ITM Firewall Gateway

Presenter: Dirk Wouters

Presentation Date: 26 September 2012

Tivoli software

© 2012 IBM Corporation

Agenda

- TEP Client to TEP Server
- Which Option to choose to traverse Firewalls
- Ephemeral Pipe
- Typical ITM Environment with Firewalls
- ITM - Data Flows in ITM and Ports Usage
- KDE Gateway Implementation
- KDE Gateway Configuration
- Debugging a KDE Gateway Configuration

© 2012 IBM Corporation

Special: TEPServer – TEP Client

- As of ITM v6.2.3, TEPS installs with IHS
- HTTP port by default 15200
- Previously: port 1920(..) (HTTP) and 15001 (…) for Corba
- As of 6.2.3: 15200 (HTTP) and 15001 for Corba
- Add Variable TEP.CONNECTION.PROTOCOL=HTTP (IIOP, HTTP, HTTPS) to use 15200 ONLY
  - WebStart and TEP ‘Fat’ Client only

© 2012 IBM Corporation

Which Option to choose to traverse Firewalls

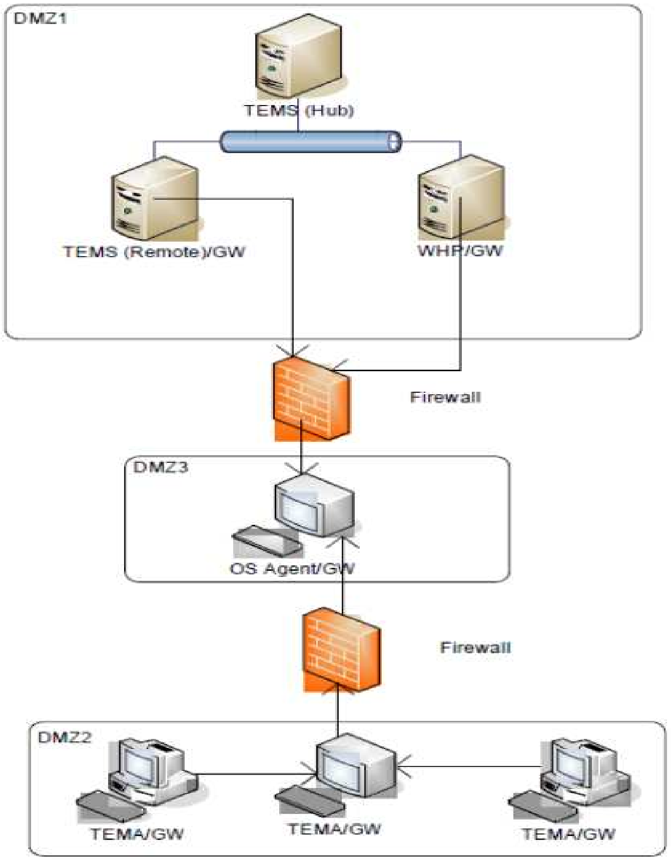
- Check the ITM Installation & Setup Guide – Appendix C
  - Permission at the Firewall
    - TEMS @ 1918
    - WPA @ 63358 (using SKIP:15)
  - Server Address Continuity
    - No NAT: no change
    - NAT: use of Ephemeral Pipe
    - NAT: Partition Files to map Server Addresses (less used)
  - Alternative: implement KDE Gateway (aka Firewall Gateway)
    - Connections initiated from most secure Zone – Port can be chosen
    - Full duplex – all logical Connections are multiplexed
    - Multiple Firewall Crossing using Relays
    - Handles both TEMS and WPA connections
    - Uses IP.PIPE or IP.SPIPE

Ephemeral Pipe

- Typical TEMA-TEMS Initialization:
  - TEMA at Startup discovers all its Network Interfaces
  - TEMA connects to its TEMS – passes on the NIC Addresses
  - TEMS tries to connect the TEMA back on any of the NIC
  - Causes failure if/when Firewall blocks this or NIC cannot be reached
- Ephemeral Pipe:
  - TEMA still discovers all NIC's
  - TEMA connects to TEMS – setting up a 'Tunnel' to TEMS
  - Since this Tunnel is Full Duplex, TEMS reconnects to TEMA using this Connection
  - In logs: IP Address shows as 0.0.0.x
- Ephemeral Pipe configured on i.e. KDE_TRANSPORT or KDC_FAMILIES at TEMA
  - ….. IP.PIPE use:y ephemeral:y…
  - Also set KPX_WAREHOUSE_LOCATION at the TEMS

Typical ITM Environment

- Server Zone with TEPS, HTEMS, RTEMS's and WPA's
- Behind Firewall(s): TEMA's
  - And Gateway Servers (OS TEMA)



- Exception: remote, slow Link

© 2012 IBM Corporation

ITM – Data Flows & Port Usage – TEP Request

- TEP Client Request:
  - Listening Ports:
    - TEPS: HTTP (1920…) and CORBA (15001)
    - HTEMS and RTEMS: 1918
    - TEMA: 1918 + x*4096 (6014 etc.)
  - Connections:
    - TEP Client to TEPS
    - TEPS to HTEMS on 1918
    - HTEMS to RTEMS on 1918
    - RTEMS to TEMA on 6014 (or higher)
    - Same Chain back

© 2012 IBM Corporation

ITM – Data Flows & Port Usage - Situations

- Situation Distribution follows same Chain as TEP Request
- Situation Data – overall, similar to return on TEP Request:
  - If Situation runs at TEMA (simple Situation):
    - TEMA evaluates Situation at every Interval
    - TEMA to RTEMS if changed
  - If Situation runs at RTEMS (complex Situation – scan etc.):
    - RTEMS requests Data from TEMA at every Interval
    - RTEMS evaluates Situation
    - If Alert: RTEMS connects with HTEMS on 1918

© 2012 IBM Corporation

ITM – Data Flows & Port Usage - Heartbeating

- TEMA to RTEMS on 1918 (default 10 mins)
- RTEMS to HTEMS on 1918 (default 3 mins)
- Represents important Part of overall Traffic in a large Environment

© 2012 IBM Corporation

ITM – Data Flows & Port Usage – Historical Collection

- Distribution of History Collection Probes (UADVISOR) same as Situations and TEP Request
- Collection at the TEMA (recommended):
  - ❑ Every Interval Collection at the TEMA (no Data Traffic)
  - ❑ Every Hour: TEMA connect to RTEMS – HTEMS Location Broker to request its WPA Address
  - ❑ Every Warehousing Interval (1 Hour rec.): TEMA connects Directly with WPA on its listening Port
    - WPA listens @Port 63358 (using SKIP:15 – 1918 + 15*4096)

ITM – Data Flows & Port Usage – Remote TEMA Deployment

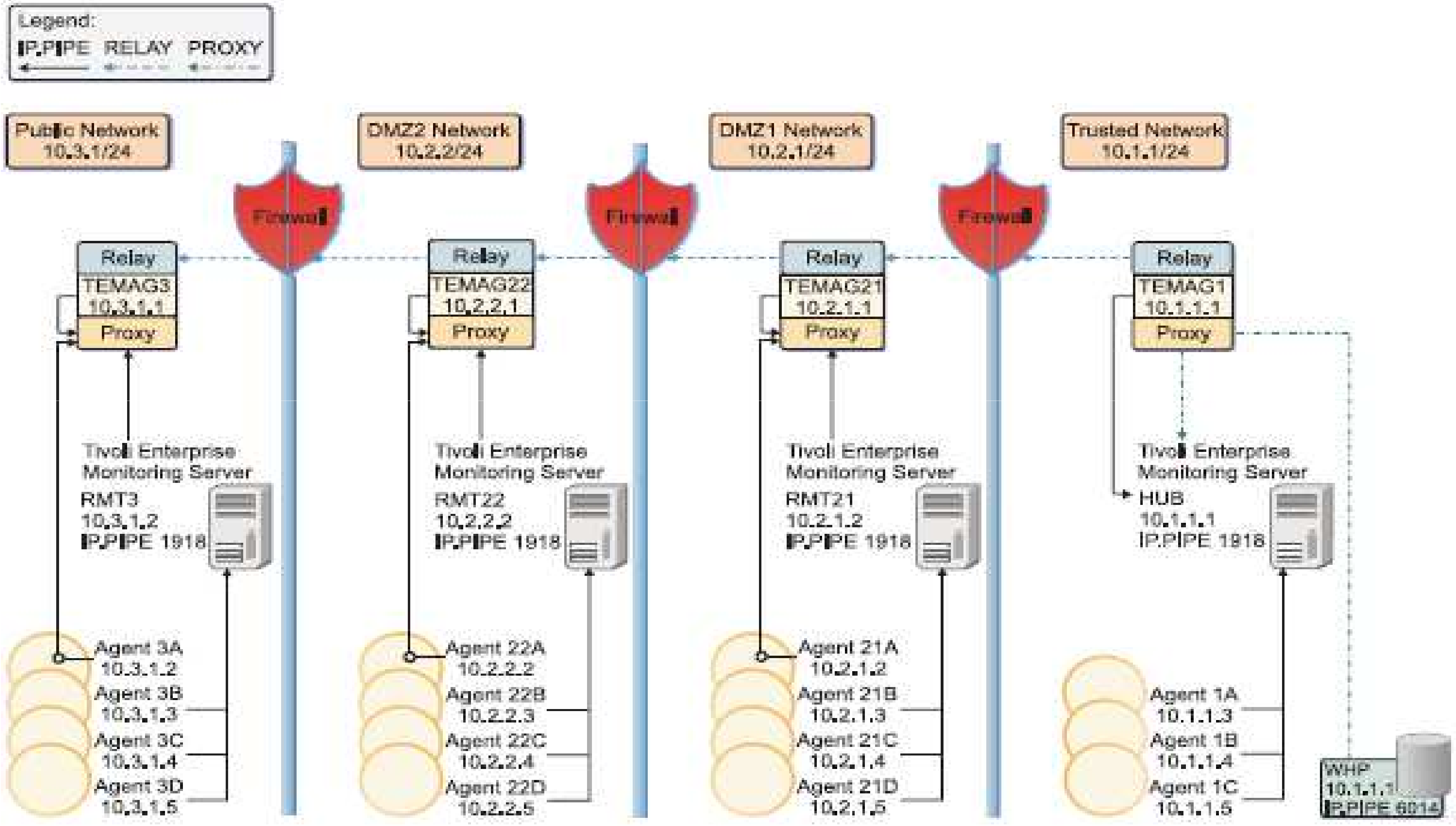
- OS Agent:
  - ❑ Request is ‘controlled’ by the TEMS
  - ❑ TEMS connects the Server using one of the Supported Protocols (SSH, SMB, RSH…) to download Image and start Install
- Non-OS Agent
  - ❑ Request is pushed from HTEMS to RTEMS (of OS TEMA)
  - ❑ RTEMS connects to OS TEMA on its listening Port (1918 + x*4096)
- OS Agent Deploy outside of KDE Gateway

ITM – Data Flows & Port Usage – HTTP Traffic

- At TEMA: Service Console & Interface
- Default Port 1920
  - First Component to start on a Server opens 1920
  - Second and following use the first component as location broker and open their own listening Port
- All Traffic outside of KDE Gateway

© 2012 IBM Corporation

KDE Gateway Implementation



© 2012 IBM Corporation

Configuring a KDE Gateway

- Select an OS TEMA in every Network Zone – including most Trusted Zone
- No Network Zone can be skipped – at least a ‘Relay’ is required
- Create an XML File with the proper Configuration Settings for every Gateway TEMA
- Add Variable KDE_GATEWAY to the TEMA KxxENV and point to the XML File

© 2012 IBM Corporation

KDE Gateway startup

- When the OS TEMA starts, it also initiates the KDE Gateway Interfaces
- 3 Functions can be defined at a Gateway:
  - role="connect“: TEMA opens the defined Port and tries a first time to connect to the defined server:port – Counterpart of LISTEN
  - role="listen“: TEMA starts to listen on de defined Port for incoming connections from the defined server/port – Counterpart of CONNECT
  - role=“proxy“: TEMA can start 2 different kinds of Proxy:
    - ClientProxy: runs in the Secure Zone and connects the incoming Gateway Connections to the TEMS or WPA
    - ServerProxy: runs in any of the Less Secure Zones and starts listening on the TEMS (1918) and/or WPA (63358) port

© 2012 IBM Corporation

KDE Gateway startup

- Connections are built in 2 Phases:
  - Connect – Listen Pairs: Connect Partners at regular Interval try to connect to the Listening Partner.
  - Until Connect-Listen Pairs have been established, Proxy Connections fail. Once established, TEMA's connect to their TEMS/WPA
- TEMA's must be configured to connect to the Gateway at the correct TEMS Port (same as the 'real' TEMS – 1918 by default)

© 2012 IBM Corporation

B1

Typical XML for Trusted Zone TEMA

```
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/" name="TEMAG1" >
<zone name="trusted">
        <interface name="clientproxy" role="proxy">
            <bind localport="poolhub" service="tems" >
                <connection remoteport="1918">10.1.1.1</connection>
            </bind>
        <interface name="downrelay2" role="connect">
            <bind localport="7000">10.1.1.1
                <connection remoteport="7100">10.2.1.1</connection>
            </bind>
        </interface>
        </interface>
</zone>
<portpool name="poolhub">20000-20099</portpool>
</tep:gateway>
```

```
+4C14925A.002A
+4C14925A.002A Loading gateway configuration: "C:\IBM\itm\tmaitm6\kde1.xml"
+4C14925A.002A
+4C14925A.002A
+4C14925A.002A Gateway configuration status: 00000000
+4C14925A.002A
(Sunday, June 13, 2010, 10:10:02 AM-{1138}kdebgog.c,44,"open_interfaces") Interface clientproxy.trusted.TEMAG1 startup complete
(Sunday, June 13, 2010, 10:10:02 AM-{1138}kdebgog.c,44,"open_interfaces") Interface downrelay2.trusted.TEMAG1 startup complete
(Sunday, June 13, 2010, 10:10:02 AM-{1138}kdebgog.c,99,"KDEBG_OpenGateway") Zone trusted.TEMAG1 startup complete: maxconn=2041
(Sunday, June 13, 2010, 10:10:02 AM-{1138}kdebgog.c,105,"KDEBG_OpenGateway") Gateway TEMAG1 startup complete
(Sunday, June 13, 2010, 10:10:02 AM-{2080}RAS1,400,"CTBLD")
```

© 2012 IBM Corporation

Slide 17

B1 BE05440, 6/13/2010

Typical XML for Trusted Zone TEMA – with WPA

```
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/" name="TEMAG1" >
<zone name="trusted">
        <interface name="clientproxy" role="proxy">
            <bind localport="poolhub" service="tems" >
                <connection remoteport="1918">10.1.1.1</connection>
            </bind>
            <bind localport="poolwhp" service="whp" >
                <connection remoteport="63358">10.1.1.1</connection>
            </bind>
        <interface name="downrelay2" role="connect">
            <bind localport="7000">10.1.1.1
                <connection remoteport="7100">10.2.1.1</connection>
            </bind>
        </interface>
        </interface>
</zone>
<portpool name="poolhub">20000-20099</portpool>
<portpool name="poolwhp">20100-20199</portpool>
</tep:gateway>
```

© 2012 IBM Corporation

Typical XML for DMZ TEMA - Endpoint

```
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/" name="TEMAG21">
 <zone name="DMZ1">
                    <interface name="uprelay" role="listen">
                                 <bind localport="7100">10.2.1.1.
                                              <connection remoteport="7000">10.1.1.1</connection>

                                 </bind>
                    <interface name="serverproxy" role="proxy">
                                 <bind localport="1918" service="tems"/>
                    </interface>
                    </interface>
   </zone>
   </tep:gateway>
```

- **Beware: NAT – 10.1.1.1 may have been translated- same with Port #**

© 2012 IBM Corporation

DMZ TEMA with NAT - random Port

- **IF: <connection>10.1.1.1</connection> - Gateway responds with**
- **“Ephemeral (0) remoteport not allowed’ with error code 1DE00062**

Remove entire Connection:

```
 <tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/" name="TEMAG21">
 <zone name="DMZ1">
                <interface name="uprelay" role="listen">
                          <bind localport="7100">10.2.1.1.
                                    <connection remoteport="7000">10.1.1.1</connection>
                          </bind>
                <interface name="serverproxy" role="proxy">
                          <bind localport="1918" service="tems"/>
                </interface>
                </interface>
</zone>
</tep:gateway>
```

- **Allows all incoming Connections**

© 2012 IBM Corporation

Alternative Configuration: Bridge Server

- Otherwise unconnected Networks
- No open Ports allowed through Firewall
- Use a Server with at least 2 NIC’s:
  - ❑ 1 NIC Connected to Secure Zone (2.2.2.2)
  - ❑ 1 NIC Connected to the DMZ (3.3.3.3)
- Sample Config XML for KDE Gateway:

```
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/" name="TEMAG1" >
<zone name="trusted">
            <interface name="clientproxy" role="proxy">
                    <bind localport="poolhub" service="tems" >2.2.2.2
                            <connection remoteport="1918">2.2.2.1</connection>
                    </bind>
            <interface name="serverproxy" role="proxy">
                    <bind localport="1918" service=”tems”>3.3.3.3
                    </bind>
            </interface>
            </interface>
</zone>
<portpool name="poolhub">20000-20099</portpool>
</tep:gateway>
```

© 2012 IBM Corporation

KDE_Gateway – Encrypting Data

- Recommended to use IP.SPIPE at TEMA and TEMS
  - ❑ TEMS to listen on Port 3660 by default
  - ❑ WPA to listen on Port 65100 with SKIP:15 (3660 + 15*4096)
  - ❑ Change Ports in XML files accordingly
- Alternatively: add ‘ssl=“yes”’ to the ‘Interface’ Tag
- All Encryption to add significant CPU Overhead
- Combination of IP.SPIPE and ssl not recommended:
  - ❑ Additional Overhead
  - ❑ Little Added Value in double Encryption

© 2012 IBM Corporation

Configuring a Failover KDE_Gateway

- ITM 6 allows many Failover Configurations – depending on needs:
  - ❑ TEMS HotStandby – Server Clustering - Implementing Spare Remote TEMS…
  - ❑ As for KDE_Gateway:
    - Typically used between TEMA and its RTEMS(‘s)
    - Use the ‘Spare Remote TEMS’ scenario:
      - ✓ I.e. 2000 TEMA’s to connect with 3 RTEMS’s
        - 1000 TEMA’s to connect to RTEMS1
        - 1000 TEMA’s to connect to RTEMS2
        - RTEMS3 is Secondary for all 2000 TEMA’s
      - ✓ I.e. All TEMA’s in DMZ1 connect to RTEMS1 – with RTEMS3 as Secondary
        - Configure 2 Gateway Proxies in DMZ1 – 1 to RTEMS1
        - Proxies must be on separate Servers – both listen on Port 1918
    - Use Multiple Addresses on the Connection Tag
      - ✓ Introduces dependency on Single Point of Failure

© 2012 IBM Corporation

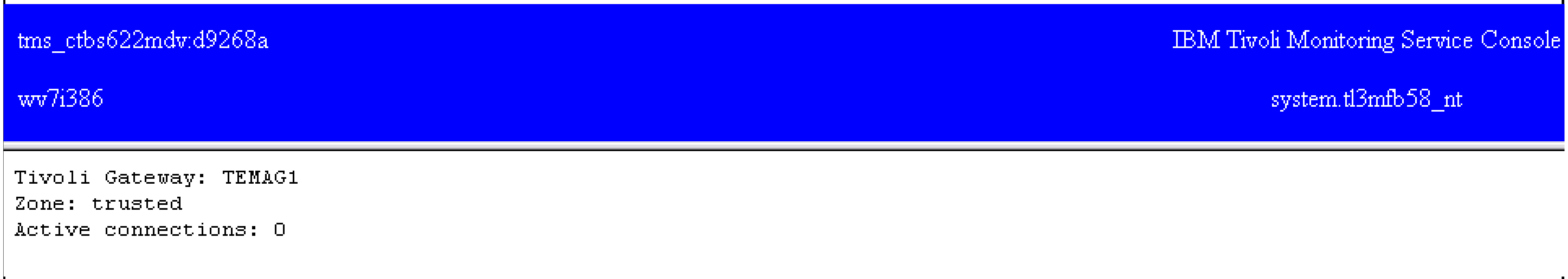
Debugging a KDE_Gateway Configuration

- Plan the entire Configuration
- Select the KDE Proxy Servers
- Implement the KDE Gateway
  - ❑ Edit the required XML Files and distribute to selected TEMA's
  - ❑ Add the KDE_Gateway Variable to the selected TEMA's
- Check the correct Working
  - ❑ On TEP Client – is TEMA online ? Workspaces provide Data ?
  - ❑ Check Warehouse
    - Check Warehouse DB Tables or Warehouselog for TEMA Entries
    - Use ITMSuper – Warehouse Tab

© 2012 IBM Corporation

Debugging a KDE_Gateway Configuration

- Use Service Console to check individual Gateway TEMA's
  - Connect your Browser to TEMA:1920
  - Select the Service Console for the Gateway TEMA and logon
  - On Console – Type Command: gateway status
  - Sample Result:



tms_ctbs622mdv:d9268a

IBM Tivoli Monitoring Service Console

wv7i386

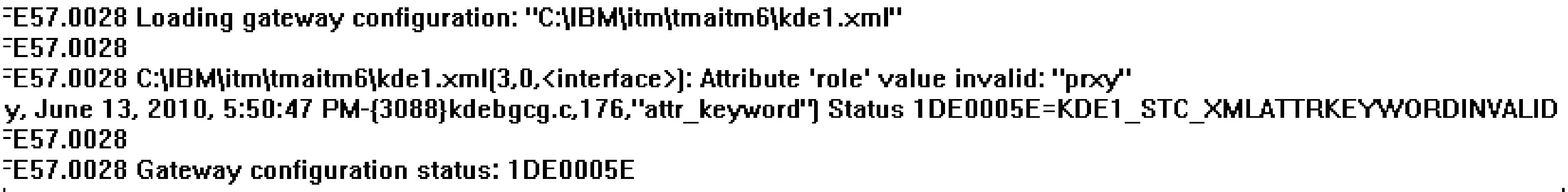
system.tl3mfb58_nt

```
Tivoli Gateway: TEMAG1
Zone: trusted
Active connections: 0
```

© 2012 IBM Corporation

Debugging a KDE_Gateway Configuration

- TEMA RAS1 Logs
- Use NETSTAT –an(b)
- Check the XML Files
- Most common Error: XML Syntax
  - In TEMA RAS1:



```
FE57.0028 Loading gateway configuration: "C:\IBM\itm\tmaitm6\kde1.xml"
FE57.0028
FE57.0028 C:\IBM\itm\tmaitm6\kde1.xml(3,0,<interface>): Attribute 'role' value invalid: "prxy"
y, June 13, 2010, 5:50:47 PM-{3088}kdebgcg.c,176,"attr_keyword"] Status 1DE0005E=KDE1_STC_XMLATTRKEYWORDINVALID
FE57.0028
FE57.0028 Gateway configuration status: 1DE0005E
```

© 2012 IBM Corporation

Debugging a KDE_Gateway Configuration

- Logical Errors or Connection lost:
  - kdebgrd.c,31,"KDEBG_RelayDisconnect") Interface downrelay.dmz.server1 connection lost: 1.1.1.1:7000
  - XML – “Service=“ on Bind Tag must be spelled identical
  - Use Port 1918 consistently – also for TEMA to Gateway Proxy
- Checking Connections:
  - First check Proxy to Proxy Connections
  - Next check the TEMA to Proxy and Proxy to TEMS Connections – these will fail as long as Proxies are not connected

© 2012 IBM Corporation

Questions ?

© 2012 IBM Corporation