AUTOMATED FIREWALL RULE SET GENERATION THROUGH PASSIVE TRAFFIC INSPECTION

Rhodes University
Where leaders learn

Georg-Christian Pranschke
g05p3292@campus.ru.ac.za

Barry Irwin
b.irwin@ru.ac.za

SNRG
Security and Networks Research Group

Department of Computer Science
Rhodes University

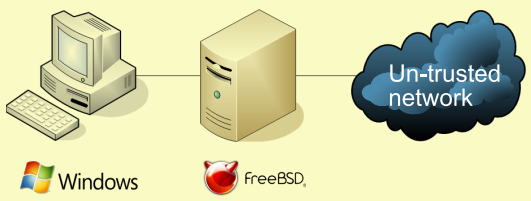
Project Objective:

Introducing firewalls and other choke point controls in existing networks is often problematic, because in the majority of cases there is already production traffic in place that cannot be interupted. This often necessitates the time consuming manual analysis of network traffic in order to ensure that when a new system is installed, there is no disruption to legitimate flows.

An added complication, that is often the case with legacies or other systems that have developed organically, is that documentation about existing legitimate communication may be very limited, or in some cases is incorrect.

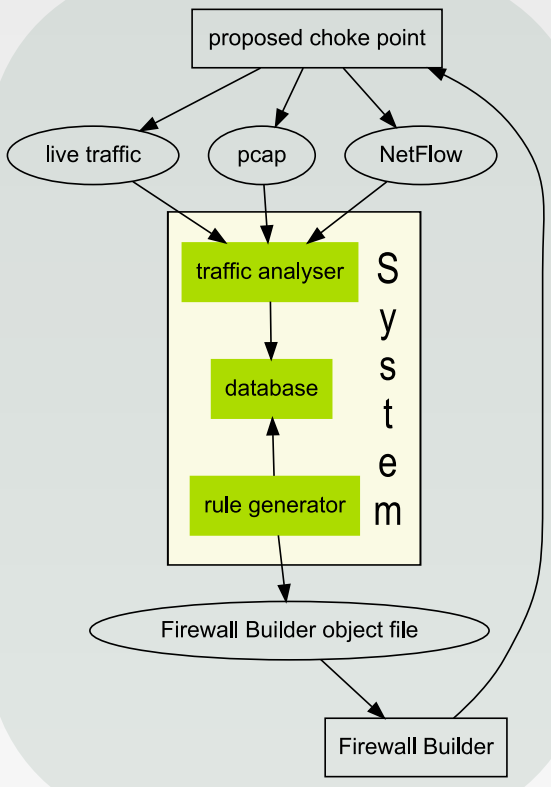
Furthermore ever increasing traffic volumes make manual traffic analysis less feasible.

1 Suppose the FreeBSD machine is to be configured as a choke point control.



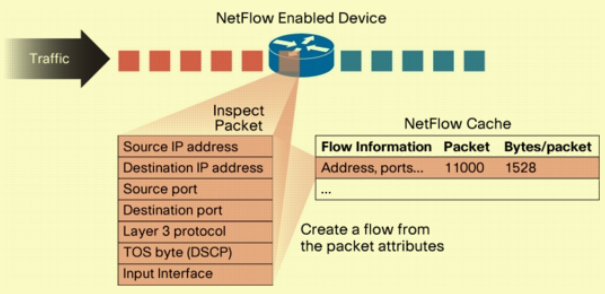
2 Live traffic at the node or trace files in pcap or NetFlow format, recorded at the node, are fed into the system.

These inputs are then converted into a custom flow format featuring various metrics such as traffic volume, packet count and flow duration.



3 The system consists of two components:

A traffic analyser that records the observed traffic flows and stores them in a database...



and a GUI-based rule generator that uses the information in the database to propose a set of rules that match the observed traffic. These rules are consequently reviewed and refined by the user.

This distributed design allows the traffic analyser to run on systems without windowing capabilities such as rack-mounted webservers.

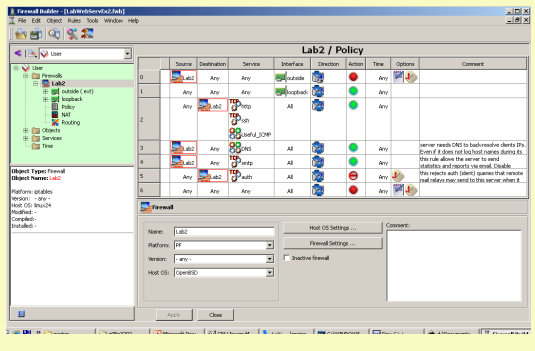
4 The rule generator outputs a FirewallBuilder network object file in XML format.

```
- <Management address="192.168.1.10">
    <SNMPManagement enabled="False" snmp_read_community="" snmp_write_community="" />
    <FWBDManagement enabled="False" identity="" port="-1" />
    <PolicyInstallScript arguments="" command="" enabled="False" />
  </Management>
- <FirewallOptions>
    <Option name="accept_established">true</Option>
    <Option name="accept_new_tcp_with_no_syn">true</Option>
    <Option name="action_on_reject" />
    <Option name="add_check_state_rule">true</Option>
    <Option name="bridging_fw">False</Option>
    <Option name="check_shading">true</Option>
    <Option name="cmdline" />
    <Option name="compiler" />
    <Option name="configure_interfaces">true</Option>
    <Option name="debug">False</Option>
```

5

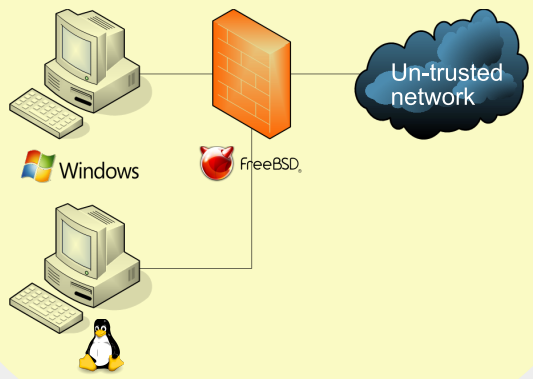
FirewallBuilder acts as the backend of the system.
It uses the file generated by the rule generator to create a rule set for the targeted firewalling solution and is also capable of deploying and maintaining the firewall at the target machine.

By utilising FirewallBuilder as a backend the system is able to support a wide range of firewalling solutions.



6 The firewall is now configured and can be maintained from within FirewallBuilder.

Target firewalling solutions include Cisco PIX/ASA, iptables, ipfilter, ipfw and pf.



sponsored by
COMVERSE
STORTECH
For Your Information
amatole
telecommunication services
Telkom
THRIP
TECHNOLOGY AND HUMAN RESOURCES FOR INDUSTRY PROGRAMME
Bright Ideas 39
Projects
tellabs