alerts. These noisy events are called *false positives* and *false alarms*.

7.3.1 False alarm

A *false alarm* is when an IDS signature triggers correctly on valid network traffic. There are many examples of false alarms, and they are typical of every IDS installation. For example, a Simple Network Management Protocol (SNMP) server doing a ping sweep might trigger the Ping Sweep IDS signature. The signature triggers correctly, but it triggers on acceptable, valid network traffic. False alarms are easy to tune out of your IDS policy by using filtering.

7.3.2 False positive

A *false positive* is when an IDS signature triggers incorrectly on valid network traffic. The level and number of *true* false positives depends on the IDS technology and the strength of the signatures used. For example, the IDS triggers a Long URL Buffer Overflow signature, but the URL is a long session ID issued in the URL (that is, *not* a buffer overflow). False positives are more difficult to tune out of your policy because they tend to be part of the nature of the signature itself.

7.3.3 Identifying false positives or false alarms

Identifying a false positive or false alarm can be a difficult process and is part of the *intrusion analysts* job description to identify. The intrusion analyst uses available clues to decide whether the signature is triggering on malicious or non-valid traffic. First the analyst looks at the source and destination IP addresses. This person asks: Should these IP addresses be communicating with each other over the network?

The analyst also looks at the event itself. This person asks the following questions:

- What protocol or protocols are involved?
- Should the protocols be allowed between the two IP addresses?
- What type of event is triggered?
- Can this situation be triggered by normal, valid traffic?

If more clues are necessary, when a signature triggers, packet captures can help identify whether the traffic is valid.

7.3.4 Types of false positives or false alarms

The following four types of false positives or false alarms are the primary types:

- One IP and All Signatures

  In this case, regardless of the signature that is triggered, it is a false alarm. This situation might be typical of a vulnerability assessment. All signatures triggered by the assessment system are triggered by valid traffic. You tune this policy by filtering out the IP address in your IDS policy.

- All IPs and One Signature

  In this case, regardless of the IP that triggers the signature, it is a false alarm. This situation might be typical of lower severity signatures. For example, Anonymous Share Enumeration triggering on a network where anonymous shares are allowed is going to trigger for every IP. You tune this policy by turning off the signature.

- One IP and One Signature

  In this case, the false alarm is with an IP and signature pair. For example, an SNMP server might trigger an SNMP broadcast signature. The SNMP broadcast signature is only a false alarm when triggered by the IP of the SNMP server. Your IDS policy should support the filtering of this type of false alarm.

- Signature Threshold

  In this case, a false positive is triggered when the threshold for the signature itself does not fit your environment. For example, a SYN Flood signature triggers with 500 unique SYNs in one second. This level of traffic is acceptable in your environment, and a SYN flood will not affect your environment unless the level reached over 2000 SYNs. With some IDS solutions, you can tune the signatures yourself.

7.3.5 Examples of false positive identification

This section highlights examples of false positive identification.

One IP and all signatures

An analyst at the cardio healthcare company identified the trigger of the *SMTP_Probe_Root* signature on the Internet DMZ Network IPS. Upon inspecting the Event Details, the analyst determined that the source IP address is 192.168.4.3 and the destination IP address is 192.168.4.25.

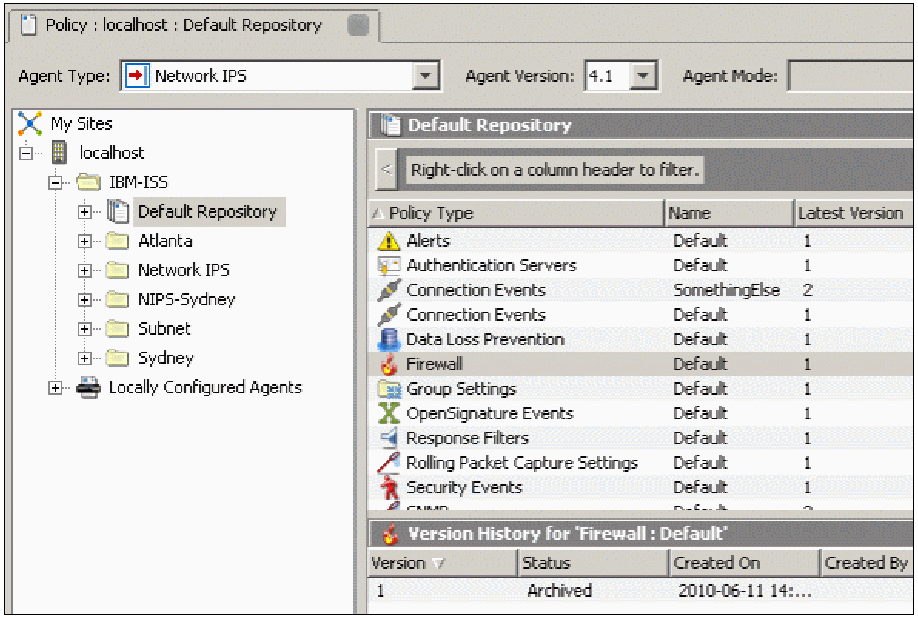
The analyst instantly identifies the destination IP address as the corporate mail server. The fact that the mail server is being attacked from a local IP address (192.168.4.3) with a mail-based attack (SMTP_Probe_Root) causes instant concern.

The analyst does further investigation using the Guided Analysis function of IBM Security SiteProtector. The analyst looks for *Show me other attacks from this source*. This person can also identify hundreds of signatures triggered by the same source IP targeting every IP address in the DMZ.

A phone call to the network administrator calms all the concerns. The unidentified source IP address is the new vulnerability assessment appliance for the company.

The analyst knows that the valid traffic from the appliance will create many false alarms in the future. This person recommends putting in place a Firewall Ignore rule. To achieve this goal, the analyst completes the following steps:

1. In the SiteProtector console, go to the Policy Management view (Figure 7-1).


Policy : localhost : Default Repository
My Sites
localhost
IBM-ISS
Default Repository
Atlanta
Network IPS
NIPS-Sydney
Subnet
Sydney
Locally Configured Agents
Default Repository
Right-click on a column header to filter.

Agent Type: Network IPS
Agent Version: 4.1
Agent Mode:

Policy Type	Name	Latest Version
Alerts	Default	1
Authentication Servers	Default	1
Connection Events	SomethingElse	2
Connection Events	Default	1
Data Loss Prevention	Default	1
Firewall	Default	1
Group Settings	Default	1
OpenSignature Events	Default	1
Response Filters	Default	1
Rolling Packet Capture Settings	Default	1
Security Events	Default	1

Version History for 'Firewall : Default'

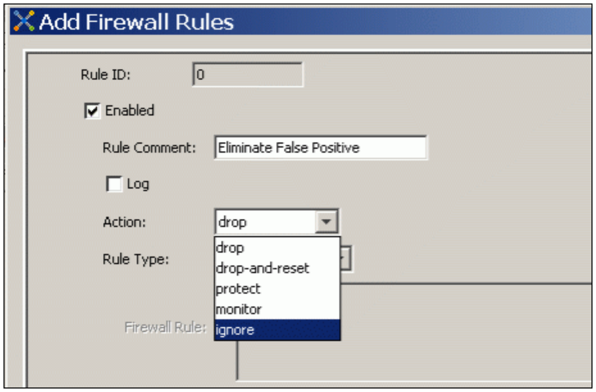
Version	Status	Created On	Created By
1	Archived	2010-06-11 14:...	

Figure 7-1 Policy Management view in SiteProtector console

2. Manage the firewall policy by opening the policy from the **Default Repository**.
3. Add a firewall rule to the rules list as shown in Figure 7-2 on page 217. The rule uses the settings shown in Example 7-1.

Example 7-1 Firewall rule

```
Action: ignore
Source IPv4: 192.168.4.3
Destionation: 192.168.4.0/24
Protocol: Any
```


Add Firewall Rules

Rule ID: 0

☑ Enabled

Rule Comment: Eliminate False Positive

☐ Log

Action: drop

Figure 7-2 Firewall ignore rule

This rule prevents the Internet DMZ Network IPS from triggering these false positives in the future.

All IPs and one signature

An analyst at the cardio healthcare company identified the trigger of the *HTTP_Novell_Files* on the Production Zone Network IPS. Upon inspecting the event details, the analyst determined that the source IP address is 192.168.3.3 and the destination IP address is 192.168.6.125.

The analyst identifies the destination IP address as one of the Novell servers and notes that the source IP address is an internal client workstation. The analyst does further investigation based on the security information included in the event details. The systems administrator confirms that the Novell server still uses Perl scripts for the Novell clients, but obtained a security exception because the scripts were personally hardened.

Because any internal IP address might trigger this signature, the analyst recommends disabling the HTTP_Novell_Files in the Network IPS policy. To achieve this goal, as the analyst for the company, complete the following steps:

1. Open the **Security Events policy** from the Default Repository.
2. Select the **Filter** option (Figure 7-3).

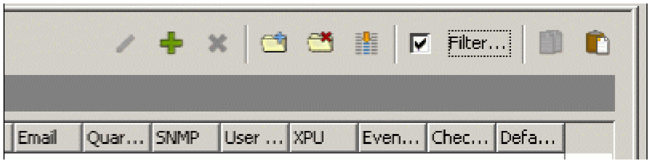
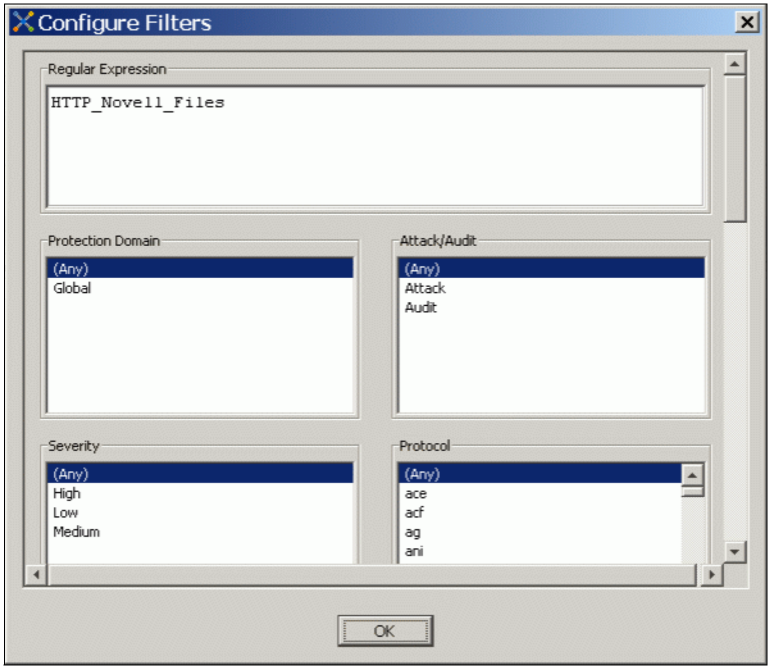

☑ Filter...

Figure 7-3 Filter check box in the Security Events policy

3. In the Configure Filters dialog box (Figure 7-4), find the exact tag name of the HTTP_Novell_Files signature. Then click **OK**.



Configure Filters

Regular Expression: HTTP_Novell_Files

Protection Domain: (Any)
Global

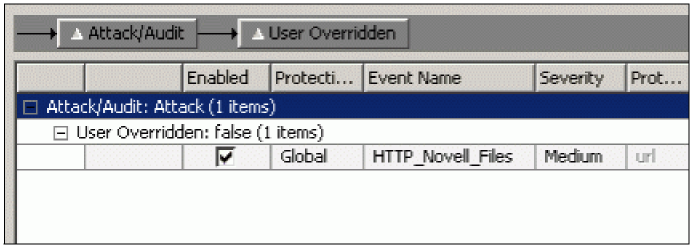
Attack/Audit: (Any)
Attack
Audit

Severity: (Any)
High
Low
Medium

Protocol: (Any)
ace
acf
ag
ani

Figure 7-4 Configure Filters

The Security Events policy is then filtered on the single signature as shown in Figure 7-5.



		Enabled	Protecti...	Event Name	Severity	Prot...
⊟ Attack/Audit: Attack (1 items)						
⊟ User Overridden: false (1 items)						
		☑	Global	HTTP_Novell_Files	Medium	url

Figure 7-5 Security Events after filtering

4. Clear the **Enabled** check box to disable the signature.

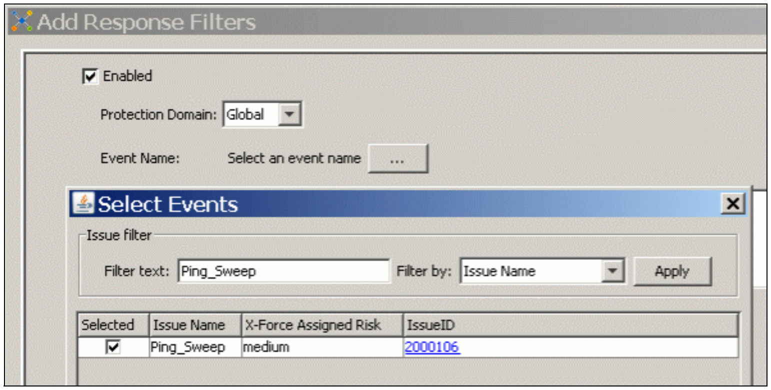
One IP and One Signature

An analyst at the cardio healthcare company identified the trigger of the *Ping_Sweep* on the Production Zone Network IPS. Upon inspecting the event details, the analyst determined that the source IP address is 192.168.4.25 and the destination IP address is 192.168.4.105.

The analyst identifies the destination IP as an SQL server and sees that the source IP address is the production SNMP server. The analyst does further investigation and confirms that this behavior is normal for the SNMP server. The analyst recommends creating a Response Filter for the Network IPS.

To achieve this goal, as the analyst for the company, complete the following steps:

1. From the Default Repository, open the **Response Filter** policy.
2. Add a Response Filter.
3. Click the **Select an Event Name** button.
4. In the Select Events window (lower part of Figure 7-6), filter for the Ping_Sweep signature. In this example, for Filter text, we enter `Ping_Sweep`, and for Filter by, we select **Issue Name**. Then click **Apply**.



Add Response Filters

☑ Enabled

Protection Domain: Global

Event Name: Select an event name ...

Select Events

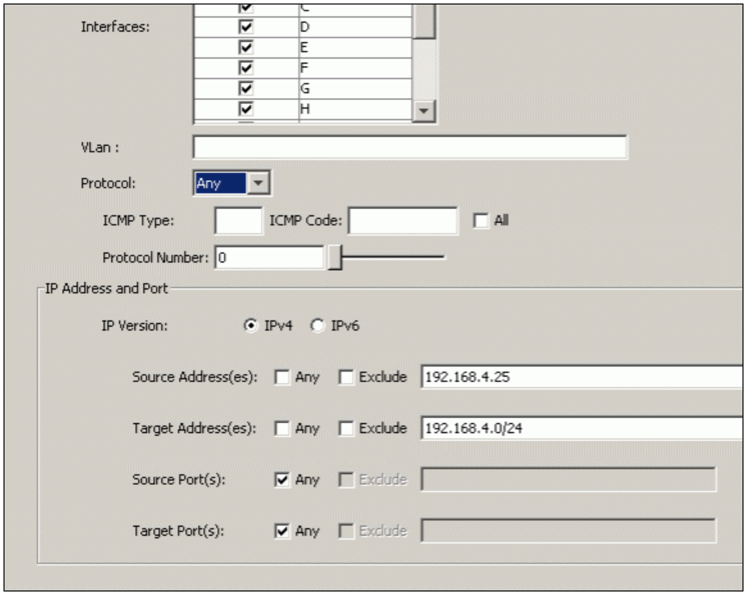
Issue filter

Filter text: Ping_Sweep Filter by: Issue Name Apply

Selected	Issue Name	X-Force Assigned Risk	IssueID
☑	Ping_Sweep	medium	2000106

Figure 7-6 Selecting an event to filter

5. Specify the source and destination IP addresses to filter out (Figure 7-7).



Interfaces:
☑ D
☑ E
☑ F
☑ G
☑ H

VLan :

Protocol: Any

ICMP Type: ICMP Code: □ All

Protocol Number: 0

IP Address and Port

IP Version: ● IPv4 ○ IPv6

Source Address(es): □ Any □ Exclude 192.168.4.25

Target Address(es): □ Any □ Exclude 192.168.4.0/24

Source Port(s): ☑ Any □ Exclude

Target Port(s): ☑ Any □ Exclude

Figure 7-7 Setting IP addresses in the Response Filter

6. To complete the filter, select the **Ignore Event** check box in the Response Filter rule. Then save the policy back to the Repository.

   This response filter disables the Ping_Sweep signature only when sourced from the SNMP server and destined for the DMZ network.

Signature threshold

An analyst at the cardio healthcare company identified the trigger of the *Radius_User_Buffer_Overflow* on a WAN-RMC Network IPS. Upon inspecting the event details, the analyst determined that the source IP address is 172.16.3.205 and the destination IP address is 172.16.3.34.

The analyst identifies the destination IP address as a local Radius server and sees that the source IP address is a local workstation. The analyst does further investigation and confirms that the local Radius administrator is using full email addresses as the user IDs on the server. This situation makes the user IDs trigger the signature by appearing to be longer than appropriate.

You can tune some signatures by using advanced tuning parameters. For a list of available tuning parameters for each signature, download the `PAM.chm` help file at:

https://www.ibm.com/support/docview.wss?uid=swg21434715&wv=1

To achieve this goal, the analyst follows these steps:

1. Using IBM Security SiteProtector, download the most recent copy of the `PAM.chm` help file. Select **Help** → **Attack Signatures** → **Protocol Analysis Module** (Figure 7-8).

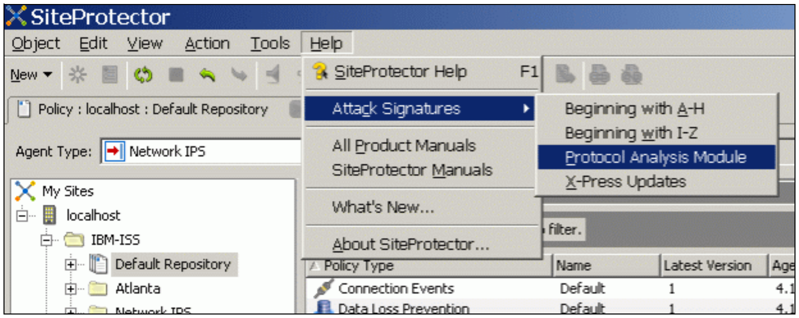
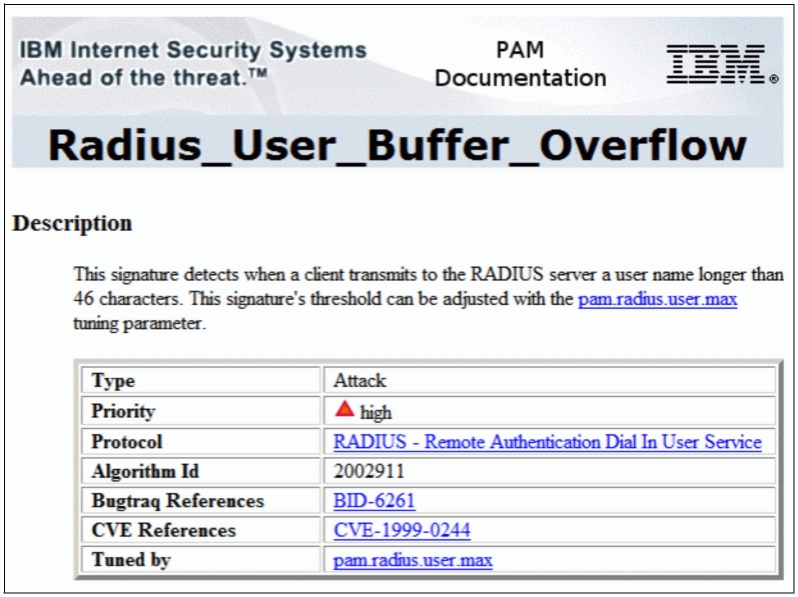


Figure 7-8 Downloading the PAM help file from SiteProtector console

2. Look up the signature to find possible tuning parameters for the signature (Figure 7-9).



IBM Internet Security Systems
Ahead of the threat.™

PAM
Documentation

IBM

Radius_User_Buffer_Overflow

Description

This signature detects when a client transmits to the RADIUS server a user name longer than 46 characters. This signature's threshold can be adjusted with the pam.radius.user.max tuning parameter.

Type	Attack
Priority	▲ high
Protocol	RADIUS - Remote Authentication Dial In User Service
Algorithm Id	2002911
Bugtraq References	BID-6261
CVE References	CVE-1999-0244
Tuned by	pam.radius.user.max

Figure 7-9 The Attack Signature page in the PAM.chm

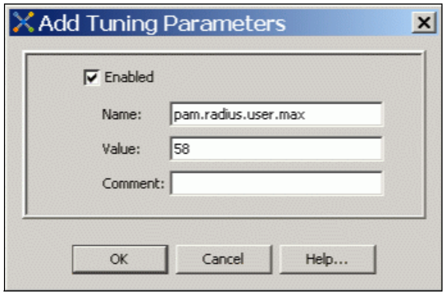
Using the `PAM.chm` file, the analyst identified that the *Radius_User_Buffer_Overflow* signature can be tuned with the advanced parameter `pam.radius.user.max`.

3. From the **Default Repository** on the SiteProtector console, open the **Tuning Parameters** policy (Figure 7-1 on page 216).

   The local Radius administrator identified that the longest user ID is 58 characters in length. The analyst recommends adjusting a tuning parameter, `pam.radius.user.max`, to the value of 58.

4. In the Add Tuning Parameters dialog box (Figure 7-10), complete the following steps for this example:

   a. Select the **Enabled** check box.
   b. For name, enter `pam.radius.user.max`.
   c. Click **OK**.



☑ Enabled
Name: pam.radius.user.max
Value: 58
Comment:

Figure 7-10 Adding a tuning parameter

7.4 False negatives

False negatives occur when traffic does not trigger a security alert when it should have. This situation typically occurs when the organization has custom applications or protocols that IBM might not know about.

7.4.1 Identifying false negatives

Identification of false negatives can come from many sources. For example, a systems administrator might discover a vulnerability in her own code that cannot be patched until the next maintenance period. Another example might come from an incident response report after a breach. The incident response auditors might discover that the breach occurred because of a local, custom web application.

7.4.2 Packet capture techniques

In attempting to create a custom signature, *packet sniffing* is often used. With packet sniffing, you can see network traffic the way the IBM Security Network IPS does. Many packet sniffers are available for download from the Internet. The IBM Security Network IPS can also provide a packet sniffing capability right in the appliance.

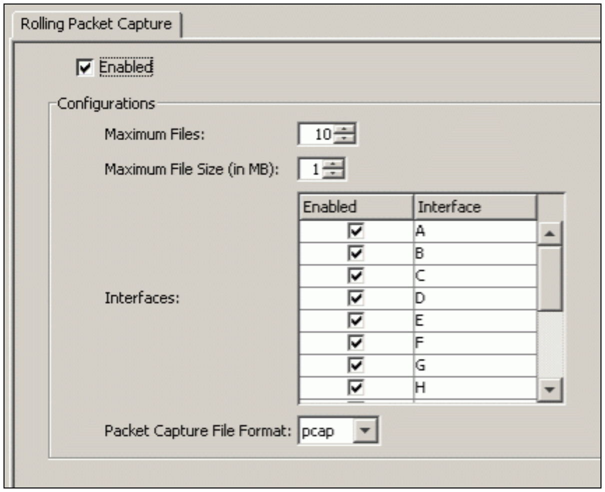
7.4.3 Packet capture example

An analyst at the cardio healthcare company must create a custom signature so that the organization can audit specific client traffic that targets their e-commerce website.

Enabling Rolling Packet Capture

As the analyst, you first enable the Rolling Packet Capture policy through SiteProtector:

1. From the Default Repository, open the **Rolling Packet Capture** policy (Figure 7-1 on page 216).
2. On the **Rolling Packet Capture** tab, complete the following actions:
   a. Select the **Enabled** check box.
   b. Select the interfaces on which you want to capture packets (Figure 7-11).
   c. Select the maximum files, maximum file size, and packet capture file format.



Rolling Packet Capture

☑ Enabled

Configurations

Maximum Files: 10

Maximum File Size (in MB): 1

Interfaces:

Enabled	Interface
☑	A
☑	B
☑	C
☑	D
☑	E
☑	F
☑	G
☑	H

Packet Capture File Format: pcap

Figure 7-11 Rolling Packet Capture policy

3. After deploying the policy to the appliance, have a client connect to the e-commerce website and perform the action that the company wants to audit.
4. After the traffic occurrs, download the packet capture by using the Network IPS Local Management Interface (Figure 7-12).

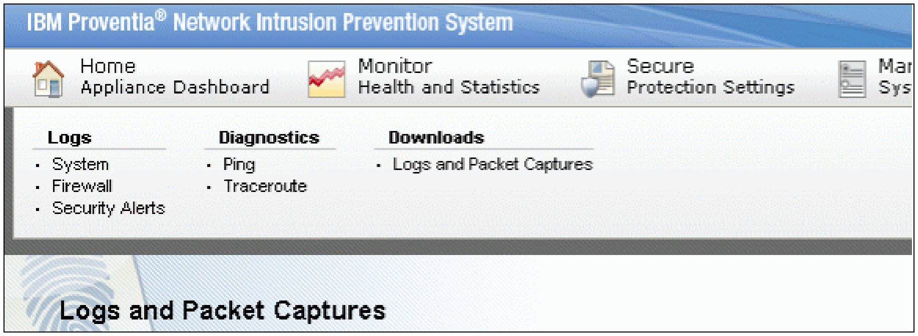
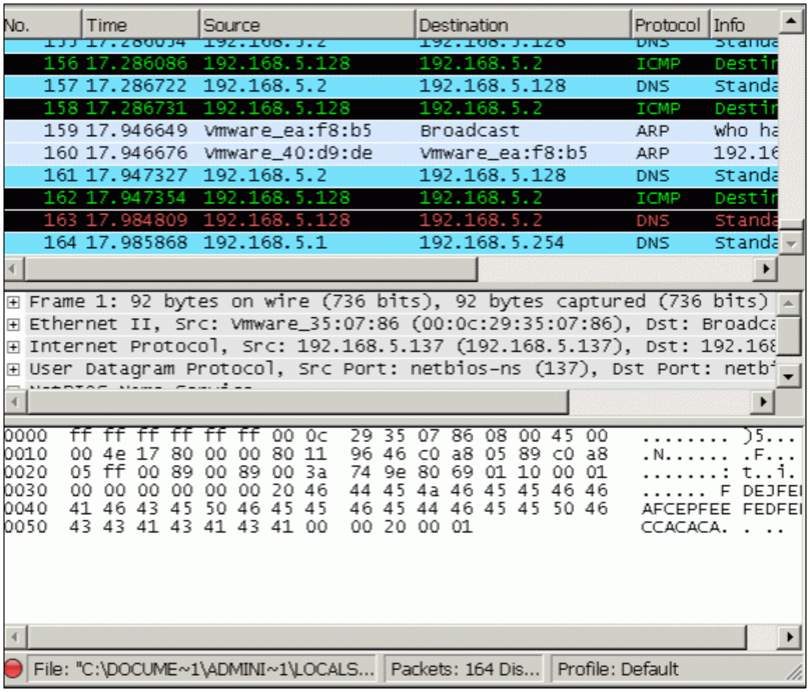


Figure 7-12 Downloading the Packet Capture from the Network IPS

5. After downloading the packet capture, open the file in a packet analysis software. Figure 7-13 shows typical output from one such analysis application. You can closely investigate network traffic between different hosts, for example.



```
No.    Time       Source               Destination          Protocol Info
  156 17.286086 192.168.5.128       192.168.5.2           ICMP     Destin
  157 17.286722 192.168.5.2         192.168.5.128         DNS      Standa
  158 17.286731 192.168.5.128       192.168.5.2           ICMP     Destin
  159 17.946649 Vmware_ea:f8:b5     Broadcast             ARP      Who ha
  160 17.946676 Vmware_40:d9:de     Vmware_ea:f8:b5       ARP      192.16
  161 17.947327 192.168.5.2         192.168.5.128         DNS      Standa
  162 17.947354 192.168.5.128       192.168.5.2           ICMP     Destin
  163 17.984809 192.168.5.128       192.168.5.2           DNS      Standa
  164 17.985868 192.168.5.1         192.168.5.254         DNS      Standa
```

```
⊞ Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)
⊞ Ethernet II, Src: Vmware_35:07:86 (00:0c:29:35:07:86), Dst: Broadca
⊞ Internet Protocol, Src: 192.168.5.137 (192.168.5.137), Dst: 192.168
⊞ User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbi
```

```
0000   ff ff ff ff ff ff 00 0c  29 35 07 86 08 00 45 00   ........ )5...
0010   00 4e 17 80 00 00 80 11  96 46 c0 a8 05 89 c0 a8   .N...... .F...
0020   05 ff 00 89 00 89 00 3a  74 9e 80 69 01 10 00 01   .......: t..i.
0030   00 00 00 00 00 00 20 46  44 45 4a 46 45 45 46 46   ...... F DEJFEI
0040   41 46 43 45 50 46 45 45  46 45 44 46 45 45 50 46   AFCEPFEE FEDFEI
0050   43 43 41 43 41 43 41 00  00 20 00 01               CCACACA. . ..
```

File: "C:\DOCUME~1\ADMINI~1\LOCALS... | Packets: 164 Dis... | Profile: Default

Figure 7-13 Packet capture

Free tools: One of the analysis applications is called *Wireshark*, which is a tool covered under GPLv2. You can download it at no charge from:

`http://wireshark.org/`

6. Examine the traffic streams and look for the specific client traffic that needs auditing. Here, you must find a specific string of characters or quality of traffic that is unique to the traffic to be audited. This information will then form the foundation of the custom signature.

7.4.4 Custom signatures overview

The IBM Security Network IPS offers two options for custom signatures: OpenSignatures and User Defined Events.

7.4.5 OpenSignatures

OpenSignatures is an implementation of the Snort syntax in the IBM Security Network IPS. Snort is an open source intrusion prevention and detection system (IDS/IPS). As such, it has an open method of signature development.

A large body of knowledge surrounds Snort, both among intrusion security professionals and freely available on the Internet. IBM uses this knowledge to allow IBM Network IPS administrators to create their own rules using the Snort signature language.

More information: Snort is developed by *Sourcefire*. For more information about Snort, see the Snort website at:

`http://www.snort.org/`

7.4.6 OpenSignature example

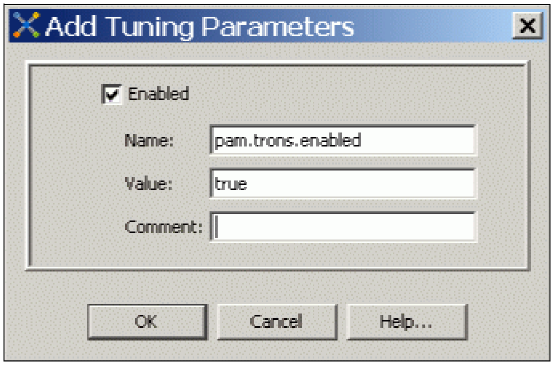
An analyst at the cardio healthcare company must create a custom signature. Based on a packet capture, the signature has the requirements shown in Example 7-2 on page 226.

Example 7-2 Custom signature requirements

```
Source IP: Any internal IP address on the 192.168.3.0/24 network
Destination IP: The ecommerce server at 192.168.6.105
Protocol: HTTP
Traffic specifics: a regular expression pay(ment|bill)\.php\?id\=payme
```

As the analyst for the cardio healthcare company, create the OpenSignature by using the following steps:

1. From the Default Repository, open the Tuning Parameters policy (Figure 7-1 on page 216).
2. In the Add Tuning Parameters dialog box (Figure 7-14), in the Name field, enter `pam.trons.enabled`. Then in the Value field, enter `true`.



Add Tuning Parameters

☑ Enabled

Name: pam.trons.enabled

Value: true

Comment:

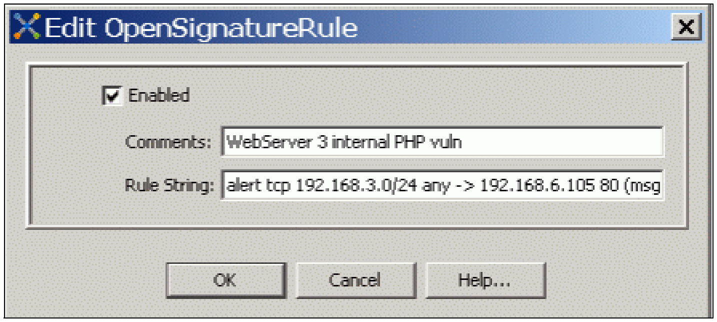
Figure 7-14 Enabling the OpenSignature engine

3. Craft an actual signature to meet the matching requirements using the open-source Snort signature syntax. The signature reads as shown in the following example:

```
alert tcp 192.168.3.0/24 any -> 192.168.6.105 80 (msg:”Custom XYZ -
php problem”,pcre:”pay(ment | bill)\.php\?id\=payme”)
```

> **Additional information available:** For more information about writing OpenSignatures, see *IBM Proventia Network Intrusion Prevention System Intrusion Prevention System OpenSignature User Guidelines*, which you can download from:
>
> http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/topic/com.ibm.opnsg.doc/pdfs/OpenSignatureUserGuide.pdf

4. Open the OpenSignature Events policy to add the rule. In the Edit OpenSignatureRule window (Figure 7-15), select **Enabled**. Enter the comments and rule string. Then click **OK**.



Comments: WebServer 3 internal PHP vuln

Rule String: alert tcp 192.168.3.0/24 any -> 192.168.6.105 80 (msg

Figure 7-15 Adding an OpenSignature rule

7.4.7 User Defined Events

With User Defined Events, an administrator can create a custom signature by using a protocol context and a regular expression. When defining a User Defined Event, the administrator starts with the protocol context. This context is a *pointer* that prompts the IPS engine for which protocols to inspect using the signature.

The context might be specific, such as a DNS query. This context might only ever apply to DNS UDP/53 query traffic. The context might also be less specific, such as email subject. This context might apply to all protocols where you find an email subject, such as POP3, SMTP, and IMAP.

Table 7-1 provides a full list of available contexts.

Table 7-1 Available protocol contexts for User Defined Events

DNS_Query	Email_Receiver	Email_Sender	Email_Subject
File_Name	News_Group	Password	SNMP_Community
URL_Data	User_Login_Name	User_Probe_Name	

After defining the context, the administrator then defines a regular expression that matches the unique traffic in the network.

7.4.8 User Defined Events example

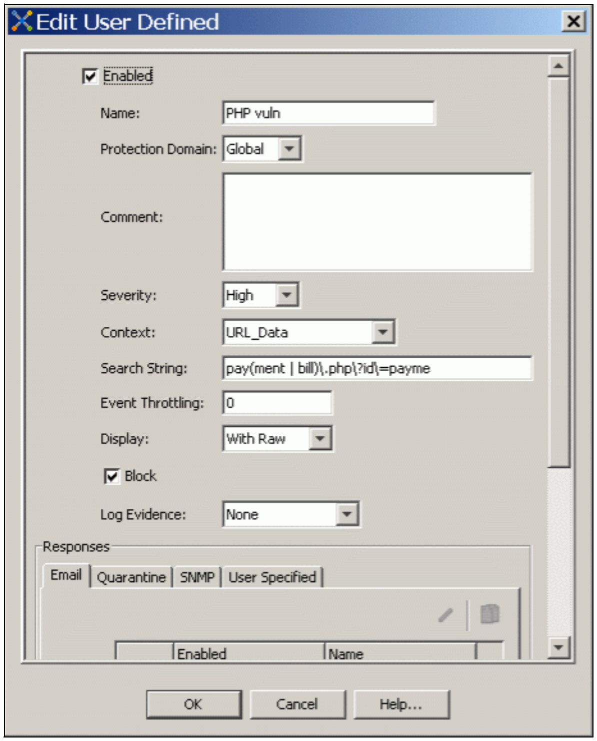
An analyst at the cardio healthcare company must create a custom signature. Based on a packet capture, the signature has the requirements shown in Example 7-3.

Example 7-3 The Custom Signature Requirements

```
Source IP: Any internal IP address on the 192.168.3.0/24 network
Destination IP: The ecommerce server at 192.168.6.105
Protocol: HTTP
Traffic specifics: a regular expression pay(ment|bill)\.php\?id\=payme
```

As the analyst for the cardio healthcare company, create the User Defined Event by using the following steps:

1. From the Default Policy Repository, open the User Defined Events policy.
2. In the Edit User Defined dialog box (Figure 7-16), for the Context drop-down list, select **URL_Data**. In the Search String field, enter `pay(ment|bill)\.php\?id\=payme`. Then click **OK**.



Edit User Defined

☑ Enabled

Name: PHP vuln

Protection Domain: Global

Comment:

Severity: High

Context: URL_Data

Search String: pay(ment | bill)\.php\?id\=payme

Event Throttling: 0

Display: With Raw

☑ Block

Log Evidence: None

Figure 7-16 A User Defined Event

7.5 Modifying default settings

Often an analyst wants to change the default settings recommended by the X-Force. There are many ways and reasons to change the default policy. This section explains how the cardio healthcare company makes bulk changes.

7.5.1 Protection domains

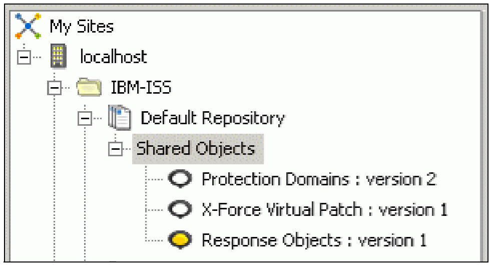
With protection domains, you can group signatures for the sake of editing all of them all at once. They can be set to match specific network IPS interfaces (for example, A, B, C, D), specific VLANs, specific IP addresses, or all of these items.

7.5.2 Protection domains example

After testing in a lab environment, an analyst decided that all HTTP-based signatures with a high severity must be enabled and set to block when targeting the web servers in the DMZ. To complete this task, the analyst uses a protection domain to filter the security events signatures for editing.

As the analyst for the cardio healthcare company, complete the following steps:

1. Define the protection domain. Protection domains are available under the Shared Objects folder (Figure 7-17).



My Sites
localhost
IBM-ISS
Default Repository
Shared Objects
Protection Domains : version 2
X-Force Virtual Patch : version 1
Response Objects : version 1

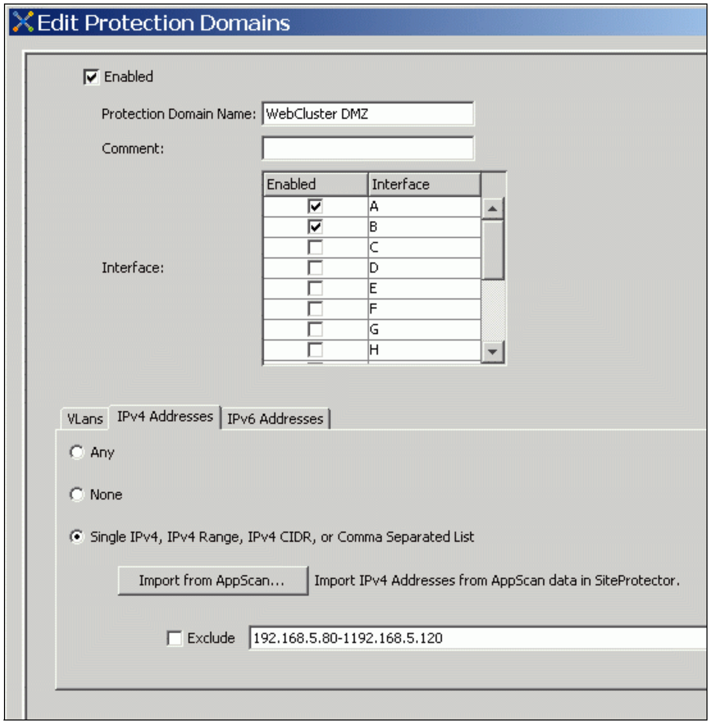
Figure 7-17 Shared Objects

2. In the Edit Protection Domains dialog box (Figure 7-18), define the protection domain to match the hosts in the DMZ that make up the web servers cluster:

   a. For Interface, under Enabled, select **A** and **B** because the DMZ is behind the A-B bridge.

   b. On the **IPv4 Addresses** tab, next to the **Exclude** check box, enter the IP range `192.168.5.80-192.168.5.120`.

   c. Click **OK**.



☑ Enabled

Protection Domain Name: WebCluster DMZ

Comment:

Interface:

Enabled	Interface
☑	A
☑	B
□	C
□	D
□	E
□	F
□	G
□	H

○ Any

○ None

● Single IPv4, IPv4 Range, IPv4 CIDR, or Comma Separated List

Import IPv4 Addresses from AppScan data in SiteProtector.

□ Exclude 192.168.5.80-1192.168.5.120

Figure 7-18 Protection domain definition

3. After the protection domain is defined, use it to categorize and modify signatures under the security events policy.

4. In the security events policy, regroup the signatures by protection domain.

5. In the Group By Columns dialog box (Figure 7-19), categorize all signatures by protection domain. From the All Columns list, select the item, and then click **Add** to move it to the Group By These Columns list. Alternatively, you can reverse the process by clicking **Remove** to move the items back to the All Columns list. Then click **OK**.

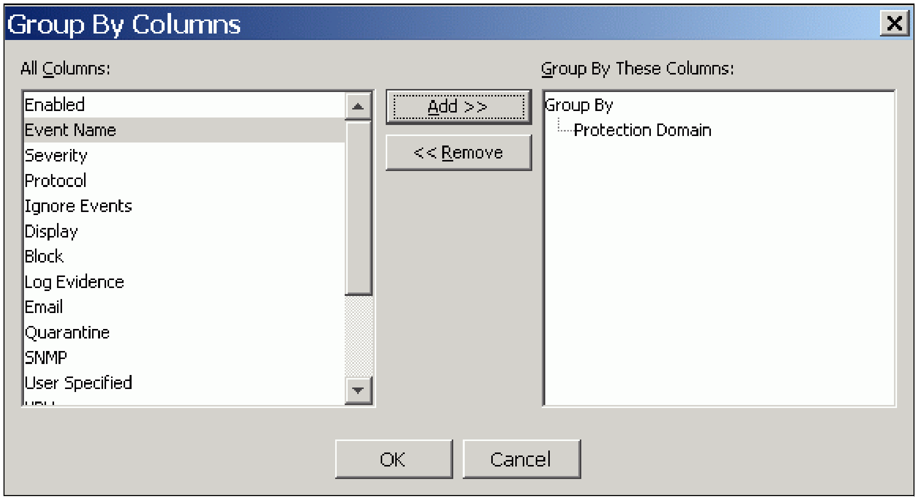
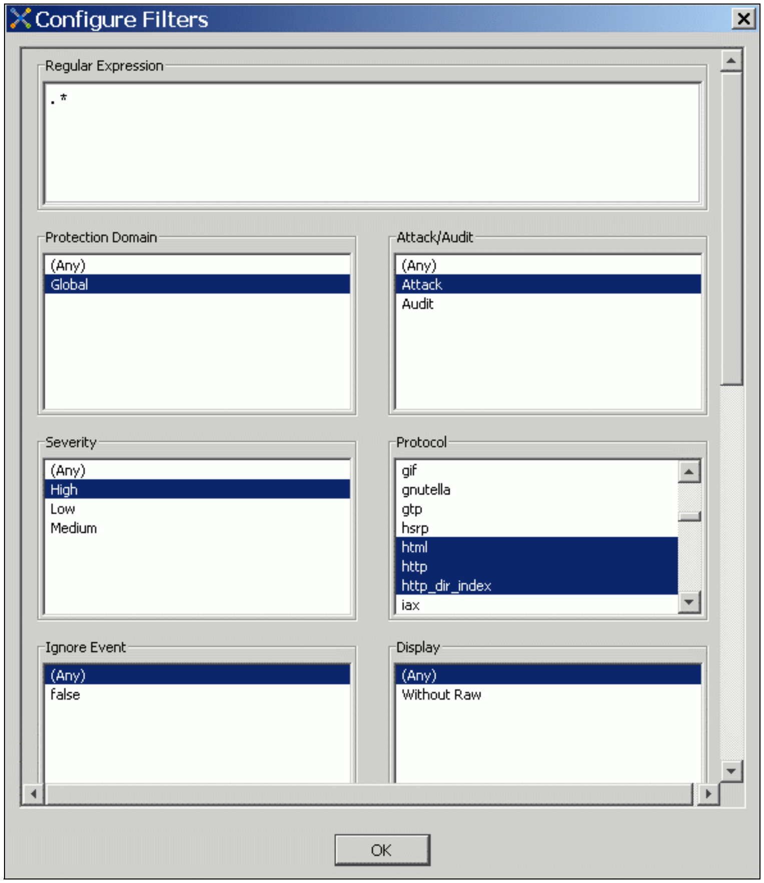


Figure 7-19 Group By Columns

6. When all signatures are grouped by protection domain, in the Configure Filters dialog box (Figure 7-20), filter the signatures for high severity, attack signatures for the web-based protocols. Then click **OK**.

> **Matching:** The regular expression of `.*` matches all patterns and, therefore, all tag names as shown in the example in Figure 7-20.



Configure Filters

Regular Expression
.*

Protection Domain
(Any)
Global

Attack/Audit
(Any)
Attack
Audit

Severity
(Any)
High
Low
Medium

Protocol
gif
gnutella
gtp
hsrp
html
http
http_dir_index
iax

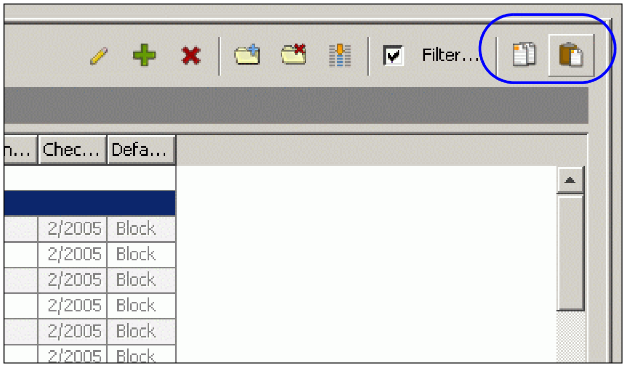
Ignore Event
(Any)
false

Display
(Any)
Without Raw

OK

Figure 7-20 Filtering for specific security event signatures

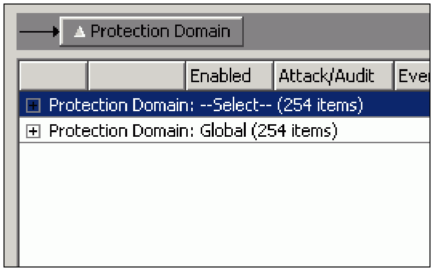
7. With this filter set, copy the filtered signatures to the clipboard, and then paste them immediately back into security events using the **Copy** and **Paste** toolbar buttons (Figure 7-21).



n...	Chec...	Defa...
	2/2005	Block
	2/2005	Block
	2/2005	Block
	2/2005	Block
	2/2005	Block
	2/2005	Block

Figure 7-21 Copy and Paste buttons on the toolbar

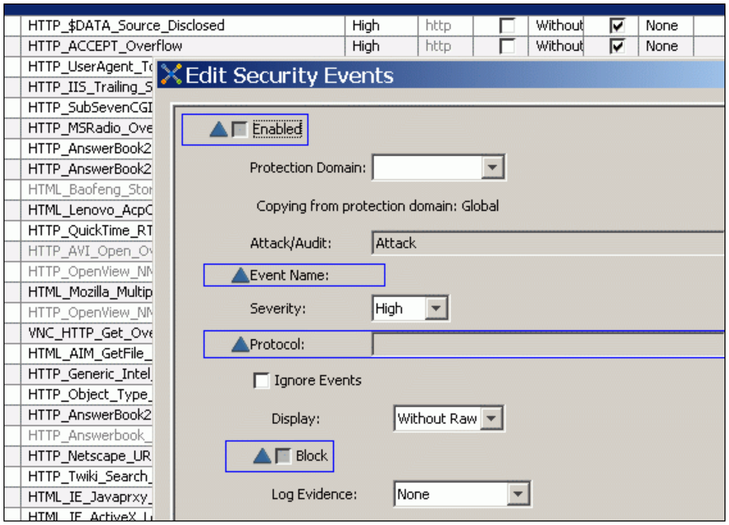
The pasted signatures are shown in the signature list without a protection domain (Figure 7-22).



		Enabled	Attack/Audit	Eve
⊞ Protection Domain: --Select-- (254 items)				
⊞ Protection Domain: Global (254 items)				

Figure 7-22 The results of the paste

8. Double-click the collection of signatures without a protection domain to edit the common features of all of the signatures (Figure 7-23).
9. In the Edit Security Events dialog box (inset in Figure 7-23), select the **Enabled** check box to enable all signatures for the WebCluster DMZ protection domain. Then select the **Block** check box for the signatures.



HTTP_$DATA_Source_Disclosed	High	http	□	Without	☑	None
HTTP_ACCEPT_Overflow	High	http	□	Without	☑	None
HTTP_UserAgent_To						
HTTP_IIS_Trailing_S						
HTTP_SubSevenCGI						
HTTP_MSRadio_Ove						
HTTP_AnswerBook2						
HTTP_AnswerBook2						
HTML_Baofeng_Stor						
HTML_Lenovo_AcpC						
HTTP_QuickTime_RT						
HTTP_AVI_Open_Ov						
HTTP_OpenView_NN						
HTML_Mozilla_Multip						
HTTP_OpenView_NN						
VNC_HTTP_Get_Ove						
HTML_AIM_GetFile_						
HTTP_Generic_Intel_						
HTTP_Object_Type_						
HTTP_AnswerBook2						
HTTP_Answerbook_						
HTTP_Netscape_UR						
HTTP_Twiki_Search_						
HTML_IE_Javaprxy_						
HTML_IE_ActiveX_L						

Edit Security Events

□ Enabled

Protection Domain:

Copying from protection domain: Global

Attack/Audit: Attack

Event Name:

Severity: High

Protocol:

□ Ignore Events

Display: Without Raw

□ Block

Log Evidence: None

Figure 7-23 Editing multiple signatures with one dialog box

7.6 Conclusion

The process of policy tuning is a constant and ongoing task because the networks and threat posture of those networks are constantly changing.

However, by performing initial tuning to remove false positives, the cardio healthcare company can move the appliances out of *inline simulation mode* and into *inline protection mode*. By understanding the process of identifying false negatives and creating custom signatures to eliminate them, the cardio healthcare company can use the full flexibility of the IBM Security Network Intrusion Prevention System to secure its networks.

A

Troubleshooting

This appendix explains where to find log information and how to use the information to identify and resolve possible issues. For additional troubleshooting and updated information, go to the IBM Support System at:

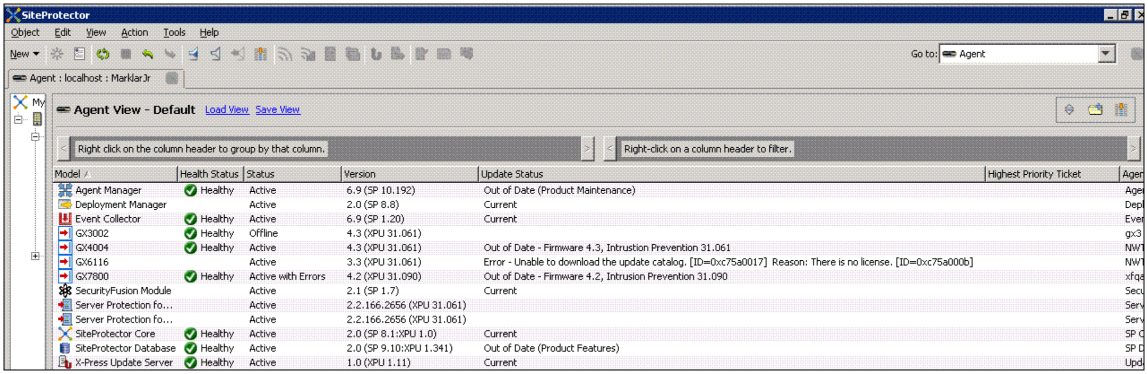
http://www.ibm.com/support

This appendix includes the following sections:

- Location of logs and system messages
- Definitions for health and system messages
- SiteProtector communication
- Identifying packet loss
- Conclusion

Location of logs and system messages

An IBM Security Network Intrusion Prevention System (IPS) agent that is registered to IBM Security SiteProtector can provide updated health and system information to the IBM Security SiteProtector system. SiteProtector shows the Health Status and Update Status of the Security Network IPS in the Agent View columns (Figure A-1). To view detailed information about the status, you can right-click the agent and choose **Properties**.


SiteProtector
Object
Edit
View
Action
Tools
Help
New
Go to:
Agent
Agent : localhost : MarklarJr
My
Agent View - Default
Load View
Save View
Right click on the column header to group by that column.
Right-click on a column header to filter.

Model	Health Status	Status	Version	Update Status	Highest Priority Ticket	Ager
Agent Manager	✓ Healthy	Active	6.9 (SP 10.192)	Out of Date (Product Maintenance)		Age
Deployment Manager		Active	2.0 (SP 8.8)	Current		Depl
Event Collector	✓ Healthy	Active	6.9 (SP 1.20)	Current		Ever
GX3002	✓ Healthy	Offline	4.3 (XPU 31.061)			gx3
GX4004	✓ Healthy	Active	4.3 (XPU 31.061)	Out of Date - Firmware 4.3, Intrustion Prevention 31.061		NWT
GX6116		Active	3.3 (XPU 31.061)	Error - Unable to download the update catalog. [ID=0xc75a0017] Reason: There is no license. [ID=0xc75a000b]		NWT
GX7800	✓ Healthy	Active with Errors	4.2 (XPU 31.090)	Out of Date - Firmware 4.2, Intrusion Prevention 31.090		xfqa
SecurityFusion Module		Active	2.1 (SP 1.7)	Current		Secu
Server Protection fo...		Active	2.2.166.2656 (XPU 31.061)			Serv
Server Protection fo...		Active	2.2.166.2656 (XPU 31.061)			Serv
SiteProtector Core	✓ Healthy	Active	2.0 (SP 8.1:XPU 1.0)	Current		SP C
SiteProtector Database	✓ Healthy	Active	2.0 (SP 9.10:XPU 1.341)	Out of Date (Product Features)		SP D
X-Press Update Server	✓ Healthy	Active	1.0 (XPU 1.11)	Current		Upd

Figure A-1 Agent view in IBM Security SiteProtector

The local management interface (LMI) of the IBM Security Network IPS can also provide updated health and system information. The Home Appliance Dashboard contains an overview of the status for Network health, Security health, System health, and SiteProtector health. If there are any warning or errors, you can view a brief description of the issue. You can click the individual dashboard links for more details:

Network dashboard Shows the current link state for each security interface. Also shows information about throughput and packet rate.

Security dashboard Shows the current license state and information about Security alerts.

System dashboard Shows the current system information, such as firmware version, uptime, memory utilization, and percentage of storage in use.

Significant events Provides details about why any of the health checks failed. To access this information, select **Monitor Health and Statistics**, and then click **System**.

System Provides detailed information about health checks. These messages include informative, warning, and error messages. The messages contain detailed information about why a health check failed. To access this information, select **Review Analysis and Diagnostics**.

The *logs* that are accessible from IBM Security SiteProtector and the LMI are also accessible from a command line when logging in remotely using Secure Shell (SSH). The logs are for experienced Network IPS users. The reason is that changes that are made while logged in as a root user can have adverse effects on the system and must generally be used only when working with IBM Technical Support. To help you better understand the implications of using root user access, see 3.6.1, “Root user considerations” on page 102.

Typically you examine the following messages and log files:

- System-level messages are in the `/cache/log/messages` logs. These logs are kept for 30 days, and they are rotated daily.
- The inspection engine logs are in the `/cache/iss/engine0.log` files. These logs contain detailed information about the initialization and running status of the inspection engine. These logs are rotated each time the system is initialized.
- The Protocol Analysis Module (PAM) logs are in the `/cache/iss/pam0.log` files. These log files contain details about the configuration of PAM and about the initialization and running status of PAM. They are rotated each time the system is initialized.

When working with IBM Technical Support, you might be asked to provide a *Provinfo* file from the appliance on which you are working. The Provinfo file contains the previously mentioned system logs, current configuration, and other information that is necessary to help troubleshoot any issues you might have. You can generate and download the Provinfo file from the LMI by following the General Support link at the bottom of any page in the LMI.

Definitions for health and system messages

This section provides definitions about the health and system messages. These definitions are the same for the information in IBM Security SiteProtector and the LMI. IBM Security SiteProtector has a link in the message details to provide possible solutions to messages that have a *Warning* or *Error* status.

System

The following system messages are possible:

Last discovery
Tracks the last time the Network IPS appliance was able to check for new content. The health check fails when the appliance is unable to check for new content in the specified time frame.

Possible causes are a missing or expired license, incorrect domain name system (DNS) settings, incorrect license and update server settings, or general networking issues.

Appliance restart
Contains information about the restart status of the IBM Security Network IPS appliance. This check fails when the appliance was restarted in the last 24 hours.

Possible causes are a scheduled appliance restart, power loss, or hardware failure.

SiteProtector policy configuration
Contains information that helps you verify that, during the last heartbeat, the IBM Security Network IPS appliance received configuration information from the IBM Security SiteProtector system.

Possible causes are an incorrectly configured policy or SiteProtector Agent Manager communication issues.

Appliance initialization
Contains information about the status of the primary initialization of the IBM Security Network IPS appliance. This health check fails when issues are detected when starting the appliance.

Possible causes are an incorrectly configured policy, incorrect network settings (such as Simple Network Management Protocol (SNMP) or EMAIL responses), or program errors that require patching.

Critical processes
Contains information about the status of critical security processes running on the IBM Security Network IPS appliance. This health check fails when any of the critical security processes stop running on the appliance.

Possible causes are an incorrectly configured policy or program errors that require patching.

Allocated user memory
Contains information about the percentage of memory that is used by the IBM Security Network IPS appliance. If

memory usage increases too much, the firmware might stop running.

Possible causes are an incorrectly configured policy or appliance performance exceeded.

Root partition Contains information about the percentage of used space in the root partition of the IBM Security Network IPS appliance. If the root partition of the appliance becomes full, the firmware might stop running.

Possible causes are an incorrectly configured policy or improper system customization that uses the root partition.

Cache partition Contains information about the percentage of used space in the cache partition of the IBM Security Network IPS appliance. If the cache partition of the appliance becomes full, the firmware might stop running.

Possible causes are an incorrectly configured policy, improper system customization that uses the root partition, an excessive number of update files, or an excessive number of log files.

Internal communication

Contains information about the status of communications between the IBM Security Network IPS appliance and the IBM Security SiteProtector system. This health check fails when the appliance is unable to communicate with the IBM Security SiteProtector system.

Possible causes are an incorrectly configured SiteProtector Management policy, incorrect DNS settings, or general networking issues.

Security

One security message might be issued, the *Intrusion Prevention license state* message. This message contains information about the Intrusion Prevention license state for the IBM Security Network IPS appliance. This health check fails when the appliance does not have an active Intrusion Prevention license. If this health check fails, the appliance does not receive content updates, nor does it apply any content that is manually transferred to the system.

The possible causes are that the license is not applied or the license expired.

Network

One network message might be issued, the *Security interfaces* message. This message contains information about the state of the security ports on the IBM Security Network IPS appliance. This health check fails when the appliance loses connectivity to one or more security ports. Only security interfaces that have had an active link since the last system start are monitored by this health check. Unused security interfaces are not monitored by this health check.

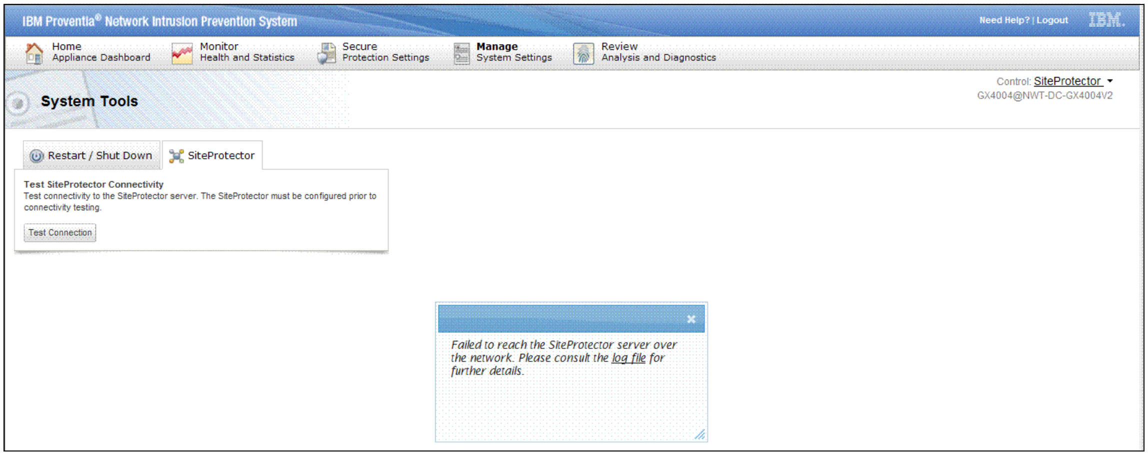
Agent messages

The Agent messages provide details about various system and health checks. The Warning and Error messages can provide more details about the cause of any system or health checks.

SiteProtector communication

Methods are available for checking the communication path between the IBM Security Network IPS appliance and IBM Security SiteProtector. When trying to register a network IPS to SiteProtector, the most common cause of failure is related to networking issues. Tools are available to help identify the issue.

To access a utility to test the connectivity of IBM Security SiteProtector, select **Manage System Settings** and then click **System Tools**. If the communication check fails, a window opens with a link to the log file (Figure A-2).



Test SiteProtector Connectivity
Test connectivity to the SiteProtector server. The SiteProtector must be configured prior to connectivity testing.

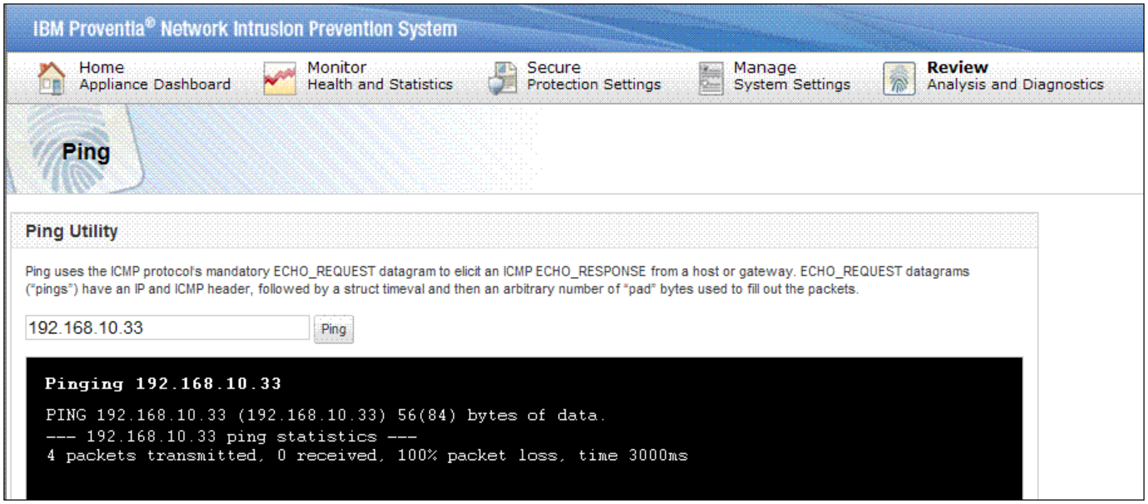
Failed to reach the SiteProtector server over the network. Please consult the log file for further details.

Figure A-2 SiteProtector communication failure

A networking issue results in the following message at the end of the log file:

```
“The send operation failed due to a communication failure.
[ID=0xc7590009]”
```

In the Review Analysis and Diagnostics section of the LMI, you can find Ping (Figure A-3) and Traceroute utilities to help confirm that the IBM Security Network IPS can reach the IBM Security SiteProtector system. These tools use Internet Control Message Protocol (ICMP) ECHO requests to attempt to reach the IBM Security SiteProtector system.


IBM Proventia® Network Intrusion Prevention System
Home Appliance Dashboard
Monitor Health and Statistics
Secure Protection Settings
Manage System Settings
Review Analysis and Diagnostics
Ping
Ping Utility
Ping

Ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams ("pings") have an IP and ICMP header, followed by a struct timeval and then an arbitrary number of "pad" bytes used to fill out the packets.

192.168.10.33

```
Pinging 192.168.10.33
PING 192.168.10.33 (192.168.10.33) 56(84) bytes of data.
--- 192.168.10.33 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3000ms
```

Figure A-3 Ping failure

If your network does not allow ICMP traffic, you can use the Telnet command to determine if the IP address is reachable from a TCP session. If the IBM Security Network IPS cannot reach the IP address, you receive an error message similar to the one in Example A-1.

Example A-1 IP connectivity problem

```
#telnet 192.168.0.33 3995
Trying 192.168.0.33...
telnet: connect to address 192.168.0.33: Connection timed out
```

The possible cause for this error message might be that the appropriate routes are not configured in the network, a firewall is not configured to allow this type of traffic, or the SiteProtector Agent Manager is not running.

If the IBM Security Network IPS can reach the IP address, but not the appropriate port, you receive an error message similar to the one in Example A-2.

Example A-2 Port connectivity problem

```
#telnet 192.168.0.33 3995
Trying 192.168.0.3...
telnet: connect to address 9.55.226.197: Connection refused
```

The possible cause for this error message might be that a firewall is not configured to allow traffic on this port or that the SiteProctector Agent Manager is not running.

Example A-3 shows a successful connection.

Example A-3 Successful connection

```
#telnet 192.168.0.33 3994
Trying 9.55.220.210...
Connected to 9.55.220.210.
Escape character is '^]'.
```

If you are using DNS entries to assign the Agent Manager, you can use the **`nslookup`** or **`dig`** commands to check DNS resolution. Example A-4 shows a DNS lookup failure by using the **`nslookup`** command.

Example A-4 An nslookup failure

```
#nslookup siteprotector.testlab.int
Server:         192.168.0.53
Address:        192.168.0.53#53

** server can't siteprotector.testlab.int: NXDOMAIN
```

The possible cause for this issue might be an incorrect DNS entry in the IBM Security Network IPS configuration or that the DNS entry does not exist on the assigned DNS.

Example A-5 shows a successful DNS lookup.

Example A-5 A successful nslookup

```
# nslookup siteprotector.testlab.int
Server:         192.168.0.53
Address:        192.168.0.53#53
```

```
Non-authoritative answer:
Name:   siteprotector.testlab.int
Address: 192.168.0.33
```

If all the communication settings are correct, you must investigate the status of the *iss-spa* process that controls the communication between the IBM Security Network IPS and IBM Security SiteProtector. You can check the status by running the **`service iss-spa status`** command.

The normal status that is returned is `running`. If the status returns as `unused` or `stopped`, the process was manually terminated or the IBM Security Network IPS is not configured to be managed by IBM Security SiteProtector. If the status returns as `dead`, a system error occurred. You can try to recover from an error state by running the **`service iss-spa start`** command.

Identifying packet loss

When the IBM Security Network IPS is configured to *inline protection mode*, packets are dropped from the network for many reasons. The main reason the drop occurs is that the IBM Security Network IPS identified traffic that matches *security events* configured in the policy.

You can view security event details that include IP and port information in the Analysis View in SiteProtector and in the Security Alerts section in the LMI. Events with block responses show that the traffic is blocked. Security events that are not configured with a block response show as *detected*. Packet loss can also occur if *connection events*, *OpenSignatures*, *user-defined events*, or *firewall rules* are configured with a block response.

Packet loss can occur due to a *quarantine response* for an event that was configured with a quarantine response and the matching security event was triggered. The quarantine rules section of the LMI shows a list of current quarantine rules.

If the security interfaces are not configured to have the same speed and duplex setting as connected devices, packets can be dropped at the physical layer. To view the current link and speed status of the security interfaces in SiteProtector, right-click the agent and choose **Properties**. In the Network Information section, you can see the current link status. You can also see the current link status on the Home dashboard page in the LMI.

For all IBM Security Network IPS G and GX systems, the following counters for dropped packets do not directly correlate to a security event, connection event, OpenSignature response, quarantine block, or a firewall drop rule. All packets that are dropped, except malformed Ethernet frames or resource errors, can be logged by using the `engine.droplog.enabled` parameter. This parameter triggers a write of the actual packets being dropped to the `/cache/iss/` directory on the G or GX system. These files ware ill be designated as `dropXXXX.enc`.

- Packets dropped due to check sum errors:
  - The number of ICMP packets with checksum errors detected

    `pam.icmp.xsum_errs`
  - The number of ICMP version 6 packets with checksum errors detected

    `pam.icmpv6.xsum_errs`
  - The number of IP version 4 packets with checksum errors

    `pam.ipv4.xsum_errs`
  - The number of Open Shortest Path First (OSPF) packets detected

    `pam.ospf.xsum_errs`
  - The number of Transmission Control Protocol (TCP) packets with checksum errors detected

    `pam.tcp.xsum_errs`
  - The number of User Datagram Protocol (UDP) packets detected

    `pam.udp.xsum_errs`

  The dropping of invalid checksums is tunable by using the `np.drop.invalid.checksum` parameter. The default value is `true`.
- Packets dropped due to protocol violation, truncation, or denial-of-service attack (DoS) protection:
  - The number of Ethernet packets dropped because they were truncated

    `pam.ethernet.truncated.dropped`
  - The number of IP version 4 packets dropped because of improper headers

    `pam.ipv4.bad_header.dropped`
  - The number of IP version 4 packets dropped because of truncated data

    `pam.ipv4.truncated.dropped`
  - The number of Point-to-Point Protocol over Ethernet (PPPoE) packets dropped because they were truncated

    `pam.pppoe.truncated.dropped`

  - The number of PPPoE packets dropped because they were of an unknown type

    `pam.pppoe.unknown.dropped`

  - Error condition tracking where data on a TCP stream cannot be correctly reassembled because the available stream buffer table is empty

    `pam.tcp.segments.dropped`

    PAM reassembles source and destination traffic to ensure that the TCP stream is processed in order. If the sensor receives a sizeable number of out-of-order segments, and the active connections are relatively high, this error condition might be reached. In a common case, the ratio of `pam.tcp.segments/pam.tcp.connections.active` is approximately 1.0. A much larger value might indicate a problem in your network.

  - The number of TCP SYN packets dropped during a SYN flood

    `pam.tcp.synflood.dropped`

  - The number of TCP connections dropped after inactivity

    `pam.tcp.timeouts`

  Dropping these types of packets is tunable by using the `np.drop.invalid.protocol` parameter. The default value is `true`.

- Packets dropped due to a resource error (disabled by default):

  - The number of IPv6 fragments dropped for a lack of resources

    `pam.ipv6.fragments.dropped`

  - Error condition tracking where data on a TCP stream cannot be correctly reassembled because the available stream buffer table is empty

    `pam.tcp.segments.dropped`

  Other packets might be dropped without being recorded due to resource errors.

- Specific to the GX7412 and GX7800 in Inline Protection Mode

  The following types of errors might result in packets being dropped by the communication processor by default. Counters for each are on the Network Statistics Page of the LMI. It is not possible to record the actual packets that are being dropped by the communication processor.

  - The number of 802.1Q frames that were truncated or that contained protocol violations

    `pam.look.vlan.errors`

- The number of PPPoE frames that were truncated or that contained protocol violations

  `pam.look.pppoe.errors`

- The number of MPLS frames that were truncated or that contained protocol violations

  `pam.look.mpls.errors`

- The number of Cisco inter-switch link (ISL) frames that were truncated or that contained protocol violations

  `pam.look.isl.frames`

- The number of IPv4 frames that were truncated or that contained protocol violations

  `pam.look.ip.errors`

- The number of IPv6 frames that were truncated or that contained protocol violations

  `pam.look.ipv6.errors`

- The number of IPv4 frames that encountered checksum errors

  `pam.look.ip.checksum.errors`

- The number of General Routing Encapsulation frames that were truncated or that contained protocol violations

  `pam.look.gre.errors`

- The number of TCP frames that were truncated or that contained protocol violations

  `pam.look.tcp.errors`

- The number of TCP frames that encountered checksum errors

  `pam.look.tcp.checksum.errors`

- The number of UDP frames that were truncated or that contained protocol violations

  `pam.look.udp.errors`

- The number of UDP frames that encountered checksum errors

  `pam.look.udp.checksum.errors`

- The number of ICMP frames that were truncated or that contained protocol violations

  `pam.look.icmp.errors`

  - The number of ICMP and ICMPv6 frames that encountered checksum errors

    `pam.look.icmp.checksum.errors`

  - The number of domain name server (DNS) frames that were truncated or that contained protocol violations

    `pam.look.dns.malformed`

  - The total number of packets that were dropped related to the previous errors

    `pam.look.route.drop`

    This statistic does not include the number of packets that were dropped due to the action result of the deep-inspection engine. This statistic includes packets that are dropped due to malformed Ethernet frames.

- Additional information regarding physical layer errors

  All Ethernet capable operating systems are susceptible to physical errors that cause malformed Ethernet frames. Packets of these types are typically never viewed by the OS and are dropped at the network interface card (NIC) level.

  For Network IPS G or GX appliances, this statistic is included in the overall drop count for Driver Statistics. You can view Malformed Ethernet frame errors in the output of the **/etc/iss/drivers/adapterdump -s** command when logged in by using SSH, as a root user. Malformed Ethernet frames are identified by the RcvErr counter. The **adapterdump -s** command produces output of the low-level driver statistics for each security interface. You can run this command on IBM Security Network IPS G or GX appliances, except for the GX7800 appliance.

  Example A-6 shows the output of the **adapterdump -s** command.

  Example A-6 Output from the adapterdump command

  ```
  Global RxdPkt= 1579 TxdPkt= 1578 FwdPkt= 1578 DrpPkt= 1
  UnpPkt= 0 InjPkt= 0 RBytes= 550107 TBytes= 549617
  RcvErr= 0
  Dvc 0 RxdPkt= 14 TxdPkt= 0 FwdPkt= 13 DrpPkt= 1
  UnpPkt= 0 InjPkt= 0 RBytes= 1928 TBytes= 0
  RcvErr= 0
  Dvc 1 RxdPkt= 0 TxdPkt= 13
  ```

  A count for RcvErr (Receive Error) greater than zero indicates that packets are lost at the physical layer. Check that the link speed and duplex settings for the security interface are the same as for connected network devices. The errors might also be caused by bad cabling or a failing NIC in the IBM Security Network IPS or connected network device.

Conclusion

This appendix helped to identify some of the more common issues when working with the IBM Security Network IPS device. For more articles about known issues and for configuration help with additional details, see the IBM Technote System.

For more information, see the IBM Support Portal at the following address, and select the **IBM Security Network Intrusion Prevention System** as your product:

http://www.ibm.com/support

If you require additional assistance, contact the IBM Technical Support Team.

Reminder: Provide IBM Support your Provinfo file.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Some publications referenced in this list might be available in softcopy only.

- *IBM Security Solutions 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
- *Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security*, REDP-4528
- *Security in Development: The IBM Secure Engineering Framework*, REDP-4641

You can search for, view, download or order these documents and other Redbooks, Redpapers, Web Docs, draft and additional materials, at the following website:

ibm.com/redbooks

Online resources

These websites are also relevant as further information sources:

- Product documentation in the IBM Security Network IPS Information Center

  http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp?topic=/com.ibm.ips.doc/IBMSecNetIPS_landing_page.html

- The Open Web Application Security Project (OWASP) site

  https://www.owasp.org/index.php/Main_Page

  OWASP is a not-for-profit worldwide charitable organization focused on improving the security of application software. Its mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks. Everyone is free to participate in OWASP and all of the materials are available under a free and open software license.

- The Web Application Security Consortium (WASC) site

  `http://www.webappsec.org/`

  WASC is a non-profit organization made up of an international group of experts, industry practitioners, and organizational representatives. They produce open source and widely agreed upon best-practice security standards for the World Wide Web.

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

IBM

Redbooks

Network Intrusion Prevention Design Guide: Using IBM Security Network IPS

(1.0” spine)
0.875”<->1.498”
460 <-> 788 pages

(0.5” spine)
0.475”<->0.875”
250 <-> 459 pages

(0.2”spine)
0.17”<->0.473”
90<->249 pages

(0.1”spine)
0.1”<->0.169”
53<->89 pages

Network Intrusion Prevention Design Guide

Using IBM Security Network IPS

Enterprise integration for network intrusion prevention

Complete information about architecture and components

Deployment scenario with hands-on details

Every organization today needs to manage the risk of exposing business-critical data, improve business continuity, and minimize the cost of managing IT security. Most all IT assets of an organization share a common network infrastructure. Therefore, the first line of defense is to establish proper network security. This security is a prerequisite for a logical set of technical countermeasures to protect from many different attack vectors that use the network to infiltrate the backbone of an organization.

The IBM Security Network Intrusion Prevention System (IPS) stops network-based threats before they can impact the business operations of an organization. Preemptive protection, which is protection that works ahead of a threat, is available by means of a combination of line-speed performance, security intelligence, and a modular protection engine that enables security convergence. By consolidating network security demands for data security and protection for web applications, the IBM Security Network IPS serves as the security platform that can reduce the costs and complexity of deploying and managing point solutions.

This IBM Redbooks publication provides IT architects and security specialists a better understanding of the challenging topic of blocking network threats. This book highlights security convergence of IBM Virtual Patch technology, data security, and Web Application Protection. In addition, this book explores the technical foundation of the IBM Security Network IPS. It explains how to set up, configure, and maintain proper network perimeter protection within a real-world business scenario.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7979-00 ISBN 0738436216