Internet Security Systems

ISS Products Overview & Technical Enablement

Tivoli Internet Security Systems

Aytug Celikbas – *IT Security Specialist, CEE*
IBM Tivoli Internet Security Systems

Tivoli. IBM Internet Security Systems

Agenda

1 IBM ISS Product Portfolio

2 IBM Security Network IPS + Initial Configuration Demo

3 IBM Security Server Protection Solutions (VSP + Host IPS)

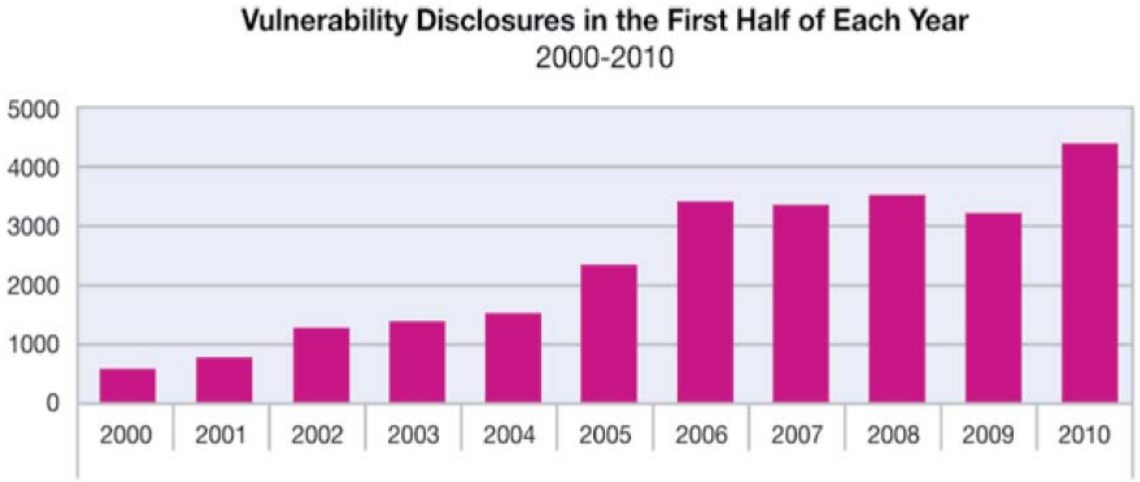
4 SiteProtector Training + Demonstration of the Products

5 Access to Resources (Training + Docs + Support)

6 Questions & Answers

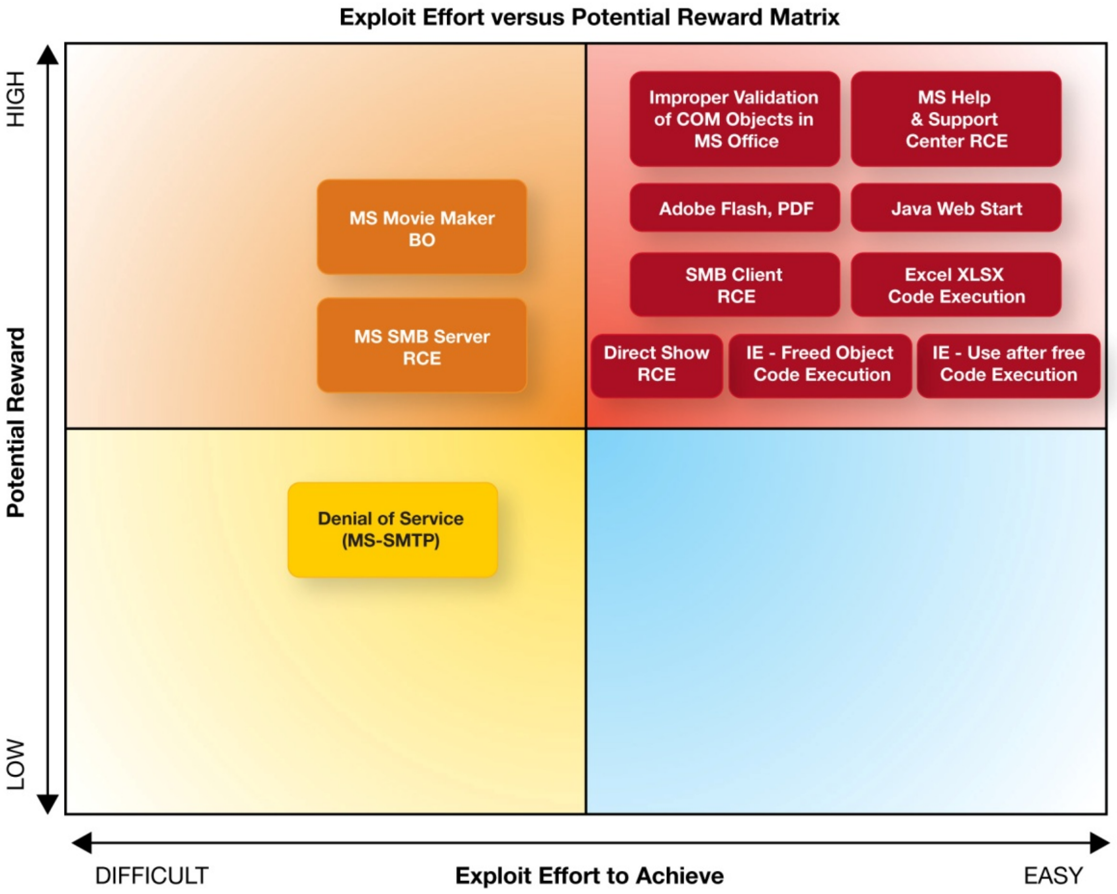
Vendors Reporting More Vulnerabilities Than Ever Before: Vulnerability Disclosures at an All-Time High

- Vulnerability disclosures up **36%.**
  - Web applications continue to be the largest category of disclosure.
- Increase in vulnerability disclosures due to significant increases in public exploit releases and to efforts by several vendors to identify and mitigate security vulnerabilities.
- The most critical two vulnerabilities disclosed in the first half of 2010 were remote code execution vulnerabilities in Java Web Start and Microsoft Windows Help and Support Center
  - Both were publicly disclosed before patches were available from the respective vendors



Exploit Effort vs. Potential Reward

- Economics continue to play heavily into the exploitation probability of a vulnerability
- Web Browser, Document Reader and Office document vulnerabilities are very profitable and easily executable

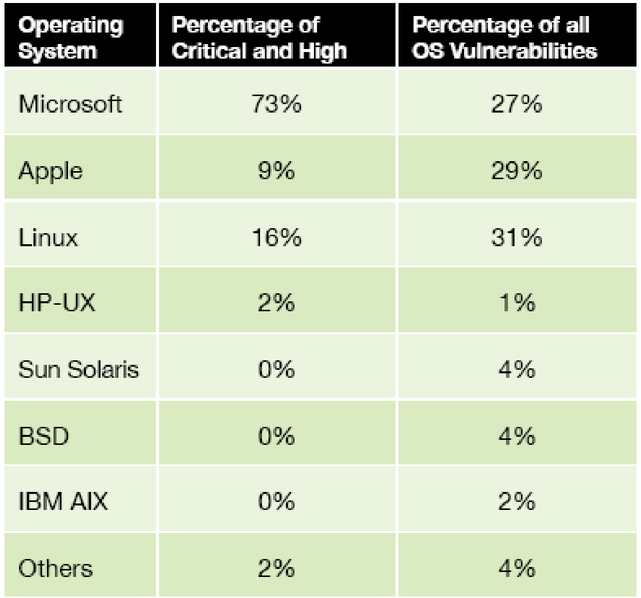

Exploit Effort versus Potential Reward Matrix
HIGH
Potential Reward
LOW
Improper Validation of COM Objects in MS Office
MS Help & Support Center RCE
Adobe Flash, PDF
Java Web Start
SMB Client RCE
Excel XLSX Code Execution
Direct Show RCE
IE - Freed Object Code Execution
IE - Use after free Code Execution
MS Movie Maker BO
MS SMB Server RCE
Denial of Service (MS-SMTP)
DIFFICULT
Exploit Effort to Achieve
EASY

Source: IBM X-Force®

Patches Still Unavailable for Over Half of Vulnerabilities

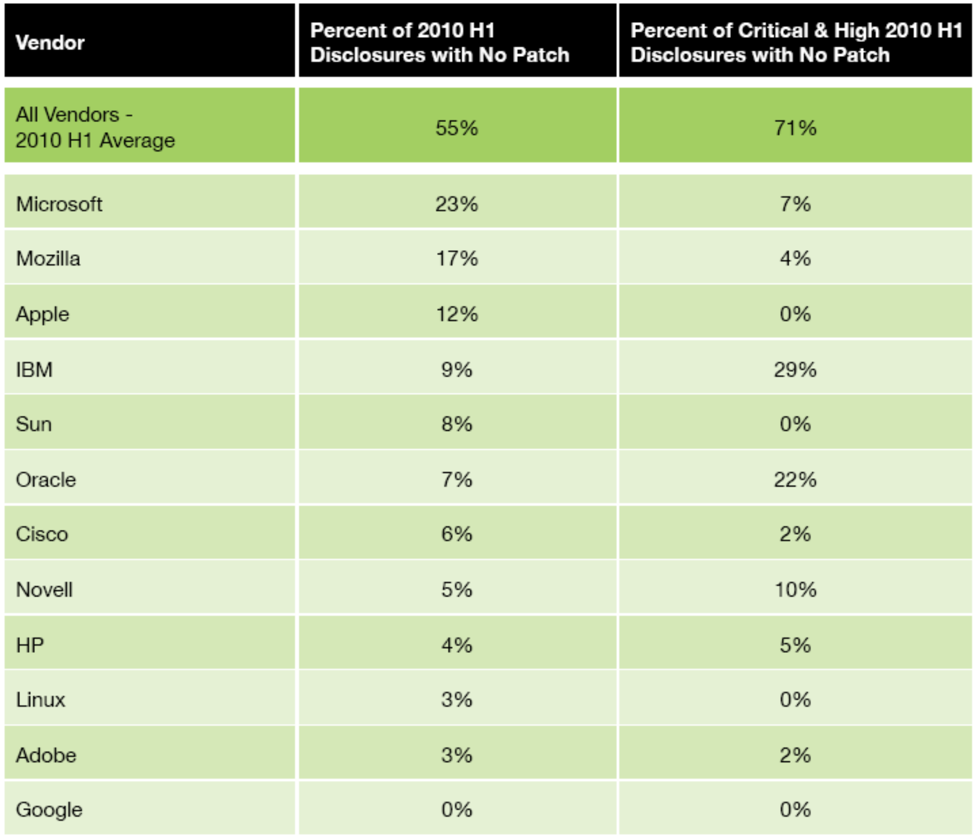
- Over half (**55%**) of all vulnerabilities disclosed in the 1st half of 2010 had no vendor-supplied patches to remedy the vulnerability. **71%** of critical & high vulnerabilities have no patch.

- Top five operating systems account for **98%** of all critical and high operating system disclosures in the first half of 2010. The top five operating systems account for **95%** of all operating system vulnerability disclosures.



Operating System	Percentage of Critical and High	Percentage of all OS Vulnerabilities
Microsoft	73%	27%
Apple	9%	29%
Linux	16%	31%
HP-UX	2%	1%
Sun Solaris	0%	4%
BSD	0%	4%
IBM AIX	0%	2%
Others	2%	4%

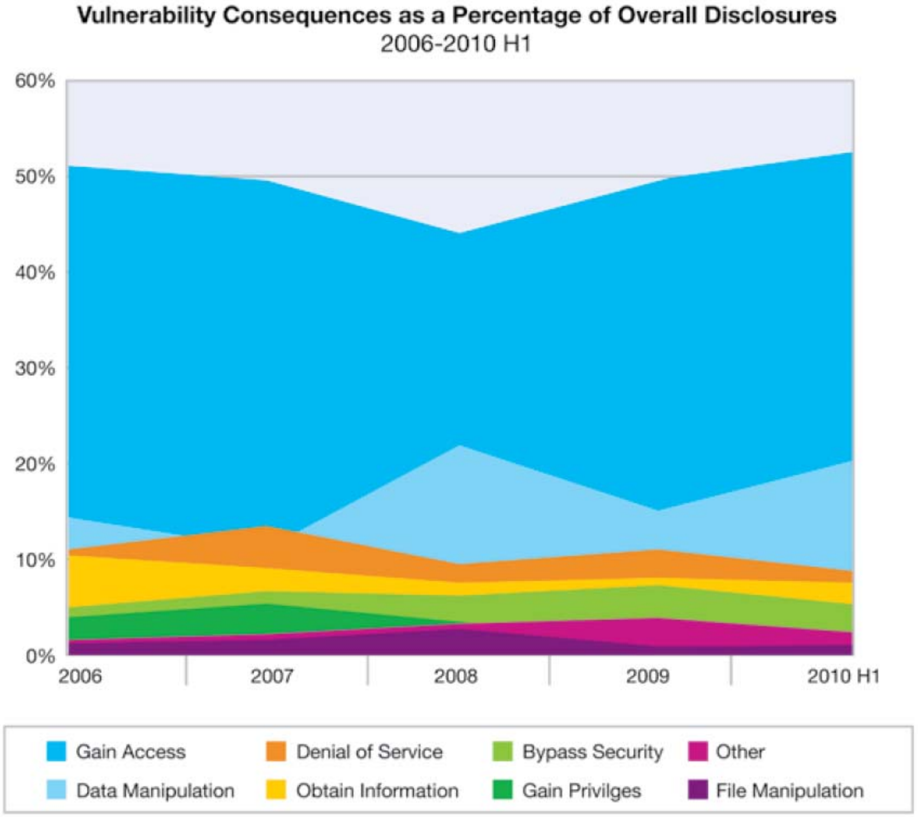
Table 9: Operating systems with the most critical and high vulnerability disclosures, 2010 H1.



Vendor	Percent of 2010 H1 Disclosures with No Patch	Percent of Critical & High 2010 H1 Disclosures with No Patch
All Vendors - 2010 H1 Average	55%	71%
Microsoft	23%	7%
Mozilla	17%	4%
Apple	12%	0%
IBM	9%	29%
Sun	8%	0%
Oracle	7%	22%
Cisco	6%	2%
Novell	5%	10%
HP	4%	5%
Linux	3%	0%
Adobe	3%	2%
Google	0%	0%

1st Half 2010 Attacker Motivation is to Gain Access and Manipulate Data

- "Gain access" remains the primary consequence of vulnerability exploitation.
  - Up to **52%** in the 1st half of 2010 as compared to 50% in 2009.
- "Data Manipulation" on the rise.
  - Up to **21%** in the 1st half of 2010
- "Bypass Security" and "Denial of Service" remain similar to previous years.



Questions to Ask:

- Are you confident that an attacker can not gain access to your system?
- Is your private data secure?

IBM Security Offerings:

- IBM Tivoli Identity & Access Management Products & Services
- IBM Security Network, Server and Endpoint Prevention products and services
- IBM Web Application Security Products & Services (Rational, IBM Security Network IPS, Data Power, MSS)
- IBM Data Security products and services (Guardium, Big Fix, MSS)

X-Force R&D - Unmatched Security Leadership

The mission of the IBM X-Force® research and development team is to:

- Research and evaluate threat and protection issues
- Deliver security protection for today’s security problems
- Develop new technology for tomorrow’s security challenges
- Educate the media and user communities

X-FORCE

X-Force Research

10B	analyzed Web pages & images
150M	intrusion attempts daily
40M	spam & phishing attacks
51K	documented vulnerabilities

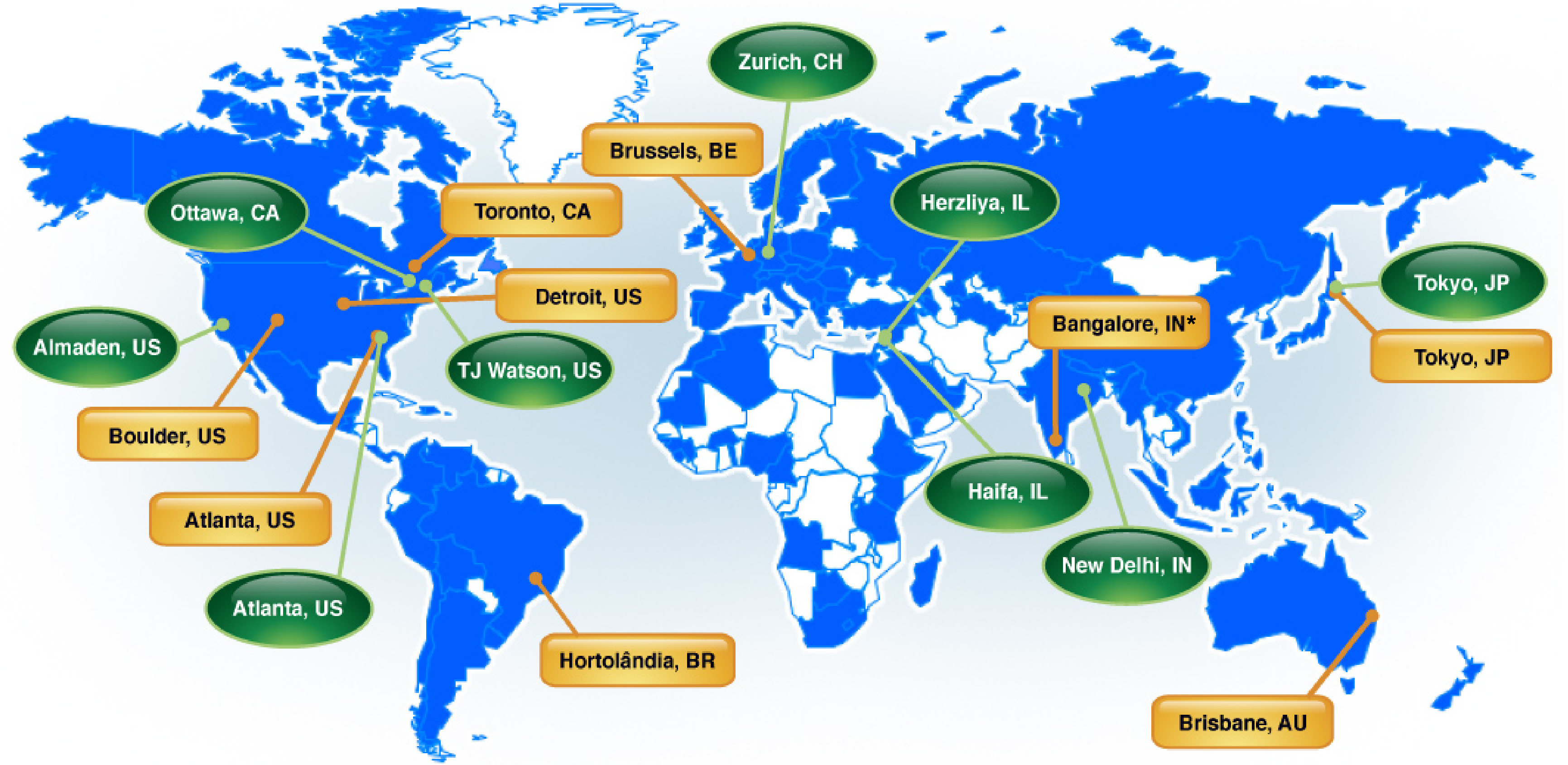
Millions of unique malware samples

Provides Specific Analysis of:

- Vulnerabilities & exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

IBM’s Global Security Reach and Expertise

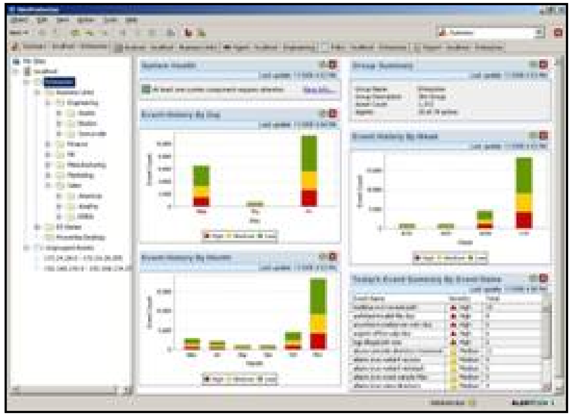
9 Security Operations Centers + 9 Security Research Centers + 133 Monitored Countries + 20,000+ Devices under Contract + 3,700+ MSS Clients Worldwide + 4 Billion+ Events Per Day



IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security

SiteProtector

Unified Enterprise Security Console for all products



Enterprise Protection Products

IBM Security Network Protection

Proventia Gx IPS

Proventia Mail Security

Enterprise Network Scanner

IBM Security Server Protection

Proventia Server

Virtual Server Security

- Protect all assets on the network with Virtual Patch
- High performance network security with real-time attack, malicious code and hybrid threat blocking.
- Allows secure open transactions in a SOA environment which is an effective way to preserve network availability, reduce the burden on your IT resources and prevent security breaches.

- Virtual Patch at the host
- Privileged User Monitoring-- Provides historical data that enables companies to find the origin of a change, breach or string of behavior.
- Holistic Security for all virtual machines running on VMware ESX vSphere 4 platforms.

Agenda

1 IBM ISS Product Portfolio

2 IBM Security Network IPS + Initial Configuration Demo

3 IBM Security Server Protection Solutions (VSP + Host IPS)

4 SiteProtector Training + Demonstration of the Products

5 Access to Resources (Training + Docs + Support)

6 Questions & Answers

Evolution of network security technology

	Firewall	Intrusion Detection	Intrusion Prevention
Overview	Blocks or allows traffic based on source and destination characteristics (address/port)	Performs deep-packet inspection of traffic and triggers alerts when malicious activity is detected	Performs deep-packet inspection of traffic and **blocks** malicious activity
Physical Security Analogy	Lock	Alarm system	Armed guard
Shortcoming	Firewalls can be evaded	Doesn’t prevent network breaches Requires human monitoring	Dependent on the quality of signatures, policies or content to accurately detect & block latest threats

IBM Security Network IPS Performance

Helping enterprises secure their networks

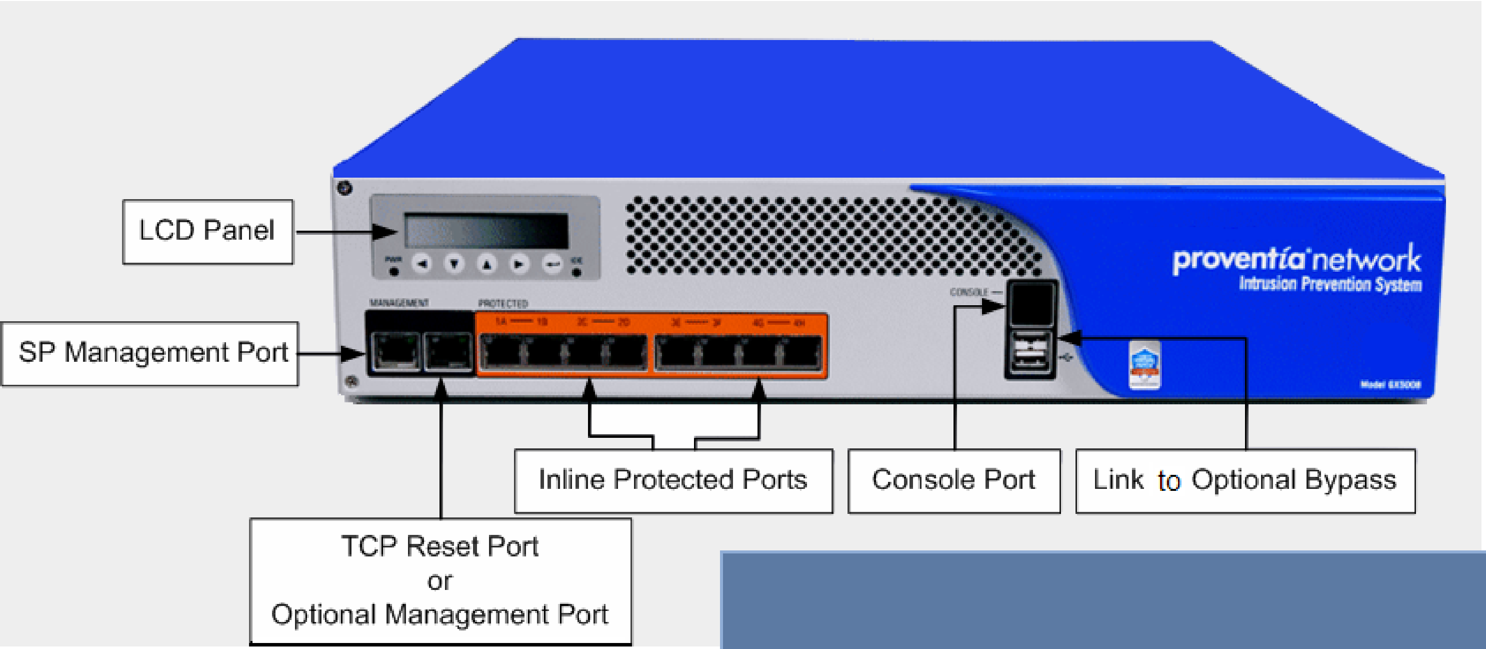
- Transparent, in-line network appliances block attacks while allowing legitimate traffic to flow unhindered
- Comprehensive line of models available:
  - Up to 8 Gbps inspected throughput capacity
  - Up to eight protected network segments

- Newly release hardware improvements include:
  - Doubled the performance & added capacity to run security convergence services – data security, web application protection
  - 64 bit processor
  - Increased memory
  - Improved motherboard for faster BUS speed

IBM Security Network IPS Throughput Metrics

	Perimeter			Core	
Model	GX4004-V2	GX5008-V2	GX5108-V2	GX5208-V2	GX6116
Inspected Throughput	800 Mbps	1.5 Gbps	2.5 Gbps	4 Gbps	8 Gbps
Protected Segments	2	4	4	4	8

A Closer Look to IBM Security IPS



LCD Panel

SP Management Port

Inline Protected Ports

Console Port

Link to Optional Bypass

TCP Reset Port
or
Optional Management Port

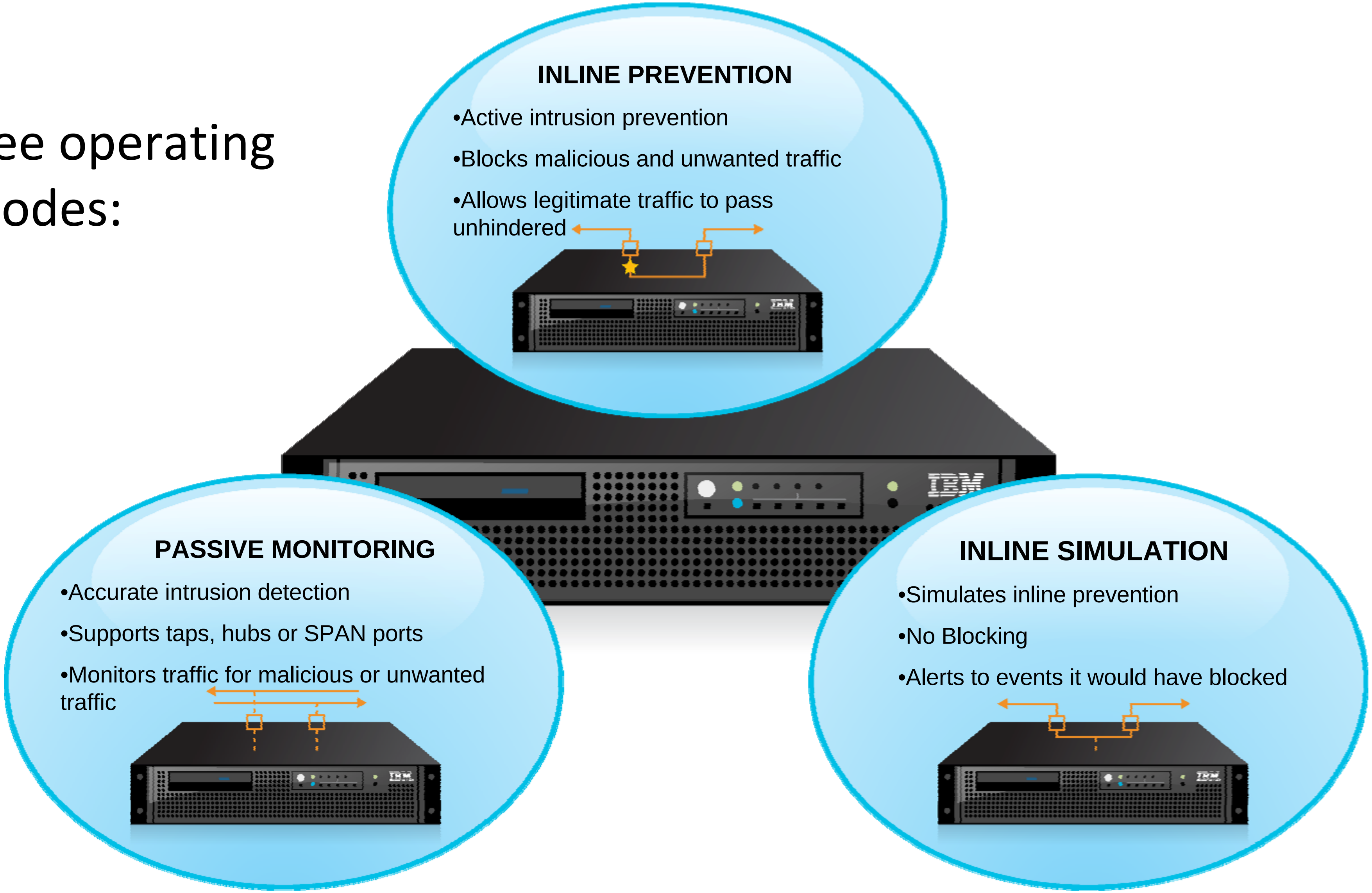
IBM Security Network Intrusion Prevention GX-V2 Hardware Refresh 2Q 2010
(Performance Enhanced)

- ❑ **GX4004-V2**
- ❑ **GX5008-V2**
- ❑ **GX5108-V2**
- ❑ **GX5208-V2**
- ❑ **GX7000 (Native 10GB+)**

- ✷Multi-Core CPU's
- ✷Next Generation hardware design
- ✷Content Analysis performance headroom Performance Optimization
- ✷Significant price/performance improvement
- ✷64 Bit PAM

IBM Security Network IPS deployment

Three operating modes:



INLINE PREVENTION

- Active intrusion prevention
- Blocks malicious and unwanted traffic
- Allows legitimate traffic to pass unhindered

PASSIVE MONITORING

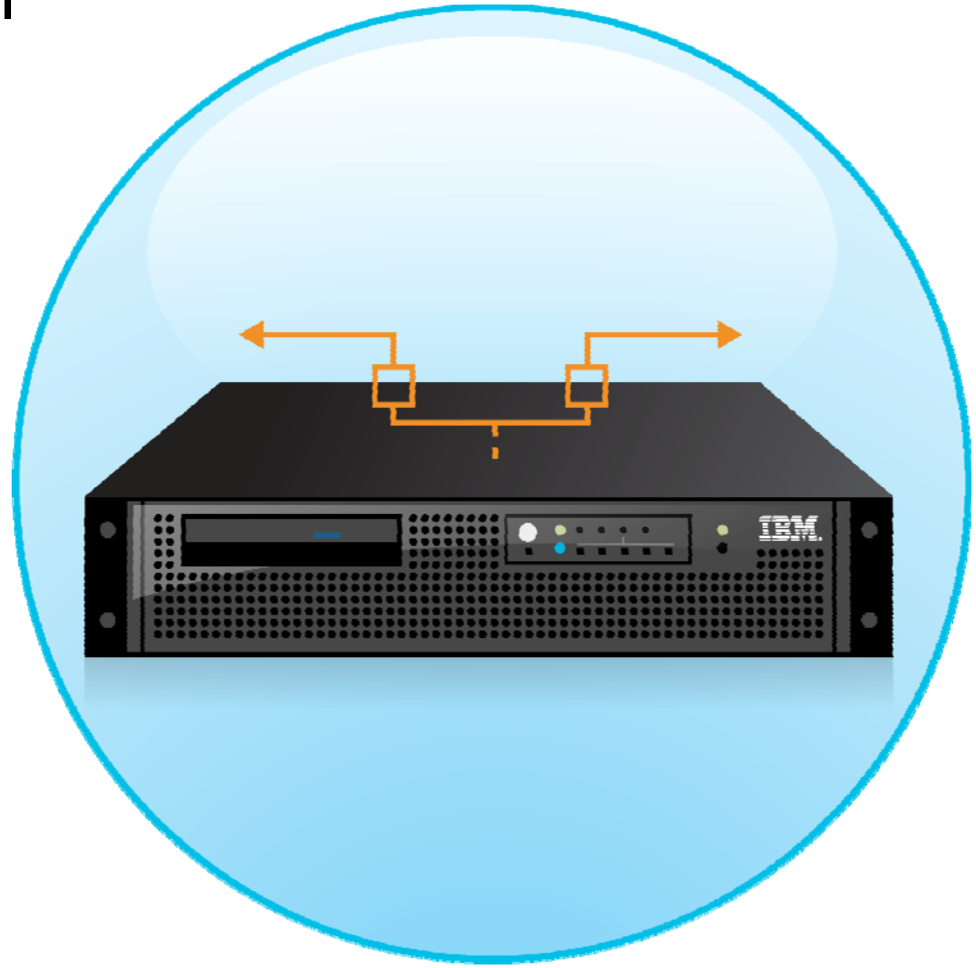
- Accurate intrusion detection
- Supports taps, hubs or SPAN ports
- Monitors traffic for malicious or unwanted traffic

INLINE SIMULATION

- Simulates inline prevention
- No Blocking
- Alerts to events it would have blocked

IBM Security Network IPS reliability

- **Automatic bypass operation allows all traffic to pass in the event of:**
  - Hardware failure
  - Power failure
  - Software crash
- **Redundant components***
  - Hard drives
  - Power supplies
  - Cooling fans

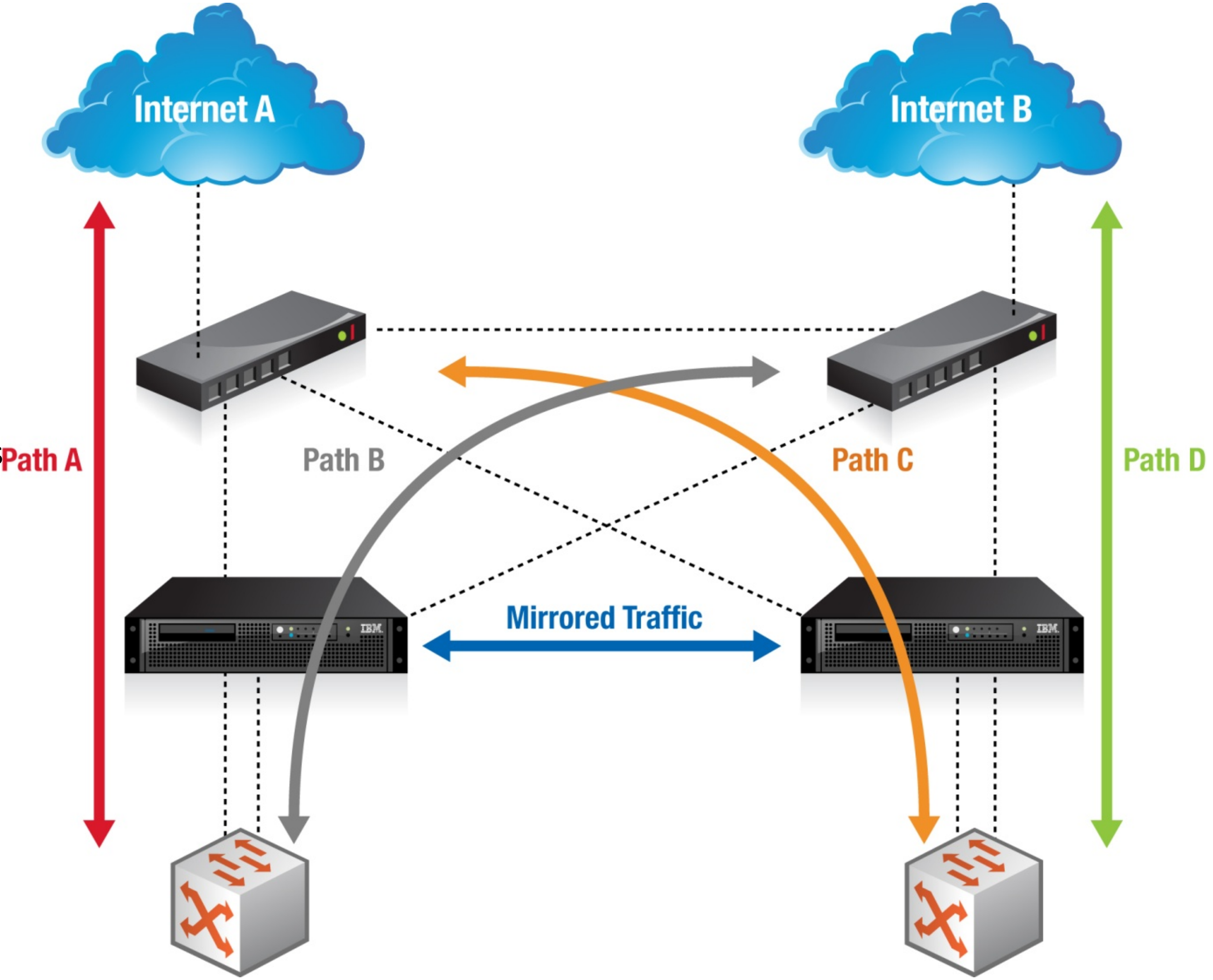


*Available in GX5008, GX5108, GX5208 and GX6116

IBM Security Network IPS reliability continued

High Availability (HA)

- Support for multiple configurations
  - Active - active
  - Active - passive
- Full state maintenance on failover
- Geographic high availability option can use the management port to share quarantine blocking decisions to ensure secure fail-over to a geographically remote standby IPS device.



Our Protocol Analysis Module is the engine behind our products

Intrusion prevention just got smarter with extensible protection backed by the power of X-Force

IBM Protocol Analysis Modular Technology

Virtual Patch

What It Does:
Shields vulnerabilities from exploitation independent of a software patch, and enables a responsible patch management process that can be adhered to without fear of a breach

Why Important:
At the end of 2009, **52%** of all vulnerabilities disclosed during the year had no vendor-supplied patches available to remedy the vulnerability.

Client-Side Application Protection

What It Does:
Protects end users against attacks targeting applications used everyday such as Microsoft Office, Adobe PDF, Multimedia files and Web browsers.

Why Important:
At the end of 2009, vulnerabilities, which affect personal computers, represent the second-largest category of vulnerability disclosures and represent about a fifth of all vulnerability disclosures.

Web Application Protection

What It Does:
Protects web applications against sophisticated application-level attacks such as SQL Injection, XSS (Cross-site scripting), PHP file-includes, CSRF (Cross-site request forgery).

Why Important:
Expands security capabilities to meet both compliance requirements and threat evolution.

Threat Detection & Prevention

What It Does:
Detects and prevents entire classes of threats as opposed to a specific exploit or vulnerability.

Why Important:
Eliminates need of constant signature updates. Protection includes the proprietary Shellcode Heuristics (SCH) technology, which has an unbeatable track record of protecting against zero day vulnerabilities.

Data Security

What It Does:
Monitors and identifies unencrypted personally identifiable information (PII) and other confidential information for data awareness. Also provides capability to explore data flow through the network to help determine if any potential risks exist.

Why Important:
Flexible and scalable customized data search criteria; serves as a complement to data security strategy.

Application Control

What It Does:
Manages control of unauthorized applications and risks within defined segments of the network, such as ActiveX fingerprinting, Peer To Peer, Instant Messaging, and tunneling.

Why Important:
Enforces network application and service access based on corporate policy and governance.

Understanding IBM Security Network IPS

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

What it Prevents	
Worms	Spyware
P2P	DoS/DDoS
Cross-site Scripting	SQL Injection
Buffer Overflow	Web Directory Traversal

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
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
IBM Security Content Analyzer	Injection Logic Engine

IBM Security® Content Analyzer

IBM Protocol Analysis Modular Technology

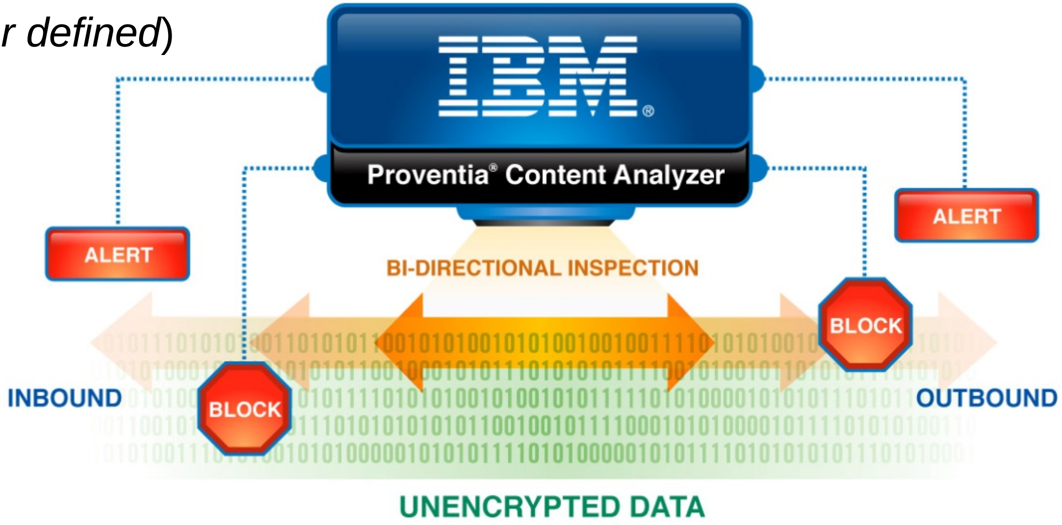
FEATURING VIRTUAL PATCH TECHNOLOGY
Virtual Patch
Client-side Application Protection
Web Application Protection
Threat Detection and Prevention
Data Security
APPLICATION CONTROL
Application Control

Deep content analysis helps prevent data loss:

- Monitors and identifies unencrypted personally identifiable information (PII) and other confidential data
- Enables data flow exploration to identify potential risks within the network
- Performs flexible and scalable customized data searches
- Enables compound data-set search string inspection

(e.g., *name AND social_security_number AND User defined*)

- Complements data security strategy



IBM Security® Content Analyzer (continued)

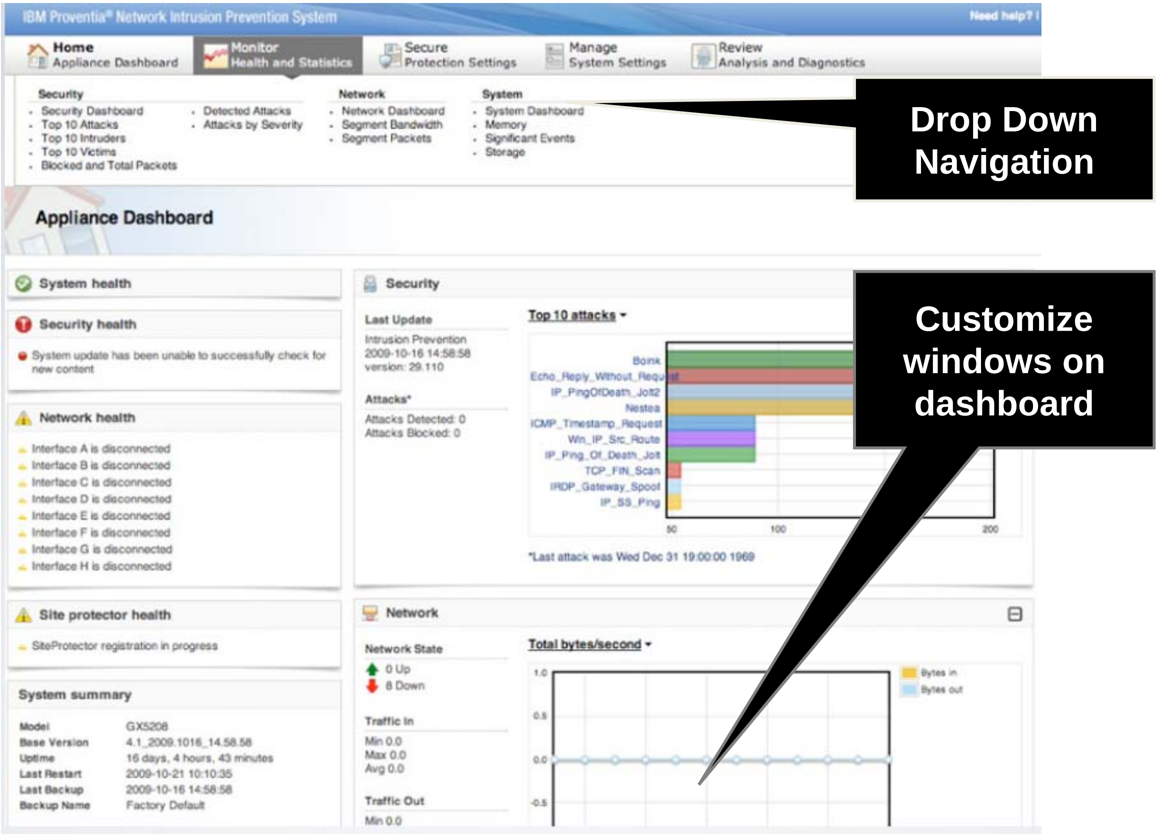
Delivers security effectiveness and data awareness. Proventia Content Analyzer inspects unencrypted data using up to 16 different signatures:

SIGNATURES	PROTOCOLS	CONTENT
Credit Card Number	*AOL IM	Microsoft Office Documents
U.S. Name	*Microsoft Messenger	PDF
Date	*Yahoo Messenger	Text
Dollar Amount	*IRC	RTF
Email Address	HTTP	XML
Social Security Number	FTP	HTML
U.S. Phone Number	SMB	GZIP
U.S. Postal Address	*SMTP	ZIP
8 User-Defined	*IMAP	
	*POP3	

*Provides for inline inspection of attached files.

IBM Security Network IPS Management

- **Browser-based local management interface (LMI)**
  - Single view of health, protection and network statistics from a customizable dashboard
  - Simplified view of data security and web application protection policies from the LMI
  - Patch Management statistics and log evidence from the LMI
- **Central management through IBM Security SiteProtector™ system**
  - Simple, powerful configuration and control
  - Robust reporting, customized event viewing and event correlation
  - Comprehensive alerting and response options
  - Scheduled data retention to be used for compliance efforts
  - Highly scalable to accommodate hundreds of IBM Security Network IPS appliances



Appliance Dashboard

System health

Security health

System update has been unable to successfully check for new content

Network health

Interface A is disconnected
Interface B is disconnected
Interface C is disconnected
Interface D is disconnected
Interface E is disconnected
Interface F is disconnected
Interface G is disconnected
Interface H is disconnected

Site protector health

SiteProtector registration in progress

System summary

Model	GX5208
Base Version	4.1_2009.1016_14.58.58
Uptime	16 days, 4 hours, 43 minutes
Last Restart	2009-10-21 10:10:35
Last Backup	2009-10-16 14:58:58
Backup Name	Factory Default

Security

Last Update
Intrusion Prevention
2009-10-16 14:58:58
version: 29.110

Attacks*
Attacks Detected: 0
Attacks Blocked: 0

*Last attack was Wed Dec 31 19:00:00 1969

Network

Network State
0 Up
8 Down

Traffic In
Min 0.0
Max 0.0
Avg 0.0

Traffic Out
Min 0.0

Drop Down Navigation

Customize windows on dashboard

IBM Security Network Active Bypass (New Hardware)

Older

Newer

❑ Maximizes network availability by minimizing “time to failover”

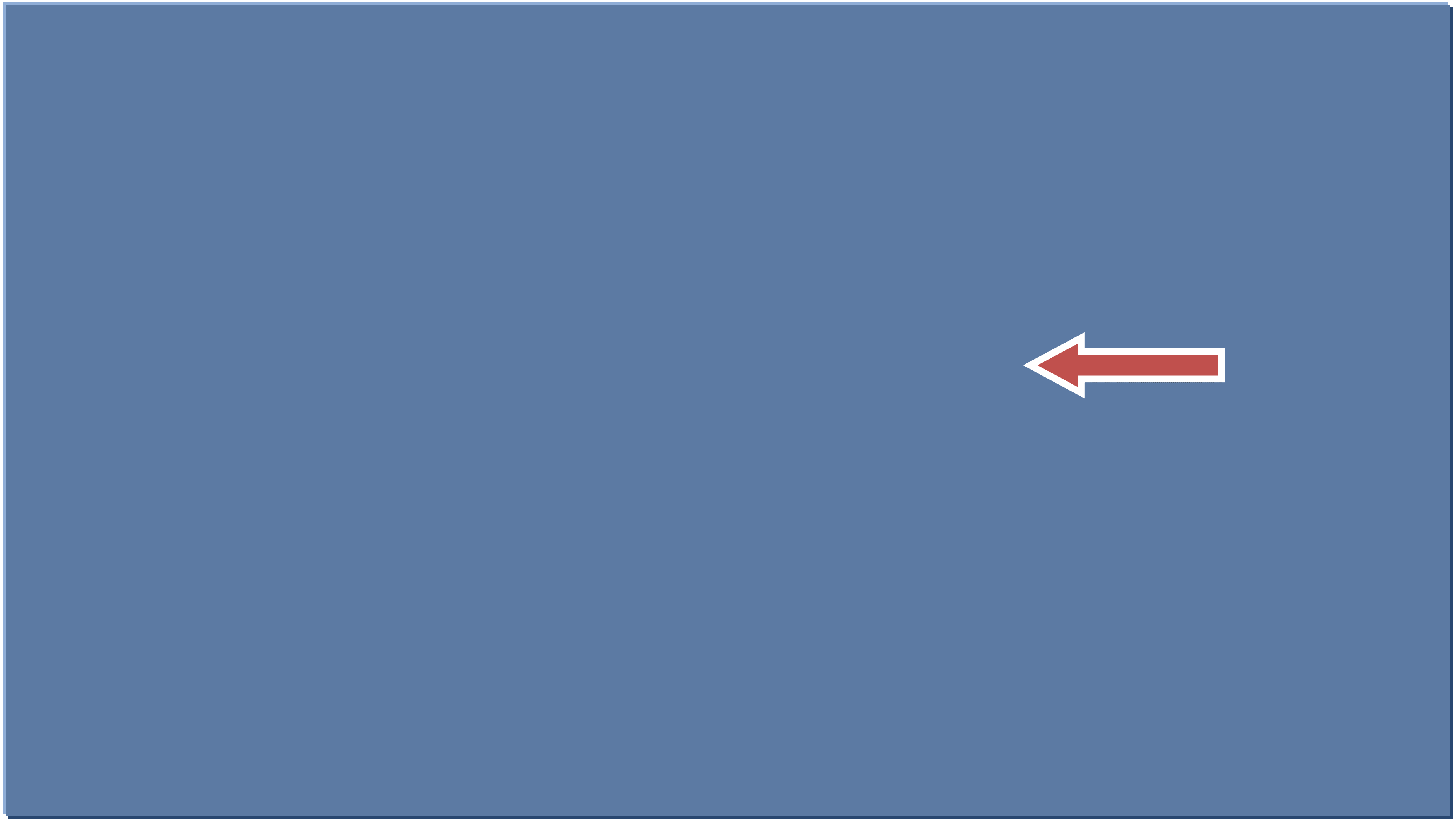
❑ Enables uninterrupted access to applications by maintaining link state during bypass operations

❑ Powers high availability network IPS deployments

❑ Simplifies troubleshooting with SNMP trap support and e-mail support

❑ Supports up to four network segments in any combination of Copper, MM Fiber and SM fiber

Configurable User Interface

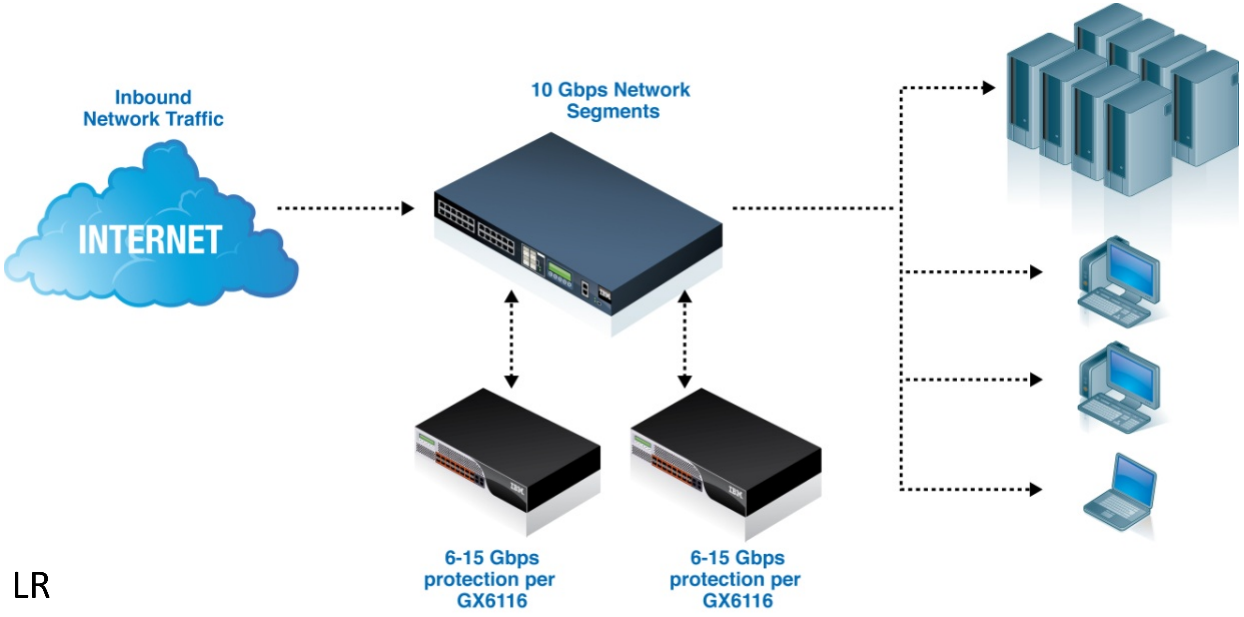


Bypass Deployment & Cabling – How to?

IBM Security Network Controller

- Provides 10 GbE connectivity for IBM Security Network IPS GX6116, GX5108 and GX5208
- Aggregates/segregates four 10 GbE ports to 24 1 GbE ports with configurable mapping
- Active bypass/switching prevents network disruption should the IPS appliance fail
- Passive bypass and power loss fail safe
- Supports multiple 10 GbE interfaces: SR and LR

10G network upgrades that leverage your existing investment in network protection


Inbound Network Traffic
INTERNET
10 Gbps Network Segments
6-15 Gbps protection per GX6116
6-15 Gbps protection per GX6116

8 Gbps Protection per GX6116

12 Gbps real time total inspection throughput with 2 x GX6116

IBM Security Network IPS Initial Configuration Demo

Agenda

1. IBM ISS Product Portfolio
2. IBM Security Network IPS + Initial Configuration
3. IBM Security Server Protection Solutions (VSP + Host IPS)
4. SiteProtector Training + Demonstration of the Products
5. Access to Resources (Training + Docs + Support)
6. Questions & Answers

Virtualization drives down total cost of ownership and helps drive efficiency within the IT organization

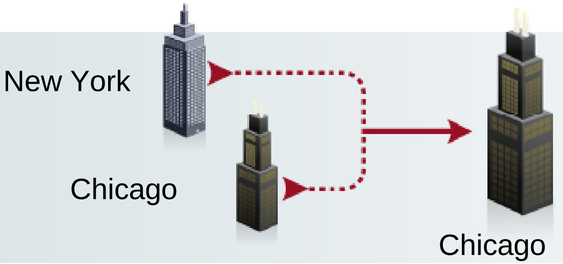
Facilitate Physical Consolidation

Enable Cloud Computing

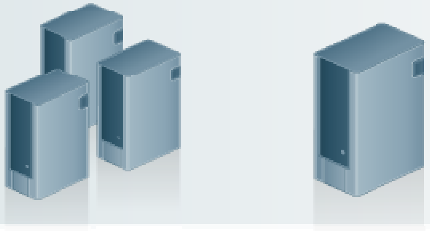
Achieve High Performance

Improve Service Levels

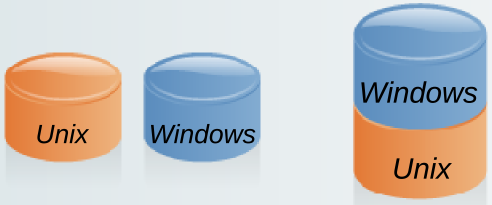
Reduce the number of sites



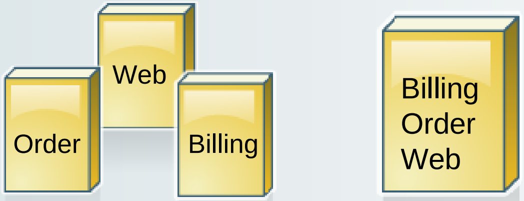
Reduce the number of servers



Centralize data from different sources



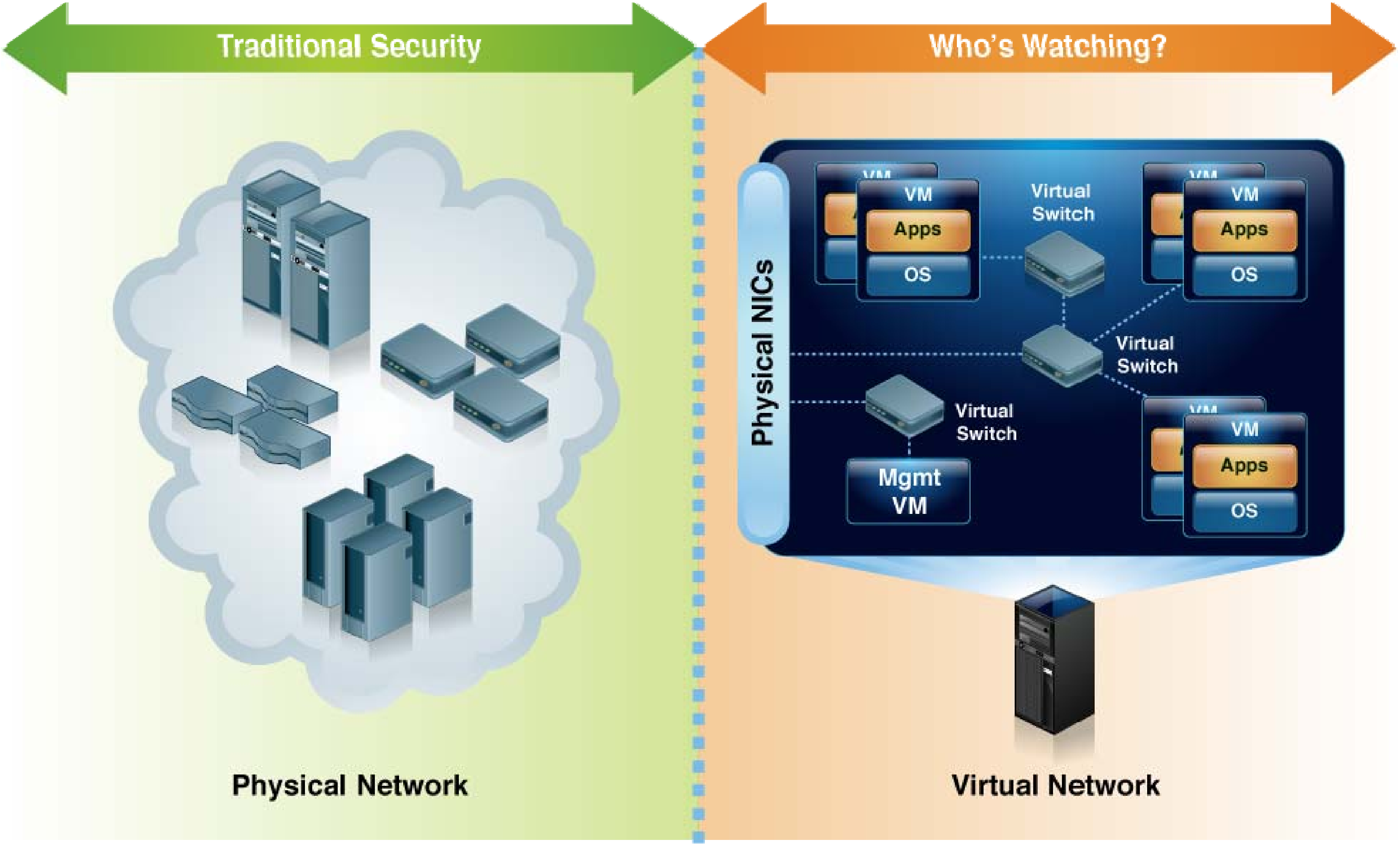
Increase application efficiency



“Through 2010, IT infrastructure consolidation will remain the focus of IT infrastructure and operations cost reduction initiatives.”

Source: Gartner, Inc.

Server and Network Convergence

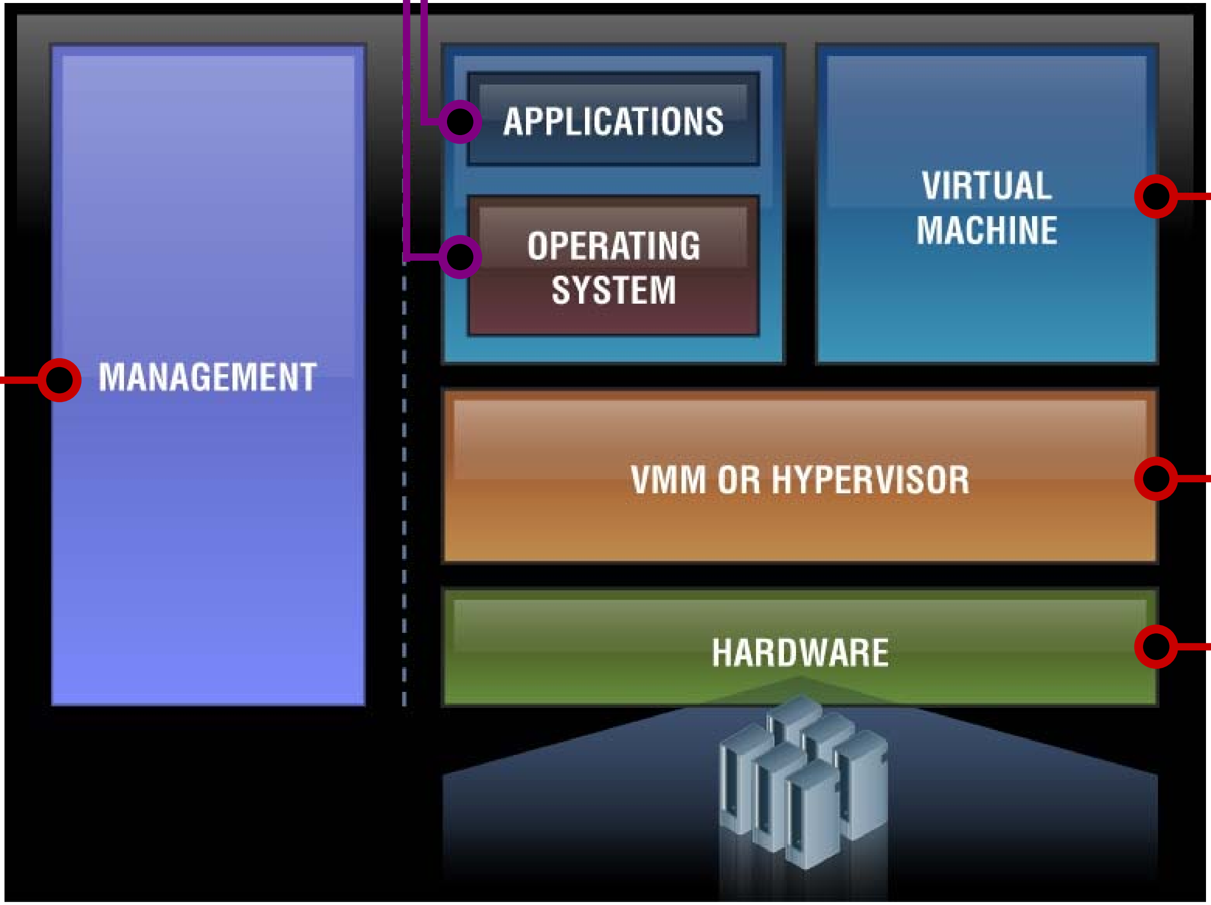


Security Challenges with Virtualization: New Risks

● Traditional Threats

● New threats to VM environments

Traditional threats can attack VMs just like real systems



Management Vulnerabilities

Secure storage of VMs and the management DATA

Requires new skill sets

Virtual sprawl

Dynamic relocation

VM stealing

Resource sharing

Single point of failure

Stealth rootkits in hardware now possible

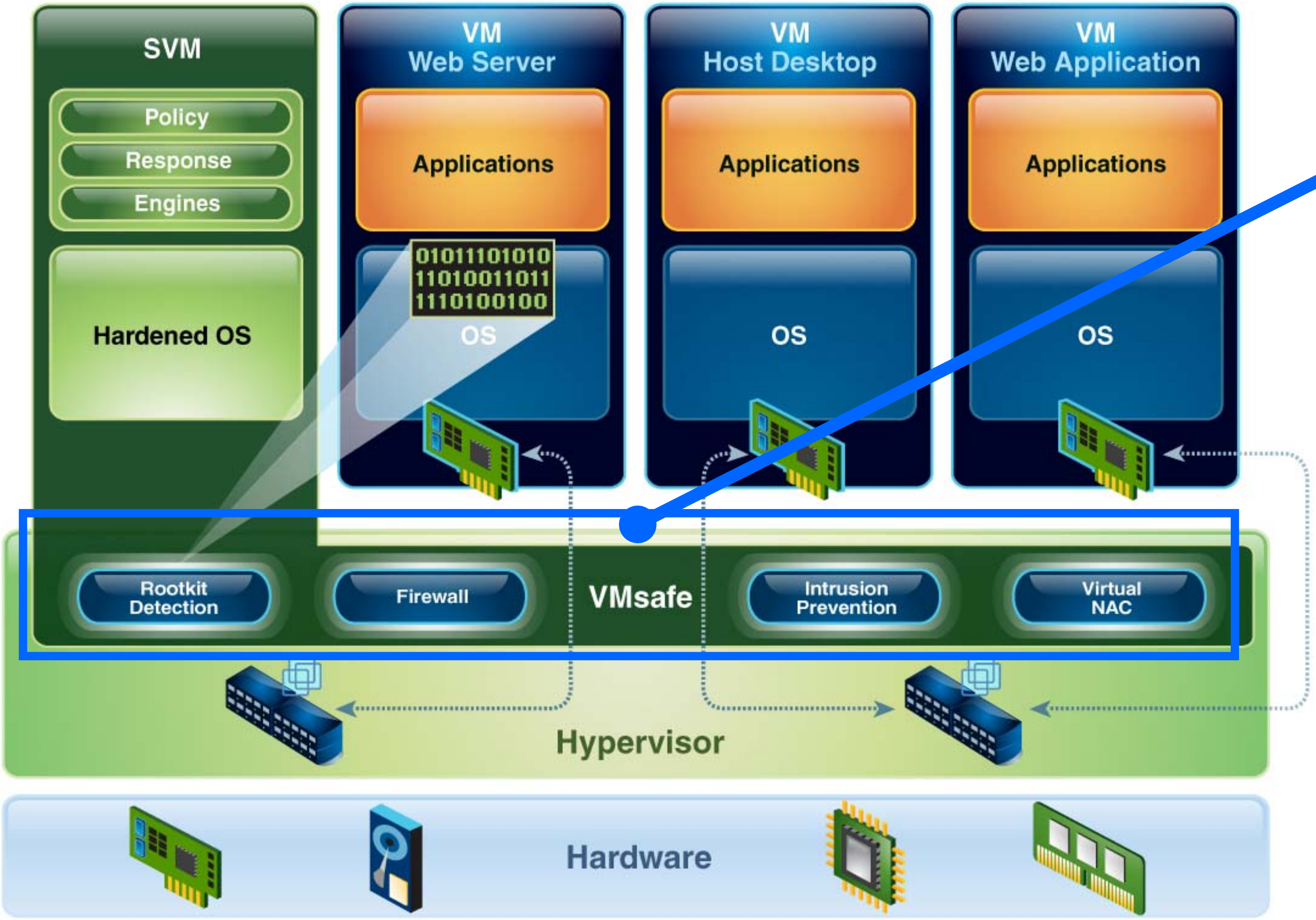
Virtual NICs & Virtual Hardware are targets

MORE COMPONENTS = MORE EXPOSURE

IBM Virtual Server Security for VMware

Integrated threat protection for VMware vSphere 4

Helps customers to be more secure, compliant and cost-effective by delivering integrated and optimized security for virtual data centers.



IBM Virtual Server Security for VMware

- ❑ VMsafe Integration
- ❑ Firewall and Intrusion Prevention
- ❑ Rootkit Detection/Prevention
- ❑ Inter-VM Traffic Analysis
- ❑ Automated Protection for Mobile VMs (vMotion)
- ❑ Virtual Network Segment Protection
- ❑ Virtual Network-Level Protection
- ❑ Virtual Infrastructure Auditing (Privileged User)
- ❑ Virtual Network Access Control
- ❑ File and Registry Monitoring with Host IPS (Real Secure and Proventia Server)

IBM Security Virtual Server Protection

- Provides integrated threat protection for VMware VSphere 4.
- Deployed as a Security Virtual Machine on the ESX hypervisor.
- Integrates with the hypervisor through VMsafe.
- Has the following features:
  - Firewall
    - Control inter-VM network traffic and shield your virtual infrastructure from the physical network.
  - Intrusion Prevention
    - IBM's Protocol Analysis Module powered by X-Force.
  - Virtual Network Access Control
    - Prevent virtual machine sprawl.
  - Rootkit Detection
    - Detect rootkit running inside virtual machines.
  - Virtual Infrastructure Auditing
    - Reports virtual machine events such as start/stop/create/remove to Siteprotector
  - Virtual Machine Discovery
    - Discovers virtual machine operating system and open ports.

Virtual Server Protection Benefits

- Non-intrusive
  - No reconfiguration of the virtual network is needed
    - When using the VMsafe Network API
  - No presence in the guest OS
    - Limitation on what can be analyzed
- Less management overhead
  - Virtual appliance form-factor
  - Only one Security Virtual Machine (SVM) required per physical server
  - 1 SVM can protect up to 200 virtual machines
    - Theoretical limit as it has not been tested with that many
- Automated
  - Privileged presence gives SVM holistic view of the virtual network
  - Protection automatically applied as VM comes online
- Protection for any guest OS
  - Exception: ARK module limited based on guest OS

Virtual Server Protection FAQ

Q1) How many of the (critical) software vulnerabilities could be fully mitigated through this Virtual Patching?

IBM Security Virtual Server Security product uses same protection engine (PAM) that network IPS has, and currently, it has same security events (2741 security events)

Q2) How much additional resources (processor power/memory) is needed?

SVM needs at least 1 GB of RAM and more than 10 GB of available hard disk space. The SVM incurs a memory overhead for each virtual machine that it protects, but only a fixed amount of processor time. The amount of RAM allocated to the SVM must be appropriately scaled for the expected number of virtual hosts.

Q3) How much delay would that add to network packages?

The VMware VMSafe API has two components, fast path and slow path, any VMsafe based products using slow-path slightly increase the virtual network latency, this is related to VMsafe slow-path performance issue. But this doesn't effect performance in virtual network.

Alternatively Bypass Filters can be written to ignore the specific VM traffic by VMsafe.

Q4) Is it possible to turn off rest of the VSP's features (which may not needed) to free up resources?

Yes, at anytime VSP can be shutdown or network monitoring option could be turned off completely or for a partucular VM.

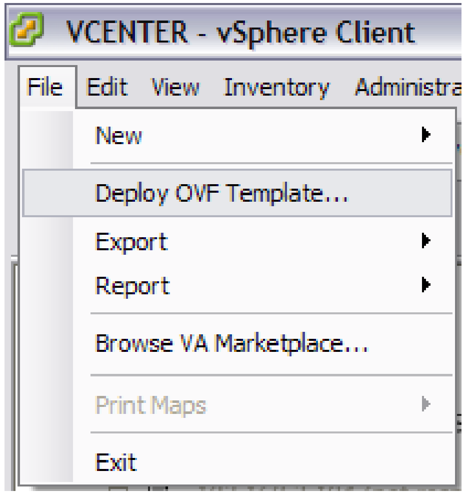
Q5) How is the product priced? (per VM or per real server?, is there possibility to buy sub-features separately - virtual patching alone?)

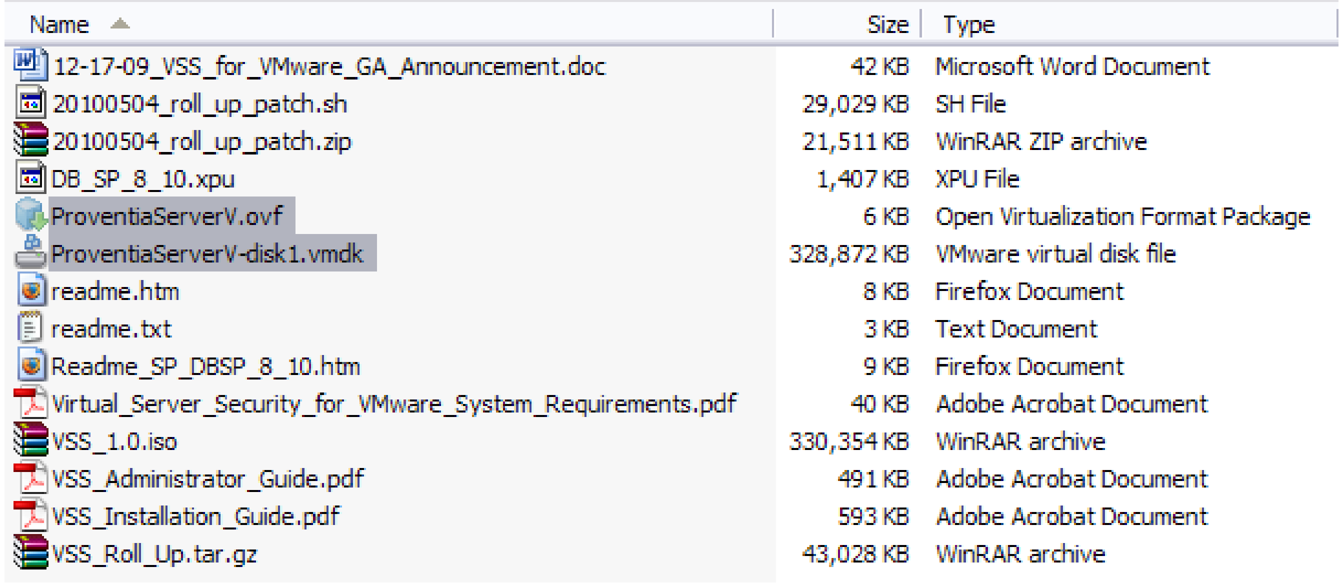
Licensing is based on CPU numbers (sockets, not cores) per ESX. Standart license include 2 x CPU, additional license should be purchased if ESX server has more than 2 CPUs.

IBM Security Virtual Server Security Installation & Integration with ESX

Virtual Server Protection - Installation

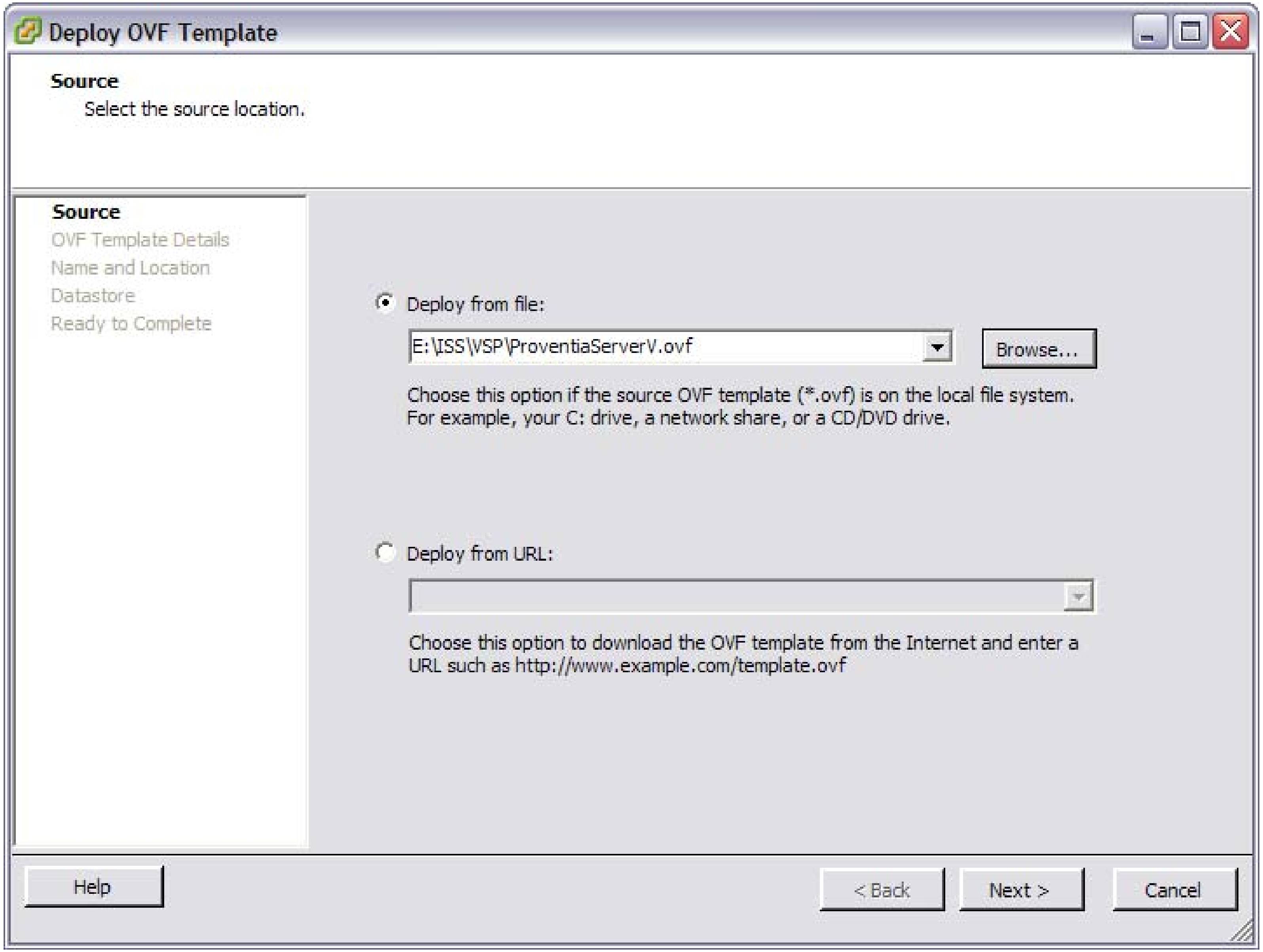
- VSP SVM is deployed to ESX via the VSphere client through means of an OVF file:
  - Open Virtualization Format: platform independent distribution format for virtual machines
  - Reduces configuration time
  - Compatible with automated image deployment solutions





Name	Size	Type
12-17-09_VSS_for_VMware_GA_Announcement.doc	42 KB	Microsoft Word Document
20100504_roll_up_patch.sh	29,029 KB	SH File
20100504_roll_up_patch.zip	21,511 KB	WinRAR ZIP archive
DB_SP_8_10.xpu	1,407 KB	XPU File
ProventiaServerV.ovf	6 KB	Open Virtualization Format Package
ProventiaServerV-disk1.vmdk	328,872 KB	VMware virtual disk file
readme.htm	8 KB	Firefox Document
readme.txt	3 KB	Text Document
Readme_SP_DBSP_8_10.htm	9 KB	Firefox Document
Virtual_Server_Security_for_VMware_System_Requirements.pdf	40 KB	Adobe Acrobat Document
VSS_1.0.iso	330,354 KB	WinRAR archive
VSS_Administrator_Guide.pdf	491 KB	Adobe Acrobat Document
VSS_Installation_Guide.pdf	593 KB	Adobe Acrobat Document
VSS_Roll_Up.tar.gz	43,028 KB	WinRAR archive

Virtual Server Protection - Installation



Source

Select the source location.

● Deploy from file:

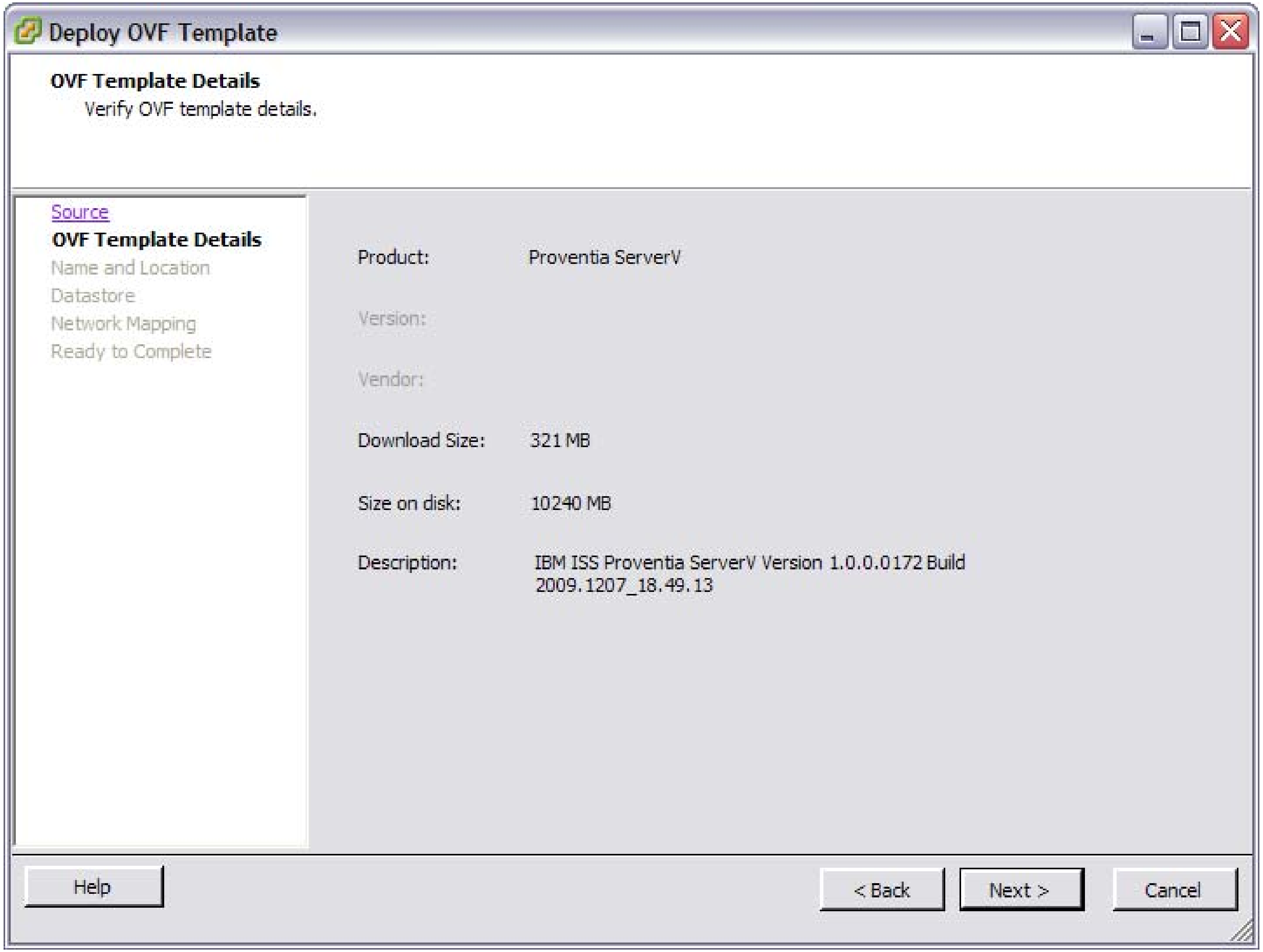
E:\ISS\VSP\ProventiaServerV.ovf

Choose this option if the source OVF template (*.ovf) is on the local file system. For example, your C: drive, a network share, or a CD/DVD drive.

○ Deploy from URL:

Choose this option to download the OVF template from the Internet and enter a URL such as http://www.example.com/template.ovf

Virtual Server Protection - Installation



OVF Template Details

Verify OVF template details.

Product: Proventia ServerV

Version:

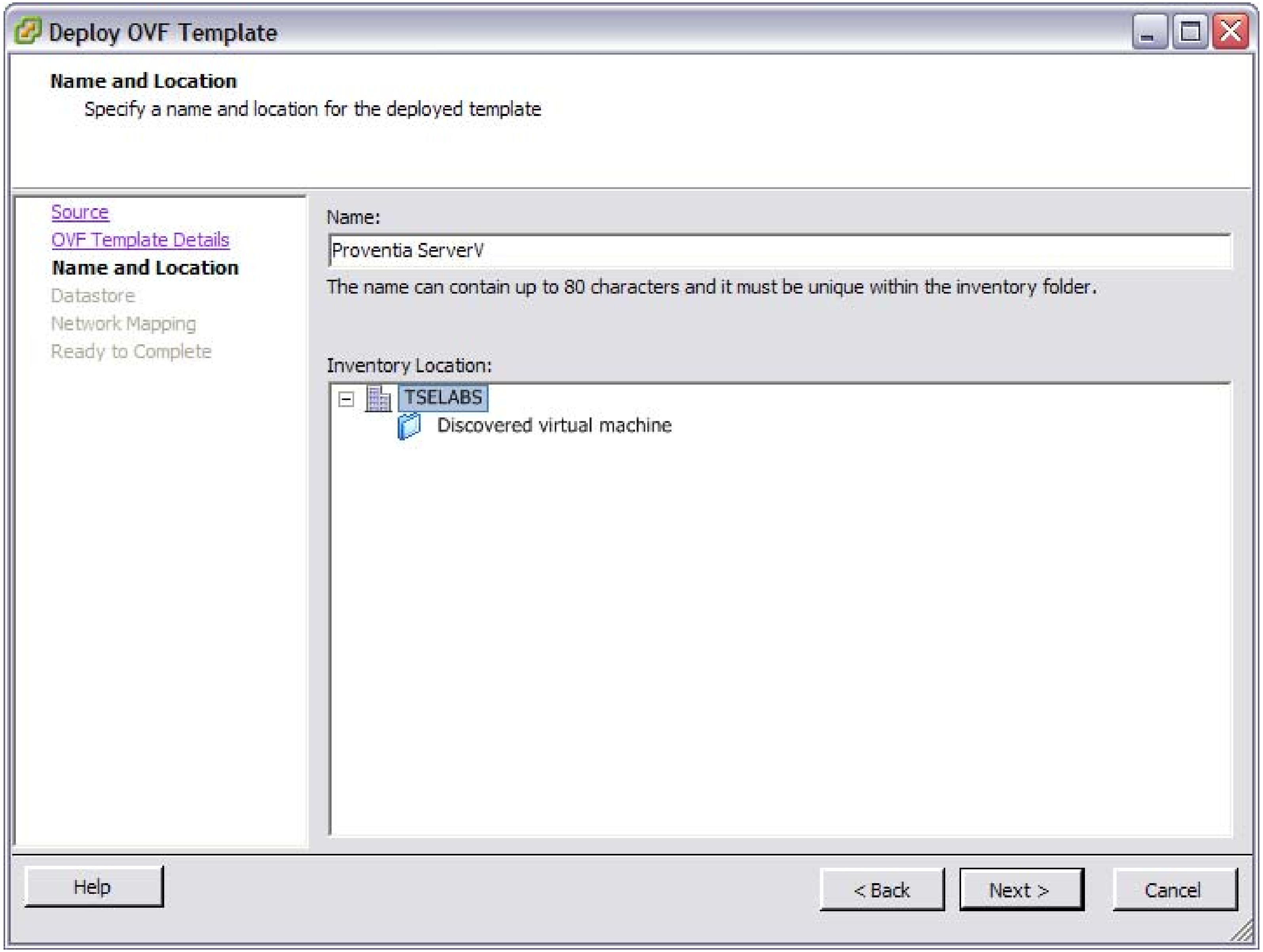
Vendor:

Download Size: 321 MB

Size on disk: 10240 MB

Description: IBM ISS Proventia ServerV Version 1.0.0.0172 Build 2009.1207_18.49.13

Virtual Server Protection - Installation



Name and Location

Specify a name and location for the deployed template

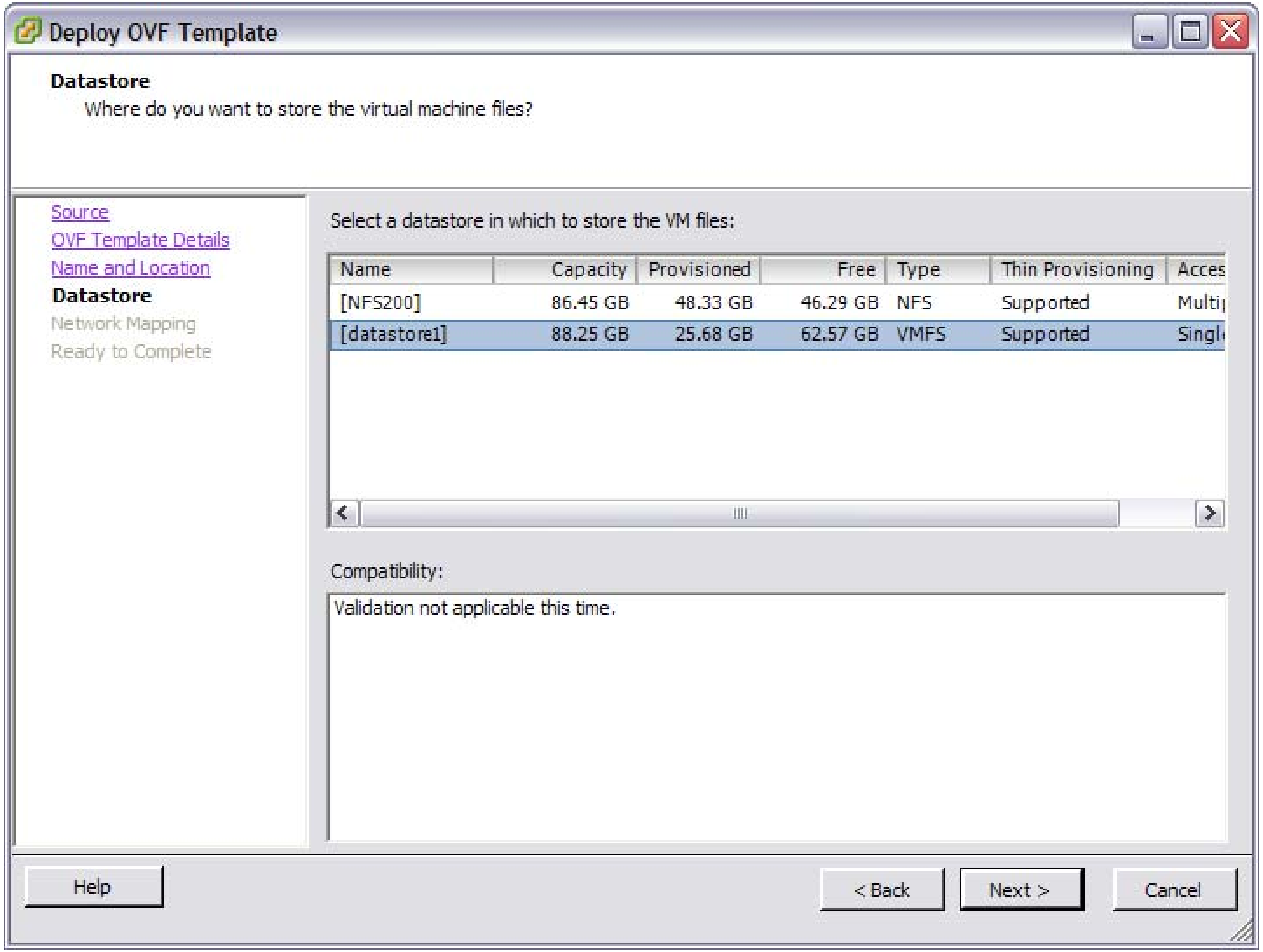
Name: Proventia ServerV

The name can contain up to 80 characters and it must be unique within the inventory folder.

Inventory Location:

- TSELABS
  - Discovered virtual machine

Virtual Server Protection - Installation



Deploy OVF Template

Datastore

Where do you want to store the virtual machine files?

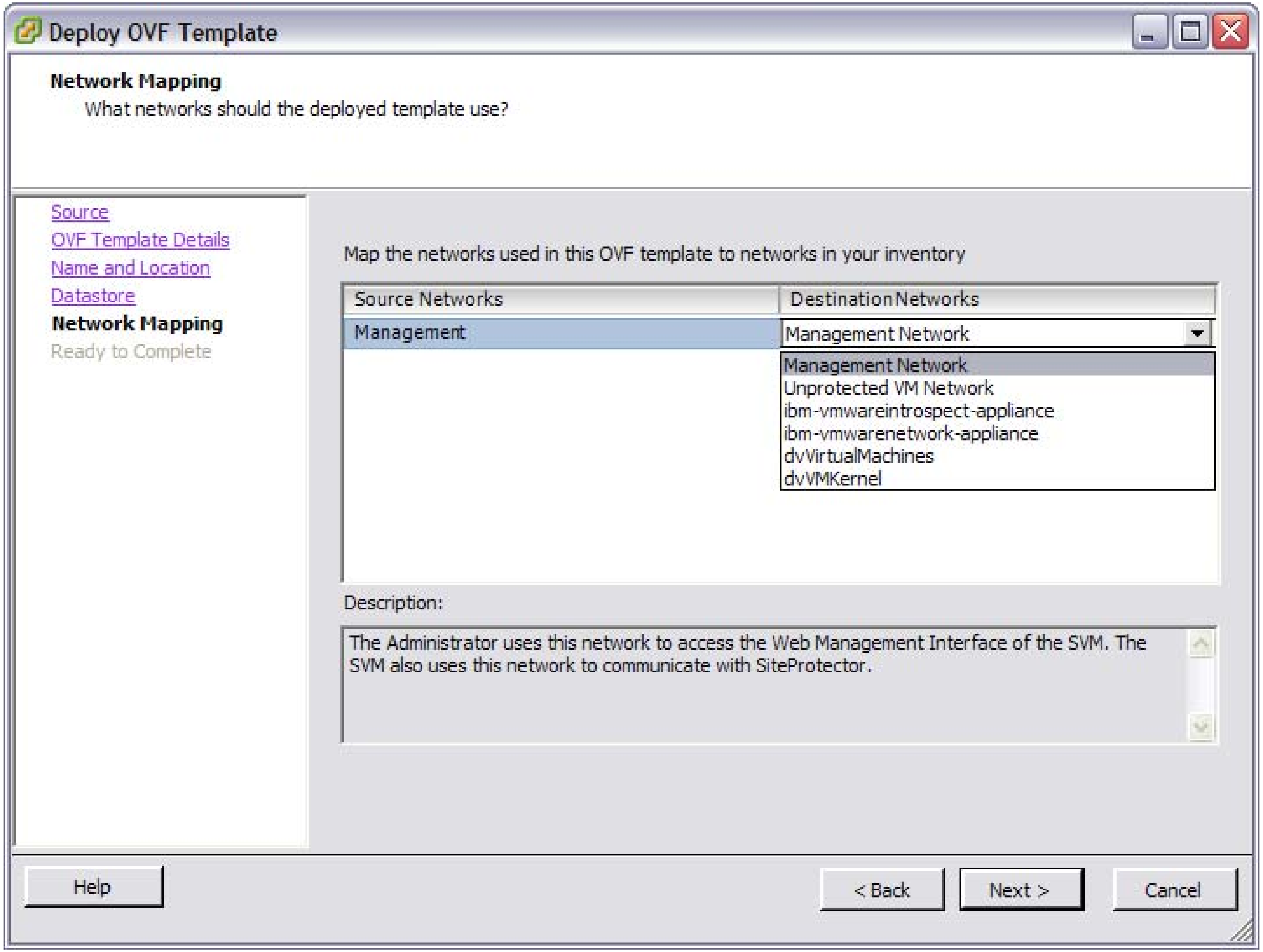
Select a datastore in which to store the VM files:

Name	Capacity	Provisioned	Free	Type	Thin Provisioning	Acces
[NFS200]	86.45 GB	48.33 GB	46.29 GB	NFS	Supported	Multi
[datastore1]	88.25 GB	25.68 GB	62.57 GB	VMFS	Supported	Singl

Compatibility:

Validation not applicable this time.

Virtual Server Protection - Installation



Deploy OVF Template

Network Mapping

What networks should the deployed template use?

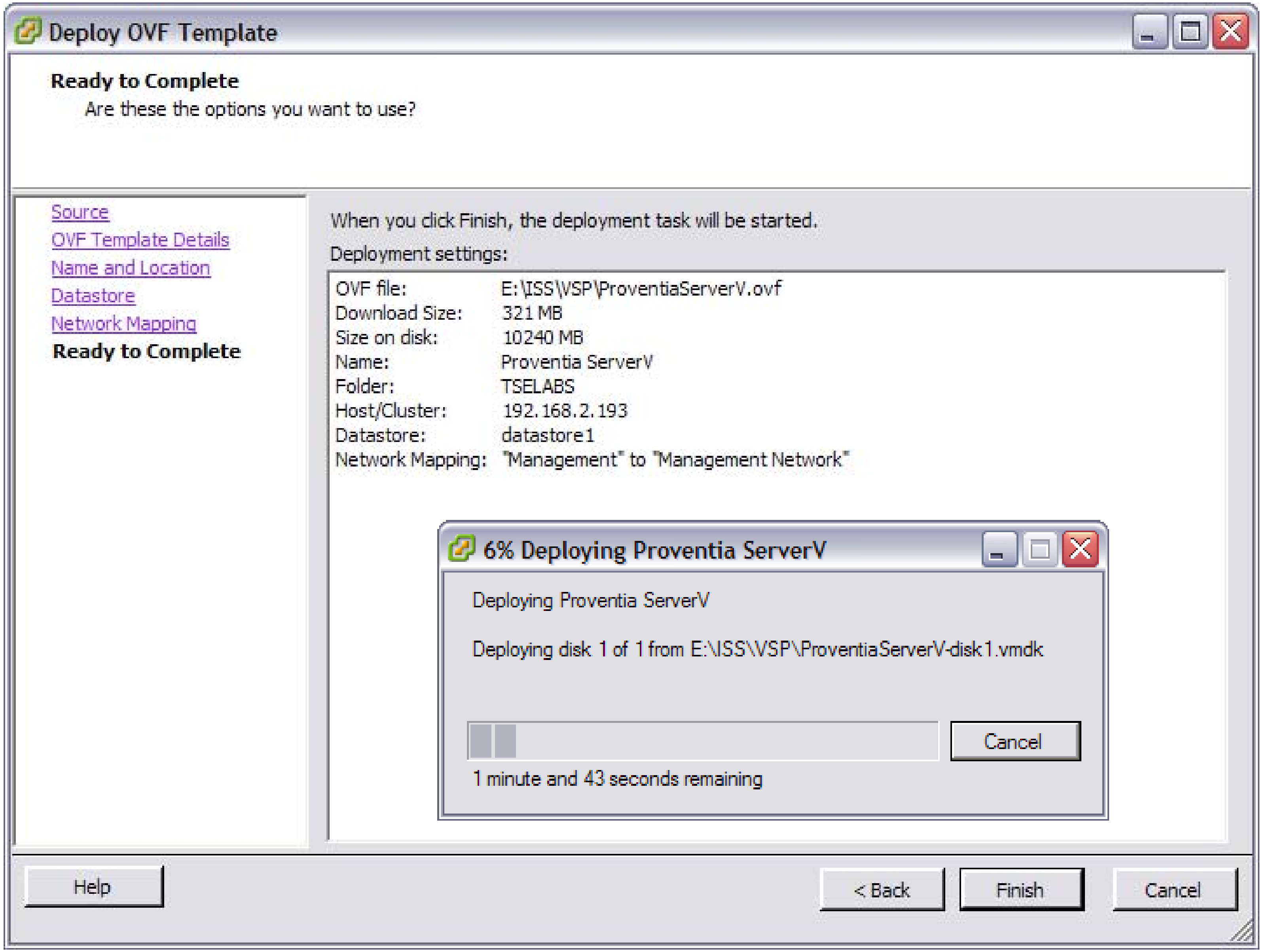
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
Management	Management Network

Description:

The Administrator uses this network to access the Web Management Interface of the SVM. The SVM also uses this network to communicate with SiteProtector.

Virtual Server Protection - Installation



Ready to Complete

Are these the options you want to use?

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	E:\ISS\VSP\ProventiaServerV.ovf
Download Size:	321 MB
Size on disk:	10240 MB
Name:	Proventia ServerV
Folder:	TSELABS
Host/Cluster:	192.168.2.193
Datastore:	datastore1
Network Mapping:	"Management" to "Management Network"

Deploying Proventia ServerV

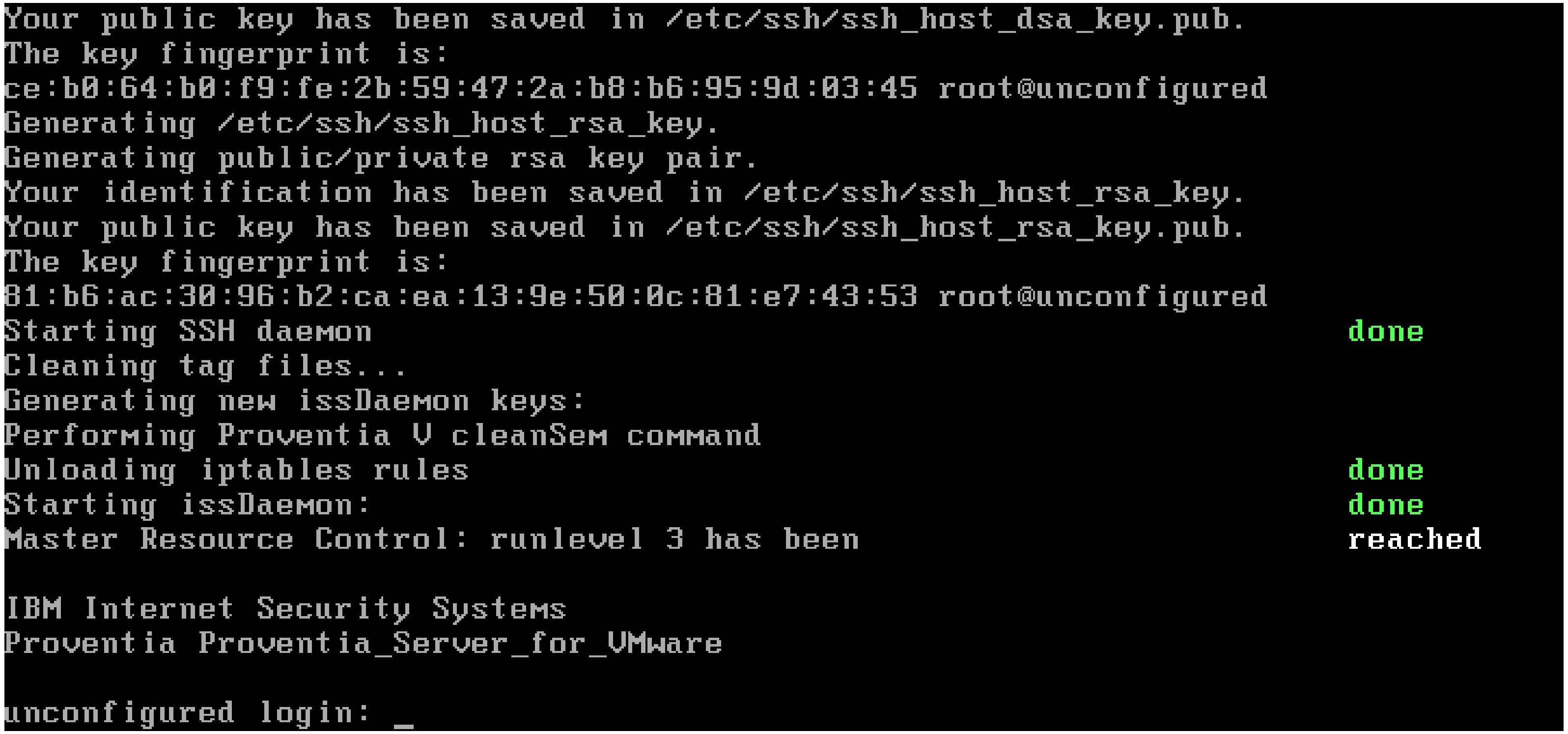
Deploying disk 1 of 1 from E:\ISS\VSP\ProventiaServerV-disk1.vmdk

1 minute and 43 seconds remaining

Virtual Server Protection – Initial Setup

Once the VSP OVF package has been deployed, the following tasks need to be performed to integrate VSP with the ESX host:

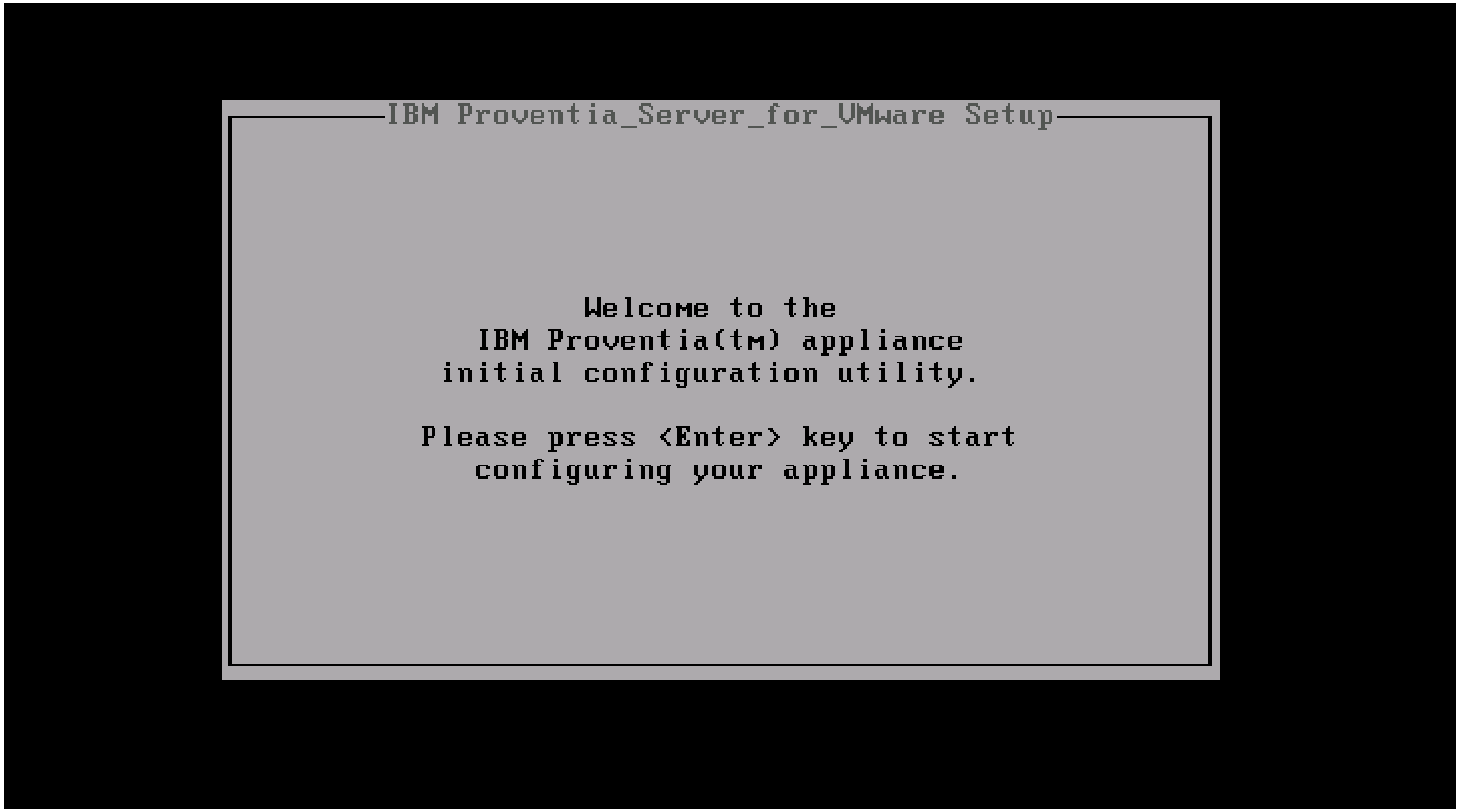
- Configure management network interface and date/time.
- Configure the Virtual Machine Observer for communication with the ESX host.
- Set up the introspection switches for virtual machine network and memory inspection.
- Configure the accelerator for network inspection (optional).
- Configure Siteprotector management communication.



```
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
ce:b0:64:b0:f9:fe:2b:59:47:2a:b8:b6:95:9d:03:45 root@unconfigured
Generating /etc/ssh/ssh_host_rsa_key.
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
81:b6:ac:30:96:b2:ca:ea:13:9e:50:0c:81:e7:43:53 root@unconfigured
Starting SSH daemon                                                    done
Cleaning tag files...
Generating new issDaemon keys:
Performing Proventia V cleanSem command
Unloading iptables rules                                               done
Starting issDaemon:                                                    done
Master Resource Control: runlevel 3 has been                           reached

IBM Internet Security Systems
Proventia Proventia_Server_for_VMware

unconfigured login: _
```

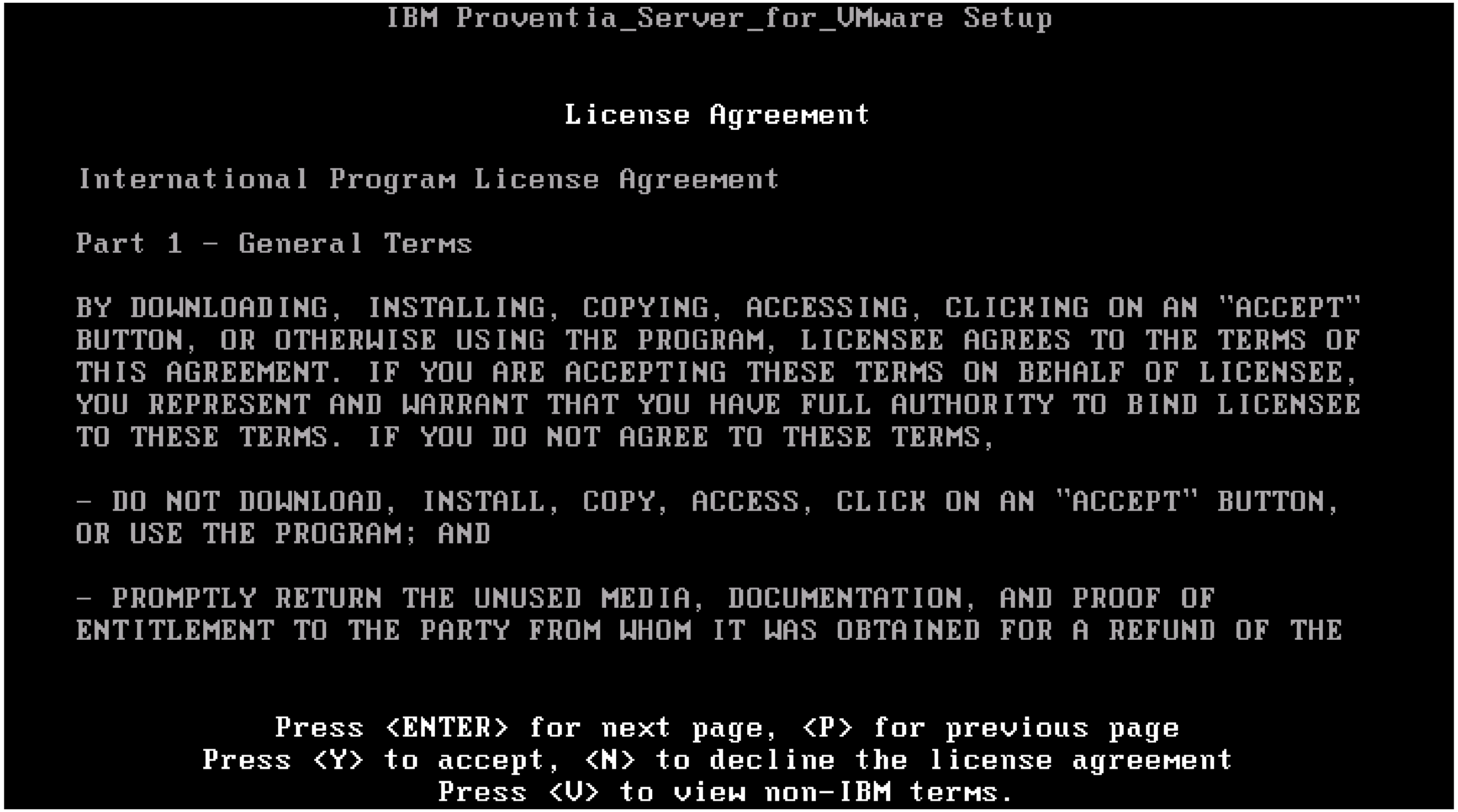
Virtual Server Protection – Initial Setup

- Log in at the unconfigured login prompt with user admin and password admin. This will launch the initial configuration utility.



```
IBM Proventia_Server_for_VMware Setup

Welcome to the
IBM Proventia(tm) appliance
initial configuration utility.

Please press <Enter> key to start
configuring your appliance.
```

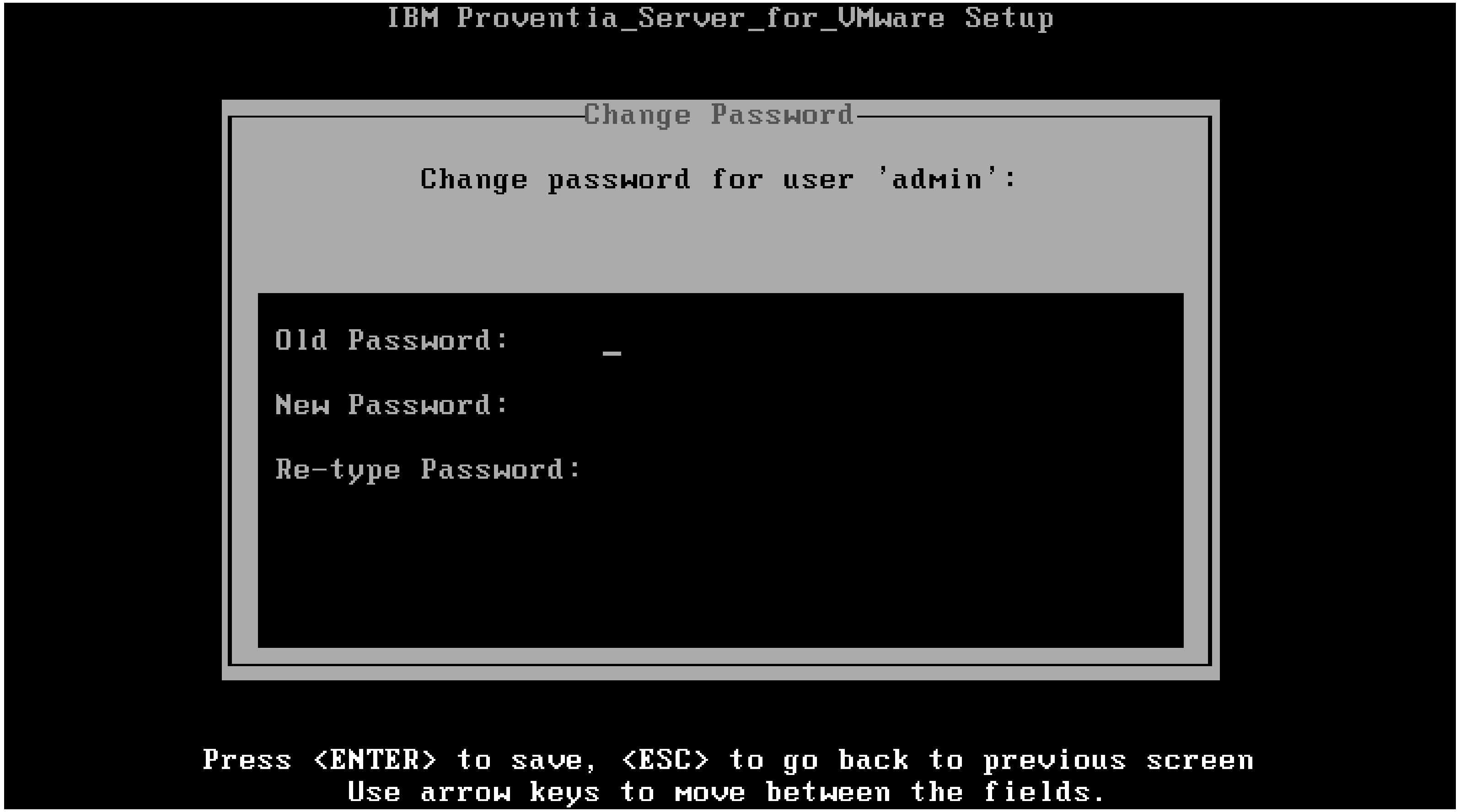
Virtual Server Protection – Initial Setup



```
                    IBM Proventia_Server_for_VMware Setup


                              License Agreement

    International Program License Agreement

    Part 1 - General Terms

    BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN "ACCEPT"
    BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO THE TERMS OF
    THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF LICENSEE,
    YOU REPRESENT AND WARRANT THAT YOU HAVE FULL AUTHORITY TO BIND LICENSEE
    TO THESE TERMS. IF YOU DO NOT AGREE TO THESE TERMS,

    - DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT" BUTTON,
    OR USE THE PROGRAM; AND

    - PROMPTLY RETURN THE UNUSED MEDIA, DOCUMENTATION, AND PROOF OF
    ENTITLEMENT TO THE PARTY FROM WHOM IT WAS OBTAINED FOR A REFUND OF THE


               Press <ENTER> for next page, <P> for previous page
           Press <Y> to accept, <N> to decline the license agreement
                       Press <V> to view non-IBM terms.
```

Virtual Server Protection – Initial Setup

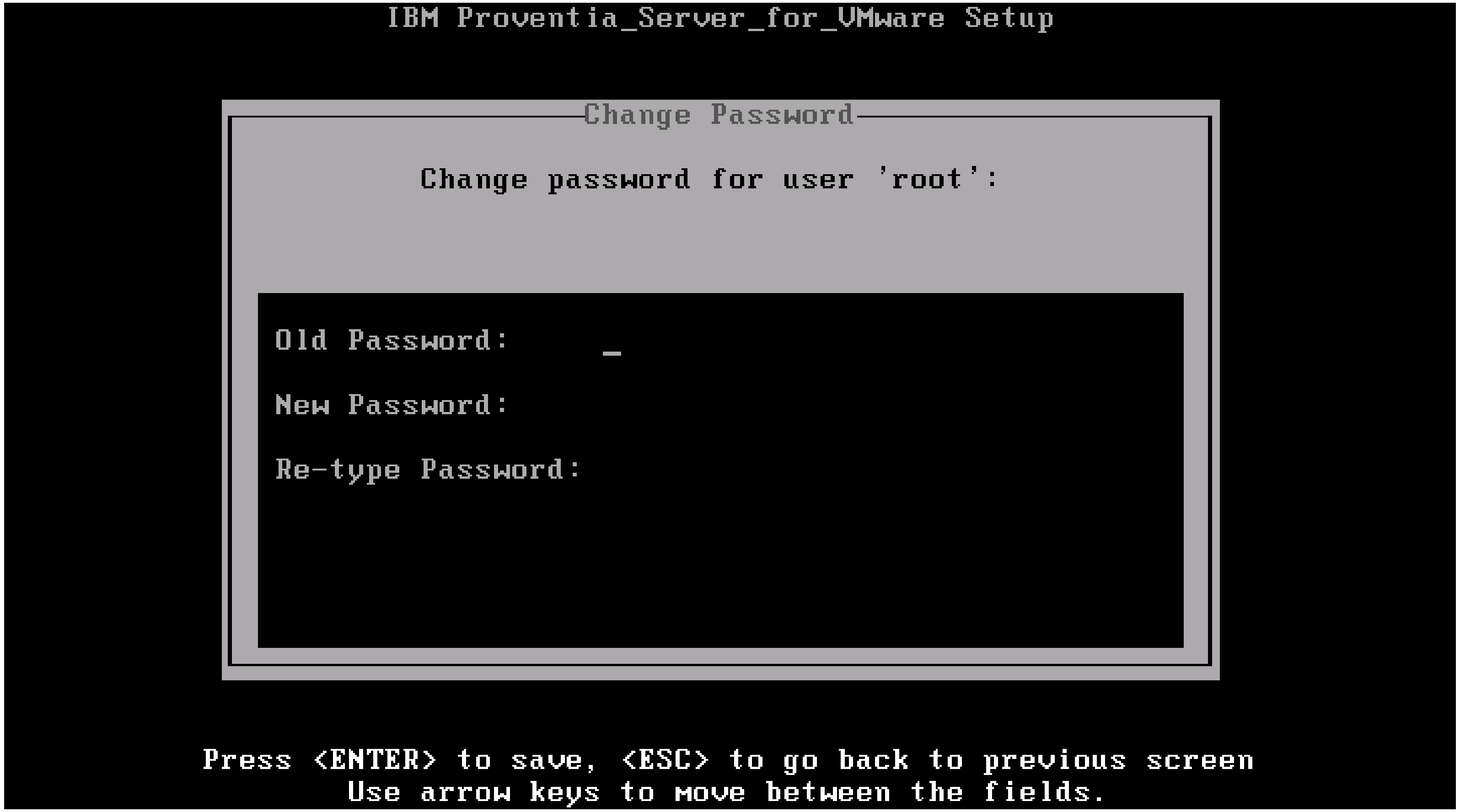
- Change the password for the admin user.



```
                 IBM Proventia_Server_for_VMware Setup

                    Change Password

              Change password for user 'admin':

        Old Password:        _

        New Password:

        Re-type Password:

      Press <ENTER> to save, <ESC> to go back to previous screen
              Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

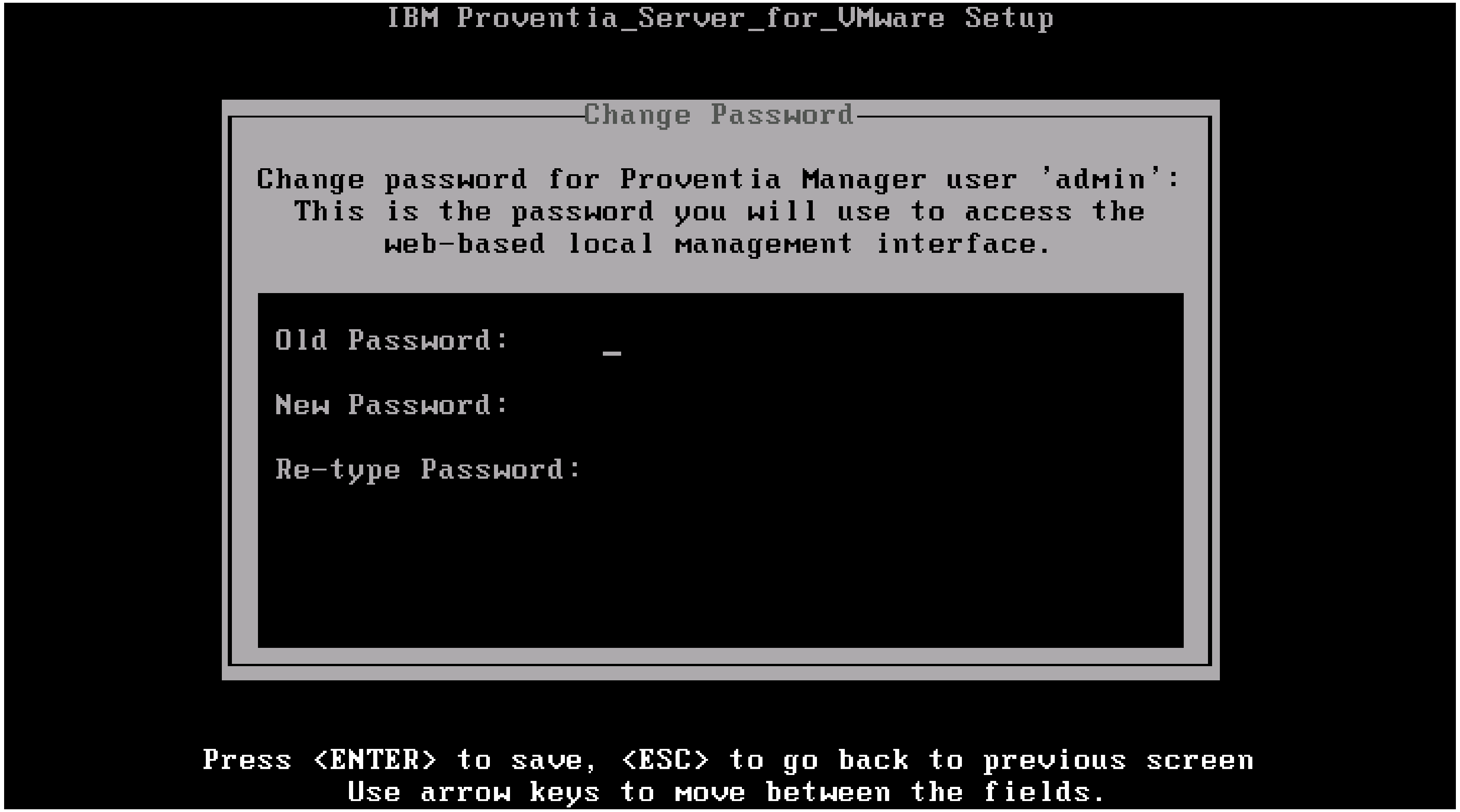
- Change the password for the root user.



```
IBM Proventia_Server_for_VMware Setup

Change Password

Change password for user 'root':

Old Password:     _

New Password:

Re-type Password:

Press <ENTER> to save, <ESC> to go back to previous screen
Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

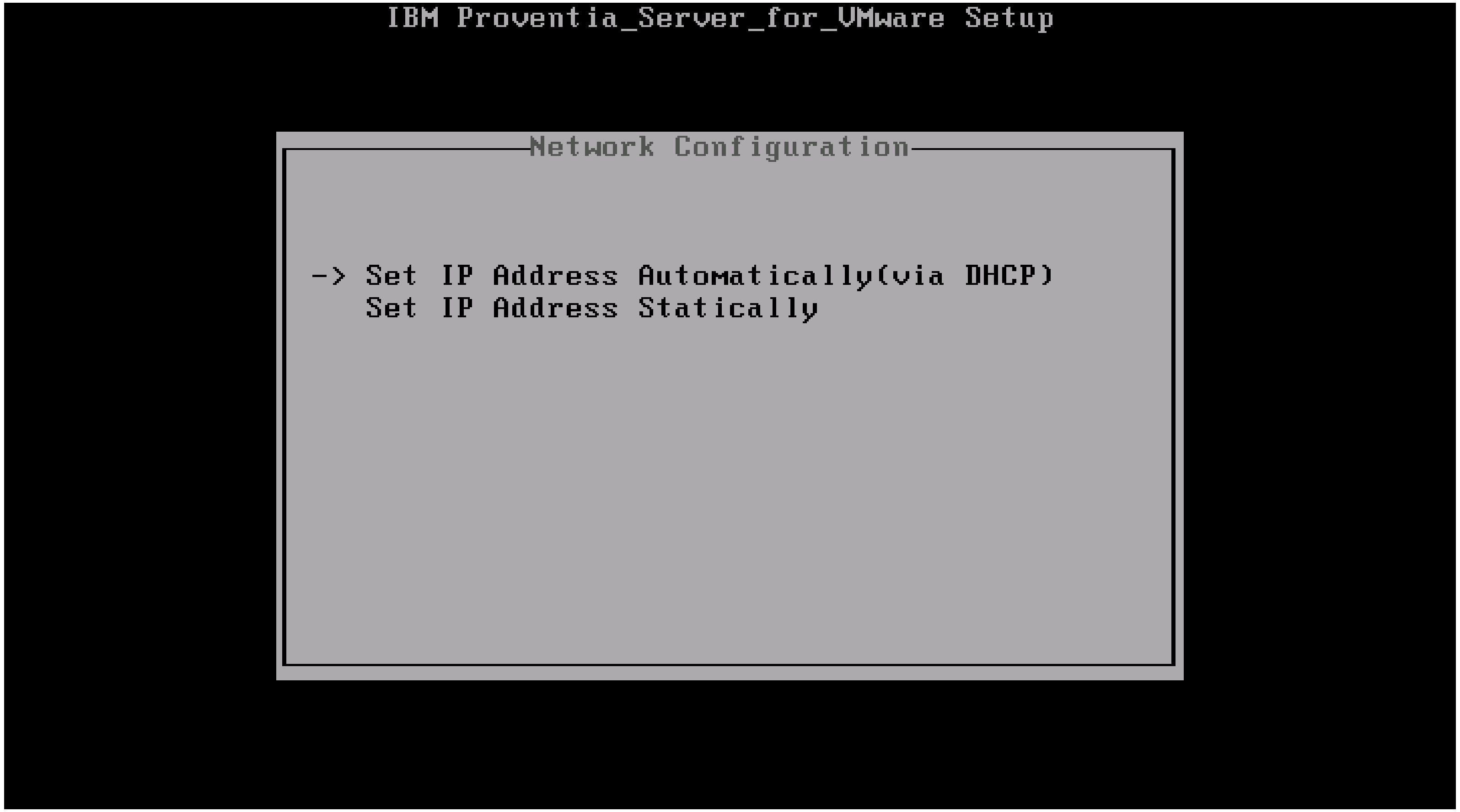
- Change the password for the web admin user.



```
IBM Proventia_Server_for_VMware Setup

Change Password

Change password for Proventia Manager user 'admin':
  This is the password you will use to access the
       web-based local management interface.

Old Password:      _

New Password:

Re-type Password:

Press <ENTER> to save, <ESC> to go back to previous screen
       Use arrow keys to move between the fields.
```

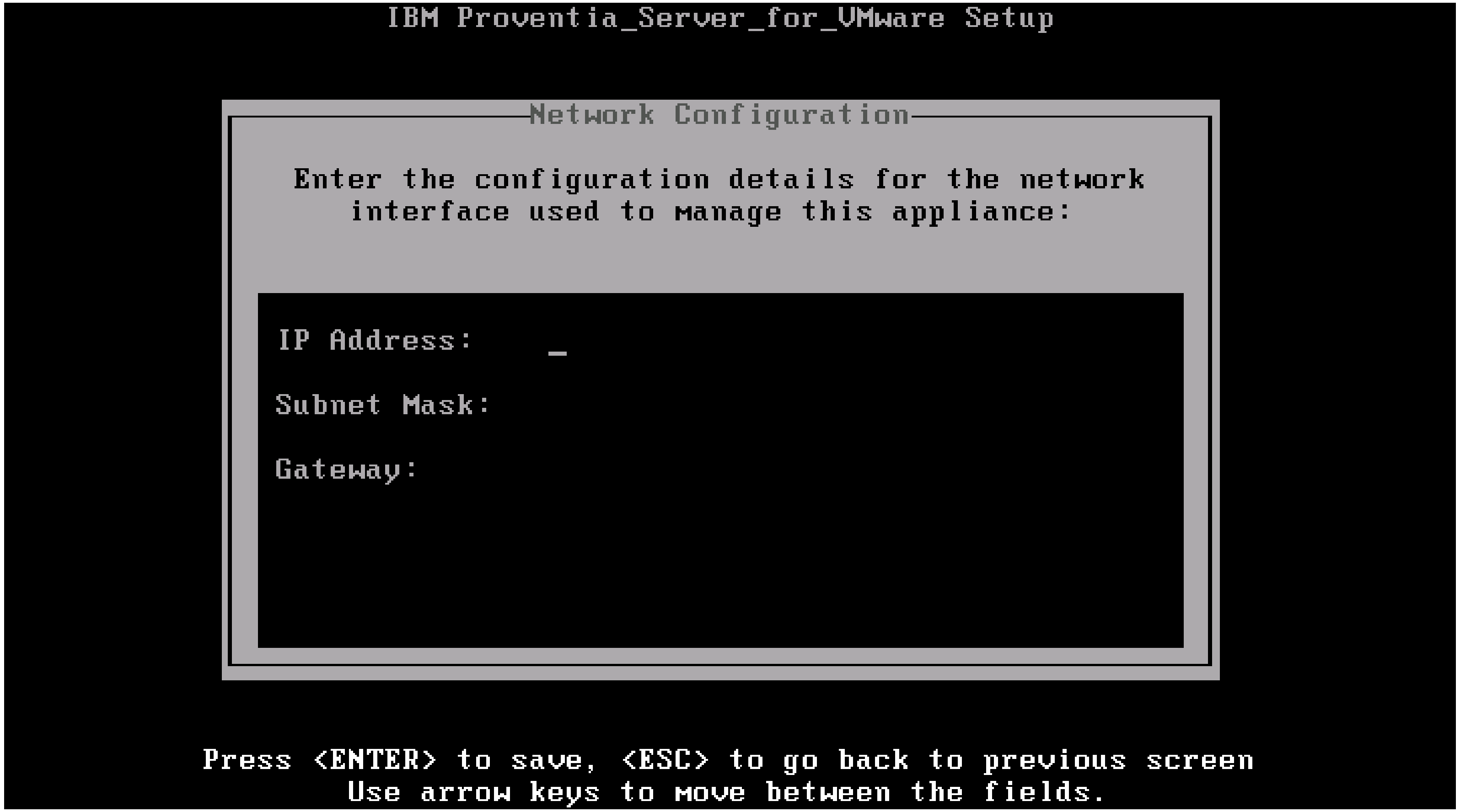
Virtual Server Protection – Initial Setup

- Configure the management interface.



```
IBM Proventia_Server_for_VMware Setup

Network Configuration

-> Set IP Address Automatically(via DHCP)
   Set IP Address Statically
```

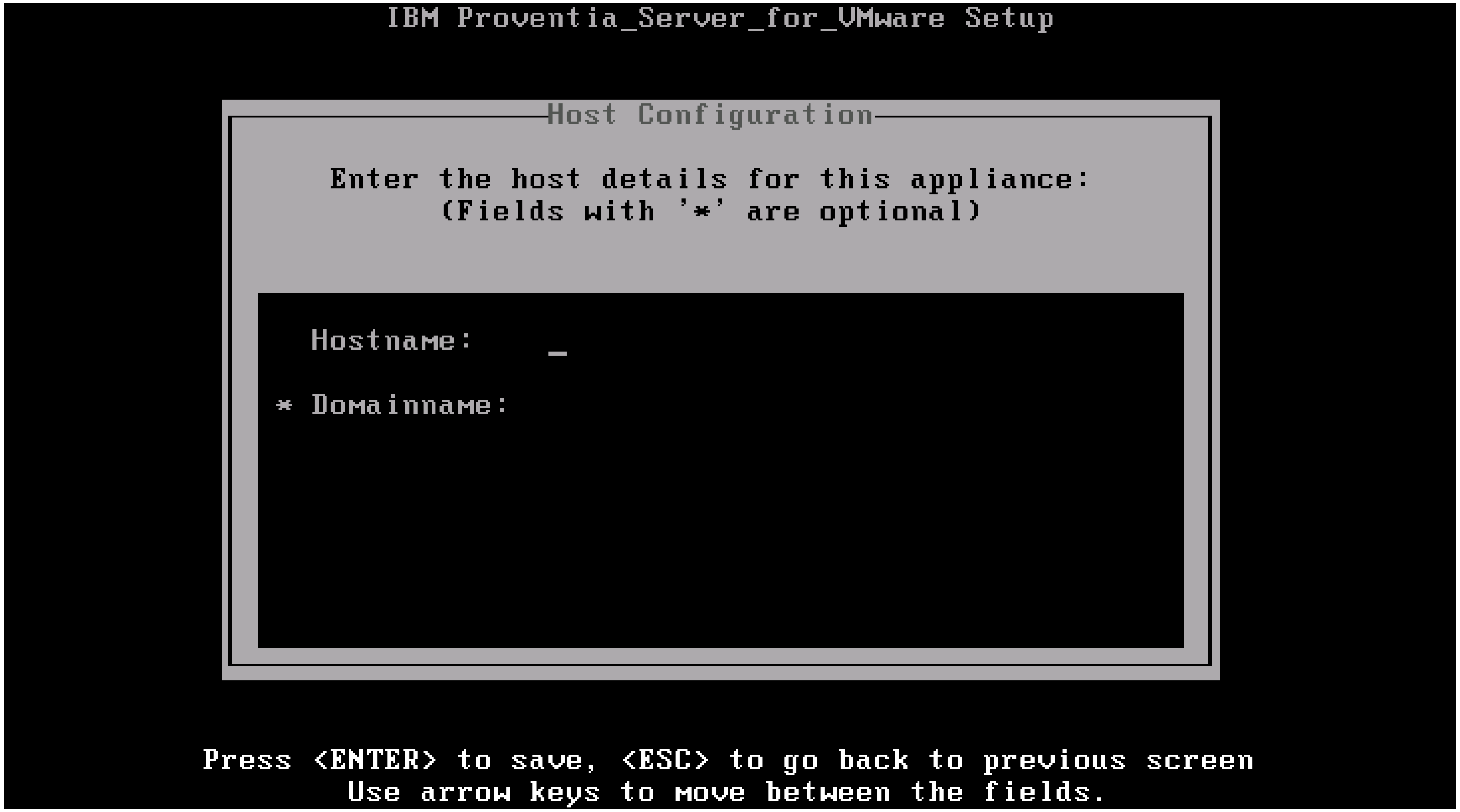
Virtual Server Protection – Initial Setup



```
                 IBM Proventia_Server_for_VMware Setup

                 Network Configuration

        Enter the configuration details for the network
          interface used to manage this appliance:

        IP Address:     _

        Subnet Mask:

        Gateway:

      Press <ENTER> to save, <ESC> to go back to previous screen
              Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

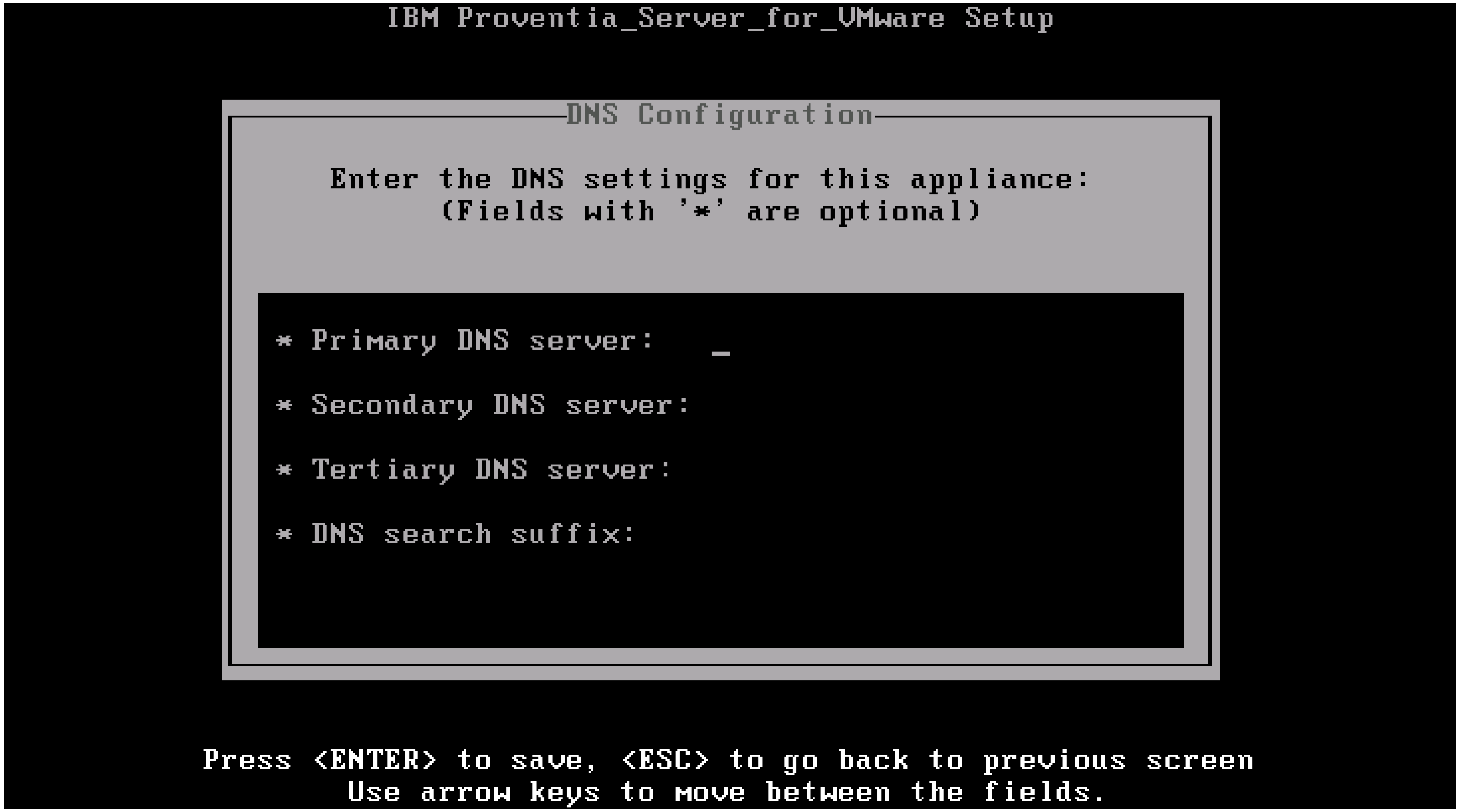
- Enter a hostname for the VSP SVM.



```
                    IBM Proventia_Server_for_VMware Setup

                        Host Configuration

              Enter the host details for this appliance:
                    (Fields with '*' are optional)

               Hostname:     _

             * Domainname:

      Press <ENTER> to save, <ESC> to go back to previous screen
              Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

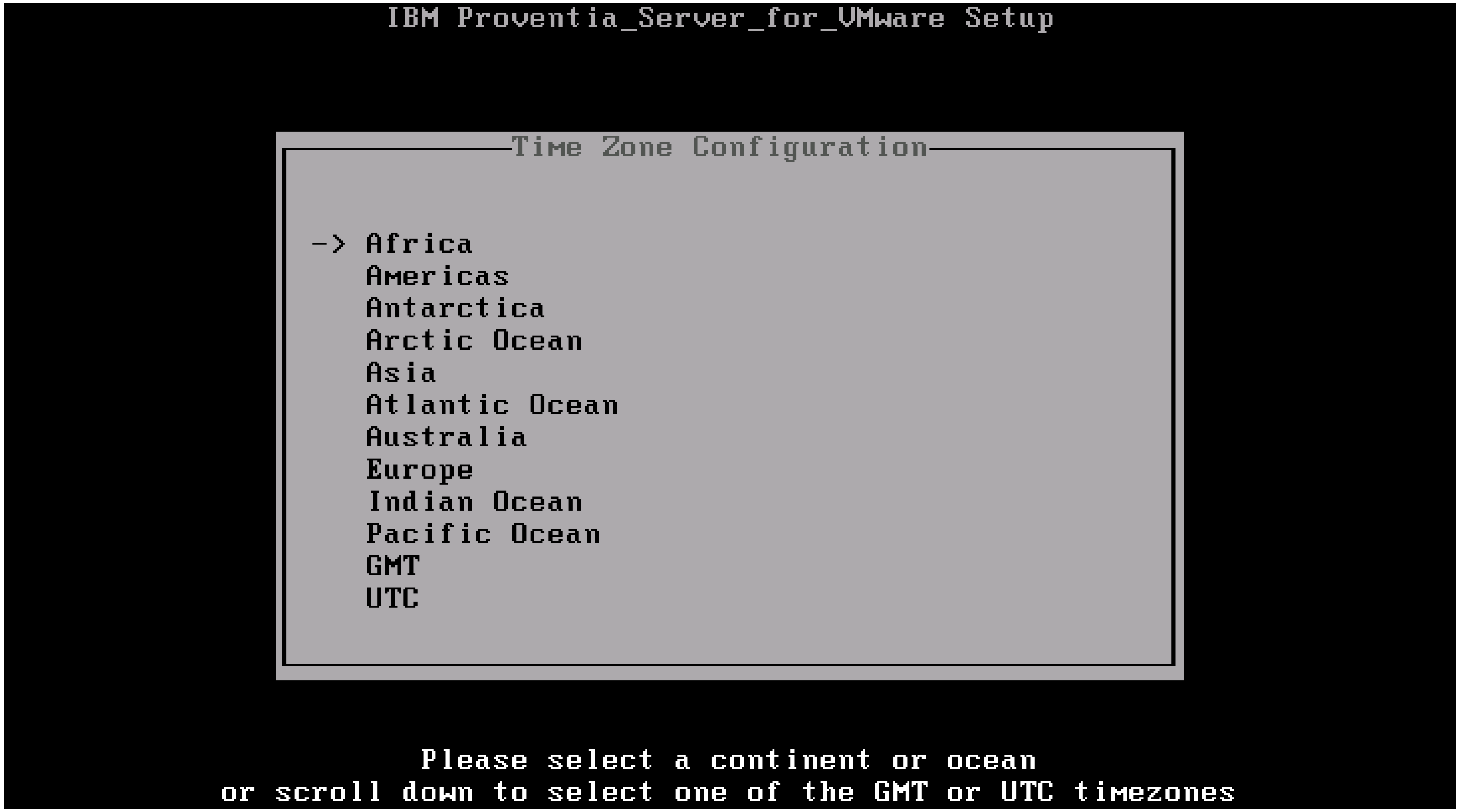
- Enter DNS configuration.



```
IBM Proventia_Server_for_VMware Setup

DNS Configuration

Enter the DNS settings for this appliance:
(Fields with '*' are optional)

* Primary DNS server:    _

* Secondary DNS server:

* Tertiary DNS server:

* DNS search suffix:

Press <ENTER> to save, <ESC> to go back to previous screen
Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

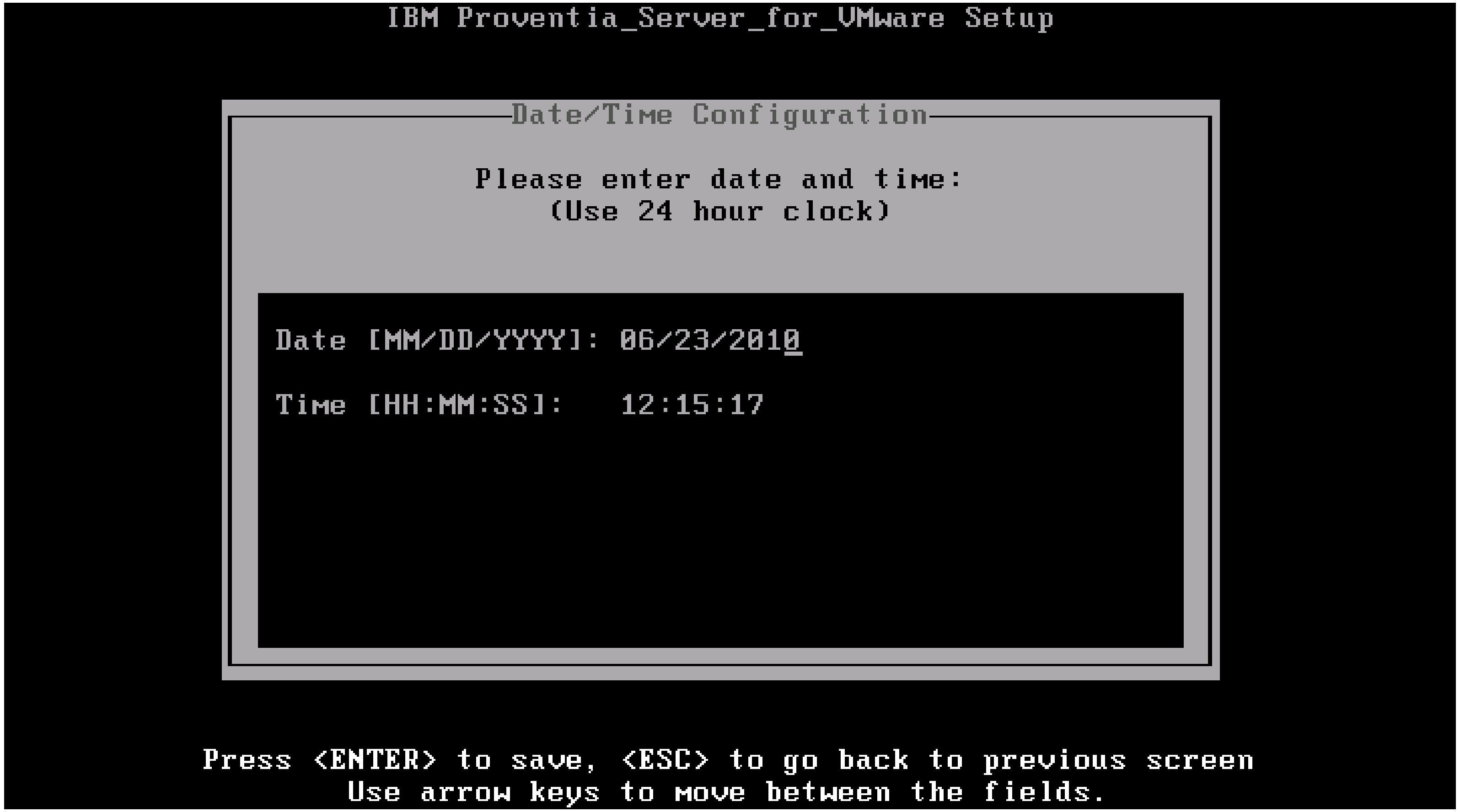
- Set the timezone for this VSP SVM. This needs to be correct for accurate communication with Siteprotector.



```
IBM Proventia_Server_for_VMware Setup

Time Zone Configuration

-> Africa
   Americas
   Antarctica
   Arctic Ocean
   Asia
   Atlantic Ocean
   Australia
   Europe
   Indian Ocean
   Pacific Ocean
   GMT
   UTC

Please select a continent or ocean
or scroll down to select one of the GMT or UTC timezones
```

Virtual Server Protection – Initial Setup

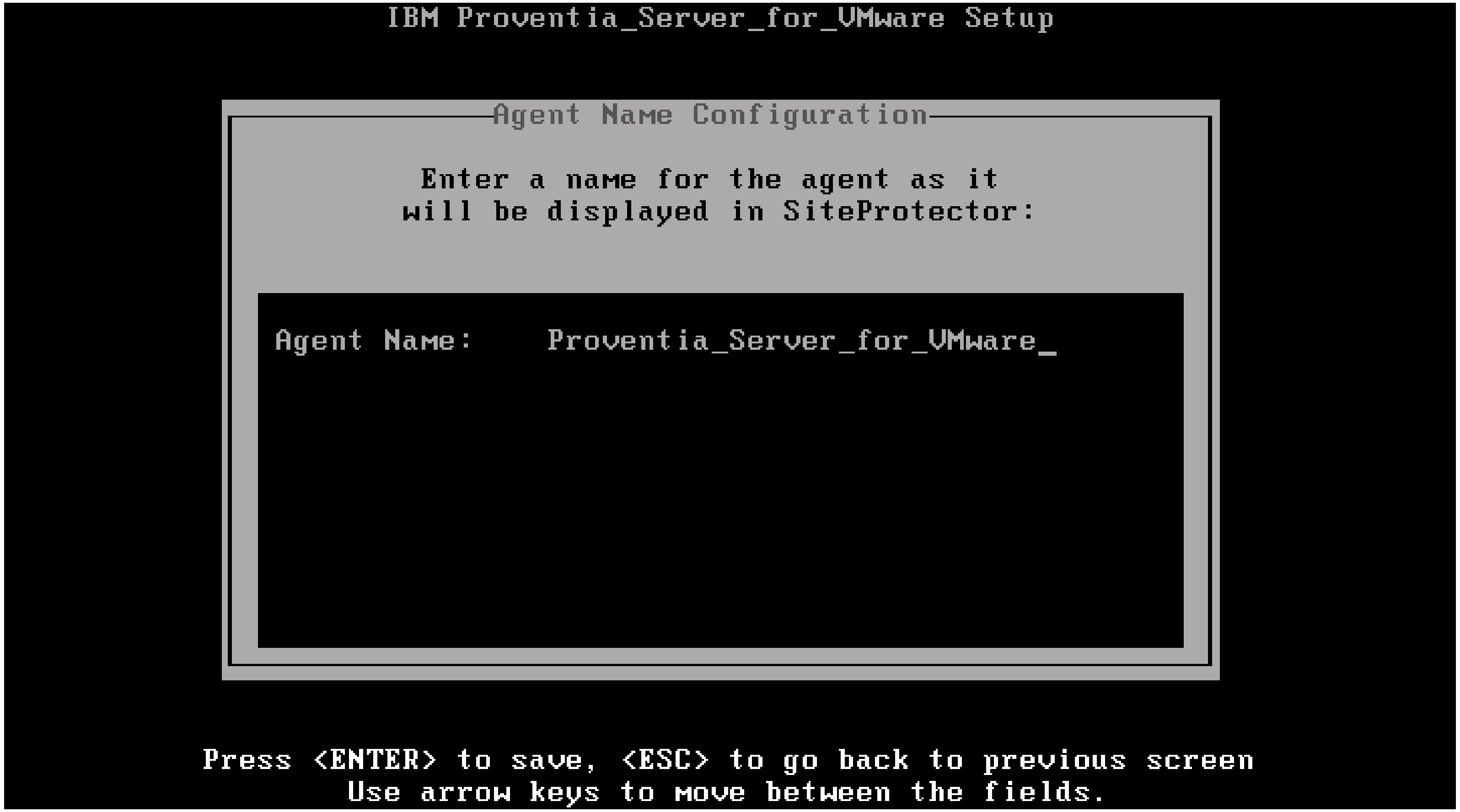
- Set the date and time for this VSP SVM. This needs to be correct for accurate communication with Siteprotector.



```
IBM Proventia_Server_for_VMware Setup

Date/Time Configuration

Please enter date and time:
(Use 24 hour clock)

Date [MM/DD/YYYY]: 06/23/2010

Time [HH:MM:SS]:   12:15:17

Press <ENTER> to save, <ESC> to go back to previous screen
Use arrow keys to move between the fields.
```

Virtual Server Protection – Initial Setup

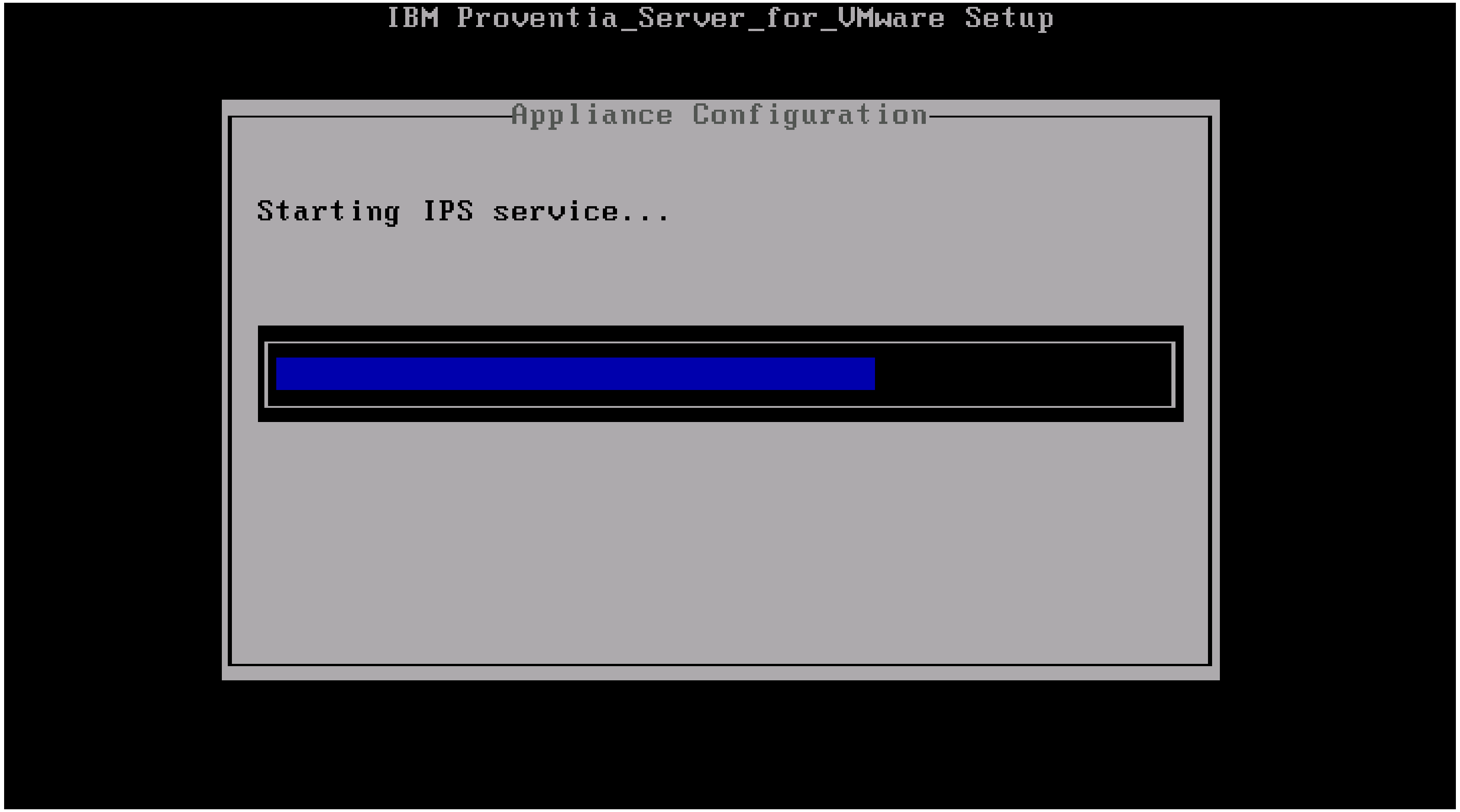
- Set the agent name for this VSP SVM. This is the agent name that will identify this VSP SVM in Siteprotector.



```
                 IBM Proventia_Server_for_VMware Setup

              Agent Name Configuration

              Enter a name for the agent as it
            will be displayed in SiteProtector:

   Agent Name:    Proventia_Server_for_VMware_

    Press <ENTER> to save, <ESC> to go back to previous screen
            Use arrow keys to move between the fields.
```

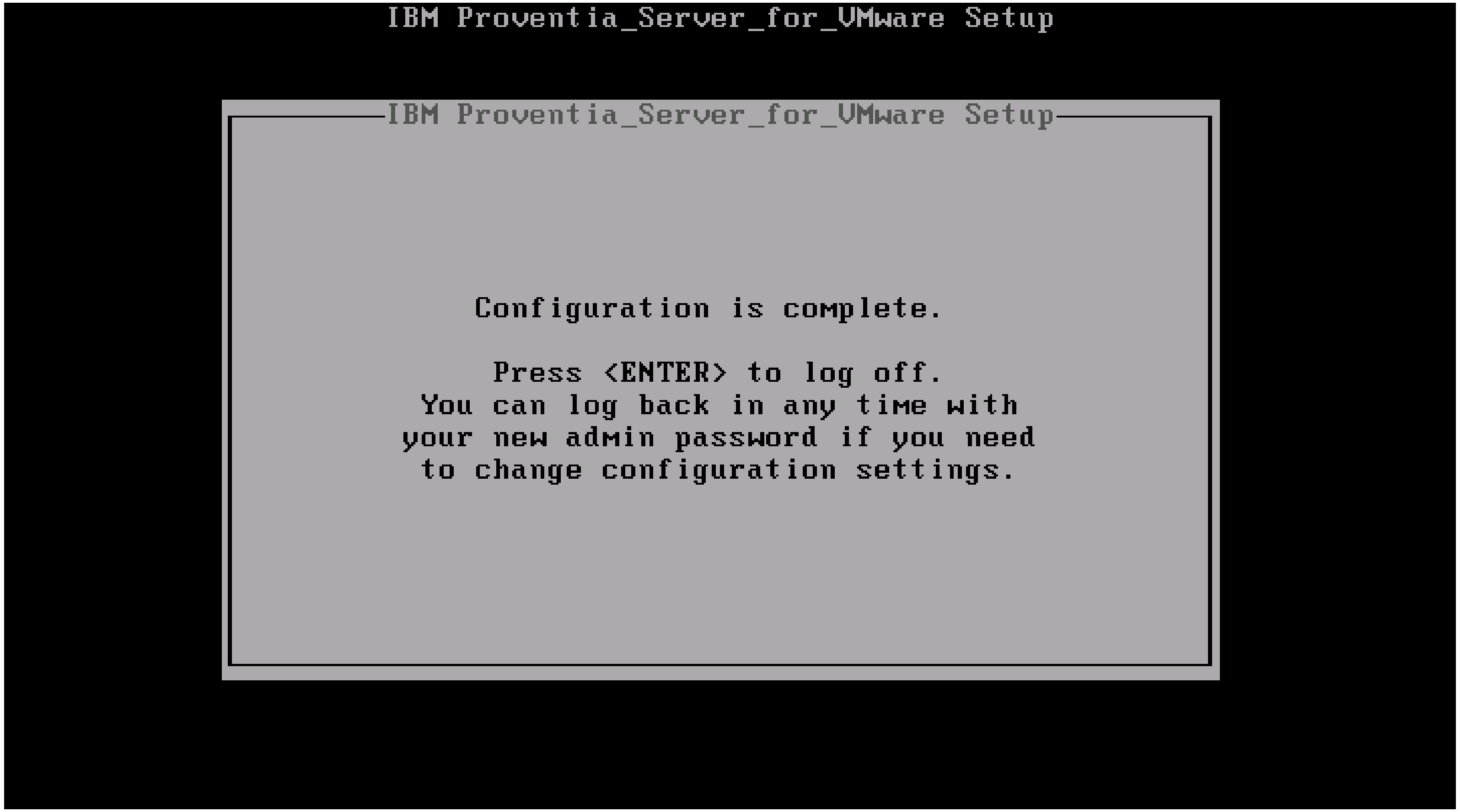
Virtual Server Protection – Initial Setup

- After the initial setup information has been entered, the appliance will be reconfigured and all necessary services will be started.



```
IBM Proventia_Server_for_VMware Setup

Appliance Configuration

Starting IPS service...
```

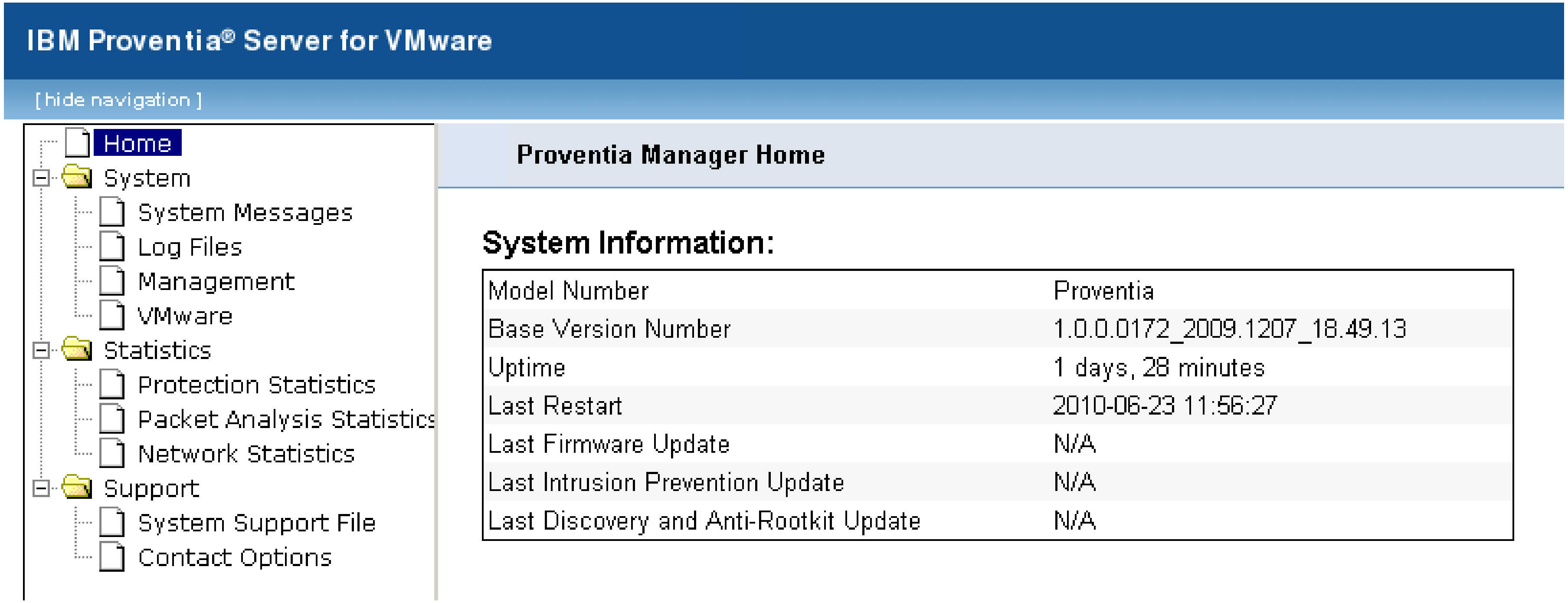
Virtual Server Protection – Initial Setup



```
IBM Proventia_Server_for_VMware Setup

IBM Proventia_Server_for_VMware Setup

Configuration is complete.

Press <ENTER> to log off.
You can log back in any time with
your new admin password if you need
to change configuration settings.
```

Virtual Server Protection – VMO Setup

- The next step is to configure the Virtual Machine Observer. This is done through the Proventia Manager web interface. Open a browser and go to https://<VSP_SVM_IP>.



IBM Proventia® Server for VMware

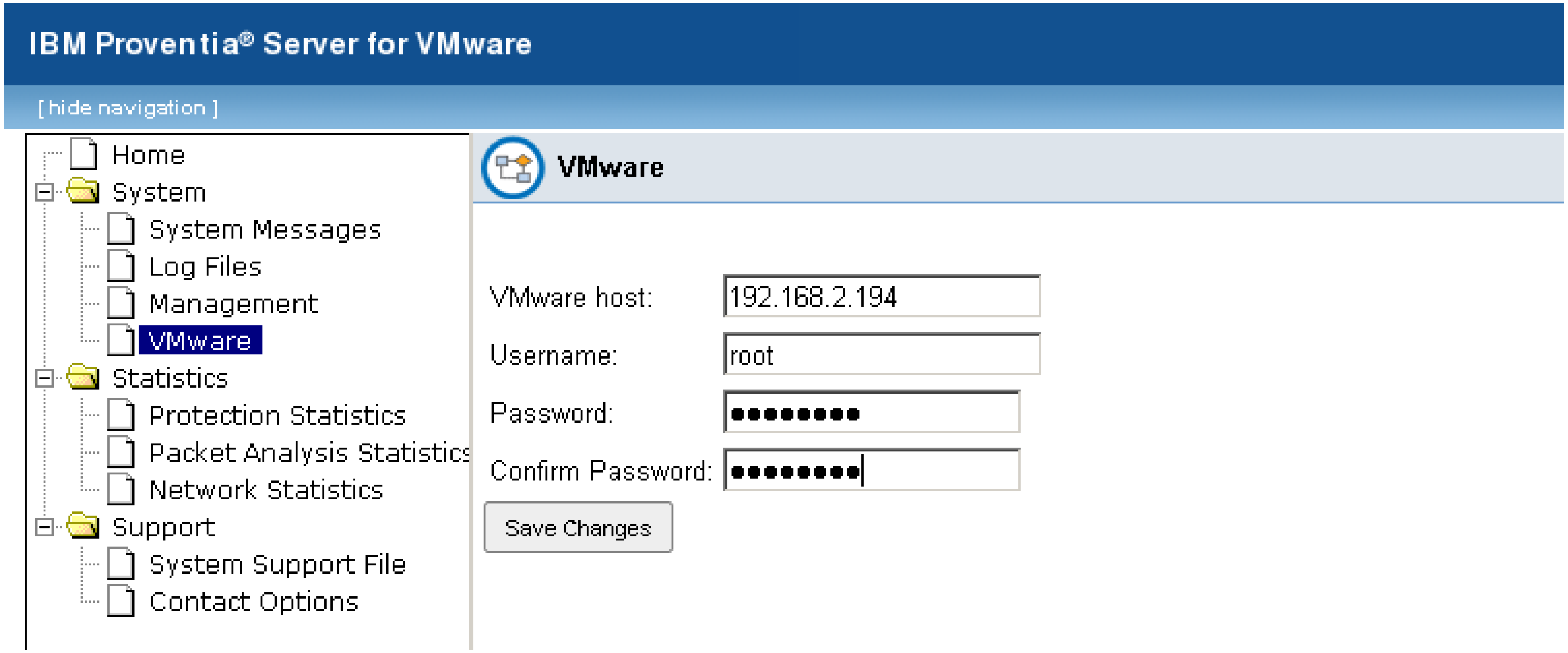
Proventia Manager Home

System Information:

Model Number	Proventia
Base Version Number	1.0.0.0172_2009.1207_18.49.13
Uptime	1 days, 28 minutes
Last Restart	2010-06-23 11:56:27
Last Firmware Update	N/A
Last Intrusion Prevention Update	N/A
Last Discovery and Anti-Rootkit Update	N/A

Virtual Server Protection – VMO Setup

- Under System on the VMware page, fill in the IP address and root user credentials for the ESX host and click save changes.
- This will allow the VSP VMO module to connect to the Virtual Infrastructure API and perform monitoring and configuration tasks on the Guest VMs.



VMware host: 192.168.2.194

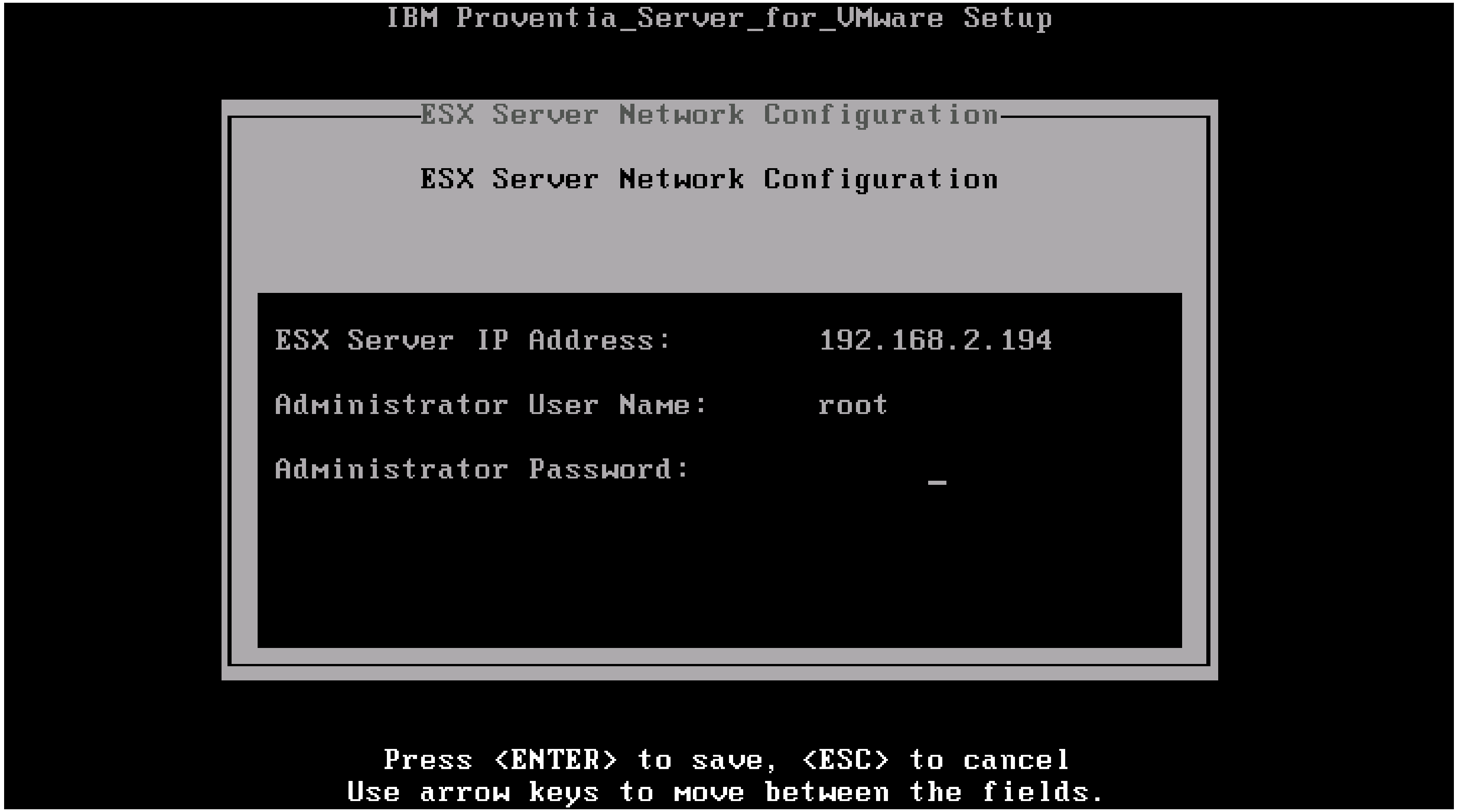
Username: root

Password: ●●●●●●●●●

Confirm Password: ●●●●●●●●●

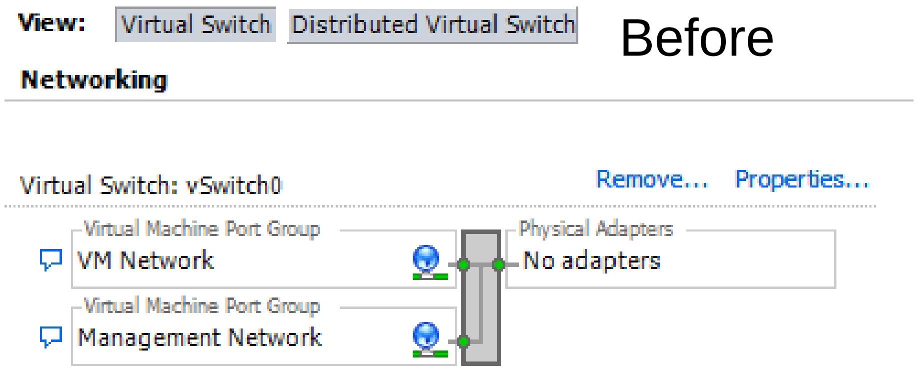
Virtual Server Protection – Introspection Setup

- For CPU/Mem and Network introspection to function, two introspection virtual switches need to be created and the ibm-iss-vmkmod module needs to be loaded in ESX.
- In the CLI configuration utility, under Network Configuration -> ESX Server Configuration, fill in the ESX host IP address and root user credentials:



```
IBM Proventia_Server_for_VMware Setup

ESX Server Network Configuration

ESX Server Network Configuration

ESX Server IP Address:          192.168.2.194

Administrator User Name:        root

Administrator Password:               _

Press <ENTER> to save, <ESC> to cancel
Use arrow keys to move between the fields.
```

Virtual Server Protection – Introspection Setup



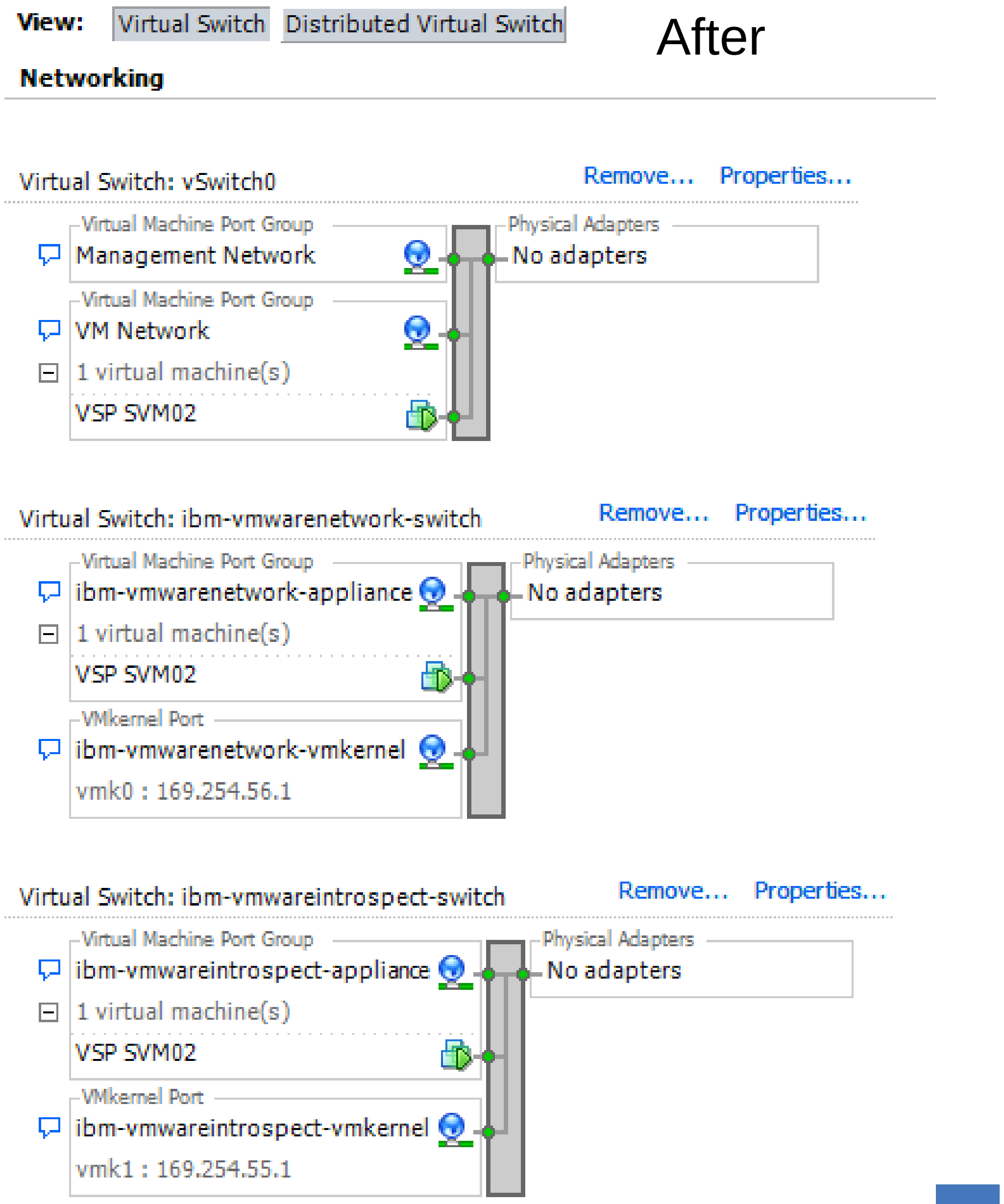
Before

View: Virtual Switch | Distributed Virtual Switch

Networking

Virtual Switch: vSwitch0 — Remove... Properties...

- Virtual Machine Port Group: VM Network
- Virtual Machine Port Group: Management Network
- Physical Adapters: No adapters



After

View: Virtual Switch | Distributed Virtual Switch

Networking

Virtual Switch: vSwitch0 — Remove... Properties...

- Virtual Machine Port Group: Management Network
- Virtual Machine Port Group: VM Network
  - 1 virtual machine(s)
  - VSP SVM02
- Physical Adapters: No adapters

Virtual Switch: ibm-vmwarenetwork-switch — Remove... Properties...

- Virtual Machine Port Group: ibm-vmwarenetwork-appliance
  - 1 virtual machine(s)
  - VSP SVM02
- VMkernel Port: ibm-vmwarenetwork-vmkernel
  - vmk0 : 169.254.56.1
- Physical Adapters: No adapters

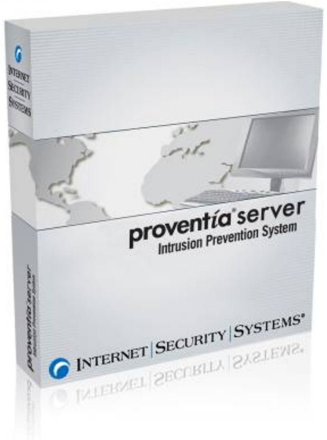
Virtual Switch: ibm-vmwareintrospect-switch — Remove... Properties...

- Virtual Machine Port Group: ibm-vmwareintrospect-appliance
  - 1 virtual machine(s)
  - VSP SVM02
- VMkernel Port: ibm-vmwareintrospect-vmkernel
  - vmk1 : 169.254.55.1
- Physical Adapters: No adapters

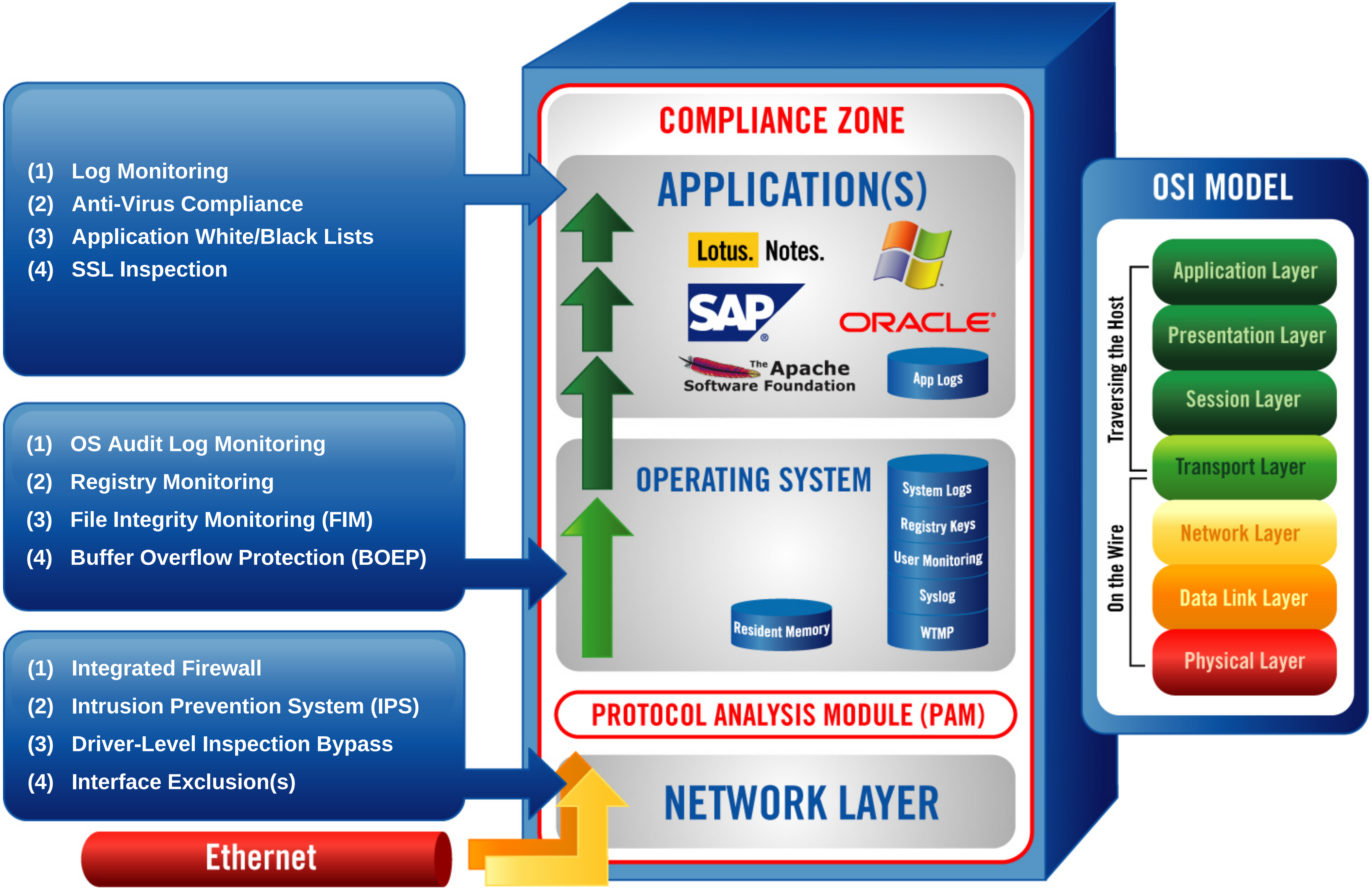
IBM Security Server Protection

RealSecure Server Sensor and **Proventia Server**

- ❑ Comprehensive, multi-layered protection in a single agent.
- ❑ Centrally managed with Proventia Management SiteProtector or MSS
- ❑ Provides the Virtual Patch® technology
- ❑ IBM has earned NSS Labs Certifications for HIPS and PCI Compliance
- ❑ IBM Server Protection agents can create a forensic trail of information by logging the Who, What, When and where of user activity
- ❑ Compliance Technologies include: File Integrity Monitoring (FIM), OS Auditing, Registry Integrity Monitoring, Anti-Virus Compliance, and Third Party Log Monitoring
- ❑ Broadest OS Coverage: **Windows, Linux, AIX, Solaris, HP-UX**



NSS Labs APPROVED



(1) Log Monitoring
(2) Anti-Virus Compliance
(3) Application White/Black Lists
(4) SSL Inspection

(1) OS Audit Log Monitoring
(2) Registry Monitoring
(3) File Integrity Monitoring (FIM)
(4) Buffer Overflow Protection (BOEP)

(1) Integrated Firewall
(2) Intrusion Prevention System (IPS)
(3) Driver-Level Inspection Bypass
(4) Interface Exclusion(s)

Agenda

1 IBM ISS Product Portfolio

2 IBM Security Network IPS + Initial Configuration

3 IBM Security Server Protection Solutions (VSP + Host IPS)

4 SiteProtector Training + Demonstration of the Products

5 Access to Resources (Training + Docs + Support)

6 Questions & Answers

SiteProtector Components and Assets

A SiteProtector deployment may include:

❑Deployment Manager

❑Event Collector and Site Database

❑Application Server (including Sensor Controller)

❑Agent Manager

❑X-Press Update Server

❑Console and Web portal

❑IBM Proventia appliances

❑IBM Proventia and other software agents

❑IBM SecurityFusion™ Module

Deployment Manager

❑Allows installation of all SiteProtector components and various ISS agents from central computer on your network

❑Can perform two types of installations:

– “Express” on a single machine

– “Recommended” on multiple machines

❑Uses Apache HTTP Server version 2.0

– Installed during Deployment Manager installation

IBM Security Site Protector and Product Demos

Agenda

1 IBM ISS Product Portfolio

2 IBM Security Network IPS + Initial Configuration

3 IBM Security Server Protection Solutions (VSP + Host IPS)

4 SiteProtector Training + Demonstration of the Products

5 **Access to Resources (Training + Docs + Support)**

6 Questions & Answers

Site Protector Licensing

Site Protector Product Codes and Descriptions

SPSW-BRNZ-P	SiteProtector Bronze Software Package - management for Proventia Protection
SPSW-BRNZ-P-M	SiteProtector Bronze Software Package - management for Proventia Protection - Maintenance
SPSW-GOLD-P	SiteProtector Gold Software Package - management for Proventia Protection
SPSW-GOLD-P-M	SiteProtector Gold Software Package - management for Proventia Protection - Maintenance
SPSW-SILV-P	SiteProtector Silver Software Package - management for Proventia Protection
SPSW-SILV-P-M	SiteProtector Silver Software Package - management for Proventia Protection - Maintenance
SPSW-UP-BRNZ-SILV-P	Upgrade SiteProtector Bronze to SiteProtector Silver
SPSW-UP-BRNZ-SILV-P-M	Upgrade SiteProtector Bronze to SiteProtector Silver - Maintenance
SPSW-UP-SILV-GOLD-P	Upgrade SiteProtector Silver to SiteProtector Gold
SPSW-UP-SILV-GOLD-P-M	Upgrade SiteProtector Silver to SiteProtector Gold - Maintenance

Network IPS Product Codes and Descriptions

GX4004C-V2-1-P	(ROHS) Proventia GX4004C-V2 Intrusion Prevention Appliance
GX4004C-V2-1-P-M	(ROHS) Proventia GX4004C-V2 Intrusion Prevention Appliance - Maintenance
GX4004C-V2-L-P	(ROHS) Proventia GX4004C-V2 Intrusion Prevention Appliance - License
GX4004C-V2-SPARE	(ROHS) Proventia GX4004C-V2 Intrusion Prevention Appliance - Spare
GX4004C-V2-SPARE-M	(ROHS) Proventia GX4004C-V2 Intrusion Prevention Appliance - Spare Maintenance
GX5008C-V2-1-P	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance
GX5008C-V2-1-P-M	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - Maintenance
GX5008C-V2-SPARE	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - Spare
GX5008C-V2-SPARE-M	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - Spare Maintenance
GX5008C-V2-HA-P	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - High Availability
GX5008C-V2-HA-P-M	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - High Availability Maintenance
GX5008C-V2-L-P	(ROHS) Proventia GX5008C-V2 Intrusion Prevention Appliance - License
GX5008SFP-V2-1-P	(ROHS) Proventia GX5008SFP-V2 Intrusion Prevention Appliance
GX5008SFP-V2-1-P-M	(ROHS) Proventia GX5008SFP-V2 Intrusion Prevention Appliance - Maintenance

Server Security Licensing and Product Codes

IBM Proventia Server & Real Secure Server Sensor

Proventia Server for Windows License - 001 - 024 Instances
Software Maintenance - Proventia Server

Proventia Server for LINUX License - 001 - 024 Instances
Software Maintenance - Proventia Server

RealSecure Server Sensor for Windows 2003 License - 001 - 024 Instances
Software Maintenance - RealSecure Server

RealSecure Server Sensor for Solaris / HPUX / AIX License - 001 - 024 Instances
Software Maintenance - RealSecure Server

IBM Virtual Server Security for VMware

(SVPV-BASE-1-P) License for 2 Processors
(SVPV-BASE-1-P-M) Maint for 2 Processors

(SVPV-ADD-1-P) License for Addl 2 Processors
(SVPV-ADD-1-P-M) Maint for Addl 2 Processors

Active Bypass Codes and Descriptions

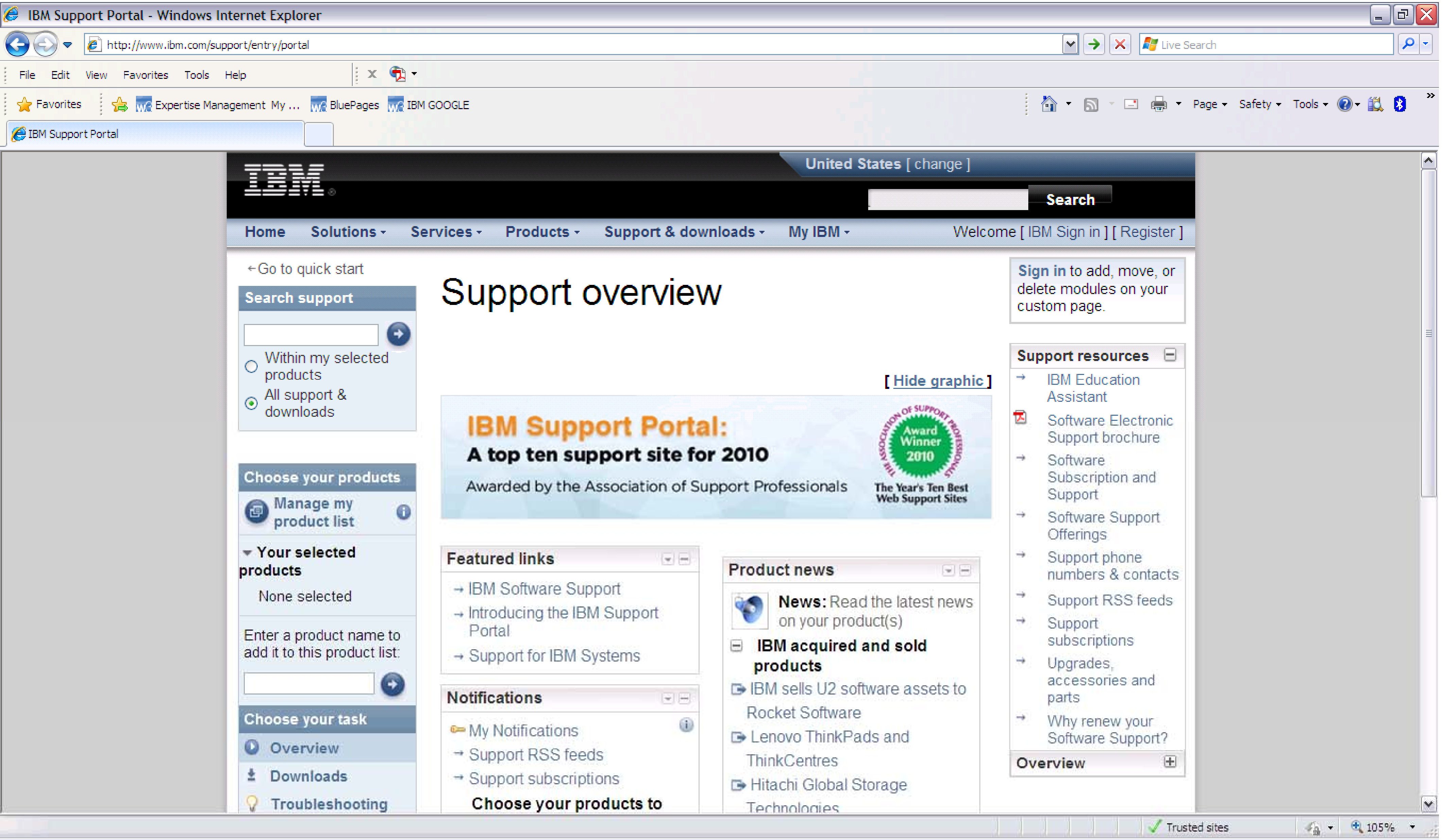
ABYP -> Active Bypass

T -> Copper Interface

S -> Short Fiber (Multi mode)

L -> Long Fiber (Single mode)

www.ibm.com/support/entry/portal



←Go to quick start

Search support

○ Within my selected products

● All support & downloads

Choose your products

Manage my product list

Your selected products

None selected

Enter a product name to add it to this product list:

Choose your task

Overview

Downloads

Troubleshooting

Support overview

[Hide graphic]

IBM Support Portal:

A top ten support site for 2010

Awarded by the Association of Support Professionals

The Association of Support Professionals Award Winner 2010

The Year's Ten Best Web Support Sites

Featured links

- → IBM Software Support
- → Introducing the IBM Support Portal
- → Support for IBM Systems

Notifications

- My Notifications
- → Support RSS feeds
- → Support subscriptions

Choose your products to

Product news

News: Read the latest news on your product(s)

IBM acquired and sold products

- IBM sells U2 software assets to Rocket Software
- Lenovo ThinkPads and ThinkCentres
- Hitachi Global Storage Technologies

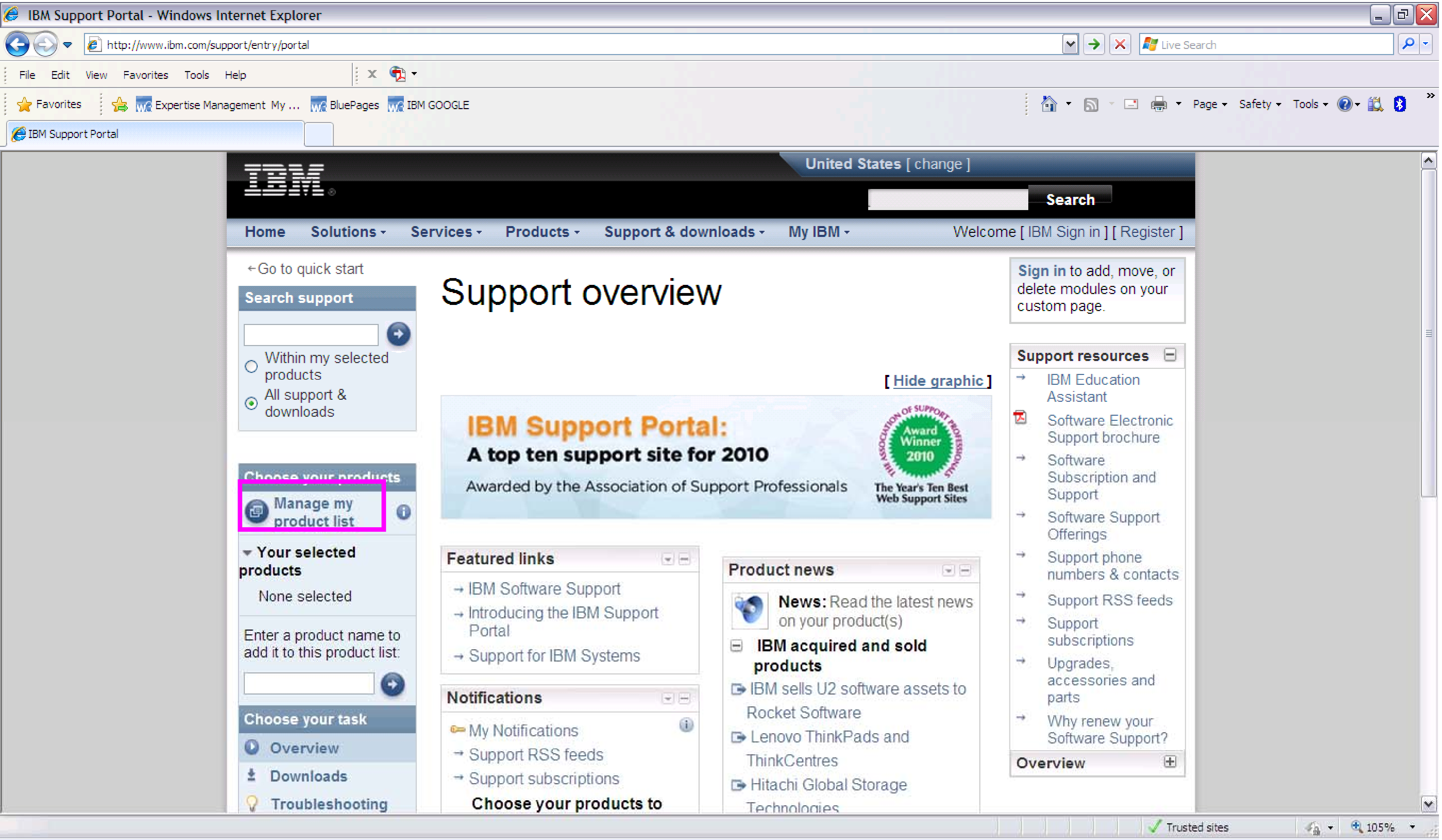
Sign in to add, move, or delete modules on your custom page.

Support resources

- → IBM Education Assistant
- Software Electronic Support brochure
- → Software Subscription and Support
- → Software Support Offerings
- → Support phone numbers & contacts
- → Support RSS feeds
- → Support subscriptions
- → Upgrades, accessories and parts
- → Why renew your Software Support?

Overview

Click – Manage my product list



IBM Support Portal - Windows Internet Explorer

http://www.ibm.com/support/entry/portal

United States [change]

Home | Solutions | Services | Products | Support & downloads | My IBM

Welcome [IBM Sign in] [Register]

←Go to quick start

Search support

○ Within my selected products
● All support & downloads

Choose your products

Manage my product list

Your selected products

None selected

Enter a product name to add it to this product list:

Choose your task

- Overview
- Downloads
- Troubleshooting

Support overview

[Hide graphic]

IBM Support Portal:
A top ten support site for 2010
Awarded by the Association of Support Professionals

Featured links

- IBM Software Support
- Introducing the IBM Support Portal
- Support for IBM Systems

Notifications

- My Notifications
- Support RSS feeds
- Support subscriptions

Choose your products to

Product news

News: Read the latest news on your product(s)

IBM acquired and sold products

- IBM sells U2 software assets to Rocket Software
- Lenovo ThinkPads and ThinkCentres
- Hitachi Global Storage Technologies

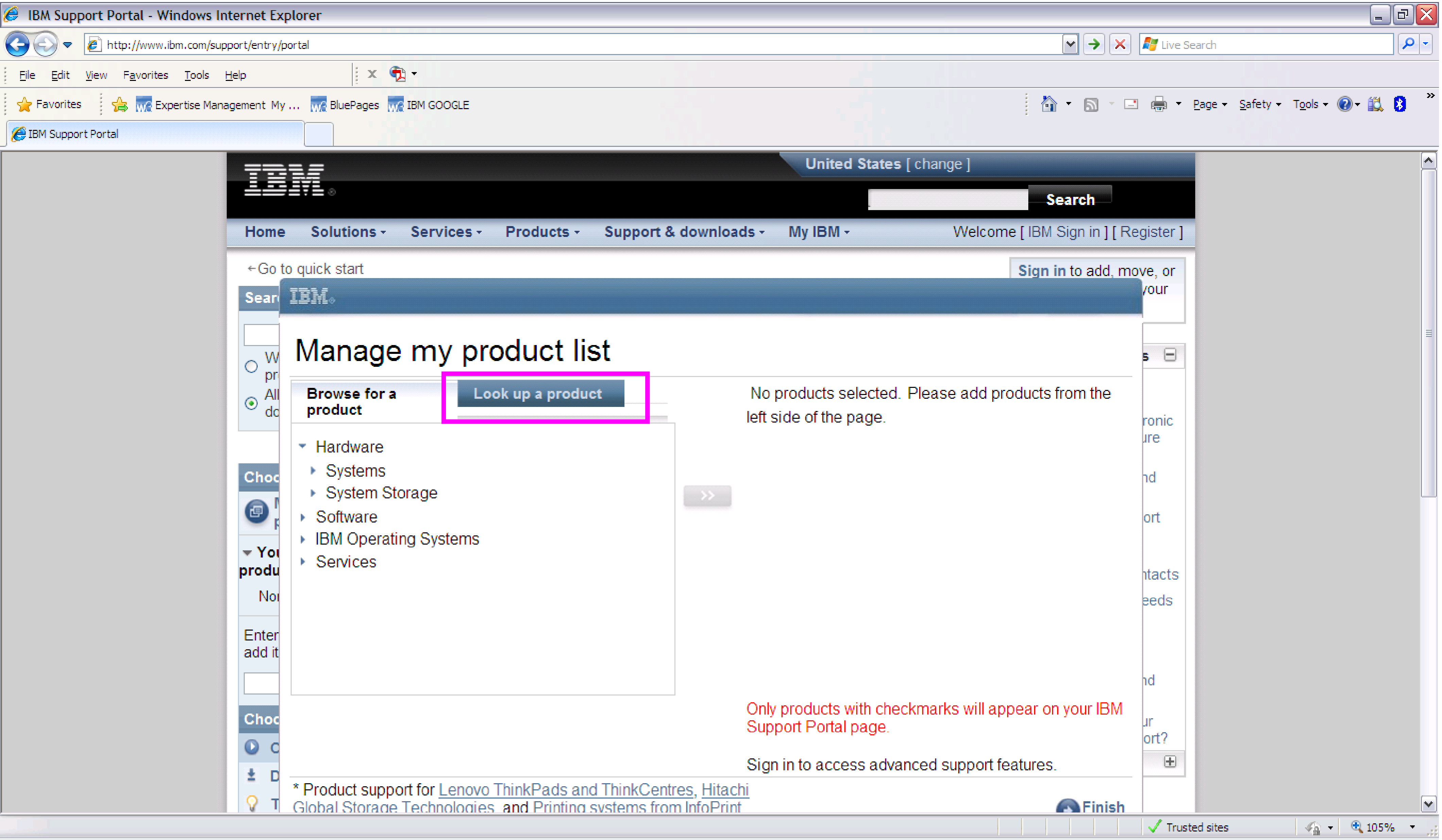
Sign in to add, move, or delete modules on your custom page.

Support resources

- IBM Education Assistant
- Software Electronic Support brochure
- Software Subscription and Support
- Software Support Offerings
- Support phone numbers & contacts
- Support RSS feeds
- Support subscriptions
- Upgrades, accessories and parts
- Why renew your Software Support?

Overview

Click – Look up a product



Manage my product list

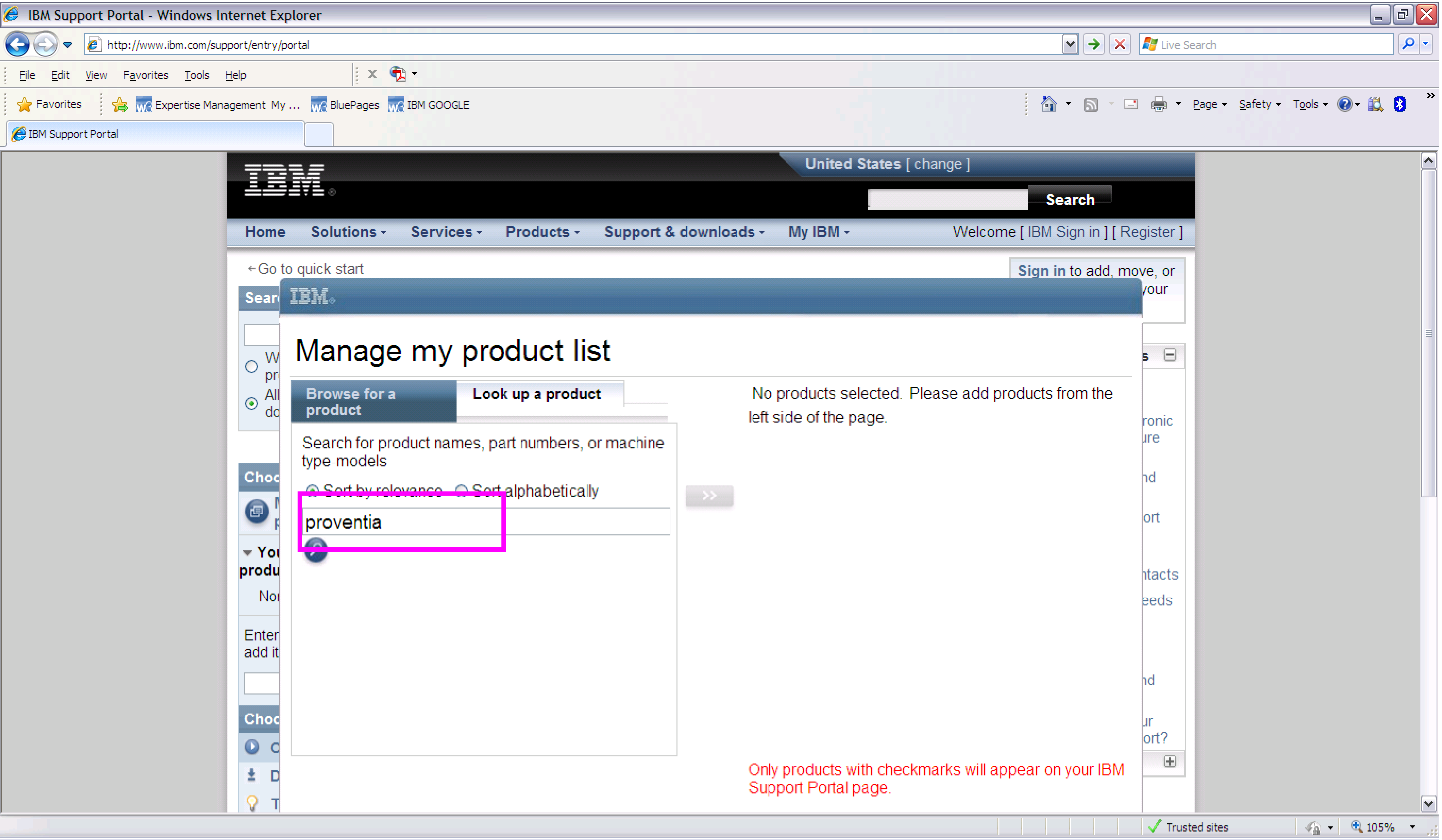
No products selected. Please add products from the left side of the page.

Only products with checkmarks will appear on your IBM Support Portal page.

Sign in to access advanced support features.

* Product support for Lenovo ThinkPads and ThinkCentres, Hitachi Global Storage Technologies, and Printing systems from InfoPrint

Search for proventia



IBM Support Portal - Windows Internet Explorer

http://www.ibm.com/support/entry/portal

Manage my product list

Browse for a product | Look up a product

Search for product names, part numbers, or machine type-models

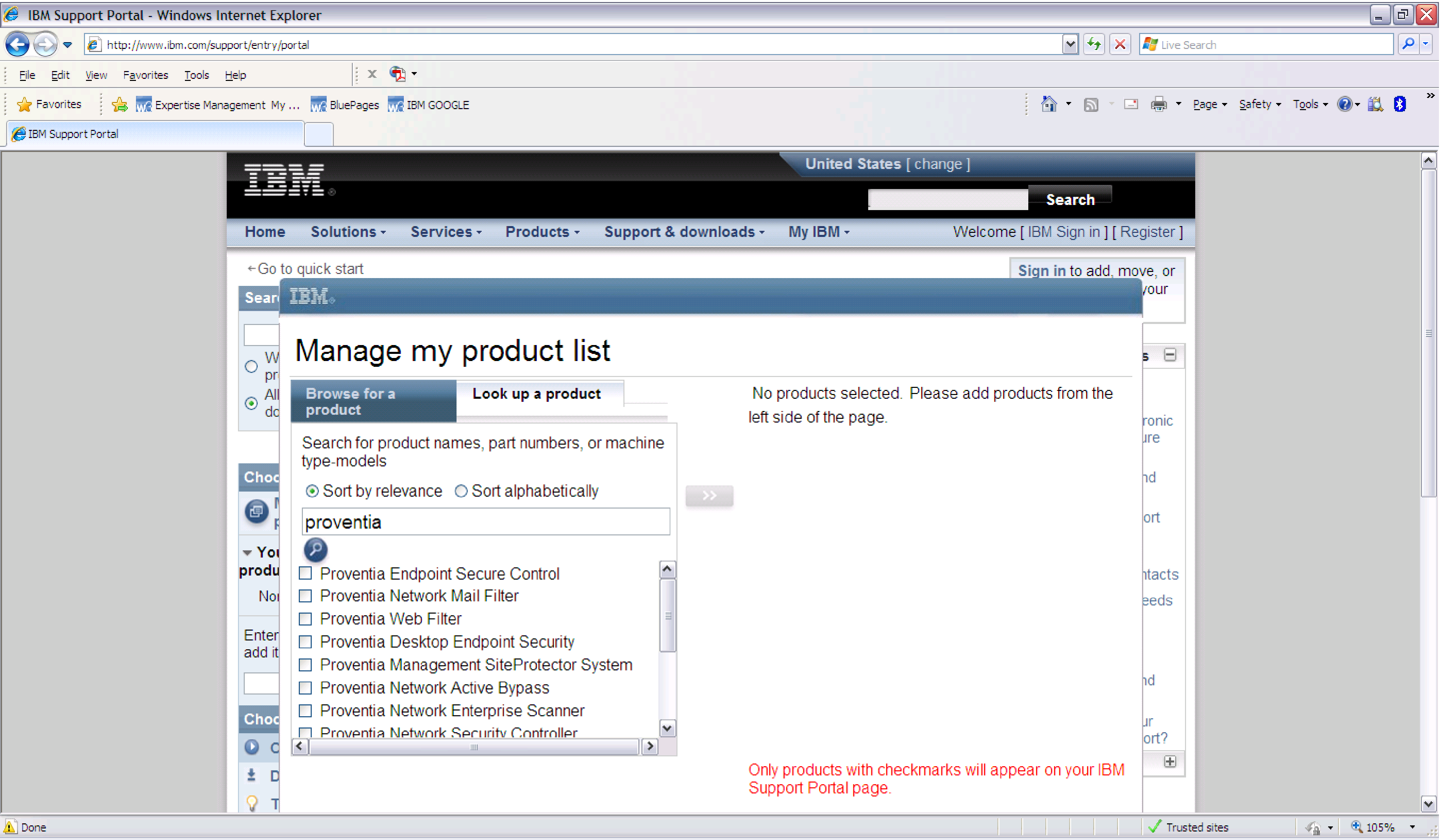
● Sort by relevance ○ Sort alphabetically

proventia

No products selected. Please add products from the left side of the page.

Only products with checkmarks will appear on your IBM Support Portal page.

Search results displayed



IBM Support Portal - Windows Internet Explorer
http://www.ibm.com/support/entry/portal
Live Search
File Edit View Favorites Tools Help
Favorites
Expertise Management My ...
BluePages
IBM GOOGLE
Page Safety Tools
IBM Support Portal
United States [change]
Search
Home Solutions Services Products Support & downloads My IBM
Welcome [IBM Sign in] [Register]
←Go to quick start
Sign in to add, move, or
Done
Trusted sites
105%

Manage my product list

Browse for a product | Look up a product

Search for product names, part numbers, or machine type-models

● Sort by relevance ○ Sort alphabetically

proventia

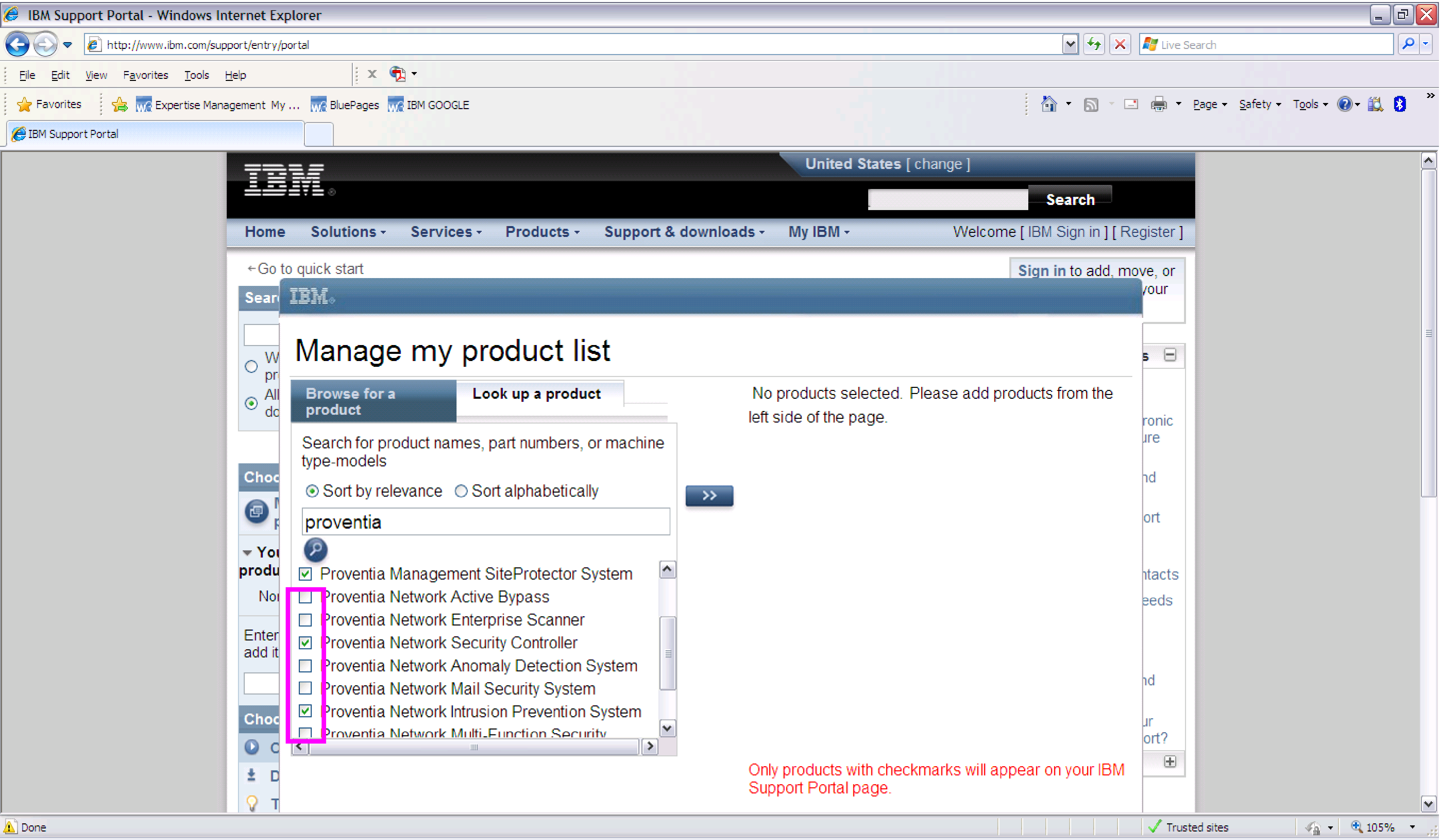
- □ Proventia Endpoint Secure Control
- □ Proventia Network Mail Filter
- □ Proventia Web Filter
- □ Proventia Desktop Endpoint Security
- □ Proventia Management SiteProtector System
- □ Proventia Network Active Bypass
- □ Proventia Network Enterprise Scanner
- □ Proventia Network Security Controller

No products selected. Please add products from the left side of the page.

Only products with checkmarks will appear on your IBM Support Portal page.

Tivoli. IBM Internet Security Systems

Select & add – proventia products of interest



Manage my product list

Browse for a product | Look up a product

Search for product names, part numbers, or machine type-models

● Sort by relevance ○ Sort alphabetically

proventia

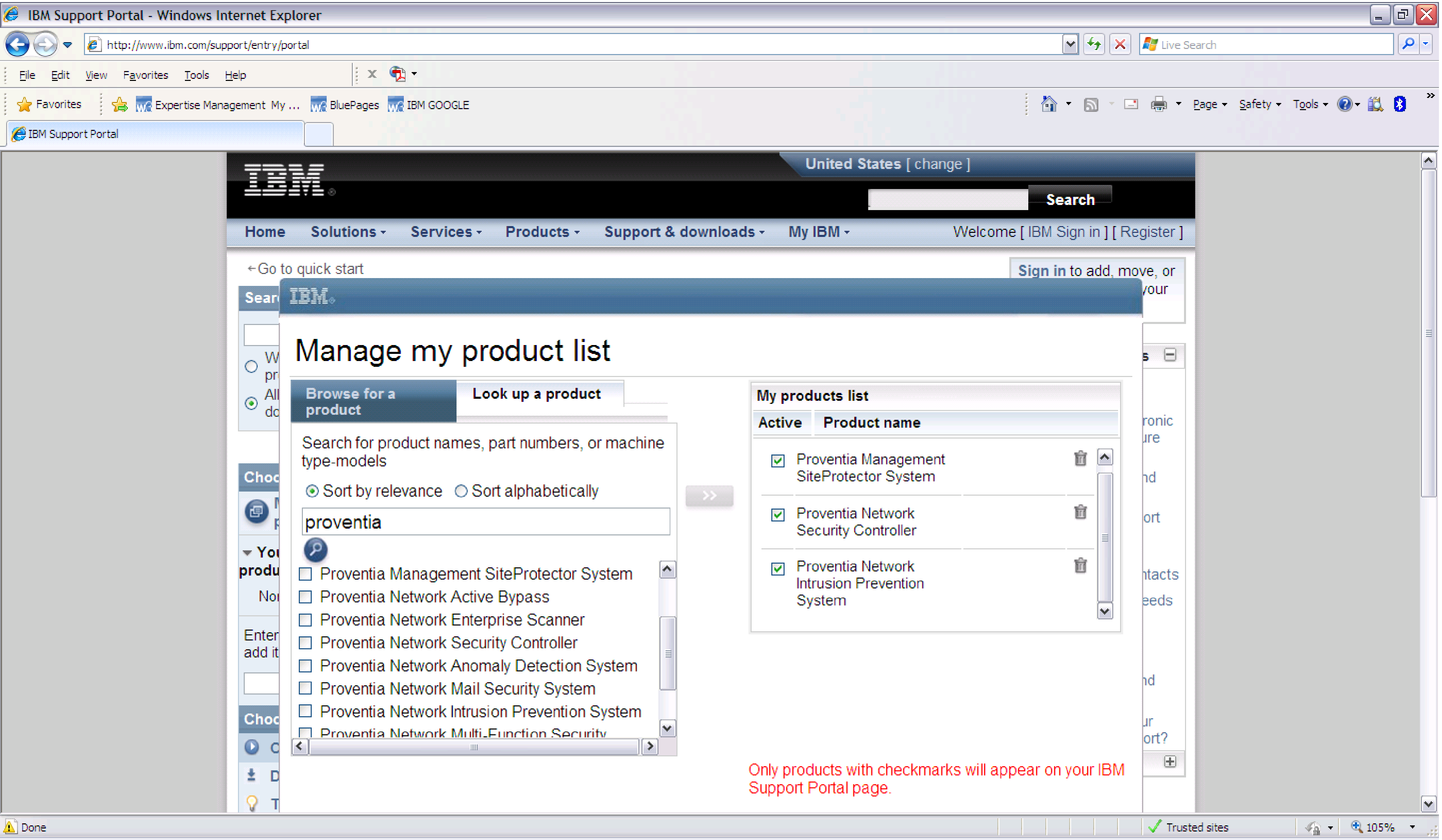
☑ Proventia Management SiteProtector System
□ Proventia Network Active Bypass
□ Proventia Network Enterprise Scanner
☑ Proventia Network Security Controller
□ Proventia Network Anomaly Detection System
□ Proventia Network Mail Security System
☑ Proventia Network Intrusion Prevention System
□ Proventia Network Multi-Function Security

>>

No products selected. Please add products from the left side of the page.

Only products with checkmarks will appear on your IBM Support Portal page.

My product list created



Manage my product list

Browse for a product | Look up a product

Search for product names, part numbers, or machine type-models

● Sort by relevance ○ Sort alphabetically

proventia

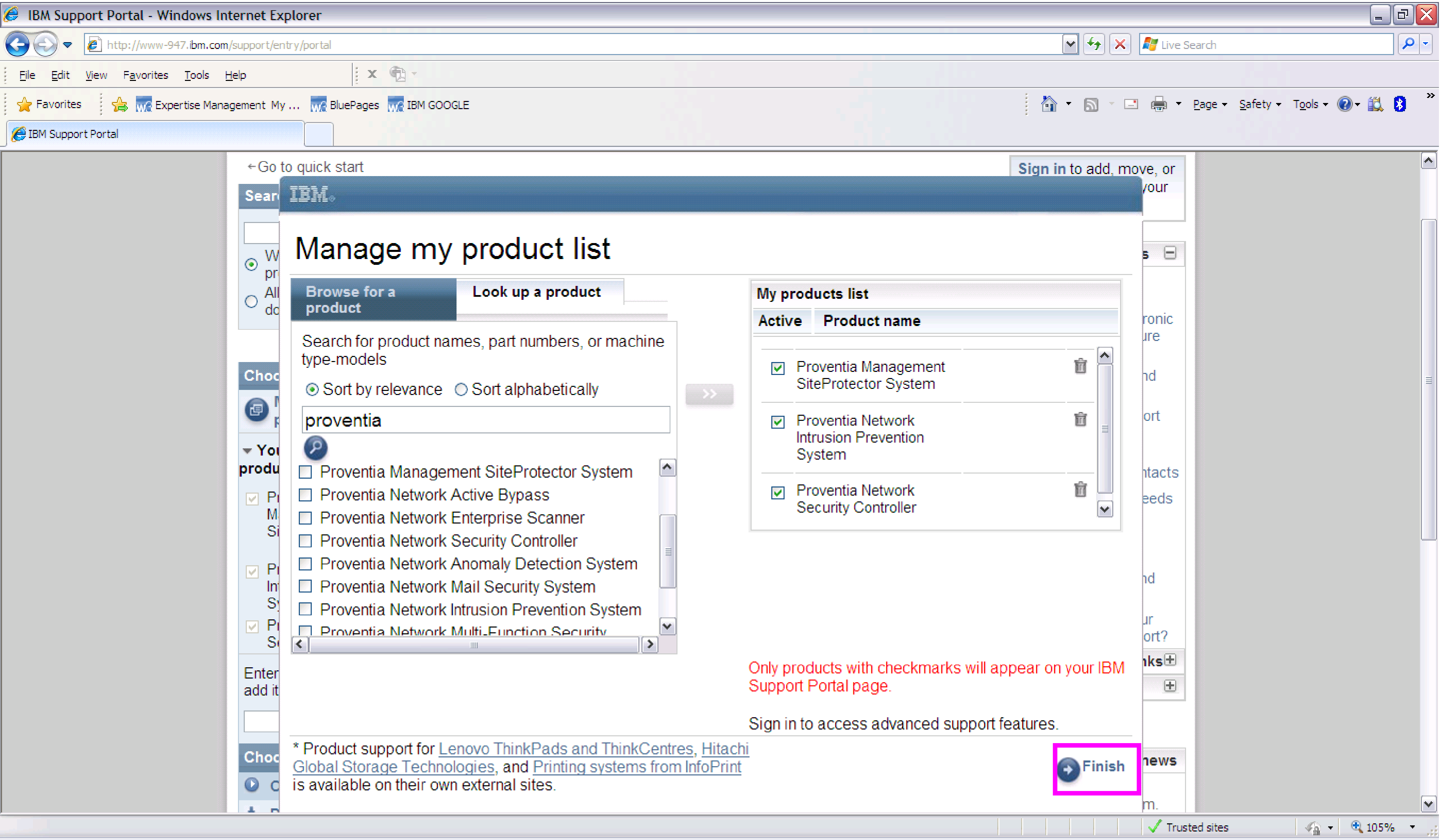
- □ Proventia Management SiteProtector System
- □ Proventia Network Active Bypass
- □ Proventia Network Enterprise Scanner
- □ Proventia Network Security Controller
- □ Proventia Network Anomaly Detection System
- □ Proventia Network Mail Security System
- □ Proventia Network Intrusion Prevention System
- □ Proventia Network Multi-Function Security

My products list

Active	Product name
☑	Proventia Management SiteProtector System
☑	Proventia Network Security Controller
☑	Proventia Network Intrusion Prevention System

Only products with checkmarks will appear on your IBM Support Portal page.

Click - Finish


IBM Support Portal - Windows Internet Explorer
http://www-947.ibm.com/support/entry/portal
Live Search
File Edit View Favorites Tools Help
Favorites
Expertise Management My ...
BluePages
IBM GOOGLE
Page Safety Tools
IBM Support Portal
←Go to quick start
Sign in to add, move, or
IBM.
Trusted sites
105%

Manage my product list

Browse for a product | Look up a product

Search for product names, part numbers, or machine type-models

● Sort by relevance ○ Sort alphabetically

proventia

- □ Proventia Management SiteProtector System
- □ Proventia Network Active Bypass
- □ Proventia Network Enterprise Scanner
- □ Proventia Network Security Controller
- □ Proventia Network Anomaly Detection System
- □ Proventia Network Mail Security System
- □ Proventia Network Intrusion Prevention System
- □ Proventia Network Multi-Function Security

My products list

Active	Product name
☑	Proventia Management SiteProtector System
☑	Proventia Network Intrusion Prevention System
☑	Proventia Network Security Controller

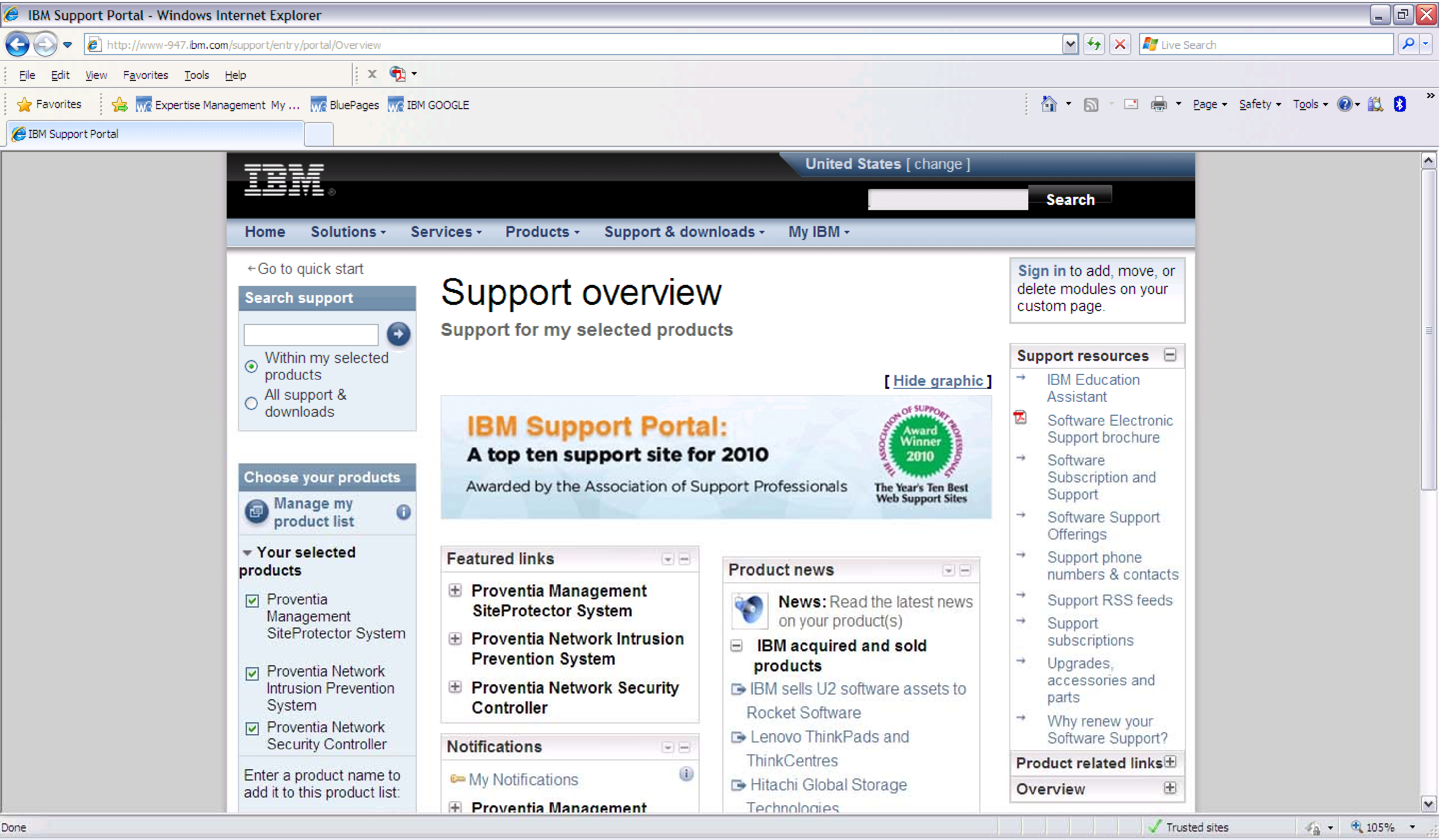
Only products with checkmarks will appear on your IBM Support Portal page.

Sign in to access advanced support features.

* Product support for Lenovo ThinkPads and ThinkCentres, Hitachi Global Storage Technologies, and Printing systems from InfoPrint is available on their own external sites.

Finish

Main page configured with my product list



←Go to quick start

Search support

● Within my selected products
○ All support & downloads

Choose your products

Manage my product list

Your selected products

☑ Proventia Management SiteProtector System
☑ Proventia Network Intrusion Prevention System
☑ Proventia Network Security Controller

Enter a product name to add it to this product list:

Support overview

Support for my selected products

[Hide graphic]

IBM Support Portal:
A top ten support site for 2010
Awarded by the Association of Support Professionals

The Association of Support Professionals Award Winner 2010
The Year's Ten Best Web Support Sites

Featured links

- Proventia Management SiteProtector System
- Proventia Network Intrusion Prevention System
- Proventia Network Security Controller

Notifications

My Notifications

Proventia Management

Product news

News: Read the latest news on your product(s)

IBM acquired and sold products

- IBM sells U2 software assets to Rocket Software
- Lenovo ThinkPads and ThinkCentres
- Hitachi Global Storage Technologies

Sign in to add, move, or delete modules on your custom page.

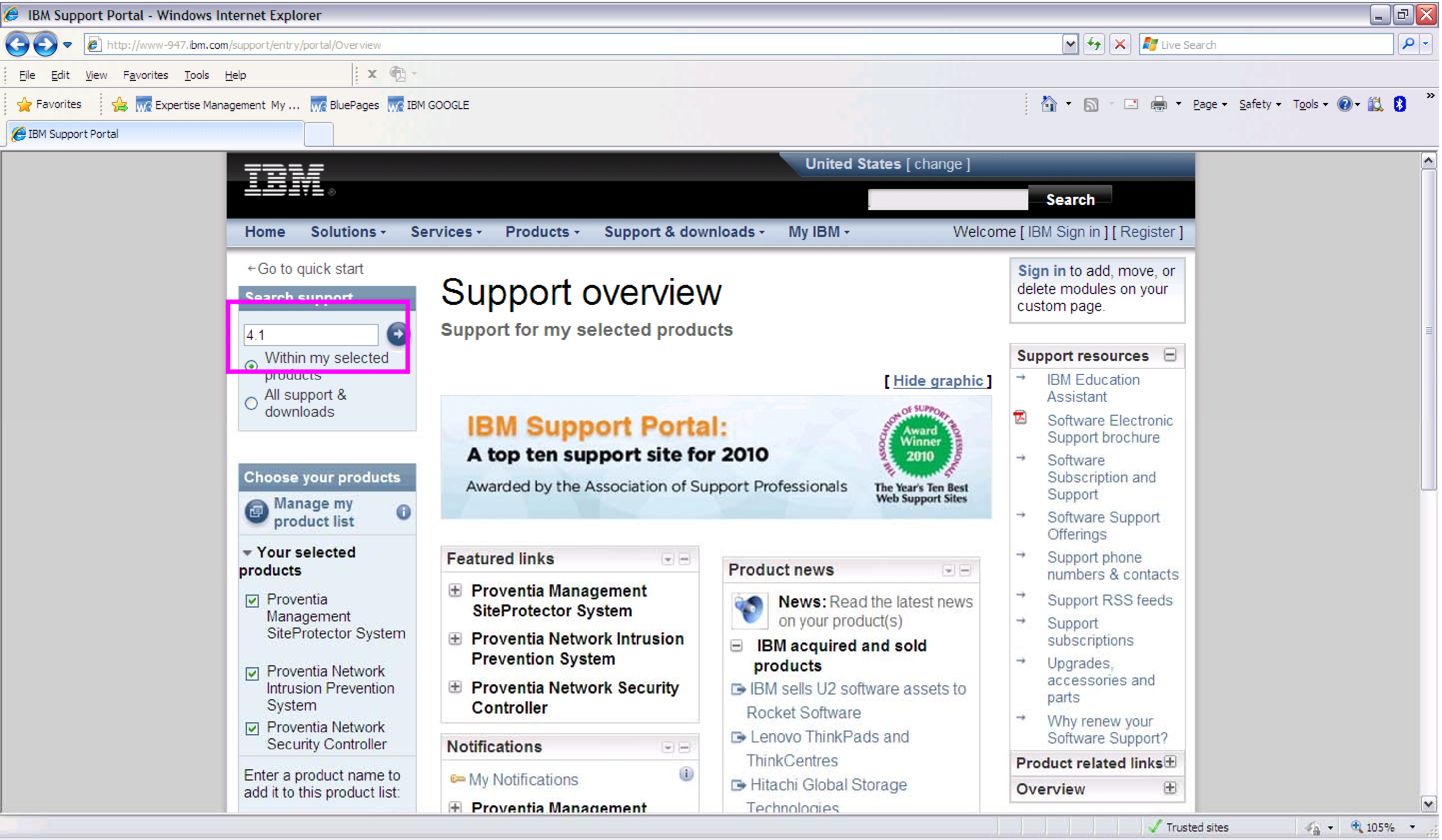
Support resources

- IBM Education Assistant
- Software Electronic Support brochure
- Software Subscription and Support
- Software Support Offerings
- Support phone numbers & contacts
- Support RSS feeds
- Support subscriptions
- Upgrades, accessories and parts
- Why renew your Software Support?

Product related links

Overview

Search for info within my selected products


IBM Support Portal - Windows Internet Explorer
http://www-947.ibm.com/support/entry/portal/Overview
Live Search
File Edit View Favorites Tools Help
Favorites
Expertise Management My ...
BluePages
IBM GOOGLE
Page Safety Tools
IBM Support Portal
Trusted sites
105%

United States [change]

Search

Home Solutions Products Support & downloads My IBM Welcome [IBM Sign in] [Register]

←Go to quick start

Search support

4.1

● Within my selected products

○ All support & downloads

Choose your products

Manage my product list

Your selected products

☑ Proventia Management SiteProtector System

☑ Proventia Network Intrusion Prevention System

☑ Proventia Network Security Controller

Enter a product name to add it to this product list:

Support overview

Support for my selected products

[Hide graphic]

IBM Support Portal:

A top ten support site for 2010

Awarded by the Association of Support Professionals

Award Winner 2010

The Year's Ten Best Web Support Sites

Featured links

- Proventia Management SiteProtector System
- Proventia Network Intrusion Prevention System
- Proventia Network Security Controller

Notifications

My Notifications

Proventia Management

Product news

News: Read the latest news on your product(s)

IBM acquired and sold products

- IBM sells U2 software assets to Rocket Software
- Lenovo ThinkPads and ThinkCentres
- Hitachi Global Storage Technologies

Sign in to add, move, or delete modules on your custom page.

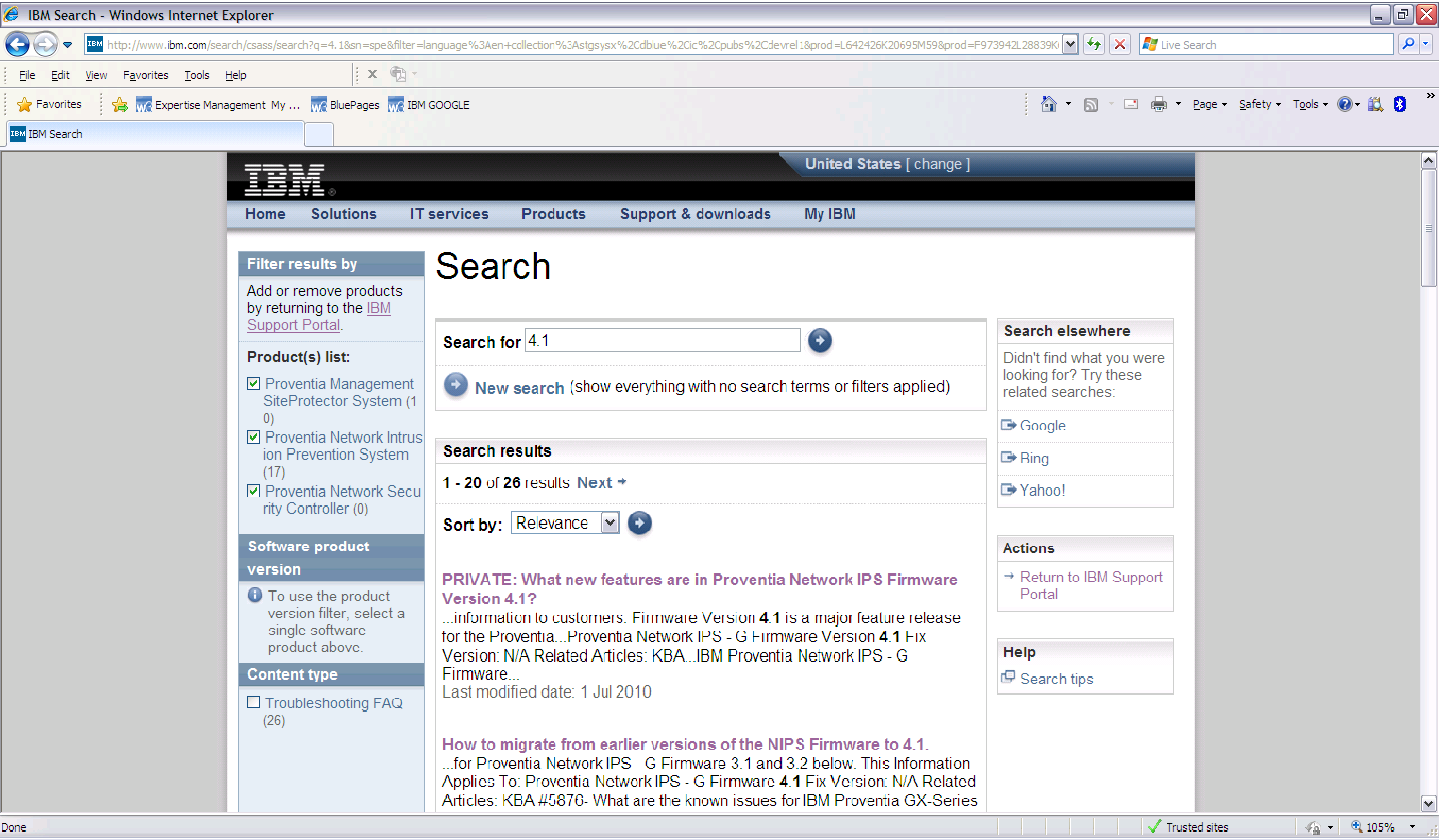
Support resources

- IBM Education Assistant
- Software Electronic Support brochure
- Software Subscription and Support
- Software Support Offerings
- Support phone numbers & contacts
- Support RSS feeds
- Support subscriptions
- Upgrades, accessories and parts
- Why renew your Software Support?

Product related links

Overview

Search results displayed



http://www.ibm.com/search/csass/search?q=4.1&sn=spe&filter=language%3Aen+collection%3Astgsysx%2Cdblue%2Cic%2Cpubs%2Cdevrel1&prod=L642426K20695M59&prod=F973942L28839K

United States [change]

Search

Filter results by

Add or remove products by returning to the IBM Support Portal.

Product(s) list:

- ☑ Proventia Management SiteProtector System (10)
- ☑ Proventia Network Intrusion Prevention System (17)
- ☑ Proventia Network Security Controller (0)

Software product version

To use the product version filter, select a single software product above.

Content type

- □ Troubleshooting FAQ (26)

Search for 4.1

New search (show everything with no search terms or filters applied)

Search results

1 - 20 of **26** results **Next**

Sort by: Relevance

PRIVATE: What new features are in Proventia Network IPS Firmware Version 4.1?
...information to customers. Firmware Version **4.1** is a major feature release for the Proventia...Proventia Network IPS - G Firmware Version **4.1** Fix Version: N/A Related Articles: KBA...IBM Proventia Network IPS - G Firmware...
Last modified date: 1 Jul 2010

How to migrate from earlier versions of the NIPS Firmware to 4.1.
...for Proventia Network IPS - G Firmware 3.1 and 3.2 below. This Information Applies To: Proventia Network IPS - G Firmware **4.1** Fix Version: N/A Related Articles: KBA #5876- What are the known issues for IBM Proventia GX-Series

Search elsewhere

Didn't find what you were looking for? Try these related searches:

- Google
- Bing
- Yahoo!

Actions

- Return to IBM Support Portal

Help

- Search tips

www.iss.net

Documentation

Knowledgebase

Training link

Thank You

IBM Security Solutions

Manage Risk. Reduce Costs. Enable Innovation.

Aytug Celikbas – *IT Security Specialist, CEE*
IBM Tivoli Internet Security Systems