

Service Description

Managed Protection Services for Networks

1. Scope of Services

IBM Managed Protection Services for Networks (called “MPS for Networks”) is designed to provide a comprehensive solution for network monitoring and a high level of security protection from external and internal threats.

MPS for Networks is designed to provide managed, inline protection of network segments using one of the IBM Proventia® G or Proventia MX appliances (called “Agents”). While Proventia G Agents operate as dedicated Intrusion Prevention Systems (“IPS”), the Proventia MX is an all-in-one appliance which includes a wide range of common security functions.

IBM offers MPS for Networks at the following alternative service levels:

- MPS for Networks – Select
- MPS for Networks – Premium

each described in further detail below.

The details of your order (e.g., the services you require (including service levels), contract period, and charges) will be specified in an Order form.

Definitions of service-specific terminology can be found at www.ibm.com/services/iss/wwcontracts

IBM will support the following product feature on both the Proventia G and Proventia MX appliances:

a. Intrusion Detection and Intrusion Prevention Systems (called “IDS/IPS”)

IDS/IPS is a security management system for computers and networks that is designed to gather and analyze information from various areas within a computer or a network and to help identify and block possible security breaches (i.e., intrusions (attacks from outside the organization) and misuse (attacks from within the organization)).

b. high availability

To help protect against hardware failure and provide high availability, two managed protection Agents may be configured and deployed; one fully operational and the other waiting as a backup to take over should the first Agent fail. Some Agents can also be deployed as clusters, such that both Agents operate and share network load.

IBM will support the following product features on only the Proventia MX appliance:

c. firewall

A firewall is a set of related programs, located at a network gateway server that is designed to allow or deny certain Hosts or networks to speak to each other, based on a set security policy. Many firewalls include a full set of networking features (e.g., routing capabilities and address and port rewriting).

d. VPNs

VPNs allow supported firewall-based VPNs to be connected to the managed Agent. IBM will configure the managed Agent to support site-to-site or client VPN tunnels.

e. antispam

Antispam technology is designed to minimize the volume of spam e-mail to user mail boxes. Spam filters utilize spam signatures, detection algorithms, and heuristic analysis to help reduce the volume of unwanted e-mail and remove objectionable content.

f. Web filtering

Web filtering helps the Customer to block objectionable content, mitigate Web-borne threats, and govern Web viewing behavior of personnel behind the managed Agent.

g. antivirus

Gateway antivirus systems scan many kinds of file transfers such as Web pages, e-mail traffic, and file transfer protocol (“FTP”) exchanges for worms, viruses, and other forms of malware.

MPS for Networks will provide the following services in support of the product features listed above:

- h. project kickoff, assessment, and implementation
During deployment of MPS for Networks, IBM will work with the Customer to help define appropriate security policies, assist with installation and configuration of the Agent(s), and verify proper device operation prior to transition of the Agent(s) to the SOC.
- i. policy management
Agents only protect Hosts when configured correctly for their network environment. IBM provides policy management services to help the Customer keep Agents configured with a valid security policy, and retain records of all changes.
- j. device management
IBM will monitor the Agent's system health and availability and periodically apply vendor updates to the Agent.
- k. security event monitoring
IDS/IPS Agents are capable of generating a high volume of alerts in response to the security conditions they are configured to detect. The actual security risk corresponding to a particular condition detected by an IDS/IPS Agent is not always clear, and it is not practical to block all data that may be harmful as the default. Additional monitoring and analysis provided by IBM security analysts on a 24 hours/day by 7 days/week basis helps cover this security gap by maintaining a focus on alerts which may be significant, validating these alerts as probable Security Incidents and escalating the probable Security Incidents to the Customer.
- l. vulnerability management
Vulnerabilities are weaknesses in Hosts in the Customer's environment, and IBM will provide vulnerability management services to help identify and remediate these vulnerabilities.
- m. IBM Internet Security Systems™ X-Force® Threat Analysis Service
IBM will provide security intelligence to the Customer based on such things as original research completed by the IBM X-Force® research and development team, worldwide threat activity as identified by the IBM Global Threat Operations Center, and secondary research from other public and private resources.
- n. Virtual-SOC
The Virtual-SOC is a Web interface which serves as the Customer's interface to management of the Agent, alerts, logs, reports, policy change requests, and other types of service tickets.

The following table provides an overview of MPS for Networks product features:

Table 1 - Product Features

Product Features	Select and Premium Levels
Supported bandwidth	Designed for 100 Mbps to multi-Gbps
Supported users	Designed for 500 and up
IDS/IPS	Support for help in blocking attacks in IBM Internet Security Systems™ X-Force® Certified Attack List and alerting of high-, medium-, and low-severity incidents
Firewall	Custom firewall policy
VPN	Support for site-to-site, client and SSL VPNs
Antispam	Filtering, tagging, and deletion of Web-based spam content
Web filtering	Web filtering with support for filter override, site blacklisting and source white listing
Antivirus	Virus protection; reports and notification through the Virtual-SOC

High availability	Support for active/active or active/passive Agents
-------------------	--

The following table provides an overview of MPS for Networks services provided in support of the product features listed above:

Table 2 – Services

Services	Select Level	Premium Level
Project kickoff, assessment, and implementation	Included	Included, with complimentary assessment of Customer's security practices
On-site Workshops	Not Included	Workshops to educate the Customer on incident response and coordinate a plan for Agent deployment
Penetration Test	Optional	Included with service for 15 managed Agents or more
Policy management	Performed by IBM only; unlimited policy change requests per month	Performed by IBM only; unlimited policy change requests per month; 2 emergency policy changes per month
Device management	24x7 device health and availability monitoring, and maintenance of Agent software and Security Content	
Security event monitoring	Active monitoring of security alerts 24x7	
Vulnerability management	Quarterly scan of 5 IP Addresses	Quarterly scan of 25 to 254 IP Addresses, depending on the number of Agents under management; semi-annual report with conference call
X-Force Threat Analysis Service	1 seat for the X-Force Threat Analysis Service (security intelligence service)	2 or 5 seats for the X-Force Threat Analysis Service, depending on the number of Agents under management
Virtual-SOC	Provides real-time access for communications	
Emergency Response Service	Optional	Included with service for 25 managed Agents or more

MPS for Networks – Select

MPS for Networks is a network-based service designed to help prevent unwanted and malicious traffic from entering or leaving the enforcement point, using a Proventia G or Proventia MX device. The service helps protect mission-critical network segments by inspecting and blocking harmful traffic using a variety of automated methods as well as monitoring by an IBM security analyst and escalation of identified incidents to the Customer.

2. IBM Responsibilities

2.1 Deployment and Initiation

During deployment, IBM will either work with the Customer to deploy a new Agent or begin management of an existing Agent. Only Proventia G and Proventia MX Agents can be managed as part of MPS for Networks – Select.

2.1.1 Project Kickoff

IBM will send the Customer a welcome e-mail and conduct a kickoff call to:

- introduce the Customer contacts to the assigned IBM deployment specialist;
- set expectations; and
- begin to assess the Customer requirements and environment.

IBM will provide a document called “Network Access Requirements”, detailing how IBM will connect remotely to the Customer’s network, and any specific technical requirements to enable such access. Typically, IBM will connect via standard access methods through the Internet; however, a site-to-site VPN may be used, if appropriate.

2.1.2 Assessment

Data Gathering

IBM will provide a form for the Customer to document detailed information for the initial setup of the Agent and associated service features. Most of the questions will be technical in nature and help determine the layout of the Customer network, Hosts on the network, and desired security policies. A portion of the requested data will reflect the Customer organization, and will include security contacts and escalation paths.

Environment Assessment

Using the provided information, IBM will work with the Customer to understand the existing Customer environment, and build a configuration and security policy for the Agent. If migrating from an existing Agent to a newer Agent, IBM will use the configuration and policy on the existing Agent. In each case, IBM may recommend policy adjustments in response to the most active worldwide threats (as determined by the IBM Global Threat Operations Center), and may tune the policy to reduce the number of erroneous alarms, if required.

During this assessment, IBM may make recommendations to adjust the policy of the Agent or the layout of the network to enhance security. IBM recommends that all Agents be deployed inline, at the network perimeter. If an Agent does not include firewall capabilities, or is implemented with firewall capabilities disabled, IBM recommends that the Agent be deployed behind a firewall. Placement outside the firewall may require policy tuning to eliminate high volumes of false alarms and may limit IBM’s ability to implement certain protection strategies.

If the Customer chooses to deploy the Agent in a passive mode, the protection provided by the Agent will be substantially decreased. Should the Customer choose to transition to an inline deployment at a later date, this transition will require advance notice due to the extra effort that will be required.

Existing Agent Assessment

If IBM will be taking over management of an existing Agent, IBM must assess the Agent to be sure it meets certain specifications. IBM may require the Agent software or Security Content to be upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts.

2.1.3 Implementation

Configuration at IBM

For Agents purchased through IBM at the time of deployment, much of the configuration and policy setting will take place at IBM facilities. For existing Agents already in use, the Customer will have the option to ship the Agent to IBM for configuration at IBM facilities.

Installation

While physical installation and cabling are a Customer responsibility, IBM will provide live support, via phone and e-mail, and will assist the Customer with location of vendor documents detailing the installation procedure for the firewall. Such support must be scheduled in advance to ensure availability of a deployment specialist.

At the Customer’s request, physical installation may be provided by IBM Professional Security Services (“PSS”) for an additional fee.

If the Customer chooses to deploy the client VPN functionality of the Proventia MX, IBM will support the deployment of client VPN software through an enablement model, as described in the section entitled “VPN Support”, subsection “Client VPNs”, below.

Remote Configuration

When taking over management of an existing Agent, IBM will typically perform the configuration remotely. The Customer may be required to physically load media.

All managed Agents will require some remote configuration, which may include the registration of the Agent with IBM Managed Security Services infrastructure.

2.1.4 Transition to SOC

Once the Agent is configured, physically installed and implemented, and connected to the IBM Managed Security Services infrastructure, IBM will provide the Customer with the option of having a demonstration of the Virtual-SOC capabilities and performance of common tasks.

The final step of services deployment is when the Security Operations Center (“SOC”) takes over management and support of the Agent and the relationship with the Customer. At this time, the ongoing management and support phase of the services officially begins. Typically, IBM will introduce the Customer via phone to the SOC personnel.

2.2 Ongoing Management and Support

The following services are supported for both the Proventia G and Proventia MX appliances unless otherwise indicated.

2.2.1 Policy Management

Changes

A single firewall policy/configuration change is defined as any authorized request for the addition or modification of one rule with five or fewer network or IP objects in a single request. Any change request requiring the addition of six or more network or IP objects, or the manipulation of two or more rules, will be counted as two or more requests. If the request applies to changes outside of the rule-based firewall policy, each submitted request will be considered a single change, within reasonable limits.

All policy and configuration changes will be completed by IBM. MPS for Networks – Select Customers may process unlimited changes to the firewall platform security policy/configuration per calendar month by submitting a policy change request through the Virtual-SOC. Additional policy changes can be provided for an additional fee. Following the closure of a calendar month, unused changes are considered void and may not be rolled over to the following month.

For Customer-requested Agent policy changes, IBM will target to:

- investigate policy change requests within two hours of receipt; and
- update the Agent policy configuration within four hours of request.

Policy change requests are subject to approval by IBM. Such approval will not be unreasonably withheld; however, among other reasons, a request will be denied if the policy change would result in a large number of false alarms.

Ongoing Policy Maintenance

IBM will work with the Customer to maintain protection strategies, including types of automatic blocking behavior in the case of Agents deployed inline.

On a quarterly basis, IBM will audit the Customer’s policy settings to verify accuracy.

One time per quarter (at the Customer’s request) IBM will work with the Customer to review all Agents under management and identify recommended changes to the network protection strategy.

Authentication Accounts

Specific firewall functionality often allows for authentication of user accounts to enable access through application proxies or for usage of specific protocols. IBM will support the enablement of such functionality; however, user account management is the responsibility of the Customer. The Customer may wish to integrate a third party authentication server with the firewall. Such a server will be managed by the Customer and provide additional options for user administration. IBM issues surrounding authentication of protocols and application proxies also extend to client and Secure Sockets Layer (“SSL”) VPN capabilities.

Notifications and Alerts

Certain Agents allow e-mails and/or SNMP traps to be generated and sent from the device when certain firewall-related events occur. By following the standard change request procedure, the Customer may request that IBM configure the Agent to deliver e-mails to a designated address, or generate SNMP traps.

Such a configuration is subject to approval by IBM, which will not be unreasonably withheld. However, among other reasons, a request will be denied if IBM believes the configuration will have an adverse impact on the ability of the platform to protect the network environment. As with other device configurations, changes to the platform notification and alerting settings will be considered a policy change request.

X-Force Certified Attack List

IBM will configure the Agent, based on a comprehensive predefined list of attacks, tailored to the Customer's network environment. Each Agent will be implemented with X-Force Certified Attack List activated. X-Force Certified Attack List is designed to help provide protection against identified high-risk attacks currently threatening organizations.

The X-Force Certified Attack List is maintained and updated quarterly on the Virtual-SOC. This list contains many types of attacks including backdoors, Trojans, and worms.

IBM will update the Agent configuration as IBM believes threats change. The Agent will be monitored 24 hours/day by 7 days/week.

2.2.2 Device Management

IBM will be the sole provider of software-level device management for the Agent. With root/super-user/administrator level access to the device, along with an out-of-band system and an Agent installed on the device, IBM will maintain system status awareness, apply operating system patches and upgrades, troubleshoot problems on the device, and work with the Customer to help ensure the device remains available. IBM will monitor for availability of the Agent, notify the Customer when certain utilization thresholds have been met, and monitor the device 24 hours/day by 7 days/week.

Regular, automatic updates will be provided for the software and firmware.

On-site assistance can be provided by IBM PSS for an additional fee.

Management Connectivity

All security logs, events and management data travel between the SOC and the managed Agent via the Internet. Typically, data traveling across the Internet is encrypted using industry-standard strong encryption algorithms. Requests for connectivity through alternate means (e.g., private data circuit and/or VPN) will be addressed on a case-by-case basis. Additional monthly fees may apply to accommodate connection requirements outside of the standard in-band connectivity.

Management Platforms

IBM will typically use the IBM SiteProtector™ management infrastructure to control Agent policy and configuration; to push updates to the Agent; and to receive data from the Agent using a SiteProtector event collector (called "Event Collector").

In some cases, the Customer may already use SiteProtector, and may elect to connect the Agent to the Event Collector on the Customer's premises. The Customer's Event Collector will then connect to the SiteProtector infrastructure at IBM. This configuration is commonly known as "stacking". Any Customer choosing to use a stacked SiteProtector configuration will be subject to additional responsibilities. Use of this configuration is subject to approval by IBM.

Log Storage

X-Force® Protection System serves as a data warehouse for event data from a variety of security devices, applications, and platforms. Following display on the Virtual-SOC, logs are migrated to a physical backup media such as tape or DVD. Backup media is archived in an environmentally controlled facility. Archived data will be available for a user-defined time period not to exceed seven years from the date of log creation.

At the Customer's request, IBM will submit a request for media location and retrieval. Hourly consulting fees will apply for all time spent restoring and preparing data in the Customer's requested format.

Health and Availability Monitoring

The health and performance of MPS for Networks – Select is monitored by using a Host-based monitoring Agent (when possible) or SNMP. The Agents are regularly polled by the SOC, keeping IBM security analysts informed of some potential problems as they develop. Key metrics analyzed by the monitoring Agent include:

- hard disk capacity (if applicable);

- CPU utilization;
- memory utilization; and
- process availability.

In addition to system health metrics, IBM will monitor Agent uptime and availability. If IBM detects that contact with a managed Agent has been lost, additional time-based checks will be initiated to verify a valid outage has been identified.

In the event system health problems or an outage has been confirmed, a trouble ticket will be created and an IBM security analyst will be notified to begin research and investigation. The status of all system health tickets is available through the Virtual-SOC.

Outage Notification

If the Agent is not reachable through standard in-band means, the Customer will be notified via telephone using an escalation procedure to be established with the customer. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed Agent.

Application/Operating System Updates

Periodically, it will be necessary for IBM to install patches and software updates to improve Agent performance, enable additional functionality, and resolve potential application problems. The application of such patches and updates may require platform downtime or Customer assistance to complete. If required, IBM will declare a maintenance window in advance of any such updates, and the notification will state the known impacts of the scheduled maintenance and any Customer-specific requirements.

Security Content Updates

To help identify the most current threats, IBM will periodically update security platforms with the most current Security Content. Security Content, delivered in the form of new checks or signatures for the IPS, antispam and antivirus modules, and new URL listings for the Web filtering module, enhances the Agent's security capabilities.

At the discretion of IBM, Security Content updates may be downloaded and installed onto the security platform at any time. This process is intended to be transparent to users.

Device Troubleshooting

If the Agent does not perform as expected, or is identified as the potential source of a network-related problem, IBM will examine the device configuration and functionality for potential issues. Troubleshooting may consist of an offline analysis by IBM, or an active troubleshooting session between IBM and the Customer. IBM will attempt to resolve any technical issues as expeditiously as feasible. If the Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

Out-of-Band Access

Out-of-band ("OOB") access is a required feature that assists the SOC in the diagnosis of potential device issues. Implementing OOB requires the Customer to purchase an IBM-supported OOB device and provide a dedicated analog phone line for connectivity.

If the Customer has an existing OOB solution, IBM will use this solution for OOB access to managed devices, provided:

- the solution does not allow IBM access to any non-managed devices;
- using the solution does not require installation of any specialized software;
- the Customer provides detailed instructions for accessing IBM-managed Agents; and
- the Customer is responsible for all aspects of managing the OOB solution.

2.2.3 Security Event Monitoring

IBM will augment the automated analysis capabilities of the X-Force Protection System infrastructure with live monitoring 24 hours/day by 7 days/week. In the event malicious activity is detected, IBM will review relevant alerts, and if necessary, generate a Security Incident ticket on the Virtual-SOC. Actionable, validated Security Incidents will be escalated to the Customer via e-mail, e-mail-based SMS notification, or telephone, depending on declared event severity, as described in the section entitled "SLA Remedies" below.

The Customer will be provided with a description of the Security Incident, the potential impact, and a recommended course of action. An e-mail containing the details of the Security Incident will be sent to the designated Customer contact.

Identified attacks covered by the Agent's policy will be reported through the Virtual-SOC, including comprehensive data. If the Agent is deployed inline with IPS functionality, many of these attacks will have been blocked, and require no further action. As malicious activity occurs 24 hours/day by 7 days/week and blocked traffic is a regular occurrence, no escalations will follow the successful inbound block of unwanted traffic.

In the case of a confirmed breach of security, IBM emergency response services are available for an additional fee. Such emergency response services may include assessments of damage, building of plans for remediation, and/or forensic examination of compromised Hosts.

2.2.4 Vulnerability Management Service

The vulnerability management service is a remotely delivered, electronic service that regularly and automatically scans the Customer's in-scope Internet perimeter devices for known vulnerabilities. Each scan results in several comprehensive reports that are designed to identify potential weaknesses, assess relative network risk, and provide recommendations to manage identified vulnerabilities. IBM will require the Customer to validate they are the owner of all IP addresses to be scanned, prior to the initial scan of such IP addresses being performed. For each Agent purchased, the Customer will receive quarterly remote vulnerability assessment scanning for up to five IP addresses.

Features of the vulnerability management service include:

- a. External vulnerability management - IBM will provide external vulnerability management for each Agent under full management, and four additional Hosts. This includes one quarterly scan of the Hosts' Internet accessible IP addresses, for the duration of the contract.
- b. Vulnerability discovery - IBM scanners are designed to detect a large set of vulnerabilities on a wide variety of Hosts.
- c. Prioritization - IBM catalogs each scanned device (asset) and allows Customers to assign business criticality ratings and system owners to specific assets. This allows IBM to notify asset owners when vulnerabilities are identified, and facilitates establishment of a personalized view into overall program impacts on security posture.
- d. Remediation - identified vulnerabilities can be assigned to designated asset owners for review and remediation. The individual asset owners are provided with access to use the Virtual-SOC as a tool for learning about a specific vulnerability, and tracking its remediation within the enterprise.
- e. Dynamic protection - vulnerability management capabilities can integrate with a Customer's existing IBM Managed Security Services to dynamically request the update of server and network IPS policies with appropriate blocking responses.
- f. Verification – after an asset owner indicates a vulnerable application or system has been effectively patched, the assignment is designed to remain active until the scanning system verifies known attack vectors for a given vulnerability have been successfully eliminated.
- g. Customized reporting - IBM provides reports of service performance and security posture, either in a stand-alone presentation, or combined with data from multiple IBM Managed Security Services.

2.2.5 X-Force Threat Analysis Service

X-Force Threat Analysis Service provides proactive security management through the evaluation of known global online threat conditions and detailed analyses.

The service provides threat information collected from the SOC's, and trusted security intelligence from the X-Force team. This combination helps to identify the nature and severity of external Internet threats.

For each Agent purchased, the Customer will receive the X-Force Threat Analysis Service for the duration of the contract.

2.2.6 Virtual-SOC

The Virtual-SOC is a Web-based interface designed to enable delivery of key service details and on-demand protection solutions. The Virtual-SOC is designed to deliver a consolidated view of the Customer's overall security posture. The portal is capable of merging data from multiple geographies or technologies into a common interface, allowing for broad analysis, alerting, remediation, and reporting.

The Virtual-SOC is designed to provide real-time access for communications including ticket creation, event handling, incident response, data presentation, report generation, and trend analysis.

Reporting

The Customer will have access to service information, through the Virtual-SOC, to review service tickets and Security Incidents at any time. One time per month, IBM will produce a summary report that includes:

- a. number of SLAs invoked and met;
- b. number and type of service requests;
- c. list and summary of service tickets;
- d. number of Security Incidents detected, priority and status; and
- e. list and summary of Security Incidents.

2.2.7 VPN Support (Proventia MX only)

The VPN feature allows supported server-based or client-based VPNs to be connected to the Agent and helps to better secure transmission of data across untrusted networks, via site-to-site communication. The default configuration of this feature is designed to activate this capability on the managed Agent and includes the initial configuration of up to two remote sites. After the initial configuration, each setup of a site-to-site VPN is considered a policy change.

IBM will support static authentication methods for both site-to-site and client VPN configurations. Static authentication also includes the use of the Customer's existing radius authentication server implementation. Certificate-based authentication is not currently supported as a part of the VPN service configuration

Site-to-Site VPNs

A site-to-site VPN is defined as a VPN created between the Agent and another supported encryption device. Site-to-site VPNs provide help to establish connectivity for entire networks by building a tunnel between the managed firewall platform and another compatible VPN endpoint. Site-to-site VPNs can be established between:

- two IBM-managed VPN-capable Agents, or
- an IBM-managed endpoint and a non-IBM-managed endpoint. A one-time fee will be charged for the initial configuration of a managed to unmanaged endpoint.

In the event problems with the VPN tunnel arise after setup, IBM will work with the Customer and vendor contacts to help identify, diagnose, and resolve performance and IBM-related issues.

Client VPNs

Client VPNs help to better secure connectivity into a protected network, from a single workstation with the appropriate client VPN software and access credentials. Client VPNs help to enable remote workers to access internal network resources without the risk of eavesdropping or data compromise.

IBM supports client VPN implementations through an enablement model. IBM will work with the Customer to configure and test the first five client VPN users. Following successful connectivity for these five users, it will be the Customer's responsibility to perform user administration for individuals requiring a client VPN connection. IBM will provide the Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and help to provide the appropriate access levels and software required to complete the setup.

Client VPN solutions typically require the installation of a client VPN application onto the specific workstations participating in the secured tunnel. The deployed Agent is designed to determine the specific client VPN applications to be supported by MPS for Networks – Select. Some client VPN applications may be available through their respective vendors at no additional cost, while others are licensed per seat. The Customer is solely responsible for the acquisition, installation, and associated costs therein of any required client VPN software.

SSL VPNs

SSL VPNs help to offer connectivity into company resources from any Web-enabled personal computer ("PC"), without the need for a dedicated client VPN application. This allows remote workers to access company resources from an Internet-connected PC. In contrast to traditional Internet Protocol Security ("IPsec") VPNs, SSL VPNs do not require installation of specialized client software on users' computers.

IBM supports SSL VPN implementations through an enablement model. IBM will work with the Customer to configure and test the first five SSL VPN users. Following successful connectivity for these five users, it will be the Customer's responsibility to perform user administration for individuals requiring an SSL VPN connection. IBM will provide the Customer with a demonstration of the user management capabilities of the deployed firewall platform (if applicable), and provide the appropriate access levels and software required to complete the setup.

2.2.8 Antispam (Proventia MX only)

The integrated antispam capabilities of many Agents check inbound and outbound e-mail messages for known spam signatures, patterns, and behaviors. The Agent must be placed in a location where e-mail passes through the device prior to reaching the mail gateway. This helps prevent undesirable messages from impacting the performance and availability of the mail gateway. While antispam technology is designed to eliminate unsolicited advertisements, most antispam technology is also designed to filter phishing attempts (i.e., e-mails designed to fool users into releasing their private data). Typically, phishing e-mails claim to be from a legitimate service, but refer the user to a malicious Web site which collects the user's personal data.

The antispam policy can typically be configured to white list or blacklist specific e-mail addresses and domains, as desired. Such configurations are designed to allow for e-mail messages from these e-mail addresses and domains to always be passed or always be deleted by the antispam module, respectively. IBM will work directly with the Customer to collect data required for IBM to construct customized white and blacklists tailored to the specific needs of the Customer.

Enabling antispam functionality may require additional licensing from the Agent's vendor, which shall be the sole responsibility of the Customer.

2.2.9 Web Filtering (Proventia MX only)

Web filtering is designed to address potential objectionable Internet content. Using content analysis technology, the managed Agent can provide policy-based content control.

Enabling Web filtering may require additional licensing for the Agent which shall be the sole responsibility of the Customer.

Configuration

In order for Web filtering to function, the Agent must be placed in a location where user Web traffic passes through the device(s) prior to reaching the intended destination. This allows the Web filtering module to compare the requested URL against the content database to validate the requested destination is authorized.

During the initial setup and deployment process, IBM will work with the Customer to create a policy that is customized to the organization's specific needs.

2.2.10 Antivirus (Proventia MX only)

Antivirus support is designed to reduce the risk of malicious code within the network data stream.

Antivirus gateways can be configured to scan Web, e-mail, and file-transfer traffic, and are designed to block the transmission of files which contain any of a number of designated threats. Most antivirus scanners will also block common forms of spyware, as well as many types of network worms.

Enabling antivirus functionality may require additional licensing for the Agent, which shall be the sole responsibility of the Customer.

Configuration

In order for antivirus implementations to be effective, the Agent must be placed in a location where user and inbound traffic passes through the device(s) prior to reaching its intended destination. This allows the Agent to compare monitored traffic against known virus signatures and/or behavior.

During the initial setup and deployment process, IBM will work with the Customer to create a policy that is customized to the organization's specific needs.

2.2.11 High Availability

High availability ("HA") increases the reliability of MPS for Networks - Select by supporting the implementation of redundant Agents into your managed environment. Adding HA to MPS for Networks - Select may require changes to the Agent, software licensing, IP addressing requirements, or managed services fees. MPS for Networks - Select does not support non-integrated, third party HA solutions.

Active/Passive Implementations

Active/passive implementations improve reliability of the Agent gateway solution through redundancy. In this configuration, a second Agent is configured as a hot-standby, ready to begin serving the network if the primary Agent experiences a critical hardware or software failure. In such a scenario, failover is designed to be automatic and nearly instantaneous. Active/passive configurations are recommended for mission critical environments with low to medium traffic loads.

Active/Active Implementations

Active/active clusters improve reliability and performance of the managed Agents by using both Agents to handle the network traffic simultaneously. In this configuration, each Agent handles a share of the network packets, determined by a load-balancing algorithm. If one Agent fails, the other Agent is designed to automatically handle all of the traffic until the failed Agent has been restored. Active/active configurations are recommended for mission critical environments with high traffic volumes and/or large fluctuations in network utilization.

3. Customer Responsibilities

While IBM will work with the Customer to deploy and implement the Agent, and IBM will manage the Agent, the Customer will be required to work with IBM in good faith and assist IBM in certain situations as requested by IBM.

3.1 Deployment and Initiation

During deployment, the Customer will work with IBM to deploy a new Agent or begin management of an existing Agent, as applicable.

The Customer will participate in a scheduled kickoff call to introduce team members, set expectations and begin the assessment process.

The Customer will be required to complete a form to provide detailed information about the network configuration (including applications and services for the Hosts on the protected network) and must work with IBM in good faith to accurately assess the Customer's network and environment. The Customer must provide contacts within the organization, and specify an escalation path through the organization in the event that IBM must contact the Customer.

The Customer must ensure that any existing Agent meets IBM specifications, and must work to meet recommendations concerning the Customer's network and network access requirements, if changes are required to ensure workable protection strategies.

If IBM will be taking over management of an existing Agent, IBM may require the Agent software or Security Content to be upgraded to the most current versions in order to provide the service. Other required criteria may include the addition or removal of applications and user accounts. Such upgrades, additions, or removals will be the sole responsibility of the Customer.

While IBM will provide support and guidance, the Customer is responsible for the physical installation and cabling of all Agents, unless such services are provided as an IBM PSS consulting project. If the Customer chooses to deploy the client VPN functionality of the Proventia MX appliance, the Customer is responsible for the actual installation and some testing of the client VPN software, with IBM support. The Customer is responsible for procuring any client VPN software directly from a vendor, although IBM may make recommendations and guide the Customer to an appropriate vendor contact.

3.2 Ongoing Management and Support

3.2.1 Policy Management

The Customer acknowledges that IBM is the sole party responsible for and possessing authority to change the Agent's policy and/or configuration.

3.2.2 Device Management

If the Customer wishes to enable the HA feature of MPS for Networks – Select, the Customer agrees to purchase a second Agent and pay for the ongoing management of such Agent.

The Customer is responsible for maintaining current hardware and software maintenance contracts.

Physical Environment

The Customer must provide a secure, physically controlled environment for the Agent.

Customers must provide an OOB solution, and ensure the OOB device is connected to the Agent and is functional at all times.

On an annual basis, the Customer agrees to work with IBM to review the current hardware configuration of the managed devices and identify required updates. These updates will be based on identified changes to the operating system and application requirements.

Network Environment

The Customer is responsible for making agreed-to changes to the network environment based upon IBM recommendations.

The Customer is required to maintain an active and fully functional Internet connection at all times, and must ensure the Agent is Internet-accessible via a dedicated, static IP address.

The Customer is responsible for ensuring the desired network traffic and applicable segments are configured to route network traffic through the Agent.

Management Platforms

Customers hosting their own SiteProtector infrastructure:

- a. must set up an event stream to IBM, via the Internet;
- b. must ensure their Event Collectors have unique, routable IP addresses to forward events to IBM;
- c. must have an Event Collector dedicated to the devices IBM will be monitoring on behalf of the Customer. Such Event Collector may not receive events from devices for which the Customer has not contracted for management or monitoring;
- d. must provide IBM with full administrative access to the SiteProtector application server, via the SiteProtector console, for the purpose of pushing updates and controlling policy;
- e. may be required to upgrade their SiteProtector infrastructure in order to transfer data to the IBM Managed Security Services infrastructure; and
- f. must not alter the Agent's policy or configuration outside of the established policy change request procedure.

3.2.3 VPN Support

For VPN connections to sites that are not being managed by IBM, the Customer must provide a completed "VPN Site Configuration" form. The VPN will be configured in accordance with the information provided. Troubleshooting of remote site connectivity is strictly limited to IBM managed sites.

Managed Protection Services for Networks - Premium

Managed Protection Services for Networks – Premium helps to protect the most valuable, mission-critical networked assets, and help the Customer meet the most stringent security requirements. Managed Protection Services for Networks – Premium requires a minimum purchase of service for ten (10) Agents.

The service will provide the same function as Managed Protection Services for Networks – Select and will include additional or expanded features as set forth below.

In connection with the above, IBM will perform the responsibilities as set forth in the section entitled "Managed Protection Services for Networks – Select", subsection "IBM Responsibilities" above. In addition, IBM will perform the responsibilities set forth in the section entitled "Managed Protection Services for Networks – Premium", subsection "IBM Responsibilities" below.

You agree to perform all of the tasks set forth in the section entitled "Managed Protection Services for Networks – Select", subsection "Customer Responsibilities" above. In addition, you agree to perform the responsibilities set forth in the section entitled "Managed Protection Services for Networks – Premium", subsection "Customer Responsibilities" below.

4. IBM Responsibilities

4.1 Deployment and Initiation

4.1.1 Managed Protection Services Assessment

IBM will provide a one-time base-lining Managed Protection Services assessment to evaluate the overall effectiveness of the Customer's security management program. Such assessment will be based on the ISO-17799 Code of Practice for information security and include technical security testing of the Customer's environment from an external perspective. IBM will work with the Customer to review the

assessment findings and compile the results into a report for Customer's relevant management. IBM will work with the Customer to create a prioritized action plan to achieve the desired security state.

4.1.2 Managed Protection Services On-site Workshop

Deployment

IBM will facilitate a workshop to assist the Customer in planning for deployment of MPS for Networks - Premium. The workshop will include approximately 12 hours of up-front information gathering and planning, followed by a one to two day on-site meeting with the Customer.

Incident Response

A second workshop will be conducted at the Customer's site to provide education on the IBM Security Incident escalation process, and the role of the SOC. The team will develop a plan to handle Security Incidents. This workshop will involve a majority of the Customer's named security contacts, and will serve to develop a decision tree in the event of a Security Incident.

During this workshop, if the Customer qualifies for the Emergency Response Service (described below), IBM will provide education on the Emergency Response Service.

4.2 Ongoing Management and Support

4.2.1 Policy Management

IBM will provide up to two emergency policy change implementations per month.

4.2.2 Vulnerability Management Service

Scans can be scheduled to occur on a weekly, monthly or quarterly basis, with the option of performing periodic on-demand scans. IBM will provide vulnerability management services for a limited number of IP addresses, commensurate with the number of Agents for which services are purchased, as follows:

- for 10 to 14 Agents, IBM will provide external vulnerability management for up to 25 IP addresses.
- for 15 to 24 Agents, IBM will provide external vulnerability management for up to 50 IP addresses.
- for 25 to 29 Agents, IBM will provide external vulnerability management for up to 100 IP addresses.
- for 30 Agents or more, IBM will provide external vulnerability management for up to 254 IP addresses.

Semi-annually, IBM will spend up to eight hours processing vulnerability data into a report that highlights changes in security profile, and documents significant security exposures in the Customer's network. IBM will review this report with the Customer in a conference call lasting approximately two hours.

4.2.3 X-Force Threat Analysis Service

IBM will provide two seats for the X-Force Threat Analysis Service to Customers who purchase services for up to 29 Agents. For 30 Agents or more, IBM will provide five seats for the X-Force Threat Analysis Service.

4.2.4 Penetration Testing

For Customers who purchase services for at least 15 Agents, IBM will perform a penetration test designed to determine the Customer's current vulnerabilities and demonstrating how attackers can significantly impact an organization's business. The penetration test utilizes IBM security experts, best-of-breed tools, X-Force research, and extensive field experience to simulate a network attack in a controlled manner. This provides a snapshot of an organization's security condition as seen from a designated, remote Internet location. Specific, exploitable vulnerabilities and risks will be identified and documented. The IBM security experts will analyze the documented vulnerabilities to provide a picture of the Customer's security posture.

4.2.5 Emergency Response Service

For Customers who purchase services for 25 Agents or more, IBM will provide Basic Emergency Response Service. As part of the service, IBM will work with the Customer to develop a Security Incident response plan designed to help prepare the Customer for, and help the Customer minimize the effects of, the Security Incident. The service combines X-Force research with IBM's Security Incident response experience to help stop attacks in progress and minimize their impact. In the case of an agreed security breach, IBM will perform a forensics examination and provide remediation guidance to help protect against future attacks.

4.3 Customer Responsibilities

5. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for Security Incidents resulting from MPS for Networks – Select or Premium. The SLAs become effective when the deployment process has been completed, the device has been set to “live”, and support and management of the device have been successfully transitioned to the SOC.

The SLA remedies are available provided the Customer meets its obligations as defined in this Service Description.

5.1 SLA Guarantees

The SLA guarantees described below comprise the measured metrics for delivery of MPS for Networks – Select or Premium. Unless explicitly stated below, no additional guarantees or warranties of any kind shall apply to services delivered under MPS for Networks – Select or Premium. The sole remedies for failure to meet the SLA guarantees are specified in the section entitled “SLA Remedies”, below.

- a. Security Incident prevention guarantee – all X-Force Certified Attack List Security Incidents will be successfully stopped on the Customer network segments that are protected and monitored by an Agent.
- b. Security Incident identification guarantee (Proventia G only) – IBM will identify all Priority 1, 2, and 3 level Security Incidents based on Agent event data received by the SOC. IBM will determine if an event is a Security Incident based on the Customer’s business requirements, network configuration, and Agent configuration.
- c. Security Incident response guarantee (Proventia G only) – IBM will respond to all identified Security Incidents within 15 minutes. The Customer’s designated Security Incident contact will be notified by telephone for Priority 1 Security Incidents and via e-mail for Priority 2 and 3 Security Incidents. During a Priority 1 Security Incident escalation, IBM will continue attempting to contact the designated Customer contact until such contact is reached or all escalation contacts have been exhausted.

Operational activities related to Security Incidents and responses are documented and time-stamped within the IBM trouble ticketing system, which shall be used as the sole authoritative information source for purposes of this SLA guarantee.

- d. Intrusion event countermeasures guarantee (Proventia G only) – IBM will recommend or implement a countermeasure within 30 minutes of Customer approval (on a per incident basis) for all Priority 1 Security Incidents. The countermeasure will be implemented (if applicable) on any managed device where such an action would be relevant, should that device provide the appropriate technical means to do so. Countermeasures for non-managed devices will be recommended to the designated Customer contact within 30 minutes of incident escalation.
- e. Policy change request acknowledgement guarantee – IBM will acknowledge receipt of the Customer’s policy change request within two hours of receipt by IBM. This guarantee is only available for policy change requests submitted by a valid security contact in accordance with the provided procedures.
- f. Policy change request implementation guarantee – the Customer policy change requests will be implemented within four hours of receipt by IBM unless the request has been placed in a “hold” status due to insufficient information required to implement the submitted policy change request. This guarantee is only available for policy change requests submitted by a valid security contact in accordance with established procedures.
- g. Proactive system monitoring guarantee – the Customer will be notified within 15 minutes after IBM determines the Customer’s Agent is unreachable via standard in-band connectivity. During an outage escalation, IBM will continue attempting to contact the designated Customer contacts (in the advised priority order) until a designated contact is reached or until all contacts have been exhausted.
- h. Proactive Security Content update guarantee – IBM will begin application of all new Security Content updates to the Customer’s managed security platform within 48 hours from the time the Security Content update was published for general availability by the vendor.

5.2 SLA Remedies

As the sole remedy for failure to meet any of the guarantees described in the section entitled “SLA Guarantees”, IBM will credit the Customer’s account if IBM fails to meet the SLA guarantees described in the section entitled “SLA Guarantees” during a given calendar month. For all SLAs other than the Security Incident prevention guarantee under MPS for Networks – Premium, the Customer may obtain no more than one credit for each SLA per day, not to exceed a total for all SLAs of \$25,000 (U.S.), or the equivalent in local currency, in a given calendar month, as stated in the section entitled “SLA Exclusions and Stipulations” below. Specific SLA recoveries are listed below:

- a. Security Incident prevention remedy (MPS for Networks – Select) – if the Security Incident prevention guarantee is not met for any given calendar month, the Customer account will be credited for the applicable charges for one month’s fees for MPS for Networks – Select for the initial Security Incident that was not prevented.
- b. Security Incident prevention remedy (MPS for Networks – Premium) – if the Security Incident prevention guarantee is not met for any given calendar month, the Customer account will be credited \$50,000 (U.S.), or the equivalent in local currency, not to exceed one occurrence per month, as stated in the section entitled “SLA Exclusions and Stipulations” below. Such payment will be the sole and exclusive remedy for all security breaches that may result from said occurrence.
- c. Security Incident identification and Security Incident response remedies – if either guarantee is not met for any given calendar month, the Customer account will be credited the pro-rated charges as specified below:
 - (1) Priority 1 Incidents: Failure to identify the security event(s) as a Security Incident will result in a one month credit for the initial device that reported the event(s).
 - (2) Priority 2 Incidents: Failure to identify the security event(s) as a Security Incident will result in a one week credit for the initial device that reported the event(s).
 - (3) Priority 3 Incidents: Failure to identify the security event(s) as a Security Incident will result in a one day credit for the initial device that reported the event(s).
- d. Intrusion event countermeasures remedy – if IBM fails to meet this guarantee for any given calendar month, the Customer account will be credited the applicable charges for one month of the monthly monitoring fee for the affected device and, if applicable, the specific managed security platform for which the respective guarantee was not met.
- e. Policy change request acknowledgement, policy change request implementation, proactive system monitoring and proactive Security Content update remedies – If IBM fails to meet any of these guarantees, the Customer account will be credited the applicable charges for one day of the monthly monitoring fee for the affected device and, if applicable, the specific managed security platform for which the respective guarantee was not met.

Table 3 - Summary of Service Level Agreements and Remedies

Service Level Agreements	Remedies for MPS for Networks – Select	Remedies for MPS for Networks – Premium
Security Incident prevention guarantee	Credit of 1 month fee for MPS for Networks – Select	\$50,000 (U.S.) – or the equivalent in local currency
Security Incident identification guarantee	<ul style="list-style-type: none"> ● Priority 1: Credit of 1 month of the monthly monitoring fee ● Priority 2: Credit of 1 week of the monthly monitoring fee for the affected device ● Priority 3: Credit of 1 day of the monthly monitoring fee for the affected device 	Credit of 1 day of the monthly monitoring fee of the affected device
Security Incident response guarantee		Credit of 1 day of the monthly monitoring fee of the affected device
Intrusion event countermeasure guarantee	Credit of 1 month of the monthly monitoring fee for the affected device	
Policy change request		

acknowledgement guarantee	Credit of 1 day of the monthly monitoring fee for the affected device
Policy change request implementation guarantee	
Proactive system monitoring guarantee	
Proactive Security Content update guarantee	

5.3 Scheduled and Emergency Portal Maintenance

Scheduled maintenance means any maintenance:

- a. of which the Customer is notified at least five days in advance; or
- b. that is performed during the standard monthly maintenance window on the second Saturday of every month from 8:00 a.m. – 4:00 p.m. United States Eastern Time. Notice of scheduled maintenance will be provided to the designated Customer contact.

No statement in the section entitled “Service Level Agreements” shall prevent IBM from conducting emergency maintenance on an “as needed” basis. During such emergency maintenance, the affected Customer’s primary point of contact will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of any emergency maintenance.

5.4 SLA Exclusions and Stipulations

5.4.1 Simulation Mode SLA Modification

The Proventia G series, firmware versions 1.2 and above, provides the Customer with the opportunity to run in simulation mode allowing the Customer to view virtual blocking and prevent attacks. When a device is in simulation mode, the Customer may view a complete list of simulated prevented attacks specific to their network, via the Virtual-SOC.

Customers may enable and disable simulation mode at any time by one of the following methods:

- a. Pre-deployment Customer - Customer must provide a written or e-mail policy change request to the assigned IBM deployment specialist.
- b. Post-deployment Customer – Customer must submit requests to begin or end simulation mode via a service ticket or policy change request within the Virtual-SOC.

During simulation mode, all active blocking functionality will be disabled, thereby preventing active blocking by the device, and IBM will cease to provide the Customer with the Security Incident prevention guarantee as described in the section entitled “SLA Guarantees” of this Service Description. All other protection guarantees and remedies shall remain in effect, with the following as the sole remedies which will be available for failure to meet the applicable guarantee, provided that as stated above no remedy shall be available for the Security Incident prevention guarantee.

Table 4 - Summary of Service Level Agreements and Remedies during Simulation Mode

Service Level Agreements	Remedies for MPS for Networks – Select	Remedies for MPS for Networks – Premium
Security Incident identification guarantee	<ul style="list-style-type: none"> ● Priority 1: Credit of 1 month of the monthly monitoring fee ● Priority 2: Credit of 1 week of the monthly monitoring fee for the affected device ● Priority 3: Credit of 1 day of the monthly monitoring fee for the affected device 	Credit of 1 day of the monthly monitoring fee of the affected device
Security Incident response guarantee		Credit of 1 day of the monthly monitoring fee of the affected device
Intrusion event countermeasure guarantee	Credit of 1 month of the monthly monitoring fee for the affected device	Credit of 1 month of the monthly monitoring fee of the affected device
Policy change request acknowledgement guarantee	Credit of 1 day of the monthly monitoring fee for the affected device	
Policy change request implementation guarantee		
Proactive system monitoring		

guarantee	
Proactive Security Content update guarantee	

5.4.2 Customer Contact Information

Multiple SLAs require IBM to provide notification to the designated Customer contact after certain events occur. In the case of such an event, the Customer is solely responsible for providing IBM with accurate and current contact information for the designated contact(s). The current contact information on record is available to authorized contacts through the Virtual-SOC. IBM will be relieved of its obligations under these SLAs if IBM contact information is out of date or inaccurate due to Customer action or omission.

5.4.3 Customer Network/Server Change Notifications

The Customer is responsible for providing IBM advance notice regarding any network or server changes to the Agent environment. If the event advance notice cannot be provided, the Customer is required to provide IBM with notification of changes within seven calendar days of said network or server changes. Notification is completed by the submission or update of a critical server ticket through the Virtual-SOC. If the Customer fails to notify IBM as stated above, all SLA remedies are considered null and void.

5.4.4 Maximum Remedies Payable to Customer

The total SLA remedies provided by MPS for Networks – Select or Premium described in the sections entitled “SLA Guarantees” and “SLA Remedies” above, will not exceed a total of \$25,000 (U.S.), or the equivalent in local currency, in one calendar month, with the exception of the Security Incident prevention guarantee for MPS for Networks – Premium, which will not be paid more than once per month.

5.4.5 Network Traffic Applicable to SLAs

Certain SLAs focus on the prevention, identification and escalation of Security Incidents. These SLAs assume that traffic has successfully reached the Agent and therefore the Agent has the ability to process the traffic against the installed policy and generate a logged event. Traffic that does not logically or electronically pass through an Agent, or that does not generate a logged event, is not covered under these SLAs.

5.4.6 SLA Compliance and Reporting

SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, Agents, and properly configured servers. If SLA compliance failure is caused by CPE hardware or software (including any and all Agents), all SLA remedies are considered null and void. IBM will provide SLA compliance reporting through the Virtual-SOC.

5.4.7 Testing of Monitoring and Response Capabilities

The Customer may test IBM monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. These activities may be initiated directly by the Customer or by a contracted third party with no advance notice to IBM. SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated guarantee(s) are not met.

6. Service Level Objectives

IBM SLOs establish nonbinding objectives for the provision of certain features of MPS for Networks – Select. The SLOs become effective when the deployment process has been completed, the device has been set to “live”, and support and management of the device have been successfully transitioned to the SOC. IBM reserves the right to modify these SLOs with 30 days prior written notice.

- a. Virtual-SOC – IBM will provide a 99.9% accessibility objective for the Virtual-SOC outside of the times detailed in the section entitled “Scheduled and Emergency Portal Maintenance”.
- b. Internet Emergency – In the event IBM declares an Internet emergency, it is IBM’s objective to notify the Customer’s specified points of contact via e-mail within 15 minutes of emergency declaration. This notification will include an incident tracking number, telephone bridge number, and the time that IBM will conduct a situation briefing

During declared Internet emergencies, IBM will provide a live telephone-conference situation briefing and summarized e-mail designed to provide information that the Customer can use to protect their organization. Situation briefings following the onset of an Internet emergency will supersede any requirement for IBM to provide Customer-specific escalations for events directly

related to the declared Internet emergency. IBM will communicate all other priority level incidents, during an Internet emergency, via automated systems such as e-mail, pager and voice mail.

Standard escalation practices will resume upon conclusion of the stated Internet emergency.

Termination of an emergency state is marked by a decrease in the AlertCon level to AlertCon 2, or an e-mail notification delivered to an authorized Customer security contact.

7. Other Terms and Conditions

IBM reserves the right to modify the terms of this Service Description, including the SLAs, with 30 days prior written notice.