TCPware

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

TCPware Advantages:

- *Secure communications with IPS, SSH, SFTP, and SCP servers and clients and FTP over TLS*
- *Investment protection with new feature support on OpenVMS v5.5-2 and higher*
- *Increase network performance and reliability with Paired Network Interface*
- *Complete, reliable DHCP solution: DHCP client and server with Safe-failover*
- *Ease of management with SMTP and FTP statistics and accounting reports*
- *Advance printing and troubleshooting with the IETF standards-based Internet Printing Protocol*
- *Improve performance and security with NFS v3 server*
- *Runs on VAX, Alpha, and Integrity systems*

TCPware TCP/IP for OpenVMS provides the proven security, functionality, dependability, and performance required for running mission-critical applications.

TCPware for OpenVMS is a full suite of TCP/IP applications and services for OpenVMS VAX, Alpha, or Integrity platforms. It enables OpenVMS systems to participate as fully functional TCP/IP hosts within an intranet and on the Internet. Leveraging existing OpenVMS resources, TCPware enables a VAX, Alpha, or Integrity system to take advantage of all the services and applications available on the Internet. OpenVMS users can easily exchange e-mail, as well as access and transfer files and data securely.

Process Software is the best choice for your OpenVMS TCP/IP requirements. Thousands of customers are using our products worldwide for their mission critical networks. Process Software products incorporate leading edge technologies and are backed with a dedicated customer support organization.

Advanced Security

TCPware provides several layers of security to protect against unauthorized network access and intruders from the Internet.

PROCESS™ SOFTWARE

Intrusion Prevention System (IPS): TCPware's IPS monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. TCPware SSH, FTP, SNMP, Telnet, IMAP, and POP3 have been instrumented with IPS to monitor traffic for malicious attacks. It is highly flexible and customizable. When an attack is detected, pre-configured rules will block an intruder's IP address from accessing their system, prevent an intruder from accessing a specific application, or both. The time period that the filter is in place is configurable. An API is provided so that TCPware customers can incorporate the IPS functionality into their applications.

Secure Shell v1 and v2 (SSH) Server and Client: SSH is a protocol that provides strong authentication and secure, encrypted communications over unsecured channels. It protects against a wide variety of potential security breaches such as spoofing, eavesdropping or hijacking of sessions, and man-in-the-middle attacks. System administrators can trust that user files, e-mails, and data will reach their destination securely. TCPware SSH server and client not only encrypts Telnet sessions, but also a wide variety of applications with its port forwarding feature including POP, SMTP, Oracle database connections and more. System administrators can choose which applications to encrypt based on their corporate security requirements, avoiding unnecessary network overhead.

SSH uses a host-based authentication exchange called Diffie-Hellman. Diffie-Hellman provides additional security by eliminating the need for exchanging private keys over the wire. It also allows users the advantage of continually authenticating throughout the entire session. Security is achieved through multiple levels of user authentication and strong encryption algorithms.

The TCPware SSH server and client are FIPs 140-2 Level 2 compliant.

They are also flexible, supporting a wide variety of third-party SSH servers and clients on OpenVMS, UNIX, Apple, Linux, and Windows platforms.

In addition, managing SSH authentication is simplified with single sign-on support. TCPware SSH works with existing PKI certificates and Kerberos infrastructure.

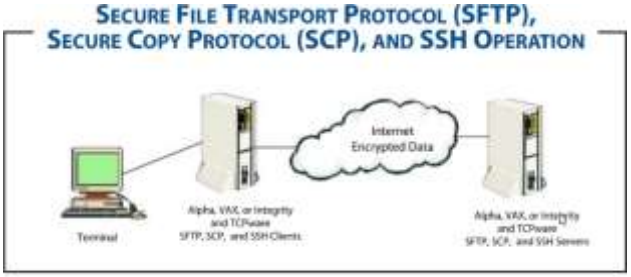

Figure 1

Secure File Transfer Protocol (SFTP) and Secure Copy Protocol (SCP): TCPware increases security with SFTP and SCP support. Both protocols allow SSH users to perform secure file transfers across an unsecured network. It provides system administrators with the ability to add, move, copy and delete files securely. SFTP and SCP utilize the SSH server and client as a basis for accomplishing this advanced level of security (see Figure 1).

Both SCP and SFTP files can be transferred as ASCII, BINARY, or in OpenVMS format when

implementing SSH file transfer protocol v4. Support for this protocol improves file transfer interoperability between different operating systems.

FTP Over TLS: FTP over TLS supports RFC 4217. TLS provides server authentication with keys that may be either self-signed or signed by a trusted authority. Servers may be configurable to require secure data transfers. FTP over TLS requires an explicit request for encryption and server authentication.

Incoming/Outgoing Access Restrictions: TCPware's access restrictions provide an additional method of security to the network. TCPware's outgoing access restrictions provide system administrators with security by controlling those applications local users can or cannot access (such as restricting Web surfing or access to services like FTP or Telnet). TCPware also imposes incoming restrictions on the remote hosts' access to local services.

Packet Filtering and Additional Security Layers: TCPware's packet filtering capability complements existing firewall security by providing an additional security layer on internal networks. It can prevent your site from receiving datagrams from certain networks or hosts. Datagrams can be filtered by protocol (IP, ICMP, UDP, or TCP), source and destination address, or source and destination port.

Network File System v3 (NFS): NFS client and server provide transparent and quick access to remote files and directories. TCPware includes a high performance NFS v3 server (RFC 1813). The NFS v3 server improves performance over the NFS v2 server by reducing the number of calls made between the client and server. File attributes are now returned during normal operations; therefore separate calls are no longer required. Other restrictions that have been eliminated in the NFS v3 server include the file storage size can exceed 2 gigabytes and data transfers can exceed 8 KB.

Security is enhanced with an access permission procedure. This procedure ensures that no unauthorized client can gain access to a server's file objects. The NFS v3 server is flexible, supporting many of the NFS v2 and v3 clients on the market today.

The NFS server also includes support for ODS-5. This feature allows for long file names and a mixed case naming convention.

DHCP Server: TCPware's DHCP server is based on ISC v3 code. Upgrading to DHCP v3 allows more granular control of the DHCP server with client classing and conditional behavior. Client classing provides system administrators with the ability to group users, based on their attributes such as MAC address or a client name. Different privileges can be assigned to these various groups of users. For example, a remote user may be assigned a shorter lease time of 2 hours versus a local user with an 8-hour lease time.

DHCP Safe-Failover: The TCPware DHCP server includes safe failover support, a protocol co-authored by Process Software and Cisco Systems. DHCP safe failover

provides uninterrupted IP services to clients during network or server failures so that they can reliably obtain IP addresses to connect to corporate resources without the need for a cluster. It increases the reliability and availability of DHCP services significantly.

DNS Server with Dynamic DNS: TCPware's DNS server is based on BIND v9. It includes support for multiple views (split DNS), DNSSEC, incremental zone transfer, Dynamic DNS (DDNS) updates, DNS notify, and enhanced standard conformance for over 25 RFCs. With split DNS, system administrators can create two zones for the same domain. One of the zones is used by internal network clients and the other zone is used by external network clients.

DNSSEC (RFC 2065) provides security when updates are made to the DNS server via zone transfer or DDNS. DNSSEC ensures that the information is coming from a legitimate source by using authentication.

Incremental zone transfer (RFC 1995) or IXFR improves the performance of a DNS environment. The name server (or DNS server) only transfers the changes in a zone, e.g., add or delete a record. Reducing the size and length of zone transfers is important where there are large zones (e.g., .com) or dynamic environments (e.g., DDNS) for DNS server efficiency. Dynamic DNS updates allow applications (such as DHCP) to modify resource records dynamically. This feature simplifies system administration management and saves time because the DNS server maintains an up-to-date record of the address space.

TCPware's DNS notify feature means that when zone changes occur on the primary server, it notifies the secondary servers, which can initiate immediately a zone transfer rather than having to wait for the polling interval to expire. Thus, zone changes propagate much faster through the servers.

TCPware's support for BIND provides granular control of which servers are allowed to do zone transfers, DDNS updates, queries, etc. Control is available on a zone-by-zone basis, not just on the entire server.

IP Stack

Paired Network Interface Support: Paired Network Interface support increases performance and reliability. It allows two or more network interface cards (NIC) with their own unique IP addresses to be connected to the same virtual cable in order to create network redundancy and optimize throughput. Any number of OpenVMS supported NIC types can be used including Ethernet, Token Ring, Fast Ethernet, FDDI, and ATM.

Paired Network Interface support provides network failover, creating network redundancy without adding a second system. If one NIC in the system fails, information will be transmitted from the second NIC (see Figure 2). Additionally, multiple NICs can be used to increase throughput if a data communications bottleneck is suspected from the server.

Areas where Paired Network Interface will improve connectivity include e-commerce applications where there are frequent database transactions, multimedia applications where there is high bandwidth consumption, and any applications where a

single server connection is causing delays for clients.

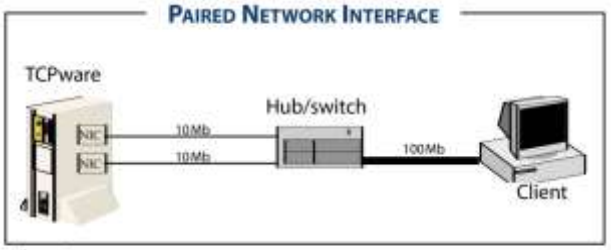

Figure 2 - *Dual 10Mb NICs improve throughput by utilizing bandwidth on a 100Mb Ethernet segment downstream from the server segment. The Paired Network Interface combines failover with an ability to use existing network interface cards as well as increase transmission performance from the server.*

New Feature Support on OpenVMS V5.5-2 and Later: TCPware offers new feature support on OpenVMS v5.5-2 or later. It provides users with the unique ability to implement new features, without having to go to the expense or time to upgrade to the latest OpenVMS release. TCP/IP Services for OpenVMS does not support new functionality unless users are running the latest major OpenVMS release. Users are forced to upgrade to the most current version in order to implement new TCP/IP Services for OpenVMS functionality.

DHCP Client: The DHCP client allows you to centralize administration of your OpenVMS server. A DHCP client is needed in order to receive IP addresses from the DHCP server. The DHCP client saves you time by enabling you to retrieve changes to the DHCP server automatically, versus having to assign IP addresses and DNS servers manually.

Router Failover: TCPware's unique router failover feature enables the configuration of backup default routers. If the default router in use is down, a backup router is automatically used to complete the communications without interruption.

NTP v4.2: TCPware includes support for Network Time Protocol (NTP) v4.2. NTP synchronizes the time of a computer client or server to another server or reference time source, such as a radio, satellite receiver, or modem.

GateD: Gateway Routing Daemon provides dynamic routing information to determine the best path to use between a source and destination host. It is more efficient than static routing because the system administrator does not have to update a host's or gateway's routing table manually. GateD determines the best route for a packet to travel by gathering and using various standard routing protocol information from OSPF (Open Shortest Path First), RIP2 (Routing Information Protocol), router discovery, and others.

CIDR: Classless Inter-Domain Router assures large organizations of connectivity to their entire network by allowing expansion of the available IP addresses. This can be critical given today's complex topologies, high traffic loads, and the explosive growth of the Internet. New scaling problems at an unprecedented rate have occurred, including exhaustion of Class B network addresses, back-bone routing overload, and exhaustion of IP network numbers. This feature implements CIDR RFC 1517, 1518, and 1519. Use of variable-length subnet masks with CIDR solves these problems by allowing for

supernetting and aggregating address assignments.

E-mail Services

SMTP Server: TCPware's SMTP server supports MIME encoded messages, letting users send files as base64-encoded MIME messages from OpenVMS Mail.

TCPware also includes a spam relay filter and an incoming e-mail spam filter. System administrators can create and maintain e-mail filter rules in a database with source/destination address combinations and specific header content.

IMAP4 Server: IMAP4 provides an alternative method of accessing messages from a mail server. IMAP4 lets a client e-mail program access messages stored on an OpenVMS server as if these messages were local. IMAP4 retains the message on the server, either in the inbox or in a folder that the user creates.

The advantage of retaining e-mail messages centrally (using IMAP4) is that if employees work from multiple locations using multiple computer systems (e.g., home or branch office), they have access to all their e-mail messages regardless of their location and systems used.

Complete Intranet and Internet File, Print, and Terminal Services

TCPware provides a wide choice of file services to access, transfer, and print networked data.

Internet Printing Protocol (IPP): IPP is an open standard protocol developed by the Printer Working Group (under IETF) for printing over the Internet. IPP provides enhancements over the existing commonly used LPD protocol including the ability for a user to print to a remote printer using the same methods and operations as if the printer was located locally.

System administrators using print protocols such as LPD have had to spend a significant amount of time administering printing tasks with limited troubleshooting capabilities. For example, a system administrator receives no information on why a print job fails. The TCPware IPP print symbiont provides a reason for a print job failure. This saves time in troubleshooting printing problems.

The TCPware IPP print symbiont provides standard commands for advanced printer functionality (e.g., double-sided printing) regardless of what printer is being used. No special programming or training is required by a system administrator. In addition, when using the TCPware IPP print symbiont, a user will not need to inquire about the functionality of a particular printer with a system administrator because this information is provided automatically.

Line Printer Daemon (LPD): Line Printer Daemon (LPD) print services are supported allowing UNIX- or OpenVMS-based hosts that are on a TCP/IP network to access print queues on OpenVMS systems. In addition,

users can print to printers connected to terminal servers.

Line Printing (LPR): Line Printing (LPR) is a feature that allows users the ability to log onto an OpenVMS system and access a printer connected to a UNIX-based workstation.

Terminal Services: TCPware supports a range of terminal types, including X terminals. In addition, access to IBM environments is made simpler with support for TN3270 and TN5250.

Management Services

Statistic and Accounting Reports: TCPware includes the ability to generate statistical and accounting reports on SMTP and FTP usage to assist with capacity planning, billing, and troubleshooting. FTP accounting and statistics are based on the Network Monitoring MIB (RFC 2788). Information that is collected on the FTP server includes: usernames logged into the server, client and server session start and end time, amount of data sent and received, total number of files sent and received, number of active connections, and other operational statistics.

SMTP accounting and statistics is based on the Mail Monitoring MIB (RFC 2789). It records a log of each message sent and received. This includes the record's message date, time, size, “from” and “to” strings. It also provides a count of detected loops.

Throughput statistics assists system administrators with troubleshooting by providing information on system performance. Information is available on the rate data was transmitted and received in bytes and packets per second.

Agent X: TCPware supports RFC 2257. Agent X allows the MIB subagents delivered with HP's Insight Manager to manage OpenVMS using TCPware. Host Resource MIB and other MIBs that ship with HP software can also be used.

Prerequisite Software

TCPware requires OpenVMS v5.5-2 or later on VAX systems, OpenVMS v6.2 or later on Alpha systems, or OpenVMS v8.2 or later on Integrity systems. Message Router v3.1 or later is required for Simple Mail Transfer Protocol (SMTP) to ALL-IN-1 gateway capability. To enable Kerberos v5 authentication in the SSH server, the OpenVMS Kerberos v5 product must be installed. This restricts support for Kerberos to OpenVMS Alpha v7.2-2 and higher.

Media

TCPware for OpenVMS is distributed on CD-ROM. It is also available for secure download.

TCPware Features at a Glance

IP Stack

DHCP Server with Safe-Failover
DHCP Client
Dynamic DNS (DDNS)
DNS BIND
New feature support for OpenVMS v5.5-2 or later
Paired Network Interface Support
GateD (RIP v2, OSPF, etc.)
CIDR
NTP
PPP
Path MTU Discovery
Router Failover

Management Services

SMTP and FTP statistics and Accounting Reports
Throughput Statistics
Agent X
SNMP Trap Program
Start/Stop Individual Services
Centralized FTP Logging
SNMP Reporting Subagent
TCP dump, ping, etc.

Supported application programming interfaces (APIs) including:

BSD Socket Library
DEC C/VAX C Socket Library
TCPware/SRI $QIO Interface
UCX $QIO Interface
ONC/RPC Interface
DECrpc
DCE for OpenVMS

Security services

Intrusion Prevention System (IPS)
Secure Shell Server and Client (SSH)
Secure Copy Protocol Server and Client (SCP)
FTP over TLS
Packet Filtering
Incoming Access Restrictions
Outgoing Access Restrictions
Token Authentication
Secure File Transfer Protocol Server and Client (SFTP)
SSH single sign-on with support for Kerberos and PKI certificates

Infrastructure

DECnet Phase IV over IP, DECnet Plus
PATHWORKS
IP over DECnet Tunneling

Applications

NFS v3 Server
NFS over TCP, UDP client/server
FTP
“R” Services
Telnet

E-mail services

SMTP
POP3
IMAP4
Spam Prevention

Printing services

IPP (Internet Printing Protocol)
LPD (Line Printer Daemon), LPR (Line printer) and printing terminal servers
Telnet/Stream Printing

About Process Software

Process Software is a premier supplier of infrastructure software solutions to mission critical environments. We deliver customer-centric and innovative IP-based technologies to our customers worldwide, and provide them with superior customer support and service.

Process Software's Technical Services Program

Process Software's Technical Services Program has a well-deserved reputation for excellence. Services include consulting, training, software maintenance, support, online resources, and 24-hour support - in short, everything you need to keep your Process Software products and your network operating at peak efficiency

Process Software
330 Cochituate Rd #922
Framingham, MA 01701

Telephone:
U.S./Canada (800) 722-7770
International (508) 879-6994

Web: www.process.com
E-mail: info@process.com

N-1003-61-NN-B