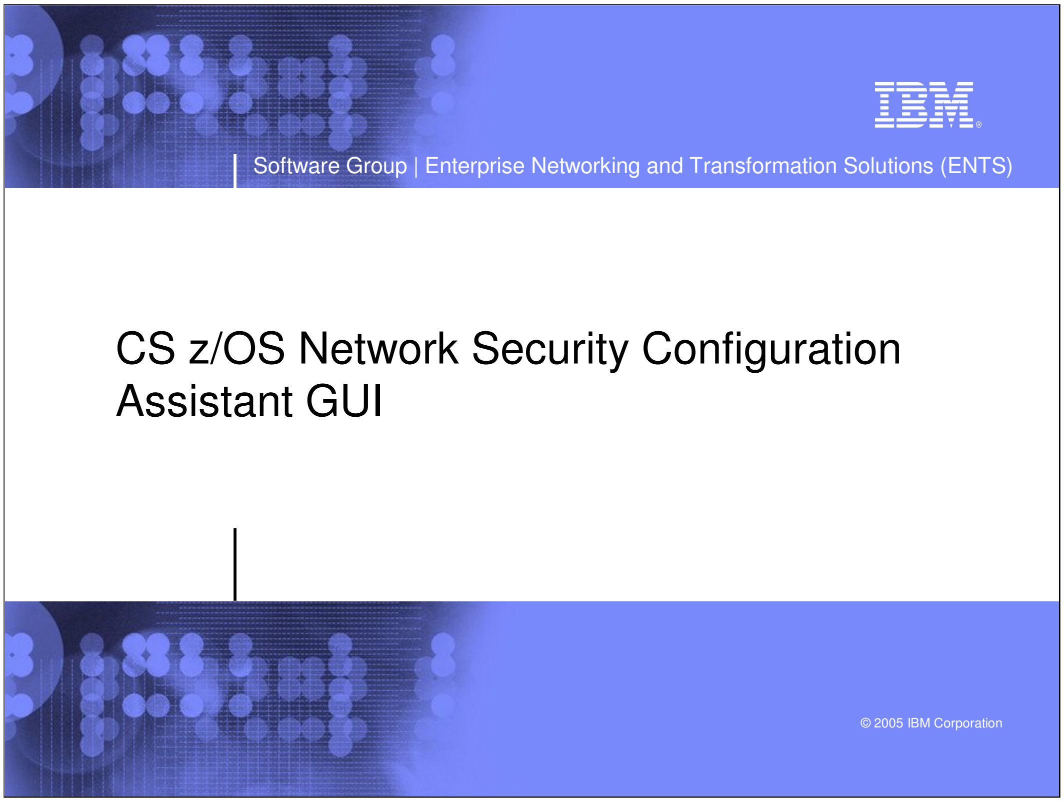
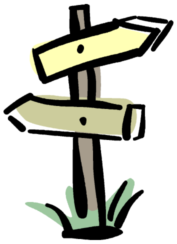
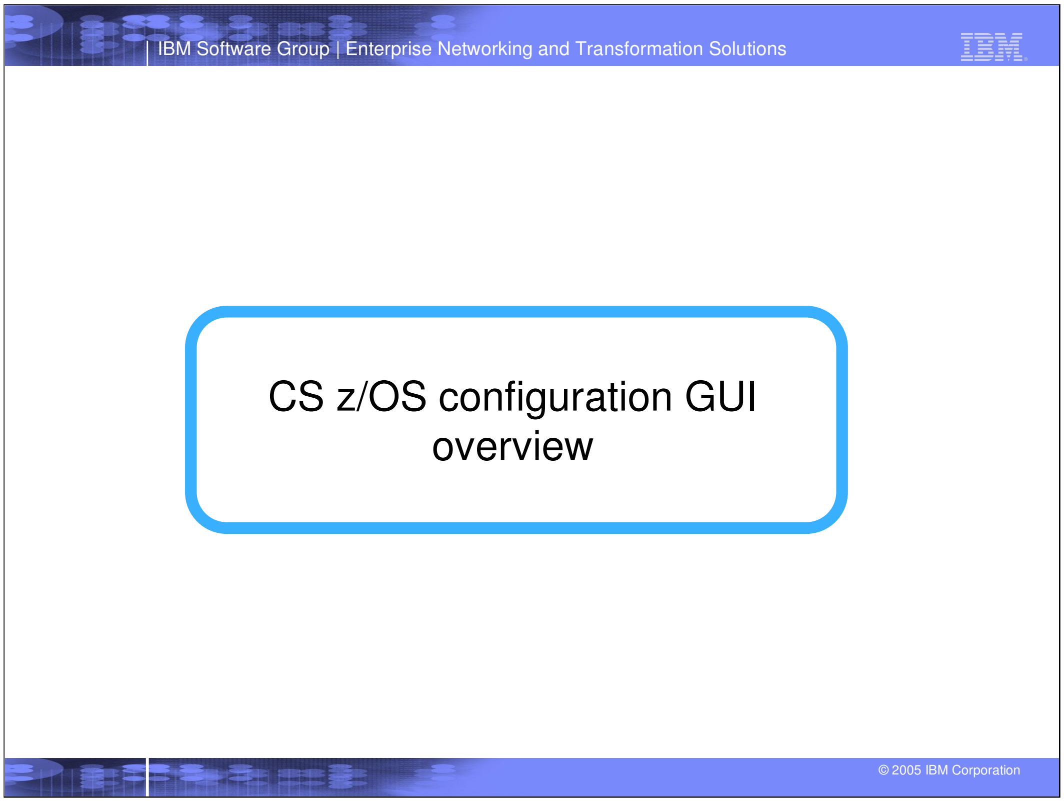


CS z/OS Network Security Configuration Assistant GUI

Security configuration agenda

- CS z/OS configuration GUI overview
- Network security configuration assistant



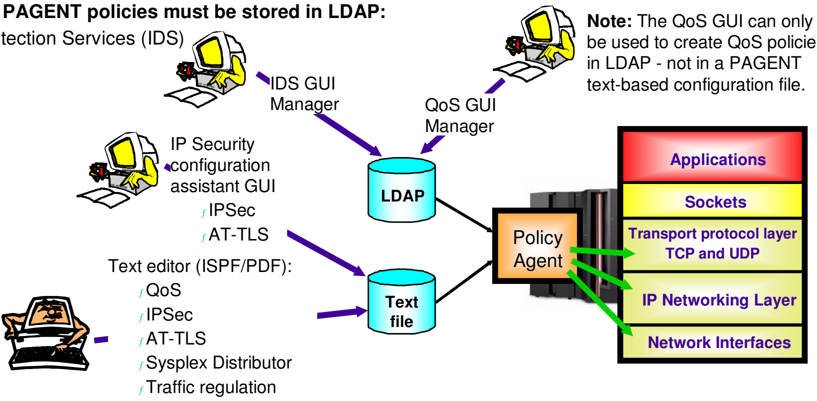


CS z/OS configuration GUI overview

Configuring the Policy Agent

- **The following PAGENT policies can be stored in a flat text file format:**
  - QoS policies (alternatively supported in LDAP)
  - IPSec VPN policies
  - IP filter policies
  - AT-TLS policies
  - Sysplex Distributor policies
  - Traffic regulation policies

- **The following PAGENT policies must be stored in LDAP:**
  - Intrusion Detection Services (IDS)



Note: The QoS GUI can only be used to create QoS policies in LDAP - not in a PAGENT text-based configuration file.

IDS GUI Manager

QoS GUI Manager

IP Security configuration assistant GUI
- IPSec
- AT-TLS

Text editor (ISPF/PDF):
- QoS
- IPSec
- AT-TLS
- Sysplex Distributor
- Traffic regulation

LDAP

Text file

Policy Agent

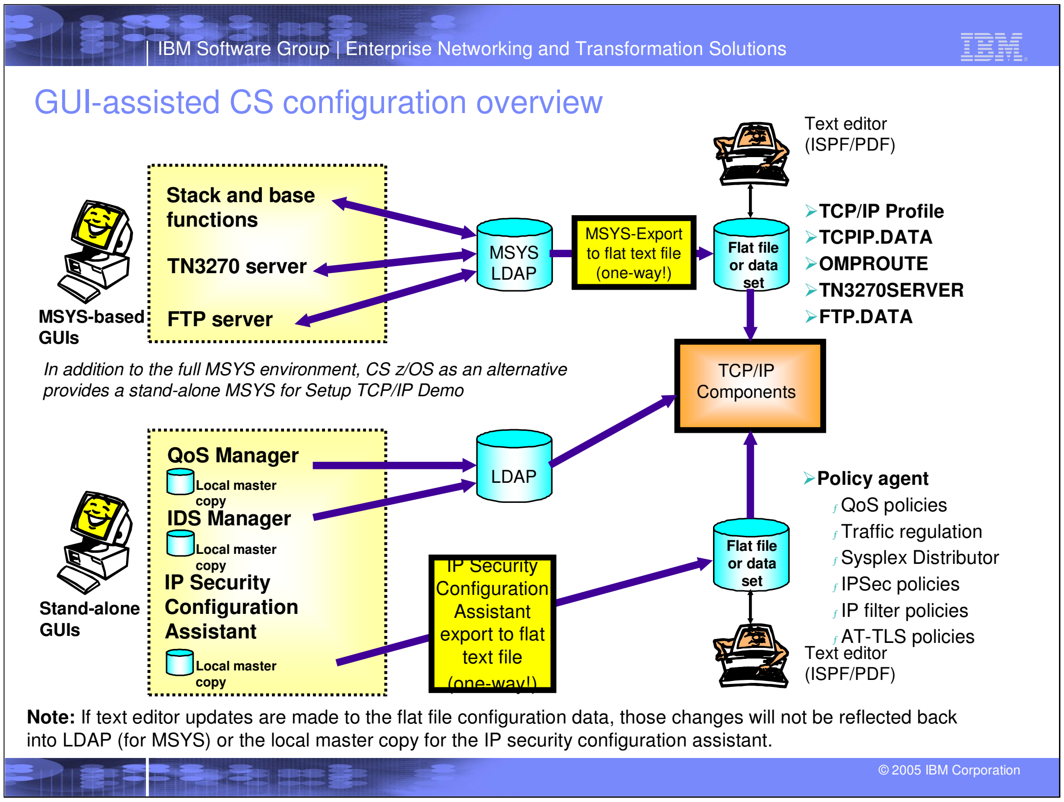
Applications

Sockets

Transport protocol layer TCP and UDP

IP Networking Layer

Network Interfaces



GUI-assisted CS configuration overview

Text editor
(ISPF/PDF)

MSYS-based GUIs

Stack and base functions

TN3270 server

FTP server

MSYS LDAP

MSYS-Export to flat text file (one-way!)

Flat file or data set

- TCP/IP Profile
- TCPIP.DATA
- OMPROUTE
- TN3270SERVER
- FTP.DATA

In addition to the full MSYS environment, CS z/OS as an alternative provides a stand-alone MSYS for Setup TCP/IP Demo

TCP/IP Components

Stand-alone GUIs

QoS Manager

Local master copy

IDS Manager

Local master copy

IP Security Configuration Assistant

Local master copy

LDAP

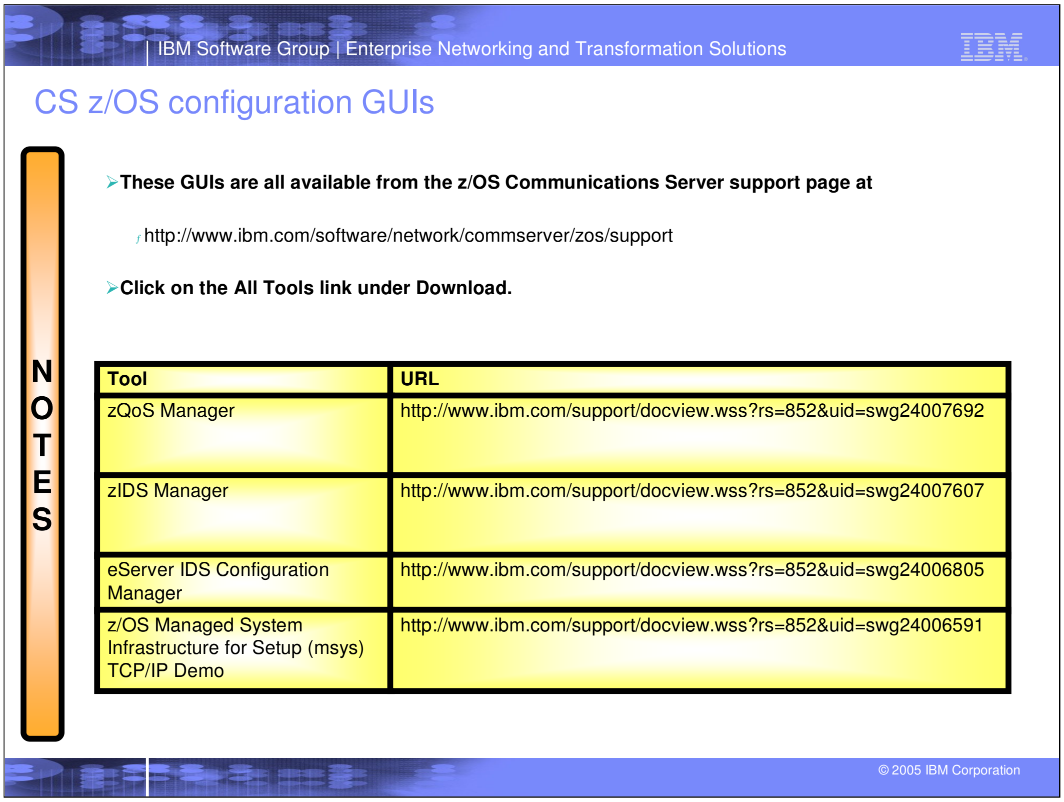
IP Security Configuration Assistant export to flat text file (one-way!)

Flat file or data set

- Policy agent
  - QoS policies
  - Traffic regulation
  - Sysplex Distributor
  - IPSec policies
  - IP filter policies
  - AT-TLS policies

Text editor
(ISPF/PDF)

Note: If text editor updates are made to the flat file configuration data, those changes will not be reflected back into LDAP (for MSYS) or the local master copy for the IP security configuration assistant.



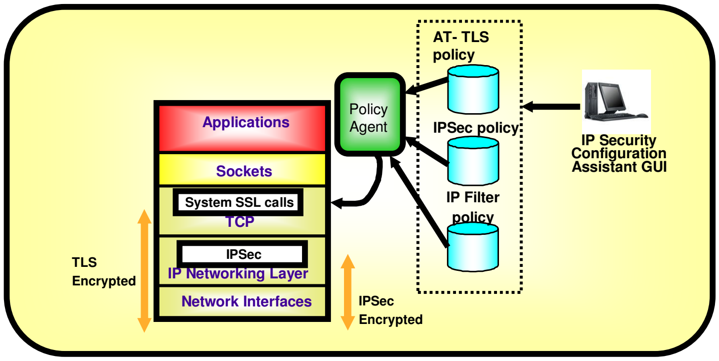
CS z/OS configuration GUIs

NOTES

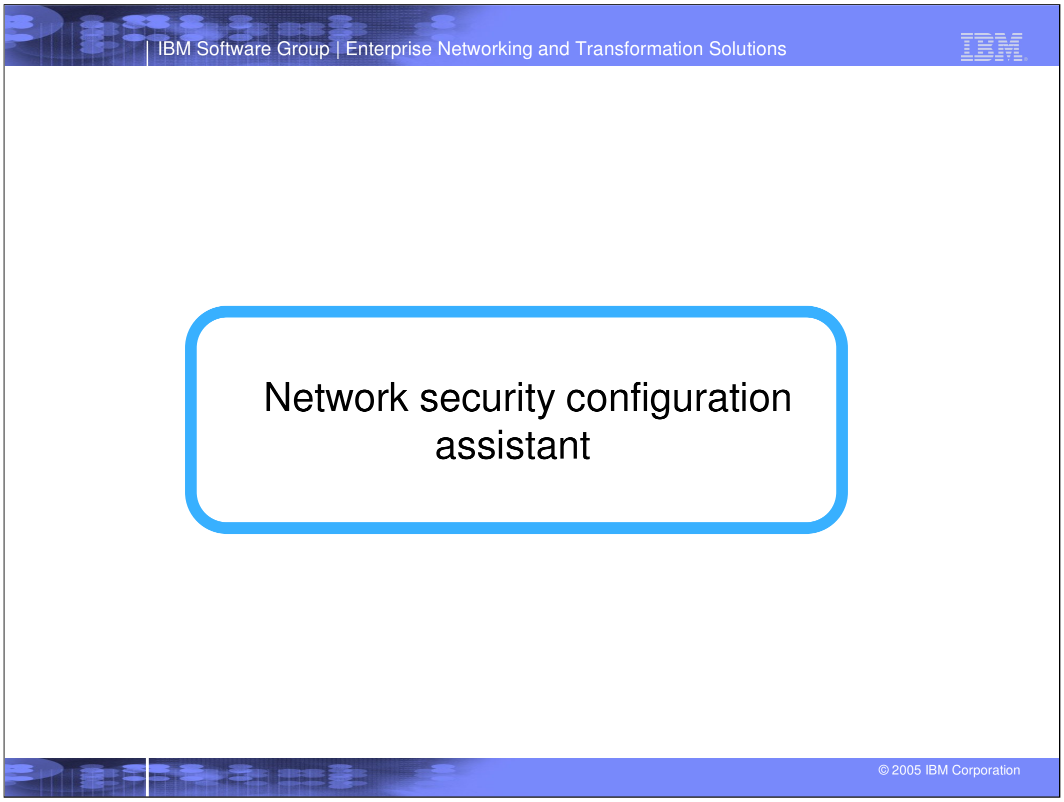
- **These GUIs are all available from the z/OS Communications Server support page at**
  - http://www.ibm.com/software/network/commserver/zos/support
- **Click on the All Tools link under Download.**

Tool	URL
zQoS Manager	http://www.ibm.com/support/docview.wss?rs=852&uid=swg24007692
zIDS Manager	http://www.ibm.com/support/docview.wss?rs=852&uid=swg24007607
eServer IDS Configuration Manager	http://www.ibm.com/support/docview.wss?rs=852&uid=swg24006805
z/OS Managed System Infrastructure for Setup (msys) TCP/IP Demo	http://www.ibm.com/support/docview.wss?rs=852&uid=swg24006591

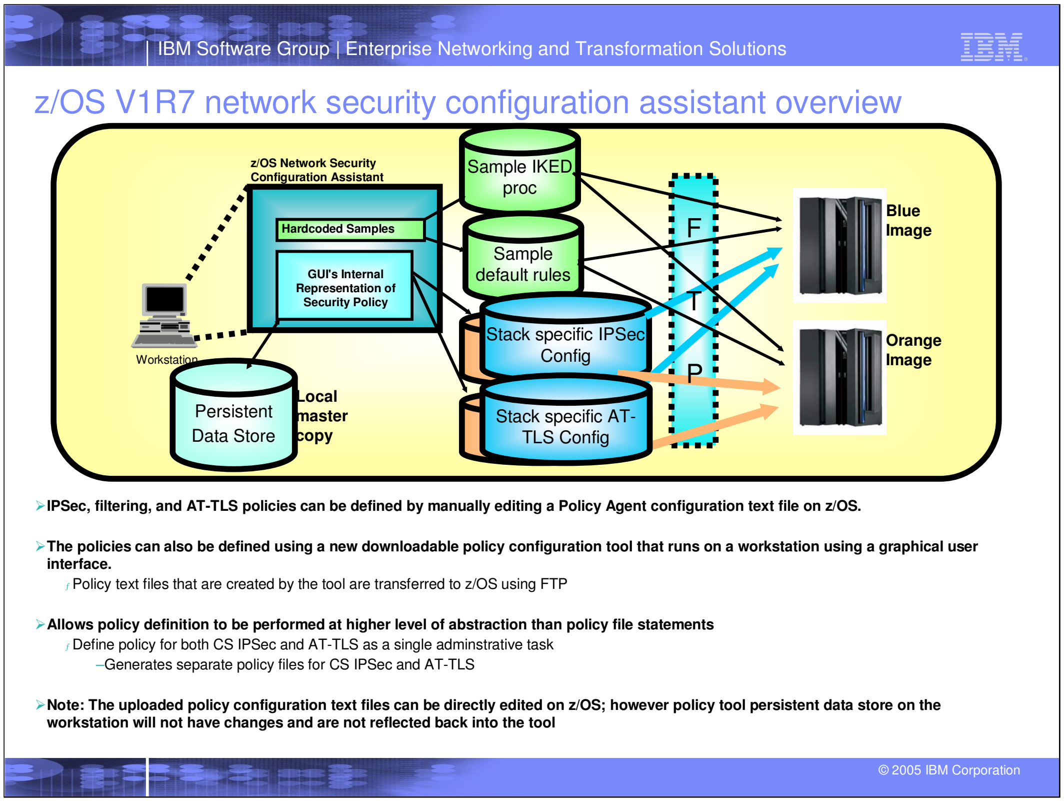
Policy-controlled application-transparent network security



- **Network security without requiring application changes**
  - IPSec
  - Transparent TLS
- **Configuration single administrative task**
  - Higher level of abstraction
    - Focus on what traffic to protect and how to protect
    - Less focus on low-level details (though available on expert panels)



Network security configuration assistant



z/OS V1R7 network security configuration assistant overview

z/OS Network Security Configuration Assistant
Hardcoded Samples
GUI's Internal Representation of Security Policy
Workstation
Persistent Data Store
Local master copy
Sample IKED proc
Sample default rules
Stack specific IPSec Config
Stack specific AT-TLS Config
F
T
P
Blue Image
Orange Image

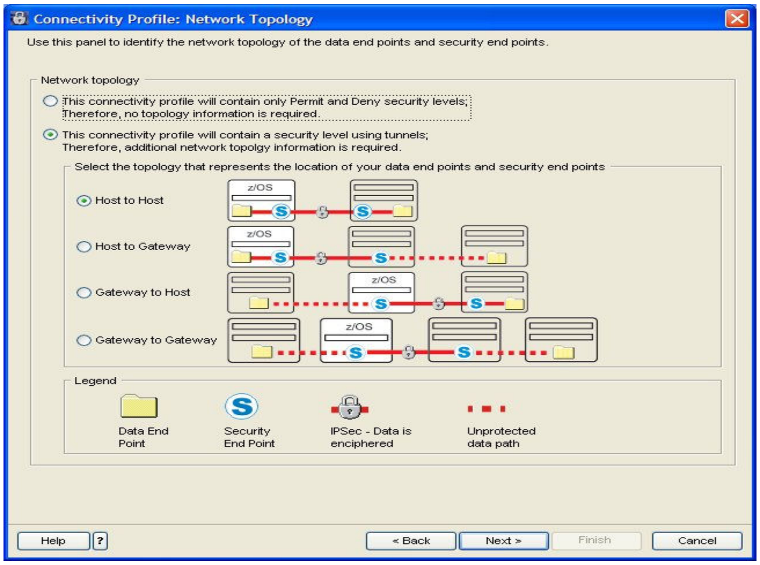
- IPSec, filtering, and AT-TLS policies can be defined by manually editing a Policy Agent configuration text file on z/OS.

- The policies can also be defined using a new downloadable policy configuration tool that runs on a workstation using a graphical user interface.
  - Policy text files that are created by the tool are transferred to z/OS using FTP

- Allows policy definition to be performed at higher level of abstraction than policy file statements
  - Define policy for both CS IPSec and AT-TLS as a single adminstrative task
    - Generates separate policy files for CS IPSec and AT-TLS

- Note: The uploaded policy configuration text files can be directly edited on z/OS; however policy tool persistent data store on the workstation will not have changes and are not reflected back into the tool

Network security configuration assistant - example



Connectivity Profile: Network Topology

Use this panel to identify the network topology of the data end points and security end points.

Network topology

○ This connectivity profile will contain only Permit and Deny security levels; Therefore, no topology information is required.

● This connectivity profile will contain a security level using tunnels; Therefore, additional network topolgy information is required.

Select the topology that represents the location of your data end points and security end points

● Host to Host

○ Host to Gateway

○ Gateway to Host

○ Gateway to Gateway

Legend

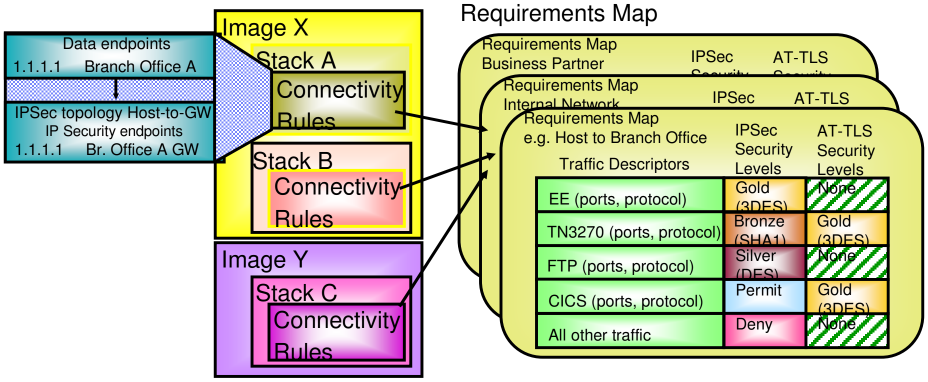
Data End Point

Security End Point

IPSec - Data is enciphered

Unprotected data path

Network security configuration assistant - configuration data model

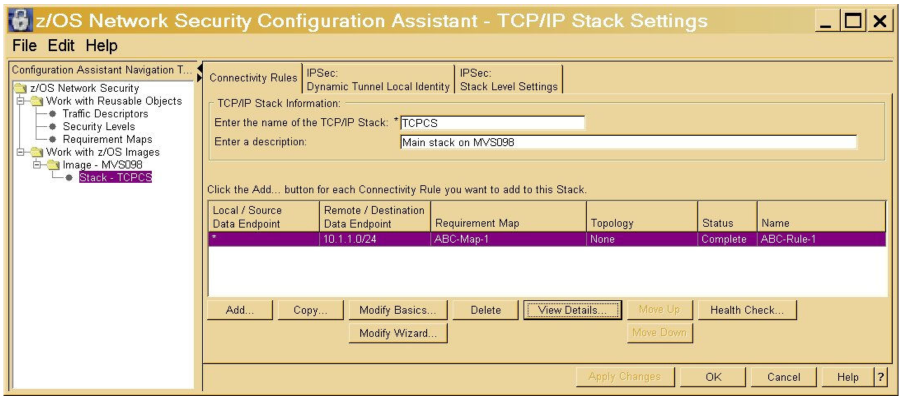


Traffic Descriptors	IPSec Security Levels	AT-TLS Security Levels
EE (ports, protocol)	Gold (3DES)	None
TN3270 (ports, protocol)	Bronze (SHA1)	Gold (3DES)
FTP (ports, protocol)	Silver (DES)	None
CICS (ports, protocol)	Permit	Gold (3DES)
All other traffic	Deny	None

- **A system image contains one or more stacks**
  - Multiple system images may be defined
- **A stack contains a set of connectivity rules**
  - Data endpoint information
  - Security endpoint information
- **Reusable objects (can be shared across images and stacks)**
  - Requirements Map, Security Level, Traffic Descriptor

Connectivity rule example

- A stack's connectivity rule applies a requirement map to a pair of data endpoints.
- The IPv4 addresses in a packet are compared with the IPv4 addresses of the data endpoints of the connectivity rules in the order that those rules appear in the table.
- When the IPv4 addresses match, the packet is compared with that connectivity rule's traffic descriptors in the order they appear in the requirement map; when a match is found, the corresponding security level is applied. For IPSec, each requirement map ends with an implicit rule to deny all traffic.
- For AT-TLS, if a packet matches no rule, it is allowed to flow with no AT-TLS protection.



z/OS Network Security Configuration Assistant - TCP/IP Stack Settings

TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: * TCPCS

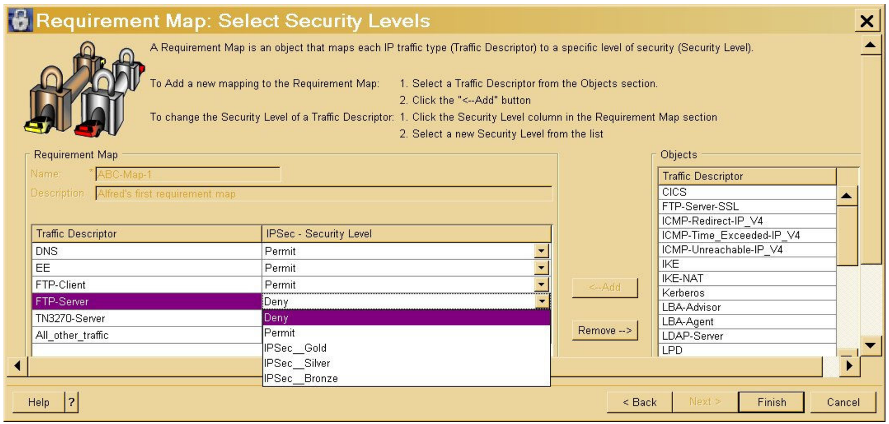
Enter a description: Main stack on MVS098

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local / Source Data Endpoint	Remote / Destination Data Endpoint	Requirement Map	Topology	Status	Name
*	10.1.1.0/24	ABC-Map-1	None	Complete	ABC-Rule-1

Requirement map example

- **A requirement map is a collection of traffic descriptors**
  - You might define a requirement map named BranchOffice that provides a high level of protection for TN3270 and Web traffic but disallows (denies) all other traffic.
  - You might define another requirement map named BusinessPartner that provides a high level of protection for Web traffic but disallows all other traffic.
  - Then you could associate BranchOffice with the addresses of your branch offices in some connectivity rules.
  - And associate BusinessPartner with the IPv4 addresses of your business partners in other connectivity rules.



Requirement Map: Select Security Levels

A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map:
1. Select a Traffic Descriptor from the Objects section.
2. Click the "<--Add" button

To change the Security Level of a Traffic Descriptor:
1. Click the Security Level column in the Requirement Map section
2. Select a new Security Level from the list

Requirement Map

Name: * ABC-Map-1

Description: Alfred's first requirement map

Traffic Descriptor	IPSec - Security Level
DNS	Permit
EE	Permit
FTP-Client	Permit
FTP-Server	Deny
TN3270-Server	
All_other_traffic	

Deny
Permit
IPSec__Gold
IPSec__Silver
IPSec__Bronze

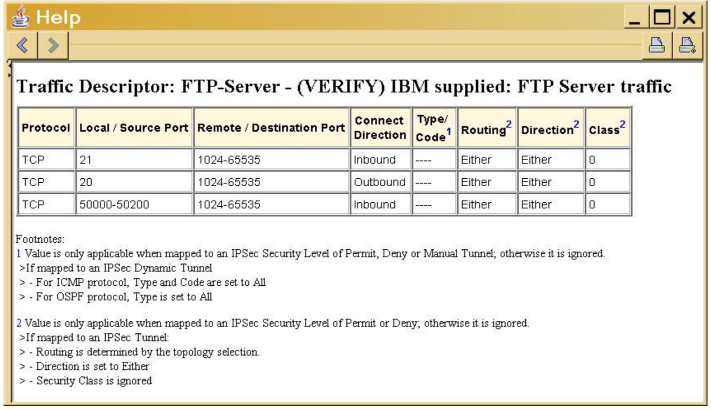
Objects

Traffic Descriptor
CICS
FTP-Server-SSL
ICMP-Redirect-IP_V4
ICMP-Time_Exceeded-IP_V4
ICMP-Unreachable-IP_V4
IKE
IKE-NAT
Kerberos
LBA-Advisor
LBA-Agent
LDAP-Server
LPD

Traffic descriptor example

- **The IP Security configuration assistant comes with many traffic types already defined**
  - They can be used as-is
  - Or they can be modified to better match your local needs

- **This is an example of FTP server traffic**
  - You may want to change the port range for passive data connections based on your local FTP server's PASSIVEDATAPORT value
    - In this example, we use the range from 50,000 to 50,200



Traffic Descriptor: FTP-Server - (VERIFY) IBM supplied: FTP Server traffic

Protocol	Local / Source Port	Remote / Destination Port	Connect Direction	Type/ Code[1]	Routing[2]	Direction[2]	Class[2]
TCP	21	1024-65535	Inbound	----	Either	Either	0
TCP	20	1024-65535	Outbound	----	Either	Either	0
TCP	50000-50200	1024-65535	Inbound	----	Either	Either	0

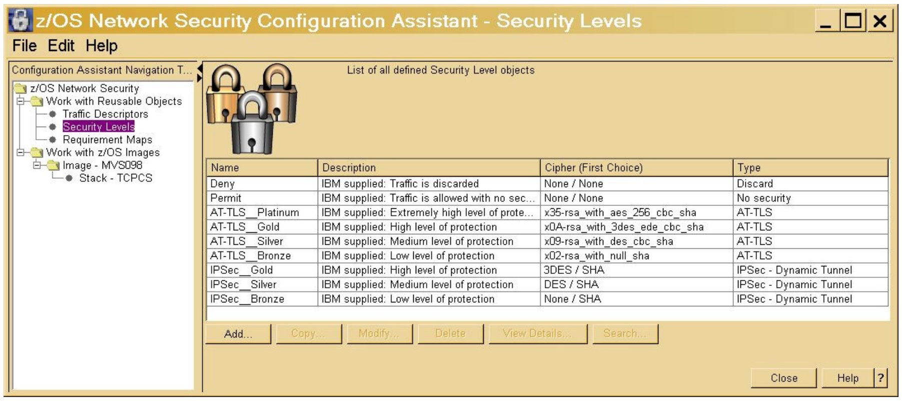
Footnotes:

[1] Value is only applicable when mapped to an IPSec Security Level of Permit, Deny or Manual Tunnel; otherwise it is ignored.
>If mapped to an IPSec Dynamic Tunnel
> - For ICMP protocol, Type and Code are set to All
> - For OSPF protocol, Type is set to All

[2] Value is only applicable when mapped to an IPSec Security Level of Permit or Deny; otherwise it is ignored.
>If mapped to an IPSec Tunnel:
> - Routing is determined by the topology selection.
> - Direction is set to Either
> - Security Class is ignored

Security levels

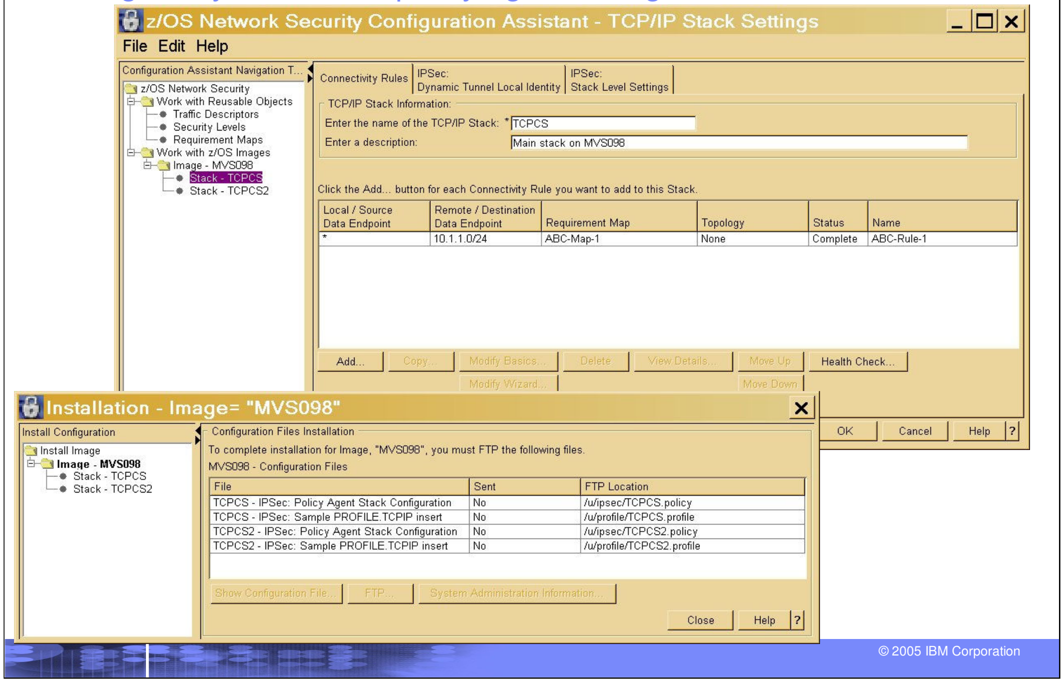
- **Security levels define different ways to protect data in the network:**
  - IPSec - Gold/Silver/Bronze levels
  - AT-TLS - Platinum/Gold/Silver/Bronze levels



List of all defined Security Level objects

Name	Description	Cipher (First Choice)	Type
Deny	IBM supplied: Traffic is discarded	None / None	Discard
Permit	IBM supplied: Traffic is allowed with no sec...	None / None	No security
AT-TLS__Platinum	IBM supplied: Extremely high level of prote...	x35-rsa_with_aes_256_cbc_sha	AT-TLS
AT-TLS__Gold	IBM supplied: High level of protection	x0A-rsa_with_3des_ede_cbc_sha	AT-TLS
AT-TLS__Silver	IBM supplied: Medium level of protection	x09-rsa_with_des_cbc_sha	AT-TLS
AT-TLS__Bronze	IBM supplied: Low level of protection	x02-rsa_with_null_sha	AT-TLS
IPSec__Gold	IBM supplied: High level of protection	3DES / SHA	IPSec - Dynamic Tunnel
IPSec__Silver	IBM supplied: Medium level of protection	DES / SHA	IPSec - Dynamic Tunnel
IPSec__Bronze	IBM supplied: Low level of protection	None / SHA	IPSec - Dynamic Tunnel

Getting ready to FTP the policy agent configuration files to z/OS



Enter the name of the TCP/IP Stack: * TCPCS

Enter a description: Main stack on MVS098

Click the Add... button for each Connectivity Rule you want to add to this Stack.

Local / Source Data Endpoint	Remote / Destination Data Endpoint	Requirement Map	Topology	Status	Name
*	10.1.1.0/24	ABC-Map-1	None	Complete	ABC-Rule-1

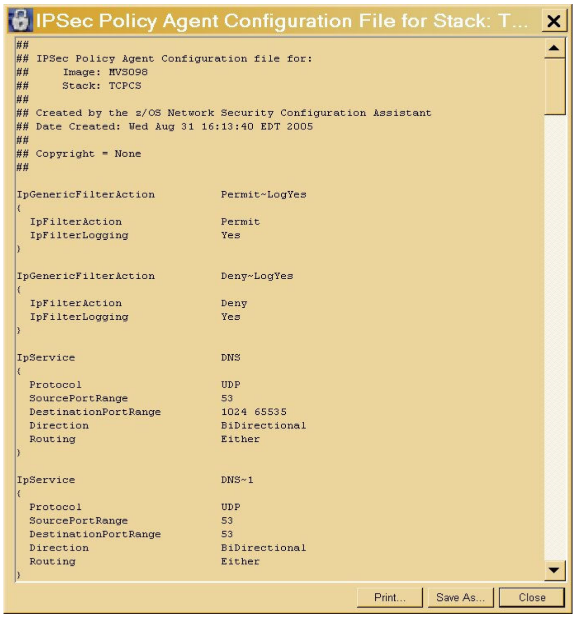
Installation - Image= "MVS098"
Install Configuration
Install Image
Image - MVS098
Stack - TCPCS
Stack - TCPCS2
Configuration Files Installation
Show Configuration File...
FTP...
System Administration Information...
Close
Help
?

To complete installation for Image, "MVS098", you must FTP the following files.

MVS098 - Configuration Files

File	Sent	FTP Location
TCPCS - IPSec: Policy Agent Stack Configuration	No	/u/ipsec/TCPCS.policy
TCPCS - IPSec: Sample PROFILE.TCPIP insert	No	/u/profile/TCPCS.profile
TCPCS2 - IPSec: Policy Agent Stack Configuration	No	/u/ipsec/TCPCS2.policy
TCPCS2 - IPSec: Sample PROFILE.TCPIP insert	No	/u/profile/TCPCS2.profile

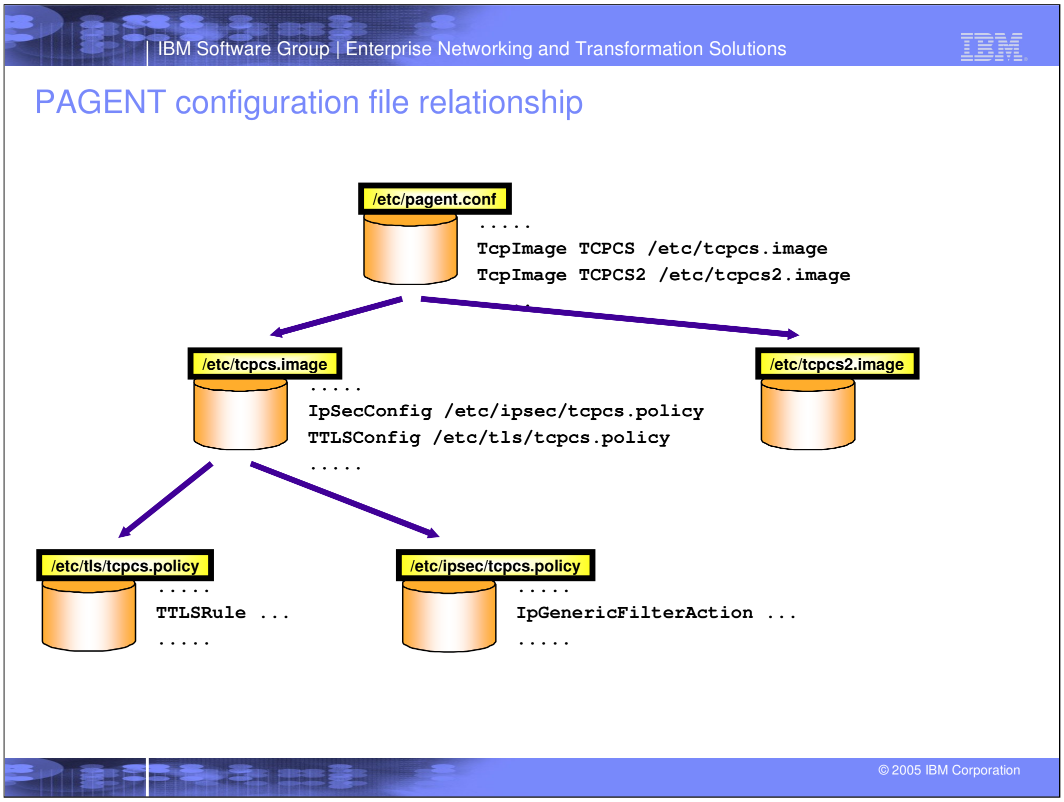
Example policy agent configuration file for IP security and AT-TLS



```
##
## IPSec Policy Agent Configuration file for:
##     Image: MVS098
##     Stack: TCPCS
##
## Created by the z/OS Network Security Configuration Assistant
## Date Created: Wed Aug 31 16:13:40 EDT 2005
##
## Copyright = None
##

IpGenericFilterAction          Permit~LogYes
{
  IpFilterAction               Permit
  IpFilterLogging              Yes
}

IpGenericFilterAction          Deny~LogYes
{
  IpFilterAction               Deny
  IpFilterLogging              Yes
}

IpService                      DNS
{
  Protocol                     UDP
  SourcePortRange              53
  DestinationPortRange         1024 65535
  Direction                    BiDirectional
  Routing                      Either
}

IpService                      DNS~1
{
  Protocol                     UDP
  SourcePortRange              53
  DestinationPortRange         53
  Direction                    BiDirectional
  Routing                      Either
}
```

- **Locate or create a new Policy Agent configuration file that identifies the target stack by jobname and the location of its image file.**
  - The image file indicates the location of the policy configuration file.
- **For example, if the stack jobname is TCPCS, then the Policy Agent configuration file /etc/pagent.conf contains the following statement:**
  - TcpImage TCPCS /etc/tcpcs1.image
- **And /etc/tcpcs.image contains the following statement:**
  - IpSecConfig /etc/tcpcs.policy
- **And start Policy Agent:**
  - pagent -c /etc/pagent.conf

PAGENT configuration file relationship



```
.....
TcpImage TCPCS /etc/tcpcs.image
TcpImage TCPCS2 /etc/tcpcs2.image
..
```

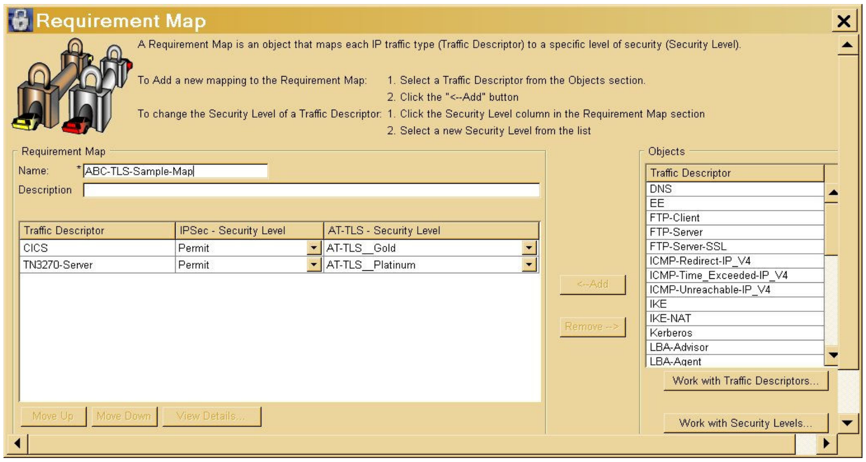
```
.....
IpSecConfig /etc/ipsec/tcpcs.policy
TTLSConfig /etc/tls/tcpcs.policy
.....
```

```
.....
TTLSRule ...
.....
```

```
.....
IpGenericFilterAction ...
.....
```

AT-TLS example for TN3270 and CICS

- **Start making a requirement map**
  - Copy the AT-TLS_Sample as a starting pint



Requirement Map

A Requirement Map is an object that maps each IP traffic type (Traffic Descriptor) to a specific level of security (Security Level).

To Add a new mapping to the Requirement Map: 1. Select a Traffic Descriptor from the Objects section.
2. Click the "<--Add" button

To change the Security Level of a Traffic Descriptor: 1. Click the Security Level column in the Requirement Map section
2. Select a new Security Level from the list

Requirement Map

Name: * ABC-TLS-Sample-Map

Description

Traffic Descriptor	IPSec - Security Level	AT-TLS - Security Level
CICS	Permit	AT-TLS__Gold
TN3270-Server	Permit	AT-TLS__Platinum

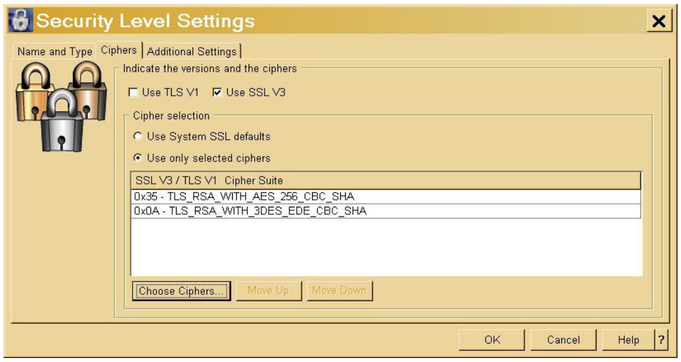
Objects

Traffic Descriptor
DNS
EE
FTP-Client
FTP-Server
FTP-Server-SSL
ICMP-Redirect-IP_V4
ICMP-Time_Exceeded-IP_V4
ICMP-Unreachable-IP_V4
IKE
IKE-NAT
Kerberos
LBA-Advisor
LBA-Agent

<--Add
Remove -->
Move Up
Move Down
View Details...
Work with Traffic Descriptors...
Work with Security Levels...

AT-TLS security level details

- The keyring may either be in an HFS file (managed by GSKKYMAN) or in RACF
- The keyring location can be specified at a z/OS image level or on a traffic descriptor that describes a specific application
- SSL/TLS protocol levels and ciphers can be chosen in the security level settings
- Support for checking with a Certificate Revocation List server (or multiple) is also supported



Security Level Settings

Indicate the versions and the ciphers

☐ Use TLS V1 ☑ Use SSL V3

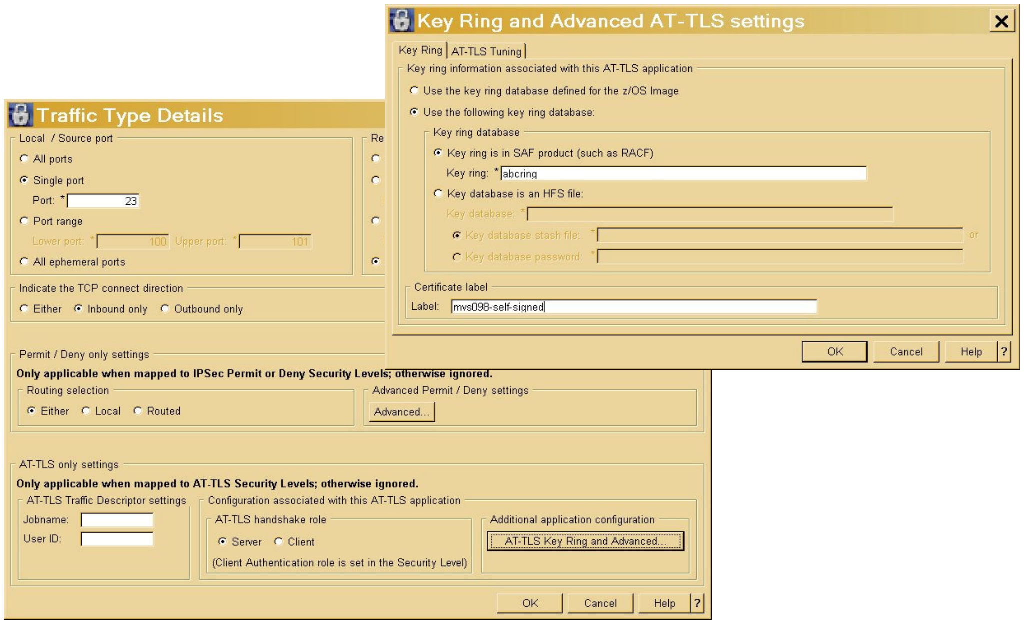
Cipher selection

○ Use System SSL defaults

● Use only selected ciphers

SSL V3 / TLS V1 Cipher Suite
0x35 - TLS_RSA_WITH_AES_256_CBC_SHA
0x0A - TLS_RSA_WITH_3DES_EDE_CBC_SHA

AT-TLS keyring specification in a traffic descriptor



Traffic Type Details

Local / Source port

○ All ports

● Single port

Port: * 23

○ Port range

Lower port: * 100 Upper port: * 101

○ All ephemeral ports

Re

Indicate the TCP connect direction

○ Either ● Inbound only ○ Outbound only

Permit / Deny only settings

Only applicable when mapped to IPSec Permit or Deny Security Levels; otherwise ignored.

Routing selection

● Either ○ Local ○ Routed

Advanced Permit / Deny settings

Advanced...

AT-TLS only settings

Only applicable when mapped to AT-TLS Security Levels; otherwise ignored.

AT-TLS Traffic Descriptor settings

Jobname:

User ID:

Configuration associated with this AT-TLS application

AT-TLS handshake role

● Server ○ Client

(Client Authentication role is set in the Security Level)

Additional application configuration

AT-TLS Key Ring and Advanced...

OK Cancel Help ?

Key Ring and Advanced AT-TLS settings

Key Ring | AT-TLS Tuning

Key ring information associated with this AT-TLS application

○ Use the key ring database defined for the z/OS Image

● Use the following key ring database:

Key ring database

● Key ring is in SAF product (such as RACF)

Key ring: * abcring

○ Key database is an HFS file:

Key database: *

● Key database stash file: * or

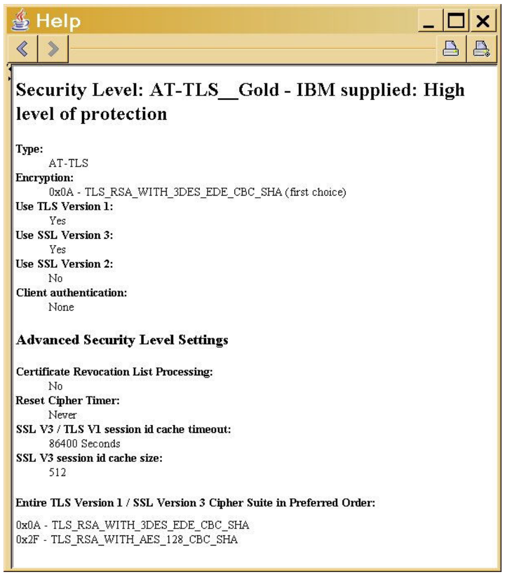
○ Key database password: *

Certificate label

Label: mvs098-self-signed

OK Cancel Help ?

AT-TLS gold and platinum service levels



Security Level: AT-TLS__Gold - IBM supplied: High level of protection

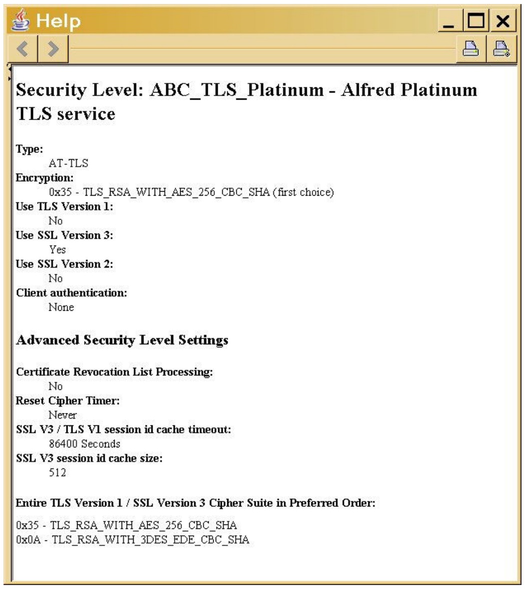
Type:
AT-TLS
Encryption:
0x0A - TLS_RSA_WITH_3DES_EDE_CBC_SHA (first choice)
Use TLS Version 1:
Yes
Use SSL Version 3:
Yes
Use SSL Version 2:
No
Client authentication:
None

Advanced Security Level Settings

Certificate Revocation List Processing:
No
Reset Cipher Timer:
Never
SSL V3 / TLS V1 session id cache timeout:
86400 Seconds
SSL V3 session id cache size:
512

Entire TLS Version 1 / SSL Version 3 Cipher Suite in Preferred Order:

0x0A - TLS_RSA_WITH_3DES_EDE_CBC_SHA
0x2F - TLS_RSA_WITH_AES_128_CBC_SHA



Security Level: ABC_TLS_Platinum - Alfred Platinum TLS service

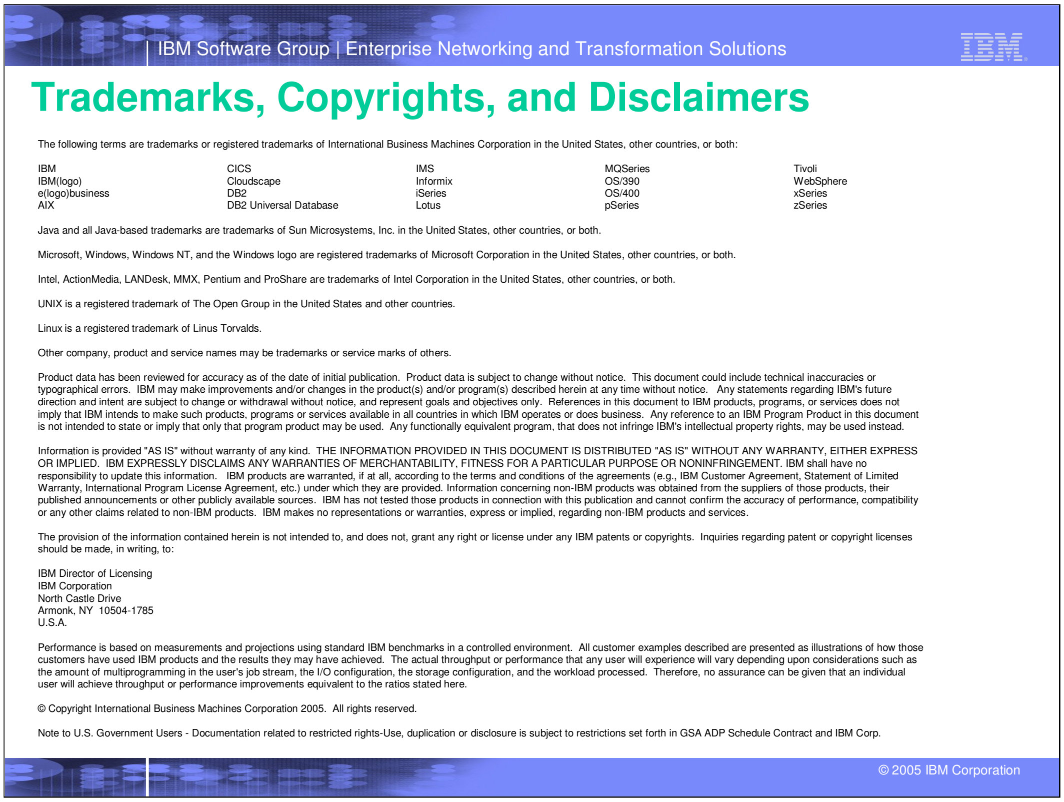
Type:
AT-TLS
Encryption:
0x35 - TLS_RSA_WITH_AES_256_CBC_SHA (first choice)
Use TLS Version 1:
No
Use SSL Version 3:
Yes
Use SSL Version 2:
No
Client authentication:
None

Advanced Security Level Settings

Certificate Revocation List Processing:
No
Reset Cipher Timer:
Never
SSL V3 / TLS V1 session id cache timeout:
86400 Seconds
SSL V3 session id cache size:
512

Entire TLS Version 1 / SSL Version 3 Cipher Suite in Preferred Order:

0x35 - TLS_RSA_WITH_AES_256_CBC_SHA
0x0A - TLS_RSA_WITH_3DES_EDE_CBC_SHA



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.