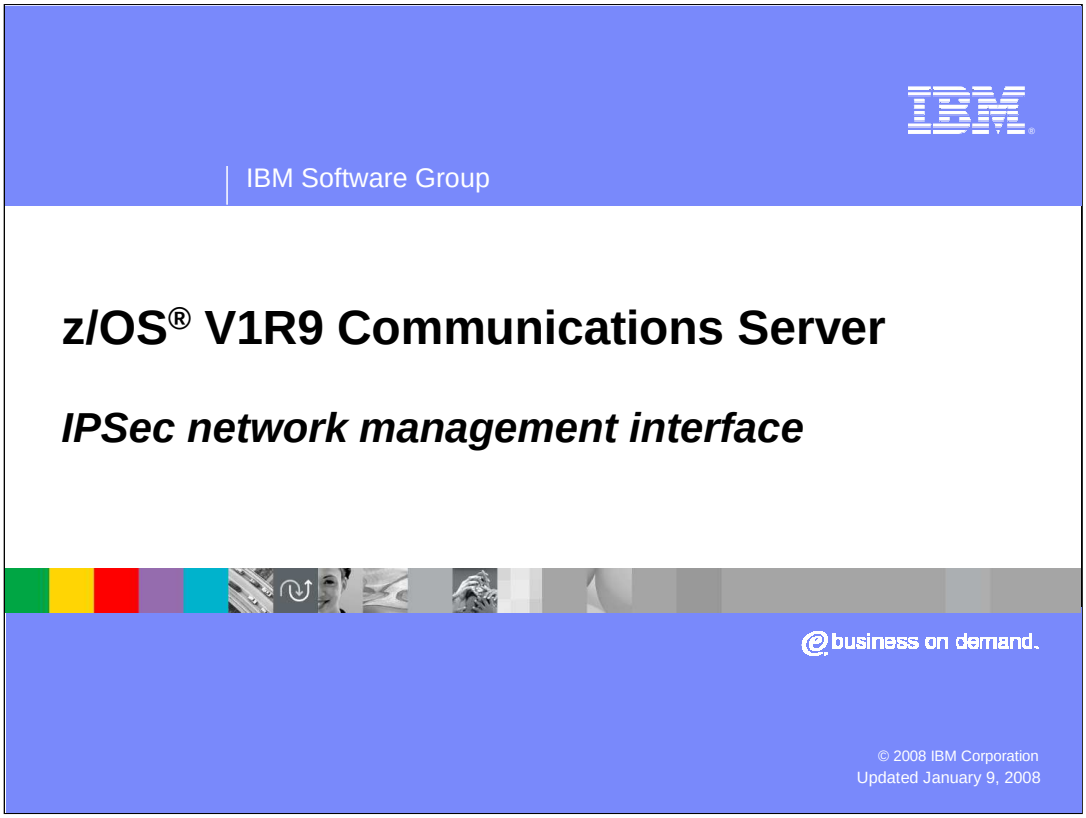
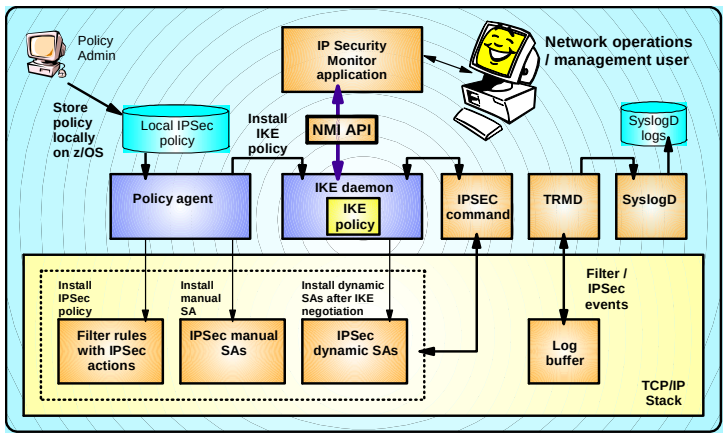


This presentation discusses the IPSec Network Management Interface for the z/OS V1R9 Communications Server.

IP security network management interface (NMI)

- In z/OS V1R7, IP security network management data was made available through a UNIX® shell command (the ipsec command)
- A programmatic IPSec management interface was needed.
- z/OS V1R9 adds a formalized network management programming interface to retrieve IP security management data, enables a network management application, such as IBM Tivoli® OMEGAMON® to access IP Security management data and integrate such data into the network management functions OMEGAMON already provide



Data similar to what can be retrieved using the ipsec command will be available over the IP Security NMI interface:

- IP filtering rules and statistics
- IKE Phase I SA information and status
- IKE Phase 2 SA information and status
- Manual SA information and status
- Port translation data

IBM Tivoli's OMEGAMON for Mainframe Network product is expected to use this interface.

In z/OS V1R7 Communications Server, IP security network management data was made available through a UNIX shell command (the ipsec command). Adding a formalized network management programming interface to retrieve IP security management data, enables a network management application to access IP Security management data and integrate such data into the network management functions already provided.

The ipsec command displays and manages system information for Integrated IPSec, but a programmatic interface was needed for network management applications to perform these actions without needing to resort to screen-scraping.

A network management interface is implemented for Integrated IPSec in the z/OS V1R9 Communications Server. The IKE daemon implements an AF_UNIX listening socket that accepts connections, and uses a request/response model for providing IPSec management data and control. Consequently, IKED must be running in order to make use of this service. Data similar to what can be retrieved using the ipsec command will be available over the IP Security NMI interface:

•IP filtering rules and statistics

•IKE Phase I SA information and status

•IKE Phase 2 SA information and status

•Manual SA information and status

•Port translation data

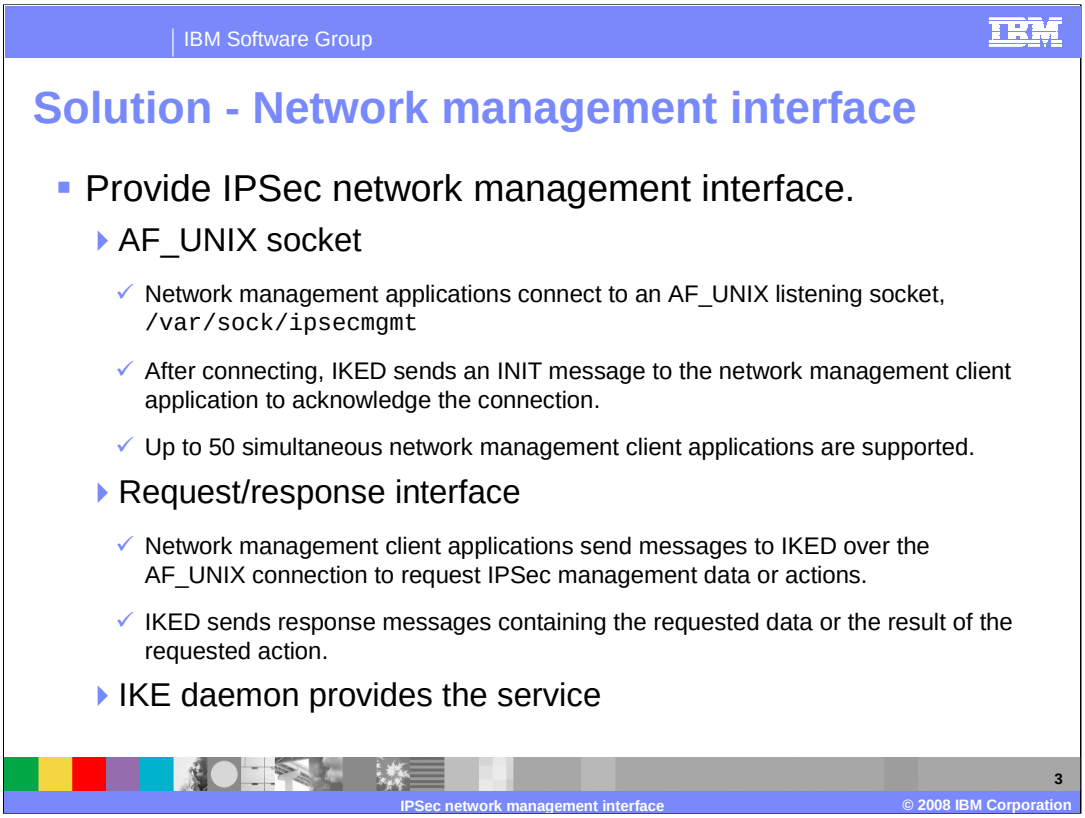
In addition the interface allows for:

•Activation or deactivation of manual tunnels

•Activation, deactivation, or refresh of IP tunnels

•Deactivation or refresh of IKE tunnels

•Load default IP filters or policy IP filters

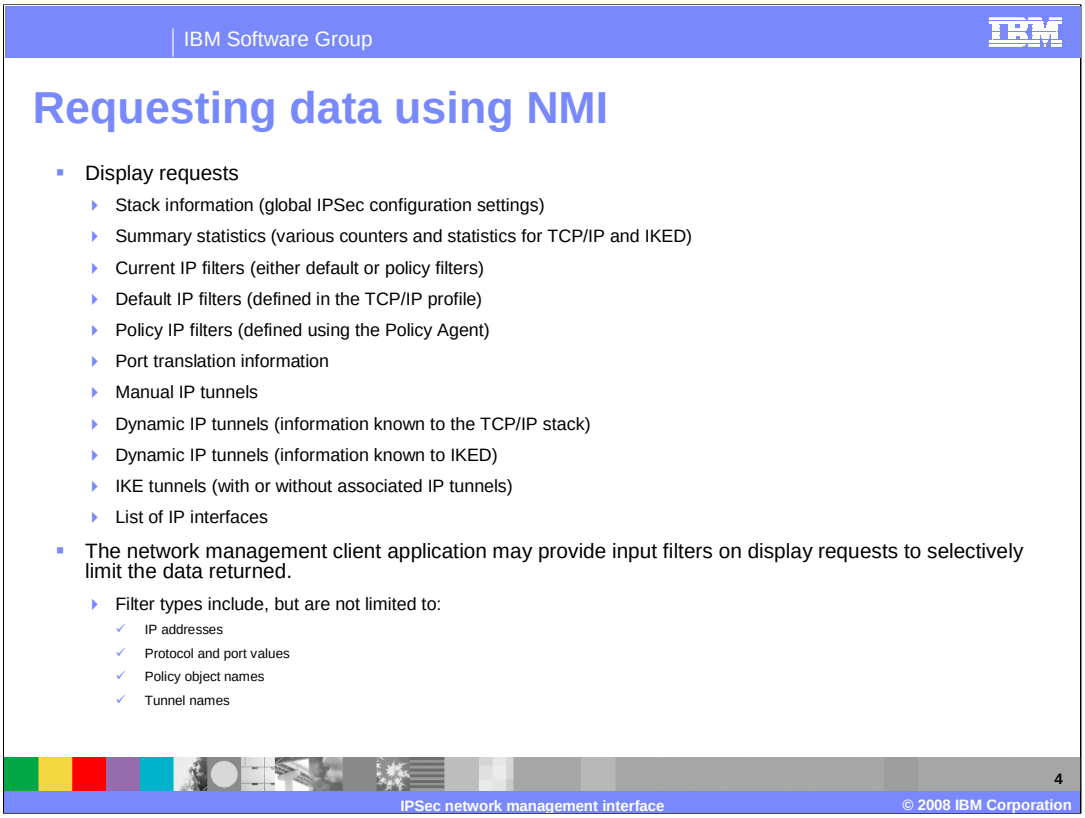


A network management interface is implemented for Integrated IPSec. The IKE daemon implements an AF_UNIX listening socket that accepts connections, and uses a request/response model for providing IPSec management data and control.

Network management client applications connect to the AF_UNIX socket located at /var/sock/ipsecmgmt. After connecting, IKED sends an INIT message to the client to acknowledge the connection. The format for IPSec NMI messages is documented in the *z/OS V1R9 Communications Server; IP Programmer's Guide and Reference*, and is defined in macro EZBNMSEA and header EZBNMSEC. The interface supports up to 50 simultaneous network management client connections

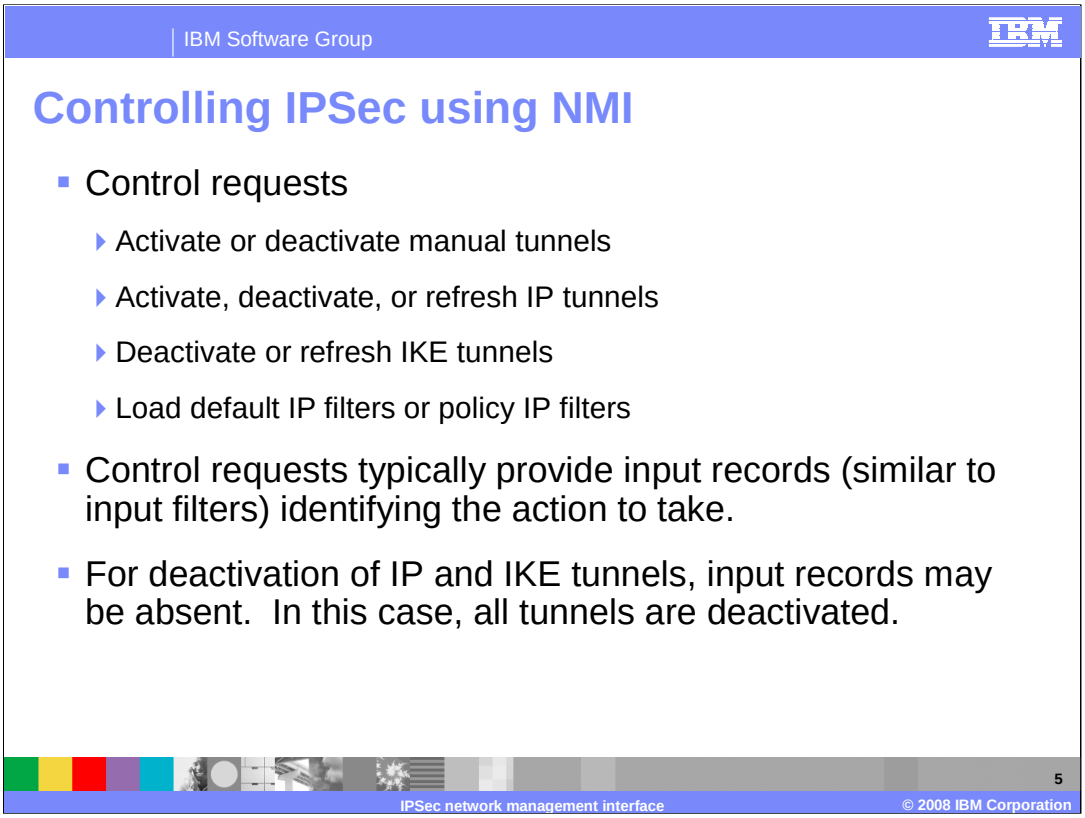
Network management client applications send requests to IKED over the AF_UNIX connection, and IKED responds with messages containing the requested data or the result of the requested action.

IKED must be running in order to make use of this service.

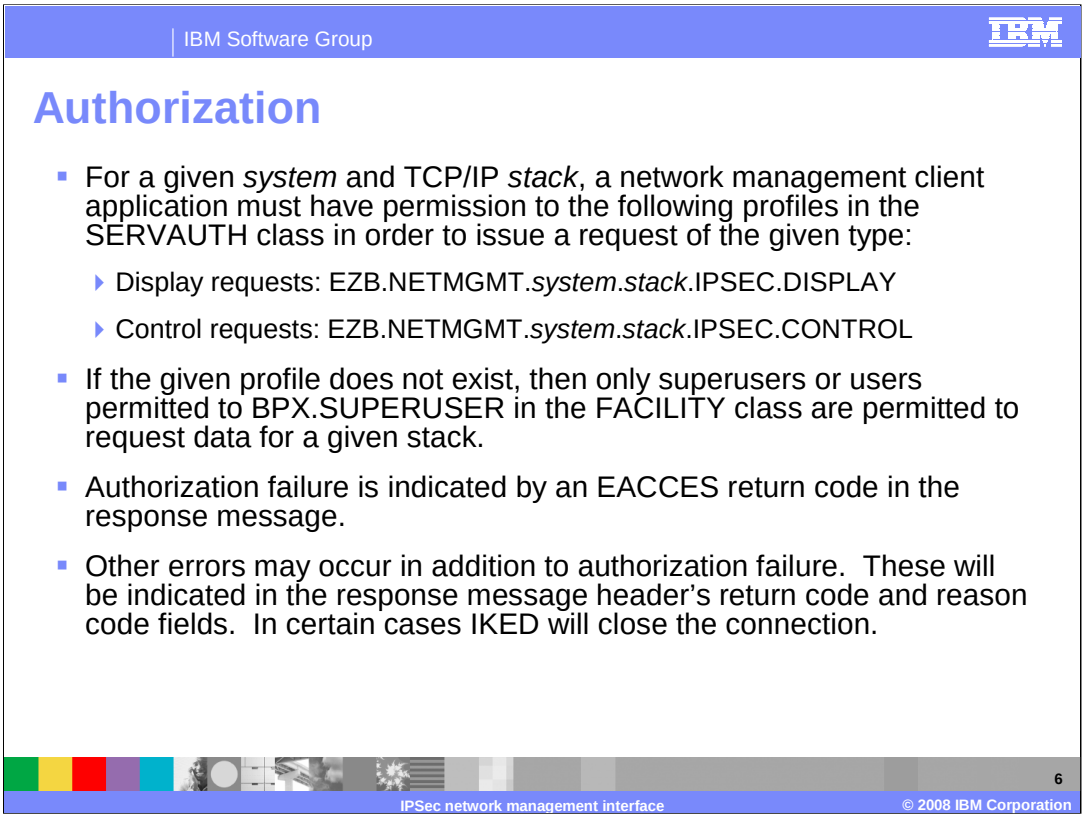


All IPSec NMI data and actions are grouped by individual TCP/IP stack. Almost all requests pertain only to a single TCP/IP stack. These requests are grouped into display requests and control requests. Display requests return various global settings or statistics, or particular information about the IP filters, IP tunnels, and IKE tunnels, and so on.

The request message sent by the network management client to IKED may contain *input filters* that are used to selectively limit the data returned for display requests. For example, the client may choose to limit the returned data by IP address, protocol, ports, policy object names, or tunnel names.



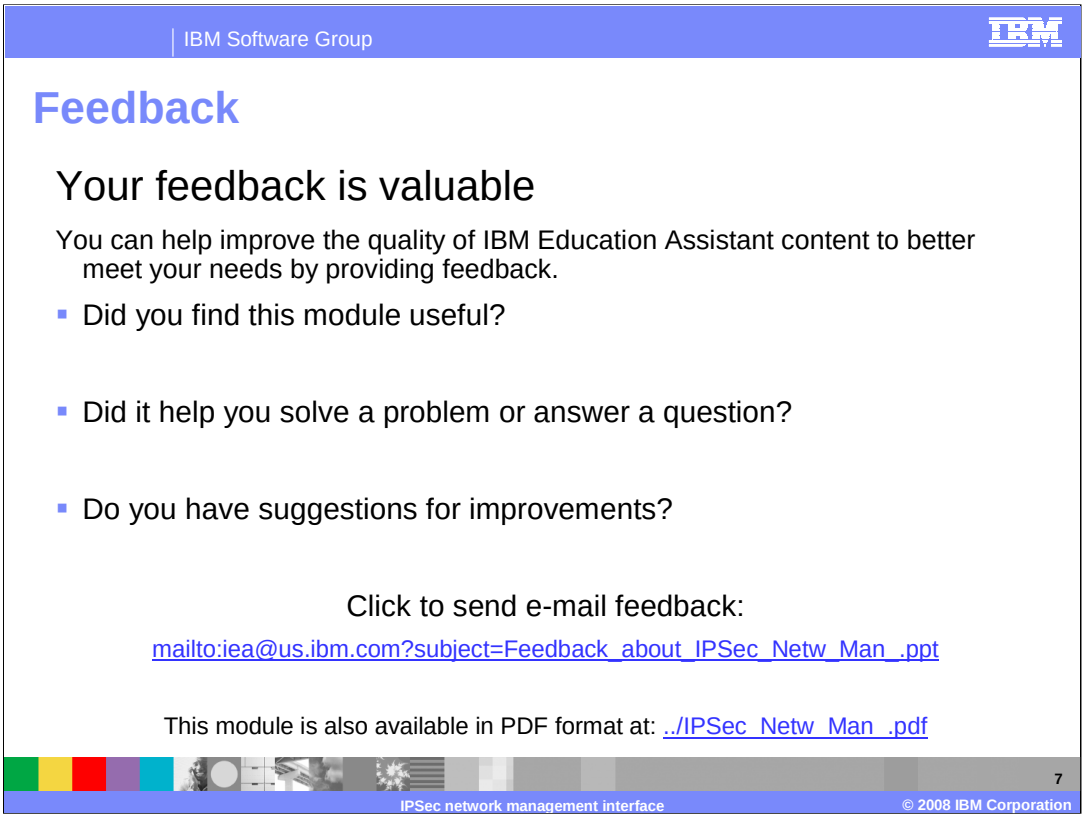
NMI control requests take particular actions on IP tunnels, IKE tunnels, and so on. Control requests must typically carry input records identifying the objects to be manipulated, similar to the way that display requests use input filters. In some cases the input records may be absent, in which case the action is taken on all objects.



SAF authorization is required for most request types, to the resource EZB.NETMGMT.*system*.*stack*.IPSEC.*type,* in the SERVAUTH class, where *type* is DISPLAY or CONTROL. If this profile does not exist, then only superusers or users permitted to BPX.SUPERUSER in the FACILITY class are permitted to request data for a given stack. Authorization failure will be indicated by an EACCES return code in the response message.

Other errors may occur in addition to authorization failure. Most such errors relate to improperly formed request messages. These errors will be indicated in the response message header's return code and reason code fields, and the possible values for these are documented in the *z/OS V1R9 Communications Server; IP Programmer's Guide and Reference*. In certain error cases IKED will close the connection.

The set of errors that may be reflected in the response message's reason code are documented in the *z/OS V1R9 Communications Server; IP Programmer's Guide and Reference*.



You can help improve the quality of IBM Education Assistant content by providing feedback.

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 OMEGAMON Tivoli z/OS

UNIX is a trademark of The Open Group in the United States, other countries, or both.

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.