



Software Group | Enterprise Networking and Transformation Solutions (ENTS)

Configuration for z/OS IPsec and IP Packet Filtering (Part 2 of 2)

SHARE Session 3907

Lin Overby - overbylh@us.ibm.com
Allen Bailey - eabailey@us.ibm.com

Trademarks and notices

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

- ▶ AIX®
- ▶ AnyNet®
- ▶ AS/400®
- ▶ Candle®
- ▶ CICS®
- ▶ CICSplex®
- ▶ CICS/ESA®
- ▶ DB2®
- ▶ DB2 Connect™
- ▶ DPI®
- ▶ DRDA®
- ▶ e business(logo)®
- ▶ ESCON®
- ▶ eServer™
- ▶ ECKD™
- ▶ FFST™
- ▶ GDDM®
- ▶ GDPS®
- ▶ HiperSockets™
- ▶ IBM®
- ▶ Infoprint®
- ▶ IMS™
- ▶ IP PrintWay™
- ▶ iSeries™
- ▶ Language Environment®
- ▶ MQSeries®
- ▶ MVS™
- ▶ MVS/ESA™
- ▶ NetView®
- ▶ OS/2®
- ▶ OS/390®
- ▶ Parallel Sysplex®
- ▶ PrintWay™
- ▶ PR/SM™
- ▶ pSeries®
- ▶ RACF®
- ▶ Redbooks™
- ▶ Redbooks (logo)™
- ▶ S/390®
- ▶ System/390®
- ▶ ThinkPad®
- ▶ Tivoli®
- ▶ Tivoli (logo)®
- ▶ VM/ESA®
- ▶ VSE/ESA™
- ▶ VTAM®
- ▶ WebSphere®
- ▶ xSeries®
- ▶ z/Architecture™
- ▶ z/OS®
- ▶ z/VM®
- ▶ zSeries®

- 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.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Refer to www.ibm.com/legal/us for further legal information.

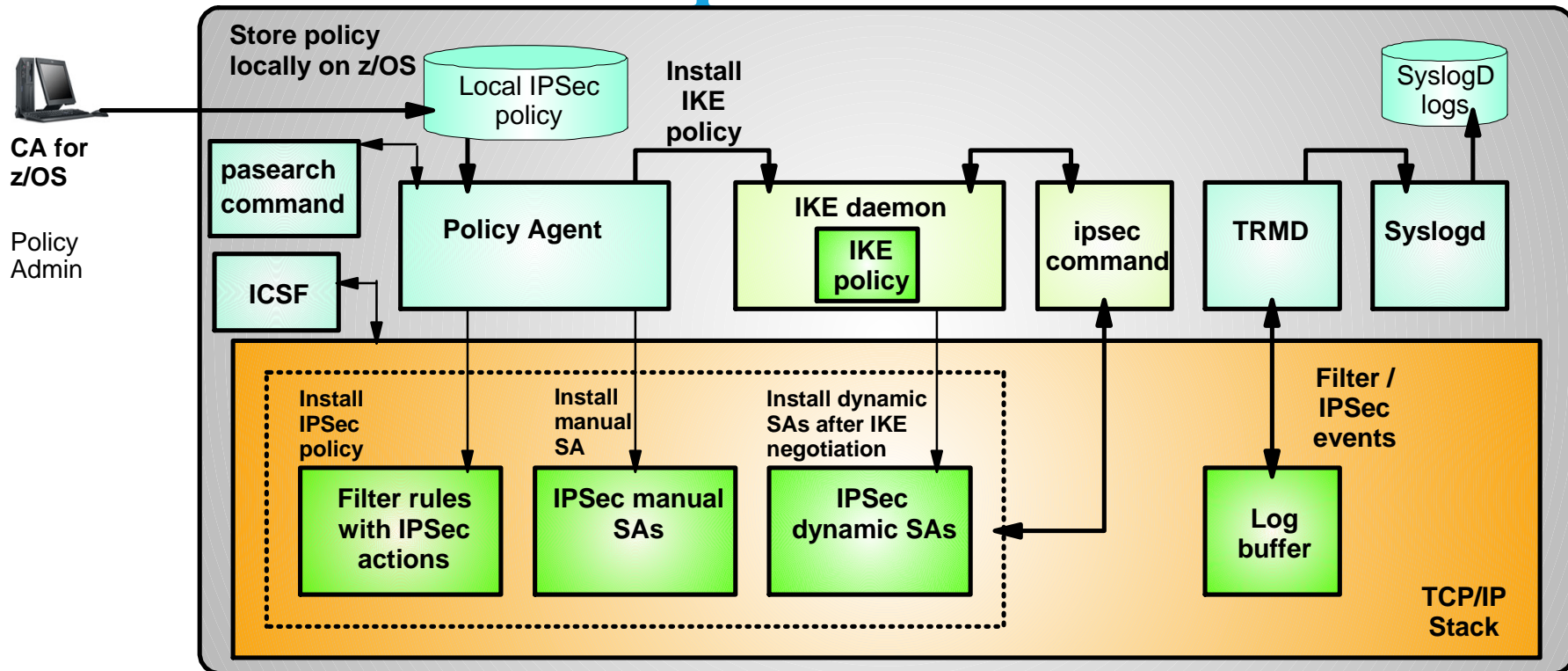
Agenda

- **z/OS System Preparation tasks**
 - ▶ Configuration of required applications
 - ▶ SAF access controls
 - ▶ SAF certificates and keyrings

- **Configuration Assistant IPsec Demo**
 - ▶ Configuration Assistant Help
 - ▶ IPsec Policy Configuration
 - Configure Image
 - Configure Stack
 - Reusable Objects
 - Configure Policy
 - Create Requirements Map
 - Create Connectivity Rule
 - Health Checker
 - ▶ Upload Policy
 - ▶ Modification of Policy
 - Activation Settings

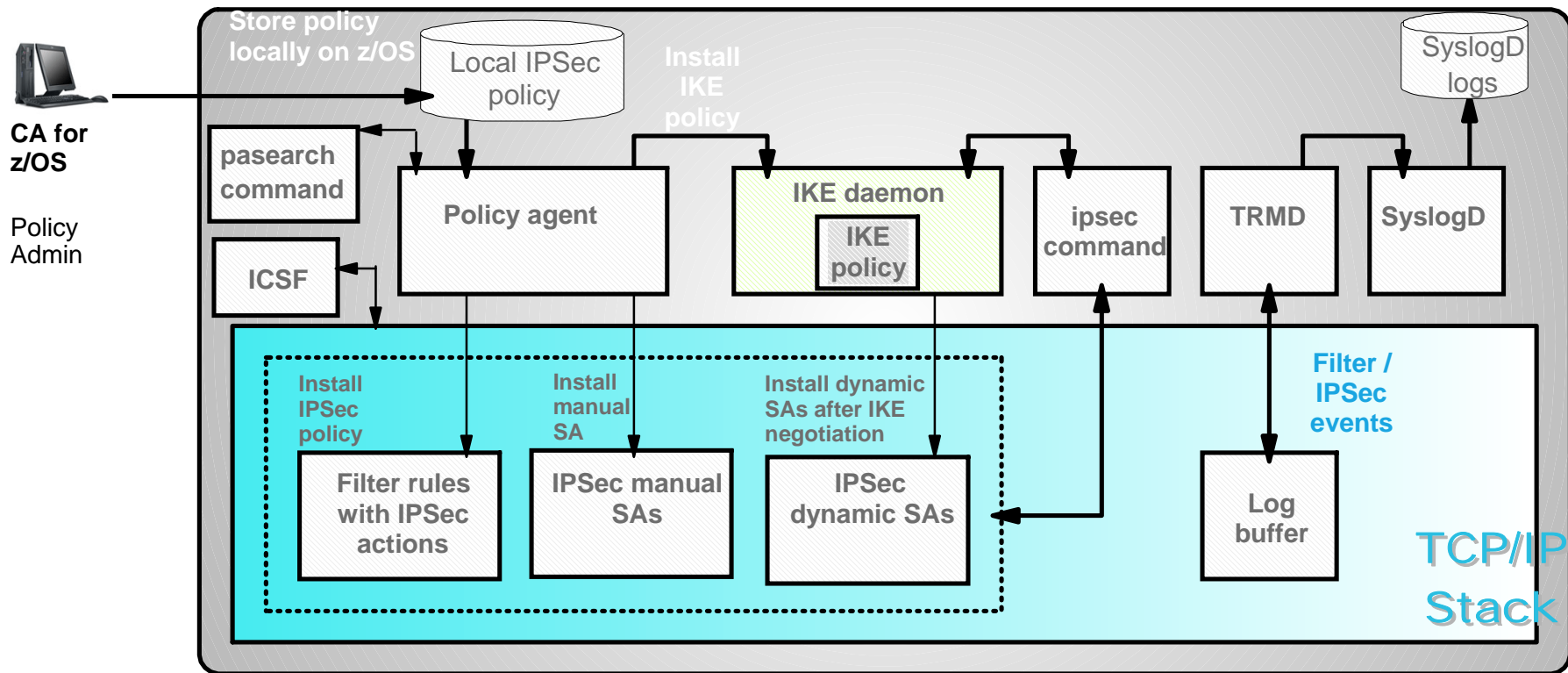
- **Display and control of IP Filtering and IPsec**

z/OS Communications Server IPsec Component Overview



- **TCP/IP stack**
 - IPsec and IP filtering
- **IKE daemon**
 - Negotiates security associations
- **Policy Agent**
 - Reads and manages IPsec and IKE policy
- **TRMD**
 - Monitors TCP/IP stacks for log messages
- **syslogd**
 - writes log messages to syslogd destinations
- **ICSF**
 - provides encryption facilities to TCP/IP stacks
- **Configuration Assistant for z/OS**
 - Creates policy definitions
- **pasearch command**
 - Displays current policy information
- **ipsec command**
 - Displays and controls IP filtering, IPsec, and IKE

TCP/IP Stack Configuration



■ TCP/IP stack

■ IPsec and IP filtering

■ IKE daemon

- Negotiates security associations

■ Policy Agent

- Reads and manages IPsec and IKE policy

■ TRMD

- Monitors TCP/IP stacks for log messages

■ syslogd

- writes log messages to syslogd destinations

■ ICSF

- provides encryption facilities to TCP/IP stacks

■ Configuration Assistant for z/OS

- Creates policy definitions

■ pasearch command

- Displays current policy information

■ ipsec command

- Displays and controls IP filtering, IPsec, and IKE

TCP/IP profile

1. Enable IP security for IPv4 and IPv6^{1,2}
 - ▶ IPCONFIG IPSECURITY
 - ▶ IPCONFIG6 IPSECURITY
 - ▶ For IPv6 support, both must be configured
2. Define default filter rules in the IPSEC/ENDIPSEC block²
 - ▶ IPSEC
 - ▶ IPSECRULE
 - ▶ ENDIPSEC

¹The **NETSTAT CONFIG** statement can be used to verify that IP security has been enabled

²Sample provided in the Configuration Assistant for z/OS

TCP/IP default filter rules

- **By default, all traffic except intra-stack traffic will be denied if IPSECURITY is enabled**
- Provide limited filtering support until the policy agent can be started
- Use of dynamic or manual tunnels is not possible when the profile rules are active.

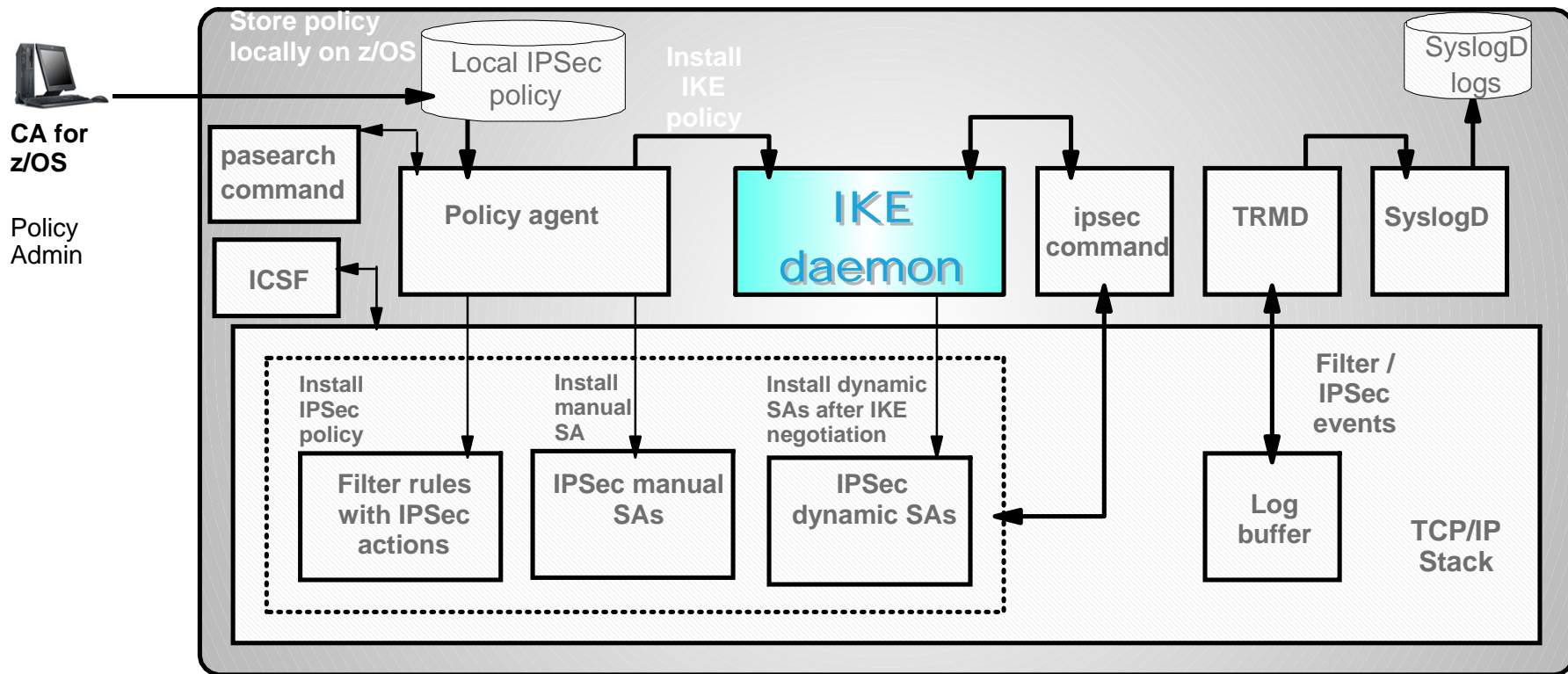
Example:

```
IPSECRULE 9.1.1.1 192.168.1.1 NOLOG PROTO TCP
```

- Reference: "TCP/IP profile and configuration statements", *z/OS Communications Server IP Configuration Reference*

★ The z/OS USS `ipsec` command can be used to display the default filter rules:
`ipsec -f display -c default`

IKE daemon Configuration



- **TCP/IP stack**
 - IPsec and IP filtering
- **IKE daemon**
 - ▶ **Negotiates security associations**
- **Policy Agent**
 - ▶ Reads and manages IPsec and IKE policy
- **TRMD**
 - ▶ Monitors TCP/IP stacks for log messages
- **syslogd**
 - ▶ writes log messages to syslogd destinations
- **ICSF**
 - ▶ provides encryption facilities to TCP/IP stacks
- **Configuration Assistant for z/OS**
 - ▶ Creates policy definitions
- **pasearch command**
 - ▶ Displays current policy information
- **ipsec command**
 - ▶ Displays and controls IP filtering, IPsec, and IKE

IKE Daemon

1. Create IKED configuration file^{1,2}
2. Create CTRACE parmlib member
3. Start procedure²

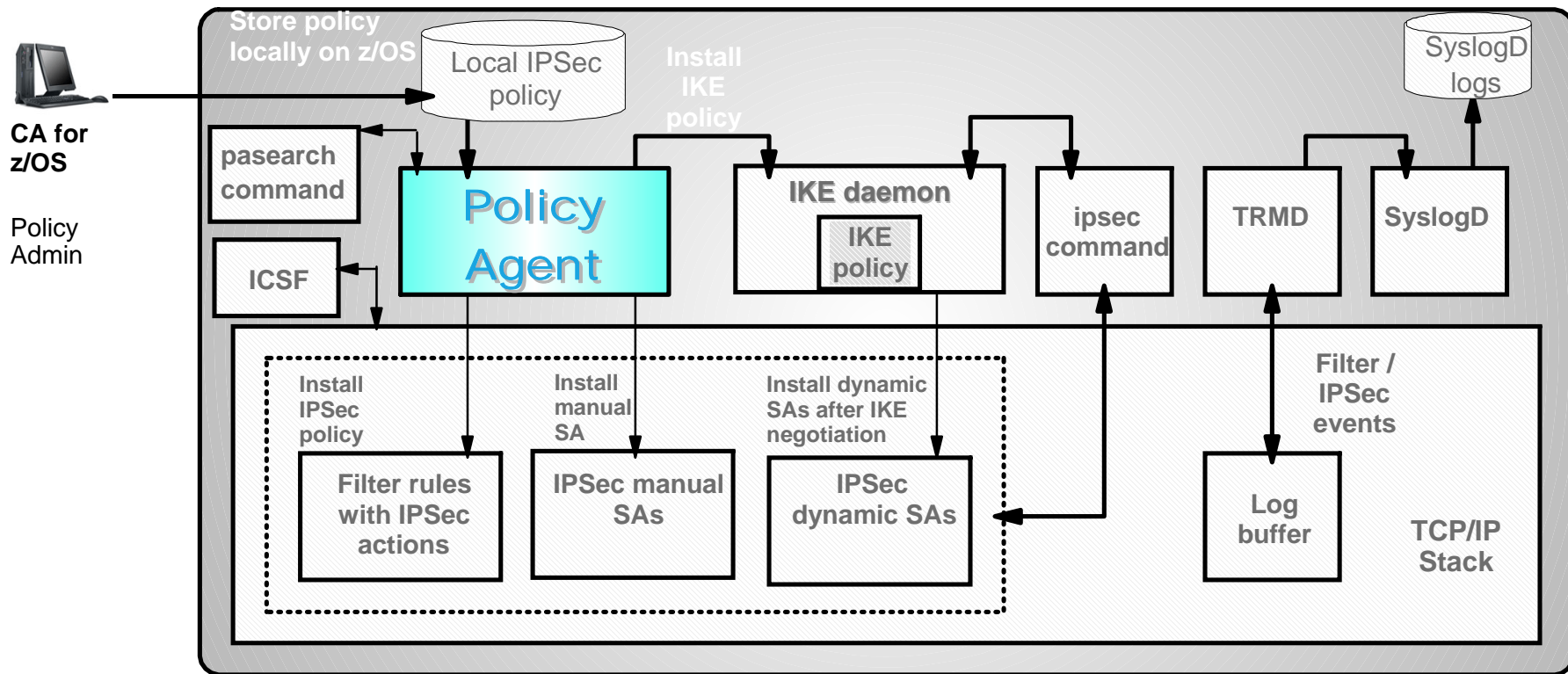
¹Can configure with Configuration Assistant for z/OS

²Sample provided in Configuration Assistant for z/OS

IKE Daemon details

- IKED configuration file
 - ▶ MVS dataset or HFS file (default location: `/etc/security/iked.conf`)
 - ▶ Fine-tunes negotiation timing
 - ▶ Sets log levels
 - ▶ Supplies SAF keyring name (needed for RSA signature mode)
- CTRACE parmlib member
 - ▶ Sample provided in SYS1.PARMLIB(CTIIKE00)
 - ▶ Default tracing set to MINIMUM if file does not exist
- Start procedure (can also be started from the z/OS USS shell)
 - ▶ Sample provided in SEZAINST(IKED)
 - ▶ Use AUTOLOG to start automatically in a single-stack environment
- Reference: "Starting the IKE daemon", *z/OS Communications Server IP Configuration Guide*

Policy Agent Configuration



- **TCP/IP stack**
 - IPsec and IP filtering
- **IKE daemon**
 - Negotiates security associations
- **Policy Agent**
 - Reads and manages IPsec and IKE policy
- **TRMD**
 - Monitors TCP/IP stacks for log messages
- **syslogd**
 - writes log messages to syslogd destinations
- **ICSF**
 - provides encryption facilities to TCP/IP stacks
- **Configuration Assistant for z/OS**
 - Creates policy definitions
- **pasearch command**
 - Displays current policy information
- **ipsec command**
 - Displays and controls IP filtering, IPsec, and IKE

Policy Agent

1. Create configuration files

▶ Hierarchy of configuration files (MVS dataset or HFS files)

- **Main configuration file** (default location: `/etc/pagent.conf`) - identifies which TCP/IP stacks have policy defined and the file in which the image configuration is found:

```
TcpImage TCPCS1 /etc/tcpimage.policy.tcpip
```

- **Image configuration file(s)** - identifies which policy disciplines are enabled for the specific TCP/IP stack and the file in which its discipline configuration is found:

```
IpSecConfig /etc/tcpip.ipsec.policy
```

- **Discipline file**¹ - includes all policy statements specific to a particular discipline (such as IPsec)

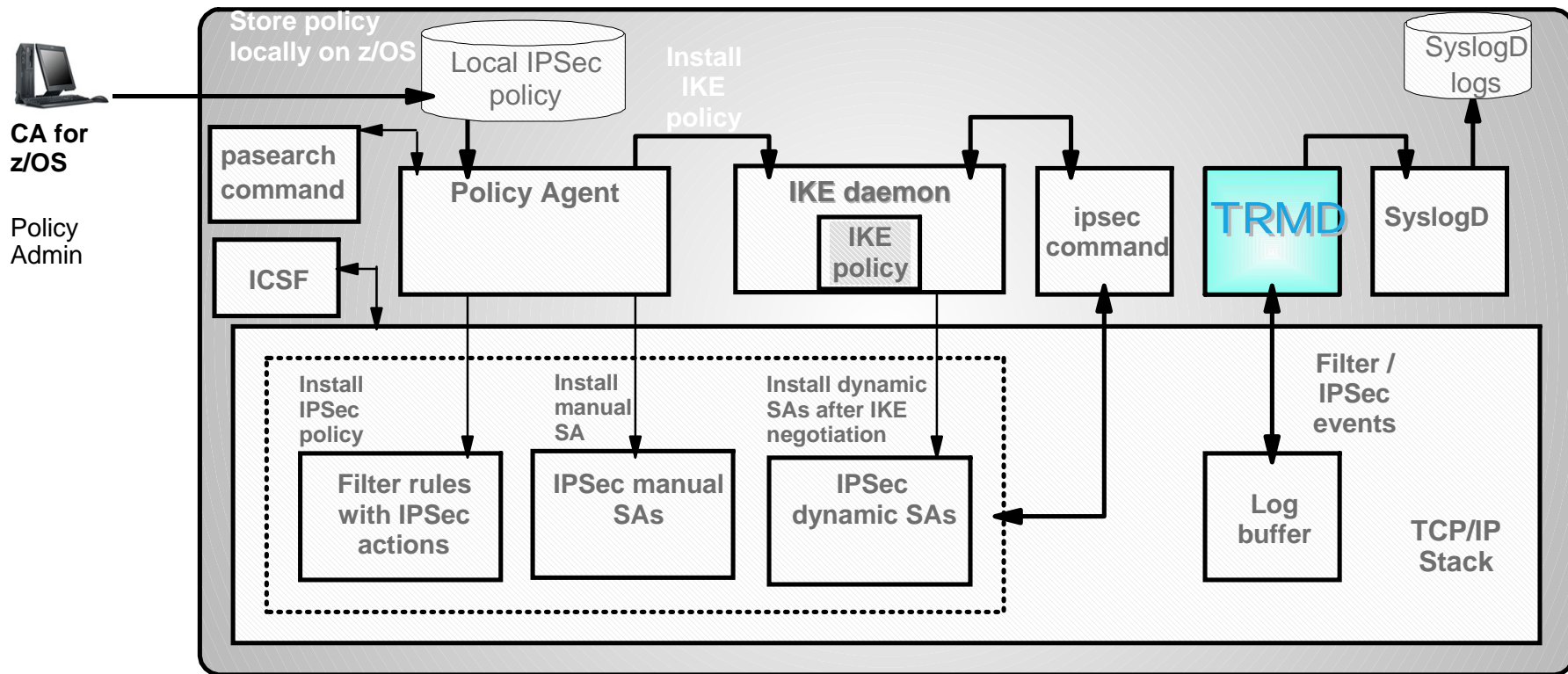
2. Start procedure (can also be started from the z/OS USS shell)

- ▶ Sample provided in SEZAINST(EZAPAGSP)
- ▶ Use AUTOLOG to start automatically

- Reference: "Starting and stopping the Policy Agent", *z/OS Communications Server IP Configuration Guide*

¹ Can configure with Configuration Assistant for z/OS

TRMD Configuration

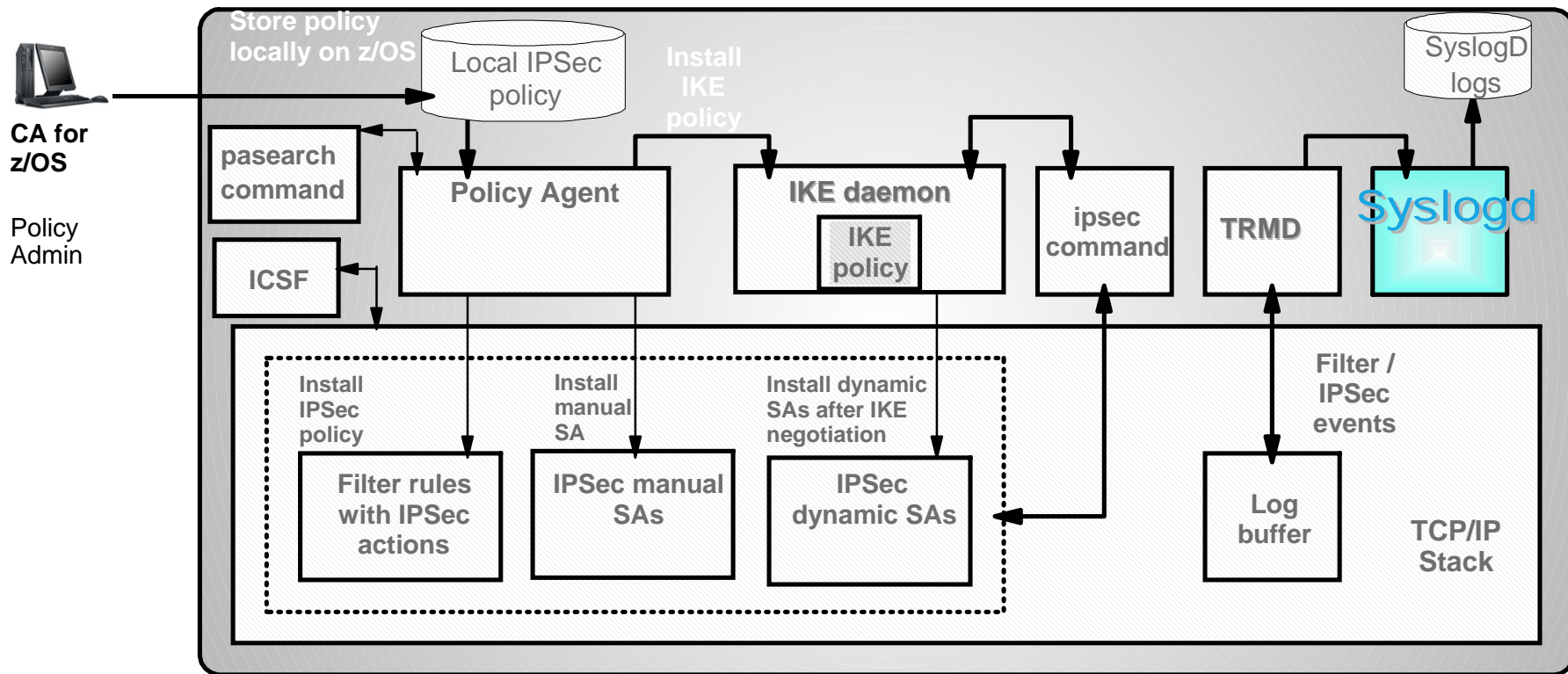


- **TCP/IP stack**
 - IPsec and IP filtering
- **IKE daemon**
 - Negotiates security associations
- **Policy Agent**
 - Reads and manages IPsec and IKE policy
- **TRMD**
 - **Monitors TCP/IP stacks for log messages**
- **syslogd**
 - writes log messages to syslogd destinations
- **ICSF**
 - provides encryption facilities to TCP/IP stacks
- **Configuration Assistant for z/OS**
 - Creates policy definitions
- **pasearch command**
 - Displays current policy information
- **ipsec command**
 - Displays and controls IP filtering, IPsec, and IKE

Traffic Regulation Management Daemon (TRMD)

1. No configuration file
 2. Start procedure (can also be started from the z/OS USS shell)
 - ▶ Sample provided in SEZAINST(TRMD)
 - ▶ Use AUTOLOG to start automatically
 - ▶ Associate with specific TCP/IP stack (**one running instance per TCP/IP stack**) using RESOLVER_CONFIG variable
-
- Reference: "TRMD", *z/OS Communications Server IP Configuration Guide*

Syslogd Configuration



- **TCP/IP stack**
 - IPsec and IP filtering
- **IKE daemon**
 - ▶ Negotiates security associations
- **Policy Agent**
 - ▶ Reads and manages IPsec and IKE policy
- **TRMD**
 - ▶ Monitors TCP/IP stacks for log messages
- **syslogd**
 - ▶ writes log messages to syslogd destinations
- **ICSF**
 - ▶ provides encryption facilities to TCP/IP stacks
- **Configuration Assistant for z/OS**
 - ▶ Creates policy definitions
- **pasearch command**
 - ▶ Displays current policy information
- **ipsec command**
 - ▶ Displays and controls IP filtering, IPsec, and IKE

Syslog Daemon

1. Create configuration file (MVS dataset of HFS file)
 - ▶ Default location: `/etc/syslog.conf`
 - ▶ Separate log files by priority, facility, jobname, or user ID
 - ▶ **IKED and TRMD use facility 'local4'**
 2. Start procedure (can also be started from the z/OS USS shell)
 - ▶ Sample provided in SEZAINST(SYSLOGD)
 - ▶ Use AUTOLOG to start automatically
- Reference: "Configuring the syslog daemon", *z/OS Communications Server IP Configuration Guide*

Integrated Cryptographic Facility (ICSF)

- Using ICSF, IPsec can leverage hardware encryption
 - ▶ Required for using AES encryption
 - ▶ Required for using z/OS CP Assist for Cryptographic Function (CPACF)

- Start procedure
 - ▶ Customize SYS1.PARMLIB
 - ▶ Create the cryptographic key data set (CKDS)
 - ▶ Create the public key data set (PKDS)
 - ▶ Sample procedure provided in SYS1.PARMLIB(CSF)

- Reference: "Steps for installation and initialization", *ICSF System Programmer's Guide*

SAF Authorization and Access Control

- **Sample RACF profile definitions required for TCP/IP and associated applications (including IP Security) can be found in SEZAINST(EZARACF)**

- **SAF definitions required for IP Security include:**
 - IKED
 - Policy Agent (and `pasearch` command)
 - TRMD
 - `syslogd`
 - `ipsec` command

IKED SAF Profiles

1. Add user ID IKED, and add IKED to the STARTED class

```
ADDUSER  IKED      DFLTGRP(OMVSGRP)  OMVS(UID(0)  HOME('/'))
RDEFINE  STARTED  IKED.*              STDATA(USER(IKED))
SETROPTS RACLIST(STARTED) REFRESH
SETROPTS GENERIC(STARTED) REFRESH
```

2. If defined, allow access to the BPX.DAEMON class

```
PERMIT   BPX.DAEMON CLASS(FACILITY) ID(IKED)      ACCESS(READ)
```

3. Allow IKED to access SYS1.PARMLIB

```
PERMIT   SYS1.PARMLIB  ID(IKED)              ACCESS(READ)
```

4. Enable IKED to access certificates on a SAF key ring (required for RSA signature)

```
RDEFINE  FACILITY  IRR.DIGTCERT.LISTRING  UACC(NONE)
RDEFINE  FACILITY  IRR.DIGTCERT.LIST      UACC(NONE)
PERMIT   IRR.DIGTCERT.LISTRING CLASS(FACILITY) ID(IKED) ACCESS(READ)
PERMIT   IRR.DIGTCERT.LIST      CLASS(FACILITY) ID(IKED) ACCESS(READ)
SETROPTS RACLIST(FACILITY) REFRESH
```

Policy Agent SAF profiles

1. Add user ID PAGENT, and add PAGENT to the STARTED class

```
ADDUSER PAGENT DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))
RDEFINE STARTED PAGENT.* STDATA(USER(PAGENT))
SETROPTS RACLIST(STARTED) REFRESH
SETROPTS GENERIC(STARTED) REFRESH
```

2. Selectively allow access to the pasearch command

```
RDEFINE SERVAUTH EZB.PAGENT.sysname.tcpprocname.type UACC(NONE)
PERMIT EZB.PAGENT.sysname.tcpprocname.* CLASS(SERVAUTH) ID(userid) ACCESS(READ)
  where 'type' is one of:
  QOS
  IDS
  IPSec
  TTLS
  * (all policy disciplines)
```

3. To control which users can start PAGENT (and thus avoiding the potential to affect policy based networking)

```
SETROPTS CLASSACT (OPERCMD5)
SETROPTS RACLIST (OPERCMD5)
RDEFINE OPERCMD5 (MVS.SERV MGR.PAGENT) UACC(NONE)
PERMIT MVS.SERV MGR.PAGENT CLASS(OPERCMD5) ACCESS(CONTROL) ID(userid)
SETROPTS RACLIST(OPERCMD5) REFRESH
```

TRMD SAF Profiles

- Add user ID TRMD and add TRMD to the STARTED class

```
ADDUSER TRMD DFLTGRP(OMVSGRP) OMVS(UID(0) HOME('/'))  
RDEFINE STARTED TRMD.* STDATA(USER(TRMD))  
SETROPTS RACLIST(STARTED) REFRESH  
SETROPTS GENERIC(STARTED) REFRESH
```


Syslogd SAF profiles

1. Add user ID SYSLOGD and add SYSLOGD to the STARTED class

```
ADDUSER  SYSLOGD  DFLTGRP(OMVSGRP)  OMVS(UID(0)  HOME('/'))  
RDEFINE  STARTED  SYSLOGD.*          STDATA(USER(SYSLOGD))  
SETROPTS RACLIST(STARTED) REFRESH  
SETROPTS GENERIC(STARTED) REFRESH
```

2. If defined, allow access to the BPX.DAEMON class

```
PERMIT   BPX.DAEMON CLASS(FACILITY) ID(SYSLOGD)  ACCESS(READ)  
SETROPTS RACLIST(FACILITY) REFRESH
```

ipsec command SAF Access Controls

1. Enable the generic profile checking facility

```
SETROPTS GENERIC(SERVAUTH)
```

2. Control access to the ipsec command

a. both the display and control capabilities

```
RDEFINE SERVAUTH EZB.IPSECCMD.sysname.tcpprocname.* UACC(NONE)  
PERMIT EZB.IPSECCMD.sysname.tcpprocname.* CLASS(SERVAUTH) ID(userid) ACCESS(READ)
```

b. specifically control access to only the display capabilities

```
RDEFINE SERVAUTH EZB.IPSECCMD.sysname.tcpprocname.DISPLAY UACC(NONE)  
PERMIT EZB.IPSECCMD.sysname.tcpprocname.DISPLAY CLASS(SERVAUTH) ID(userid) ACCESS(READ)
```

c. specifically control access to only the control capabilities

```
RDEFINE SERVAUTH EZB.IPSECCMD.sysname.tcpprocname.CONTROL UACC(NONE)  
PERMIT EZB.IPSECCMD.sysname.tcpprocname.CONTROL CLASS(SERVAUTH) ID(userid) ACCESS(READ)
```

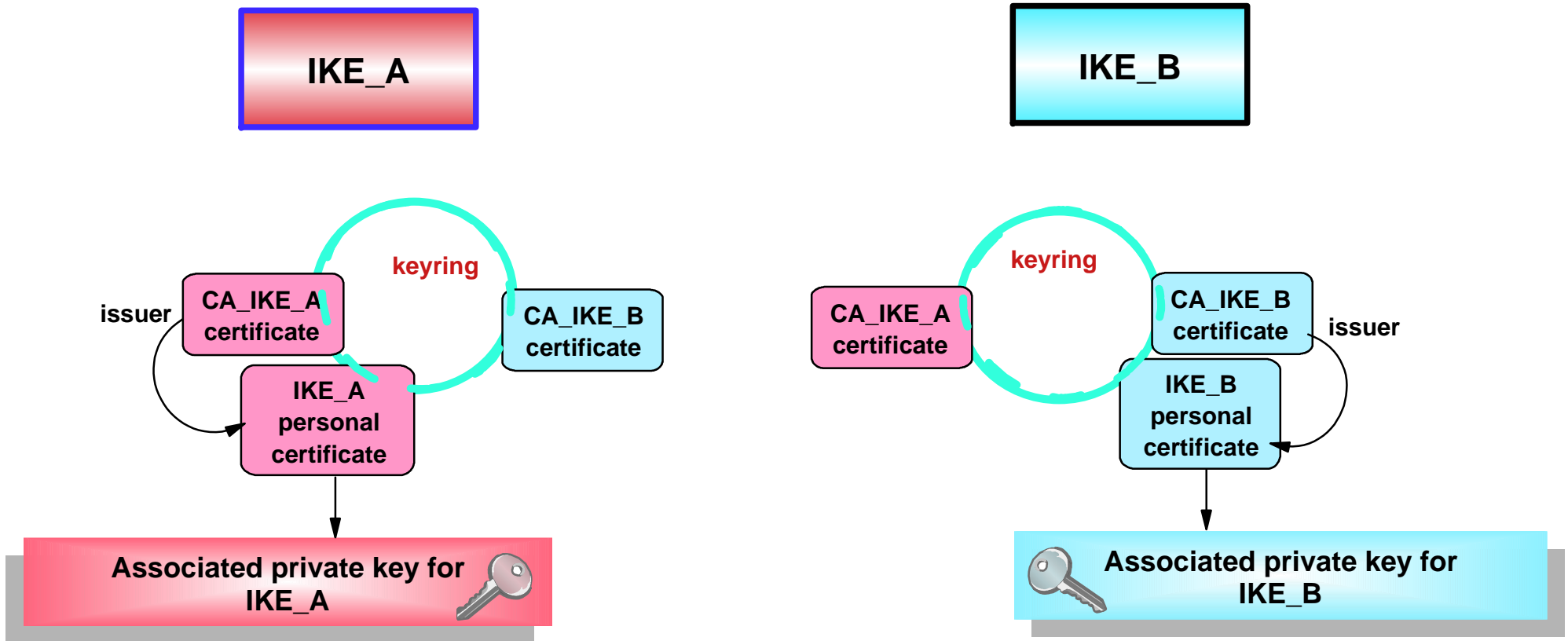
3. Refresh the in-storage RACF profiles in the SERVAUTH class

```
SETROPTS RACLIST(SERVAUTH) REFRESH
```

SAF Certificates and Keyrings

- X509 certificates are required for RSA signature mode authentication between IKE peers.
- Certificates need to contain an endpoint's identity in the certificate's SubjectName (for DNs) or the SubjectAlternate name (for RFC 822 names, FQDNs, or IPv4 addresses).
- Identity information is used to locate policy and to validate the remote peer's identity during an IKE negotiation.
- Often used when dynamic SAs are widely deployed because this configuration is easily scalable.

Keyring Setup for IKE peers



Creating RACF Certificates

```
//CERTADD JOB 1,ALFRED,CLASS=A,MSGCLASS=X,NOTIFY=USER1
//*
//IEFPROC EXEC PGM=IKJEFT01,REGION=4M,DYNAMNBR=10
//SYSTSPT DD SYSOUT=*                                BATCH TSO SESSION LOG
//SYSTSIN DD *
RACDCERT CERTAUTH GENCERT -
    SUBJECTSDN(CN('ABC CA')) -
    OU('CS Z/OS CA') -
    O('IBM') C('US')) -
    NOTBEFORE(DATE(2007-01-01))-
    NOTAFTER(DATE(2010-12-31)) -
    WITHLABEL('ABC CA')
RACDCERT ID(IKED) GENCERT -
    SUBJECTSDN(CN('ABC IKE Daemon')) -
    OU('CS Z/OS Server') -
    O('IBM') C('US')) -
    NOTBEFORE(DATE(2007-01-01)) -
    NOTAFTER(DATE(2010-12-31)) -
    WITHLABEL('IKE Daemon')
    SIGNWITH(CERTAUTH LABEL('ABC CA'))
RACDCERT CERTAUTH EXPORT(LABEL('ABC CA')) DSN('USER1.ABCCA.B64')
RACDCERT ID(IKED) ADDRING(IKEDKEYRING)
RACDCERT ID(IKED) CONNECT(LABEL('IKE Daemon') -
    RING(IKEDKEYRING) USAGE(PERSONAL) )
RACDCERT ID(IKED) CONNECT(CERTAUTH LABEL('REMOTE IKE CA') -
    RING(IKEDKEYRING) USAGE(CERTAUTH) )
RACDCERT ID(IKED) LISTRING(IKEDKEYRING)
/*
```

Create our selfsigned CA certificate by which all our other certificates will be signed.

Create our IKE daemon certificate and sign it with our CA certificate.

Export our CA certificate so that the remote IKE peer can download and install as trusted root in remote key database

Create our IKED keyring

Connect both our IKE daemon certificate and our peer's CA certificate to that keyring (presumes that remote peer's CA certificate has been added to the certificate database).

RACF Certificates: Tips

- The IKE daemon started task user ID (IKED) must have READ access to
 - IRR.DIGTCERT.LIST
 - IRR.DIGTCERT.LISTRING
- Individual users who execute the z/OS FTP client and transmit user certificates must also have READ access to the above two profiles.
- All certificate-related tasks can be performed using the RACF command interface (RACDCERT) or using the RACF ISPF interface.
- RACF certificate labels and keyrings are case sensitive; observe case when configuring IPsec policy.

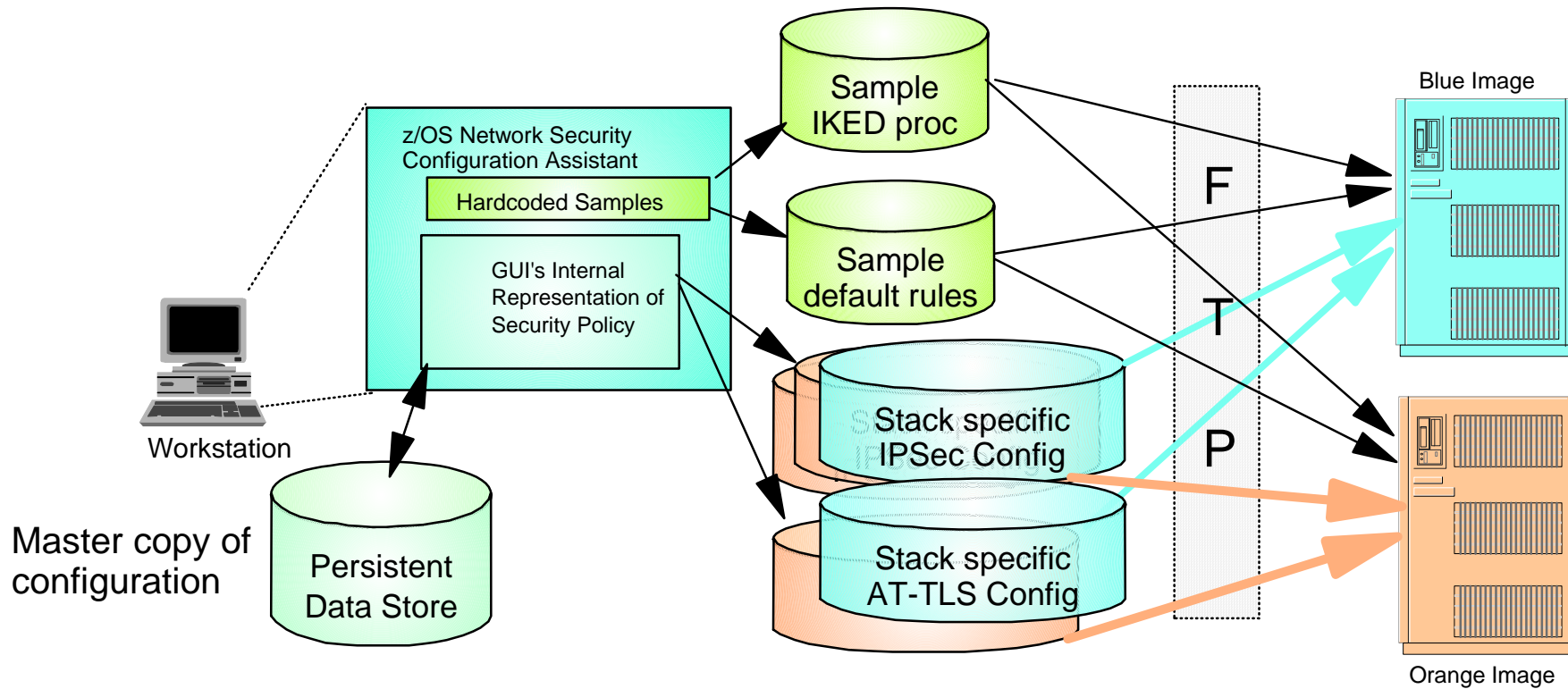
Reference

- For more information and additional options for creating server certificates, see APPENDIX E, Step 4: "Setting up the IKE server for RSA signature mode authentication", *z/OS Communications Server IP Configuration Guide*
- For more information on the RACDCERT command, see "Using the RACDCERT Command to Administer Certificates", *z/OS Security Server RACF Security Administrator's Guide*
- For the complete syntax of the RACDCERT command, see "RACDCERT (RACF Digital Certificate)", *z/OS Security Server RACF Command Language Reference*

IPSec Policy Configuration Steps with the Configuration Assistant

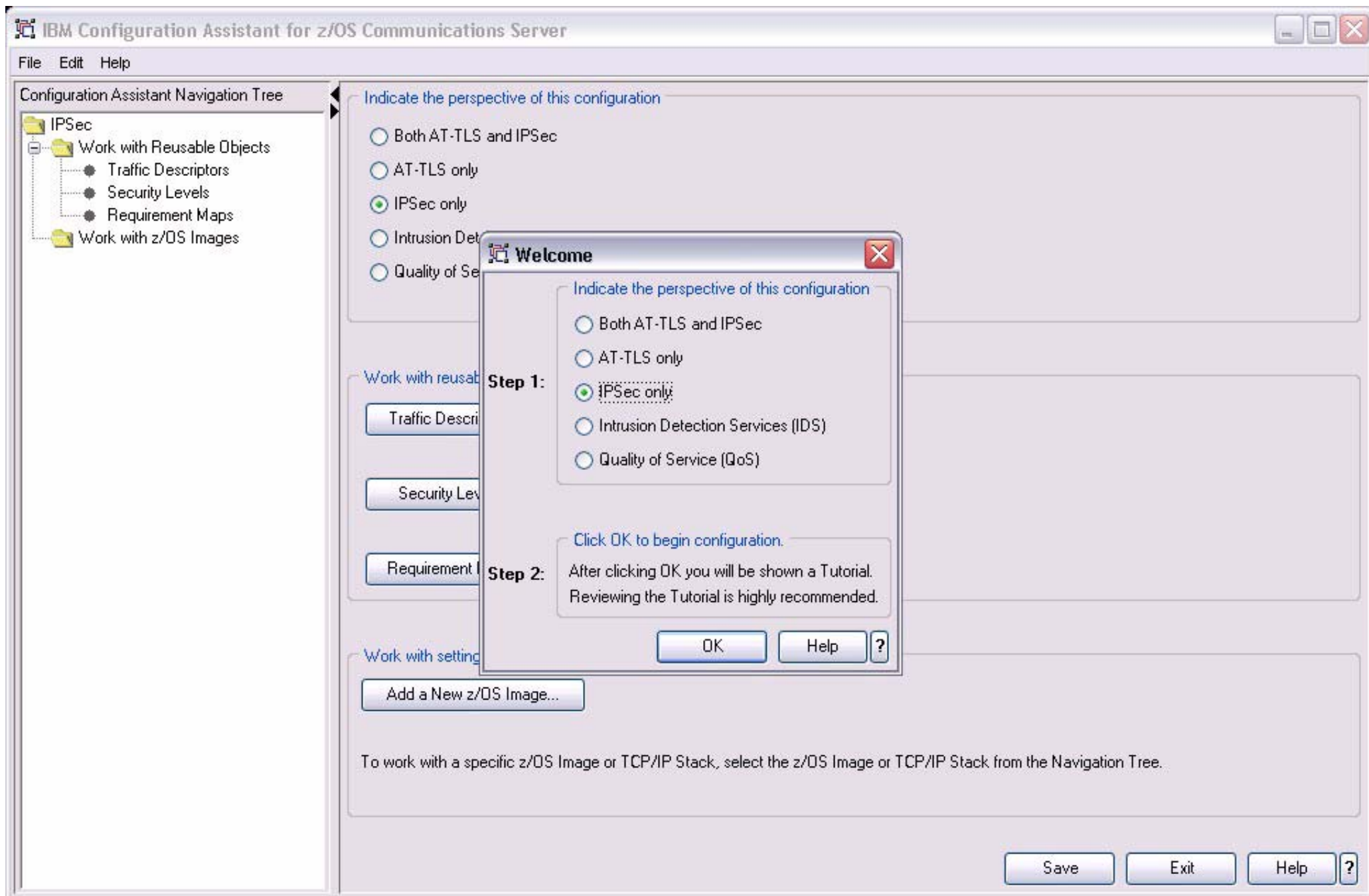
1. Download and install the Configuration Assistant configuration tool
<http://www.ibm.com/software/network/commserver/zos/support/>
2. Create system image and TCP/IP stack image
3. Configure IP Security policies
 - a. Create one or more Requirement Maps to define desired security for specific types of IP traffic
 - b. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a configured Requirement Map
 - c. If using IPSec, configure Security Endpoints (IKE peers)
4. Optionally, set additional options (e.g. logging, SA activation methods, effective time for Connectivity Rules)
5. Transfer IP Security policy to z/OS

Configuration Assistant Overview



- Allows policy definition to be performed at higher level of abstraction than policy file statements
 - ▶ Define policy for both CS IP security and AT-TLS as a single administrative task
 - Generates separate policy files for CS IP security and AT-TLS
 - ▶ Files created are transferred to z/OS image
- **In V1R9**, new file management improvements
 - ▶ Persistent data store can be stored on z/OS
 - ▶ Locking support at the persistent data store level to prevent inadvertent loss of data

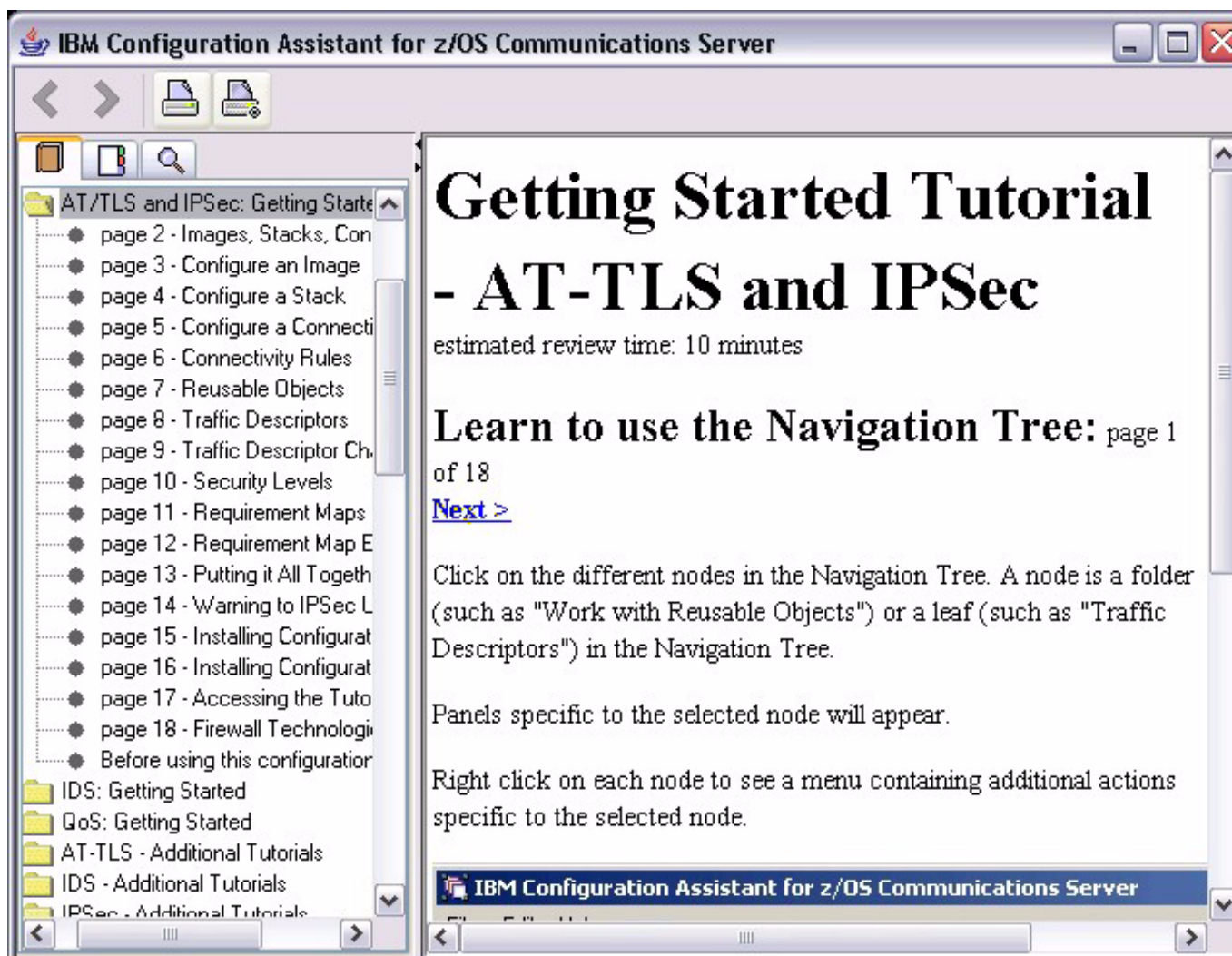
Configuration Assistant Initial Sreen



Configuration Assistant Help

1. Tutorial starts automatically when first installed
2. Help for all Configuration Assistant Elements
3. Additional Tutorials include individual help on
 - a. IDS
 - b. QoS
 - c. AT-TLS
 - d. IPSec

Configuration Assistant Tutorial



Configure Image

1. Select the "Work with z/OS Images in the Navigation Tree.
2. Click "Add a New z/OS Image..." button.
3. If IKE/IPSec will be used, then select "Yes, this Image will use IPSec dynamic tunnels"
4. Optionally configure global options for the IKE daemon:
 - a. SAF keyring name
 - b. Certificate Authorities that this system will support
 - c. IKE daemon logging level¹
 - d. Advanced options

¹**For normal operation, do not run at log levels > 1**

Configure Image

New z/OS Image: Information

z/OS Image Information

Enter a name for the z/OS Image: *

Enter a description:

Indicate if this z/OS Image will use IPSec dynamic tunnels

Yes, this Image will have dynamic tunnels

No, this Image will not have dynamic tunnels

Help ? < Back Next > Finish Cancel

IKE Daemon Settings

New z/OS Image: IPsec IKE Daemon Settings

The settings on this panel are only applicable to IPsec.
Dynamic tunnels are managed by Internet Key Exchange (IKE) daemons.
There is one IKE daemon for each z/OS Image. Use this panel for the IKE daemon settings for this z/OS Image.

Key ring data (used for Dynamic Tunnels only)

SAF (such as RACF) key ring database:

List of supported certificate authorities

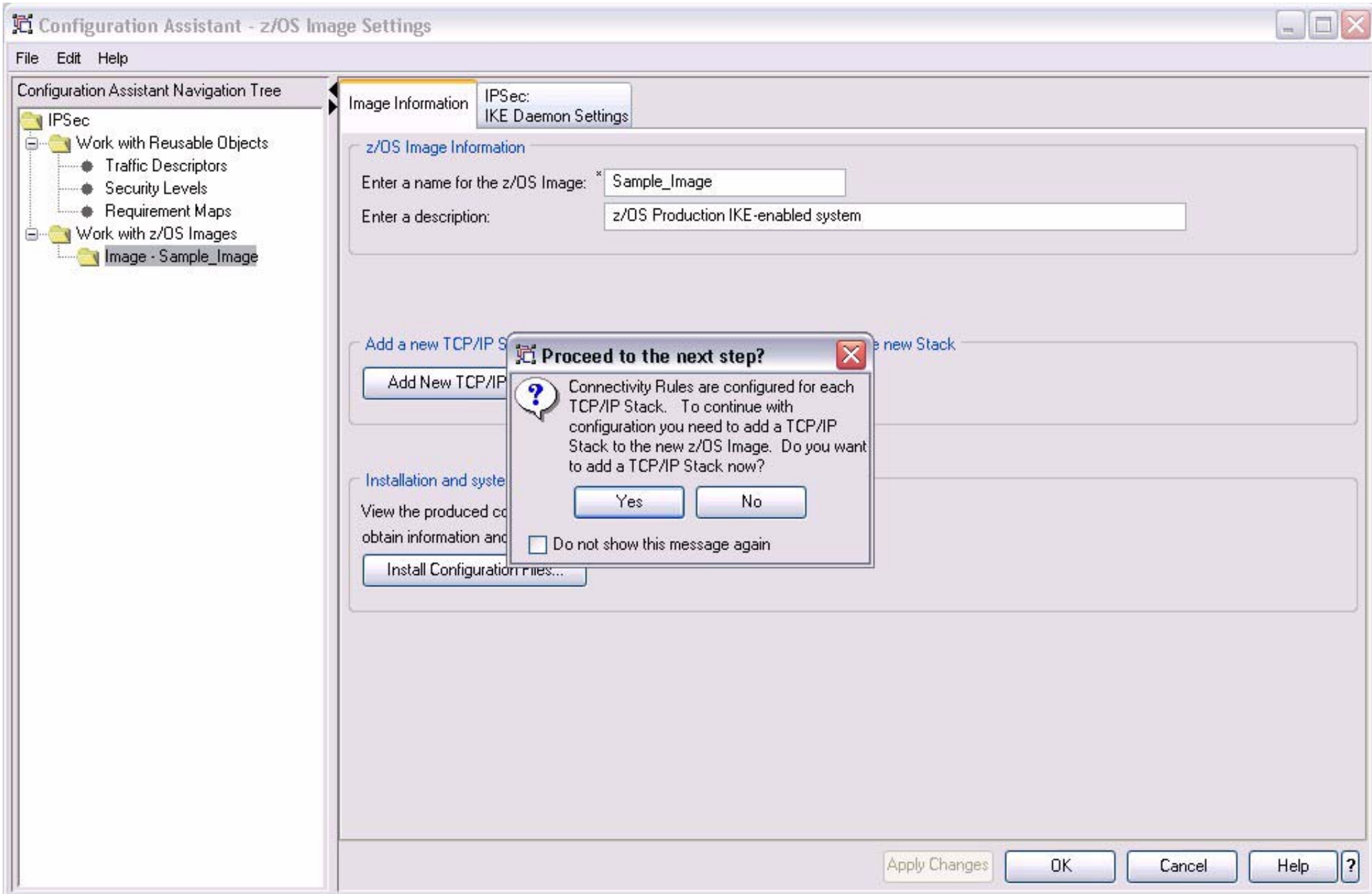
Labels
IBM World Registry CA

Logging

Click below to modify the IKE daemon or Policy Agent trace levels.

Additional Advanced IKE Daemon Settings

Configure Stack



Configure Stack Name

New TCP/IP Stack: Name

TCP/IP Stack Information:

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

Enter a description: Secure IPSec-protected stack

Indicate if this Stack will use dynamic tunnels

Yes, this Stack will have dynamic tunnels

No, this Stack will not have dynamic tunnels

Help ? < Back Next > Finish Cancel

Configure Stack IKE Identity

New TCP/IP Stack: IPSec Dynamic Tunnel Local Identity

The settings on this panel are only applicable to the IPSec dynamic tunnels.
When starting dynamic tunnels the local and remote IKE daemons must exchange identities.
You must configure a local identity.
You can configure a single identity for all IP addresses on this TCP/IP Stack or you can configure separate identities for each IP address on this Stack.

I want to configure separate local identities for each IP address local to this Stack;
I will be prompted later for this information.

I want to use a single identity for all IP addresses on this Stack

Enter the local identity for all IP addresses on this Stack

IP address: *

Fully qualified domain name (FQDN): * zos.raleigh.ibm.com

User id @ FQDN: *

X.500 distinguished name: *

Help ? < Back Next > Finish Cancel

Configure IPSec Stack Level Settings

New TCP/IP Stack: IPSec Stack Level Settings

The settings on this panel are only applicable to IPSec.

Network Address Translation (NAT) Traversal Policy (only for Dynamic Tunnels)
Indicate the default setting for NAT traversal to be used in Connectivity Rules.

NAT Default

Do not allow Allow Allow - no port translation

NAT keepalive messages

Do not send NAT keepalive messages

Send NAT keepalive message after specified interval of inactivity: * (Seconds)

Filter Logging Policy
Indicate whether you want all filter logging disabled.

Disable all filter logging

Enable filter logging

Log implicit deny events Do NOT log implicit deny events

Indicate whether IPSec (AH or ESP) headers should be filtered

Do not filter the IPSec (AH or ESP) headers, decapsulate them prior to filtering

Filter the IPSec (AH or ESP) headers

Automatically allow for IP V6 link activation

Allow Do not allow

Help ? < Back Next > Finish Cancel

Reusable Objects

- Can configure Top-down, Bottom-up or anywhere in between
- Configuration Assistant provides buttons to link to other objects where and when you need them:
 1. Traffic Descriptors
 2. Security Levels
 3. Requirement Maps

Traffic Descriptors


Configuration Assistant - Traffic Descriptors

File Edit Help

Configuration Assistant Navigation Tree

- IPSec
 - Work with Reusable Objects
 - Traffic Descriptors**
 - Security Levels
 - Requirement Maps
 - Work with z/OS Images
 - Image - Sample_Image
 - Stack - TCPIP

List of all defined Traffic Descriptor objects



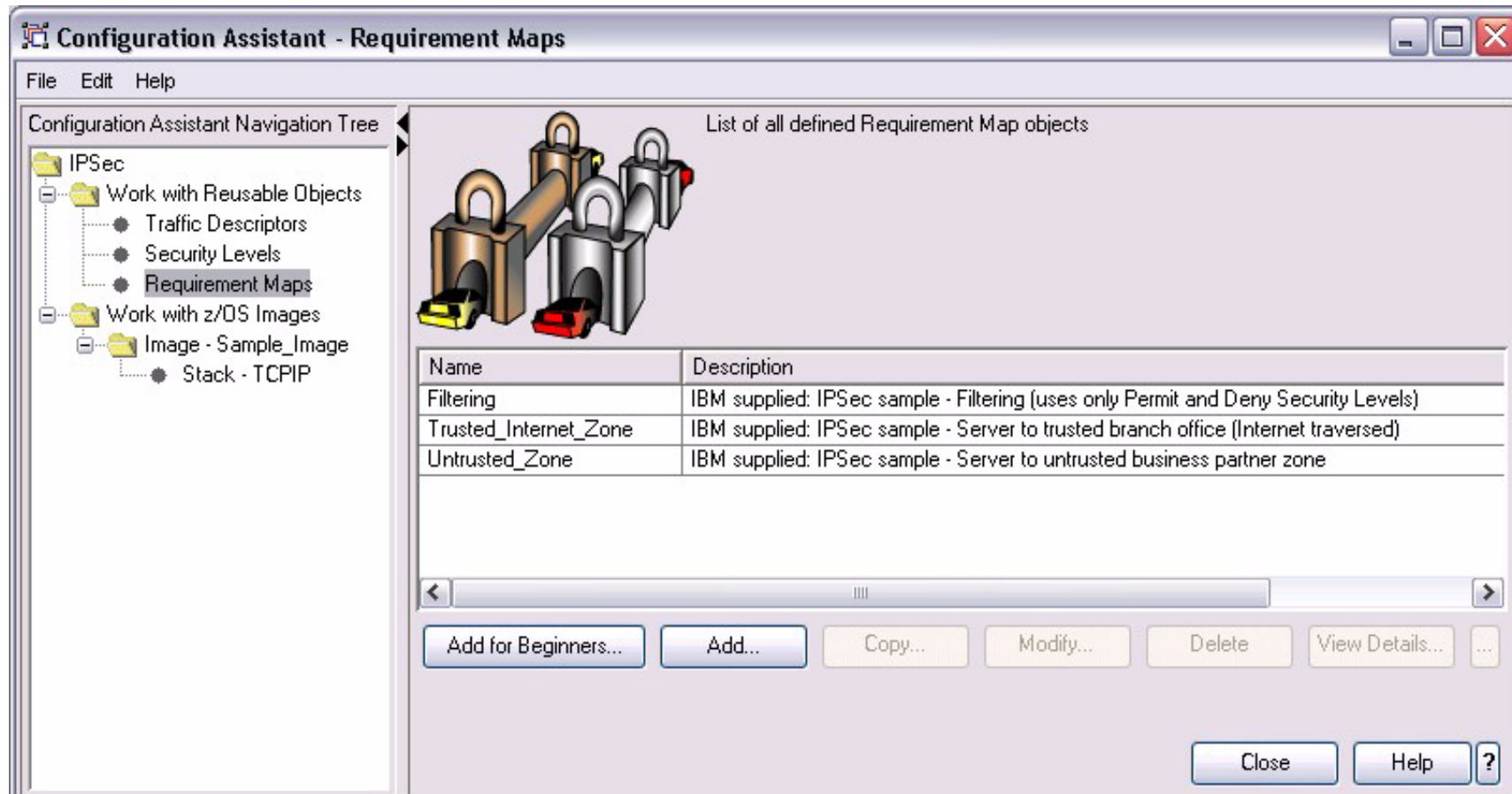
(VERIFY) IBM supplied - contents should be verified and modified to match your network traffic.

Name	Description
CICS	(VERIFY) IBM supplied: CICS traffic
DNS	(VERIFY) IBM supplied: Domain Name Server traffic
EE	IBM supplied: Enterprise Extender (EE) traffic
FTP-Client	(VERIFY) IBM supplied: FTP Client traffic
FTP-Server	(VERIFY) IBM supplied: FTP Server traffic
FTP-Server-SSL	(VERIFY) IBM supplied: FTP Server SSL traffic using port 990
ICMP-Redirect-IP_V4	IBM supplied: IP V4 ICMP - Redirect traffic
ICMP-Redirect-IP_V6	IBM supplied: IP V6 ICMP - Redirect traffic
ICMP-Time_Exceeded-IP...	IBM supplied: IP V4 ICMP - Time Exceeded traffic
ICMP-Time_Exceeded-IP...	IBM supplied: IP V6 ICMP - Time Exceeded traffic
ICMP-Unreachable-IP_V4	IBM supplied: IP V4 ICMP - Unreachable traffic
ICMP-Unreachable-IP_V6	IBM supplied: IP V6 ICMP - Unreachable traffic
IKE	IBM supplied: Internet Key Exchange daemon traffic
IKE-NAT	IBM supplied: NAT - Internet Key Exchange daemon traffic
IKE-NAPT	IBM supplied: NAPT - Internet Key Exchange daemon traffic
Kerberos	(VERIFY) IBM supplied: Kerberos Server traffic
LBA-Advisor	(VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic
LBA-Agent	(VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic
LDAP-Server	(VERIFY) IBM supplied: LDAP Server traffic

Security Levels



Requirement Maps



Configuration Assistant Demo Task

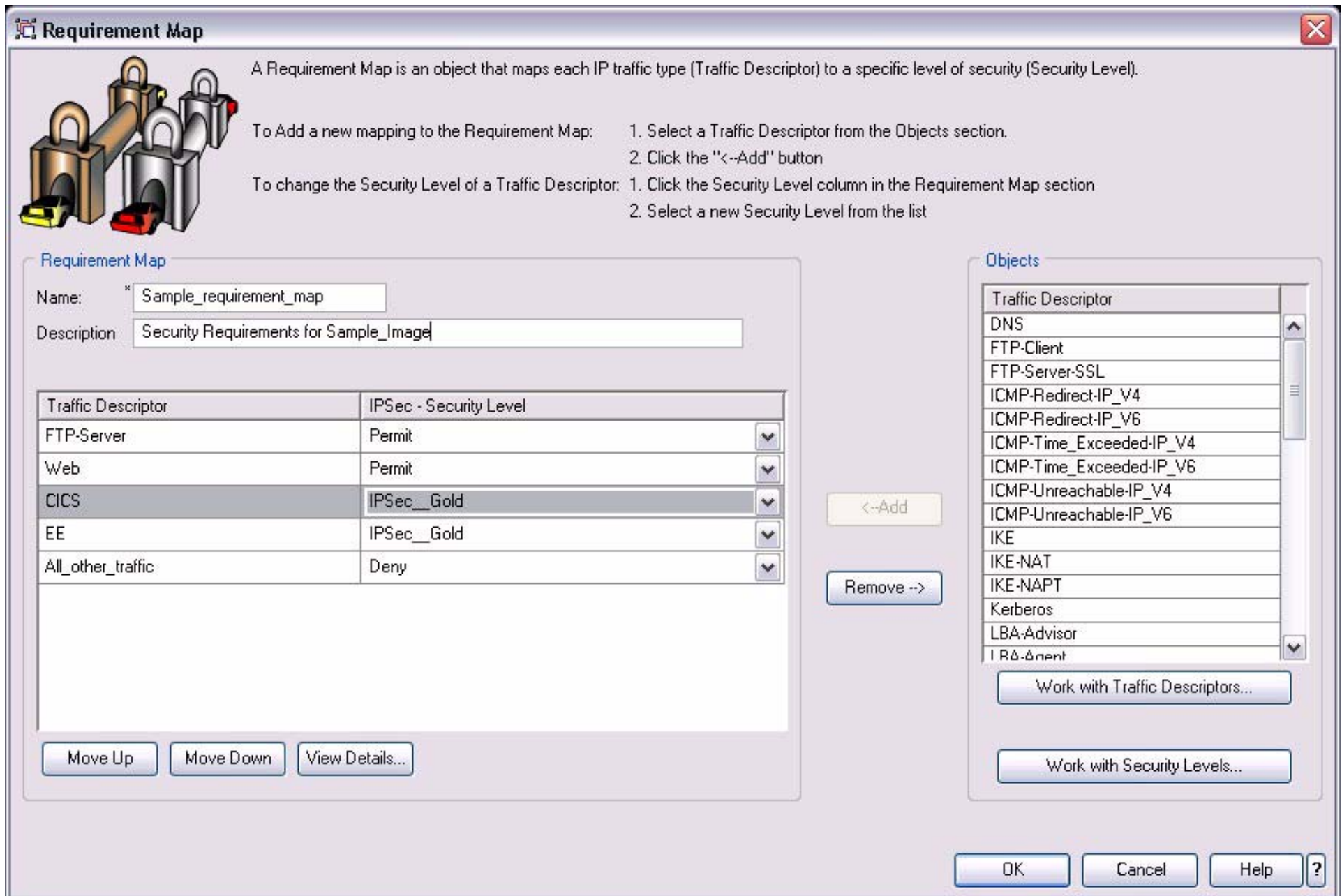
- Create a Connectivity Rule with the four following requirements:
 - ✓ Permits connections to an FTP server
 - ✓ Permits connections to a Web server
 - ✗ Encrypts CICS traffic
 - ✗ Encrypts EE traffic

- Steps for accomplishing the above task
 1. Create a Requirements Map
 2. Create a Connectivity Rule
 3. Iteratively Copy a Connectivity Rule
 4. Run the Configuration Assistant Health Checker
 5. Upload and install the policy

Step One: Create a Requirement Map

- Select "Requirement Maps" from the Navigation Tree
- Use "Add..." to create the set of desired traffic (FTP-Server, Web, CICS, EE)
- Select Security Level of "Permit" for FTP and Web server traffic
- Select Security Level of "IPSec__Gold" for EE and CICS traffic

Step One: Create a Requirement Map



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: * Sample_requirement_map

Description: Security Requirements for Sample_Image

Traffic Descriptor	IPSec - Security Level
FTP-Server	Permit
Web	Permit
CICS	IPSec_Gold
EE	IPSec_Gold
All_other_traffic	Deny

Move Up Move Down View Details...

Objects

Traffic Descriptor
DNS
FTP-Client
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
ICMP-Unreachable-IP_V6
IKE
IKE-NAT
IKE-NAPT
Kerberos
LBA-Advisor
IRDAgent

<--Add

Remove -->

Work with Traffic Descriptors...

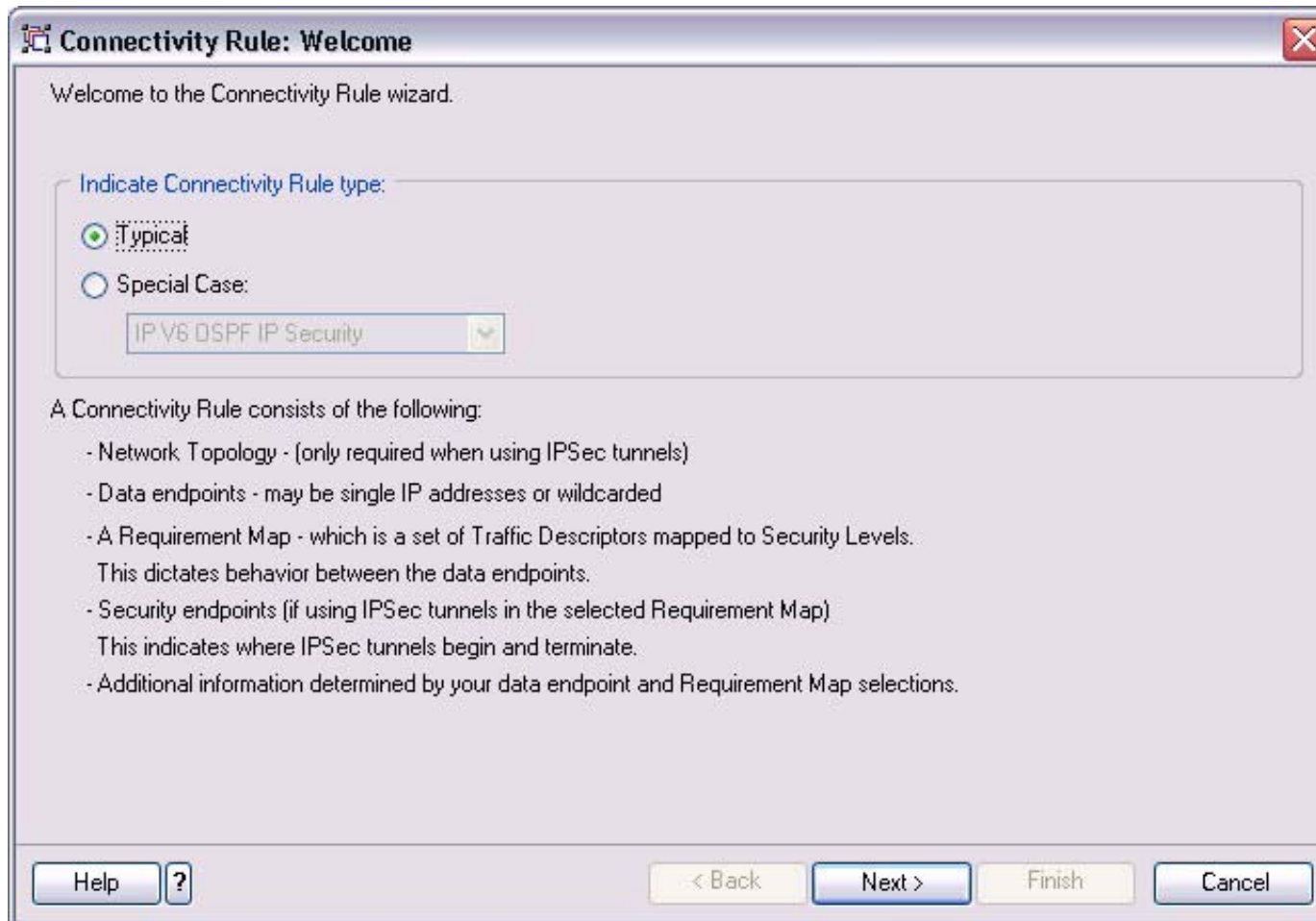
Work with Security Levels...

OK Cancel Help ?

Step Two: Create a Connectivity Rule

- Select the appropriate TCP/IP stack
- Add a "Typical" rule
- Select a topology
- Specify the local and remote Data Endpoints
 - applies bidirectionally to traffic
 - outbound from local to remote
 - inbound from remote to local
- Select the appropriate Requirement Map
- Configure the Security Endpoint information
- If the IKE daemon is using a single Identity, only the remote Identity is required (can use wildcarding for remote Identity)
- Select the IKE authentication method (the RSA method requires certificates)


Step Two: Create a Connectivity Rule



Step Two: Create a Connectivity Rule

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:
* 9.9.9.9

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:
* 1.1.1.1

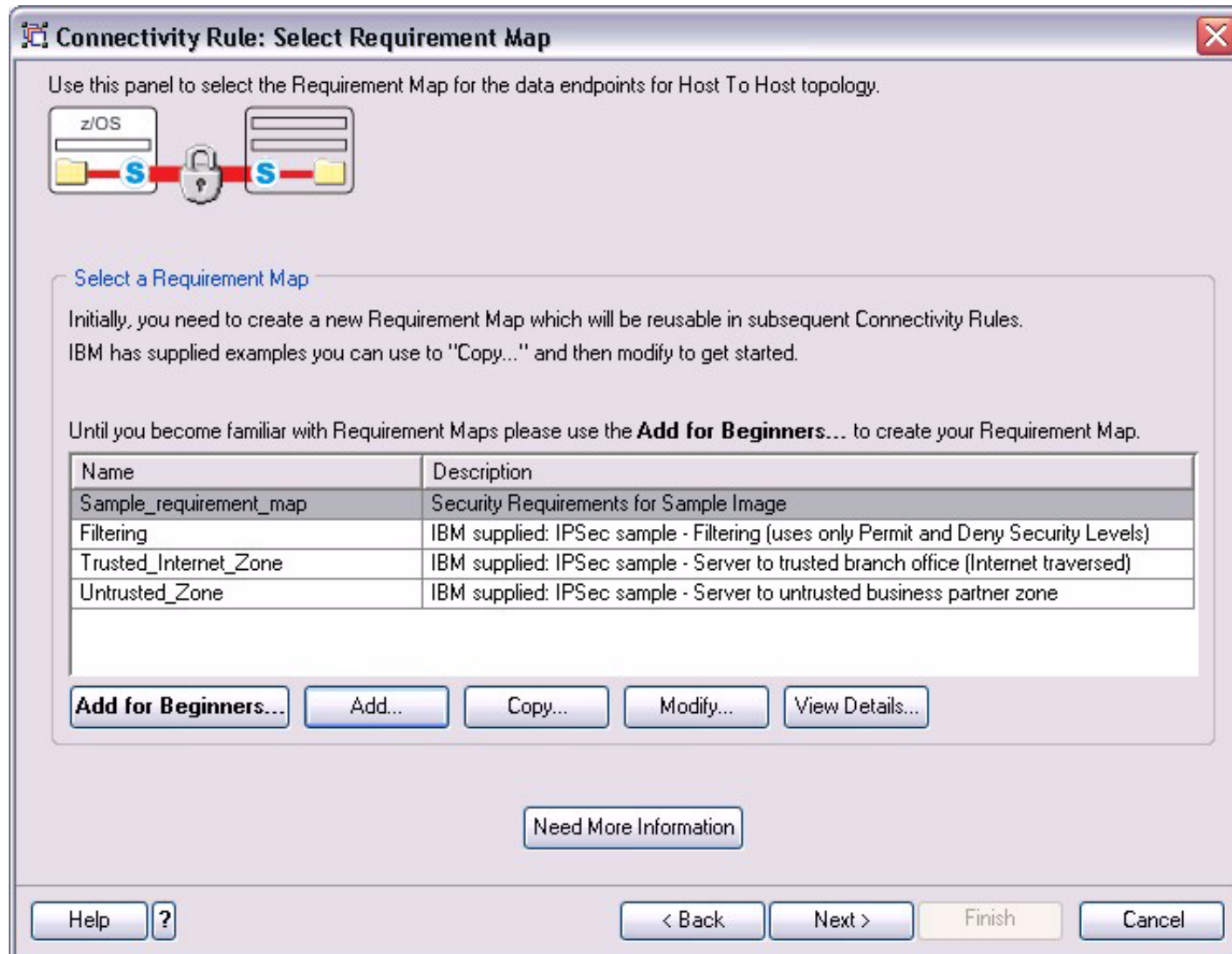
Syntax: Single IP V4 address: x.x.x.x
IP V4 subnet: x.x.x.x/yy
IP V4 range: x.x.x.x-y.y.y.y
Single IP V6 address: x::x
IP V6 subnet: x::x/yyy
IP V6 range: x::x-y::y

Connectivity Rule Name

Name: * IP_FilterRule_Endpoint1

Help ? < Back Next > Finish Cancel


Step Two: Create a Connectivity Rule



Step Two: Create a Connectivity Rule

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: *

Fully qualified domain name (FQDN): * *.ibm.com

User id @ FQDN: *

X.500 distinguished name: *

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

RSA signature

Shared key: EBCDIC ASCII Hexadecimal *

Help ? < Back Next > Finish Cancel

Connectivity Rule - Additional Settings

- Filter logging
- Advanced settings
 - Activation settings
 - Encapsulation mode
 - SA granularity
 - Key Exchange Settings
 - Remote Security Endpoint Certificate Authority certificate settings
 - Time of day settings (determines when the rule is active)

Connectivity Rule - Additional Settings

Connectivity Rule: Additional Settings

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

Step three: Copy a Connectivity Rule

- For each remote endpoint which has the same security requirements
 - Highlight the Connectivity Rule and click "Copy..."
 - Enter the new remote Data Endpoint
 - Type a new Rule name
 - Click "Apply Changes" after modifications

- ★ Note that each rule created uses the same Requirement Map and is described by the same topology

Step three: Copy a Connectivity Rule

Configuration Assistant - TCP/IP Stack Settings

File Edit Help

Configuration Assistant Navigation Tree

- IPSec
 - Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
 - Work with z/OS Images
 - Image - Sample_Image
 - Stack - TCPIP

Connectivity Rules

IPSec: Dynamic Tunnel Local Identity

IPSec: Stack Level Settings

TCP/IP Stack Information:

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

Enter a description: IPSECURITY-enabled TCP/IP stack

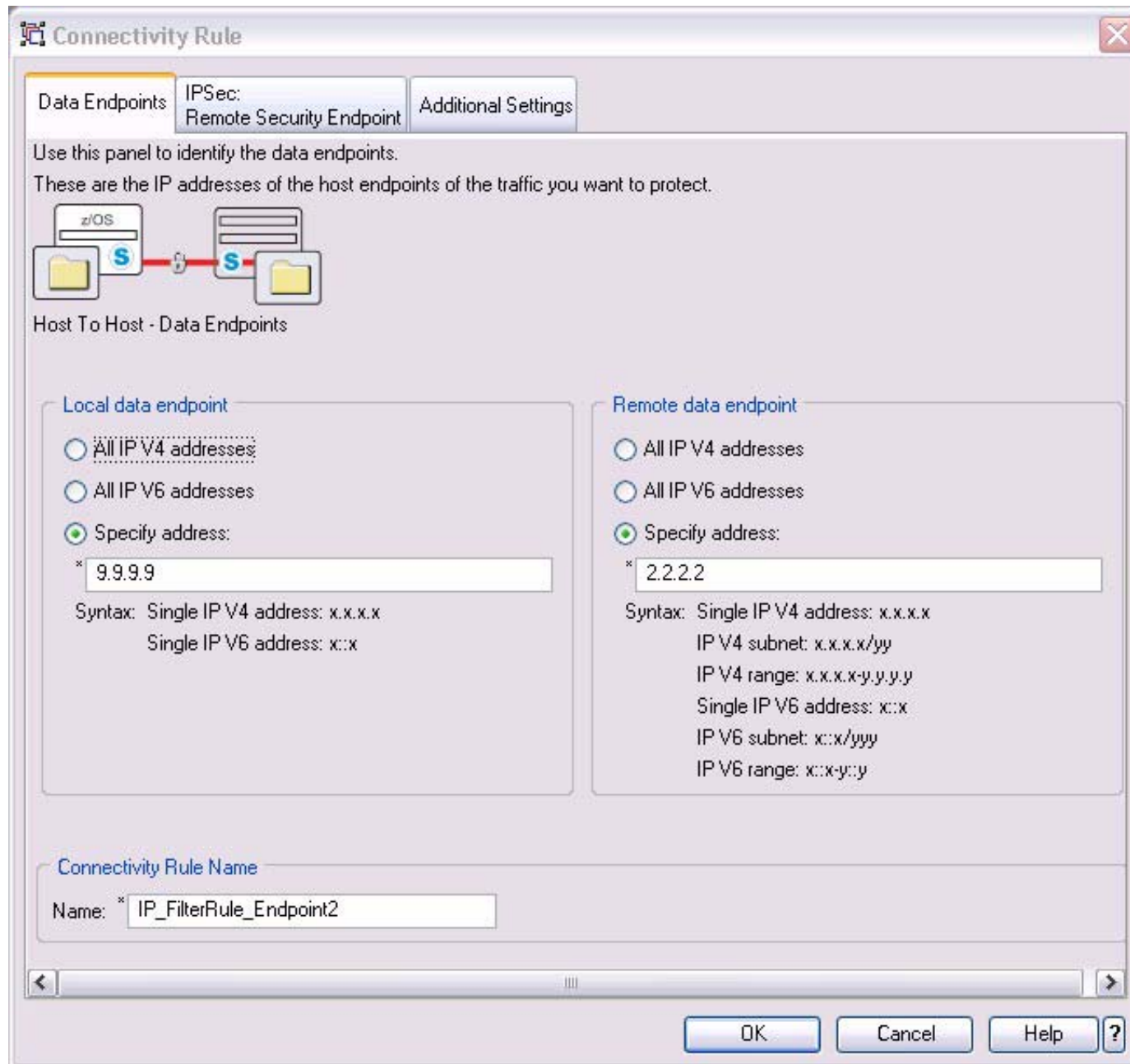
Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local / Source Data Endpoint	Remote / Destination Data Endpoint	Requirement Map	Topology	Status	Name
9.9.9.9	1.1.1.1	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint1

Buttons: Add... Copy... Modify Basics... Delete View Details... Move Up Health Check... Modify Wizard... Move Down

Buttons: Apply Changes OK Cancel Help ?

Step three: Copy a Connectivity Rule



Step three: Copy a Connectivity Rule

Configuration Assistant - TCP/IP Stack Settings

File Edit Help

Configuration Assistant Navigation Tree

- IPSec
 - Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
 - Work with z/OS Images
 - Image - Sample_Image
 - Stack - TCPIP

Connectivity Rules IPsec: Dynamic Tunnel Local Identity IPsec: Stack Level Settings

TCP/IP Stack Information:

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

Enter a description: IPSECURITY-enabled TCP/IP stack

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

Local / Source Data Endpoint	Remote / Destination Data Endpoint	Requirement Map	Topology	Status	Name
9.9.9.9	1.1.1.1	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint1
9.9.9.9	2.2.2.2	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint2
9.9.9.9	3.3.3.3	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint3
9.9.9.9	4.4.4.4	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint4
9.9.9.9	5.5.5.5	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint5

Step four: Run Health Checker

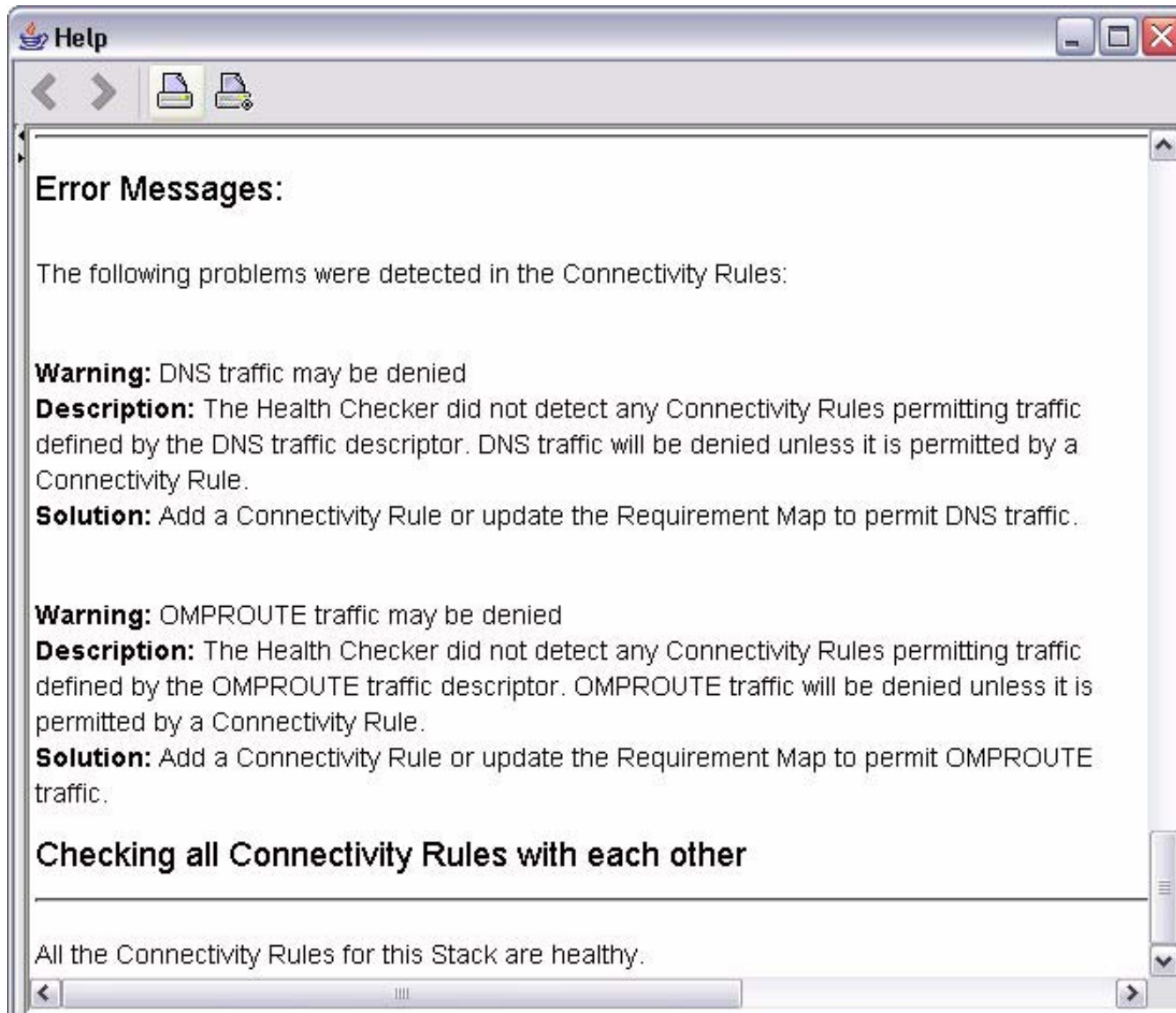
Health Check: IPsec

Below are the results from running a health check against this stack.

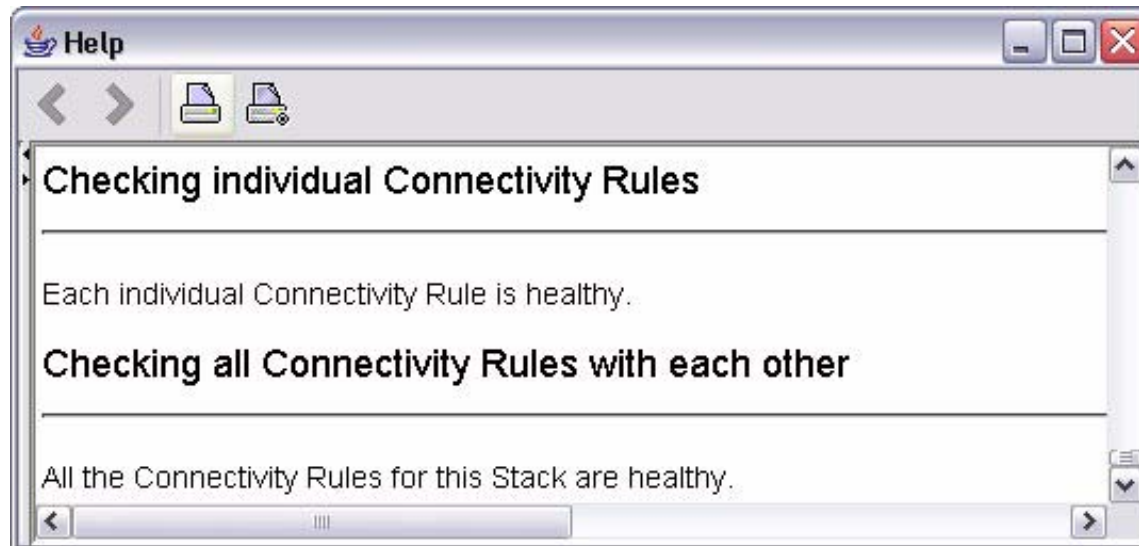
Table of the Connectivity Rules with the Traffic Descriptors and Security Levels in the order as was defined.

Connectivity Rule	Traffic Descriptor	Security Level	Index	Protocol	Source Port	Dest Port	Connect Direction	Type Code 1
IP_FilterRule_Endpoint1 9.9.9.9 1.1.1.1 Host to Host	FTP-Server	Permit	1	TCP	21	1024-65535	Inbound	---
			2	TCP	20	1024-65535	Outbound	---
			3	TCP	50000-50200	1024-65535	Inbound	---
	Web	Permit	4	TCP	80	1024-65535	Inbound	---
	FF	IPSec__	5	UDP	12000	12000	Both	---
			6	UDP	12001	12001	Both	---
			7	UDP	12002	12002	Both	---

Scan Health Checker Output for Warnings



Warnings Fixed



Step five: Upload IPSec policy

- Right click on the appropriate TCP/IP stack
- Select "Install Configuration Files..."
- Select the "IPSec: Policy Agent Stack Configuration" file
- Optionally, view or save the generated configuration file ("Show Configuration File..." button)
- Use the Configuration Assistant built-in FTP client to transfer IPSec policy file
- Refresh the policy using the console MODIFY command

Step five: Upload IPSec policy

Configuration Assistant - TCP/IP Stack Settings

File Edit Help

Configuration Assistant Navigation Tree

- IPSec
 - Work with Reusable Objects
 - Traffic Descriptors
 - Security Levels
 - Requirement Maps
 - Work with z/OS Images
 - Image - Sample_Image
 - Stack TCP/IP

Connectivity Rules

IPSec: Dynamic Tunnel Local Identity

IPSec: Stack Level Settings

TCP/IP Stack Information:

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

Enter a description: IPSECURITY-enabled TCP/IP stack

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

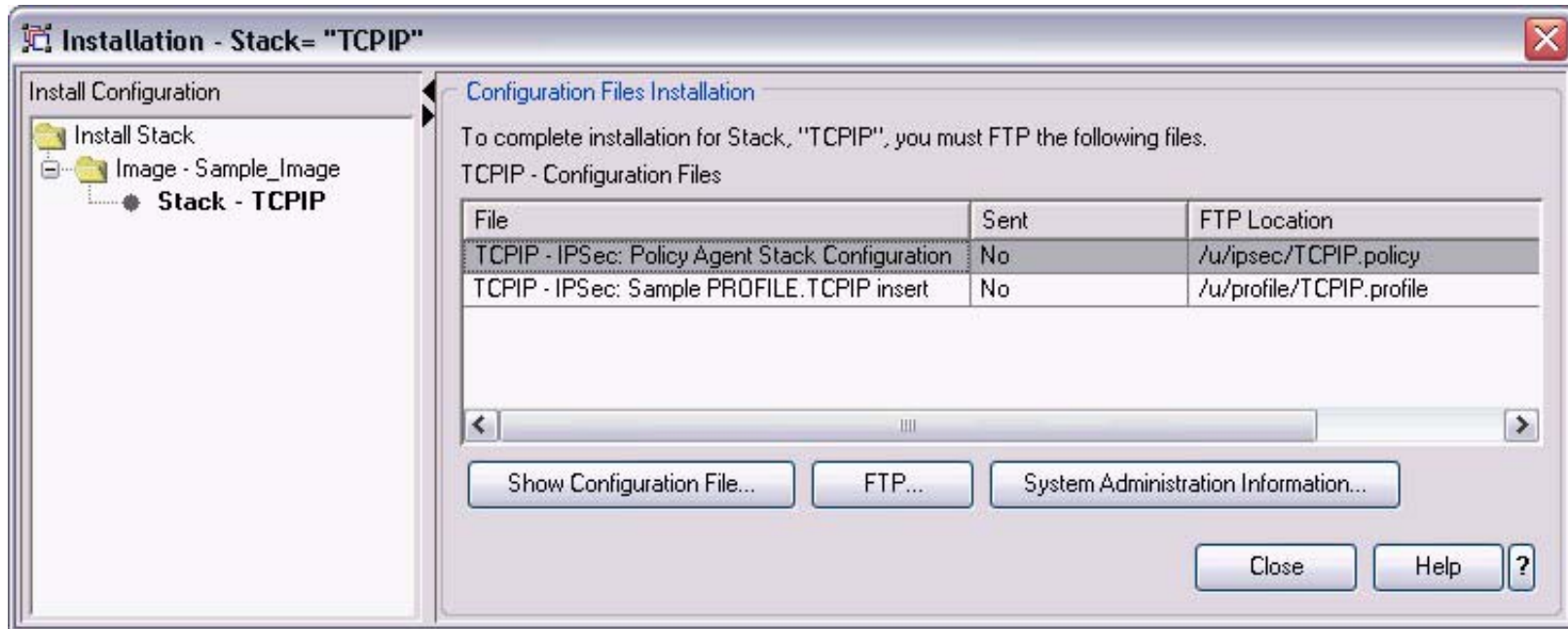
Data Endpoint	Remote / Destination Data Endpoint	Requirement Map	Topology	Status	Name
9.9.9.9	1.1.1.1	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint1
9.9.9.9	2.2.2.2	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint2
9.9.9.9	3.3.3.3	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint3
9.9.9.9	4.4.4.4	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint4
9.9.9.9	5.5.5.5	Sample_requirement_map	Host to Host	Complete	IP_FilterRule_Endpoint5

Copy the TCP/IP Stack...
Delete the TCP/IP Stack
Install Configuration Files...

Add... Copy... Modify Basics... Delete View Details... Move Up Health Check...
Modify Wizard... Move Down

Apply Changes OK Cancel Help ?

Step five: Upload IPsec policy



Step five: Upload IPsec policy

FTP Configuration File

Enter FTP information to send the files.

Login information

Host name: * zos.raleigh.ibm.com

Port number: * 21

User ID: * user1

Password: * ***** Save password

Use SSL

FTP file including full path

File name and location: * /etc/ipsec/TCPIP.policy

Send Close Help ?

Modifying existing policies

- Modification of reusable objects will affect all rules which use them
- Modification of individual Connectivity Rules can be done with either the
 - Modify Basics (modify endpoint addresses, rule name, identities, etc.)
 - Modify Wizard (modify anything, including the items listed above)

Activation Settings

- Security Associations can be activated in one of four ways

▶ Ondemand	activated without user intervention
▶ Command-line	activated with the <code>ipsec</code> command
▶ Autoactivation	activated when IPSec policy is installed in the TCP/IP stack
▶ Remote	activated when a remote host initiates a negotiation (policy can restrict to local activation only)

- Activation method can be configured in the "Advanced Connectivity Rule Settings" panel

Activation Settings

Advanced Connectivity Rule Settings

IPSec: Dynamic Tunnels: How to Activate | IPSec: Dynamic Tunnels: OnDemand Granularity / Encapsulation Mode | IPSec: Dynamic Tunnels: Key Exchange Settings | IPSec: Dynamic Tunnels: Remote Security Endpoint Settings | IPSec: Filter Logging / Effective Time

The settings on this panel are only applicable to the IPSec dynamic tunnels.
Use this panel to indicate how each dynamic tunnel may be activated.

Indicate "Yes" or "No" in each activation column. When using "ipsec Command Activation", edit the "ipsec Command Handle" column to enter a required handle; see Helps for details

Traffic Descriptor	Protocol	Local Port	Remote Port	Connect Direction	IPSec Security Level	Allow Remote Activation	Allow OnDeman Activation	Auto Activate	ipsec Command Activation	ipsec Command Handle
EE	UDP	12000	12000	----	IPSec_Gold	Yes	Yes	No	No	
EE	UDP	12001	12001	----	IPSec_Gold	Yes	Yes	No	No	
EE	UDP	12002	12002	----	IPSec_Gold	Yes	Yes	No	No	
EE	UDP	12003	12003	----	IPSec_Gold	Yes	Yes	No	No	
EE	UDP	12004	12004	----	IPSec_Gold	Yes	Yes	No	No	
CICS	TCP	3000	All Ephemeral	Inbound only	IPSec_Gold	Yes	No	No	No	

Click To Refine Selected Port Range: Only Required for Auto Activation or ipsec Command Activation...

OK Cancel Help ?

IPSec Features Summary

■ IP Filtering

- Source Address
- Destination Address
- Source Port
- Destination port
- Protocol
- Direction
- Routing
- Security class

■ IPSec protection

- Protocols
 - AH
 - ESP
- Algorithms
 - Authentication
 - MD5
 - SHA
 - Encryption
 - DES
 - 3DES
 - AES-128
- Diffie-Hellman groups 1, 2, 5, 14
- SA activation
- NAT traversal

ipsec Command Summary

Primary Command Options

Primary Command	Main functions provided
ipsec -f	<ul style="list-style-type: none"> • Display information about active filter set • Display information about default IP filter rules • Display information about IP Security filter rules • Make the default IP filter rules the active filter set • Make the IP Security filter rules the active filter set
ipsec -m	<ul style="list-style-type: none"> • Display information about manual tunnels • Activate manual tunnels • Deactivate manual tunnels
ipsec -k	<ul style="list-style-type: none"> • Display information about IKE tunnels • Deactivate IKE tunnels • Refresh IKE tunnels
ipsec -y	<ul style="list-style-type: none"> • Display information about dynamic tunnels (stack's view) • Display information about dynamic tunnels (IKED's view) • Activate dynamic tunnels • Deactivate dynamic tunnels • Refresh dynamic tunnels
ipsec -i	<ul style="list-style-type: none"> • Display interface information
ipsec -t	<ul style="list-style-type: none"> • Locate matching filter rule
ipsec -o	<ul style="list-style-type: none"> • Display NATT port translation table information
ipsec -?	Help

See the "IP System Administrator's Commands" for the complete syntax

For More Information...

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/servers/eserver/zseries/networking/technology.html	IBM Enterprise Servers: Networking Technologies
http://www.ibm.com/software/network/commserver	Communications Server product overview
http://www.ibm.com/software/network/commserver/zos/	z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	Communications Server for Linux on zSeries
http://www.ibm.com/software/network/ccl	Communication Controller for Linux on zSeries
http://www.ibm.com/software/network/commserver/library	Communications Server products - white papers, product documentation, etc.
http://www.redbooks.ibm.com	ITSO redbooks
http://www.ibm.com/software/network/commserver/support	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 (RFC)