

Re: [fw-wiz] Firewall policy generator, capture based – Any idea?

## Re: [fw-wiz] Firewall policy generator, capture based – Any idea?

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2008-01/msg00027.html>

---

- *From:* "Paul Melson" <[pmelson@xxxxxxxxxx](mailto:pmelson@xxxxxxxxxx)>
  - *Date:* Wed, 30 Jan 2008 12:08:09 –0500
- 

I would like to find out if you know any tool that can help me with this:

I want to capture my Data Center traffic, with a NAM or Sniffer.  
Taken the capture I would like to have a tool that can interpret the

traffic flows and

automatically generate firewall rules to allow those flows.  
I really don't want to waste time inspecting each single PCAP packet!

For example if there are multiple flows from the same subnet, create a  
permit rule for that

subnet matching the destination range.

Basically a packetflow capture based firewall rules generator.

Having done pretty much exactly this twice before, I can tell you that I wouldn't use a sniffer, and I especially wouldn't use an automated rule generator of any sort. You need to make sure any traffic you allow is deliberate and important to the organization. An automated tool won't make such judgments, and you will end up allowing all of the crap that's already on your network that you should probably be blocking.

My advice on how to proceed:

Step 1. Put the firewall in place with a policy that allows all traffic to pass. Turn on logging. Use this instead of a sniffer as analyzing firewall logs will be much easier. It will also separate the physical and routing changes you make to the network from the policy changes. This will aid in troubleshooting connectivity issues down the road.

Step 2. Analyze logs. I wrote a shell script to do this with PIX logs, and basically all I did was identify each of the unique sets of srcaddr,dstaddr,dstport and then count the number of times each unique set occurred in the log file. Sort results by number of occurrences and you

Re: [fw-wiz] Firewall policy generator, capture based – Any idea?

Re: [fw-wiz] Firewall policy generator, capture based – Any idea?

will find either a) common traffic or b) crappy protocols.

Step 3. Investigate findings from logs. Find out what things are and then compare them to your business requirements and security policy. Determine whether or not the traffic should be allowed.

Step 4. Write rules for the traffic you decide to allow in Step 3. To help with your process, you may also want to write rules for traffic you wish to block.

Step 5. This is really a GOTO for step 2. You're going to eliminate known traffic from your logs and then analyze again. It's especially cool if the firewall includes rule numbers in its logs, so when you made those rules in step 4, they make it easier to separate the known from unknown traffic. Loop through steps 2–5 for as many iterations as appropriate.

Step 6. Change from 'permit all' to 'deny all' policy. Once you've sufficiently analyzed data and implemented rules, cut over your default policy and test your business–related stuff. If you made block rules in step 4 that are superseded by this policy change, you may want to remove them now in order to keep your firewall rule set as simple as it can be.

Step 7. Wait for the phone to ring. Depending on the size of the network and the volume of traffic, it will take you anywhere from a week to a month to get through step 6. Step 7 should last another 30–90 days, and basically you want to let the organization go through a long enough business cycle that things like payroll and billing to run through to completion at least once. You probably trampled on one or two things that are seldom used so they didn't generate traffic before, and this is when you find them and write rules for them.

Good luck. This kind of work is typically a real bear.

PaulM

---

firewall-wizards mailing list  
firewall-wizards@xxxxxxxxxxxxxxxxxxxxxxxxx  
<https://listserv.icsalabs.com/mailman/listinfo/firewall-wizards>

Re: [fw-wiz] Firewall policy generator, capture based – Any idea?