

Service Description

IBM Managed Security Services for Network Management and Security

1. Scope of Services

IBM Managed Security Services for Network Management and Security (called “MSS for Network Management and Security”) is comprised of the following alternative service levels which are designed to address the needs of small and medium business operations, as well as distributed enterprises.

- MSS for Network Management and Security – Standard
- MSS for Network Management and Security – Select
- MSS for Network Management and Security – Premium

The details of your order (e.g., the services you require, 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

The following table provides an overview of the service features at the different service levels (i.e., standard, select and premium).

Table 1 - Standard Features

Feature	Standard Level	Select Level	Premium Level
Firewall	Yes	Yes	Yes
VPN	Yes	Yes	Yes
Network Monitoring	Yes	Yes	Yes
Gateway Security	No	Yes	Yes
Content Filtering	No	No	Yes

MSS for Network Management and Security – Standard

The following services are provided as part of MSS for Network Management and Security – Standard.

2. IBM Responsibilities

2.1 Deployment and Initiation

IBM will arrange for the shipment of the CPE Appliance within approximately ten business days after receipt of the signed Order and any other required contractual documents. The Customer administrator will be notified (by electronic communication) that the CPE Appliance has been shipped. In addition, IBM will provide telephone support for the installation of the CPE Appliance.

After the CPE Appliance has been installed, IBM will enable functionality of MSS for Network Management and Security – Standard, permit remote user capability, and provide a Microsoft Windows XP compatible VPN client.

The Customer will be provided with password access to a proprietary Web-based reporting and management tool to allow viewing of data and statistics on Customer use of MSS for Network Management and Security – Standard. This tool will also offer a number of configuration and management facilities the customer may utilize as part of the service.

IBM will retain ownership of all hardware and software provided with MSS for Network Management and Security – Standard, including but not limited to the CPE Appliance.

2.2 Ongoing Management and Support

After the MSS for Network Management and Security – Standard environment has been established, and during any renewal contract period, IBM will provide MSS for Network Management and Security – Standard on a 24 hours/day by 7 days/week basis. Regular, automatic updates will be provided for the software and firmware.

Support for the service will be provided to the Customer by electronic mail or telephone 24 hours/day by 7 days/week (in English only).

2.2.1 Firewall Service

IBM will enable functionality for the firewall service. The firewall service provides an interface for the Customer which is designed to identify and block illegitimate access to the network. Quality of Service (“QoS”) functionality is designed to prioritize data to optimize Internet access.

2.2.2 VPN Service

IBM will enable VPN functionality. The VPN service is designed to permit the Customer to configure secure connections between multiple sites and/or remote users into their network. The service is designed to automatically establish secure sockets layer (“SSL”) tunnels to transfer data among CPE devices at different locations.

2.2.3 Network Monitoring Service

IBM will provide monitoring services for the CPE Appliance. The network monitoring service provides two capabilities: 1) network and device monitoring, and 2) network reporting. The network and device monitoring capabilities allow users to configure network and device statistics. Network reporting collects multiple network monitoring statistics and security events to create automated reports and graphs for Customer review.

MSS for Network Management and Security – Select

2.3 Ongoing Management and Support

MSS for Network Management and Security – Select is designed to provide the same functionality as MSS for Network Management and Security - 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 Management and Security – Standard”, subsection “IBM Responsibilities”. In addition, IBM will perform the responsibilities in the section entitled “MSS for Network Management and Security – Select”, subsection “Gateway Security Service”, below.

2.3.1 Gateway Security Service

IBM will enable services to provide gateway security functionality. The gateway security service provides gateway antivirus filtering, and Intrusion Detection and Intrusion Prevention System (called “IDS/IPS”) capabilities. The antivirus engine scans for worms, viruses, and Trojan horses at the network gateway. The IDS/IPS engine performs real-time traffic analysis, establishes log files, and is designed to take corrective action when an intrusion attempt is detected on the Customer network. The Customer will enable/disable the antivirus engine, the IDS/IPS engine, and IDS/IPS signatures for known attacks at their discretion. Every CPE Appliance can be automatically updated by IBM 24 hours/day by 7 days/week with the latest Intrusion Detection signatures.

MSS for Network Management and Security – Premium

2.4 Ongoing Management and Support

MSS for Network Management and Security – Premium is designed to provide the same functionality as MSS for Network Management and Security - 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 Management and Security – Select”, subsection “Ongoing Management and Support”. In addition, IBM will perform the responsibilities in the section entitled “MSS for Network Management and Security – Premium”, subsection “Content Filtering Service”, below.

2.4.1 Content Filtering Service

IBM will enable content filtering functionality. The content filtering service provides filtering capabilities and network protection by file type (e.g., chat, jpeg, mpeg, etc.), virus definitions, intrusion protection signatures (e.g., Trojan horses, denial of service attacks, etc.) and other external threats. IBM maintains and updates data tables with URL addresses classified by category type. The Customer will enable/disable these categories and sub-categories at its discretion. These definitions and future updates are incorporated within each subscriber’s service. Additional Web site URLs are added automatically to system-defined categories. Both “white listing” and “blacklisting” are supported, as well

as the ability to define parameters for different users or groups of users. Users are able to implement simultaneous white and black lists.

3. Customer Responsibilities

In support of MSS for Network Management and Security, the Customer will provide IBM with the name, telephone number and e-mail address of a focal point (administrator) to whom IBM will send notifications, as required. The Customer will implement and maintain the configuration settings required to direct traffic to IBM via MSS for Network Management and Security.

The Customer will maintain the security of the password provided for access to the proprietary Internet-based reporting and management tool, including not disclosing to any third party and will ensure compliance at all times with the provisions of the IBM Acceptable Use Policy for IBM e-business Services located at <http://www.ibm.com/services/e-business/aup.html>;

The Customer will ensure that they, or any member of their Enterprise, do not use MSS for Network Management and Security (or any part or portion thereof) to in any way develop or promote commercial services similar to said MSS for Network Management and Security.

SHOULD THE CUSTOMER FAIL TO MEET THESE OBLIGATIONS AND DISRUPTION OCCURS TO MSS FOR NETWORK MANAGEMENT AND SECURITY – PREMIUM, IBM WILL INFORM YOU OF SUCH FAILURES AND RESERVES THE RIGHT TO WITHHOLD PROVISION OF OR SUSPEND ALL OR PART OF THE SERVICES IMMEDIATELY AND UNTIL SUCH USE IS TERMINATED.

All cost of repair, replacement, or refurbishment caused by accident, misuse, abuse, neglect, or the Customer's failure to install, use and maintain the CPE Appliances in accordance with the applicable documentation and specifications will be the responsibility of the Customer. In addition, it will be the Customer's responsibility to furnish all labor for packing, unpacking, and installation and to immediately return all CPE Appliances as directed by IBM, upon termination or expiration of MSS for Network Management and Security. The CPE Appliances are to be returned in the same condition as when delivered to you, excepting reasonable wear and tear.

The Customer agrees not to:

- a. rent, lease, or loan MSS for Network Management and Security, or any part thereof. You also may not permit third parties to benefit from the use or functionality of MSS for Network Management and Security via timesharing, service bureau arrangements or otherwise;
- b. reverse translate, decompile, or disassemble or otherwise transfer any software that is embedded in or related to the CPE Appliances or that provides MSS for Network Management and Security;
- c. attempt to derive the processes by which the services are provided, except to the extent the foregoing restriction is expressly prohibited by applicable law;
- d. make any alteration, addition or modification to the CPE Appliances; and
- e. transfer possession of the CPE Appliances to any third party.

The Customer will be responsible for installing and configuring workstation software required for implementing remote user access to the VPN service.

The Customer is responsible for implementing and maintaining the configuration settings required to direct traffic via the firewall and VPN service.

The Customer is responsible for the management, configuration, and security settings of all services and service levels enabled by IBM for each contracted CPE Appliance as set forth in the sections entitled "MSS for Network Management and Security – Standard", "MSS for Network Management and Security – Select", and "MSS for Network Management and Security – Premium" of this document .