This presentation covers enhancements to the Configuration Assistant for z/OS Communications Server

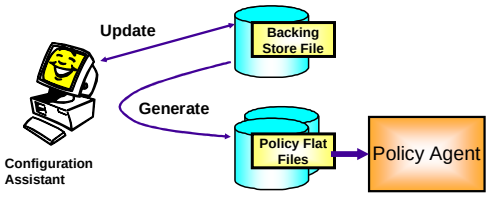
Configuration Assistant for z/OS Communications Server

- Configuration Assistant provides a GUI for configuration.
  - Configuration done through series of panels and wizards
  - Configuration files created and sent to z/OS using FTP

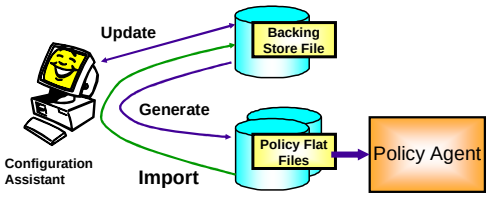
The Configuration Assistant for z/OS Communications Server was originally released in z/OS V1R7. It provides a modern GUI for configuration of z/OS Communication Server technologies including IPSecurity, Application Transparent – Transport Layer Security, Policy Based Routing , Intrusion Detection Services, Quality of Service, and Network Security Services.

The configuration work is done through a series of panels and wizards, and then the Configuration Assistant creates host configuration files and FTPs them to z/OS.

Import of policy configuration data



In V1R9 and earlier releases, configuration assistant's creation of policy configuration files is a one-way trip.



V1R10 adds ability to re-import policy configuration information back into the tool.

3 Configuration Assistant for z/OS Communication Server

The configuration assistant tool reads and stores all policy-related information in binary form in the backing store file, which is a workstation file. When a policy has been created, the configuration assistant can generate the policy flat file that can be read by Policy Agent.

The created policy flat file is a text file and can be altered with an editor, such as ISPF. However, if such manual edits are done in V1R9, those changes are never reflected back into the backing store file, as is shown in the first figure.

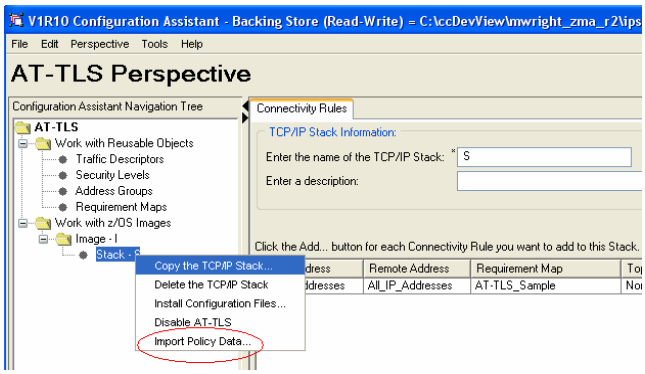
The configuration assistant tool in V1R10 adds a policy flat file import function. Changes made using an editor can now be picked up by the configuration assistant tool. Also, existing manually created policy flat files can be imported into the configuration assistant, and then subsequent changes can be implemented using the configuration assistant tool, as is shown in the second figure.

IBM doesn't recommend doing this as standard practice. It is geared toward one-time migration to the configuration assistant, or incorporating emergency updates. The configuration assistant should be the primary method of maintaining this configuration information.

z/OS V1R10 will add support for some, but not all of the policy types: IPSec, Application Transparent TLS, Policy Based Routing, and Intrusion Detection System.

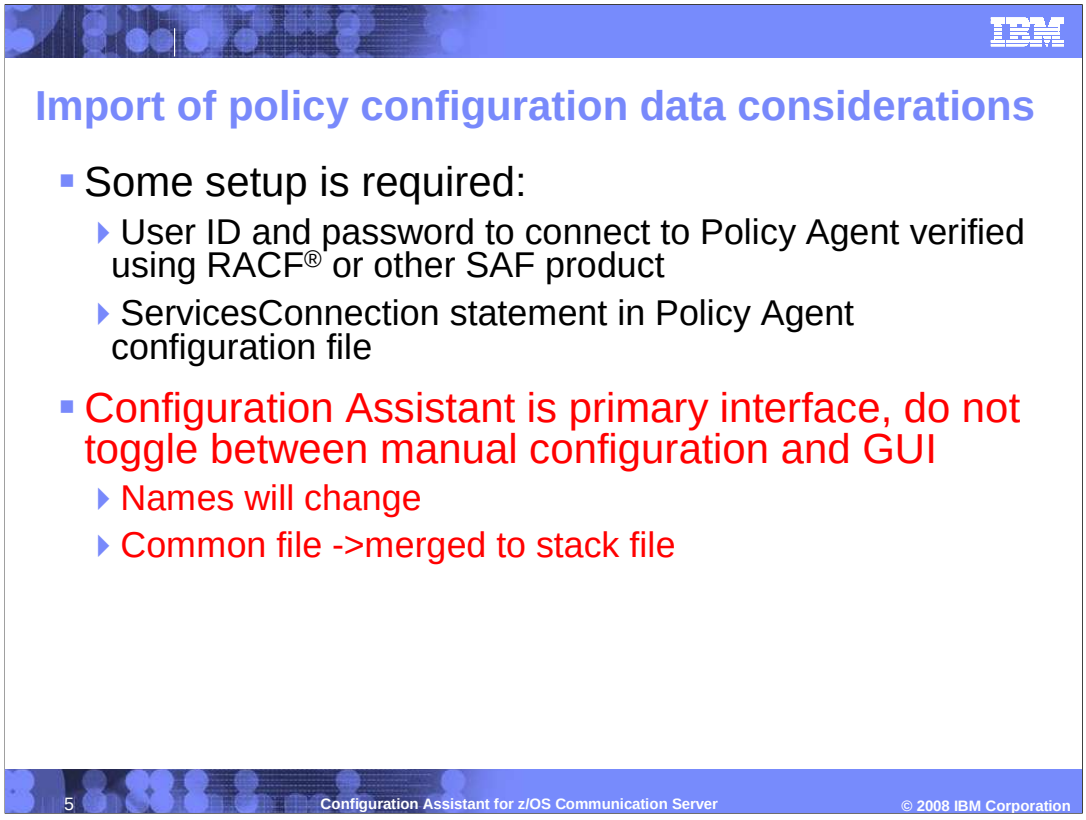
Import of policy configuration data

- Works by having the Policy Agent read the configuration
  - Configuration assistant opens a socket to the policy agent and gets the parsed configuration



To initiate an import, select the target TCP/IP stack and right click to use the pop-up menu to select the Import Policy Data item as shown in the figure on this slide.

Configuration assistant will then open a socket to the policy agent running on z/OS and gets the parsed configuration, which it operates on.



Before importing some setup is required. You need to add a ServicesConnection statement in the main Policy Agent configuration file to specify the listening port and key ring database.

You also need to authorize users by issuing security product commands in this SERVAUTH profile:

EZB.PAGENT.*sysname.image.ptype*

The *image* value is the import request name used by the import requestor. For local policies this is the TCP/IP stack name specified on the TcpImage statement.

Import of policy configuration data considerations

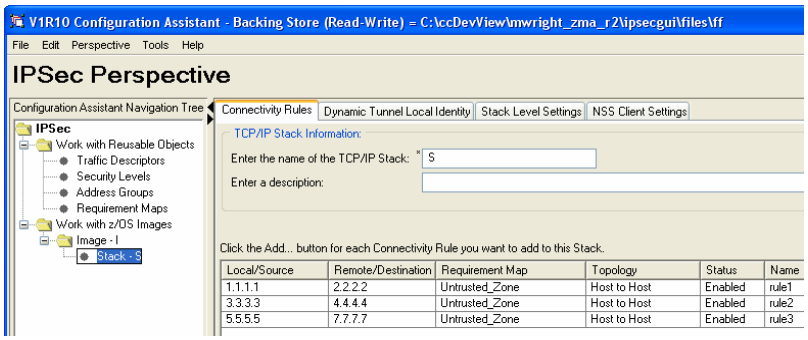
- Should be used for:
  - One time read in from manual configuration
  - Emergency updates by way of manual configuration
- Provided for: IPSec, AT-TLS, IDS, and PBR

The import function is intended for one time only or emergency use only. Do not consider using on a regular basis since style changes in your configuration can change the structure and layout of your configuration files.

Qualities of service and Network Security Services (NSS) technologies do not support importing.

Address group support

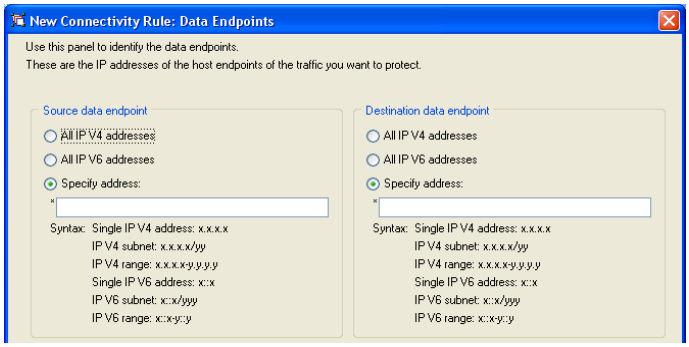
- Use Configuration Assistant to create sets of rules.
- Packets match rules based on IP addresses, protocols, ports



For IPSec and AT-TLS technologies, you configure a set of rules. Each rule includes the IP addresses of the local and remote endpoints. IP packets might match rules based on the IP address in the rules. When a rule is matched, then the action defined for the rule is obeyed. This slide shows an example of a configuration assistant screen in which multiple rules were created to match multiple IP addresses. Except for the IP addresses, the rules are functionally identical

Address groups support

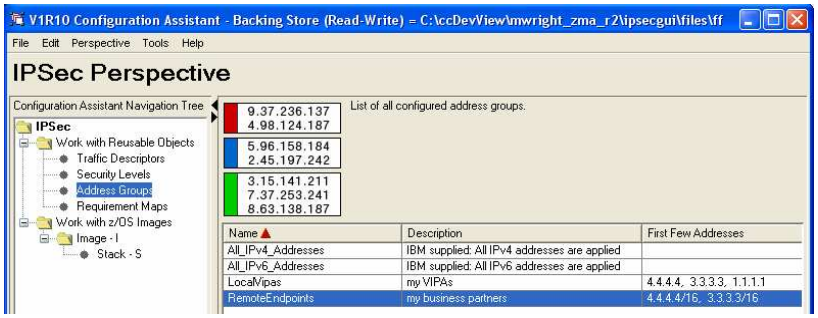
- For each rule you configure IP address, range, or subnets
- V1R9 Configuration Assistant can not configure address groups



For each rule you might configure the data endpoints as an IP address, subnet or range. Those choices are shown in the configuration assistant example on this page. If multiple IP addresses are needed for the same action, for V1R9 you have to configure a separate rule for each address.

Configuration assistant address group support

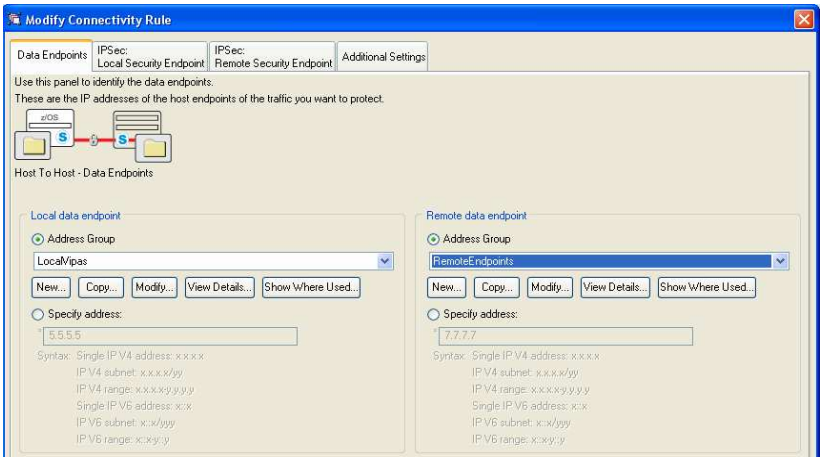
- In V1R10, the configuration Assistant provides IP address groups as reusable objects to IPSec and AT-TLS technologies.



In V1R10 IP address groups are added to the IPSec and AT-TLS technologies. The address groups are configured as reusable objects so they can be used in multiple rules and in multiple TCP/IP stacks. Each address group can contain a set of IP addresses, subnets, or ranges. You create and select address groups using the Address Groups reusable objects as shown in this configuration assistant example.

Configuration assistant address groups

- You can create and select an address group for each rule.



When configuring rules, users can now select an address group as the endpoint, as shown in this configuration assistant example

Address group support considerations

- Address groups added in V1R10 for IPSec and AT-TLS
- Already supported for policy-based routing in V1R9
- Address groups can be copied between technologies
  - they are not shared across technologies
- For some customers, can drastically reduce number of rules.

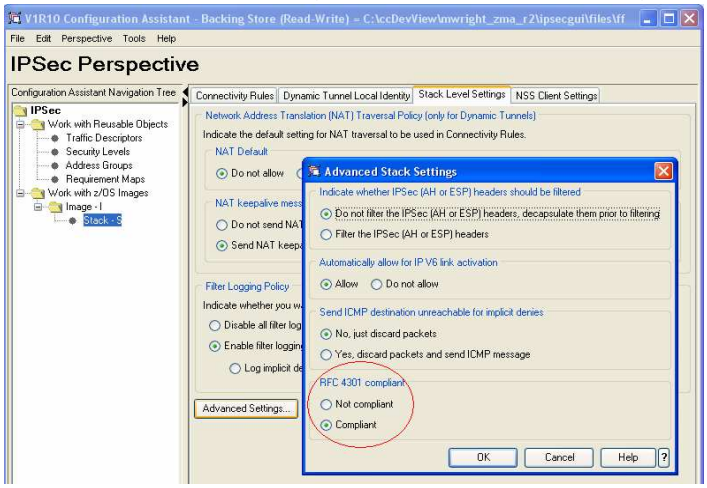
Address groups are included for PBR in V1R9 and are added to V1R10 for IPSec and AT-TLS.

Address groups for a single technology, such as IPSec, cannot be reused for configuring another technology. An address group can be copied from one technology to another.

For some customers, use of address groups can drastically reduce the number of rules you have to create.

IPSec RFC currency

- RFC 4301: Should not filter on ports/type/code for routed traffic
- Can have GUI enforce this or just health check warning



z/OS V1R10 Communications Server introduces new restrictions on filter rules to comply with RFC 4301. These restrictions only apply to routed or forwarded traffic; if all of your filter rules apply to local packets then you are not affected by this restriction.

RFC 4301 identifies potential security risks in routed traffic where packets might be fragmented. If a forwarding host has rules that apply to specific TCP or UDP ports, some of the fragmented packets will have ambiguous filtering decisions because their ports are not known. This ambiguity introduces several security risks.

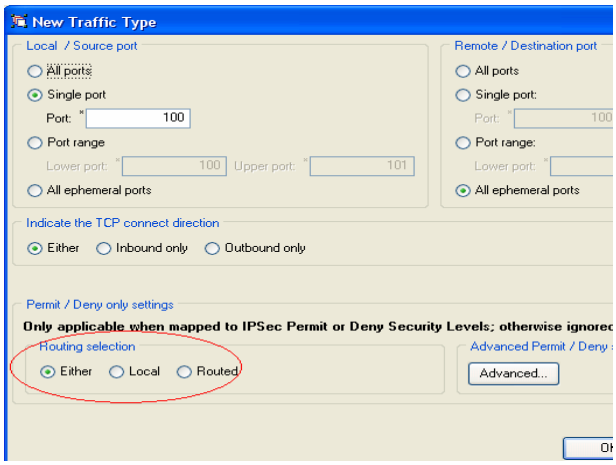
RFC 4301 allows two possible solutions. One is to implement statefull fragment checking, which temporarily stores the port values from the first fragment so that they can be used later to properly filter subsequent fragments. z/OS Communications Server does not support statefull fragment checking. The second solution allowed by RFC 4301 is to prevent routed filter rules from specifying specific ports.

Beginning in V1R10, z/OS Communications Server Policy Agent and Configuration Assistant discourage definitions that apply to specific ports for routed traffic. All filter rules for routed traffic must apply to all ports. You are affected by this restriction if you have any port-specific rules that apply to routed traffic, or that apply to both routed and local traffic. In particular, the Configuration Assistant has the ability to import your policy and recommend updates to comply with the restriction.

This restriction can be temporarily suspended until you update your policy to comply with the restriction. As an interim measure, can configure the stack as Not compliant in the Advanced Stack Settings dialog, as shown on this slide. You might choose to relax the restriction until you have updated your configuration. If you choose to relax the restriction, you should be aware that the vulnerabilities cited in RFC 4301 concerning routed traffic and fragmented packets will apply to you.

IPSec RFC currency ports/type/code migration

- Previously routing configured on traffic descriptor
- Setting was used for filter rules

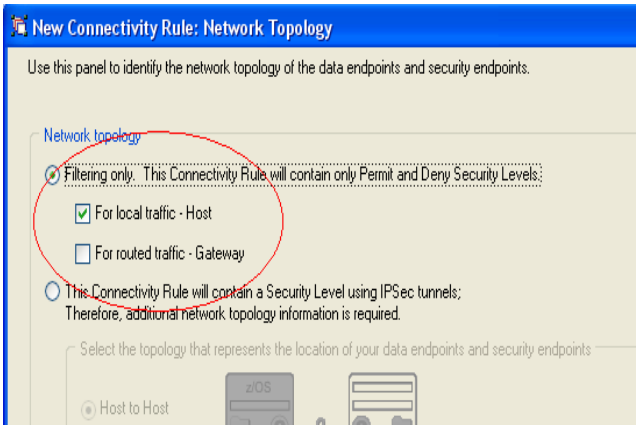


To enforce RFC 4310 routed traffic restrictions, a significant change is occurring in the Configuration Assistant. For filter only rules (rules with an action of Permit or Deny), the Configuration Assistant is no longer using the routing selection previously configured in the traffic descriptor. The default setting was either local or routed traffic, which for most users only applied to local traffic and not routed traffic. However, a setting of either also means routed and is considered in violation of RFC 4301.

This routing setting in the traffic descriptor that is shown on this slide is removed and no longer exists in V1R10.

IPSec RFC currency ports/type/code migration

- Now routing is determined based on topology for filter rules
- Routing was already determined based on topology for IPSec tunnels



The routing setting for each rule is now determined exclusively based on the topology selection in the rules. Previously the routing setting for IPSec tunnels was already determined based on the topology. With this change both tunnels and filters use the topology selection in the rule to properly determine if the rule is for routed traffic or local traffic, as shown on this slide.

IPSec RFC currency ports/type/code migration

When opening pre-V1R10 backing store

- The routing setting is removed from traffic descriptors and set on each rule
- A report is launched and shown in your browser
  - User actions recorded if migration is not seamless
  - RFC 4301 report shown indicating use of ports/types/codes for routed traffic

Due to the change in how routing is determined for filter rules, when migrating pre-V1R10 backing store files to V1R10, the Configuration Assistant will automatically update your configuration settings to the new routing methodology. It is possible that a user has complex rules that cannot be easily migrated. During a migration for each rule the Configuration Assistant might easily adopt the rule. Alternatively, it might adopt the rule but provide a warning indicating you should verify the rule was properly migrated, or not know how to do the migration for the rule, and mark the rule incomplete.

Most of the rules should be easily adopted. However, a complete report is provided after the migration indicating any user actions required to manually complete the migration.

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 RACF z/OS

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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.