IBM

z/OS Communication Server IPSec and IP Packet Filtering

Lin Overby - overbylh@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:

- ► Advanced Peer-to-Peer Networking®
- ► AIX®
- ► alphaWorks®
- ► AnyNet®
- ► AS/400®
- ► BladeCenter®
- ► Candle®
- ► CICS®
- ► DB2 Connect
- ► DB2®
- ► DRDA®
- ► e-business on demand®
- ► e-business (logo)
- ► e business(logo)®
- ► ESCON®
- ► FICON®

- ► GDDM®
- ► HiperSockets
- ► HPR Channel Connectivity
- ► HyperSwap
- ► i5/OS (logo)
- ► i5/OS®
- ► IBM (logo)®
- ► IBM®
- ► IMS
- ► IP PrintWay
- ► IPDS
- ► iSeries
- ► LANDP®
- ► Language Environment®
- ► MQSeries®
- ► MVS
- ► NetView®

- ► OMEGAMON®
- ► Open Power
- ► OpenPower
- ► Operating System/2®
- ► Operating System/400®
- ► OS/2®
- ► OS/390®
- ► OS/400®
- ► Parallel Sysplex®
- ► PR/SM
- ► pSeries®
- ► RACF®
- ► Rational Suite®
- ► Rational®
- ► Redbooks
- ► Redbooks (logo)
- ► Sysplex Timer®

- ► System i5
- ► System p5
- ► System x
- ► System z
- ► System z9
- ► Tivoli (logo)®
- ► Tivoli®
- ► VTAM®
- ► WebSphere®
- ► xSeries®
- ► z9
- ► zSeries®
- ► z/Architecture
- ► z/OS®
- ► z/VM®
- ► z/VSE

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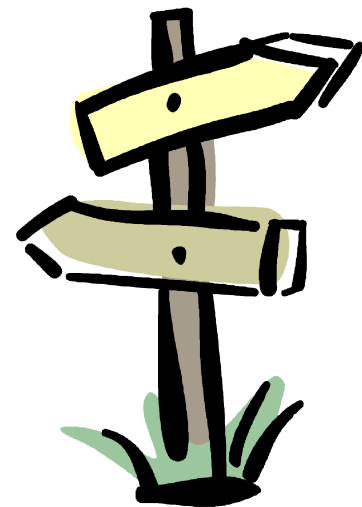
All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

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

z/OS Communications Server IP security agenda
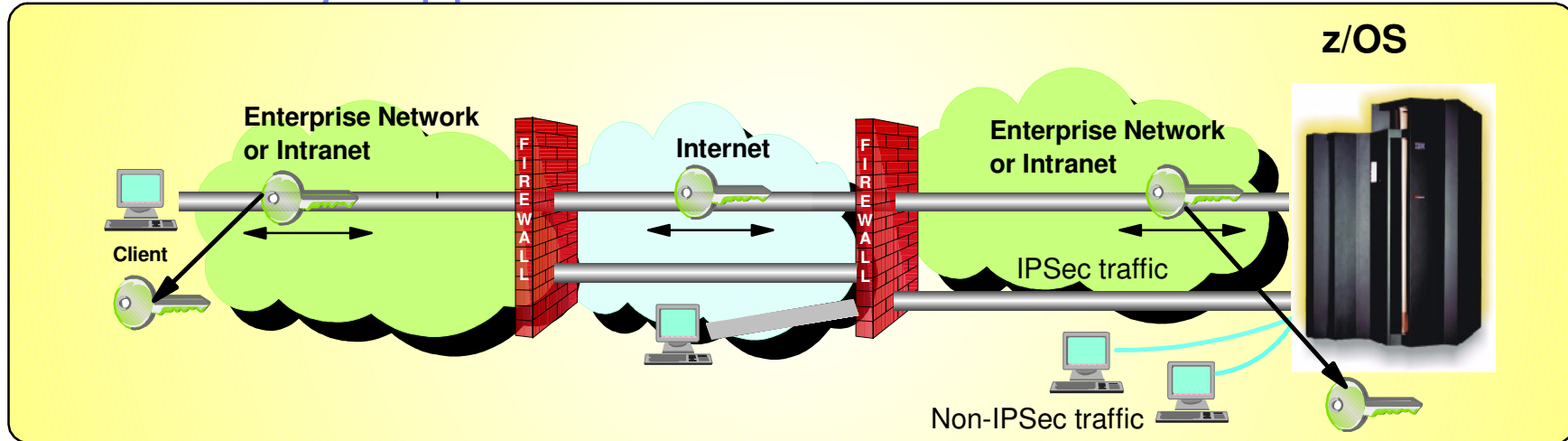
- **Introduction to IP security on z/OS**

- **IP filtering**

- **IPSec**

- **Special topics**

- **IP security displays and controls**

- **Configuring and enabling IP Security**

z/OS Communications Server IP security

Introduction

z/OS IP security support

z/OS

Enterprise Network or Intranet

Internet

Enterprise Network or Intranet

F I R E W A L L

F I R E W A L L

Client

IPSec traffic

Non-IPSec traffic

- z/OS IP Security is a complete IPSec, IP filtering, and IKE solution and is part of z/OS Communications Server

- Services
  - ► Protect the system from the network
    - – IP filtering to control which packets can enter the system
  - ► Protect against data leakage from the system
    - – IP filtering to control which packets can leave the system
  - ► Cryptographic protection of data in the network
    - – Manual IPSec (statically defined security associations)
    - – Dynamic negotiation of IPSec security associations using Internet Key Exchange (IKE)
  - ► Filter directed logging of IP Security actions to syslogd

z/OS Communications Server IP security features

- **Supports many configurations**
  - ➤ Optimized for role as endpoint (host), but also support routed traffic (gateway)
  - ➤ IPSec NAT Traversal support (address translation and port translation)
  - ➤ IPv4 and IPv6 support

- **Policy-based**
  - ➤ Configuration Assistant GUI for both new and expert users
  - ➤ Direct file edit into local configuration file

- **Default filters in TCP profile provide basic protection before policy is loaded**

- **Cryptographic algorithms**
  - ➤ RSA signature-based authentication
  - ➤ ECDSA signature-based authentication **(V1R12)**
  - ➤ HMAC-SHA-1, HMAC-MD5 authentication
  - ➤ HMAC-SHA-2, AES-XCBC, AES-GMAC authentication **(V1R12)**
  - ➤ AES-CBC, 3DES and DES encryption
  - ➤ AES-GCM (128- and 256-bit) encryption **(V1R12)**
  - ➤ Uses cryptographic hardware if available for most algorithms
  - ➤ FIPS 140 mode **(V1R12)**

- **zIIP Assisted IPSec**
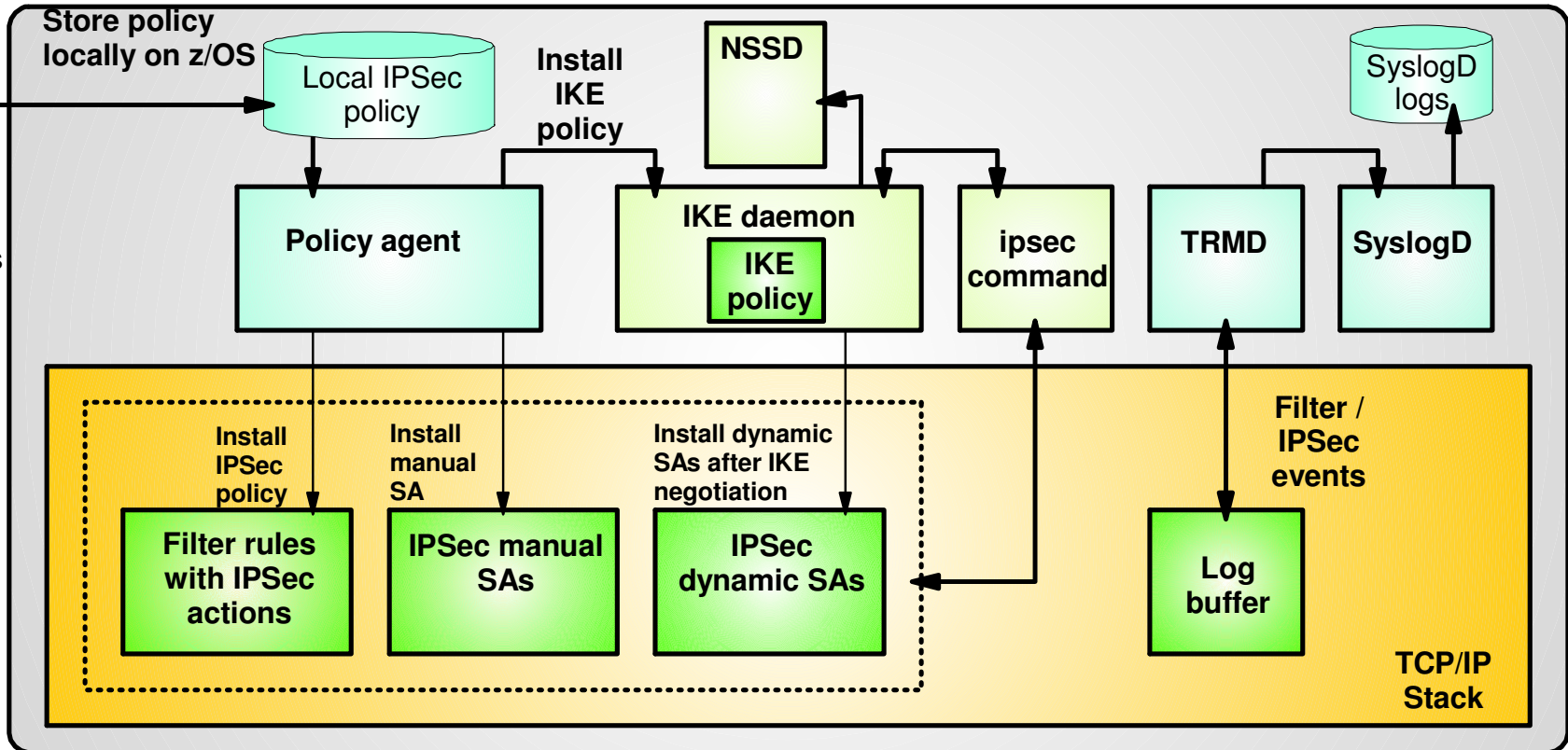 - ➤ Moves most IPSec processing from general purpose processors to zIIPs

- **IP Security Monitoring Interface**
  - ➤ IBM Tivoli OMEGAMON XE for Mainframe Networks uses the CommServer NMI interfaces for IP Security

- **Support for latest IPSec RFCs**
  - ➤ RFCs 4301-4305, 4307-4308 **(V1R10)**
  - ➤ RFC 4306 (IKEv2) **(V1R12)**

z/OS Communications Server IP security infrastructure overview

- **TCP/IP stack**
  - ➤ IPSec and IP filtering
- **Policy agent**
  - ➤ Reads and manages IPSec and IKE policy
- **Configuration Assistant for z/OS Communications Server**
  - ➤ Creates policy definitions
- **IKE daemon**
  - ➤ Negotiates security associations

- **ipsec command**
  - ➤ Displays and controls IP filtering, IPSec, and IKE
- **trmd**
  - ➤ Monitors TCP/IP stacks for log messages
- **syslogd**
  - ➤ Write log messages to syslogd destinations
- **Network Security Services daemon**
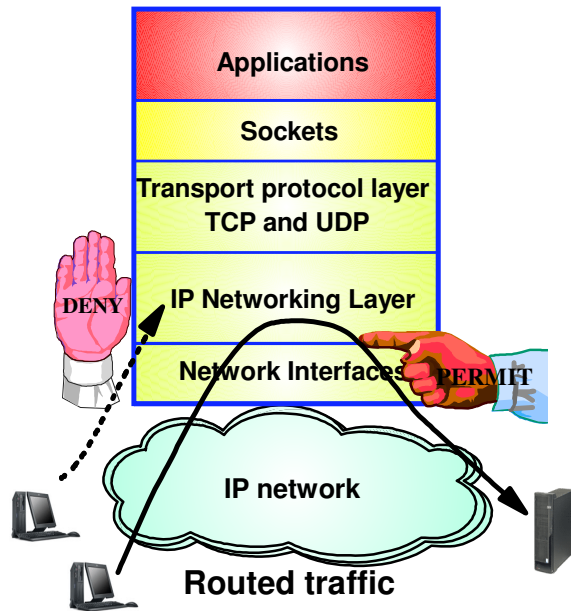 - ➤ Provides certificate services for IKE

z/OS Communications Server IP security

IP filtering

Basics of IP packet filtering

IP packet filtering used to control:

Traffic being routed

Routed traffic

Access at source / destination host

Local traffic

- **Filter rules defined to match on inbound and outbound packets based on:**
 - ➤ packet information
  - ➤ network attributes
  - ➤ time
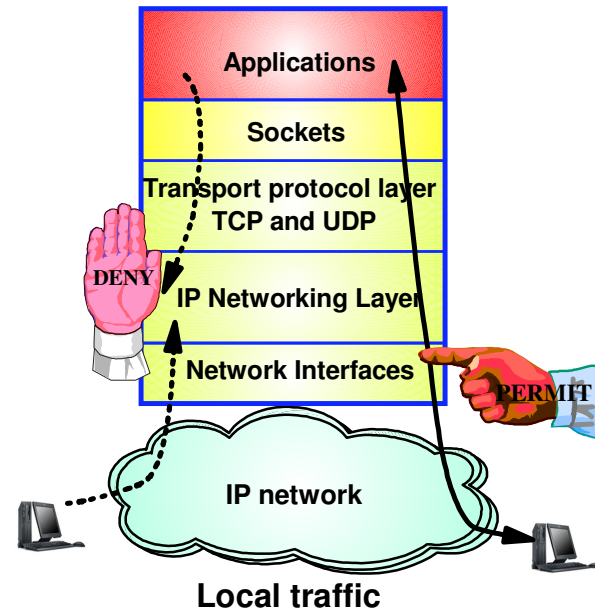
- **Possible actions**
  - ➤ Permit
  - ➤ Deny
  - ➤ Permit with manual IPSec
  - ➤ Permit with dynamic IPSec
  - ➤ Log (in combination with other actions)

IP filtering processing overview

1. **Inbound or outbound IP packet arrives**

2. **Consult set of filter rules in a filter rule table - Security Policy Database (SPD)**
   - ➤ Rules have conditions and actions

3. **Apply action of matching rule to packet**
   - ➤ Deny
   - ➤ Permit
   - ➤ Permit with additional processing applied

TCP/IP Stack

| IP Header | Transport Header | Data |

SPD

Filter Rules

Conditions
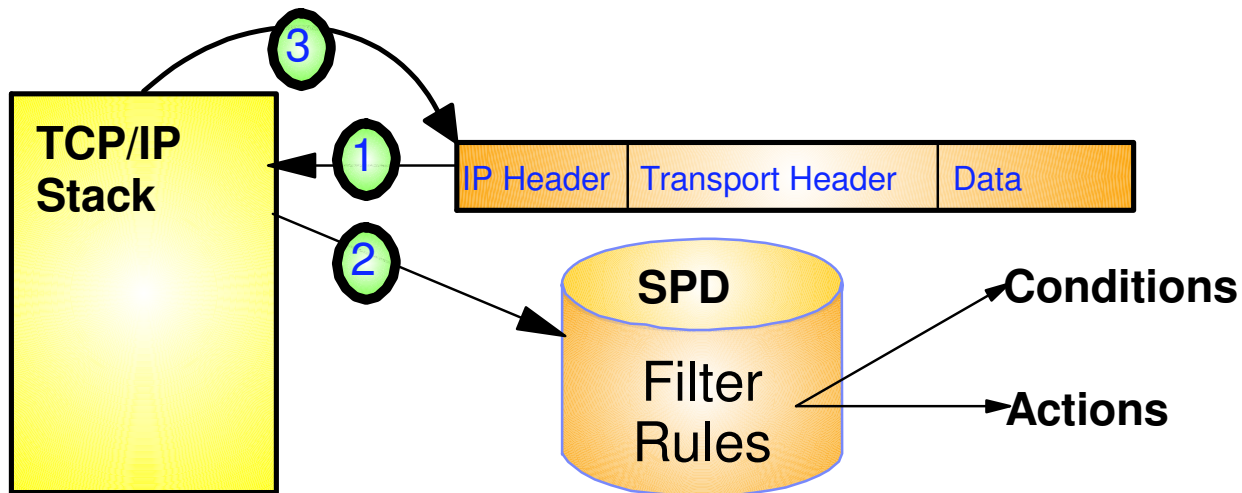
Actions

- Filter rules are searched in the order they were configured
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and the action is performed

IP security - filter policies

- IP security's Security Policy Database (SPD)

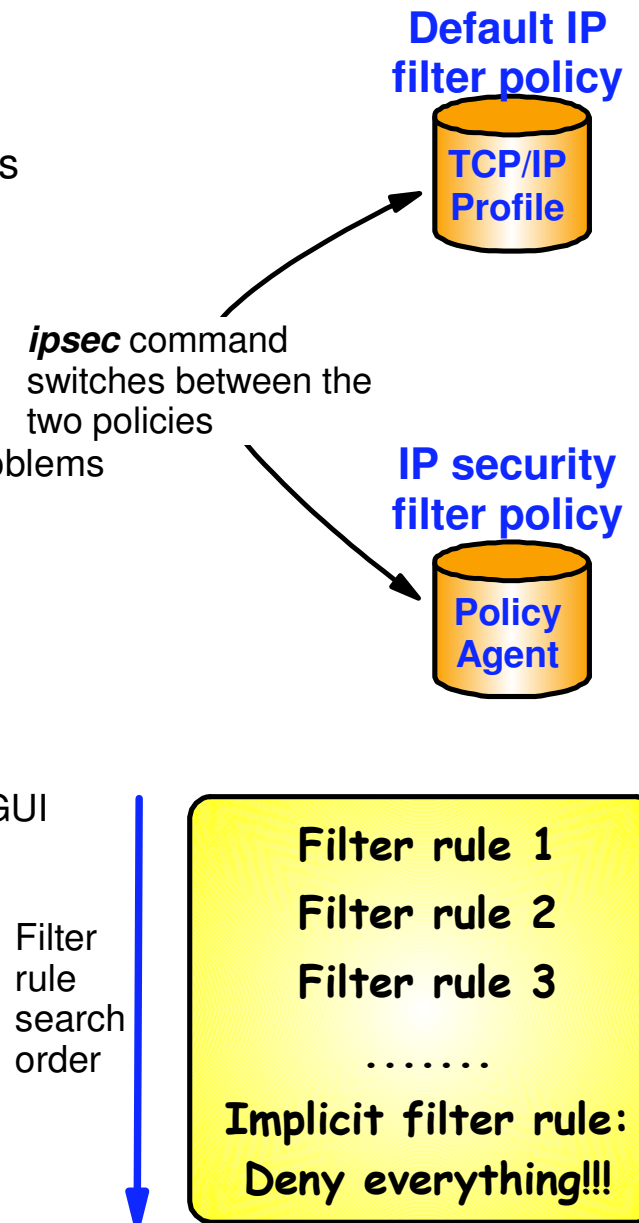 1. Default IP filter policy
     - Intended to allow limited access while IP security filter policy is being loaded
       - Can be reverted to in an "attack" situation
     - Defined in the TCP/IP profile
       - Default is to deny all traffic
     - Provides basic filtering function
       - Permit rules only - Permit traffic needed for basic services / fix problems with IP security filter policy
       - No IPSec support

  2. IP security filter policy
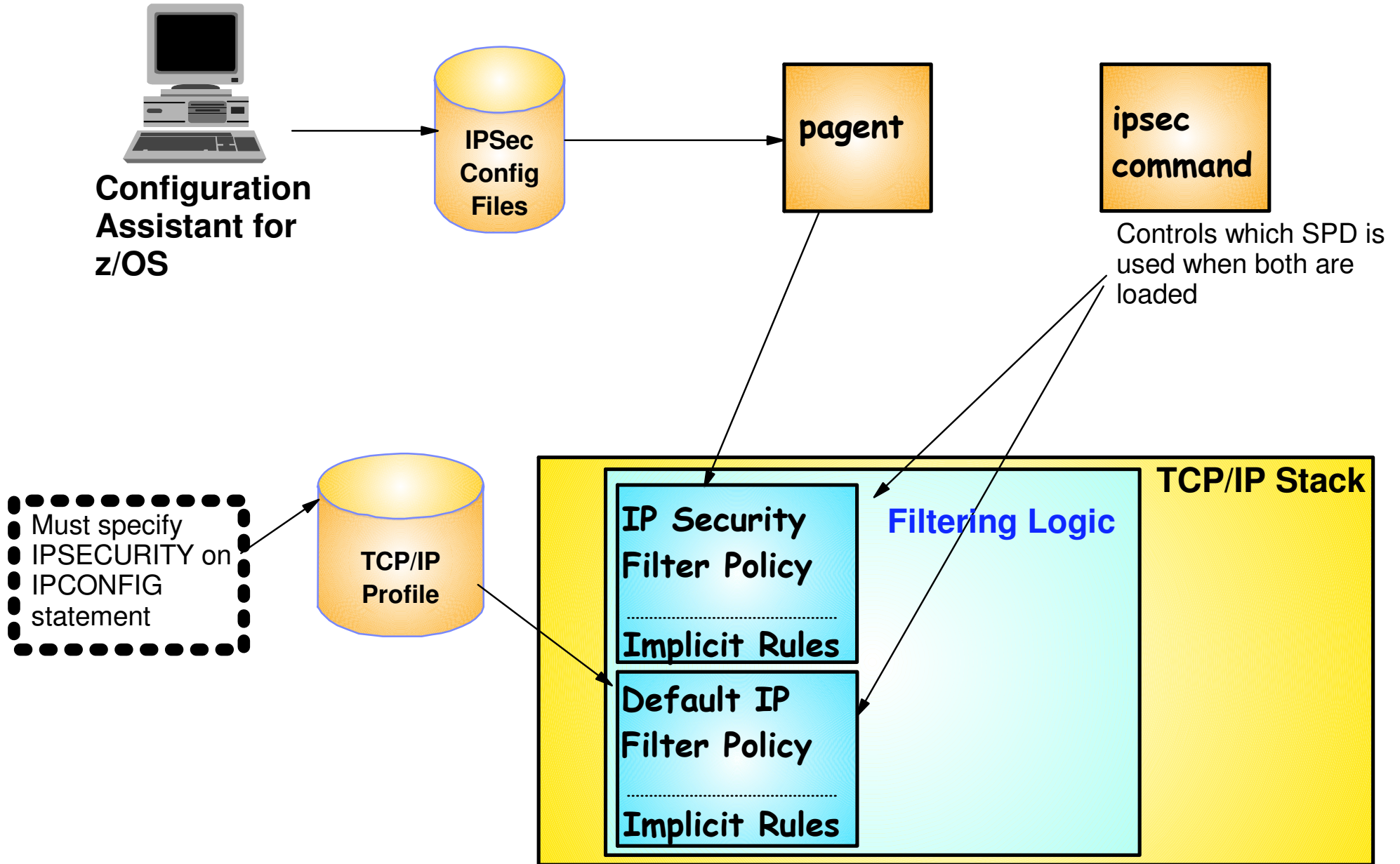   - Intended to be the primary source of filter rules
     - Defined in a Policy Agent IPSec configuration file
       - Policy can be generated by the Configuration Assistant for z/OS GUI

- Implicit filter rules
  - Always present, not user-defined
    - Deny all inbound traffic
    - Deny all outbound traffic
  - Appended to Default IP filter policy by the TCP/IP stack
  - Appended to IP Security filter policy by Pagent
  - If neither policies are defined, the implicit rules become the default policy (deny all)

Default IP filter policy

TCP/IP Profile

ipsec command switches between the two policies

IP security filter policy

Policy Agent

Filter rule search order

Filter rule 1

Filter rule 2

Filter rule 3

. . . .

Implicit filter rule: Deny everything!!!

IP filter policy on z/OS - overview

Configuration Assistant for z/OS

IPSec Config Files

pagent

ipsec command

Controls which SPD is used when both are loaded

Must specify IPSECURITY on IPCONFIG statement

TCP/IP Profile

TCP/IP Stack

IP Security Filter Policy

Filtering Logic

Implicit Rules

Default IP Filter Policy

Implicit Rules

Filtering conditions

Criteria	Description
From packet	
Source address	Source IP address in IP header of packet
Destination address	Destination IP address in IP header of packet
Protocol	Protocol in the IP header of packet (TCP, UDP, OSPF, etc.)
Source port	For TCP and UDP, the source port in the transport header of packet
Destination port	For TCP and UDP, the destination port in the transport header of packet
ICMP type and code	For ICMP, type and code in the ICMP header of packet
OSPF type	For OSPF, type located in the OSPF header of packet
IPv6 Mobility type (V1R10)	For traffic with IPv6 mobility headers, MIPv6 type in header of packet.
Fragments Only (V1R10)	Matches fragmented packets only (applicable to routed traffic only)
Network attributes	
Direction	Direction of packet.
Routing	Packet is local if source or destination IP address exists on local host, otherwise it is routed
Link security class	A virtual class that allow you to group interfaces with similar security requirements. Non-VIPA addresses can be assigned a security class. Packets inherit the security class of the interface over which packet is sent/received.
Time condition	
Time, Day, Week, Month	Indicates when filter rule is active

New routed port restrictions added for RFC4301 compliance (Added in V1R10)

- **Prior to RFC 4301 support, IPsec filters all routed IP fragments using a policy of first possible filter match**
  - ➤ Fragmentation comes into play here for routed traffic only
    - – Local traffic is reassembled before packet filtering
  - ➤ Fragmented packets do not carry the transport headers meaning that only the first of a set of fragmented packets can be properly classified on basis of port
    - – Subsequent fragments would match on rules without port specification

| First fragment	IP Hdr first part	TCP Hdr (port)	Data first part	Can apply filter rule to this packet	Routing filter rule using port number as selection
Second fragment	IP Hdr second part	Data second part		But not to this	
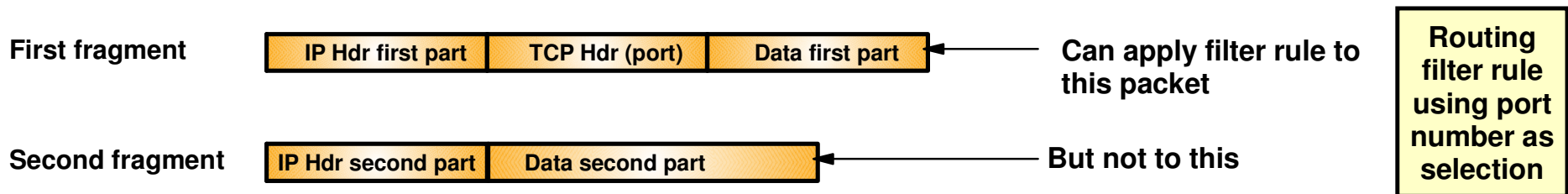
- **RFC 4301 introduces rules and restrictions to ensure proper classification of fragments**
  - ➤ RFC 4301 states that ports, types, and codes can no longer be specified as a filter condition for routed traffic
    - – Affects "Routed" or "Either" direction condition on filter rule

Where routed port restrictions apply

Local Traffic
(No changes to become RFC4301 compliant)

Routed Traffic
(Possibly changes to become RFC4301 compliant)

Filters for local traffic can be based on ports, types, or codes. Fragments are reassembled before filter rules are checked.
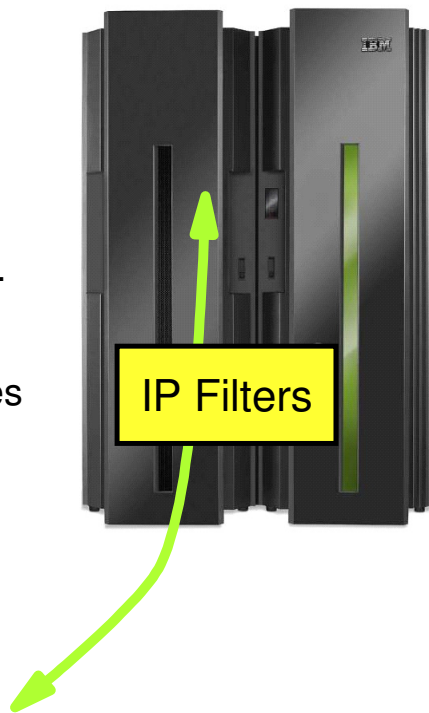
IP Filters

If all your filter rules are defined as *local*, no changes are required to become RFC4301 compliant.

IP Filters

Filters that are defined as **routed** or **either** cannot be based on ports, types, or codes. Each fragment is checked against filter rules as fragments are routed through this node.
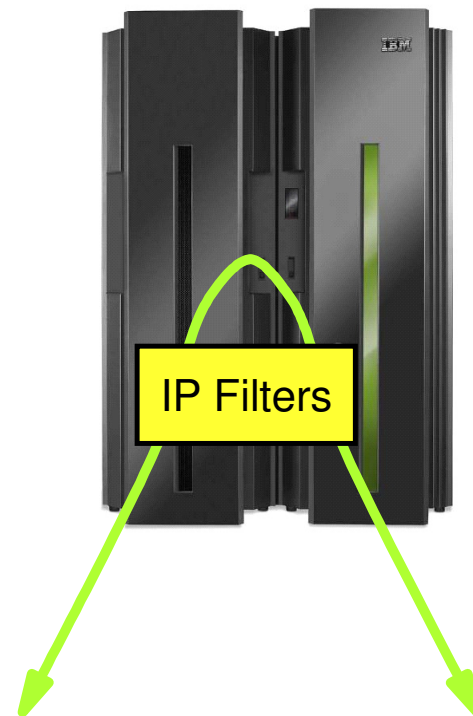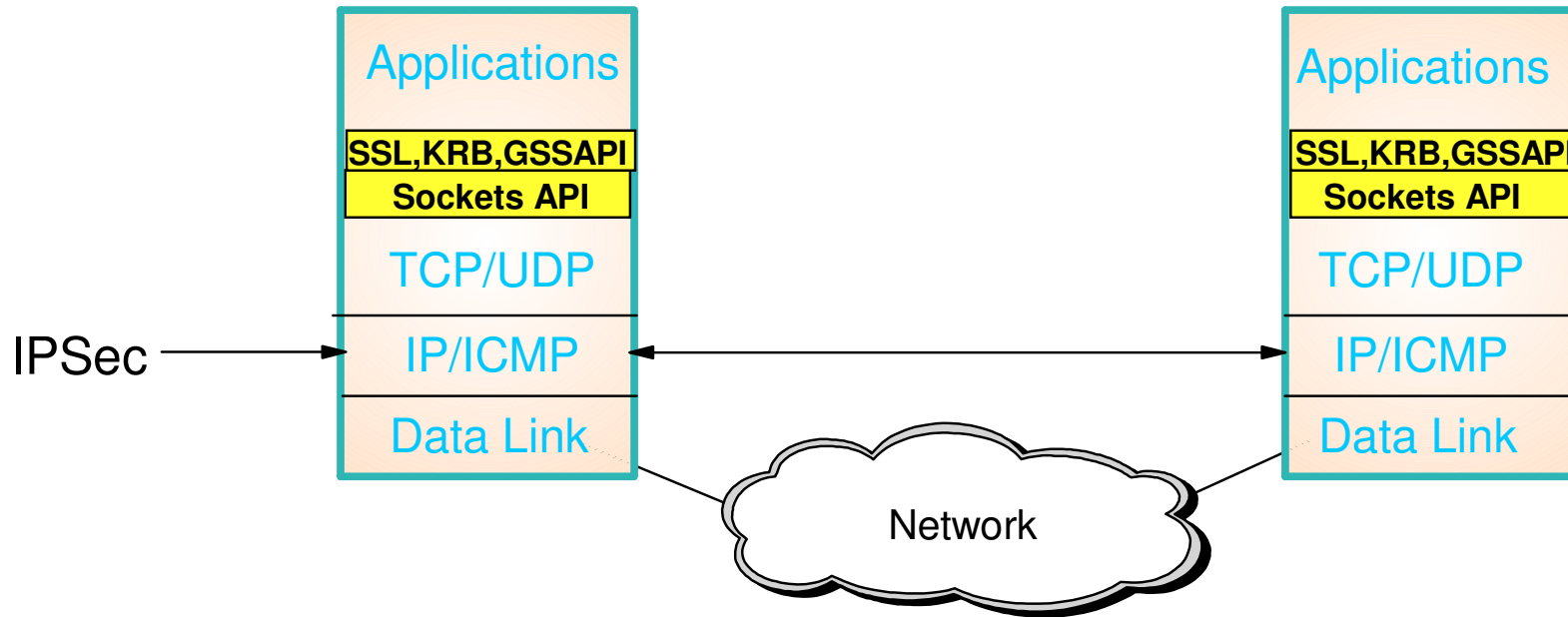
How to be compliant with RFC4301 routed port restrictions

- **z/OS V1R10 Communications Server allows you to choose which filtering logic to use**
  - ➤ RFC4301Compliance parameter on the IpFilterPolicy statement
    - No (default): continue to accept and apply all filter rules as before V1R10
      - port, type, or code specifications are allowed on routed traffic rules
      - filter all IP fragments by first possible filter match - except: non-initial IP fragments only match rules covering All ports, types, or codes
    - Yes: Use and enforce the RFC 4301 restrictions on IP filter rules no port, type, or code specifications on routed traffic rules

- **Configuration Assistant can help you migrate an existing non-compliant config to RFC 4301 compliance**

- **z/OS V1R11 is the last z/OS release where RFC4301 compliance is optional**

- **In z/OS V1R12, RFC4301 compliance is mandatory.**

z/OS Communications Server IP security

IPSec

IPSec protocol overview

Applications
SSL,KRB,GSSAPI
Sockets API
TCP/UDP
IP/ICMP
Data Link

Applications
SSL,KRB,GSSAPI
Sockets API
TCP/UDP
IP/ICMP
Data Link

IPSec

Network

- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - IPSec security protocols
    - **Authentication Header (AH)** - provides data authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional authentication/integrity
- Implemented at IP layer
  - Requires no application change
  - Secures traffic between any two IP resources
    - Security Associations (SA)
- Management of crypto keys and security associations can be
  - manual
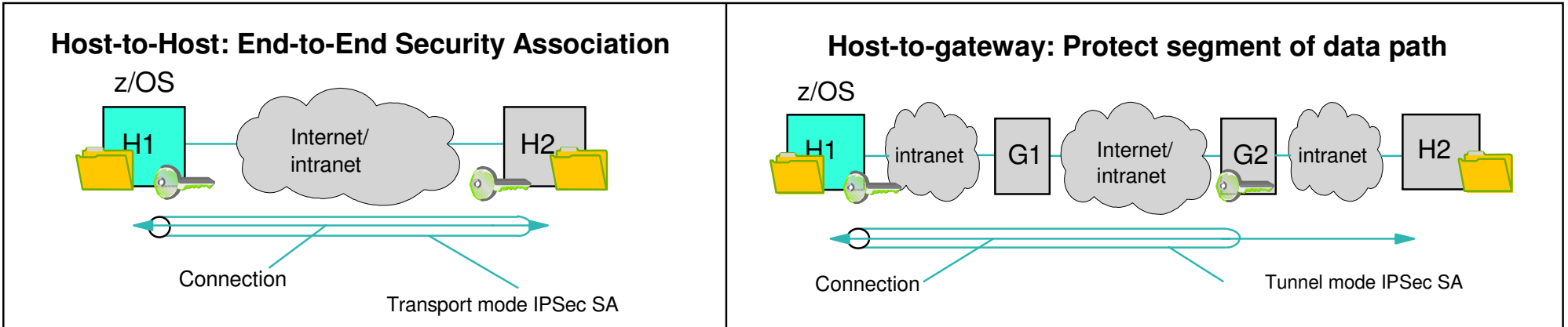 - automated via key management protocol (Internet Key Exchange (IKE))
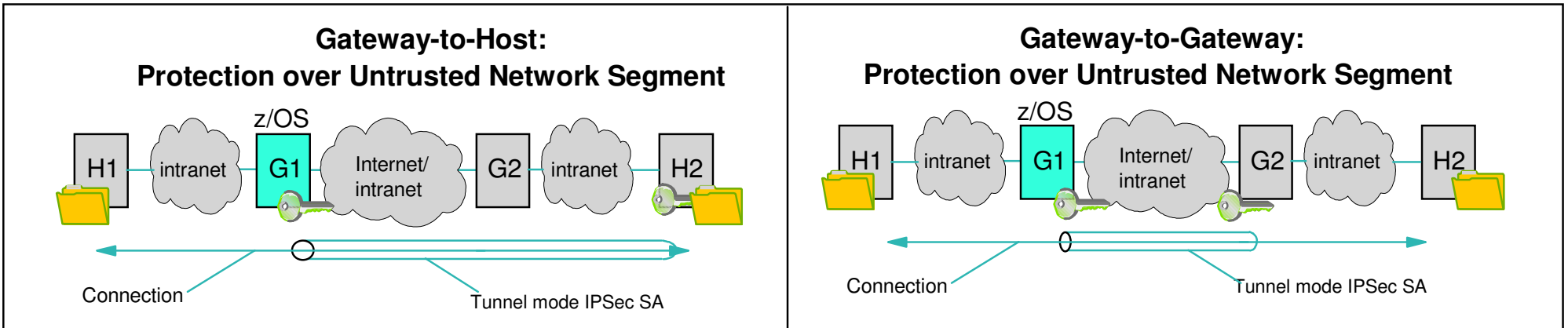
IPSec security associations
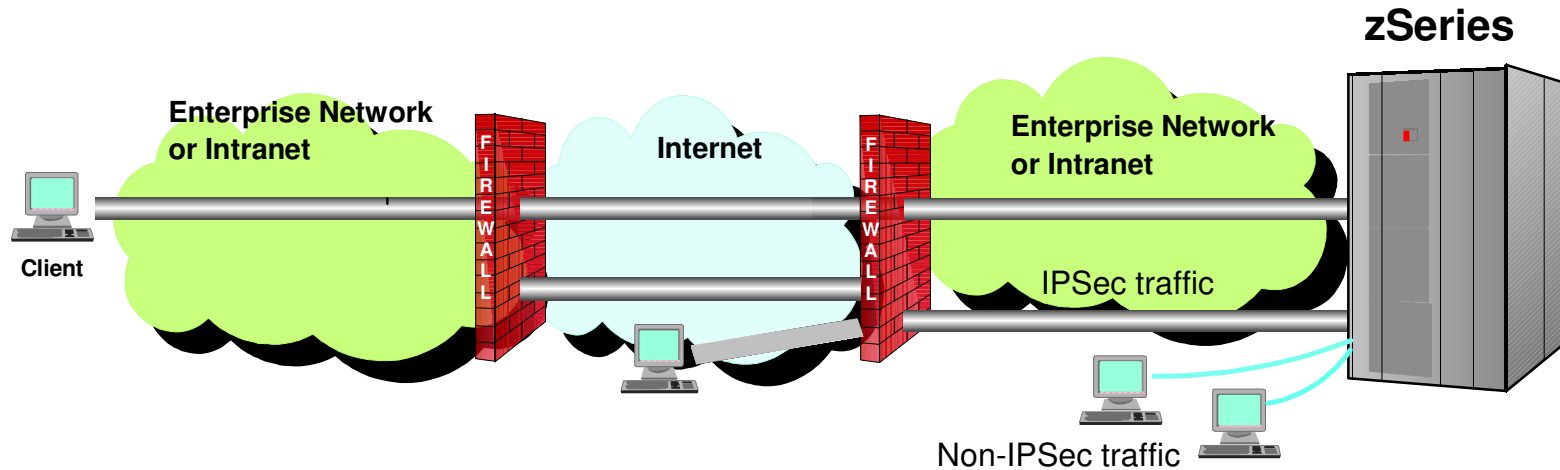
- IPSec Security Association (SA) defines security services for a defined traffic type
  - Unidirectional logical connection between 2 IPSec hosts
  - Used in pairs for bidirectional traffic
- SA scope of protection can vary
  - Wide - Traffic protection for multiple connections e.g. Protect all traffic between 2 hosts
  - Narrow - Traffic protection for a single connection
- SA endpoints can vary
  - Entire data path can be secured with IPSec
    - Security and connection endpoints are the same - Transport mode
  - Portion of data path considered "untrusted" can be secured with IPSec
    - Security and connection endpoints are different - Tunnel mode

IPSec scenarios and z/OS roles

z/OS as Host (Data Endpoint)

Host-to-Host: End-to-End Security Association

z/OS

H1 — Internet/intranet — H2

Connection

Transport mode IPSec SA

Host-to-gateway: Protect segment of data path

z/OS

H1 — intranet — G1 — Internet/intranet — G2 — intranet — H2

Connection

Tunnel mode IPSec SA

z/OS as Gateway (Routed Traffic)

**Gateway-to-Host:
Protection over Untrusted Network Segment**

z/OS

H1 — intranet — G1 — Internet/intranet — G2 — intranet — H2

Connection

Tunnel mode IPSec SA

**Gateway-to-Gateway:
Protection over Untrusted Network Segment**

z/OS

H1 — intranet — G1 — Internet/intranet — G2 — intranet — H2
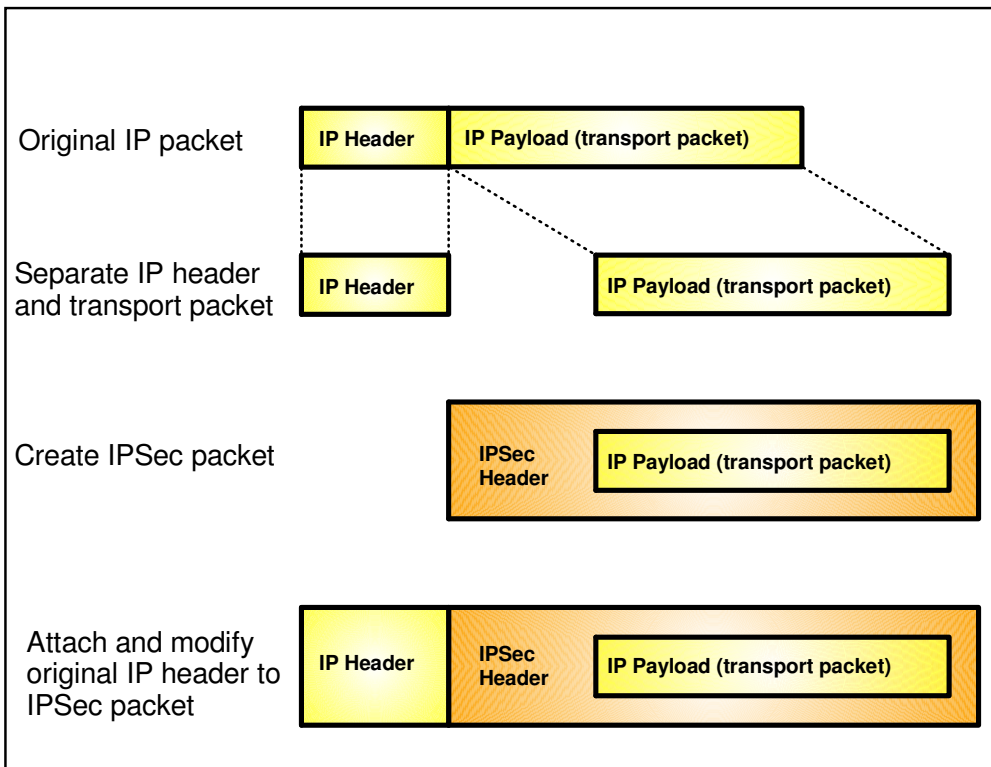
Connection

Tunnel mode IPSec SA

Legend

Data endpoint

Security endpoint

IPSec encapsulating modes - transport and tunnel mode
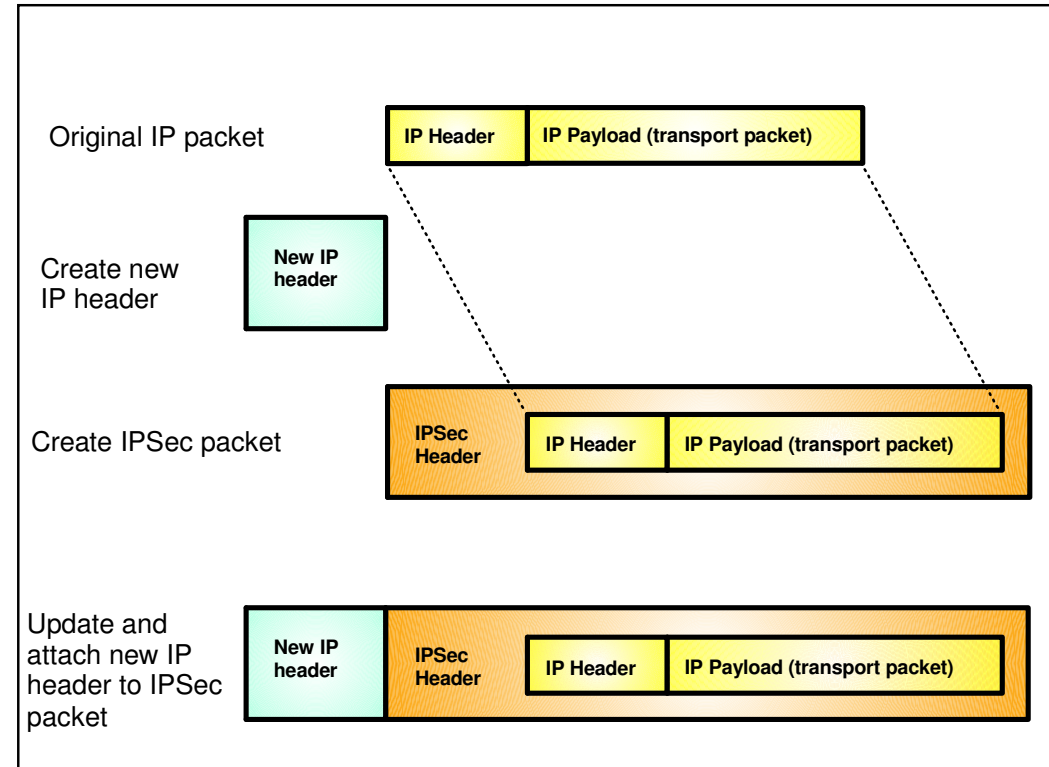
Creating an IPSec transport mode packet
- Inserts IPSec headers between original IP header and protected data

Creating an IPSec tunnel mode packet
- Creates a new IP header with an IPSec header
- IPSec header followed by original IP header and protected data

Original IP packet — IP Header | IP Payload (transport packet)

Separate IP header and transport packet — IP Header | IP Payload (transport packet)

Create IPSec packet — IPSec Header | IP Payload (transport packet)

Attach and modify original IP header to IPSec packet — IP Header | IPSec Header | IP Payload (transport packet)

Original IP packet — IP Header | IP Payload (transport packet)

Create new IP header — New IP header

Create IPSec packet — IPSec Header | IP Header | IP Payload (transport packet)

Update and attach new IP header to IPSec packet — New IP header | IPSec Header | IP Header | IP Payload (transport packet)

Transport mode is typically used between two hosts that establish an IPSec SA end-to-end between them.

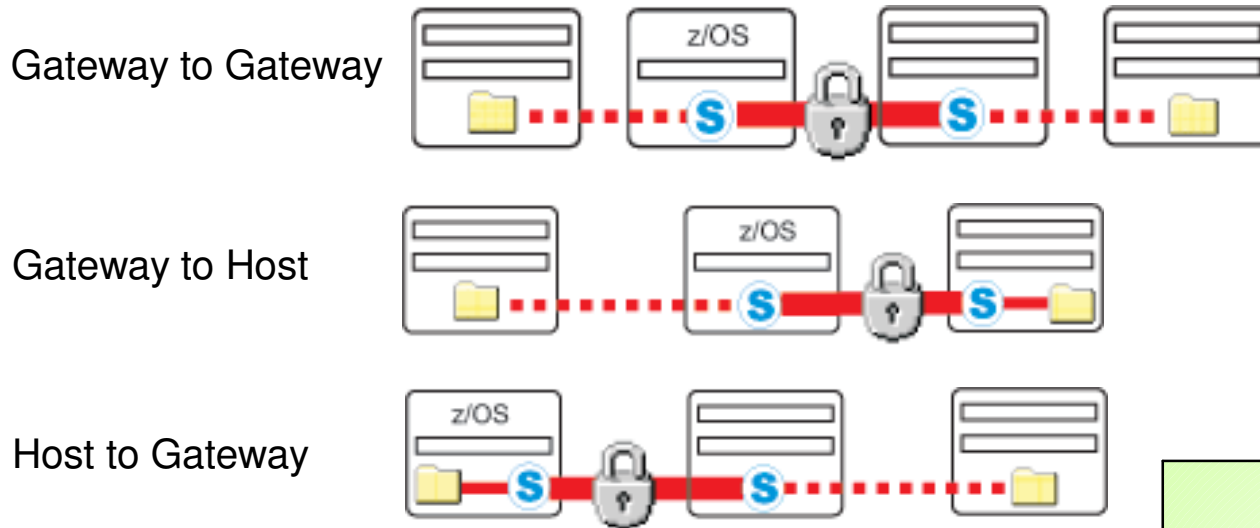Tunnel mode is used if at least one of the two IPSec SA end-points is a gateway.

Encapsulation mode rules

- **Must use tunnel mode:**

  Gateway to Gateway

  Gateway to Host

  Host to Gateway

- **May use tunnel or transport mode:**
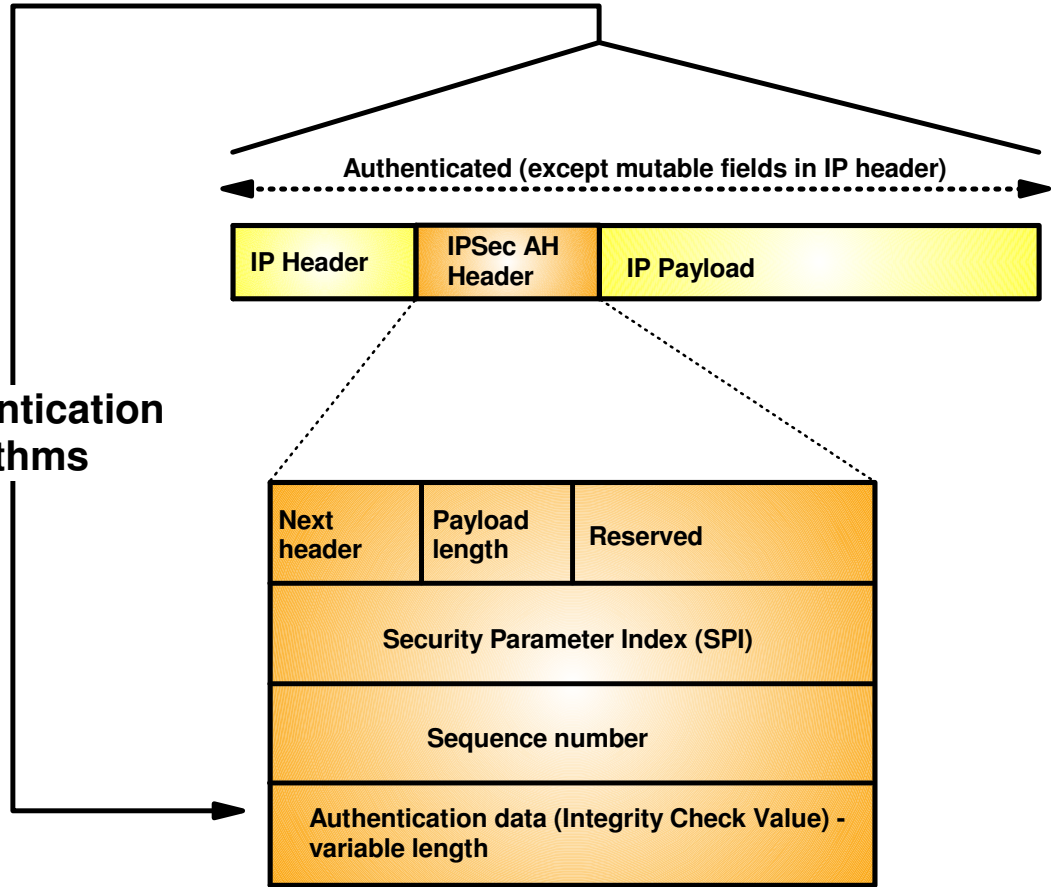
  Host to Host

Legend

Security Endpoint (S)

Data Endpoint 📁

Protected Data 🔒

Unprotected Data ▪ ▪ ▪

Data Endpoint same as Security Endpoint 📁—(S)

IPSec Authentication Header (AH) protocol

AH provides authentication / integrity
– Authenticates <u>entire</u> datagram including IP header (excluding changeable or "mutable" fields)
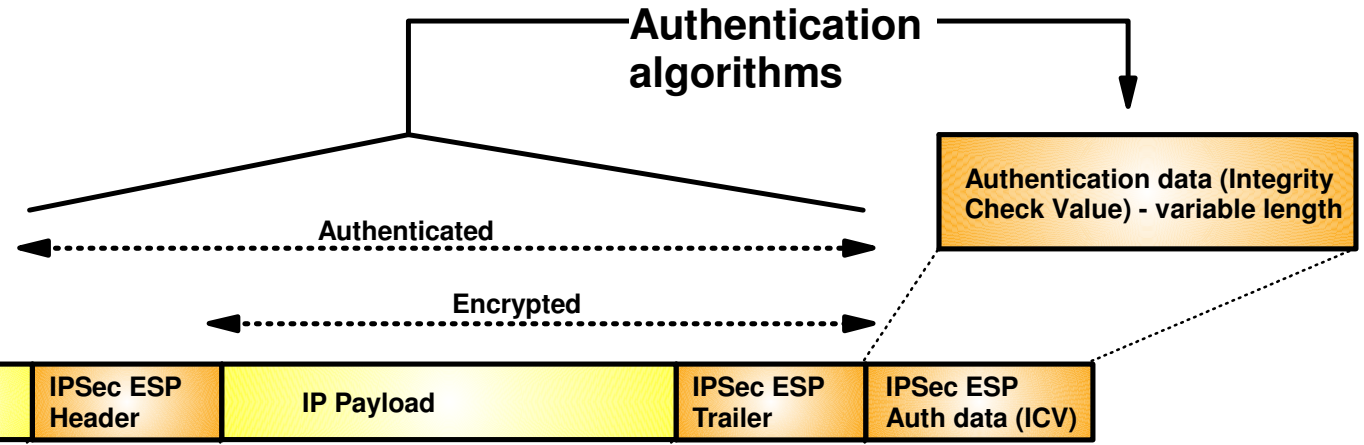
Authentication algorithms

Authenticated (except mutable fields in IP header)

IP Header	IPSec AH Header	IP Payload

Next header	Payload length	Reserved
Security Parameter Index (SPI)		
Sequence number		
Authentication data (Integrity Check Value) - variable length		

- If transport mode then "Payload" contains the original transport header and original data
- If tunnel mode then "Payload" contains the original IP header, original transport header, and original data
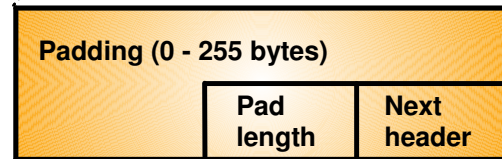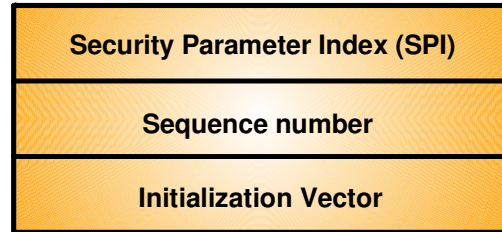
IPSec Encapsulating Security Payload (ESP) protocol

ESP provides privacy with optional authentication / integrity
- Authentication coverage does not cover IP header

Authentication algorithms

Authentication data (Integrity Check Value) - variable length

Authenticated

Encrypted

IP Header	IPSec ESP Header	IP Payload	IPSec ESP Trailer	IPSec ESP Auth data (ICV)

- **Encryption algorithms**
  - ► Protects IP payload and IPSec ESP trailer
  - ► Null encryption option allows authentication only as AH protocol alternative

Security Parameter Index (SPI)

Sequence number

Initialization Vector

Padding (0 - 255 bytes)

	Pad length	Next header

- **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

IPSec security associations (SAs)

- **Endpoints must agree on how to protect traffic**

  - ➤ Security protocol
    - AH
    - ESP

  - ➤ Algorithms to be used by the security protocols
    - Encryption Algorithm
    - Authentication Algorithm

  - ➤ Cryptographic keys

  - ➤ Encapsulation mode
    - tunnel
    - transport

  - ➤ Lifetime/lifesize (for dynamic SAs)

- **This agreement is known as a "security association"**

- **IPSec security associations can be manually configured in the IPSec policy or created dynamically using the IKE protocol**

Manually defined SAs

- **Not commonly used**
  - ➤ Do not provide a scalable solution
  - ➤ In the long run difficult to manage

- **Defined in a Policy Agent IPSec configuration file**
  - ➤ Utilized by filter rules with an action of ipsec
  - ➤ SA is defined by a manual VPN action
    - – Can be generated by the Configuration Assistant for z/OS GUI

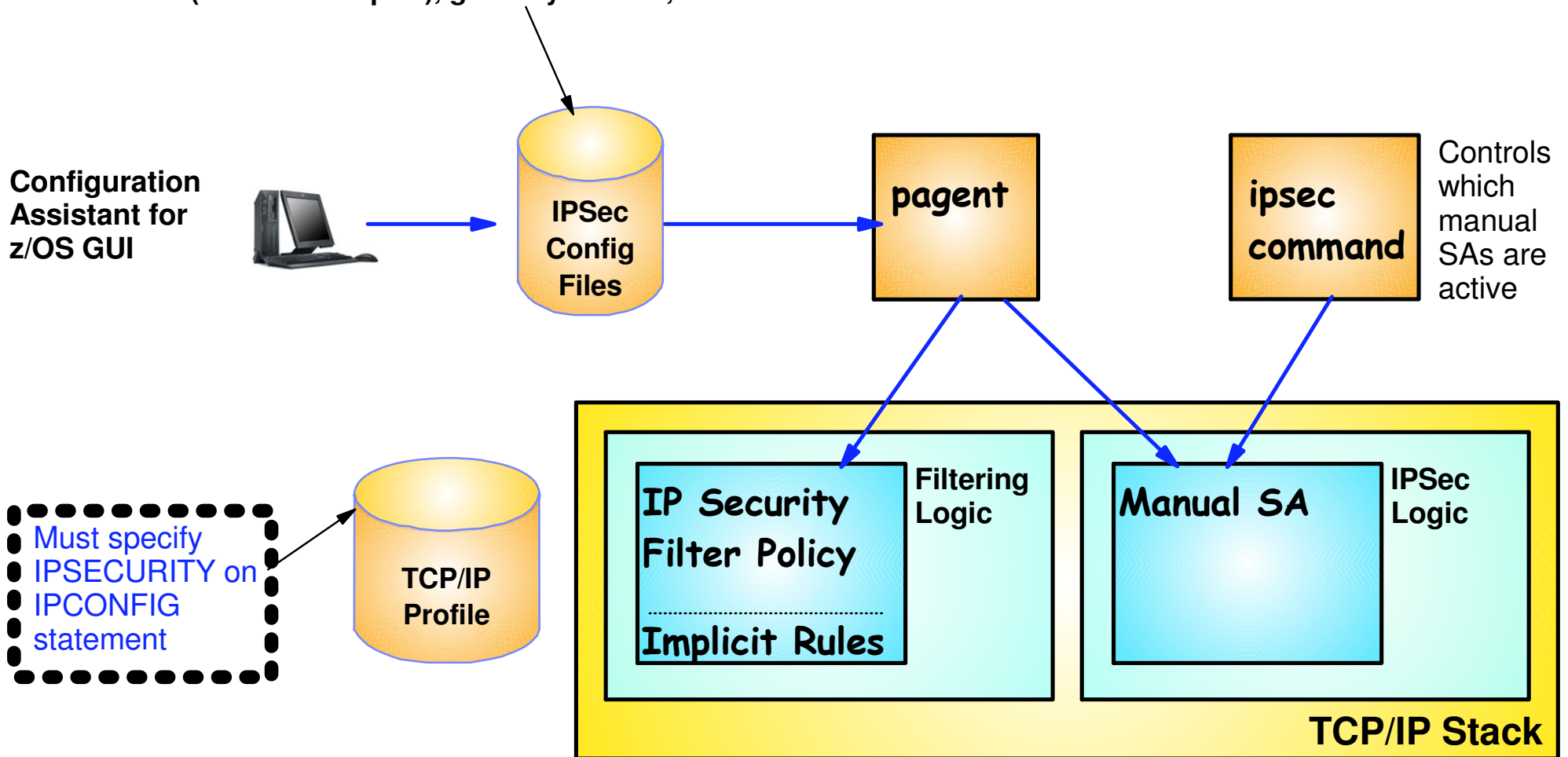- **Use ipsec command activate/deactivate manual SAs**
  - ➤ Can also be automatically activated when policy is installed

- **Definition of SA attributes require mutual agreement between tunnel endpoint administrators**
  - ➤ Cryptographic keys and IPSec security protocol parameters must be mutually agreed to between tunnel endpoint administrators
  - ➤ Need to decide how to safely exchange keys
  - ➤ Need to decide how to refresh keys
    - – Manual SAs must be deactivated and activated when refreshing keys
    - – Refreshing keys must be coordinated with the remote tunnel endpoint's administrator
  - ➤ Remote endpoint may need to reactivate a manual SA if you locally deactivate the SA and then locally activate the SA.

IPSec manual SAs overview

- **Define IP filter conditions here (which packets using manual tunnels for encryption)**

- **Define all encryption info between 2 data endpoints here (Ciphersuite, spi, keys, method (AH/ESP), Mode (Tunnel/Transport), gateways to use, etc.**

Configuration Assistant for z/OS GUI

IPSec Config Files

pagent

ipsec command

Controls which manual SAs are active

Must specify IPSECURITY on IPCONFIG statement

TCP/IP Profile

IP Security Filter Policy

Filtering Logic

Implicit Rules

Manual SA

IPSec Logic

TCP/IP Stack

Dynamically defined SAs

- **Currently state of the art**
  - ➤ Scalable
  - ➤ Automatic, non-disruptive refresh of SAs and session keys
- **Initially requires more configuration than a manual SA**
  - ➤ In the long run easier to manage
    - – Set and forget it
- **Dynamic SAs are negotiated by the IKE daemon**

- **Dynamic IPSec policy defined in a Pagent IPSec configuration file**
  - ➤ Can be generated by the Configuration Assistant for z/OS Communications Server GUI
  - ➤ Dynamic VPN action identifies "acceptable" SA attributes
    - – Utilized by filter rules with an action of IPSEC
- **Authentication methods**
  - ➤ Pre-shared key
    - – Each host needs to be keyed with key of <u>each</u> potential IKE partner
      - ● This key is not directly used to encrypt data.
    - – Often used during the initial stages of dynamic SA deployment
  - ➤ Digital signature (most scalable)
    - – Uses x.509 certificates for host-based authentication
      - ● Each host needs only its own host-based certificate and the certificate of the trusted Certificate Authority that signed the IKE peer's host-based certificate
        - *(Requirements for the CA of the peer certificate can differ with V1R12 Certficate Trust Chain support)*
    - – Algorithms
      - ● RSA Signature
      - ● Elliptical Curve Digital Signature **(V1R12)**

The IKE daemon

- **The IKE daemon implements the Internet Key Exchange protocol**
  - ➤ A two phase approach to negotiating dynamic IPSec SAs
  - ➤ Two versions:
    - – IKEv1 - Defined in RFC 2409
    - – IKEv2 - Defined in RFC 4306 (z/OS V1R12)

- **The IKE daemon obtains its policy from Pagent**
  - ➤ Policy information for negotiating IPSec SAs
    - – Dynamic VPN actions
  - ➤ Policy for creating a secure channel used to negotiate IPSec SAs
    - – Key Exchange Policy
  - ➤ Policy for ipsec command activation and autoactivation
    - – Local Dynamic VPN Policy

- **Utilizes UDP ports 500 and 4500 to communicate with remote security endpoints**
  - ➤ Negotiating SAs
 - ➤ Sending informational messages

Two phases of IKE negotiations

- Phase 1
  - ➤ 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
  - ➤ Done infrequently

- Phase 2
  - ➤ Negotiates an IPSec SA 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
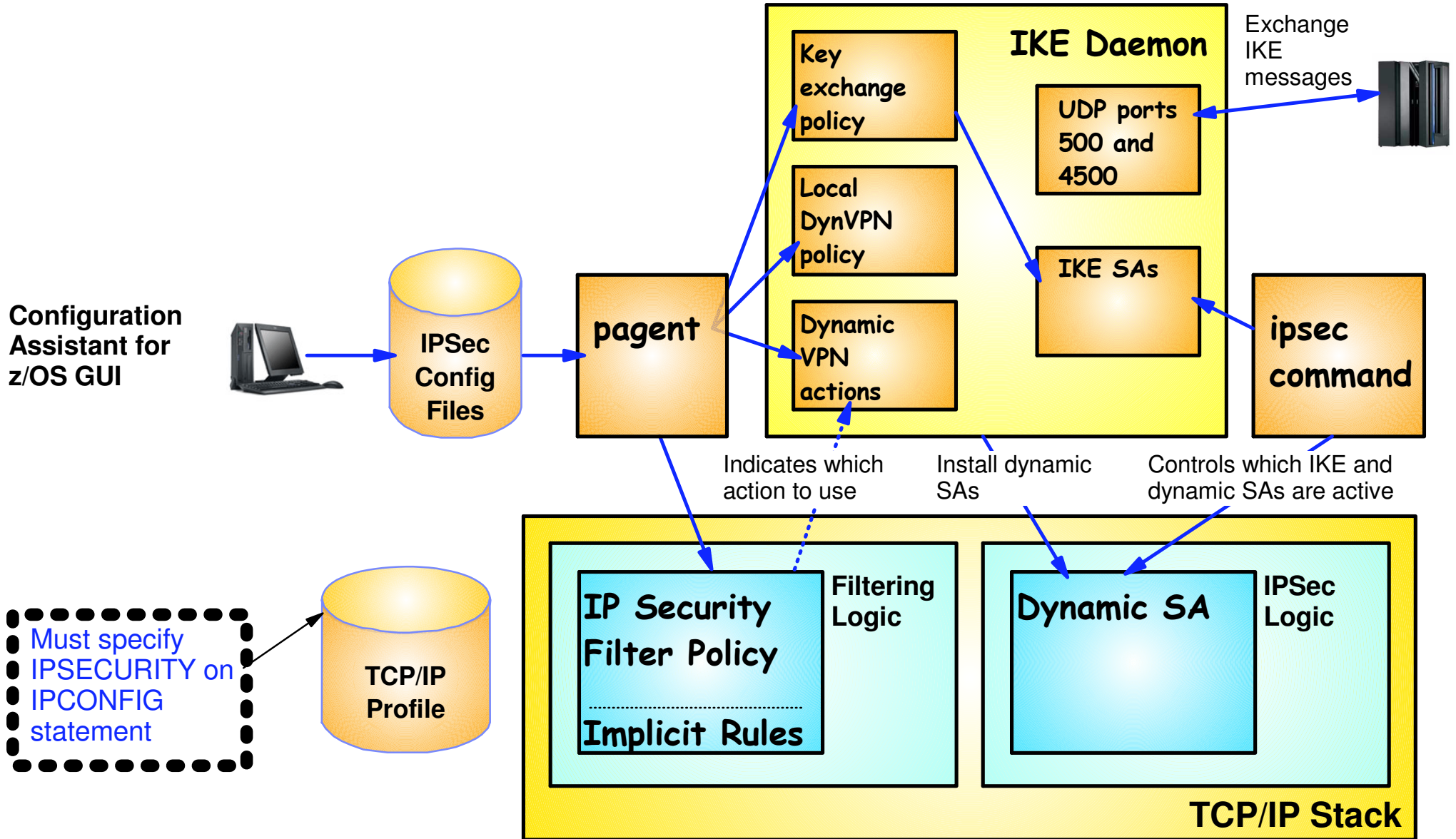 - ➤ Done more frequently than phase 1
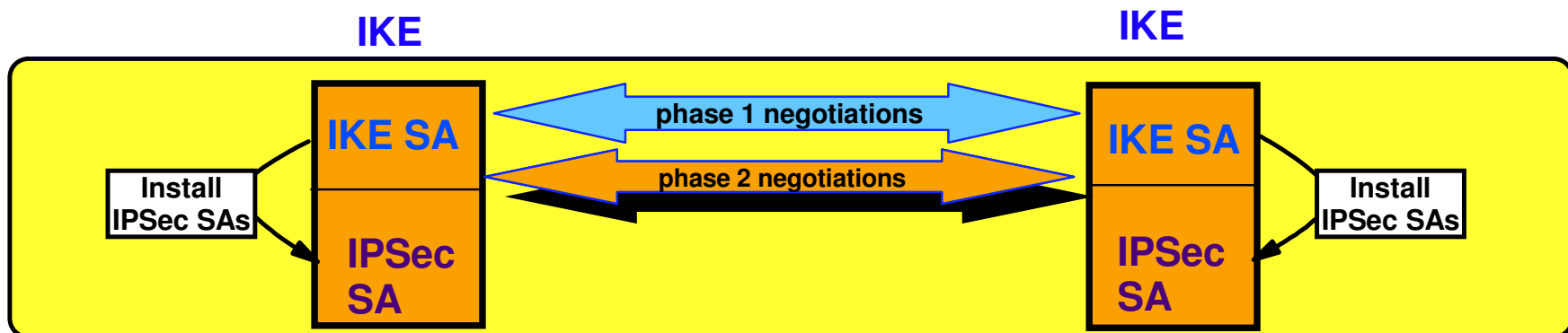
Dynamic SA activation methods

Security associations can be activated in one of four ways:

- On-demand activation
  - ➤ Activation attempted when the stack receives an outbound packet requiring the protection of a new dynamic tunnel
- Remote activation
  - ➤ A remote security endpoint initiates the negotiation of a new SA
- Command activation
  - ➤ ipsec -y activate command
    - – Requires definition of local dynamic VPN policy:
- Autoactivated
  - ➤ Activation attempted when a stack connects to IKED or when IP Security filter policy is reloaded
    - – Requires definition of local dynamic VPN policy:

IP Security dynamic SAs overview

Configuration Assistant for z/OS GUI

IPSec Config Files

pagent

IKE Daemon

Key exchange policy

Local DynVPN policy

Dynamic VPN actions

UDP ports 500 and 4500

IKE SAs

Exchange IKE messages

ipsec command

Indicates which action to use

Install dynamic SAs

Controls which IKE and dynamic SAs are active

Must specify IPSECURITY on IPCONFIG statement

TCP/IP Profile

IP Security Filter Policy

Filtering Logic

Implicit Rules

Dynamic SA

IPSec Logic

TCP/IP Stack

z/OS Communications Server IP security

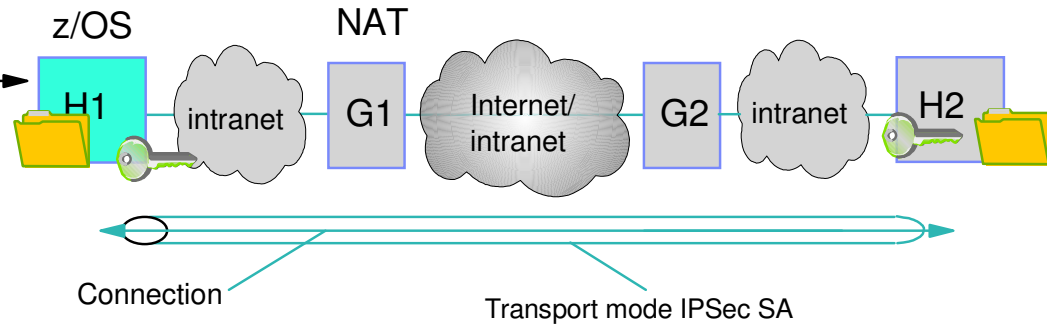## Special Topics

The IPSec NAT traversal problem

- Network Address Translation (NAT) alters addressing information in packet
  - ➤ IP addresses in IP headers
  - ➤ Addresses in data payload for some protocols
- Some NATs do port translation (NAPT)
  - ➤ IP addresses in IP headers
  - ➤ Ports in TCP and UDP headers
  - ➤ Addresses and ports in data payload for some protocols
- IPSec and NAT / NAPT at original RFC levels were not compatible
  - ➤ IPSec SA could not traverse NAT/NAPT device
  - ➤ Forced configuration where multiple SAs required to make end-to-end connection
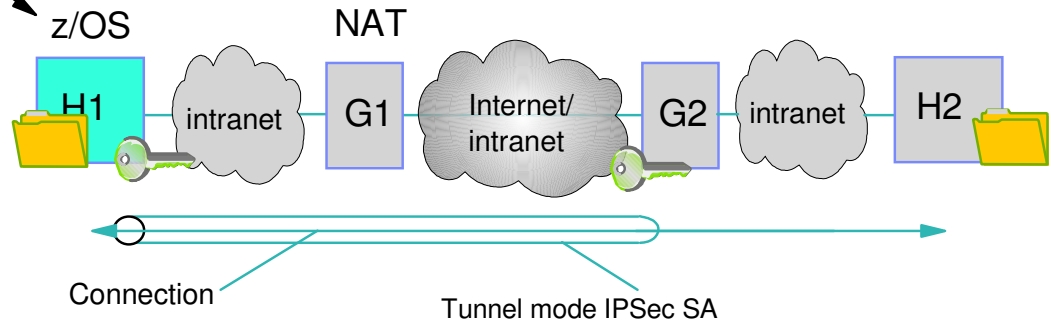   - – Cascaded SAs
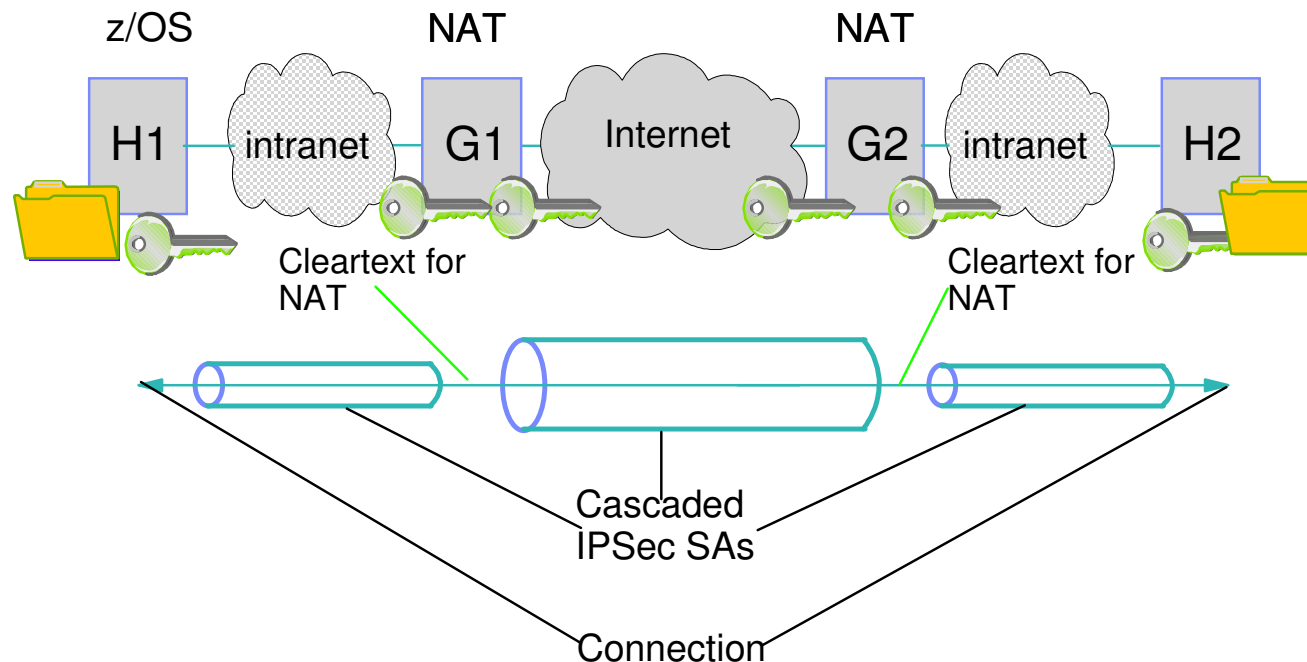
The IPSec NAT Traversal Solution

- Later IETF RFCs address this incompatibility for NAT / NAPT alterations in IP and transport headers
  - RFC 3947 and 3948
  - Does not address translation of addresses in data payload
    - Application protocol specific solution required (e.g. FTP EPSV support which eliminates use of addresses in data payload)
  - ESP only
    - AH not allowed
- z/OS NAT traversal support
  - z/OS Host-to-host
    - transport or tunnel mode
  - z/OS Host-to-gateway
    - tunnel mode
  - No z/OS gateway support
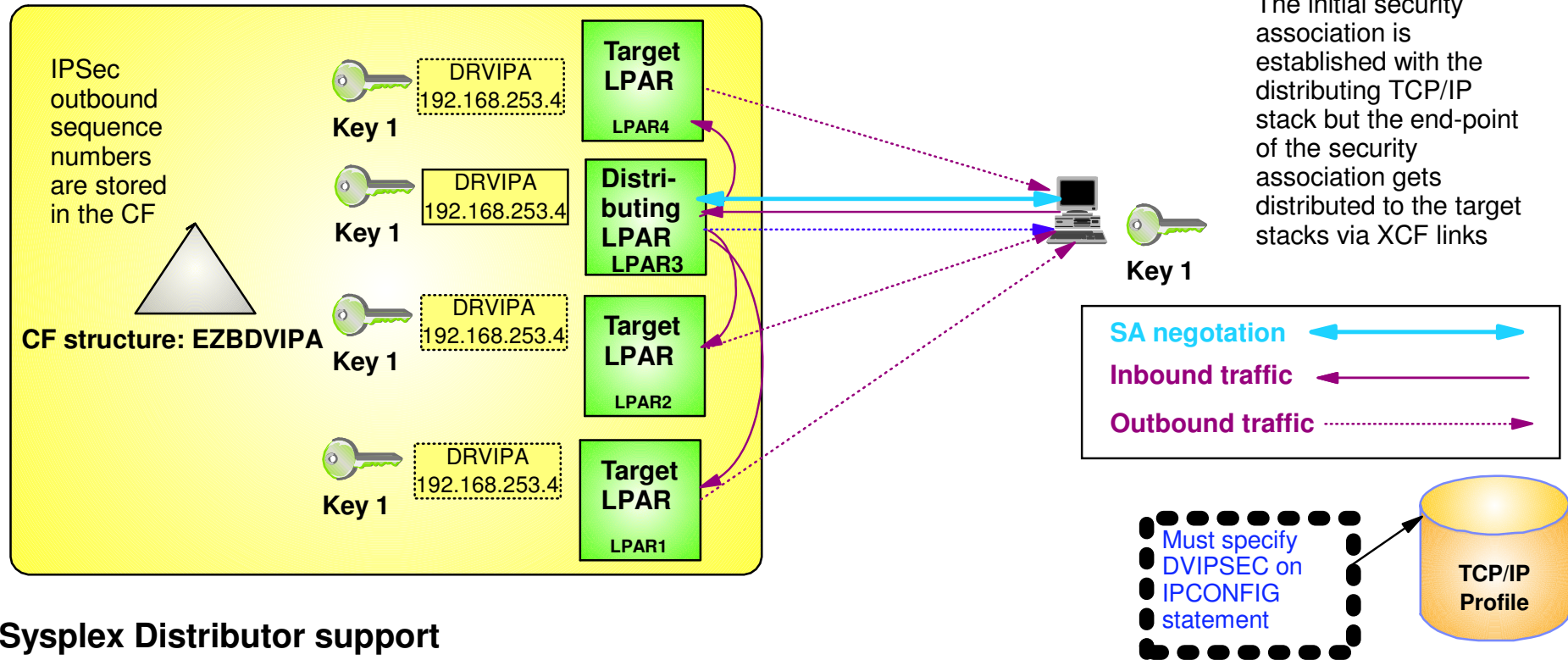 - NAT / NAPT

Host-to-Host: End-to-End Security Association

z/OS   NAT

H1   intranet   G1   Internet/intranet   G2   intranet   H2

Connection   Transport mode IPSec SA

Host-to-gateway: Protect segment of data path

z/OS   NAT

H1   intranet   G1   Internet/intranet   G2   intranet   H2

Connection   Tunnel mode IPSec SA

VIPA takeover and sysplex distributor support for IPSec traffic - Sysplex Wide Security Associations

Sysplex Wide Security Assocations (SWSA) provides sysplex support to IPSec protected traffic with a DVIPA security endpoint

The initial security association is established with the distributing TCP/IP stack but the end-point of the security association gets distributed to the target stacks via XCF links

- **SWSA Sysplex Distributor support**
  - ➤ Distributes IPSec-protected workload with connection distribution
    - – Consistent filter policies needed across processors in Sysplex
- **SWSA VIPA Takeover support**
  - ➤ IPSec phase 1 & 2 SAs automatically restarted on backup after takeover
    - – Phase 1 & 2 info needed for restart saved in Coupling Facility
  - ➤ No administrative movement of SAs required.
    - – Policy filters at backup host must be able to accommodate filter rules and SAs for backup processor

IKEv2 (added in V1R12)

- IKE version 1 (IKEv1) specified by RFCs 2407-2409
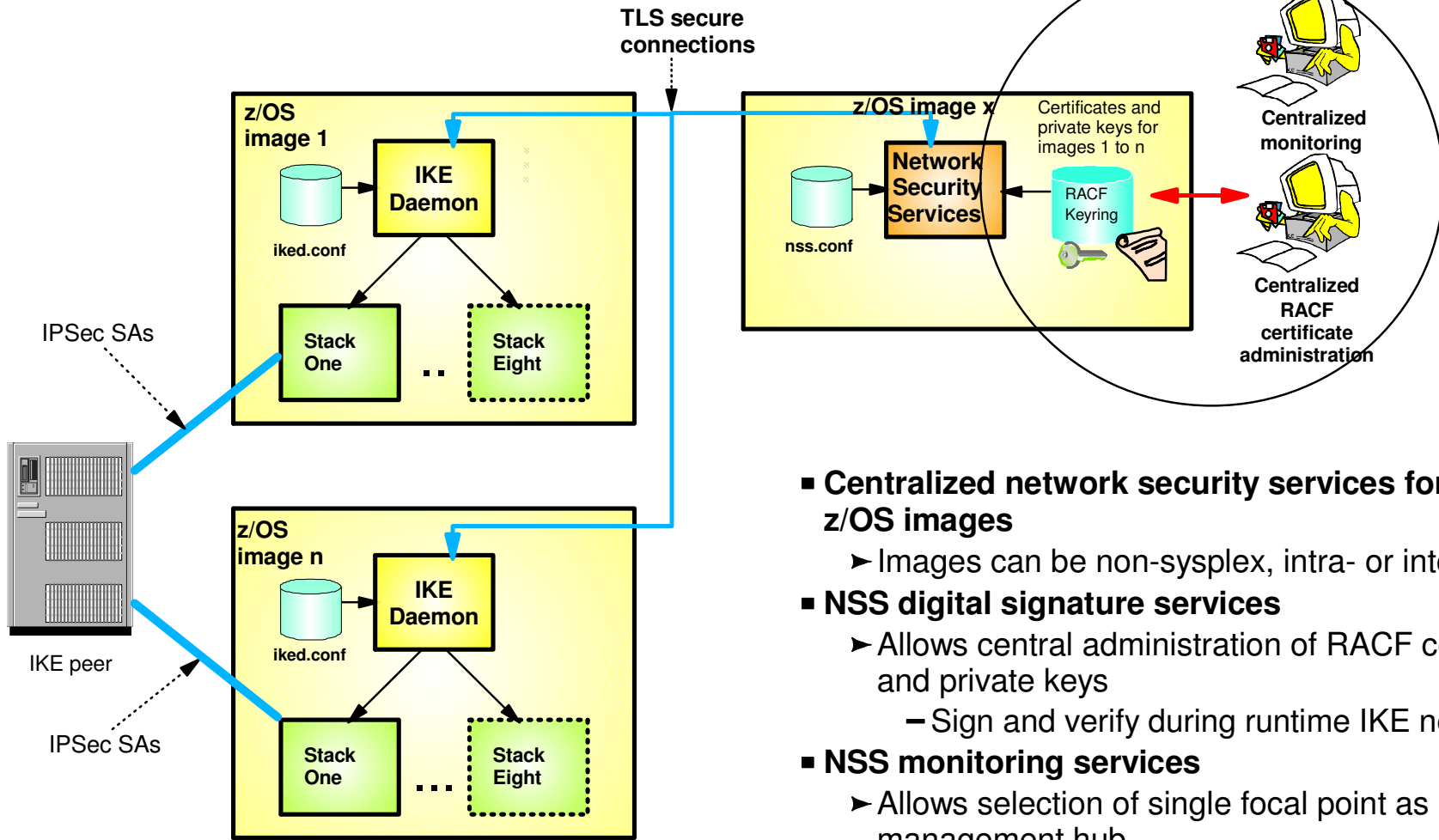- **IKE version 2 (IKEv2) specified by RFC 4306**
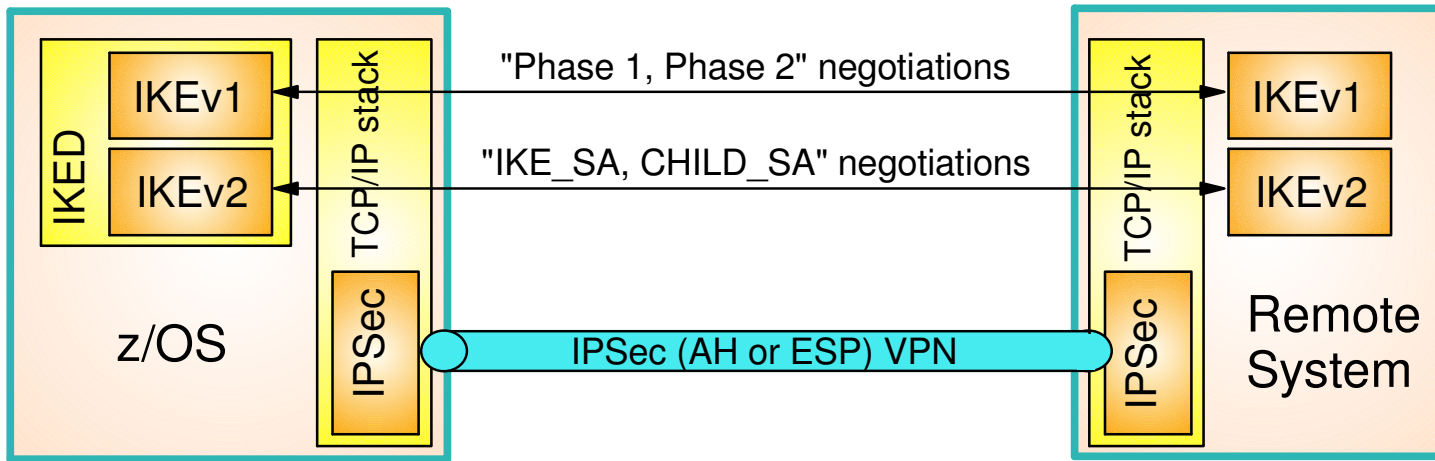
- **IKEv2 protocol**
  - ➤ Supports all of the same configurations as IKEv1
  - ➤ Different protocol than IKEv1
    - – similar function
    - – different messages and flows
    - – different terminology
  - ➤ More efficient than IKEv1:
    - – fewer messages per negotiation
    - – new formats allow for smaller messages
  - ➤ More robust than IKEv1:
    - – Request/response model for all flows
    - – Built-in dead peer detection

- **z/OS IKEv2 implementation**
  - ➤ Coexists and concurrently supported with IKEv1 in IKED
  - ➤ Fully supported by Configuration Assistant for z/OS
  - ➤ Requires network security services (NSS) for certificate-based authentication
  - ➤ Does not support:
    - – NAT traversal for IPv4
    - – System-Wide Security Associations (SWSA)

Network Security Services for IPSec

TLS secure connections

z/OS image 1

IKE Daemon

iked.conf

Stack One .. Stack Eight

z/OS image x

Network Security Services

nss.conf

Certificates and private keys for images 1 to n

RACF Keyring

Centralized monitoring

Centralized RACF certificate administration

IPSec SAs

IKE peer

IPSec SAs

z/OS image n

IKE Daemon

iked.conf

Stack One ... Stack Eight

NSS role extended in z/OS V1R12
- NSS is required for z/OS V1R12 advanced certificate support
  - ➤ Certificate Revocation List
  - ➤ Certificate Trust Chain
- NSS is required for ALL IKEv2 certificate services

- **Centralized network security services for a set of z/OS images**
  - ➤ Images can be non-sysplex, intra- or inter-sysplex
- **NSS digital signature services**
  - ➤ Allows central administration of RACF certificates and private keys
    - – Sign and verify during runtime IKE negotiations
- **NSS monitoring services**
  - ➤ Allows selection of single focal point as IPSec management hub
    - – ipsec command for administrator
    - – NMI API for management applications
- **Availability options**
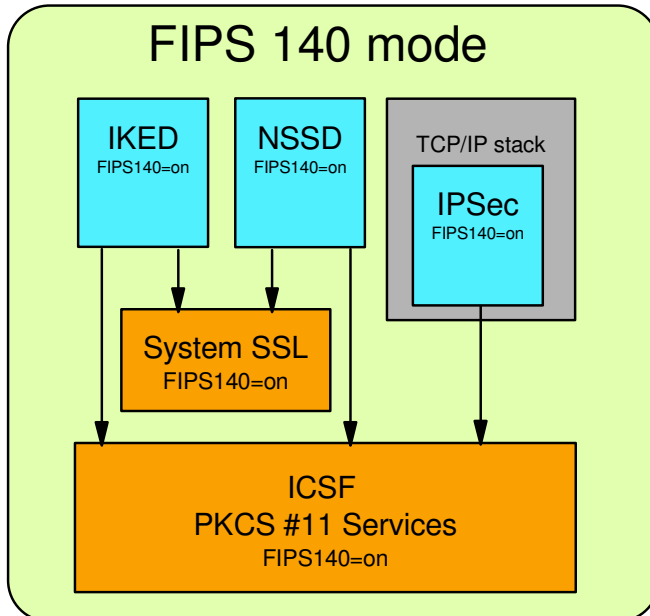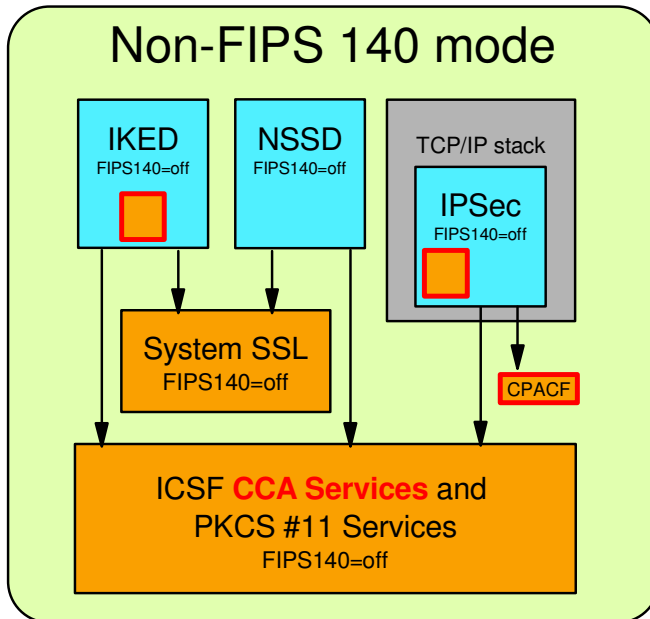 - ➤ Backup NSS can be specified

IPSec Cryptographic Enhancements (V1R12)

IKEv1 Phase 1 and IKEv2 IKE SA			IKEv1 Phase 2 and IKEv2 Child SA		
Purpose	**Existing**	**New z/OS V1R12**	**Purpose**	**Existing**	**New z/OS V1R12**
Encryption algorithm	DES, 3DES, AES_CBC KeyLength 128	AES_CBC Keylength 256	Encryption algorithm	DES, 3DES, AES_CBC KeyLength 128	AES_CBC KeyLength 256, AES_GCM_16 KeyLength 128 | 256
Diffie-Hellman group	Group1, Group2, Group5, Group14	Group19, Group20, Group21, Group24	Authentication algorithm	HMAC_MD5, HMAC_SHA1	AES_GMAC_128 | 256, AES128_XCBC_96, HMAC_SHA2_256_128, HMAC_SHA2_384_192, HMAC_SHA2_512_256
IKEv1 hash algorithm	MD5, SHA1	SHA2_256, SHA2_384, SHA2_512	Perfect forward secrecy group	Group1, Group2, Group5, Group14	Group19, Group20, Group21, Group24
Partner authentication	PreSharedKey, RSASignature	ECDSA-256, ECDSA-384, ECDSA-521 (these are only for IKEv2)			
IKEv2 message verification algorithm	N/A	HMAC_MD5_96, HMAC_SHA1_96 AES128_XCBC_96, HMAC_SHA2_256_128, HMAC_SHA2_384_192, HMAC_SHA2_512_256			
IKEv2 pseudo random function	N/A	HMAC_MD5, HMAC_SHA1 AES128_XCBC, HMAC_SHA2_256, HMAC_SHA2_384, HMAC_SHA2_512			

IKE	**IKE**

Phase 1 or IKE SA

TCP/IP	**TCP/IP**

Phase 2 or Child SA
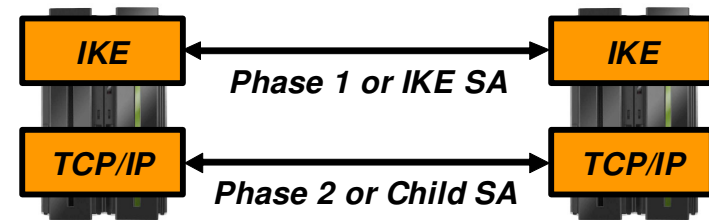
SA: Security Association aka. the tunnel

FIPS 140 mode for IPSec (added in V1R12)

Non-FIPS 140 mode

```
IKED          NSSD          TCP/IP stack
FIPS140=off   FIPS140=off
                            IPSec
                            FIPS140=off


System SSL                  CPACF
FIPS140=off

ICSF CCA Services and
PKCS #11 Services
FIPS140=off
```

FIPS 140 mode

```
IKED          NSSD          TCP/IP stack
FIPS140=on    FIPS140=on
                            IPSec
                            FIPS140=on


System SSL
FIPS140=on

ICSF
PKCS #11 Services
FIPS140=on
```

- **Federal Information Processing Standard 140**
  - ➤ US government standard
  - ➤ Current version is FIPS 140-2
  - ➤ Governs the integrity and functionality of <u>cryptographic modules</u> (not systems or even applications)
    - – Clearly defined boundaries and interfaces
    - – Integrity of algorithms including self-test
    - – Limits on supported algorithms (no MD5, DES, 512-bit RSA or certain AES modes)
    - – Security of keys
    - – Other things that are beyond the scope of this discussion
  - ➤ Originally written for hardware devices - now extending to software modules

- **When enabled for z/OS IPSec, all crypto functions are performed by z/OS FIPS 140 crypto modules:**
  - ➤ System SSL in with FIPS 140 mode enabled
  - ➤ ICSF's PKCS #11 interface with FIPS 140 mode enabled
  - ➤ All other crypto services that IKED or the stack's IPSec support may otherwise use are disabled

- **FIPS 140 option provided for IKED, NSSD and stack's IPSec function**
  - ➤ Stacks configured individually
  - ➤ IKED and NSSD must be enabled if any TCP/IP stack is enabled

z/OS Communications Server IP security

IP Security
Displays and Controls

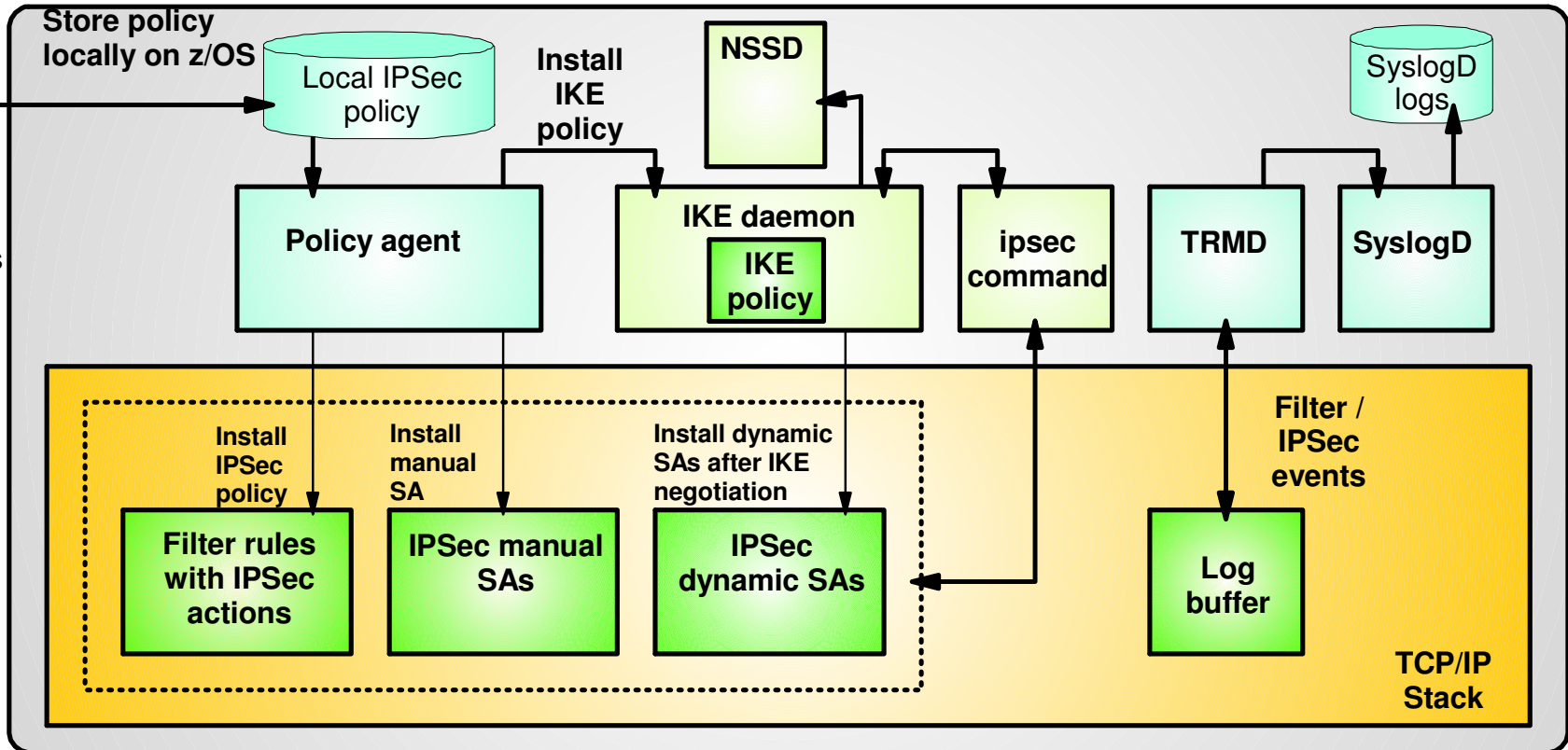# ipsec command summary - primary command options

Primary Command	Main functions provided
ipsec -f	• 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	• Display information about manual tunnels • Activate manual tunnels • Deactivate manual tunnels
ipsec -k	• Display information about IKE tunnels • Deactivate IKE tunnels • Refresh IKE tunnels
ipsec -y	• 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	• Display interface information
ipsec -t	• Locate matching filter rule
ipsec -o	• Display NAT port translation table information
ipsec -?	Help

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

z/OS Communications Server IP security

Configuring and Enabling
IP Security

z/OS Communications Server IP security infrastructure overview

- **TCP/IP stack**
  - ➤ IPSec and IP filtering
- **Policy agent**
  - ➤ Reads and manages IPSec and IKE policy
- **Configuration Assistant for z/OS Communications Server**
  - ➤ Creates policy definitions
- **IKE daemon**
  - ➤ Negotiates security associations

- **ipsec command**
  - ➤ Displays and controls IP filtering, IPSec, and IKE
- **trmd**
  - ➤ Monitors TCP/IP stacks for log messages
- **syslogd**
  - ➤ Write log messages to syslogd destinations
- **Network Security Services daemon**
  - ➤ Provides certificate services for IKE

Configuration required for IP security

- **z/OS system preparation tasks**
  - ➤ TCP Profile updates to enable IP security, define default filter rules, enable SWSA
  - ➤ Policy infrastructure applications configuration and JCL procedures
    - – IKE daemon (IKED)
    - – Policy agent
    - – Network Security Services daemon (NSSD)
    - – Traffic regulation management daemon (TRMD)
    - – Syslog daemon (syslogd)
  - ➤ SAF access control for:
    - – Applications
    - – ipsec command
  - ➤ Integrated Cryptographic Services Facility (ICSF) for hardware encryption
    - – Preparation not included with Configuration Assistant
- **IP security policy definition**
  - ➤ For each TCP/IP stack create a policy rule set
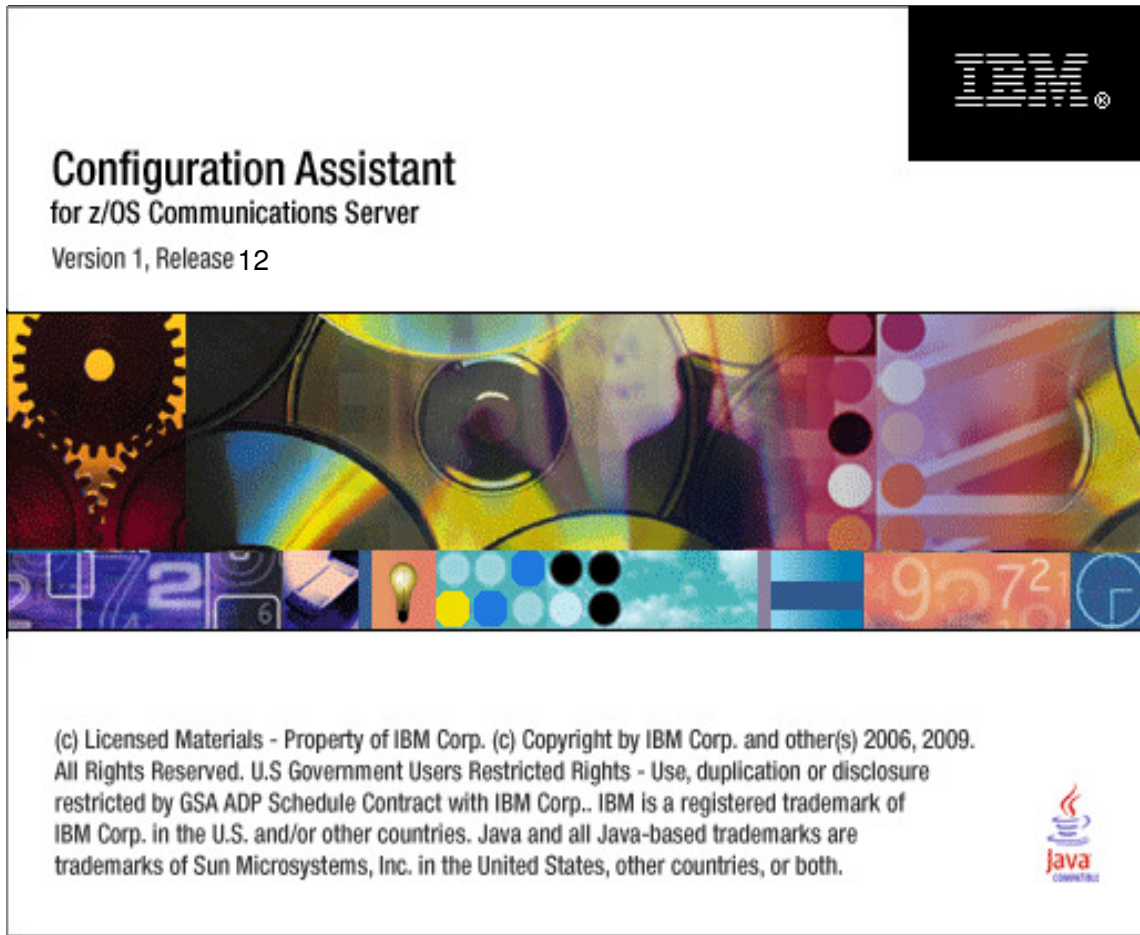   - – Policy is composed of conditions and actions
- **SAF keyrings for x.509 certificates**
  - ➤ Certificate Authority certificates and Host certificates

> Prior to z/OS V1R11, the Configuration Assistant helps configure the policy definitions
>
> Starting in z/OS V1R11, the Configurations Assistant can help with the z/OS System Preparation Tasks !

Configuration Assistant for z/OS Communications Server

Configuration Assistant
for z/OS Communications Server

Version 1, Release 12

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2009. All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

- **GUI-based approach to configuring:**
  - ➤ IDS
  - ➤ AT-TLS
  - ➤ IPSec and IP filtering
  - ➤ QoS
  - ➤ Policy-based Routing (PBR)
- **Focus on high level concepts vs. low level file syntax**
- **Runs on Windows and under z/OSMF (V1R11)**
- **Builds and maintains**
  - ➤ Policy files
  - ➤ Related configuration files
  - ➤ JCL procedures and RACF directives **(V1R11)**
- **Supports import of existing policy files (V1R10)**

Download the Windows-based Configuration Assistant at: **http://tinyurl.com/cgoqsa**

Application setup task checklist

Assistance with the z/OS System Preparation Tasks - Use the Application Setup Task Checklist

IPSec policy definition steps

1. Create system image and TCP/IP stack image

2. Create one or more Requirement Maps to define desired security for common scenarios (e.g. intranet, branch office, business partner)
   - ► Create or reuse Security Levels to define security actions
   - ► Create or reuse Traffic descriptors to define application ports to secure

3. Create one or more Connectivity Rules between Data Endpoints (IP addresses) and associate with a configured Requrement Map

4. If using IPSec, configure Security Endpoints (IKE peers)

5. Optionally, set additional options (e.g. logging, SA activation methods, effective time for Connectivity Rules)

Configuration Assistant Policy Definition Model

Group IP addresses that need the same treatment. For example all VIPA addresses, or all real network interface addresses. Simplifies creation of connectivity rules

Identifies a specific type of application network traffic. Based on protocol (TCP/UDP), local and/or remote ports, connection direction, z/OS jobname, etc.

Identifies the IP security requirements, such as permit/deny/IPSec with ciphersuites allowed.

IP Address group

Traffic Descriptor

Security Level

IP Address

IP Address

IP Address

IP Address

Requirement Map

Identifies what type of IP security applied to your traffic descriptors

Per policy type (not all object types are used with all policy types)

Connectivity Rule

Connectivity rules are stack-specific and ties IP addresses to requirement maps

LPARs (Images)

Stacks

SAF Certificates and Keyrings
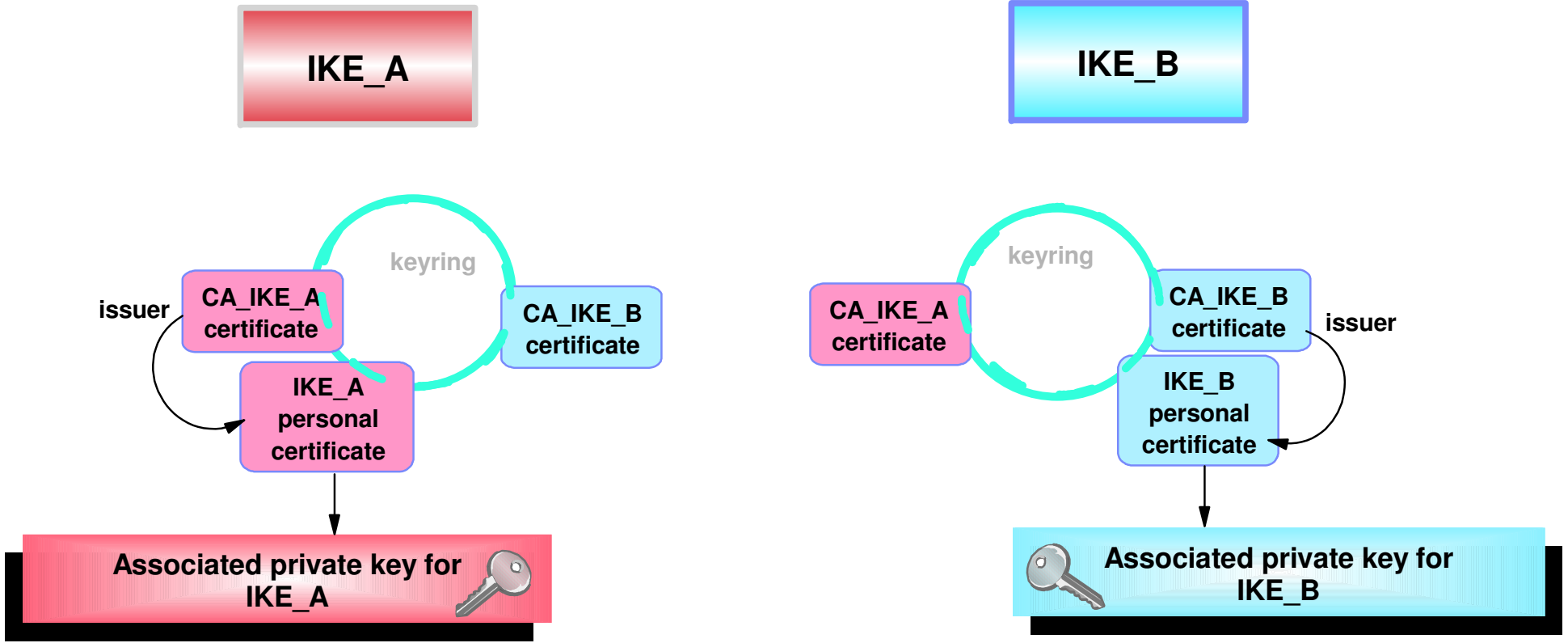
Certificate Creation and Installation Example Using RACF

```
//CERTADD JOB 1,ALFRED,CLASS=A,MSGCLASS=X,NOTIFY=USER1
//*
//IEFPROC  EXEC PGM=IKJEFT01,REGION=4M,DYNAMNBR=10
//SYSTSPRT 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).

z/OS Communications Server IP security features summary

- **Supports many configurations**
  - ➤ Optimized for role as endpoint (host), but also support routed traffic (gateway)
  - ➤ IPSec NAT Traversal support (address translation and port translation)
  - ➤ IPv4 and IPv6 support

- **Policy-based**
  - ➤ Configuration Assistant GUI for both new and expert users
  - ➤ Direct file edit into local configuration file

- **Default filters in TCP profile provide basic protection before policy is loaded**

- **Cryptographic algorithms**
  - ➤ RSA signature-based authentication
  - ➤ ECDSA signature-based authentication **(V1R12)**
  - ➤ HMAC-SHA-1, HMAC-MD5 authentication
  - ➤ HMAC-SHA-2, AES-XCBC, AES-GMAC authentication **(V1R12)**
  - ➤ AES-CBC, 3DES and DES encryption
  - ➤ AES-GCM (128- and 256-bit) encryption **(V1R12)**
  - ➤ Uses cryptographic hardware if available for most algorithms
  - ➤ FIPS 140 mode **(V1R12)**

- **zIIP Assisted IPSec**
  - ➤ Moves most IPSec processing from general purpose processors to zIIPs

- **IP Security Monitoring Interface**
  - ➤ IBM Tivoli OMEGAMON XE for Mainframe Networks uses the CommServer NMI interfaces for IP Security

- **Support for latest IPSec RFCs**
  - ➤ RFCs 4301-4305, 4307-4308 **(V1R10)**
  - ➤ RFC 4306 (IKEv2) **(V1R12)**

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/servers/eserver/zseries/networking		Networking: IBM zSeries Servers
http://www.ibm.com/software/network/commserver		IBM Software Communications Server products
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/zos/support/		IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs		Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html		Requests For Comment (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