#SHAREorg

SHARE

Protecting Enterprise Extender Traffic with a VPN

IBM Lab Services
Thomas Cosenza, CISSP
tcosenza@us.ibm.com

SHARE in Boston

Agenda

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

Why Add Security

- ID theft is on the rise
- Meet new standards
  - PCI standard (Session S1713)
  - European Common Standard
  - US regulations starting to come around
    - *California SB 1386*
- Keep the business out of the paper

Why Add Security

- Failure to Secure your business
  - Fines and penalties
  - Incidents from loss of credit card holder data
    - *Costs for forensics examinations*
    - *Liability for card issuers*
    - *Dispute resolution costs*
  - Stock Shares plummet
  - Loss of Customers

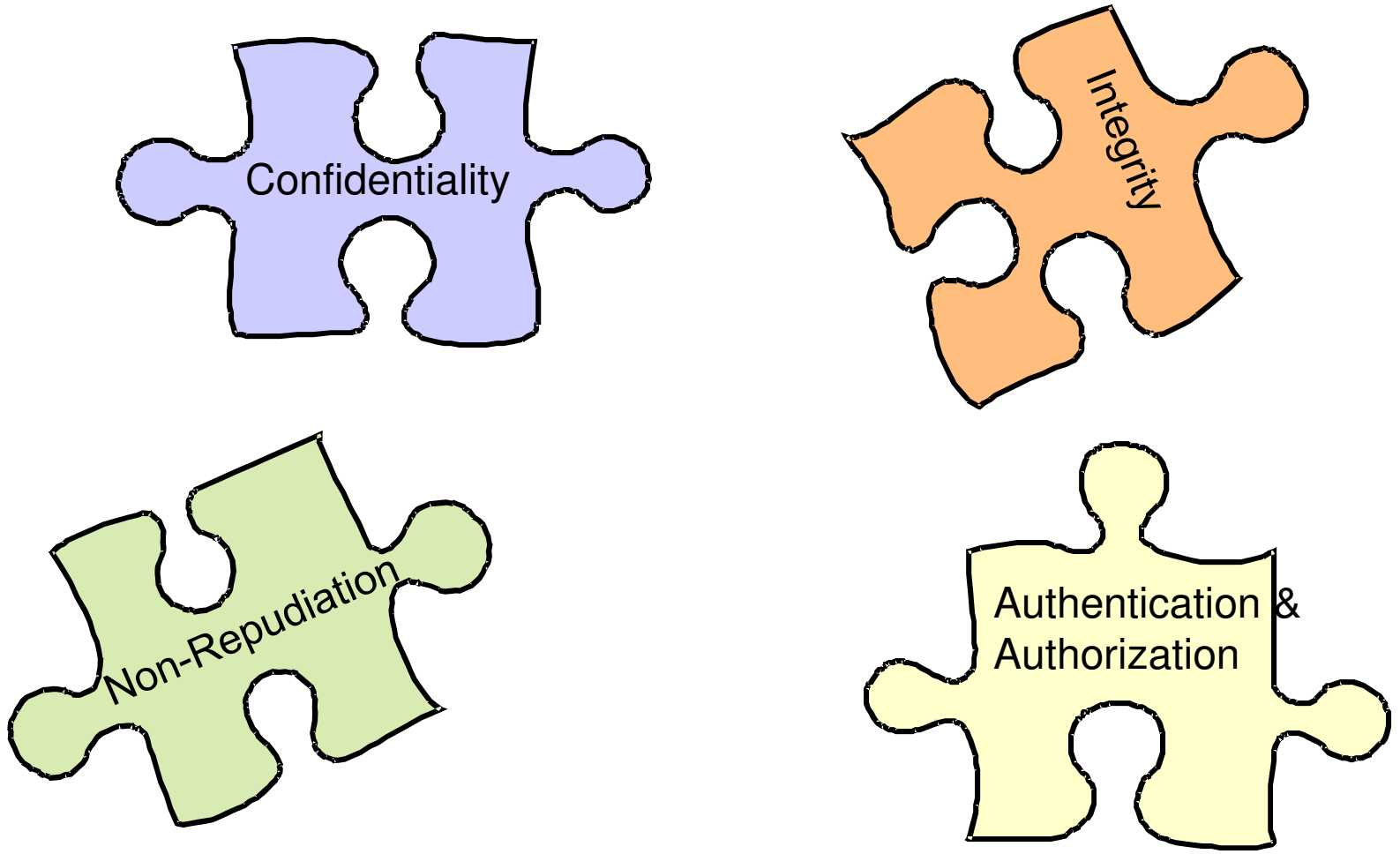
Words to Live By

- "The Security Perimeter is now at the End Point" Anonymous

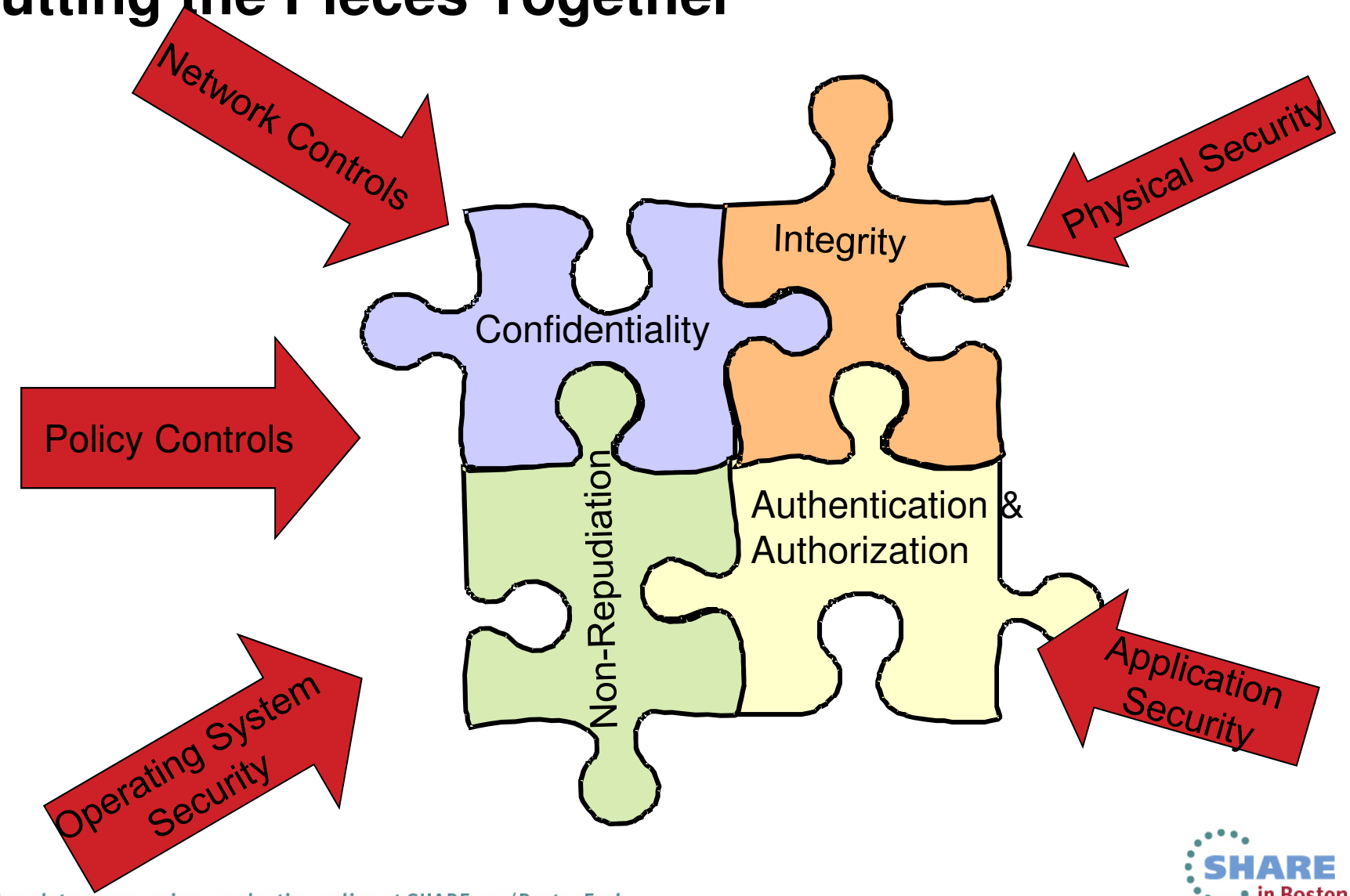
Agenda

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

The Puzzle pieces of Security



Putting the Pieces Together



How Does EE Measure UP

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

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

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

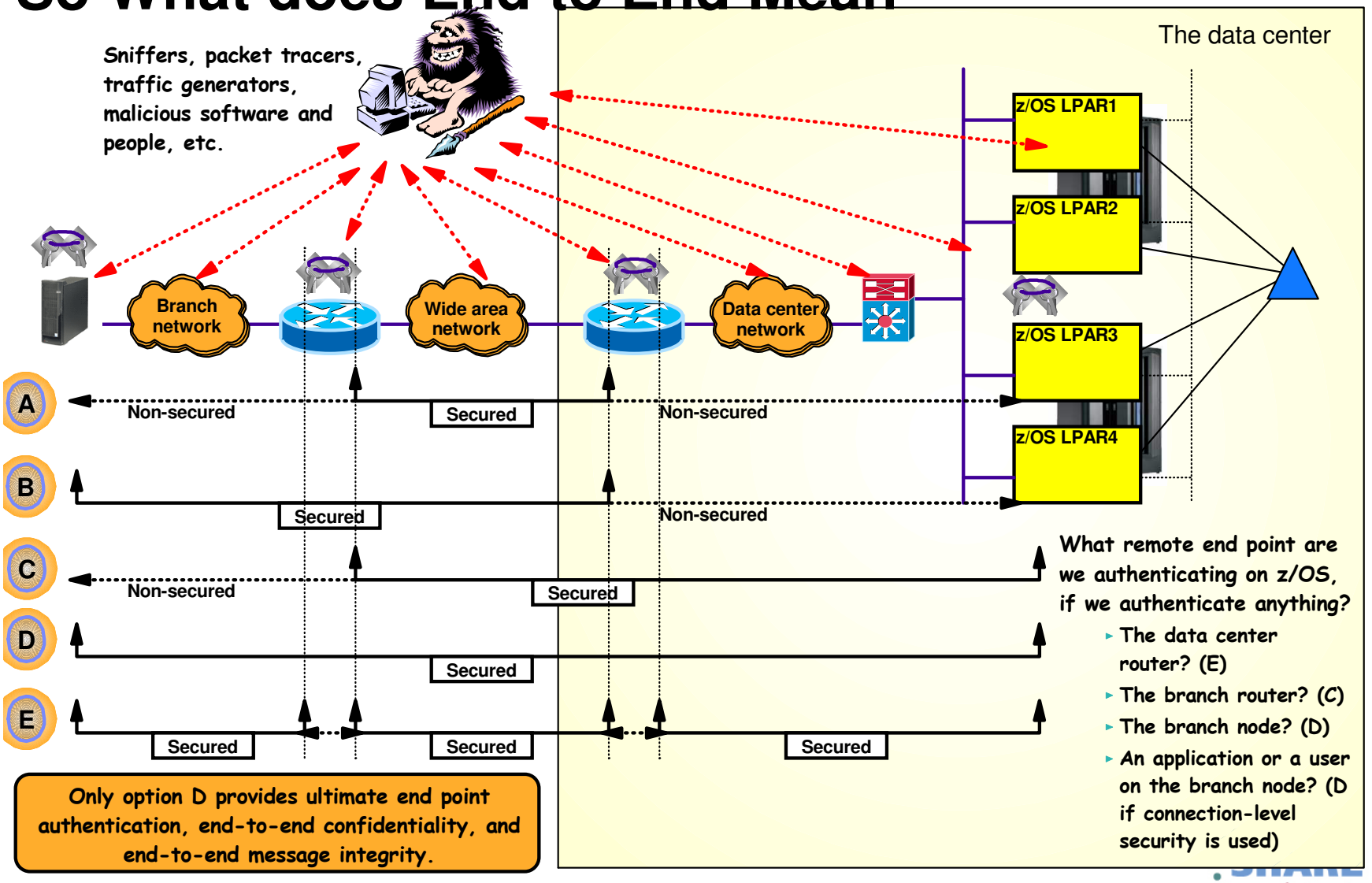
Agenda

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

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

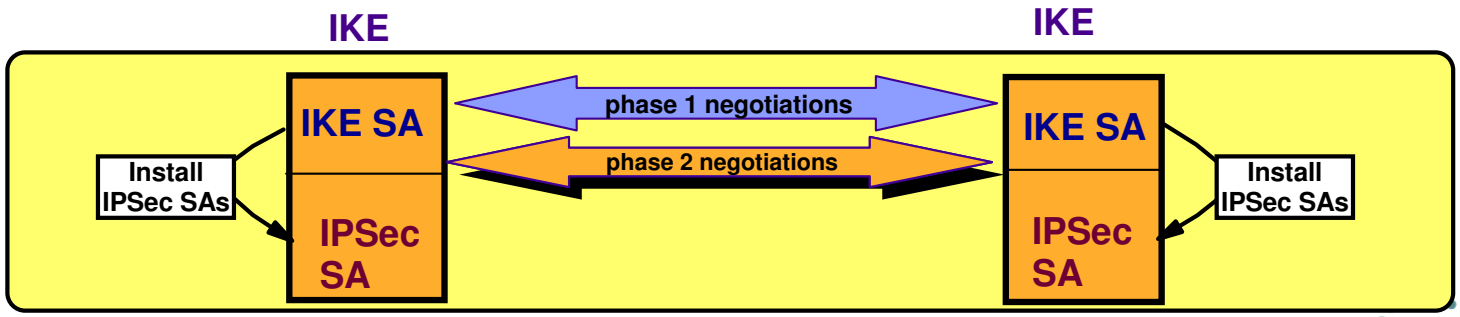
So What does End to End Mean



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

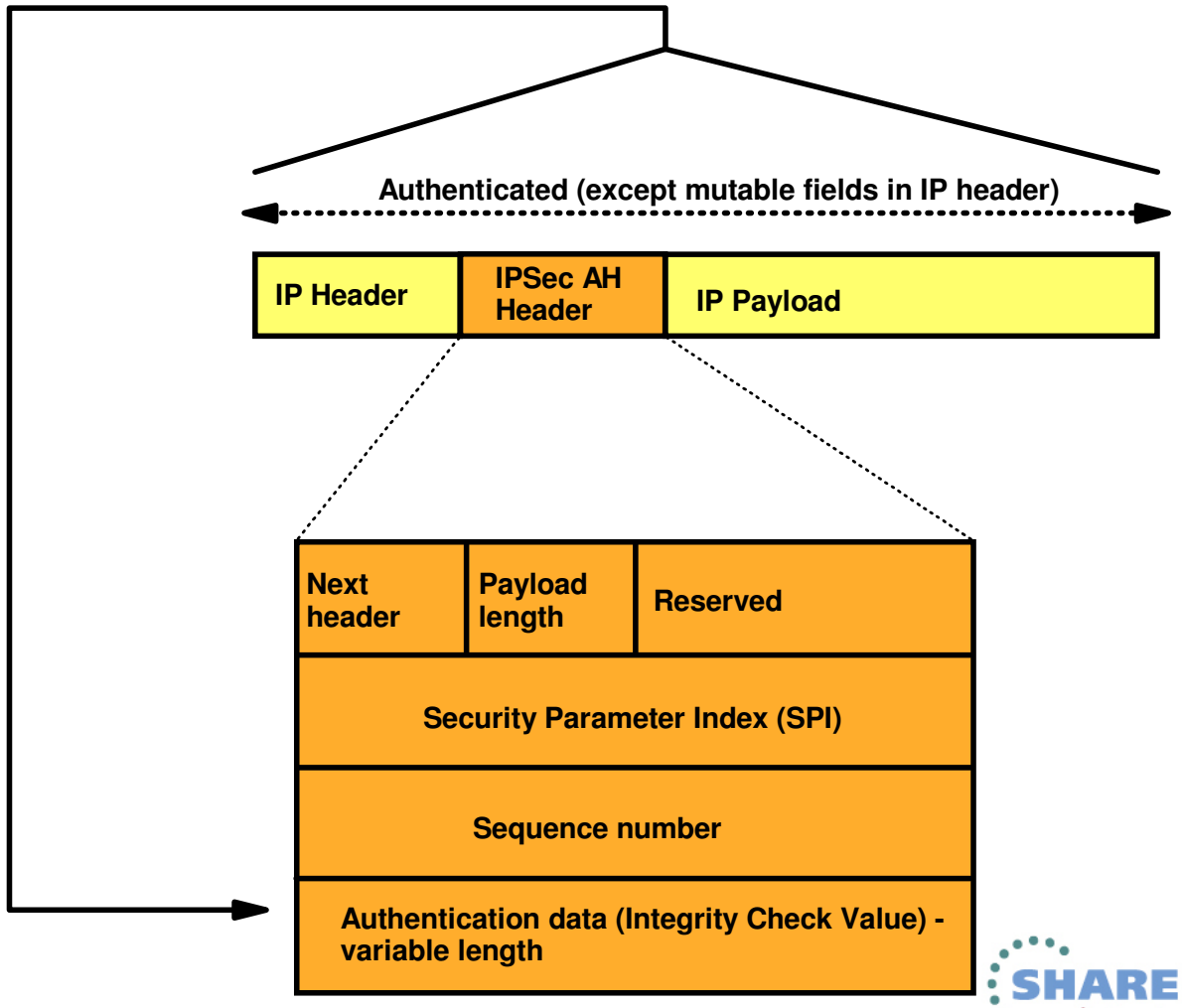
- **Phase 2 negotiation**
  - Negotiates a pair of IPSec SAs with a remote security endpoint
    - Generates cryptographic keys that are used to protect data
      - Authentication keys for use with AH
      - Authentication and/or encryption keys for use with ESP
  - Performed under the protection of an IKE SA
  - Done more frequently than phase 1



Make up of an Authentication Header packet (AH)

IP Protocol number 51

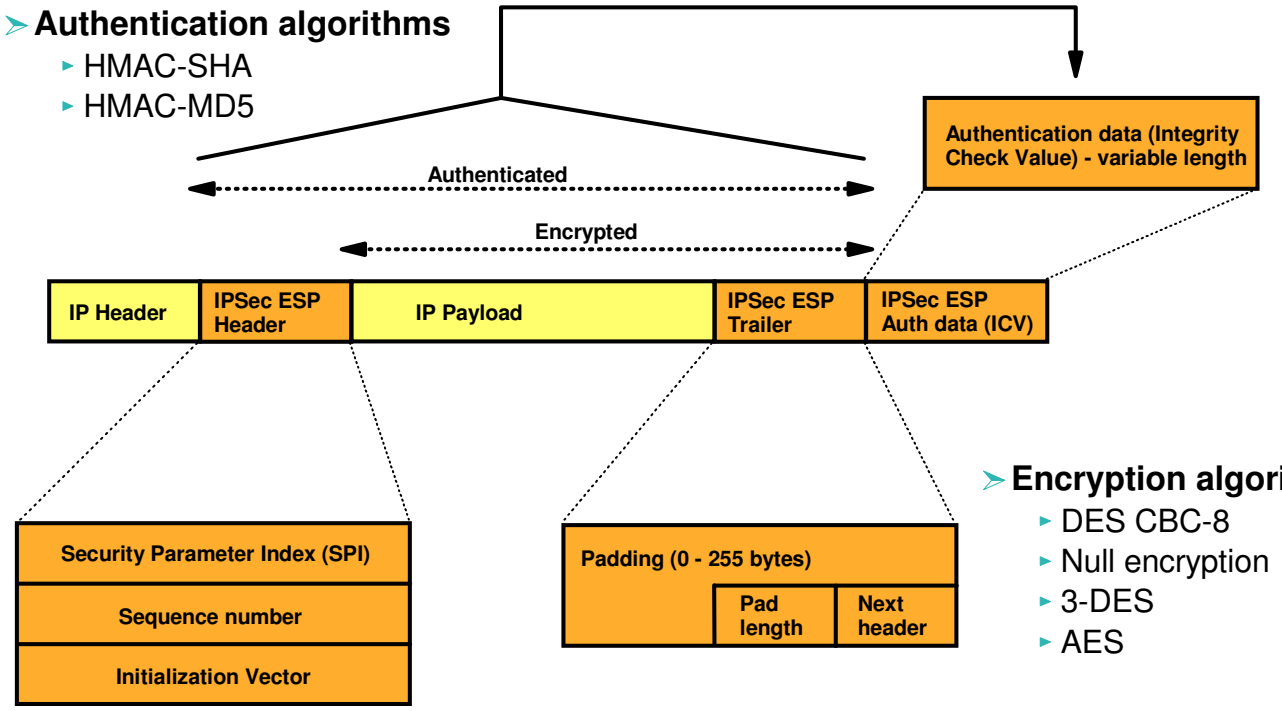
- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



Make up of an Encapsulated Security Payload (ESP)

IP Protocol number 50

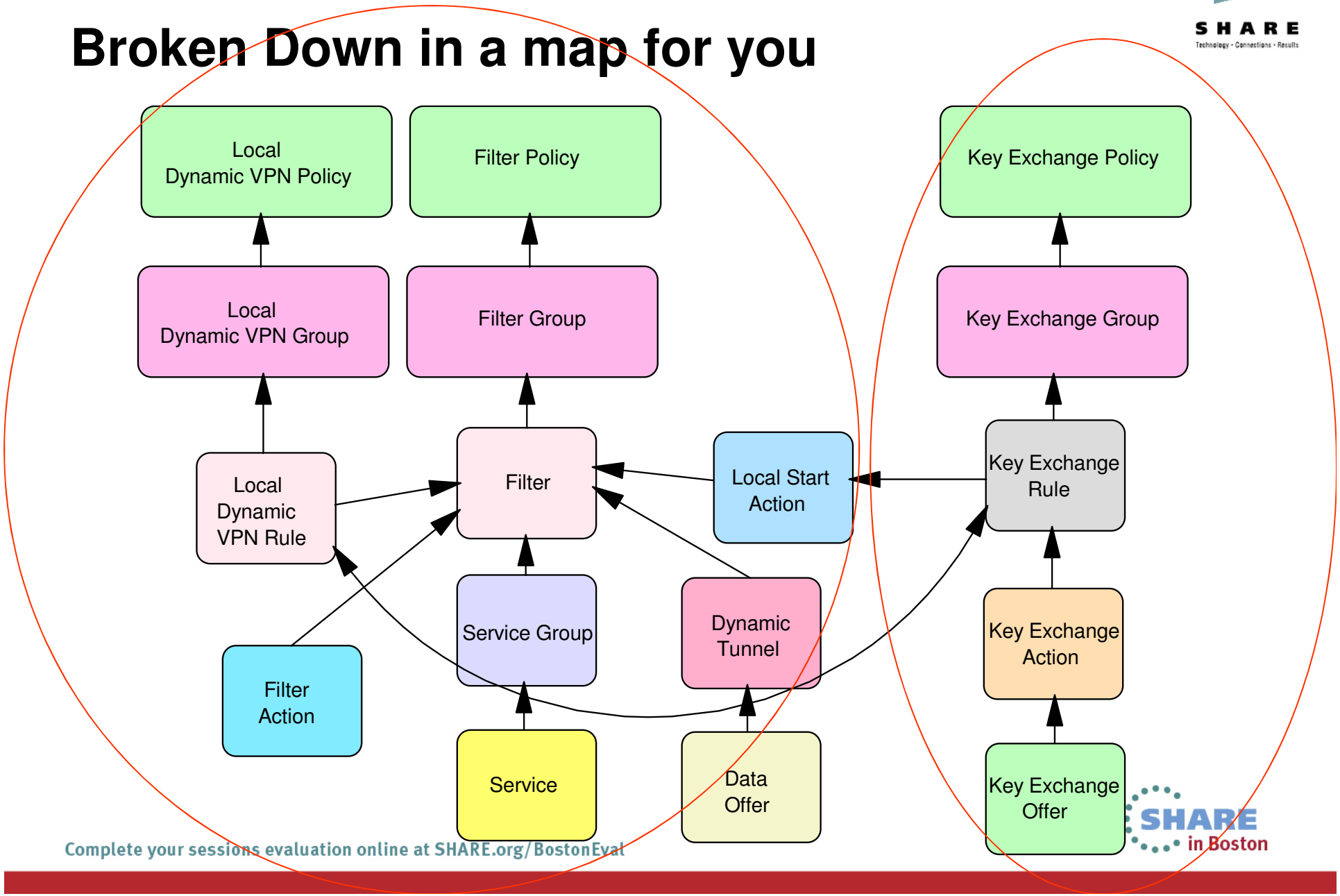
- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



- **Encryption algorithms**
  - DES CBC-8
  - Null encryption
  - 3-DES
  - AES

- **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

Broken Down in a map for you



Tip for IPSEC

- Use the IBM Configuration Assistant for z/OS Communications Server
- Pre V2R1
  - http://www-306.ibm.com/software/network/commserver/
- V2R1 You will need to use zOSMF
  - Note zOSMF is available for V1R12 and higher

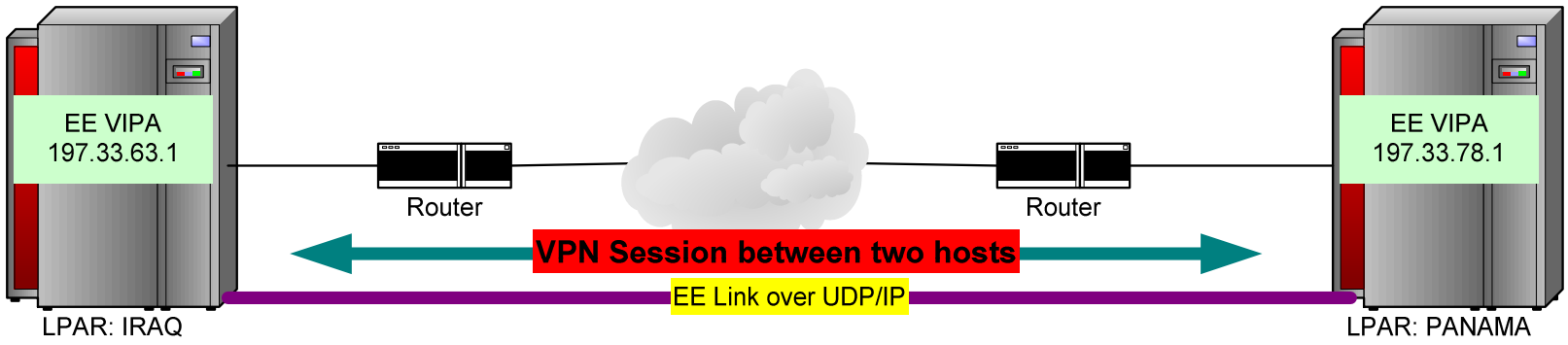
Agenda

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

Some preparation needed

- IPCONFIG IPSECURITY
- POLICY AGENT SETUP
- EE Deck Creation
  - XCA
  - SMN
- You may want to invest in a zIIP

Overview of the Demo




The Demo!!!

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 13th 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

For more information ...

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