QUALYS®
ON DEMAND SECURITY

TECHNICAL BRIEF

Using the QualysGuard® Ticket Notification Engine (TNE) to Integrate with Remedy Ticketing Systems (v1.0)

Overview

There are a myriad of ticket systems available to customers for operational incident management in the enterprise. Many QualysGuard customers have asked for the ability to integrate tickets generated with QualysGuard into their own ticketing and remediation systems. This has many advantages. Operations personnel are able to work through these issues in a system that is familiar to them with specific reporting capabilities that are not possible in the QualysGuard ticketing system.

Qualys provides a Ticket Notification Engine (TNE) that outputs SMTP messages based on XML versions of individual tickets in QualysGuard that are consumable by Remedy ticketing systems. The TNE can also be configured to support some customization to support the receiving ticketing system.

Distributed as RPM installer files, customer companies can use any flavor of Linux or UNIX that supports RPM package manager.

Process

The TNE solution represents a 'one-way' integration with verification. The user, using the remediation workflow feature in QualysGuard, sets the circumstance under which a ticket is created. Once configured, the TNE will retrieve an XML version of each ticket and convert it into an SMTP message and send it to the external ticketing system. Once the issue is resolved and the ticket is closed in the external system, the ticket is not automatically closed in QualysGuard. QualysGuard will close the ticket once the issue is no longer detected on the host e.g. the vulnerability is no longer found on the system.

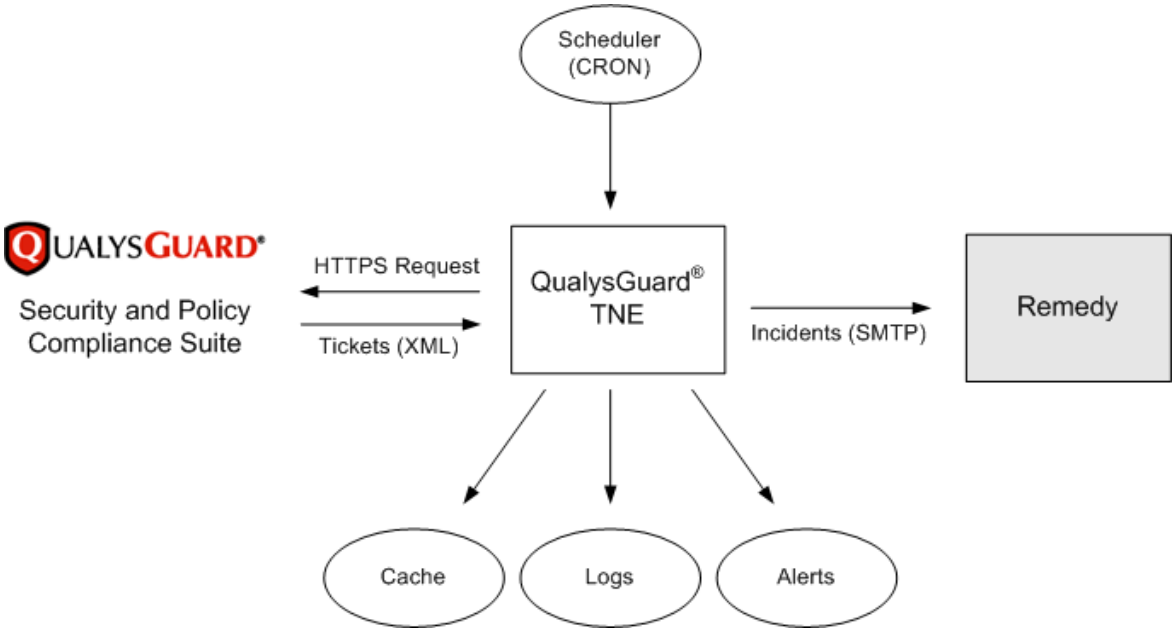
November 23, 2009

TNE Operation Overview

Once configured, the TNE starts and pulls ticket information from QualysGuard using the QualysGuard APIs. The XML data returned is parsed and saved in a local cache based on the severity of the ticket. The criteria used to pull tickets from QualysGuard are defined in the configuration files. The saved data is then processed (tickets with highest severity are processed first) and a ticket is created based on the user defined template format that will be accepted by the ticketing application. This ticket is emailed to the recipient list as defined in the configuration file. Log messages are written to a log file and Alert messages are emailed to the TNE admin user defined in the configuration file. SMTP protocol is used to email the tickets to the mail gateway defined in the configuration file.

TNE keeps track of which tickets have been processed and an email is sent to summarize the number of tickets processed. Processed tickets are deleted from the cache. The rate of tickets to be processed in one hour is configurable. This throttling allows a manageable number of tickets to be sent to the ticketing application. The TNE process can be configured to run on a user-defined frequency using a cron job – anytime, from once an hour to once a day.

TNE will retry and attempt to resend a ticket based on a user-defined number of retries in the configuration file. This will account for any intermittent network and connectivity issues.



Installation (RPM)

Please follow the following steps to install the "rpm" image on your Linux/Unix system. Two set of RPMs need to be installed: 1) the core TNE RPM itself and 2) the configuration setup RPM.

1. Login as root.
   `[command prompt$] su`

2. To carry out a fresh install, install the RPM file.
   `[command prompt$] rpm –i TNE-1.0.rpm`

3. Install the TNE core RPM and perform an upgrade.
   `[command prompt$] rpm -Uvh TNE-1.0.9-1.i386_24.rpm`

4. Run the Perl Module Installer after navigating to the "TNE" installation directory (usually /usr/local/qualys/tne) and "bin" subdirectory. This will ensure that all required libraries and CPAN modules are installed for the software to run properly.

   ```
   [command prompt$] cd /usr/local/qualys/tne/bin
   [command prompt$] perl module_installer.pl
   ```

   Accept the defaults at the prompts during module installations.

Next, install the configuration setup RPM.

5. To install the configuration setup RPM, first copy the RPM to an appropriate directory (same directory the main RPM was installed from). Ensure that you are logged in as root.
   `[command prompt$] rpm –Uvh TNE_CONF_SMTP-1.0.9-1.i386_24.rpm`

6. If you navigate to the installation directory /usr/local/qualys/tne you should see the following 3 directories and QualysGuard_TNE.pdf (this document):
   ```
   [command prompt$] cd /usr/local/qualys/tne
   [command prompt$]ls
   bin  conf  conf_smtp  QualysGuard_TNE.pdf
   ```

7. If the "conf" directory is not present, then create it by copying the directory contents of "conf_smtp" as follows.
   `[command prompt$] cp –R conf_smtp conf`

8. Change ownership to the user that TNE will be run as.
   `chown –R user:group /usr/local/qualys/tne`

9. Follow the instructions given below to setup and configure TNE.

Features

TNE implements the following features:

1. User Configurable Template based ticket sent over SMTP email.
2. A hard limit on the number of tickets that can be sent in a given hour.
3. A soft limit on the number of tickets that TNE can cache locally.
4. Handling higher priority tickets first.
5. Reverse the severity scale of tickets making 1 the highest severity in lieu of QualysGuard's severity scale that uses 5 as the highest.
5. Toggle ON/OFF email notifications to administrators in case of critical exceptions.
6. Test mode to see if the format specified in template file is correct.
7. Toggle ON/OFF statistical data which includes message counts.

Setup

The TNE is configured using two files: tne.conf and tne.tmpl. Samples of each of these two files are already installed as sample.conf and sample.tmpl respectively. Prior to working with these files, it is desireable to make backup copies that can be used if needed.

The tne.conf contains all configuration settings available for the TNE engine. The tne.tmpl file allows you to set up an email template that represents a mock up of the email (subject and email text) that the TNE engine will send to your ticketing system. Please consult your ticketing system's documentation for information about the email format your system will accept. A special section below outlines configuration settings for the TNE.

Editing tne.conf

The tne.conf contains configuration parameters for your TNE integration. Please edit this file to enter the required parameters. TNE requires configuration parameters in the "tne.conf" file.

For your convenience a "sample.conf" is provided as a reference and learning tool. The "sample.conf" shows you some of the minimum configuration parameters that need to be defined. This file includes inline comments to assist you with making entries.

```
### Parameters pertaining to TNE itself.
[TNE]
lock_file=lock_file

### This directory will contain the log files.
### Note: No trailing slash, please.
log_dir=logs
log_file=tne_log.txt

### The directory where tickets will be stored before being sent to
### the ticketing application
### Note: No trailing slash, please.
cache_dir=cache
```

```
### Maximum number of tickets that TNE can send to the ticketing application
### in a given hour.
### If QualysGuard has more than this number of tickets, an admin is alerted.
max_tickets_per_run=5

### Maximum number of tickets that TNE should cache.
### Caveat: This is a soft-limit.
### It's possible that a request to QualysGuard will
### return a number of tickets that exceeds this threshold.
### In this case, all those tickets will be cached,
### and no further tickets will be request from QualysGuard
### until all tickets in cache are sent to the ticketing application.
max_tickets_to_cache=5

### Sleep this many seconds after sending each ticket
sleep_between_sends=2

### When TNE is executed first,
### how many past days of tickets should be retrieved?
# history_days=2
history_days=200

##########################################################

[TEST_TICKETS]
### tickets to test
tickets_to_test=1

### test tickets from
from=mailtest@customer-domain.com

### test tickets to send to
to=sendtest@customer-domain.com

##########################################################

### Parameters that determine how TNE sends email alerts to administrators.

[ADMIN_EMAILS]
# enter 'on' to get email notifications for errors, API failures...
# enter 'off' for not getting notifications
notifications=on

# enter 'on' to get statistical data-Message counts (number of tickets
# successfully processed and number of failures.)
# enter 'off' for not getting data.
statistical_data=on

# Example host=mail.qualys.com
host=mail.customer-domain.com
```

```
# Email address from which TNE's emails should originate.
from=origin@customer-domain.com

# A comma-separated list of email addresses.
# These email addresses will be sent a message in case of exceptions.
admins=admin@customer-domain.com

##################################################################

### Parameters regarding connectivity to QualysGuard.

[QG]
url=https://qualysapi.qualys.com/msp/
# url=https://api1.qa.qualys.com/msp/

username=your_username
password=your_password

timeout=900
max_transmission_attempts=4

### Uncomment and edit the parameters below, to configure a proxy server.
# proxy_url=
# proxy_username=
# proxy_password=

### List schemes separated by colons, as below.
# proxy_schemes=http:ftp


##################################################################

### Parameters for SMTP, an alternative method to send tickets

[SMTP]

### SMTP mail server
# Example: host=mail.qualys.com
host=mail.customer-domain.com

### number of attempts to try connecting to smtp mail server
num_of_attempts=4

### seconds to wait between retries connecting to smtp mail server
sleep_between_sends=4


##################################################################


### Parameters regarding POSTEMSG, a special protocol used to communicate
### with TEC (Tivoli Enterprise Console)
### Not required to be set for SMTP protocol
[POSTEMSG]
```

```
### Location of the POSTEMSG binary file.
postemsg=/usr/local/bin/postemsg

### Name of the POSTEMSG server
postemsg_server=

### Location of the POSTEMSG configuration file
postemsg_conf_file=/usr/local/bin/postemsg.conf

event_source=qualys

##########################################################################

[TEMPLATE]
### location of the template file
file=/usr/local/qualys/tne/conf/tne.tmpl

[CUSTOMER]

### POSTEMSG, SMTP, or OPAL
protocol=SMTP

[CUSTOMER_EMAIL]

# from email address
from=from-cust@customer-domain.com
# to email address
to=recipient@customer-domain.com

[ATTRIBUTES]
# Tickets with certain ticket numbers. Specify one or more ticket numbers and/or
# ranges.Use a dash(-) to separate the ticket range start and end. Multiple
# entries are comma separated.
ticket_numbers=

# Tickets until a certain ticket number. Specify the highest ticket number
# to be selected. Selected tickets will have numbers less than or
# equal to the ticket number specified.
until_ticket_number=

# Tickets with a certain assignee. Specify the user login of an active user account.
ticket_assignee=

# Tickets that are overdue or not overdue. When not specified, overdue and
# non-overdue tickets are selected. Specify 1 to select only overdue tickets.
# Specify 0 to select only tickets that are not overdue.
overdue=

# Tickets that are invalid or valid. When not specified, both valid and invalid
# tickets are selected. Specify 1 to select only invalid tickets. Specify
# 0 to select only valid tickets.
# You can select invalid tickets owned by other users, not yourself.
invalid=
```

```
# Tickets with certain ticket state/status. Specify one or more state/status
# codes. A valid value is OPEN(for state/status OPEN or OPEN?REOPENED),
# RESOLVED (for state Resolved), CLOSED(for state CLOSED/FIXED) or
# IGNORED(for state Closed/Ignored). Multiple entries are comma separated.
# To select ignored vulnerabilities on hosts, specify states=IGNORED.
states=OPEN

# Tickets modified since a certain date/time. Specify a date (required) and
# time (optional) since tickets were modified. Tickets modified on or after
# the date/time are selected.
# The start date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format(UTC/GMT),
# like "2006-01-01" or "2006-05-25T23:12:00Z".
# If this is empty, then the tickets will be from the days ago which is
# specified in history_days in this config file. If history_days is also
# blank, then the tickets are from 1970-01-01.
# At least one of modified_since_datetime or unmodified_since_datetime must be given.
modified_since_datetime=2009-01-30

# Tickets not modified since a certain date/time. Specify a date (required) and
# time (optional) since tickets were not modified. Tickets not modified on or after the
# date/time are selected.
# The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format(UTC/GMT),
# like "2006-01-01" or "2006-05-25T23:12:00Z".
unmodified_since_datetime=

# Tickets on hosts with certain IP addresses. Specify one or more IP
# addresses and /or ranges. Multiple entries are comma separated.
# At least one of ips or asset_groups must be given.
ips=

# Tickets on hosts with IP addresses which are defined in certain asset groups.
# Specify the title of one or more asset groups.
# Multiple asset groups are comma separated.
# The title "All" may be specified to select all IP addresses in the user account
asset_groups=All

# Tickets on hosts that have a DNS hostname which contains a certain
# text string. Specify a text string to be used. This string may include
# a maximum of 100 characters(ascii)
dns_contains=

# Tickets on hosts that have a NetBIOS hostname which contains a certain
# text string. Specify a text string to be used. This string may include
# a maximum of 100 characters(ascii)
netbios_contains=

# Tickets for potential vulnerabilities with certain severity levels.
# Specify one or more severity levels. Multiple levels are comma separated.
potential_vuln_severities=

# Tickets for vulnerabilities with certain QIDs(Qualys IDs). Specify one or more
# QIDs. A maximum of 10 QIDs may be specified. Multiple levels are comma separated.
qids=
```

```
# Tickets for vulnerabilities that have a title which contains a certain text
# string. The vulnerability title is defined in the Knowledgebase. Specify a
# text string.This string may include a maximum of 100 characters(ascii)
vuln_title_contains=

# Tickets for vulnerabilities that have vulnerability details which contains
# a certain text string. Vulnerability details provide descriptions for
# threat, impact, solution and results(scan test results, when available).
# Specify a text string.This string may include a maximum of 100 characters (ascii)
vuln_details_contains=

# Tickets for vulnerabilities that have a vendor reference which contains
# a certain text string. Specify a text string.This string may include a maximum of 100
# characters(ascii)
vendor_ref_contains=
```

Editing tne.tmpl

The tne.tmpl contains the values from your QualysGuard account that make up the ticket content. This file includes default values so you need to edit tne.tmpl only if you want to change the default ticket content.

The ticket values start with $. For example the value of ticket number is $tic_num. If you want this value, just insert in [BODY] section like { $tic_num }. Make sure you include the left and right brackets { }.

If you want the reverse value of QG severity or if you want to call with some other name, it can be done as follows:

```
{ if ($qg_severity == 5) {
    '1';
  }
}
or
{ if ($qg_severity == 5) {
    'blocker';
  }
}
```

Whatever you insert between [SUBJECT] and [BODY] will be taken as subject for your email.

Whatever you insert below [BODY] will be taken as body for your email.

The text above [SUBJECT] is for your reference.

Scheduling the TNE

If running the TNE as part of a Windows image, Windows scheduled tasks tool can be used to set a schedule for retrieving and sending the tickets to your ticketing system.

To schedule a new task, Open Scheduled Tasks, and Double-click Add Scheduled Task. Follow the instructions in the Scheduled Task Wizard.

To open Scheduled Tasks, click Start, click All Programs, point to Accessories, point to System Tools, and then click Scheduled Tasks.

If you want to configure advanced settings for the task, select the Open advanced properties for this task then click Finish check box on the final page of the wizard.

Confirm that the system date and time on your computer are accurate, because Scheduled Tasks relies on this information to run scheduled tasks. To verify or change this information, double-click the time indicator on the taskbar.

If you leave the password blank and you want the task to run when you are logged on, open the task. On the Task tab, select the Run only if logged on check box. The task will run at its scheduled time when the user who created the task is logged on to the computer.

If running the system as part of a Linux image, you can create a Cron job for the TNE.

Example: Insert the following in the crontab to run the tne script at 22:00hrs every day.

```
$crontab -e

00 22 * * * root /usr/bin/perl /usr/local/qualys/tne/bin/tne.pl >>
/usr/local/qualys/tne/bin/logs/output.txt
```

TNE can be executed from the command line:

```
cd /usr/local/qualys/tne/bin/

/usr/bin/perl /usr/local/qualys/tne/bin/tne.pl
```

System Messages

The system can be configured to send error and status messages. These messages will indicate the number of tickets successfully or unsuccessfully processed.

```
From: Bill Smith
Sent: Wednesday, May 21, 2008 3:32 PM
To: Bill Smith; Ann Gho
Subject: TNE Alert!

Tickets successfully processed: 1
Number of failures with messages: 0
==================================
This alert message is auto-generated by the TNE (Ticket Notification Engine)
script.
```

```
From: Bill Smith
Sent: Friday, May 16, 2008 12:21 PM
To: Bill Smith; Ann Gho
Subject: TNE Alert!

ERROR: while getting SMTP connection [Net::SMTP: Bad hostname 'mail.ualys.com']
==================================
This alert message is auto-generated by the TNE (Ticket Notification Engine)
script.
```

Log Messages

Detailed log messages are also saved in /usr/local/qualys/tne/bin/logs/tne_log.txt

These will be useful in debugging any issues.

2008/05/30 10:27:02 7:tne.pl:1230:Unlocked lock file: [lock_file]
2008/05/30 10:29:04 7:tne.pl:1093:Directory already exists: [logs]
2008/05/30 10:29:04 7:tne.pl:1093:Directory already exists: [cache]
2008/05/30 10:29:04 7:tne.pl:1098:Directory already exists: [cache/5]
2008/05/30 10:29:04 7:tne.pl:1098:Directory already exists: [cache/4]
2008/05/30 10:29:04 7:tne.pl:1098:Directory already exists: [cache/3]
2008/05/30 10:29:04 7:tne.pl:1098:Directory already exists: [cache/2]
2008/05/30 10:29:04 7:tne.pl:1098:Directory already exists: [cache/1]
2008/05/30 10:29:04 7:tne.pl:1009:Created necessary directories.
2008/05/30 10:29:04 7:tne.pl:1198:Now attempting to lock [lock_file]
2008/05/30 10:29:04 7:tne.pl:1206:Locked [lock_file]
2008/05/30 10:29:04 7:tne.pl:1015:Read state
2008/05/30 10:29:04 7:tne.pl:1017:Skipping rule map
2008/05/30 10:29:04 7:tne.pl:67:Begin======================
2008/05/30 10:29:04 6:tne.pl:96:ERROR: The cache is configured for a maximum of 5 tickets, and it has 28 tickets.
2008/05/30 10:29:04 6:tne.pl:101:Trying to send some tickets to make room.
2008/05/30 10:29:04 7:tne.pl:1352:Directory: [cache/5]
2008/05/30 10:29:04 7:tne.pl:1367:Opened directory: [cache/5] and read 0 tickets.
2008/05/30 10:29:04 7:tne.pl:105:Sent data for severity level [5]
2008/05/30 10:29:04 6:tne.pl:119:Not enough tickets for severity level [5] were sent to customer to make some room in the cache. Continuing with next severity level.
2008/05/30 10:29:04 6:tne.pl:96:ERROR: The cache is configured for a maximum of 5 tickets, and it has 28 tickets.
2008/05/30 10:29:04 6:tne.pl:101:Trying to send some tickets to make room.
2008/05/30 10:29:04 7:tne.pl:1352:Directory: [cache/4]
2008/05/30 10:29:04 7:tne.pl:1367:Opened directory: [cache/4] and read 0 tickets.
2008/05/30 10:29:04 7:tne.pl:105:Sent data for severity level [4]
2008/05/30 10:29:04 6:tne.pl:119:Not enough tickets for severity level [4] were sent to customer to make some room in the cache. Continuing with next severity level.
2008/05/30 10:29:04 6:tne.pl:96:ERROR: The cache is configured for a maximum of 5 tickets, and it has 28 tickets.
2008/05/30 10:29:04 6:tne.pl:101:Trying to send some tickets to make room.
2008/05/30 10:29:04 7:tne.pl:1352:Directory: [cache/3]
2008/05/30 10:29:04 7:tne.pl:1367:Opened directory: [cache/3] and read 0 tickets.
2008/05/30 10:29:04 7:tne.pl:105:Sent data for severity level [3]
2008/05/30 10:29:04 6:tne.pl:119:Not enough tickets for severity level [3] were sent to customer to make some room in the cache. Continuing with next severity level.
….
….
2008/06/17 17:38:19 7:tne.pl:67:Begin======================
2008/06/17 17:38:19 6:tne.pl:96:ERROR: The cache is configured for a maximum of 5 tickets, and it has 189 tickets.
2008/06/17 17:38:19 6:tne.pl:101:Trying to send some tickets to make room.
2008/06/17 17:38:19 7:tne.pl:1380:Directory: [cache/5]
2008/06/17 17:38:19 7:tne.pl:1395:Opened directory: [cache/5] and read 189 tickets.
2008/06/17 17:38:19 7:tne.pl:477:Processing file: [cache/5/1212883965_72433]
2008/06/17 17:38:19 7:tne.pl:478:tickets_sent_this_hour=[0]
2008/06/17 17:38:19 7:tne.pl:479:max_tickets_per_run=[1]
2008/06/17 17:38:19 6:tne.pl:492:tickets_sent_this_hour=[0]
2008/06/17 17:38:26 6:tne.pl:428:url=[https://qualysapi.qualys.com/msp/asset_range_info.php?target_ips=10.10.25.130]
2008/06/17 17:38:26 7:tne.pl:432:Successfully retrieved HTML response
2008/06/17 17:38:26 7:parser.pl:19:Parsing data for qg_service_name=[asset_range_info.php]
2008/06/17 17:38:26 7:parser.pl:264:LAST_LOGGED_ON_USER=[Administrator]
2008/06/17 17:38:28 7:tne.pl:794:Parsed XML from asset_range_info.php

```
2008/06/17 17:38:28 7:tne.pl:524:$protocol=[SMTP]
2008/06/17 17:38:28 7:tne.pl:720:from email is [tne@qualys.com]
2008/06/17 17:38:28 7:tne.pl:739:recipents is [Sending email to the following: [bsmith@qualys.com]]
2008/06/17 17:38:30 6:tne.pl:538:$successful_transmission=[1]
2008/06/17 17:38:30 7:tne.pl:548:Transmission success=[1]
2008/06/17 17:38:30 7:tne.pl:575:Deleted [cache/5/1212883965_72433]
2008/06/17 17:38:30 7:tne.pl:576:BEFORE tickets_in_cache=[189]
2008/06/17 17:38:30 7:tne.pl:581:AFTER tickets_in_cache=[188]
2008/06/17 17:38:30 7:tne.pl:477:Processing file: [cache/5/1212883965_72435]
2008/06/17 17:38:30 7:tne.pl:478:tickets_sent_this_hour=[1]
2008/06/17 17:38:30 7:tne.pl:479:max_tickets_per_run=[1]
2008/06/17 17:38:30 4:tne.pl:485:ERROR: Reached maximum number of tickets to send this hour.
2008/06/17 17:38:30 4:tne.pl:108:Reached max_tickets_per_run limit.
2008/06/17 17:38:30 3:tne.pl:225:Tickets successfully processed: 1
 Number of failures with messages: 0

2008/06/17 17:38:30 7:tne.pl:331:ADMIN_EMAILS.host=[mail.qualys.com]
2008/06/17 17:38:30 7:tne.pl:345:$smtp is defined
2008/06/17 17:38:30 7:tne.pl:355:Sending email to the following: [bsmith@qualys.com]
2008/06/17 17:38:30 7:tne.pl:69:End=========================
```