



GSE 2009: Protecting Enterprise Extender Traffic with a VPN

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

IBM Raleigh Development Lab
Michael Fitzpatrick

IBM Systems

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
 - HIPPA
 - SOX
 - 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
 - Dispute resolution costs
 - Stock Shares plummet
 - Loss of Customers

Words to Live By

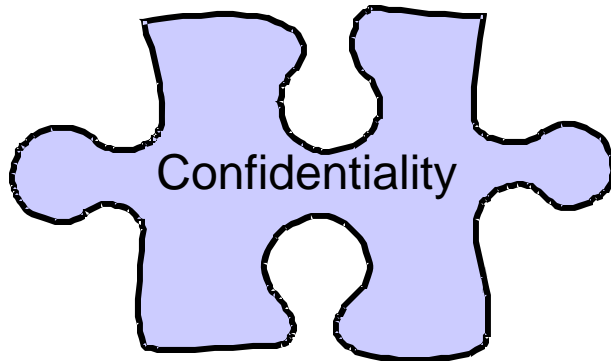
- **“The Security Perimeter is now at the End Point”**
Anonymous



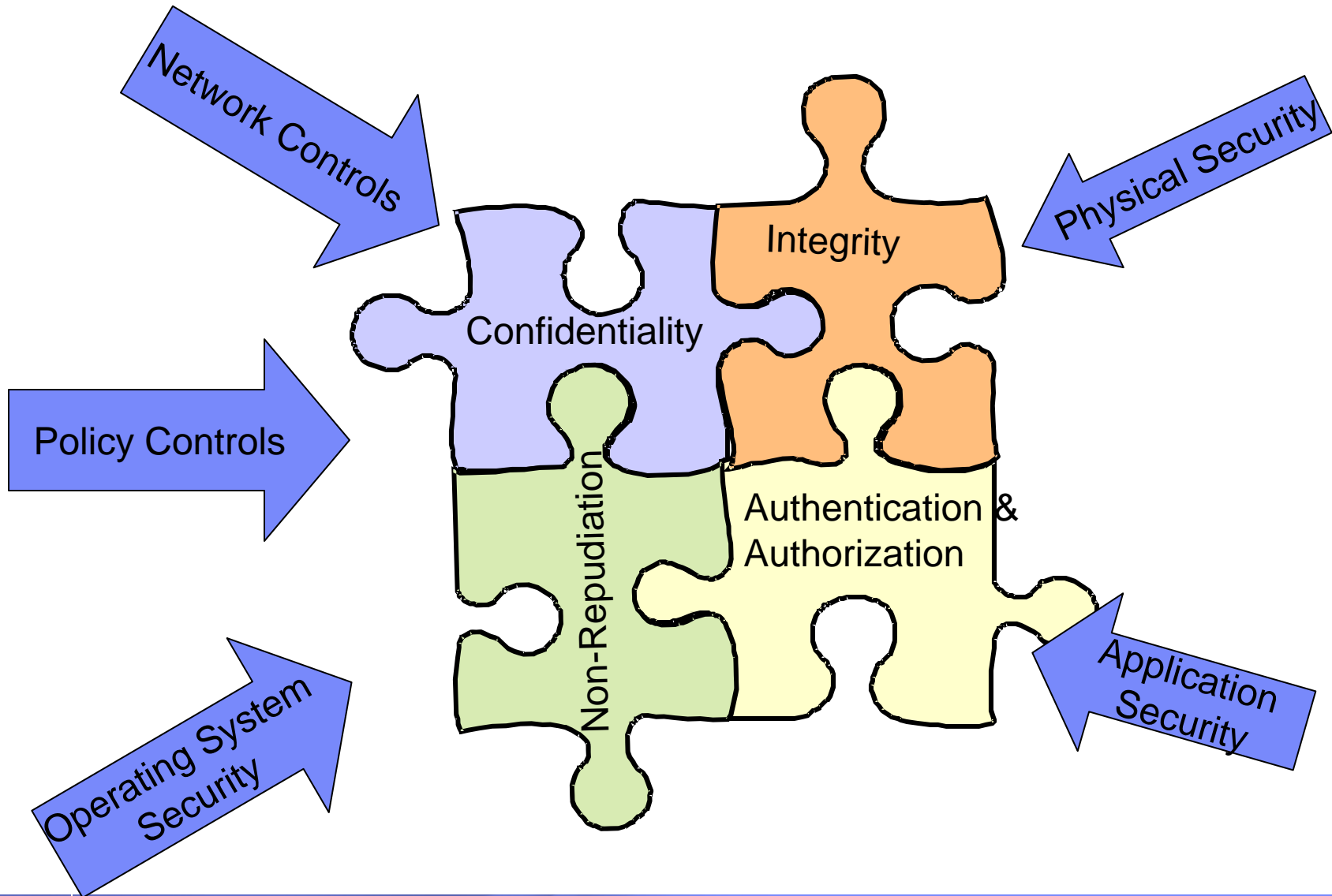
Agenda

- **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



*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

How Does EE Measure UP

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



More is
needed!!!!

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

Agenda

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

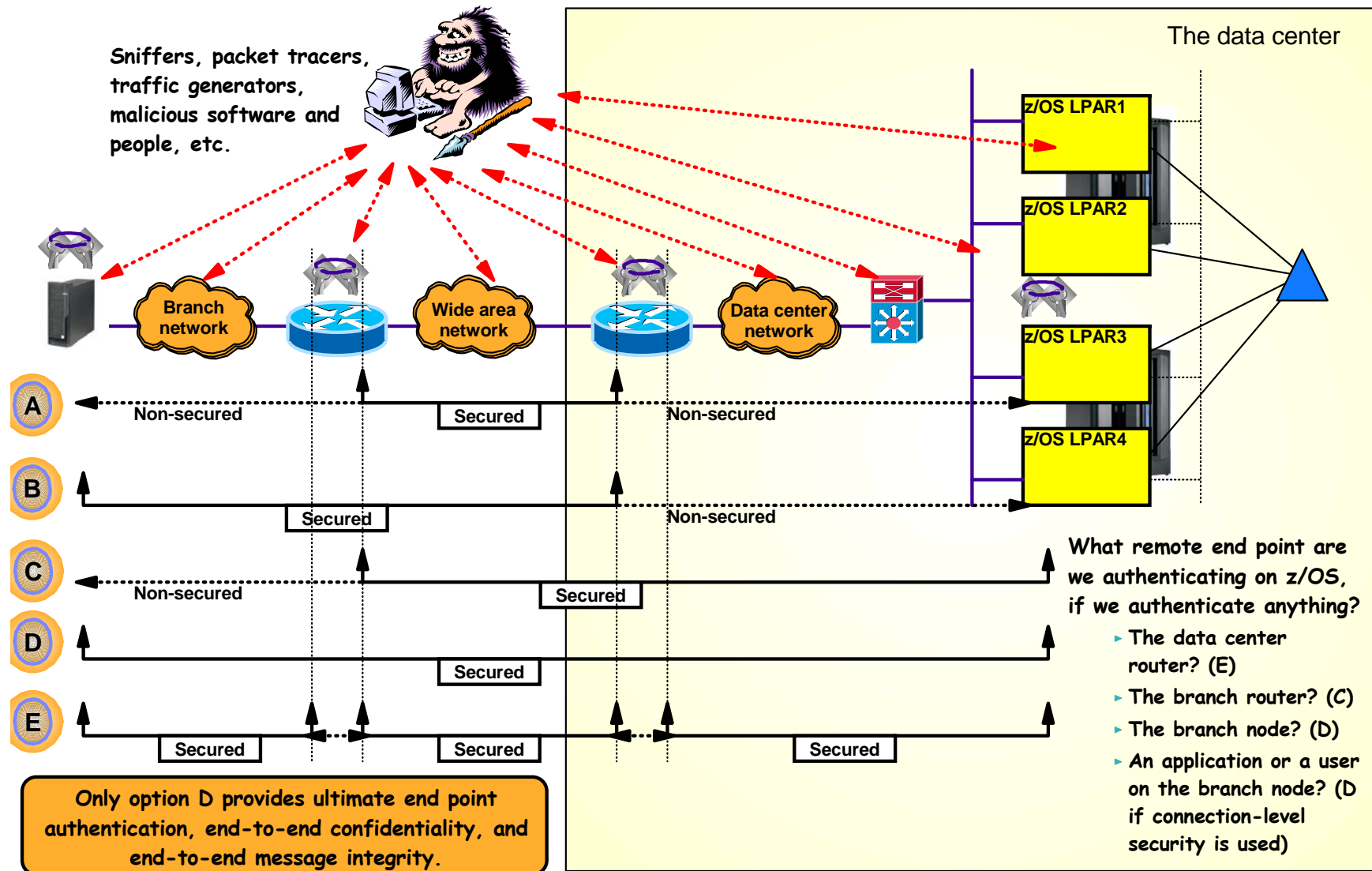
IPSec Overview

- **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**

* IBM is not a law firm and does not have the authority to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

So What does End to End Mean



*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

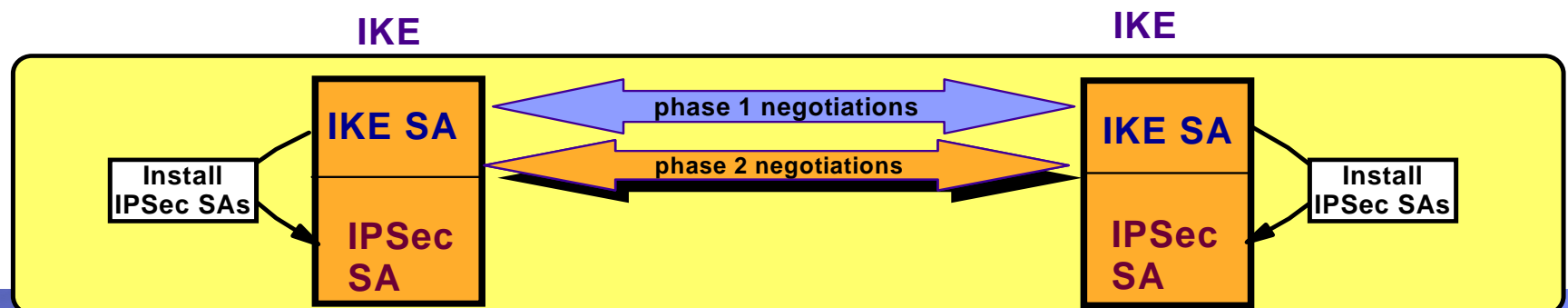
Break down of VPN

➤ 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

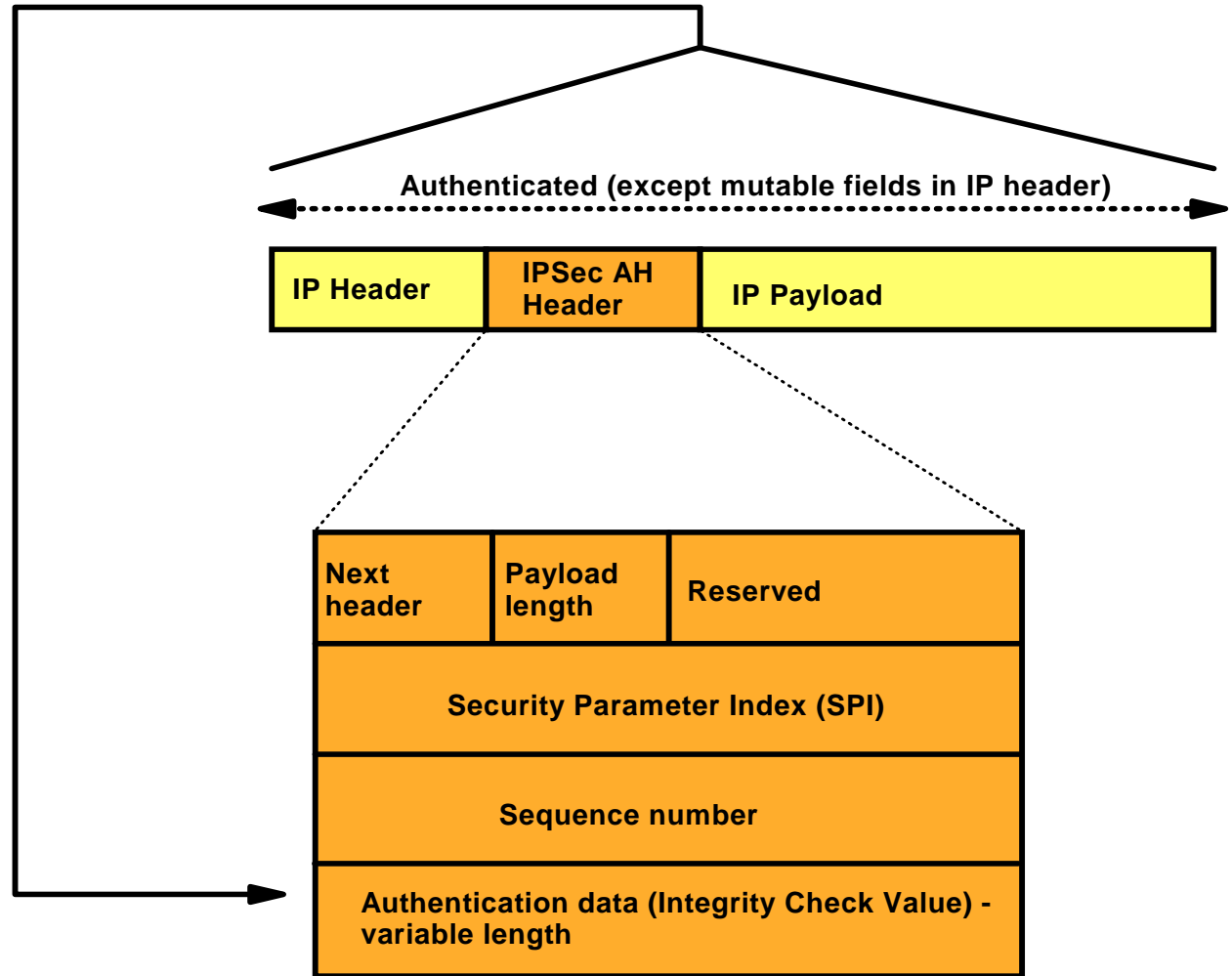
➤ Phase 2 negotiation

- ▶ 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

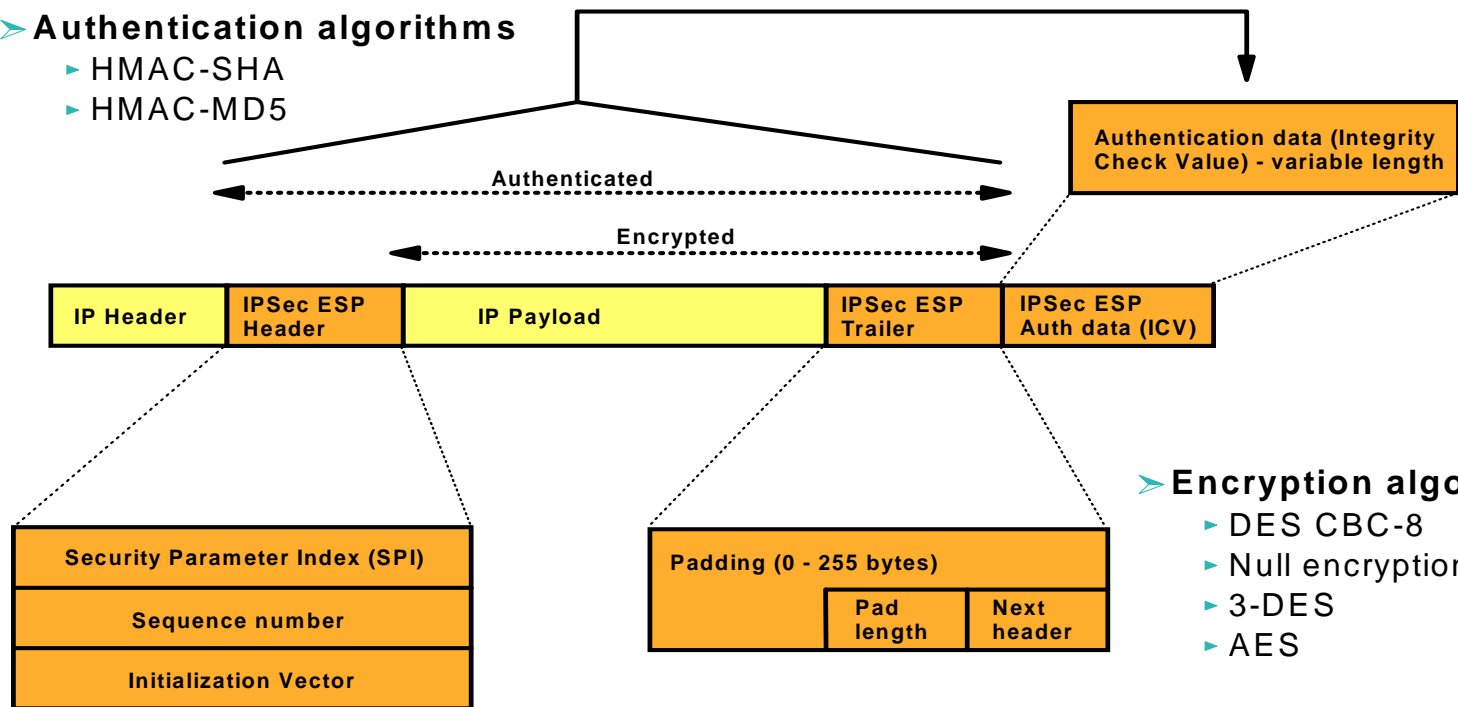
- ▶ HMAC-SHA
- ▶ HMAC-MD5

Make up of an Encapsulated Security Payload (ESP)

IP Protocol number 50

➤ Authentication algorithms

- ▶ HMAC-SHA
- ▶ HMAC-MD5



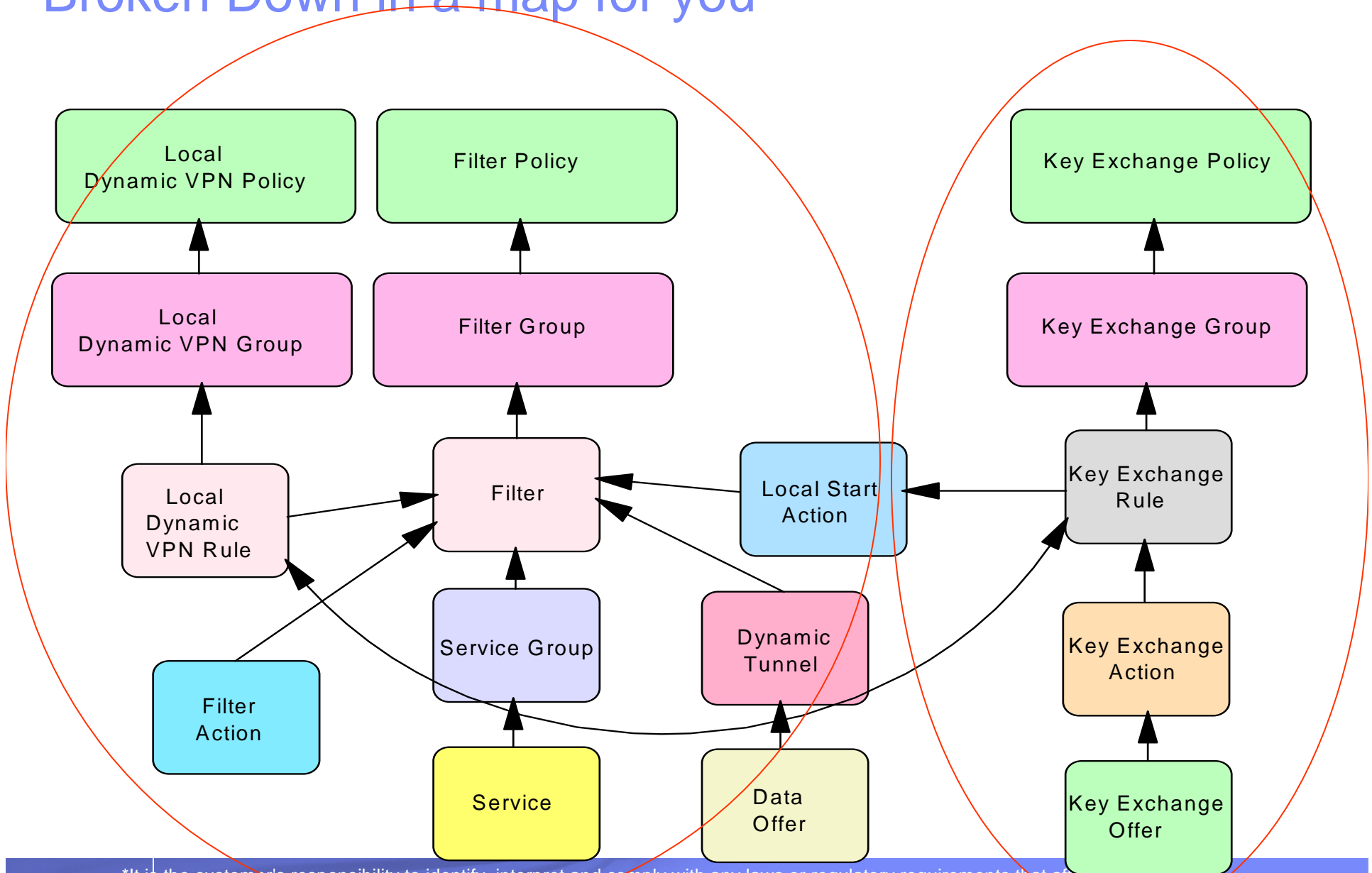
➤ Encryption algorithms

- ▶ 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

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Broken Down in a map for you



*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

Tip for IPSEC

- Use the IBM Configuration Assistant for z/OS Communications Server
- <http://www-306.ibm.com/software/network/commserver/>

*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

- [1]** [IBM Configuration Assistant for z/OS Communications Server](#) 2007-08-07
 IBM Configuration Assistant for z/OS Communications Server provides centralized configuration of AT-TLS, IP Security, NSS, PBR, QoS, and IDS policies.
 [More items like this found in [Enterprise Connectivity](#)]
 [This item's topic: Configuration]

Download package

Download	RELEASE DATE	LANGUAGE	SIZE (Bytes)	Download Options
All releases (V1R9; V1R8; V1R7)	8/10/2007	English	78291621	HTTPS

Download using http

To use http to download click on the 'Download now' button below

V1R9 IBM Configuration Assistant for z/OS Communications Server (8/7/2007)

ConfigAssistV1R9Setup.exe (74.6MB)

 [Download now](#)

V1R8 IBM Configuration Assistant for z/OS Communications Server (3/30/2007)

ConfigAssistV1R8Setup.exe (54.1MB)

 [Download now](#)

V1R7 z/OS Network Security Configuration Assistant (2/21/2007)

zNetworkSecuritySetup.exe (47.6MB)

 [Download now](#)

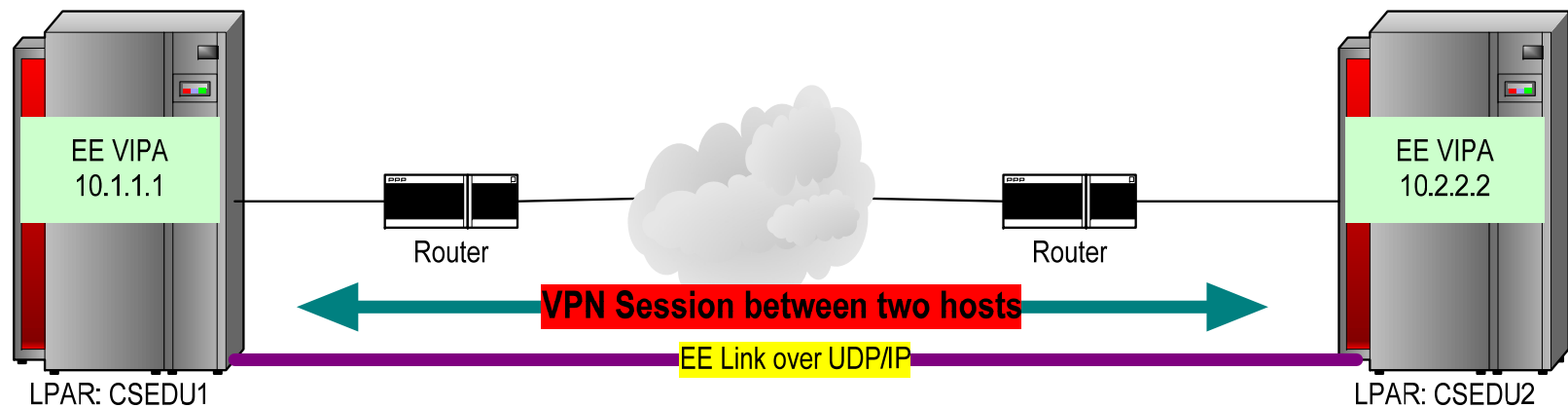
Agenda

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

Some preparation needed

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

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 <-r wide>**
- **ipsec -k display**

This Demo is on the Web

- 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>

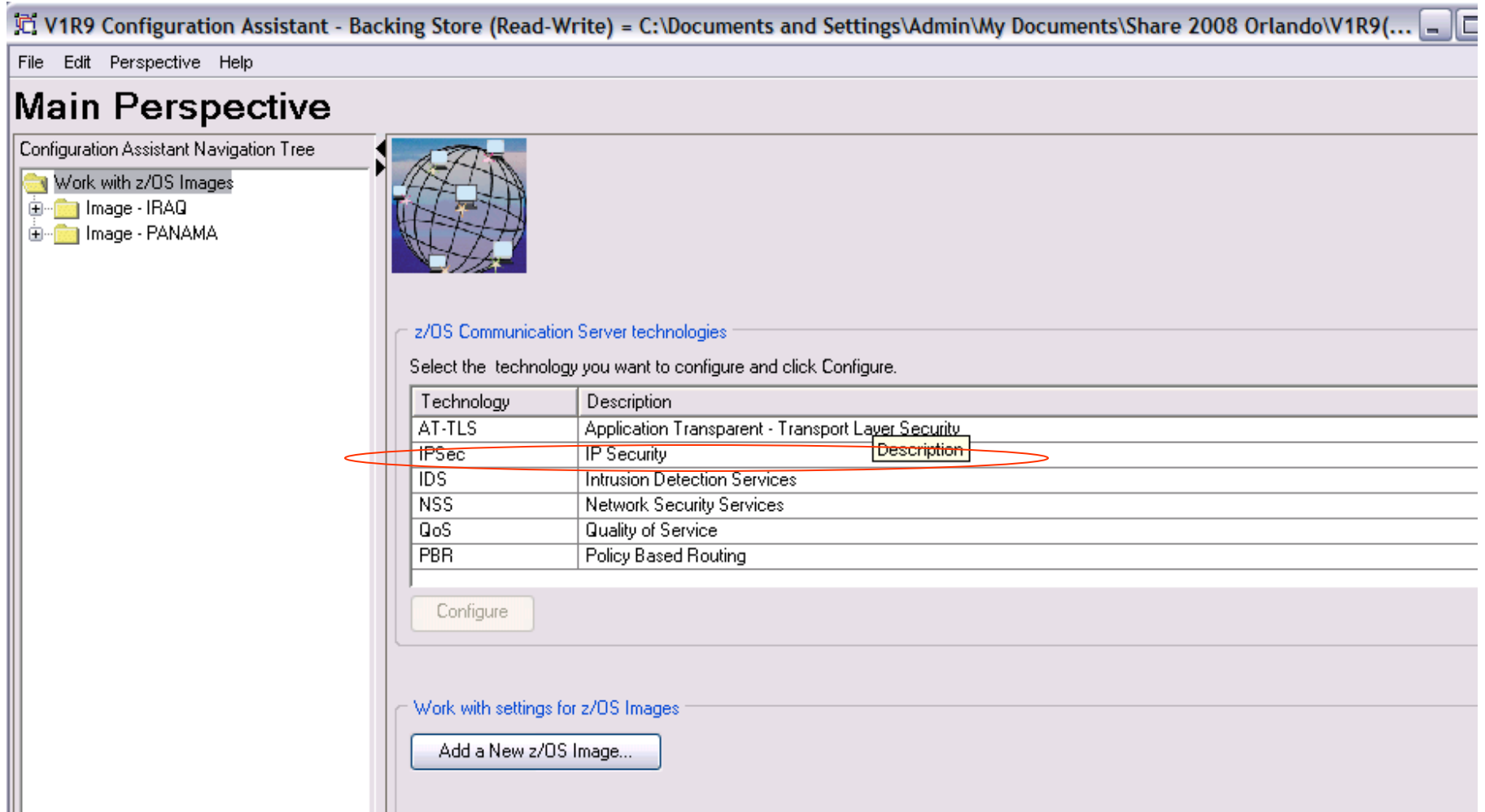
For More Information....

URL	Content
http://www.ibm.com/systems/z/	IBM System z
http://www.ibm.com/systems/z/hardware/networking/index.html	IBM System z Networking
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 zSeries
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library	IBM Communications Server Library - white papers, product documentation, etc.
http://www.redbooks.ibm.com	IBM Redbooks
http://www.ibm.com/software/network/commserver/support	IBM Communications Server Technical Support
http://www.ibm.com/support/techdocs/	Technical Support Documentation (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFCs)
http://publib.boulder.ibm.com/infocenter/ieduasst/stgy1r0/index.jsp	IBM Education Assistant

APENDIX

- **See the following slides for the Gui**

How do you do it



V1R9 Configuration Assistant - Backing Store (Read-Write) = C:\Documents and Settings\Admin\My Documents\Share 2008 Orlando\V1R9(...)

File Edit Perspective Help

Main Perspective

Configuration Assistant Navigation Tree

- Work with z/OS Images
 - Image - IRAQ
 - Image - PANAMA

z/OS Communication Server technologies

Select the technology you want to configure and click Configure.

Technology	Description
AT-TLS	Application Transparent - Transport Layer Security
IPSec	IP Security
IDS	Intrusion Detection Services
NSS	Network Security Services
QoS	Quality of Service
PBR	Policy Based Routing

Configure

Work with settings for z/OS Images

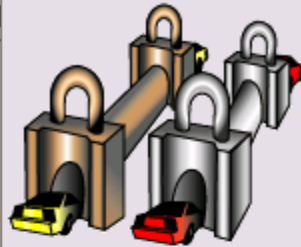
Add a New z/OS Image...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Image - PANAMA



List of all defined Requirement Map objects

Name ▲	Description
Basic_Connectivity	These are the basic connectivity rules for operation
DENYALL	Always at the bottom of the list
Filtering	IBM supplied: IPSec sample - Filtering (uses only Permit and Deny Security Levels)
Trusted_Internet_Zone	IBM supplied: IPSec sample - Server to trusted branch office (internet traversed)
Untrusted_Zone	IBM supplied: IPSec sample - Server to untrusted business partner zone

- Add for Beginners...
- Add...
- Copy...
- Modify...
- Delete
- View Details...
- Show Where Used...

IPsec Perspective

New Requirement Map

A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map: 1. Select a Traffic Descriptor from the Objects section.
2. Click the "<-Add" button

To change the Security Level of a Traffic Descriptor: 1. Click the Security Level column in the Requirement Map section
2. Select a new Security Level from the list

1 Name the service

Requirement Map

Name: * ALLOW_IKE
Description: Allow IKE Negotiation

Traffic Descriptor	IPsec - Security Level
IKE	Deny
	IPSec_EE_Authenticate
	IPSec_EE_High
	Deny
	Permit
	IPSec_Gold
	IPSec_Silver
	IPSec_Bronze

1 Change the service to Permit

Objects

- Traffic Descriptor ▲
- FTP-Server
- FTP-Server-SSL
- ICMP-Redirect-IP_V4
- ICMP-Redirect-IP_V6
- ICMP-Time_Expired-IP_V4
- ICMP-Time_Expired-IP_V6
- ICMP-Unreachable-IP_V4
- ICMP-Unreachable-IP_V6
- ICMP-Unreachable-IP_V6**
- IKE-NAPT
- IKE-NAT
- Kerberos
- LBA-Advisor
- LBA-Agent
- LDAP-Server
- LPD

2-Select IKE Traffic Descriptor

Work with Traffic Descriptors...
Work with Security Levels...

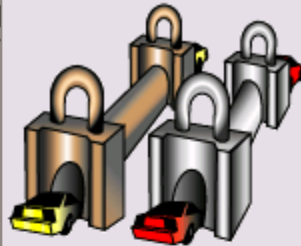
Move Up Move Down View Details... <-Add Remove -> OK Cancel Help ?

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Image - PANAMA



List of all defined Requirement Map objects

Name ▲	Description
ALLOW_IKE	Allow IKE Negotiation
Basic_Connectivity	These are the basic connectivity rules for operation
DENYALL	Always at the bottom of the list
Filtering	IBM supplied: IPSec sample - Filtering (uses only Permit and Deny Security Levels)
Trusted_Internet_Zone	IBM supplied: IPSec sample - Server to trusted branch office (internet traversed)
Untrusted_Zone	IBM supplied: IPSec sample - Server to untrusted business partner zone

- Add for Beginners...
- Add...**
- Copy...
- Modify...
- Delete
- View Details...
- Show Where Used...

Sec Perspective

Duration

IPSec

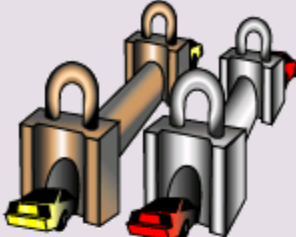
Wo

Wo

+

+

New Requirement Map



A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map: 1. Select a Traffic Descriptor from the Objects section.
2. Click the "<-Add" button

To change the Security Level of a Traffic Descriptor: 1. Click the Security Level column in the Requirement Map section
2. Select a new Security Level from the list

Requirement Map

Name: * SECURE EE TRAFFIC

Description

Traffic Descriptor	IPSec - Security Level
EE_Ports_12000_12002	IPSec_EE_High
EE_Ports_12003_12004	IPSec_EE_Authenticate
	IPSec_EE_Authenticate
	IPSec_EE_High
	Deny
	Permit
	IPSec_Gold
	IPSec_Silver
	IPSec_Bronze

Move Up

Move Down

View Details...

Objects

- Traffic Descriptor ▲
- All_other_traffic
- ALLOW_IPSec_Protocols
- Centralized_Policy_Client
- Centralized_Policy_Server
- CICS
- DNS
- EE
- FTP-Client
- FTP-Server
- FTP-Server-SSL
- ICMP-Redirect-IP_V4
- ICMP-Redirect-IP_V6
- ICMP-Time_Exceeded-IP_V4
- ICMP-Time_Exceeded-IP_V6
- ICMP-Unreachable-IP_V4

<-Add

Remove -->

Work with Traffic Descriptors...

Work with Security Levels...

OK

Cancel

Help ?

Requirement Map: SECURE_EE_TRAFFIC

Traffic Descriptor	IPSec Security Level
EE_Ports_12000_12002 - First 3 ports of EE	IPSec_EE_High - IPSec Encryption Tunnel
EE_Ports_12003_12004	IPSec_EE_Authenticate - IPSec Tunnel to authenticate

Requirement Map traffic - Shown in Configured Order

Traffic Descriptor						IPSec Security Level		
Name	Protocol	Local / Source Port	Remote / Destination Port	Connect Direction	Type/ Code	Name	Type	Encryption / Authentication / Protocol
EE_Ports_12000_12002	UDP	12000-12002	12000-12002	---	---	IPSec_EE_High	IPSec - Dynamic Tunnel	3DES / MD5 / ESP
EE_Ports_12003_12004	UDP	12003-12004	12003-12004	---	---	IPSec_EE_Authenticate	IPSec - Dynamic Tunnel	None / MD5 / AE

Security Level Details

Note that these were created for the DEMO earlier. You can just us the defaults if you so desire

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

Connectivity Rules Dynamic Tunnel Local Identity Stack Level Settings Client NSS settings

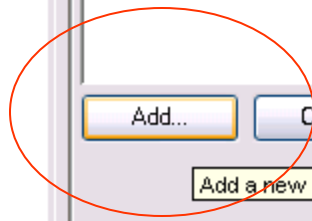
TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: * TCPSVT

Enter a description: Main Stack on IRAQ

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local/Source	Remote/Destination	Requirement Map	Topology	Status	Name
All IP V4	All IP V4	Basic_Connectivity	None	Enabled	Basic_Connection_Rule
197.33.63.1	197.33.78.1	ALLOW_IKE	None	Enabled	ISAKMP
All IP V4	All IP V4	DENYALL	None	Enabled	Deny_ALL



- Add...
- Copy...
- Modify Basics...
- Delete
- View Details...
- Move Up
- Health Check...
- Add a new Connectivity Rule
- Modify Wizard...
- Move Down

Sec Perspective

Configuration Assistant Navigation Tree

PSec

Work with Reusable Objects

- Traffic Descriptors
- Security Levels
- Requirement Maps

Work with z/OS Images

- Image - IRAQ
 - Stack - TCPSVT
- Image - PANAMA

New Connectivity Rule: Welcome

Welcome to the Connectivity Rule wizard.

Indicate Connectivity Rule type:

Typical

Special Case:

IP V6 OSPF IP Security

A Connectivity Rule consists of the following:

- Network Topology - (only required when using IPSec tunnels)
- Data endpoints - may be single IP addresses or wildcarded
- A Requirement Map - which is a set of Traffic Descriptors mapped to Security Levels. This dictates behavior between the data endpoints.
- Security endpoints (if using IPSec tunnels in the selected Requirement Map) This indicates where IPSec tunnels begin and terminate.
- Additional information determined by your data endpoint and Requirement Map selections.

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Network Topology

Use this panel to identify the network topology of the data endpoints and security endpoints.

Network topology

- This Connectivity Rule will contain only Permit and Deny Security Levels; therefore, no topology information is required.
- This Connectivity Rule will contain a Security Level using IPSec tunnels; therefore, additional network topology information is required.

Select the topology that represents the location of your data endpoints and security endpoints

- Host to Host
- Host to Gateway
- Gateway to Host
- Gateway to Gateway

Legend

- Data Endpoint (Folder icon)
- Security Endpoint (S in a circle icon)
- IPSec - Data is enciphered (Padlock icon)
- Unprotected data path (Dotted line icon)

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Select Requirement Map X

Use this panel to select the Requirement Map for the data endpoints for Host To Host topology.

Select a Requirement Map

Initially, you need to create a new Requirement Map which will be reusable in subsequent Connectivity Rules. IBM has supplied examples you can use to "Copy..." and then modify to get started.

Until you become familiar with Requirement Maps please use the **Add for Beginners...** to create your Requirement Map.

Name ▲	Description
ALLOW_IKE	Allow IKE Negotiation
Basic_Connectivity	These are the basic connectivity rules for operation
DENYALL	Always at the bottom of the list
Filtering	IBM supplied: IPsec sample - Filtering (uses only Permit and Deny Security Levels)
SECURE_EE_TRAFFIC	
Trusted_Internet_Zone	IBM supplied: IPsec sample - Server to trusted branch office (internet traversed)
Untrusted_Zone	IBM supplied: IPsec sample - Server to untrusted business partner zone

Add for Beginners...
Add...
Copy...
Modify...
View Details...

Need More Information

Help ?
< Back
Next >
Finish
Cancel

action_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

Connectivity Rules Dynamic Tunnel Local Identity Stack Level Settings Client NSS settings

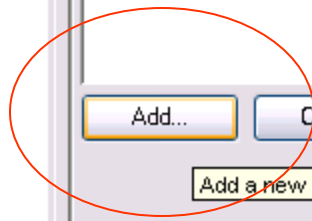
TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: * TCPSVT

Enter a description: Main Stack on IRAQ

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local/Source	Remote/Destination	Requirement Map	Topology	Status	Name
All IP V4	All IP V4	Basic_Connectivity	None	Enabled	Basic_Connection_Rule
197.33.63.1	197.33.78.1	ALLOW_IKE	None	Enabled	ISAKMP
All IP V4	All IP V4	DENYALL	None	Enabled	Deny_ALL



Buttons in the bottom toolbar: Add... Copy... Modify Basics... Delete View Details... Move Up Health Check... Add a new Connectivity Rule Modify Wizard... Move Down

Sec Perspective

Configuration Assistant Navigation Tree

PSec

Work with Reusable Objects

- Traffic Descriptors
- Security Levels
- Requirement Maps

Work with z/OS Images

- Image - IRAQ
 - Stack - TCPSVT
- Image - PANAMA

New Connectivity Rule: Welcome

Welcome to the Connectivity Rule wizard.

Indicate Connectivity Rule type:

Typical

Special Case:

IP V6 OSPF IP Security

A Connectivity Rule consists of the following:

- Network Topology - (only required when using IPSec tunnels)
- Data endpoints - may be single IP addresses or wildcarded
- A Requirement Map - which is a set of Traffic Descriptors mapped to Security Levels. This dictates behavior between the data endpoints.
- Security endpoints (if using IPSec tunnels in the selected Requirement Map) This indicates where IPSec tunnels begin and terminate.
- Additional information determined by your data endpoint and Requirement Map selections.

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Network Topology

Use this panel to identify the network topology of the data endpoints and security endpoints.

Network topology

- This Connectivity Rule will contain only Permit and Deny Security Levels; therefore, no topology information is required.
- This Connectivity Rule will contain a Security Level using IPSec tunnels; therefore, additional network topology information is required.

Select the topology that represents the location of your data endpoints and security endpoints

- Host to Host
- Host to Gateway
- Gateway to Host
- Gateway to Gateway

Legend

- Data Endpoint
- Security Endpoint
- IPSec - Data is enciphered
- Unprotected data path

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective


Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Data Endpoints

Use this panel to identify the data endpoints.
These are the IP addresses of the host endpoints of the traffic you want to protect.



Host To Host - Data Endpoints

Local data endpoint

All IP V4 addresses
 All IP V6 addresses
 Specify address:
* 197.33.63.1

Syntax: Single IP V4 address: x.x.x.x
Single IP V6 address: x::x

Remote data endpoint

All IP V4 addresses
 All IP V6 addresses
 Specify address:
* 197.33.78.1

Syntax: Single IP V4 address: x.x.x.x
IP V4 subnet: x.x.x.x/yy
IP V4 range: x.x.x.x-y.y.y.y
Single IP V6 address: x::x
IP V6 subnet: x::x/yyy
IP V6 range: x::x-y::y

Connectivity Rule Name

Name: * Secure_EE_TRAFFIC

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Select Requirement Map

Use this panel to select the Requirement Map for the data endpoints for Host To Host topology.

Select a Requirement Map

Initially, you need to create a new Requirement Map which will be reusable in subsequent Connectivity Rules. IBM has supplied examples you can use to "Copy..." and then modify to get started.

Until you become familiar with Requirement Maps please use the **Add for Beginners...** to create your Requirement Map.

Name ▲	Description
ALLOW_IKE	Allow IKE Negotiation
Basic_Connectivity	These are the basic connectivity rules for operation
DENYALL	Always at the bottom of the list
Filtering	IBM supplied: IPsec sample - Filtering (uses only Permit and Deny Security Levels)
SECURE_EE_TRAFFIC	
Trusted_Internet_Zone	IBM supplied: IPsec sample - Server to trusted branch office (internet traversed)
Untrusted_Zone	IBM supplied: IPsec sample - Server to untrusted business partner zone

Add for Beginners...
Add...
Copy...
Modify...
View Details...

Create a new Requirement Map by copying the one selected

Need More Information

Help ?
< Back
Next >
Finish
Cancel

action_Rule

check...

Sec Perspective


Configuration Assistant Navigation Tree

PSec

- Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
- Work with z/OS Images
 - Image - IRAQ
 - Stack - TCPSVT
 - Image - PANAMA

New Connectivity Rule: Remote Security Endpoint Information

Use this panel to enter information about the IPSec **remote** security endpoint for Host To Host topology.



A remote IKE identity is required for IKE negotiations (used for Dynamic Tunnels only)

- IP address: * 197.33.78.1
- Fully qualified domain name (FGDN): *
- User id @ FGDN: *
- X.500 distinguished name: *

Indicate how to authenticate the remote IKE peers (used for Dynamic Tunnels only)

- RSA signature
- Shared key: EBCDIC ASCII Hexadecimal

* testtesttest

Help ? < Back Next > Finish Cancel

ection_Rule

check...

Sec Perspective

Configuration Assistant Navigation Tree

PSec

Work with Reusable Objects

- Traffic Descriptors
- Security Levels
- Requirement Maps

Work with z/OS Images

- Image - IRAQ
 - Stack - TCPSVT
- Image - PANAMA

New Connectivity Rule: Finish

Indicate if you want use filter logging for this Connectivity Rule

- No - do not log filter matches
- Yes, log all filter matches
- Yes, but only log filter matches with valid Security Associations
- Yes, but only log filter matches **without** valid Security Associations

Optional advanced Connectivity Rule settings

Advanced...

Help ? < Back Next > Finish Cancel

ection_Rule

check...