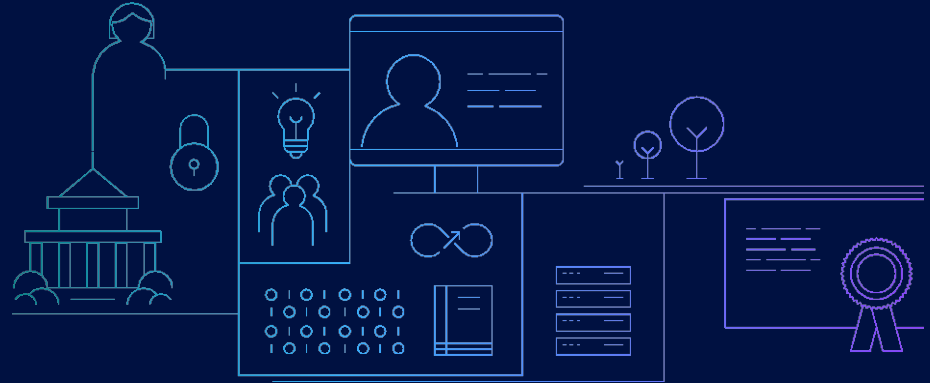


Using Network Configuration Assistant to configure zERT Policy Enforcement

—
Mike Fox
Senior Software Architect
IBM Enterprise Network Solutions
mjfox@us.ibm.com





Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

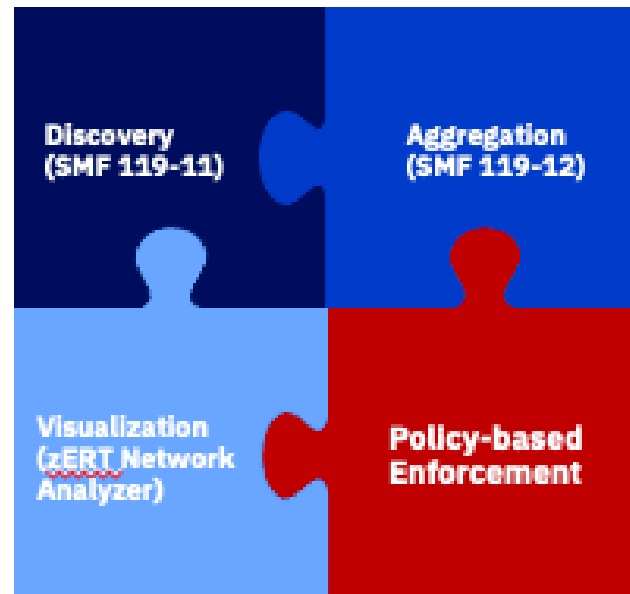
Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

zERT policy-based enforcement

Directs the TCP/IP stack to take specific actions when a user-defined security policy is or is not met for TCP/IP connections

- A new technology implemented through Network Configuration Assistant (NCA) and Policy Agent
- Rule conditions describe connections (ports, addresses, etc.) along with acceptable or unacceptable protection attributes
- Rule actions determine what happens when a connection matches the rule conditions



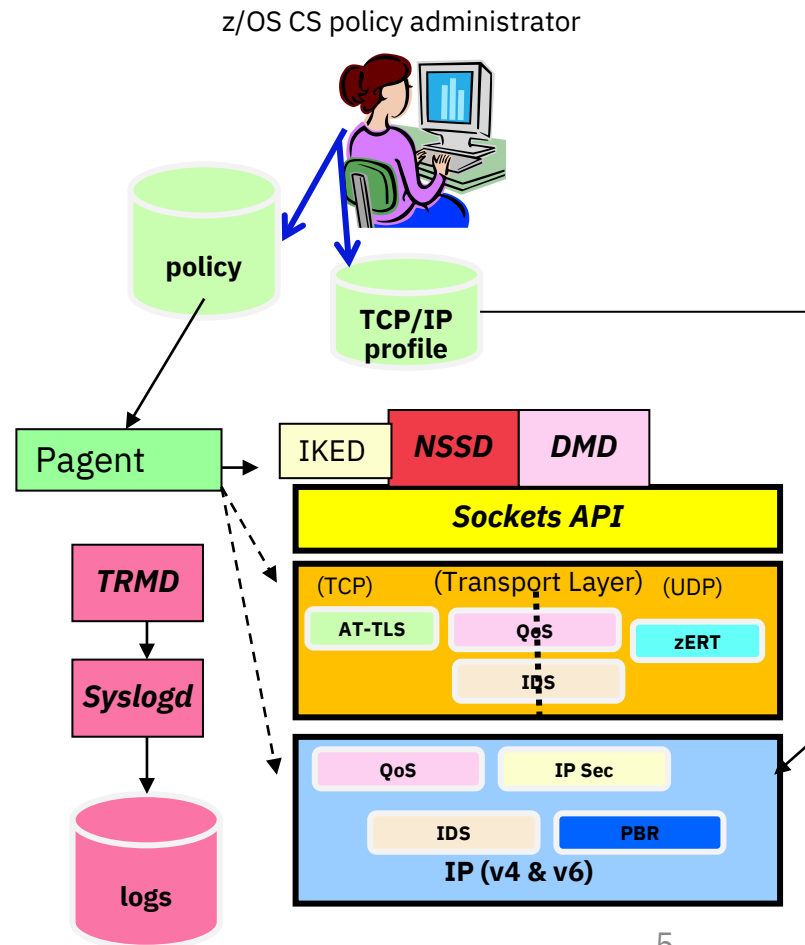
For a detailed deep dive into zERT policy-based enforcement see session: z203709 z/OS Encryption Readiness Technology goes live!

Network Configuration Assistant

GUI tool to simplify configuration of z/OS Communications Server

- TCP/IP profile
- Policy-based networking technologies
 - IP Security – IP Filter rules and VPN tunnels
 - Application Transport TLS (AT-TLS)
 - Intrusion Detection Services (IDS)
 - Policy-based Routing (PBR)
 - Quality of Service (Qos)
 - **zERT enforcement**

The focus of this presentation!



Network Configuration Assistant is a z/OSMF plug-in

You access the Network Configuration Assistant from the z/OSMF desktop by clicking on its icon

A screenshot of the 'Network Configuration Assistant' window. The title bar says 'Network Configuration Assistant'. The main content area has a blue header with the text 'Welcome to V2R5 Configuration Assistant for z/OS Communications Server' and a subtitle 'Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.' Below this, there are radio button options: 'Manage z/OS Cloud configuration' (unselected), 'Manage TCP/IP profile and policy-based networking functions' (selected), 'Create or transfer a new backing store' (unselected), and 'Open an existing backing store' (selected). There is a dropdown menu showing 'MJF_ZPE' and a text input field with '30'. A note says '* Minutes to allow backing store to open. Range is 1-30.' A 'Proceed' button is below. At the bottom, there is a section 'Learn more about Network Configuration Assistant:' with a table of links.

Learn more about Network Configuration Assistant:	
What's New	See what is new in this release.
Getting Started	First time users can learn about Network Configuration Assistant.
Migrating to z/OSMF	Migrate backing stores from Windows to z/OSMF.
Application Setup Tasks	Workflows to guide the setup of required applications.
Tutorials	Link to tutorials.
FAQs	Link to Frequently Asked Questions.
Collect Problem Determination Data	Get assistance with gathering problem determination data.

Quick links to commonly used help files

Technologies configured by the Network Configuration Assistant

Network Configuration Assistant

Network Configuration Assistant (Home) ▸ zERT [Help](#)

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT Tools

Systems Reusable Rule Sets Address Groups Traffic Descriptors Protection

Actions ▾

↔ No filter applied

	System Group or Sysplex / System Image Filter	Type Filter	Status Filter	Install S Filter
<input type="radio"/>	Default	System Group	Complete	
<input type="radio"/>	PL@X	Sysplex	Complete	N/A
<input type="radio"/>	@M@GE3	System Image	Complete	N/A
<input type="radio"/>	\$T@CK3	Stack	Incomplete	

Total: 8 Selected: 0

Home Save



The systems tree

Network Configuration Assistant

Network Configuration Assistant (Home) » zERT

Help

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT

Tools

Systems

Reusable Rule Sets

Reusable Rules

Address Groups

Traffic Descriptors

Protection Characteristics

Actions

No filter applied

	System Group or Sysplex / System Image / Stack	Type	Status	Install Status	Release	Description
<input type="radio"/>	Default	System Group	Complete			
<input type="radio"/>	[-] PLEX	Sysplex	Complete	N/A		The production sysplex
<input type="radio"/>	[-] IMAGE1	System Image	Complete	N/A	V2R5	The banking image
<input type="radio"/>	STACK1	Stack	Incomplete		V2R5	The banking stack
<input type="radio"/>	[-] IMAGE2	System Image	Complete	N/A	V2R5	The credit card image
<input type="radio"/>	STACK2	Stack	Incomplete		V2R5	The credit card stack
<input type="radio"/>	[-] IMAGE3	System Image	Complete	N/A	V2R5	The test image
<input checked="" type="radio"/>	STACK3	Stack	Incomplete		V2R5	The test stack

Total: 8 Selected: 1

Home

Save

Agenda

- Introduction to zERT Policy Enforcement and NCA
- **zERT policy rules and object structure**
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration



Comparing zERT rules to other policy rule types

In zERT policy enforcement technology, **TCP connections** are examined against the zERT policy rules

- In most other policy technologies, **packets** are examined against the policy rules
- AT-TLS is also connection-based, as are some IDS attack types
- zERT is only applicable to **TCP** connections, similar to AT-TLS

TCP connections are examined against zERT policy rules **after** they are established and re-examined when there is a significant change to their security characteristics.

- This means zERT policy rules are reactive, not proactive.

In zERT policy enforcement technology, **multiple rules** can apply to the same TCP connection

- In most other policy technologies, **only one rule** can apply to a packet or connection
- IDS is another technology in which multiple rules can apply to a connection

For example, if a TCP connection is protected by both TLS and IPsec, both a TLS rule and an IPsec rule can apply to it.

However: only one rule of a security protocol can apply to a connection.



zERT rules: Security protocols and types

zERT rules are specific to security protocols, which are:

- TLS
- IPSEC
- SSH
- No recognized protection

Within a security protocol there are three rule types:

- General rule
- Specific rule(s)
- Catch-all rule

Important note: in policy agent, these are all simply rules.

- NCA users will work with these types of rules in the GUI and NCA will provide the appropriate configuration in each rule to implement the type.



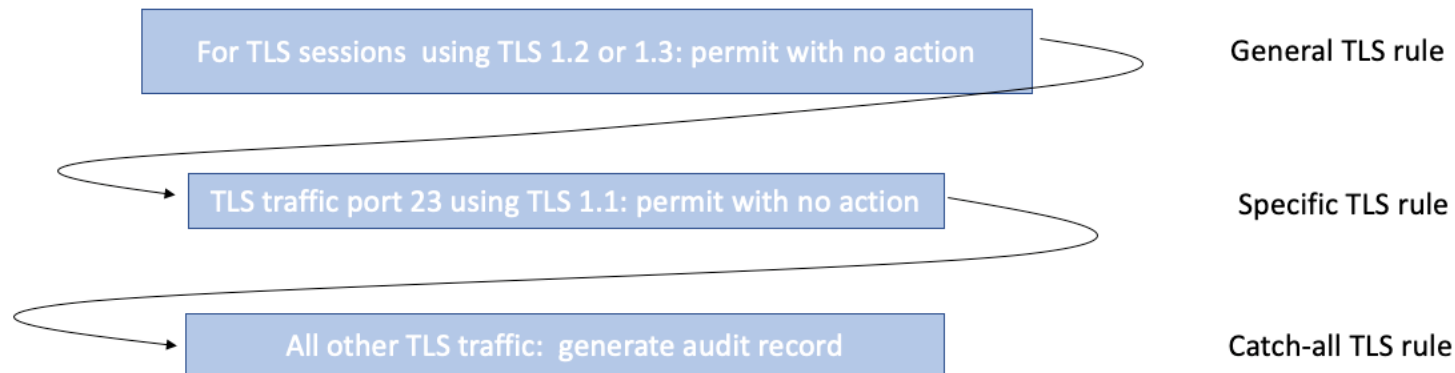
General/specific/catch-all rules use case

Customer wants at least TLS 1.2 to be used for all connections (general rule) but..

Connections to or from a specific application or address can use TLSv1.1 (specific rule)

- Perhaps because it is known that the application migration to TLSv1.2 is still in progress.

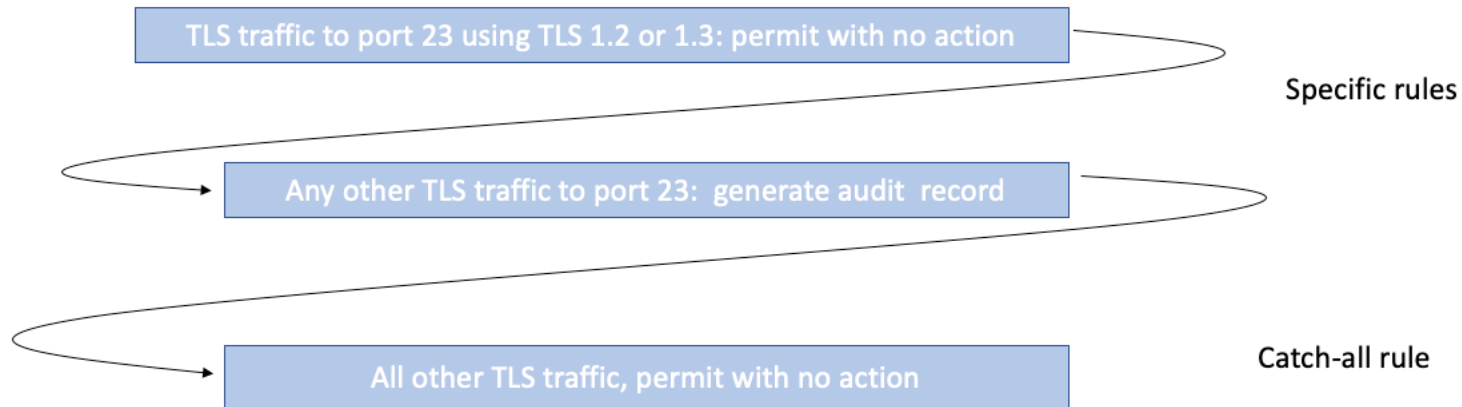
Any other connections, create an audit record





Specific rules only use case

Customer wants to verify that a specific application is using the correct levels of protection and doesn't care about the rest.

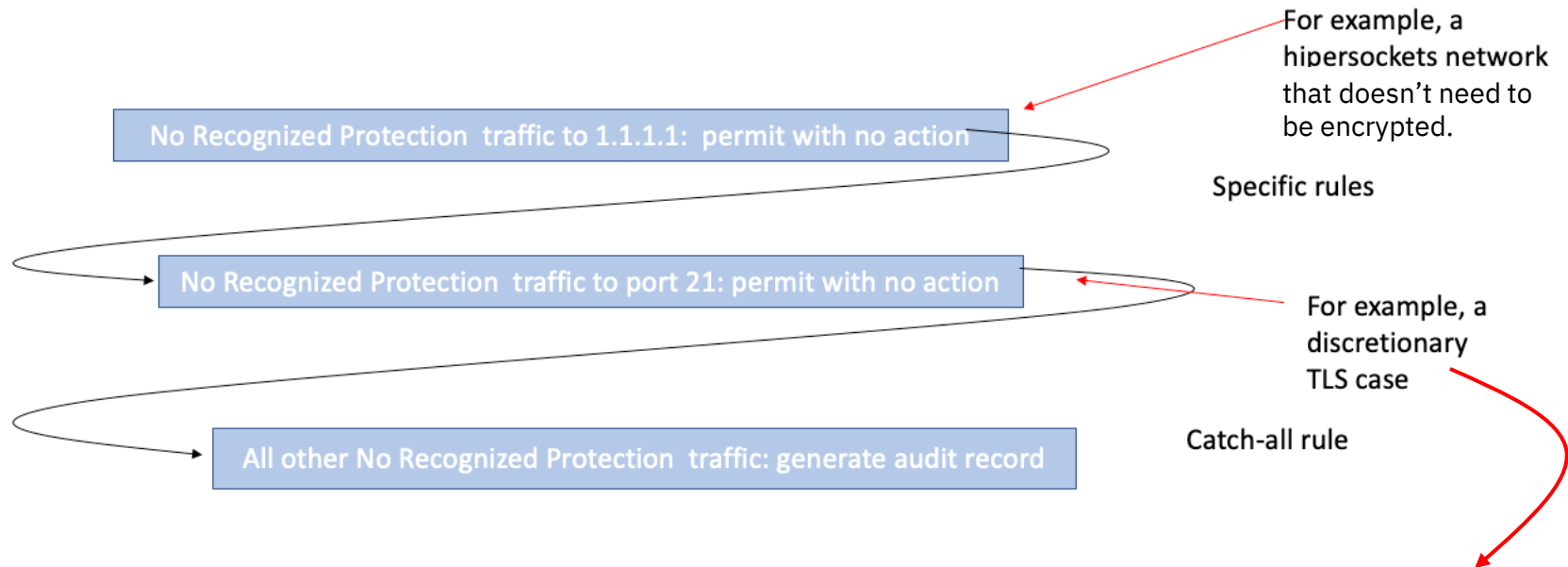




No recognized protection use case

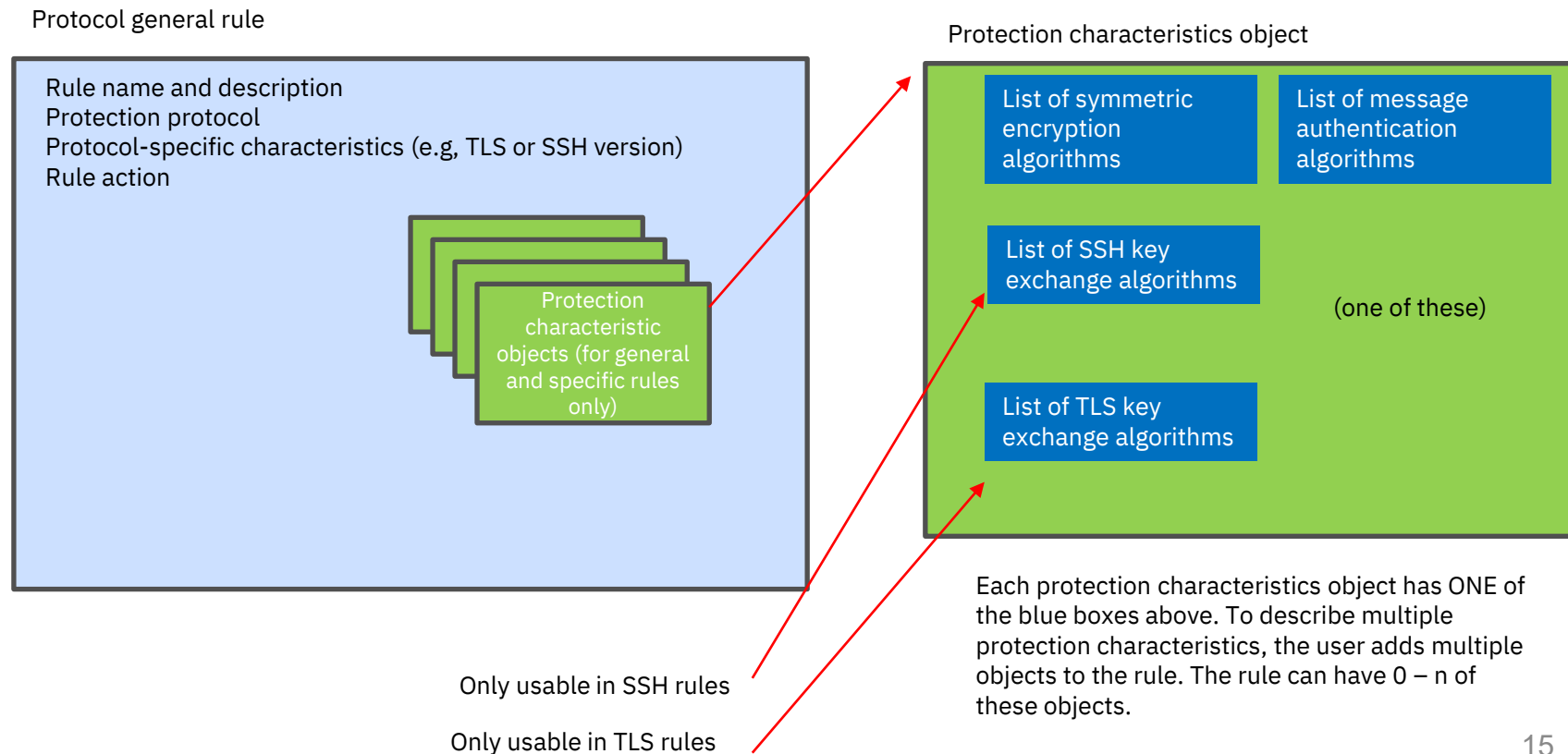
Connections with no recognized protection need to be logged, with some exceptions.

Important note: NCA does not support general rules for no recognized protection.



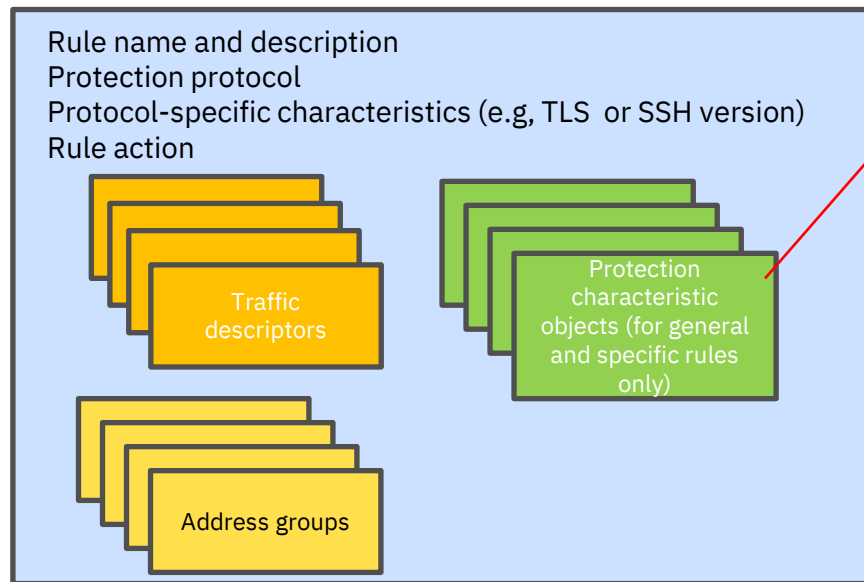
“Discretionary TLS” means the application is permitted to turn TLS on and off during the life of a connection (examples: FTP, CSSMTP, TN3270 with NEGTSURE coded).

Conceptual structure of a zERT protocol rule in NCA: general rule for TLS, IPSEC, or SSH



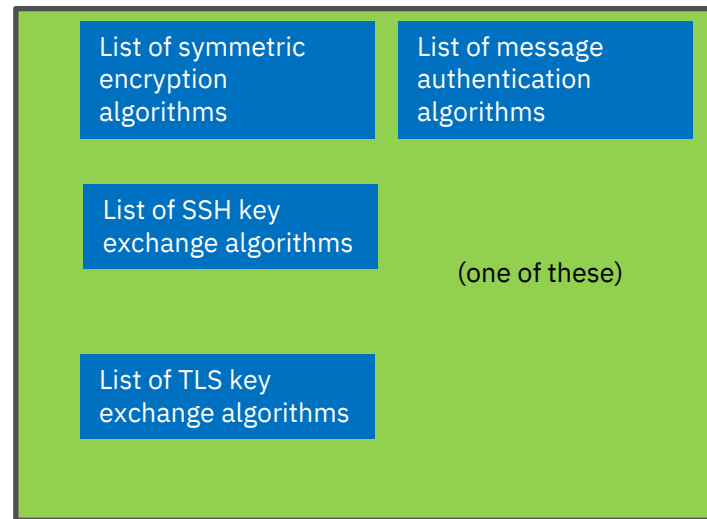
Conceptual structure of a zERT protocol rule in NCA: specific rule for TLS, IPSEC, or SSH

Specific rule for a protocol



Traffic descriptors and/or address groups specify the traffic that the specific rule applies to. May have 0-n of each of these objects.

Protection characteristics object

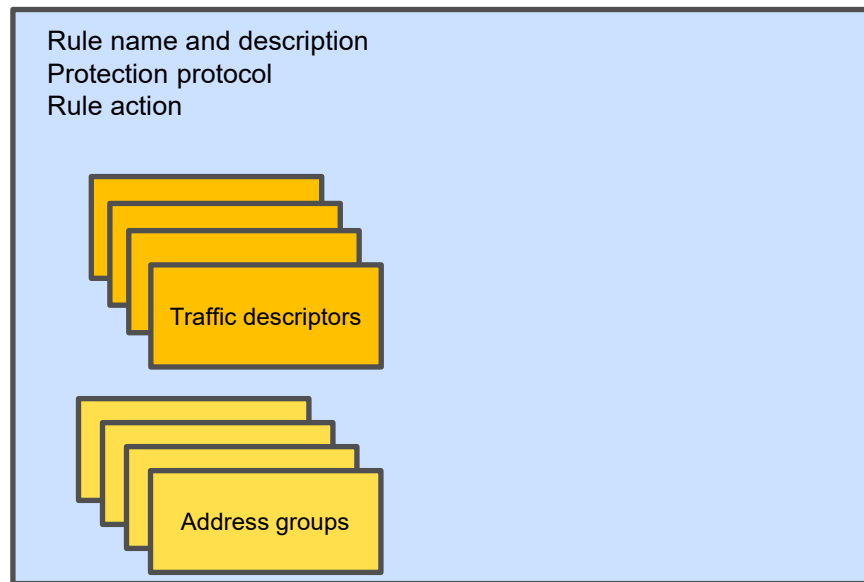


Each protection characteristics object has ONE of the blue boxes above. To describe multiple protection characteristics, the user adds multiple objects to the rule. The rule can have 0 – n of these objects.



Conceptual structure of a zERT protocol rule in NCA: specific rule for No Recognized Protection traffic

Specific rule for No Recognized Protection traffic



Traffic descriptors and/or address groups specify the traffic that the specific rule applies to. May have 0-n of each of these objects.

Because it's a rule for No Recognized Protection traffic, it has no protection characteristics.



Conceptual structure of a zERT protocol rule in NCA: Catch-all rule for TLS, IPSEC, SSH, or No Recognized Protection

Catch-all rules only contain a protection protocol specification and an action.

In the NCA GUI, users specify the catch-all action directly in the rule sets. NCA will use that information to generate a catch-all rule.

This simplifies the number of rules and objects the user has to maintain.

Note: the catch-all rule will be generated even if the action is to allow silently, so the users can see the results of their setting in the configuration file.

- Allow silently is the default action

The zERT rule set

ZERT rule set

Rule set name
Rule set description
Rule set security protocol

General protocol rule for the security protocol

Specific rules for the security protocol

Catch-all rule for the security protocol

zERT rules are always grouped into rule sets for associating to stacks

- zERT rule sets are reusable across stacks

A zERT rule set is always for one specific security protocol.

- A stack can have at most one zERT rule set associated to it for each security protocol.

A zERT rule set can contain three types of rules for its security protocol:

- Zero or one general rule
- 0-n specific rules
- One Catch-all rule



zERT rules and rule sets – reusable

All zERT rules are reusable.

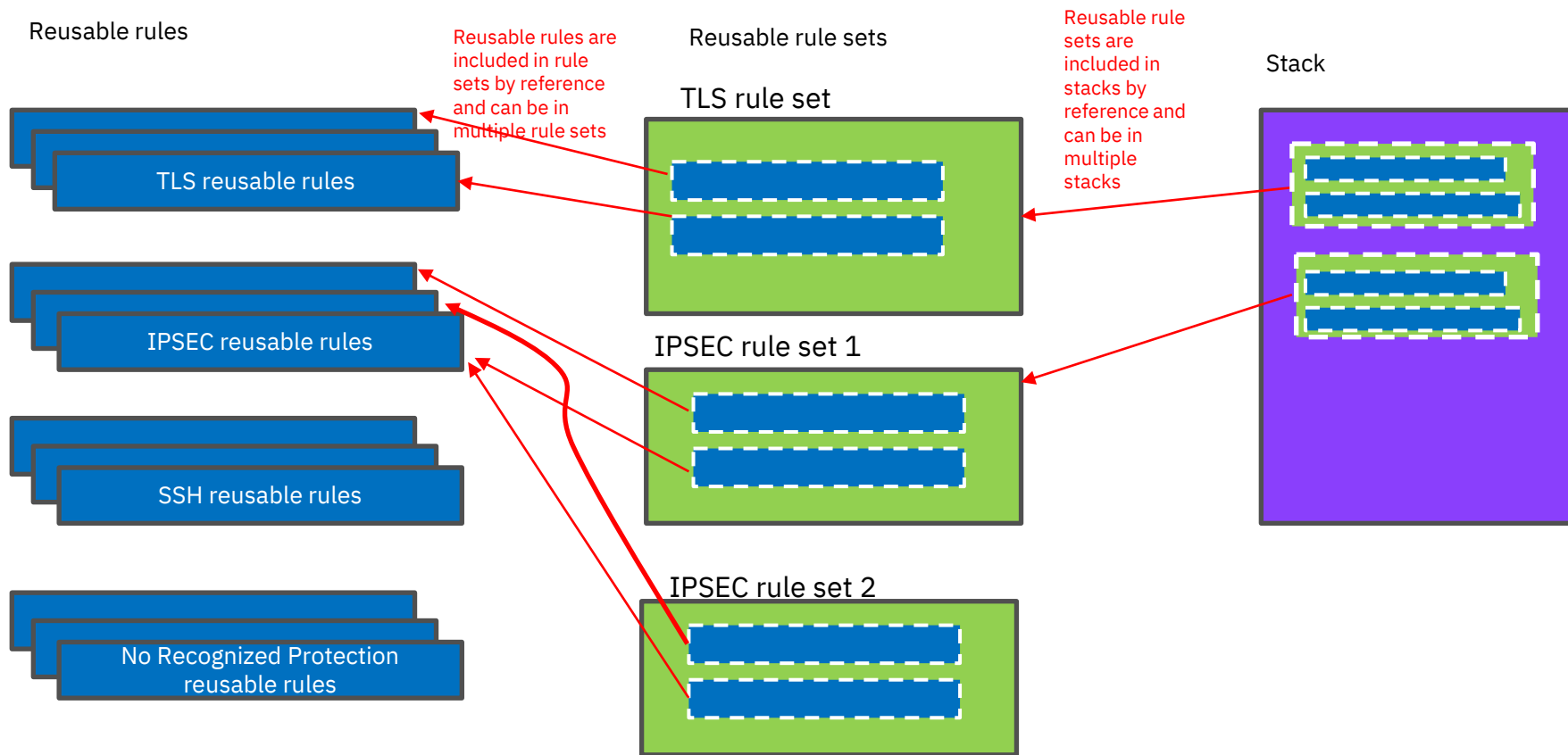
zERT rules are defined in a way that allows them to be associated with multiple rule sets, which can then be associated with multiple stacks.

- Changes made to a reusable zERT rule automatically ripple into all rule sets using that reusable rule, which will then ripple into all stacks using that rule set. Then the next time you install configuration, those changes take effect in the policy agent and the TCP/IP stack.
- “Stack specific” rules are not supported

Similarly, all zERT rule sets are reusable.



Rules, Rule Sets, and Stacks: relationship



Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- **Creating basic zERT objects in NCA**
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

The basic NCA zERT objects

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT Help

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT Tools

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors Protection Characteristics

Actions

No filter applied

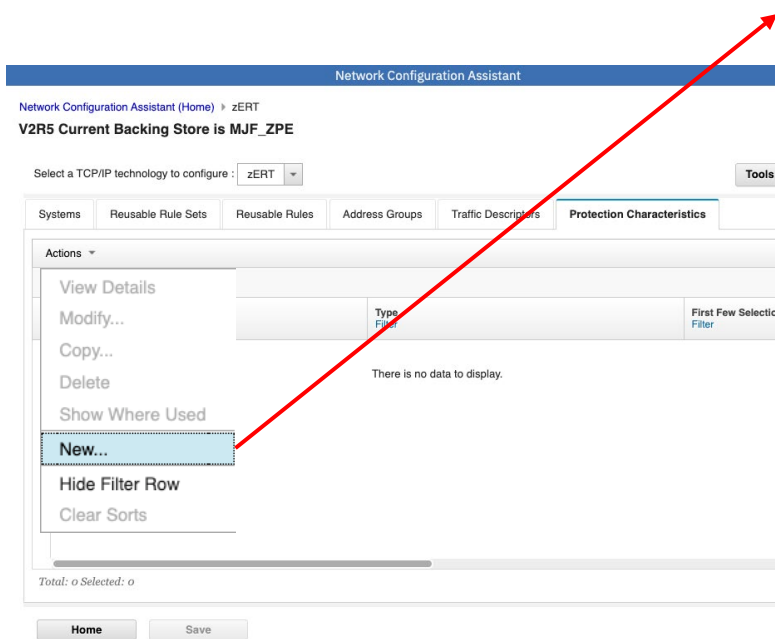
	System Group or Sysplex / System Image / Stack Filter	Type Filter	Status Filter	Install Status Filter	Release Filter
<input type="radio"/>	Default	System Group	Complete		
<input type="radio"/>	PLEX	Sysplex	Complete	N/A	
<input type="radio"/>	IMAGE1	System Image	Complete	N/A	V2R5
<input type="radio"/>	STACK1	Stack	Incomplete		V2R5
<input type="radio"/>	IMAGE2	System Image	Complete	N/A	V2R5
<input type="radio"/>	STACK2	Stack	Incomplete		V2R5
<input type="radio"/>	IMAGE3	System Image	Complete	N/A	V2R5

Total: 8 Selected: 0

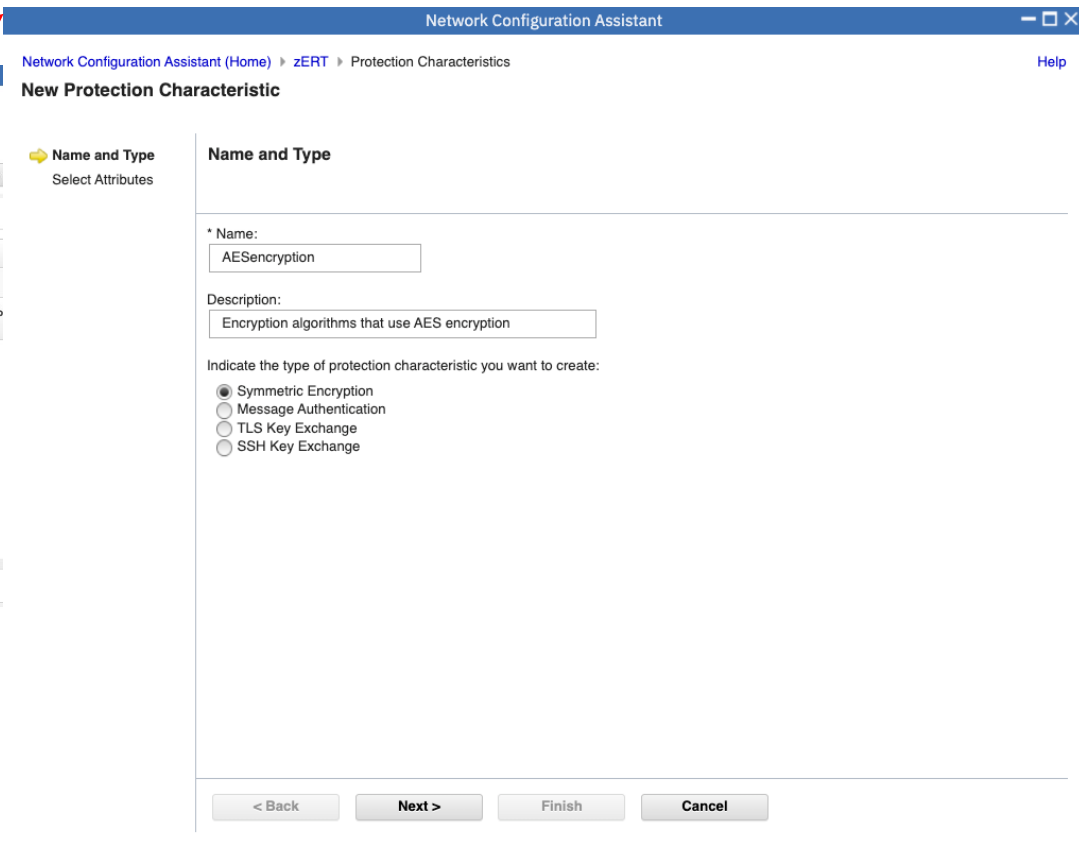
Home Save

These are the basic objects that are used to build zERT rules.

zERT protection characteristics



These objects describe algorithms for encryption, message authentication, or key exchange.

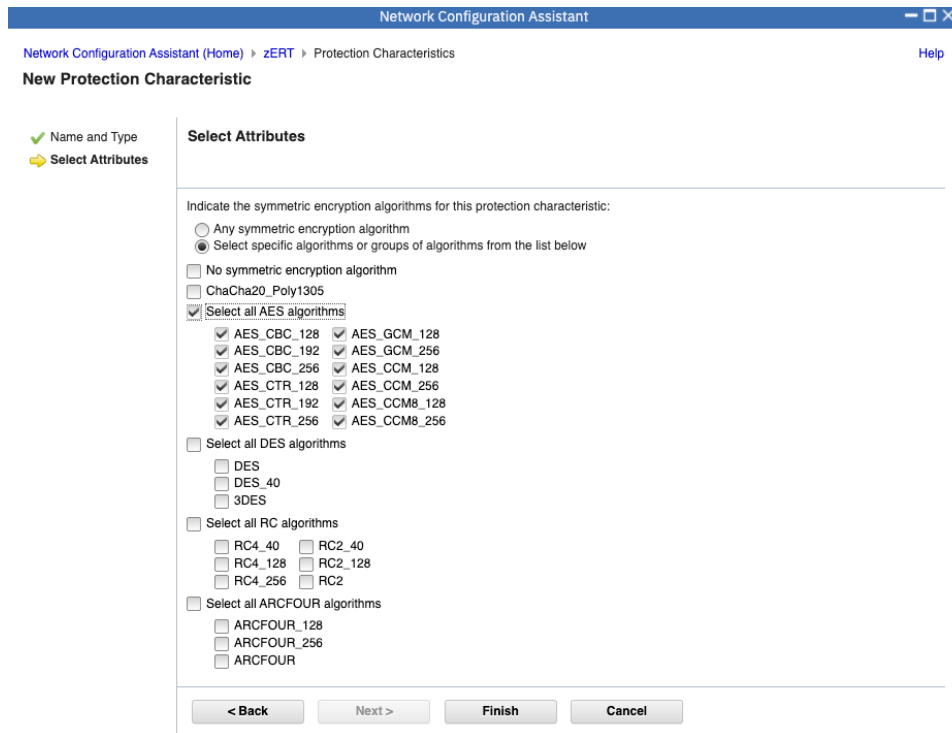


Configuring a protection characteristic

This is an example of a symmetric encryption protection characteristic.

You can select specific algorithms or you can select similar algorithms in groups.

Each protection characteristic type lists algorithms that are relevant to that type, and you select the ones that are relevant to this object.



Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Protection Characteristics

Help

New Protection Characteristic

✓ Name and Type
✚ Select Attributes

Select Attributes

Indicate the symmetric encryption algorithms for this protection characteristic:

☐ Any symmetric encryption algorithm
☒ Select specific algorithms or groups of algorithms from the list below

☐ No symmetric encryption algorithm
☐ ChaCha20_Poly1305
☒ Select all AES algorithms

<input checked="" type="checkbox"/> AES_CBC_128	<input checked="" type="checkbox"/> AES_GCM_128
<input checked="" type="checkbox"/> AES_CBC_192	<input checked="" type="checkbox"/> AES_GCM_256
<input checked="" type="checkbox"/> AES_CBC_256	<input checked="" type="checkbox"/> AES_CCM_128
<input checked="" type="checkbox"/> AES_CTR_128	<input checked="" type="checkbox"/> AES_CCM_256
<input checked="" type="checkbox"/> AES_CTR_192	<input checked="" type="checkbox"/> AES_CCM8_128
<input checked="" type="checkbox"/> AES_CTR_256	<input checked="" type="checkbox"/> AES_CCM8_256

☐ Select all DES algorithms

☐ DES
☐ DES_40
☐ 3DES

☐ Select all RC algorithms

☐ RC4_40 ☐ RC2_40
☐ RC4_128 ☐ RC2_128
☐ RC4_256 ☐ RC2

☐ Select all ARCFOUR algorithms

☐ ARCFOUR_128
☐ ARCFOUR_256
☐ ARCFOUR

< Back Next > Finish Cancel

zERT traffic descriptors

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT

Systems

Reusable Rule Sets

Reusable Rules

Address Groups

Traffic Descriptors

Protection Characteristics

Actions

View Details

Modify...

Copy...

Delete

Show Where Used

New...

Hide Filter Row

Clear Sorts

CSSMTP

Connect-Direct-Server

Connect-Direct-Client

Connect-Direct-API-Server

Connect-Direct-API-Client

FTP-Client

FTP-Server

LBA-Advisor

LBA-Agent

LDAP-Server

Description

Filter

(VERIFY) IBM supplied: Automated Domain Name Registration traffic

(VERIFY) IBM supplied: Centralized Policy Server

(VERIFY) IBM supplied: CICS traffic

(VERIFY) IBM supplied: CSSMTP traffic

(VERIFY) IBM-supplied Connect:Direct acting as a data transfer server

(VERIFY) IBM-supplied Connect:Direct acting as a data transfer client

(VERIFY) IBM-supplied Connect:Direct acting as RESTful API server

(VERIFY) IBM-supplied Connect:Direct acting as a RESTful API client

(VERIFY) IBM supplied: FTP Client traffic

(VERIFY) IBM supplied: FTP Server traffic

(VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic

(VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic

(VERIFY) IBM supplied: LDAP Server traffic

Total: 27 Selected: 0

Home

Save

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Traffic Descriptor

Help

New Traffic Descriptor

Traffic descriptors contain details of traffic types which are mapped to security levels within requirement maps. A traffic descriptor can contain a single type of traffic or multiple types of traffic.

* Name: MyAppTraffic

Description: My custom application

List of traffic types in this traffic descriptor

Actions

Move Up

Move Down

Modify...

Delete

Move Up

Move Down

New...

Local Port	Remote Port	Connect Direction	Job Name	User ID
There is no data to display.				

Total: 0 Selected: 0

OK

Cancel

Next slide

These objects describe traffic patterns for specific workloads. IBM provides a set of standard traffic descriptors.

26

Enterprise Networking Solutions | © 2022 IBM Corporation

zERT traffic type

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Traffic Descriptor > Traffic Type - TCP

Help

New Traffic Type - TCP

Details

Local port

☐ All ports

☒ Single port

100

☐ Port range

* Lower port: 100 * Upper port: 101

☐ Ephemeral ports

Remote port

☐ All ports

☐ Single port

100

☐ Port range

* Lower port: 100 * Upper port: 101

☒ Ephemeral ports

Indicate the TCP connect direction

☐ Either ☒ Inbound only ☐ Outbound only

Discretionary TLS

☐ A connection using this traffic pattern is expected to switch TLS protection on and off during its lifetime.

RESULT: This property is only effective when this traffic descriptor is used in a TLS rule

Jobname: JOB100

User ID: USER1*

OK Cancel

Discretionary TLS is unique to zERT and only applies to TLS zERT rules.

zERT address groups

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT

Systems Reusable Rule Sets Reusable Rules **Address Groups** Traffic Descriptors Protection Characteristic

Actions

- View Details
- Modify...
- Copy...
- Delete
- Show Where Used
- New...**
- Hide Filter Row
- Clear Sorts

First Few Addresses	Description
Filter	Filter
	IBM supplied: All IPv4 addresses are applied
	IBM supplied: All IPv6 addresses are applied
	IBM supplied: All IPv4 and IPv6 addresses are applied

Total: 3 Selected: 0

Home Save

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Address Group

Help

New IP Address Group

Use this panel to configure a group of IP addresses.

9.37.236.137
4.98.124.187

5.96.158.184
2.45.197.242

3.15.141.211
7.37.253.241
8.63.138.187

* Name:
my-application-addr

Description:
Addresses for my application

Click a table cell and type the IP address or description.

Actions

IP Address	Description
<input type="radio"/> 1.1.1.1	<input type="text" value="a single IP address"/>
<input type="radio"/> 10.1.1.2-10.1.1.99	<input type="text" value="a range of IP addresses"/>
<input type="radio"/> 2.2.2.0/24	<input type="text" value="an IP prefix"/>
<input type="radio"/> 2001:0db8::1	<input type="text" value="Can include IPv6 too!"/>
<input type="radio"/> 2001:0db8:99::1-2001:0db8:99::120	<input type="text" value="an IPv6 range"/>
<input type="radio"/> 2001:0db8:101::/64	<input type="text" value="an IPv6 prefix"/>
<input type="radio"/> @partner-ip-addr	<input type="text" value="Can nest address groups up to 3 deep"/>

Total: 7 Selected: 0

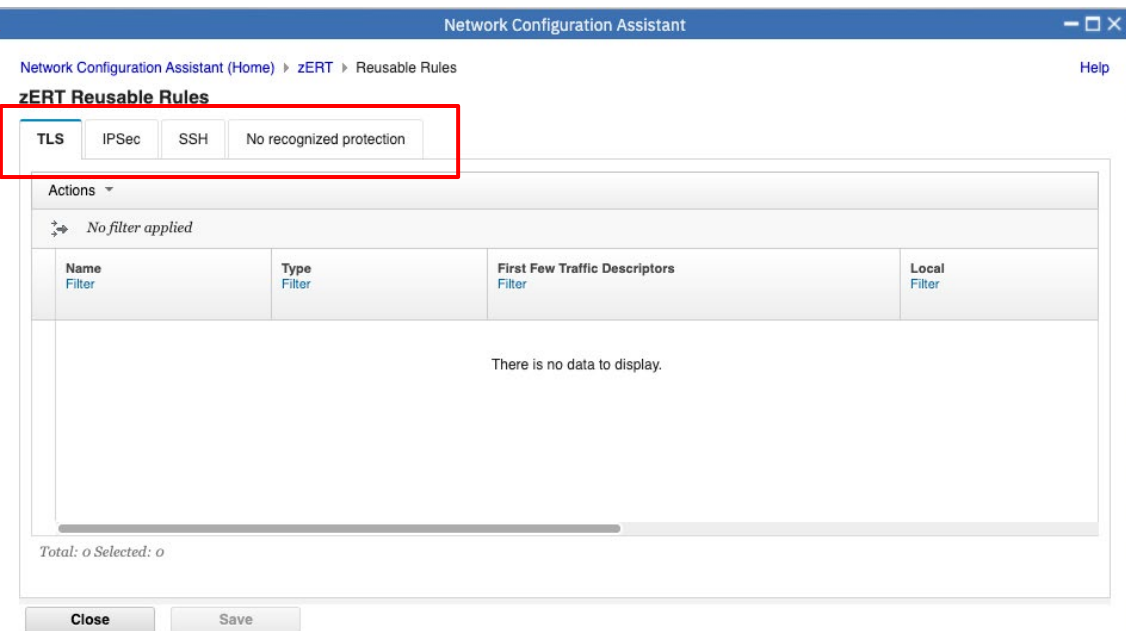
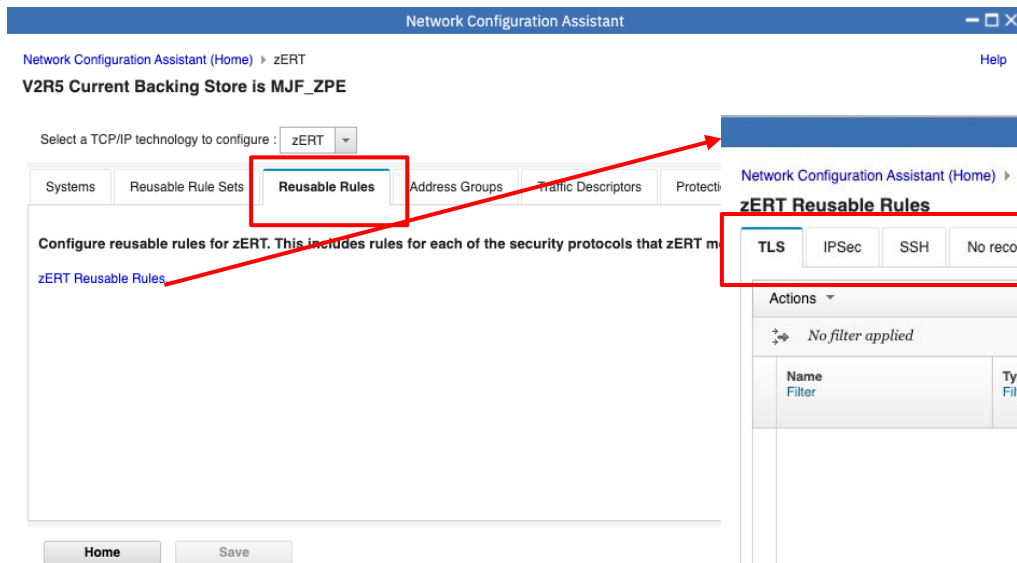
OK Cancel

This slide illustrates some of the things you can do with zERT address groups.

Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- **Creating zERT rules in NCA**
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

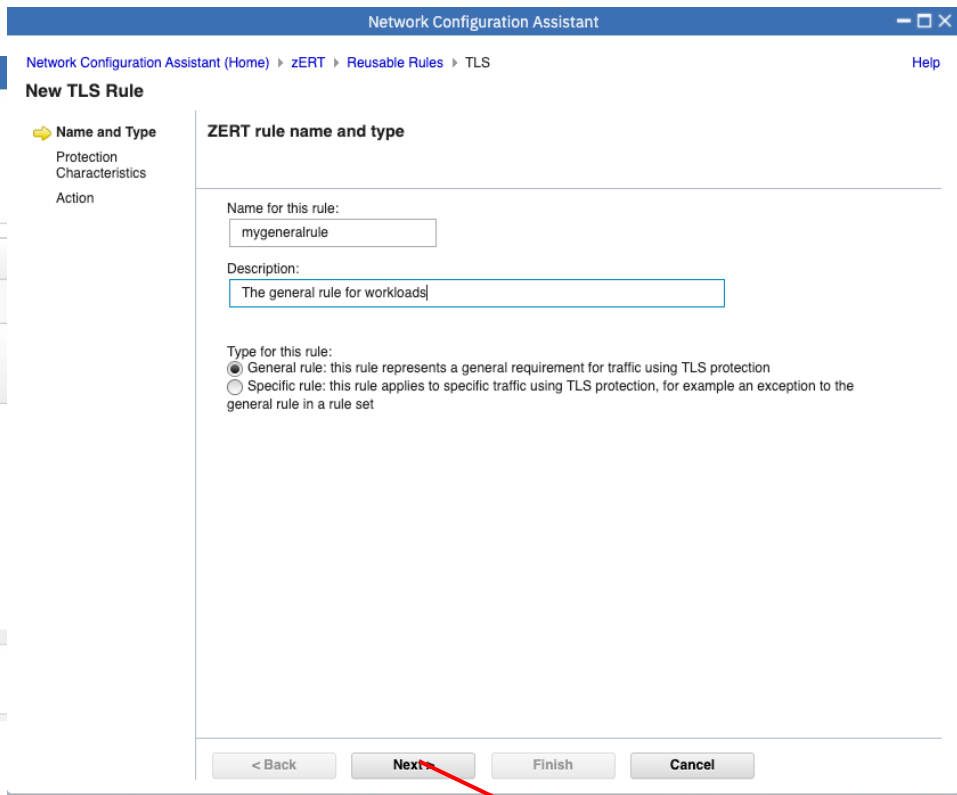
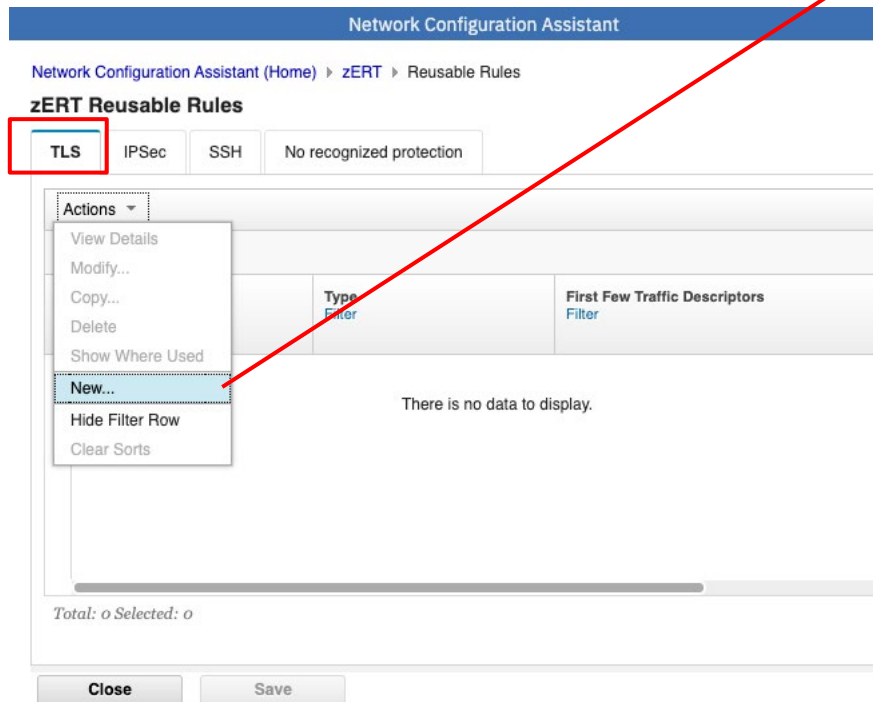
Where to create and manage zERT rules in NCA



Two things to remember about zERT rules in NCA:

1. They are all reusable.
2. They are organized into different tabs by security protocol.

Creating a TLS general rule



When creating a new rule, you first give it a name, (optionally) a description, and indicate whether it's a general rule or a specific rule.

Next slide

New TLS general rule: protection characteristics

Network Configuration Assistant

Network Configuration Assistant (Home) > ZERT > Reusable Rules > TLS

New TLS Rule

✓ Name and Type
👉 Protection Characteristics
Action

Protection Characteristics

Select TLS versions for this rule:

☐ Any TLS version

☒ Select from the choices below:

☐ SSL V2 ☐ TLS 1.1
☐ SSL V3 ☒ TLS 1.2
☐ TLS 1.0 ☒ TLS 1.3

Specify protection characteristics for this rule

Actions ▾

➡ No filter applied

<input type="checkbox"/> Name Filter	Type Filter	First Few Selections Filter	Description Filter
<input checked="" type="checkbox"/> tlske-RSA	TLSKeyExchange	RSA, RSA_EXPORT, RSA_PSK	TLS key exchange algorithms using RSA
<input type="checkbox"/> msgauth-small-SHA	MessageAuthentication	HMAC_SHA2_256_128, HMAC_SHA1_96, HMAC_SHA1	Message authentication using SHA less than 192 bits
<input checked="" type="checkbox"/> msgauth-SHA192	MessageAuthentication	HMAC_SHA2_224, HMAC_SHA2_256, HMAC_SHA2_384, HMAC_SHA2_512, HMAC_SHA2_384_192, HMAC_SHA2_512_256,...	Message authentication using SHA-192 or greater
<input type="checkbox"/> symmcntr-DES	SymmetricEncryption	DES, DES_40, 3DES	Symmetric encryption using DES
<input checked="" type="checkbox"/> symmcntr-AES	SymmetricEncryption	AES_CBC_128, AES_GCM_128, AES_CBC_192, AES_GCM_256, AES_CBC_256, AES_CCM_128,...	Symmetric encryption using AES

Total: 5 Selected: 3

< Back Next > Finish Cancel

Checkboxes make selecting TLS versions and protection characteristics objects quick and easy!

New ones can also be created from this panel.

Next slide



New TLS general rule: action

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules > TLS [Help](#)

New TLS Rule

- ✓ Name and Type
- ✓ Protection Characteristics
- 👉 Action

Action

Specify action to take on TLS traffic that matches this rule

☒ Allow silently (take no action)

☐ Take the following actions

- ☐ Write an audit record (zERT connection detail SMF record)
- ☐ Log connection to syslogd at log level: 4 - Warning ▾
- ☐ Log connection to the console (TCPIP job log)
- ☐ Reset TCP Connection

< Back Next > **Finish** Cancel

Finally you pick the action for traffic that matches this rule.

Next slide

Creating a TLS specific rule

The screenshot shows the 'Network Configuration Assistant' interface. On the left, the 'zERT Reusable Rules' section is active, displaying a table with one rule: 'general'. A red arrow points from the 'New...' button in the 'Actions' menu to the 'New TLS Rule' configuration page on the right.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules

zERT Reusable Rules

TLS | IPSec | SSH | No recognized protection

Actions

- View Details
- Modify...
- Copy...
- Delete
- Show Where Used
- New...
- Hide Filter Row
- Clear Sorts

Type Filter	First Few Traffic Descriptors Filter	Local Filter
general	n/a	n/a

Total: 1 Selected: 1

Close Save

New TLS Rule

Network Configuration Assistant (Home) > zERT > Reusable Rules > TLS

Name and Type

- Traffic Descriptors
- Data Endpoints
- Protection
- Characteristics
- Action

ZERT rule name and type

Name for this rule:
Tlnet-TLS-rule

Description:
Specific rule for Tlnet traffic which is not fully up to date

Type for this rule:
☐ General rule: this rule represents a general requirement for traffic using TLS protection
☒ Specific rule: this rule applies to specific traffic using TLS protection, for example an exception to the general rule in a rule set

< Back Next > Finish Cancel

Now let's create a specific rule, for traffic that doesn't match the general rule but is allowed as an exception.

Next slide



TLS specific rule: Traffic descriptors

The screenshot shows the 'Network Configuration Assistant' window with the 'New TLS Rule' dialog open. The 'Traffic Descriptors' tab is selected, showing a list of traffic descriptors. The first descriptor is 'TN3270-Server', which is selected. Below it are two more descriptors, both labeled 'Select a traffic descriptor'. The 'Total: 3 Selected: 0' status is shown at the bottom of the list. The 'Next >' button is highlighted with a red arrow pointing to the 'Next slide' text.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules > TLS Help

New TLS Rule

- ✓ Name and Type
- ➡ **Traffic Descriptors**
- Data Endpoints
- Protection
- Characteristics
- Action

Traffic Descriptors

Actions ▾ | Move Up Move Down

	Traffic Descriptor
<input checked="" type="radio"/>	TN3270-Server ▾
<input type="radio"/>	Select a traffic descriptor ▾
<input type="radio"/>	Select a traffic descriptor ▾

Total: 3 Selected: 0

< Back Next > Finish Cancel

The traffic descriptor describes the workload pattern that will match this rule. In this example it's the TN3270 server.

Next slide



TLS specific rule: data endpoints

Network Configuration Assistant

Network Configuration Assistant (Home) > ZERT > Reusable Rules > TLS

Help

New TLS Rule

- ✓ Name and Type
- ✓ Traffic Descriptors
- ➡ Data Endpoints
- Protection
- Characteristics
- Action

Data Endpoints

Local data endpoint

☒ Address group:
All_IP_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y

Remote data endpoint

☒ Address group:
All_IP_Addresses

☐ * IPv4 or IPv6 address, subnet, or range:

Examples: x.x.x.x, x.x.x.x/yy, x.x.x.x-y.y.y.y
x::x, x::x/yyy, x::x-y::y

< Back Next > Finish Cancel

In this example the default endpoints of “All_IP_Addresses” is the appropriate choice, but you may have other use cases that require this to be specified.

Next slide

TLS specific rule: protection characteristics

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules > TLS

New TLS Rule

- ✓ Name and Type
- ✓ Traffic Descriptors
- ✓ Data Endpoints
- Protection Characteristics**
- Action

Protection Characteristics

Select TLS versions for this rule:

☐ Any TLS version

☒ Select from the choices below:

☐ SSL V2 ☒ TLS 1.1

☐ SSL V3 ☐ TLS 1.2

☐ TLS 1.0 ☐ TLS 1.3

Specify protection characteristics for this rule

Actions ▾

✚ No filter applied

<input type="checkbox"/> Name Filter	Type Filter	First Few Selections Filter	Description Filter
<input checked="" type="checkbox"/> tiske-RSA	TLSKeyExchange	RSA, RSA_EXPORT, RSA_PSK	TLS key exchange algorithms using RSA
<input type="checkbox"/> msgauth-small-SHA	MessageAuthentication	HMAC_SHA2_256_128, HMAC_SHA1_96, HMAC_SHA1	Message authentication using SHA less than 192
<input checked="" type="checkbox"/> msgauth-SHA192	MessageAuthentication	HMAC_SHA2_224, HMAC_SHA2_256, HMAC_SHA2_384, HMAC_SHA2_512, HMAC_SHA2_384_192, HMAC_SHA2_512_256...	Message authentication using SHA-192 or greater
<input type="checkbox"/> symmcncr-DES	SymmetricEncryption	DES, DES_40, 3DES	Symmetric encryption using DES
<input checked="" type="checkbox"/> symmcncr-AES	SymmetricEncryption	AES_CBC_128, AES_GCM_128, AES_CBC_192, AES_GCM_256, AES_CBC_256, AES_CCM_128,...	Symmetric encryption using AES

Total: 5 Selected: 3

< Back Next > Finish Cancel

This is the same panel as in the general rule. You pick the protection characteristics you are looking for in the specific traffic.

Next slide

TLS specific rule: action

The screenshot shows the 'Network Configuration Assistant' window with the 'New TLS Rule' dialog open. The 'Action' tab is selected, showing options to 'Allow silently' or 'Take the following actions'. The 'Take the following actions' section includes checkboxes for writing an audit record, logging to syslog, logging to the console, and resetting the TCP connection. The 'Log connection to syslogd' checkbox is checked, and the log level is set to '4 - Warning'. The 'Finish' button is highlighted with a red arrow pointing to the text 'Next slide'.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules > TLS Help

New TLS Rule

- ✓ Name and Type
- ✓ Traffic Descriptors
- ✓ Data Endpoints
- ✓ Protection Characteristics
- ➡ Action

Action

Specify action to take on TLS traffic that matches this rule

☒ Allow silently (take no action)

☐ Take the following actions

- ☐ Write an audit record (zERT connection detail SMF record)
- ☒ Log connection to syslogd at log level: 4 - Warning
- ☐ Log connection to the console (TCPIP job log)
- ☐ Reset TCP Connection

< Back Next > Finish Cancel

This panel is the same for specific and general rules.

Next slide

Two rules now created

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Reusable Rules

Help

zERT Reusable Rules

TLSIPSecSSHNo recognized protection

Actions

No filter applied

	Name Filter	Type Filter	First Few Traffic Descriptors Filter	Local Filter	Remote Filter	First Few Protection Characteristics Filter	Action Filter	Description Filter
<input checked="" type="radio"/>	Telnet-TLS-rule	specific	TN3270-Server	All_IP_Addresses	All_IP_Addresses	tlske-RSA, msgauth-SHA192, symmencr-AES, TLSv1.1	Allow silently (take no action)	Specific rule for Telnet traffic which is not fully up to date
<input type="radio"/>	mygeneralrule	general	n/a	n/a	n/a	tlske-RSA, msgauth-SHA192, symmencr-AES, TLSv1.2, TLSv1.3	Allow silently (take no action)	The general TLS rule for workloads

Total: 2 Selected: 1

CloseSave

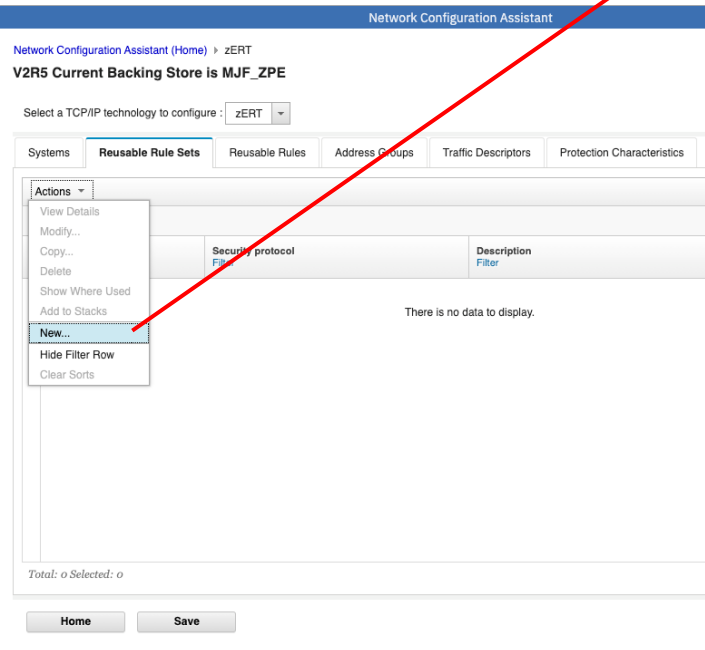
We now have a general TLS rule and a specific TLS rule.

Note that you do not create catch-all rules here. They are automatically created for you in rule sets, which we will discuss next.

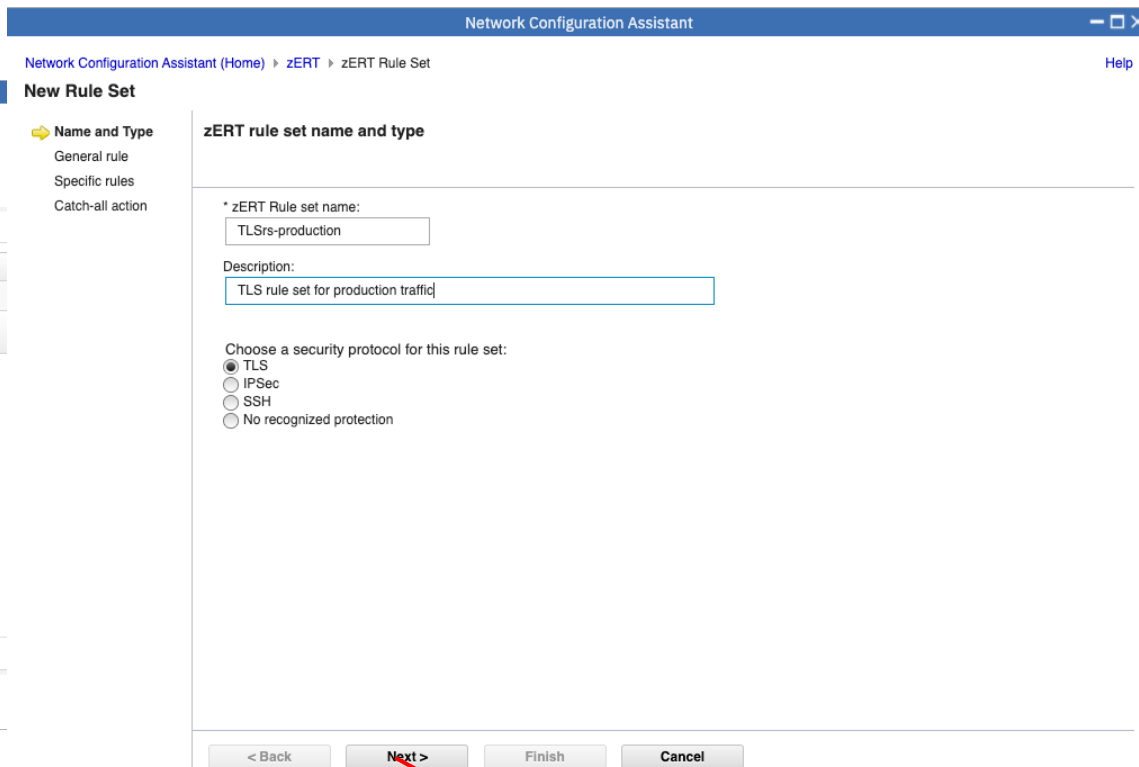
Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- **Creating zERT rule sets in NCA**
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

zERT rule sets



Use zERT rule sets to organize rules for a single security protocol in a hierarchical fashion.



Next slide

Rule set: General Rule

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > zERT Rule Set [Help](#)

New Rule Set

- ✓ Name and Type
- ➡ **General rule**
- Specific rules
- Catch-all action

General TLS Rule

If you have a general rule for how TLS traffic should be protected by this rule set, choose it here. If not, click Next to move on to specific rules.

Actions ▾

✚✚ No filter applied

	Name	First Few Protection Characteristics	Action	Description
<input type="radio"/>	No General Rule	N/A	N/A	
<input checked="" type="radio"/>	mygeneralrule	tlske-RSA, msgauth-SHA192, symmcncr-AES, TLSv1.2, TLSv1.3	Allow silently (take no action)	The general TLS rule for workloads

Total: 2 Selected: 1

< Back **Next >** Finish Cancel

Recall that the general rule represents the general requirement for traffic in your network that uses the rule set's security protocol.

You can have zero or one general rule per rule set.

You can select an existing reusable general rule or create a new one from this panel.

Next slide

Rule set: Specific Rules

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > zERT Rule Set

New Rule Set

- ✓ Name and Type
- ✓ General rule
- ➡ **Specific rules**
 - Catch-all action

Specific rules

Specify rules for specific traffic. If you have a general rule, these represent the exceptions to that rule.

Actions ▾

✚✚ No filter applied

<input type="checkbox"/>	Name	First Few Traffic Descriptors	Local	Remote	First Few Protection Characteristics
<input checked="" type="checkbox"/>	Telnet-TLS-rule	TN3270-Server	All_IP_Addresses	All_IP_Addresses	tlske-RSA, msgauth-SHA192, symmencr-AES, TLSv1.1
<input type="checkbox"/>	TLS-file-transfer	FTP-Server, Connect-Direct-Server	All_IP_Addresses	All_IP_Addresses	msgauth-SHA192, symmencr-DES, symmencr-AES, TLSv1.1

Total: 2 Selected: 1

< Back Next > Finish Cancel

Recall that specific rules represent exceptions to the general rule.

All existing reusable specific rules for the rule set's security protocol are presented in a table and you simply select the ones that you want to use in this rule set.

You can also create new reusable specific rules in this panel.

You can set the order of selected specific rules in this panel as well.

Next slide

Rule set: Catch-all action

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > zERT Rule Set

Help

New Rule Set

- ✓ Name and Type
- ✓ General rule
- ✓ Specific rules
- ★ Catch-all action

Catch-all action

Choose the action for all TLS traffic that doesn't match the general rule or any specific rules

☐ Allow Silently (take no action)

☒ Take the following actions

- ☒ Write an audit record (zERT connection detail SMF record)
- ☐ Log connection to syslogd at log level: 4 - Warning
- ☒ Log connection to the console (TCPIP job log)
- ☐ Reset TCP Connection

< Back Next > Finish Cancel

The catch-all action tells zERT what to do about connections that do not match the general rule or any of the specific rules.

You will likely want to take some sort of action on these connections.

Next slide

Rule set completed

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT [Help](#)

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT [Tools](#)

Systems **Reusable Rule Sets** Reusable Rules Address Groups Traffic Descriptors Protection Characteristics

Actions

No filter applied

Name Filter	Security protocol Filter	Description Filter
<input checked="" type="radio"/> TLSrs-production	TLS	TLS rule set for production traffic

Total: 1 Selected: 1

[Home](#) [Save](#)

We now have a rule set for TLS traffic. You use the same flow to create rule sets for the other security protocols, including no recognized protection.

You can create multiple rule sets for a security protocol.

The next step is to associate the rule sets to TCP/IP stacks.

Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- **Associating zERT rule sets to stacks in NCA and generating configuration**
- NCA reports to analyze your zERT configuration

The stack's rule sets panel

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > TCP/IP Stack

Reusable Rule Sets available to add to stack STACK1

Actions ▾

No filter applied

Name Filter	Security protocol Filter	Description Filter
<input checked="" type="checkbox"/> TLSrs-production	TLS	TLS rule set for production traffic
<input checked="" type="checkbox"/> NRP-production	NONE	No Recognized Protection rules for the production environment
<input type="checkbox"/> TLS-sandbox	TLS	TLS rule set for the test sandbox
<input type="checkbox"/> NRP-sandbox	NONE	No Recognized Protection rule set for the sandbox environment

Total: 4 Selected: 2

OK Cancel

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure: zERT ▾

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors

Actions ▾

No filter applied

System Group or Sysplex / System Image / Stack Filter	Type Filter	Status Filter
<input type="radio"/> Default	System Group	Complete
<input type="radio"/> PLEX	Sysplex	Complete
<input type="radio"/> IMAGE1	System Image	Complete
<input checked="" type="radio"/> STACK1	Stack	Incomplete
<input type="radio"/> IMAGE2	System Image	Complete
<input type="radio"/> STACK2	Stack	Incomplete
<input type="radio"/> IMAGE3	System Image	Complete
<input type="radio"/> STACK3	Stack	Incomplete

Properties...
Rule Sets...
Copy...
Delete
View Details

Total: 8 Selected: 1

Home Save

To add rule sets to a stack, you simply open its Rule Sets panel and select which reusable rule sets you want to associate with the stack.

Note that for each security protocol, only one rule set can be added to a stack, which is why the additional TLS and no recognized protection rule sets are greyed out in this example.

Actions menu can also be brought up by right-clicking on a table entry as shown here.

Installing the zERT policy

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure: zERT

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors

Actions

- Properties...
- Rule Sets...
- Copy...
- Delete
- View Details
- Add z/OS Group...
- Add z/OS System Image...
- Add TCP/IP Stack...
- Install All Files for This Group...
- Install Configuration Files...
- Hide Filter Row
- Expand All
- Collapse All

Image / Stack	Type	Status
IMAGE2	STACK2 - zERT Policy	Never installed
IMAGE1	STACK1 - zERT Policy	Never installed

Show Configuration File...

- Install...
- Configure Install...
- Install Multiple
- View Details
- History

Next slide

Network Configuration Assistant (Home) > zERT > Configuration Files > Configuration Files

List of Configuration Files for All System Images In Group PLEX

List of Configuration Files for All System Images In Group PLEX

Actions

System Image	Configuration Type	Status	Last Install	Configured File Name	Configured Host Name	Configured Installation Method
IMAGE2	STACK2 - zERT Policy	Never installed	Never	/etc/cfgasst/v2r2/PLEX/IMAGE2		Save to disk
IMAGE1	STACK1 - zERT Policy	Never installed	Never	/etc/cfgasst/v2r2/PLEX/IMAGE1		Save to disk

Total: 2 Selected: 1

Close

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure: zERT

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors

Actions

- Properties...
- Rule Sets...
- Copy...
- Delete
- View Details
- Add z/OS Group...
- Add z/OS System Image...
- Add TCP/IP Stack...
- Install All Files for This Group...
- Install Configuration Files...
- Hide Filter Row
- Expand All
- Collapse All

Image / Stack	Type	Status	Image	Stack	Policy
IMAGE3	System Image	Complete	N/A	V2R5	The credit card image
STACK3	Stack	Complete	Never installed	V2R5	The credit card stack
IMAGE3	System Image	Complete	N/A	V2R5	The test image
STACK3	Stack	Incomplete		V2R5	The test stack

Total: 8 Selected: 1

Home Save

Installation means generating the policy configuration file and placing it into the file system of a z/OS image to be read by policy agent.



The generated zERT policy configuration file (1/3)

zERTAction objects created by NCA for the actions that were selected in rules and rule sets

If you include a description of any object, NCA will include it in the configuration file as a comment

ConnectionDescriptor objects are created for the traffic descriptors that you used in rules.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Configuration Files > Configuration Files > Configuration File

Configuration File

Close Printable page

```
##
## ZERT Policy Agent Configuration file for:
##   Group:Image: PLEX.IMAGE1
##   Stack: STACK1
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 5
## Backing Store = MJF_ZPE
## Install History:
##
## End of Network Configuration Assistant information

zERTAction Allow_Silently
{
    LogSyslogd      No
    AuditRecord     No
    LogConsole      No
    ResetTCPConn    No
}

zERTAction Allow__Audit
{
    LogSyslogd      No
    AuditRecord     Yes
    LogConsole      No
    ResetTCPConn    No
}

zERTAction Allow__Audit__Console
{
    LogSyslogd      No
    AuditRecord     Yes
    LogConsole      Yes
    ResetTCPConn    No
}

## (VERIFY) IBM-supplied: TN3270 server with NEGTSURE enabled
ConnectionDescriptor TN3270-Server-NEGTSURE
{
    Protocol          TCP
    LocalPortRange    23
    RemotePortRange   1024-65535
    TCPConnectionDirection Inbound
}
```

The generated zERT policy configuration file (2/3)

Protection characteristics objects in the GUI result in corresponding objects generated in the configuration file.

GUI Protection Characteristic object type	Generated configuration object
Symmetric Encryption	ZERTSymmetricEncryption
Message Authentication	zERTMessageAuthentication
TLS key exchange	ZERTKeyExchange with TLSKeyEXchange Parameters
SSH key exchange	zERTKeyEXChange with SSHKeyExchange parameters

Network Configuration Assistant

Network Configuration Assistant (Home) › zERT › Configuration Files › Configuration Files › Configuration File

Configuration File

```
# Message authentication using SHA-192 or greater
ZERTMessageAuthentication      msgauth-SHA192
{
    MessageAuthentication      HMAC_SHA2_224
    MessageAuthentication      HMAC_SHA2_256
    MessageAuthentication      HMAC_SHA2_384
    MessageAuthentication      HMAC_SHA2_512
    MessageAuthentication      HMAC_SHA2_384_192
    MessageAuthentication      HMAC_SHA2_512_256
}

# Message authentication using SHA less than 192 bits
ZERTMessageAuthentication      msgauth-small-SHA
{
    MessageAuthentication      HMAC_SHA2_256_128
    MessageAuthentication      HMAC_SHA1_96
    MessageAuthentication      HMAC_SHA1
}

# Symmetric encryption using DES
ZERTSymmetricEncryption        symmcncr-DES
{
    SymmetricEncryption        DES
    SymmetricEncryption        DES_40
    SymmetricEncryption        3DES
}

# TLS key exchange algorithms using RSA
ZERTKeyExchange                tske-RSA
{
    TLSKeyExchange             RSA
    TLSKeyExchange             RSA_EXPORT
    TLSKeyExchange             RSA_PSK
}
```

Close Back to Top



The generated zERT policy configuration file (3/3)

NCA generates rules according to your rule sets.

The rules are generated with priority values that ensure they are evaluated in the order specified by your rule sets.

The catch-all rule is generated by NCA based on the catch-all action in your rule set.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Configuration Files > Configuration Files > Configuration File

Configuration File

```
# The general TLS rule for workloads
ZERTRule mygeneralrule
{
  Priority 499900
  SecurityProtocol TLS
  ZERTTLSProtocol
  {
    TLSProtocol TLSv1.2
    TLSProtocol TLSv1.3
  }
  ZERTKeyExchangeRef tlske-RSA
  ZERTMessageAuthenticationRef msgauth-SHA192
  ZERTSymmetricEncryptionRef symmcncr-AES
  zERTActionRef Allow_Silently
}

# Specific rule for Telnet traffic which is not fully up to date
ZERTRule Telnet-TLS-rule
{
  Priority 499800
  SecurityProtocol TLS
  LocalAddr ALL
  RemoteAddr ALL
  ConnectionDescriptorRef TN3270-Server
  ZERTTLSProtocol
  {
    TLSProtocol TLSv1.1
  }
  ZERTKeyExchangeRef tlske-RSA
  ZERTMessageAuthenticationRef msgauth-SHA192
  ZERTSymmetricEncryptionRef symmcncr-AES
  zERTActionRef Allow_Silently
}

# Catch-all action for the rule set TLSrs-production
ZERTRule TLSrs-production~catchall
{
  Priority 400000
  SecurityProtocol TLS
  zERTActionRef Allow___Audit___Console
}
```

Close Back to Top

Installing the generated zERT configuration file

Network Configuration Assistant (Home) > zERT > Configuration Files > Configuration Files

List of Configuration Files for All System Images In Group PLEX

Actions ▾

System Image	Configuration Type	Status	Last Install	Configured File Name	Config
<input type="radio"/> IMAGE2	STACK2 - zERT Policy	Never installed	Never	/etc/cfgasst/v2r2/PLEX/IMAGE2/...	
<input checked="" type="radio"/> IMAGE1	STACK1 - zERT Policy	Never installed	Never	/etc/cfgasst/v2r2/PLEX/IMAGE1/...	

Context menu for IMAGE1:

- Show Configuration File...
- Install...**
- Configure Install...
- Install Multiple
- View Details
- History

Total: 2 Selected: 1

Close

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > Configuration Files > Configuration Files > Install

Install File for PLEX.IMAGE1.STACK1

* Install file name:

/etc/cfgasst/v2r2/PLEX/IMAGE1/STACK1/zertPol

Installation method

☐ Save to disk

☒ FTP

FTP information

* Host name: host.example.com

* Port number: 21

User ID: admin ☒ Save User ID

* Password: ***** ☐ Save Password

☒ Use TLS/SSL
Guideline: If Application Transparent TLS (AT-TLS) is being used to protect FTP connections between this z/OSMF server and the target z/OS system, clear this check box.

☐ Create the directories if they do not exist

Data transfer mode

☒ Default ☐ Passive ☐ Active

☒ Propagate this FTP configuration to all files on this image

Comment for the configuration file prologue (optional)

Initial install of the file

Selecting the GO button may do an automatic save of backing store before the install, based on your preference setting.

Go **Close** View FTP Log

Installation for zERT policy configuration files works the same way it does for all other NCA technology perspectives.

Agenda

- Introduction to zERT Policy Enforcement and NCA
- zERT policy rules and object structure
- Creating basic zERT objects in NCA
- Creating zERT rules in NCA
- Creating zERT rule sets in NCA
- Associating zERT rule sets to stacks in NCA and generating configuration
- NCA reports to analyze your zERT configuration

Analysis reports available on NCA zERT objects

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors

Actions

No filter applied

Name Filter	Security protocol Filter	Description Filter
<input checked="" type="radio"/> TLSs-pr	TLS	TLS rule set fo
<input type="radio"/> NRP-proc	NONE	No Recognize
<input type="radio"/> TLS-sand	TLS	TLS rule set fo
<input type="radio"/> NRP-sank	NONE	No Recognize

View Details

Modify...

Copy...

Delete

Show Where Used

Add to Stacks

View Details provides a formatted, detailed report about an object in NCA zERT.

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT

V2R5 Current Backing Store is MJF_ZPE

Select a TCP/IP technology to configure : zERT

Systems Reusable Rule Sets Reusable Rules Address Groups Traffic Descriptors Protection C

Actions

No filter applied

Name Filter	First Few Addresses Filter	Description Filter
<input type="radio"/> agnest2	@agnost1, 10.4.1.6	An address group with two level:
<input type="radio"/> agnest1	@ag1, 10.3.1.1	An address group with one level
<input checked="" type="radio"/> ag1	10.1.1.1, 10.2.1.1	An address group of two address
<input type="radio"/> All_IPv		IBM supplied: All IPv4 address:
<input type="radio"/> All_IPv		IBM supplied: All IPv6 address:
<input type="radio"/> All_IP		IBM supplied: All IPv4 and IPv6 :

View Details

Modify...

Copy...

Delete

Show Where Used

Show Where Used provides a formatted report showing all the references to an object in NCA zERT.

View Details examples

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > View Details

View Details

Close Printable page

Address Group: agnest2 - An address group with two levels of nested addresses

Addresses	Nested Second Level	Nested Third Level
@ag1	@ag1	10.1.1.1
10.3.1.1	10.3.1.1	10.2.1.1
10.4.1.6	---	---

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > View Details

View Details

Close Printable page

Traffic Descriptor: complexTD - A complex traffic descriptor

Protocol	Local Port	Remote port	Connect Direction	Job Name	User ID	Discretionary TLS
TCP	100	All ephemeral ports	Inbound	JOB100	USER100	YES
TCP	200	All ephemeral ports	Either	JOB*	USER2*	NO
TCP	All ephemeral ports	30100-30200	Outbound	---	---	NO
TCP	All ephemeral ports	21	Outbound	---	FTPUSER	YES

Network Configuration Assistant

Network Configuration Assistant (Home) > zERT > View Details

View Details

Close Printable page

zERT Reusable Rule Set Summary

Rule Set Name	Security Protocol	General Rules	Specific Rules	Description
TLRSs-production	TLS	---	2	TLS rule set for production traffic

List of rules in reusable rule set: TLRSs-production

General Rule	n/a
Specific Rules (in order)	Telnet-TLS-rule TLS-partner-rule
Generated name for catch-all rule	TLRSs-production-catchall

Rule Set TLRSs-production Specific Rules

zERT Reusable Rule Information

Name	Security Protocol	Type	Local Data Endpoint	Remote Data Endpoint	Description
Telnet-TLS-rule	TLS	specific	All_IP_Addresses	All_IP_Addresses	Specific rule for Telnet traffic which is not fully up to date

Traffic Descriptors

Traffic Descriptor: TN3270-Server - (VERIFY) IBM supplied: TN3270 Server traffic

Protocol	Local Port	Remote port	Connect Direction	Job Name	User ID	Discretionary TLS
TCP	23	All ephemeral ports	Inbound	---	---	NO

Close Back to Top

As you can see from this Details example report for a rule set, when objects contain other objects, the contained objects are also expanded in the View Details report, so the report provides complete information.

Show Where Used examples

Show Where Used

Close

Printable page

Address Groups: ag1

Used in the following address groups:

Address Group	Description	Parent Address Group	Parent Address Group Description
agnest1	An address group with one level of nesting	agnest2	An address group with two levels of nesting

Used in the following Reusable Rules:

Reusable Rule	Security Protocol	Local Data Endpoint	Remote Data Endpoint	Description
TLS-partner-rule	TLS (SSLv2,SSLv3)	All_IP_Addresses	ag1	TLS rule for specific partner addresses

Reusable rules using this address group are used in the following stacks:

Group	Image	Stack	Security Protocol	Rule	Local Data Endpoint	Remote Data Endpoint	Rule Set
PLEX	IMAGE1	STACK1	TLS (SSLv2,SSLv3)	TLS-partner-rule	All_IP_Addresses	ag1	TLSrs-

Show Where Used

Close

Printable page

Protection Characteristic: msgauth-SHA192

Used in the following reusable rules:

Reusable Rule	Security Protocol	Traffic Descriptor	Protection Characteristics	Description
mygeneralrule	TLS (TLSv1.2, TLSv1.3)	n/a	tlske-RSA, msgauth-SHA192, symmencr-AES	The general TLS rule for workloads
Telnet-TLS-rule	TLS (TLSv1.1)	TN3270-Server	tlske-RSA, msgauth-SHA192, symmencr-AES	Specific rule for Telnet traffic which is not fully up to date
TLS-file-transfer	TLS (TLSv1.1)	FTP-Server, Connect-Direct-Server	msgauth-SHA192, symmencr-DES, symmencr-AES	TLS rule for file transfer workloads

Reusable rules using this protection characteristic are used in the following stacks:

Group	Image	Stack	Security Protocol	Rule	Traffic Descriptor	Protection Characteristics	Rule Set
PLEX	IMAGE1	STACK1	TLS (TLSv1.1)	Telnet-TLS-rule	TN3270-Server	tlske-RSA, msgauth-SHA192, symmencr-AES	TLSrs-production
PLEX	IMAGE2	STACK2	TLS (TLSv1.1)	Telnet-TLS-rule	TN3270-Server	tlske-RSA, msgauth-SHA192, symmencr-AES	TLS-sandbox

Show Where Used

Close

Printable page

Reusable Rule: Telnet-TLS-rule

Included in the following reusable rule sets and stacks

Rule Set	Rule Set description	Included in Stacks
TLSrs-production	TLS rule set for production traffic	PLEX.IMAGE1.STACK1
TLS-sandbox	TLS rule set for the test sandbox	PLEX.IMAGE2.STACK2

z/OS Encryption Readiness Technology

Scan the QR code to visit
z/OS Communications Server
product page on IBM Community.



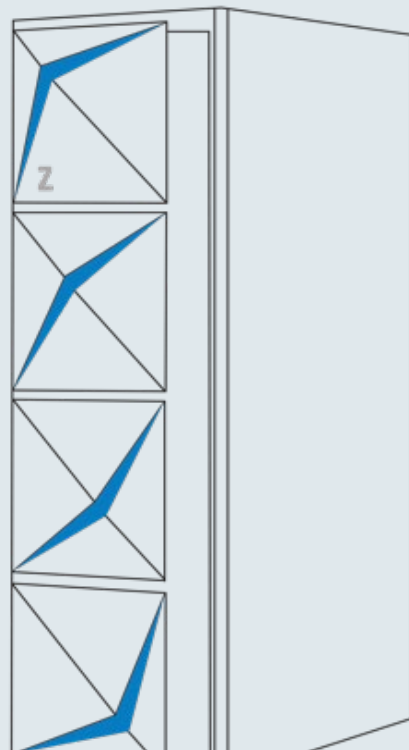
zERT policy-based enforcement – *new in z/OS V2R5*

- Enforce local network encryption standards for TCP traffic in real time.
- Policy-based rules you build in the Network Configuration Assistant describe acceptable or unacceptable levels of cryptographic protection along with the actions to take when TCP connections match those rules.

What are users saying about zERT?

- “Once we communicated to our business what we're doing with zERT, they wanted to be able to do it across all our platforms!”
- “We use zERT data for compliance checks.”
- “zERT has given us the upper hand in monitoring mainframe connection security.”

 Visit *Things you should know about zERT* on IBM Community and discover blogs, product documentation, videos, event information, webinar, and presentations about zERT.



Digital Badges & Online Courses



Networking on z/OS - Foundations

- **IBM Open Badge:**
<https://ibm.biz/zosnetworkingbadge>
- **Online course:**
<https://ibm.biz/zosnetworkingcourse>

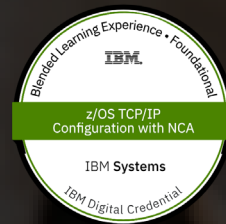
Foundational understanding of networking on z/OS.



z/OS Network Security - Foundations

- **IBM Open Badge:**
<http://ibm.biz/zosnetsecuritybadge>
- **Online course:**
<http://ibm.biz/zosnetsecuritycourse>

Knowledge and foundational understanding of z/OS network security.



z/OS TCP/IP Configuration with NCA

- **IBM Open Badge:**
<http://ibm.biz/NCABadge>
- **Online course:**
<http://ibm.biz/NCATCIPcourse>

Use the NCA to create and manage TCP/IP profiles.

Join z/OS Comm Server
on **IBM Community** !



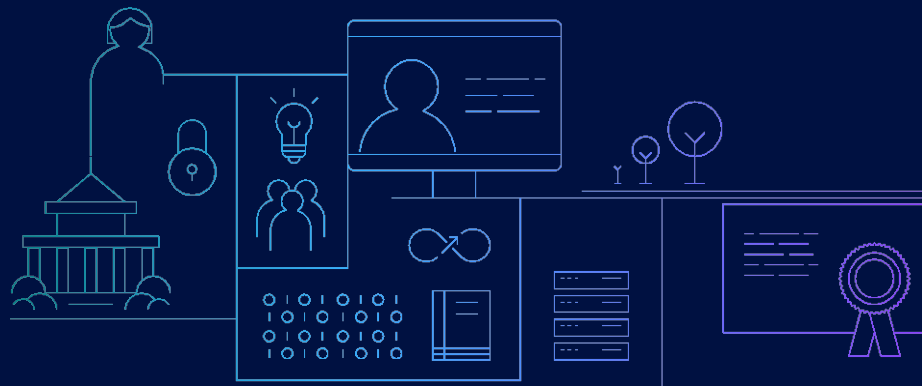
<https://ibm.biz/cscommunity>

Rich and up-to-date technical content, including blogs, videos, and events.



Thank you

Mike Fox
Senior Software Architect, IBM Enterprise Networking Solutions
mjfox@us.ibm.com





Notices and disclaimers

© 2021 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed “as is” without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.**

IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.

IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply.”

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.

- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- 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.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.



Notices and disclaimers

- 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 about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml

