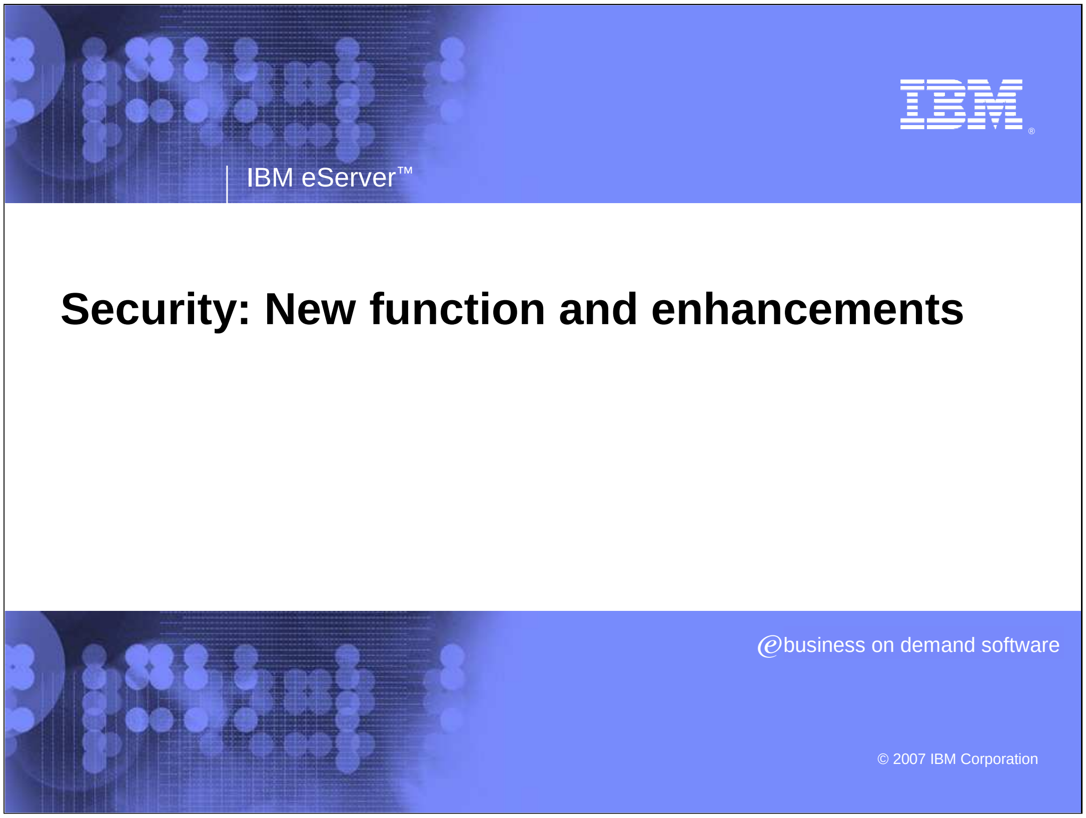
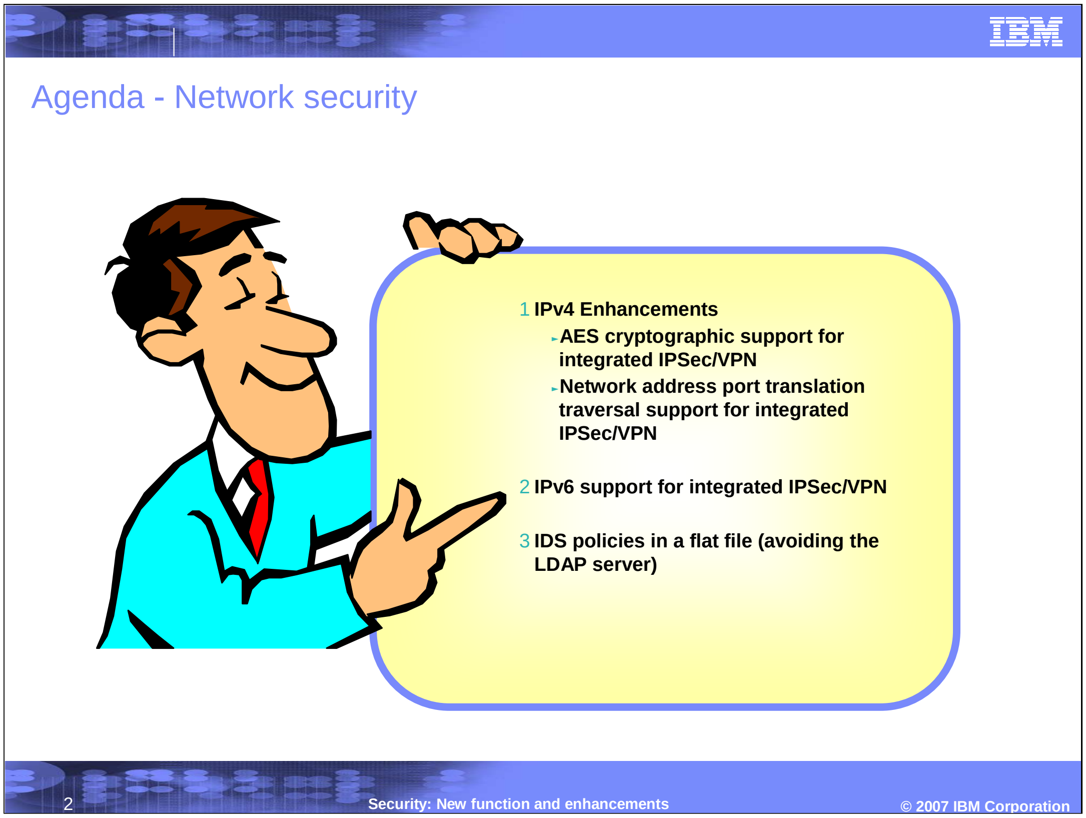


IBM eServer™

Security: New function and enhancements

*e*business on demand software

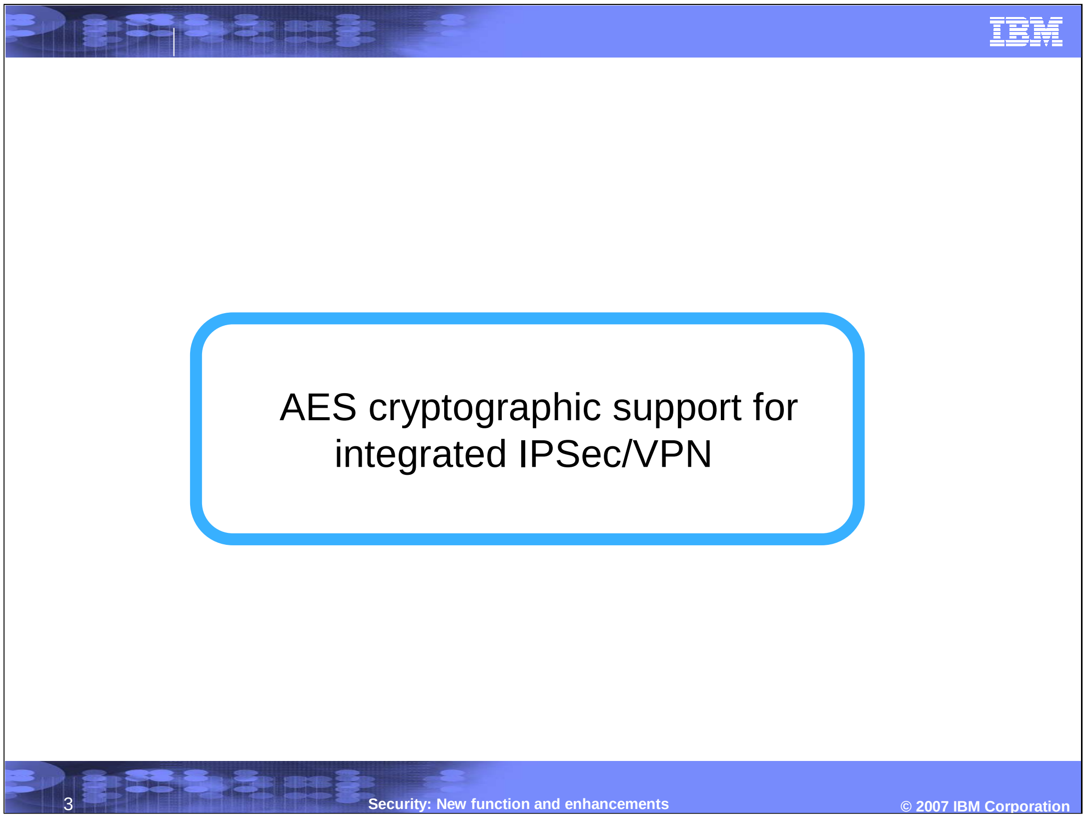


Agenda - Network security

1 IPv4 Enhancements
  - AES cryptographic support for integrated IPSec/VPN
  - Network address port translation traversal support for integrated IPSec/VPN

2 IPv6 support for integrated IPSec/VPN

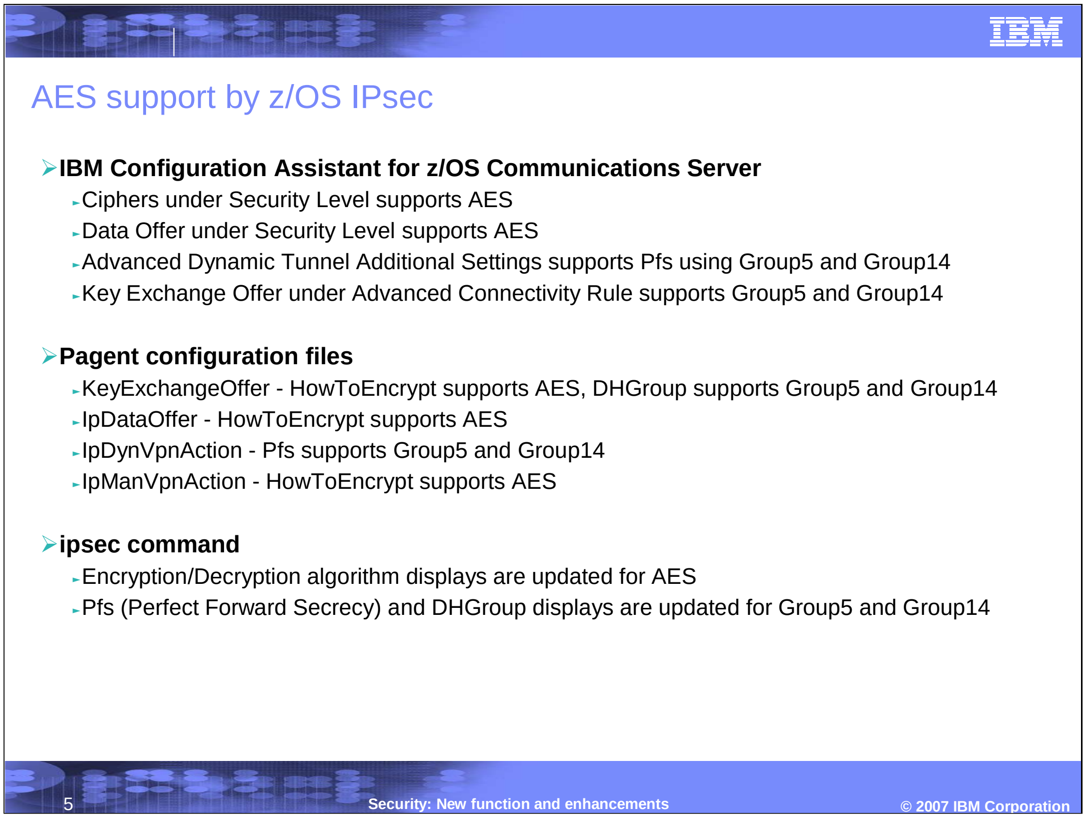
3 IDS policies in a flat file (avoiding the LDAP server)



AES cryptographic support for integrated IPSec/VPN

AES background information - IPSec support for AES 128-bit encryption

- **AES stands for Advanced Encryption Standard**
- **The National Institute of Standards and Technology has named AES as the "replacement" for DES as the standard encryption algorithm**
- **It is the intention of the IETF IPSec Working Group that AES will eventually be adopted as the default IPSec ESP cipher and will obtain the status of MUST be included in compliant IPSec implementations**
- **AES is "at least" as secure as triple DES**
- **IKE/IPSec in z/OS® V1R8 supports 128-bit AES encryption for dynamic and manual tunnels**
- **IKE in z/OS V1R8 also supports Diffie-Hellman Groups 1,2,5 and 14**
  - AES requires stronger keying material than DES/3DES so Diffie-Hellman groups 5 and 14 should be supported
  - Suggest using group 5 or 14 for AES cryptography
- **REQUIREMENT: Integrated Cryptographic Service Facility (ICSF) implements the AES algorithm and is required in order to use AES**



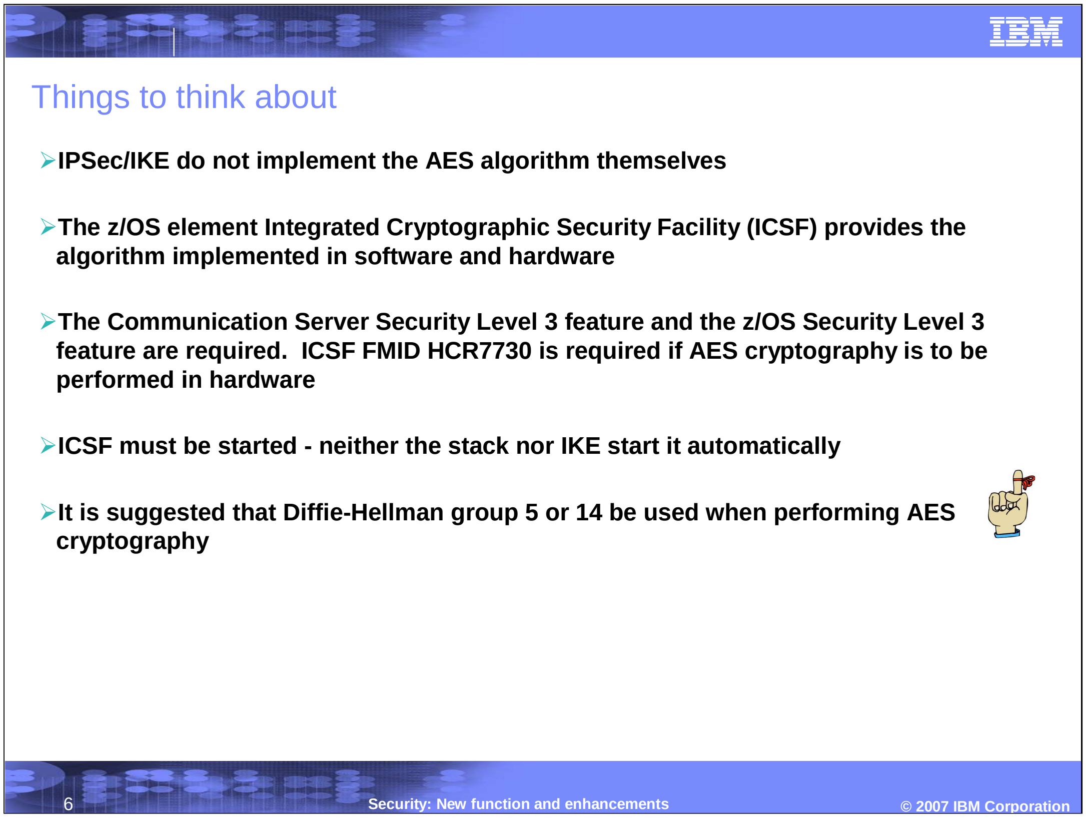
IBM

AES support by z/OS IPsec

- **IBM Configuration Assistant for z/OS Communications Server**
  - Ciphers under Security Level supports AES
  - Data Offer under Security Level supports AES
  - Advanced Dynamic Tunnel Additional Settings supports Pfs using Group5 and Group14
  - Key Exchange Offer under Advanced Connectivity Rule supports Group5 and Group14

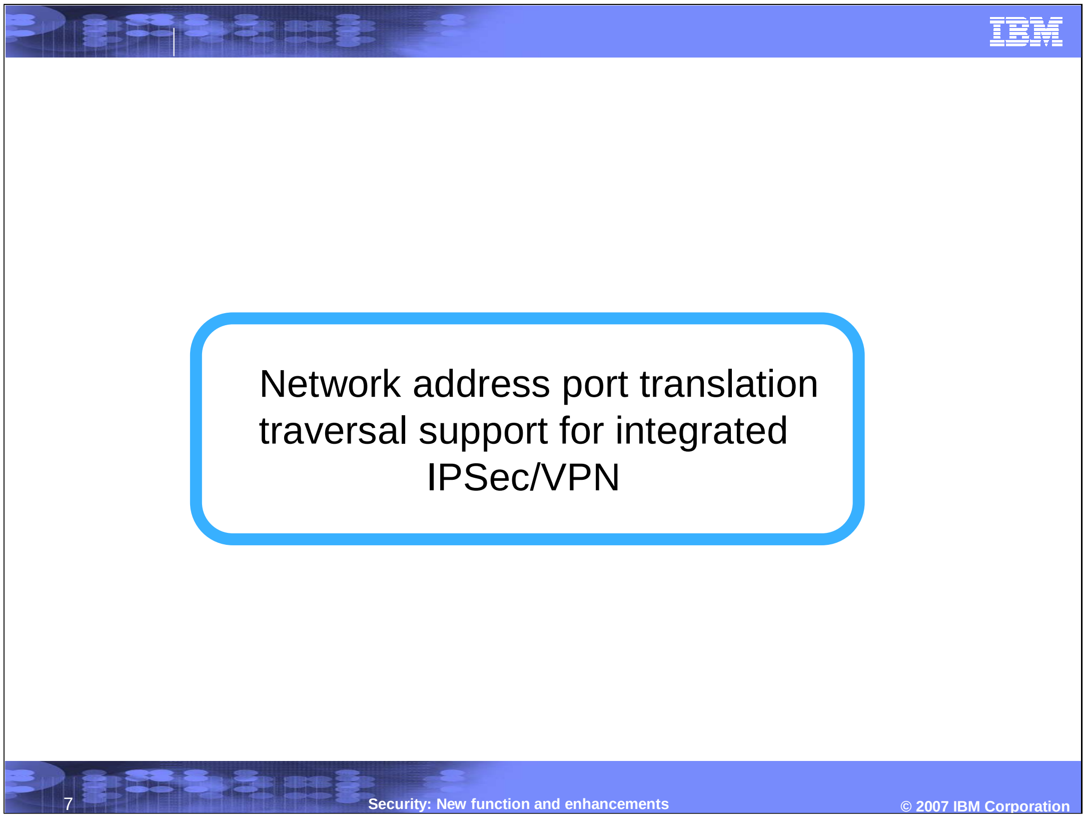
- **Pagent configuration files**
  - KeyExchangeOffer - HowToEncrypt supports AES, DHGroup supports Group5 and Group14
  - IpDataOffer - HowToEncrypt supports AES
  - IpDynVpnAction - Pfs supports Group5 and Group14
  - IpManVpnAction - HowToEncrypt supports AES

- **ipsec command**
  - Encryption/Decryption algorithm displays are updated for AES
  - Pfs (Perfect Forward Secrecy) and DHGroup displays are updated for Group5 and Group14

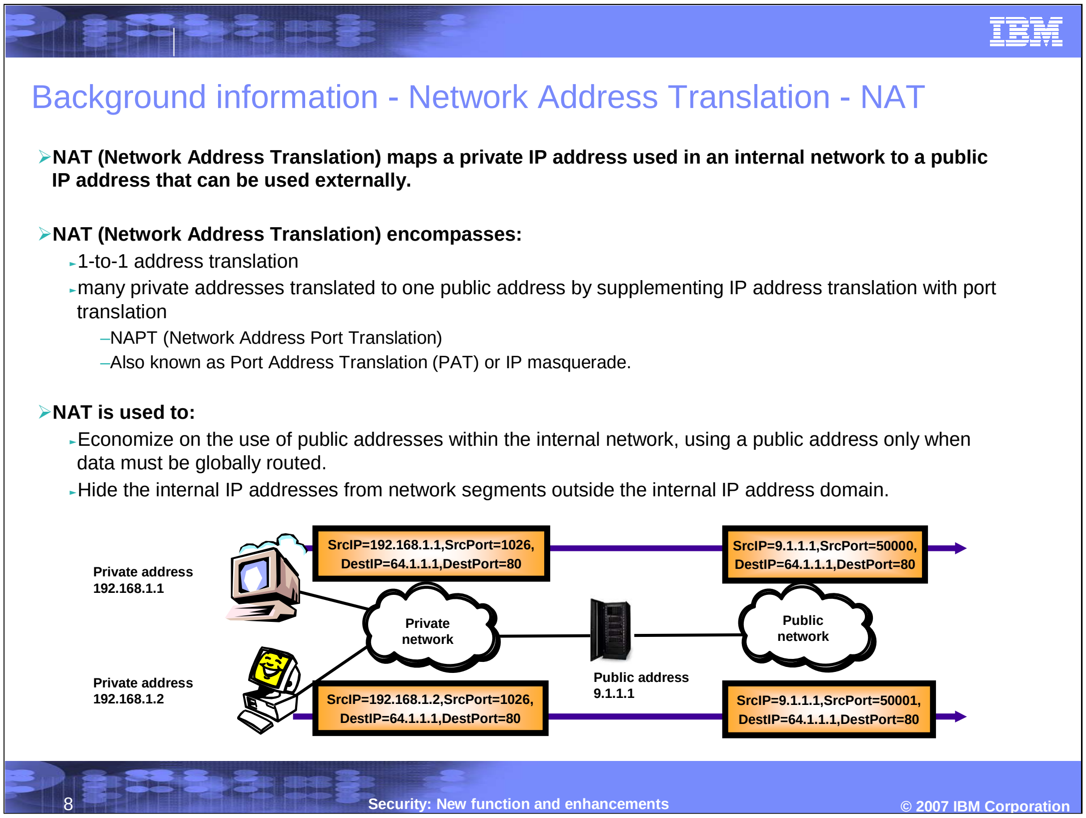


Things to think about

- IPSec/IKE do not implement the AES algorithm themselves
- The z/OS element Integrated Cryptographic Security Facility (ICSF) provides the algorithm implemented in software and hardware
- The Communication Server Security Level 3 feature and the z/OS Security Level 3 feature are required. ICSF FMID HCR7730 is required if AES cryptography is to be performed in hardware
- ICSF must be started - neither the stack nor IKE start it automatically
- It is suggested that Diffie-Hellman group 5 or 14 be used when performing AES cryptography



Network address port translation traversal support for integrated IPSec/VPN



Background information - Network Address Translation - NAT

- **NAT (Network Address Translation) maps a private IP address used in an internal network to a public IP address that can be used externally.**

- **NAT (Network Address Translation) encompasses:**
  - 1-to-1 address translation
  - many private addresses translated to one public address by supplementing IP address translation with port translation
    - NAPT (Network Address Port Translation)
    - Also known as Port Address Translation (PAT) or IP masquerade.

- **NAT is used to:**
  - Economize on the use of public addresses within the internal network, using a public address only when data must be globally routed.
  - Hide the internal IP addresses from network segments outside the internal IP address domain.

Private address
192.168.1.1

SrcIP=192.168.1.1,SrcPort=1026,
DestIP=64.1.1.1,DestPort=80

SrcIP=9.1.1.1,SrcPort=50000,
DestIP=64.1.1.1,DestPort=80

Private network

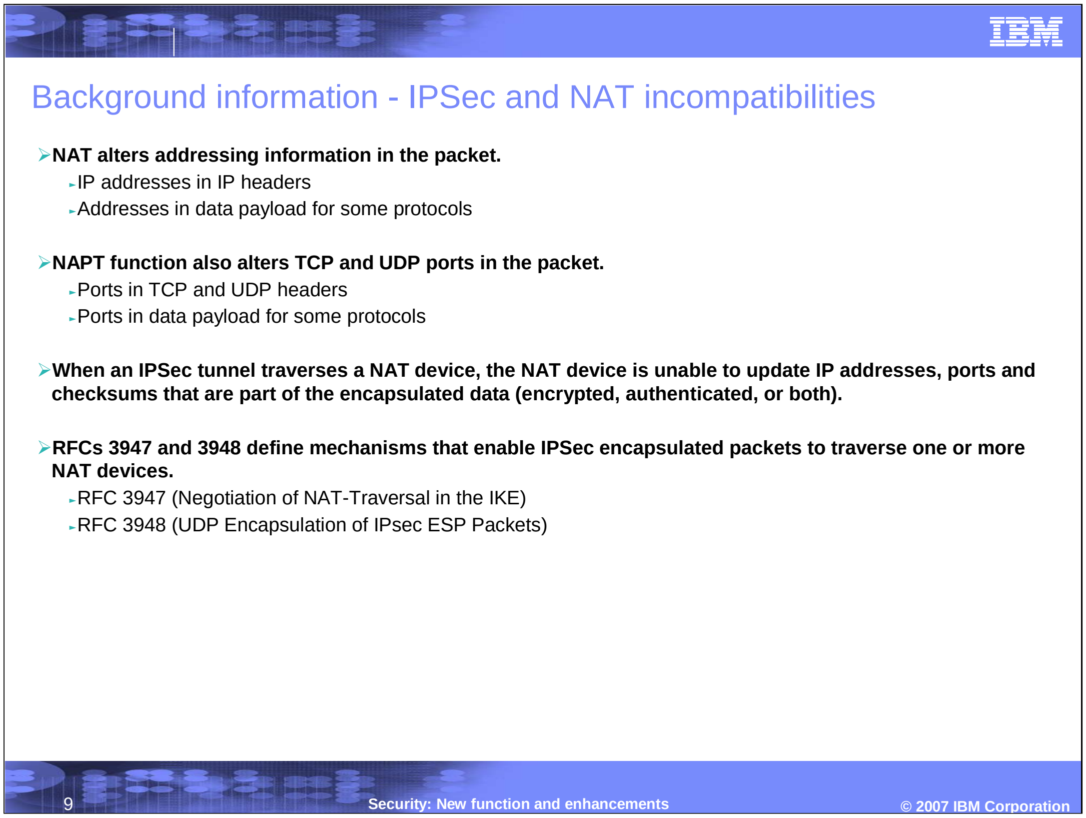
Public network

Public address
9.1.1.1

Private address
192.168.1.2

SrcIP=192.168.1.2,SrcPort=1026,
DestIP=64.1.1.1,DestPort=80

SrcIP=9.1.1.1,SrcPort=50001,
DestIP=64.1.1.1,DestPort=80



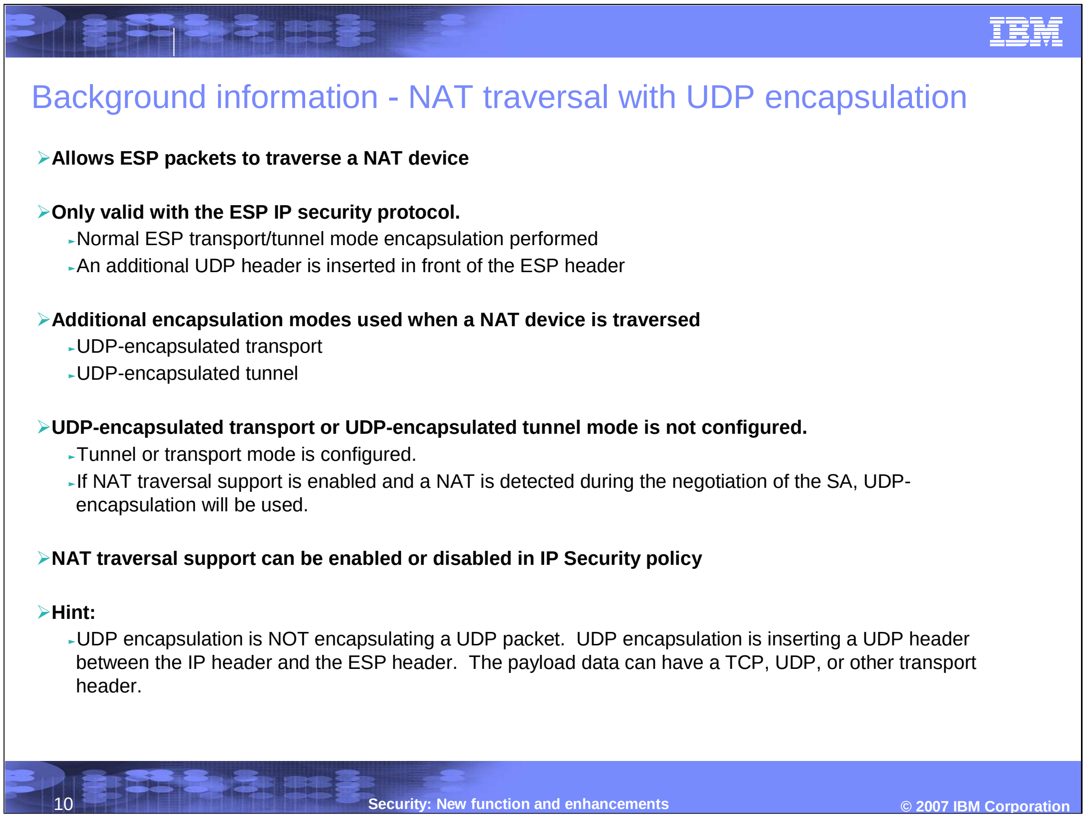
Background information - IPSec and NAT incompatibilities

- **NAT alters addressing information in the packet.**
  - IP addresses in IP headers
  - Addresses in data payload for some protocols

- **NAPT function also alters TCP and UDP ports in the packet.**
  - Ports in TCP and UDP headers
  - Ports in data payload for some protocols

- **When an IPSec tunnel traverses a NAT device, the NAT device is unable to update IP addresses, ports and checksums that are part of the encapsulated data (encrypted, authenticated, or both).**

- **RFCs 3947 and 3948 define mechanisms that enable IPSec encapsulated packets to traverse one or more NAT devices.**
  - RFC 3947 (Negotiation of NAT-Traversal in the IKE)
  - RFC 3948 (UDP Encapsulation of IPsec ESP Packets)



Background information - NAT traversal with UDP encapsulation

- **Allows ESP packets to traverse a NAT device**

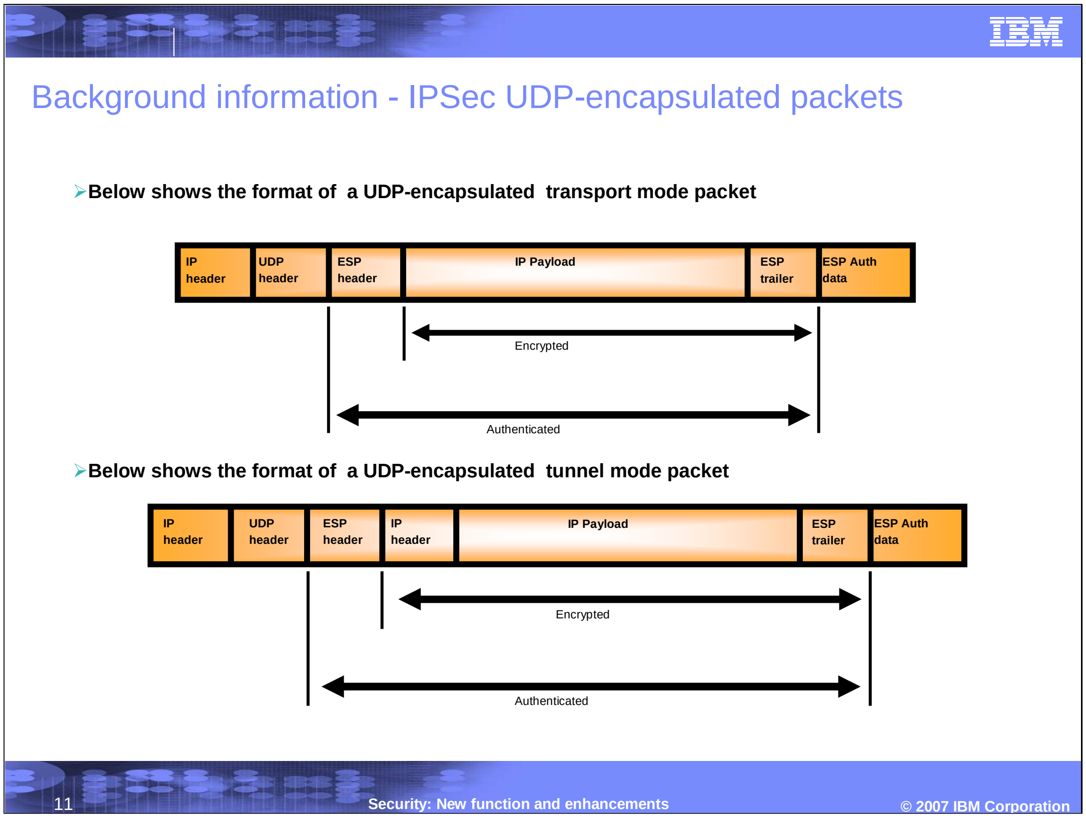
- **Only valid with the ESP IP security protocol.**
  - Normal ESP transport/tunnel mode encapsulation performed
  - An additional UDP header is inserted in front of the ESP header

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

- **UDP-encapsulated transport or UDP-encapsulated tunnel mode is not configured.**
  - Tunnel or transport mode is configured.
  - If NAT traversal support is enabled and a NAT is detected during the negotiation of the SA, UDP-encapsulation will be used.

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

- **Hint:**
  - UDP encapsulation is NOT encapsulating a UDP packet. UDP encapsulation is inserting a UDP header between the IP header and the ESP header. The payload data can have a TCP, UDP, or other transport header.



Background information - IPSec UDP-encapsulated packets

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

IP header | UDP header | ESP header | IP Payload | ESP trailer | ESP Auth data

Encrypted

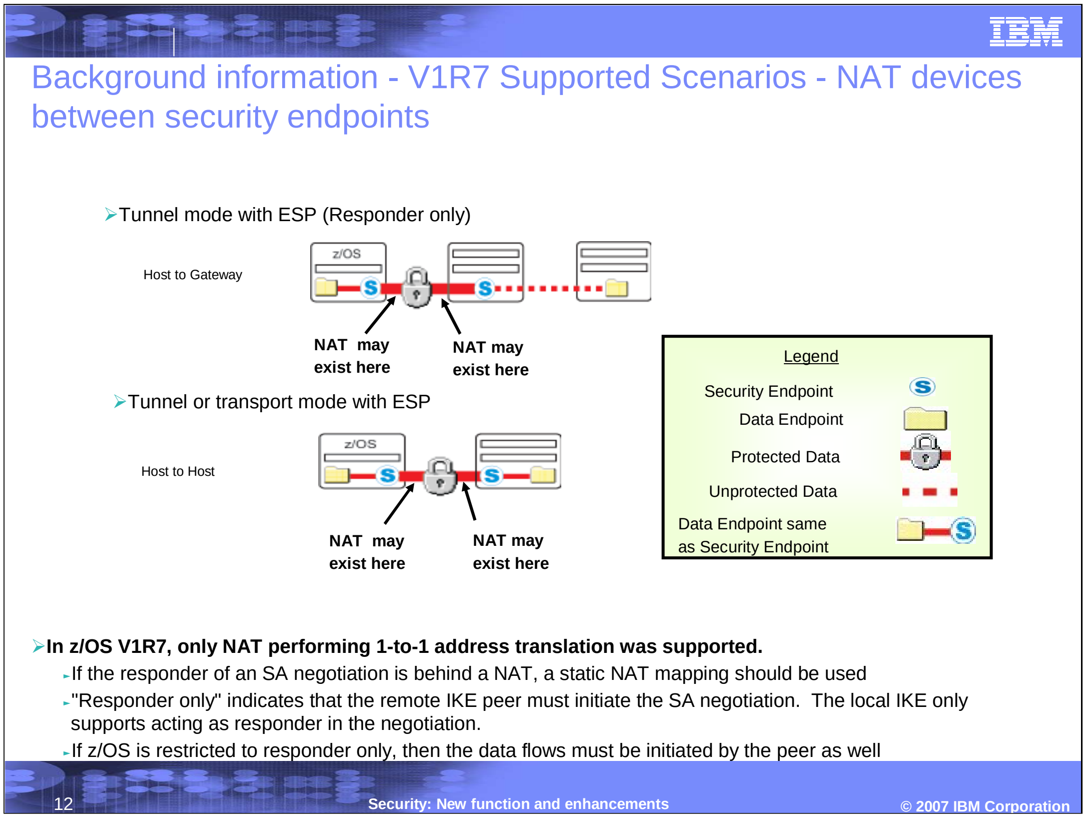
Authenticated

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

IP header | UDP header | ESP header | IP header | IP Payload | ESP trailer | ESP Auth data

Encrypted

Authenticated



Background information - V1R7 Supported Scenarios - NAT devices between security endpoints

- Tunnel mode with ESP (Responder only)

Host to Gateway

NAT may exist here

NAT may exist here

- Tunnel or transport mode with ESP

Host to Host

NAT may exist here

NAT may exist here

Legend

Security Endpoint

Data Endpoint

Protected Data

Unprotected Data

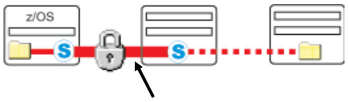
Data Endpoint same as Security Endpoint

- **In z/OS V1R7, only NAT performing 1-to-1 address translation was supported.**
  - If the responder of an SA negotiation is behind a NAT, a static NAT mapping should be used
  - "Responder only" indicates that the remote IKE peer must initiate the SA negotiation. The local IKE only supports acting as responder in the negotiation.
  - If z/OS is restricted to responder only, then the data flows must be initiated by the peer as well

z/OS V1R8 Supported Scenarios - NAPT devices between security endpoints

- Tunnel mode with ESP (Responder only)

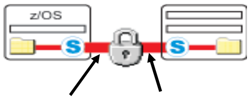
Host to Gateway



NAPT may exist here

- Tunnel or transport mode with ESP

Host to Host



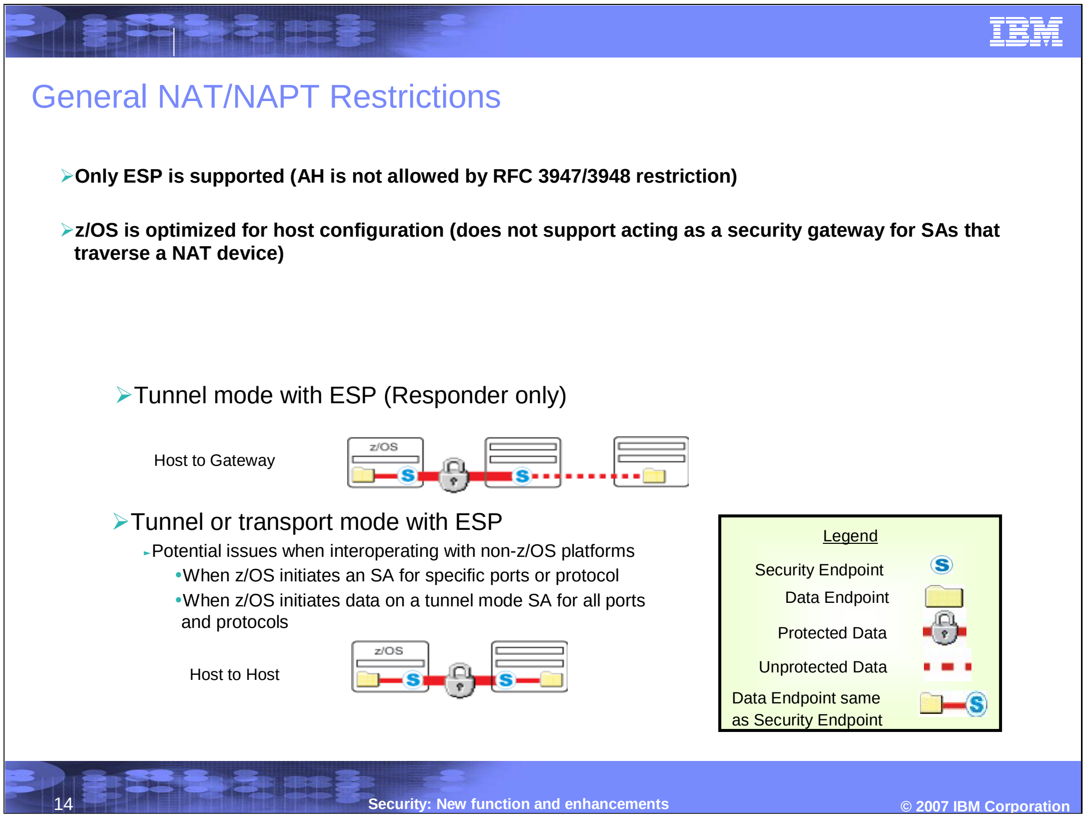
NAPT may exist here

or NAPT may exist here

<u>Legend</u>

Security Endpoint	Ⓢ
Data Endpoint	🟨
Protected Data	🟥🔒🟥
Unprotected Data	▪ ▪ ▪
Data Endpoint same as Security Endpoint	🟨—Ⓢ

- **NAT performing many-to-1 address/port translation (NAPT) supported.**
  - The z/OS host is restricted to responder mode when the remote peer is behind an NAPT.
  - If z/OS is restricted to responder only, then the data flows must be initiated by the peer as well



General NAT/NAPT Restrictions

- **Only ESP is supported (AH is not allowed by RFC 3947/3948 restriction)**
- **z/OS is optimized for host configuration (does not support acting as a security gateway for SAs that traverse a NAT device)**

- Tunnel mode with ESP (Responder only)

Host to Gateway
z/OS
S
S

- Tunnel or transport mode with ESP
  - Potential issues when interoperating with non-z/OS platforms
    - When z/OS initiates an SA for specific ports or protocol
    - When z/OS initiates data on a tunnel mode SA for all ports and protocols

Legend

Security Endpoint Ⓢ

Data Endpoint 📁

Protected Data 🔒

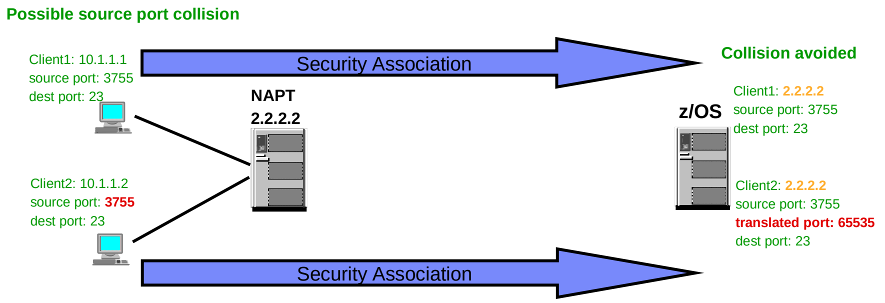
Unprotected Data ▪ ▪ ▪

Data Endpoint same as Security Endpoint 📁—Ⓢ

Source port translation for NAT traversal

- **Done when the remote security endpoint is behind a NAT/NAPT device**
  - Only done for TCP and UDP packets
  - Since only the public (NAT'ed) address of the remote security endpoint is known to z/OS:
    - Clients that reside behind a NAT/NAPT device might choose identical source ports
    - z/OS translates source ports to distinguish connections that have a duplicate source port

- **Connection information displayed on z/OS:**
  - Netstat shows translated port
  - ipsec command can be used to show the port mapping (ipsec -o)
  - system logs show when a port translation was performed



Possible source port collision

Client1: 10.1.1.1
source port: 3755
dest port: 23

Client2: 10.1.1.2
source port: **3755**
dest port: 23

Security Association

NAPT
2.2.2.2

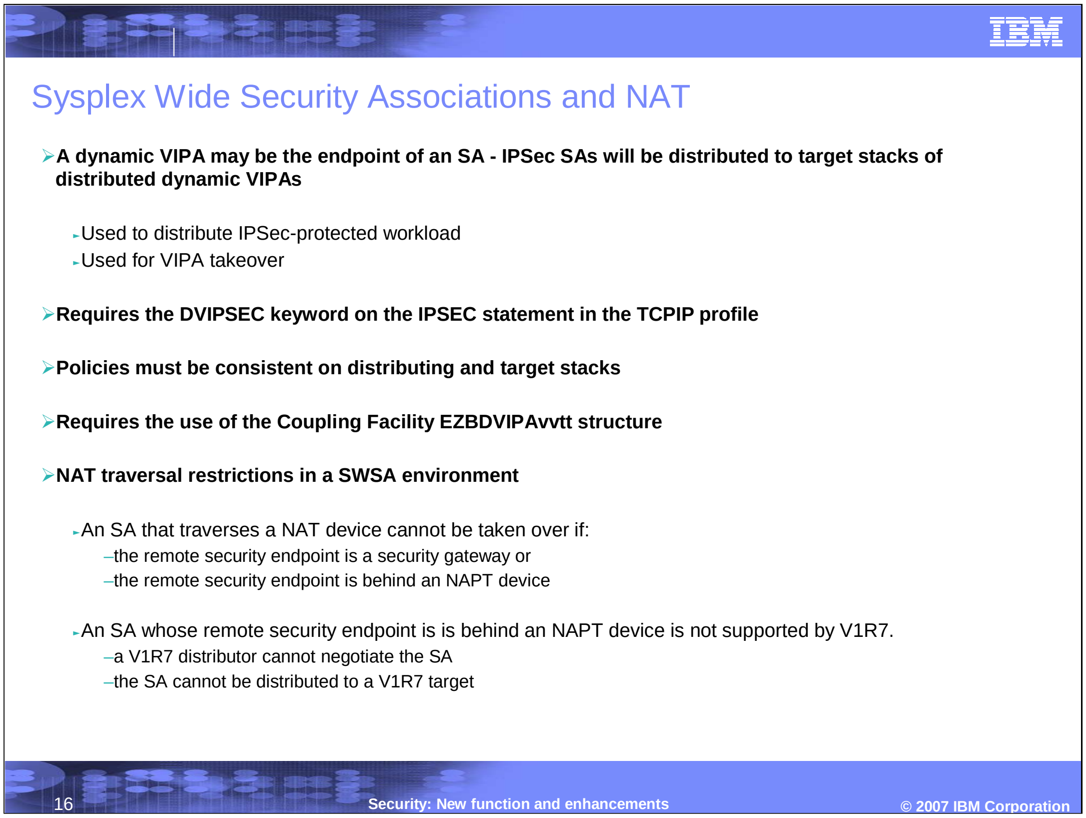
Security Association

Collision avoided

z/OS

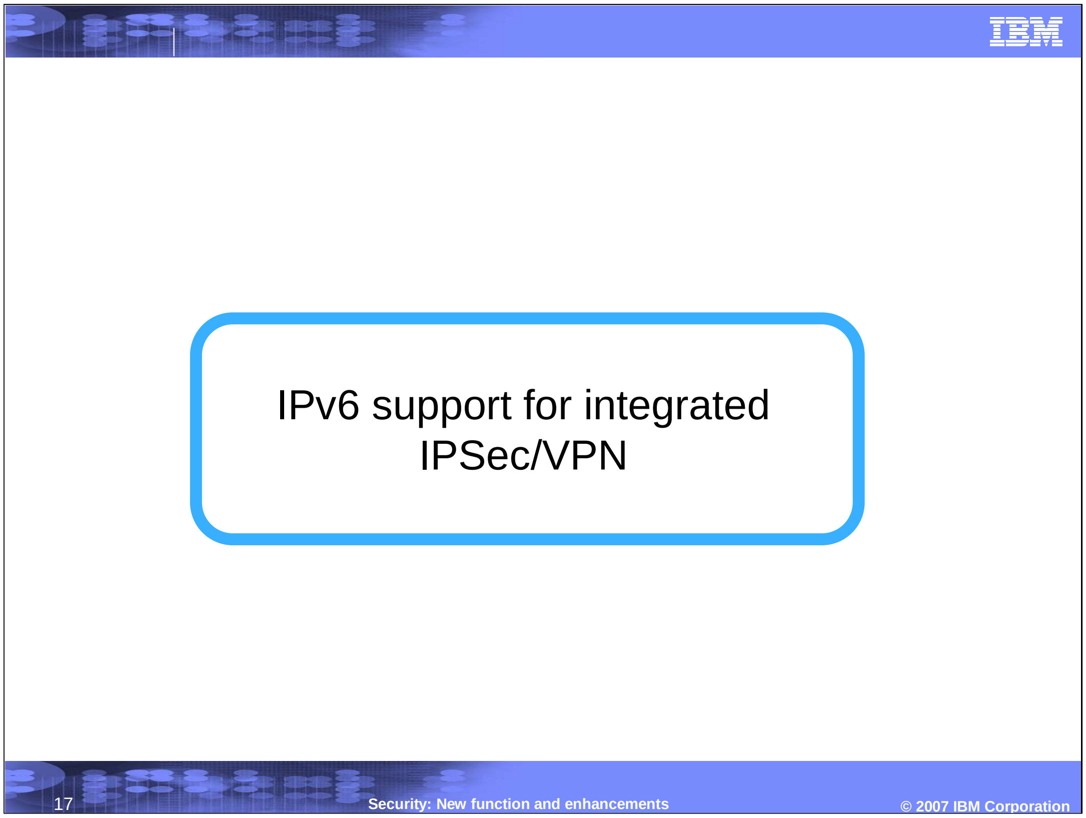
Client1: 2.2.2.2
source port: 3755
dest port: 23

Client2: 2.2.2.2
source port: 3755
translated port: 65535
dest port: 23



Sysplex Wide Security Associations and NAT

- **A dynamic VIPA may be the endpoint of an SA - IPSec SAs will be distributed to target stacks of distributed dynamic VIPAs**
  - Used to distribute IPSec-protected workload
  - Used for VIPA takeover
- **Requires the DVIPSEC keyword on the IPSEC statement in the TCPIP profile**
- **Policies must be consistent on distributing and target stacks**
- **Requires the use of the Coupling Facility EZBDVIPAvvtt structure**
- **NAT traversal restrictions in a SWSA environment**
  - An SA that traverses a NAT device cannot be taken over if:
    - the remote security endpoint is a security gateway or
    - the remote security endpoint is behind an NAPT device
  - An SA whose remote security endpoint is is behind an NAPT device is not supported by V1R7.
    - a V1R7 distributor cannot negotiate the SA
    - the SA cannot be distributed to a V1R7 target



IPv6 support for integrated IPSec/VPN

17

Security: New function and enhancements

© 2007 IBM Corporation

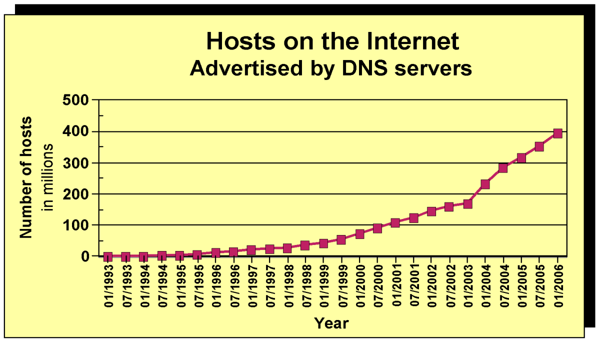
Extending integrated IP Security functions to include IPv6 traffic

- **z/OS V1R5 and V1R6 have both been IPv6 Ready Logo Phase-1 certified**

- **IPv6 Ready Logo Phase-2 has now been defined and the main addition is required support for IPv6 IP Security (IPSec)**
  - Standard requirement for all IPv6 platforms
  - Replace application-specific security, such as OSPFv3
  - Opportunity for end-to-end IPSec security between all IPv6 hosts

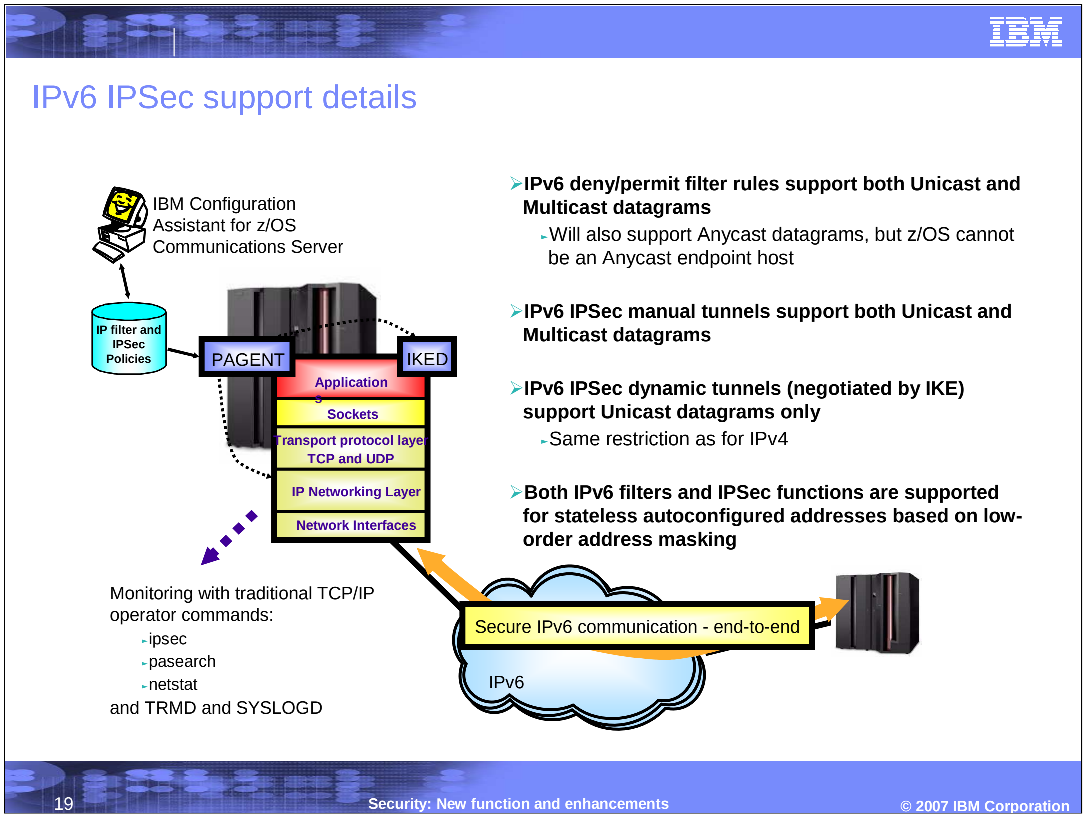
Phase-1

Phase-2



- **z/OS V1R7 re-implemented IPSec support for IPv4:**
  - Fully integrated into Communications Server
  - IP filtering
  - Static IPSec tunnels
  - Dynamic IPSec tunnels (IKE)
  - IPv4 NAT traversal support
  - Simplified configuration and operation
  - Improved scalability and performance

- **z/OS V1R8 extends IPSec support to IPv6**



IBM Configuration Assistant for z/OS Communications Server
IP filter and IPSec Policies
PAGENT
IKED
Application
Sockets
Transport protocol layer
TCP and UDP
IP Networking Layer
Network Interfaces
Secure IPv6 communication - end-to-end
IPv6

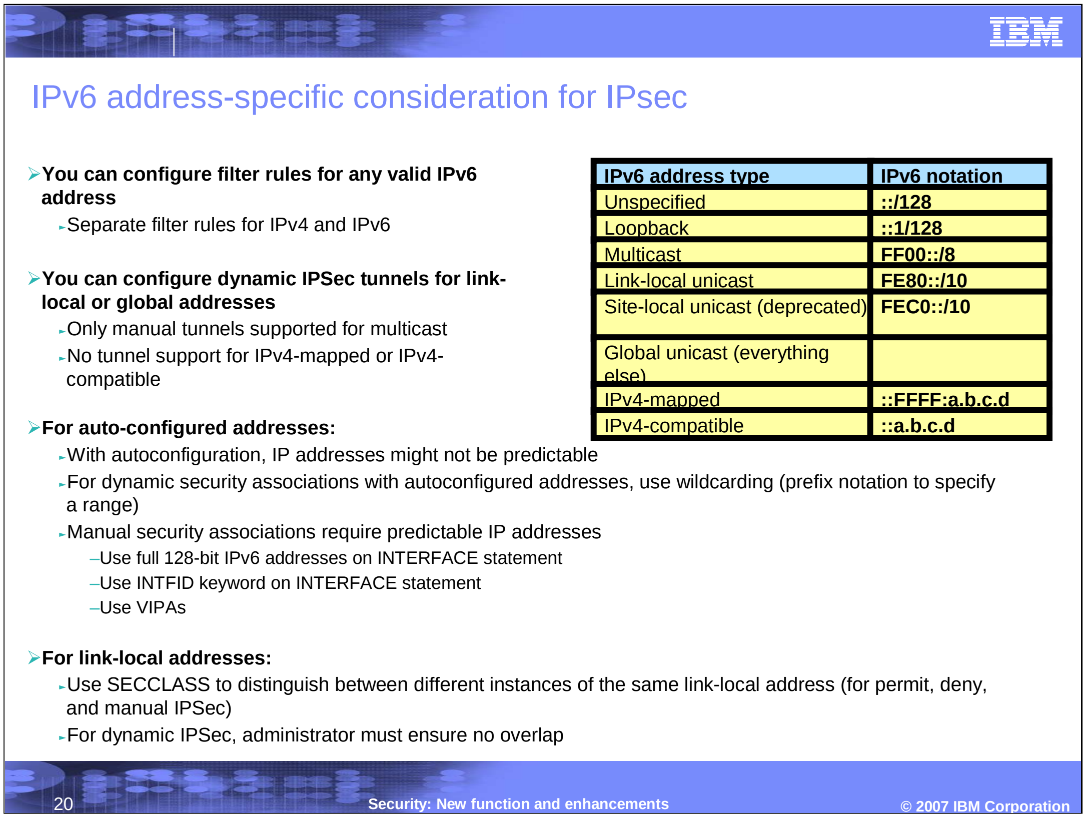
IPv6 IPSec support details

- **IPv6 deny/permit filter rules support both Unicast and Multicast datagrams**
  - Will also support Anycast datagrams, but z/OS cannot be an Anycast endpoint host
- **IPv6 IPSec manual tunnels support both Unicast and Multicast datagrams**
- **IPv6 IPSec dynamic tunnels (negotiated by IKE) support Unicast datagrams only**
  - Same restriction as for IPv4
- **Both IPv6 filters and IPSec functions are supported for stateless autoconfigured addresses based on low-order address masking**

Monitoring with traditional TCP/IP operator commands:

- ipsec
- pasearch
- netstat

and TRMD and SYSLOGD

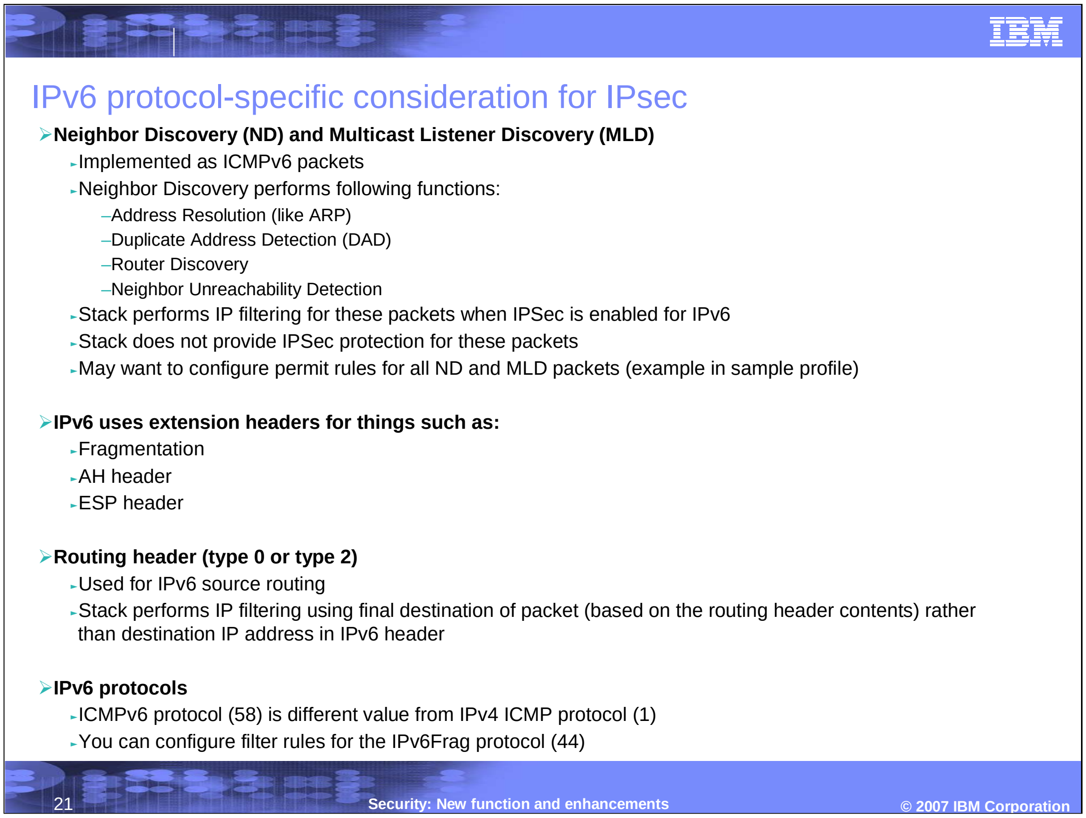


IPv6 address-specific consideration for IPsec

- **You can configure filter rules for any valid IPv6 address**
  - Separate filter rules for IPv4 and IPv6
- **You can configure dynamic IPSec tunnels for link-local or global addresses**
  - Only manual tunnels supported for multicast
  - No tunnel support for IPv4-mapped or IPv4-compatible

IPv6 address type	IPv6 notation
Unspecified	**::/128**
Loopback	**::1/128**
Multicast	**FF00::/8**
Link-local unicast	**FE80::/10**
Site-local unicast (deprecated)	**FEC0::/10**
Global unicast (everything else)	
IPv4-mapped	**::FFFF:a.b.c.d**
IPv4-compatible	**::a.b.c.d**

- **For auto-configured addresses:**
  - With autoconfiguration, IP addresses might not be predictable
  - For dynamic security associations with autoconfigured addresses, use wildcarding (prefix notation to specify a range)
  - Manual security associations require predictable IP addresses
    - Use full 128-bit IPv6 addresses on INTERFACE statement
    - Use INTFID keyword on INTERFACE statement
    - Use VIPAs
- **For link-local addresses:**
  - Use SECCLASS to distinguish between different instances of the same link-local address (for permit, deny, and manual IPSec)
  - For dynamic IPSec, administrator must ensure no overlap



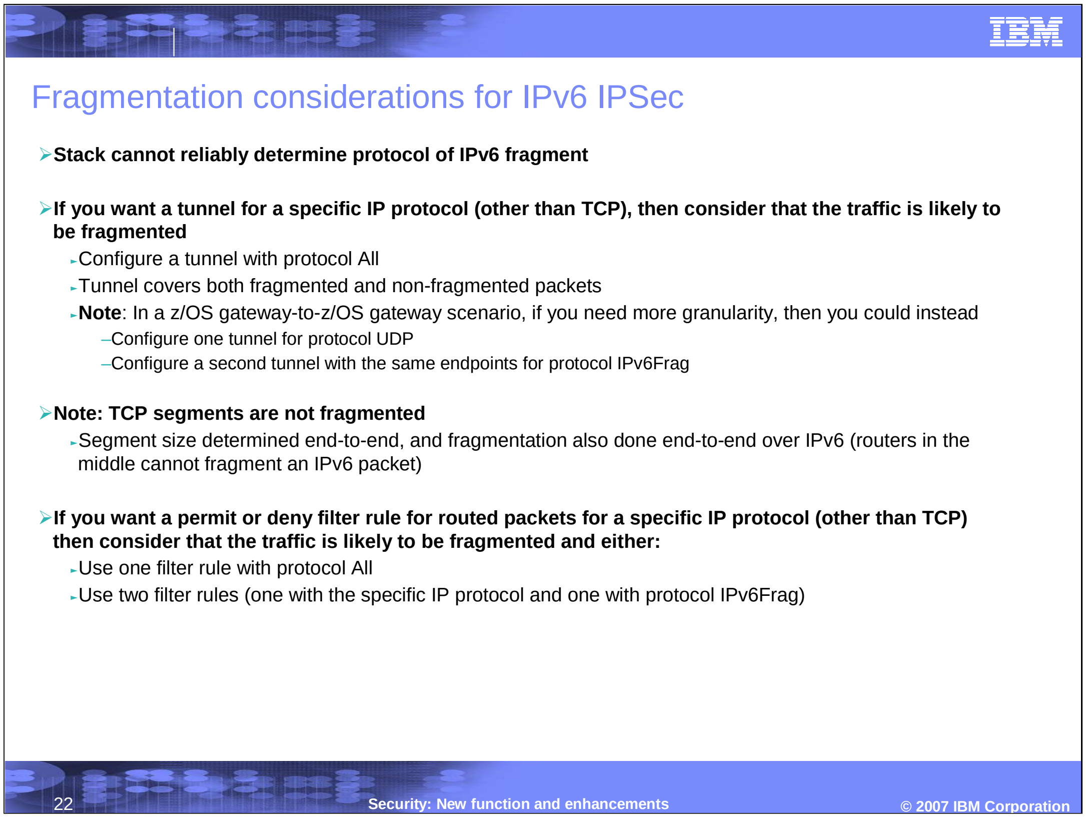
IPv6 protocol-specific consideration for IPsec

- **Neighbor Discovery (ND) and Multicast Listener Discovery (MLD)**
  - Implemented as ICMPv6 packets
  - Neighbor Discovery performs following functions:
    - Address Resolution (like ARP)
    - Duplicate Address Detection (DAD)
    - Router Discovery
    - Neighbor Unreachability Detection
  - Stack performs IP filtering for these packets when IPSec is enabled for IPv6
  - Stack does not provide IPSec protection for these packets
  - May want to configure permit rules for all ND and MLD packets (example in sample profile)

- **IPv6 uses extension headers for things such as:**
  - Fragmentation
  - AH header
  - ESP header

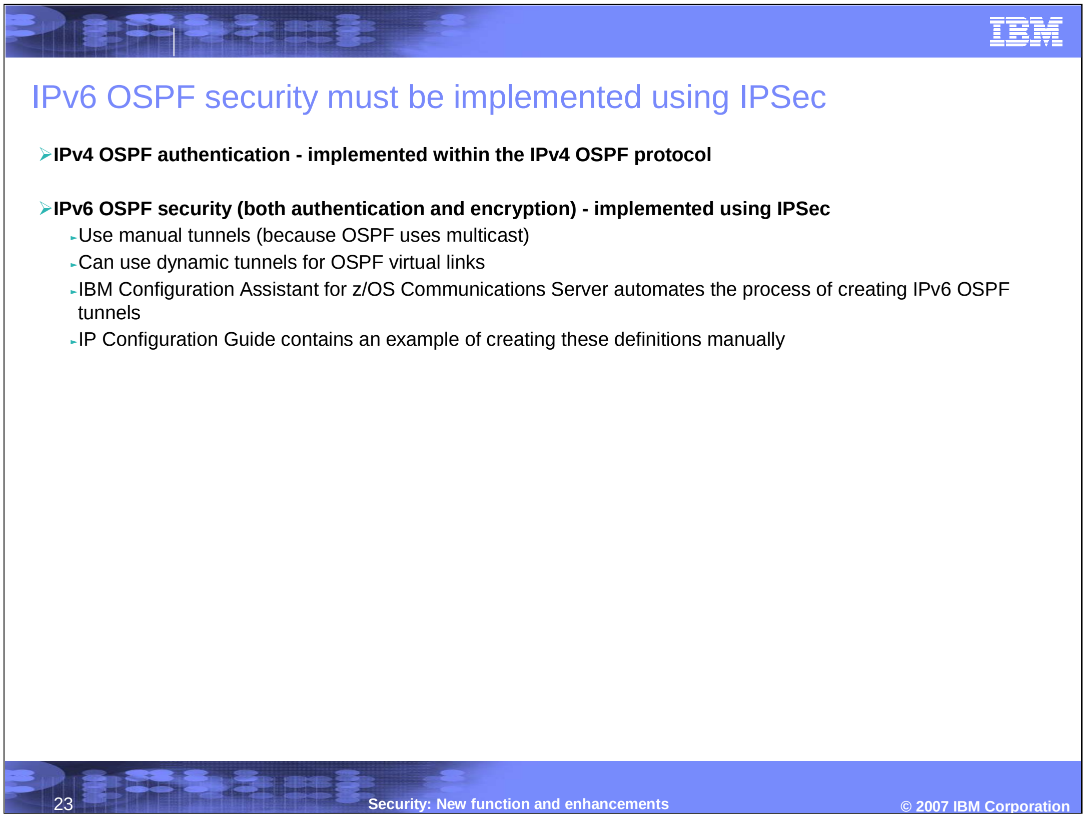
- **Routing header (type 0 or type 2)**
  - Used for IPv6 source routing
  - Stack performs IP filtering using final destination of packet (based on the routing header contents) rather than destination IP address in IPv6 header

- **IPv6 protocols**
  - ICMPv6 protocol (58) is different value from IPv4 ICMP protocol (1)
  - You can configure filter rules for the IPv6Frag protocol (44)



Fragmentation considerations for IPv6 IPSec

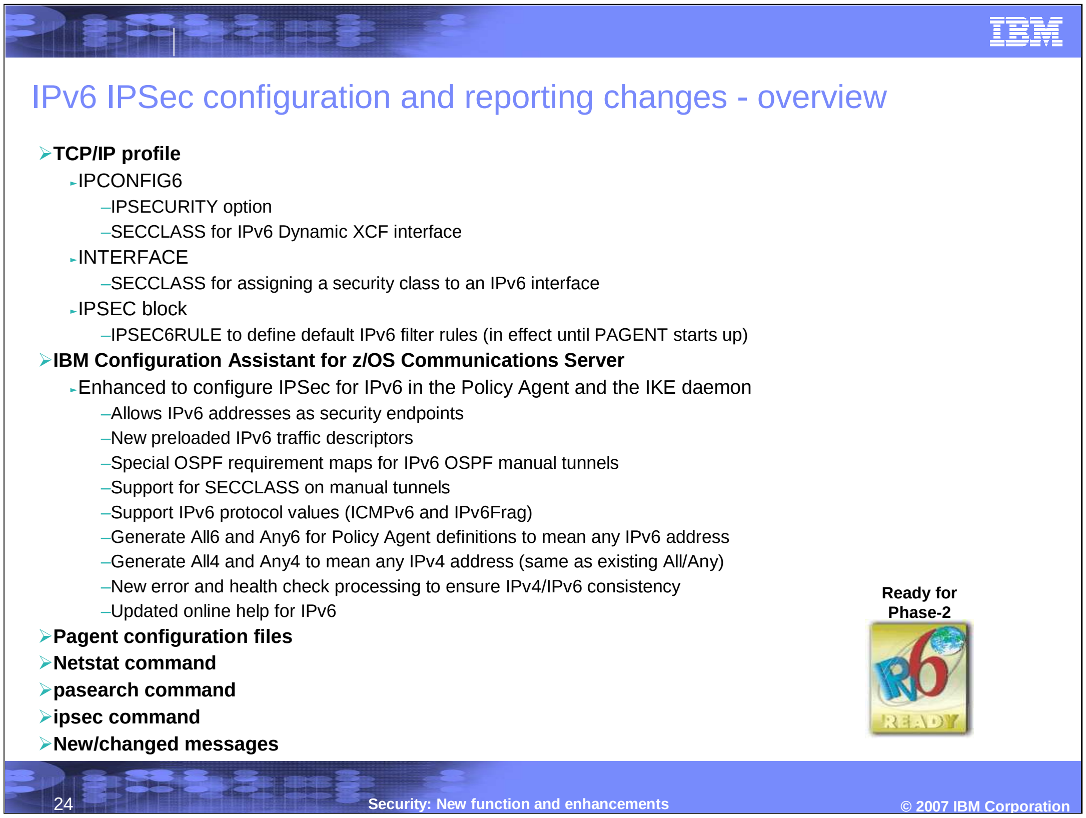
- **Stack cannot reliably determine protocol of IPv6 fragment**
- **If you want a tunnel for a specific IP protocol (other than TCP), then consider that the traffic is likely to be fragmented**
  - Configure a tunnel with protocol All
  - Tunnel covers both fragmented and non-fragmented packets
  - **Note**: In a z/OS gateway-to-z/OS gateway scenario, if you need more granularity, then you could instead
    - Configure one tunnel for protocol UDP
    - Configure a second tunnel with the same endpoints for protocol IPv6Frag
- **Note: TCP segments are not fragmented**
  - Segment size determined end-to-end, and fragmentation also done end-to-end over IPv6 (routers in the middle cannot fragment an IPv6 packet)
- **If you want a permit or deny filter rule for routed packets for a specific IP protocol (other than TCP) then consider that the traffic is likely to be fragmented and either:**
  - Use one filter rule with protocol All
  - Use two filter rules (one with the specific IP protocol and one with protocol IPv6Frag)



IPv6 OSPF security must be implemented using IPSec

- **IPv4 OSPF authentication - implemented within the IPv4 OSPF protocol**

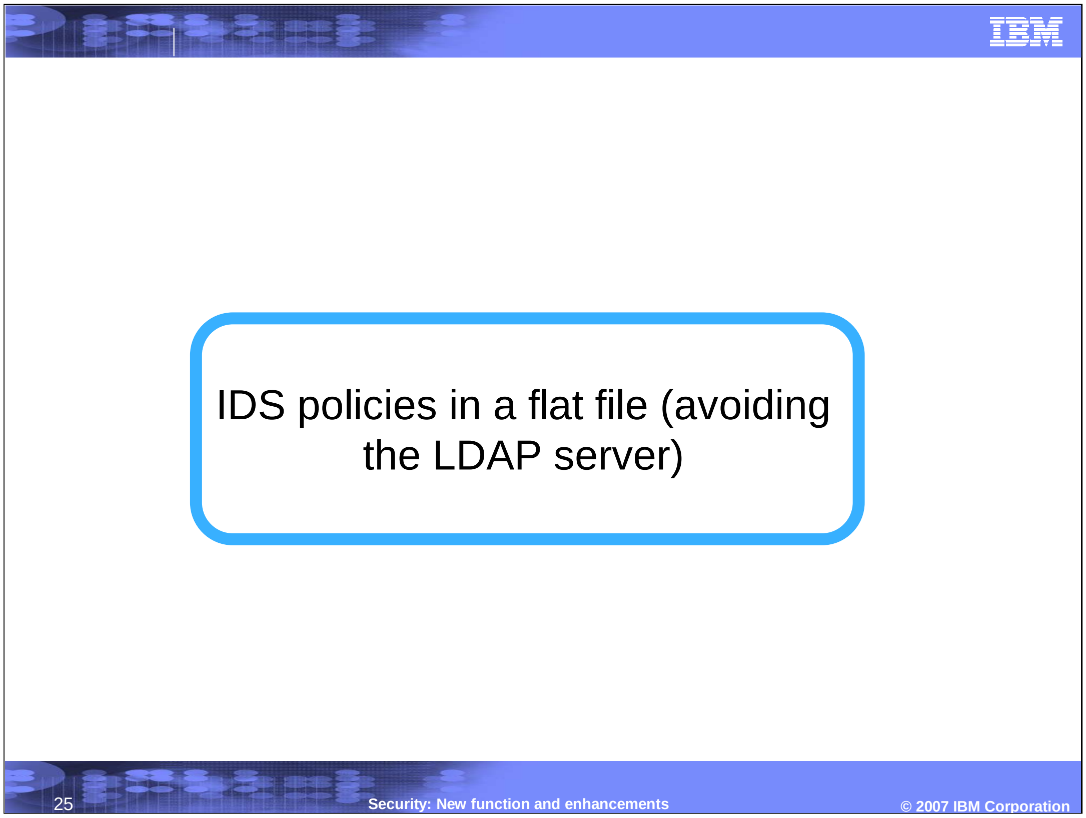
- **IPv6 OSPF security (both authentication and encryption) - implemented using IPSec**
  - Use manual tunnels (because OSPF uses multicast)
  - Can use dynamic tunnels for OSPF virtual links
  - IBM Configuration Assistant for z/OS Communications Server automates the process of creating IPv6 OSPF tunnels
  - IP Configuration Guide contains an example of creating these definitions manually



IPv6 IPSec configuration and reporting changes - overview

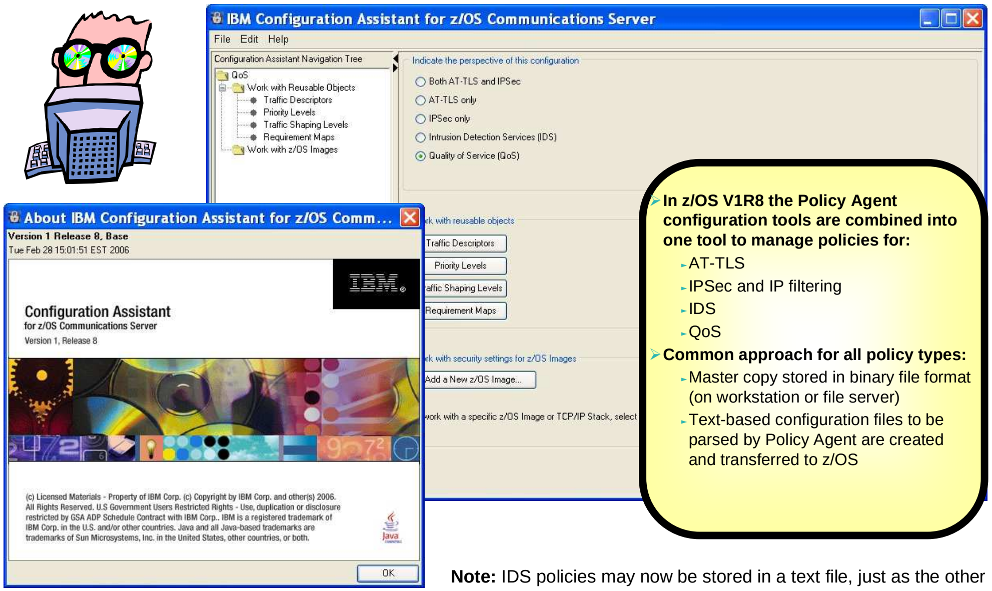
- **TCP/IP profile**
  - IPCONFIG6
    - IPSECURITY option
    - SECCLASS for IPv6 Dynamic XCF interface
  - INTERFACE
    - SECCLASS for assigning a security class to an IPv6 interface
  - IPSEC block
    - IPSEC6RULE to define default IPv6 filter rules (in effect until PAGENT starts up)
- **IBM Configuration Assistant for z/OS Communications Server**
  - Enhanced to configure IPSec for IPv6 in the Policy Agent and the IKE daemon
    - Allows IPv6 addresses as security endpoints
    - New preloaded IPv6 traffic descriptors
    - Special OSPF requirement maps for IPv6 OSPF manual tunnels
    - Support for SECCLASS on manual tunnels
    - Support IPv6 protocol values (ICMPv6 and IPv6Frag)
    - Generate All6 and Any6 for Policy Agent definitions to mean any IPv6 address
    - Generate All4 and Any4 to mean any IPv4 address (same as existing All/Any)
    - New error and health check processing to ensure IPv4/IPv6 consistency
    - Updated online help for IPv6
- **Pagent configuration files**
- **Netstat command**
- **pasearch command**
- **ipsec command**
- **New/changed messages**

Ready for Phase-2



IDS policies in a flat file (avoiding the LDAP server)

IBM Configuration Assistant for z/OS Communications Server



Indicate the perspective of this configuration

○ Both AT-TLS and IPSec
○ AT-TLS only
○ IPSec only
○ Intrusion Detection Services (IDS)
● Quality of Service (QoS)

work with a specific z/OS Image or TCP/IP Stack, select

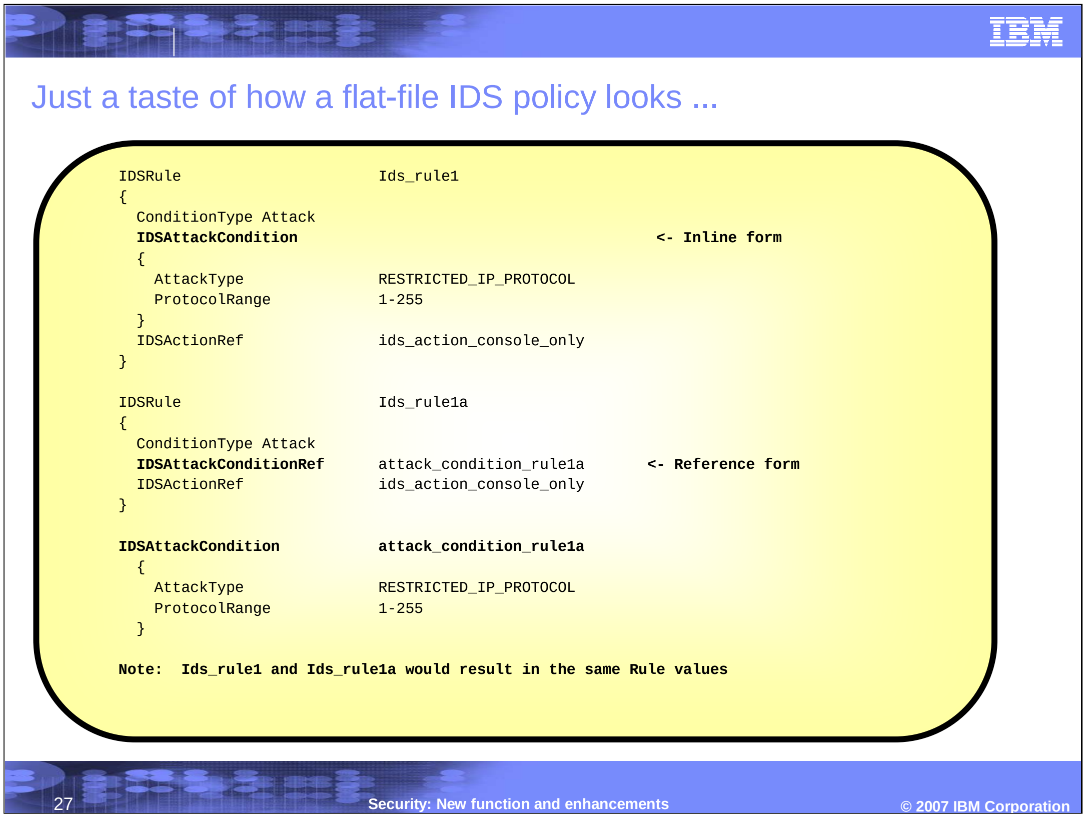
Version 1 Release 8, Base
Tue Feb 28 15:01:51 EST 2006

Configuration Assistant
for z/OS Communications Server
Version 1, Release 8

(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006. 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.

- **In z/OS V1R8 the Policy Agent configuration tools are combined into one tool to manage policies for:**
  - AT-TLS
  - IPSec and IP filtering
  - IDS
  - QoS
- **Common approach for all policy types:**
  - Master copy stored in binary file format (on workstation or file server)
  - Text-based configuration files to be parsed by Policy Agent are created and transferred to z/OS

Note: IDS policies may now be stored in a text file, just as the other policy types. There is no longer a requirement for LDAP.



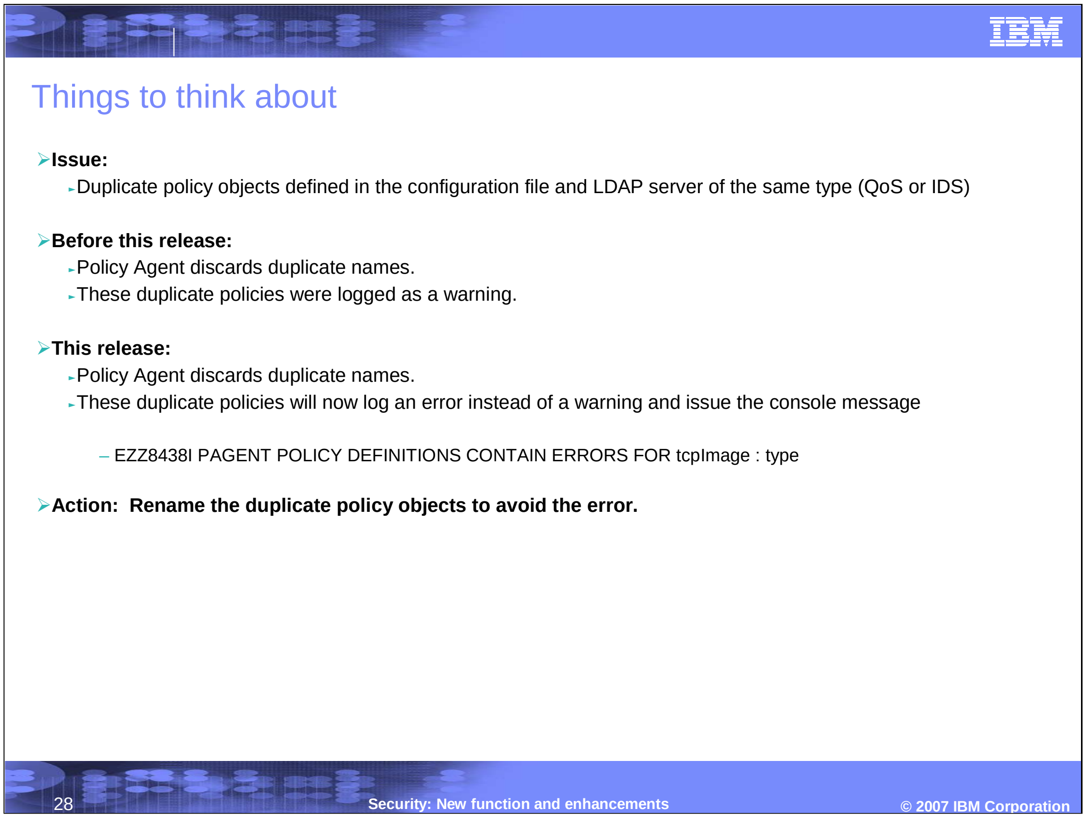
Just a taste of how a flat-file IDS policy looks ...

```
IDSRule                      Ids_rule1
{
  ConditionType Attack
  IDSAttackCondition                                        <- Inline form
  {
    AttackType               RESTRICTED_IP_PROTOCOL
    ProtocolRange            1-255
  }
  IDSActionRef               ids_action_console_only
}

IDSRule                      Ids_rule1a
{
  ConditionType Attack
  IDSAttackConditionRef      attack_condition_rule1a       <- Reference form
  IDSActionRef               ids_action_console_only
}

IDSAttackCondition           attack_condition_rule1a
  {
    AttackType               RESTRICTED_IP_PROTOCOL
    ProtocolRange            1-255
  }
```

Note: Ids_rule1 and Ids_rule1a would result in the same Rule values



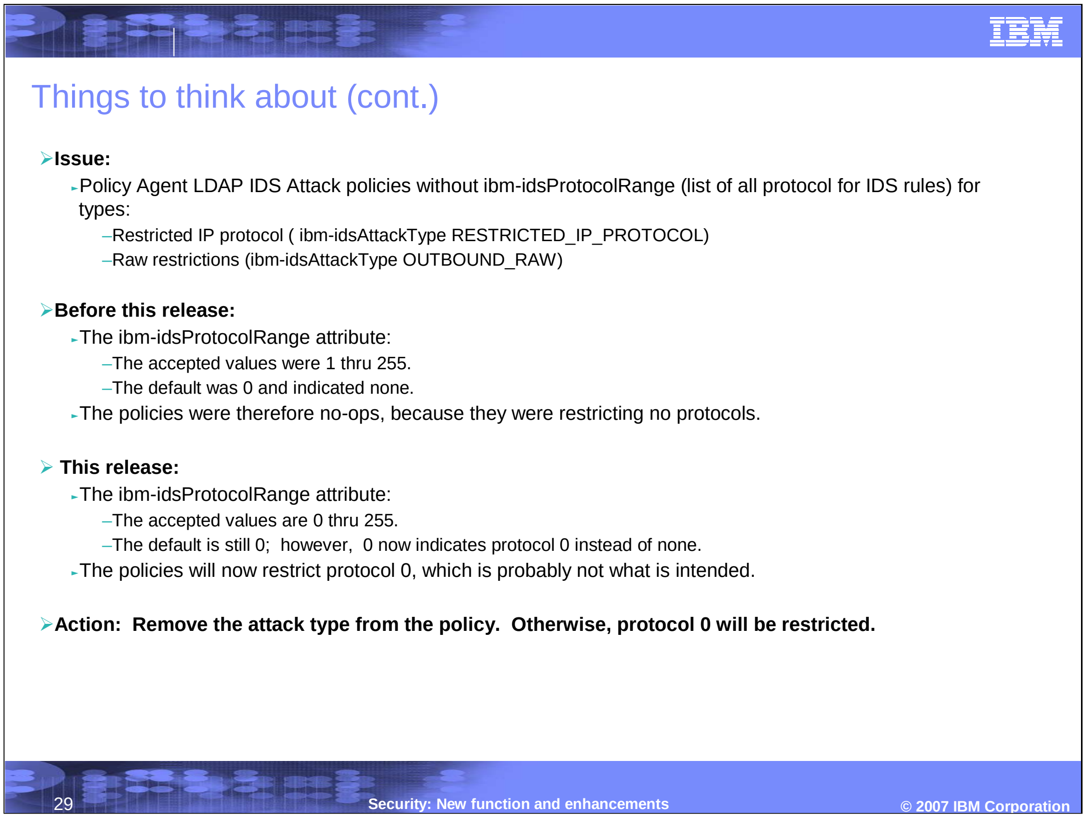
Things to think about

- **Issue:**
  - Duplicate policy objects defined in the configuration file and LDAP server of the same type (QoS or IDS)

- **Before this release:**
  - Policy Agent discards duplicate names.
  - These duplicate policies were logged as a warning.

- **This release:**
  - Policy Agent discards duplicate names.
  - These duplicate policies will now log an error instead of a warning and issue the console message
    - EZZ8438I PAGENT POLICY DEFINITIONS CONTAIN ERRORS FOR tcpImage : type

- **Action: Rename the duplicate policy objects to avoid the error.**



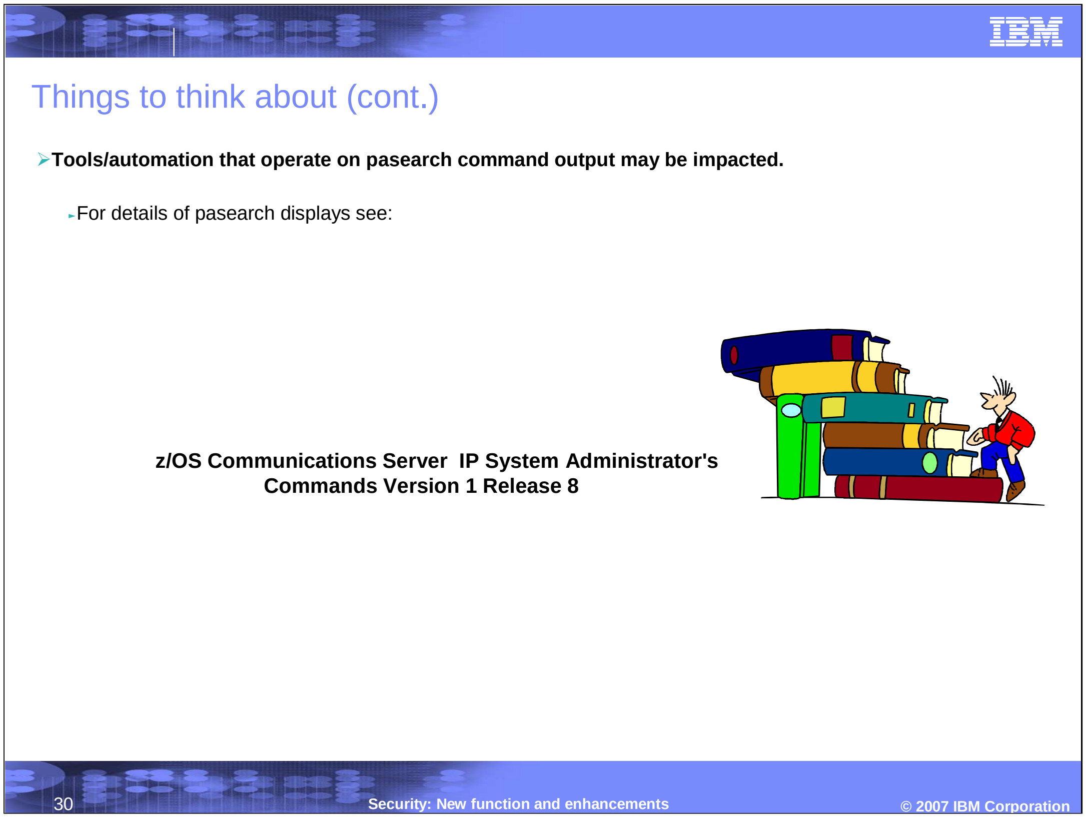
Things to think about (cont.)

- **Issue:**
  - Policy Agent LDAP IDS Attack policies without ibm-idsProtocolRange (list of all protocol for IDS rules) for types:
    - Restricted IP protocol (ibm-idsAttackType RESTRICTED_IP_PROTOCOL)
    - Raw restrictions (ibm-idsAttackType OUTBOUND_RAW)

- **Before this release:**
  - The ibm-idsProtocolRange attribute:
    - The accepted values were 1 thru 255.
    - The default was 0 and indicated none.
  - The policies were therefore no-ops, because they were restricting no protocols.

- **This release:**
  - The ibm-idsProtocolRange attribute:
    - The accepted values are 0 thru 255.
    - The default is still 0; however, 0 now indicates protocol 0 instead of none.
  - The policies will now restrict protocol 0, which is probably not what is intended.

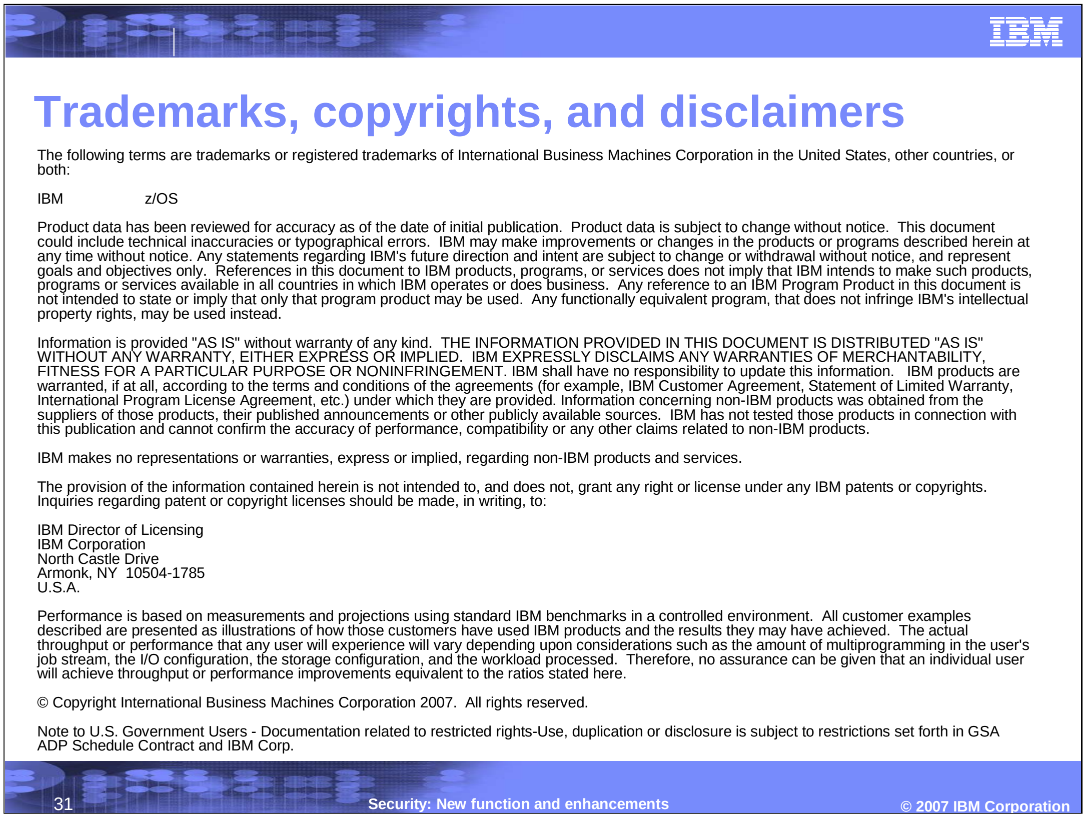
- **Action: Remove the attack type from the policy. Otherwise, protocol 0 will be restricted.**



Things to think about (cont.)

- **Tools/automation that operate on pasearch command output may be impacted.**
  - For details of pasearch displays see:

z/OS Communications Server IP System Administrator's Commands Version 1 Release 8



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	z/OS

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 or changes in the products or programs 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 (for example, 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.