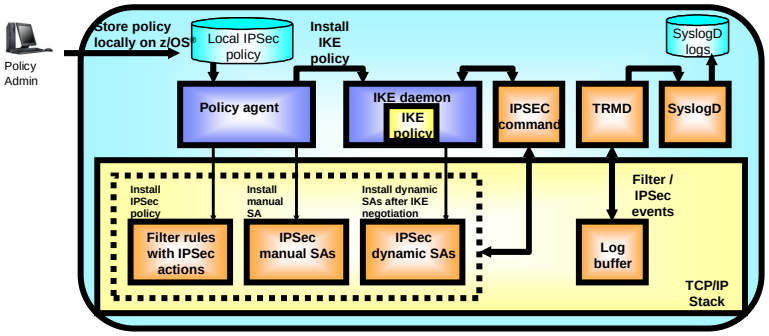
IBM eServer™

Security: Background information

ebusiness on demand software

Integrated IP security infrastructure in z/OS V1R7

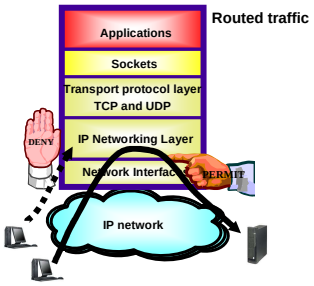


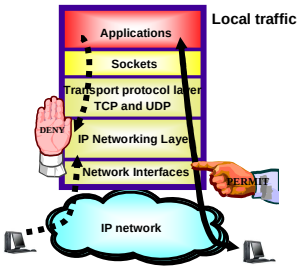
- **Integrated IP security in z/OS V1R7 covers:**
  - IP filtering
  - Virtual private networks based on IPSec
  - IPv4 only

- **Configuration support**
  - Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
  - NAT IP address traversal support
- **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, new IPSec command

Basics of IP filtering

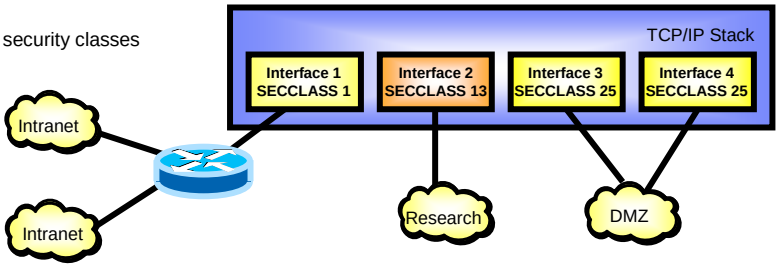
- **Packet filtering at IP layer**
  - Filter rules defined to match on inbound and outbound packets based on:
    - Packet information
    - Network attributes
    - Time of day
  - Used to control
    - Traffic being routed
    - Access at destination host
  - Possible actions
    - 1. Permit
    -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





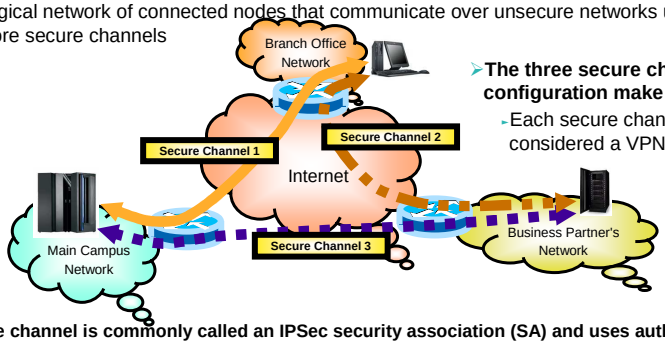
Interface security class (SECCLASS)

- **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



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



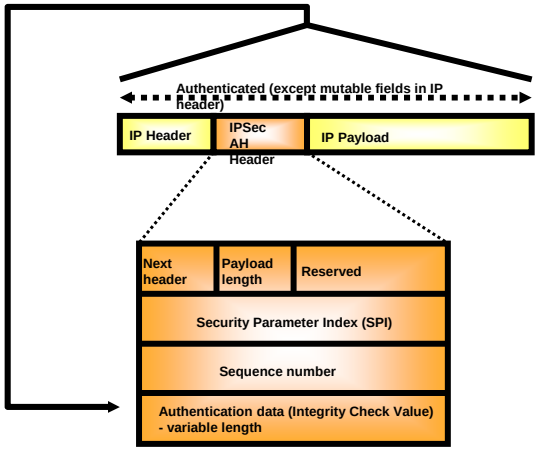
- **The three secure channels in this sample configuration make up a VPN**
  - Each secure channel in itself can be considered a VPN
- **A secure channel is commonly called an IPSec security association (SA) and uses authentication and/or encryption**
  - The term "tunnel" is also sometimes used in this 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

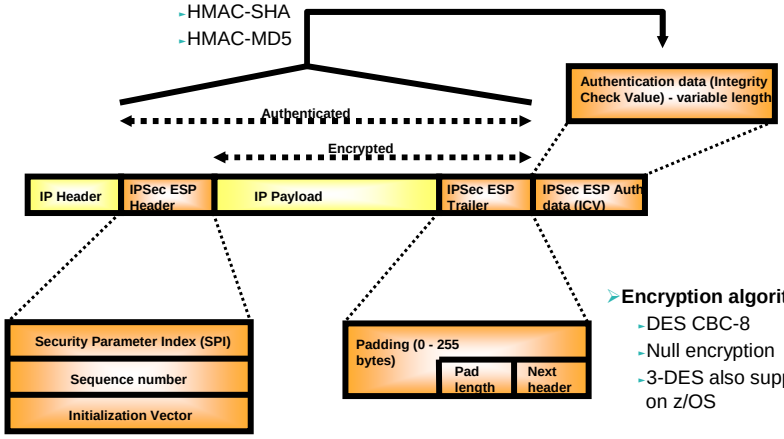
- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



- **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

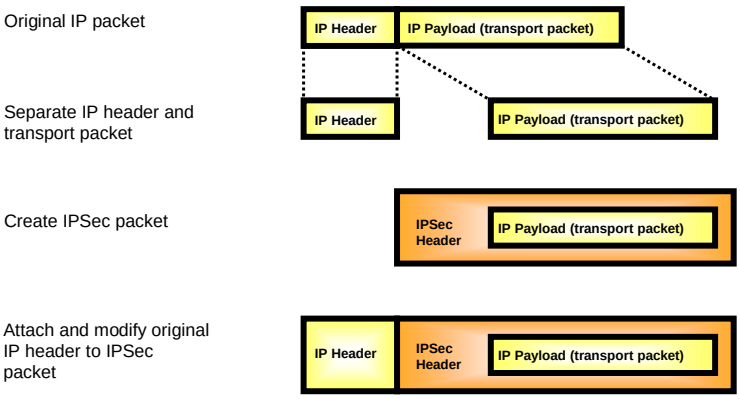
- **Authentication algorithms**
  - HMAC-SHA
  - HMAC-MD5



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

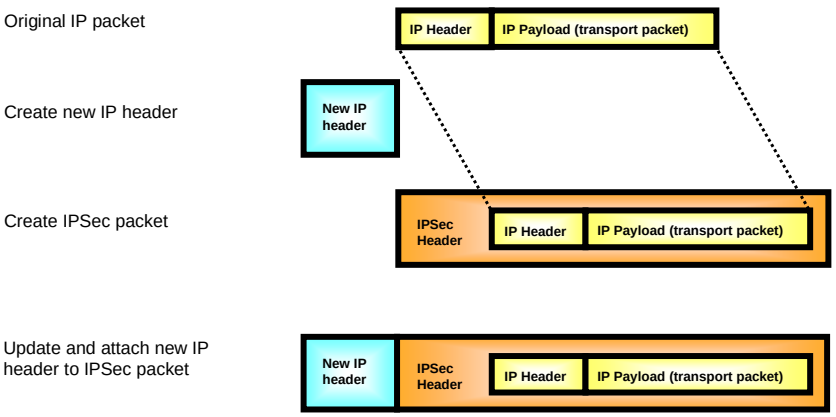
- **If transport mode, then "Payload" contains the original transport header and original data (possibly encrypted)**
- **If tunnel mode, then "Payload" contains original IP header, original transport header, and original data**
  - "Payload" can be encrypted

IPSec VPN concepts - creating an IPSec packet using transport mode



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

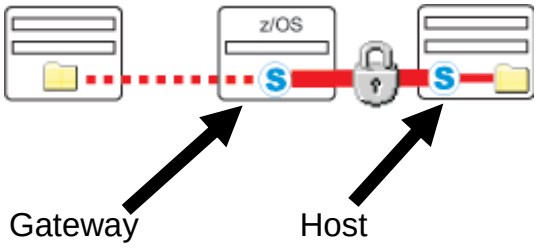
IPSec VPN concepts - creating an IPSec packet using tunnel mode

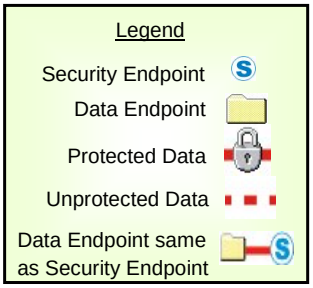


Tunnel mode is used if at least one of the two IPSec VPN endpoints is a gateway.

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





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 - 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

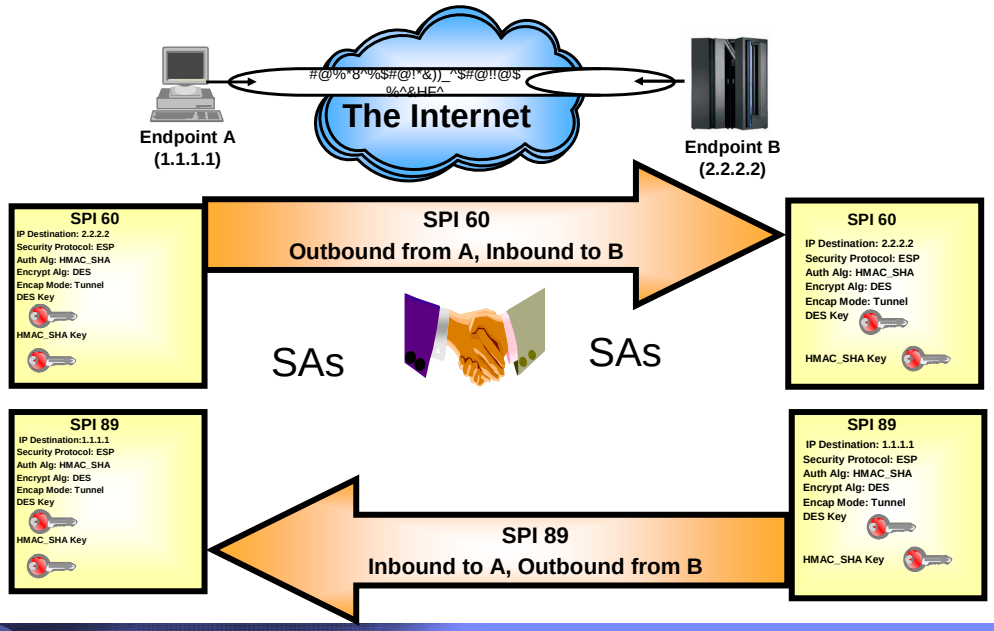
- **An SA is identified by:**
  - A Security Parameter Index (SPI)
    - The SPI is a 32-bit value
    - SPI numbers in themselves may not be unique on a given IPSec node
    - The SPI is carried in the IPSec headers
  - IPSec protocol
  - Destination IP address information

- **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



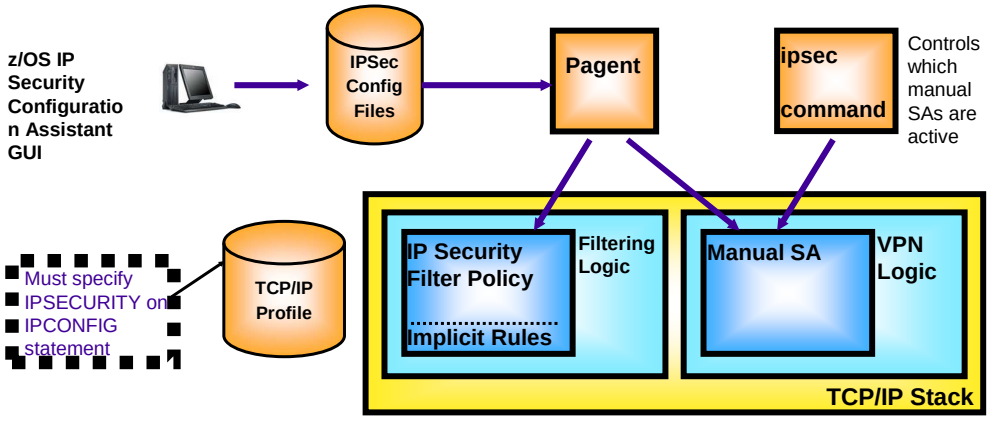
IPSec VPN concepts - manually defined SAs

- **Not commonly used**
  - Do not provide a scalable solution
  - In the long run difficult to manage
- **Require the IPSECURITY option on the IPCONFIG statement**
  - Mutually exclusive with the FIREWALL option
- **Defined in a Pagent IPSec configuration file**
  - Cannot be used when default filter policy is in effect
  - Utilized by filter rules with an action of "ipsec"
  - 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**
  - 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.

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.

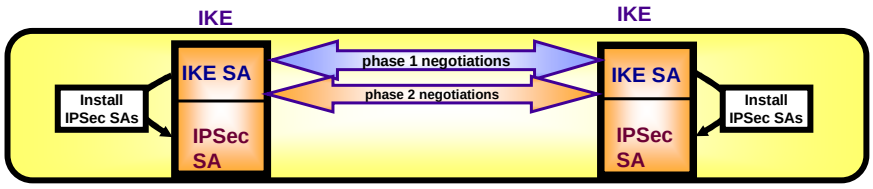


IPSec VPN concepts - dynamically defined SAs

- **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

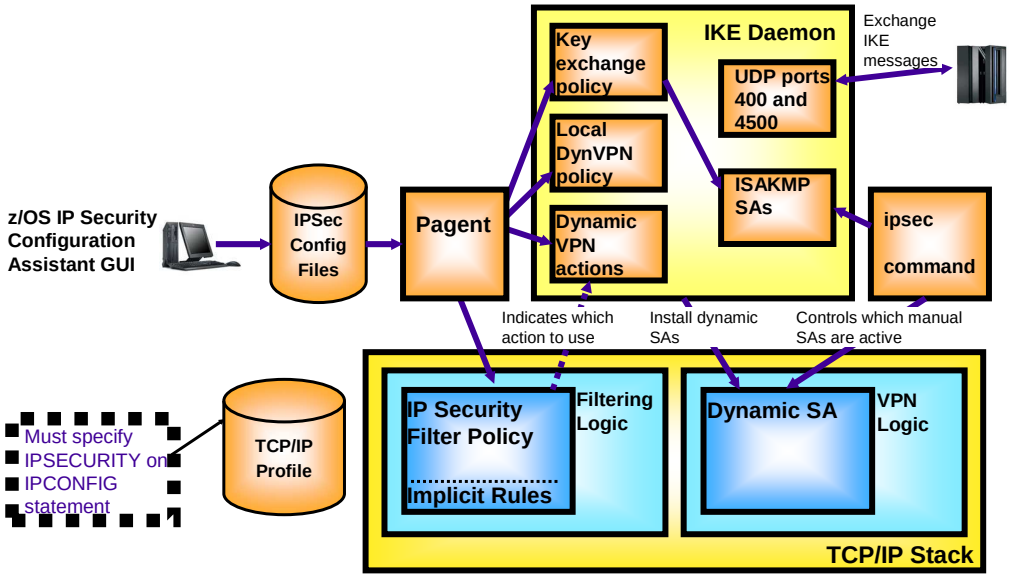
- **Phase 1 negotiation**
  - Creates a secure channel with a remote security endpoint
    - Negotiates an IKE SA
      - Generates cryptographic keys that will be used to protect Phase 2 negotiations and Informational exchanges
      - Authenticates the identity of the parties involved
      - Bidirectional, 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 - integrated IP Security dynamic SAs overview



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.