Generic Firewall Rule Compiler and Modeller

Christopher Geeringh - BSc (Hons) Network Computing.
Matriculation No.: 05001842
Submission Date: 9 May 2007
Project Supervisor: Professor William J. Buchanan
Second Marker: Andrew Cumming

Introduction

The firewall is the first line of defence to a network, and controls the flow of traffic entering and exiting network boundaries. However, this commonly deployed device frequently exhibits configuration errors, which are unknown to the administrator (Wool, 2004). These errors can cause unexpected traffic behaviour within a network.

The aim of this project is to investigate work in the field of firewall modelling, and develop a system which can effectively model firewall policies. Through investigation of existing work, policy anomaly definitions allow for the creation of anomaly discovery algorithms, to find configuration errors in an automated manner. Furthermore A novel approach to firewall rule management is taken, with the concept of rule crunching. The system will provide a complete and novel approach to firewall modelling and management for network and security administrators.

Rule Anomalies

Anomaly discovery is an integral part of policy optimisation. Research indicates that policy violations occur in all organisation firewalls (Wool, 2004).
Policy violations are determined by investigating the relationship between all rules within a firewall policy.

Shadowing Anomaly

```
1.   tcp 192.168.0.0/24 any 10.100.100.100 80 deny
...
...
...
10.  tcp  192.168.0.30 any 10.100.100.100 80 accept
```

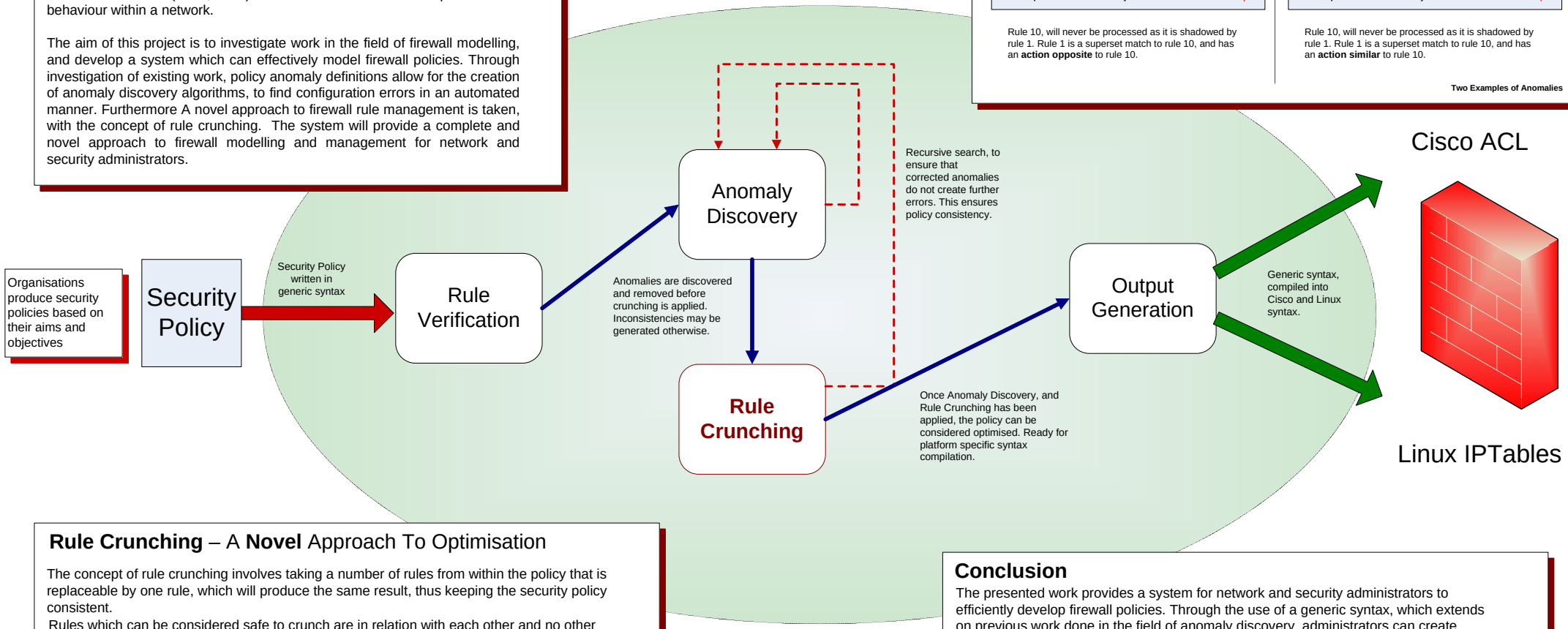
Rule 10, will never be processed as it is shadowed by rule 1. Rule 1 is a superset match to rule 10, and has an **action opposite** to rule 10.

Redundancy Anomaly

```
1.   tcp 192.168.0.0/24 any 10.100.100.100 80 accept
...
...
...
10.  tcp  192.168.0.30 any 10.100.100.100 80 accept
```

Rule 10, will never be processed as it is shadowed by rule 1. Rule 1 is a superset match to rule 10, and has an **action similar** to rule 10.

Two Examples of Anomalies



Rule Crunching – A **Novel** Approach To Optimisation

The concept of rule crunching involves taking a number of rules from within the policy that is replaceable by one rule, which will produce the same result, thus keeping the security policy consistent.
Rules which can be considered safe to crunch are in relation with each other and no other rules within the policy, this ensures consistency between a policy which has not been crunched and one which has.

In the example shown, it can be seen that the three rules can be crunched into a single rule. However, the resulting rule applies to **192.168.0.4,** thus loosing some accountability.

```
1.  tcp 192.168.0.5 any 123.100.100.100 80 deny
2.  tcp 192.168.0.6 any 123.100.100.100 80 deny
3.  tcp 192.168.0.7 any 123.100.100.100 80 deny
```

```
tcp 192.168.0.4/29 any 123.100.100.100 80 deny
```

Conclusion

The presented work provides a system for network and security administrators to efficiently develop firewall policies. Through the use of a generic syntax, which extends on previous work done in the field of anomaly discovery, administrators can create policies without needing a working knowledge of the vendor specific hardware (Al-Shaer et al. 2004, Cadwell et al. 2004).

Rule crunching presents an **novel** approach to rule set optimisation and improved manageability. Furthermore, the presented system allows for an automated method of anomaly discovery, and rectification.