

Chapter 3



Configuration and Operations

3.1 Overview

This document provides step-by-step instructions on how to configure and run NetVigil on your production environment. It is assumed that the software package has been extracted and installed into a specific directory on your server(s) as described in Chapter 2, “Installation and Upgrade Guide”. In this document, `NETVIGIL_HOME` refers to the top level directory where the package has been extracted and will be running from.

3.2 Installing A New License Key

NetVigil components rely on a license key to indicate which features are available, and also to impose time restrictions (if any) on when the application “expires”. It may be necessary to install a new license key, for example, when a permanent license key is provided by Fidelia at the end of a trial period, or when the key format changes between different versions of the application. Once a new key has been delivered, here are the steps you need to take to install the new key:

□ To install a new license key:

1. Save/copy the downloaded file as `NETVIGIL_HOME/etc/licenseKey.xml`. On Linux/Solaris platforms this is `/usr/local/netvigil` by default, and on Windows platforms this directory is `\Program Files\Fidelia NetVigil`.
2. Make sure to replace the contents of the existing `licenseKey.xml` with this new file.

3. Restart NetVigil using `NETVIGIL_HOME/etc/netvigil.init` restart on Linux/Solaris platforms, or Start | Programs | Fidelia NetVigil | Start Fidelia NetVigil on Windows platforms.

3.3 Starting/Stopping NetVigil

On Linux/Solaris platforms, different components of NetVigil are started and stopped using the `NETVIGIL_HOME/etc/netvigil.init` script. This script should be called from `/etc/rc.local` or other startup directory appropriate to your operating system with a parameter of `start` so that NetVigil components start automatically when the system reboots. Before the script can be used, you will need to edit the script and uncomment the components you would run on that particular machine. For example, if you are running the web application and DGE monitor components on the same host, `netvigil.init` should be edited like this:

```
PROVDB="N"  
BVEAPI="N"  
WEBAPP="Y"  
MESSAGE="Y"  
DGE="Y"
```

On Windows, various services are created. To start all services at once, select Start | Programs | Fidelia NetVigil | Start Fidelia NetVigil.

To control the startup behavior of individual components, use Service Control Manager which is accessible via Control Panel | Administrative Tools | Services. All the NetVigil service names are prefixed with `NetVigil`. If you wish to have the web application and DGE component to start up when the system reboots, edit the properties of the corresponding service (as well as for NetVigil Provisioning Database and NetVigil Aggregated Database) and set the Startup Type to `Automatic`.

Although under normal circumstances you would run the `netvigil.init` script or menu items from Program Files, each component of NetVigil system has its own startup script in-case you would like to start/stop any of the components individually. These scripts are located under the `NETVIGIL_HOME/etc` directory on

Linux/Solaris platforms. On the Windows platform, use `net start <service_name>` and `net stop <service_name>`. The scripts are named:

Table 3.1

| Script Name | Windows Service | Description |
|--------------|-----------------|-------------------------------------|
| provdb.init | nvprovdb | provisioning server/database (poet) |
| dgedb.init | nvdgedb | DGE/monitor database (mysql) |
| monitor.init | nvmonitor | DGE/monitors |
| webapp.init | nvwebapp | web interface |
| bveapi.init | nvbveapi | BVE API server |

Each of these scripts accepts the parameters `start` and `stop` which will start and stop the respective component.

3.3.1 Starting the system

The provisioning database should always be started first since all other components will request configuration information from the provisioning database. The DGE database and monitors should follow since they will provide information on the status of all configured devices and tests. The web application should be started next. The BVE socket server can be started at any point after the provisioning database has been started. The `netvigil.init` script on Linux/Solaris platforms will take care of maintaining this order.

```
% /etc/init.d/netvigil.init start
```

On Windows platforms, select `Start | Programs | Fidelia NetVigil | Start Fidelia NetVigil` to start the entire application.

3.3.2 Stopping the system

When shutting down the system, the components should be shutdown one by one in the opposite order they were started. On Linux/Solaris:

```
% /etc/init.d/netvigil.init stop
```

and on Windows, `Start | Programs | Fidelia NetVigil | Stop Fidelia NetVigil`.

If you want to stop the components of NetVigil that read configuration files (to re-read these config files), then you can also use

```
% /etc/init.d/netvigil.init stopcore
```

This will not stop the various databases or the messaging bus.

NOTE: *If you have recently stopped the provisioning database, it may take a few seconds until you can start the database again while it shuts down completely. The startup scripts will let you know if the Poet database was unable to start up properly and you should try again after a few seconds.*

3.3.3 Verifying proper operation

On Linux/Solaris platforms, using the `status` parameter with the `netvigil.init` script will display the status of the different components. Example:

```
% ./netvigil.init status
messaging server (openjms) ... running
provisioning database (poet) ... running
bve (socket) server api ... running
dge (monitor) components ... running
dge/jms database (mysql) ... running
application server (tomcat) ... running
virtual frame buffer (xvfb) ... running
```

Alternatively, you can use `status` parameter with other startup scripts to check the status of individual components/software. This option is only available on Linux/Solaris platforms.

On Windows platform, you can check the status of individual components using the Service Control Manager where the Status column should indicate `Started` when a particular component is running. You can also execute `net start | more` from a command prompt to get a list of running services. NetVigil components are prefixed with “NetVigil”.

3.4 Configuration Files

NetVigil system utilizes several configuration files to obtain information about different components and system parameters. Before starting the application, you need to make sure that the default values match your local network and server configurations in the following files:

3.4.1 Application installation path

| Configuration File | Affected Components | Affected Operating Systems |
|--------------------------------|-------------------------------------------------|----------------------------|
| NETVIGIL_HOME/etc/netvigil.env | Provisioning database, Web application, Monitor | Linux, Solaris |

This file contains environment variables that specify the location of different supporting software needed to run NetVigil. `INSTALL_DIR` should be set to the installation directory, `NETVIGIL_HOME` (as described above). All other variables should be left unchanged unless specified otherwise by Fidelia support.

3.4.2 BVE Config Database host/location

| Configuration File | Affected Components | Affected Operating Systems |
|--------------------------------|--------------------------|----------------------------|
| NETVIGIL_HOME/etc/netvigil.xml | Web application, Monitor | Linux, Solaris, Windows |

This file is used by the monitors that are part of the DGE component and web interface to identify the provisioning database. If the DGE or web component is running on the same server as the provisioning database, there is no need to change this file. Otherwise edit the following line:

```
<provisioning
name="provisioning"
host="localhost"
[...]
```

`localhost` should be changed to the fully qualified domain name (fqdn) or ip address of the server where the provisioning database is going to be located. The user and password parameters should not be changed.

3.4.3 Logging configuration

| Configuration File | Affected Components | Affected Operating Systems |
|------------------------------|-------------------------------------------------|----------------------------|
| NETVIGIL_HOME/etc/log4j.conf | Provisioning database, Web application, Monitor | Linux, Solaris, Windows |

Different components of NetVigil provide useful diagnostic and/or informative log messages, and you can control how much information is logged by editing this file. Change `LOGLEVEL` to one of the following to fine tune the level of details you would like:

Table 3.2 Log message detail levels

| LOGLEVEL | Level of Detail |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| INFO | Informational messages that highlight the progress of the application at coarse-grained level |
| WARN | Designates potentially harmful situations |
| ERROR | Designates error events that might still allow the application to continue running |
| FATAL | Designates very severe error events that will presumably lead the application to abort |
| DEBUG | Additional detailed information that is useful for debugging an application. Do not enable debug messages unless asked to do so by Fidelia technical support. |

By default, messages are only logged into NetVigil's own log files stored in the directory specified by `$LOGDIR` variable. If you would like to send the logs to a Unix syslog host, either at a central location, or on same host(s), uncomment the following section:

```
#log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender
#log4j.appender.SYSLOG.SyslogHost = localhost
#log4j.appender.SYSLOG.facility =
org.apache.log4j.net.SyslogAppender.LOG_LOCAL7
```

and change `localhost` to the fqdn or ip address of the host where you want the log messages to be sent. If you would like the messages to be sent as a facility other than `local7`, change `LOG_LOCAL7` to `LOG_<FACILITY>` where `<FACILITY>` is one of the facilities listed in the Unix manual (man5) of `syslogd.conf`. Make sure to enter the facility name in upper case.

3.4.4 Test Definitions & Defaults

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------------|----------------------------------------|----------------------------|
| NETVIGIL_HOME/etc/TestTypes.xml | Provisioning database, Web application | Linux, Solaris, Windows |

This file contains information on default values for thresholds and display properties of various tests. When new tests are being provisioned, or existing test results are being displayed, information in this file dictates how to group similar tests together and what units to use to display test results. The file is in XML format and the format should be strictly maintained while making any changes. This information is used by the provisioning server/webapp when no thresholds have been setup using the admin interface on the web application. Once an admin user has assigned default thresholds for any Department, the information in this file is no longer used for populating default thresholds when tests are created for that particular Department.

Please refer to Chapter 27, “Plugin Monitors” for details of the layout and customizing of this file.

3.4.5 Web application external help

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/tomcat/webapps/ROOT/WEB-INF/web.xml | Web application | Linux, Solaris, Windows |

NetVigil provides an easy way to add escalation information, procedures or any other information related to individual tests, or on a global basis on test type, device, or Department context. Each test item on the web application includes a **HELP** link, which when clicked on, shows any such information. This information is obtained by running an external script. Locate the section containing:

```
<param-name>help.script.path</param-name>
```

This parameter identifies the location of this script. NetVigil includes a default script, located at `NETVIGIL_HOME/Utils/externalTestHelp.pl`, which looks for such information in a directory hierarchy of specific layout.

If you would like to have a different script used for this feature, you can change the `externalTestHelp.pl` script name and path to specify the different script.

For the algorithm that is used to find test-specific information, see Section 12.1, “External Help” on page 163.

3.4.6 Web application external authentication

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/tomcat/webapps/ROOT/WEB-INF/web.xml | Web application | Linux, Solaris, Windows |

The `<param-name>externalLoginKey</param-name>` section is used to configure the shared key for external authentication. NetVigil makes it easy to integrate the web application into an existing web portal or single-login system. Using the external authentication mechanism, you can bypass the initial authentication web page and go directly into the device summary page. This is accomplished by encoding user Department and login information in an md5 hash, using the shared key and passing into the authentication engine of the web application component. See the section “Web Portal Authentication” on page 355 for further details on setting this up.

NOTE: *It is highly recommended that the `<param-value>payday</param-value>` section be edited and the default shared key be changed to something different and secure. A sample CGI script (`NETVIGIL_HOME/utils/externalWebLogin.cgi`) illustrating how to use the external authentication mechanism is provided with NetVigil.*

3.4.7 DGE Identity

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/etc/dge.xml | Monitor | Linux, Solaris, Windows |

The following entry sets the name a DGE identifies itself with against the provisioning database:

```
<dge name="my_dge" user="emerald" password="null"/>
```

The name `my_dge` should be changed to the name of the DGE you have (or are going to) setup. The name does not need to be an fqdn, only something meaningful. However, you will need to use the same name when creating DGE information in the provisioning database using the superuser interface. For example, if you plan to have a DGE with the name "dge01.central" with an fqdn of "dge01.central.mycompany.com", then `my_dge` should be replaced with `dge01.central`, and you must use the same DGE name when you create the DGE using the superuser interface. (For more information on creating DGEs, see Chapter 10, "DGE Management".)

3.4.8 DGE controller port/password

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/etc/dge.xml | Monitor | Linux, Solaris, Windows |

Each DGE process listens on a TCP/IP port for incoming connection requests and provides status on each of the monitors it supports. By default this port is set to 7655, but this can be configured by editing the following section:

```
<controller port="7655" password="fixme"/>
```

If you change the port from 7655 to something different, make sure that no other application running on the machine is going to bind to that port. You should also change the password `fixme` to a different and more secure password. You will use this password to log into the status server.

3.4.9 EDF server port/password

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------|-----------------------------|----------------------------|
| NETVIGIL_HOME/etc/dge.xml | Monitor, External Data Feed | Linux, Solaris, Windows |

Each DGE process listens on a TCP/IP port for incoming connection requests and allows integration with external tools utilizing the External Data Feed API. By default this port is set to 7657, but this can be configured by editing the following section:

```
<edfMonitor>  
<port>7657</port>
```

```
<connections>1</connections>
<timeout>120</timeout>
<userName>edfuser</userName>
<password>fixme</password>
</edfMonitor>
```

If you change the port from 7657 to something different, make sure that no other application running on the machine is going to use that port. You should also change the password `fixme` to a different and more secure password. You will use this password along with the specified user name to log into the EDF server. The `connections` parameter configures the number of concurrent connections to the EDF server that should be allowed. If you expect to run a lot of external monitors that need to insert results into NetVigil, this number should be set to a suitably large number.

3.4.10 E-mail servers

| Configuration File | Affected Components | Affected Operating Systems |
|--------------------------------|------------------------|----------------------------|
| NETVIGIL_HOME/etc/netvigil.xml | Monitor, Report Server | Linux, Solaris, Windows |

The DGE and Report Server components need to know which E-mail server(s) they should use to send notifications or reports via E-mail. Edit the following section:

```
<email-servers>
<host name="my_mail_server" priority="10"/>
</email-servers>
```

Change `my_mail_server` to the fqdn of your local E-mail server or the E-mail server that you use for sending outgoing E-mail. If you have more than one E-mail server, you may add additional servers with a different priority value (the lowest priority server is preferred). You should make sure that the E-mail server(s) is configured properly to allow NetVigil to relay E-mail to any E-mail address. (Please refer to your E-mail server's administration guide for instructions on how to accomplish this). See Chapter 4, "Configuration for Actions & Notifications" for more details.

3.4.11 Web server TCP/IP port

| Configuration File | Affected Components | Affected Operating Systems |
|--------------------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/tomcat/conf/server.xml | Web application | Linux, Solaris, Windows |

This is the configuration file for Jakarta Tomcat application server. By default, NetVigil Web Application will run on TCP port 80. If you already have another web server or another application using that port, you will need to configure the Web Application to run on an alternate port:

1. Edit NETVIGIL_HOME/tomcat/conf/server.xml using a text editor (e.g. vi, wordpad) and locate the following section:

```
<Connector
className="org.apache.coyote.tomcat4.CoyoteConnector" port="80"
minProcessors="20" maxProcessors="80"
```

Change the port 80 to a new unused port. For example, port 8080

2. Edit NETVIGIL_HOME/tomcat/webapps/ROOT/WEB-INF/web.xml and locate the following section:

```
<init-param>
  <param-name>report.server.port</param-name>
  <param-value>80</param-value>
```

Change the port 80 to the same port number used in the previous step

3. Save the file and restart the Web Application (if already running). On Linux/Solaris platform this is accomplished using NETVIGIL_HOME/etc/webapp.init restart.

On Windows platform use the NetVigil Service Controller to restart the web application.

Wait 15-20 seconds for the Web Application to initialize and use your web browser to connect to http://your_netvigil_host:8080/ and you should see the NetVigil login page

3.4.12 Web User Interface Appearance

| Configuration File | Affected Components | Affected Operating Systems |
|---------------------------------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/tomcat/webapps/ROOT/resources/skins | Web application | Linux, Solaris, Windows |

This directory has the HTML stylesheets and the graphics/icons used by each skin. You can edit the stylesheets and change the image files to change the look and feel of the web interface to suit your needs. You can create new directories to create a new skin, and the name of the directory is used as the skin names under `Manage->Prefs` for the users.

3.4.13 Customizing Device Tag Labels

| Configuration File | Affected Components | Affected Operating Systems |
|--------------------------------|---------------------|----------------------------|
| NETVIGIL_HOME/etc/netvigil.xml | Web application | Linux, Solaris, Windows |

NetVigil provides five customizable device tags, which you can define to meet your needs. For example, you can store information about where a device is located (city, state, building, room, rack) or what corporate group it belongs to (payroll, helpdesk, etc.) By default, these attributes are displayed with the labels Custom Attribute 1, Custom Attribute 2, etc. You can change these labels to more meaningful names by editing the following section:

```
<device-tags>
  <tag index="1" description="Custom Attribute 1"/>
  <tag index="2" description="Custom Attribute 2"/>
  <tag index="3" description="Custom Attribute 3"/>
  <tag index="4" description="Custom Attribute 4"/>
  <tag index="5" description="Custom Attribute 5"/>
</device-tags>
```

Replace the `description` parameters with the labels that you want to see in the Web application. For example:

```
<device-tags>
  <tag index="1" description="City"/>
  <tag index="2" description="State"/>
  <tag index="3" description="Building"/>
  <tag index="4" description="Room"/>
  <tag index="5" description="Rack"/>
</device-tags>
```

NOTE: These definitions do not affect the way custom attributes are stored or used. They affect the display labels only for the tags.

3.5 SSL Support on Web Application

Since the NetVigil Web Application is pure HTML based, the GUI component can be accessed using both regular and secure (SSL) HTTP protocol. Use the following steps to setup SSL support in NetVigil (replace NETVIGIL_HOME with the correct installation directory name):

1. The application server (Apache Tomcat) used by NetVigil uses a JKS format keystore. NetVigil by default ships with a keystore with self-signed certificate. If you are not ready to install a valid key yet, you can skip to step 9. Otherwise, first rename or move the existing keystore under `NETVIGIL_HOME/etc/netvigil.keystore`

2. Create a private/public (RSA) key pair using the following command:

```
NETVIGIL_HOME/jdk/bin/keytool -genkey -keyalg RSA -storepass  
changeit -alias tomcat -keystore  
NETVIGIL_HOME/etc/netvigil.keystore
```

3. Answer the questions, making sure to specify the fully-qualified domain name when asked for first/last name. Do not use comma (,) in any of the answers as it will cause problems. When asked for key password for tomcat, press return/enter
4. Generate a Certificate Signing Request (CSR) using the following command:

```
NETVIGIL_HOME/jdk/bin/keytool -certreq -storepass changeit -alias  
tomcat -keystore NETVIGIL_HOME/etc/netvigil.keystore -file  
my_new_key.csr
```

5. You will need to send the CSR (`my_new_key.csr`) to a valid certificate authority (CA) such as Verisign or Thawte. Usually the CA will send you a signed certificate via email. If you are acting as your own CA, the CSR can be signed using OpenSSL or other SSL tools.
6. Save the certificate in `my_new_cert.pem` and make sure that the certificate begins with `-----BEGIN CERTIFICATE-----` and ends with `-----END CERTIFICATE-----`. All other text above/below the specified section should be deleted
7. Import the new certificate into a new keystore using:

```
NETVIGIL_HOME/jdk/bin/keytool -import -v -trustcacerts -alias  
tomcat -storepass changeit -file my_new_cert.pem -keystore  
NETVIGIL_HOME/etc/netvigil.keystore
```

8. When asked “Trust this certificate?”, answer yes and The certificate will be installed into the keystore.

Verify that the certificate has been imported correctly using:

```
NETVIGIL_HOME/jdk/bin/keytool -list -v -storepass changeit -  
keystore NETVIGIL_HOME/etc/netvigil.keystore
```

9. Edit NETVIGIL_HOME/tomcat/conf/server.xml using a text editor (e.g. vi, wordpad) and locate the following section (for NetVigil version 3.4.2 or earlier):

```
<Connector className="org.apache.tomcat.service.PoolTcpConnector">  
<Parameter name="handler"  
value="org.apache.tomcat.service.http.HttpConnectionHandler"/>  
<Parameter name="port" value="443"/>  
<Parameter name="socketFactory"  
value="org.apache.tomcat.net.SSLSocketFactory" />  
<Parameter name="keystore"  
value="NETVIGIL_HOME/etc/netvigil.keystore" />  
<Parameter name="keypass" value="changeit"/>  
</Connector>
```

On NetVigil 3.6 or later, the following section should be located:

```
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"  
port="443" minProcessors="20" maxProcessors="80"  
enableLookups="false" acceptCount="100" debug="0"  
scheme="https" secure="true" useURISValidationHack="false"  
disableUploadTimeout="true">  
  
<Factory  
className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"  
clientAuth="false" protocol="TLS" keystorePass="chageit"  
keystoreFile="/usr/local/netvigil/etc/netvigil.keystore"/>  
</Connector>
```

which should be commented out by default. Remove the comment (<!--
- .. -->) and make sure that the keystore, keypass and port
parameters are set correctly

10. Save the file and restart the Web Application (if already running).

On Linux/Solaris platform this is accomplished using
NETVIGIL_HOME/etc/webapp.init restart. On Windows platform
use Start -> Programs -> Fidelia NetVigil -> Individual Components
-> Stop/Start Web Application

11. Wait 15-30 seconds for the Web Application to initialize and use your
web browser to connect to https://your_netvigil_host/ and you
should see the NetVigil login page

3.6 Operating NetVigil Behind Firewalls

If any component of NetVigil is going to be installed behind a firewall, depending on the existing policies, some changes may be necessary to the rules to accommodate the requirements. In the following requirements, “remote” host implies a host that is outside of the firewall while a “local” host is a device on the secure side of the firewall. Also, note that the requirements are not applicable for cases where the two hosts in question are on the same side of the firewall (i.e. packets are not crossing the firewall).

3.6.1 Requirements for the BVE Provisioning Database

The provisioning server stores all device, test, action, threshold, authentication and other provisioning information. This information is retrieved on-demand by both the web server(s) and DGEs. This is accomplished by creating connections to the database server on specific TCP ports running on the provisioning host. The following firewall rules will need to be applied for a provisioning server which is behind a firewall:

Table 3.3 Firewall rules for a provisioning server that is behind a firewall

| protocol | direction | local port | remote host | remote port | reason |
|----------|-----------|------------|-------------|-------------|----------------------------------------|
| tcp | incoming | 7651 | any | any | NetVigil provisioning database |
| tcp | incoming | 7653 | any | any | NetVigil messaging protocol #1 |
| tcp | incoming | 7654 | any | any | NetVigil messaging protocol #2 |
| tcp | incoming | 7661 | any | any | NetVigil BVE (provisioning) API server |
| udp | incoming | 162 | any | any | snmp traps |
| tcp | outgoing | any | any DGE | 7657 | external data feed API server |

Table 3.3 Firewall rules for a provisioning server that is behind a firewall

| protocol | direction | local port | remote host | remote port | reason |
|----------|-----------|------------|-------------|-------------|---------------------------------|
| tcp | outgoing | any | any DGE | 7659 | input stream monitor |
| udp | outgoing | any | dns servers | 53 | dns queries for name resolution |

3.6.2 Requirements for Web Server(s)

The web server(s) provides an interface for displaying all collected information as well as reports generated from those information. If a location is served by more than one web server, we will be installing a load balancer to distribute the load and the load balancer will need the same firewall rule changes as the web servers themselves. The load balancer might have additional firewall specific requirements. The following firewall rules will need to be applied for web server(s) which is behind a firewall:

Table 3.4 Firewall rules for a web server that is behind a firewall

| protocol | direction | local port | remote host | remote port | reason |
|----------|-----------|------------|-------------|-------------|----------------------------------------|
| tcp | incoming | 80 | any | any | any access to web application |
| tcp | incoming | 443 | any | any | any access to web application over ssl |
| udp | outgoing | any | dns servers | 53 | dns queries for name resolution |

3.6.3 Requirements for DGE (monitors)

The DGEs perform actual monitoring of all provisioned devices and store the data on a local database. The web server(s) will need access to this stored data on-demand for report generation. The provisioning server also needs access to the data to fulfill requests made via the BVE socket API. Since the DGE perform monitoring tasks, it will need

outbound access via a multitude of ports and protocols. The following firewall rules will need to be applied for a DGE server which is behind a firewall:

Table 3.5 Firewall rules for a DGE that is behind a firewall

| protocol | direction | local port | remote host | remote port | reason |
|----------|-----------|------------|------------------|-------------|-----------------------------------------------------------------------------------------|
| tcp | incoming | 7657 | any | any | external data feed API server |
| tcp | outgoing | 7659 | any | any | input stream monitor |
| tcp | incoming | 7663 | web app | any | dge database lookup |
| tcp | incoming | 7655 | any | any | dge status server |
| tcp | outgoing | any | WMI query server | 7667 | dge connection to WMI query server |
| tcp | incoming | 20 | any | any | ftp servers create incoming connection on port 20 in response to connections on port 21 |
| icmp | outgoing | any | any | "echo" | packet loss, round trip time tests |
| udp | outgoing | any | any | 161 | snmp queries |
| udp | outgoing | any | any | 53 | dns queries, tests |
| udp | outgoing | any | any | 123 | ntp service tests |
| udp | outgoing | any | any | 1645 | radius service tests |
| tcp | outgoing | any | any | 21 | ftp service tests |
| tcp | outgoing | any | any | 25 | smtp service tests, alerts via E-mail |
| tcp | outgoing | any | any | 80 | http service tests |
| tcp | outgoing | any | any | 110 | pop3 service tests |

Table 3.5 Firewall rules for a DGE that is behind a firewall

| protocol | direction | local port | remote host | remote port | reason |
|----------|-----------|------------|-------------|-------------|------------------------------------------------------------------------------------------------------|
| tcp | outgoing | any | any | 143 | imap service tests |
| tcp | outgoing | any | any | 389 | ldap service tests |
| tcp | outgoing | any | any | 443 | http over ssl service tests |
| tcp | outgoing | any | any | 993 | pop3 over ssl service tests |
| tcp | outgoing | any | any | 995 | imap over ssl service tests |
| tcp | outgoing | any | windows | 135 | WMI queries to windows hosts being monitored via DCOM. See "Windows monitoring using WMI" on page 74 |

3.7 NetVigil Operation in NAT Networks

NAT (Network Address Translation) devices usually translate connections between a public network and a private address space. There are several issues to consider while monitoring in a NAT network:

NAT Port Translation In this NAT method, one or more public IP address are mapped to one or more private IP addresses by manipulation of the source port. It is difficult to permit an external monitoring server to query an internal host unless such translation is set up.

Firewalls Disable Queries from public network Several NAT and firewall devices (such as the PIX firewall) disable SNMP queries from their public interfaces.

Dynamic NAT For non-server type devices (such as user systems), they usually get a dynamic IP address instead of a fixed address. These devices cannot be queried since the IP address is changing all the time.

NetVigil can be deployed in a NAT environment as long as there is a way to query the device being monitored. If the DGE is co-located near the private LAN, then an ethernet interface from the DGE can be attached to the NAT network directly.

NetVigil can be deployed in an environment with similar private addresses, as long as each of these networks has its own DGE. The provisioning database does NOT reference devices by IP addresses, so many devices can exist in the system with the same IP address. Each device is allocated to a DGE, so as long as the respective DGE can access the private (or NAT) network, the devices on these networks can be monitored by NetVigil.

