Layer 2 Encryption vs. Layer 3 Encryption
What is the right choice for my network?

Layer 2 Encryption Overview

The term “Layer 2” refers to the Data Link Layer of the protocol stack defined by the Open System Interconnection (OSI) model for data communications. Layer 2 establishes the physical connection between the local telecommunications device and the remote destination and defines the Data Frame as the physical transmission medium between nodes.

Layer 2 is primarily used for high-speed/high-data throughput point-to-point applications between telecommunication facilities. In order to achieve these high-speeds, hardware encryption is predominantly used. Encryption at this level encapsulates any Layer 2 protocol crossing the link, unlike Layer 3 where only IP packets are encrypted. For this reason, Layer 2 encryption is much more flexible for point-to-point applications where routing is not a consideration. Layer 2 encryption also provides platform independence because client systems will not require special software or hardware to manage routing decisions.

Virtual Private Network (VPN) is the term commonly used to describe the capability to segregate private traffic on a publicly shared network infrastructure. While at Level 3 this capability is commonly secured through the use of IP Security (IPSec), at the Layer 2 level, it is commonly provided by Asynchronous Transfer Mode (ATM) and Frame Relay encryption; or simple bulk encryption for point-to-point connections. While the bulk of the VPN market is focused on tunneling and encryption, this works at Layer 3 and thus is subject to the configuration overheads associated with routing decisions.

Enterprise organization most often purchase Layer 2 services such as ATM, Frame Relay, and SONET/SDH from Service Providers (SPs) such as AT&T, Sprint, or Regional Bell Operating Companies such as Verizon. In some cases, large organizations lease fiber or private line directly from the SP and purchase their own SONET/SDH or ATM equipment. Customers with infrastructures characteristic of the above are likely candidates for a Layer 2 encryption solution.

Characteristics of Layer 2 Encryption

Layer 2 encryption is characterized by the fact that it creates the least latency and overhead drain on a network over any other encryption alternative. Additional characteristics include ease of deployment and management once installed. Layer 2 encryption devices are commonly referred to as “bump-in-the-wire” solutions as they require little or no configuration and maintenance once deployed. They are best suited for point-to-point applications connecting networks to networks in a static configuration.

Encryption solutions for Layer 2 are commonly used from 256K speeds up to 1 Gbps or higher with fiber connections. Typical applications of Layer 2 encryption at the enterprise level include data center connectivity to branch sites. Applications include point-to-point connections between sites where, because of the nature of the traffic, latencies cannot be tolerate, and where because of the nature of the operation, a simplified solution with little or no configuration and maintenance is desired for deployment.

Advantages of Layer 2 Encryption

A solution based on encryption at Layer 2 offers considerable advantages over IP-based encryptors where networks are using multiple protocols. Unlike Layer 3 IPSec encryption which expands the size of packets and causes fragmentation problems, Layer 2 encryption introduces virtually no latency to the network and can make use of lease line, Frame Relay circuits, or ATM rings. Because they operate one layer below the network, they are not affected by the use of Token Ring, SNA, or TCP/IP, and no protocol converters are required because the devices are protocol independent. A Layer 2 encryptor does not consider the nature of the traffic, it is only concerned with deciding whether a link with a particular destination must be encrypted or not. Consequently, its decision database has far fewer rules, resulting in a solution that is simpler and less expensive to manage with less opportunity for error. Layer 2 encryption is also independent of network configurations. This means that changes to the LAN/WAN do not require the involvement of the manager responsible for the encryption devices. To meet security certifications, the Datacryptors will not pass data if the unit fails. The unit will not allow data to pass in the clear. In the case of a Frame Relay connection, a unit failure would fail the entire link.

The technology allows organizations the opportunity to implement a security solution quickly with minimal network disruption while preserving current investments. Organizations requiring both security and multiple protocols consider strong encryption at layer 2 to protect sensitive mission-critical functions for the network backbone and network access.

Key Advantages of Layer 2

No Packet Size Overhead

IPSec adds 38 bytes to each packet encrypted. Therefore the total overhead is completely based on the average packet size on the network. For voice packets which are 64 packets IPSec adds 62% overhead. IPSec overhead also add increased latency to the devices that must encrypt or decrypt the packets. The industry has accepted the fact that on a average network IPSec can add as much as 50% delay on the network. Layer 2 solutions add no overhead - a significant performance advantage.

Layer 2 Security Appliance vs. Layer 3 in a switch or router embedded solutions

A Layer 2 appliance will consistently perform better than any switch or router based IPSec solution. Switch based IPSec solutions will add significant latency to the network. An appliance will encrypt/decrypt the packet and transmit the packet all on the same hardware board in under 5 microseconds (under normal conditions). A switch based solution typically has a WAN card, a main processor card and an encryption card. The packet enters the WAN card is routed to the processor card, then routed to the encryption card, back to the processor card, then to the WAN card to be transmitted out of the system. The delays due to the backplane processing and the delay associated with each card is a magnitude more than the appliance. The delay is measured in milliseconds or seconds instead of microseconds. The Layer 2 appliance has a significant advantage.

Configuration

A Layer 2 appliance is very simple to configure and is a plug and play device. A Layer 3 IPSec based solution must be configured to accept IP addresses and policy decisions must be made for each endpoint adding significant time and complexity to the provisioning or system turn up.

Conclusion

Layer 2 encryption applications are ideal for point to point deployments. IPSec solutions have gained popularity in the recent years, but the major WAN deployments for key applications delivering critical data for federal governments and for financial institutions continue to be Layer 2 based solutions. The significant cost savings from a deployment/management standpoint, the minimal latency impact and the reduced complexity make a Layer 2 solution cost effective and manageable for large scale networks.

THALES

AMERICAS
THALES e-SECURITY, INC.
2200 N. Commerce Parkway
Suite 200
Weston, Florida 33326, USA
Tel: +1 888 744 4976
or: +1 954 888 6200
Fax: +1 954 888 6211
email: sales@thalesesec.com