
Firewall Configuration Management

Course: CS6315 Mobile Systems Security
Lecturer: Simon Foley

William Fitzgerald

Cork Constraint Computation Centre,
Department of Computer Science,
University College Cork,
Ireland.

Web: www.williamfitzgerald.net

Email: wfitzgerald@4c.ucc.ie

February, 2010

Definitions: Network Security Policy and Firewall Configuration

- ▷ Recap
- Configuration
- Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- Inter-Conflicts
- Summary

- A network security policy describes an organisation's network security concerns when providing access internally and externally to its network resources.
- A firewall configuration implements a network security policy and is defined by a sequence of firewall rules against which all packets traversing the firewall are filtered.
- Firewall rules are order dependent.

Firewall Configuration Management

- Recap
 - Configuration
 - ▷ Complexity
 - Configuration
 - Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
 - Summary

Implementing a firewall configuration involves either:

- the use of a graphical user interface (GUI) or
- writing low-level command syntax (CLI).

Configuring a firewall is complex and error prone. Examples of such errors are:

- Invalid syntax.
- Inappropriate rule ordering.
- Poor comprehension of a configuration.

Implementation via a Graphical User Interface

- Recap
 - Configuration
 - ▷ Complexity
 - Configuration
 - Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
 - Summary

A commonly used approach amongst novice administrators. However, it is not without its shortcomings.

- Lack of granularity: there are options that cannot be easily configured using a GUI.
- Comprehension issues: a single rule tends to be divided into its constituent filtering components accross several GUI tabs.

Example: DD-WRT GUI Firewall Access Control

Recap
 Configuration
▷ Complexity
 Configuration
 Conflicts
 Intra-Conflicts
 Inter-Conflicts
 Summary

The screenshot shows the DD-WRT GUI with the 'Security' tab selected. The 'Firewall' sub-tab is active. The 'Security' section is expanded to show 'Firewall Protection', where 'SPI Firewall' is enabled. Under 'Additional Filters', 'Filter Proxy', 'Filter Cookies', 'Filter Java Applets', and 'Filter ActiveX' are all disabled. Under 'Block WAN Requests', 'Block Anonymous WAN Requests (ping)', 'Filter Multicast', and 'Filter IDENT (Port 113)' are checked, while 'Filter WAN NAT Redirection' is unchecked.

Setup Wireless Services **Security** Access Restrictions NAT / QoS Administration

Firewall VPN

Security

Firewall Protection

SPI Firewall Enable Disable

Additional Filters

Filter Proxy

Filter Cookies

Filter Java Applets

Filter ActiveX

Block WAN Requests

Block Anonymous WAN Requests (ping)

Filter Multicast

Filter WAN NAT Redirection

Filter IDENT (Port 113)

Example: DD-WRT GUI Firewall Access Control

- Recap
 - Configuration
 - ▷ Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- Inter-Conflicts
- Summary

The screenshot shows the DD-WRT control panel interface. At the top, the logo 'dd-wrt.com' and 'control panel' are visible. The top right corner displays system information: 'Firmware: DD-WRT v24-sp1 (07/26/08) std', 'Time: 19:28:54 up 14:28, load average: 0.25, 0.12, 0.04', and 'WAN IP: 192.168.1.2'. The navigation menu includes 'Setup', 'Wireless', 'Services', 'Security', 'Access Restrictions', 'NAT / QoS', 'Administration', and 'Status'. The 'NAT / QoS' menu is expanded to show 'Port Forwarding', 'Port Range Forwarding', 'Port Triggering', 'UPnP', 'DMZ', and 'QoS'. The 'Port Forwarding' sub-menu is selected, showing a 'Port Forward' section with a 'Help' link and a 'more...' link. Below this is a 'Forwards' table with columns for 'Application', 'Port from', 'Protocol', 'IP Address', 'Port to', and 'Enable'. The table currently contains a single entry: '- None -'. There are 'Add' and 'Remove' buttons below the table. At the bottom of the page are 'Save', 'Apply Settings', and 'Cancel Changes' buttons. A help text box on the right explains that certain applications may require open ports and provides instructions on how to configure port forwarding.

dd-wrt.com ... control panel

Firmware: DD-WRT v24-sp1 (07/26/08) std
Time: 19:28:54 up 14:28, load average: 0.25, 0.12, 0.04
WAN IP: 192.168.1.2

Setup Wireless Services Security Access Restrictions **NAT / QoS** Administration Status

Port Forwarding Port Range Forwarding Port Triggering UPnP DMZ QoS

Port Forward Help more...

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable
- None -					

Add Remove

Save Apply Settings Cancel Changes

Port Forward:
Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the *Enable* checkbox after you are finished.

Example: DD-WRT GUI Firewall Access Control

Recap

- Configuration
- ▷ Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- Inter-Conflicts
- Summary

The screenshot shows the DD-WRT GUI configuration page for Firewall Access Control. The navigation tabs at the top are Setup, Wireless, Services, Security, Access Restrictions (selected), NAT / QoS, and Administration. The main heading is WAN Access. The configuration is divided into several sections:

- Access Policy:** Shows 1 policy. Status is set to Disable. Policy Name is empty. PCs are set to Filter. A description reads: "Internet access during selected days and hours."
- Days:** A row of checkboxes for days of the week. "Everyday" is checked, while Sun, Mon, Tue, Wed, Thu, Fri, and Sat are unchecked.
- Times:** The "24 Hours" option is selected. The "From" time is set to 0:00 and "To" is set to 0:00.
- Blocked Services:** A checkbox for "Catch all P2P Protocols" is unchecked. Below are four rows, each with a "None" dropdown menu and two empty input fields.
- Website Blocking by URL Address:** Two empty input fields are provided.

Implementation via a Command Line Interface

- Recap
 - Configuration
 - ▷ Complexity
 - Configuration Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
 - Summary

This is an approach used by experienced administrators as it provides fine-grained access control.

However . . .

- Hard to comprehend.
- Easy to make a mistake (syntax or otherwise).
- Enterprise firewall configuration may contain 1000's of rules!

Example: iptables CLI Firewall Access Control

- Recap
 - Configuration
 - ▷ Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- Inter-Conflicts
- Summary

Fragment of stateless filtering of TCP protocol communication.

```
ipt="/sbin/iptables"
$ipt -N HTTP
$ipt -N HTTP-FIN
$ipt -N HTTP-FIN-1
$ipt -N HTTP-FIN-2
$ipt -A INPUT -p tcp -dport 80 -j HTTP
$ipt -A HTTP-FIN -p tcp -m recent --name HTTP-LIST -j HTTP-FIN-1
$ipt -A HTTP-FIN -p tcp -m recent --name HTTP-FINAL -j HTTP-FIN-2
$ipt -A HTTP-FIN-1 -p tcp --tcp-flags SYN,ACK,FIN FIN,ACK -m recent --name HTTP-LIST --close -j ACCEPT
$ipt -A HTTP-FIN-1 -p tcp --tcp-flags SYN,ACK,FIN FIN,ACK -m recent --name HTTP-FIN --set -j ACCEPT
$ipt -A HTTP-FIN-2 -p tcp --tcp-flags SYN,ACK NONE -m recent --name HTTP-FIN --update -j ACCEPT
$ipt -A HTTP-FIN-2 -p tcp --tcp-flags SYN,ACK ACK -m recent --name HTTP-FIN --update -j ACCEPT
$ipt -A HTTP-FIN-2 -p tcp --tcp-flags SYN,ACK,FIN FIN -m recent --name HTTP-FIN --update -j ACCEPT
$ipt -A HTTP-FIN-2 -p tcp --tcp-flags SYN,ACK,FIN FIN,ACK -m recent --name HTTP-FIN --close -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,ACK,FIN,RST SYN -m recent --name HTTP-LIST --set -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,ACK,FIN,RST SYN,ACK -m recent --name HTTP-LIST --update -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,ACK,FIN ACK -m recent --name HTTP-LIST --update -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,ACK NONE -m recent --name HTTP-LIST --update -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,ACK ACK -m recent --name HTTP-LIST --update -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,FIN,ACK FIN -m recent --name HTTP-LIST --update -j ACCEPT
$ipt -A HTTP -p tcp --tcp-flags SYN,FIN,ACK FIN,ACK -m recent --name HTTP-LIST -j HTTP-FIN
$ipt -A HTTP -p tcp --tcp-flags SYN,FIN,ACK,RST RST -m recent --name HTTP-LIST --remove -j ACCEPT
```

Firewall Rule Semantics

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
- Summary

Cannot consider the semantics (meaning) of a rule in isolation.

- Must consider a rule in the context of previous rules.
- Rules are order dependent.
- The order/sequence of rules govern the overall semantics of the firewall configuration.

Example: Firewall Rule Semantics

Independent of other rules, Rule 2 states that *“all packets originating from a set of blacklisted hosts are to be denied”*

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	Action
1	in	eth0	tcp	*.*.*.*	webIP	*	80	Allow
2	in	eth0	tcp	blacklistIP	lanIP	*	*	Deny

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
- Intra-Conflicts
- Inter-Conflicts
- Summary

Example: Firewall Rule Semantics

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
- Summary

However, Rule 2 based on its semantic relationship with Rule 1, does not state “*all packets originating from a set of blacklisted hosts are to be denied*” .

Rather it states that “*all non-HTTP packets originating from a set of blacklisted hosts are to be denied*” .

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	Action
1	in	eth0	tcp	*.*.*.*	webIP	*	80	Allow
2	in	eth0	tcp	blacklistIP	lanIP	*	*	Deny

Example: Firewall Rule Semantics

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
 - Summary

An incorrect ordering of rules may change the intended semantics of the firewall configuration, resulting in incorrect network security policy enforcement!

- *“Deny all non-HTTP packets originating from a set of blacklisted hosts.”*

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	Action
1	in	eth0	tcp	*.*.*.*	webIP	*	80	Allow
2	in	eth0	tcp	blacklistIP	lanIP	*	*	Deny

≠

- *“Allow all HTTP packets that originate from a set of non-blacklisted hosts only.”*

Index	Dir	Iface	Proto	Src IP	Dst IP	Src Port	Dst Port	Action
1	in	eth0	tcp	blacklistIP	lanIP	*	*	Deny
2	in	eth0	tcp	*.*.*.*	webIP	*	80	Allow

Structural Analysis

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
- Summary

Structural Analysis examines the relationship that rules have with one another within a firewall configuration or accross multiple firewall configurations.

- A conflict occurs when two or more rules that are seemingly different match the same packet.
- While the individual rules themselves may be consistent with a network security policy, a rule placed out of sequence may unintentionally change the intended meaning of the firewall configuration, and thus, be inconsistent with the network security policy.

Structural Analysis Continued . . .

- Recap
- Configuration
- Complexity
 - Configuration
- ▷ Conflicts
 - Intra-Conflicts
 - Inter-Conflicts
 - Summary

Intra-Conflicts: conflicts that occur between rules on a single firewall.

Inter-Conflicts: conflicts that occur between rules accross different firewalls.

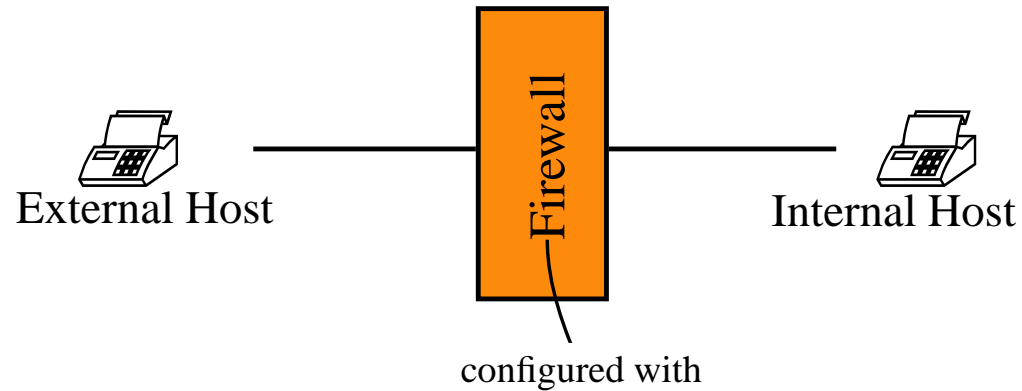
Firewall configuration conflicts are classified as follows [1]:

- intra-, inter-redundancy
- intra-, inter-shadowing
- intra-, inter-correlation
- intra-, inter-generalistation
- intra-irrelevance
- inter-spuriousness

[1] Ehab Al-Shaer, Hazem Hamed, Raouf Boutaba and Masum Hasan, *Conflict Classification and Analysis of Distributed Firewall Policies*, IEEE Journal on Selected Areas in Communications, Issue: 10, Volume: 23, Pages: 2069 - 2084, October 2005

Intra-Conflict Scenario

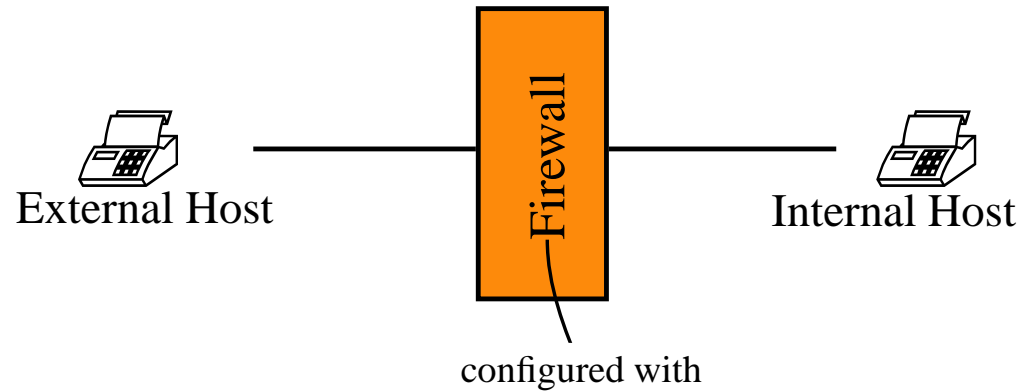
Conflicts that occur between rules on a single firewall are known as *intra-conflicts*



Index	Src IP	Src Port	Dst IP	Dst Port	Action
1	*.*.*.*	*	192.168.1.2	80	Deny
2	*.*.*.*	*	192.168.1.2	80	Deny
3	192.168.1.6	*	192.168.1.2	80	Allow
4	*.*.*.*	*	192.168.1.1	22	Allow
5	192.168.1.10	*	192.168.1.1	22	Allow
6	192.168.*.*	*	192.168.1.2	443	Allow
7	*.*.*.*	*	192.168.1.2	443	Allow
8	192.168.1.*	*	192.168.1.3	25	Deny
9	192.168.*.*	*	192.168.1.3	25	Allow
10	*.*.*.*	*	192.168.1.3	25	Deny
11	192.168.1.9	*	*.*.*.*	21	Deny
12	192.168.1.*	*	192.168.1.6	21	Allow
13	192.168.1.17	*	10.37.2.*	5060	Deny
14	192.168.1.*	*	10.37.2.*	5060	Allow
15	97.37.1.*	*	97.37.1.*	*	Deny

Intra-Conflict Scenario

Conflicts that occur between rules on a single firewall are known as *intra-conflicts*



Index	Src IP	Src Port	Dst IP	Dst Port	Action
1	*.*.*.*	*	192.168.1.2	80	Deny
2	*.*.*.*	*	192.168.1.2	80	Deny
3	192.168.1.6	*	192.168.1.2	80	Allow
4	*.*.*.*	*	192.168.1.1	22	Allow
5	192.168.1.10	*	192.168.1.1	22	Allow
6	192.168.*.*	*	192.168.1.2	443	Allow
7	*.*.*.*	*	192.168.1.2	443	Allow
8	192.168.1.*	*	192.168.1.3	25	Deny
9	192.168.*.*	*	192.168.1.3	25	Allow
10	*.*.*.*	*	192.168.1.3	25	Deny
11	192.168.1.9	*	*.*.*.*	21	Deny
12	192.168.1.*	*	192.168.1.6	21	Allow
13	192.168.1.17	*	10.37.2.*	5060	Deny
14	192.168.1.*	*	10.37.2.*	5060	Allow
15	97.37.1.*	*	97.37.1.*	*	Deny

Conflicts?

Definition: Intra-Redundancy Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

An *Intra-Redundancy* conflict occurs when two firewall rules can filter the same packets and those rules have the same target actions over those packets such that the removal of the redundant rule does not affect the semantics of the firewall configuration.

Redundancy in general takes one of two forms:

- equivalence (\equiv)
- subsumption (\subseteq)

Example: Intra-Redundancy Equivalence Conflict

Equivalence occurs when a rule is 'equivalent' to a previous rule, for example, Rule 2 and Rule 1.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	
6	192.168.*.*	*	192.168.1.2	443	Allow	
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	
12	192.168.1.*	*	192.168.1.6	21	Allow	
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Example: Intra-Redundancy Subsumption Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Scenario 1 occurs when a rule is a 'subset' of a previous rule.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	
12	192.168.1.*	*	192.168.1.6	21	Allow	
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

Example: Intra-Redundancy Subsumption Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Scenario 2 occurs when a rule is a superset of a previous rule where a previous rule is not also equivalent or subsumed by an intermediary rule having a different action.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	
12	192.168.1.*	*	192.168.1.6	21	Allow	
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

Example: Intra-Redundancy Subsumption Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Note, Rule 8 cannot be made intra-redundant to Rule 10 as its removal will have unintended side affects on the network security policy due to Rule 9.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	NOT Intra-Redundant(10)
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	
12	192.168.1.*	*	192.168.1.6	21	Allow	
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

Definition: Intra-Shadowing Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

An *Intra-Shadowing* conflict occurs when a rule that is never matched due to a previous rule filtering the same kinds of packets (equivalence or subsumption) and both rules have different target actions.

Remember: Firewall rules are matched in sequence, starting at Rule 1.

Example: Intra-Shadowing Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Rule 3 is intra-shadowed independently by both Rule 1 and Rule 2. Since Rule 3 is never matched, intended HTTP traffic from a specific host is not permitted.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	Intra-Shadowed(1,2)
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	
12	192.168.1.*	*	192.168.1.6	21	Allow	
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

As a general rule of thumb, one either deletes the intra-shadowed rule or re-orders the two rules, such that the more specific rule is placed before it's more general counterpart.

Definition: Intra-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

An *Intra-Correlation* conflict occurs when the actions of two rules under investigation are different and the first rule can filter some packets of the second rule and the second rule can filter some packets of the first rule.

- Intra-correlation conflicts have the form of the first rule having some of its filtering fields as subsets or equivalences of the corresponding second rule filter fields and the remaining filter fields of the first rule are supersets of corresponding filter fields of the second rule.
- Considered only as an administrator warning.

Example: Intra-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
- Inter-Conflicts
- Summary

Both Rule 11 and Rule 12 are intra-correlated (source and destination IP addresses).

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	Intra-Shadowed(1,2)
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	Intra-Correlated(12)
12	192.168.1.*	*	192.168.1.6	21	Allow	Intra-Correlated(11)
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	
15	97.37.1.*	*	97.37.1.*	*	Deny	

Definition: Intra-Generalisation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Intra-Generalisation conflicts occur between firewall rules when both rules under investigation have different target actions and if a rule can filter the same packets as a result of being a superset of the previous rule.

- Intra-Generalisation conflicts can be viewed as an administrator warning due to the fact that the proceeding more specific rule makes an exception of the generalised rule.

Example: Intra-Generalisation Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

Rule 13 and Rule 14 illustrate this.

Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	Intra-Shadowed(1,2)
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	Intra-Correlated(12)
12	192.168.1.*	*	192.168.1.6	21	Allow	Intra-Correlated(11)
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	Intra-Generalised(13)
15	97.37.1.*	*	97.37.1.*	*	Deny	

Definition: Intra-Irrelevance Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
 - ▷ Intra-Conflicts
 - Inter-Conflicts
- Summary

An *Intra-Irrelevance* conflict occurs when a rule cannot match any traffic based on either the source and destination IP addresses.

- This kind of conflict is considered a warning while it does not affect the semantics of the firewall configuration, it may add unnecessary firewall rule lookup overhead.

Example: Intra-Irrelevance Conflict

Rule 15 is irrelevant compared to the previous rules.

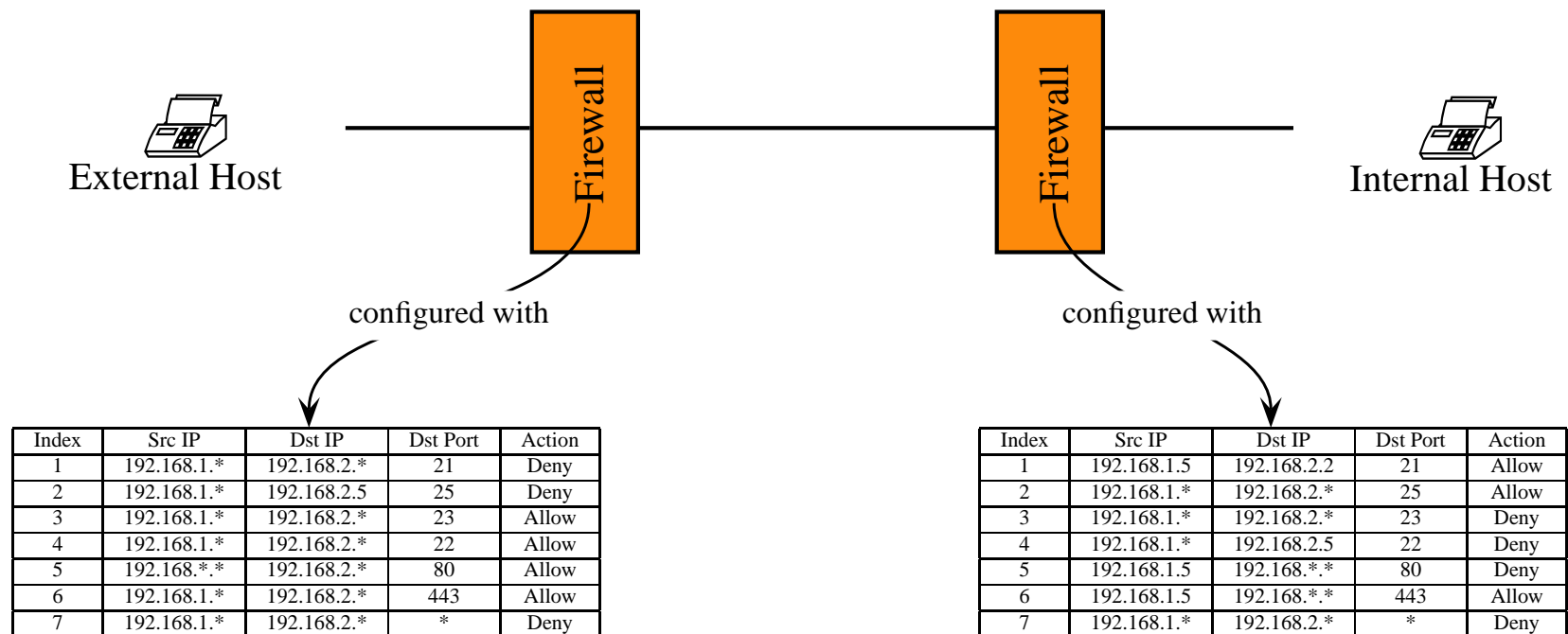
Index	Src IP	Src Port	Dst IP	Dst Port	Action	Conflict
1	*.*.*.*	*	192.168.1.2	80	Deny	
2	*.*.*.*	*	192.168.1.2	80	Deny	Intra-Redundant(1)
3	192.168.1.6	*	192.168.1.2	80	Allow	Intra-Shadowed(1,2)
4	*.*.*.*	*	192.168.1.1	22	Allow	
5	192.168.1.10	*	192.168.1.1	22	Allow	Intra-Redundant(4)
6	192.168.*.*	*	192.168.1.2	443	Allow	Intra-Redundant(7)
7	*.*.*.*	*	192.168.1.2	443	Allow	
8	192.168.1.*	*	192.168.1.3	25	Deny	
9	192.168.*.*	*	192.168.1.3	25	Allow	
10	*.*.*.*	*	192.168.1.3	25	Deny	
11	192.168.1.9	*	*.*.*.*	21	Deny	Intra-Correlated(12)
12	192.168.1.*	*	192.168.1.6	21	Allow	Intra-Correlated(11)
13	192.168.1.17	*	10.37.2.*	5060	Deny	
14	192.168.1.*	*	10.37.2.*	5060	Allow	Intra-Generalised(13)
15	97.37.1.*	*	97.37.1.*	*	Deny	Intra-Irrelevant(1-14)

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - ▷ Intra-Conflicts
- Inter-Conflicts
- Summary

Inter-Conflict Scenario

- Recap
- Configuration Complexity
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

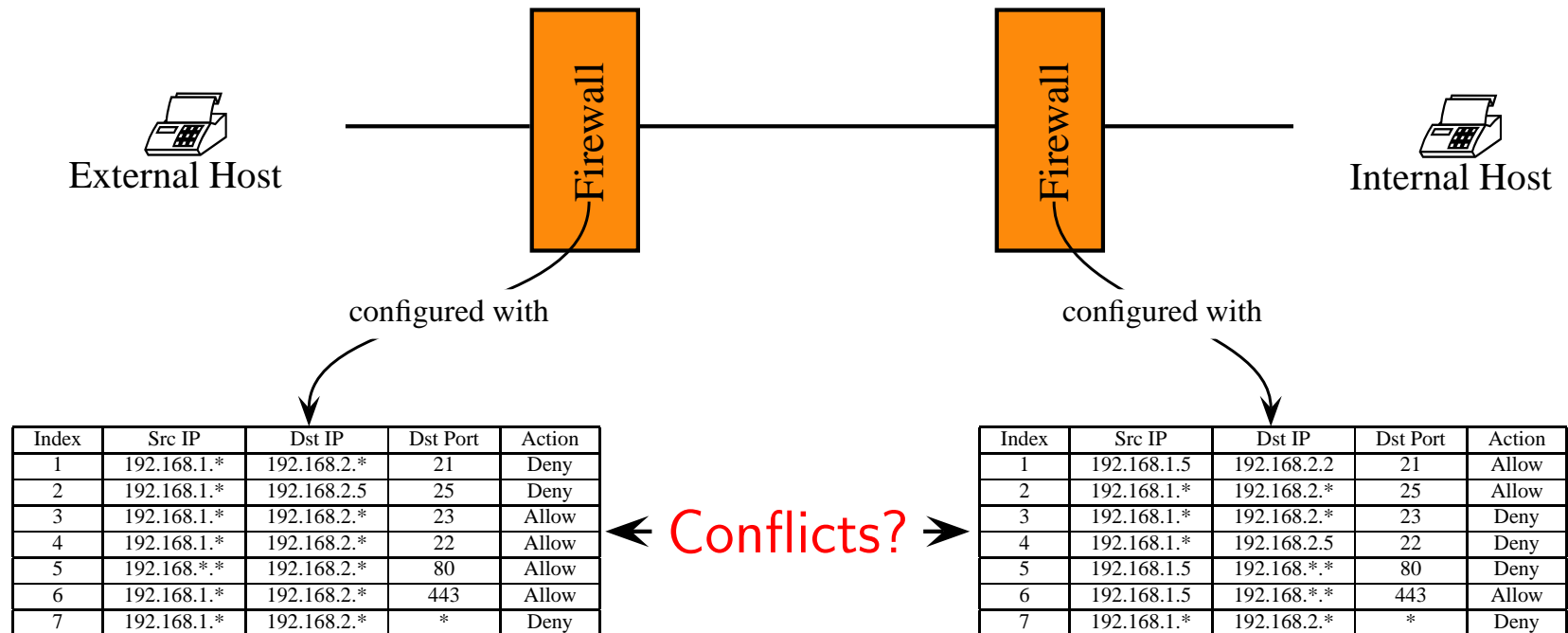
Conflicts that occur between rules across different firewalls are known as *inter-conflicts*.



Inter-Conflict Scenario

- Recap
- Configuration Complexity
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Conflicts that occur between rules across different firewalls are known as *inter-conflicts*.



Defintion: Inter-Redundancy Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
- Intra-Conflicts
- ▷ Inter-Conflicts
- Summary

An *Inter-Redundancy* conflict occurs when a downstream firewall is filtering an equivalent or a subset of packets that an upstream firewall is currently filtering, where both firewalls apply the same deny action to those filtered packets.

Example: Inter-Redundancy Conflict

- Recap
- Configuration Complexity
- Configuration Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Rule 7 of downstream firewall is inter-redundant to Rule 7 of upstream firewall.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-CorrelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-CorrelatedTo(down:6)
7	192.168.1.*	192.168.2.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-CorrelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-CorrelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Definition: Inter-Shadowing Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- ▷ Inter-Conflicts
- Summary

An *Inter-Shadowing* conflict occurs when a downstream firewall is filtering an equivalent, a subset or superset of packets that an upstream firewall is currently filtering, but the upstream firewall is denying what the downstream firewall is permitting.

Example: Inter-Shadowing Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Downstream Scenario: intended FTP access from a specific client (192.168.1.5) to a specific server (192.168.2.2) defined by Rule 1 (downstream firewall) is being inter-shadowed by by Rule 1 (upstream firewall) which denies the entire subnet of that client from reaching the destination subnet.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-RelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-RelatedTo(down:6)
7	192.168.1.*	192.168.2.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-RelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-RelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Example: Inter-Shadowing Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Upstream Scenario: Rule 2 (Upstream firewall) partially inter-shadows the intended SMTP traffic required by the downstream firewall.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-RelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-RelatedTo(down:6)
7	192.168.1.*	192.168.2.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-RelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-RelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Definition: Inter-Spuriousness Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- ▷ Inter-Conflicts
- Summary

An *Inter-Spuriousness* conflict occurs when a downstream firewall is filtering an equivalent, a subset or superset of packets that an upstream firewall is currently filtering, but the upstream firewall is permitting what the downstream firewall is denying.

Example: Inter-Spuriousness Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

The upstream firewall is permitting unwanted Telnet and SSH traffic (Rule 3 and Rule 4) that is being denied by the downstream firewall (Rule 3 and Rule 4).

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-RelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-RelatedTo(down:6)
7	192.168.1.*	192.168.2.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-RelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-RelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Definition: Inter-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- ▷ Inter-Conflicts
- Summary

An *Inter-Correlation* conflict occurs between two rules, independent of their target actions, when the first rule of an upstream firewall is filtering some packets of the second rule in a downstream firewall and that same rule of the downstream firewall is filtering some packets of the first rule in the upstream firewall.

- Inter-Correlation conflicts not only creates an ambiguity between two inter-dependent firewall configurations but also creates spurious and shadowing conflicts.

Example: Inter-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Rule 5 (upstream firewall) permits the traffic that is coming from 192.168.1.5 and destined to 192.168.2.*. However, this same traffic is being denied by the downstream firewall (Rule 5) and as a consequence a inter-spurious conflict occurs.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-RelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-RelatedTo(down:6)
7	192.168.1.*	192.168.2.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-RelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-RelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Example: Inter-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
- Intra-Conflicts
- ▷ Inter-Conflicts
- Summary

A scenario where both inter-shadowing and inter-spurious occur simultaneously is illustrated by the semantic union of rules Rule 6 (upstream firewall) and Rule 6 in (downstream firewall).

- HTTPS traffic sourced from 192.168.1.5 and destined to 192.168.2.* will be permitted. However, intended traffic sourced from 192.168.1.5 destined to 192.168.*.* will be inter-shadowed by the upstream firewall, while inter-spurious traffic from 192.168.1.* will be permitted to the downstream firewall. The reason for the inter-shadowing is not as a result of the pairwise comparison of both rules but the union of rules Rule 6 and Rule 7 (upstream firewall) and its semantic impact on Rule 6 (downstream firewall).

Example: Inter-Correlation Conflict

- Recap
- Configuration
- Complexity
- Configuration
- Conflicts
 - Intra-Conflicts
 - ▷ Inter-Conflicts
- Summary

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.*	192.168.2.*	21	Deny	
2	192.168.1.*	192.168.2.5	25	Deny	
3	192.168.1.*	192.168.2.*	23	Allow	Inter-SpuriousTo(down:3)
4	192.168.1.*	192.168.2.*	22	Allow	Inter-SpuriousTo(down:4)
5	192.168.*.*	192.168.2.*	80	Allow	Inter-RelatedTo(down:5)
6	192.168.1.*	192.168.2.*	443	Allow	Inter-RelatedTo(down:6)
7	192.168.1.*	192.168.*.*	*	Deny	

Upstream Firewall Configuration.

Index	Src IP	Dst IP	Dst Port	Action	Conflict
1	192.168.1.5	192.168.2.2	21	Allow	Inter-Shadowed(up:1)
2	192.168.1.*	192.168.2.*	25	Allow	Inter-ShadowedBy(up:2)
3	192.168.1.*	192.168.2.*	23	Deny	
4	192.168.1.*	192.168.2.5	22	Deny	
5	192.168.1.5	192.168.*.*	80	Deny	Inter-RelatedTo(up:5)
6	192.168.1.5	192.168.*.*	443	Allow	Inter-RelatedTo(up:6)
7	192.168.1.*	192.168.2.*	*	Deny	Inter-RedundantTo(up:7)

Downstream Firewall Configuration.

Firewall configuration management is complex and error prone.

Related Research:

1. W. M. Fitzgerald, S. N. Foley: "Aligning Semantic Web Applications with Network Access Controls", International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, Interfaces and Measurement, Computer Standards & Interfaces, Elsevier, October 2009, (In Print).
2. W. M. Fitzgerald, S. N. Foley, M. O Foghlu : "Network Access Control Configuration Management using Semantic Web Techniques", Journal of Research and Practice in Information Technology, Vol. 41, No. 2, May, 2009.
3. S. N. Foley, W. M. Fitzgerald: "An Approach to Security Policy Configuration using Semantic Threat Graphs", 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec'09), Concordia University, Montreal, Canada, July 12-15, 2009.
4. W. M. Fitzgerald, S. N. Foley, M. O Foghlu : "Network Access Control Interoperation using Semantic Web Techniques", 6th International Workshop on Security in Information Systems (WOSIS), Barcelona, Spain, June, 2008.
5. S. N. Foley, W. M. Fitzgerald : "Semantic Web and Firewall Alignment", First International Workshop on Secure Semantic Web (SSW), IEEE CS Press, Cancun, Mexico, April 7-12, 2008.
6. W. M. Fitzgerald, S. N. Foley, M. O Foghlu: "Confident Firewall Policy Configuration Management using Description Logic", Proceedings of The Twelfth Nordic Workshop on Secure IT Systems, Short Paper, Reykjavik, Iceland, October 11-12, 2007.