Using the KDE gateway to cross firewalls in IBM Cloud Application Performance Management (Cloud APM)

Document Owners:

Ayron Dal Pont (dalpont@br.ibm.com)

Ben Stern (bstern@us.ibm.com)

Table of Contents

1. Introduction:

This document describes how to connect APM agents to an APM server using the KDE gateway feature in the agent. Use this procedure when the agents and the server are in different zones of the network and APM communication is blocked by a firewall. The KDE gateway enables traffic to flow through a firewall in a direction and over a port that is specified by network administrators.

This document does not replace the official APM documentation.

2. Prerequisites:

The KDE gateway feature is part of the APM agent. To use this procedure, an APM agent must exist on both sides of the firewall, that is, on the less secure side and on the more secure side.

A TCP port must be opened on the firewall for KDE communication so that a connection can be established from downstream to upstream components.

3. Naming Conventions

In this document, the following systems are included in the example configuration:

- **upstream-hostname** is the host name of the upstream KDE gateway. It is the server that communicates with the APM 8.1.x server.
- **downstream-hostname** is the host name of the downstream KDE gateway. It is the server that the agents connect to and send their data.
- **apm-hostname** is the host name of the APM 8.1.x server.

4. Network Flows:

Use the KDE gateway to connect APM agents to an APM server when a direct connection between these components is not possible.

There are two ways to use KDE gateways, as outlined in the following sections.

Scenario 1: APM server is in a more secure network zone than the APM agents

When the APM server is in the more secure network zone, the upstream KDE gateway initiates a connection to the downstream KDE gateway using the configured port. The port that is used is configurable. Port 55555 is used in the example configuration. After a network connection between the upstream and the downstream gateway is established, it remains open and traffic flows over it. APM agents connect to the downstream KDE gateway on the usual APM port (either 443 or 80) and the agent data flows to the upstream KDE gateway, and on to the APM server. Port 443 is used when the APM server is set up for HTTPS communication and port 80 is used when the APM server is set up for HTTP communication. The examples use HTTPS and port 443.

Note: In this scenario, communication is always initiated from the upstream KDE gateway to the downstream KDE gateway.

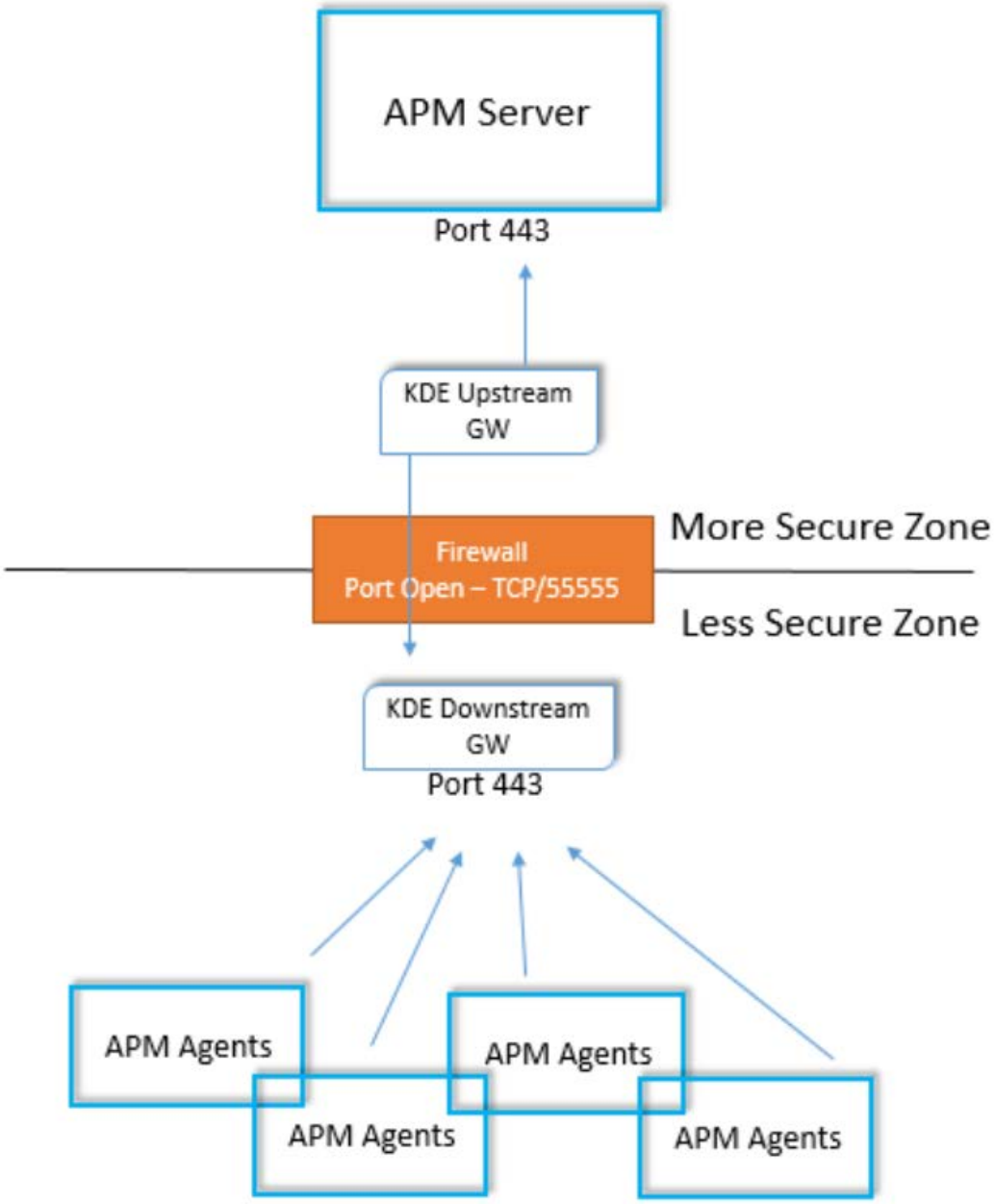
Scenario 2: APM server is in a less secure network zone than the APM agents

The configuration in scenario 2 is the opposite of scenario 1. In scenario 2, the APM server is in a less secure network zone than the APM agents. The downstream KDE gateway initiates a connection to upstream KDE gateway using the configured port. Port 55555 is used in the example configuration. The APM agents connect to downstream KDE gateway on the usual APM port (either 443 or 80) and the agent data flows to the upstream KDE gateway, and on to the APM server.

Note: Typically, it is not necessary to use a KDE gateway when the APM server is in the less secure network zone. Instead, configure HTTP or HTTPS traffic to flow directly from the agents to the APM server or set up a forwarding proxy.

Typical data flow between components

This diagram shows a typical configuration when using a KDE Gateway. The KDE gateway helps to securely negotiate firewall zones.



5. Setting up a KDE gateway

Complete the following steps to enable the KDE gateway on two APM agents. Then, use that configuration to establish TCP communication across the firewall.

Step 1: Enable KDE gateways on agents

Enable the KDE gateway feature on existing APM agents. Typically, the OS agent is used as the upstream and downstream KDE gateways, but you can use any agent. In the following examples, the OS agent is used.

The KDE gateway is configured on two APM agents on either side of the firewall to establish the communication between the sender (downstream) and the receiver (upstream).

Remember: even though traffic flows from the sender to the receiver, it is the receiver that typically initiates network communication.

The downstream gateway is the system where the APM agents connect. The upstream gateway is the system that forwards the data to the APM v8.1.x server.

Complete the following steps to configure the downstream KDE gateway:

i. Create a file to define the downstream configuration (e.g. downstream.xml). In the following example, the downstream.xml file is in the /opt/ibm/apm/agent/config directory. You can assign any name to the file, but you must reference the file name in the agent configuration file.

ii. Identify whether the downstream KDE gateway is in a more secure zone than upstream gateway. In addition, confirm that the firewall is open for communication between the upstream and downstream KDE gateways over the configured port.

iii. Add the XML content to the file (see section 6) depending on whether the downstream gateway is in the less secure network zone or the downstream gateway is in the more secure network zone.

iv. Edit the APM agent environment file (e.g. /opt/ibm/apm/agent/config/lz.environment) and add following content

KDE_GATEWAY=/opt/ibm/apm/agent/config/downstream.xml

KDE_DEBUG=N

KDC_DEBUG=N

Initially, when you set up the KDE gateway, you can set KDE_DEBUG and KDC_DEBUG to Y to debug.

Note: The path /opt/ibm/apm/agent/config/downstream.xml is the full path to the created downstream configuration file.

To use a Windows OS agent as the KDE Gateway, edit the <*Install_dir*>\TMAITM6_x64\KNTENV file and add the same variables. Place the XML file in a typical Windows path such as C:\IBM\APM\CONFIG\downstream.xml

For example, on a Windows systems, edit C:\IBM\APM\TMAITM6_x64\KNTENV

v. Restart the APM agent that you are using for the KDE config (e.g lz agent)

On UNIX or Linux:

/opt/ibm/apm/agent/bin/os-agent.sh stop

/opt/ibm/apm/agent/bin/os-agent.sh start

On Windows:

C:\IBM\APM\BIN\os-agent.bat stop

C:\IBM\APM\BIN\os-agent.bat start

Complete the following steps to configure the upstream KDE gateway:

i. Create a file to define the upstream configuration (e.g. upstream.xml). In the example below, the upstream.xml file is in the /opt/ibm/apm/agent/config directory. You can assign any name to the file, but you must reference the file name in the agent configuration file.

i. Identify whether the KDE upstream gateway is in a more secure zone than downstream gateway. Confirm that the firewall is open for communication between the upstream and downstream KDE gateways over the configured port.

ii. Add XML content to the file (see section 6) depending on whether the upstream gateway is in the more secure network zone or in the less secure network zone.

iii. Edit the APM agent environment file (e.g. /opt/ibm/apm/agent/config/lz.environment) and add following content:

KDE_GATEWAY=/opt/ibm/apm/agent/config/upstream.xml

KDE_DEBUG=Y

KDC_DEBUG=Y

Note: The path /opt/ibm/apm/agent/config/upstream.xml is the full path to the created upstream configuration file.

To use a Windows OS agent as the KDE Gateway, edit the <*Install_dir*>\TMAITM6_x64\KNTENV file and add the same variables. Place the XML file in a typical Windows path such as C:\IBM\APM\CONFIG\downstream.xml

For example, on a Windows system, edit C:\IBM\APM\TMAITM6_x64\KNTENV

v. Restart the APM agent that you are using for the KDE config (e.g lz agent)

/opt/ibm/apm/agent/bin/os-agent.sh stop

/opt/ibm/apm/agent/bin/os-agent.sh start

Important: Start the agent that is running the KDE gateway in the less secure zone first. The agent in the less secure zone starts listening on port 55555. Next, start the agent with the KDE gateway that is configured in the more secure zone. The KDE gateway in the more secure zone attempts to establish a network connection with the KDE gateway in the less secure zone.

Step 2: Configure agents to use the KDE gateways

To use the KDE gateway tunnel, the APM agent must be configured. Normally, the APM agents are configured to communicate directly with the APM server. But, when you use a KDE gateway, you must configure the agents to communicate with the downstream KDE gateway.

You have two options. Normally, you configure the agent media so that agents communicate with the KDE gateway rather than the APM server. Then, when the agents are installed, they automatically communicate with the downstream KDE gateway. Alternatively, if an agent is already deployed, you can reconfigure the agent to use the KDE Gateway.

Option 1: configuring the APM agent media

The process is different for SaaS and on-premise environments.

On-premise APM servers:

Use the existing APM commands on the APM server to configure the agent media. Additional information on configuration the agent media for on-premise environments can be found here: https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.4/com.ibm.pm.doc/install/install_agent_preconfig.htm

First, run the /opt/ibm/ccm/make_configuration_packages.sh command and follow the prompts.

You are prompted to "Enter the IP address/hostname that should be used by agents to communicate with the server." When prompted, instead of specifying the IP address of the APM server, specify either the fully qualified hostname or IP address of the downstream KDE gateway.

> *Enter the IP address/hostname or accept the default [9.42.13.95]: <downstream-hostname>*

Next, you are prompted for the path to the directory where the configuration packages are stored. You can accept the default path or specify your own directory.

> *Enter the path to the directory where you want to store the configuration packages or accept the default value [/opt/ibm/ccm/mkcustpkg_workdir.24423]:*

Finally, you are prompted to specify whether to use HTTP or HTTPS for agent communication. Specify HTTP or HTTPS based on how your APM server is configured. For SaaS environments, you must specify HTTPS.

Agents can connect to the server using secure https or unsecure http protocol.

Enter your choice [1-http, 2-https; "http" is default]? http

Next, you run the /opt/ibm/ccm/ configure_agent_images.sh command and follow the prompts.

First, you are prompted for the directory that contains the configuration package. Specify the path you chose when you ran the make_configuration_package.sh command:

/opt/ibm/ccm/mkcustpkg_workdir.24423

Next, specify the path where the APM media is located. For example /media

Finally, you are prompted to specify the directory where to place the updated media. The default is /opt/ibm/ccm/depot. Either choose the default directory or specify your own path. If you need to retain multiple agent media packages so that a subset of your agents can communicate through a different KDE gateway or directly to the APM server, then specify a different directory for the agent media. Install your agents using the agent media placed in the specified directory.

For SaaS APM servers:

For SaaS environments, you must edit the TAR/ZIP file media. Extract the TAR or ZIP file. Then, edit the global environment file using the following instructions:

On Linux and UNIX media, edit the following file:

/<media location>/APMADV_Agent_Install_8.1.4.0/.apm_config/agent_global.environment

On Windows media, edit the following file:

C:\<media location>\APMADV_Agent_Install_8.1.4\apm_config\framework_silent_install

You must modify two parameters in the agent_global.environment file on UNIX/Linux or framework_silent_install on Windows. Replace the host name or IP address and port number with the fully qualified host name or IP address of the downstream KDE gateway.

Example, you see something like this in the original files

IRA_ASF_SERVER_URL=http://9.42.13.95:80/ccm/asf/request

IRA_API_DATA_BROKER_URL=http://9.42.13.95:80/1.0/monitoring/data

Replace the IP address so that the entries look like this:

IRA_ASF_SERVER_URL=http://<downstream-hostname>:80/ccm/asf/request

IRA_API_DATA_BROKER_URL=http://<downstream-hostname>:80/1.0/monitoring/data

You can now install agents using the updated installation media. The agents connect to the downstream KDE gateway and traffic flows through the KDE gateway and up to the APM server.

Option 2: reconfiguring an existing APM agent

Follow these steps to configure a previously installed APM agent to use a KDE gateway.

i. On the APM agent, edit the file /opt/ibm/apm/agent/config/global.environment and update the following lines. Replace "downstream-hostname" with the fully qualified host name of the downstream KDE gateway.

IRA_ASF_SERVER_URL=https://downstream-hostname:443/ccm/asf/request

IRA_API_DATA_BROKER_URL=https://downstream-hostname:443/1.0/monitoring/data

Note: the address downstream-hostname:443 is the one created by downstream KDE to receive connections from APM agents. The data flows from the KDE to the upstream KDE and on to the target server (that is, the APM server). If the APM server is configured for HTTP, use 80 instead of 443 for the port.

ii. Reconfigure the agent using the "agent2server.sh" or "agent2server.bat" command and specify the IP address or the fully qualified host name of the downstream KDE gateway. Replace <downstream-hostname> in the following command with the IP address or host name of the downstream gateway.

UNIX and Linux systems:

/opt/ibm/apm/agent/bin/agent2server.sh -s <downstream-hostname>

Windows systems:

C:\IBM\APM\BIN\agent2server.bat –s <downstream-hostname>

iii. Restart the APM agent that you updated in the previous step. For example, to restart the OS Agent, enter:

UNIX and Linux systems:

/opt/ibm/apm/agent/bin/os-agent.sh stop

/opt/ibm/apm/agent/bin/os-agent.sh start

Windows systems:

C:\IBM\APM\BIN\os-agent.bat stop

C:\IBM\APM\BIN\os-agent.bat start

Step 3: Validate the agent communication flow

To validate that the APM agent is correctly using the KDE flow, follow these steps. In the examples, 10.146.94.69 is the IP address.

Validate the downstream KDE Gateway

i. Check that the TCP/443 port is in LISTEN mode by typing the following command. If your environment is using HTTP, change the port number to 80.

[root@rcpengine01 bin]# *netstat -an | grep 443 | grep LIST*

Confirm that it is listening on port 443 or port 80.

tcp 0 0 0.0.0.0:443 0.0.0.0: LISTEN*

ii. Check the connection between the two KDE gateways. They must communicate on TCP port 55555.

When downstream KDE is on a **more secure** zone, enter:

[root@rcpengine01 bin]# *netstat -an | grep 55555*

Confirm that communication is established on port 55555

tcp 0 0 10.146.94.69:55555 10.146.94.109:55555 ESTABLISHED

When downstream KDE is on a **less secure** zone, enter:

[root@rcpengine01 kde]# *netstat -an | grep 55555*

Confirm that you see the following:

tcp 0 0 10.146.94.69:55555 0.0.0.0: LISTEN*

tcp 0 0 10.146.94.69:55555 10.146.94.109:55555 ESTABLISHED

iii. Check the APM agent connection status. Enter:

[root@rcpengine01 bin*]# ./os-agent.sh status*

Confirm that you see results like the ones below. You should see a connection status of "Connected"

Agent status:

Agent is running. Process ID is 2740

Server connection status: Connected

iv. Check whether the APM agent is using the downstream KDE to connect to APM server. Enter:

[root@rcpengine01 bin]# *cat /opt/ibm/apm/agent/logs/lz_ServerConnectionStatus.txt*

Confirm that you see results like the ones below.

*Thu Sep 14 08:42:57 2017 Agent ASF server connection status is **CONNECTED***
*Server URL (https://**10.146.94.69**:443/ccm/asf/request)*

Thu Sep 14 08:43:02 2017 Agent CCS server connection status is DISCONNECTED-NORMAL Server URL (http://10.146.94.109:80/CentralConfigurationServer/)

Thu Sep 14 08:43:04 2017 Agent EIF server connection status is DISCONNECTED-NORMAL Server URL (https://10.146.94.69:443/ccm/asf/request)

Thu Sep 14 08:42:54 2017 Agent REST server connection status is INACTIVE

Validate the upstream KDE Gateway

i. Check the connection between the KDE gateways and check that the port is in LISTEN mode on TCP port 55555.

When upstream KDE is in the **more secure** zone, enter:

[root@cogauto-apm02 kde]# *netstat -an | grep 55555*

Confirm that the communications are established on port 55555.

tcp 0 0 10.146.94.109:55555 10.146.94.69:55555 ESTABLISHED

When the upstream KDE gateway is in the **less secure** zone, enter:

[root@cogauto-apm02 ~]# *netstat -an | grep 55555*

Confirm that the results are like the ones below:

tcp 0 0 10.146.94.109:55555 0.0.0.0: LISTEN*

tcp 0 0 10.146.94.109:55555 10.146.94.69:55555 ESTABLISHED

ii. Check the APM agent connection status. Enter:

[root@cogauto-apm02 bin]# *./os-agent.sh status*

Confirm that the connection status is “Connected” as shown in the following example.

Agent status:

Agent is running. Process ID is 7435

Server connection status: Connected

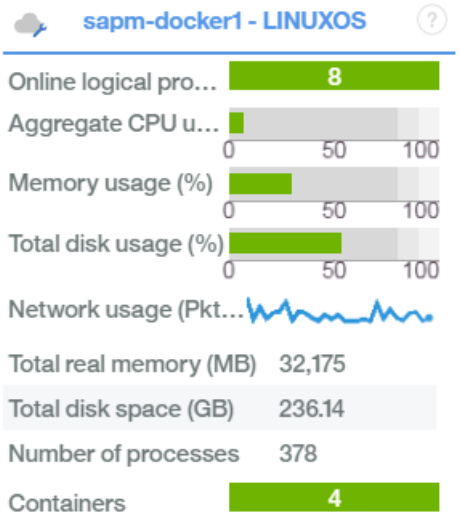
Step 4: Validate that the APM agent data displays on the console

To validate that the APM agent data displays on the APM console, complete these steps.

i. Start the APM console.

ii. Under “All my applications”, click “My Components”. Note: In a large APM environment “My Components” is not available. To validate agent connectivity, add the agent to a business application.

iii. Locate the APM agent that was used to connect to the downstream KDE and check that the agent is online.



At this point, the agent should be fully functional. You should receive events from the agent, be able to drill down into the agent details, see transaction tracking and deep dive diagnostic data, and so on.

6. KDE gateways configuration files

To configure the KDE gateways, use the XML files that are described in the following section. You will use two of the XML examples depending on whether your upstream gateway is in the more or less secure network zone. The most common configuration is for the downstream gateway to be in the less secure zone and the upstream gateway to be in the more secure zone.

The example XML files use the following variables:

- **upstream-hostname** is the host name of the upstream KDE gateway. It is the server that communicates with the APM 8.1.x server.
- **downstream-hostname** is the host name of the downstream KDE gateway. It is the server that the agents connect to and send their data.
- **apm-hostname:** This is the host name of the APM 8.1.x server.

In the XML files, you can either specify the host name of the server or you can specify the IP address. If you use the host name, it is recommended that you specify the fully qualified host name.

In the following examples, port 443 is used for communication from the agent to the downstream KDE gateway and from the upstream KDE gateway to the APM v8 server. Set the port value based on whether your APM server is configured for HTTP or HTTPS communication. If your APM server is set up for HTTPS, use port 443. Otherwise, use port 80.

Upstream gateway in a more secure zone / Downstream gateway in less secure zone

This section provides XML examples for when the upstream KDE gateway is in the more secure network zone and the downstream KDE gateway is in the less secure network zone. For this configuration, the upstream KDE gateway initiates network communication over port 55555 to the downstream KDE gateway. In the following examples, replace the text in **blue** with the fully qualified host names or IP addresses of the servers in your environment. Replace the text in **red** with the port that your APM server is using for agent communication (443 or 80).

Upstream Gateway (XML example)

```
<?xml version="1.0" encoding="UTF-8"?>
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/"
name="upstream_gw">
  <zone name="trusted">
    <interface name="clientproxy" ipversion="4" role="proxy">
      <bind localport="poolapm" service="apm">
```

```
      <connection remoteport="443">apm-hostname</connection>
    </bind>
    <interface name="downrelay" ipversion="4" role="connect">
     <bind localport="55555">
      upstream-hostname
      <connection remoteport="55555">downstream-hostname</connection>
     </bind>
    </interface>
   </interface>
  </zone>
  <portpool name="poolapm">23000-23999</portpool>
</tep:gateway>
```

Downstream Gateway (XML example)

```
<?xml version="1.0" encoding="UTF-8"?>
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/"
name="downstream_gw">
  <zone name="lessSecure">
   <interface name="uprelay" ipversion="4" role="listen">
    <bind localport="55555">
     downstream-hostname
    </bind>
    <interface name="serverproxy" ipversion="4" role="proxy">
     <bind localport="443" service="apm" />
    </interface>
   </interface>
  </zone>
</tep:gateway>
```

Upstream gateway in less secure zone / downstream gateway in more secure zone

This section provides XML examples for when the upstream KDE gateway is in the less secure network zone and the downstream KDE gateway is in the more secure network zone. For this configuration, the downstream KDE gateway initiates network communication over port 55555 to the upstream KDE gateway.

Upstream Gateway (XML example)

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/"
name="upstream_gw">
  <zone name="lessSecure" maxconn="512" error="ignore">
    <interface name="clientproxy" ipversion="4" role="proxy">
      <bind localport="poolapm" service="apm">
        <connection remoteport="443">apm-hostname</connection>
      </bind>
      <interface name="downrelay" ipversion="4" role="listen">
        <bind localport="55555">upstream-hostname</bind>
      </interface>
    </interface>
  </zone>
  <portpool name="poolapm">23000-23999</portpool>
</tep:gateway>
```

Downstream Gateway (XML example)

```
<?xml version="1.0" encoding="UTF-8"?>
<tep:gateway xmlns:tep="http://xml.schemas.ibm.com/tivoli/tep/kde/"
name="downstream_gw">
  <zone name="moreSecure" maxconn="512" error="ignore">
    <interface name="uprelay" ipversion="4" role="connect">
      <bind localport="55555">downstream-hostname
        <connection remoteport="55555">upstream-hostname</connection>
      </bind>
      <interface name="serverproxy" ipversion="4" role="proxy">
        <bind localport="443" service="apm"/>
      </interface>
    </interface>
  </zone>
</tep:gateway>
```

Note: in the above configuration examples, port 55555 is used by KDE gateway (upstream and downstream) to establish a connection and to transfer APM agent data to the APM server. The APM server is listening on port 443. Traffic flows from the agent to the downstream KDE on port 443 (or 80). Then, it flows over the existing KDE gateway connection from the downstream gateway to the upstream gateway. Finally, the traffic flows from the upstream gateway to the APM server on port 443 (or 80).

Note: You can set up the KDE gateway for multiple firewall hops. This documentation does not attempt to document all of the possible configurations. The IBM Tivoli Monitoring v6 documentation has examples of multi-hop configurations.