SEW

TASK 02 Rock the net

Ahmed Aly Helmut Brunner Stefan Pitirut

October 10, 2014

5AHITT

Contents

1 Task **3**
- 1.0.1 Basic tasks . . . 3
- 1.0.2 Advanced tasks (obligatory for grades better than C) . . . 3

2 Design concept **5**

3 User Stories **6**

4 Libraries **7**

5 Diagrams **8**
- 5.0.3 Policy Design . . . 8
- 5.0.4 UML Class Diagram . . . 8

6 Time Estimation **10**

7 Technical Description **12**

8 Results and Defeats **13**

9 Testreview **14**
- 9.0.5 Main Unittest list . . . 14
- 9.0.6 Systemtest . . . 14

10 Sources **15**

1 Task

1.0.1 Basic tasks

Implement a simple-to-use application to monitor and configure a hardware firewall appliance "Juniper NetScreen 5GT ". The firewall allows read access over the SNMP-protocol (your app should be able to test if SNMPv3 is available and if not fallback on SNMPv2c) and write access over Telnet.

Your app should accomplish following tasks:

- List all configured firewall rules (policies) on the device, add the details of the mentioned services and zones as well.
- Allow refreshing of the list by clicking a button and by a configurable time-intervall. Your GUI should remain responsive even with short refresh-intervals!
- Visualize the thru-put for a highlighted firewall-rule (nice2have: multiple rows) in a line-chart (configurable refresh-interval, unit bytes/sec)
- Encapsulate the data retrieval for further reuse and easy expansion. An UML-model of your design will help you defend it at the review!
- Build a visual appealing and easy to use interface (there is more than Swing out there).

1.0.2 Advanced tasks (obligatory for grades better than C)

Additionally to the basic tasks your app should accomplish the following:

- Alarm the user visually and per email if the config of the firewall-rules changes. To avoid polling use the SNMP-trap mechanism.
- Allow managing of firewall-rules (CRUD). To accomplish this, you will have to send configuration commands via telnet or ssh. An admin-account is available per request.
- Use multicast-groups to build a simple transaction system to serialize administrative tasks on the firewall (for example pass an "admin token" to recognize the collaborator who is allowed to write to the firewall). This should also work in a heterogenous environment (different implementations, different OSes), so you have to coordinate with other teams.

- Make sure, that your interface to the firewall allows an easy change of the firewall-model (new releases, manufacturer, ...). It is not necessary to make this configurable in the GUI but must (explicitly) be considered in your software-design!

2 Design concept

SNMP Package: The SNMP package has an OIDDecoder, which defines the Standard OID's in static final variables. The OIDDecoder is now deprecated, because it is not dynamic. The OID will be handelt with a new library Mibble, which will make it possible to load mib files and map them.

The Factory pattern is used here to allow the class SNMPManager to use the right SNMP version. This pattern also allows the developer to add to SNMP version, if there are any new ones coming.
The SNMP Manager sends a package with a specific OID and returns the receive message. This Class will be used as a Connector and a Receiver, which will be called by a command class.

Command pattern: A command pattern is used to create specific actions, which can any connectors like SNMP, SSH or Telnet.

Naturally there will be self written exceptions, which will be in the exceptions package.

The Unit and GUI tests will be in a own test package.

3 User Stories

As a user, I want to visually see the thru-put in bytes/sec as a chart on my Graphical User Interface.

As a user, I want to set the refresh-timer for the visualized thru-put on my Graphical User Interface.

As a user, I want to manually refresh the visualization for the thru-put on the Graphical User Interface.

As a user, I want to see the rules/zones/services of the firewall listed on the Graphical User Interface.

As a user, I want set the refresh-timer for the listing of the rules/zones/services of the firewall on the Graphical User Interface.

As a user, I want to manually refresh the listing of the rules/zones/services of the firewall on the Graphical User Interface.

As a user, I want to configure the application threw the Graphical User Interface.

4 Libraries

The required libraries will be:

- SNMP4J
- LOG4J
- JUNIT
- Mockito
- Java Secure Channel (JSCH) |SSH|
- JFreeSVG (charts)
- JavaFX
- Mibble

5 Diagrams

5.0.3 Policy Design

The policy date will be shown in a table, which consists of 9 Elements.

The table header would look like this:
policyId | policyName | policyServiceName | policySrcZone | policyDestZone | policySrcAddr | policyDestAddr | policyAction | policyStatus

OIDs:

policyId	.1.3.6.1.4.1.3224.10.1.1.1	branch
policyName	.1.3.6.1.4.1.3224.10.1.1.24	branch
policyServiceName	.1.3.6.1.4.1.3224.10.1.1.25	branch
policySrcZone	.1.3.6.1.4.1.3224.10.1.1.3	branch
policyDestZon	.1.3.6.1.4.1.3224.10.1.1.4	branch
policySrcAddr	.1.3.6.1.4.1.3224.10.1.1.5	branch
policyDestAddr	.1.3.6.1.4.1.3224.10.1.1.6	branch
policyAction	.1.3.6.1.4.1.3224.10.1.1.8	branch
policyStatus	.1.3.6.1.4.1.3224.10.1.1.23	branch

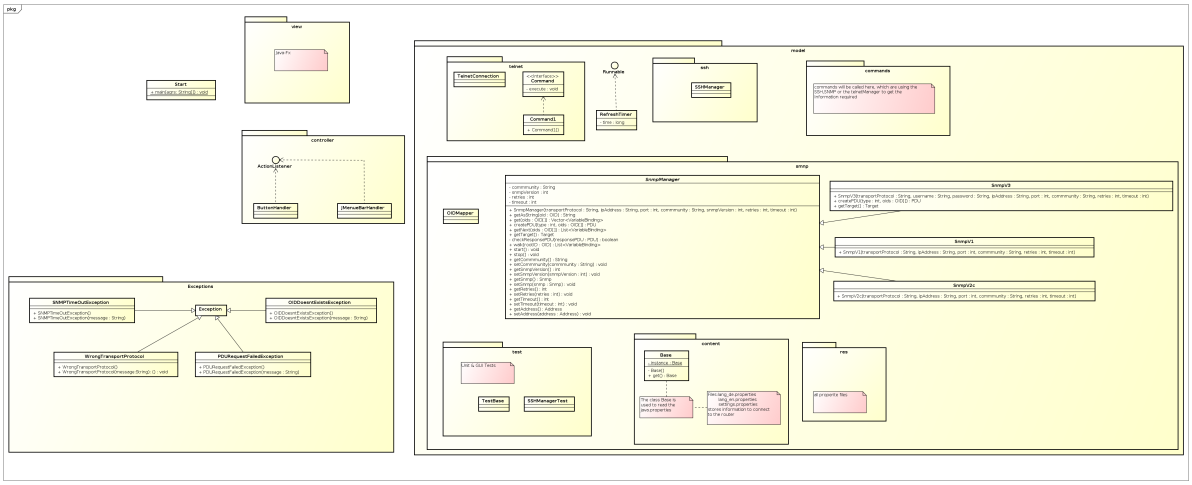
The next step is to draw a chart with the thru-put of the firewall-rule in a line-chart, which is possible with the value policyBps.

OID:

policyBps	.1.3.6.1.4.1.3224.10.2.1.6	branch

5.0.4 UML Class Diagram

Figure 5.1: UMLClass Diagram



6 Time Estimation

Packages	Time needed	Time Estimated	Description	Date	Teammember
Kick-off Meeting	null	00:40h	Start of the Design-concept	18.09.2014	All
Libraries research	01:30h	01:00h	looking for libraries	19.09.2014	ALY Ahmed
SNMP research	04:00h	02:00h		20.09.2014	ALY Ahmed
Prototype SNMP client	02:00h	02:00h		21.09.2014	ALY Ahmed
Start of the Designconcept	00:45h	01:00h		22.09.2014	All
GUI Design	00:45h	01:00h		22.09.2014	All
SMNP comandline tool, tests	01:00h	null		20.09.2014	Helmut Brunner
desgin, concept	02:00h	null		22.09.2014	Helmut Brunner
desgin improved	02:00h	null		23.09.2014	Helmut Brunner
MIB browser, OID executed	02:00h	null		24.09.2014	Helmut Brunner
reading up on mibbrowser and snmp	01:00h	02:00h		19.09.2014	Stefan Pitirut
creating a concept and a slight design	02:00h	03:00h		22.09.2014	Stefan Pitirut
further work for the design, commands for snmp	02:00h	01:00h		23.09.2014	Stefan Pitirut
working with mibbrowser, userstories	02:00h	03:00h		24.09.2014	Stefan Pitirut
SSH Manager + tests	02:30h	01:00h		28.09.2014	ALY Ahmed

OID Decoder	00:30h	00:30h		27.09.2014	ALY Ahmed
policy table	04:30h	06:00h	research what each value means and the return value	25.09.2014	ALY Ahmed
policy tests in mibbrowser	00:30h	02:00h		25.09.2014	ALY Ahmed
FX evaluation	03:00h	03:30h		25.09.2014	Stefan Pitirut
Implementing FX	01:00h	04:00h		29.09.2014	Stefan Pitirut
SNMP Manager	06:00h	02:00h		05.10.2014	Ahmed ALY
Properties & Tests	03:00h	02:00h		05.10.2014	Helmut Brunner
UML	01:00h	00:30h		07.10.2014	Helmut Brunner
GUI	?	?		?	Stefan Pitirut
Total	35:30h	33:30h	null	02.10.2014	—-

7 Technical Description

8 Results and Defeats

9 Testreview

9.0.5 Main Unittest list

coming soon

9.0.6 Systemtest

10 Sources

http://sourceforge.net/p/devmon/mailman/message/20347524/ http://www.oidview.com/mibs/3224/POLICY-MIB.html http://www.circitor.fr/Mibs/Html/NETSCREEN-POLICY-MIB.php