Swiss Re

zERT Policy Enforcement

GSE Kartause Ittingen – Marco Egli

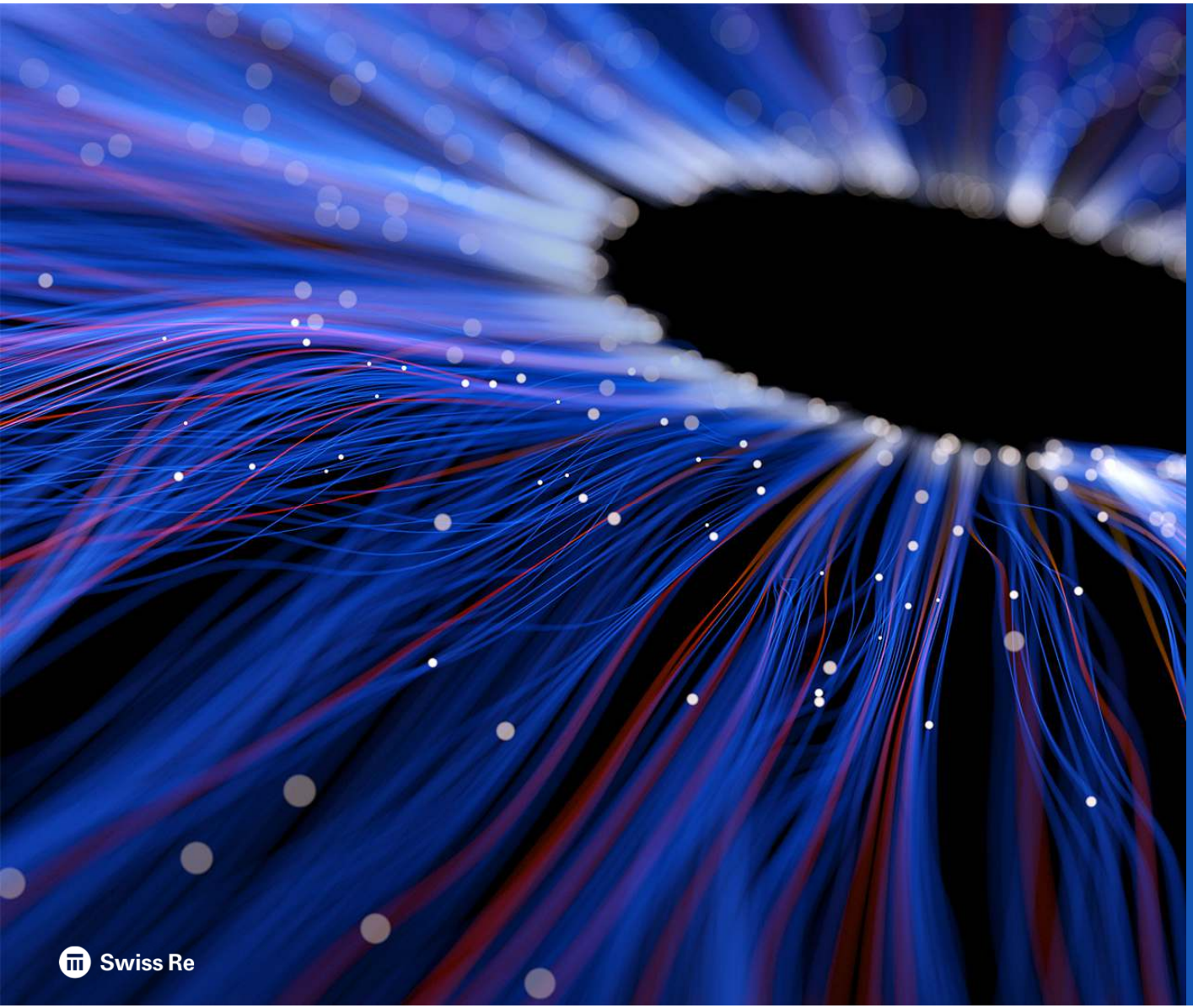


Table of Contents

Swiss Re

What is zERT Policy Enforcement?

- zERT policy-based enforcement, the TCP/IP stack uses the cryptographic protection attributes observed by zERT discovery to enforce policy rules that you create based on your local network security requirements.
- For questionable or unacceptable protection, actions such as notification through messages, auditing through SMF records, and even dropping the connection can be configured.
- Managing and enforcing security requirements for TCP (IPsec, TLS, SSH)

zERT discovery Vs. zERT Policy Enforcement

- zERT discovery
  - Collect cryptographic attributes in two ways
    - Notification by Cryptographic Protocol Providers (CCP) enabled for zERT
    - Observational discovery of the TCP stream passing the TCP/IP stack for TLS, SSL and SSH handshake
  - Writes SMF 119(12) that can be processed by the zOSMF zERT Network Analyzer
  - Do not execute actions on connections, only log them into SMF

- zERT Policy Enforcement
  - Writes SMF 119(11) record
  - Supports IPsec, TLS and SSH but not EE
  - Connection can match more than one rule
  - Execute action(s) on connection
    - Log a message through syslogd
    - Log a message to the console (TCPIP Joblog)
    - Write audit record SMF 119(11) event 7
    - Reset the connection
    - Allow the connection with no logging

Technical Requirements for zERT Policy Enforcement

```
;*******************************************************************
; NETMONITOR Parameters                                            *
;*******************************************************************

GlobalConfig
  ZERT Aggregation

;*******************************************************************
; NETMONITOR Parameters                                            *
;*******************************************************************

Netmonitor
  ZERTService
  ZERTServiceByPolicy

;*******************************************************************
; SMF  Configuration Parameters                                    *
;*******************************************************************

SMFConfig
   Type119 ZERTDetail
           ZERTDetailByPolicy
           ZERTSummary
```

Disclaimer: Only zERT details shown in TCP/IP Profile, other data intentionally removed

zERT Discovery
GlobalConfig ZERT
(Aggregeation optional)

Policy Agent (PAGENT)
STC must be up and running to handle zERT Policy

SMF Record 119 recording
SMF Parmlib member

Enable ByPolicy
Netmonitor ZERTServiceByPolicy
SMFConfig Type119 ZERTDetailByPolicy

Traffic Regulation Manager Daemon (TRMD)
Only required if the zERT Policy must execute actions (reset)

zOS 2.5
With new function APAR PH35304

Additional Requirements

01 **Knowledge about Protocol and Crypto requirements from internal/external Standards**
Fulfil compliance requirements

02 **Knowledge what network consumers are currently accessing the stack**
Enablement to define the rules for all consumers

03 **zOSMF Configuration Assistant**
Define the rules and create the policy

04 **Syslog Daemon**
Required if message logging with syslogd as a destination is selected

05 **Concept/Plan about implementation**
Create a plan based on zERT Discovery

06 **Naming Concept**
Plan ahead the expected naming conventions for all the rules and protection characteristics

How does it work?

01
Define a Policy

There can be one zERT Policy defined per Policy Agent. The policy consists of many rules.

02
Activate the Policy

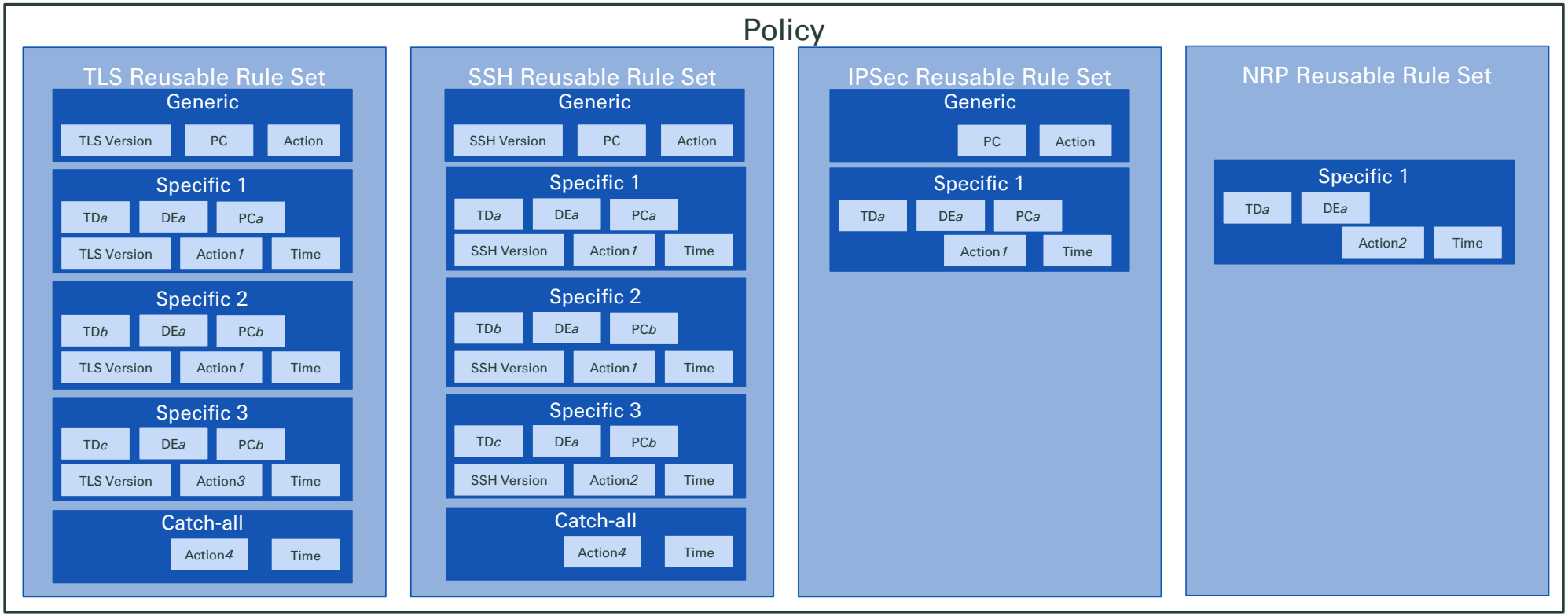
Install the policy into the policy agents directory and refresh the started task with the modify command.

03
Verify results

Use zSecure Events (EV) panel to work with I (IP) addresses and specifically with 'Further IP selection' to work on zERT SMF Data or via the preferred/selected logging option as defined in the actions for the rules. Other tools are also available.

Conclusion:
Good preparation is essential to create meaningful results and to avoid analysing millions of records

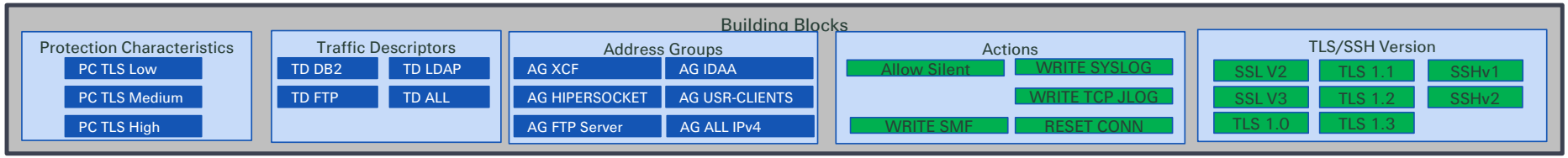
Define a Policy – What is a Policy?

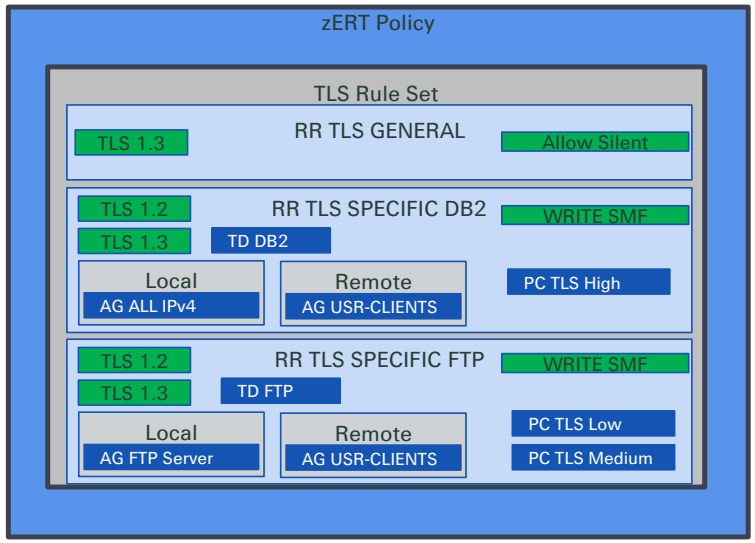


PC: Protection Characteristics
TD: Traffic Descriptor
AG: Address Groups

RR: Reusable Rules
RRS: Reusable Rule Sets
DE: Data Endpoint

Define a Policy – Building Blocks





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

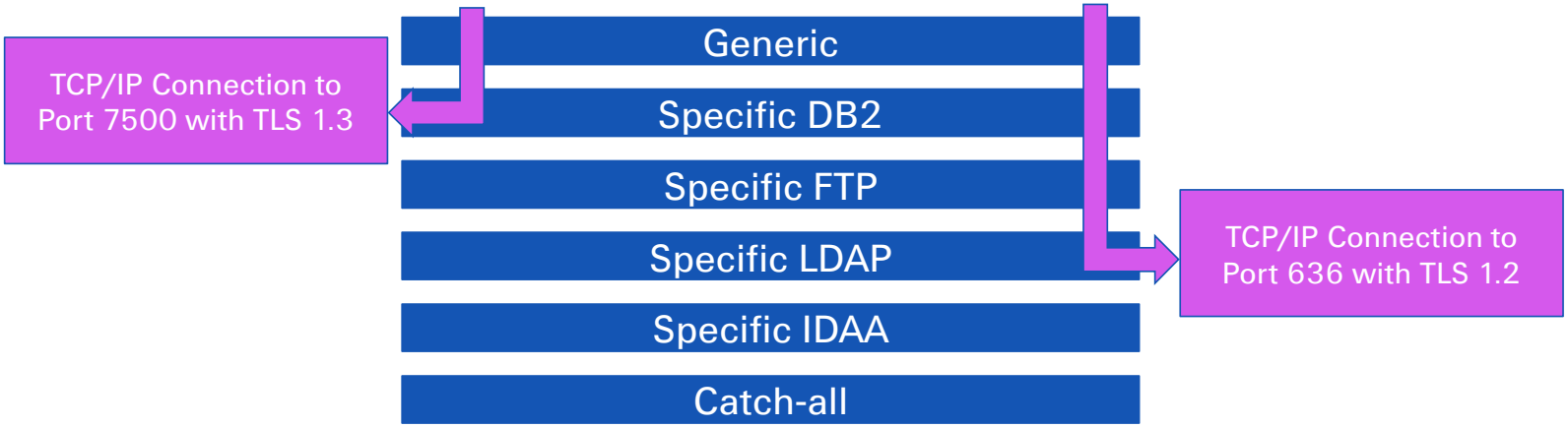
- Zero or one general rule
- 0-n specific rules
- One Catch-all rule

Disclaimer: For simplicity zERT Policy shows only TLS

PC: Protection Characteristics
TD: Traffic Descriptor
AG: Address Groups

RR: Reusable Rules
RRS: Reusable Rule Sets
DE: Data Endpoint

Define a Policy – Processing



A connection can match only 1 rule for each Protocol -> First match wins!
A connection can match more than one Protocol!

Define a Policy – Sample to assist in creation

Name	Protocol	Order	Type	Traffic Descriptor								Data Endpoints		TLS Version						SSH V.		Protection Characteristics											Action					
		Order per Protocol		SR-TD-All	SR-TD-DB2Q-Server	SR-TD-DB2F-Server	SR-TD-DB2D-Server	SR-TD-DB2I-Server	SR-TD-DB2O-Server	SR-TD-WAS-M7	SR-TD-WAS-E7	SR-TD-LDAP-Server	Local data endpoint	Remote Data endpoint	SSL V2	SSL V3	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3	SSHv1	SSHv2	SR-TLS-PC-Encryption-H	SR-TLS-PC-Encryption-M	SR-TLS-PC-Encryption-L	SR-TLS-PC-TLSKEX-H	SR-TLS-PC-TLSKEX-M	SR-TLS-PC-TLSKEX-L	SR-TLS-PC-MsgAuth-H	SR-TLS-PC-MsgAuth-M	SR-TLS-PC-MsgAuth-L	SR-SSH-PC-SSHKEX-H	SR-SSH-PC-SSHKEX-M	SR-SSH-PC-SSHKEX-L	Allow silently	or	Write SMF Record	Write Syslogd Message	Write TCPIP Joblog	Reset Connection
SR-TLS-GenericRule	TLS		Generic																	X																	X			
SR-TLS-SR-MP-Internal-AS	TLS		Specific	X									SR-MAINTPLEX	SR-MAINTPLEX					X	X			X			X			X								X			
SR-TLS-SR-MP-Internal-Log	TLS		Specific	X									SR-MAINTPLEX	SR-MAINTPLEX				X						X			X			X							X			
SR-TLS-SR-MP-Internal-Rst	TLS		Specific	X									SR-MAINTPLEX	SR-MAINTPLEX	X	X	X								X			X			X						X		X	X
SR-TLS-SR-MP-LDAP-AS	TLS		Specific									X	SR-MAINTPLEX	All_IPv4_Addresses					X	X			X			X			X								X			
SR-TLS-SR-MP-LDAP-Log	TLS		Specific									X	SR-MAINTPLEX	All_IPv4_Addresses				X						X			X			X							X			
SR-TLS-SR-MP-LDAP-Rst	TLS		Specific									X	SR-MAINTPLEX	All_IPv4_Addresses	X	X	X								X			X			X						X		X	X
SR-TLS-SR-MP-DB2-AS	TLS		Specific		X	X							SR-MAINTPLEX	All_IPv4_Addresses					X	X			X			X			X								X			
SR-TLS-SR-MP-DB2-Log	TLS		Specific		X	X							SR-MAINTPLEX	All_IPv4_Addresses				X						X			X			X							X			
SR-TLS-SR-MP-DB2-Rst	TLS		Specific		X	X							SR-MAINTPLEX	All_IPv4_Addresses	X	X	X								X			X			X						X		X	X
SR-TLS-SR-MP-AS	TLS		Specific	X									SR-MAINTPLEX	All_IPv4_Addresses					X	X			X			X			X								X			
SR-TLS-SR-MP-Log	TLS		Specific	X									SR-MAINTPLEX	All_IPv4_Addresses				X						X			X			X							X			
SR-TLS-SR-MP-Rst	TLS		Specific	X									SR-MAINTPLEX	All_IPv4_Addresses	X	X	X								X			X			X						X		X	X
SR-SSH-GenericRule	SSH		Generic																			X															X			
SR-SSH-SR-MP-AS	SSH		Spe																																		X			
SR-SSH-SR-MP-Log	SSH		Spe																																		X			
SR-SSH-SR-MP-Rst	SSH		Spe																																X		X		X	X
SR-NRP-SpecificRule	NRP		Spe																																		X			
SR-IPSEC-GenericRule	IPS		Gen																																		X			

Name	Protocol	Generic Rule			Specific Rules																			Catch-all action					
		SR-TLS-GenericRule	SR-SSH-GenericRule	SR-IPSEC-GenericRule	SR-TLS-SR-MP-Internal-AS	SR-TLS-SR-MP-Internal-Log	SR-TLS-SR-MP-Internal-Rst	SR-TLS-SR-MP-LDAP-AS	SR-TLS-SR-MP-LDAP-Log	SR-TLS-SR-MP-LDAP-Rst	SR-TLS-SR-MP-DB2-AS	SR-TLS-SR-MP-DB2-Log	SR-TLS-SR-MP-DB2-Rst	SR-TLS-SR-MP-AS	SR-TLS-SR-MP-Log	SR-TLS-SR-MP-Rst	SR-SSH-GenericRule	SR-SSH-SR-MP-AS	SR-SSH-SR-MP-Log	SR-SSH-SR-MP-Rst	SR-NRP-SpecificRule	Allow silently	or	Write SMF Record	Write Syslogd Message	Write TCPIP Joblog	Reset Connection
		------>>Order ---->>																											
SR-TLS-RuleSet	TLS	X			X	X	X	X	X	X	X	X	X	X	X	X								X			
SR-NRP-RuleSet	NONE																			X				X			
SR-SSH-RuleSet	SSH		X														X	X	X	X				X			
SR-IPSEC-RuleSet	IPSec			X																				X			

Activate the Policy - Steps

1. Install into Policy into configured path for Policy Agent
2. Refresh the Policy Agent
   - `F <policy-agent-stc-name>,REFRESH`

```
F PAGENT,REFRESH
EZZ8443I PAGENT MODIFY COMMAND ACCEPTED
```

3. Verify Refresh

```
EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : ZERT
```

Verify Results – zSecure

- Select SMF Dataset or Logstream containing SMF 119 records as input (SE.1 or ‘setup files’)
- zSecure Menu EV.I for “IP events from SMF and other logs”
- Select fields as required but at least “Further IP selection”

```
Show records that fit all of the following criteria:
IP address  . . . . ____________________________________________
Port  . . . . . . . ________      (IP port number)
Host name . . . . . ____________________________________________
System  . . . . . . ____          (system name or EGN mask)

Advanced selection criteria
_  Date and time          /  Further IP selection
```

- Select fields as required but at least “zERT”

```
IP address(es) to select (IP address, network prefix, or hostname)
_______________________________________________
_______________________________________________
_______________________________________________

IP address(es) to exclude (IP address, network prefix, or hostname)
_______________________________________________
_______________________________________________
_______________________________________________

zERT policy rule name
_____________________________________________

Record types to include
_  FTP    _  Telnet   _  z/OS Firewall   _  SMTP   /  zERT     HTTP logs (non-SMF)
_  SSH    _  Other
```

Verify Results – zSecure

- Select fields of interest for the report

```
Specify record subtypes to select:
_  Connection Detail                    _  Summary

Specify security protocol types to select:
_  SSL/TLS                              _  SSH
_  IPsec                                _  Other

Specify Security Association event types to select:
_  Connection initiation                _  Cryptographic attributes change
_  Connection termination               _  Short connection termination
_  zERT Enabled                         _  zERT Disabled
_  zERT Aggregation Enabled             _  zERT Aggregation Disabled
_  zERT Summary Interval                _  zERT Enforcement Action

Reset by zERT enforcement        _  (Y/N)
Transport layer connection ID    ________________________________________________
Search IP filter rule name       ____________________________________________
```

- Select fields as required (no selection includes all) – Sample shows only panel for SSL/TLS selection on previous panel

```
Specify TLS/SSL protocol types to select:
_  SSLv2        _  SSLv3        _  TLSv1        _  TLSv1.1      _  TLSv1.2
_  TLSv1.3

Specify FIPS 140 mode enablement levels to select:
_  Off          _  Level 1      _  Level 2      _  Level 3

Specify TLS/SSL symmetric encryption algorithm family to select:
_  None         _  DES          _  3DES         _  RC2          _  RC4
_  AES          _  Blowfish     _  CAST         _  ACSS         _  ARIA
_  Camellia     _  ChaCha20     _  IDEA         _  SEED         _  Fortezza
_  GOST28147    _  Twofish      _  Serpent
Specify TLS/SSL symmetric encryption chaining method to select:
_  None         _  CBC          _  CCM          _  CCM8         _  CFB
_  CTR          _  GCM
Key length . . __  _____       operator ( > >= < <= = <> ^= ) + length
```

Verify Results – zSecure

- Overview page of the report (for SSL/TLS sample)

```
Date/time          Description
 7Sep22 00:00:01.43 Short connection termination TLSv1.3 AES-GCM-256 server RSA-4096 client None-0 25532/273 bytes inbound/outbound local port 33642
 7Sep22 00:00:01.44 zERT enforcement action TLSv1.3 AES-GCM-256 local port 8803
 7Sep22 00:00:01.44 Short connection termination TLSv1.3 AES-GCM-256 server RSA-4096 client None-0 272/1506 bytes inbound/outbound local port 8803
 7Sep22 00:00:01.44 zERT enforcement action TLSv1.3 AES-GCM-256 local port 33643
 7Sep22 00:00:01.44 Short connection termination TLSv1.3 AES-GCM-256 server RSA-4096 client None-0 1506/272 bytes inbound/outbound local port 33643
 7Sep22 00:00:01.55 zERT enforcement action TLSv1.2 AES-GCM-256 141/355 bytes inbound/outbound local port 17284
 7Sep22 00:00:01.55 zERT enforcement action TLSv1.2 AES-GCM-256 355/141 bytes inbound/outbound local port 25022
 7Sep22 00:00:01.55 Short connection termination TLSv1.2 AES-GCM-256 1067/3780 bytes inbound/outbound local port 17284
 7Sep22 00:00:01.55 Short connection termination TLSv1.2 AES-GCM-256 3749/1067 bytes inbound/outbound local port 25022
 7Sep22 00:00:01.56 zERT enforcement action TLSv1.2 AES-GCM-256 141/355 bytes inbound/outbound local port 17285
 7Sep22 00:00:01.56 zERT enforcement action TLSv1.2 AES-GCM-256 355/141 bytes inbound/outbound local port 25022
 7Sep22 00:00:01.56 Short connection termination TLSv1.2 AES-GCM-256 1214/4446 bytes inbound/outbound local port 17285
```

- Example of a detailed view for a selected line (due to space constraints focus only on TLS/SSL specifics)

```
zERT policy rule names
IPsec policy rule name
SSH policy rule name
TLS policy rule name          SR-TLS-GenericRule
NRP policy rule name
```

```
TLS/SSL-specific data
TLS protocol version          TLSv1.3
TLS handshake type            Full
TLS local handshake role      Client
TLS session ID
TLS protocol provider         Observation
TLS cipher suite ID           1302
TLS encryption method         AES-GCM-256
TLS message auth method       HMAC-SHA-384
TLS key exchange method       DHE-EC
TLS FIPS 140 mode             Off
TLS Encrypt-then-MAC          No
```

```
TLS/SSL server certificate information
TLS server cert sig method
TLS server cert encr method
TLS server cert digest method
TLS server certificate serial
TLS server cert notAfter
TLS server cert key type
TLS server cert keylen (bits)
```

```
TLS/SSL client certificate information
TLS client cert sig method
TLS client cert encr method
TLS client cert digest method
TLS client certificate serial
TLS client cert notAfter
TLS client cert key type
TLS client cert keylen (bits)
```

Verify Results – zSecure

- Great overview to get quick results
- All required details available
- Cumbersome to analyze a lot of data
- No out of the box support from IBM via zOSMF. zOSMF Network Analyzer only support SMF 119(12) zERT discovery records. Users without zSecure Suite must code their own SMF reports. If you are unhappy with that too, please vote for the IBM Idea: https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-3412

- Hint:
  - When selecting all available options in zSecure the report fails due to syntax error
    -> https://www.ibm.com/support/pages/apar/OA63716?mhq=OA63716&mhsrc=ibmsearch_a

Verify Results – Carla and DB2

- Generate CSV Reports for SMF 119(11) and load into DB2 for analysis
- Sample Carla to report NRP (other Protocol Types are to big to show on slides)
- header=csvt not used as it does not enclose all fields in “”
  - complicates the csv load with db2 utility, hence creating csv ‘manually’
- Only NRP type requires RACF DB as input, for other protocol types SMF is enough
  - RECORDDSC requires SMF and RACF DB

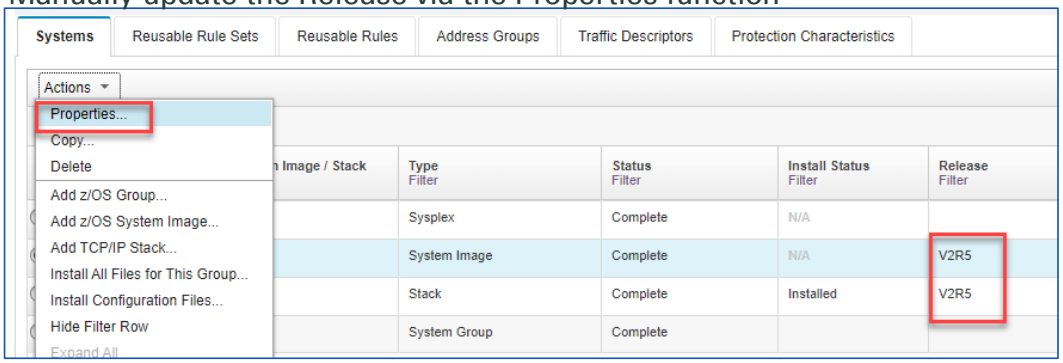
```
ALLOC TYPE=SMF    DD=C2SMF0    COMPLEX=MAINT
ALLOC TYPE=RACF PRIMARY ACTIVE COMPLEX=MAINT

 n type=smf n=smfsel outlim=0
S,
 (,
       type=119(11) and ,
       (                                  ,
        not(security_proto_tls_ssl)    ,
        not(security_protocol_ssh)     ,
        not(security_protocol_IPsec)   ,
       )
 )

 list type
  n type=smf noaction nodup pl=0 nopage
 s likelist=SMFSEL
 sortlist ,
    '"' | CONNECTION_INIT_DATETIME(0) | '"' | ';' | ,
    '"' | CONNECTION_END_DATETIME(0)   | '"' | ';' | ,
    '"' | SYSTEM(0)                    | '"' | ';' | ,
    '"' | SUBSYS(0)                    | '"' | ';' | ,
    '"' | USERID(0)                    | '"' | ';' | ,
    '"' | LOGONID(0)                   | '"' | ';' | ,
    '"' | JOBID(0)                     | '"' | ';' | ,
    '"' | JOBNAME(0)                   | '"' | ';' | ,
    '"' | ACTION(0)                    | '"' | ';' | ,
    '"' | DSTIP(0)                     | '"' | ';' | ,
    '"' | DSTPORT(0)                   | '"' | ';' | ,
    '"' | SRCIP(0)                     | '"' | ';' | ,
    '"' | SRCPORT(0)                   | '"' | ';' | ,
    '"' | IP_FILTERING_DONE(0)         | '"' | ';' | ,
    '"' | IP_PROTOCOL(0)               | '"' | ';' | ,
    '"' | BYTES_IN(0)                  | '"' | ';' | ,
    '"' | PACKETS_IN(0)                | '"' | ';' | ,
    '"' | BYTES_OUT(0)                 | '"' | ';' | ,
    '"' | PACKETS_OUT(0)               | '"' | ';' | ,
    '"' | RESET_ENFORCED(0)            | '"' | ';' | ,
    '"' | SA_EVENT_TYPE(0)             | '"' | ';' | ,
    '"' | NRP_POLICY_RULE_NAME(0)      | '"' | ';' | ,
    '"' | RECORDDESC(0)                | '"'
```

Verify Results – Carla and DB2

- Run SQL queries for all available SMF 119(11) fields
- We created four table(spaces) to hold data for the specific protocol types:
  - ZERTIPS
  - ZERTNRP
  - ZERTSSH
  - ZERTTLS
- Ad-hoc Reporting over large amount of data to verify policy behaviour

Stepping Stones

- Manual upgrade of the zOS Version for each TCP/IP technology required!
  - Manually update the Release via the Properties function



- When manually changed the Release, clear the browser cache und re-launch zOSMF otherwise unpredicted results occur when working with zERT
- Consider the order of zERT rules carefully

Additional information

- Useful enhancements you can vote for
  - zOSMF Network Analyzer must support SMF 119(11)
    - https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-3412
  - Simple Ordering of rules in zOSMF Configuration Assistant
    - https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-3411
  - Get dynamic window sizes in zOSMF NCA
    - https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-3406
  - Reuse of address groups in zOSMF Configuration Assistant
    - https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-3400
- Monitoring cryptographic network protection: z/OS encryption readiness technology (zERT)
  - https://www.ibm.com/docs/en/zos/2.5.0?topic=security-monitoring-cryptographic-network-protection-zos-encryption-readiness-technology-zert
- NEW FUNCTION IN V2R5 NETWORK CONFIGURATION ASSISTANT UPDATES
  - https://www.ibm.com/support/pages/apar/PH35304
- NEW FUNCTION IN V2R5 ZOSMF ZERT ANALYZER (Passphrase Support)
    - https://www.ibm.com/support/pages/apar/PH43119
- z/OSMF NCA Automatically detect the z/OS release level of a system image
  - https://ibm-z-hardware-and-operating-systems.ideas.ibm.com/ideas/ZOS-I-542
- Policy Agent and policy applications (zERT, AT-TLS, IDS and so on) TRDM
  - https://www.ibm.com/docs/en/zos/2.5.0?topic=papa-starting-traffic-regulation-manager-daemon-trmd-as-started-task
- Collection of good articles and further references about the full zERT topic
  - https://community.ibm.com/community/user/ibmz-and-linuxone/blogs/flora-gui1/2019/12/31/things-about-zert

Any questions?

Swiss Re

Thank you!

Contact us

Follow us

Legal notice

The information and opinions contained in the presentation are provided as at the date of the presentation and may change. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for its accuracy or comprehensiveness or its updating. All liability for the accuracy and completeness of the information or for any damage or loss resulting from its use is expressly excluded.