

Re: Analysing and configuring IPS/IDS Policies

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ids/2005-08/0006.html>

From: Fergus Brooks (*fergwa_at_gmail.com*)

Date: 08/02/05

Date: Tue, 2 Aug 2005 13:31:01 +0800

To: AsTriXs <astrixs@gmail.com>

Hi there,

If you have no faith in the firewall or you are concerned about more than just inbound traffic from the Internet via the firewall I would always take the first approach but to mitigate the risk of the IPS causing a DoS I would follow this methodology (off the top of my head – this is my version of best practices from a former employer...)

1) Remove the IPS from the network. As with firewalls you should stage them in a lab environment and perform as much testing as possible (not just of the hardware, also of the policy) before you put it inline.

2) Spend a fair amount of time with the fwadmin looking at the policies and logs on those devices. Understand the flow of traffic and the existing security policy the firewalls enforce.

3) Get everybody who looks after the networks and devices into a room with a whiteboard. Map out the network and the current and planned flow of data. Isolate that data down to an application and port level. Raise some what-ifs. A good one I find is "what if we shut down all xxx traffic?" The network peeps will then remember that they are using it or they need it if it was not shut down before. I would also make it very clear in this session that everything not expressly permitted will be blocked and that it is their responsibility to profile their own apps etc.

4) Define this flow and what you propose to do with the policy very clearly in a working document, this step is the first sanity check. Send this to everyone involved for checking. If it is a large organisation copy their line managers and departmental heads. Make sure everyone has given you all the information you need.

5) With all the information you have now you should know exactly what traffic you will see at the point the IPS is supposed to go into (but you probably won't...) Put a network analyser where you will plug the IPS and capture as much data as you can. Take the capture data away and use filters to check thoroughly through for apps & hosts that have

SecurityFocus IDS: Re: Analysing and configuring IPS/IDS Policies

not been accounted for.

6) Repeat steps 3 & 4 with this new information. You will have earned the added advantage that lazy sysops etc will now be taking you seriously.

7) Once you are happy that everything is accounted for perform as much testing as possible. You could use a method like simulating the production environment and using tcpdump/tcpreplay to replay exact streams of data.

8) Prepare a change control procedure for implementing the IPS, including detailed testing & backout plans. Make sure the support and infrastructure management teams are sufficiently staffed to accommodate the change. Make sure that anyone who may be required to help in the worst-case scenario is contactable. Brief these teams on what you are doing and let them know that you want to hear about anything weird that occurs around the time of deployment.

9) Install the policy-applied IPS, ask the test teams to start testing all applications & watch the logs carefully. Fix any minor problems if they come up. Should you start to see serious problems emerge decide whether or not to implement the backout plan/s. I would always prefer to backout than leave any application not functioning without a process to get it functioning in place.

10) Write a detailed report and forward to those involved.

(And this is not best practice but you've earned it – ask for a pay increase...)

Hope this helps – regards.

On 7/30/05, AsTriXs <astrixs@gmail.com> wrote:

> *Hello All,*

>

> *I am currently in the process of implementing an IPS at a client site.*

> *I have reached the stage where I have to configure and deploy*

> *policies.*

>

> *There are various approaches to deploying policies from ground up and*

> *then fine tuning them through their lifecycle. I have mentioned the*

> *two that I am aware and also the environment in which they need to be*

> *deployed.*

>

> *The IPS appliance has been deployed behind a firewall in front of a*

> *server farm.*

> *The traffic passing through the appliance is what is configured to*

> *pass on the firewall.*

>

> *First Approach*

>

Re: Analysing and configuring IPS/IDS Policies

SecurityFocus IDS: Re: Analysing and configuring IPS/IDS Policies

- > *We analyse alerts observed on the allowed protocols and create*
- > *exceptions (within trusted domains) for all false positives (or any*
- > *traffic which is permitted on the network but flagged off as malicious*
- > *by the IPS) observed. Set a policy (block or log) for all other*
- > *alerts. Appropriate policies for inbound and outbound traffic flows*
- > *are set. Alerts are closely monitored and fine tuned over time to*
- > *avoid self imposed DoS.*
- >
- > *This way we create exceptions for legitimate traffic and block*
- > *everything else. There is a possibility that a legitimate action,*
- > *which was not observed before, may get blocked. However, this approach*
- > *makes the target environment most secure in my opinion.*
- >
- > *Second Approach*
- >
- > *Alerts observed on the allowed protocols are analysed and policies are*
- > *set only for the malicious traffic observed. Policies are added at*
- > *each instance of malicious traffic observed on the network. Protocols*
- > *not allowed in the environment are set to be dropped. Appropriate*
- > *policies for inbound and outbound traffic flows are set.*
- >
- > *In this approach, we are open to attacks but the chances of self*
- > *inflicted DoS are minimal.*
- >
- > *I request comments & views from all on the advantages and*
- > *disadvantages of each approach to help me deploy policies effectively.*
- > *Information on other approaches would also be appreciated.*
- >
- > *Also, is there a method or a best practice followed while analysing*
- > *alerts and deploying policies.*
- >
- > *Thank you,*
- >
- > --
- > *[AsTriXs]*
- >
- >

> *Test Your IDS*

- >
- > *Is your IDS deployed correctly?*
- > *Find out quickly and easily by testing it*
- > *with real-world attacks from CORE IMPACT.*
- > *Go to http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708*
- > *to learn more.*
- >

>

>

Test Your IDS

Is your IDS deployed correctly?

Find out quickly and easily by testing it
with real-world attacks from CORE IMPACT.

Go to http://www.securityfocus.com/sponsor/CoreSecurity_focus-ids_040708
to learn more.
