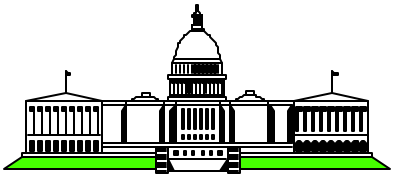
Virtual Private Networks
Overview for z/OS



Mary Sweat
E - Mail: sweatm@us.ibm.com

Washington System Center

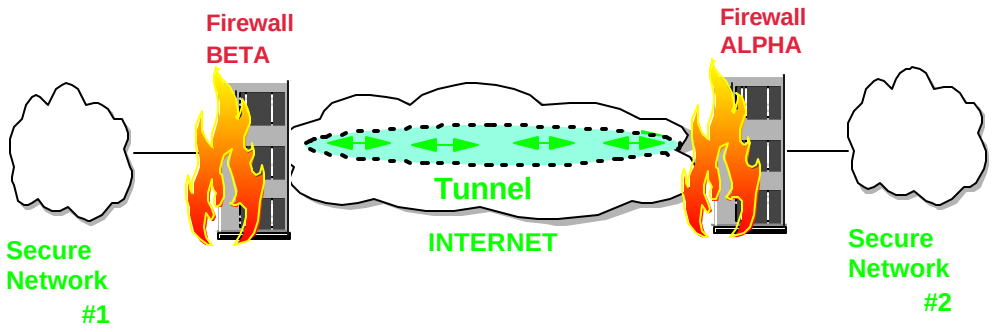
Agenda

WSC
Advanced
Technical Support

- Virtual Private Networks (tunnels)
  - tunnel types and modes
  - IPSec
    - Authentication
    - Encryption
  - IPSec vs SSL
  - benefits

Virtual Private Networks

- Virtual Private Networking (VPN) allows secure communications between remote sites over a public network like the internet
- Secures data traffic at the IP layer
  - secure traffic for all applications, without modifications to applications

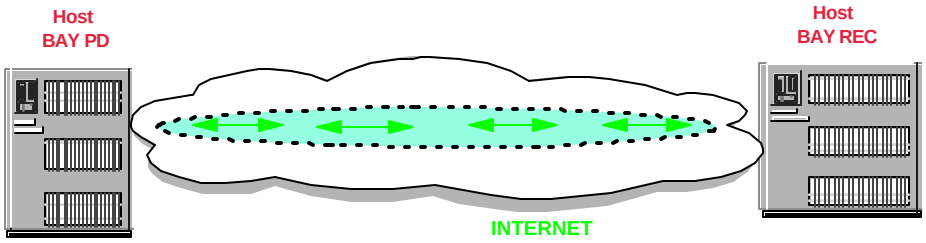


- In the z/OS operating system Virtual Private Networks are part of the z/OS Firewall Technologies.
- To configure and use the VPN in a z/OS environment you must install the z/OS Firewall and have it operational.
- Illustrated is a tunnel between two firewall hosts across the Internet. The two secure networks are in effect combined into a Virtual Private Network and it allows secure communications between the two hosts.

Secure Tunnels

WSC Advanced Technical Support

- Virtual tunnels created between two hosts
  - uses IPSec protocol not TCP or UDP
    - referred to as a Virtual Private Network
    - user specifies method of encapsulation for IP traffic
    - provides integrity, privacy and authentication



- The level of security can include using an authentication header or encryption or both.
- How the tunnel is defined by the user will be the control point for the security associated with this tunnel
- Security Association is information shared between two devices that enables them to protect IP traffic using an IPSec security service protocol
- The encapsulation process defines the syntax and rules of placing one data packet inside another

Tunnel Types

WSC Advanced Technical Support

- Manual, keys are static
  - encryption & authentication keys are the same for the life of the tunnel
  - must be manually updated
  - has the widest choice of header and encryption options
- Dynamic tunnels (ISAKMP), keys are dynamic
  - based on Internet Security Association and Key Management Protocol (ISAKMP)
  - defines message formats and flows that will allow two devices to dynamically agree to the information shared between them
  - negotiate and refresh security parameters and exchange keys securely

- Ability to inter-operate with another OS/390 system or any other compatible IBM platforms is simplified by using export/import capability of the **fwtunn**l command or via the configuration client.
- For communicating with non-IBM platforms the tunnel information will have to be entered manually.

IP Security

WSC Advanced Technical Support

- IPSec is a security protocol used as a industry standard in the area of VPNs
  - defined by Internet Engineering Task Force (IETF)
    - multiple Internet drafts and RFCs
- Basic rules to apply to attributes and encryption keys used by IPSec known as Security Association (SA)
- Uses protocols to secure data
  - Authentication Header (AH) - verifies identity of a host or tunnel end point
  - Encapsulating Security Payload (ESP) - process to ensure data can not be viewed by unauthorized personnel
- Provides specific operation modes
- Uses other protocols to dynamically generate cryptograhic keys

- The S/390 hardware cryptographic facility (ICSF) will be used when available. If system has ICSF setup then the VPN can take advantage of it and use the hardware encryption. Otherwise VPN will use software encryption provided by RSA BSAFE.

- Data passing through a tunnel can be either;
  > encrypted (ESP)
  > authenticated (AH)
  > encrypted and authenticated

- IETF is a large, open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

Security Association (SA)

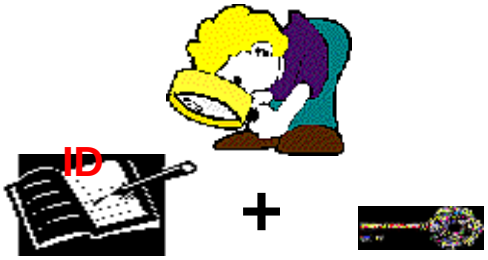
WSC Advanced Technical Support

- Defines basic concepts required to agree to attributes and encryption keys used by IPSec
  - information shared between two devices that enables them to protect IP traffic
    - identifies parameters/functions needed to create IPSec packetS
      - destination ID/IP address
      - type of security service used (AH or ESP)
      - keys used by cryptographic operations
      - tunnel mode
      - Security Parameter Index (value used in identifying an SA)

IPSec Authentication & Integrity

WSC Advanced Technical Support

- Uses IP Authentication Header (AH) protocol
  - proof of the sender's identity and data integrity
    - uses cryptographic hash function with a secret key
      - produces unique digest
    - receiver de-capsulates using same function and key
    - verifies data and sender's key
      - discards data if key is not valid or data has been altered



- The AH protocol may be used in combination with ESP.

IPSec Encryption

WSC Advanced Technical Support

- Uses IP Encapsulating Security Payload (ESP) protocol
  - provides integrity, authentication and encryption to IP packetS
    - uses certain algorithms and keys to produce cyphertext
      - same algorithms and keys used by sender and receiver
      - knows as symmetric encryption algorithms

- ESP and AH protocols can be applied alone or in combination or even nested within another instance of itself.

- ESP uses the following encryption algorithms;
  - > Triple Data Encryption standard (DES)
  - > DES
  - > Commercial Data Masking Facility (CDMF)
  - > Keyed Message Digest-5
  - > Two versions of the Hashed-Based Message
  - > Authentication Code (HMAC) used to perform authentication

Tunnel Modes

WSC Advanced Technical Support

- Operational Modes
  - transport - only protects the transport-layer packet (such as TCP or a UDP) inside an IP packet
    - data is protected, source and destination addresses remain unchanged
  - tunnel - protects entire IP packet
    - data as well as source and destination addresses are protected

How IPSec Compares to SSL

- Both are similar:
  - provides client and server authentication
  - provides data authentication and secrecy (encryption)
- SSL is implemented at the transport level, IPSec is implemented at the Internet Layer
- SSL does not protect IP headers, IPSec does
- SSL does not protect UDP traffic, IPSec does
- Applications require modification to be made SSL aware, IPSec is transparent to applications
- SSL provides application to application security, IPSec provides device to device security

- Both SSL and IPSec provide a way to encrypt data contained in IP packets
- Both prevent modification of data contained in IP packets
- Both provide a way to authenticate the communicating parties
- The biggest difference is where each protocol is implemented. SSL sits between the application layer and the transport layer of the TCP/IP protocol stack. Therefore SSL does not protect the IP header, nor the UDP traffic and it requires applications to be modified to make use of it.

Internet Security Association Key Management Protocol Server

WSC Advanced Technical Support

- Server uses ISAKMP/OAKLEY protocol
  - supports automatic generation of tunnel definitions
- Provides a more automated alternative to manual Virtual Private Networks (VPNs)
  - dynamically establish VPNs
  - negotiate VPN attributes
  - dynamically manage VPN encryption keys
- Offers a method of exchanging encryption keys in a secure manner

Internet Security Association Key Management Protocol

WSC Advanced Technical Support

- Enables dynamic SAs and key management
  - enables two devices to dynamically agree to the setup of a tunnel
- Creates common framework for handling SAs
  - definition
  - negotiating
  - modifying
  - deleting
  - authenticating peers
  - exchanging keys
- Key management protocol
- Implemented at the application layer
  - communicates useing UDP port 500

- ISAKMP provides the building blocks for handling the security associations but it does not define specifics.

Tunnel Benefits

WSC Advanced Technical Support

- Creates a secure private connection through what is basically a private tunnel
- VPNs securely convey information across the Internet connecting remote users, branch offices, and business partners/suppliers into an extended corporate network
- Access to the Internet via service providers is more cost effective
- Eliminate need for
  - expensive leased lines
  - long-distance calls
  - toll-free telephone numbers

Why Dynamic Tunnels

WSC Advanced Technical Support

- Ensure interoperability
  - ensure businesses can communicate regardless of vendors VPN
- Address security concerns with key management
  - offers secure manner for exchanging keys
- Ease of use for environments managing numerous VPNs

IPSec Standard References

WSC Advanced Technical Support

- Request for Commends (RFCs)
  - located at www.ietf.org
    - 1825 Security Architecture for Internet Protocol
    - 1826 IP Authentication Header
    - 1827 IP Encapsulating Security Payload
    - 1828 IP Authentication Using Keyed MD5
    - 1829 The ESP DES_CBC Transform
    - 2401 Security Architecture for Internet Protocol
    - 2402 IP Authentication Header
    - 2403 HMAC-MD5-96 within ESP and AH
    - 2404 HMAC-SHA-1-96 within ESP and AH
    - 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
    - 2406 IP Encapsulating Security Payload
    - 2407 Internet IP Domain of Interpretation for ISAKMP
    - 2408 Internet Security Association and Key Management Protocol (ISAKMP)
    - 2409 Internet Key Exchange
    - 2410 NULL Encryption Algorithm and Its Use With IPSec

References

WSC Advanced Technical Support

- OS/390 Security Server 1999 Updates Technical Presentation Guide (SG24-5627-00)
  - located at www.redbooks.ibm.com
- Security in OS/390-based TCP/IP Network (SG24-5383)
- SecureWay Security Server Firewall Technologies Guide and Reference (SC24-5835-05)