Resource MIB and other MIBs

Insight Manager to manage subagents delivered with HP's 2257. Agent X allows the MIB

EASE OF MANAGEMENT:

STATISTICS AND ACCOUNTING

MANAGEMENT SERVICES

This includes the record's message of each message sent and received. MIB (RFC 2789). It records a log connections, and other operational received, number of active total number of files sent and server session start and end time, logged into the server, client and FTP server includes: user names Monitoring MIB (RFC 2788). shooting. FTP accounting and also simplifies network manage-

Throughput statistics assists sys- tors can perform a rolling conver-

Complete reliable DHCP client and network performance

MS-DOS

NLM (Network Loadable Module) (v4.3 BSD)

Socket Library: (v4.3 BSD)

TCP/IP. Because no DECnet protocols are involved, there is no

DCE for OpenVMS

DEC C/V AX C Socket Library

Sendmail 8.11

PPPoE (PPP over Ethernet)

Secure File Transfer Protocol (SFTP)

FTP over TLS

Ephemeral Port Randomization

IETF: Internet Engineering Task Force

The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document. © Process Software, January 2009. TCPware and MultiNet are regis-

PROCESS SOFTWARE'S TECHNICAL SERVICES PROGRAM

about the Internet. OpenVMS users can

MultiNet provides several layers of security to protect against

Complete TCP/IP Networking Solution for HP VAX, Alpha, and Integrity Systems

MultiNet TCP/IP for OpenVMS provides reliability, functionality, and security for running mission-critical applications.

MultiNet for OpenVMS is a full suite of TCP/IP networking services and products for HP VAX, Alpha, and Integrity systems. This suite of TCP/IP products allows OpenVMS systems to participate as fully-functional TCP/IP hosts. Leveraging existing MultiNet for OpenVMS, the Alpha, or Integrity system to take advantage of expanded services and applications available on the Internet. OpenVMS users can easily exchange e-mail, as well as access and transfer files and data securely.

MultiNet is the preferred TCP/IP stack for systems allowing that are running mission critical applications. Process Software provides the most secure, reliable, and feature-rich TCP/IP stack for OpenVMS systems.

We have a proven track record of success within many Global 2000 companies and mission-critical applications using OpenVMS. MultiNet products include a zero-packet loss TCP/IP stack that keeps your OpenVMS system connected.

Process Software, a premier supplier of communications software solutions to mission critical environments. The company has been in business since 1984 and is a trusted name of over 5,000 organizations worldwide. MultiNet is also a Gold sponsor of Internet2 and the leader in OpenVMS 2000 and future 1000 campaigns. Process Software has earned a strong reputation for meeting the stringent reliability and performance requirements of enterprise networks.

Process Software’s Technical Services Program

provide the most secure, reliable, and feature-rich TCP/IP stack for OpenVMS systems.
functionality into their applica-
tions. An API is a set of rules and protocols that allows third parties to access and interact with an application's data and functions. APIs can be used to integrate different systems and applications, allowing developers to create new features and services.

In the context of security, APIs can be used to implement various security mechanisms, such as authentication, authorization, and encryption. For example, MultiNet's API allows system administrators to control access to local services, restrict Web surfing, or implement encryption algorithms to protect data in transit. APIs can also be used to automate routine tasks, such as system updates or monitoring, reducing the burden on system administrators.

However, APIs also introduce potential security risks, such as the risk of unauthorized access or data breaches. It is crucial to implement robust security measures, such as authentication and authorization mechanisms, to protect APIs from unauthorized access. Additionally, it is important to regularly update and patch APIs to address any vulnerabilities that may be exploited by attackers.

In conclusion, APIs are a powerful tool for integrating different systems and applications, but they also require careful consideration of security impacts. System administrators should implement robust security measures to protect APIs and reduce the risk of unauthorized access or data breaches.
Figure 1

**Secure File Transfer Protocol (SFTP), Secure Copy Protocol (SCP), and SSH Operation**

Secure File Transfer Protocol (SFTP) provides a reliable, secure mechanism for transferring files over a TCP/IP network. It is built on SSH (Secure Shell) and provides the same functionality as FTP (File Transfer Protocol) but with strong authentication and privacy guarantees. SFTP is a command-line tool and is compatible with Windows, UNIX, Linux, and Mac OS X environments.

Secure Copy Protocol (SCP) is a reliable, secure method of transferring files between two systems over a TCP/IP network. SCP uses the same cryptographic algorithms as SFTP and provides equivalent security features. SCP is primarily used in environments where high security is required, such as financial institutions and government agencies.

**SSH (Secure Shell)**

SSH is a protocol that provides secure remote login and secure shell services over an unsecured channel. This transport protocol is used to secure application-level communication. Systems can be connected using SSH to exchange data securely and maintain confidentiality and integrity of data exchanged.

**MultiNet’s SSH**

MultiNet offers SSH v1 and v2 interfaces, allowing users to access remote systems securely. SSH provides strong authentication, integrity, and confidentiality of data transmitted over the network. SSH is supported on various operating systems, including Windows, UNIX, Macintosh, Linux, and openVMS.

**MultiNet’s SSH Server and Client**

MultiNet’s SSH server and client provide flexible and secure access to remote systems. The server is configurable. An API is provided so that MultiNet can create and incorporate the SSH functionality into their application, which enables users to access remote systems securely.

**IP Security (IPSEC)**

IPSEC is a protocol that provides higher-level security mechanisms, such as tunneling, encryption, and integrity checks, at the network layer of the OSI model. It is useful for securing data exchange over public networks, protecting against Denial of Service (DoS) attacks, and ensuring data integrity.

**MultiNet’s Support for IPSEC**

MultiNet’s support for IPSEC includes Transport mode and Tunnel mode. It provides strong authentication for tunnels, message protection, and data confidentiality. IPSEC is supported on various platforms, including Windows, UNIX, Macintosh, Linux, and openVMS.

**New Feature Support on OpenVMS v5.5-2 or Later**

MultiNet’s support for OpenVMS v5.5-2 or later includes new features, such as client credential gathering and running standard commands (SCCM) after authentication.

**Dynamic DNS Support**

MultiNet offers Dynamic DNS (DDNS) support, which allows users to automatically update DNS records with their IP address changes. This is useful for dynamic IP addresses and is supported on both Windows and UNIX/Linux platforms.

**Telnet Printing**

Telnet printing is supported, allowing users to print to a remote printer using the same methods and operations as if the printer was locally located.

**Summary**

MultiNet’s SSH support provides secure remote login and secure shell services over an unsecured channel. SSH is supported on various operating systems, including Windows, UNIX, Macintosh, Linux, and openVMS. This transport protocol is used to secure application-level communication. Systems can be connected using SSH to exchange data securely and maintain confidentiality and integrity of data exchanged.

**RESTRICTIONS**

MultiNet offers new features and enhancements to its SSH functionality. These enhancements include support for multiple printers, enhanced security features, and improved user experience. MultiNet’s SSH server and client are flexible, supporting a wide range of applications and use cases. The server is configurable, allowing users to incorporate the SSH functionality into their application.
MULTIPLATFORM, MULTI-PROTOCOL, MULTISYSTEM

MultiNet offers SSH v1 and v2 (SCP) and Secure Copy (SFTP). MultiNet also imposes incoming access restrictions for services like FTP or TELNET. These restrictions can be made based on the information is coming from a legitimate source by using the DNS server via zone transfer or zone updates. MultiNet also allows you to remotely centralize administration of your VAX, Alpha, or VAX system. DHCP Safe-failover provides uninterrupted IP services using the same methods and protocols software and Cisco routers. IP addresses can be assigned to printers using the same method and operations as if the printer was located locally.

System administrators using print services should implement new features, without having to go to the expense or time to upgrade to the latest OpenSSH release. TCP/IP (Software for UNIX/Linux) does not support new functionality introduced in the latest major OpenSSH releases. Users are forced to upgrade to the newer version in order to use new features for Opennet and OpenSSH facilities.

Classless Inter-Domain Routing (CIDR): MultiNet’s DNS server is based on OpenDNS from Internet Systems Consortium (ISOC). MultiNet includes support for multiple views (BIND DNS, INMDN, incremental zone transfer, Dynamic DNS updates, DNSSEC), and IPv6, enhancement of the print service by integrating with the OpenVMS and the native network services. Dynamic DNS (DNSSEC) provides enhanced security when updates are made to resource records dynamically. INMDN assures large networks and backbone ports of connectivity to their network interface cards as well as increase transmission performance from the server.

MultiNet’s Paired Network Interface classifies support provides network visualization, reliability, and scalability without the use of additional systems.

The incoming/outgoing access restrictions for services like FTP or TELNET are configured based on whether the client is in a client class or class A. When packets pass between any compliant host, MultiNet also supports those that have used Kerberos for mutual authentication and generates the required key automatically (see Figure 2).

RESTRICTIONS: MultiNet’s Kerberos oneway NIC and that will be transmitted from the server to the client. Once a client and server have used Kerberos to prove their identity, all communications are automatically secure privacy, and data integrity. MultiNet runs with Kerberos on Windows, Macintosh, Linux, and VAX, Alpha, or Integrity systems. Dynamic DNS (DNSSEC) provides enhanced security when updates are made to resource records dynamically. INMDN assures large networks and backbone ports of connectivity to their network interface cards as well as increase transmission performance from the server.

The incoming/outgoing access restrictions for services like FTP or TELNET are configured based on whether the client is in a client class or class A. When packets pass between any compliant host, MultiNet also supports those that have used Kerberos for mutual authentication and generates the required key automatically (see Figure 2).

RESTRICTIONS: MultiNet’s Kerberos oneway NIC and that will be transmitted from the server to the client. Once a client and server have used Kerberos to prove their identity, all communications are automatically secure privacy, and data integrity. MultiNet runs with Kerberos on Windows, Macintosh, Linux, and VAX, Alpha, or Integrity systems. Dynamic DNS (DNSSEC) provides enhanced security when updates are made to resource records dynamically. INMDN assures large networks and backbone ports of connectivity to their network interface cards as well as increase transmission performance from the server.

The incoming/outgoing access restrictions for services like FTP or TELNET are configured based on whether the client is in a client class or class A. When packets pass between any compliant host, MultiNet also supports those that have used Kerberos for mutual authentication and generates the required key automatically (see Figure 2).

RESTRICTIONS: MultiNet’s Kerberos oneway NIC and that will be transmitted from the server to the client. Once a client and server have used Kerberos to prove their identity, all communications are automatically secure privacy, and data integrity. MultiNet runs with Kerberos on Windows, Macintosh, Linux, and VAX, Alpha, or Integrity systems. Dynamic DNS (DNSSEC) provides enhanced security when updates are made to resource records dynamically. INMDN assures large networks and backbone ports of connectivity to their network interface cards as well as increase transmission performance from the server.
MULTINET - FEATURES AT A GLANCE

**IP Stack**
- IPv6 support
- TCP/IP stack with RFC 1349
- TCP/IP stack for DECnet

**Security Services**
- SSH, SFTP
- FTP

**Printing Services**
- LPD (Line Printer Daemon)
- UCX $QIO Interface

**E-mail Services**
- IMAP, POP3
- SMTP

**Terminal Services**
- DECnet Applications over IP
- IP over DECnet Tunneling
- DECnet Applications over IP

**FTP Usage**
- Secure Copy Protocol (SCP) client and server
- FTP over TLS

**Accounting Reports**
- DHCP Server with Safe-failover
- DHCP Client

**Network Monitoring**
- Multinet
- Telnet

**MultiNet Advantages**
- Security communications
- Telnet, IMAP, and POP3 have been instrumented with IPS to detect unauthorized network access and block or prevent those activities.
- Increased reliability
- Secure communications
- Telnet, IMAP, and POP3 have been instrumented with IPS to detect unauthorized network access and block or prevent those activities.

**MULTINET - TCP/IP for OpenVMS**

**Complete TCP/IP Networking Solution for HP VAX, Alpha, and Integrity Systems**

**MULTINET TCP/IP for OpenVMS provides redundancy, functionality, and security for running mission-critical applications.**

**Multinet for OpenVMS is a full suite of TCP/IP solutions and services for HP VAX, Alpha, and Integrity Systems.**

**FTP OVER TLS:** FTP over TLS supports RFC 4217. TLS provides an encrypted channel that can be either self-signed or certified by a trusted authority. Services may be configurable to require secure data transfer. FTP over TLS requires an explicit request for encryption and server authentication.

**Internet Protection System:** (IPS) MultiNet's advanced security network architecture for malicious or unwanted behaviors. It is highly flexible and customizable. When an attack is detected, pre-configured rules are activated.

**Advanced Security:** MultiNet provides several layers of security to protect against unauthorized network access and intrusions.

Process Software
999 Concord Street
Franklin, MA 02038

Telephone: (508) 879-0042
Web: www.process.com
E-mail: info@process.com
MultiNet includes a wide choice of file services to access, transfer, and share files. The File System (NFS) client and server provides transparent and quick access to remote files and directories. The NFS server provides access to the OpenVMS file system. The NFS client requires the NFS client daemon (NFSd) support. The NFS client daemon supports long file names and a mixed case naming convention. The NFS server is required to run as a daemon and support long file names.

Process Software’s Technical Services Program has a well-deserved reputation for meeting the stringent reliability and performance requirements of mission critical environments. The company has been in business since 1984 and is fully committed to excellence in all its products and services. The company provides installation and training services on a wide range of products, including the latest in networking, distributed systems, and security. The company also provides customer support and technical assistance on a 24/7 basis.

The information contained in this document is subject to change without notice. Process Software assumes no responsibility for any errors that may appear in this document. © Process Software, January 2009.