IPSec in the Solaris™ 9 Operating Environment

A Technical White Paper

Sun microsystems

Table of Contents

Chapter 1

Executive Summary

The Solaris™ Operating Environment (OE) is a leading provider of secure network computing capabilities. This lead is extended with the extension of the Internet Protocol Security (IPSec) capabilities in the Solaris 9 OE.

Keeping systems data secure — and this includes corporate and partner information — is of strategic importance in this age of connected business. IPSec, which provides highly configurable protection at the IP layer, can be a major advantage in protecting a business. Because the protection occurs at the IP layer, all types of Internet traffic can be protected, transparently to the applications and services that use the network.

The level and type of IPSec protection to be applied is both flexible and negotiable. Combining various types of authentication and encryption mechanisms with different policy rules, IPSec can protect all communications between two network nodes, specific types of traffic, a single application-specific session, or virtually any other situation. IPSec can be implemented incrementally, and may be used on part or all of the corporate intranet, extranet, as well as between remote users and branch offices.

Just as specific applications do not have to be IPSec-aware, users do not have to change the way they use the system. The network protection provided by IPSec is transparent. A network administrator can determine and enforce both network-wide and host-specific policies.

IPSec is a more comprehensive solution than another security capability that has been introduced in the Solaris 9 OE — Secure Shell. Secure Shell is a powerful security tool that can be implemented relatively easily in most user environments. Secure Shell is a lightweight application — easily deployed — that offers strong security for user sessions, enabling those users to control the client-side configuration. IPSec is a more flexible and pervasive solution, but it requires additional effort to implement and manage. It provides specific protection for systems, and the configuration is managed by codified policy that is set by administrators. IPSec is transparent to applications, and no changes are required to protect the network traffic associated with them. Properly implemented in the appropriate environment, each method offers strong security for remote and network computing tasks.

These two security technologies are compared in TABLE 1, below:

TABLE 1 A comparison of IPSec and Secure Shell technologies

Feature	**IPSec**	**Solaris 9 OE Secure Shell**
Ease of configuration and maintenance	More difficult	Less difficult
Centralized policy control	Yes	No
Transparent to applications	Yes	No
Transparent to users	Yes	Application commands, such as `rcp`, are similar (`scp`)
Network protections	Privacy, strong host-to-host authentication, VPN, integrity, automatic keying	Privacy, strong user and host authentication, session integrity
Secure X-Windows sessions	Yes	Yes

The Solaris OE has a strong legacy of promoting and providing standards-based technologies for IT solutions. The IPSec implementation in the Solaris OE is designed and built with adherence to Internet Engineering Task Force (IETF) standards. An additional benefit of Sun’s implementation of IPSec is that Solaris software includes application programming interfaces (APIs) that enable application-level specification of IPSec policies. This enables application developers to take full advantage of the additional security IPSec offers.

This paper contains a description of network threats, and an overview of how IPSec can provide protection against these threats. It includes a description of IPSec features, capabilities, and underlying technology. Information on key management capabilities, and a discussion on using IPSec in a virtual private network (VPN) environment, is also provided.

Chapter 2

Network Threats

Companies rely on network systems to run their operations and do businesses with customers, partners, and suppliers. The Internet can help organizations reach new markets, create a closer relationship with customers, partners, and suppliers, and improve overall productivity. Offsetting these benefits is the increasing threat of attacks, as well as misuse or compromise of systems and data. As enterprises rely more on the network for both internal and external relationships, the importance of security increases.

Yet organizations everywhere face increasing risk of security attacks, both from internal and external sources. According to the 2001 CSI/FBI Computer Crime and Security Survey:

- 91% of respondents detected employee abuse of Internet access privileges
- 85% reported security breaches within the last 12 months
- 76% reported that a likely source of attack would be disgruntled employees
- 40% detected system penetration from the outside
- 78% reported denial of service attacks
- 13% reported theft of transaction information (up from 8% in 2000)

Security threats may be categorized in a number of ways. The techniques listed below can be used to attack systems, affecting availability and reliability; or compromise data, resulting in loss of intellectual property.

Session Eavesdropping

With relatively simple equipment or software, it's possible for someone to eavesdrop on a user session, recording everything associated with it — keystrokes, data, and login information. The information is obtained without modification, and there is no transmission latency. Because it's difficult to know when this is happening, victims go on about their work, unaware that they are supplying information to an unknown attacker.

Password Theft

Many conventional network commands, such as `telnet`, `ftp`, and `rlogin`, send passwords in the clear to remote hosts as part of the login process. In these situations, login information can be read and used later for unauthorized access to computing resources. In addition, Trojan horse keystroke loggers, which are spread using computer virus technologies, can capture passwords and send them to unauthorized users. A more common and decidedly low-tech method is to steal passwords written on a piece of paper.

Exploiting a Trust Relationship

By masquerading as another system, it is possible for attackers to use ARP spoofing to exploit a trust relationship, gaining entry to another system. A trusted node listed in the `.rhosts` file can be attacked by sending it false hardware address information, convincing the node that packets from the attacking system are actually from a trusted system. Applications and utilities such as `rsh`, `rlogin`, and `rcp` check the IP address on incoming connections, and match the address with the one listed in the `.rhosts` file. This is inherently unsecure, and exposes the hosts listed in this file to attack.

Information Exposure

Information travelling around the network is essentially unprotected. Without proper security procedures, such as authentication and encryption, users cannot be sure who is reading their data. It is critical to segment and protect information from various sources, such as data from partners and suppliers.

Host Spoofing

When one host masquerades as another machine, it attempts to fool systems that are trying to access it as the original. The normal flow of data is disrupted, resulting in data being sent to the wrong system, or altered data being sent from the spoofing host to other systems. The results may be significant. Users can inadvertently send name, password, or credit card information, orders may be misdirected, or e-mail or other data routed to the wrong host.

Session Hijacking

TCP session hijacking occurs when someone takes over a TCP session between two machines. This can happen when an unauthorized user redirects the TCP stream through another machine, bypassing the protection offered by simple login, one-time password, or ticketing authentication systems such as Kerberos. Since most authentication occurs only at the start of a TCP session, this allows the hacker to gain access to a machine. TCP connections are vulnerable to anyone with a TCP packet sniffer and generator located on the path followed by the connection.

Unprotected Network Services

Many network services — such as LDAP, NFS, `lpd`, and `syslog` — are unprotected and must be secured through cumbersome configurations. For example, maintaining the integrity of syslog traffic is essential to maintaining accurate system log files. If securing these essential services is too complex a task, it can lead to misconfiguration, leaving them open to attack.

Replay Attacks

A replay attack is when someone obtains a copy of unauthenticated packets, transmitting them to the intended destination later. The receipt of this duplicate authenticated packet may disrupt service in some way. For example, the attacker may resend packets containing the “`rm -rf /`” command.

Chapter 3

IPSec Protection — Overview

IPSec is a network-level protocol for strong pervasive security. It can provide privacy, block a variety of threats, and control host access for network traffic through standards-based encryption and authentication mechanisms.

Because IPSec encrypts and authenticates at the IP level — below the transport layer — it is transparent to all network applications such as e-mail, file transfer, Web access, and so on. Because IPSec is transparent to end-users, there is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keys when users leave the organization.

IPSec can also provide security for individual users. This is especially useful for off-site employees and remote offices. Secure communication links over the Internet can be established using
virtual private networks (VPNs).

At the core of IPSec security are two network packet protocols, which facilitate a wide range of security options:

- *Authentication Header (AH):* A new IP header which provides strong integrity, partial sequence integrity (replay protection), and data authentication to IP datagrams. AH is inserted between the IP header and the transport header. The transport header can be TCP, UDP, ICMP, or another IP header when tunnels are being used. AH does not protect against eavesdropping, and adversaries can still see data protected with it.

- *Encapsulating Security Payload (ESP) Header:* Provides data confidentiality (encryption) and traffic analysis protection. The latter is a measure of protection against an eavesdropper who is trying to determine the identities, frequencies, and volume of traffic between specific entities. ESP headers also provide some of the same protections offered by AH, including connectionless integrity, data origin authentication, and replay protection. An ESP header's authentication services are optional.

ESP and AH can be used together on the same datagram without redundancy. ESP encapsulates its data, so it only protects the data that follows its beginning in the datagram. In a TCP packet, ESP encapsulates only the TCP header and its data. If the packet is an IP-in-IP datagram, ESP protects the inner IP datagram. Per-socket policy allows self-encapsulation, so ESP can encapsulate IP options when necessary. Unlike AH, ESP allows multiple kinds of datagram protection, because using only a single form may make the datagram vulnerable. For example, if ESP is used to provide confidentiality only, the datagram is still vulnerable to replay and cut-and-paste attacks. Similarly, if ESP protects only integrity and does not fully protect against eavesdropping, it could provide weaker protection than AH.

The term "tunnel mode" is used to describe a situation when the entire datagram is inside the protection of IPSec headers, but the outer IP header is unprotected. Typically, the outer IP header has a different source and destination addresses than the inner (protected) IP header. The original addresses are restored when the destination host decrypts the packet. Tunnel mode is usually performed in ESP.

"Transport mode" is used to describe datagrams where the original source and destination addresses remain unaltered — only the data portion (payload) is encrypted. This is typically used behind a firewall or on a private LAN If the situation warrants transport mode. Throughput may be increased, because there is less processing than with tunnel mode.

The following sections provide more information on the functionality and capabilities of the Solaris 9 OE implementation of IPSec.

Security Associations

IPSec is able to differentiate between the security services it offers to various types of data traffic by the use of security association (SA). An SA is an agreement between communicating peers on factors such as the IPSec protocol, mode of operation of the protocols (tunnel or transport mode), cryptographic algorithms and keys, key lifetime, and policy statements. SAs are unidirectional — separate SAs are required for inbound and outbound traffic.

Using SAs, the granularities of protection may vary broadly. A single SA can protect all communication between two hosts or networks; just specific types of traffic; a single application-specific session;, or provide other levels of protection. The level and type of IPSec protection to be applied, as well as the key strength that affords this protection, are both flexible and negotiable.

Automatic Keying

SAs are negotiated between communicating peers using the Internet Key Exchange (IK). The Solaris 9 OE implementation of IPSec includes an IKE mechanism that enables the on-demand negotiation of keys for SAs. This facilitates the use of keys in a large distributed environment with an evolving configuration. Smaller systems may want to use manual key management, where the system administrator manually configures each system with the required keys.

The IKE protocol is used to negotiate the cryptographic algorithm choices to be used by AH and ESP, and put in place the necessary keys that are required. IKE also performs key management for the Solaris 9 OE IPSec.

Private Network Communication

IPSec implementations may be configured to encrypt network traffic to help ensure communication privacy. IPSec offers flexibility in how it is deployed — different encryption algorithms can be used between defined hosts or services, as specified in the SAs. Solaris 9 IPSec may use the following encryption mechanisms:

- *Data Encryption Standard (DES):* Uses Cipher-Block Chaining (CBC) per RFC 2405. It is effectively a 56-bit key length (64-bit key, of which there are eight parity bits), with a block size of 64 bits.
- *Triple DES (3DES):* Uses CBC per RFC 2451. 3DES is the application of DES three times using three different keys, which roughly doubles the effective key strength of DES. The key size is 192 bits, with a 64-bit block size.
- *Advanced Encryption Standard (AES):* Uses CBC per RFC 2451. The key size can be configured to 128, 192, or 256 bits.The key length affects the number of rounds performed per cipher block, and therefore affects the speed of the algorithm. The block size is 128 bits.
- *Blowfish:* Uses CBC per RFC 2451. The key size varies from 32 to 448 bits. Keys are encoded internally as 448-bit quantities. Smaller key sizes will repeat its pattern until 448 bits are reached. The block size is 64 bits.

Virtual Private Networks (VPNs)

Solaris 9 IPSec uses encryption in a feature called tunneling that is used to hide actual source and destination addresses. Tunneling mode provides traffic analysis protection. This is a useful feature when using a public network, such as the Internet, as a medium for a VPN, because information such as source and destination IP addresses is hidden. Tunneling mode can provide protection for multiple hosts on a network.

In tunneling mode, packet header information and data are encapsulated in new IP packets. When the source encrypts a packet, it replaces the packet's source address with the tunnel address, and replaces the packet's destination address with the tunnel address. When the destination decrypts the packets, the original addresses are restored. More information on VPNs is included in the next section.

Strong Host Authentication

IPSec capabilities in the Solaris OE feature strong host authentication capabilities to ensure hosts and other network identities are verified. Standards-based authentication mechanisms provide superior interoperability among all components, both internal and external to the enterprise.

Authentication algorithms work by producing a digest or integrity checksum value based on the data and a key. IPSec in the Solaris OE uses two authentication mechanisms:

- *HMAC-MD5:* Utilizes the MD5 message-digest algorithm and HMAC technique documented in RFC 2104. It uses a 128-bit key and a 96-bit digest (truncated from 128 bits).
- *HMAC-SHA-1:* Utilizes the SHA-1 hash algorithm and HMAC technique set forth in RFC 2104. It is more secure than HMAC-MD5, using a 160-bit key and a 96-bit digest (truncated from 160 bits).

Communication Integrity

IPSec in the Solaris OE provides capabilities that can prevent alteration of network traffic while in transit. This helps ensure that the traffic is received as it was sent: in order and with no duplication. Note that nothing is added or deleted from the session traffic.

Integrity is verified using a Message Authentication Code (MAC). The MAC calculation takes place over the entire enclosed datagram plus the AH. When the IP packet is received at its destination, the same calculation is performed using the same key. If the values are the same, then the packet is deemed authentic.

MAC values are also used to help prevent replay attacks.

Protected Communications

IPSec protects all IP traffic, including TCP, UDP, and ICMP protocols. Because IPSec protection takes place at the IP layer, all types of Internet traffic are protected. This occurs transparently to the applications and services that use the network.

Application Protection

IPSec in Solaris 9 OE can protect applications and services. For example, for a host that provides Web services, the SA can be configured to reject all packets except those which are Web client requests. In the same way, a host running a human resources database can be configured to accept traffic only from a predefined series of IP addresses, and with a more rigorous authentication mechanism. If the data on this application is considered sensitive, all traffic can be encrypted — even though it's on a local LAN. IPSec offers significant flexibility in how security capabilities are configured and deployed throughout the organization — and beyond.

IPv4/IPv6 Protocols

IPSec supports both the IPv4 and IPv6 protocols, while IKE supports IPv4. Although IPSec is a mandatory part of IPv6, it can provide protection for datagrams in both IPv4 and IPv6 networks. For example, IPv6-in-IPv4 tunnels allow IPv6 packets to be encapsulated within IPv4 packets.

As hosts and routers are upgraded to support IPv6, they must be able to interoperate over the network with the nodes (hosts and routers) that support only IPv4. In the Solaris 9 OE, tools are provided to help users transition from IPv4 to IPv6. RFC 1933 also provides detailed solutions to transition issues. Additional information is available in System Administration Guide: IP Services.

Chapter 4

Virtual Private Networks (VPNs)

VPNs represent a way to securely communicate between two or more places that are connected by a public network. All traffic between nodes on the VPN is encrypted, which excludes other nodes on the public network from listening. The facilities comprising IPSec — authentication, encryption, policy enforcement — make it ideal for setting up VPNs that connect remote offices and mobile users, or isolate internal networks and resources.

Protecting Remote Sites

VPNs are a cost-effective way to connect remote sites with headquarters IT resources, such as business-critical applications. Rather than using expensive dedicated communication lines from telecom providers, VPNs enable secure communication over the Internet, using relatively inexpensive hardware and software components. VPNs can leverage the flexibility offered by the Solaris IPSec environment, and they may be configured to address a variety of security options.

Depending on the security requirements, VPNs can require more than a security gateway (firewall or other access point on the network that controls access). Firewalls typically authorize traffic, but lack a full complement of authentication and security policy capabilities found in IPSec.

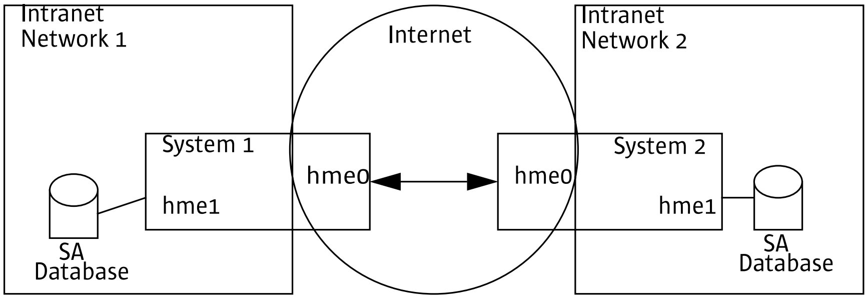

Figure 4-1: How a branch office connects to corporate headquarters using a VPN

A typical scenario would use end-to-end authentication and encryption. This offers a high degree of privacy for data traffic, with minimal likelihood that spoofing can occur.

This scenario shown in Figure 1 describes how a branch office might connect to corporate headquarters:

- The headquarters (Network 1) host negotiates an SA with the branch office host
- (Network 2).
  - SA specifies the security services required (for example, using AH or ESP packet headers), mode of operation of these services, and required authentication and encryption algorithms.
  - IKE protocol generates and puts in place the necessary authentication keys on the communicating hosts.
- Packets traveling between each host are compared against the destination security policy database at the security gateway to see if they can be accepted.
- If they are accepted, the security gateway will consult the SA database to determine the appropriate SA destination.
  - The packet is authenticated using the algorithm specified by SA.
- If the authentication succeeds, the packet is forwarded to the intended host.
- When the destination host receives the packet, it verifies that the SA is applicable to the packet by consulting the SA database.
  - The packet is authenticated to ensure it has not been modified in transit.
- If authentication succeeds, the destination hosts accepts the packet and processes it based on the negotiated SA for the traffic.

Protecting Mobile Users

It can be difficult to enable secure communications for mobile users. IPSec capabilities in the Solaris OE can offer a solution for securing ad hoc connections from outside the firewall.

The Public Key Infrastructure (PKI) provides the most secure solution. Clients are issued digital certificates, and the security gateways on the corporate network can be configured to give access only to clients with valid certificates issued by a recognized CA.

Isolating and Protecting Network Resources

Solaris IPSec can be used to isolate and protect network resources. For example, a Web server can be secured by using IPSec to check all incoming traffic except Web client requests and DNS client requests from this Web server. All other traffic — such as management traffic — can be required to use IPSec encryption and authentication as specified in the SA. In this way, the Web server is available for use by a broader audience, but is protected from inadvertent or intentional misuse.

This same concept may be applied to other critical aspects of an organization's IT infrastructure. Internal networks can be protected to varying degrees. Highly secure VPNs protect both access and traffic, effectively making them "invisible" to all unauthorized users. Less secure measures either encrypt traffic or require strong authentication. The IPSec protocols offer great latitude in how they are applied. For example, a network host may require one set of authentication procedures when accessed from an internal LAN, while a different set of procedures may be required when a user requests access from a remote office. The SA may provide unencrypted communication to users inside the corporate firewall, and encrypt all traffic to users outside the firewall. This occurs transparently to users and applications.

Chapter 5

End Systems

Using the IPSec implementation in the Solaris 9 OE offers platform-based security solutions for enterprise IT environments. Beyond VPN functionality, IPSec provides fine-grain protection that may be used throughout the network. Below are sample scenarios that can be considered for many organizations.

Protecting Individual Services

IPSec provides protection for specific services, without imposing overhead on all network traffic. Confidentiality and integrity protection can be used to protect a specific service. For example, an organization's security policy may require that syslog traffic be authenticated, in order to maintain accurate logs. IPSec can provide protection to this UDP service only — but not all traffic, which would impact system capacity and performance.

Simple Packet Filtering

The IPSec policy file can be configured to block traffic to services that users or hosts are not using, or deny traffic from specific hosts. IPSec is not a firewall — for example, it does not perform stateful packet inspection or proxy services. IPSec does enable access control at the host level. Specific rules may be applied to both incoming and outgoing traffic flows. These rules can permit and deny access, and apply specific authentication or encryption requirements. Traffic destined for named ports can also be allowed to bypass any rules.

Hardened Systems

The Solaris Security Toolkit provides a mechanism to minimize, harden, and secure Solaris OE systems. With the IPSec implementation in the Solaris 9 OE, administrators can more easily harden the network layer in addition to the operating environment. Web servers, Solaris management servers, and other business-critical servers are all prime candidates for using IPSec to provide maximum security.

Management Networks

Many management subsystems reside on separate networks. Using IPSec, administrators can set up a VPN for their management and administrative needs, without the need for deploying additional hardware. IPSec enables administrators to more effectively manage multiple servers.

Backup Networks

Backup networks typically are used for performance reasons — to ensure that maintenance traffic does not overwhelm the production network. IPSec confidentiality and integrity protocols can be enabled on these networks, helping to ensure that this traffic, which contains critical and confidential data, is unseen and unmodified.

Storage Networks

IPSec is typically used in storage networks. If data protection is implemented, it is done with secure RPC, which may be difficult to use. IPSec is well-suited for this type of network. It can be used to provide protection at the host level, without the requirement for user-level authentication.

Key Management

Key management in the Solaris 9 OE is performed using the capabilities available in the IKE mechanism. IKE negotiates between IPSec SAs, authenticating users and services, and determining what keys are needed to meet specific SA policy rules. This negotiation happens automatically and without costly manual preconfiguration.

When the IKE daemon discovers a remote host’s public encryption key, the local system can then encrypt messages destined for the remote host whose public key it has discovered.

The IKE daemon uses random seeds for keys from the pseudo random number generator (PRNG) functions provided by the Solaris OE. IKE provides Perfect Forward Secrecy (PFS). This means that the keys that protect data transmission are not used to derive additional keys, and seeds used to create data transmission keys are not reused.

IKE uses the following components and capabilities:

Managing Host Keys

Automated key management in IPSec is performed by two protocols, referred to as ISAKMP/Oakley:

- *Internet Security Association and Key Management Protocol (ISAKMP):* Provides a framework for Internet key management, including payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

- *Oakley Key Determination Protocol:* A key exchange protocol based on the Diffie-Hellman algorithm, with added security. By itself, Diffie-Hellman does not authenticate the two entities that are exchanging keys — so the Oakley mechanism includes authentication.

Public Key Infrastructure (PKI)

PKI is made up of the policies and components needed to create, distribute, revoke, and otherwise manage X.509 digital certificates. It is a system for publishing the public keys used in public key cryptography. PKI enables users to interact with other users and applications, obtain and verify identities and keys, and register with trusted third parties.

PKI includes the following components:

- *Certificate Authority (CA):* The system that issues and revokes certificates for a set of subjects, with responsibility for their authenticity. Before signing and issuing certificates, CA tracks its status. For example, certificates carry expiration dates, and CA revokes them when they expire.
- *Registration Authority (RA):* Verifies identity and registration information.
- *Public Key Certificate Directory:* Stores the public key certificate information in a central location.
- *Certification Revocation List (CRL):* A directory for listing certificates that have been revoked. CRL is created by CA, listing the serial numbers that have been revoked during their validity periods, indicating they should no longer be trusted. For example, if an authorization expires, a certificate is compromised, or there is a fault in binding the certificate to the holder, they are revoked and placed in the CRL.
- *Repository:* A database where the certificates and CRLs are stored.

In addition, PKI describes the management protocols used for CA functions. These protocols include PKIX Certificate Management Protocol (CMP), message formats such as Certificate Management Message Format (CMMF), and Public Key Cryptography Standards (PKCS).

PKI also includes policies and guidelines, including rules governing certificate usage, technical and administrative security controls, CA contractual requirements, and subscriber enrollment and termination processes.

Creating And Distributing Keys

If IKE successfully negotiates a connection between two entities, keys are created and exchanged using the Diffie-Hellman algorithm. The two entities exchange their public keys, combining them with their respective secret keys. The results of these two computations will be identical — and the two entities have used a public network to securely compute a shared secret value. This works because the two parties possess a secret key known only to them. This shared secret, along with other information, is plugged into a keyed hash algorithm. The output of the hash is used as a secret key, which can be used to encrypt communications between them.

A new feature of the Solaris 9 OE is a pseudo random number generator. Cryptographic algorithms and protocols require a source of random bits — entropy. An entropy collection is a pool of random bytes that can be used for cryptographic operations. /dev/random is a source for high-quality random bytes generated by a kernel PRNG. /dev/random provides a constantly filled entropy pool. Encryption facilities within IPSec draw from this pool, without pausing, and use the byte strings as input for their own random number generation systems. This assures high-quality random byte strings with virtually no impact on performance.

Chapter 6

Security Policy Considerations

Standard Solaris 9 OE software can now be used to protect traffic that extends beyond the intranet. This has a number of advantages, including the ability to more comprehensively and uniformly monitor and administer security throughout the IT infrastructure. This also minimizes costs and training, because fewer third-party products are required. When shifting more of the security burden to the Solaris environment, a number of policy issues should be considered.

Specific Policy Statements

With Solaris OE platforms used as network routers, IT staff needs to take another look at their network traffic policies. For example, it may be prudent to incorporate a high-level policy objective that states that, where possible, traffic should be encrypted to maintain confidentiality for all sessions extending beyond the intranet.

Managing Secure Networks/VPNS

As outlined earlier in this document, IPSec can be used to effectively set up VPNs, providing secure, point-to-point communication over public networks. VPNs are used to communicate with remote sites over the Internet. IT staff will want to consider the way they manage Solaris systems located at the border of the internal network. These systems are no longer part of the firewall, but instead part of the operating environment. Other precautions include:

- IT administrators should also take care of how they manage the installation of both ends of a VPN. The initial key exchange must be carefully conducted to avoid disclosing it to a public network.

- Care should be taken with the `/etc/inet/IPSecinit.conf, /etc/inet/secret/IPSeckeys`, and `/etc/inet/secret/IPSeckeys files as` well as files contained in the `/etc/inet/secret/ike.privatekeys` directory. If these files are exposed, an adversary can modify the data contained in the file, and even make changes to the configured policy or use the key information to snoop network sessions.
- Be cautious when using the `IPSecconf(1m)`, `IPSeckey(1m), ikeadm(1m)`, and `ikecert(1m)`commands. The safest mode of operation is from a console or other direct-connected TTY (TeleTyper).

Service Protection Requirements

Security policies may need to be updated on a service-by-service basis to take advantage of the fine-grain control offered by IPSec. Network architects and security officers may want to define what levels of protection each service should have. For example, a network security policy may state that http traffic should not fall under IPSec control, but all database traffic should be protected with confidentiality, integrity, and authorization.

Minimum Safe Encryption Requirements

IPSec offers flexibility in the level of encryption used to help assure confidentiality. If the encryption methods are too weak, the data may not be secure. Also, some algorithms require a higher level of computation that can impact system performance. For example, DES is less secure and slightly slower than newer algorithms, such as AES or Blowfish. AES offers greater protection and requires less processing power.

Security policies should state the minimum level of protection required for each service, to help administrators in the trade off between protection and performance. For example, a policy may state that all business-critical information must use 3DES or higher.

Legal Requirements

Note that the use of encryption may be governed by national or other laws. Administrators should verify that they are acting in compliance with any such laws before installing and configuring IPSec encryption.

The IPSec implementation in the Solaris 9 OE can use X.509 digital certificates. These are virtually tamper-evident digital receipts based on the PKCS#7 standard for signed data for "nonrepudiation." Nonrepudiation means ensuring that data cannot be renounced or a transaction denied. It is a result of using public key cryptography — because it can be proven that only the owner associated with a public key could have signed a document or approved a transaction. While this is an emerging concept in legal case law, nonrepudiation is the basis for building trust in e-commerce transactions.

Chapter 7

Conclusion

As the network has become an integral part of business operations — connecting employees, customers, suppliers, and partners — there is a compelling need for an operating environment that provides strong, flexible security capabilities. Administrators and developers need to be able to design and configure network resources to match the requirements demanded by each situation, and the security capabilities should enable or complement the solution. IPSec protects assets and network traffic with a number of mechanisms and protocols.

The IPSec implementation in the Solaris 9 OE offers:

- End-to-end communication security with transport and tunnel modes
- Automatic keying, which eases deployment and management issues
- Transparency to both users and applications

While IPSec can be used at virtually any point throughout the intranet, it can also be used to securely connect remote sites over the Internet. The combination of tunneling, strong authentication, and automatic keying means that IPSec is an ideal way to securely connect the intranet and remote sites.

While deploying IPSec is a significant task, it may be accomplished incrementally. IPSec can be configured to different levels of security protection around the network, providing the appropriate balance between security and performance. Network architects and system administrators should carefully consider policy issues before any roll out, as this can have a significant impact on resources required and user acceptance.

IPSec is a powerful mechanism that can be used to protect information and control access to network and IT resources. As part of the Solaris 9 OE, it offers an integrated, end-to-end security solution.

Please
Recycle

Adobe PostScript™

Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, CA 94303-4900 USA **Phone** 800 786-7638 or +1 512 434-1577 **Web** sun.com

We make the net work.

Sun Worldwide Sales Offices: Africa (North, West and Central) +33-13-067-4680, Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India–Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand–Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China–Beijing +86-10-6803-5588; Chengdu +86-28-619-9333; Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland–German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800

5/02 FE1810-0