

Firewall-Wizards: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

## RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-08/0303.html>

---

**From:** Gibson, Brian ([bgibson@RyanBeck.com](mailto:bgibson@RyanBeck.com))

**Date:** 08/01/02

From: "Gibson, Brian" <[bgibson@RyanBeck.com](mailto:bgibson@RyanBeck.com)>

To: "'Pieper, Rodney'" <[rodney.pieper@eds.com](mailto:rodney.pieper@eds.com)>, 'Frank Darden' <[fdarden@locked.com](mailto:fdarden@locked.com)>, Gregory Aust

Date: Thu Aug 1 21:52:01 2002

Rod,

Not sure if you really needed to do a lot of sleuthing to figure out that he was from Mission Critical Systems. He did leave a Sig on his email that said he was the CTO of Mission Critical Systems. Even had a phone number.

Also not sure why he deserved the hostility.

But aside from that either you or he don't have your facts straight.

According to the information that Frank provided it is not 1000 rules per se but 1000 combinations in the rules. My rule base only has about 30-40 rules in it but their is EASILY 1000 different permutations.

Are you saying that this is not the case? Is it 1000 explicit rules that are the limitation?

I am apolitical regarding Netscreen. I actually have a sales rep coming in next week to spin his product. But this does seem like a problem if what Frank says is correct.

-----Original Message-----

From: Pieper, Rodney [<mailto:rodney.pieper@eds.com>]

Sent: Thursday, August 01, 2002 2:51 PM

To: 'Frank Darden'; Gregory Austin; [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

Subject: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

Your 'recent awareness' is old history. And it shows your corporate bias.

The report you cite is CheckPoint originated and deals with older NetScreen version.

Backtracking your e-mail shows locked.com is Mission Critical Systems of Florida which is the master CheckPoint sales outlet for Florida.

RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

Firewall-Wizards: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

On a further note. What security engineer would recommend a firewall rule set that has a 1000 rule policy? A. trying to keep logical track of the rule set and B. with a fall out rule set how much traffic actually gets to the last few rules?

But, then if a 1000 rule set makes you feel safer then go for it.

Rod

-----Original Message-----

From: Frank Darden [mailto:[fdarden@locked.com](mailto:fdarden@locked.com)]

Sent: Thursday, August 01, 2002 1:09 PM

To: Gregory Austin; [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

Subject: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

I will add my 2 cents on the Netscreen side. I recently became aware of serious weaknesses in the Netscreen product. I have a paper which outlines the issues and problems with the Netscreen firewall. If your choice is between Check Point or Netscreen, I would strongly urge you to read the information below carefully. Please send your comments/questions my way.

Frank

Basically what it boils down to with Netscreen is the following

All NetScreen appliances rely on custom-designed ASICs (Application Specific Integrated Circuits) for security policy enforcement. Appliances cannot be field upgraded to accommodate new or additional ASIC devices.

Each NetScreen ASIC is limited to the size of security policy it can support. Once customers reach this limit they are unable to expand their security policy to meet future needs. The NetScreen appliance continues to function, but no additional rules can be added to the policy.

NetScreen is aware of this limitation and provides a utility for customers to check the remaining capacity of the ASIC before hitting the limit. NetScreen's recommended resolution is to either redesign the security policy to meet the unique constraints of the NetScreen appliance or upgrade to a more expensive NetScreen product as well as pay for the software license again.

NetScreen customers are adversely affected by this design constraint. There are no other known security/VPN products in the market that have inherent limitations to the size of policy that can be defined and enforced.

Problem Details:

Each NetScreen ASIC (i.e. MegaScreen, GigaScreen and GigaScreen II)

RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

supports a finite number of "rules" or "policies" (N). If the addition of a single rule beyond the hard limit is attempted (N+1), the NetScreen device operator sees the following error message:

"The Maximum Number of ASIC rules has been reached. Cannot add this policy"

At that point the operator cannot add any more rules to the security policy. This limitation restricts granular access control and, therefore, the security of the network.

Term definition:

#### ASIC Rules

NetScreen uses the terms "policies", "rules" and "ASIC rules" somewhat interchangeably. An ASIC rule is defined by the following equation: (reference from NetScreen support site provided at end of this document)

$$\#ASIC\ rules = \#source\ addresses * \#destination\ addresses * \#services$$

Note that the number of ASIC rules consumed is not the sum of individual objects, but the product of those objects used in a rule. This has the effect of consuming the finite number of ASIC rules rapidly.

#### Groups

The terms "Grouping" and "Groups" refer to a NetScreen feature by which several servers or gateways (e.g. individually defined web servers or branch office locations) and services (e.g. FTP, FTP get, FTP put) are joined to one logical name, for instance "Web Servers", "Branch Offices" or "FTP Services". It is common for security administrators to group like objects to facilitate the definition of security rules.

For example, an object may be created that includes all company web servers. The security administrator can use this object when defining the security policy, rather than including separate security rules for each web server. This useful feature makes the creation and subsequent editing of security rules more efficient.

Surprisingly, the use of groups in a NetScreen policy results in FEWER ASIC rules being available to the security administrator. Although the use of group objects provides efficiency to the administrator, it rapidly exhausts the number of ASIC rules available to NetScreen customers.

#### A practical example

The NetScreen 100 has a rule limit 733 applying to traffic originating from an external interface (Internet) to the Demilitarized Zone (DMZ).

Firewall-Wizards: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

The following is a NetScreen rule base showing a group of 10 branch offices granted access to mail, FTP and web-based services hosted by 10 separate servers located on a company's DMZ.

The service groups have been defined as follow:

Web and FTP Services: HTTP, HTTPS, FTP, FTP-Get, FTP-Put

Mail Group: SMTP, POP3, IMAP, HTTPS

Teleconferencing Services: H.323, NetMeeting

All other services are pre-defined within the NetScreen device. The rulebase as shown uses 732 ASIC rules.

At this point, the device will not allow the addition of any more rules no matter how simple. Adding another branch office or trying to give remote access VPN users access to the DMZ, yields the following message:

#### NetScreen Response to Customers

Recently NetScreen acknowledged the policy limitation in a mailing to partners. The Company contends that the security policy limits will not affect customers as long as the right device is selected for the application. This is a highly unconventional design approach. Since granular access control translates to degree of security, imposing limits on the number of rules is effectively restricting security for any size deployment. The restriction also requires that customers and resellers be aware of the ASIC limits per platform before purchasing, so that they can perform the complex calculations which would guide product selection. Assuming that this is even feasible given an existing security policy, it is not an approach which accounts for network growth or expansion.

NetScreen has implicitly admitted this by promising to extend the limits in a future release. It is clear however, that since the limits are tied to the ASIC type that these restrictions will always be imposed. It is also likely that extending the limits may affect the advertised performance of the devices since according to the company:

"What is important is that a NetScreen device with it's ASIC-based security acceleration functions, can maintain predictably high performance at the indicated policy count levels."

(excerpt from NetScreen channel partner mailing)

#### NetScreen Technical Support Posting

>-----  
-----  
>-----

RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

Firewall-Wizards: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

DOC #: 549

Subject: Maximum number of policies

Question: I am configuring the firewall, and I don't have too many policies. However, I get the following error message: Policy: Can't add item. Asic limit reached What does this mean?

Answer: Check and see if you are using the "Grouping" feature on address books and services. If you are, then you have reached the policy limit on the Netscreen.

Internally, the Netscreen logs policies on the ASIC ACL. You can check the capacity of your Netscreen by telnetting into the device and enter the command,

```
get policy <out|in|todmz|fromdmz> asic
```

This will give you the total number of policies available in that direction, the number of policies currently configured, and the number of policies remaining.

To calculate how many ASIC ACL rules are used, do the following:

#Asic rules = #source address \* #destination address \* #services

The number of policies enforced due to groupings multiply as you add more entries per group.

<https://www2.netscreen.com/cgi-bin/restricted/sla/kb.cgi?1?549?2>

-----

DOC #: 569

Subject: Maximum Policies for Netscreen 5

Question: How many policies can a Netscreen 5 handle?

Answer: The Netscreen 5 can only handle 95 policies total.

<https://www2.netscreen.com/cgi-bin/restricted/sla/kb.cgi?1?569?2>

=====

Frank Darden  
Chief Technology Officer  
Mission Critical Systems  
3320 NW 53rd St. Suite 202  
Fort Lauderdale, FL 33309  
Phone (954)766-2550 x203  
Fax (954-766-2580  
AIM/MSN FishinCritical

=====

-----Original Message-----

From: Gregory Austin [mailto:[greg@austinconsulting.com](mailto:greg@austinconsulting.com)]

Sent: Monday, July 29, 2002 10:28 PM

To: [firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)

Subject: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

Hello all,

Felt I too had to throw my \$0.02 on this little Checkpoint versus Netscreen discussion. I work for a security services company, and we sell a whole bunch of Checkpoint. I touch a whole bunch of Checkpoint, quite a

RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

## Firewall-Wizards: RE: [fw-wiz] PIX vs Checkpoint vs Sonicwall vs Netscreen – comme nts?

bit of PIX, and a little bit of Netscreen, Watchguard, etc.--but that's changing. In my experience the Netscreen product is not only vastly superior to Checkpoint in terms of price and performance, but the company actually seems to be working to improve their product (unlike Checkpoint and their latest piece of betaware, No-Go).

On performance consider this: I have a customer who put in 100mbps service between their major metro sites on one of those big fiber carriers. They want the traffic between the sites tunneled. For close to the same money it would cost them to get tiny little Nokia IP-120's that can only push <3mbps VPN traffic, they can get Netscreen 204's that can push >100mbps of VPN traffic.

Good central management is nice, agreed, but is it worth getting bent over on the price? Any way you look at it, rape is the best term to describe their licensing. I will admit that you can't beat Checkpoint when it comes to interoperability, though. Through all of their OPSEC alliances they've built up a huge stable of products that will play (mostly) nicely with FW-1.

Also, consider another reason to not go Checkpoint. The last time I remember a company with this big a market share being this arrogant and making this many bad moves was Novell in '93. They'll be able to coast for 5 or 6 years on declining market share alone, but I can't imagine a rosy future for them unless something changes. When you can buy technically superior better performing products for vastly less money it's only a matter of time before the market gets a clue.

Just my opinion, certainly not that of my employer (party line: We love Checkpoint!),  
Greg

---

firewall-wizards mailing list  
[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

---

firewall-wizards mailing list  
[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

---

firewall-wizards mailing list  
[firewall-wizards@honor.icsalabs.com](mailto:firewall-wizards@honor.icsalabs.com)  
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>