Moving IPSec from the Defense to the Offense

IPSec and SSL Technology and Market

Serge-Paul Carrasco
February 2006

Table Of Content

IPSec and SSL

Protocol Overview

IPSec Protocol Overview (1)

- IPSec provides network-layer security services for IP upper-layer protocols (TCP and UDP). IPSec enables:
  - Data origin authentication: guarantee that the message actually was sent by the apparent originator of the message;
  - Connectionless data integrity: guarantee that the message that is received is the exact one that was sent;
  - Data content confidentiality: guarantee that the message cannot be read by a third-party; that is loss of privacy.
- IPSec security services are created between two end-points through a Security Association (SA):
  - SA makes IPSec connection-oriented when IP is connectionless-oriented.
- IPSec Policy defines which traffic to be protected, how to protect it and with whom the protection is shared.

IPSec Protocol Overview (2)

- IPSec' suite of protocols includes:
  - AH (Authentication Header):
    - Data origin authentication;
    - Connectionless integrity;
    - Anti-replay protection:
      - the same message is not delivered multiple times and that the message is not delivered grossly out of order.
  - ESP (Encapsulating Security Payload):
    - AH capabilities (but with a different scope of authentication coverage);
    - Plus optional data confidentiality e.g. data encryption
- IKE (Internet Key Management) provides key negotiation for IPSec:
    - Dynamic authentication of IPSec peers;
    - Negotiation of security services;
    - Generating shared keys (but keys can be manually set-up).
- ESP functionality overlapped with AH (still a topic of discussion). AH and ESP are optional for IPv4 but required for IPv6.

IPSec
Tunnel and Transport Modes

- IPSec protocols AH and ESP can be used in two different ways or "modes":
  - Transport mode: to protect only the upper-layer protocols of an IP payload. IPSec is used between the IP header the upper-layer protocol payload.
  - Tunnel mode: to protect the entire IP payload. IPSec encapsulates the whole IP packet and a new IP header is created to transmit the packet.
- Because of its construction, transport mode can only be used between end-point communication e.g. the hosts have cryptographic capabilities whereas tunnel mode is typically used by IPSec gateways.

Internet Key Exchange (IKE)

- IKE authenticates each peer involved in IPSec, negotiates the security policy and handles the secure exchange of session keys. IKE is a request-response protocol with an initiator and a responder.
- IKE creates first an authenticated secure tunnel between two entities called IKE phase I and then negotiates the IPSec SA, called IKE phase II:
  - Traffic is generated or received by one of the IPSec peers that is identified to require IPSec protection to its destination;
  - IKE phase I creates an IKE SA between the two IPSec peers that enable a secure communication channel;
  - IKE phase II results in the creation of two IPSec SAs between the two IPSec peers. This pair of unidirectional SAs creates the secure IPSec tunnel;
  - Data starts passing between the IPSec peers over the established secure IPSec tunnel.

SSL Protocol Overview

- SSL provides a secure connection over TCP transport for HTTP applications between the Web server and a browser.
- SSL Handshakes:
  - Authenticates the server using RSA public key;
  - Establish the cryptographic keys for the connection;
  - Optionally provide client authentication.
- SSL Record Protocol:
  - Provide data encryption by fragmenting the application data;
  - Provide message integrity using message authentication code (MAC).
- SSL Change CipherSpec:
  - Indicate a change in the encryption and authentication.
- SSL Alert Protocol:
  - Signal various types of errors.

IPSec and SSL

Market Overview

Firewall IPSec VPNs Market (1)

- Includes two types of products:
  - Integrated Firewall IPSec Appliance;
  - Primary function in an "all-in-one security" appliance that might include as well:
    - IDS/IDP;
    - Virus scanning/Web Content Filtering/Anti-Spam.
- Product price range:
  - Between $500 and $1,500: 13% of revenues;
  - Between $1,500 and $30,000: 50% of revenues;
  - Beyond $30,000: 14% of revenues;
    - Source: Infonetics, Nov 2004.

Firewall IPSec VPNs Market (2)

- Market:
  - 2004: $1,966 M (23% growth over 2003)
  - 2007: $2,217 M
  - CAGR: 12%
    - Source: Infonetics, Nov 2004
- Top 5 vendors:
  - Cisco Systems: 35%
  - CheckPoint/Nokia: 20%
  - Juniper Networks: 10%
  - Nortel: 7%
  - SonicWall, Fortinet, Symantec: 2%
- Cisco is definitely the revenue leading vendor. Juniper seems to have stopped taking significant market shares to CheckPoint.

Firewalls VPN Market/Product Trends

- Firewall technology has not significantly evolved over the last few years.
- Most vendors are increasing the functionality of IDS/IDP and application-layer security into the firewall:
  - As a consequence, the IPSec function becomes a secondary feature.
- Perimeter firewalls are re-packaged to be used inside LANs such as CheckPoint with its InterSpect product line that does not include application proxy-firewall (in order not to slow down intra-enterprise communications).
- Wireless LAN security is driving as a short-term solution, sales of firewalls until wireless equipment vendors come-up with an ubiquity solution.
- New low-end products are now used for PCs.

SSL VPN Technologies/Products

- Includes three types of products:
  - Dedicated SSL VPN Appliance;
  - SSL-encrypted enterprise portal;
  - Integrated to an “all-in-one security appliances;
- Dedicated SSL VPN Appliance are ranging from $3K to $100K.

SSL VPN Appliance Market Trends

- Worldwide Market:
  - 2004: $201.5 M (173% growth over 2003)
  - 2009: $898.6 M
  - CAGR: 34.9%
    - IDC, March 2005
- Top 5 vendors:
  - Juniper Networks
  - Aventail
  - Nortel Networks
  - F5 Networks
  - Whale Communications
- 10 public companies and 13 private companies are competing in that market!
- Cisco does not offer a standalone SSL VPN but its VPN concentrator handles both IPSec and SSL-VPN.

SSL VPN Appliance Product Trends

- SSL VPNs are likely to move inside corporate LANs.
- SSL VPN connectivity is likely to merge for some vendor as a feature part of another security product such as application firewall or threat management like IPSec VPNs integrated to Firewalls.
- All SSL VPNs products are leveraging and driving client integrity checking and endpoint security technologies;
- Demand for non-PCs clients will expand the application:
  - Nortel plans to provide persistent VPN user tunnel while roaming;
- Extended to work with e-mail, files and telnet/SSH applications;
- As the demand grows so will SSL hardware cryptographic acceleration.

Moving IPSec

From the Defense to the Offense

Moving IPSec from the Defense to the Offense: Myth Number 1

- SSL is simpler than IPSec:
  - IPSec challenges:
    - Setting the peer gateway IP address and remote IP address subnet;
    - Configuring the IPSec policies and SA parameters;
    - Loading the certificates.
  - SSL is easy:
    - The Web browser takes care of any configuration issue!
  - The reality:
    - IPSec addressing can be automated through the discovery of the remote subnets;
    - Certificates must be loaded in both SSL and IPSec.

Moving IPSec from the Defense to the Offense: Myth Number 2

- SSL works everywhere. IPSec does not:
  - SSL VPNs works:
    - Not only for enterprise users but as well for business partners and customers;
    - Not only for remote but as well mobile users;
    - Not only for PCs but as well PDA and Internet Kiosks;
  - The reality:
    - Yes if the application is Web-based;
    - But any application that is not Web-based will require some custom program loaded on the target machine.

Moving IPSec from the Defense to the Offense: Myth Number 3

- SSL does not require specialized client software or hardware.
- The reality:
  - Yes, if the application is Web-based;
  - But any application that is not Web-based will require some custom program loaded on the target machine: SSL faces the same challenges as IPSec even more when it tries to run full application transport over an SSL connection;
  - Any solution that involves clients will require that policy configuration be automatic and that user configuration be minimal to non-existent: SSL faces the same challenges as IPSec;
  - Yes, by nature encryption requires some use of hardware optimization.

Moving IPSec from the Defense to the Offense: Myth Number 4

- SSL security control is more granular than IPSec:
  - The reality:
    - Yes if the application is Web-based;
    - With IPSec, application security is left to the application.
- SSL VPN better scales than IPSec:
  - The reality:
    - SSL appliance are by nature client/server and can only serve a specific populations of users accessing an application.

Moving IPSec from the Defense to the Offense: Myth Number 5

- IPSec is slow:
  - Yes, IPSec adds more header to the packet than SSL;
  - But using SSL as a tunnel for non-TCP native applications will add considerably more;
  - And a Web-based application will add latency and overhead by running the application through another program and by adding SSL handshakes.
- IPSec can break networks with firewalls, IDS/IDP and NAT:
  - Static-NAT can be solved by providing IPSec encryption around;
  - Dynamic-NAT is solved with IPSec NAT traversal (T-NAT);
  - Encryption of the traffic poses the same problem to existing Firewalls and IDS/IDP to both IPSec and SSL.

Thank you for your attention