

# Protecting Enterprise Extender Traffic with a VPN

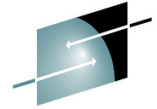
*IBM z/Center of Excellence  
Thomas Cosenza, CISSP  
tcosenza@us.ibm.com*



SHARE is an independent volunteer-run information technology association that provides **education, professional networking and industry influence.**



# Trademarks and Notices



The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

- |  |   |   |  |  |
|--|---|---|--|--|
| <ul style="list-style-type: none"> <li>• Advanced Peer-to-Peer Networking®</li> <li>• ADX®</li> <li>• alphaWorks®</li> <li>• AnyNet®</li> <li>• AS/400®</li> <li>• BladeCenter®</li> <li>• Candle®</li> <li>• CICS®</li> <li>• DataPower®</li> <li>• DB2 Connect</li> <li>• DB2®</li> <li>• DRDA®</li> <li>• e-business on demand®</li> <li>• e-business (logo)</li> <li>• e-business (logo)®</li> <li>• ESCON®</li> <li>• FICON®</li> </ul> | <ul style="list-style-type: none"> <li>• GDDM®</li> <li>• GDPS®</li> <li>• Geographically Dispersed Parallel Sysplex</li> <li>• HiperSockets</li> <li>• HPR Channel Connectivity</li> <li>• HyperSwap</li> <li>• i5/OS (logo)</li> <li>• i5/OS®</li> <li>• IBM eServer</li> <li>• IBM (logo)®</li> <li>• IBM®</li> <li>• IBM zEnterprise™ System</li> <li>• IMS</li> <li>• InfiniBand®</li> <li>• IP PrintWay</li> <li>• IPDS</li> <li>• iSeries</li> <li>• LANDP®</li> </ul> | <ul style="list-style-type: none"> <li>• Language Environment®</li> <li>• MQSeries®</li> <li>• MVS</li> <li>• NetView®</li> <li>• OMEGAMON®</li> <li>• Open Power</li> <li>• OpenPower</li> <li>• Operating System/2®</li> <li>• Operating System/400®</li> <li>• OS/2®</li> <li>• OS/390®</li> <li>• OS/400®</li> <li>• Parallel Sysplex®</li> <li>• POWER®</li> <li>• POWER7®</li> <li>• PowerVM</li> <li>• PR/SM</li> <li>• pSeries®</li> <li>• RACF®</li> </ul> | <ul style="list-style-type: none"> <li>• Rational Suite®</li> <li>• Rational®</li> <li>• Redbooks</li> <li>• Redbooks (logo)</li> <li>• Sysplex Timer®</li> <li>• System i5</li> <li>• System p5</li> <li>• System x®</li> <li>• System z®</li> <li>• System z9®</li> <li>• System z10</li> <li>• Tivoli (logo)®</li> <li>• Tivoli®</li> <li>• VTAM®</li> <li>• WebSphere®</li> <li>• xSeries®</li> <li>• z9®</li> <li>• z10 BC</li> <li>• z10 EC</li> </ul> | <ul style="list-style-type: none"> <li>• zEnterprise</li> <li>• zSeries®</li> <li>• z/Architecture</li> <li>• z/OS®</li> <li>• z/VM®</li> <li>• z/VSE</li> </ul> |
|--|---|---|--|--|
- \* All other products may be trademarks or registered trademarks of their respective companies.

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Intel Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

## Notes

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Refer to [www.ibm.com/legal/us](http://www.ibm.com/legal/us) for further legal information.



# Introduction



- Work for IBM for 17 years
- IBM Consultant for 11 years
  - Working with customers in different business meeting their Network and Security needs

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

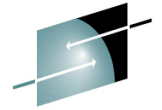


# Agenda

- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

2014 was .....



**SHARE**  
Educate · Network · Influence

The Year of the HACK

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



## 2014 a Scary Look Back

- Hacking has gone into overdrive
- 2014 have seen an increase in every type of hacking
  - Denial of Service
  - Criminal
  - Hacktivism
  - Terrorism
  - State Sponsored Attacks

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## Some Highlights

- Major US Retail Outlets
  - Point of Sales terminals Targeted
- US Banks
  - State Sponsored
  - 76 Million US Households effected
- SONY hack
  - Possibly State Sponsored
  - Hackers had months in their network
  - Demands shut down of a movie
    - So not all bad, I mean did you see it

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## Some you may not have hear of

- Foreign Nuclear Plant
  - Server administrator discovers access to servers on the site
- Government
  - Homeland Security
    - Web Portal Breach exposes US contractors
  - Immigration Services
    - POS terminals have been breached
  - Justices Services
    - DDOS attacks
- MANY MANY MORE
  - <http://hackmageddon.com/2014-cyber-attacks-timeline-master-index/>

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



## Words to Live By

- “The Security Perimeter is now at the End Point”  
Anonymous

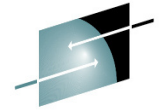


Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# Agenda

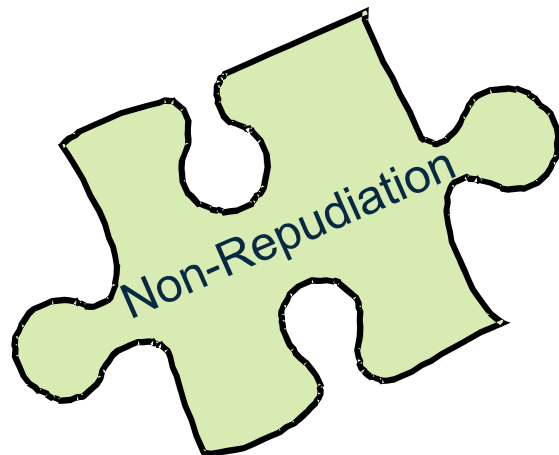
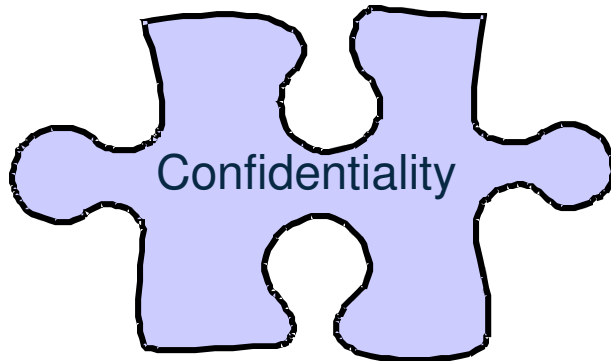
- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



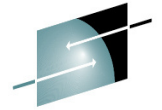
**SHARE**  
Educate · Network · Influence

# The Puzzle pieces of Security



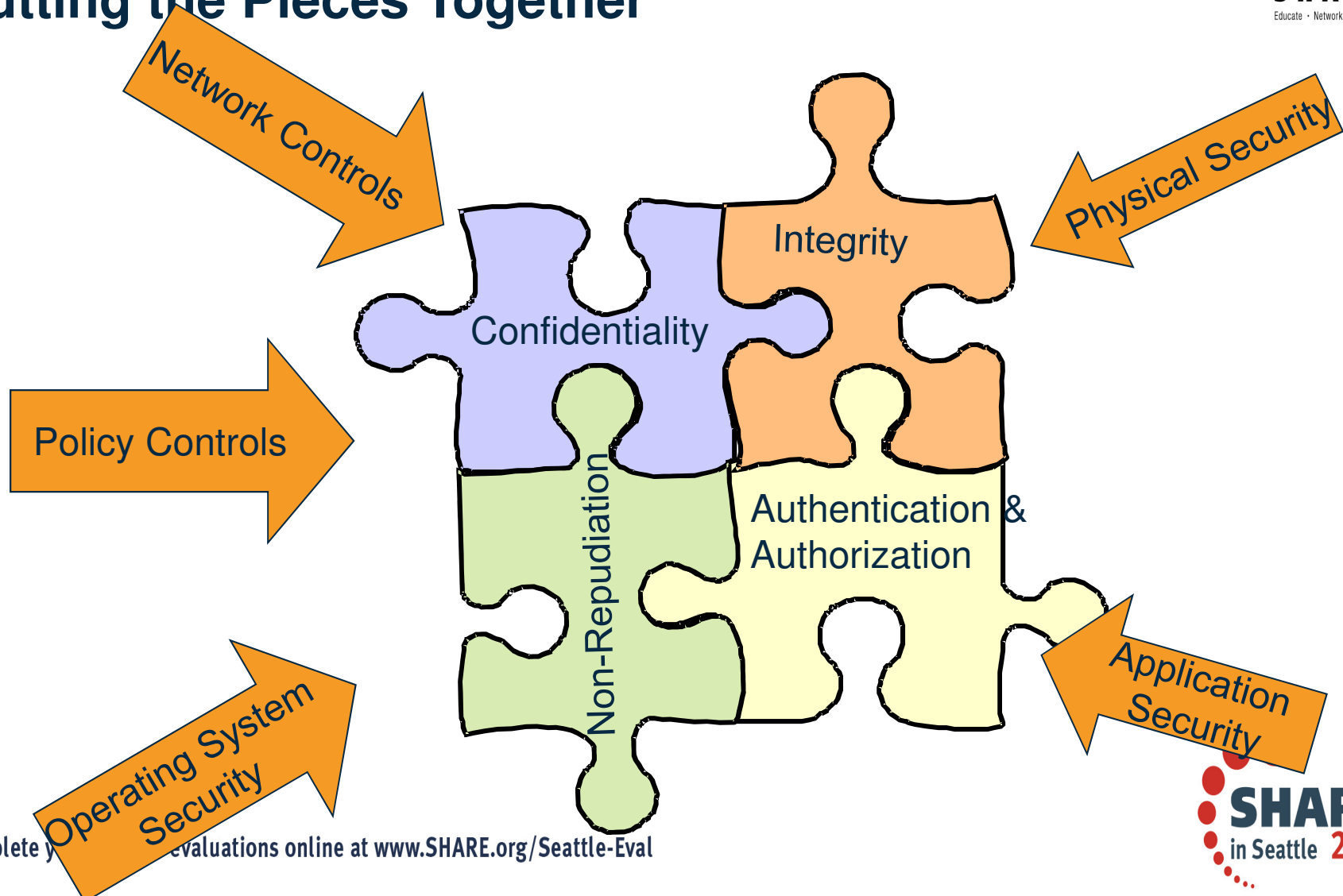
Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)





**SHARE**  
Educate · Network · Influence

# Putting the Pieces Together



Complete your evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# How Does EE Measure UP

- Authorization
  - OS control of datasets
- Access Control
  - APPN Topology Definitions
- Data Confidentiality
  - Session Level Encryption (static)
- Data Integrity
  - Checksums
- Non-Repudiation
  - None



More is  
needed!!!!

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## EE with VPN

- Authorization
  - EE Traffic can be authenticated with x.509 Certificates
- Access Control
  - Have to have the properly negotiated keys
- Data Confidentiality
  - Can Take advantage of AES or Triple DES encryption and Dynamic Key creation
- Data Integrity
  - IPSec has built in integrity checks
- Non-Repudiation
  - If you are using “End to End” VPNs the certificate you negotiate with had to come from a known party

# Agenda

- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# Modeling the EE traffic

- What is EE from an IP Perspective
  - Uses UDP
  - Ports 12000 – 12004
    - 12000 – Signaling
    - 12001 – EE Network Flow Control
    - 12002 – High Priority Traffic
    - 12003 – Medium Priority Traffic
    - 12004 – Low Priority Traffic
  - Using Static VIPA Addresses

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# Agenda

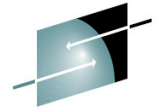
- Reasons for Security
- Overview of Security
- Modeling EE Traffic
- Overview of VPN
- Demo of EE over VPN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

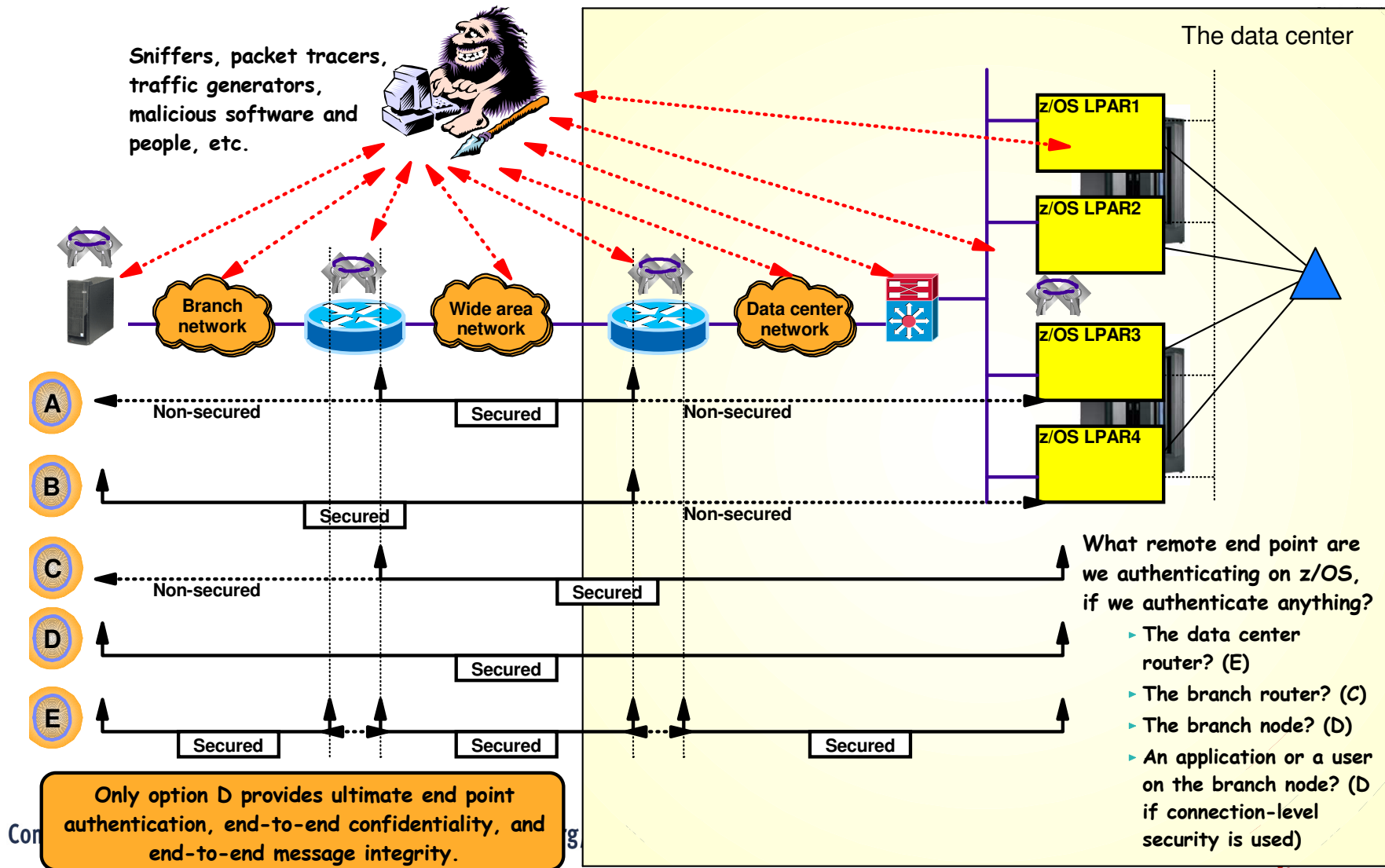
# IPSec Overview

- Increasing the Network Security Layer
- Created for IPv6
- Adopted for IPv4
- Dynamic Key Exchange
  - Internet Key Exchange (IKE) – Uses UDP 500
  - Two phases to this
- Available on most platforms
- Two Protocols
  - AH
  - ESP
- Two modes
  - Tunnel Mode
  - Transport – Can only be used in end to end case

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# So What does End to End Mean



Con

g

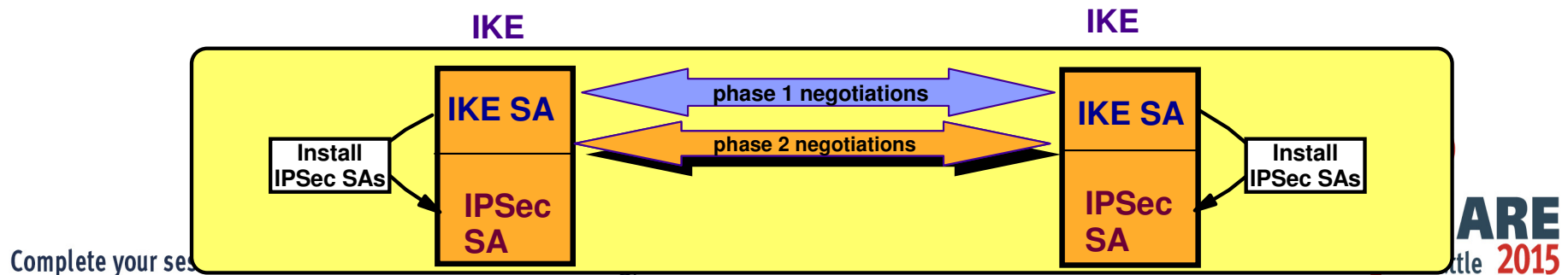
# Break down of VPN

## ➤ Phase 1 negotiation

- ▶ Creates a secure channel with a remote security endpoint
  - Negotiates an IKE SA
    - Generates cryptographic keys that will be used to protect Phase 2 negotiations and Informational exchanges
    - Authenticates the identity of the parties involved
    - Bidirectional, and not identified via SPIs
- ▶ Requires processor-intensive cryptographic operations
- ▶ Done infrequently

## ➤ Phase 2 negotiation

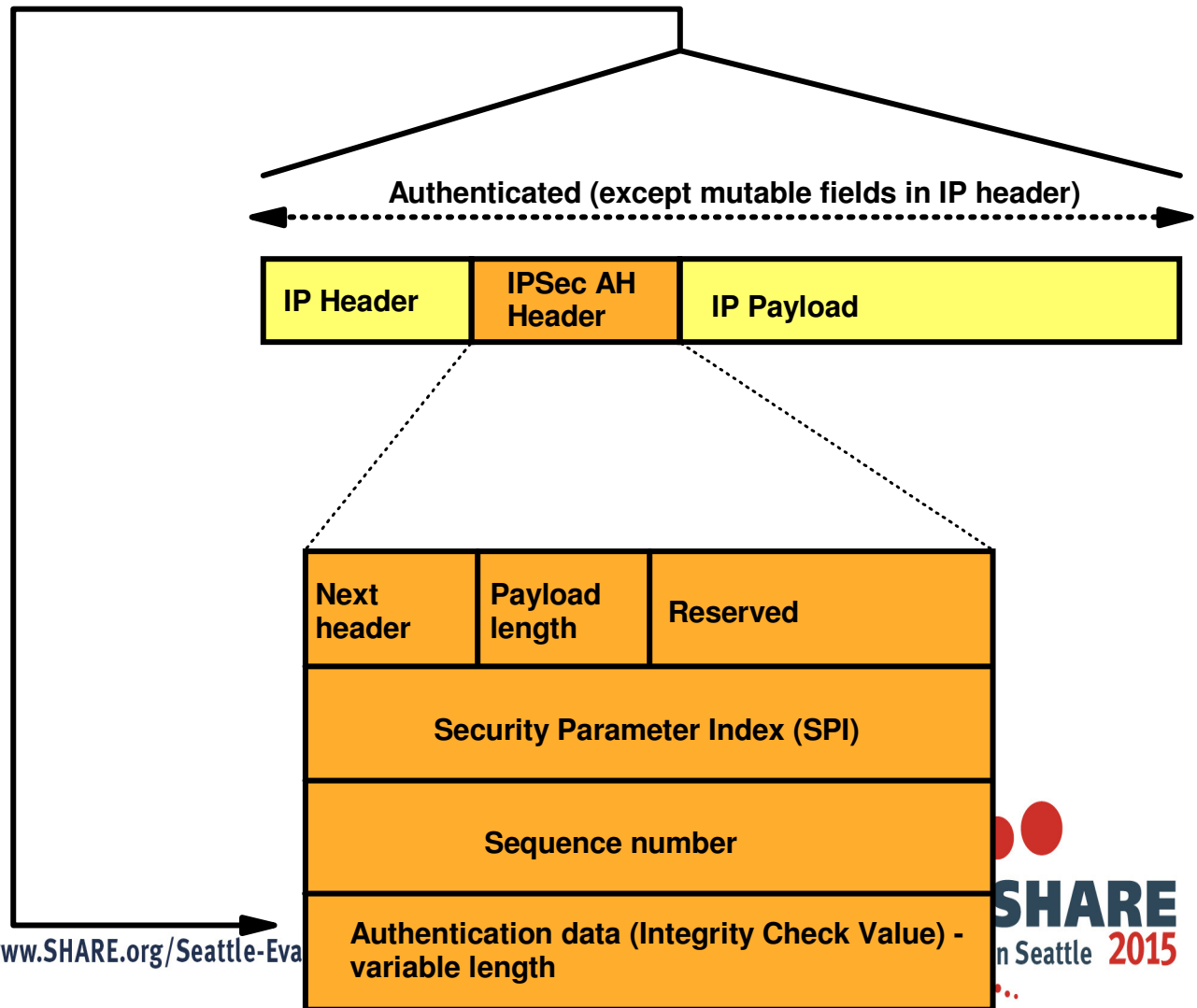
- ▶ Negotiates a pair of IPsec SAs with a remote security endpoint
  - Generates cryptographic keys that are used to protect data
    - Authentication keys for use with AH
    - Authentication and/or encryption keys for use with ESP
- ▶ Performed under the protection of an IKE SA
- ▶ Done more frequently than phase 1



Complete your ses

# Make up of an Authentication Header packet (AH)

IP Protocol number 51



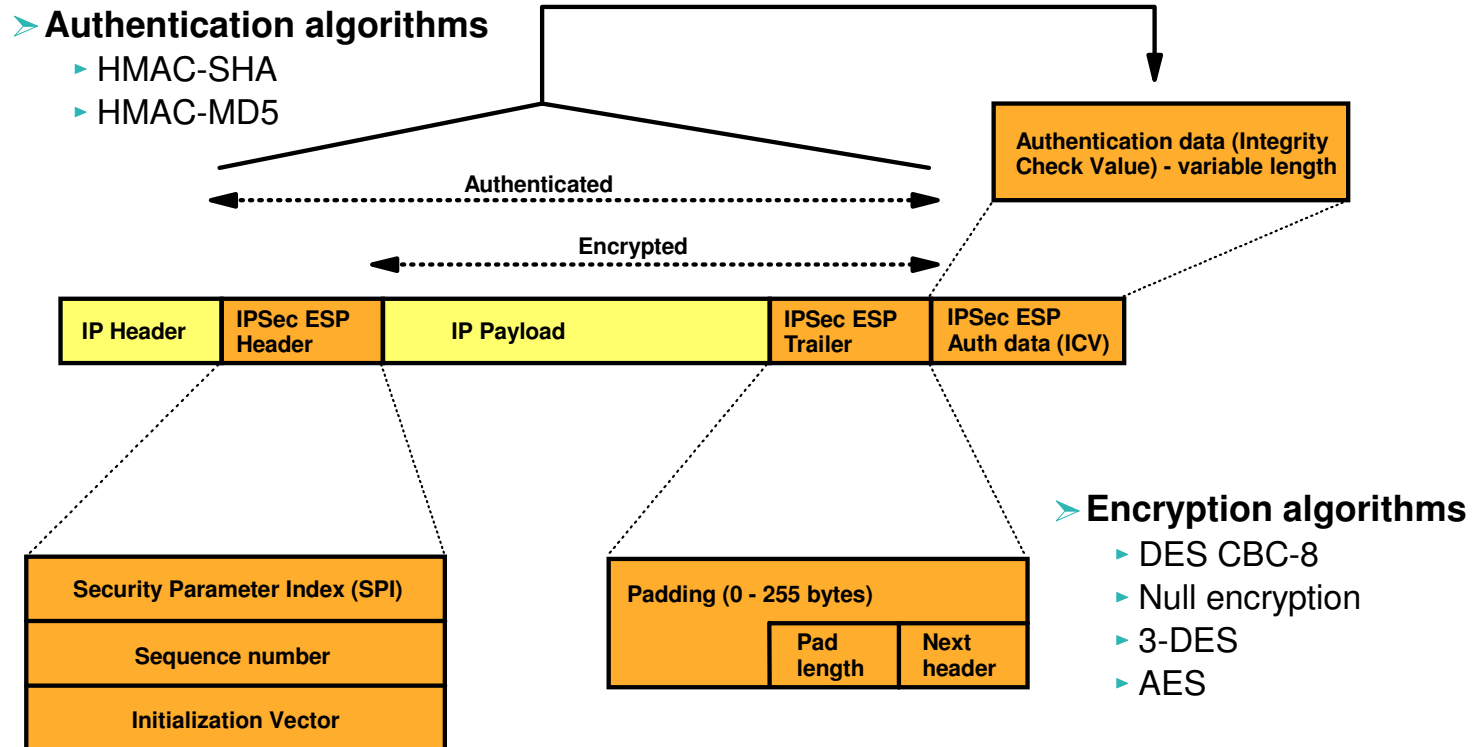
➤ Authentication algorithms

- ▶ HMAC-SHA
- ▶ HMAC-MD5

Complete your session evaluations online at [www.SHARE.org/Seattle-Eva](http://www.SHARE.org/Seattle-Eva)

# Make up of an Encapsulated Security Payload (ESP)

**IP Protocol number 50**



- If transport mode, then "Payload" contains the original transport header and original data (possibly encrypted)
- If tunnel mode, then "Payload" contains original IP header, original transport header, and original data
  - ▶ "Payload" can be encrypted

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

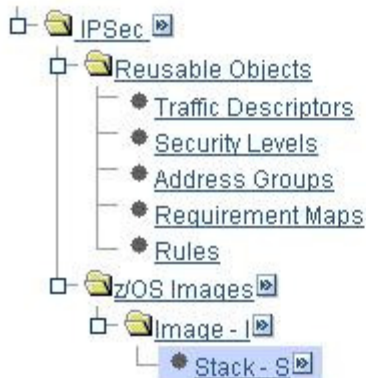


## Tip for IPSEC

- Use the z/OSMF tool to configure your IPsec VPN (Only tool for V2R1 and above)
- <http://www-03.ibm.com/systems/z/os/zos/features/zosmf/>

### IPSec Perspective

Navigation tree



The screenshot shows the 'Local Addresses' tab in the IPsec Perspective tool. The 'Local Addresses' tab is highlighted with a red box. Below the tab is a table with columns: Select, IP Address, Name, and Discovered Information. The table contains several rows of data, with the row for IP Address 3.3.3.3 and Name local\_3 selected.

Select	IP Address	Name	Discovered Information
<input type="radio"/>	6.7.7.7	local1	
<input type="radio"/>	5.5.5.5	ipv4_a	
<input type="radio"/>	4.4.4.4	local2	
<input checked="" type="radio"/>	3.3.3.3	local_3	
<input type="radio"/>	2.2.2.2	ipv4	
<input type="radio"/>	1.1.1.1	OSA	

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



# Agenda

- Reasons for Security
- Overview of Security
- Overview of VPN
- Modeling EE Traffic
- Demo of EE over VPN

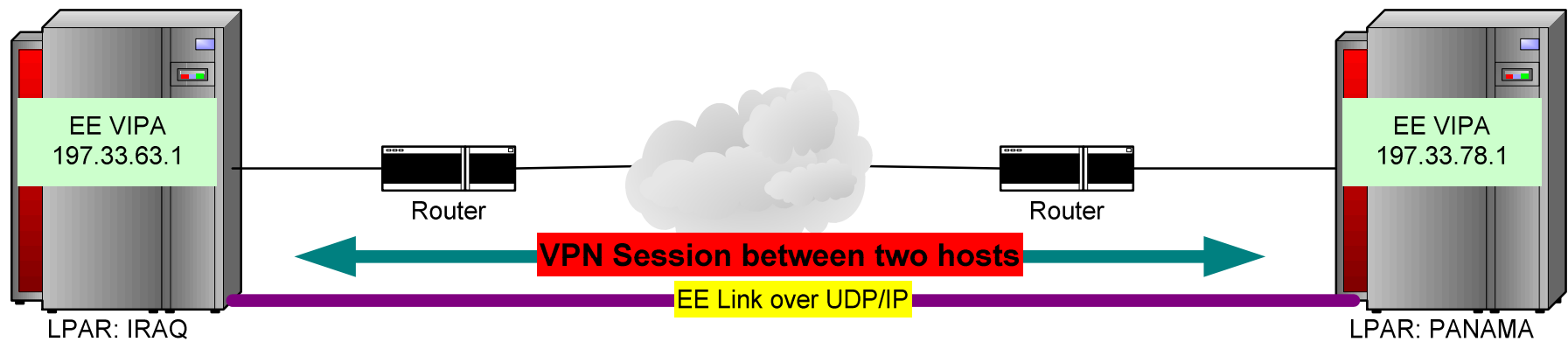
Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

## Some preparation needed

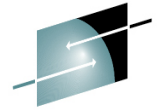
- IPCONFIG IPSECURITY (Replace IPCONFIG FIREWALL)
- POLICY AGENT SETUP
- EE Deck Creation
  - XCA
  - SMN

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# Overview of the Demo



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



**SHARE**  
Educate · Network · Influence

# The Demo!!!

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)



## Useful commands

- D NET,EE
- D NET,EE,IPADDR=static Vipa
- D NET,EEDIAG
- D TCPIP,<stack>,n,config
- ipsec -y display
- ipsec -k display

## This Demo is on the Web

- On August 13<sup>th</sup> of 2008 this demo from beginning to end will be available for you to watch on the web

Communication Server Security Site

<http://www-306.ibm.com/software/network/commserver/zos/security/>



Direct Link

<http://www.ibm.com/support/docview.wss?rs=852&uid=swg27013261>

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

# For more information



URL		Content
<a href="http://www.twitter.com/IBM_Commserver">http://www.twitter.com/IBM_Commserver</a>		IBM Communications Server Twitter Feed
<a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a>		IBM Communications Server Facebook Fan Page
<a href="http://www.ibm.com/systems/z/">http://www.ibm.com/systems/z/</a>		IBM System z in general
<a href="http://www.ibm.com/systems/z/hardware/networking/">http://www.ibm.com/systems/z/hardware/networking/</a>		IBM Mainframe System z networking
<a href="http://www.ibm.com/software/network/commserver/">http://www.ibm.com/software/network/commserver/</a>		IBM Software Communications Server products
<a href="http://www.ibm.com/software/network/commserver/zos/">http://www.ibm.com/software/network/commserver/zos/</a>		IBM z/OS Communications Server
<a href="http://www.ibm.com/software/network/commserver/z_lin/">http://www.ibm.com/software/network/commserver/z_lin/</a>		IBM Communications Server for Linux on System z
<a href="http://www.ibm.com/software/network/ccl/">http://www.ibm.com/software/network/ccl/</a>		IBM Communication Controller for Linux on System z
<a href="http://www.ibm.com/software/network/commserver/library/">http://www.ibm.com/software/network/commserver/library/</a>		IBM Communications Server library
<a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a>		ITSO Redbooks
<a href="http://www.ibm.com/software/network/commserver/zos/support/">http://www.ibm.com/software/network/commserver/zos/support/</a>		IBM z/OS Communications Server technical Support – including TechNotes from service
<a href="http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atmastr.nsf/Web/TechDocs</a>		Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
<a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>		Request For Comments (RFC)
<a href="http://www.ibm.com/systems/z/os/zos/bkserv/">http://www.ibm.com/systems/z/os/zos/bkserv/</a>		IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server

Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

 in Seattle 2015

# Don't forget your evals



Complete your session evaluations online at [www.SHARE.org/Seattle-Eval](http://www.SHARE.org/Seattle-Eval)

