

Application Note

Configuration Options for Hardware Rule Search (RMS) and Software Rule Search (SWRS)

Discover Which ScreenOS Rule Search Works for Your Network

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

Introduction	3
Scope	3
Design Considerations	3
Hardware Requirements	3
Software Requirements	3
Description and Deployment Scenario	4
RMS	4
SWRS	6
Summary	6
About Juniper Networks	6

Introduction

There are two implementations of rule search in ScreenOS. Platforms that include the GigaScreen application-specific integrated circuit (ASIC) use a hardware-assisted method that provides linear performance, or $O(N)$. Software-only devices utilize a more sophisticated algorithm that is implemented in a CPU, which provides better (logarithmic) average performance, or $O(\log N)$, but consumes CPU. In some cases, especially with large rule-sets, it may be beneficial to overall performance to trade CPU utilization for the better algorithm, so hardware capable platforms can be configured to use the software-only version.

Scope

This document will help customers understand the performance implications of not using Security Zones to partition the rule set when using ASIC-based platforms; provide information to allow customers to analyze their situation and present an option that may help mitigate this situation without redesigning.

Design Considerations

This document is most relevant to designs derived from the direct conversion of deployments of devices that don't have the concept of Security Zones, which leads to very large rule sets divided into very few zones. This is especially relevant when installing ASIC-based systems.

Hardware Requirements

ASIC based platforms:

- ISG1000/ISG2000
- NS-5000

Software Requirements

- ScreenOS 5.2

Description and Deployment Scenario

Configured firewall policies need to be expanded into rules before they can be used to match incoming traffic. The number of rules a policy is translated into depends on the number of objects involved, the firmware version and the hardware revision. In general terms, it will be somewhere between the addition and product of source subnets, destination subnets and port ranges.

The following table has some examples:

Source	Destination	Service	Min # of Rules	Max # of Rules
ANY	ANY	ANY	1	3
1.2.3.0/24	3.2.1.0/24	HTTP	1	3
1.2.3.0/24	3.2.1.0/24	HTTP	2	4
1.2.4.0/24				
1.2.3.4/32	3.2.1.2/32	TCP/1025-65535	4	5
1.2.3.5/32	3.2.1.3/32			
1.2.3.4/32	3.2.1.2/32	HTTP	6	8
1.3.3.0/24	4.3.0.0/16	HTTPS		
1.2.3.4/32	3.2.1.2/32	HTTP	9	27
1.3.3.0/24	4.3.0.0/16	HTTPS		
1.3.4.0/24	5.0.0.0/8	TELNET		

RMS

The hardware-assisted rule search mechanism (default on devices with GigaScreen ASIC), stores rules in a linked list of hardware sectors hanging from a “context,” which is a zone pair that has rules defined between them. This leads to linear performance on the number of rules between the zones, or O(N).

A sector can hold 64 rules and is dedicated to a context (zone pair). This works very well for small rule-sets when multiple zones are in place, but it can lead to fragmentation. It is important to note that sectors are hardware entities and are platform dependent.

For example, an NS-5200 with the following policy (2 source prefixes, 2 destination prefixes and 2 services) is configured as follows:

```

set policy id 1 from "Trust" to "Untrust" "1.2.3.4/32" "3.2.1.2/32" "HTTP"
permit
set policy id 1
set src-address "1.3.3.0/24"
set dst-address "4.3.0.0/16"
set service "HTTPS"
exit
    
```

This will produce the following output for “get rms”:

```

ns5200-> get rms
RMS internal information: - Saturn
Total sectors: 4,091          available: 4090
Total rules: 261,824  used: 9  avail: 261,815
Ctx created: 1             sectors used: 1
    
```

Information derived for this example is as follows:

- The hardware used is a “Saturn,” which is the codename for a family of ASICs present in the NS-5000 blades and Integrated Security Gateway (ISG) platforms.
- This chip has 4,091 sectors, where 4,090 are available and one is used (4,091-1 = 4,090).
- The maximum number of rules supported is 261,824, which is equal to the number of available sectors in hardware multiplied by their capacity (4,091 Sectors * 64 Rules/Sector = 261,824 Rules).
- There are nine rules stored, leaving room for 261,815 (261,824-9 = 261,815).
- There is only one context present in the system, since the only policies are from Trust to Untrust.

The detailed output from “get rms ctx” will show:

```
ns5200-> get rms ctx
```

RMS Contexts:

ctx_id	name	policy	rule	sect	start
0	Trust->Untrust:0	1	9	1	0x00006800

This reports that “Context 0” from Trust to Untrust has one policy that turns into nine rules (eight for the policy and one for the implicit “deny any any”), all stored in one sector.

```
ns5400-> get pol
```

Total regular policies 1, Default deny.

ID	From	To	Src-address	Dst-address	Service	Action	State
1	Trust	Untrust	10.1.1.0/24	20.1.1.100/32	dns	Permit	enabled

```
ns5400-> get pol asic
```

system has total 65216 rules, 9 rules are in use.

```
ns5400-> get rms ctx 1 sect 0
```

ctx_id	name	policy	rule	sect	start
1	Trust->Untrust:0	1	5	1	0x00000800

sect_id rule memory shadow pol_tab

```
0 5 0x00800080 0x290796b0 0x296796a0
```

Rules in shadow mem 0x290796b0, 5 rule(s):

rule	src	dst	prot:sport-dport	act/pid
0000	10.1.1.0/24	20.1.1.100	17:fff0001-00350035	1
0001	10.1.2.0/24	20.1.1.100	17:fff0001-00350035	1
0002	10.1.1.0/24	20.1.1.100	6:fff0001-00350035	1
0003	10.1.2.0/24	20.1.1.100	6:fff0001-00350035	1
0004	Any	Any	Any	

End(320000)

```
ns5400->
```

SWRS

Devices without hardware assistance for rule search use an optimized and mature “longest prefix match” algorithm with a logarithmic average performance, or $O(\log N)$.

This Software Rule Search (SWRS) does not suffer from sector limitation or other hardware constraints from hardware implementation (RMS), since it is a pure software implementation limited only by memory consumption that is typically modest.

CPU utilization is very efficient, and SWRS usually outperforms RMS for long searches due to large rule-sets.

Summary

RMS may become a constraint in platforms like ISGs, where performance suffers when the CPU idly waits for the hardware to find the appropriate rule in the presence of large rule sets (few zones in place), or limits capacity when numerous zones are meshed, leading to a large number of contexts (zone pairs with rules) and fragmentation.

Even though SWRS provides a solution to both of these situations, RMS outperforms SWRS in situations with small rule-sets, where the algorithm advantage doesn't offset CPU utilization. This is due to the fact that $O(N)$ performance in hardware is more effective than $O(\log N)$ in CPU when N is small. This is a fairly common situation in traditional deployments where traffic is divided into multiple zone pairs, like Untrust to multiple DMZs, and Trust to multiple DMZs.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

CORPORATE HEADQUARTERS
AND SALES HEADQUARTERS FOR
NORTH AND SOUTH AMERICA
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

EUROPE, MIDDLE EAST, AFRICA
REGIONAL SALES HEADQUARTERS
Juniper Networks (UK) Limited
Building 1
Aviator Park
Station Road
Aldlestone
Surrey, KT15 2PG, U.K.
Phone: 44.(0).1372.385500
Fax: 44.(0).1372.385501

EAST COAST OFFICE
Juniper Networks, Inc.
10 Technology Park Drive
Westford, MA 01886-3146 USA
Phone: 978.589.5800
Fax: 978.589.0800

ASIA PACIFIC REGIONAL SALES HEADQUARTERS
Juniper Networks (Hong Kong) Ltd.
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

Copyright 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

**To purchase Juniper Networks solutions, please
contact your Juniper Networks sales representative
at 1-866-298-6428 or authorized reseller.**