1. **Scope of Services**

IBM Managed Security Services for Network Firewalls (called “MSS for Network Firewalls”) provides the Customer with comprehensive access controls and connectivity.

IBM offers MSS for Network Firewalls at the following alternative service levels:

- MSS for Network Firewalls – Standard
- MSS for Network Firewalls – Select
- MSS for Network Firewalls – 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 the Order.

Definitions of service-specific terminology can be found at [www.ibm.com/services/iss/wwcontracts](http://www.ibm.com/services/iss/wwcontracts)

IBM will support the following product features, as applicable:

a. **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).

b. **VPNs**

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

c. **high availability (optional)**

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

IBM will provide the following services in support of the product features listed above, as applicable:

a. **project kickoff, assessment, and implementation**

During deployment and initiation of MSS for Network Firewalls, IBM will work with the Customer to help define appropriate security policies, assist with installation and configuration of the firewall(s), and verify proper device operation prior to transition of the firewall(s) to the SOC.

b. **policy management**

Firewalls only protect Hosts when configured correctly for their network environment. IBM provides policy management services to help the Customer keep firewalls configured with a valid security policy, and retain records of all changes.

c. **device management**

IBM will maintain the firewall by monitoring its system health and availability and applying vendor updates to the firewall.

d. **security event monitoring**

Firewalls 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 a firewall 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.

e. 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.

f. 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.

g. Virtual-SOC
The Virtual-SOC is a Web interface which serves as the Customer’s interface to management of the firewall, alerts, logs, reports, policy change requests, and other types of service tickets.

The following table provides an overview of the MSS for Network Firewalls product features for the Standard, Select, and Premium service levels.

Table 1 - Product Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard Level</th>
<th>Select Level</th>
<th>Premium Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported bandwidth</td>
<td>Up to 100MB</td>
<td>100MB through 1 GB and up</td>
<td>100MB through 1 GB and up</td>
</tr>
<tr>
<td>Supported users</td>
<td>Up to 500</td>
<td>500 and up</td>
<td>500 and up</td>
</tr>
<tr>
<td>Firewall</td>
<td>Custom firewall policy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN</td>
<td>Support for site-to-site, client and SSL VPNs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High availability</td>
<td>Support for active/active or active/passive.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Out of band (“OOB”) access</td>
<td>Optional</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Security event monitoring</td>
<td>Available as an option</td>
<td>Available as an option</td>
<td>Included as part the service</td>
</tr>
<tr>
<td>Web Security</td>
<td>Not available</td>
<td>Available as an option for supported platforms only</td>
<td>Available as an option for supported platforms only</td>
</tr>
<tr>
<td>Antivirus</td>
<td>Not available</td>
<td>Available as an option for supported platforms only</td>
<td>Available as an option for supported platforms only</td>
</tr>
</tbody>
</table>

The following table provides an overview of the MSS for Network Firewalls services for the Standard, Select, and Premium service levels, provided in support of the product features listed above.

Table 2 - Services

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard Level</th>
<th>Select Level</th>
<th>Premium Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project kickoff, assessment, and implementation</td>
<td>Included</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy management</td>
<td>Up to 2 policy change requests per month</td>
<td>Up to 4 policy change requests per month</td>
<td>Unlimited policy change requests per month</td>
</tr>
<tr>
<td>Device management</td>
<td>24x7 device health and availability monitoring, and maintenance of firewall software</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MSS for Network Firewalls – Standard

MSS for Network Firewalls – Standard is a network-based firewall designed to prevent unwanted and malicious traffic from entering or leaving the enforcement point. The service identifies and blocks access to certain applications and data attempting to enter your network, using stateful inspection (also called “dynamic packet filtering”).

MSS for Network Firewalls – Standard is designed to support up to 500 users.

2. IBM Responsibilities

2.1 Deployment and Initiation

2.1.1 Data Gathering

During deployment and initiation, IBM will either work with the Customer to deploy a new firewall or begin management of an existing firewall.

2.1.2 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.

2.1.3 Assessment

Data Gathering

IBM will provide a form for the Customer to document detailed information for the initial setup of the firewall 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 firewall. If migrating from an existing firewall to a newer firewall, IBM will use the configuration and policy on the existing firewall.

During this assessment, IBM may make recommendations to adjust the policy of the firewall or the layout of the network to enhance security. IBM recommends that all firewalls be deployed inline, at the network perimeter.

If the Customer chooses to deploy the firewall in a passive mode, the protection provided by the firewall 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.

IBM will work with the Customer to help determine an optimal firewall configuration based on the Customer’s network and firewall configuration, and the most active worldwide threats (as determined by the IBM Global Threat Operations Center). IBM may tune the policy to reduce the number of erroneous alarms, if required.
Existing Firewall Assessment
If IBM will be taking over management of an existing firewall, IBM must assess the firewall to be sure it meets certain specifications. IBM may require the firewall 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.

2.1.4 Implementation

Configuration at IBM
For firewalls purchased through IBM at the time of deployment, much of the configuration and policy setting will take place at IBM facilities. For existing firewalls already in use, the Customer will have the option to ship the firewall 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 firewall, IBM will typically perform the configuration remotely. The Customer may be required to physically load media.

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

2.1.5 Transition to SOC

Once the firewall 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 SOC takes over management and support of the firewall 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

After the MSS for Network Firewalls – Standard environment has been established, and during any renewal contract period, IBM will provide MSS for Network Firewalls – Standard on a 24 hours/day by 7 days/week basis.

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. MSS for Network Firewalls – Standard Customers may process up to two 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.

Ongoing Policy Maintenance
IBM will work with the Customer to maintain protection strategies, including types of automatic blocking behavior in the case of firewalls 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 firewalls 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 firewalls 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 firewall 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 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.

### 2.2.2 Device Management

Typically, IBM will be the sole provider of software-level device management for the firewall. With root/super-user/administrator level access to the device, along with an out-of-band system and an firewall installed on the device, IBM will maintain system status awareness, apply operating system ("OS") 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 firewall, 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 firewall via the Internet. Data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible.

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.

**Log Storage**

The X-Force® Protection System ("XPS") 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 a secure, 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 MSS for Network Firewalls – Standard is monitored by using a Host-based monitoring firewall (when possible) or SNMP. The devices are regularly polled by the SOC, keeping IBM security analysts informed of potential problems as they develop. Key metrics analyzed by the monitoring firewall include:

- hard disk capacity (if applicable);
- CPU utilization;
- memory utilization; and
- process availability.

In addition to system health metrics, IBM will monitor device uptime and availability. If contact with a managed device is 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 firewall is not reachable through standard in-band means, the Customer will be notified via telephone using a predetermined escalation procedure. Following telephone escalation, IBM will begin investigating problems related to the configuration or functionality of the managed device.

**Application/Operating System Updates**

Periodically, it will be necessary for IBM to install patches and software updates to improve device 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 clearly state the impacts of the scheduled maintenance and any Customer-specific requirements.

**Security Content Updates**

To help ensure that the most current threats are properly identified, IBM will update security platforms with the most current Security Content. Such Security Content, delivered in the form of new checks or signatures for the Intrusion Prevention system, antispam and antivirus modules, and new URL listings for the Web filtering module, enhances the firewall’s security capabilities.

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

**Device Troubleshooting**

If the firewall 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 firewall is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

**Out-of-Band Access (Optional)**

Out-of-band ("OOB") access is a highly recommended 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.

OOB is optional at the Standard level of service.

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 devices; and
- the Customer is responsible for all aspects of managing the OOB solution.

### 2.2.3 Vulnerability Management Service

The vulnerability management service is a remotely delivered, electronic service that regularly and automatically scans the Customer’s 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 the IP address range to be scanned, prior to the initial scan of such IP address range being performed. For each firewall purchased, the Customer will receive quarterly remote vulnerability assessment scanning for one IP address.
Features of the vulnerability management service include:

a. **External vulnerability management** - IBM will provide external vulnerability management for each firewall under full management. 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 Intrusion Prevention 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.

### 2.2.4 X-Force Threat Analysis Service

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

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

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

### 2.2.5 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 structured 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 comprehensive analysis, alerting, remediation, and reporting.

The Virtual-SOC provides 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 comprehensive service information, via the IBM security Web portal, 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.

### 2.2.6 VPN Support

The VPN feature allows supported server-based VPNs to be connected to the firewall and helps to enable secure transmission of data across untrusted networks, via site-to-site communication. The default configuration of this feature activates this capability on the managed firewall 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 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 firewall and another supported encryption device. Site-to-site VPNs provide help to secure 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 firewalls, 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 identify, diagnose, and resolve performance and IBM-related issues.

### 2.2.7 High Availability (Optional)

High Availability ("HA") increases the reliability MSS for Network Firewalls - Standard by supporting the implementation of redundant firewall devices into your managed environment. Adding HA to MSS for Network Firewalls - Standard may require changes to the firewall platform, software licensing, IP addressing requirements, or managed service fees. MSS for Network Firewalls - Standard does not support non-integrated, third party HA solutions. HA is an optional feature that is available for an additional fee.

**Active/Passive Implementations**

Active/passive implementations improve reliability of the firewall solution through redundancy. In this configuration, a second firewall is configured as a hot-standby, ready to begin serving the network if the primary firewall experiences a critical hardware or software failure. In such a scenario, failover is 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 network firewalls by using both firewalls to handle the network traffic simultaneously. In this configuration, each firewall handles a share of the network packets, determined by a load-balancing algorithm. If one firewall fails, the other firewall is designed to automatically handle all of the traffic until the failed firewall has been restored. Active/active configurations are recommended for mission critical environments with high traffic volumes and/or large fluctuations in network utilization.

### 2.2.8 Security Event Monitoring (Optional)

IBM will augment the automated analysis capabilities of the XPS 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 text messaging notification, or telephone, depending on declared event severity, as described in the section of this Service Description entitled “SLA Remedies”.

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 firewall’s policy will be reported through the Virtual-SOC, including comprehensive data. 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. Security event monitoring is an
optional service for MSS for Network Firewall – Standard and Select service levels, and is available for an additional fee.

3. **Customer Responsibilities**

While IBM will work with the Customer to deploy and implement the firewall, and IBM will manage the firewall, 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**

The Customer is responsible for all physical installation and cabling, and may be required to physically load media. IBM will provide live support during normal business hours, via phone and e-mail.

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

If IBM will be taking over management of an existing firewall, IBM may require the firewall 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.

The Customer must ensure that any existing firewall 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.

While IBM will provide support and guidance, the Customer is responsible for the physical installation and cabling of all firewalls, unless such service is provided as an IBM PSS consulting project. If the Customer chooses to deploy client VPN functionality, 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 firewall’s policy and/or configuration.

While IBM may assist, the Customer is ultimately responsible for its own network security strategy, including incident response procedures.

3.2.2 **Device Management**

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

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. Internet access service and telecommunications transport circuits are solely the Customer’s responsibility.

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.

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.

If the Customer wishes to enable the HA feature of MSS for Network Firewalls – Standard, the Customer agrees to purchase a second firewall and pay for the ongoing management of such firewall.
Implementing a new OOB solution requires the Customer to purchase an IBM-supported OOB device and provide a dedicated analog telephone line for access. The Customer agrees to acquire and pay for the device and telephone line and pay for the ongoing management of same.

3.2.3 Data Gathering
The Customer consents to IBM gathering security event log data to look at trends, and real or potential threats. IBM may gather this security event log data with similar data of other clients so long as such data is gathered in a manner that will not in any way reveal the data as being attributable to the Customer.

MSS for Network Firewalls – Select
MSS for Network Firewalls – Select is designed to support more than 500 users. The service will provide the same function as MSS for Network Firewalls - Standard 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 “MSS for Network Firewalls – Standard”, subsection “IBM Responsibilities” above. In addition, IBM will perform the responsibilities set forth in the section entitled “MSS for Network Firewalls – Select”, subsection “IBM Responsibilities” below.


4. IBM Responsibilities
4.1 Ongoing Management and Support
IBM will provide the following services in support of MSS for Network Firewalls – Select during the initial contract term after the services environment has been established, and during any renewal contract term.

4.1.1 Policy Management
Changes
The Customer may process up to four 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.

Additionally, the Customer may specify a time period for IBM to implement a single policy or configuration change. The Customer may specify a start time, and optionally, and end time for the window, but the window must be at least 30 minutes long.

If the Customer does not specify an end time for this maintenance window, IBM will begin implementation of the requested policy change within 30 minutes of the window start time. If the Customer specifies a start and end time, IBM will begin implementation of the policy change within the maintenance window.

4.1.2 Vulnerability Management Service
For each firewall purchased, the Customer will receive quarterly remote vulnerability assessment scanning for two IP addresses. This includes scanning of the Internet-accessible IP addresses of the firewall and one additional Host.

4.1.3 VPN Support
MSS for Network Firewalls – Select allows Customers to create an unlimited number of site-to-site, client and SSL VPN connections. The total number of supported tunnels, and the ability to implement SSL tunnels are subject to the technological limitations of the deployed firewall platforms. IBM will only support static authentication mechanisms for client VPN connections.

Client VPNs
Client VPNs help to provide 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 firewall is designed to determine the
specific client VPN applications to be supported by MSS for Network Firewalls - 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 secure 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.

### 4.2 External Content Security (Optional)

#### 4.2.1 Web Filtering

Content security support for MSS for Network Firewalls is designed to address the concerns of
organizations that wish to leverage the benefits of Internet Web access, yet are concerned about the
possible loss of productivity and potential of encountering objectionable Internet content.

**Availability**

Support for content security management is available in two forms depending on the capabilities of the
deployed firewall platform and Customer preference.

- **External (unmanaged)** – most firewall platforms do not include integrated Web content security
  functionality. For these platforms, IBM will support the integration of a compatible Customer-
  managed Web content security server into the firewall implementation. The Customer will be solely
  responsible for all maintenance, configuration, troubleshooting, and support of the content security
  implementation.

- **External (managed)** – IBM will support the integration and full management of content filtering with
  compatible firewall platforms. Such services are provided for an additional monthly fee.

For content security to be effective, the firewall platform (and if applicable, its external content security
server) must be placed in a location where user Web traffic passes through the device(s) prior to reaching
its intended destination. This allows the firewall to compare the requested URL against the content
database and validate the requested destination is authorized.

Configuration of the content security module/server will vary depending on the firewall platform and
content security solution deployed. Following is a general overview of features that extend across all
supported content security solutions:

- **Category Lists** – a selection of content categories to block.
- **Destination White Lists** – specific sites that should be allowed even if they exist within a denied
  content category.
- **Destination Black Lists** – specific sites that should be blocked even if they exist within an allowed
  content category.
- **Source White List** – specific IP addresses that should be excluded from content filtering.

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.

**Policy and Configuration Changes**
Following successful deployment of the content security solution, Customers may submit requests to modify the content security policy and/or configuration features (including content category selections) at any time by submitting a policy change request through the Virtual-SOC, following normal change submission procedures.

**Security Content Updates**

To help ensure that the most current threats are properly identified, 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 antivirus module, and new URL listings for the Web filtering module, enhances the firewall’s security capabilities.

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

### 4.2.2 Antivirus

**MSS for Network Firewalls - Select** provides two types of antivirus management to minimize the risk of malicious code within the network data stream:

- **External (unmanaged)** – Most firewall platforms do not include integrated antivirus functionality. For these platforms, IBM will support the integration of a compatible Customer-managed antivirus security server into the firewall implementation. The Customer is solely responsible for all maintenance, configuration, troubleshooting, and support of the content security implementation.

- **External (managed)** – IBM will support the integration and full management of selected antivirus platforms. Such services are provided for an additional monthly fee.

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

Configuration of the content security server will vary depending on the firewall and antivirus platforms. 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.

### 5. Customer Responsibilities

#### 5.1 Policy Management

Any changes submitted with a specified maintenance window must be specified before the start of the window, and must be submitted far enough in advance that IBM can implement the change within the window and still comply with SLA guarantees for policy change implementation.

#### 5.2 Device Management

The Customer must deploy an IBM-supported OOB device and provide a dedicated analog telephone line for access. The Customer agrees to acquire and pay for the device and telephone line and pay for the ongoing management of same.

#### 5.3 VPN Support

During site-to-site VPN creation, Customers will work with IBM to assist in defining key VPN parameters such as:

- endpoint details
- encryption types
- shared secret information
- encryption domains / groups
- applicable policy requirements

#### 5.4 External Content Security

Enabling the Web content security and antivirus functionality at any service level may require additional licensing for the firewall platform which shall be the sole responsibility of the Customer.

External (Unmanaged) – most firewall platforms do not include integrated Web content security and/or antivirus functionality. For these platforms, IBM will support the integration of a compatible Customer-managed Web content security and/or antivirus security server into the firewall implementation. In such a scenario, the Customer is solely responsible for all additional licensing for the firewall platform,
maintenance, configuration, troubleshooting, and support of the Web content and/or antivirus security implementation.

**MSS for Network Firewalls – Premium**

MSS for Network Firewalls – Premium is designed to support more than 500 users. The service will provide the same function as MSS for Network Firewalls - 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 “MSS for Network Firewalls – Select”, subsection “IBM Responsibilities” above. In addition, IBM will perform the responsibilities set forth in the section entitled “MSS for Network Firewalls – Premium”, subsection “IBM Responsibilities” below.


6. **IBM Responsibilities**

6.1 **Ongoing Management and Support**

IBM will provide the following services in support of MSS for Network Firewalls – Premium during the initial contract term after the services environment has been established, and during any renewal contract term.

6.1.1 **Policy Management**

**Changes**

MSS for Network Firewalls – Premium 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.

**Emergency Policy Changes**

If a policy/configuration change is deemed an emergency, IBM will perform one emergency change per managed firewall under management during each calendar month of the contract. Unused emergency changes do not roll over to the following calendar month.

To submit an emergency change request, Customers must submit the change request through the Virtual-SOC, following normal change submission procedures. During the electronic submission of the change request, the change must be clearly identified as an emergency. Following electronic submission, an authorized security contact must place a follow-up phone call to the SOC and escalate the change submission to emergency status.

6.1.2 **Vulnerability Management Service**

For each firewall purchased, the Customer will receive quarterly remote vulnerability assessment scanning for three IP addresses. This includes scanning of the Internet-accessible IP addresses of the firewall and two additional Hosts.

6.1.3 **Security Event Monitoring**

Security event monitoring is included as part of the MSS for Network Firewalls – Premium.

7. **Customer Responsibilities**

7.1 **Policy Management**

**Emergency Policy Changes**

To submit an emergency change request, Customers must submit the change request through the Virtual-SOC, following normal change submission procedures. During the electronic submission of the change request, the change must be clearly identified as an emergency. Following electronic submission, an authorized security contact must place a follow-up phone call to the SOC and escalate the change submission to emergency status.

8. **Service Level Agreements for Standard, Select, and Premium Service Levels**

IBM SLAs establish response time objectives and countermeasures for Security Incidents resulting from MSS for Network Firewalls. 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.

8.1 SLA Guarantees

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

a. 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.

b. Policy change request implementation guarantee

(1) Standard level - the Customer policy change requests will be implemented within 24 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.

(2) Select and Premium level - the Customer policy change requests will be implemented within eight 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.

c. Emergency change request implementation guarantee (available for MSS for Network Firewalls - Premium only) – IBM will implement Customer emergency policy change requests within two hours of the Customer’s declaration of emergency (by telephone) following change submission through the Virtual-SOC.

This guarantee is only available for policy change requests submitted by a valid security contact in accordance with established procedures. Further, this guarantee is based on actual time of implementation, and not on the time that the Customer was notified the request was completed.

IBM will promptly notify the Customer upon implementation of a change request by telephone, e-mail, fax, pager, or electronic response via the Virtual-SOC and will continue attempting to contact the designated Customer contact until a contact is reached or all escalation contacts have been exhausted.

d. Security Incident identification guarantee for firewall security event monitoring (available for Premium level only) - IBM will identify all Priority 1, 2, and 3 level Security Incidents based on firewall 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, or firewall configuration.

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.

e. Security Incident response guarantee (applies to firewall security event monitoring 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.

f. Proactive system monitoring guarantee:

(1) Standard level - the Customer will be notified within 30 minutes after IBM determines the Customer’s firewall is unreachable via standard in-band connectivity.
(2) Select and Premium level - the Customer will be notified within 15 minutes after IBM determines the Customer’s firewall is unreachable via standard in-band connectivity.

**Table 3 – SLA Summary**

<table>
<thead>
<tr>
<th>Service Level Agreement</th>
<th>Standard</th>
<th>Select</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy change request acknowledgement guarantee</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Policy change request implementation guarantee</td>
<td>Yes, within 24 hours of receipt</td>
<td>Yes, within 8 hours of receipt</td>
<td>Yes, within 8 hours of receipt</td>
</tr>
<tr>
<td>Emergency change request implementation guarantee</td>
<td>No</td>
<td>No</td>
<td>Yes, within 2 hours after declaration</td>
</tr>
<tr>
<td>Security Incident identification guarantee</td>
<td>No</td>
<td>No</td>
<td>Yes, applies to firewall security event monitoring only</td>
</tr>
<tr>
<td>Security Incident response guarantee</td>
<td>No</td>
<td>No</td>
<td>Yes, applies to firewall security event monitoring only</td>
</tr>
<tr>
<td>Proactive system monitoring guarantee</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**8.2 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 any given calendar month. For all SLAs, 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 in a given calendar month, as stated in the section entitled “SLA Exclusions and Stipulations” below. Specific SLA recoveries are listed below:

**Table 4 - Summary of Service Level Agreements and Remedies**

<table>
<thead>
<tr>
<th>Service Level Agreements</th>
<th>Remedies for MSS for Network Firewalls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy change request acknowledgement guarantee</td>
<td>Credit of 1 day of the monthly monitoring fee for the affected device</td>
</tr>
<tr>
<td>Policy change request implementation guarantee</td>
<td></td>
</tr>
<tr>
<td>Emergency change request implementation guarantee</td>
<td></td>
</tr>
<tr>
<td>Security Incident identification guarantee</td>
<td></td>
</tr>
<tr>
<td>Security Incident response guarantee</td>
<td></td>
</tr>
<tr>
<td>Proactive system monitoring guarantee</td>
<td></td>
</tr>
</tbody>
</table>

**8.3 SLA Exclusions and Stipulations**

**8.3.1 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.

8.3.2 Customer Network/Server Change Notifications
The Customer is responsible for providing IBM advance notice regarding any network or server changes to the firewall 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.

8.3.3 Maximum Penalties/Remedies Payable to Customer
The total SLA credits (called “remedies”) provided by MSS for Network Firewalls – Standard, Select, and Premium levels, described in the sections entitled “SLA Guarantees” and “SLA Remedies” above, will not exceed the service fees for one calendar month.

8.3.4 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 firewall and therefore the firewall 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 firewall, or that does not generate a logged event, is not covered under these SLAs.

8.3.5 SLA Compliance and Reporting
SLA compliance and the associated remedies are based on fully functional network environments, Internet and circuit connectivity, firewalls, 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.

8.3.6 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.

9. Service Level Objectives
IBM service level objectives (called “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.
10. **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.