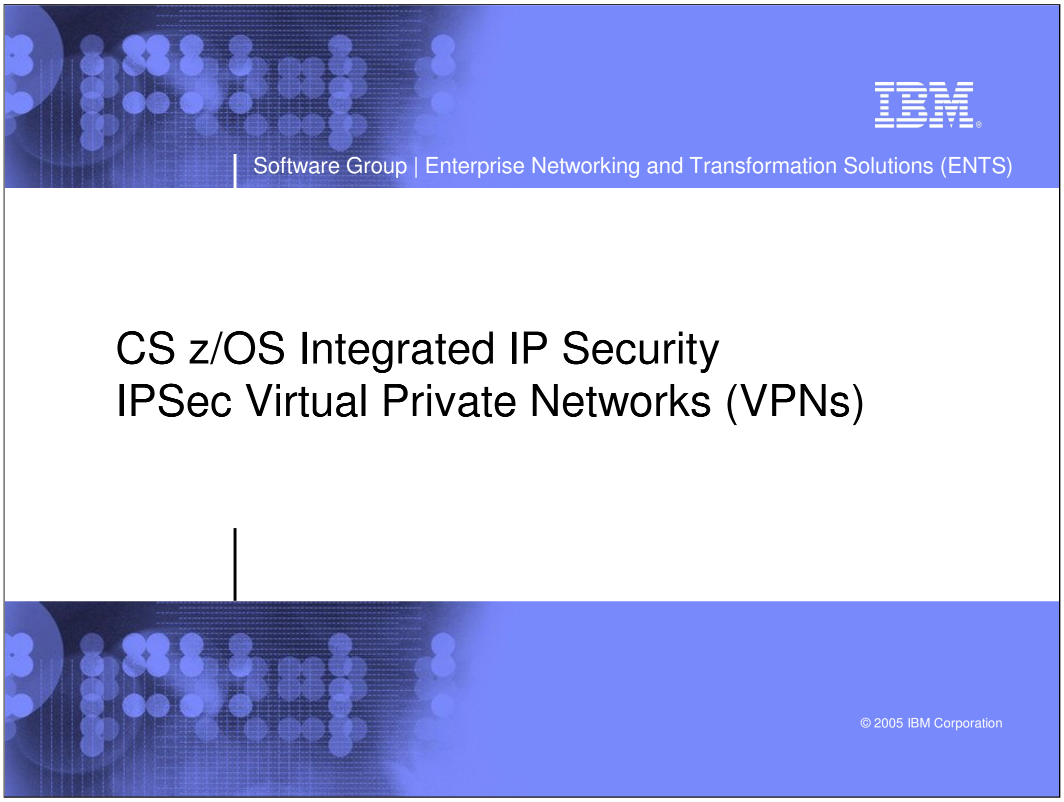
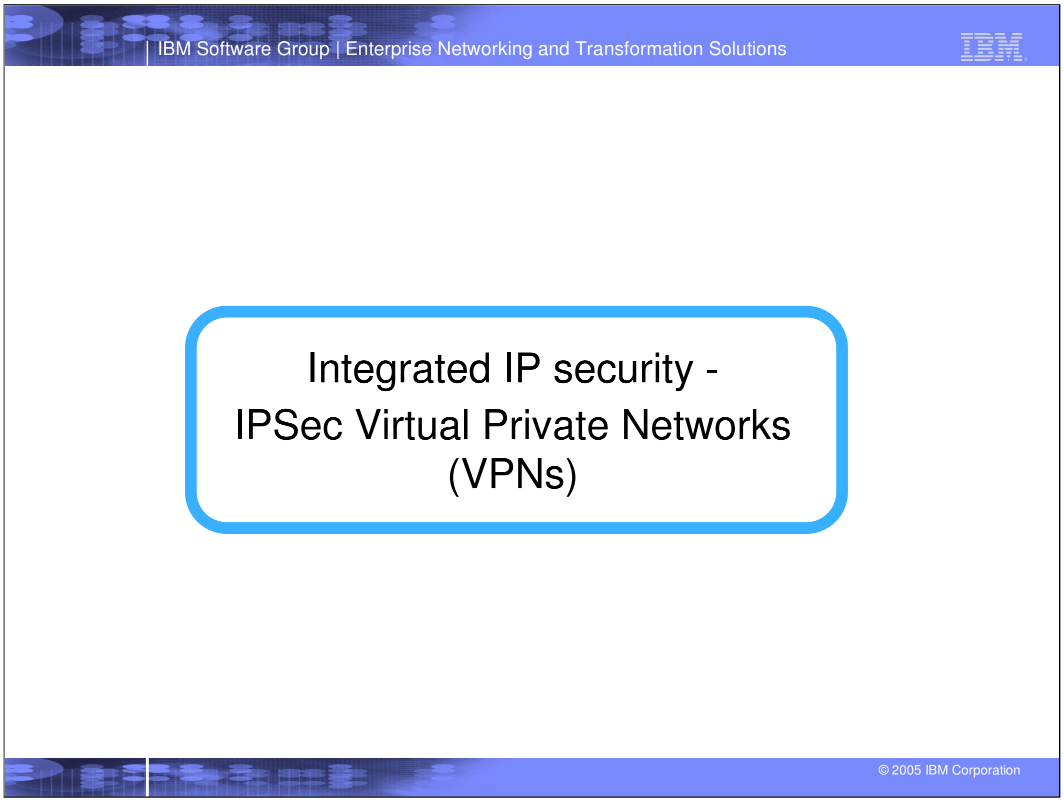


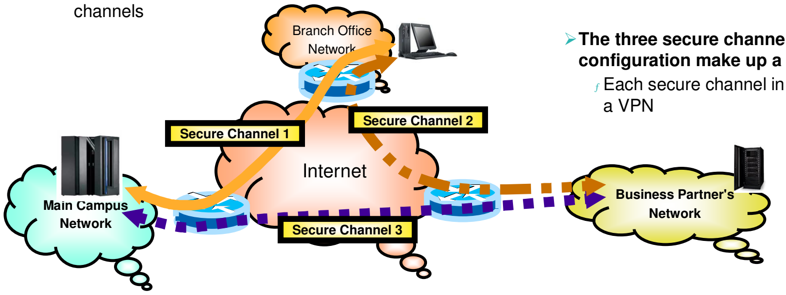
CS z/OS Integrated IP Security
IPSec Virtual Private Networks (VPNs)



Integrated IP security - IPSec Virtual Private Networks (VPNs)

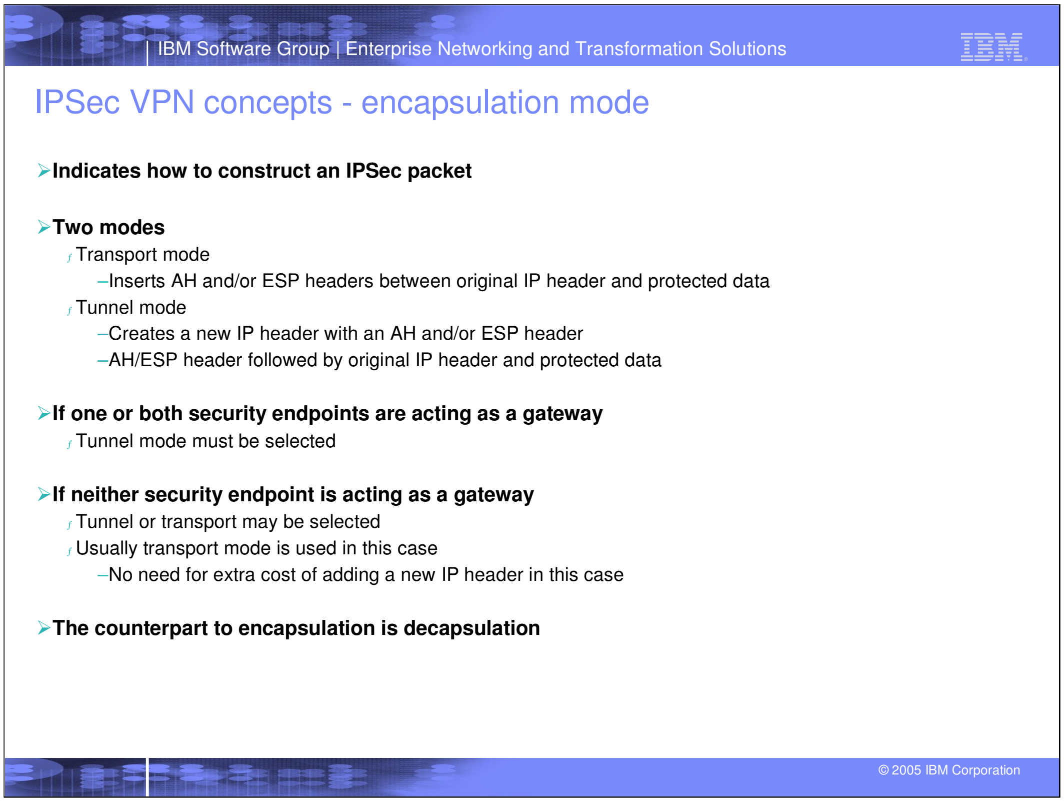
IPSec Virtual Private Network (VPN) overview

- **Virtual Private Network**
  - Logical network of connected nodes that communicate over unsecure networks using one or more secure channels



- **The three secure channels in this sample configuration make up a VPN**
  - Each secure channel in itself can be considered a VPN

- **A secure channel is commonly called an IPSec security association (SA) and uses authentication and/or encryption**
  - The term "tunnel" is also sometimes used in this context, but it is ambiguous and can be confused with tunnel vs. transport mode
- **A secure channel provides point-to-point security**
- **Integrated IPSec utilizes IP security protocols defined by the IPSec working group**
  - RFC 2402 - IP Authentication Header (AH) protocol
    - Data authentication
    - IP header authentication
    - Data origin authentication
  - RFC 2406 - IP Encapsulating Security Payload (ESP)
    - Data authentication
    - Data origin authentication
    - Data privacy



IPSec VPN concepts - encapsulation mode

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

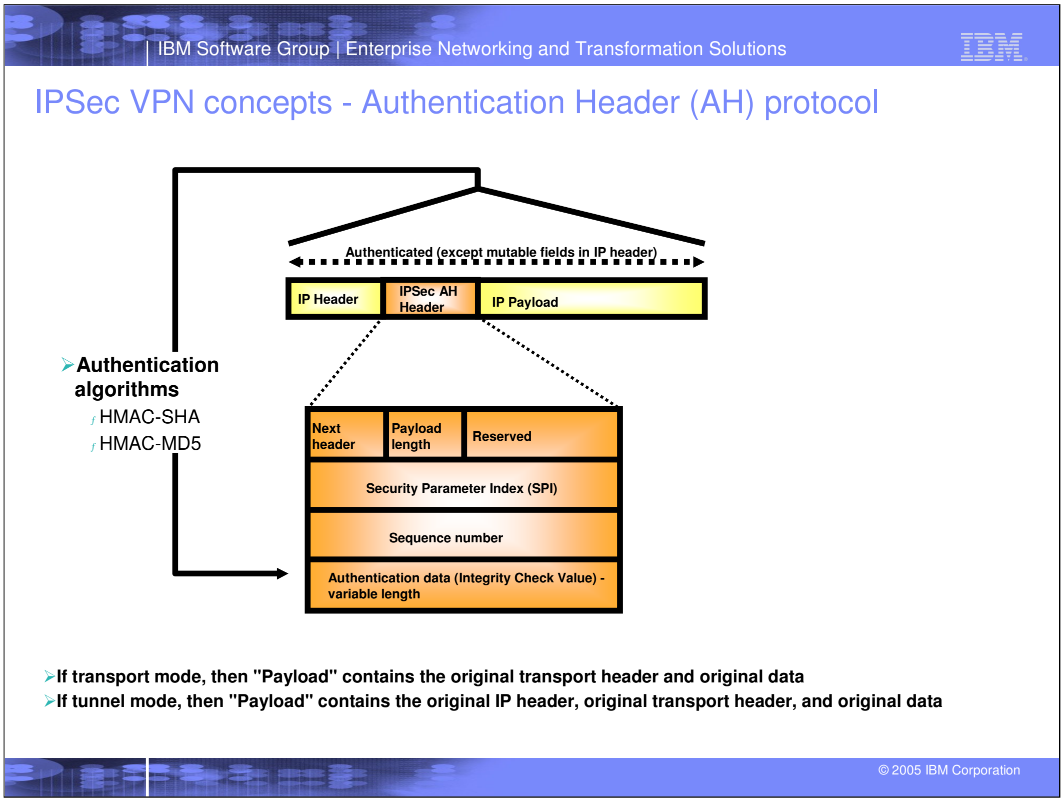
- **Two modes**
  - Transport mode
    - Inserts AH and/or ESP headers between original IP header and protected data
  - Tunnel mode
    - Creates a new IP header with an AH and/or ESP header
    - AH/ESP header followed by original IP header and protected data

- **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**

IPSec VPN concepts - Authentication Header (AH) protocol



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

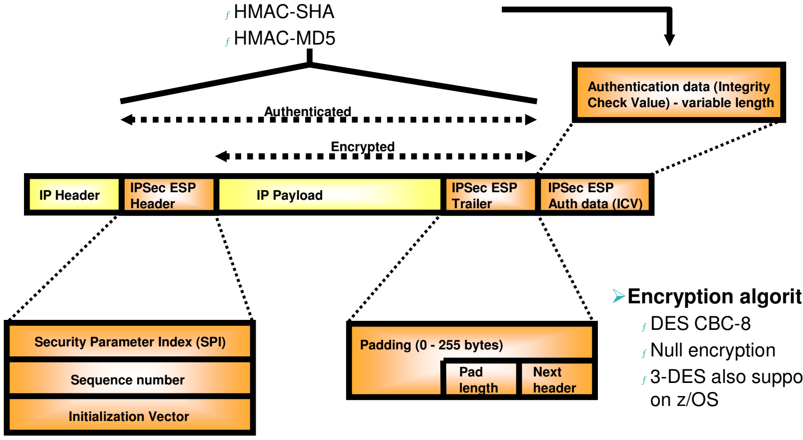
Authentication data (Integrity Check Value) - variable length

- **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**

IPSec VPN concepts - Encapsulating Security Payload (ESP) protocol

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



Authentication data (Integrity Check Value) - variable length

Authenticated

Encrypted

IP Header

IPSec ESP Header

IP Payload

IPSec ESP Trailer

IPSec ESP Auth data (ICV)

Security Parameter Index (SPI)

Sequence number

Initialization Vector

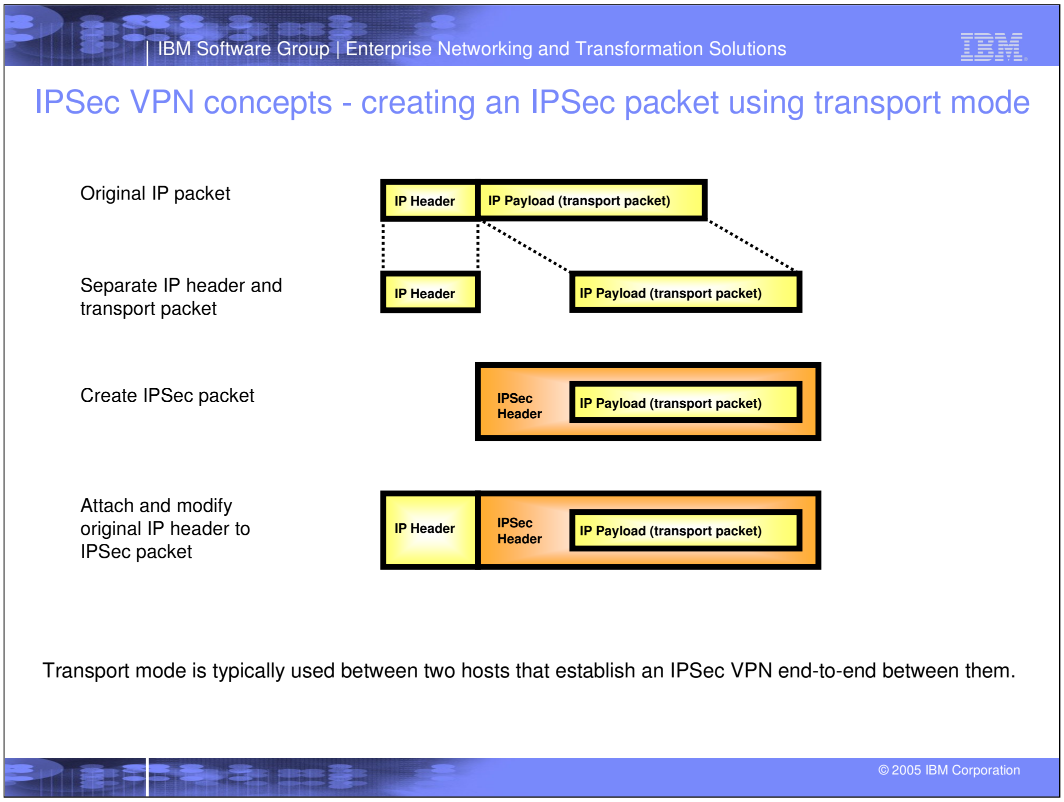
Padding (0 - 255 bytes)

Pad length

Next header

- **Encryption algorithms**
  - DES CBC-8
  - Null encryption
  - 3-DES also supported on z/OS

- **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 VPN concepts - creating an IPSec packet using transport mode

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)

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

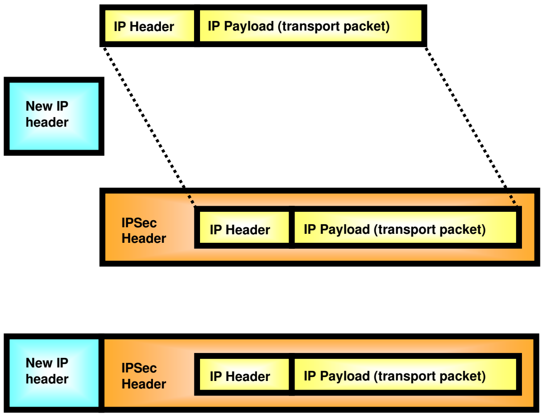
IPSec VPN concepts - creating an IPSec packet using tunnel mode

Original IP packet

Create new IP header

Create IPSec packet

Update and attach new IP header to IPSec packet

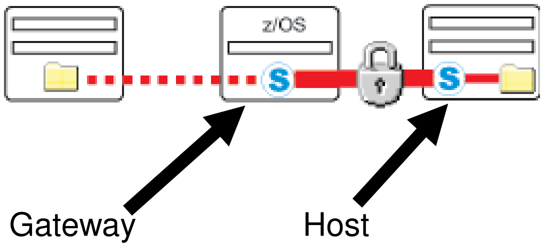

IP Header
IP Payload (transport packet)
New IP header
IPSec Header
IP Header
IP Payload (transport packet)
New IP header
IPSec Header
IP Header
IP Payload (transport packet)

Tunnel mode is used if at least one of the two IPSec VPN endpoints is a gateway.

IPsec VPN concepts - security endpoint

- **The endpoints of an IPSec secure channel**
  - Where IPSec protection is applied

- **Endpoint roles**
  - Host
    - Local data endpoint and secure channel endpoint are the same IP address
  - Gateway (or Security Gateway)
    - Local data endpoint and secure channel endpoint are different IP addresses



Legend

Security Endpoint	Ⓢ
Data Endpoint	🗀
Protected Data	🔒
Unprotected Data	▪ ▪ ▪
Data Endpoint same as Security Endpoint	🗀—Ⓢ

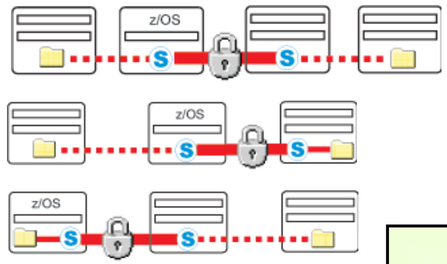
IPsec VPN concepts - encapsulation mode rules

- **Must use tunnel mode:**

Gateway to Gateway

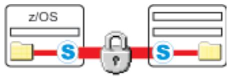
Gateway to Host

Host to Gateway



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

Host to Host



Legend

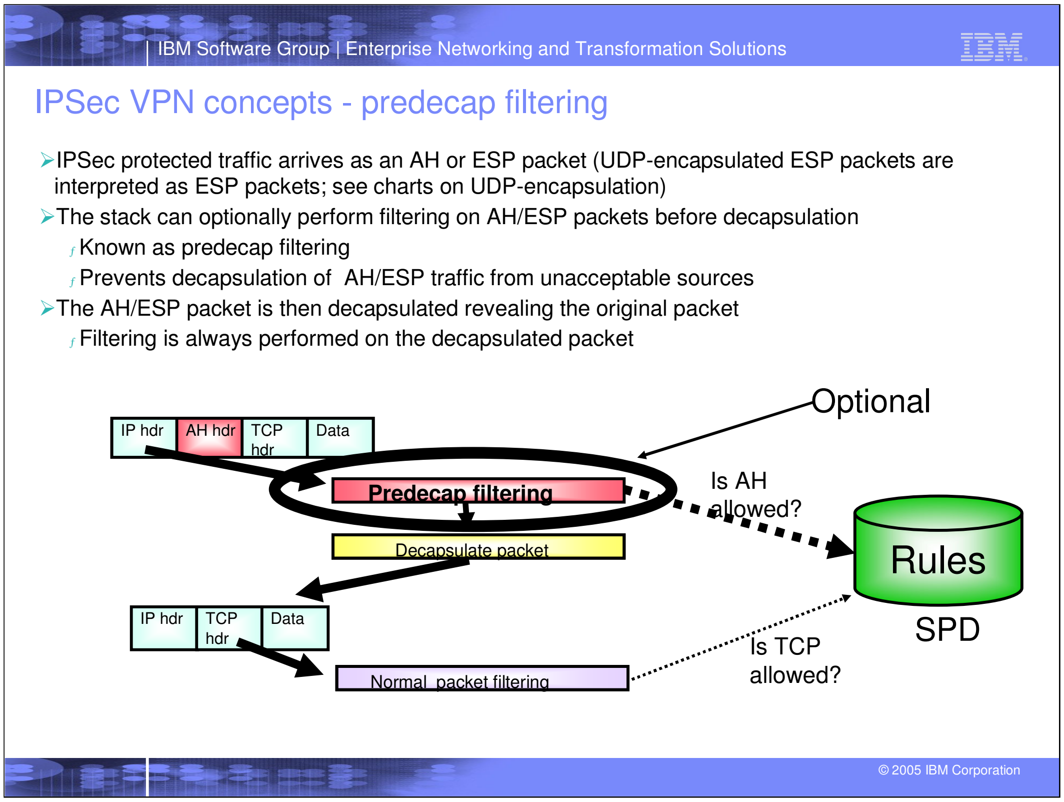
Security Endpoint Ⓢ

Data Endpoint 📁

Protected Data 🔒

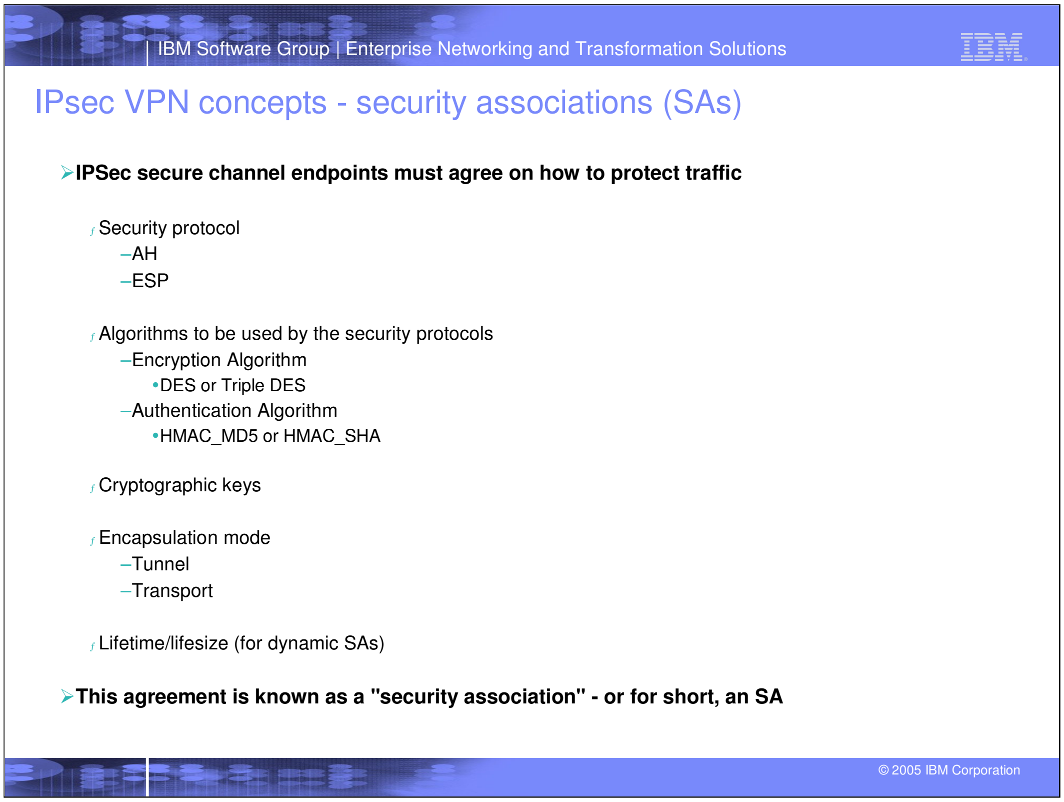
Unprotected Data ▪ ▪ ▪

Data Endpoint same as Security Endpoint 📁—Ⓢ



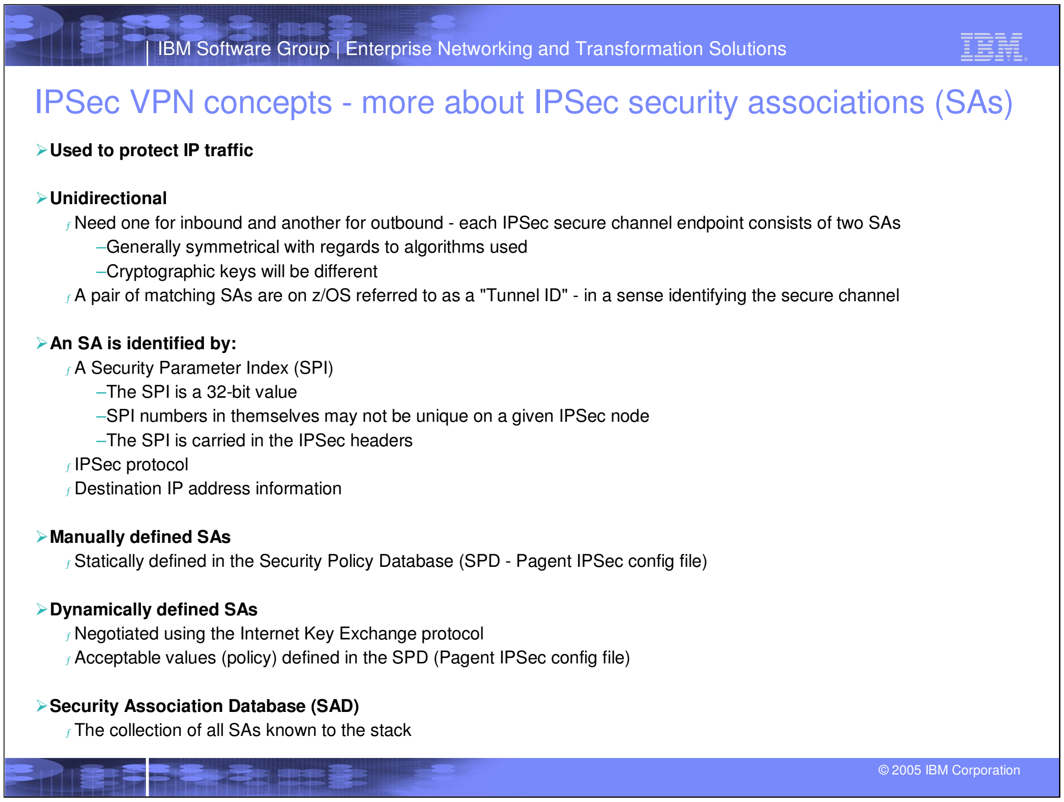
IPSec VPN concepts - predecap filtering

- 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



IPsec VPN concepts - security associations (SAs)

- **IPSec secure channel endpoints must agree on how to protect traffic**
  - Security protocol
    - AH
    - ESP
  - Algorithms to be used by the security protocols
    - Encryption Algorithm
      - DES or Triple DES
    - 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" - or for short, an SA**



IPSec VPN concepts - 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 as a "Tunnel ID" - in a sense identifying the secure channel

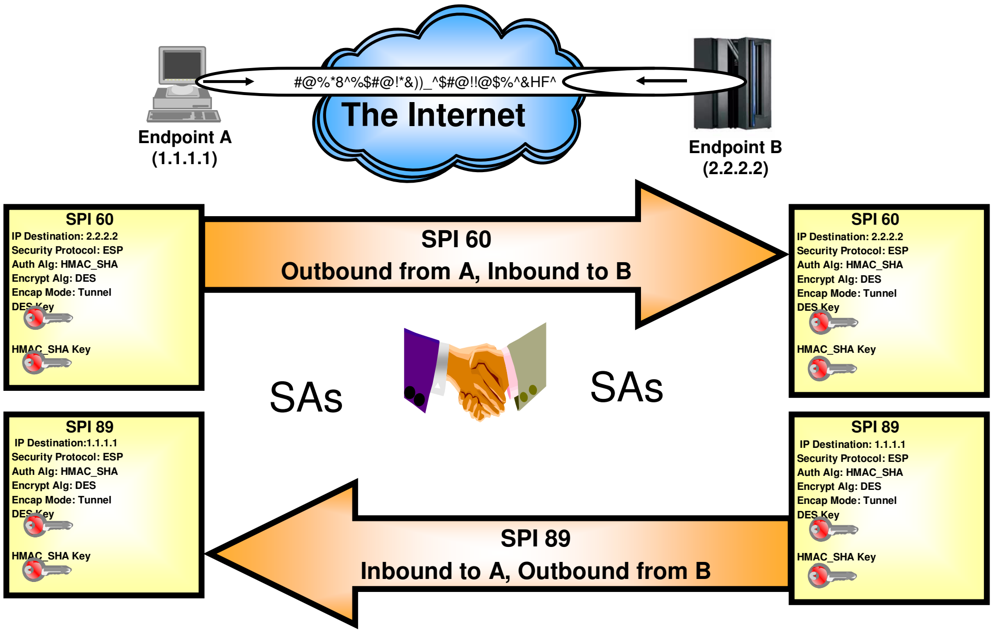
- **An SA is identified by:**
  - A Security Parameter Index (SPI)
    - The SPI is a 32-bit value
    - SPI numbers in themselves may not be unique on a given IPSec node
    - The SPI is carried in the IPSec headers
  - IPSec protocol
  - Destination IP address information

- **Manually defined SAs**
  - Statically defined in the Security Policy Database (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

IPSec VPN concepts - IPSec security association example



Endpoint A
(1.1.1.1)

#@%*8^%$#@!*&))_^$#@!!@$%^&HF^

The Internet

Endpoint B
(2.2.2.2)

SPI 60
IP Destination: 2.2.2.2
Security Protocol: ESP
Auth Alg: HMAC_SHA
Encrypt Alg: DES
Encap Mode: Tunnel
DES Key
HMAC_SHA Key

SPI 60
Outbound from A, Inbound to B

SPI 60
IP Destination: 2.2.2.2
Security Protocol: ESP
Auth Alg: HMAC_SHA
Encrypt Alg: DES
Encap Mode: Tunnel
DES Key
HMAC_SHA Key

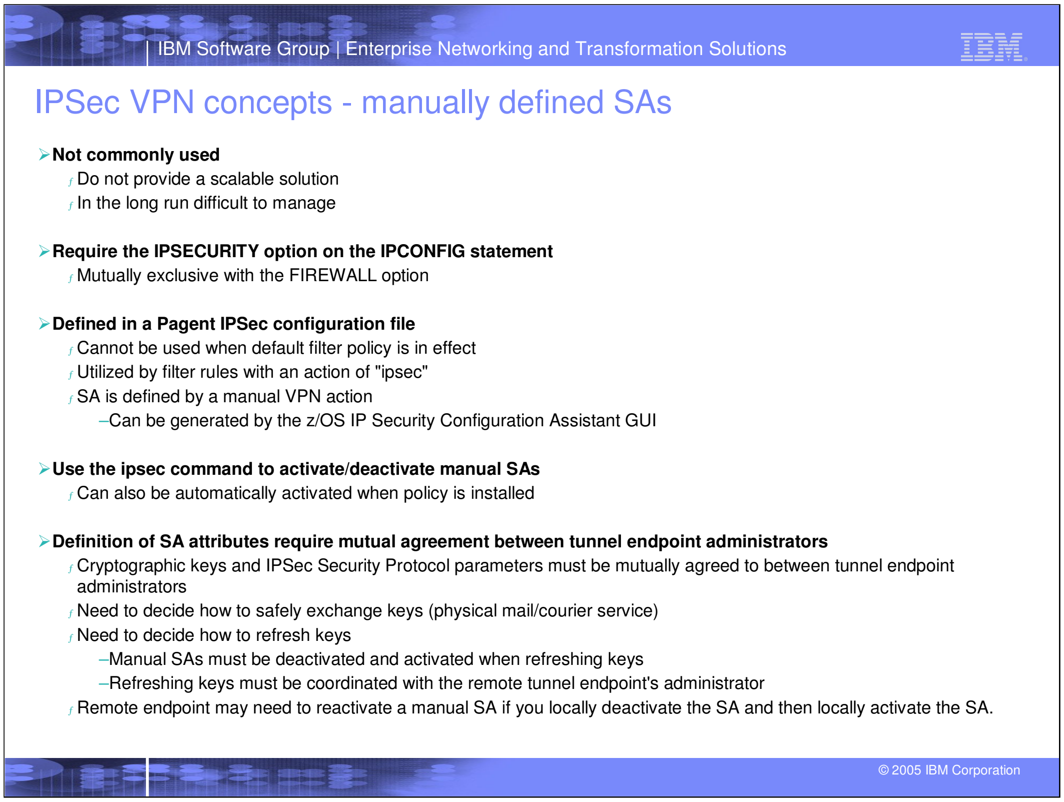
SAs

SAs

SPI 89
IP Destination:1.1.1.1
Security Protocol: ESP
Auth Alg: HMAC_SHA
Encrypt Alg: DES
Encap Mode: Tunnel
DES Key
HMAC_SHA Key

SPI 89
Inbound to A, Outbound from B

SPI 89
IP Destination: 1.1.1.1
Security Protocol: ESP
Auth Alg: HMAC_SHA
Encrypt Alg: DES
Encap Mode: Tunnel
DES Key
HMAC_SHA Key



IPSec VPN concepts - manually defined SAs

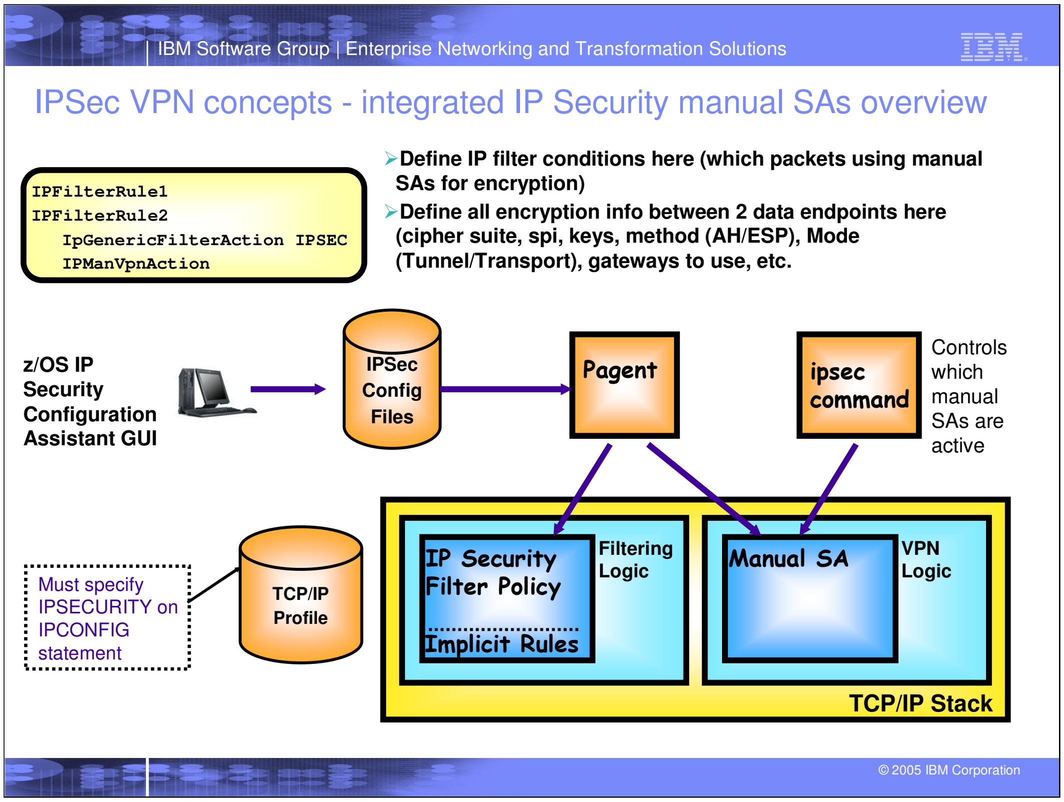
- ➢**Not commonly used**
  - ƒ Do not provide a scalable solution
  - ƒ In the long run difficult to manage

- ➢**Require the IPSECURITY option on the IPCONFIG statement**
  - ƒ Mutually exclusive with the FIREWALL option

- ➢**Defined in a Pagent IPSec configuration file**
  - ƒ Cannot be used when default filter policy is in effect
  - ƒ Utilized by filter rules with an action of "ipsec"
  - ƒ SA is defined by a manual VPN action
    - –Can be generated by the z/OS IP Security Configuration Assistant GUI

- ➢**Use the ipsec command to activate/deactivate manual SAs**
  - ƒ Can also be automatically activated when policy is installed

- ➢**Definition of SA attributes require mutual agreement between tunnel endpoint administrators**
  - ƒ Cryptographic keys and IPSec Security Protocol parameters must be mutually agreed to between tunnel endpoint administrators
  - ƒ Need to decide how to safely exchange keys (physical mail/courier service)
  - ƒ 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
  - ƒ Remote endpoint may need to reactivate a manual SA if you locally deactivate the SA and then locally activate the SA.



IPSec VPN concepts - integrated IP Security manual SAs overview

```
IPFilterRule1
IPFilterRule2
   IpGenericFilterAction IPSEC
   IPManVpnAction
```

- Define IP filter conditions here (which packets using manual SAs for encryption)
- Define all encryption info between 2 data endpoints here (cipher suite, spi, keys, method (AH/ESP), Mode (Tunnel/Transport), gateways to use, etc.

z/OS IP Security Configuration Assistant 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

Implicit Rules

Filtering Logic

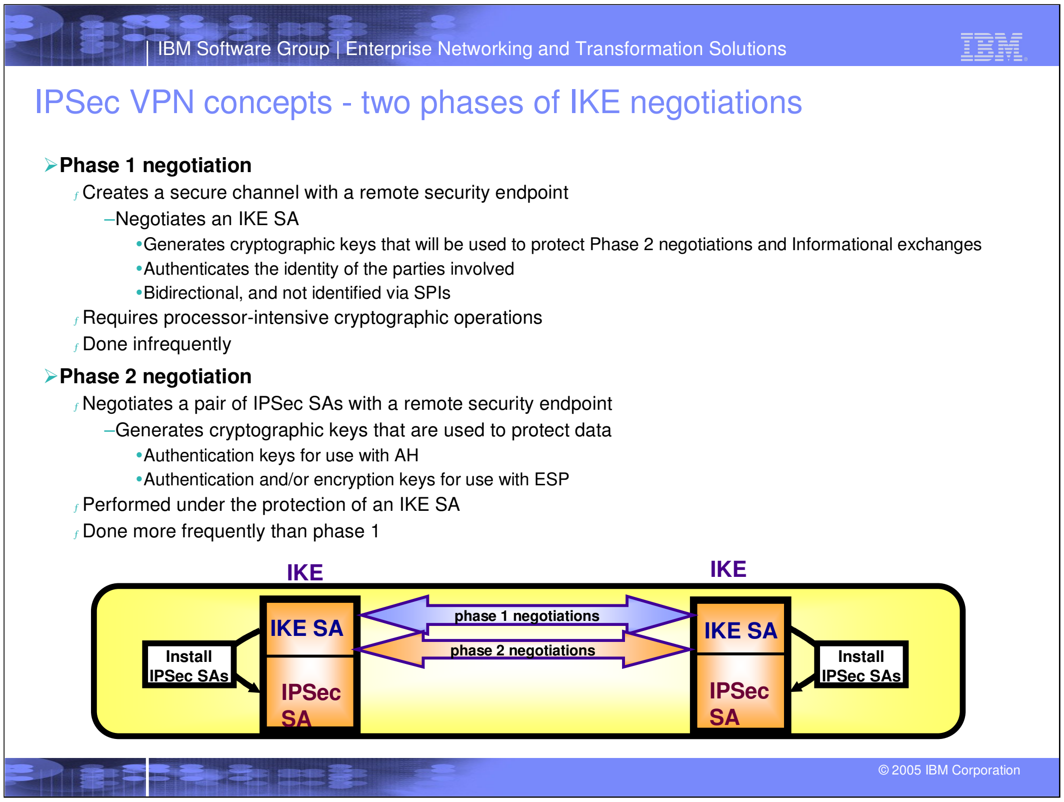
Manual SA

VPN Logic

TCP/IP Stack

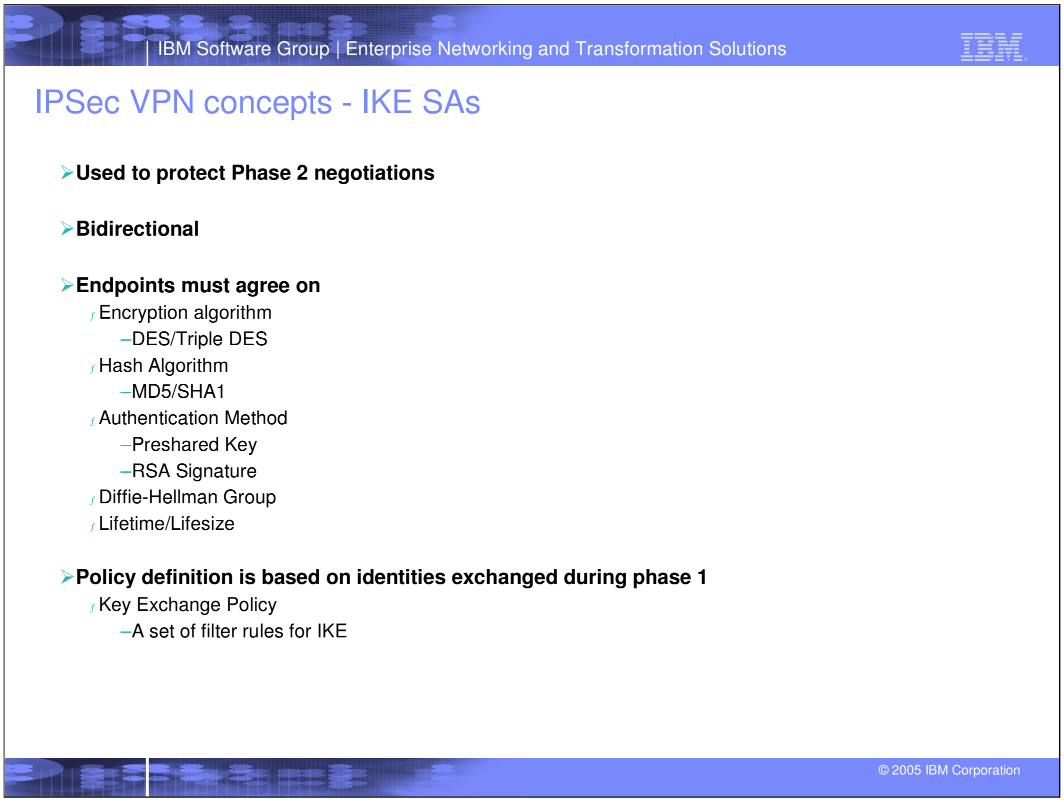
IPSec VPN concepts - dynamically defined SAs

- **Currently state of the art**
  - Scalable
  - Initially requires more configuration than a manual SA
  - In the long run easier to manage
    - Set and forget it
- **Require the IPSECURITY option on the IPCONFIG statement**
  - Mutually exclusive with the FIREWALL option
- **Cannot be used when default filter policy is in effect**
- **Dynamic SAs are negotiated by the IKE daemon**
- **Dynamic IPSec VPN policy defined in a Pagent IPSec configuration file**
  - Can be generated by the z/OS IP Security Configuration Assistant GUI
  - Dynamic IPSec VPN action identifies "acceptable" SA attributes
    - Utilized by filter rules with an action of "ipsec"
  - Key exchange policy defines how to protect dynamic SA negotiations
- **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 IPSec 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 IPSec VPN Policy
- **Utilizes UDP ports 500 and 4500 to communicate with remote security endpoints**
  - Negotiating SAs
  - Sending informational messages



IPSec VPN concepts - two phases of IKE negotiations

- **Phase 1 negotiation**
  - Creates a secure channel with a remote security endpoint
    - Negotiates an IKE SA
      - Generates cryptographic keys that will be used to protect Phase 2 negotiations and Informational exchanges
      - Authenticates the identity of the parties involved
      - Bidirectional, and not identified via SPIs
  - Requires processor-intensive cryptographic operations
  - Done infrequently
- **Phase 2 negotiation**
  - Negotiates a pair of IPSec SAs with a remote security endpoint
    - Generates cryptographic keys that are used to protect data
      - Authentication keys for use with AH
      - Authentication and/or encryption keys for use with ESP
  - Performed under the protection of an IKE SA
  - Done more frequently than phase 1



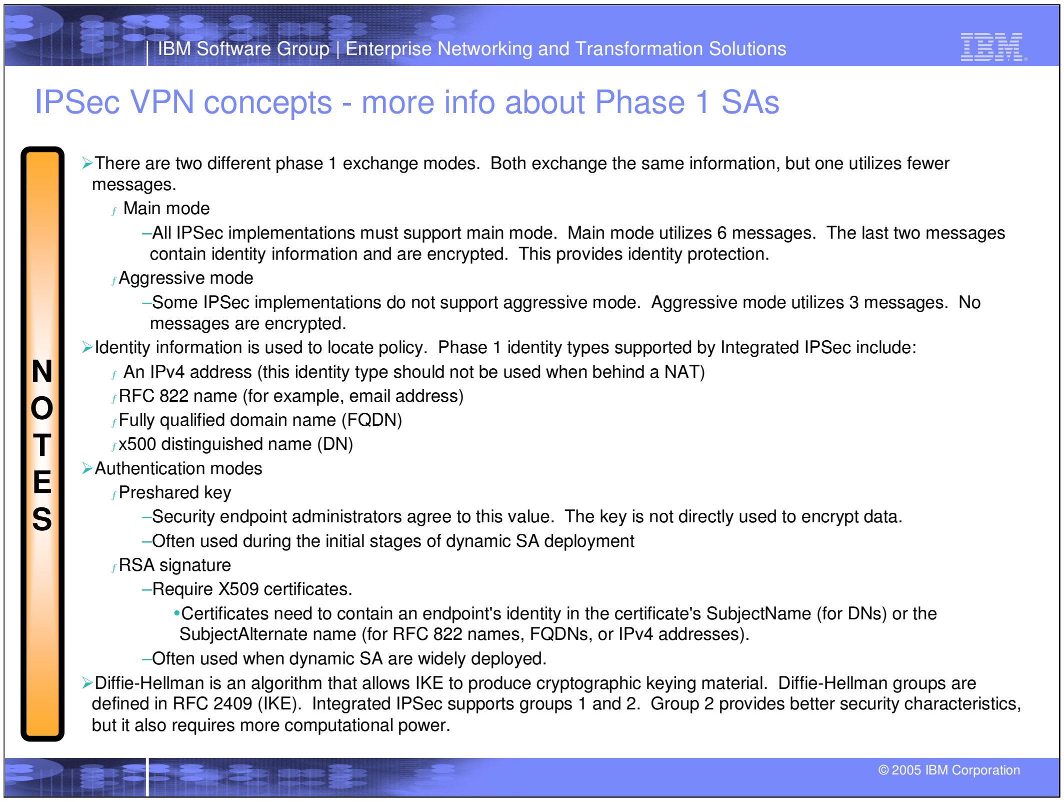
IPSec VPN concepts - IKE SAs

- **Used to protect Phase 2 negotiations**

- **Bidirectional**

- **Endpoints must agree on**
  - Encryption algorithm
    - DES/Triple DES
  - Hash Algorithm
    - MD5/SHA1
  - Authentication Method
    - Preshared Key
    - RSA Signature
  - Diffie-Hellman Group
  - Lifetime/Lifesize

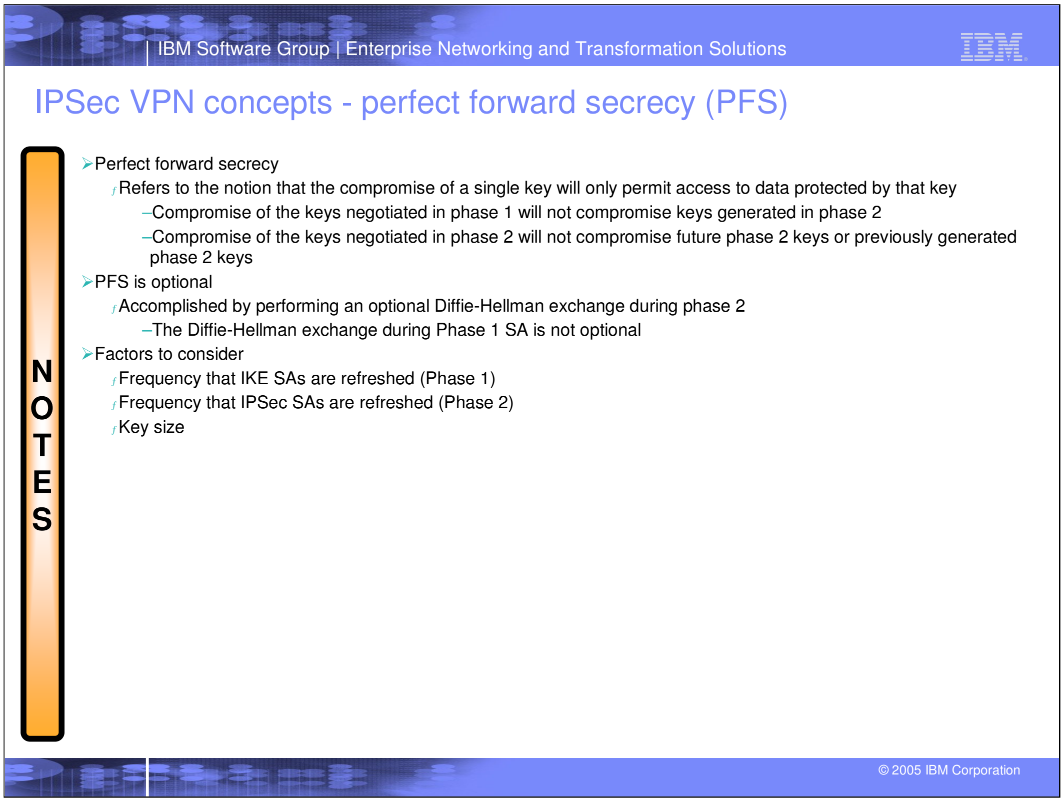
- **Policy definition is based on identities exchanged during phase 1**
  - Key Exchange Policy
    - A set of filter rules for IKE



IPSec VPN concepts - more info about Phase 1 SAs

NOTES

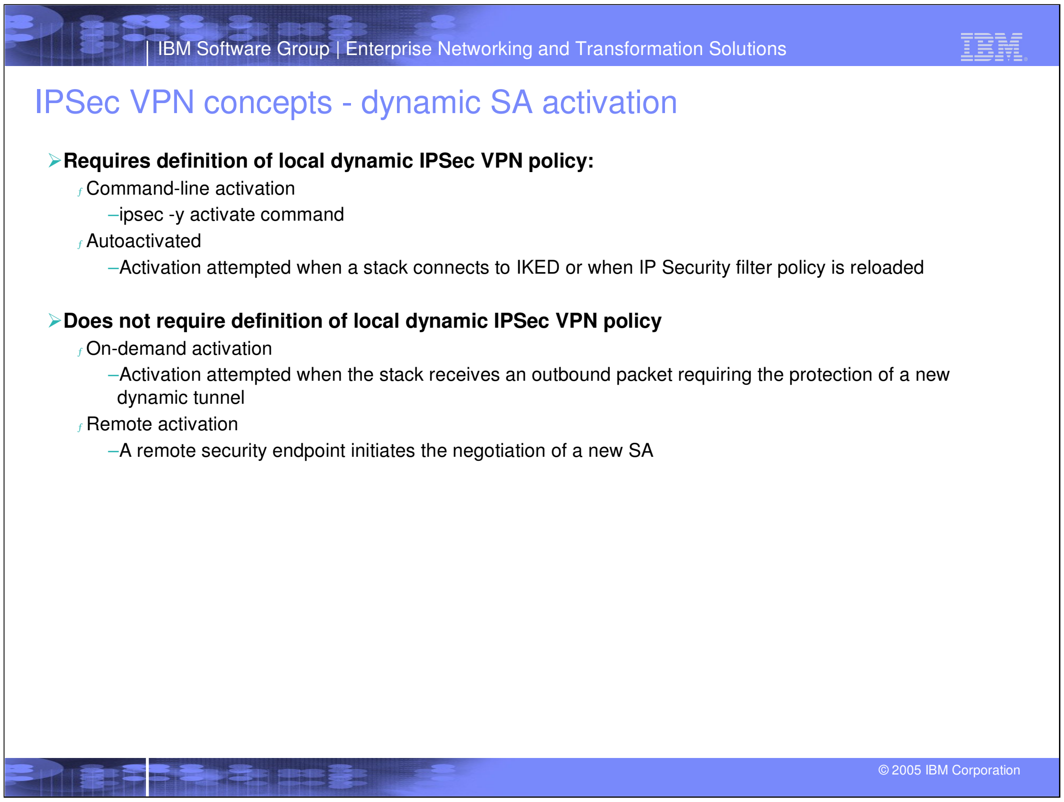
- There are two different phase 1 exchange modes. Both exchange the same information, but one utilizes fewer messages.
  - Main mode
    - All IPSec implementations must support main mode. Main mode utilizes 6 messages. The last two messages contain identity information and are encrypted. This provides 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 by Integrated IPSec include:
  - An IPv4 address (this identity type should not be used when behind a NAT)
  - RFC 822 name (for example, email address)
  - Fully qualified domain name (FQDN)
  - x500 distinguished name (DN)
- Authentication modes
  - Preshared key
    - Security endpoint administrators agree to this value. The key is not directly used to encrypt data.
    - Often used during the initial stages of dynamic SA deployment
  - RSA signature
    - Require X509 certificates.
      - 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).
    - Often used when dynamic SA are widely deployed.
- Diffie-Hellman is an algorithm that allows IKE to produce cryptographic keying material. Diffie-Hellman groups are defined in RFC 2409 (IKE). Integrated IPSec supports groups 1 and 2. Group 2 provides better security characteristics, but it also requires more computational power.



IPSec VPN concepts - perfect forward secrecy (PFS)

NOTES

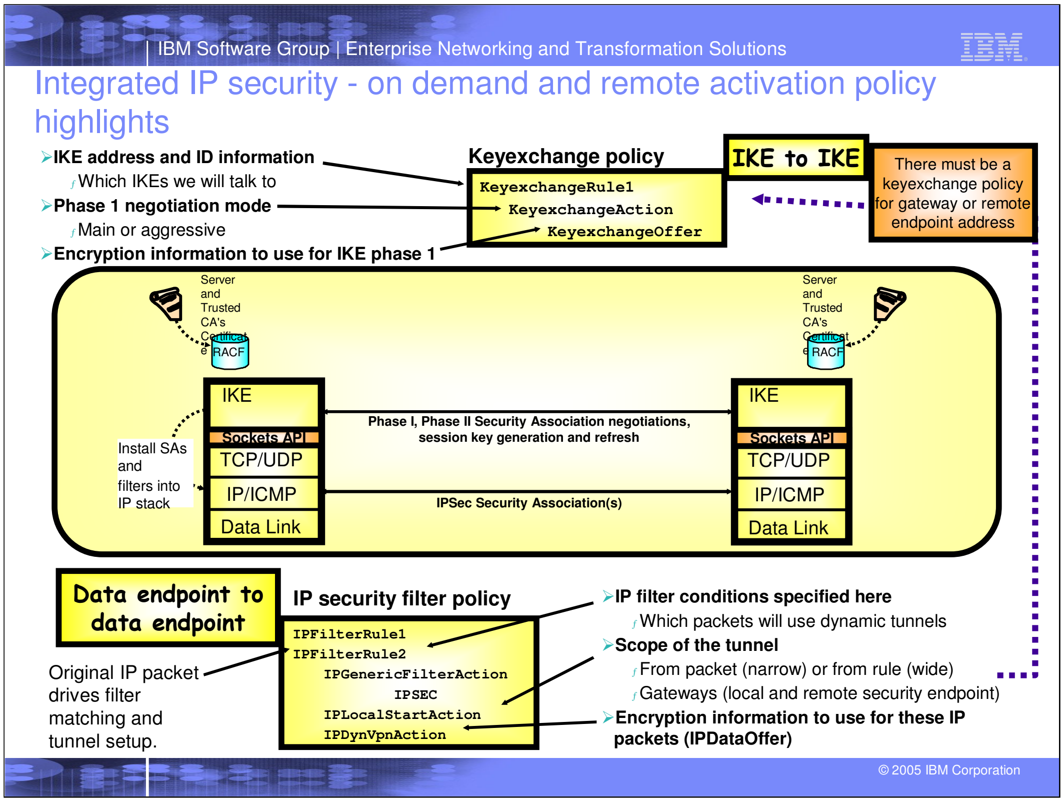
- ➢Perfect forward secrecy
  - ƒRefers to the notion that the compromise of a single key will only permit access to data protected by that key
    - –Compromise of the keys negotiated in phase 1 will not compromise keys generated in phase 2
    - –Compromise of the keys negotiated in phase 2 will not compromise future phase 2 keys or previously generated phase 2 keys
- ➢PFS is optional
  - ƒAccomplished by performing an optional Diffie-Hellman exchange during phase 2
    - –The Diffie-Hellman exchange during Phase 1 SA is not optional
- ➢Factors to consider
  - ƒFrequency that IKE SAs are refreshed (Phase 1)
  - ƒFrequency that IPSec SAs are refreshed (Phase 2)
  - ƒKey size



IPSec VPN concepts - dynamic SA activation

- **Requires definition of local dynamic IPSec VPN policy:**
  - Command-line activation
    - ipsec -y activate command
  - Autoactivated
    - Activation attempted when a stack connects to IKED or when IP Security filter policy is reloaded

- **Does not require definition of local dynamic IPSec VPN policy**
  - 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



Integrated IP security - on demand and remote activation policy highlights

- **IKE address and ID information**
  - Which IKEs we will talk to
- **Phase 1 negotiation mode**
  - Main or aggressive
- **Encryption information to use for IKE phase 1**

Keyexchange policy

```
KeyexchangeRule1
   KeyexchangeAction
       KeyexchangeOffer
```

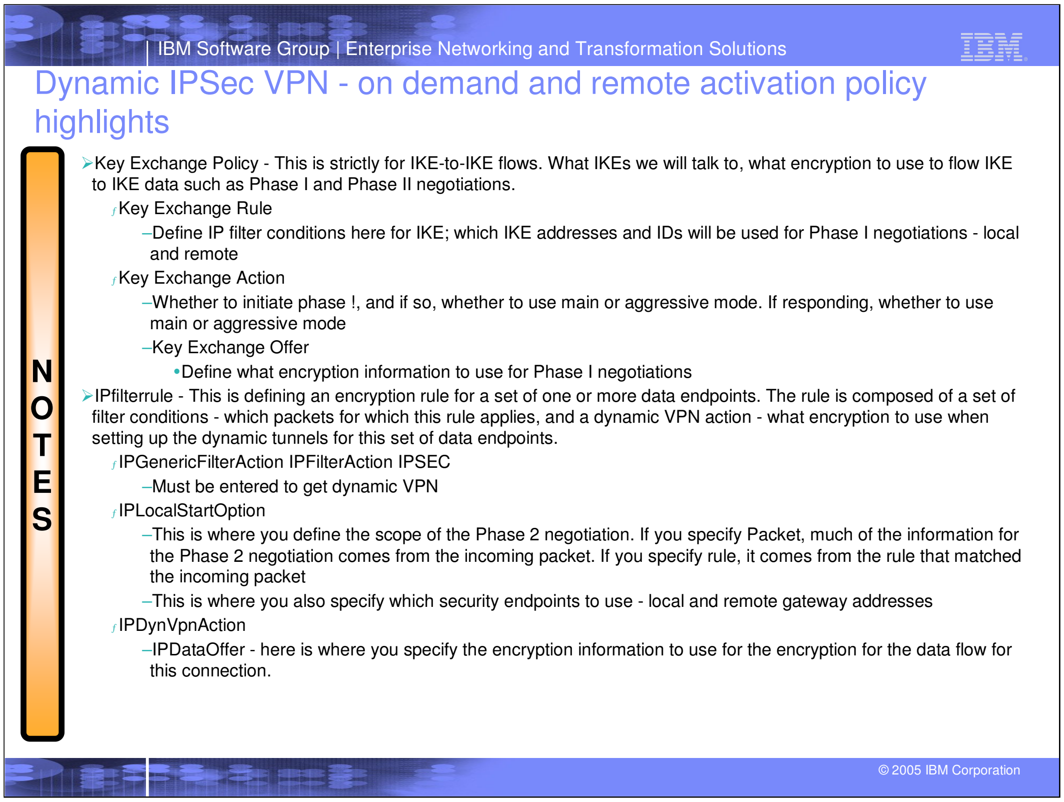
IKE to IKE
There must be a keyexchange policy for gateway or remote endpoint address
Server and Trusted CA's Certificate
RACF
Server and Trusted CA's Certificate
RACF
IKE
Sockets API
TCP/UDP
IP/ICMP
Data Link
Install SAs and filters into IP stack
Phase I, Phase II Security Association negotiations, session key generation and refresh
IPSec Security Association(s)
IKE
Sockets API
TCP/UDP
IP/ICMP
Data Link
Data endpoint to data endpoint

Original IP packet drives filter matching and tunnel setup.

IP security filter policy

```
IPFilterRule1
IPFilterRule2
    IPGenericFilterAction
             IPSEC
    IPLocalStartAction
    IPDynVpnAction
```

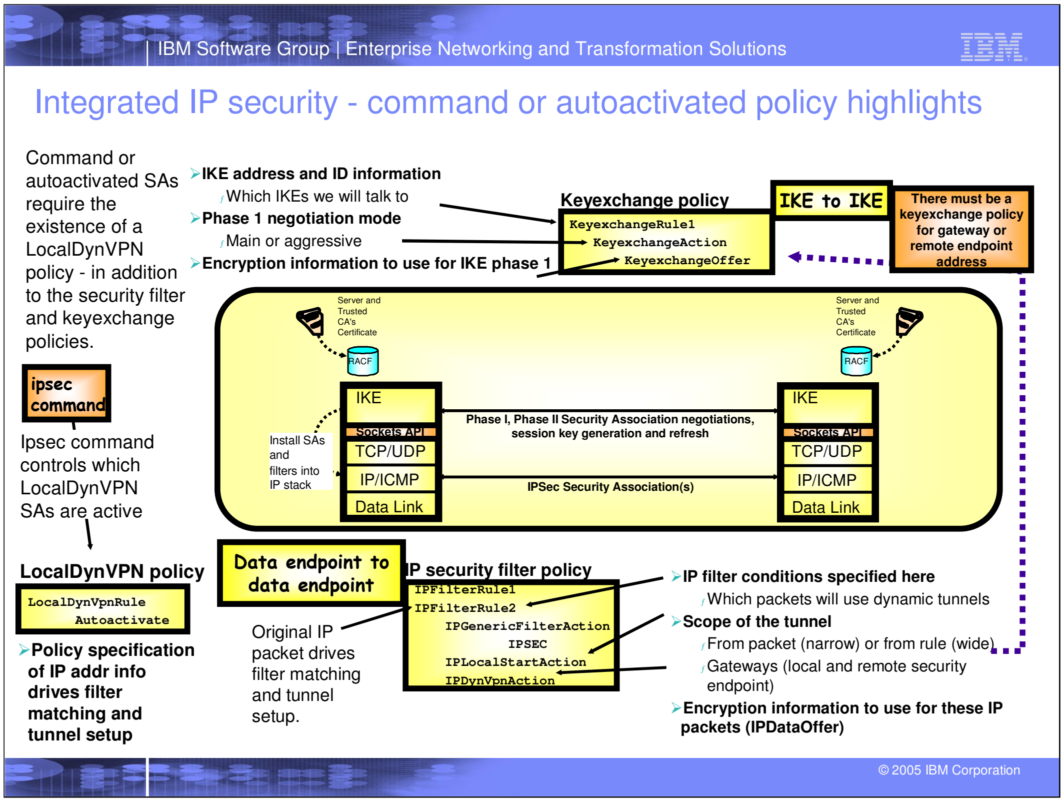
- **IP filter conditions specified here**
  - Which packets will use dynamic tunnels
- **Scope of the tunnel**
  - From packet (narrow) or from rule (wide)
  - Gateways (local and remote security endpoint)
- **Encryption information to use for these IP packets (IPDataOffer)**



Dynamic IPSec VPN - on demand and remote activation policy highlights

NOTES

- Key Exchange Policy - This is strictly for IKE-to-IKE flows. What IKEs we will talk to, what encryption to use to flow IKE to IKE data such as Phase I and Phase II negotiations.
  - Key Exchange Rule
    - Define IP filter conditions here for IKE; which IKE addresses and IDs will be used for Phase I negotiations - local and remote
  - Key Exchange Action
    - Whether to initiate phase !, and if so, whether to use main or aggressive mode. If responding, whether to use main or aggressive mode
    - Key Exchange Offer
      - Define what encryption information to use for Phase I negotiations
- IPfilterrule - This is defining an encryption rule for a set of one or more data endpoints. The rule is composed of a set of filter conditions - which packets for which this rule applies, and a dynamic VPN action - what encryption to use when setting up the dynamic tunnels for this set of data endpoints.
  - IPGenericFilterAction IPFilterAction IPSEC
    - Must be entered to get dynamic VPN
  - IPLocalStartOption
    - This is where you define the scope of the Phase 2 negotiation. If you specify Packet, much of the information for the Phase 2 negotiation comes from the incoming packet. If you specify rule, it comes from the rule that matched the incoming packet
    - This is where you also specify which security endpoints to use - local and remote gateway addresses
  - IPDynVpnAction
    - IPDataOffer - here is where you specify the encryption information to use for the encryption for the data flow for this connection.



Integrated IP security - command or autoactivated policy highlights

Command or autoactivated SAs require the existence of a LocalDynVPN policy - in addition to the security filter and keyexchange policies.

- IKE address and ID information
  - Which IKEs we will talk to
- Phase 1 negotiation mode
  - Main or aggressive
- Encryption information to use for IKE phase 1

Keyexchange policy

```
KeyexchangeRule1
   KeyexchangeAction
       KeyexchangeOffer
```

IKE to IKE

There must be a keyexchange policy for gateway or remote endpoint address

Server and Trusted CA's Certificate
RACF
Server and Trusted CA's Certificate
RACF
IKE
Sockets API
TCP/UDP
IP/ICMP
Data Link
Install SAs and filters into IP stack
Phase I, Phase II Security Association negotiations, session key generation and refresh
IPSec Security Association(s)
IKE
Sockets API
TCP/UDP
IP/ICMP
Data Link

ipsec command

Ipsec command controls which LocalDynVPN SAs are active

LocalDynVPN policy

```
LocalDynVpnRule
      Autoactivate
```

- **Policy specification of IP addr info drives filter matching and tunnel setup**

Data endpoint to data endpoint

IP security filter policy

```
IPFilterRule1
IPFilterRule2
    IPGenericFilterAction
        IPSEC
    IPLocalStartAction
    IPDynVpnAction
```

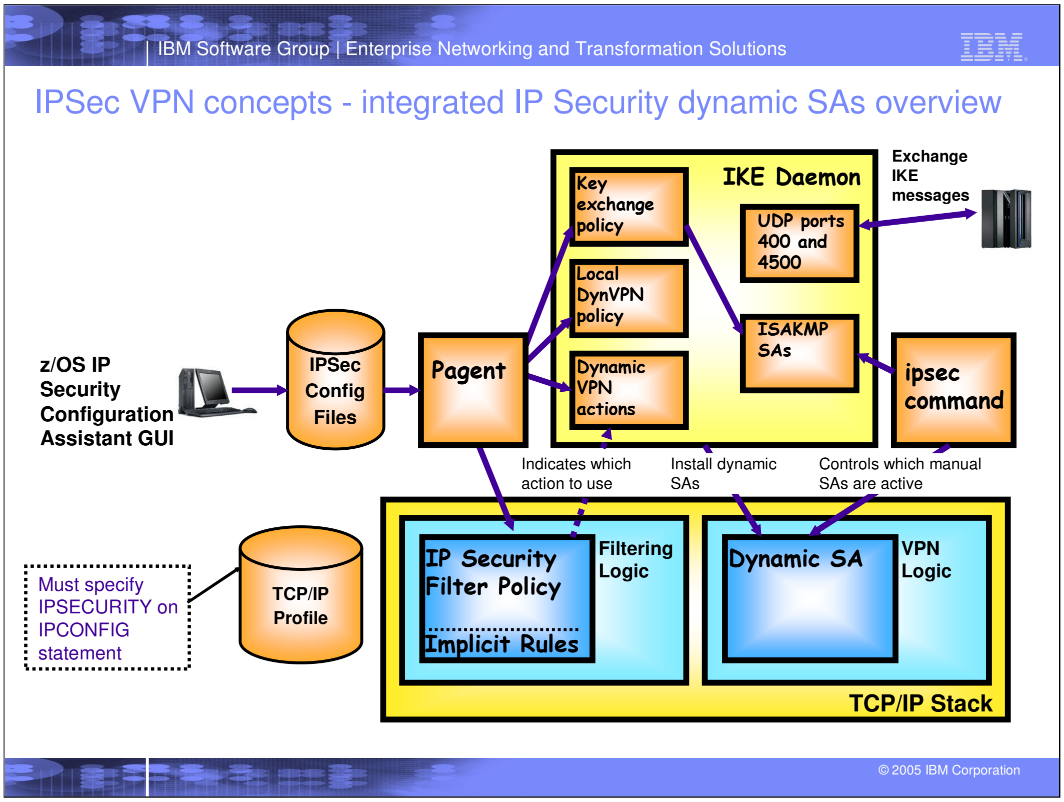
Original IP packet drives filter matching and tunnel setup.

- **IP filter conditions specified here**
  - Which packets will use dynamic tunnels
- **Scope of the tunnel**
  - From packet (narrow) or from rule (wide)
  - Gateways (local and remote security endpoint)
- **Encryption information to use for these IP packets (IPDataOffer)**

Dynamic IPSec VPN - command or autoactivated policy highlights

NOTES

- Key Exchange Policy - This is strictly for IKE to IKE flows. What IKEs we will talk to, what encryption to use to flow IKE to IKE data such as Phase I and Phase II negotiations.
  - Key Exchange Rule
    - Define IP filter conditions here for IKE; which IKE addresses and IDs will be used for Phase I negotiations - local and remote
  - Key Exchange Action
    - Whether to initiate phase !, and if so, whether to use main or aggressive mode. If responding, whether to use main or aggressive mode
    - Key Exchange Offer
      - Define what encryption information to use for Phase I negotiations
- IPfilterrule - This is defining an encryption rule for a set of one or more data endpoints. The rule is composed of a set of filter conditions - which packets for which this rule applies, and a dynamic VPN action - what encryption to use when setting up the dynamic tunnels for this set of data endpoints.
  - IPGenericFilterAction IPFilterAction IPSEC
    - Must be entered to get dynamic VPN
  - IPLocalStartOption
    - This is where you define the scope of the Phase 2 negotiation. If you specify Packet, much of the information for the Phase 2 negotiation comes from the incoming packet. If you specify rule, it comes from the rule that matched the incoming packet
    - This is where you also specify which security endpoints to use - local and remote gateway addresses
  - IPDynVpnAction
    - IPDataOffer - here is where you specify the encryption information to use for the encryption for the data flow for this connection.
- LocalDynVPNPolicy - This gives the customer a way to drive Phase 1 and Phase 2 tunnel activation without a packet coming in. Effectively, this LocalDynVPNRule defines a set of addresses/ports/protocols. When the LocalDynVpnRule has the autoactivate parm, or is activated by IPSEC cmd, dynamic tunnels and IKE tunnels are created/used as though a packet with these addresses/ports/protocols was received.



IPSec VPN concepts - integrated IP Security dynamic SAs overview

z/OS IP Security Configuration Assistant GUI

IPSec Config Files

Pagent

IKE Daemon

Key exchange policy

Local DynVPN policy

Dynamic VPN actions

UDP ports 400 and 4500

ISAKMP SAs

Exchange IKE messages

ipsec command

Indicates which action to use

Install dynamic SAs

Controls which manual SAs are active

Must specify IPSECURITY on IPCONFIG statement

TCP/IP Profile

IP Security Filter Policy

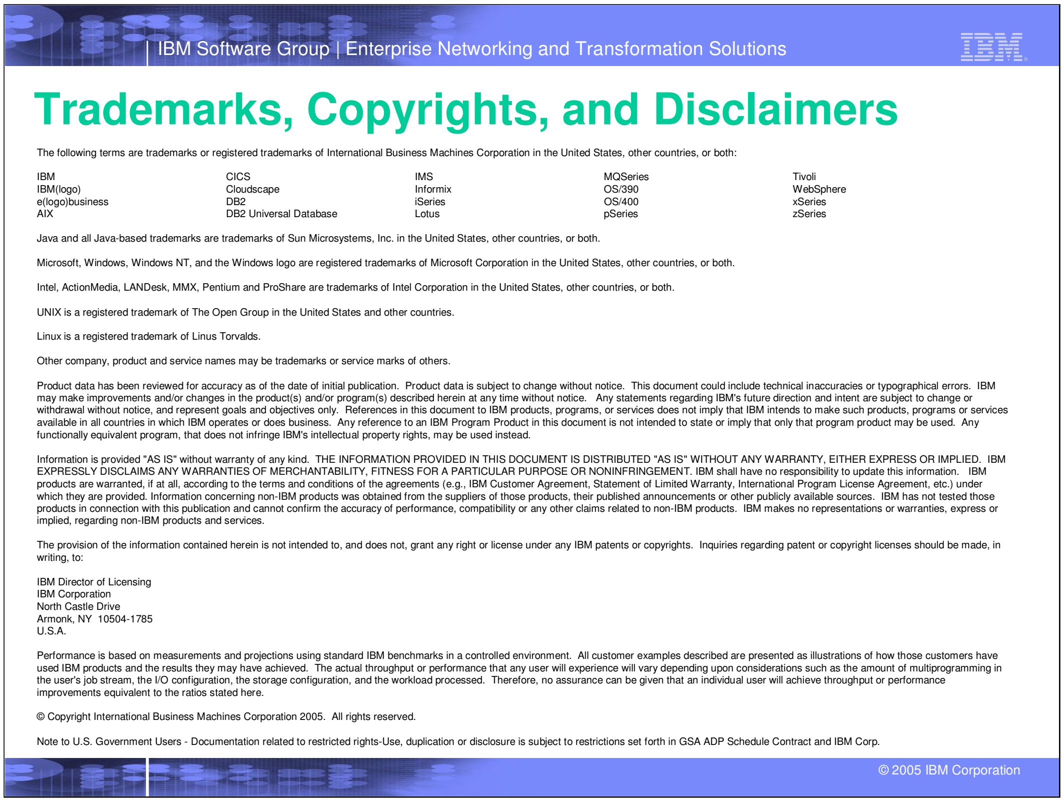
Implicit Rules

Filtering Logic

Dynamic SA

VPN Logic

TCP/IP Stack



Trademarks, Copyrights, and Disclaimers

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

- IBM
- IBM(logo)
- e(logo)business
- AIX
- CICS
- Cloudscape
- DB2
- DB2 Universal Database
- IMS
- Informix
- iSeries
- Lotus
- MQSeries
- OS/390
- OS/400
- pSeries
- Tivoli
- WebSphere
- xSeries
- 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 registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare 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 registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.