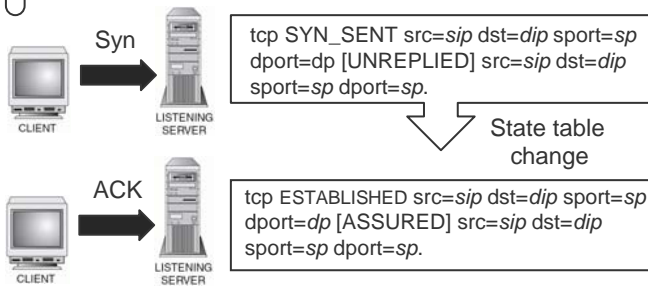


Stateful firewall

- Handle more protocols than stateless firewalls.
- More secure than stateless firewalls.
- Connection tracking and stateful rules.

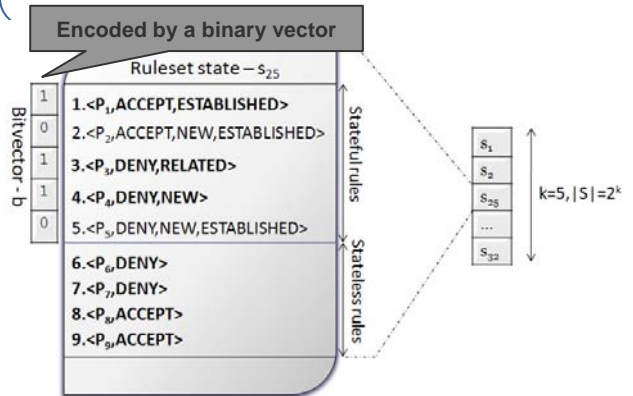
Ruleset

```
1. iptables -A OUTPUT -p tcp -m state --state NEW,ESTABLISHED -j ACCEPT;
2. iptables -A INPUT -p tcp -m state --state ESTABLISHED -j ACCEPT;
```



Definition and model of state

The state of a firewall includes all the static firewall rules and those stateful rules that have an associated entry in the connection-tracking table.



Problems

Inconsistencies can be found in a ruleset of many firewalls.

Shadowing (r2 is shadowed by r1)

Generalization (r4 is a generalization of r2)

Correlation (r1 and r3 are correlated)

1.	udp	any	192.168.1.0/24	accept
2.	udp	172.16.1.0/24	192.168.1.0/24	deny
3.	udp	10.1.1.0/24	192.168.0.0/16	deny
4.	udp	172.16.1.0/24	any	accept

Shadowing is an error: Rule 1 can accept malicious traffic that Rule 2 intends to drop.

Definition of Security

Definition: A stateful firewall is said to be free from inconsistencies if it is free from inconsistencies in all possible states of a firewall.

Results

Consistency verification of stateful firewalls is not harder than the stateless case !!!

1. **Theorem:** Let S be the state that contains all dynamic rules of the rule set. If no inconsistencies exist in state S , then all states are free from inconsistencies, and hence, the firewall configuration is correct.

2. **Verification tool:**

- Verified the firewall of our labour.
- Effective and efficient.

Motivation and Goal

- Verification methods for finding inconsistencies are proposed for *only* stateless firewalls so far.
- Stateful firewalls are more broadly used than stateless firewalls.

Goal: Inconsistency verification of stateful firewalls.

Challenges

- How to model states, define misconfigurations and security in case of stateful firewalls?
- There can be large number of states to be checked in stateful firewalls (exponential to number of rules).
- Manually checking for inconsistencies is error-prone in large ruleset.

