z/OS Encryption Readiness Technology (zERT) Goes Live!

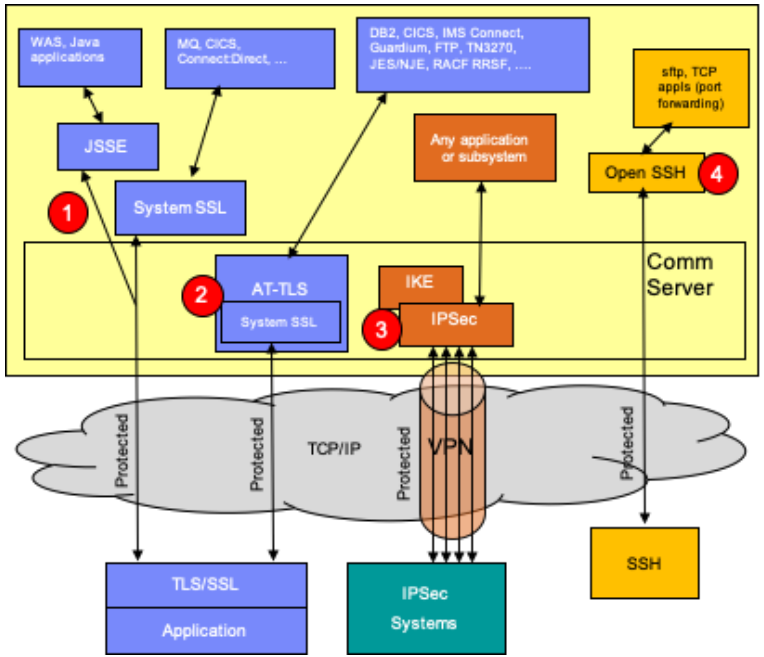
—
Navya Ramanjulu (navyaram@us.ibm.com)
IBM

Agenda

1	zERT background
2	zERT policy-based enforcement
3	Summary

zERT background

TCP/IP cryptographic protection on z/OS



z/OS provides 4* mechanisms to protect TCP/IP traffic:

1. **TLS/SSL direct usage – TCP only**
   - Application is explicitly coded to use these
   - Per-session protection
   - Configuration and auditing is unique to each application

2. **Application Transparent TLS (AT-TLS) – TCP only**
   - Configured in AT-TLS policy via Network Configuration Assistant
   - Typically, transparent to application
   - TCP/IP stack is user of System SSL services
   - Auditing via SMF 119 records

   (Can also have 3rd party TLS implementations like OpenSSL)

3. **Virtual Private Networks using IPSec and IKE – IP (any traffic)**
   - "Platform to platform" encryption
   - Configured in IPSec policy via Network Configuration Assistant
   - Completely transparent to application
   - IKE negotiates IPSec tunnels dynamically
   - Auditing via SMF 119 records at tunnel level only

4. **Secure Shell using z/OS OpenSSH – TCP only**
   - Configured in SSH configuration file and on command line
   - Auditing via SMF 119 records

* z/OS also provides Kerberos support, but that is focused mainly on peer authentication

z/OS Encryption Readiness Technology (1 of 4)

With all this complexity, how can you tell…

- Which traffic is being protected? Which is not?
- How is the traffic being protected?
- Who does the traffic belong to?
- Do existing and new configurations adhere to your company's security policies?

zERT is designed specifically to answer the above questions

z/OS Encryption Readiness Technology (2 of 4)

zERT positions the **TCP/IP stack** as a central collection point of cryptographic protection attributes for:

- **TCP** connections that are protected by TLS, SSL, SSH, IPsec or are unprotected*
- **Enterprise Extender** connections that are protected by IPsec or are unprotected*

Two methods for discovering the security sessions and their attributes:

- **Stream observation** (for TLS, SSL and SSH) – the TCP/IP stack observes the protocol handshakes as they flow over the TCP connection
- **Advisory observation** by the cryptographic protocol provider (System SSL, ZERTJSSE provider, OpenSSH, z/OS IPsec support)

Reported through **SMF 119 records** via:

- SMF and/or
- Real-time network management interfaces (NMIs)

unprotected* = no protection that zERT recognizes

z/OS Encryption Readiness Technology (3 of 4)

zERT Discovery

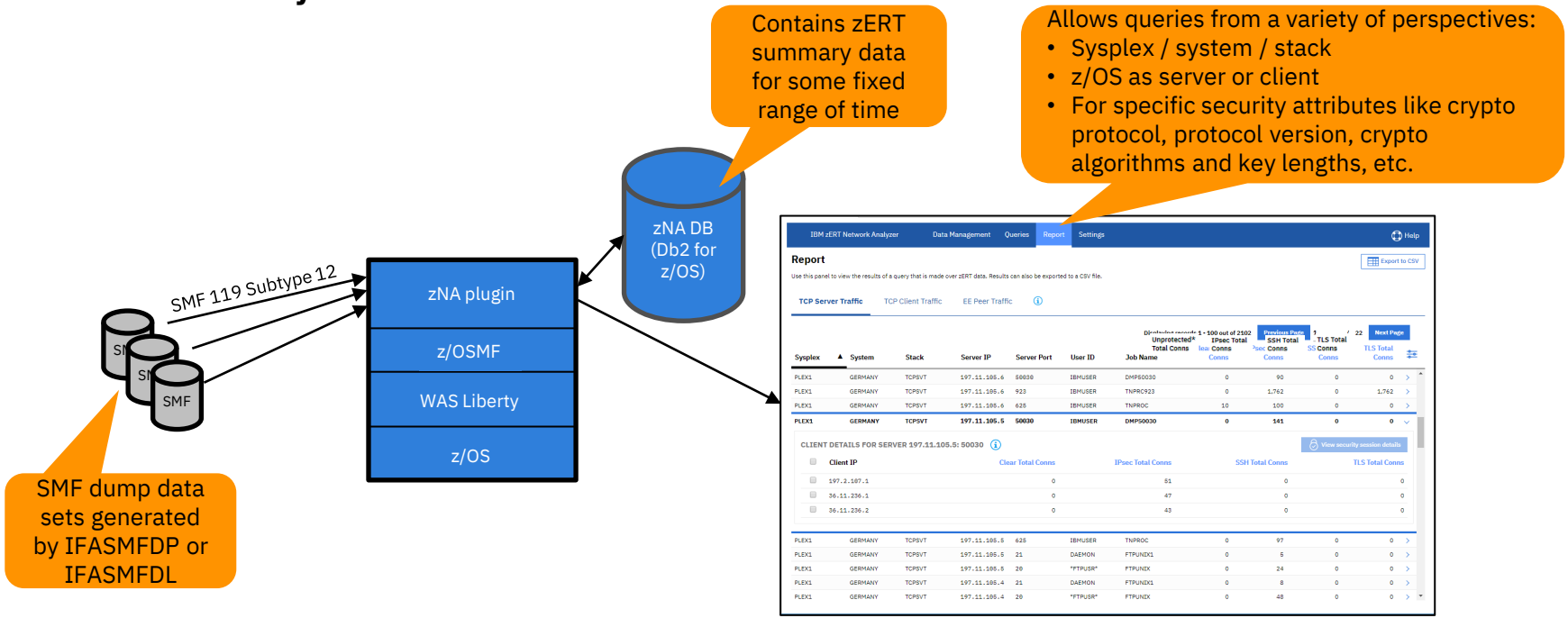
- SMF 119 subtype 11 "**zERT Connection Detail**" records
- Describe the cryptographic protection history of each TCP and EE connection
- At least one record per connection
- Depending on your z/OS network traffic, these could be generated in very high volumes
- Well suited for real-time monitoring applications

zERT Aggregation

- SMF 119 subtype 12 "**zERT Summary**" records
- Describe the repeated use of security sessions over time
- One record per recording interval for each security session active during the interval
- Greatly reduces the volume of SMF records while providing the same level of cryptographic detail
- Well suited for reporting and analysis

z/OS Encryption Readiness Technology (4 of 4)

zERT Network Analyzer



- Web UI makes zERT data consumable for z/OS network security administrators
- Comes with z/OS Communications Server at no extra cost but relies on Db2 for z/OS 11 or 12
- Used primarily to investigate specific network encryption questions and periodic report generation

What data does zERT collect and record?

Significant attributes (subtype 11 and 12)
- Identifying attributes like IP addresses, ports, jobname, userid, etc.
- Protection attributes like protocol version, cryptographic algorithms, key lengths, etc.
  - Changes in these cause a protection state change record to be written if they change

Informational attributes (subtype 11 only)
- Protocol session identifiers, session or certificate expiry data, certificate serial numbers
- Changes in these attributes do not affect the strength of the cryptographic protection

zERT does not collect, store or record the values of secret keys, initialization vectors, or any other secret values that are negotiated or derived during session establishment.

zERT monitors the cryptographic protection attributes of all TCP and EE connections that terminate on the local z/OS TCP/IP stack.

See the z/OS Communications Server IP Programmer's Guide for all the details

Configuring zERT in the TCP/IP profile (1 of 2)

```
                        .--NOZERT-----------------------------.
>>-GLOBALCONFig-------+-------------------------------------+-----<<
                      |        .--NOAGGregation-------------.  |
                      '--ZERT--+-----------------------------+--'
                               '--AGGregation---[agg-parms]-'

agg-subparms:  INTVAL SMF | interval [SYNCVAL hh:mm ]

INTVAL is the recording interval:
   SMF - uses system's SMF interval (default)
   interval is a specific interval in hours (1-24)
   SYNCVAL hh:mm - specifies the time of day from which INTVAL is calculated
                   (default 00:00)
```

Specifying a non-SMF recording interval reduces the number of SMF 119-12 records written.

Configuring zERT in the TCP/IP profile (2 of 2)

zERT in-memory collection enabled independently of destinations to which records are written.

SMFCONFIG controls writing of zERT records to System Management Facility.

- `SMFCONFIG TYPE119 ZERTDetail | NOZERTDetail (Default is NOZERTDetail)`
- `SMFCONFIG TYPE119 ZERTSUMmary | NOZERTSUMmary (Default is NOZERTSummary)`

NETMONITOR controls writing of zERT records to real-time network monitoring services.

- `NETMONITOR ZERTService | NOZERTService (Default is NOZERTService)`
- `NETMONITOR ZERTSUMmary | NOZERTSUMmary (Default is NOZERTSummary)`

Verification (NETSTAT CONFIG and DISPLAY TCPIP commands)

All parameters can be dynamically enabled or disabled

Can be configured through the Network Configuration Assistant

zERT support in other products (as of July, 2020)

IBM is aware of the following products that have shipped support for zERT data. Note that this **should not be considered to be a comprehensive list** as there may be others of which IBM is currently unaware:

- IBM zSecure Audit V2.3 (subtype 11 and subtype 12 records)
- IBM QRadar SIEM (supports what zSecure feeds it)
- Merrill Technologies MXG (feeds subtype 11 and subtype 12 records into SAS)
- Broadcom NetMaster Network Management for TCP/IP 12.2.03 (subtype 11 records through NMI)
- BMC Mainview for IP 3.6 (subtype 11 and subtype 12 records through NMI)
- Vanguard Advisor 2.3 (subtype 11 records)
- IntelliMagic Vision (subtype 12 records)
- IBM Z Common Data Provider 2.1.0 (subtype 11 and 12 records)
- IBM NetView Version 6.3 (supports subtype 11 records through NMI)
- IBM Omegamon for Networks on z/OS version 550, fixpack 4 (APAR OA57939 - subtype 11 records through NMI)
- Pacific Systems Group's Spectrum SMF Writer (subtype 11 and 12 records)
- IBM Z Performance and Capacity Analytics V3.1.0 with APAR PH12196 (subtype 11 and 12 records)

zERT limitations

- Connection protected by cryptographic protocols NOT recognized by zERT – reported as **no recognized cryptographic protection**
- Connections protected by cryptographic protocol providers that are NOT enabled for zERT:
  - zERT collects limited information using TCP stream observation only
  - Any attributes determined through encrypted flows are not seen
  - Any changes to the protection attributes of such a security session after it begins cryptographically protecting the connection are not seen
  - Certificate-related attributes are not collected due to avoid significant performance impact
  - Some other specific attributes may not be available
- Connections that
  - initiate TLS protection after application data has flowed will not be recognized as having TLS protection
  - terminate in zCX containers are routed traffic - not monitored by zERT
- zERT monitors TCP and EE connections that terminate on the local TCP/IP stack

See the z/OS Communications Server IP Configuration Guide for a complete list of limitations

zERT policy-based enforcement

Statement of direction

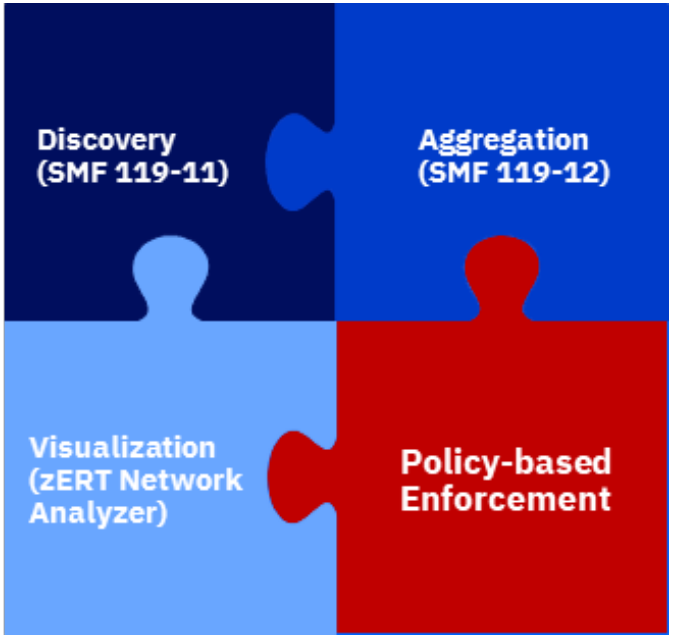
zERT policy-based enforcement

In the future, IBM intends to extend zERT to support policy-based rules that describe different levels of cryptographic protection along with optional actions to take when TCP connections match those rules. Since z/OS V2.3, zERT has provided a detailed view of the cryptographic protection attributes used on connections that terminate on the z/OS TCP/IP stack. The zERT policy-based enforcement feature would enable immediate notification through messages, auditing through SMF records, and even automatic connection termination when questionable or unacceptable cryptographic protection is used. IBM plans to enable z/OS network security administrators to create and manage zERT enforcement rules and actions through the z/OSMF Network Configuration Assistant and the z/OS Communications Server policy agent.

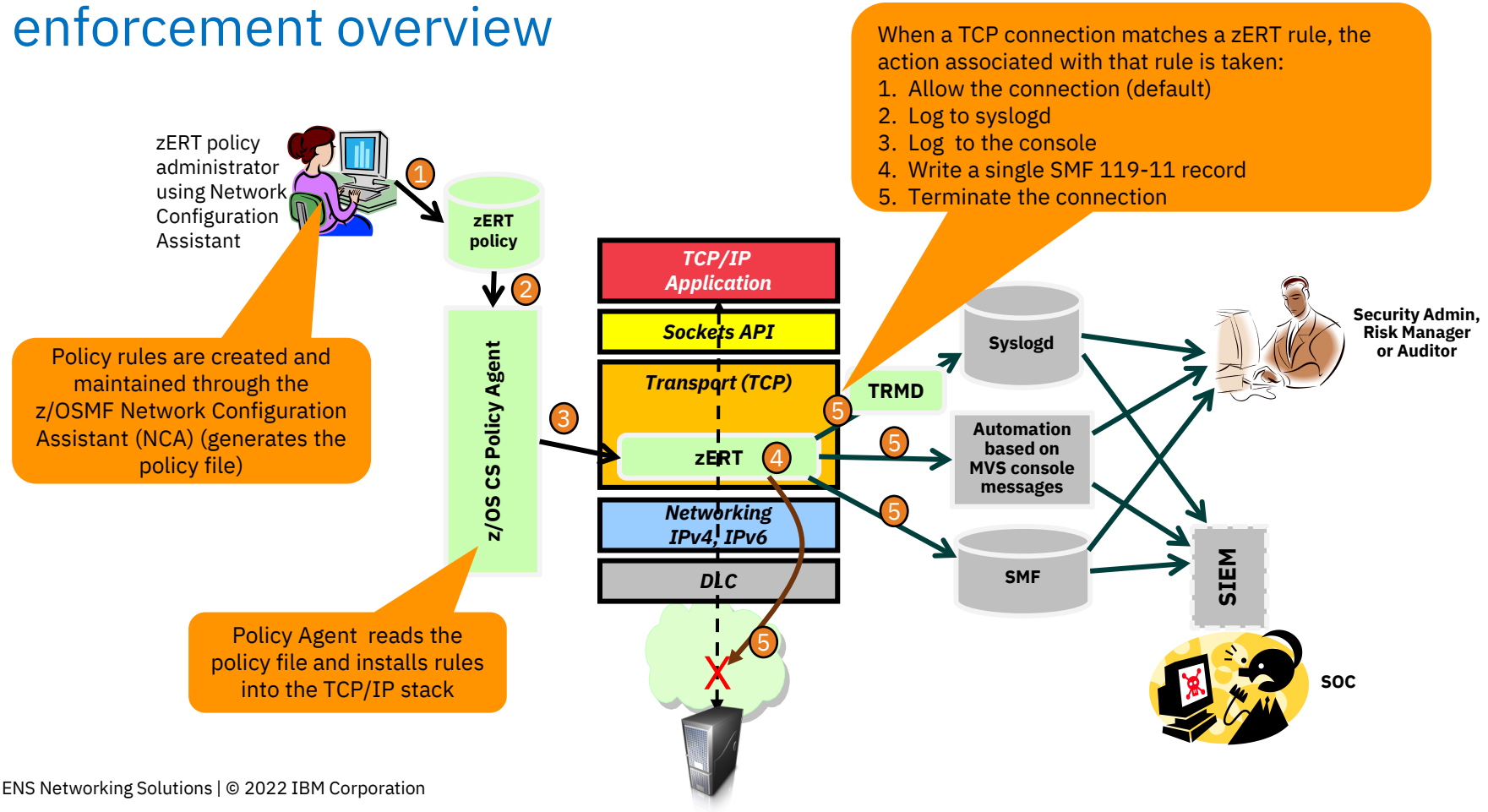
zERT policy-based enforcement

Directs the TCP/IP stack to take specific actions when a user-defined security policy is met for a new TCP connection

- **Rule conditions** describe traffic along with acceptable or unacceptable protection attributes
- **Rule actions** determine what happens when a connection matches the rule conditions
- zERT enforcement only monitors TCP connections – it does not monitor EE
- New technology implemented through Policy Agent and Network Configuration Assistant (NCA)



zERT policy-based enforcement overview



zERT enforcement rules

Up to four separate “sets” of ZERT rules:

- TLS/SSL - IPsec - SSH - No recognized protection (NONE)

Each TCP connection is evaluated against each rule set based on the security protocol(s) used to protect it

General rule

A single rule to describe the generally accepted levels of protection for the specified security protocol

- Protocol versions
- Encryption algorithms
- Message integrity algorithms

Typical Action:

- Allow Silently

One or more specific rules

Exceptions for cases that are known (and allowed) to use cryptographic protection of lesser strength than is generally accepted OR cases using prohibited protection that needs to be flagged or blocked

Example of allowed exception:

- Allow connections from known back-level clients

Example of prohibited exception:

- Reset connections that use a prohibited protocol and log to console (on which automation can trigger)

Catch-all rule

Catches any traffic that uses the specified security protocol and does not match the general rule or any of the specific rules

Typical Action(s):

- Log to syslogd and/or SMF 119-11 record that can be consumed in real-time if need be

zERT enforcement rules: General points

A connection is evaluated against the zERT rules per security protocol(s) used to protect that connection
- One connection can match multiple rules (one per protocol)
- If a connection does not match any rule, it is allowed (implicit “allow all” rule)
- Specific events drive evaluation or re-evaluation of a connection against a given rule set

NCA guides you in the creation of these rule sets
- “general”, ”specific” and “catch-all” rules is Network Configuration Assistant terminology
- Generated policy agent zERT rules have no such categorization
- Simply constructed in a fashion that accomplishes the stated purpose – prioritized order

zERT enforcement rules: Conditions

A zERT rule can be defined with the following conditions:

- **Connection attributes** (specific rules only)
  - Local, remote IP addresses and ports
  - Jobname
  - z/OS user ID (that opened the socket)
  - Connection direction
  - TCP protocol only
- **Protection attributes**:
  - Security protocol (TLS/SSL, IPsec, SSH, No Recognized Protection)
  - Protocol version (for TLS/SSL and SSH)
  - Symmetric encryption algorithms (including key lengths)
  - Message authentication/integrity algorithms (including key lengths)
  - Key exchange algorithms
  - In V2R5, zERT enforcement will NOT include digital signature algorithms or key lengths

zERT enforcement rules: Actions

- Allow the TCP connection (default action)
- Reset TCP connection
- Reporting actions:
  - Log to syslogd
  - Log to console (TCPIP job log)
  - Write an SMF 119-11 “zERT Detail” record to SMF and/or NMI (provides full audit trail)
- Logging, audit and reset actions can be specified in any combination

zERT enforcement action: Logging actions

LogSyslogd – log a message about the connection to the syslog daemon
- Requires traffic regulation manager daemon (TRMD) to be started
- Written to syslogd facility local5

LogLevel *n* - Defines the syslogd priority for logging zERT messages to the syslog daemon
- 0 – Emergency/Panic
- 1 – Alert
- 2 – Critical
- 3 – Error
- 4 – Warning. This is the default
- 5 – Notice
- 6 – Information
- 7 – Debug

LogConsole – log a message about the connection to the console (TCP/IP job log)
- Multi-line, WTO message
- Allows for automation

zERT enforcement action: Logging to syslogd

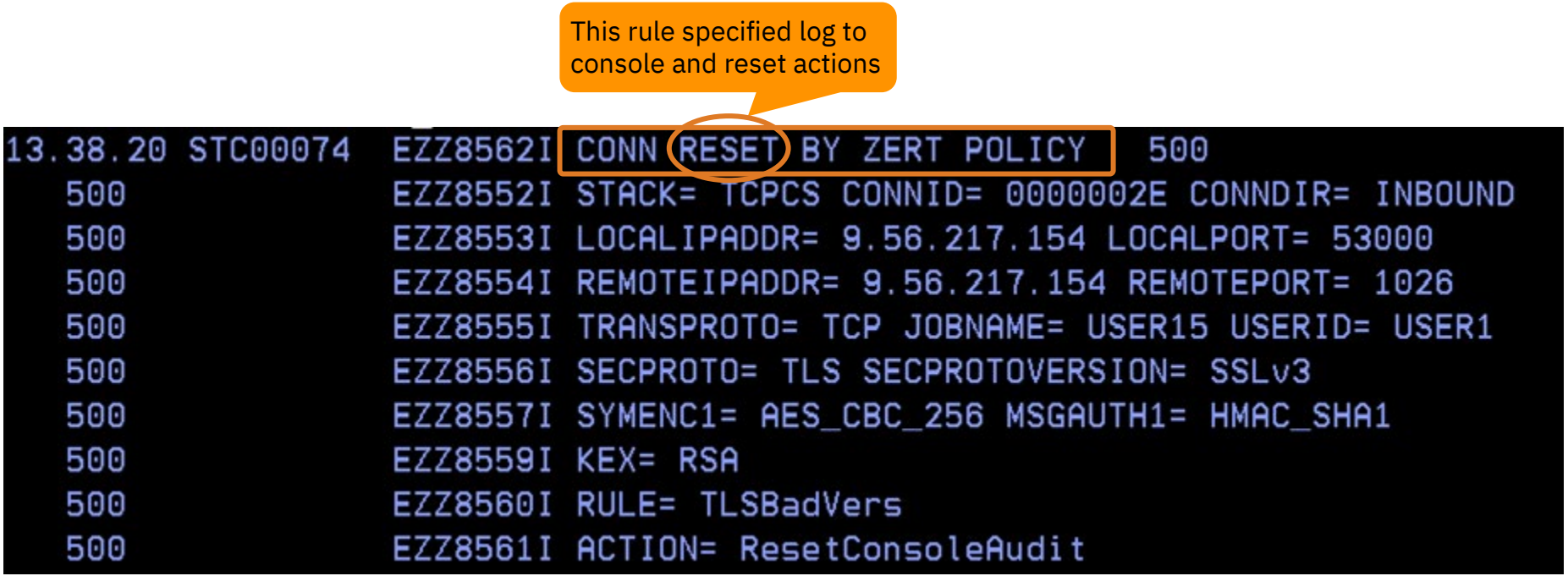
This rule specified log to syslogd action but not the reset action

```
May 18 12:33:49 MVS312/IBMUSER  TRMD1    TRMD.TCPCS[55]:
EZZ8583I Connection logged by ZERT Policy Enforcement:
05/18/2021 15:33:49.28 connid= 000000DB localipaddr= 10.56.217.154 localport=
1046 remoteipaddr= 10.56.217.154 remoteport= 53000 transproto= TCP jobname=
USER15 userid= USER1 conndir= Outbound secproto= TLS secprotoversion= TLSv1.0
symenc1= AES_CBC_256 symenc2= N/A msgauth1= HMAC_SHA1 msgauth2= N/A kex= RSA
rule= TLSCatchAll action= LogAudit
```

```
EZZ8584I Connection reset by ZERT Policy Enforcement:
```

This rule specified log to syslogd and reset actions

zERT enforcement action: Logging to console



zERT enforcement action: Log flood prevention (for both syslogd and console messages)

- Messages are suppressed if:
  - The same rule has been matched 10 times within a 5-minute interval
  - 100 messages have been logged across all rules within a 5-minute interval
- At least one message will be logged for each unique rule that is matched within the 5-minute interval
- For a complete record of every rule match, use the Audit action

```
May 18 12:40:19 MVS312/IBMUSER  TRMD1    TRMD.TCPCS[55]:
EZZ8585I ZERT Log suppressed: 05/18/2021 15:33:49.28 count= 13 reset=No rule=
TLSCatchAll

May 18 12:40:19 MVS312/IBMUSER  TRMD1    TRMD.TCPCS[55]:
EZZ8583I Connection logged by ZERT Policy Enforcement:
05/18/2021 15:40:10.34 connid= 0000013D localipaddr= 9.56.217.154 localport= 1073
remoteipaddr= 9.56.217.154 remoteport= 53000 transproto= TCP jobname= USER15
userid= USER1 conndir= Outbound secproto= TLS secprotoversion= TLSv1.0 symenc1=
AES_CBC_256 symenc2= N/A msgauth1= HMAC_SHA1 msgauth2= N/A kex= RSA rule=
TLSCatchAll action= LogAudit
```

Suppression message is written when suppression interval expires, and the next logged event occurs

zERT enforcement action: Audit record

AuditRecord - Writes a SMF 119 subtype 11 record
- A new event type “zERT Enforcement” (x'07’)
- New zERT policy-based enforcement section with the matching policy rule name

For audit records to be written to System Management Facility (SMF)
- AuditRecord Yes in zERT policy rule
- `SMFCONFIG TYPE119 ZERTDETAILBYPOLICY` in the TCP/IP profile

For audit records to be written to Real-time zERT Detail SMF NMI service SYSTCPER
- AuditRecord Yes in zERT policy rule
- `NETMONITOR ZERTSERVICEBYPOLICY` in the TCP/IP profile

zERT enforcement action: Auditing to SMF

```
    4 MVS312   ZERT     0077000B 13:43:42.050000 Zert Connection Details
SMF 119 Header:     Length..      650  Flags...       5E
 Type.... 119       Date.... 121.131   Time.... 13:43:42.05                SysID... 3090      SSysID.. STC
 SubType. 11        Zert Detail        TRN..... 8
************************************************
Identification:
 SysName. MVS312    SysplexN LOCAL     Stack... TCPCS     Release. 020500    Comp.... STACK
 ASName.. TCPCS     UserId.. USER1     Asid.... 4E        Reason.. Event complete              RcdID... 0
Connection Identification Section:
 EventType. ENFORCEMENT  SecProtos. (TLS) SAFlags.  1000000
 IPSecFlg. ()
 IPProto. TCP       JobName. USER16    JobID... STC00047  UserID.. USER1
 STime... 17:43:42.03  SDate... 121.131
 ETime... 00:00:00.00  EDate... 0.000
 RIP..... 9.56.217.154    RPort... 1027
 LIP..... 9.56.217.154    LPort... 53000
 ConnID.. 00000051
 InBytes. 0            OutBytes. 0
 InSegDG. 8            OutSegDG. 7
TLS Protocol Section:
 ProtoVer. TLSv1.0              Source. OBSERVATION
 HSType. FULL_HS                HSRole. SERVER
```

Event type 7

Displayed by a homegrown formatting program – NOT a product display

```
zERT Policy Enforcement (ZPE) Section:
  IPSec Policy Rule Name..
  TLS Policy Rule Name.... TLSPort53000
  SSH Policy Rule Name....
  No Recognized Policy Rule Name..
```

zERT enforcement action: Auditing failures

Messages logged to the console when zERT enforcement policies are installed in the TCP/IP stack.

When zERT discovery not enabled and at least one zERT policy exists

```
EZZ8564I ZERT POLICY WILL BE NOT ENFORCED FOR tcpname BECAUSE ZERT FUNCTION
IS NOT ENABLED
```

When ZERTDETAILBYPOLICY and ZERTSERVICEBYPOLICY not specified and at least one ZERT policy has AuditRecord action

```
EZZ8565I NO AUDIT RECORD WILL BE WRITTEN BY ZERT POLICY ENFORCEMENT FOR
tcpname - ZERTDETAILBYPOLICY AND ZERTSERVICEBYPOLICY NOT ENABLED
```

zERT enforcement action: Reset connection

A connection is reset when

- The TCP three-way handshake is complete, and connection is in established state
- zERT has determined the security protocol being used or no recognized protection
  - IPsec protection is determined before TLS/SSH protection is observed
- The connection is mapped to a rule with that security protocol and reset action is specified

Recommendation: specify a log action to get a message when a connection is reset

zERT enforcement action: Reset connection

zERT connection detail record (SMF 119 subtype 11)

Offset	Name	Length	Format	Description
2(X'2')	SMF119SC_SAFlags	1	Binary	Flags: • X'20': Connection reset by zERT policy-based enforcement o Can only be set when event type (SMF119SC_SAEvent_Type) is connection termination or short connection termination o otherwise, 0

TCP connection termination record (SMF 119 subtype 2)

Offset	Name	Length	Format	Description
14(X'E')	SMF119AP_TTTermCode	1	Binary	• Reason code for termination: • X'77': The connection was reset by zERT policy-based enforcement reset action

zERT enforcement: Netstat ALL/-A report

```
Client Name: TCPCS                      Client Id: 0000000C
Local Socket: 9.67.115.5..23            Foreign Socket: 9.27.11.182..4665
BytesIn:             0000001062         BytesOut:            0000000480
SegmentsIn:          0000000019         SegmentsOut:         0000000019
…
…
QOSPolicy:           Yes
  QOSRuleName:       QosRule1
TTLSPolicy:          Yes
  TTLSRule:          TTLSRule1
  TTLSGrpAction:     TTLSGrpAction1
  TTLSEnvAction:     TTLSEnvAction1
  TTLSConnAction:    TTLSConnAction1 (Stale)
RoutingPolicy:       Yes
  RoutingTableName:  prTabl
  RoutingRuleName:   SecLow2
ZERTPolicy:          Yes
  ZERTIPSecRule:     zert_ipsecr1
  ZERTIPSecAction:   zert_ipseca1
  ZERTTLSRule:       zert_tlsr1
  ZERTTLSAction:     zert_tlsa1
```

Displays zERT enforcement policy rule(s) matched by the connection

In summary

zERT Discovery:
- SMF 119 Connection Detail (subtype 11) records
- Per-connection
- Well-suited for real-time monitoring applications

zERT Aggregation:
- SMF 119 Summary (subtype 12) records
- Same level of cryptographic detail in fewer SMF records
- Well suited to historical reporting applications

zERT Network Analyzer:
- Easy UI for z/OS network security admins to query and search zERT data
- Granular queries can be built for regular compliance checks or for special purpose investigations
- Query results can be viewed through a browser or exported

zERT policy-based enforcement:
- Policy rules configured through NCA and installed through Policy Agent
- Provides real-time monitoring, auditing and even defensive actions based on zERT data

z/OS Encryption Readiness Technology

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

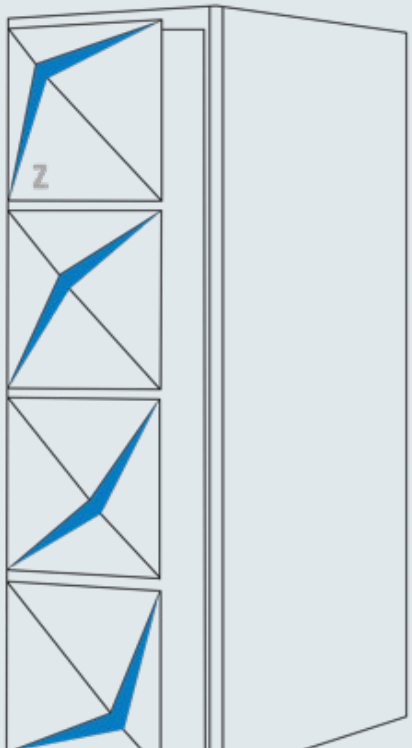
zERT policy-based enforcement – *new in z/OS V2R5*

- 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 the 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/NCATCPIPcourse

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

Navya Ramanjulu
zERT Goes Live!
navyaram@us.ibm.com

Notices and disclaimers

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