Hardware Management Console External Connectivity Security for IBM POWER5 Processor-based Systems

March 2, 2007

by: Jason Stapels
Ann Burkes
Brian Myers

Table of Contents

1 Introduction

This document describes data that is exchanged between the Hardware Management Console (HMC) and the IBM Service Delivery Center (SDC) and the methods and protocols for this exchange. All the functionality that is described here refers to HMC version V6.1.0 and later.

1.1 Terms and Definitions

It is assumed that the reader has a basic understanding of Internet Protocol (IP) networks and protocols. The following is a list of terms and acronyms that may not be familiar to the reader.

3DES	Triple DES
AES	Advanced Encryption Standard
CHAP	Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
ESP	Encapsulated Security Payload, Protocol 50
HMAC	Hashing Message Authentication Code
HMC	Hardware Management Console
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
L2TP	Layer 2 Tunneling Protocol
LIG	Local Interface Gateway
MD5	Message Digest Algorithm 5
PAP	Password Authentication Protocol
PPP	Point-to-Point Protocol
PSK	Pre-Shared Key
RC4	Rivest Cipher 4
SDC	Service Delivery Center
SNAT	Source Network Address Translation
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

2 HMC Connectivity Methods

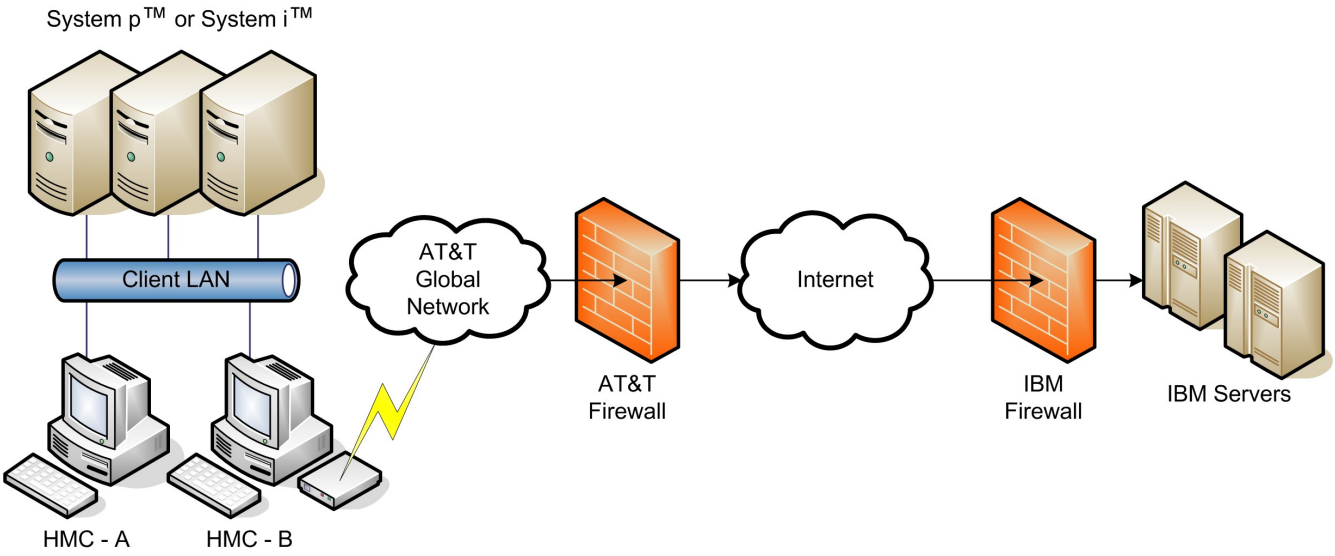
The HMC uses various methods for communicating back to IBM to match different client environments. This section outlines all the different ways in which an HMC can be configured to communicate with IBM.

2.1 Outbound Configurations

Outbound configurations are used to configure the HMC to connect back to IBM. The HMC uses its ability to connect to IBM for various situations including reporting problems, downloading system fixes, reporting inventory, and transmitting error data. The types of data the HMC sends to IBM are covered in more detail in Section 4.

2.1.1 Modem Connectivity

The following diagram shows a typical dial environment. This configuration allows the HMC to use a modem to dial the AT&T global network and connect to the IBM POWER5™ processor-based systems. The HMC automatically detects the modem when it boots up.



In this scenario the HMC uses one of the configured phone numbers to dial the modem, connecting to the AT&T Global Network. After the modem connects the HMC authenticates itself and establishes a Point-to-Point Protocol (PPP) session between the two modems. Finally, after the PPP session has finished, AT&T allows IP connections through a “Fenced Internet,” which completes the network between the HMC and the IBM servers.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use Secure Sockets Layer (SSL) to encrypt the data that is being sent back and forth.

The “Fenced Internet” connection uses a firewall to limit access between the HMC and the Internet. Specifically it allows communication only between the HMC and a list of IBM IP addresses. All other access to and from the Internet is blocked.

Note that the client can also configure the HMC 's internal firewall, which also applies to IP connections over the modem.

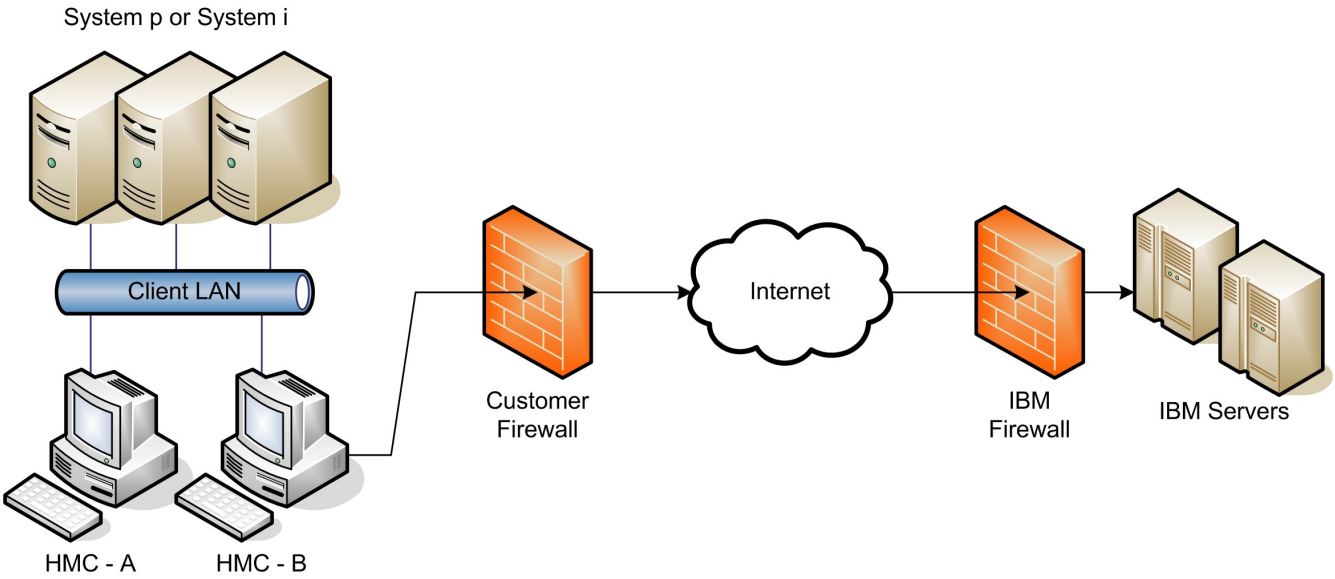
2.1.2 Internet Connectivity

In this configuration the HMC uses a client-provided Internet connection to connect to the IBM servers. All the communications are handled through TCP sockets (which always originate from the HMC) and use SSL to encrypt the data that is being sent back and forth.

Optionally, the HMC can also be enabled to connect to the Internet through a client-configured proxy server.

2.1.2.1 Without Proxy Server

The following diagram shows the HMC connecting to IBM without a proxy server.

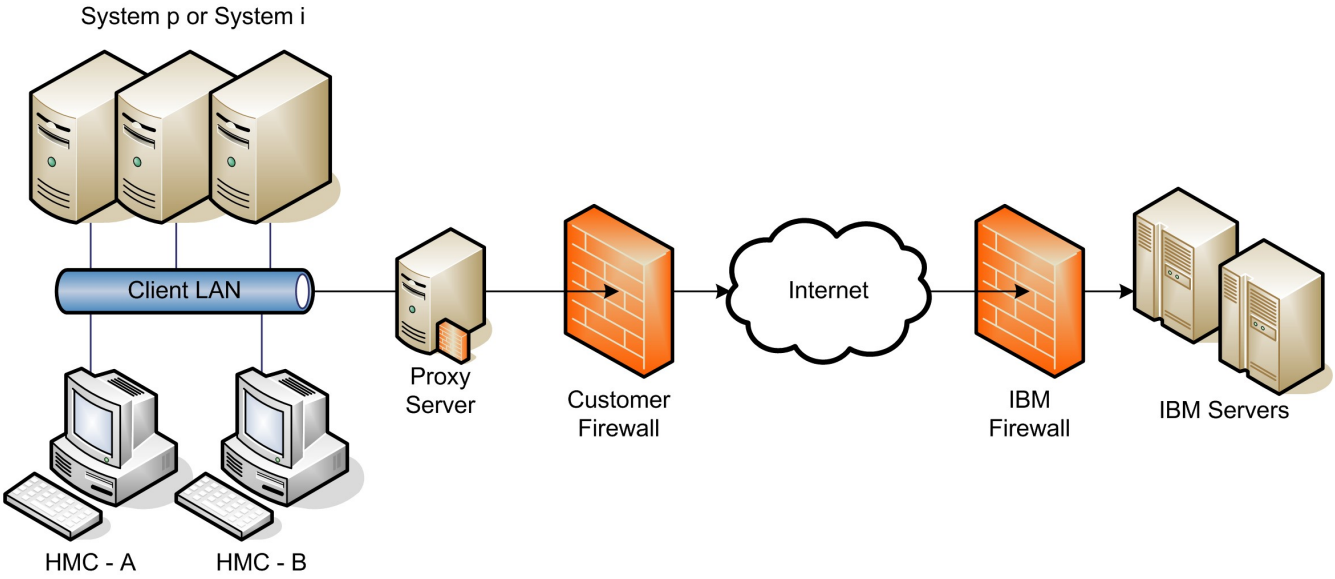


In this setup the HMC connects through the client-provided Internet connection by the default route. For this type of configuration the client can optionally use a second network card to physically separate the local system network from the Internet-enabled network.

For the HMC to communicate successfully, the client's external firewall must allow established TCP packets to flow freely on port 443. The use of Source Network Address Translation (SNAT) and masquerading rules to mask the HMC's source IP address are both acceptable. The firewall may also limit the specific IP addresses to which the HMC can connect. Section 5.1 contains the list of IP addresses.

2.1.2.2 With Proxy Server

The following diagram shows the HMC connecting to IBM using a client-provided proxy server.

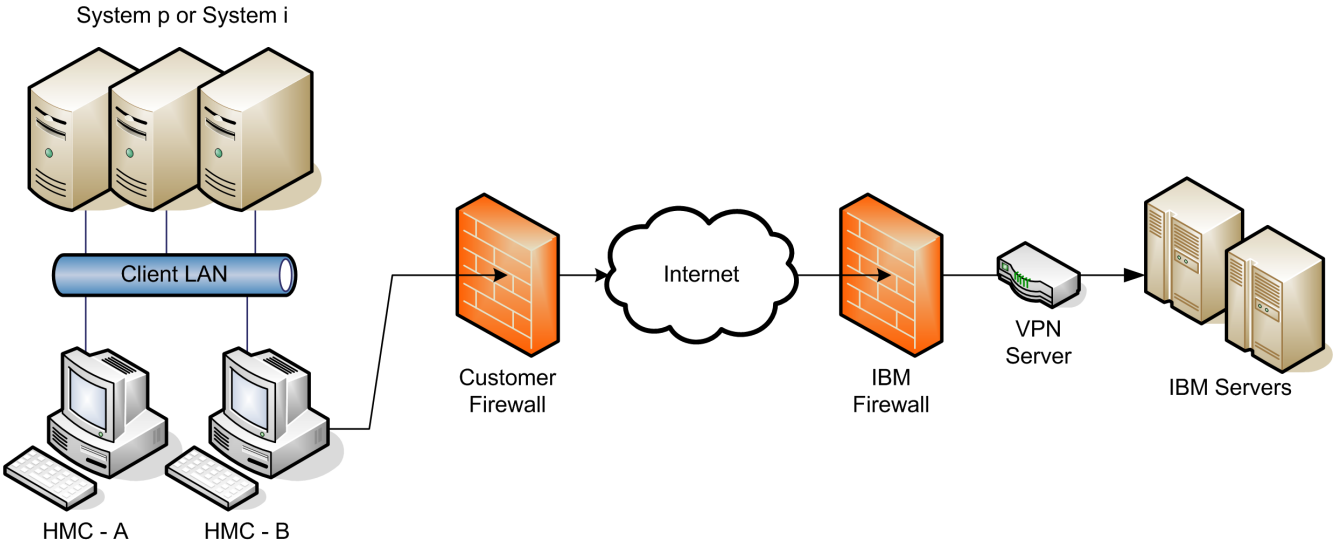


To forward SSL sockets, the proxy server must support the basic proxy header functions (as described in RFC #2616) and the CONNECT method. Optionally, basic proxy authentication (RFC #2617) may be configured so that the HMC authenticates before attempting to forward sockets through the proxy server.

For the HMC to communicate successfully, the client's proxy server must allow connections to port 443. The proxy server may also limit the specific IP addresses to which the HMC can connect. Section 5.1 contains the list of IP addresses.

2.1.3 Internet Virtual Private Network (VPN) Connectivity

The following diagram shows the HMC connecting to IBM using Internet VPN. This is similar to the Internet Connectivity in Section 2.1.2.1, except that the connections are tunneled inside of another network layer. (This configuration is required to use the VPN Inbound Connectivity described in Section 2.2.2.)



In this setup the HMC connects through the client-provided Internet connection by the default route. For this type of configuration the client can optionally use a second network card to physically separate the local system network from the Internet enabled network.

Before the HMC tries to connect to the IBM servers, it first establishes an encrypted VPN tunnel between the HMC and the IBM VPN server gateway. The HMC initiates this tunnel using Encapsulated Security Payload (ESP, Protocol 50) and User Datagram Protocol (UDP). After it is established, all further communications are handled through TCP sockets, which always originate from the HMC.

For the HMC to communicate successfully, the client's external firewall must allow traffic for protocol ESP and port 500 UDP to flow freely in both directions. The use of SNAT and masquerading rules to mask the HMC's source IP address are both acceptable, but port 4500 UDP must be open in both directions instead of protocol ESP. The firewall may also limit the specific IP addresses to which the HMC can connect. Section 5.2 contains the list of IP addresses.

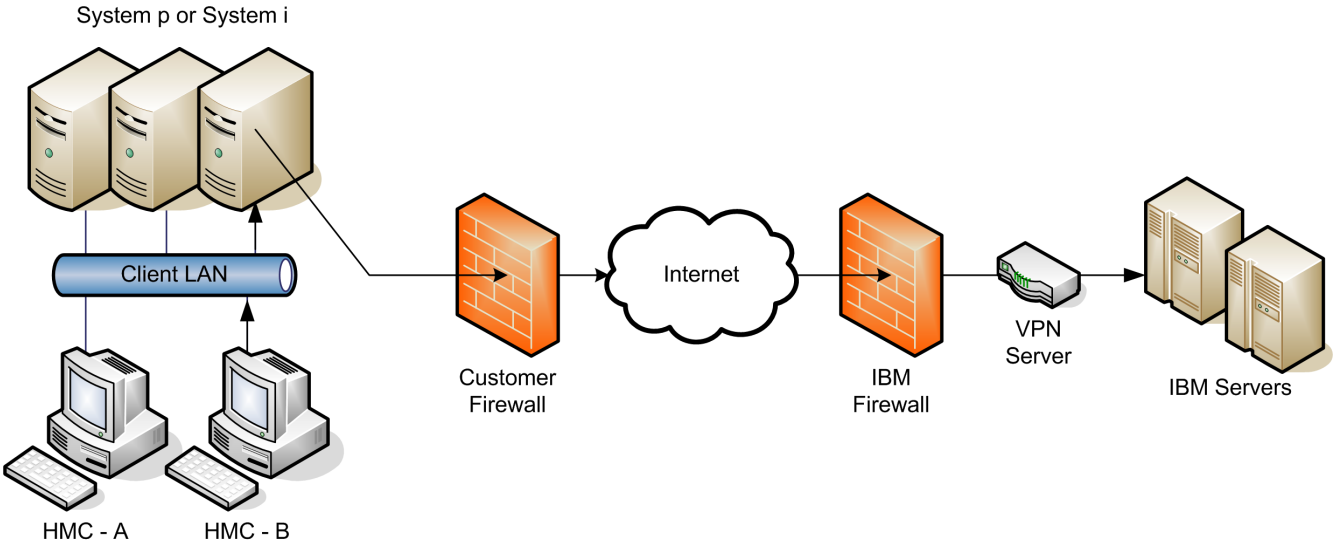
Note that the client can also configure the HMC's internal firewall, which applies to IP connections that go through the VPN tunnel.

2.1.4 Pass-Through Server Connectivity

Configuring pass-through server connectivity allows an HMC to borrow a shared VPN connection or modem from a properly configured i5/OS® partition. (This configuration is not intended to allow an HMC to borrow another HMC's connectivity; for that type of configuration see Section 5.4.)

2.1.4.1 Multi-Hop VPN

The following diagram shows a configuration that allows the HMC to use the multi-hop VPN capability of a client's i5/OS partition.



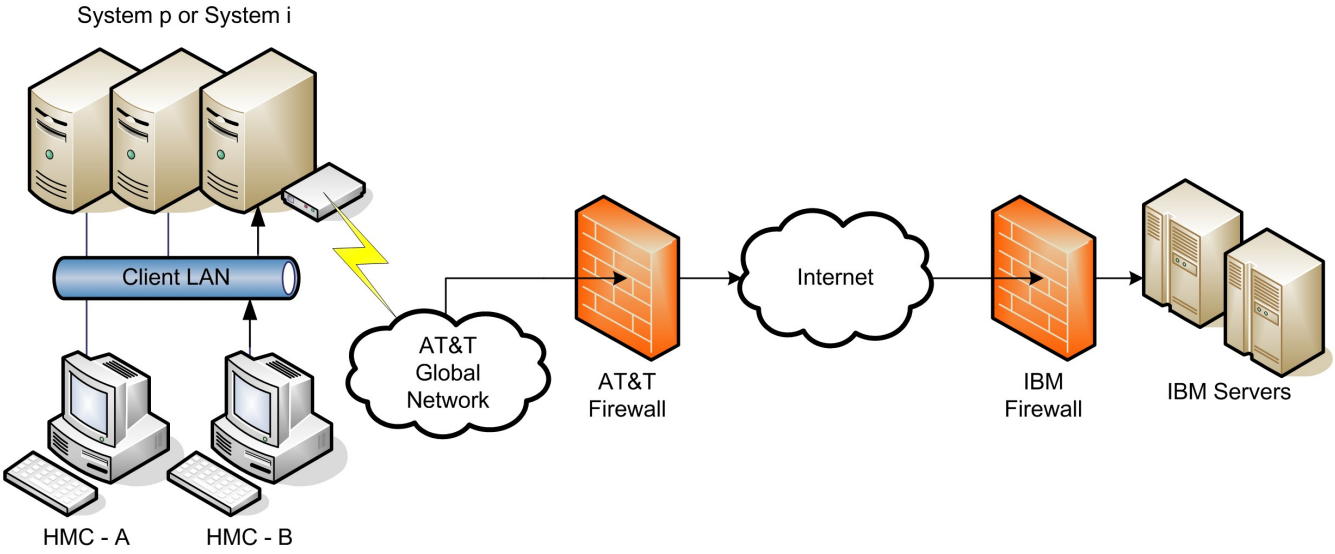
Before the HMC tries to connect to the IBM servers, it first establishes an unencrypted Layer 2 Tunneling Protocol (L2TP) tunnel to the i5/OS partition and requests the creation of an encrypted VPN tunnel between the partition and the IBM VPN server. The HMC initiates this tunnel using a UDP socket. After it is established, all further communications are handled through TCP sockets, which always originate from the HMC.

For the HMC to communicate successfully, the HMC must be able to open a 2-way UDP socket to the i5/OS partition on port 1701. Additionally, the client's external firewall must be configured to allow the partition to properly establish the VPN tunnel to IBM.

Note that the client can also configure the HMC's internal firewall, which also applies to IP connections that go through the VPN tunnel.

2.1.4.2 Remote Modem

The following diagram shows a configuration in which the modem the HMC uses is shared with a client's I5/OS partition.



Before the HMC tries to connect to the IBM servers, it first establishes an unencrypted L2TP tunnel to the i5/OS partition and requests the establishment of a modem connection to the AT&T Global Network. The HMC initiates this tunnel using a UDP socket. After the modem connection is established, the HMC authenticates itself and establishes a PPP session between itself and the dialed AT&T modem. Finally, after the PPP session is finished, AT&T allows IP connections through a “Fenced Internet,” which completes the network between the HMC and the IBM servers.

All the communications between the HMC and the IBM servers are handled through TCP sockets. These sockets always originate from the HMC and use SSL to encrypt the data that is being sent back and forth.

The “Fenced Internet” connection uses a firewall to limit access between the HMC and the Internet. Specifically it allows communication only between the HMC and a list of IBM IP addresses. All other access to and from the Internet is blocked.

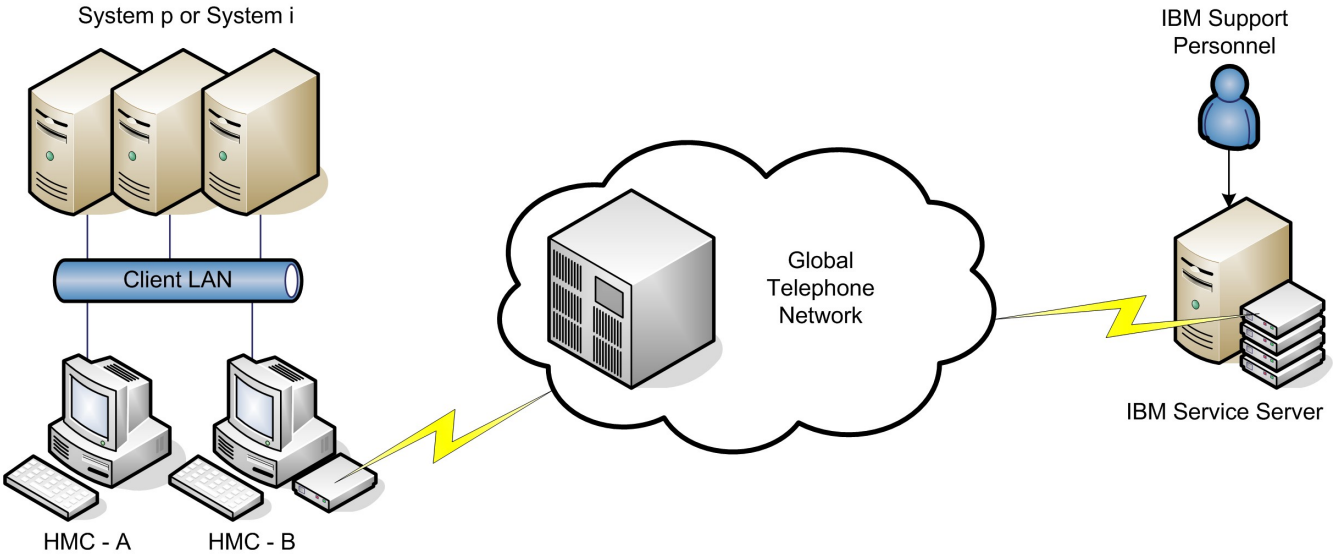
Note that the client can also configure the HMC's internal firewall, which also applies to IP connections over the modem.

2.2 Inbound Configurations

Inbound connectivity configurations allow an IBM Service Representative to connect from IBM directly to your HMC or the systems that the HMC manages. The following sections describe two different approaches to remote service. Both approaches will only allow a one-time use after enabling.

2.2.1 Modem

The following diagram shows an inbound configuration using a modem.



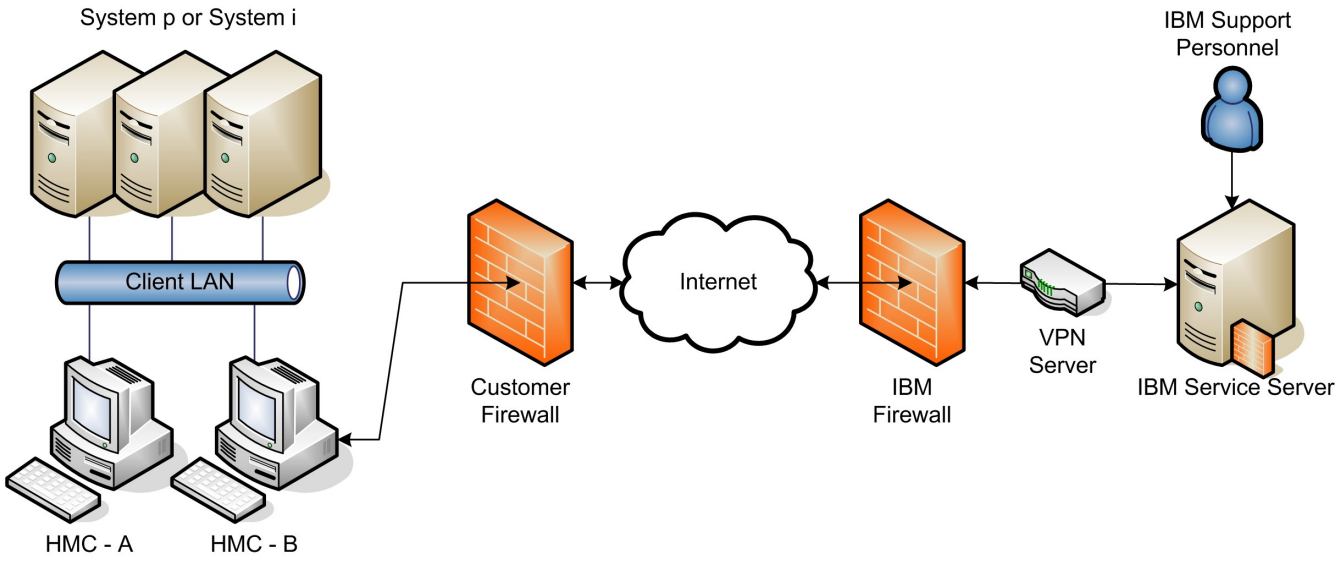
For remote service over a modem, the modem must be set up to accept incoming phone calls. An IBM representative then logs into a special server and uses that to dial directly into the client's modem. After the modem answers, a PPP session is initiated, and the IBM representative must authenticate using credentials based on the value the client entered into the **PPP address** field on the Customize Inbound Connectivity panel.

After the PPP session is successfully initiated, the HMC creates an alternate IP address and attaches it to the virtual PPP network device for each partition to which the client has allowed access. Special routing rules are then put in place to route network packets to those IP addresses and over to the intended partition.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, then the firewall blocks all traffic except for packets targeting the ports outlined in Section 5.3. Note that these rules override any rules that the client set through the Customize Network Settings panel.

2.2.2 VPN

The following diagram shows an inbound configuration using VPN.



A remote service VPN session can be initiated over a modem, Internet VPN, or a pass-through i5/OS partition. At least one of these methods of connectivity must be configured through the Outbound Connectivity panel.

To initiate the VPN session the HMC connects into the IBM VPN server as described in Section 2.1.3. A client who configures the Outbound Internet VPN to use the existing Internet connection must ensure the firewall has been properly configured to allow connections to the servers listed in Section 5.2.

After the VPN session has been initiated, the HMC initiates additional L2TP+PPP tunnels for each partition to which the client has allowed access. Special routing rules are then put in place to route network packets on those tunnels over to the intended partitions.

Finally, if the client has disabled access to the HMC, firewall rules are put in place to block all traffic that goes to the HMC. If the client has allowed access to the HMC, then the firewall blocks all traffic except for packets targeting the ports outlined in Section 5.3. Note that these rules override any rules that the client set through the Customize Network Settings panel.

After the VPN session has been fully established, an authorized IBM Service Representative logs into the IBM Service Server and connects to the HMC through the VPN session. The IBM Service Server has a special firewall in place that keeps the client's VPN session completely separated from the IBM intranet. Access to the client's VPN session through the IBM Service Server is possible only through the use of special tools that require special authorization and knowledge to use.

3 Protocols and Encryption

This section describes the protocols, encryption algorithms, and security that the different communication methods use. It is intended to be a conceptual overview, not to provide implementation details for particular technologies.

3.1 AT&T Global Network

When the HMC tries to connect to IBM using one of the phone numbers available from the Outbound Connectivity Modem panel, it is dialing into the AT&T Global Network Fenced Internet Remote Access Dial Service.

After the HMC's modem successfully connects into one of AT&T's Local Interface Gateways (LIGs), it initiates a PPP session and authenticates with the server using a special account and user ID that are sent using Password Authentication Protocol (PAP). Upon successful authentication, the LIG assigns the HMC a dynamic IP address from a pool for the duration of the connection.

All packets that flow through the LIG from the HMC are inspected to ensure that the source of the packet is the assigned IP address and that the destination matches one of the authorized IBM servers or to one of the utility services provided by AT&T (such as domain name servers). Return packets that flow through the LIG back to the HMC must have destinations that match the assigned IP addresses and the source must match the IBM server with which the IP addresses are communicating. Any packets not matching these criteria are discarded.

3.2 SSL

The SSL sockets used by the HMC are actually Transport Layer Security (TLS) sockets (sometimes referred to as SSLv4). The initial handshake uses a public/private asymmetric 1024-bit key. After the handshake they negotiate the bulk encryption depending on the IBM server to which a connection is being made. IBM systems in the SDC use a symmetric 128-bit Rivest Cipher 4 (RC4) encryption or a symmetric 256-bit Advanced Encryption Standard (AES) encryption.

3.3 VPN

The VPN connection that is used by the HMC is an IP Security (IPSec) implementation in tunnel mode over a UDP socket that uses L2TP+PPP encapsulation for the actual data transmission. The VPN key exchange is done using Internet Key Exchange (IKE), which is authenticated as part of the ESP encryption using a Pre-Shared Key (PSK). The ESP encryption uses a 192-bit Triple DES (3DES) encryption key with a 160-bit Message Digest Algorithm 5 (MD5) hash authentication key. The authentication and encryption keys are renegotiated at a random time interval around every 30 minutes.

After the IPSec tunnel has been properly established, the HMC creates an L2TP tunnel between itself and the VPN server. Within that tunnel the HMC then establishes one or more PPP sessions that the server authenticates using the Challenge Handshake Authentication Protocol (CHAP). All further HMC data sockets are then opened over one of the established PPP sessions.

4 Data and Information

This section outlines what data is sent and the reasons for sending data when the HMC connects to the IBM Service Delivery Center.

4.1 Reasons For Connecting to IBM

- Reporting a problem with the HMC or one of the systems it is managing back to IBM
- Downloading fixes for systems the HMC manages
- Reporting inventory and system configuration information back to IBM
- Sending extended error data for analysis by IBM
- Repairing and verifying system parts and enclosures
- Reporting heartbeat and status of monitored systems
- Sending performance and utilization data for system I/O, network, memory, and processors.

4.2 Data Sent to IBM

This is a list of the files that may be sent to IBM, plus short descriptions of the contents of those files. Along with the information contained in these files, the HMC also sends back client contact information, machine model and serial numbers, and debug traces for HMC software. None of the information or debug data sent to IBM contains client data.

File	Description
actzuict.dat	Tasks performed
hmc.eed	HMC code level obtained from “lshmc -V” and connection information obtained from “lssysconn -r all”
iqyvpd.dat	Configuration information associated with the HMC
iqyvpdc.dat	Configuration information associated with the HMC
iqyycom0.log	HMC firmware log information backup0
iqyycom1.log	HMC firmware log information backup1
iqyycom2.log	HMC firmware log information backup2
iqyylog.log	HMC firmware log information
PMap.eed	Partition map, obtained from “lshsc -w -c machine”
problems.xml	XML version of the problems opened on the HMC for the HMC and the server
sys.eed	Output from the following commands: lssyscfg -r cage lssyscfg -r frame lsdump -e $machine -s a lsdump -e $machine -s b lshsc -i -a >> managedSystems lssyscfg -r lpar lshwres -r proc –level lpar lshwres -r mem -m $machine --level lpar lshwres -r io -m $machine --rsubtype slot lsdump -m $machine lssyscfg -r sys -m $machine lssyscfg -m $machine -r sys lssyscfg -m $machine -r lpar

	lssyscfg -m $machine -r sysprof
machType-Model_Serial.VPD.xml	Configuration information associated with the managed system
filetype.machineSerial.dumpID .yyyymmddhhmmss	Dump file type, set to one of the following: “SYSDUMP” for a platform system dump “FSPDUMP” for a FipS Service Processor dump “BMCDUMP” for a BMC SP dump “SMADUMP” for a SMA dump “PWRDUMP” for a power subsystem dump “LOGDUMP” for a platform event log entry dump “RSCDUMP” for a platform resource dump These dumps do not contain any client-related information.

5 Appendix

5.1 IBM Server Address List

The following IP addresses are used by an HMC when it is configured to use Internet connectivity. All connections to these IP addresses use port 443 TCP.

Americas

- 129.42.160.48
- 129.42.160.49
- 207.25.252.200
- 207.25.252.204

Non-Americas

- 129.42.160.48
- 129.42.160.50
- 207.25.252.200
- 207.25.252.205

Note When configuring a firewall to allow an HMC to connect to these servers, only the IP addresses specific to the client's region are needed.

5.2 VPN Server Address List

These IP addresses are used by an HMC when it is configured to use Internet VPN connectivity. All connections use protocol ESP and port 500 UDP, or ports 500 and 4500 UDP when a Network Address Translation (NAT) firewall is being used.

VPN Servers for All Regions

- 129.42.160.16

- 207.25.252.196

5.3 Remote Service HMC Port List

When an inbound remote service connection to the HMC is active, only the following ports are allowed through the firewall for TCP and UDP.

22,23, 2125, 2300	These ports are used for access to the HMC.
9090, 9735, 9940, 30000-30009	These ports are used for Web-based System Manager.

5.4 Multiple HMCs

This section describes an environment with multiple HMCs configured with Outbound Connectivity.

5.4.1 Discovery and Inter-Console Communication

Consoles have the ability to discover and communicate with each other. A console discovers other consoles by using a UDP broadcast (port 9900) on the subnet of each configured network card. A console will also discover any other console managing the systems it manages. Communication with any discovered console is established using an SSL socket (port 9920) with Diffie-Hellman key exchange.

5.4.2 Call-Home Servers

A console automatically forwards its call-home requests to any discovered console that is configured as a call-home server. When more than one call-home server console is available, a brokering process involving inter-console communication selects a console to handle each request. Failures are automatically retried at remaining call-home server consoles.

IBM Corporation
Marketing Communications
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
January 2007.

This document was developed for products and/or services offered in the United States. IBM may not offer the products, features, or services discussed in this document in other countries.

The information may be subject to change without notice. Consult your local IBM business contact for information on the products, features and services available in your area.

All statements regarding IBM future directions and intent are subject to change or withdrawal without notice and represent goals and objectives only.

IBM hardware products are manufactured from new parts, or new and used parts. Regardless, our warranty terms apply.

This equipment is subject to FCC rules. It will comply with the appropriate FCC rules before final delivery to the buyer.

Information concerning non-IBM products was obtained from the suppliers of these products.

Questions on the capabilities of the non-IBM products should be addressed with the suppliers.

The IBM home page on the Internet can be found at http://www.ibm.com.

The IBM System p home page on the Internet can be found at http://www.ibm.com/systems/p.

The IBM System I home page on the Internet may be found at http://www.ibm.com/systems/i.

PSW03007-USEN-00