QuickSec Toolkit for Access Networks

Security for Edge and Access Applications

Addresses all practical IPSec layer problems regarding dynamic addressing and configuration, integration to existing Authentication Authorization Accounting infrastructure, support for legacy tunneling technologies, NAT issues, and the need for multilayer stateful inspection TCP/IP firewalling and attack prevention.

There is an increasing number of different access network technologies consisting of both wireline and wireless. These technologies share a common concern relating to security in terms of privacy and access control. SafeNet QuickSec™ Toolkit for Access Networks is designed for developers who are implementing security technology on edge and access devices.

SafeNet QuickSec Toolkit for Access Networks addresses all practical IPSec layer problems found in access network applications regarding dynamic addressing & configuration, integration to existing AAA (Authentication Authorization Accounting) infrastructure, support for legacy tunneling technologies, NAT issues, and the need for multilayer stateful inspection TCP/IP firewalling and attack prevention.

SafeNet’s experienced technical support team and professional services group are available to assist OEM’s/ODM’s during the implementation stage.

Firewall

Today protection against attacks is a mandatory feature in gateway appliances that connect LANs to the Internet. Incoming traffic needs to be inspected on multiple layers to detect and prevent various attacks and probes ranging from port scanning to known exploits for applications.

IPSec—Internet Engineering Task Force (IETF) has endorsed vendor independent network layer protocol for implementing end-to-end security. IPSec is an application and media independent layer for bringing security to heterogeneous networks.

Internet Key Exchange (IKE)—Session management and authentication protocol of choice for IPSec data layer. SafeNet’s IKE implementation is among the first to introduce support for the latest IETF standards.

X.509 PKI Client Functionality—X.509 Public Key Infrastructures provide a scalable solution for managing authentication in networks with thousands of devices, such as centrally managed corporate infrastructure with remote clients, or managed gateways in residential access networks.
Technical Specifications

IPSec Support
- AH and ESP encapsulations
- Tunnel & transport mode operation
- SA bundles
- 64-bit sequence numbers in ESP
- Path MTU discovery
- AES counter mode

IKE Support
- Main Mode and Aggressive Mode for peer authentication
- Quick Mode for IPSec Security Association establishment
- Preshared keys and X.509 certificates

X.509 PKI Client Functionality
- Certificate chain validation
- Revocation status checking using CRLs (Certificate Revocation Lists)
- OCSP (Online Certificate Status Protocol)
- Certificate enrollment protocols
- CMP v2
- SCEP
- Command line tools for encoding end entity and CA certificates and CRLs

Remote Access Support
- L2TP
- User identity-based firewall policy
- IKE Configuration Mode / XAUTH
- NAT
- NAT Traversal
- RADIUS client

Stateful Inspection Firewall
- Detection and avoidance of common TCP/IP attacks (IDS/IPS)
- Application Layer Gateways
- FTP, SIP, DNS, CIFS, NetBios over TCP, HTTP, and Sun RPC

Platform Support
- Generic Linux, MontaVista Linux, VxWorks, NetBSD, Nucleus, Solaris
- Portable to proprietary environments by writing code to the well-defined porting APIs

Cryptographic Processing
- Hardware-based encryption and decryption
- Advanced encryption standards
- High-performance encryption engines

Secure File Access
- Secure key management
- Access control lists
- Encryption of data at rest and in transit

Secure Network Interconnection
- IPSec over IPv4 and IPv6
- L2TP over IPv4 and IPv6
- GRE over IPv4

Secure Remote Access
- L2TP/IPSec
- PPTP
- PowerIP

Secure Web Access
- SSL/TLS
- Secure Sockets Layer
- Transport Layer Security

Secure Email Access
- S/MIME
- PGP
- Secure MIME

Secure Storage Access
- Secure file systems
- Secure data backup
- Secure data archiving

Secure Network Administration
- Secure administration protocols
- Secure configuration management
- Secure system updates

Secure Application Access
- Secure application protocols
- Secure application gateways
- Secure application firewalls

Secure Network Services
- Secure network services
- Secure network devices
- Secure network appliances