

Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

Traffic Regulation Management Daemon (TRMD)



IBM Washington System Center
IBM Technical Sales Support

Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
 - **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
 - All other products may be trademarks or registered trademarks of their respective companies.
 - Refer to www.ibm.com/legal for further legal information.
-
- OSA-Express Features
 - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

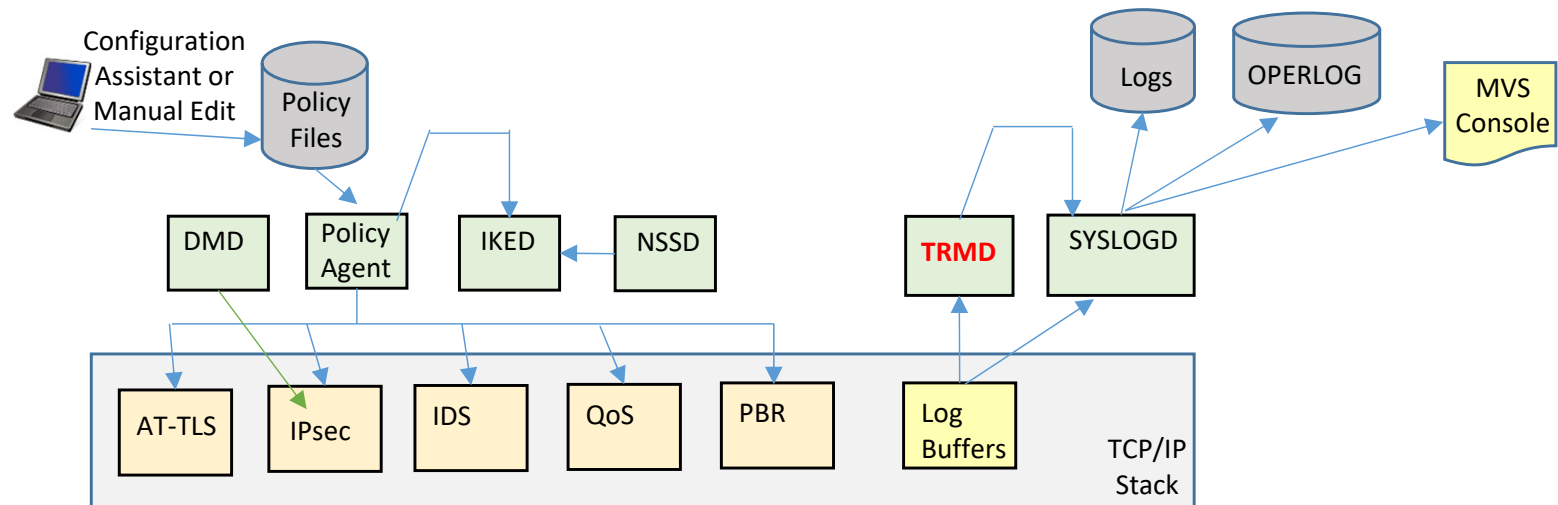
Agenda

- TRMD's Role in Policy Agent
- Implementing TRMD
 - Prerequisites
 - Setting the Timezone variable
 - Initializing and stopping TRMD
 - Format of the Environment Variable file or dataset
- Generating Formatted Reports for IDS with the 'trmdstat' Command

TRMD's Role in Policy Usage

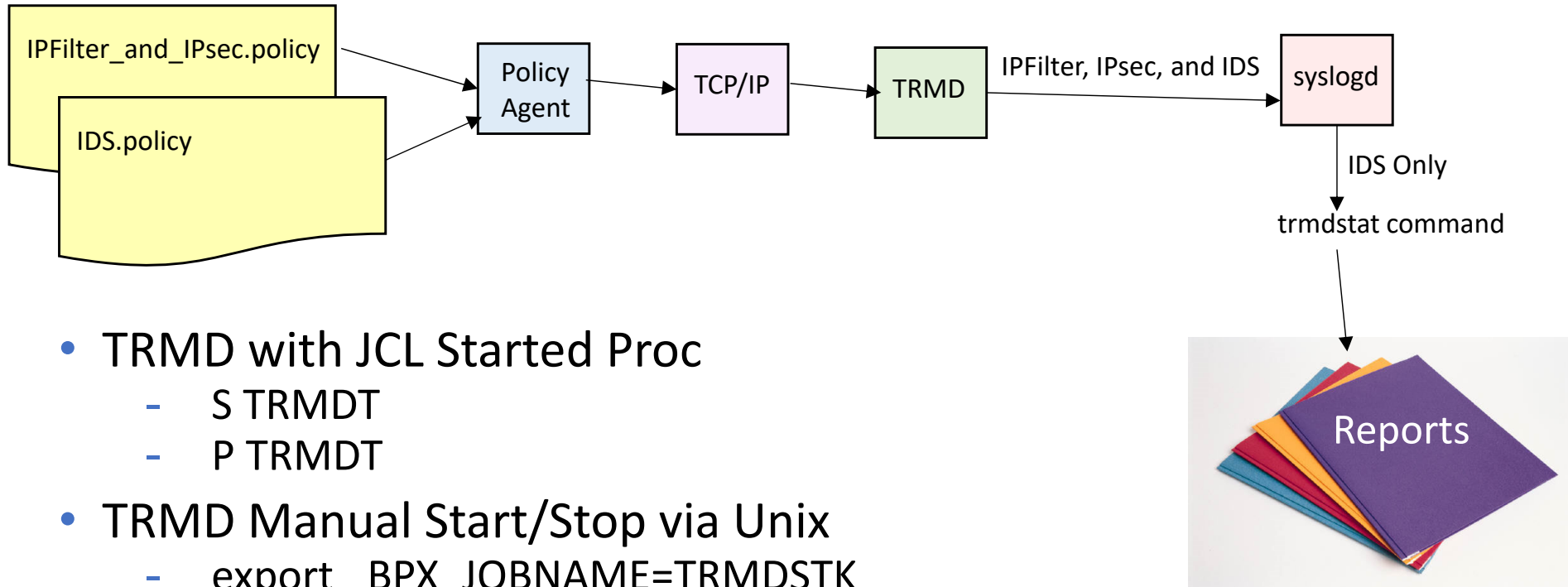


Lots of Different Policy Types and Started Tasks



- Policy Agent
 - Installs Policies into the TCP/IP stack
- TCP/IP Stack
 - Enforces the Policies
- DMD (Defense Manager Daemon)
 - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
 - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
 - Required for IKEv2
 - Provides central RACF certificate repository for remote IKED applications
 - Provides DataPower access to RACF
- **TRMD (Traffic Regulation Management Daemon)**
 - **Required for log messages to syslogd for IP Filter, IPsec, and IDS**
- SyslogD
 - Recommended for logging

TRMD (Traffic Regulation Management Daemon)



- TRMD with JCL Started Proc
 - S TRMDT
 - P TRMDT
- TRMD Manual Start/Stop via Unix
 - export _BPX_JOBNAME=TRMDSTK
 - export _RESOLVER_CONFIG=/etc/trmdenv
 - trmd &
 - ps -ef |grep trmd
 - 126 ttyp000 0:00 /usr/sbin/trmd
 - kill -9 126

TRMD can only connect to a single TCP/IP stack. There must be a second TRMD for a second TCP/IP stack, etc.

Implementing TRMD



TRMD Prerequisites

- APF Authorization:
 - SYS1.TCPIP.SEZALOAD
- UID=0 or Authorization to BPX.SUPERUSER

```
//*
//*TRMD EXEC PGM=IKJEFT01
/*SYSTSPRT DD SYSOUT=*
/*SYSTSIN DD *
/* SETROPTS CLASSACT(STARTED)
/* SETROPTS RACLIST(STARTED)
/* SETROPTS GENERIC(STARTED)
/* ADDUSER TRMD DFLTGRP(OMVSGRP) OMVS(UID(nn) HOME('/'))
/* RDEFINE STARTED TRMD.* STDATA(USER(TRMD))
/* SETROPTS RACLIST(STARTED) REFRESH
/* SETROPTS GENERIC(STARTED) REFRESH
/*
/* Permit access to BPX.SUPERUSER
/* PERMIT BPX.SUPERUSER CLASS(FACILITY) ID(TRMD) ACCESS(READ)
/*
```

hlq.SEZAINST(EZARACF)

- Associated TCP/IP stack must be initialized
- Resolver Config to locate the TCP/IP Stack must be correct prior to initialization
- Logging Timestamps:
 - Event detection in UTC time (Greenwich Mean Time)
 - Recording time (according to Timezone variable)

TRMD Sample Procedure in hlq.SEZAINST(TRMD)

```
//TRMD      PROC
//TRMD      EXEC PGM=EZATRMD,REGION=4096K,TIME=NOLIMIT,
//      PARM=('POSIX(ON) ALL31(ON)',
//      'ENVAR("LIBPATH=/usr/lib")/')
//* - To pass parameters to TRMD, specify them after the final slash
//*   on the PARM statement.  For example:
//*       //      PARM=('POSIX(ON) ALL31(ON)/-d 1')
//*
//*** Examples for specifying configuration data sets
//*
//* Example 1: TCPIP.DATA in partioned data set
//*       //      PARM=('POSIX(ON) ALL31(ON)',
//*       //      'ENVAR("RESOLVER_CONFIG=//''SYS1.TCPPARMS(TCPDATA)''")/')
//*
//* Example 2: TCPIP.DATA in HFS file
//*       //      PARM=('POSIX(ON) ALL31(ON)',
//*       //      'ENVAR("RESOLVER_CONFIG=/etc/resolv.conf")/')
//*
//* Example 3: Specification of data sets via STDENV DD statement
//*       //      'ENVAR("_CEE_ENVFILE=DD:STDENV")/')
//*
//STDENV    DD DUMMY
//SYSPRINT  DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//SYSIN     DD DUMMY
//SYSERR    DD SYSOUT=*
//SYSOUT    DD SYSOUT=*,DCB=(RECFM=
//CEEDUMP   DD SYSOUT=*,DCB=(RECFM=
```

Resolver_Config MVS

Resolver_Config Unix

- STDENV stored in MVS (V, VB) or in a unix file
 - Remember STDENV must not be in Fixed Block dataset.
- ```
RESOLVER_CONFIG=//''SYS1.CS.TCPPARMS(DAT1A) '
TZ=EST5EDT
```

# Class Example: TRMD Proc

```
//TRMDT PROC DATA=DAT&CL1.A,
// CS=SYS1
//* CS=USER
//TRMD EXEC PGM=EZATRMD,REGION=4096K,TIME=NOLIMIT,
// PARM=('POSIX(ON) ALL31(ON) ',
// 'ENVAR("RESOLVER CONFIG=//'&CS'.CS.TCPPARMS(&DATA) ' '") ',
// '"TZ=EST5EDT"7')
//* '"TZ=EST5EDT"/ -d1')
//STDENV DD DUMMY
//SYSPRINT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//SYSIN DD DUMMY
//SYSERR DD SYSOUT=*
//SYSOUT DD SYSOUT=*,DCB=(RECFM=F,LRECL=80,BLKSIZE=80)
//CEEDUMP DD SYSOUT=*,DCB=(RECFM=FB,LRECL=132,BLKSIZE=132)
```

Using MVS System Symbols  
"&CL1" = MVS SYSNAME in SYS1.PARMLIB(IEASYMnn)

LE Environment Variables on EXEC Statement

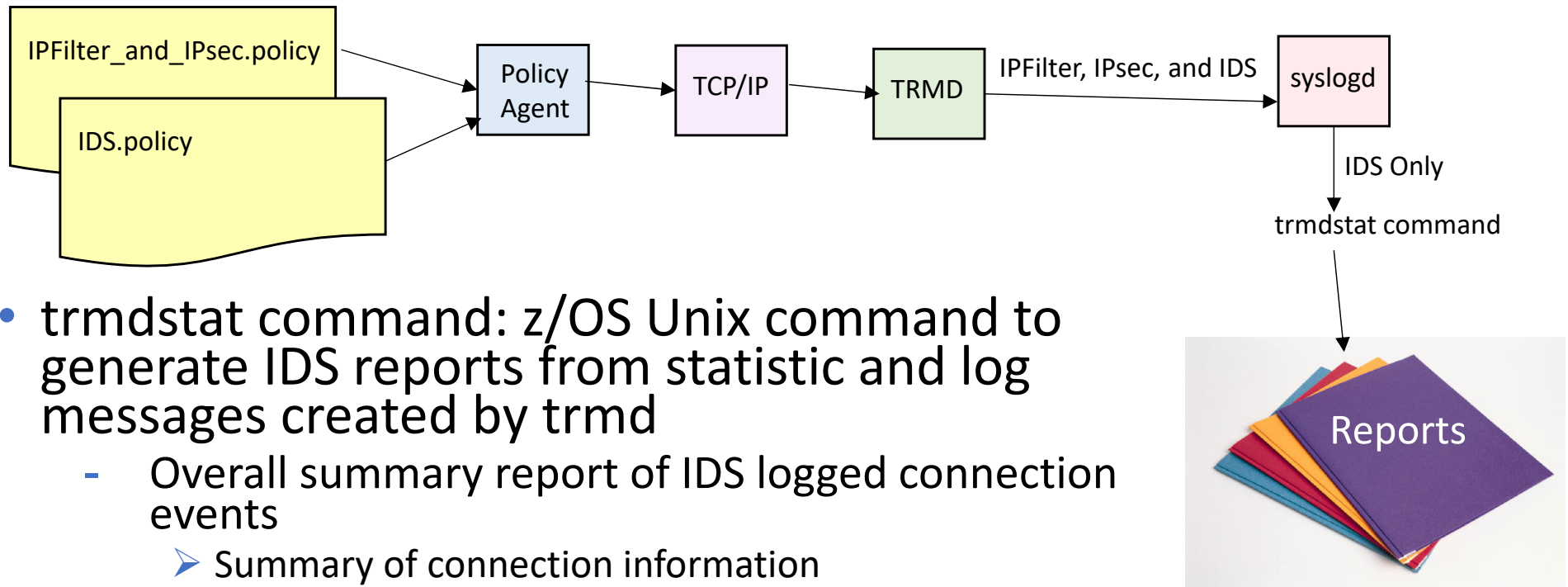
- If executing at MVS2, above JCL resolves to:

```
//TRMDT PROC
//TRMDT PROC DATA=DAT2A,
// CS=SYS1
//TRMD EXEC PGM=EZATRMD,REGION=4096K,TIME=NOLIMIT,
// PARM=('POSIX(ON) ALL31(ON) ',
// 'ENVAR("RESOLVER CONFIG=//'SYS1'.CS.TCPPARMS(DAT2A) ' '") ',
// '"TZ=EST5EDT"7')
```

# trmdstat Command



# Create IDS Reports



- trmdstat command: z/OS Unix command to generate IDS reports from statistic and log messages created by trmd
  - Overall summary report of IDS logged connection events
    - Summary of connection information
    - Summary of connection information for a specified host
  - Detailed reports of IDS logged events
    - Details of connection information
    - Details of connection information for a specified host
  - Examples:
    - Reports of logged intrusions defined in the ATTACK policy
    - Reports of logged intrusions defined in the TCP policy
    - Reports of logged intrusions defined in the UDP policy
    - Reports of statistics events

# trmdstat Syntax

```
>>---trmdstat---| Report Option |---+-----+---log_filename---><
 +---| Report Content |---| Filter |---| Global |---+
```

## Report Options:

```
+--- -I---+
|---+-----+---|
+--- -A---+
+--- -C---+
+--- -F---+
+--- -G---+
+--- -I---+
+--- -N---+
+--- -Q---+
+--- -T---+
+--- -U---+
+--- -?---+
```

## Report Content:

```
|---+-----+---|
+--- -D---+
+--- -E---+
+--- -S---+
```

## Filter:

```
|---+-----+---|
+--- -i initial_time-----+
+--- -f final_time-----+
| +--- -p 1=65535 -----+ |
+---+-----+---+
| +--- -p port_range----+ |
+--- -h ip_address-----+
+--- -j stack_name-----+
+--- -k ip_address-----+
+--- -s ip_address-----+
+--- -t ip_address-----+
+--- -c correlator-----+
+--- -n interface_name-----+
```

## Global:

```
+--- -d 0 ---+
|---+-----+---|
+--- -d n ---+
```

- A Displays the attack summary.
- C Displays the connection summary.
- F Displays the flood summary.
- G Displays the Global TCP Stall summary.
- I Displays the IDS Overall Summary Report.
- N Displays the scan summary.
- Q Displays the TCP Queue Size summary
- T Displays the TCP TR summary.
- U Displays the UDP TR summary.
- D Displays detailed information.
- E Specifies the TCP extended summary report.
- S Displays statistics summary.

# Attack Detail Report

```
trmdstat -A -D /tmp/tstlog.log
```

```
trmdstat for z/OS CS V1Rn
```

```
Wed Nov 8 09:55:36 2008
```

```
Log Time Interval : Aug 21 08:32:09 - Aug 21 10:32:09
```

```
Stack Time Interval : Aug 21 14:32:09 - Aug 21 14:32:09
```

```
TRM Records Scanned : 71
```

```
Port Range : ALL
```

## ATTACK Events

### Packets Discarded

| Attack | Date and Time        | Dst IpAddr  | Src IpAddr  | Dst Port | Src Port | Correlator | ProbeID  |
|--------|----------------------|-------------|-------------|----------|----------|------------|----------|
| Malf   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 0        | 0        | 82334      | 04010009 |
| IPFr   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 0        | 0        | 82336      | 04030001 |
| IPOP   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 0        | 0        | 82338      | 04050001 |
| PRTO   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 0        | 0        | 82339      | 04060001 |
| Perp   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 13001    | 10001    | 82342      | 04080001 |
| ICMP   | 8/21/2008 14:32:9.53 | 51.52.53.54 | 41.42.43.44 | 12001    | 10001    | 82337      | 04040009 |

Packets would have been Discarded

| Attack | Date and Time        | Dst IpAddr  | Src IpAddr  | Dst Port | Src Port | Correlator | ProbeID  |
|--------|----------------------|-------------|-------------|----------|----------|------------|----------|
| ORAW   | 8/21/2008 14:32:9.54 | 41.42.43.44 | 71.72.73.74 | 0        | 0        | 87999      | 04020001 |

```
TRMD Started : Aug 21 10:32:09
```

# End of Topic



# End of Topic

