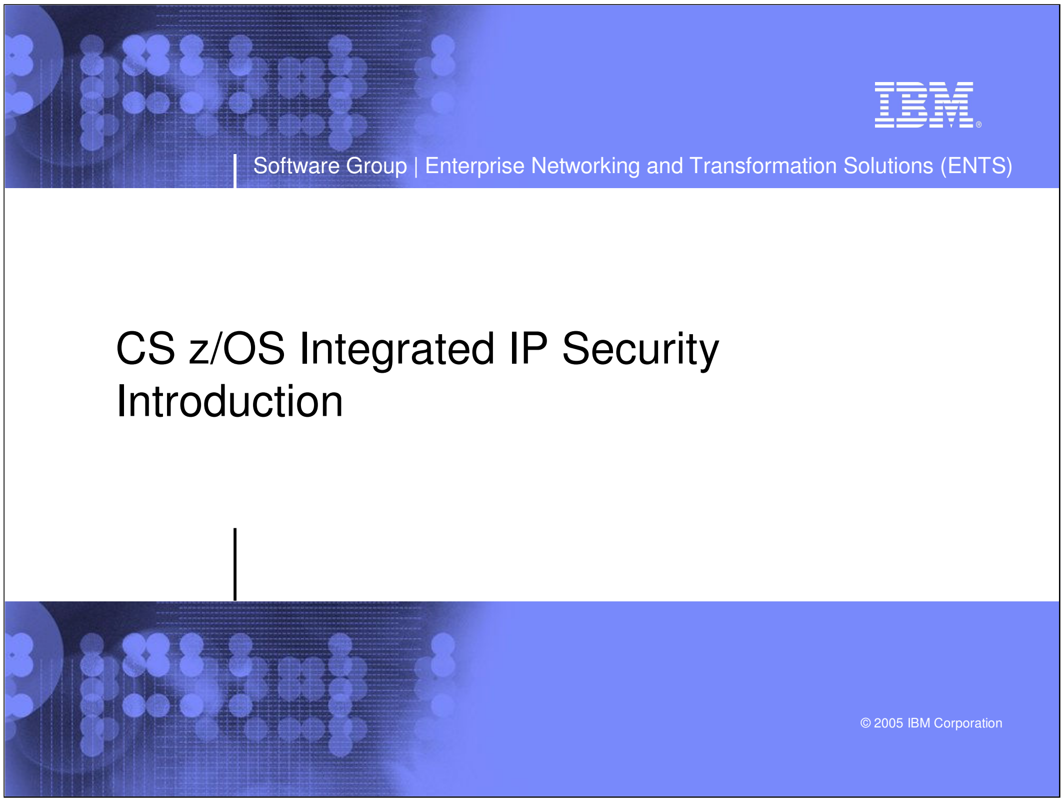
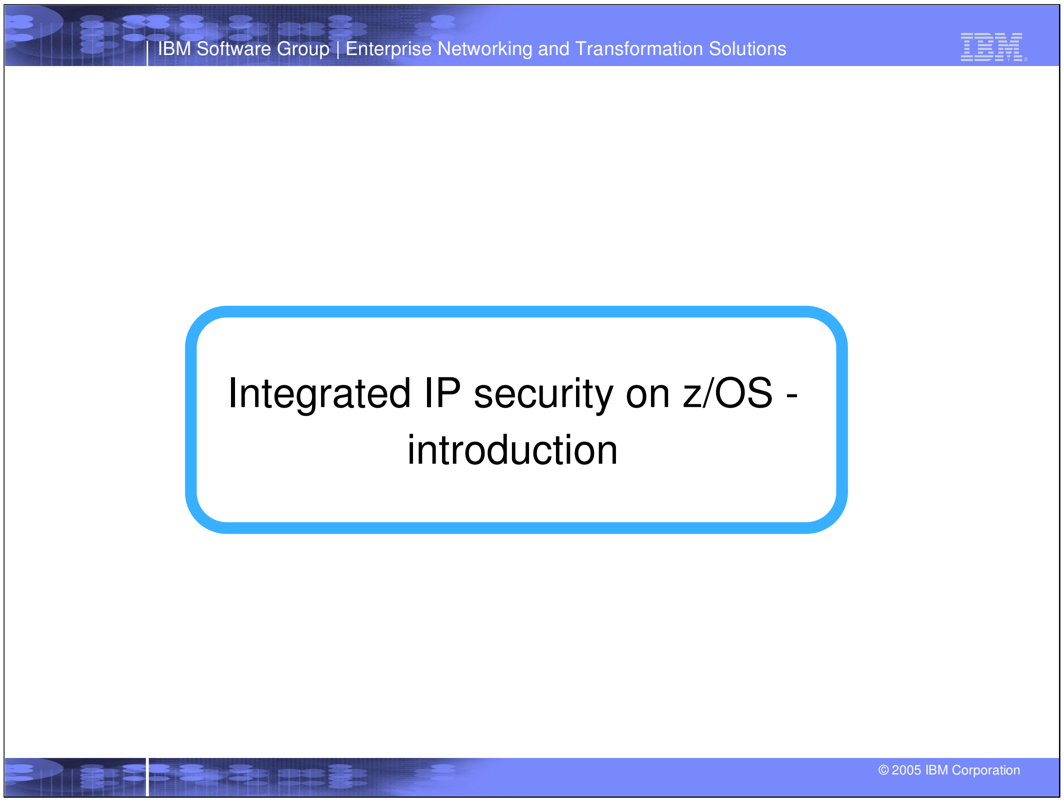
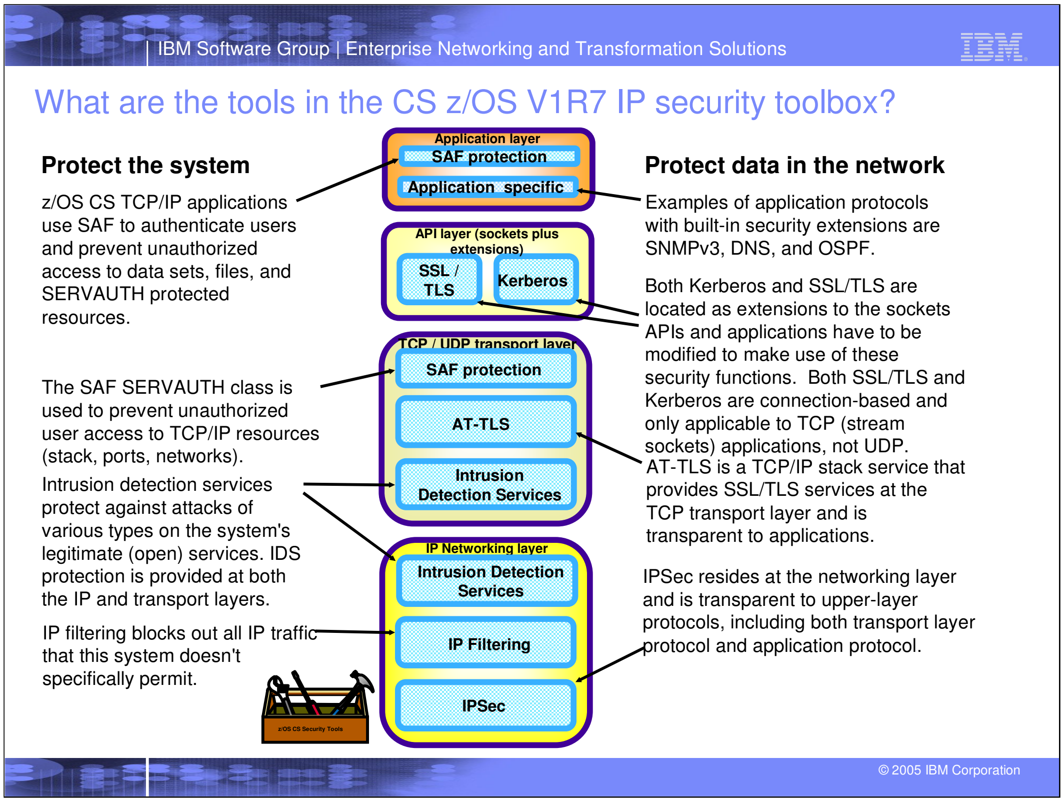


CS z/OS Integrated IP Security Introduction



Integrated IP security on z/OS - introduction



What are the tools in the CS z/OS V1R7 IP security toolbox?

Protect the system

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

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

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

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

Protect data in the network

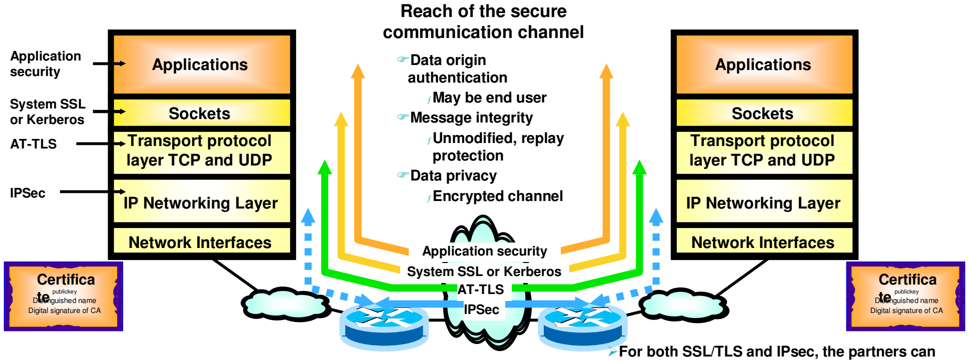
Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.

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

AT-TLS is a TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to applications.

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

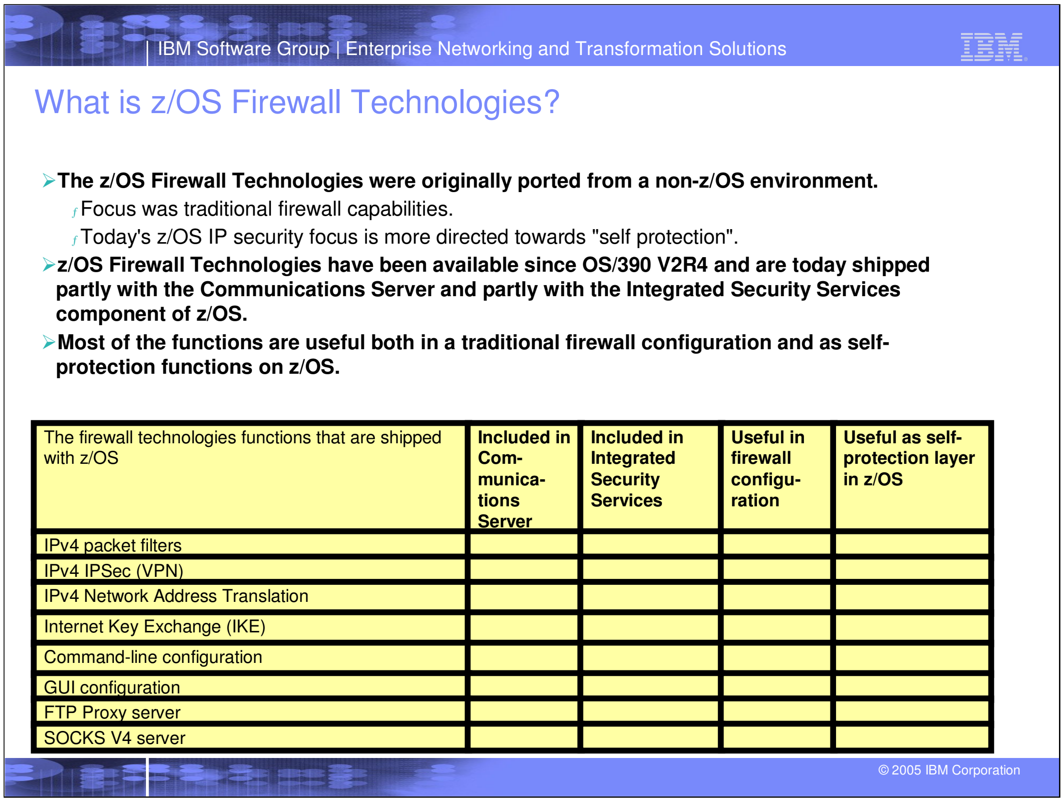
Secure network communication between two endpoints



- Data origin authentication
  - May be end user
- Message integrity
  - Unmodified, replay protection
- Data privacy
  - Encrypted channel

- For both SSL/TLS and IPsec, the partners can authenticate each other based on digital certificates, and perform a public/private key encryption handshake to generate and exchange a symmetric encryption session key to be used for encrypting and decrypting the data between the partners.
  - SSL/TLS defines this as the handshake phase
  - For IPsec it is part of the IKE negotiation

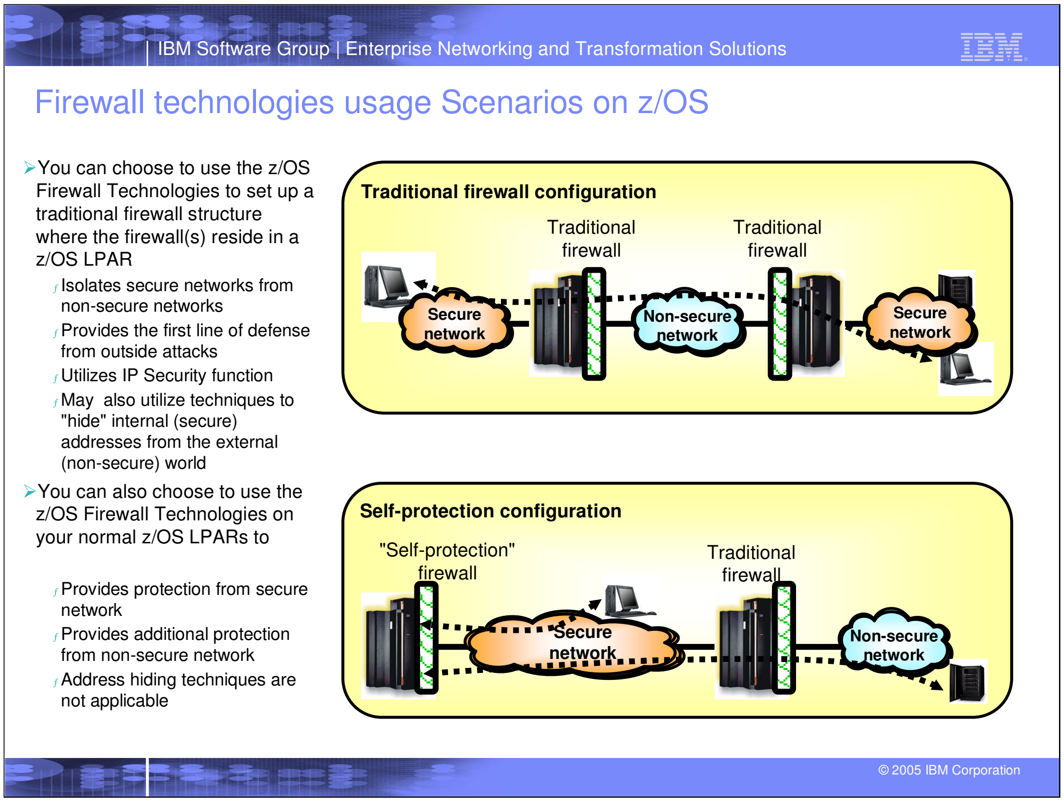
- **Message level security at the application layer**
  - Secure Network Services (SNMPv3, Secure DNS) - always end-to-end
- **Socket layer security service**
  - TLS/SSL, Kerberos - always end-to-end and TCP only
- **Transparent application security services over IP network**
  - IPSec provides blanket protection for all IP applications - end-to-end or segment of data path between two VPN routers
  - Application transparent TLS -provides connection level protection for TCP applications - always end-to-end
  - SSL TN3270 securely extends reach of SNA applications over IP network - TN3270 client to TN3270 server data path secured
  - SNA Session Level Encryption - secures SNA session traffic transparently between two SNA application end points (LUs) of which one end could be the TN3270 server and the other the final SNA application



What is z/OS Firewall Technologies?

- **The z/OS Firewall Technologies were originally ported from a non-z/OS environment.**
  - Focus was traditional firewall capabilities.
  - Today's z/OS IP security focus is more directed towards "self protection".
- **z/OS Firewall Technologies have been available since OS/390 V2R4 and are today shipped partly with the Communications Server and partly with the Integrated Security Services component of z/OS.**
- **Most of the functions are useful both in a traditional firewall configuration and as self-protection functions on z/OS.**

The firewall technologies functions that are shipped with z/OS	**Included in Communications Server**	**Included in Integrated Security Services**	**Useful in firewall configuration**	**Useful as self-protection layer in z/OS**
IPv4 packet filters				
IPv4 IPSec (VPN)				
IPv4 Network Address Translation				
Internet Key Exchange (IKE)				
Command-line configuration				
GUI configuration				
FTP Proxy server				
SOCKS V4 server				



Firewall technologies usage Scenarios on z/OS

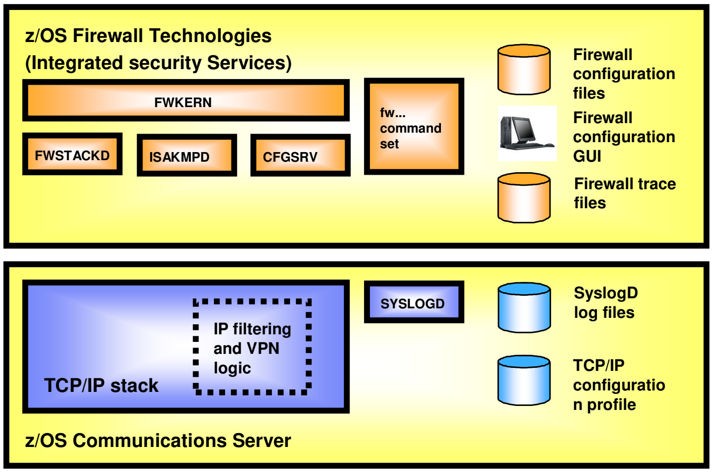
- You can choose to use the z/OS Firewall Technologies to set up a traditional firewall structure where the firewall(s) reside in a z/OS LPAR
  - Isolates secure networks from non-secure networks
  - Provides the first line of defense from outside attacks
  - Utilizes IP Security function
  - May also utilize techniques to "hide" internal (secure) addresses from the external (non-secure) world
- You can also choose to use the z/OS Firewall Technologies on your normal z/OS LPARs to
  - Provides protection from secure network
  - Provides additional protection from non-secure network
  - Address hiding techniques are not applicable

Traditional firewall configuration

Self-protection configuration

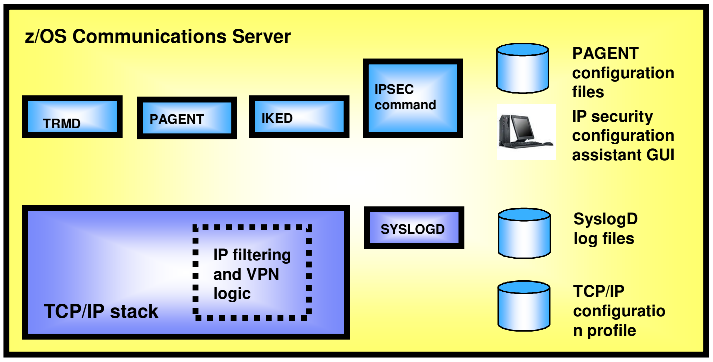
Customer-identified issues with the current firewall technologies implementation

- **z/OS Communications Server prior to z/OS V1R7 does not provide all the elements required for IP Security**
  - z/OS Firewall Technologies must be installed and configured
  - Documentation split across multiple z/OS elements
  - Configuration does not exploit z/OS Communications Server configuration techniques
    - Policy Agent (Pagent)
  - Firewall command set is large
  - Overhead to maintain firewall servers (fwkern, fwstackd, isakmpd, and cfgsrv)
  - Service ambiguity
    - Which service group is responsible for an IP Security problem
  - Scalability and performance in general

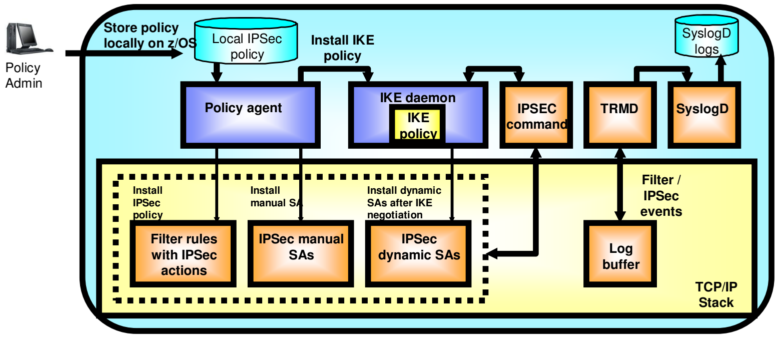

z/OS Firewall Technologies
(Integrated security Services)
FWKERN
FWSTACKD
ISAKMPD
CFGSRV
fw... command set
Firewall configuration files
Firewall configuration GUI
Firewall trace files
TCP/IP stack
IP filtering and VPN logic
SYSLOGD
SyslogD log files
TCP/IP configuratio n profile
z/OS Communications Server

Integrated IP Security in z/OS V1R7

- **Provide a z/OS Communications Server alternative to using the z/OS Firewall Technologies IP Security support**
  - Provide a Communications Server equivalent to z/OS Firewall Technologie's ISAKMPD
  - Eliminate the need to run z/OS Firewall Technologies's fwkern, fwstackd, and cfgsrv
  - Provide a Pagent-based configuration file to replace the existing z/OS Firewall Technologies configuration commands.
  - Provide one new UNIX System Service command to replace the multiple existing z/OS Firewall Technologies IP security management commands.
  - Continue to ship the z/OS Firewall Technologies IPSec support in z/OS V1R7
    - In a future release z/OS Firewall Technologies will no longer be shipped (this includes the IP Security functions and the additional traditional firewall functions (NAT, SOCKS, and FTP proxy))
  - A stack can use Integrated IPSec or z/OS Firewall Technologies IPSec, but not both
  - In z/OS V1R7, Integrated IP Security is an IPv4-only solution


z/OS Communications Server
TRMD
PAGENT
IKED
IPSEC command
PAGENT configuration files
IP security configuration assistant GUI
TCP/IP stack
IP filtering and VPN logic
SYSLOGD
SyslogD log files
TCP/IP configuratio n profile

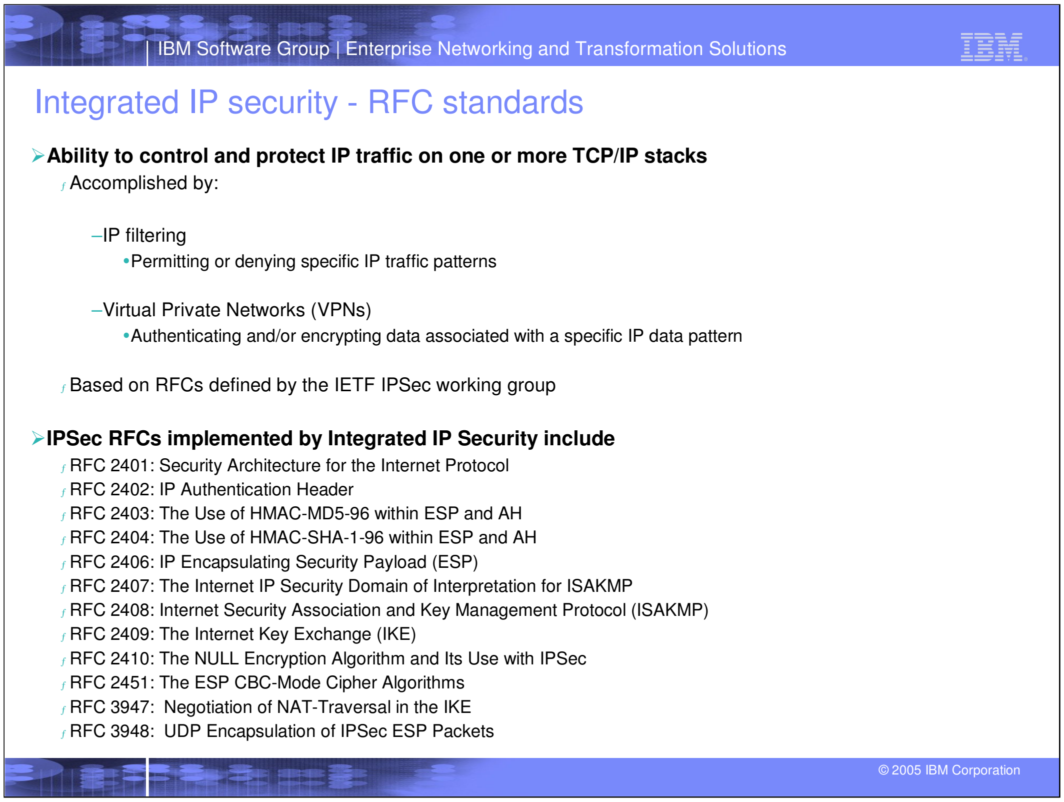
Integrated IP security infrastructure in z/OS V1R7



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

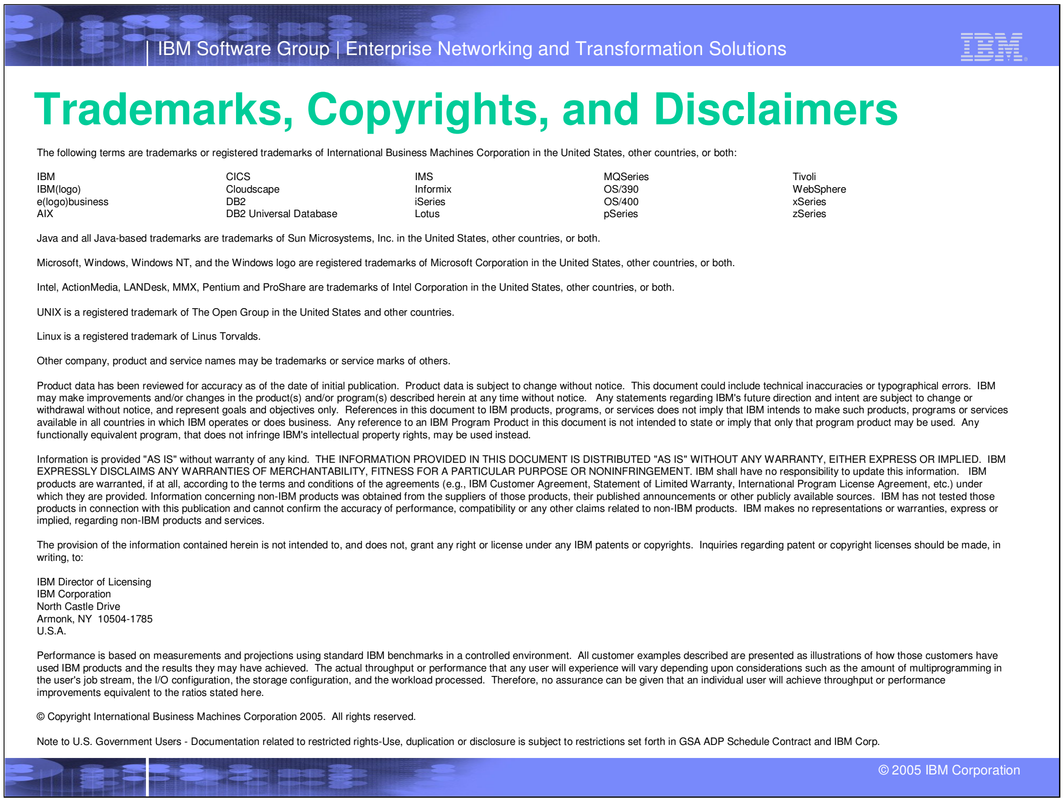
- **Configuration support**
  - Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
  - NAT IP address traversal support
- **Simplified infrastructure**
  - Eliminates need for FW Technologies daemons
  - Policy agent reads and manages IPSec and IKE policy

- **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



Integrated IP security - RFC standards

- **Ability to control and protect IP traffic on one or more TCP/IP stacks**
  - Accomplished by:
    - IP filtering
      - Permitting or denying specific IP traffic patterns
    - Virtual Private Networks (VPNs)
      - Authenticating and/or encrypting data associated with a specific IP data pattern
  - Based on RFCs defined by the IETF IPSec working group
- **IPSec RFCs implemented by Integrated IP Security include**
  - RFC 2401: Security Architecture for the Internet Protocol
  - RFC 2402: IP Authentication Header
  - RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
  - RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
  - RFC 2406: IP Encapsulating Security Payload (ESP)
  - RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP
  - RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)
  - RFC 2409: The Internet Key Exchange (IKE)
  - RFC 2410: The NULL Encryption Algorithm and Its Use with IPSec
  - RFC 2451: The ESP CBC-Mode Cipher Algorithms
  - RFC 3947: Negotiation of NAT-Traversal in the IKE
  - RFC 3948: UDP Encapsulation of IPSec ESP Packets



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.