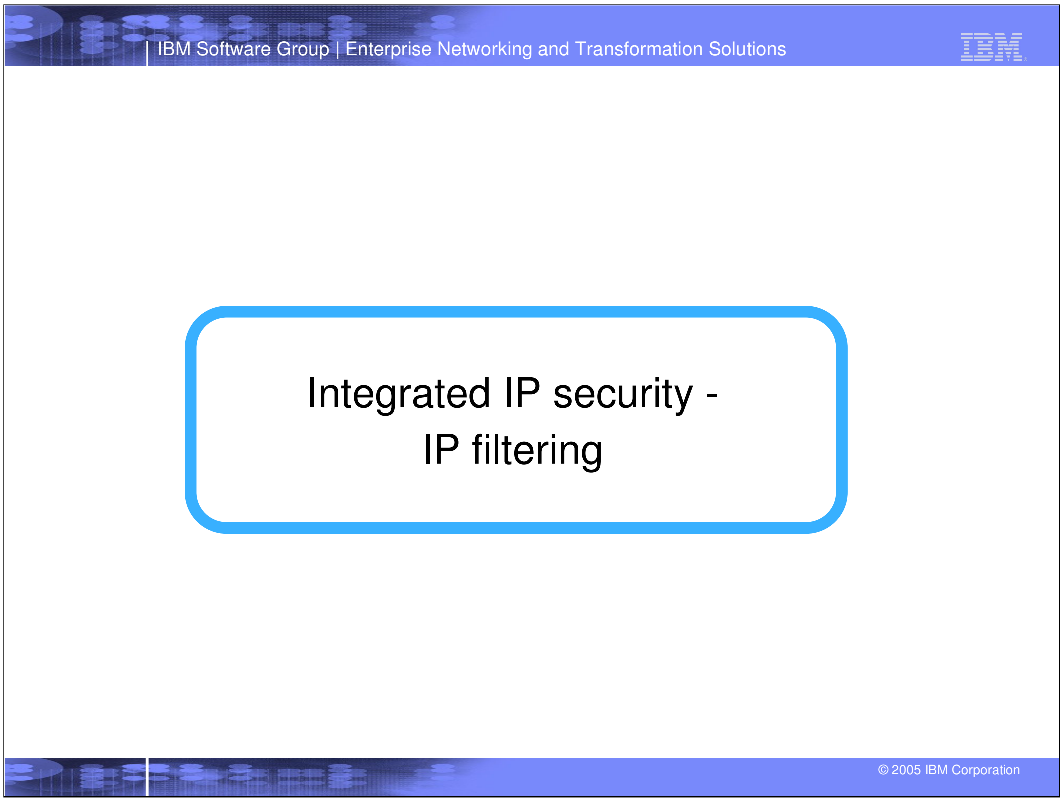
Software Group | Enterprise Networking and Transformation Solutions (ENTS)

CS z/OS Integrated IP Security
IP Filtering



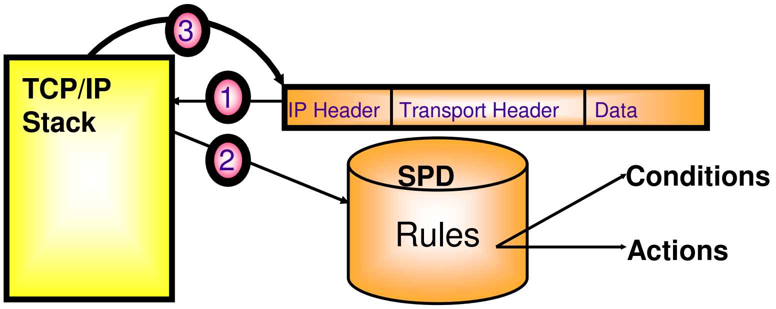
Integrated IP security -
IP filtering

IP filtering overview

1 **Inbound or outbound IP packet arrives**

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

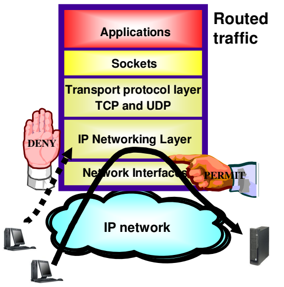
3 **Apply action of matching rule to packet**
- Deny
- Permit
- Permit with additional processing applied

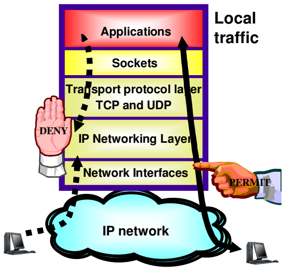


Basics of IP filtering

➢Packet filtering at IP layer

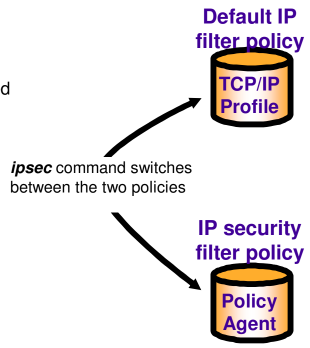
- Filter rules defined to match on inbound and outbound packets based on:
  - Packet information
  - Network attributes
  - Time of day
- Used to control
  - Traffic being routed
  - Access at destination host
- Possible actions
  - 1. Permit
  - 2. Deny
  - 3a. Permit with manual IPSec
  - 3b. Permit with dynamic IPSec
  - Log (in combination with others)





Integrated IP security - filter policies

- **Integrated IPSec's Security Policy Database (SPD)**
  - 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
  - IP security filter policy
    - Intended to be the primary source of filter rules
    - Defined in a Policy Agent IPSec configuration file
      - Can be generated by the z/OS IP Security Configuration Assistant GUI
    - Default is to deny all traffic
  - ***ipsec*** command is used to switch between default and IP security filter policy
- **Requires the IPSECURITY option on the IPCONFIG statement**
  - IPSECURITY option enables use of the new integrated IP security functions
  - The IPSECURITY option is mutually exclusive with the FIREWALL option
    - Separate FIREWALL and IPSECURITY stacks may coexist on one z/OS image



Default IP filter policy

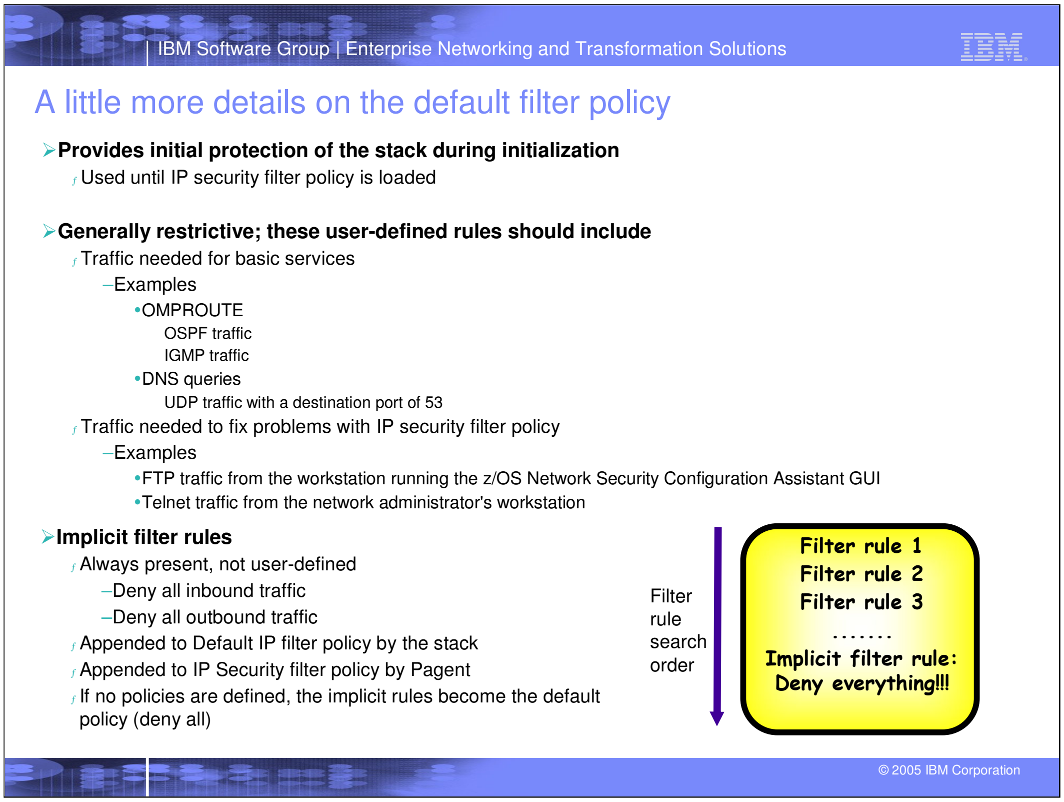
TCP/IP Profile

ipsec command switches between the two policies

IP security filter policy

Policy Agent

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

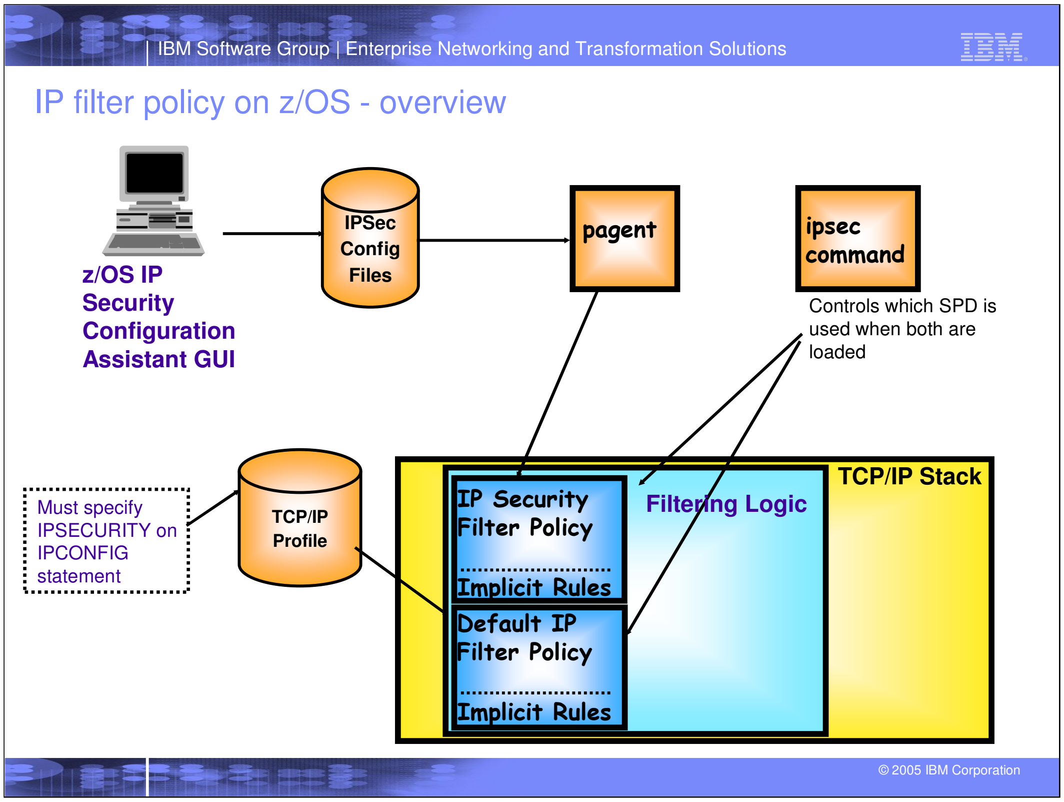


A little more details on the default filter policy

- **Provides initial protection of the stack during initialization**
  - ƒ Used until IP security filter policy is loaded
- **Generally restrictive; these user-defined rules should include**
  - ƒ Traffic needed for basic services
    - –Examples
      - •OMPROUTE
        - OSPF traffic
        - IGMP traffic
      - •DNS queries
        - UDP traffic with a destination port of 53
  - ƒ Traffic needed to fix problems with IP security filter policy
    - –Examples
      - •FTP traffic from the workstation running the z/OS Network Security Configuration Assistant GUI
      - •Telnet traffic from the network administrator's workstation
- **Implicit filter rules**
  - ƒ Always present, not user-defined
    - –Deny all inbound traffic
    - –Deny all outbound traffic
  - ƒ Appended to Default IP filter policy by the stack
  - ƒ Appended to IP Security filter policy by Pagent
  - ƒ If no policies are defined, the implicit rules become the default policy (deny all)

Filter rule search order

Filter rule 1
Filter rule 2
Filter rule 3
....
Implicit filter rule:
Deny everything!!!



IP filter policy on z/OS - overview

z/OS IP Security Configuration Assistant GUI

IPSec Config Files

pagent

ipsec command

Controls which SPD is used when both are loaded

Must specify IPSECURITY on IPCONFIG statement

TCP/IP Profile

TCP/IP Stack

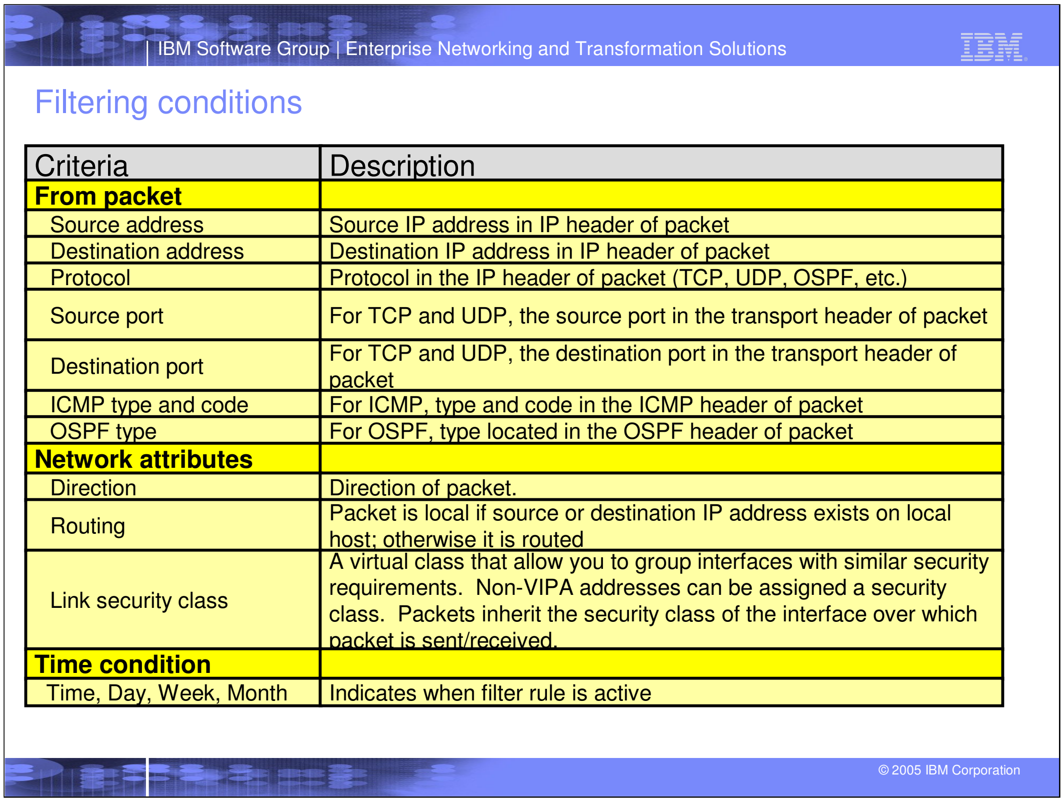
IP Security Filter Policy

Implicit Rules

Default IP Filter Policy

Implicit Rules

Filtering Logic



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

Interface security class (SECCLASS)

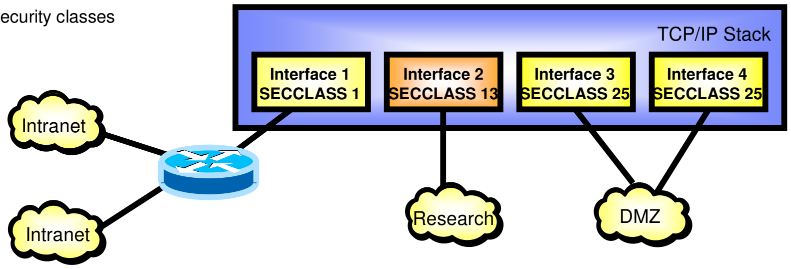
- **Can be assigned only to non-virtual interfaces**

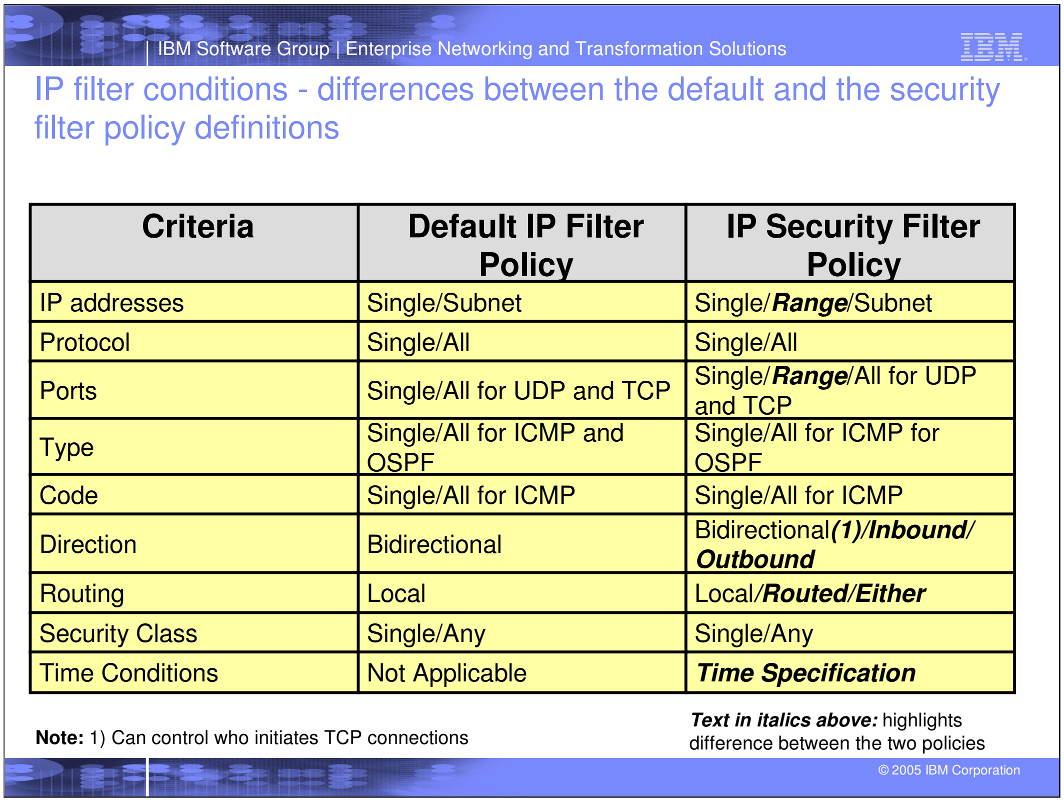
- **Defined in the TCP/IP profile**
  - LINK statement (SECCLASS parameter)
  - IPCONFIG DYNAMICXCF statement (SECCLASS parameter)

- **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



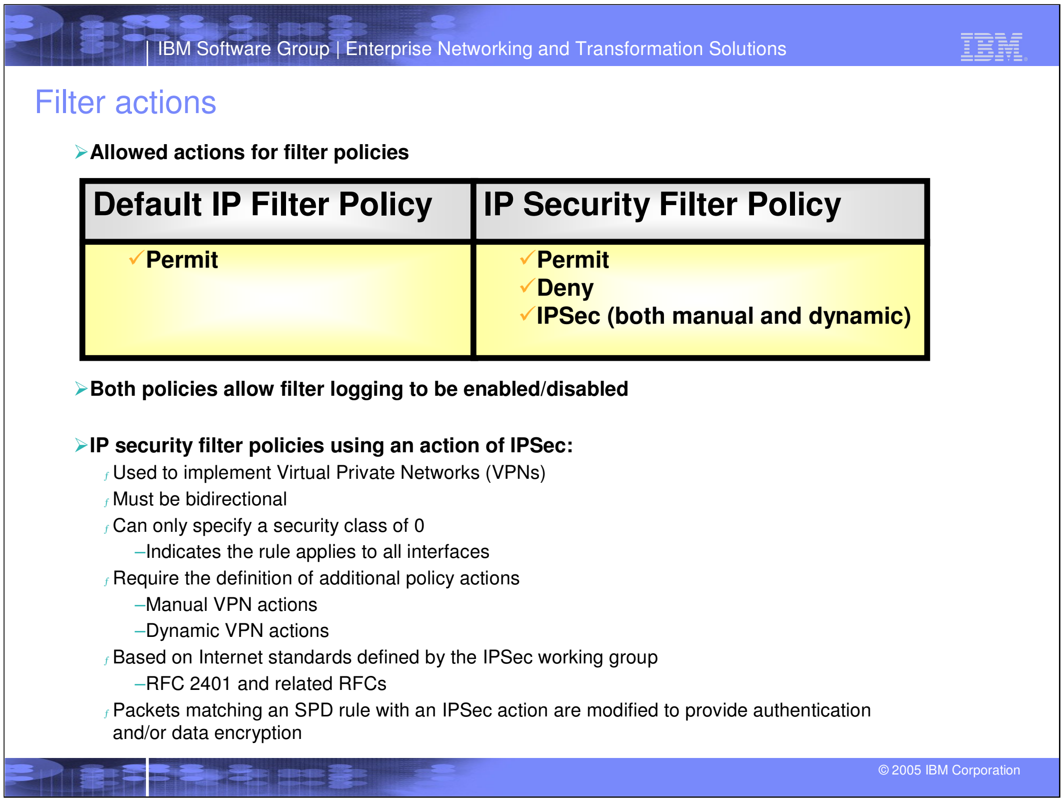


IP filter conditions - differences between the default and the security filter policy definitions

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	Bidirectional***(1)/Inbound/ Outbound***
Routing	Local	Local/***Routed***/***Either***
Security Class	Single/Any	Single/Any
Time Conditions	Not Applicable	***Time Specification***

Note: 1) Can control who initiates TCP connections

Text in italics above: highlights difference between the two policies



Filter actions

- **Allowed actions for filter policies**

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:**
  - Used to implement Virtual Private Networks (VPNs)
  - 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
  - Based on Internet standards defined by the IPSec working group
    - RFC 2401 and related RFCs
  - Packets matching an SPD rule with an IPSec action are modified to provide authentication and/or data encryption

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.