Configuration for z/OS IPSec and IP Packet Filtering (Part 1 of 2)

SHARE Session 3914

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

© 2007 IBM Corporation

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 7
- AnyNet 7
- AS/400 7
- Candle 7
- CICS 7
- CICSPlex 7
- CICS/ESA 7
- DB2 7
- DB2 Connect™
- DPI 7
- DRDA 7
- e business(logo) 7
- ESCON 7
- eServer™
- ECKD™
- FFST™
- GDDM 7
- GDPS 7
- HiperSockets™
- IBM 7
- Infoprint 7
- IMS™
- IP PrintWay™
- iSeries™
- Language Environment 7
- MQSeries 7
- MVS™
- MVS/ESA™
- NetView 7
- OS/2 7
- OS/390 7
- Parallel Sysplex 7
- PrintWay™
- PR/SM™
- pSeries 7
- RACF 7
- Redbooks™
- Redbooks (logo)™
- S/390 7
- System/390 7
- ThinkPad 7
- Tivoli 7
- Tivoli (logo) 7
- VM/ESA 7
- VSE/ESA™
- VTAM 7
- WebSphere 7
- xSeries 7
- z/Architecture™
- z/OS 7
- z/VM 7
- zSeries 7

- 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.

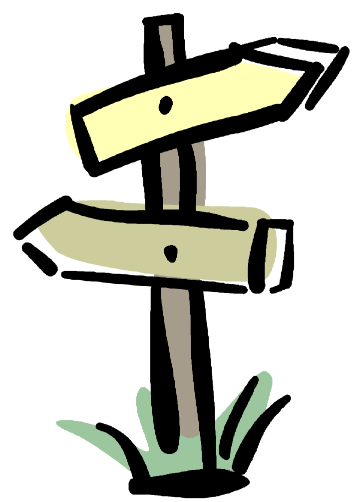
All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

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

© 2007 IBM Corporation

z/OS Communications Server IP security agenda

- Part 1 - Session 3914
  - Introduction to IP security on z/OS
  - IP filtering
  - IPSec
- Part 2 - Session 3907
  - Configuring and enabling IP Security
  - IP security displays and controls



© 2007 IBM Corporation

z/OS Communications Server IP security

Introduction

© 2007 IBM Corporation

Protocol stack view of TCP/IP security functions

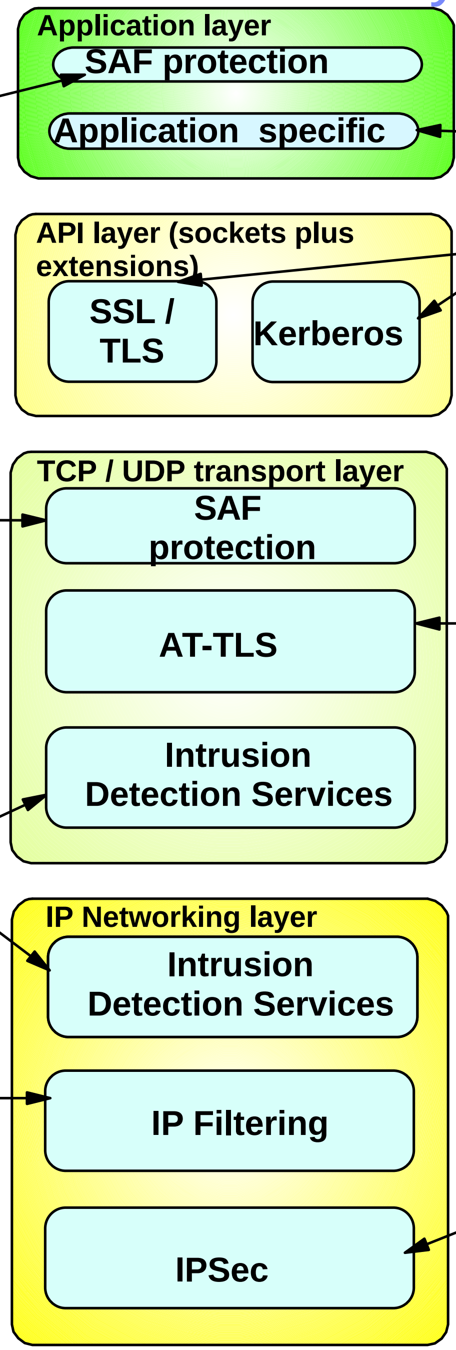
Protect the system

z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources..

The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks)

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers

IP filtering blocks out all IP traffic that this systems doesn't specifically permit.



Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.

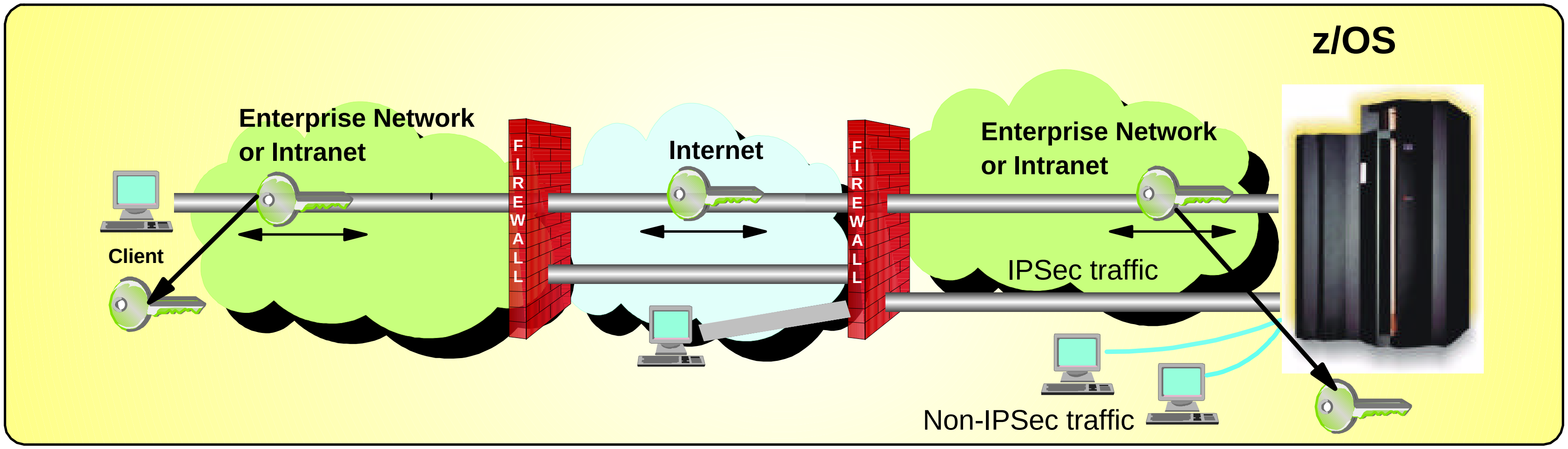
Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is avaliable to TCP applications in all programming languages except PASCAL.

IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

© 2007 IBM Corporation

z/OS IP security support



- Prior to z/OS V1R7, IP security packaged with Firewall Technologies
  - TCP/IP IPSec and IP filtering support
    - Communications Server
  - IKE daemon and configuration
    - Integrated Security Services
- In z/OS V1R7, complete IPSec, IP filtering, and IKE solution part of z/OS Communications Server
  - Alternative to Firewall Technologies
    - New IKE daemon and configuration
  - Services
    - IP filtering
    - Manual IPSec
    - Dynamic IPSec (IKE)
    - Filter directed logging to syslogd

© 2007 IBM Corporation

Firewall Technologies

- Starting in z/OS V1R8, Firewall Technologies is no longer available

Announced Feb 15th, 2005

- z/OS V1.7 is the last z/OS release to include the Firewall Technologies component of the Integrated Security Services element.
- Many Firewall Technologies functions have been stabilized for some time and can be replaced using comparable or better functions provided by or planned for Communications Server, notably,
  - IPSec
  - IP packet filtering
  - In addition, a functionally rich downloadable tool is planned to replace the IPSecurity and IP Filtering configuration GUI support.
- The following functions will be removed without replacement:
  - FTP Proxy services
  - Socks V4 services
  - Network Address Translation (NAT)
  - RealAudio support

© 2007 IBM Corporation

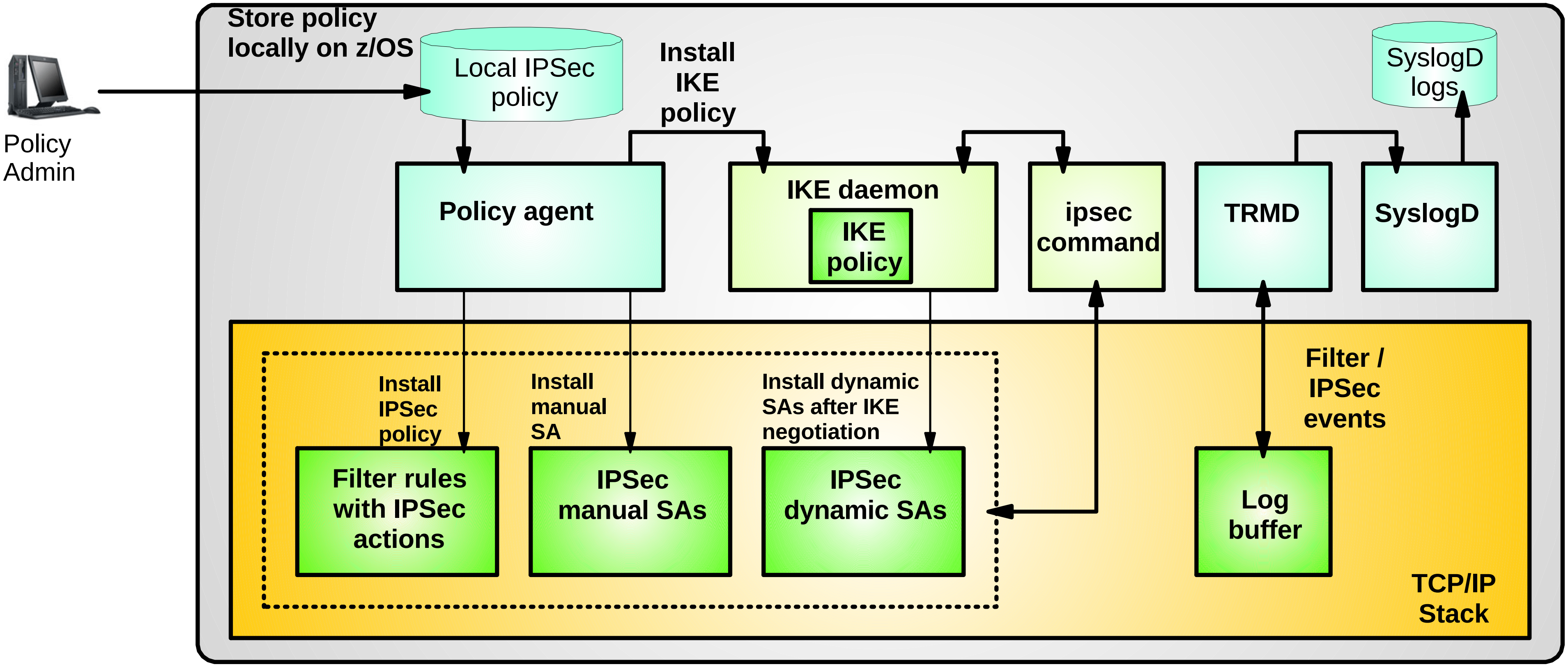
z/OS Communications Server IP security features

- **Configuration support**
  - ➤ Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
  - ➤ IPSec NAT Traversal support
    - – IP address translation
    - – Port translation **(V1R8)**
  - ➤ IPv4 and IPv6 support **(IPv6 in V1R8)**
- **Simplified infrastructure**
  - ➤ Eliminates need for FW Technologies daemons
  - ➤ Policy agent reads and manages IPSec and IKE policy
- **Simplified configuration**
  - ➤ New configuration GUI for both new and expert users
  - ➤ Direct file edit into local configuration file
  - ➤ Reduced definition, more "wildcarding"
- **Improved serviceability**
  - ➤ Improved messages and traces
- **Default filters part of TCP profile**
  - ➤ More granular control before policy is loaded
- **Administrative controls**
  - ➤ pasearch
  - ➤ ipsec command
- **Cryptographic algorithms (** uses cryptographic hardware if available)**
  - ➤ DES(**) and 3DES(**) encryption
  - ➤ HMAC-SHA (**) and HMAC-MD5 authentication
  - ➤ AES (**) encryption **(V1R8)**

- **z/OS Communications Server IP security covers:**
  - ➤ IP filtering
  - ➤ IPSec

© 2007 IBM Corporation

z/OS Communications Server IP security Infrastructure overview



- **TCP/IP stack**
  - ➤ IPSec and IP filtering
- **IKE daemon**
  - ➤ Negotiates security associations
- **Policy agent**
  - ➤ Reads and manages IPSec and IKE policy
- **Network Security Configuration Assistant**
  - ➤ Creates policy definitions
- **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

© 2007 IBM Corporation

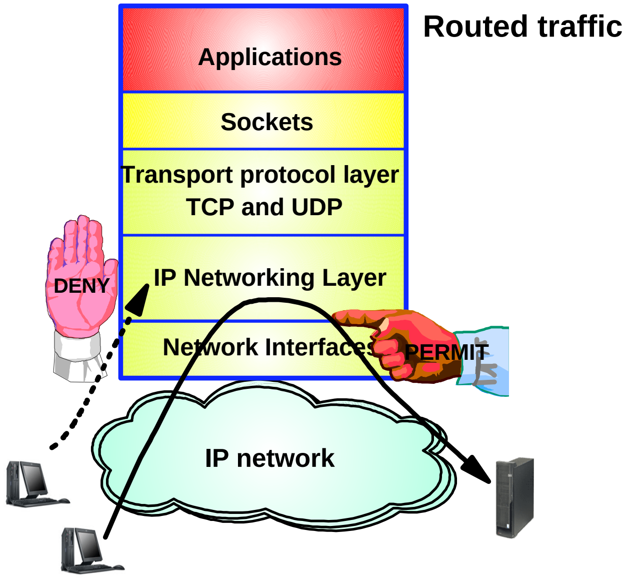
z/OS Communications Server IP security

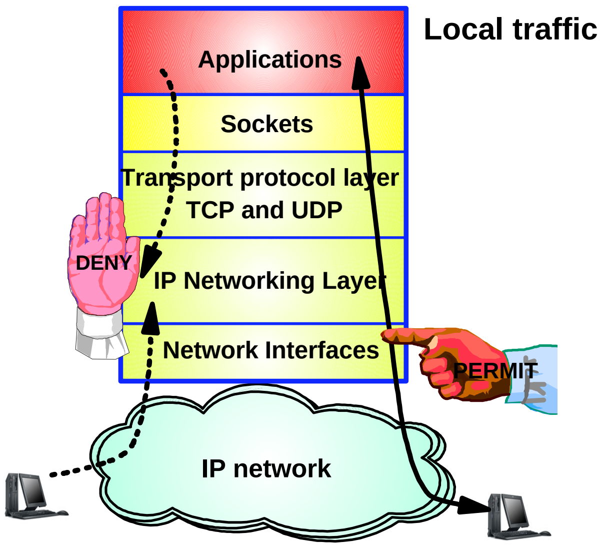
IP filtering

© 2007 IBM Corporation

Basics of IP filtering

- **Packet filtering at IP Layer**
  - Filter rules defined to match on inbound and outbound packets based on:
    - packet information
    - network attributes
    - time
  - Used to control
    - traffic being routed
    - access at destination host
  - Possible actions
    - 1. Permit
    - 2. Deny
    - 3a. Permit with manual IPSec
    - 3b. Permit with dynamic IPSec
    - Log (in combination with others)





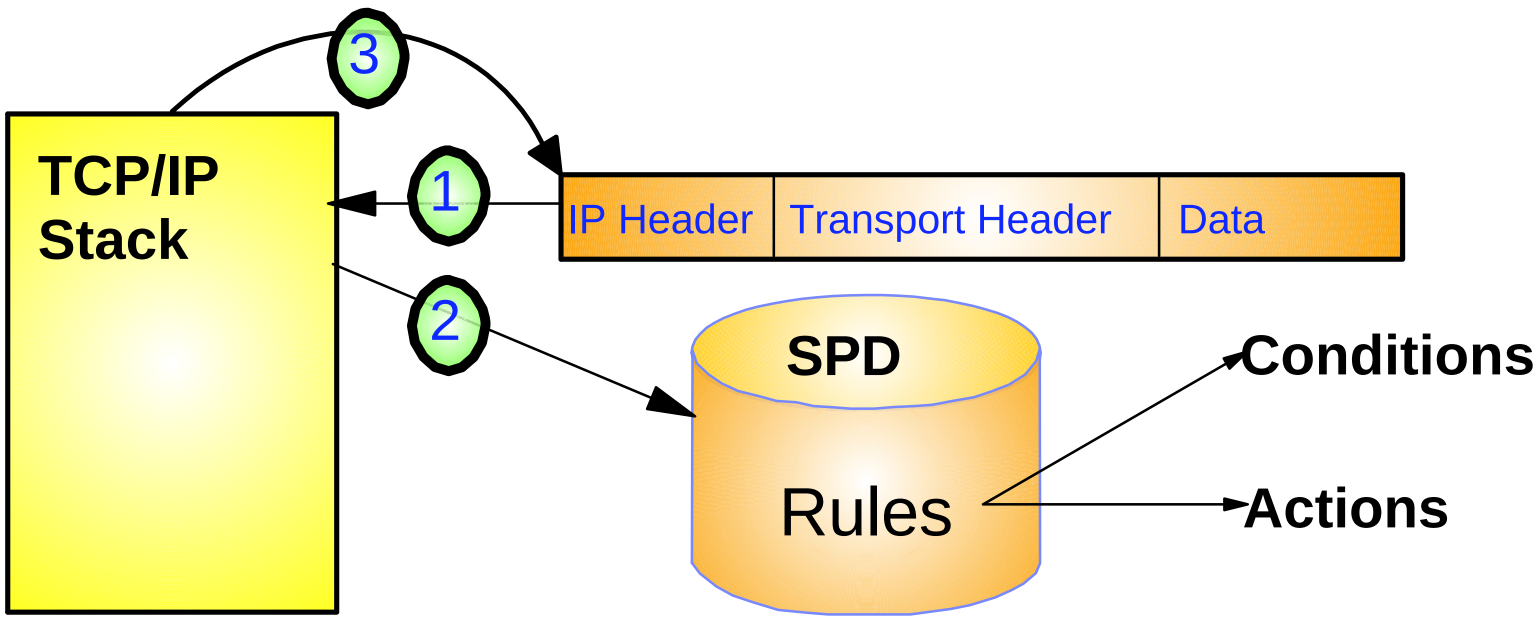
© 2007 IBM Corporation

IP filtering processing overview

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

2. **Consult filter rules in a Security Policy Database (SPD)**
   - ➢ Rules have conditions and actions

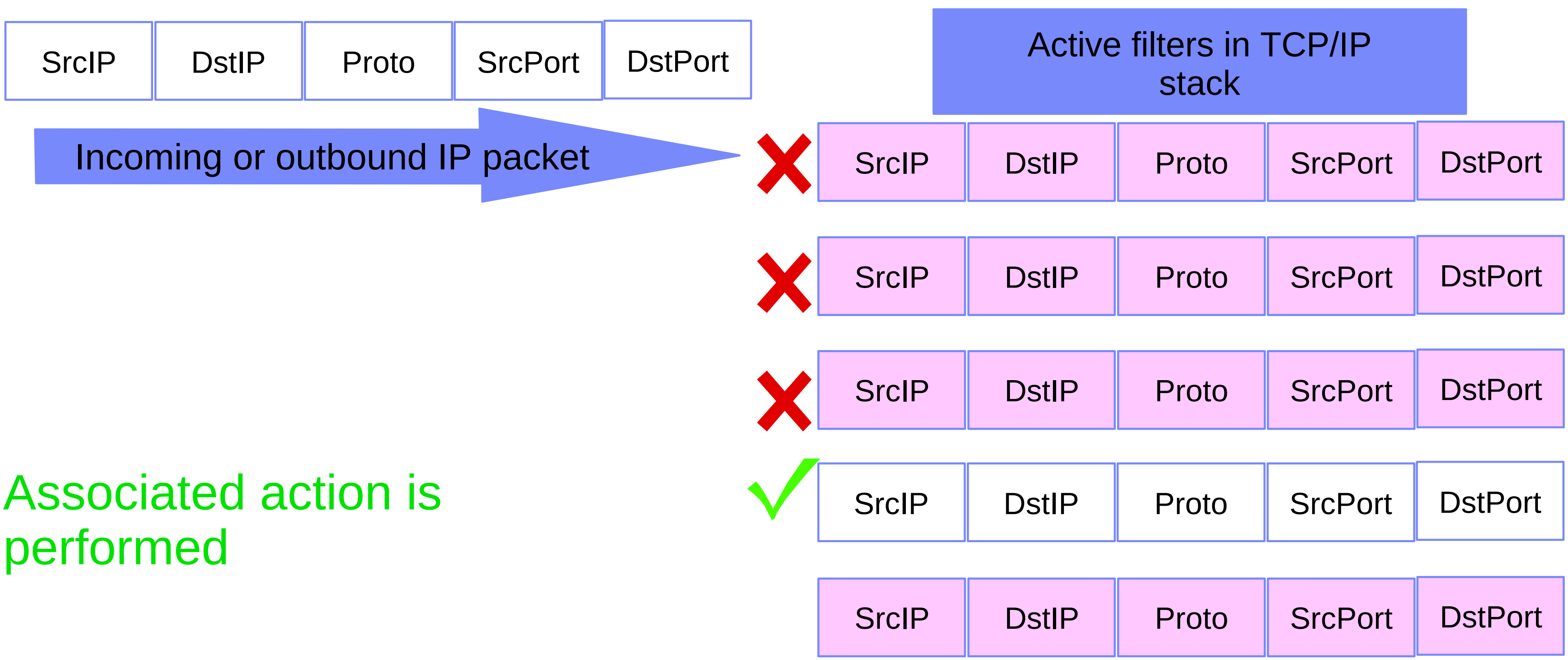
3. **Apply action of matching rule to packet**
   - ➢ Deny
   - ➢ Permit
   - ➢ Permit with additional processing applied



© 2007 IBM Corporation

IP Filtering Concepts
Filter Matching

1. Filters are searched in the order they were configured
2. Each rule is inspected, from top to bottom, for a match
3. If a match is found, the search ends and the action is performed



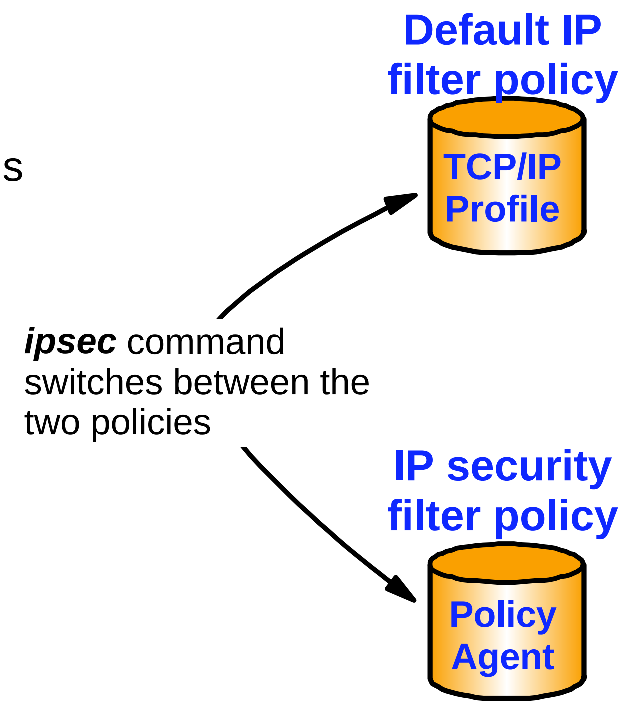
© 2007 IBM Corporation

IP security - filter policies

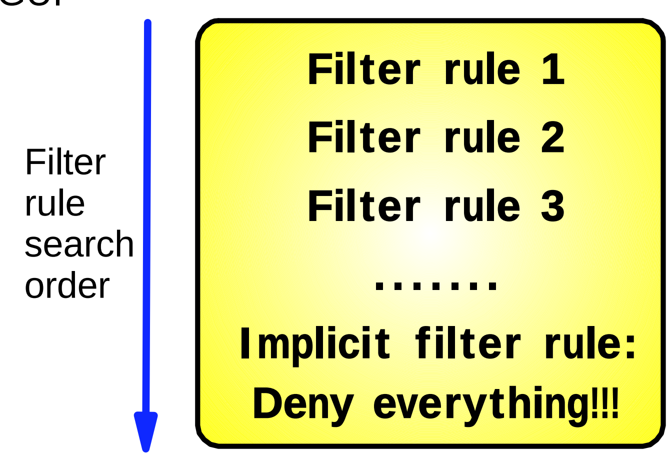
- IP security's Security Policy Database (SPD)

  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
       - No VPN 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)



© 2007 IBM Corporation

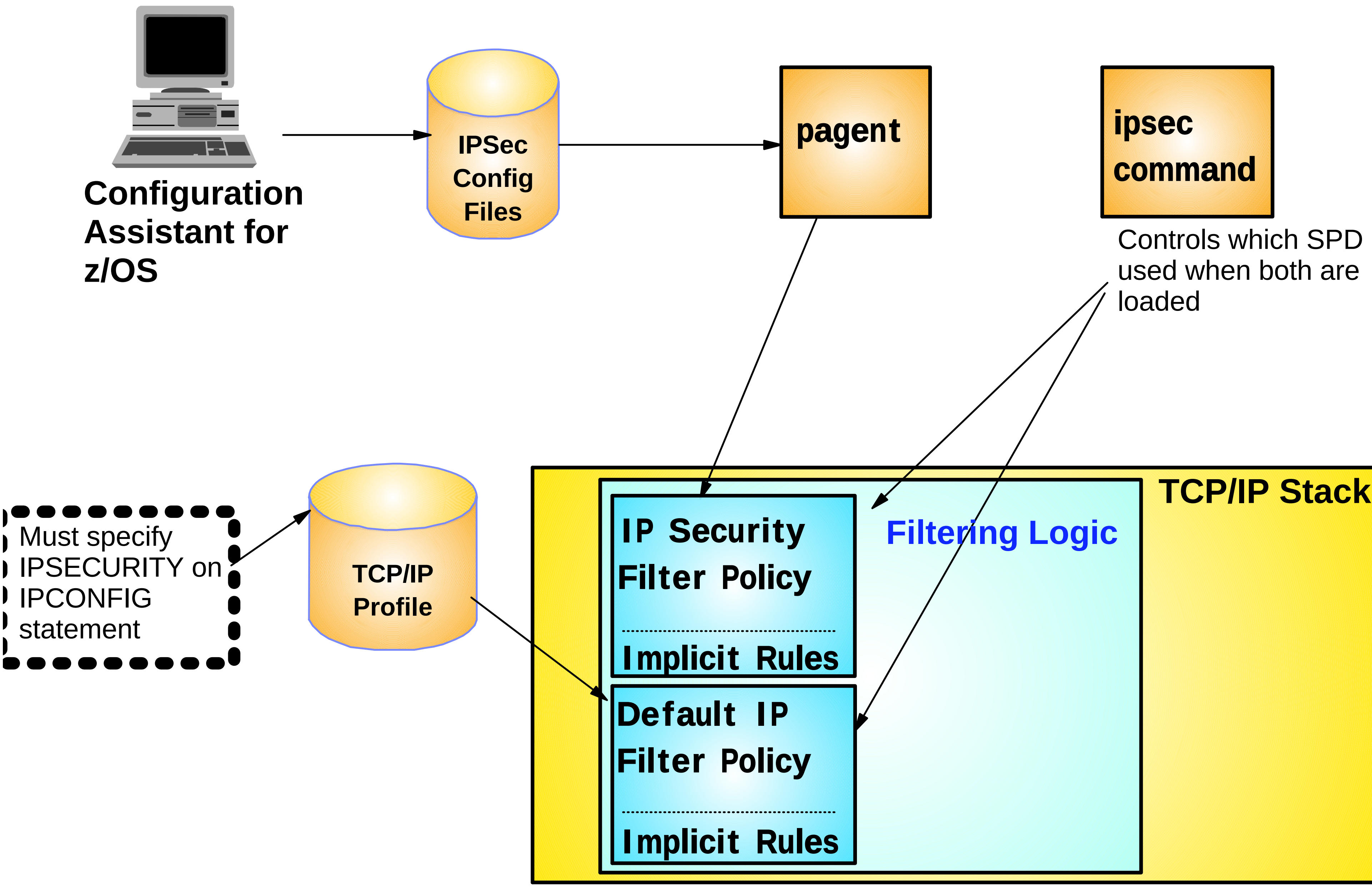
A little more detail on the default filter policy

- Provides initial protection of the stack during initialization
  - Used until IP security filter policy is loaded

- Generally restrictive; these user-defined rules should include
  - Traffic needed for services
    - Examples
      - Omproute
        - OSPF traffic
        - IGMP traffic
      - DNS queries
        - UDP traffic with a destination port of 53
  - Traffic needed to fix problems with IP security filter policy
    - Examples
      - FTP traffic from the workstation running the Configuration Assistant for z/OS GUI
      - Telnet traffic from the Network Administrator's workstation

© 2007 IBM Corporation

IP filter policy on z/OS - overview



© 2007 IBM Corporation

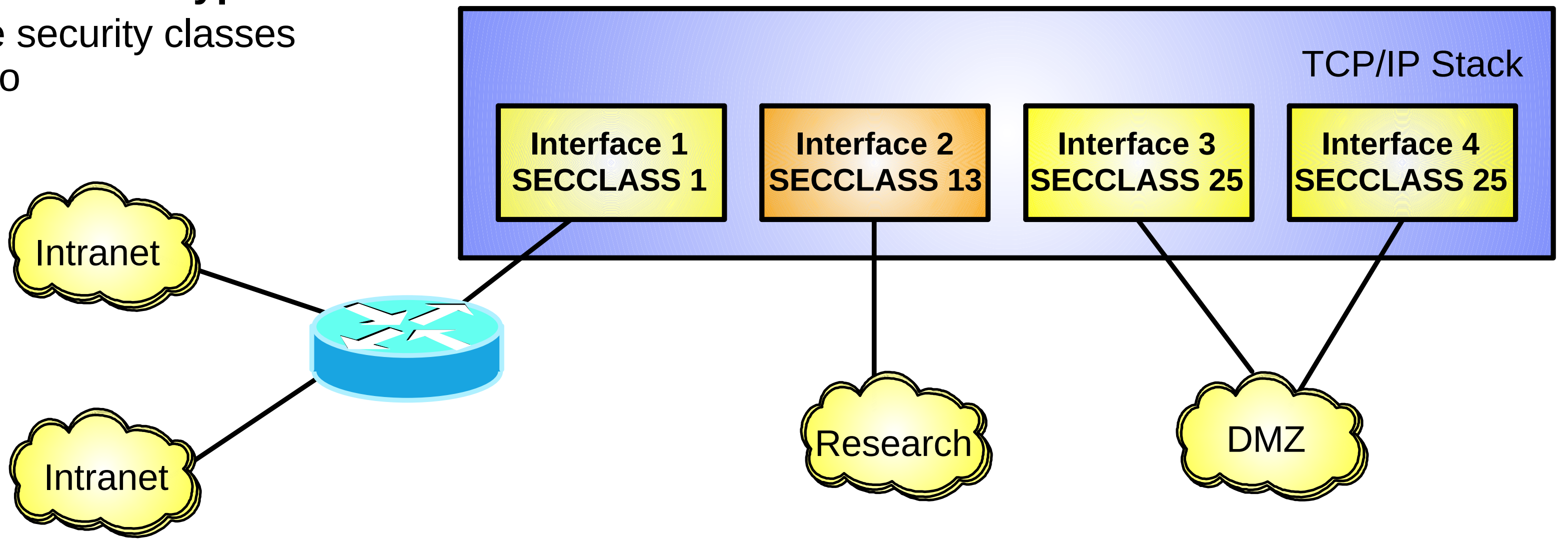
Filtering conditions

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
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

© 2007 IBM Corporation

Interface security class (SECCLASS)

- **Can be assigned only to non-virtual interfaces**
- **Defined in the TCP/IP profile**
  - LINK statement (SECCLASS parameter)
  - IPCONFIG DYNAMICXCF statement (SECCLASS parameter)
- **Value 1 to 255 (default is 255)**
  - Value is just a classification identifier, it has no inherent meaning
    - Can be referred to in the filter rules
- **Packets inherit the security class of the interface they traverse**
- **A more flexible and expandable mechanism than the traditional firewall's "secure" vs. "non-secure" interface types**
  - 254 interface security classes instead of two



© 2007 IBM Corporation

Allowed IP filter conditions - Differences between the default and IP security filter policy definitions

Criteria	Default IP Filter Policy	IP Security Filter Policy
IP addresses	Single/Subnet	Single/***Range***/Subnet
Protocol	Single/All	Single/All
Ports	Single/All for UDP and TCP	Single/***Range***/All for UDP and TCP
Type	Single/All for ICMP and OSPF	Single/All for ICMP for OSPF
Code	Single/All for ICMP	Single/All for ICMP
Direction	Bidirectional	***Inbound***/***Outbound***/ Bidirectional ***(1)InboundConnect/ OutboundConnect***
Routing	Local	Local***/Routed/Either***
Security Class	Single/Any	Single/Any
Time Conditions	Not Applicable	***Time Specification***

Note: 1) Optional conditions specified with bidirectional that control who initiates TCP connections

Text: highlights difference between the two policies

© 2007 IBM Corporation

Allowed IP filter actions - Differences between the default and IP security filter policy definitions

Default IP Filter Policy	IP Security Filter Policy
✓ Permit	✓ Permit ✓ Deny ✓ IPSec (both manual and dynamic)

- Both policies allow filter logging to be enabled/disabled
- IP Security filter policies using an action of IPSec:
  - Must be bidirectional
  - Can only specify a security class of 0
    - Indicates the rule applies to all interfaces
  - Require the definition of additional policy actions
    - Manual VPN actions
    - Dynamic VPN actions
  - Packets matching an SPD rule with an IPSec action are modified to provide authentication and/or data encryption

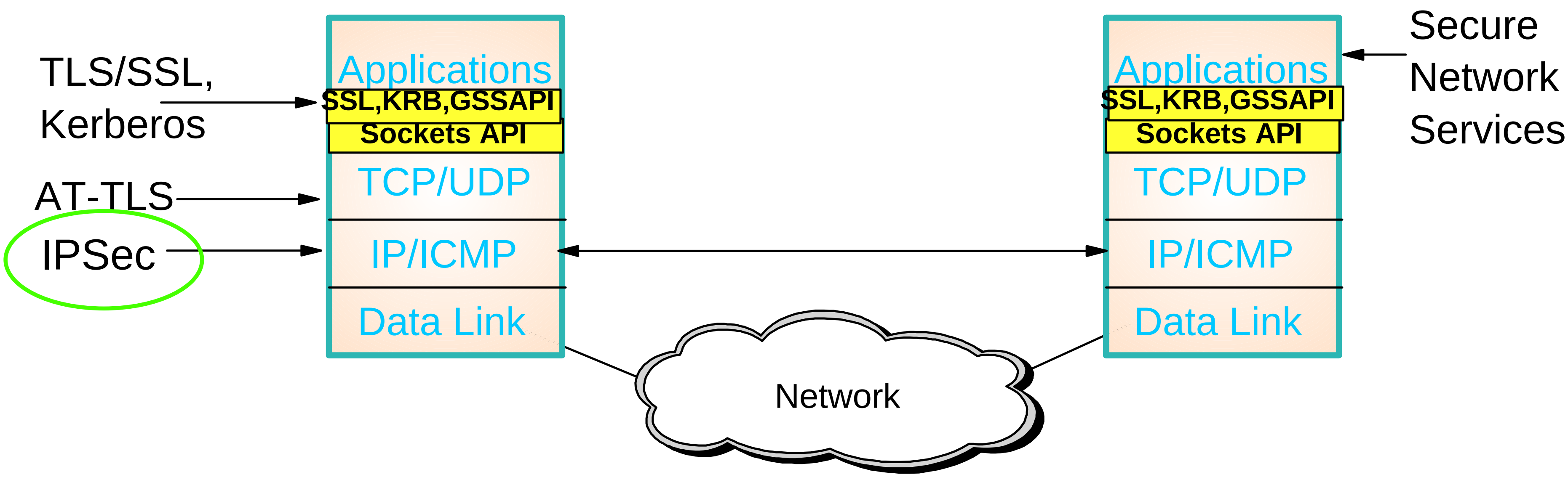
© 2007 IBM Corporation

z/OS Communications Server IP security

IPSec

© 2007 IBM Corporation

IPSec protocol overview

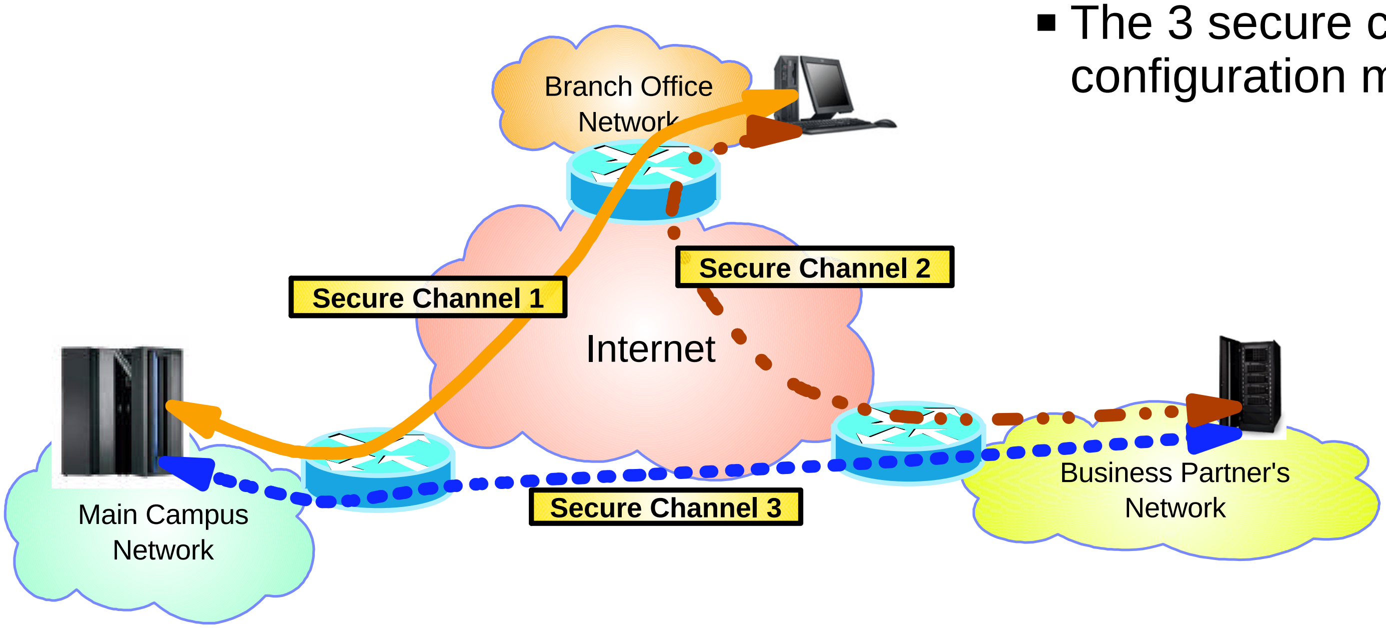


- Open network layer security protocol defined by IETF
- Provides authentication, integrity, and data privacy
  - IPSec security protocols
    - **Authentication Header (AH)** - provides authentication / integrity
    - **Encapsulating Security Protocol (ESP)** - provides data privacy with optional authentication/integrity
- Implemented at IP layer
  - Requires no application changes
  - 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 (IKE)

© 2007 IBM Corporation

Virtual Private Network (VPN) overview

- Virtual Private Network
  - Logical network of connected nodes that communicate over unsecure networks using a secure channel

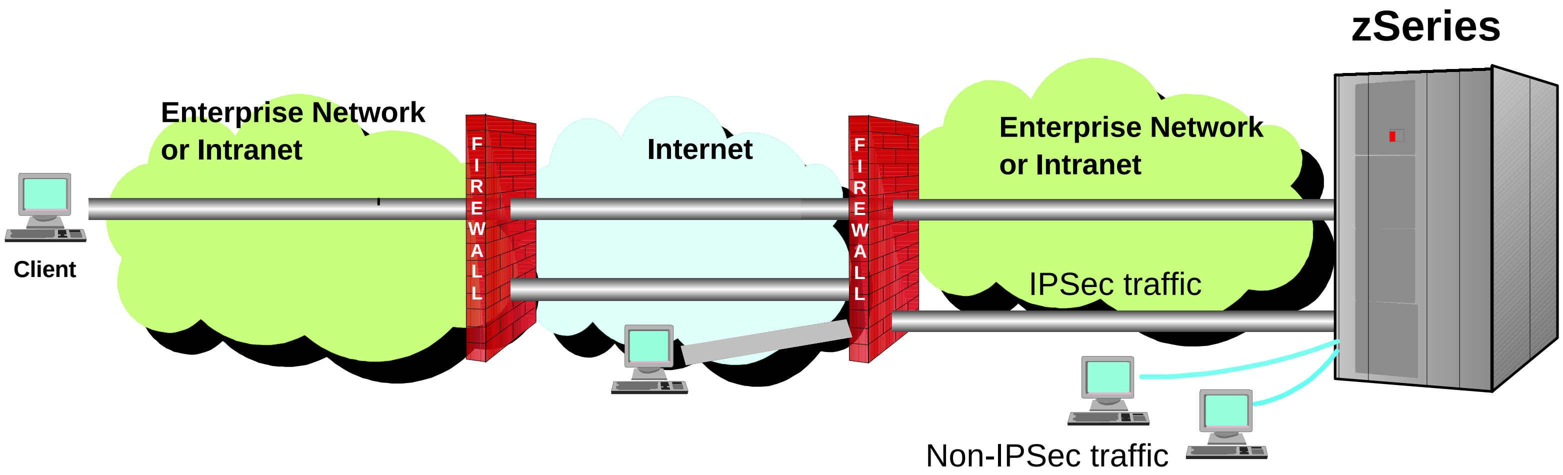


- The 3 secure channels in this sample configuration make up a VPN

- A secure channel is commonly called a tunnel and uses authentication and/or encryption
  - A secure channel provides point to point security
- VPNs are built using IPSec security protocols

© 2007 IBM Corporation

IPSec security associations

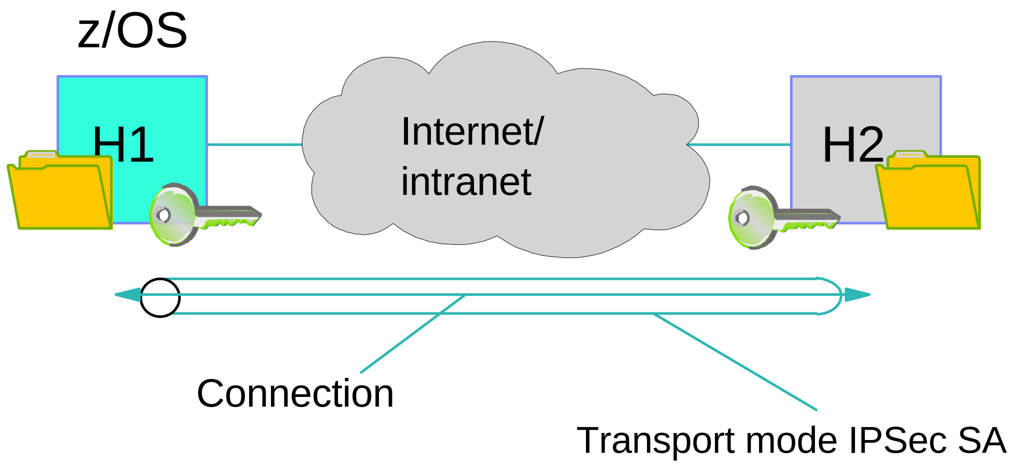


- IPSec Security Association (SA) defines security services for a defined traffic type
  - Unidirectional logical connection between 2 IPSec hosts
  - Used in pairs for bidirectional traffic
- SA scope of protection can vary
  - Wide - Traffic protection for multiple connections e.g. Protect all traffic 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

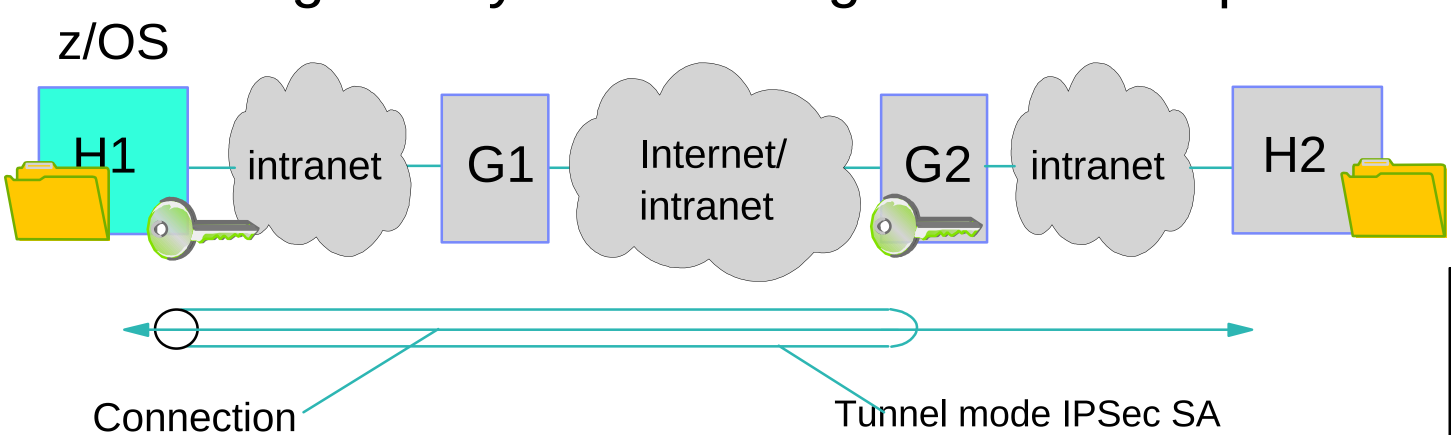
© 2007 IBM Corporation

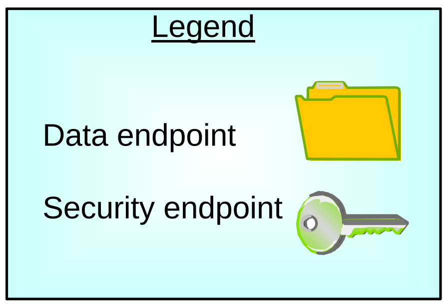
IPSec Scenarios
z/OS as Host

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



Host-to-gateway: Protect segment of data path

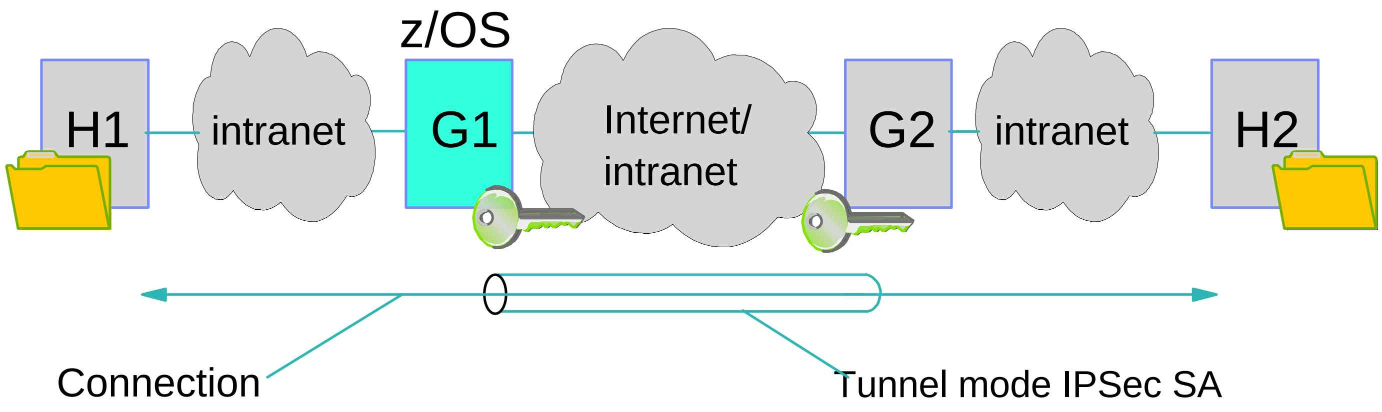




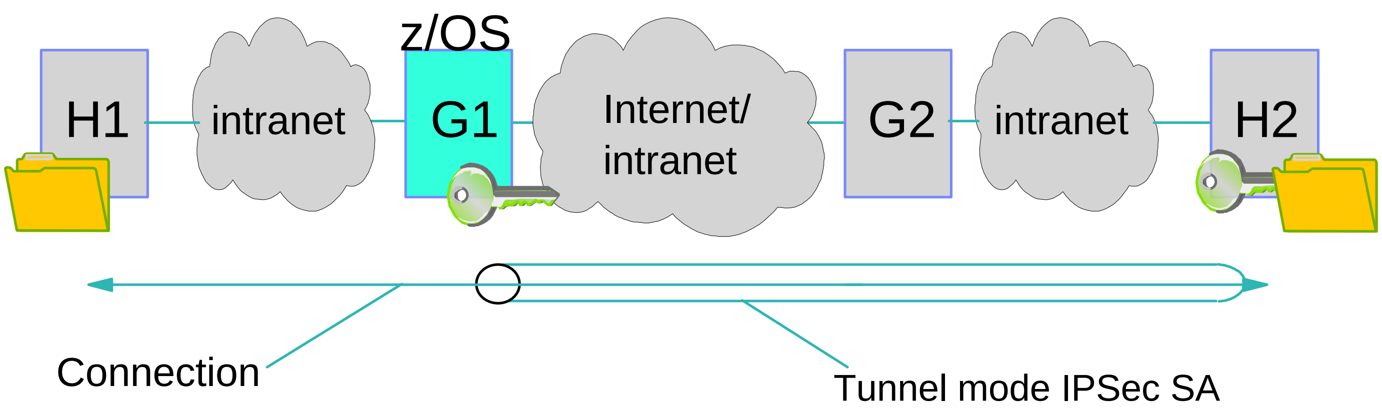
© 2007 IBM Corporation

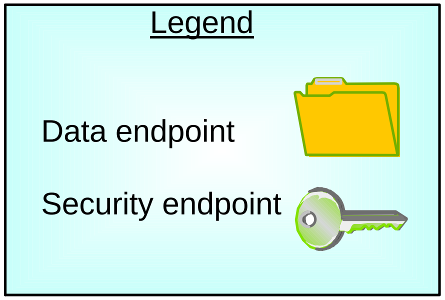
IPSec Scenarios
z/OS as Gateway

Gateway-to-Gateway: Protection over Untrusted Network Segment



Gateway-to-Host: Protection over Untrusted Network Segment



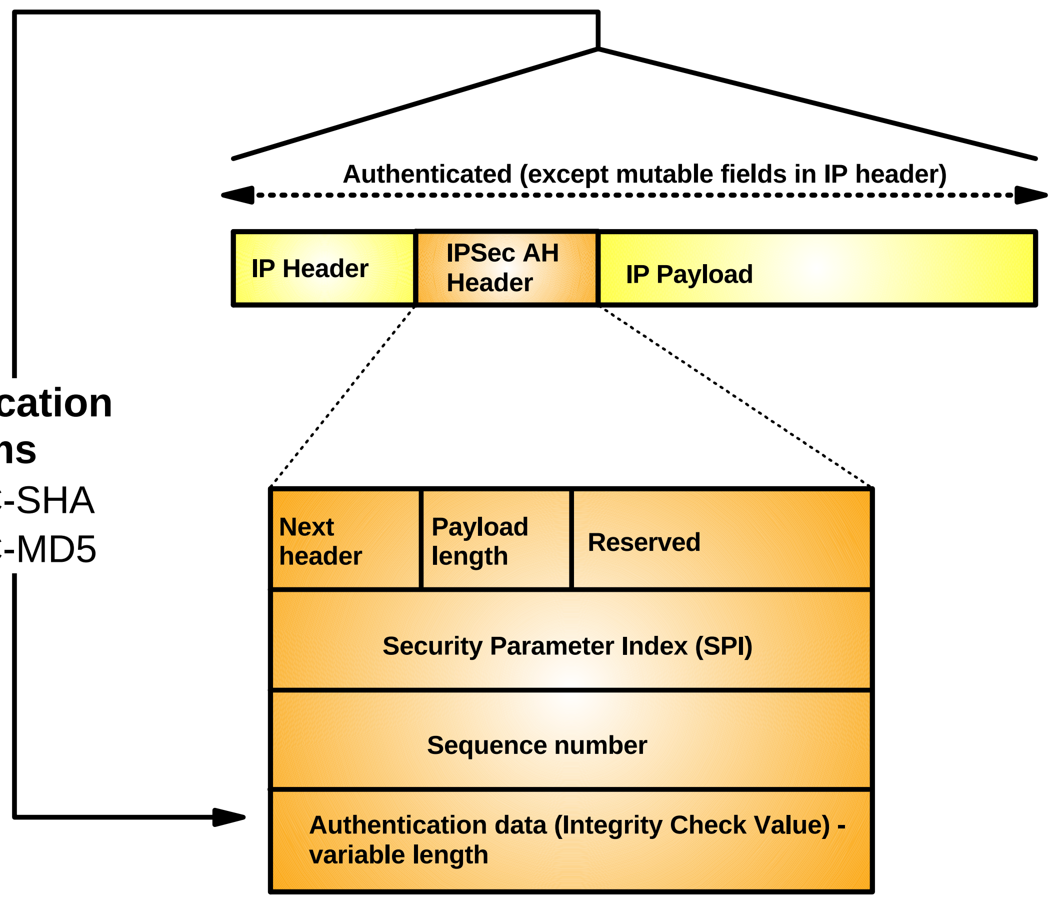


© 2007 IBM Corporation

IPSec Authentication Header (AH) protocol

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

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



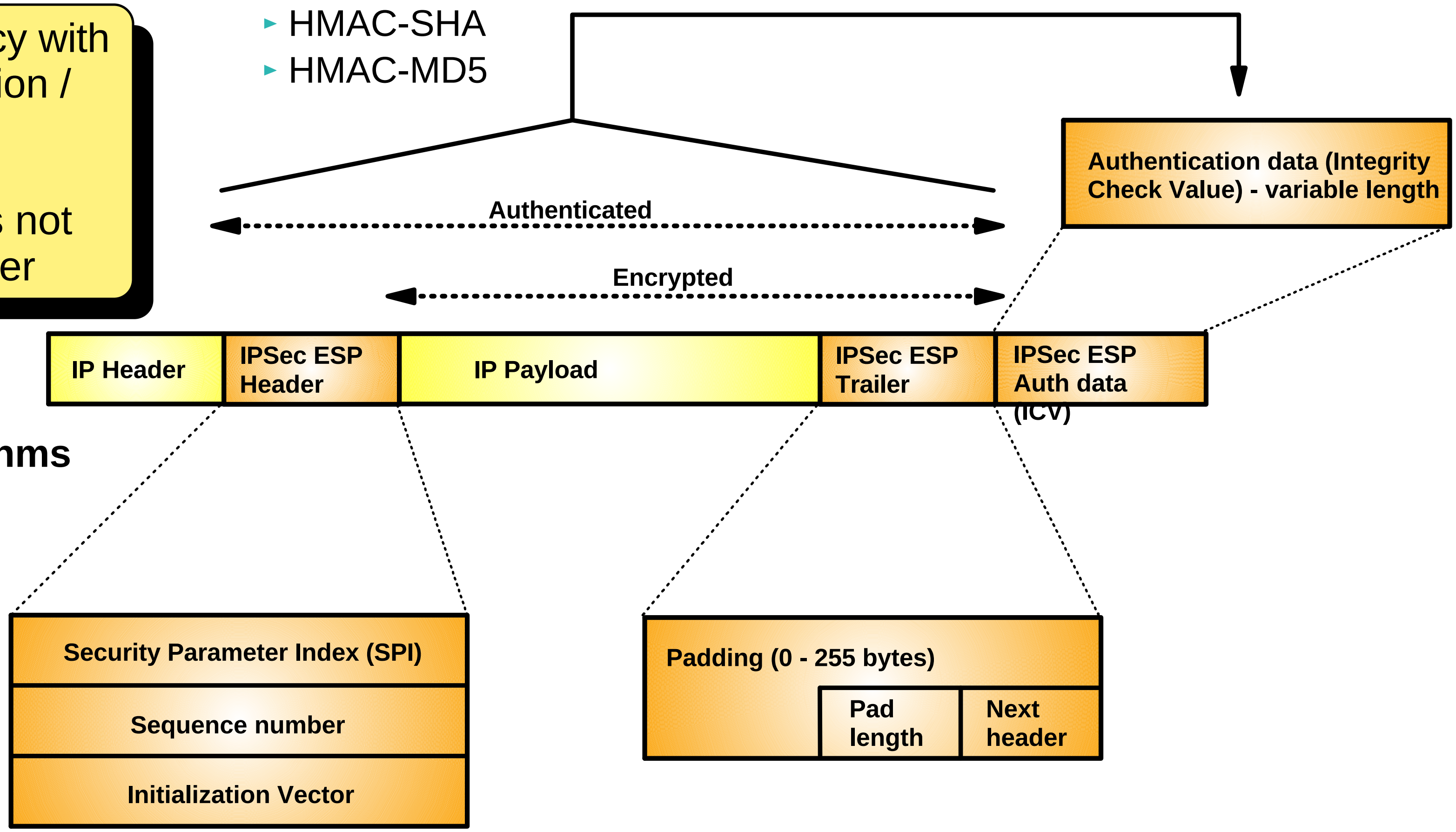
- **If transport mode then "Payload" contains the original transport header and original data**
- **If tunnel mode then "Payload" contains the original IP header, original transport header, and original data**

© 2007 IBM Corporation

IPSec Encapsulating Security Payload (ESP) protocol

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

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



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

- **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

© 2007 IBM Corporation

Encapsulation mode

- **Indicates how to construct an IPSec packet**

- **Two modes**
  - Transport mode
    - Inserts AH and/or ESP headers between original IP header and protected data
  - Tunnel mode
    - Creates a new IP header with an AH and/or ESP header
    - AH/ESP header followed by original IP header and protected data

- **If one or both security endpoints are acting as a gateway**
  - Tunnel mode must be selected

- **If neither security endpoint is acting as a gateway**
  - Tunnel or transport may be selected
  - Usually transport mode is used in this case
    - No need for extra cost of adding a new IP header in this case

- **The counterpart to encapsulation is decapsulation**

© 2007 IBM Corporation

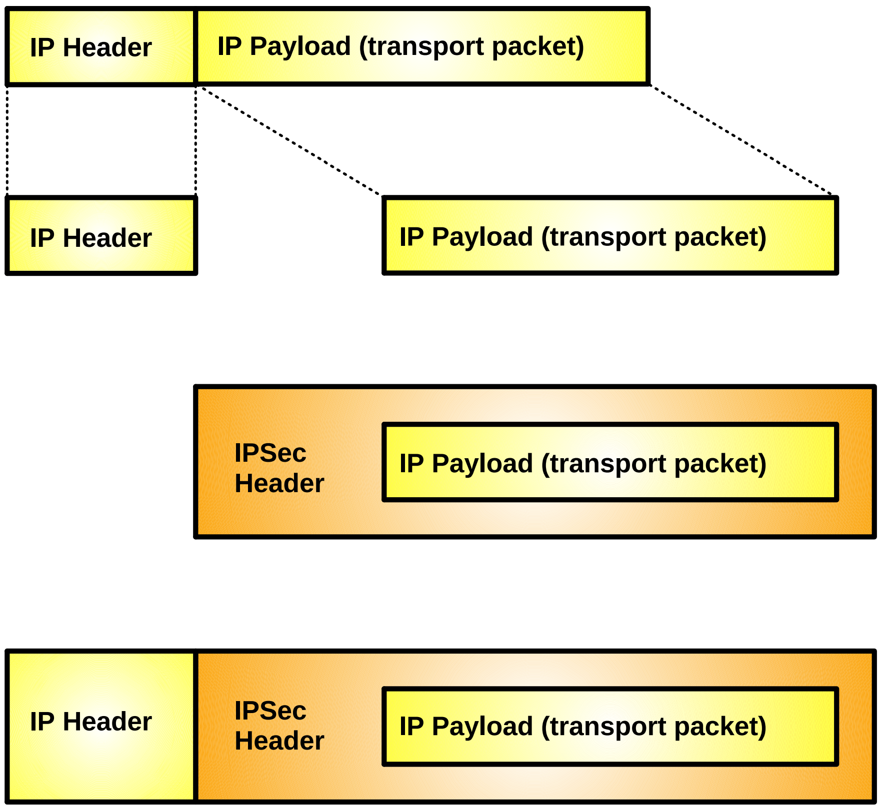
Creating an IPSec packet using transport mode

Original IP packet

Separate IP header and transport packet

Create IPSec packet

Attach and modify original IP header to IPSec packet



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

© 2007 IBM Corporation

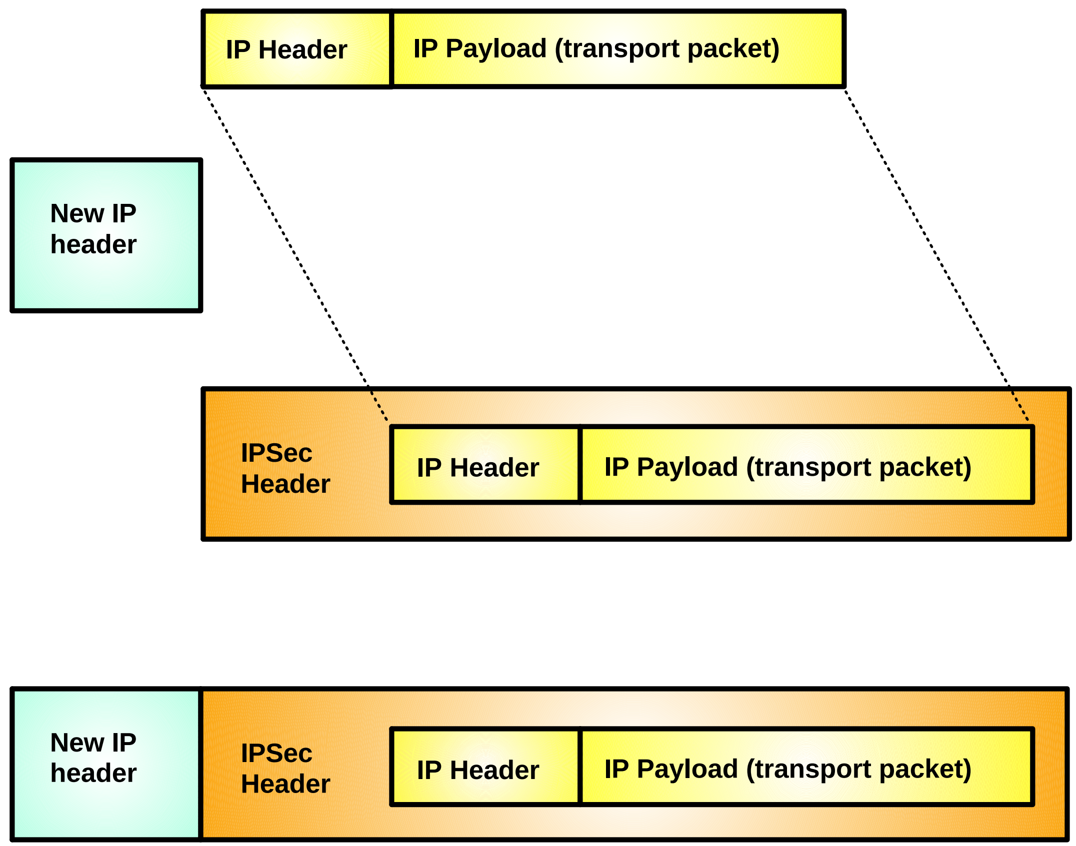
Creating an IPSec packet using tunnel mode

Original IP packet

Create new IP header

Create IPSec packet

Update and attach new IP header to IPSec packet

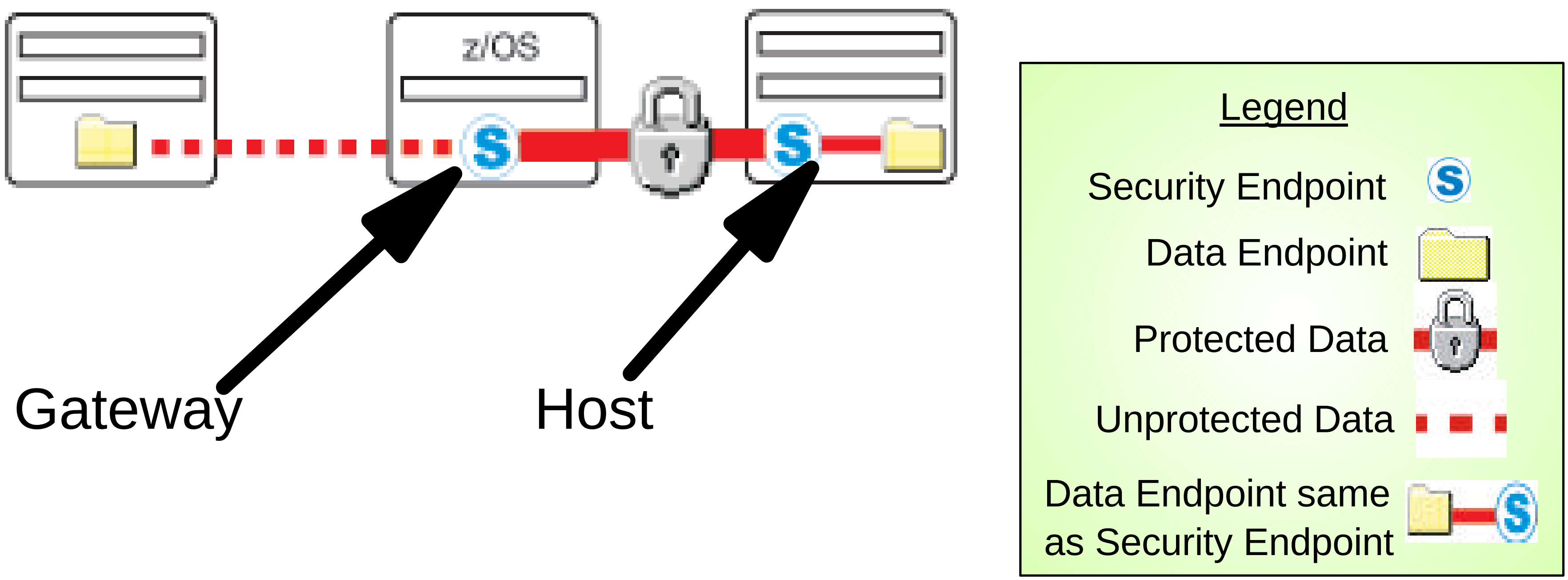


Tunnel mode is used if at least one of the two IPSec SA end-points is a gateway.

© 2007 IBM Corporation

Security endpoints

- **The endpoints of an IPSec security association**
  - Where IPSec protection is applied
- **Endpoint roles**
  - Host
    - Local data endpoint and IPSec security endpoint (SA) are the same IP address
  - Gateway
    - Local data endpoint and IPSec security endpoint (SA) are different IP addresses

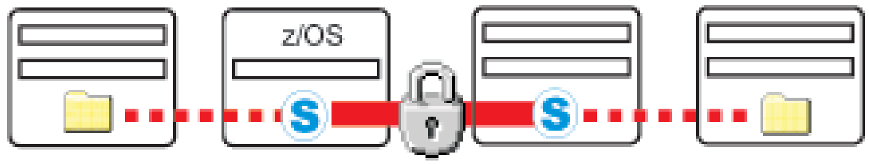


© 2007 IBM Corporation

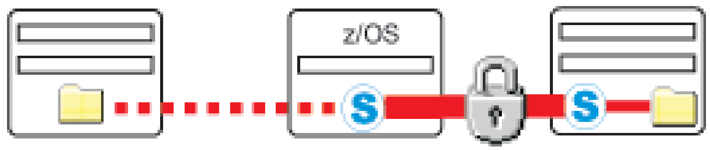
Encapsulation mode rules

- **Must use tunnel mode:**

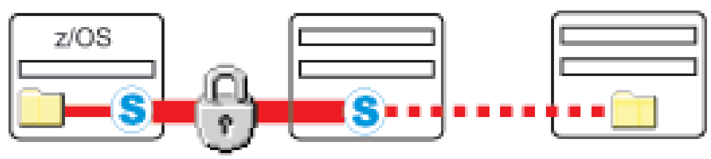
Gateway to Gateway



Gateway to Host

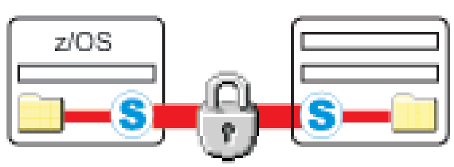


Host to Gateway



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

Host to Host



Legend

Security Endpoint

Data Endpoint

Protected Data

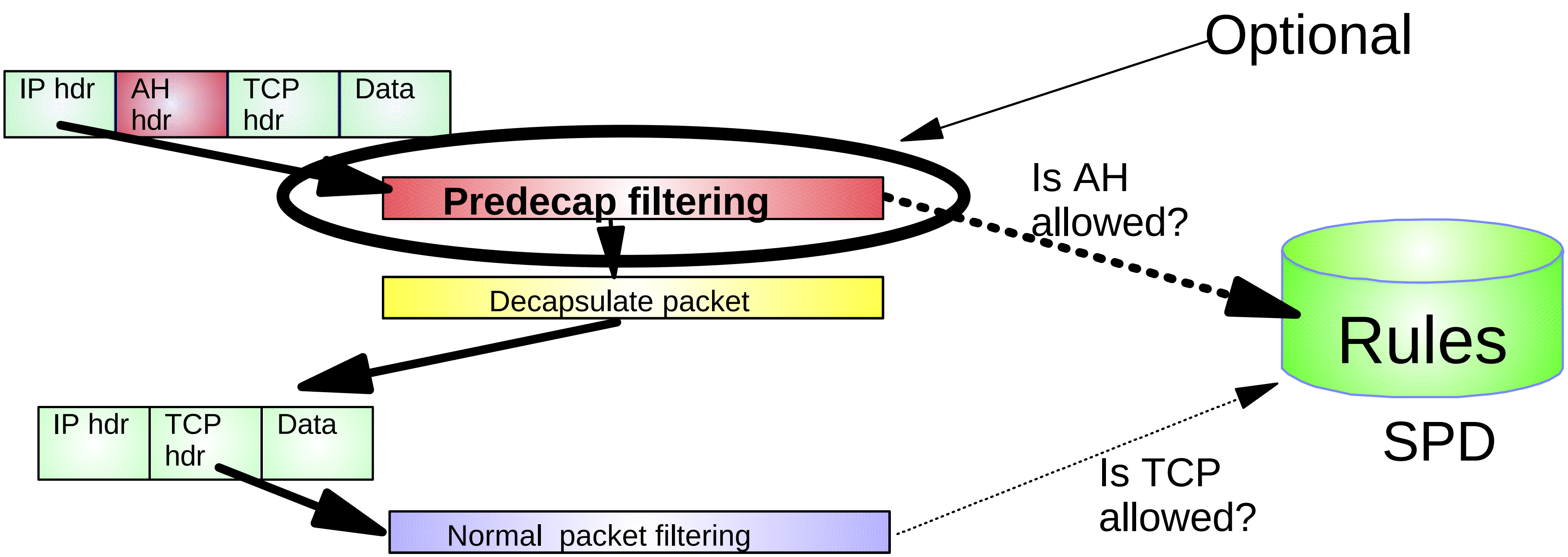
Unprotected Data

Data Endpoint same as Security Endpoint

© 2007 IBM Corporation

Predecap filtering

- IPSec protected traffic arrives as an AH or ESP packet (UDP-encapsulated ESP packets are interpreted as ESP packets; see charts on UDP-encapsulation)
- The stack can optionally perform filtering on AH/ESP packets before decapsulation
  - Known as predecap filtering
  - Prevents decapsulation of AH/ESP traffic from unacceptable sources
- The AH/ESP packet is then decapsulated revealing the original packet
  - Filtering is always performed on the decapsulated packet



© 2007 IBM Corporation

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
      - DES, Triple DES, AES, Null
    - Authentication Algorithm
      - HMAC_MD5 or HMAC_SHA
  - Cryptographic keys
  - Encapsulation mode
    - tunnel
    - transport
  - Lifetime/lifesize (for dynamic SAs)
- **This agreement is known as a "security association"**

© 2007 IBM Corporation

More about IPSec security associations (SAs)

- **Used to protect IP traffic**

- **Unidirectional**
  - Need one for inbound and another for outbound - each IPSec secure channel endpoint consists of two SAs
    - Generally symmetrical with regards to algorithms used
    - Cryptographic keys will be different
  - A pair of matching SAs are, on z/OS, referred to by a "Tunnel ID" - in a sense identifying the secure channel

- **An SA is identified by:**
  - A Security Parameter Index (SPI)
    - The SPI is a 32 bit value
    - SPI numbers in themselves may not be unique on a given IPSec node
    - The SPI is carried in the IPSec headers
  - IPSec protocol
  - Destination IP address information

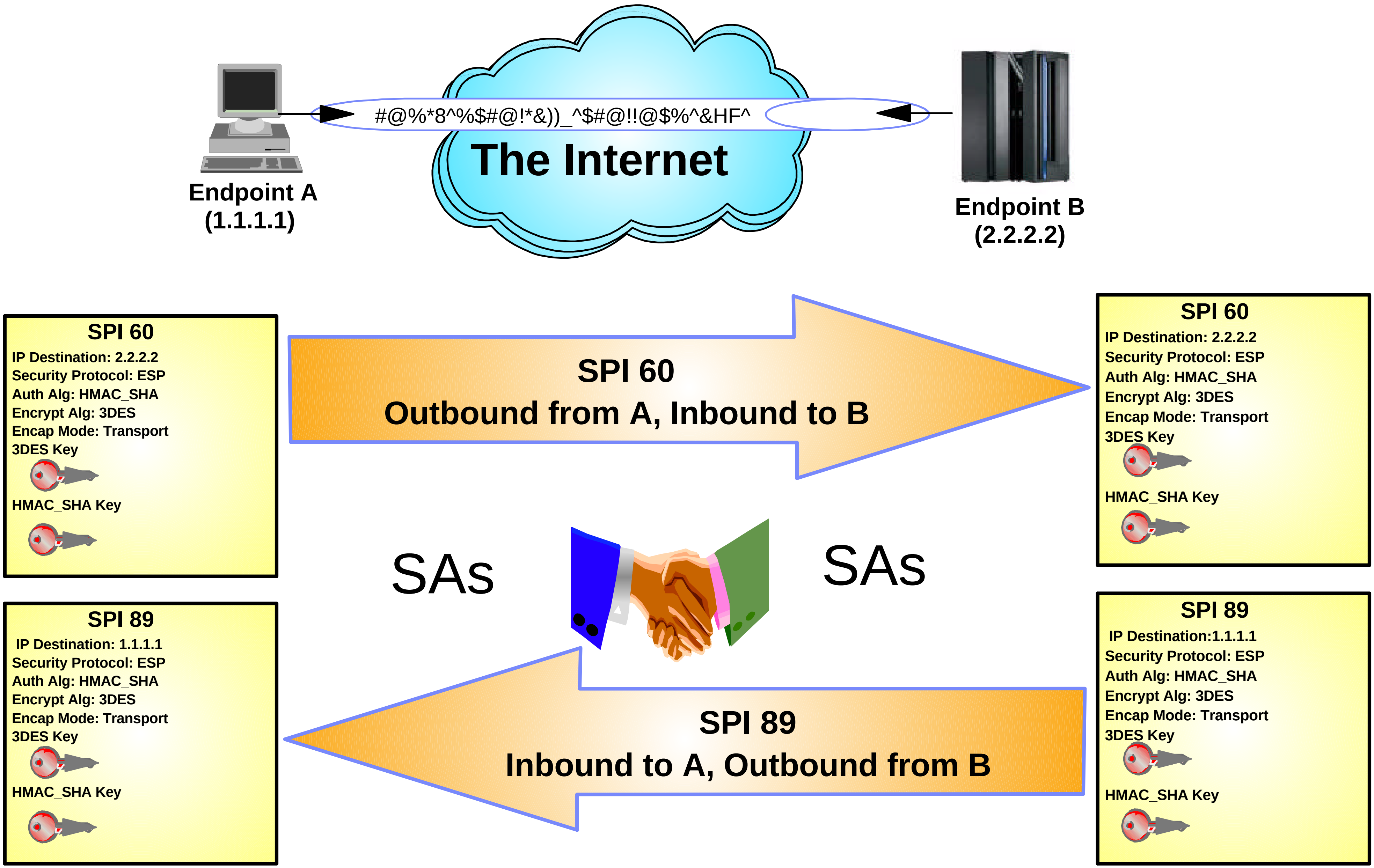
- **Manually defined SAs**
  - Statically defined in the SPD (Pagent IPSec config file)

- **Dynamically defined SAs**
  - Negotiated using the Internet Key Exchange protocol
  - Acceptable values (policy) defined in the SPD (Pagent IPSec config file)

- **Security Association Database (SAD)**
  - The collection of all SAs known to the stack

© 2007 IBM Corporation

IPSec security association example



© 2007 IBM Corporation

Manually defined SAs

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

- **Defined in a Pagent 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

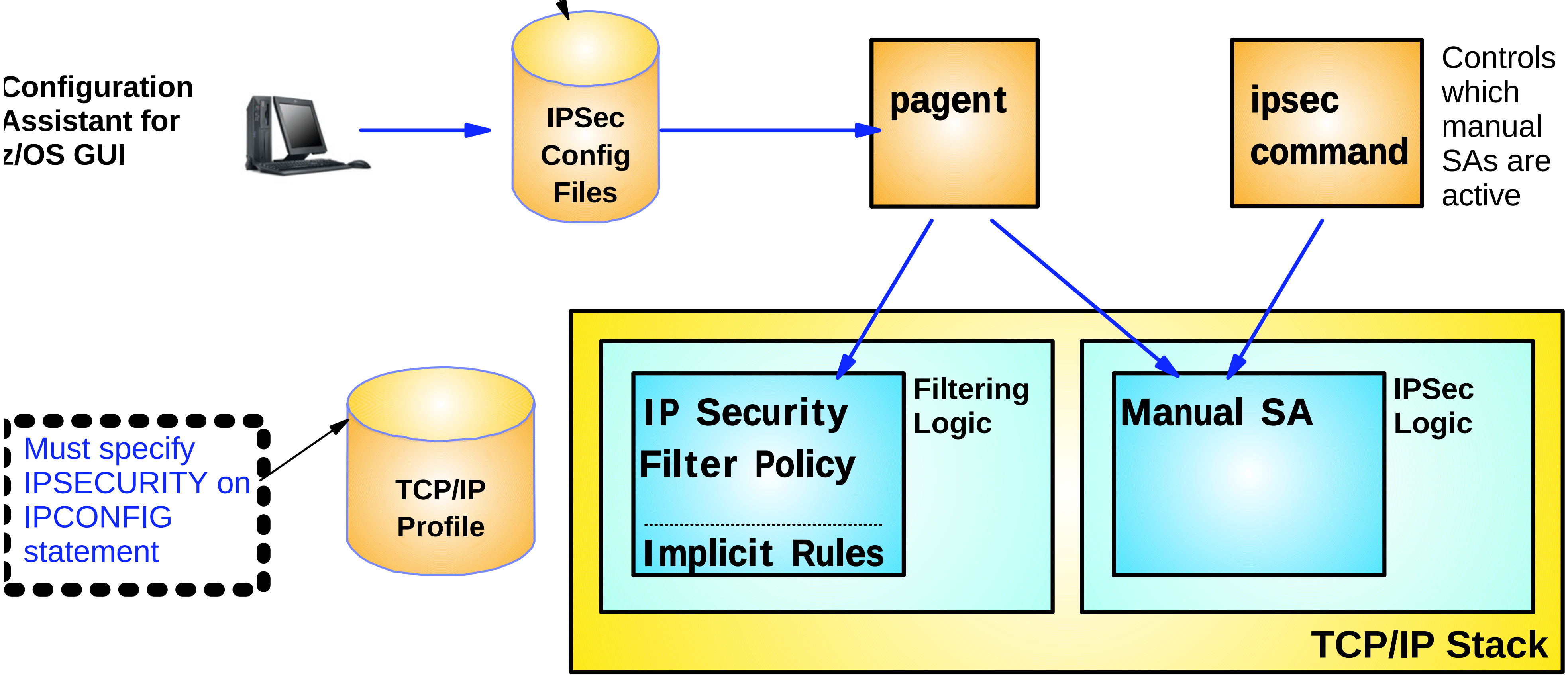
- **Use ipsec command activate/deactivate manual SAs**
  - ➤ Can also be automatically activated when policy is installed

- **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 (physical mail/courier service)
  - ➤ 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.

© 2007 IBM Corporation

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.



© 2007 IBM Corporation

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 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 each potential IKE partner
      - This key is not directly used to encrypt data.
    - Often used during the initial stages of dynamic SA deployment
  - RSA 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 for the IKE peer
    - Often used during the initial stages of dynamic SA deployment

© 2007 IBM Corporation

The IKE Daemon

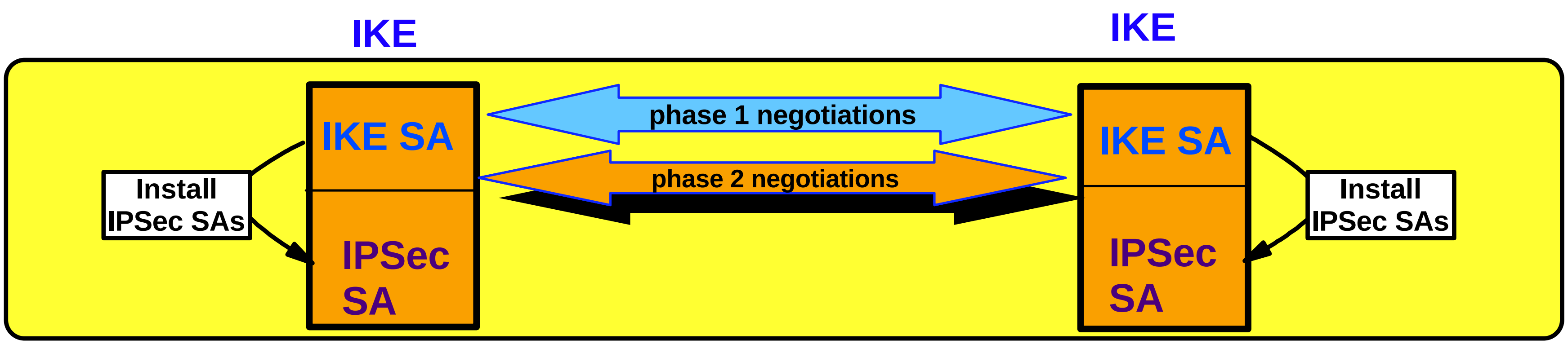
- **The IKE deamon implements the Internet Key Exchange protocol**
  - Defined in RFC 2409
  - A two phase approach to negotiating dynamic IPSec SAs
- **The IKE daemon obtains its policy from Pagent**
  - Policy information for negotiating IPSec SAs
    - Dynamic VPN actions
  - Policy for creating a 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

© 2007 IBM Corporation

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



© 2007 IBM Corporation

IKE Phase 1 SAs

- Used to protect Phase 2 negotiations
- Bidirectional
- Endpoints must agree on
  - Encryption algorithm
    - AES / Triple DES / DES
  - Hash Algorithm
    - MD5 / SHA1
  - Authentication Method
    - Preshared Key
    - RSA Signature
  - Diffie-Hellman Group
  - Lifetime/Lifesize
- Policy definition is based on identities exchanged during phase 1
  - Key Exchange Policy
    - A set of filter rules for IKE

© 2007 IBM Corporation

More info about Phase 1 SAs

- There are two different phase 1 exchange modes. Both exchange the same information, but one utilizes fewer messages.
  - ➢ Main Mode
    - – All IPSec implementations must support Main Mode. Main mode utilizes 6 messages. The last two messages contain identity information and are encrypted. This provides identity protection.
  - ➢ Aggressive Mode
    - – Some IPSec implementations do not support Aggressive mode. Aggressive mode utilizes 3 messages. No messages are encrypted.
- Identity information is used to locate policy.
  - ➢ Phase 1 identity types supported include:
    - – An IPv4 address (this identity type should not be used when behind a NAT)
    - – RFC 822 name (i.e. email address)
    - – Fully qualified Domain Name (FQDN)
    - – x500 Distinguished Name (DN)
- Diffie-Hellman is an algorithm that allows IKE to produce cryptographic keying material. Diffie-Hellman groups are defined in RFC 2409 (IKE).
  - ➢ Original options are groups 1 and 2.
  - ➢ Group 2 provides better security characteristics, but is also requires more computational power.
  - ➢ Groups 5 and 14 are new for use with AES.

© 2007 IBM Corporation

Perfect forward secrecy (PFS)

- Perfect Forward Secrecy
  - ➤ Refers to the notion that the compromise of a single key will only permit access to data protected by that key
    - – Compromise of the keys negotiated in phase 1 will not compromise keys generated in phase 2
    - – Compromise of the keys negotiated in phase 2 will not compromise future phase 2 keys or previously generated phase 2 keys
- PFS is optional
  - ➤ Accomplished by performing an optional Diffie-Hellman exchange during phase 2
    - – The Diffie-Hellman exchange during Phase 1 SA is not optional
- Factors to consider
  - ➤ Frequency that IKE SAs are refreshed (Phase 1)
  - ➤ Frequency that IPSec SAs are refreshed (Phase 2)
  - ➤ Key size

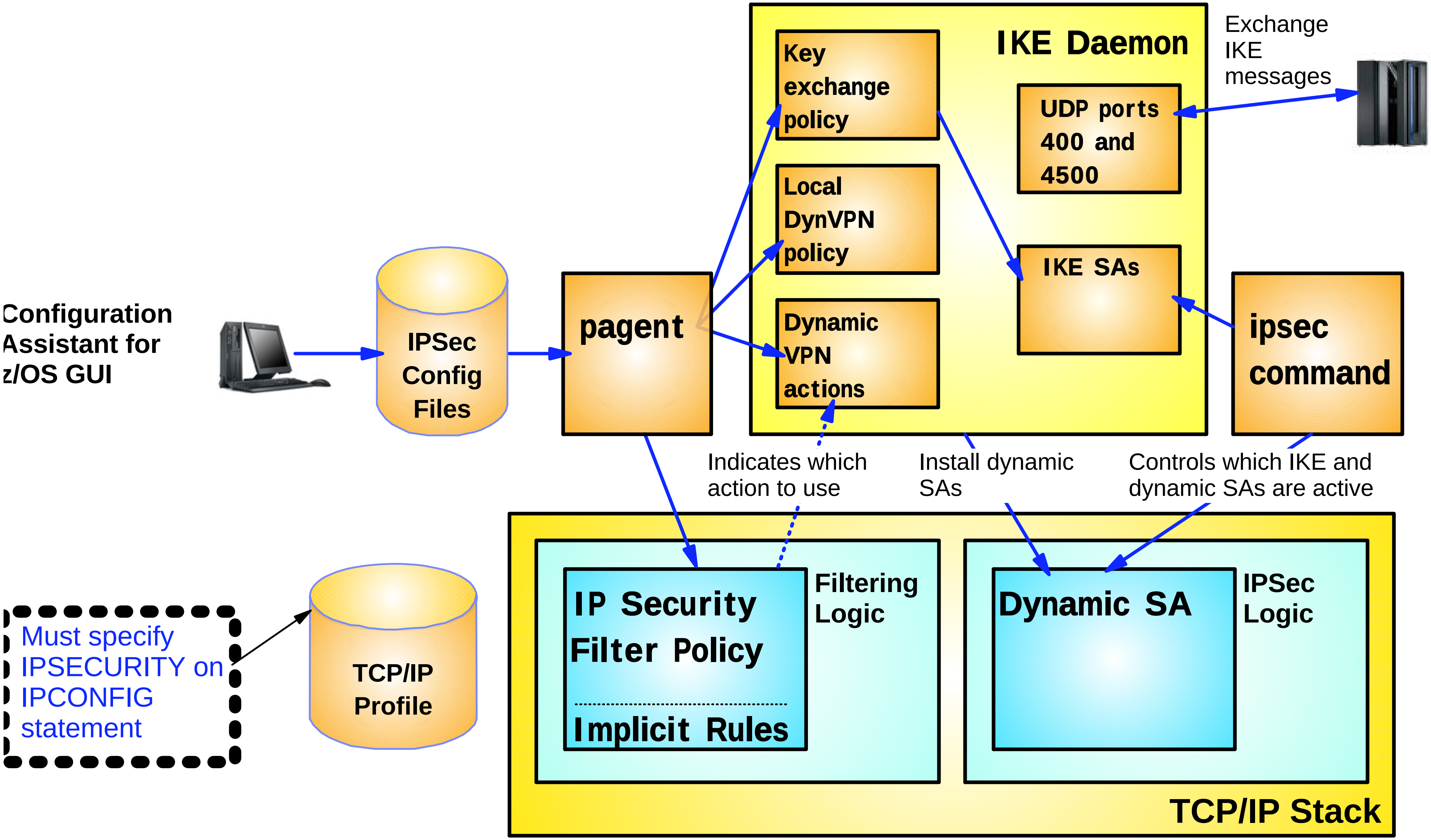
© 2007 IBM Corporation

Dynamic SA activation methods

- 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:

© 2007 IBM Corporation

IP Security dynamic SAs overview



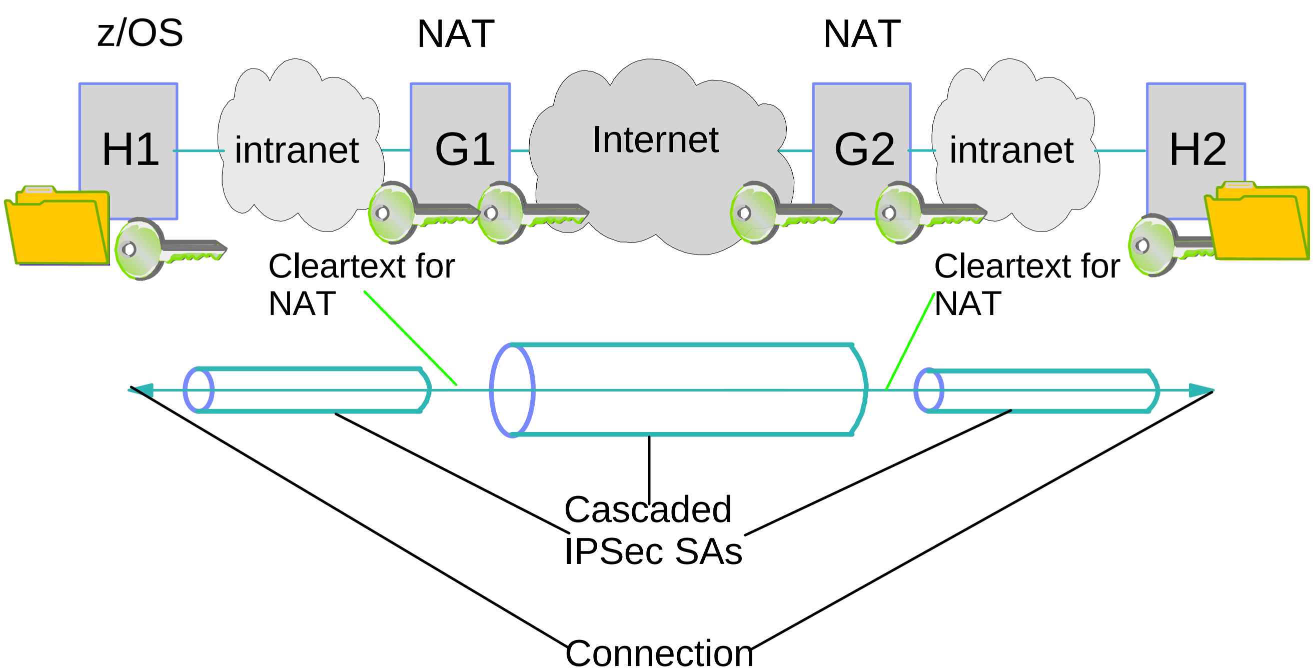
© 2007 IBM Corporation

IPSec and NAT traversal

© 2007 IBM Corporation

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 historically have not been compatible
  - IPSec SA could not traverse NAT/NAPT device
  - Forced configuration where multiple SAs required to make end-to-end connection
    - Cascaded SAs

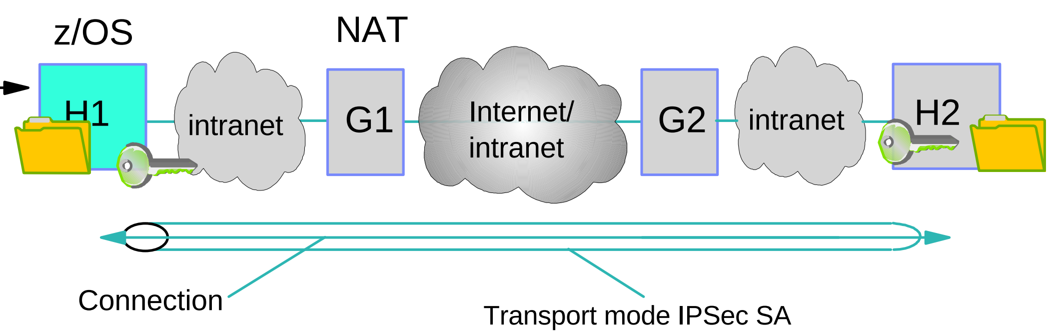


© 2007 IBM Corporation

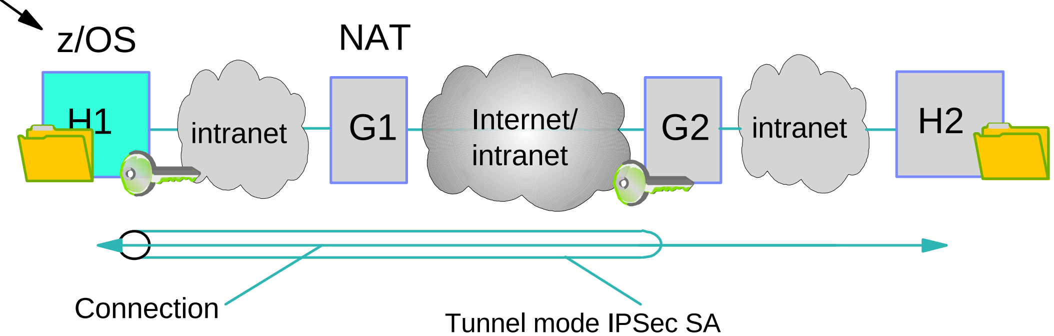
The IPSec NAT Traversal Solution

- New 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
    - supported in V1R7
  - NAPT
    - supported in V1R8

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



Host-to-gateway: Protect segment of data path



© 2007 IBM Corporation

NAT traversal - UDP encapsulation

- Additional encapsulation modes used when a NAT is traversed
  - UDP-encapsulated transport
  - UDP-encapsulated tunnel

- Only valid with ESP packets
  - Normal transport/tunnel mode encapsulation performed
  - Inserts an additional UDP header in front of the ESP header

- Allows ESP packets to traverse a NAT

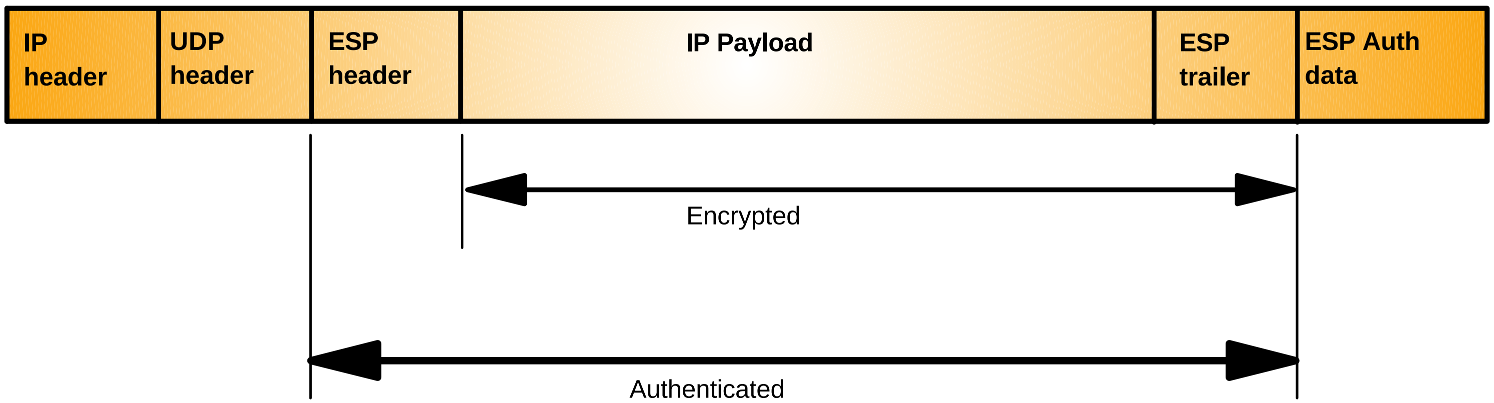
- On z/OS the decision to use UDP-encapsulation is made by the IKE daemon if a NAT is detected

- NAT traversal support can be enabled or disabled in IP Security policy

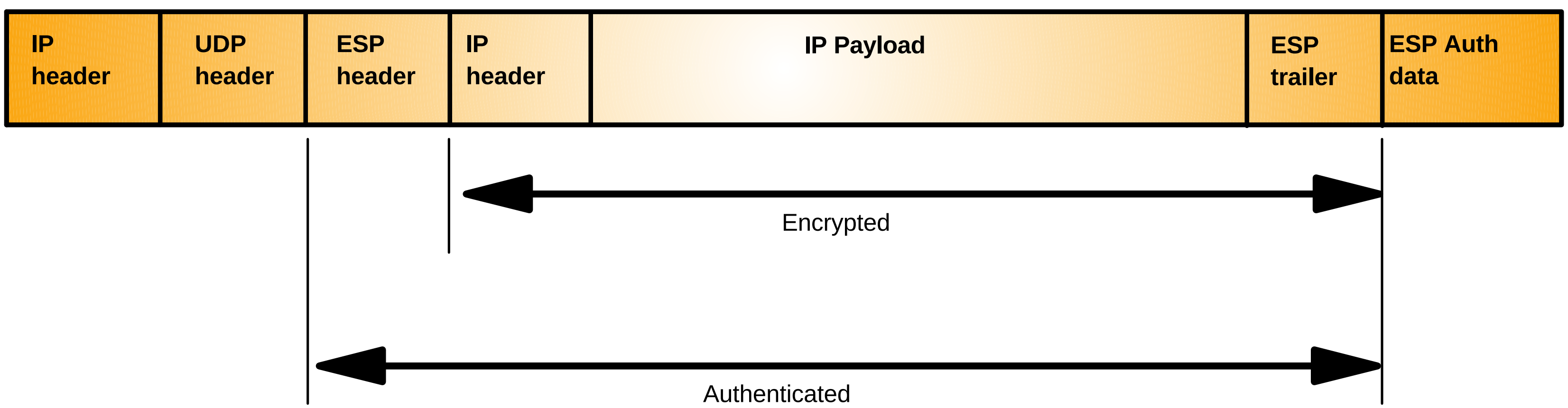
© 2007 IBM Corporation

NAT traversal - UDP-encapsulated packets

- **Below shows the format of a UDP-encapsulated transport mode packet**



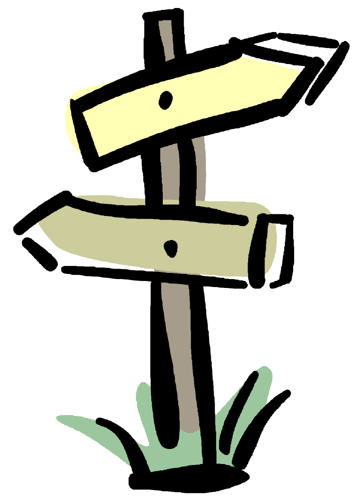
- **Below shows the format of a UDP-encapsulated tunnel mode packet**



© 2007 IBM Corporation

z/OS Communications Server IP security agenda

- Part 1 - Session 3914
  - ➤ Introduction to IP security on z/OS
  - ➤ IP filtering
  - ➤ IPSec
- Part 2 - Session 3907
  - ➤ Configuring and enabling IP Security
  - ➤ IP security displays and controls



© 2007 IBM Corporation

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)

© 2007 IBM Corporation