



Securing Enterprise Extender

Sam Reynolds

IBM z/OS Communications
Server Design
samr@us.ibm.com

Ray Romney

Cisco Systems
romney@cisco.com

Tony Amies

William Data Systems
Product Architect
tony.amies@willdata.com

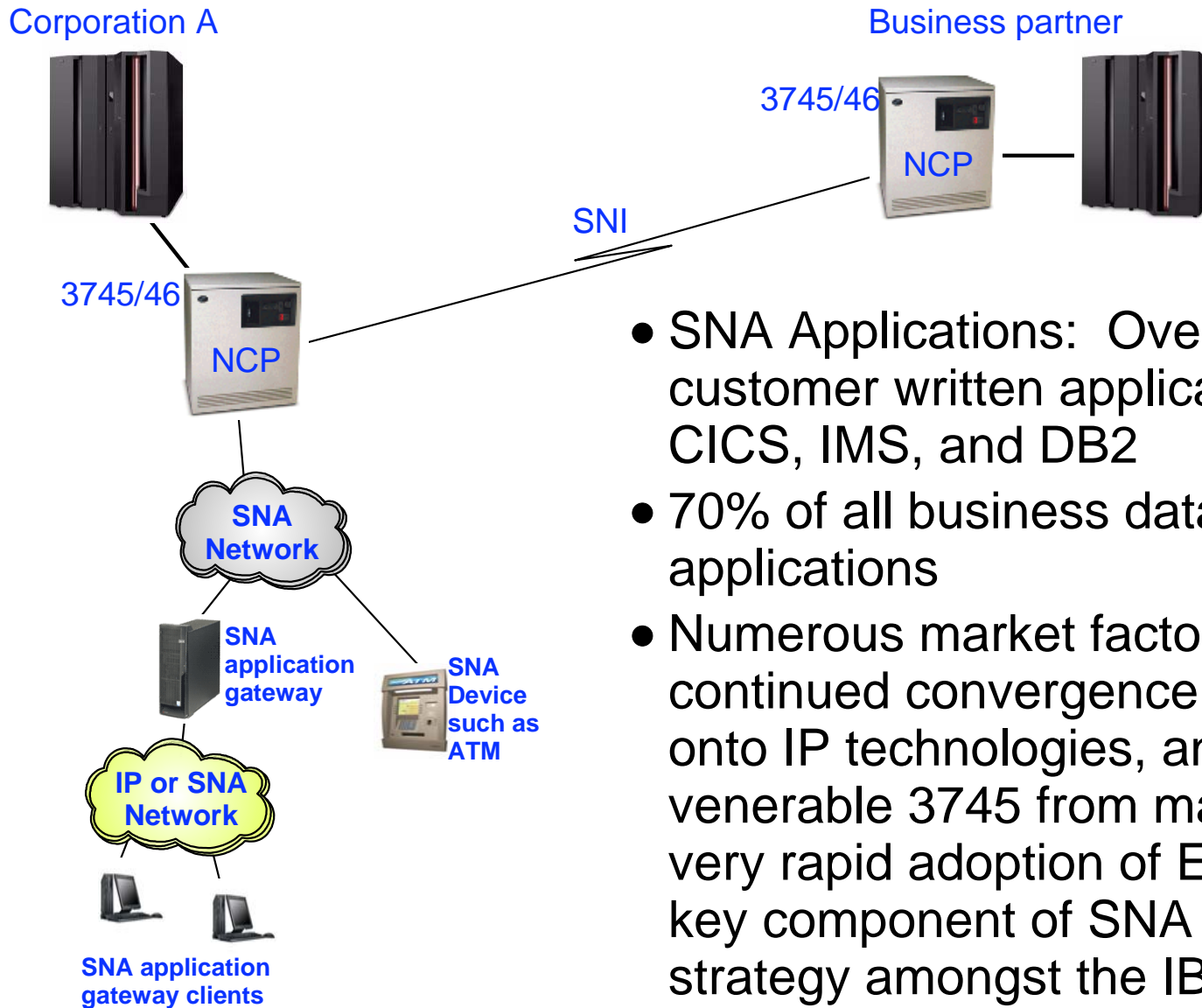
Agenda



- The Evolution of SNA: SNI To EE
- Security Objectives/Issues
- Security Mechanisms
- Proxy Implementation: Apias
- Summary
- References

The Evolution of SNA: SNI to EE

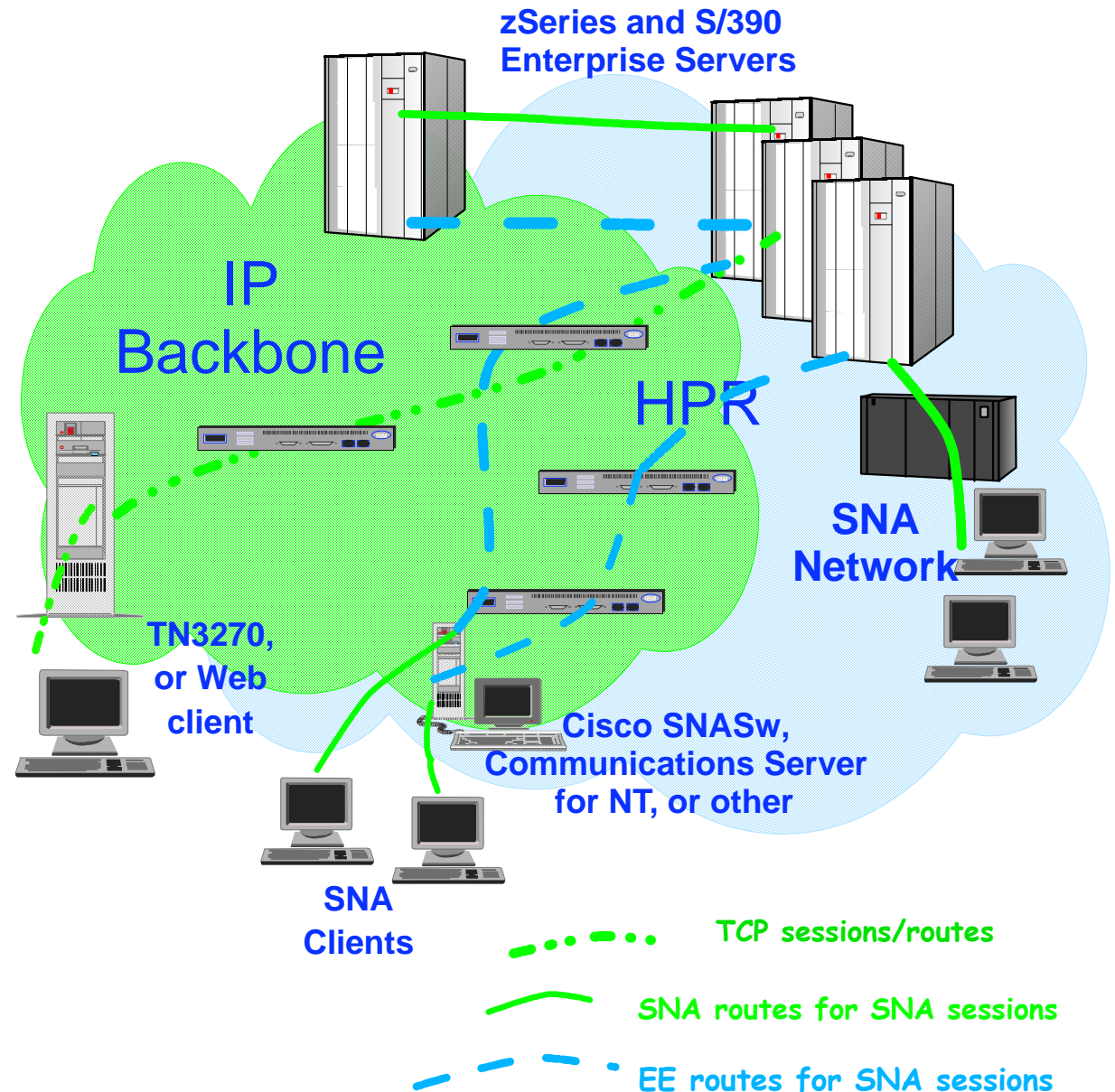
Traditional SNA Networking Infrastructure



- SNA Applications: Over a trillion lines of customer written application code based on CICS, IMS, and DB2
- 70% of all business data still accessed via SNA applications
- Numerous market factors including the continued convergence of enterprise networks onto IP technologies, and the withdrawal of the venerable 3745 from marketing, have led to a very rapid adoption of Enterprise Extender as a key component of SNA application access strategy amongst the IBM customer set.

What is Enterprise Extender?

- Allows use of IP network for SNA sessions
- EE allows enablement of IP applications and convergence on a single network transport while preserving SNA application and endpoint investment.
- Typically isolates SNA footprints to the "outside" of the network.

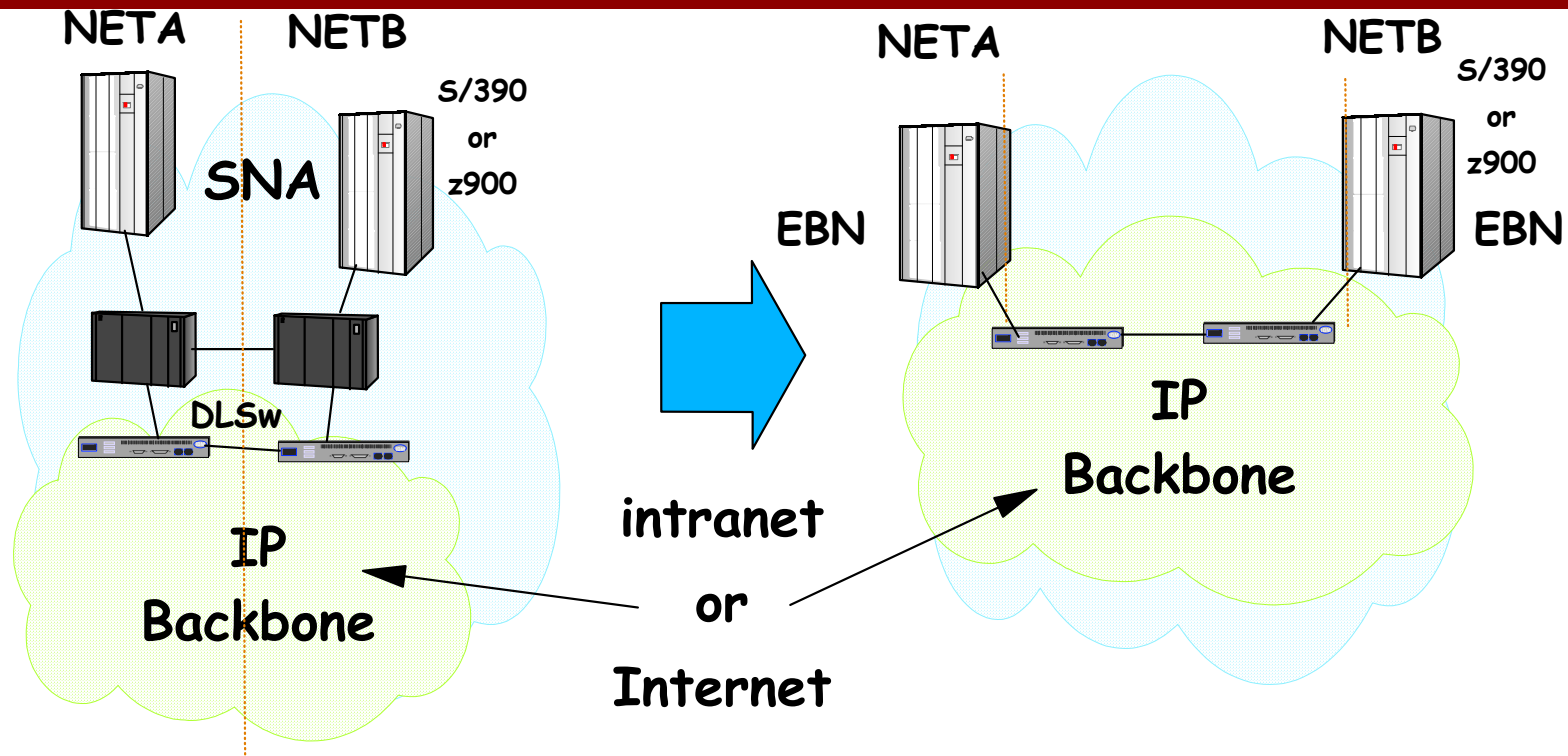


Advantages of Enterprise Extender



- SNA transport over native IP network
 - Native IP routing within network maximizes router efficiency
 - Enables SNA applications to take advantage of advances in IP routing
 - SNA traffic can exploit OSA Gigabit Ethernet & HiperSockets
 - EE can use any zSeries or S/390 IP network connection -- channel attached router, OSA, etc.
 - Allows convergence of voice and data on single network
- No changes to SNA applications
- End-to-End failure protection and data prioritization
 - SNA priority mapped to IP Type of Service (TOS)

EE/EBN As An SNI Alternative



- Traditional SNI
 - Requires 37xx for interconnectivity
 - Complex to define and reconfigure
 - HPR (e.g. non-disruptive session switch) not available
- Enterprise Extender with Extended Border Node (EBN)
 - Configure border node in z/OS CS only
 - Single hop SNA connection
 - SNA apps unchanged
 - Eliminates DLSw

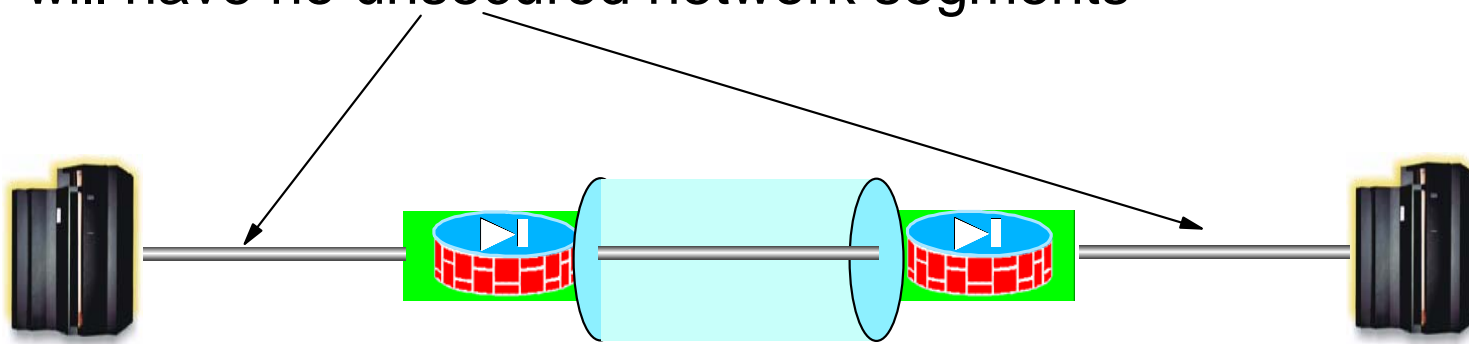
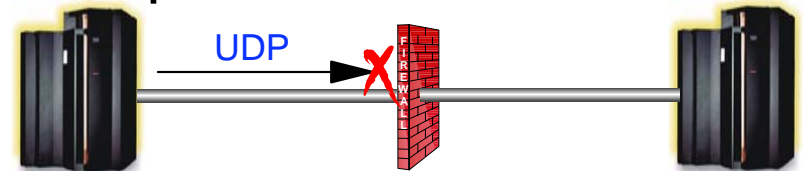
Security Objectives



- Protect data and other resources on the system
 - **System availability**
 - Protect system against unwanted access and denial of service attacks from network
 - **Identification and authentication**
 - Verify identity of users
 - **Access control**
 - Protect data and other system resources from unauthorized access
- Protect data in the network using cryptographic security protocols
 - **Data Origin Authentication**
 - Verify that data was originated by claimed sender
 - **Message Integrity**
 - Verify contents were unchanged in transit
 - **Data Privacy**
 - Conceals cleartext using encryption

Security Issues/Requirements when Implementing EE

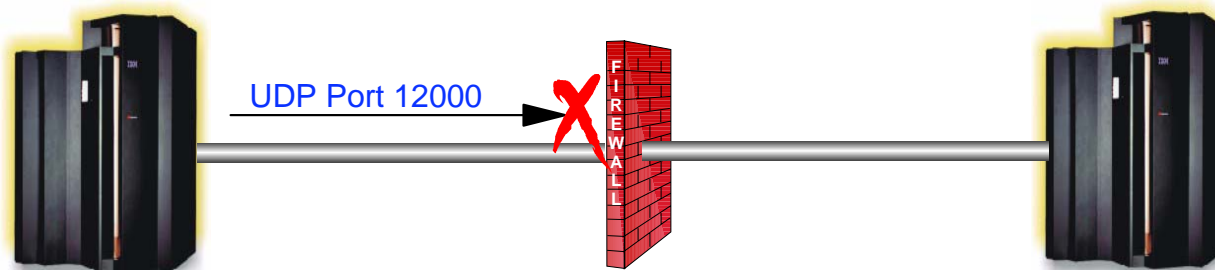
- EE is a UDP-based protocol
 - Your firewalls must allow UDP packets over ports 12000-12004, at least for specific partner EE IP addresses
- Going from private lines to public Internet use may bring new requirements for:
 - Encryption
 - Partner authentication
- Corporate policies may further restrict your options:
 - Some companies refuse to allow UDP through their firewalls
 - Some companies mandate that they will have no unsecured network segments



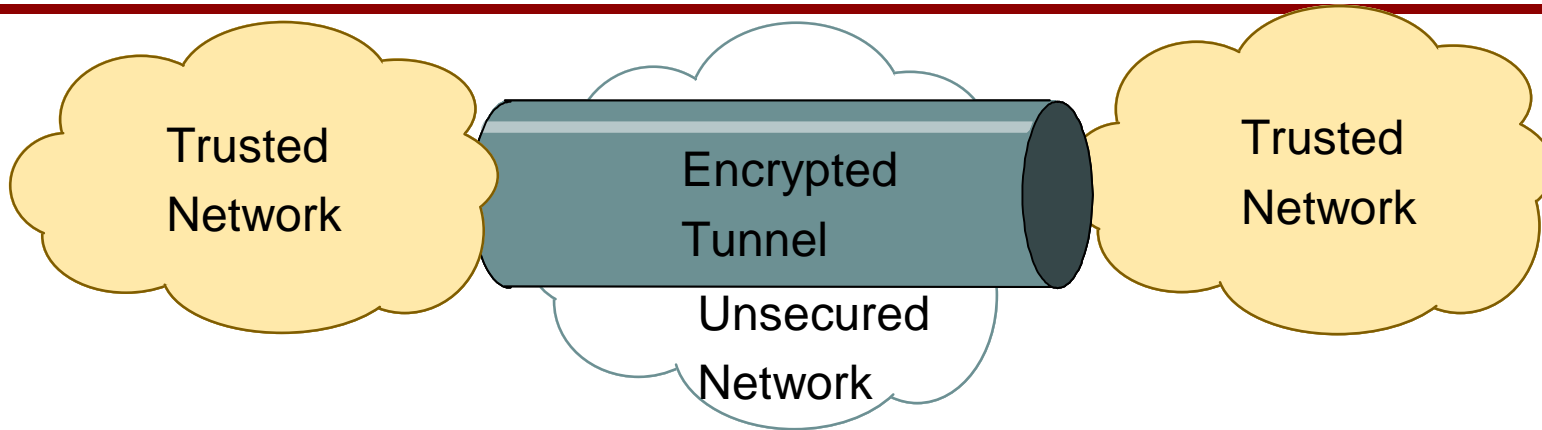
Security Mechanisms

Firewall/NAT

- A firewall is an entry/exit point to your network used to control access
- You can filter packets based on source IP address, destination port, or protocol
- Private IP addresses can be translated to public IP addresses using Network Address Translation (NAT)
- You probably already have a firewall in place
- You must allow UDP ports 12000-12004 through the firewall for Enterprise Extender
- At SNA network boundaries, may want to define filter rules to limit UDP traffic to the IP addresses of the EBN partners



VPN/IPSec



- Firewalls aren't a total solution--addresses can be spoofed, no control beyond firewall, etc.
- VPN- a private network (tunnel) over a public network (the Internet/intranet)
- IPSec with Internet Key Exchange (IKE) secures the VPN tunnel
- Very similar to how you probably connect remotely to your corporate network
- Data Encrypted/Decrypted at Tunnel Endpoints
- Firewalls can limit access to tunnel
- Split tunneling can be done to allow traffic outside tunnel

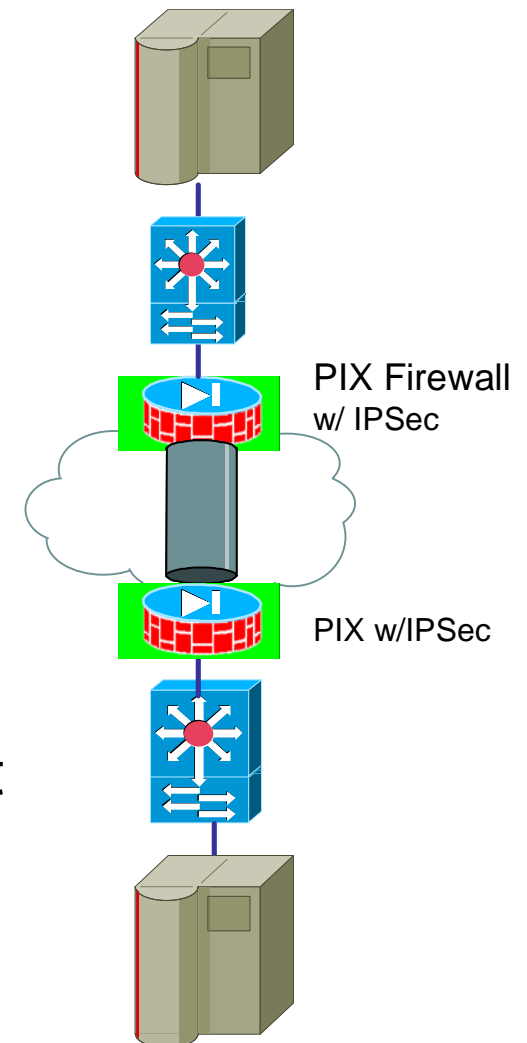
Dedicated IPSec VPN Firewall

- Advantages

- ✓ Offloads processing
- ✓ Combines firewall and IPSec in one box
- ✓ May already exist
- ✓ Firewalls can be load balanced

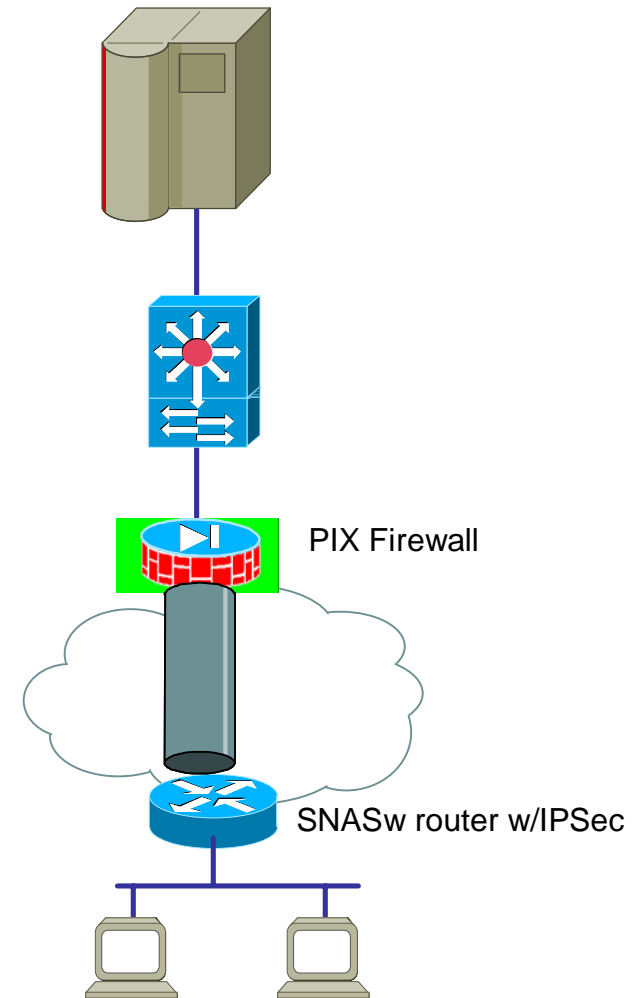
- Disadvantages

- × Unsecured network segments in data center
- × New firewall adds to cost, possible failure point



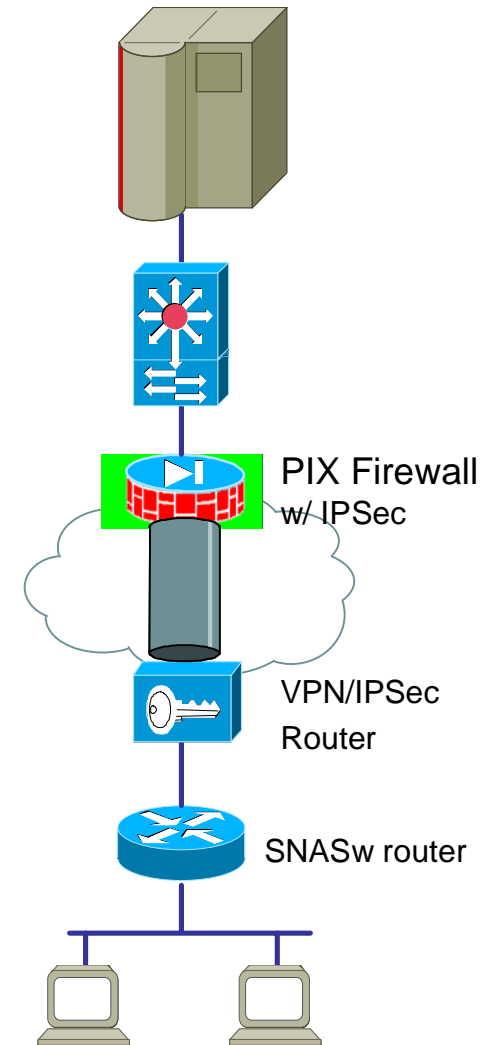
IPSec on SNASw Router

- Advantages
 - ✓ Cost effective for a small branch
 - ✓ One less failure point
- Disadvantages
 - × Router CPU intensive
 - × All traffic through SNASw/VPN router
 - × Not a good fit for large branches or data centers



PIX Firewall to SNASw Branch

- IPSec in branch on separate router
- Advantages
 - ✓ Offloads processing
 - ✓ May already exist
- Disadvantages
 - × Cost of another device
 - × Another point of failure



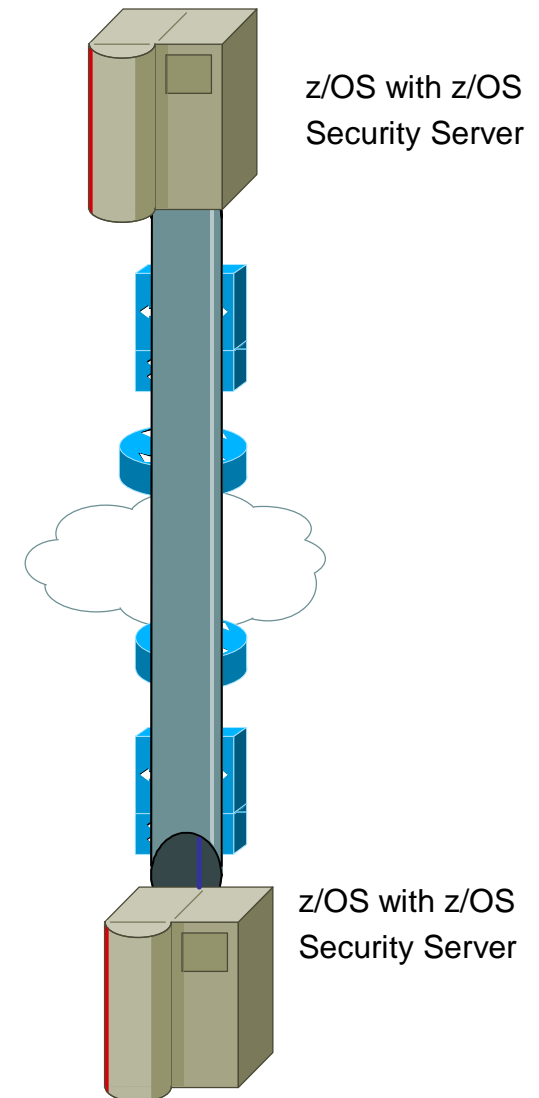
IPSec on z/OS

- Advantages

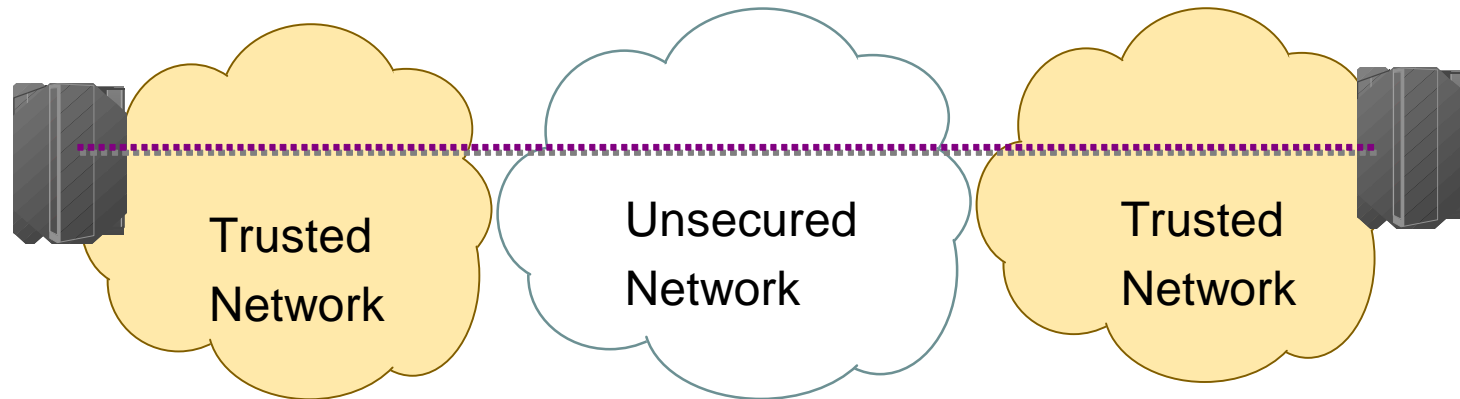
- ✓ Secure encryption even inside data center
- ✓ One less point of failure

- Disadvantages

- × Cost of MIPS to perform encryption
- × Complexity of VPN configuration prior to V1R7
 - ✓ z/OS V1R7 CS will offer numerous IPSec improvements, including a new configuration GUI that should greatly simplify z/OS IPSec configuration



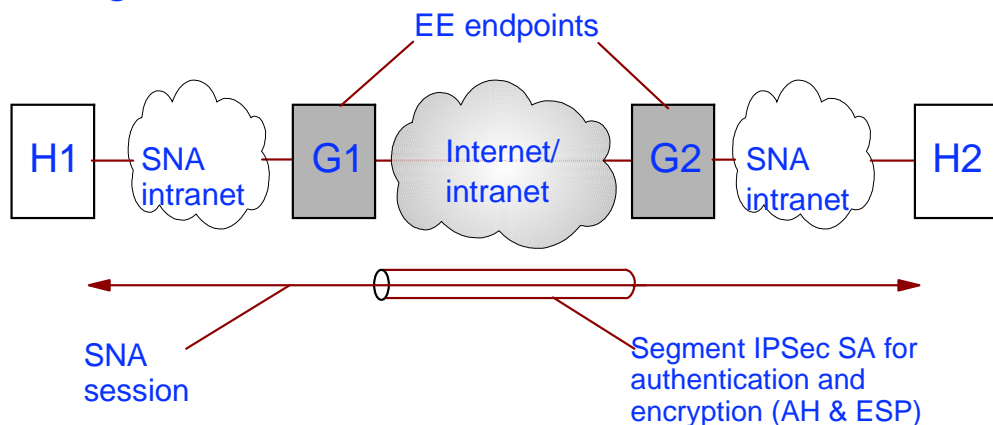
SNA Session Level Encryption



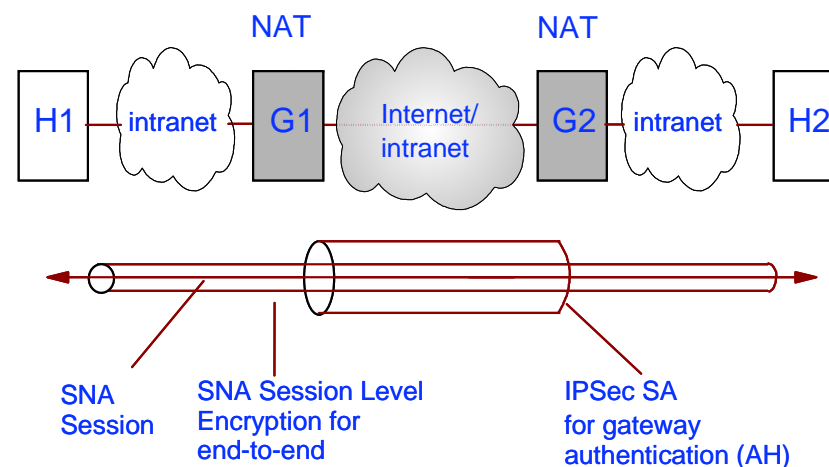
- Data Encrypted/Decrypted at each z/OS host
- Works in Subarea and APPN networks
- Can be done in addition to other security measures (VPN, IPSec, etc.)
 - There may be advantages to combining them to satisfy certain configurations and requirements
- Does have performance impact

IPSec and SNA SLE Combined Solutions for EE

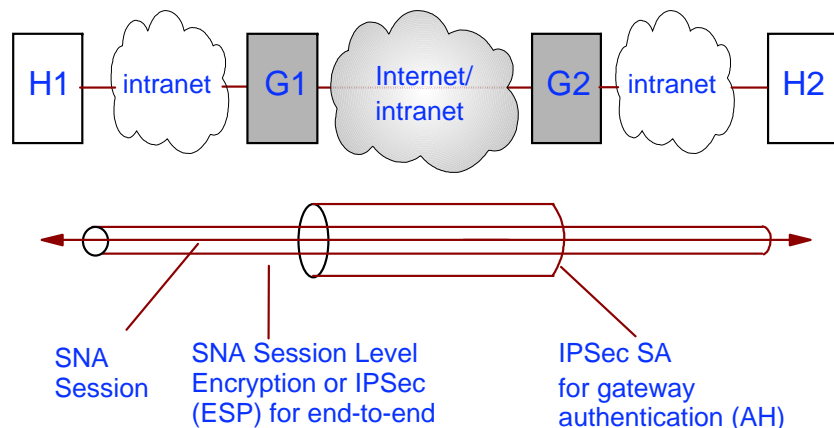
Case 1: Protection over Untrusted Network Segment



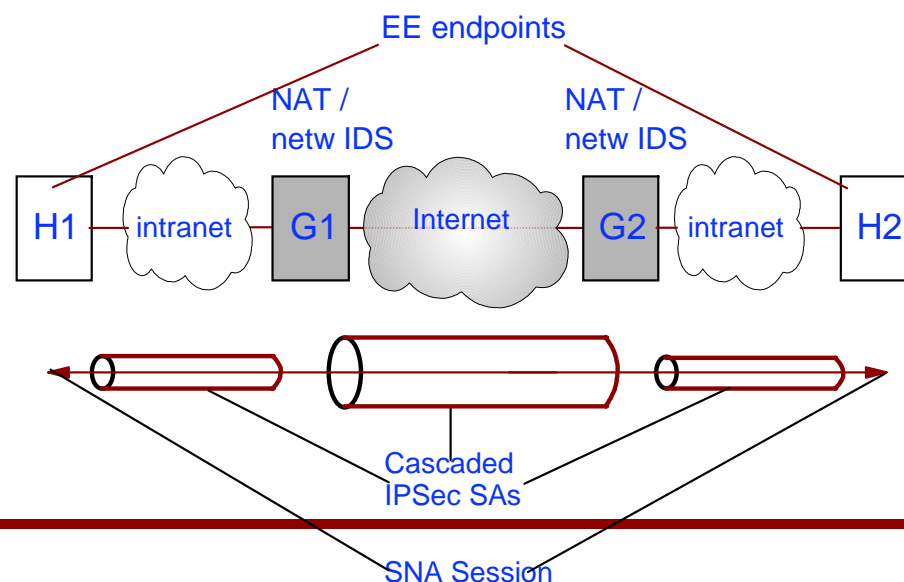
Case 2: End-to-End Security with Added Gateway Authentication (NAT)



Case 3: End-to-End Security with Added Gateway Authentication (NAT traversal solution at H1 and H2 / no NAT)



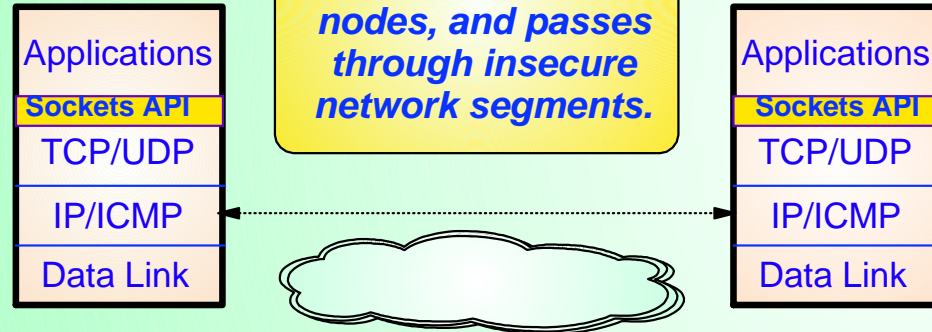
Case 4: End-to-End Security with Cascaded SAs (NAT/network IDS)



What about SSL?

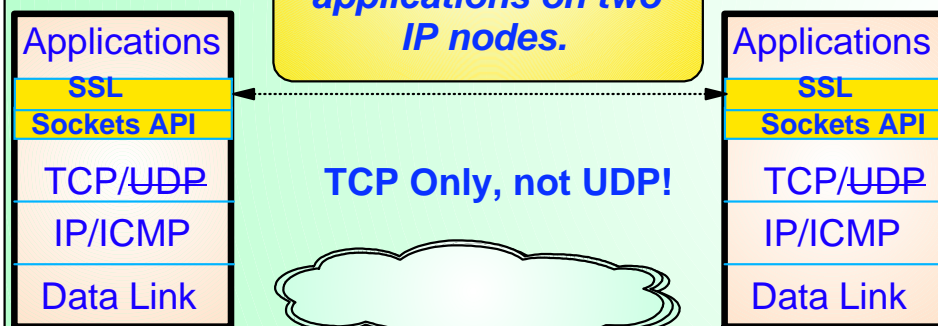
IPSec and SSL/TLS Compared

IPSec



- Provides authentication, integrity, and data privacy at IP layer
 - AH protocol provides authentication and integrity
 - ESP protocol provides data privacy (auth/integrity optional).
 - IKE protocol includes key exchange using public key cryptography and negotiation of security parameters
 - Mgmt of crypto keys and SAs can also be manual
- IP node authentication, not user authentication
- Use of IPSec is transparent to upper layers including application
 - Blanket level protection for upper layer protocols

SSL/TLS



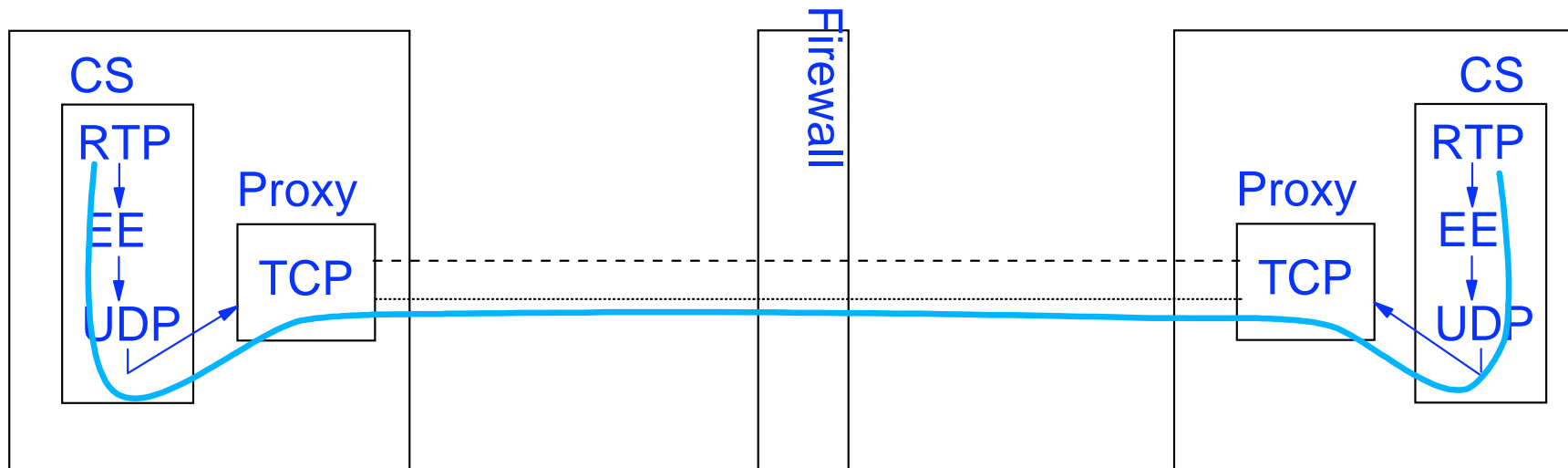
- Provides authentication, integrity, and data privacy above TCP layer.
 - SSL handshake protocol includes key exchange using public key cryptography and negotiation of security parameters
- User authentication if client certificates used
- Applications must be changed to use SSL APIs
 - UDP applications cannot be SSL-enabled

EE is a UDP Protocol



- SSL/TLS has not been applicable to EE traffic since EE is UDP-based, and SSL is a TCP-based protocol.
- In addition to authentication and encryption requirements, a remaining inhibitor for many enterprises considering EE is the necessity of opening up firewall ports to UDP traffic.
- Are there any alternatives?

Enterprise Extender Proxy

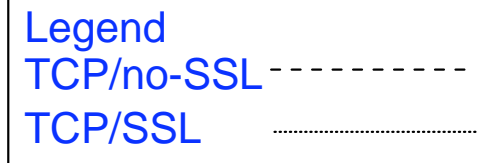


- A proxy approach could allow the transport of the EE traffic over a TCP connection, thereby allowing several options:

- ✓ TCP transport without SSL. This avoids opening the firewall ports to UDP.
- ✓ TCP transport with SSL authentication only. This addresses the firewall concern and provides partner authentication without incurring encryption costs.
- ✓ TCP transport with SSL encryption.

- Disadvantages:

- × Separate process to configure
- × CPU cost and throughput reduction due to traversal of TCP stack
 - Total cost can be mitigated by protecting only EBN connections



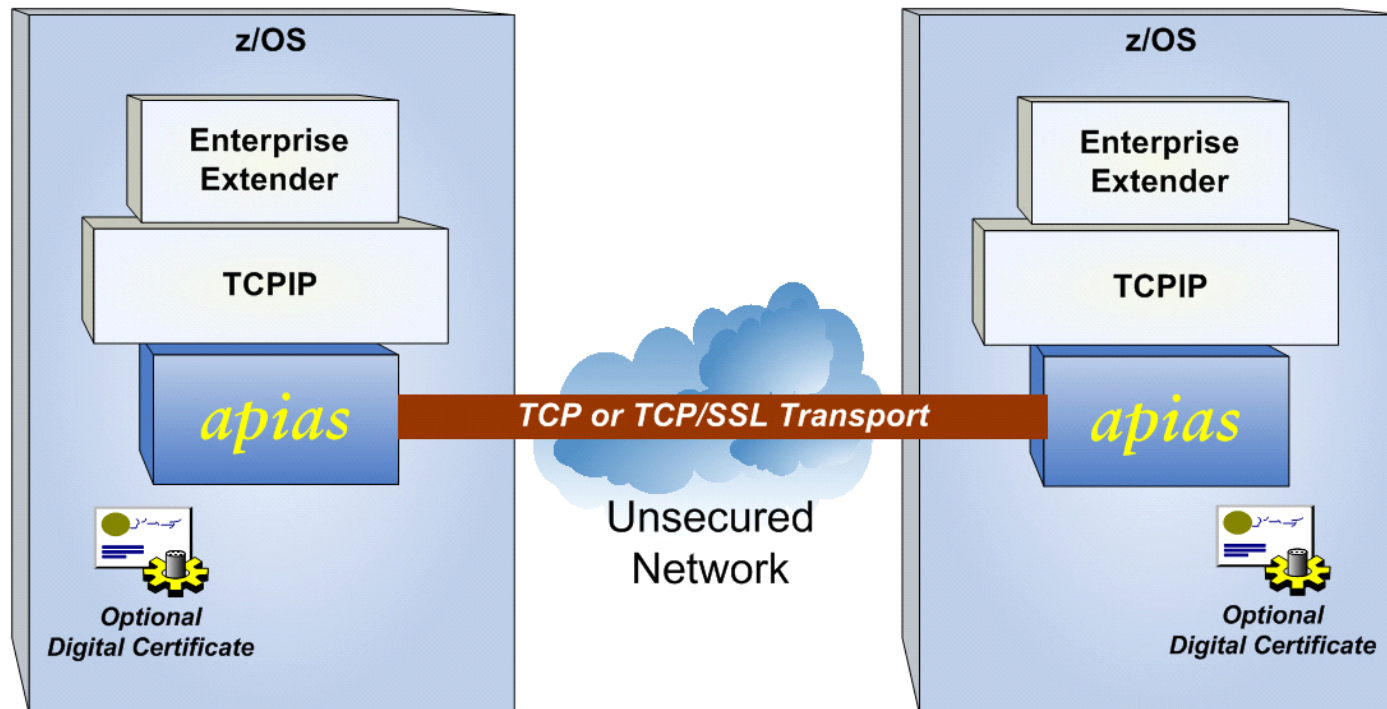
Proxy Implementation: Apias

Apias - Proxy Implementation for EE



- Removes need to open firewall ports to UDP
- Optional partner authentication and end-to-end encryption
- Supports :
 - TCP transport
 - TCP transport with SSL authentication
 - Partner authentication using digital certificates
 - TCP transport with SSL encryption and authentication
 - Partner authentication using digital certificates
 - SSL encryption
 - UDP transport
 - Multi-stack support
 - Optional SSL authentication using digital certificates

Apias - Architecture



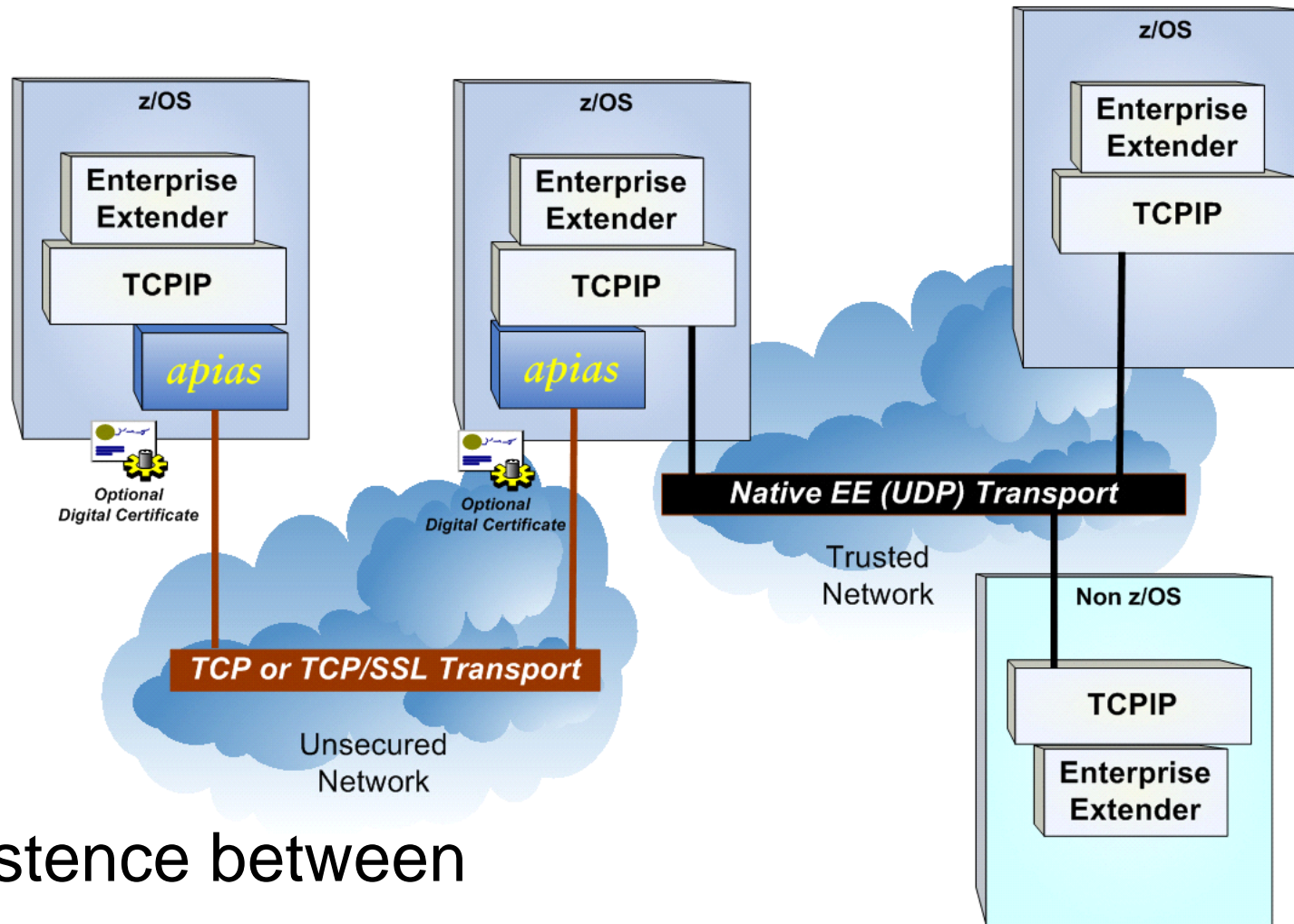
- No UDP traffic between EBNs
- Optional digital certificates for partner authentication
- Can coexist with SLE or IPSec encryption
- SSL can be used for encryption and authentication

Apias - Configuration



- Operates in own address space
 - As a started task
 - Requires APF Authorization
 - Uses TCP Ports 12000-12004
 - Uses Dynamic/Static VIPA
- Simple Configuration
- Hot Native EE to APIAS switching
 - Controlled by VTAM Major Nodes
- Multiple EE Paths/Transport Protocols
 - Single or multiple Apias instances

Apias - Coexistence



Coexistence between

- Native EE
- TCP Transport
- SSL Transport

Apias - Performance



- TCP Performance Considerations
 - TCP has more overhead than UDP
 - Packets transverse TCP/IP stack twice
 - TCP handles retransmissions
 - TCP streaming
- SSL Performance Considerations
 - Same TCP overheads + encryption costs
 - Uses cryptographic coprocessor if available

Apias - Operation



- Pre z/OS 1.4
 - Cannot operate on same IP stack as EE
 - 2nd stack on EE LPAR required, OR
 - Run Apias on another non-EE LPAR
- z/OS 1.4 and above
 - IBM maintenance required to eliminate need for second TCP/IP stack
- zSeries Linux version in development
 - Lower costs per packet
- Intel Linux version in development
 - Support for distributed EE

Summary



- A number of options are available to secure Enterprise Extender traffic, including
 - IPSec
 - SNA Session Level Encryption
 - Proxy-based solutions, such as Apias
 - Combinations of the above techniques
- You must enable UDP ports 12000-12004 through firewalls, unless using an EE proxy
- Your company's policies may dictate which of these solutions is acceptable

Related SHARE Sessions



- Session 3607 - Understanding Enterprise Extender: Concepts and Considerations (Tuesday, 8:00)
- Session 3608 - Understanding Enterprise Extender: Nuts and Bolts (Tuesday, 9:30)
- Session 3609 - Enterprise Extender Cisco SNA Switch Design, Implementation, and Debug: The Details - Part 1 of 2 (Tuesday, 1:30)
- Session 3610 - Enterprise Extender Cisco SNA Switch Design, Implementation, and Debug: The Details - Part 2 of 2 (Tuesday, 3:00)
- Session 3611 - The Evolution of SNA: z/OS CS Enterprise Extender Hints and Tips (Tuesday, 4:30)
- Session 3612 - What's New with Enterprise Extender? (Wednesday, 8:00)
- Session 3613 - Managing Enterprise Extender in z/OS, Part 1 (Wednesday, 9:30)
- Session 3614 - Managing Enterprise Extender in z/OS, Part 2 (Wednesday, 11:00)
- Session 3963 - A practical look at Enterprise Extender Security, Problem Diagnosis and Performance Monitoring (Wednesday, 11:00)

References



URL

Content

http://www.ibm.com/servers/eserver/zseries	IBM eServer zSeries Mainframe Servers
http://www.ibm.com/servers/eserver/zseries/networking	Networking: IBM zSeries Servers
http://www.ibm.com/software/network/commserver	Communications Server
http://www.redbooks.ibm.com	IBM Redbooks
http://www.ibm.com/software/network/commserver/os390/support	Communications Server Technical Support
http://www.cisco.com/go/snasw	Cisco SNASw
http://www.cisco.com/univercd/cc/td/doc/product/software... .../ios122/122cgcr/fsecur_c/index.htm	IPSec and IKE Configuration in IOS
http://www.cisco.com/safe	Cisco SAFE Blueprint
http://www.willdata.com	William Data Systems
http://www.willdata.com/v2/products/apias.htm	Apias Product Description