endian

Secure everyThing
www.endian.com

HOW-TO Enable IPS/IDS via CLI - Preview Feature

Marco Pomalo

Document Revision: 7

Last Modification: 05/07/2021

Exported on: 05/17/2021

Exported by: Luis Aigner

Document URL: https://confluence.endian.com/pages/viewpage.action?pageId=54598927

Table of contents

HOW-TO Enable IPS/IDS via CLI - Preview Feature

Document Version: 1.0

Applies to EOS 5 and EOS 6

Applies to platform: all

This lesson shows how to switch between Endian's Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) from the Command Line Interface (CLI). This is a preview feature, the GUI will be updated accordingly in the next EOS Release.

Requirements

This how-to needs an updated appliance to EOS 5.2.6 or EOS 6.1.3

What is IPS/IDS

An Intrusion Prevention System (IPS) is available on every Endian appliance. It is very powerful by performing a deep packet inspection on the network in charge. This means that every single packet gets inspected, and the system reacts according to predefined rules.

An Intrusion Detection System (IDS) instead, only monitors the network traffic marking the suspicious behaviors in the log. The subsequent analysis of the logs, which allows to take countermeasures, is then usually performed by specific tools of various types.

Choosing between IPS and IDS, a matter of compromise

We need to protect our network from unauthorized accesses, and generally speaking, from criminal behaviors. Endian appliances have an Intrusion System onboard, which can be enabled from the web interface as described in this guide: https://help.endian.com/hc/it/articles/218144318-How-to-Enable-Configure-the-IPS

Since this is a preview version, the GUI only shows IPS, so the two Intrusion System Modes, which are the following, must be set via CLI:

IPS mode (full deep inspection)

This is the default mode on Endian appliances. An IPS gives the maximum protection because no network packet is left out from being deeply inspected. The downside is that it needs a considerable amount of resources, which slow down the system performance, and make the bandwidth much worse.

The IDS mode (traffic monitoring)

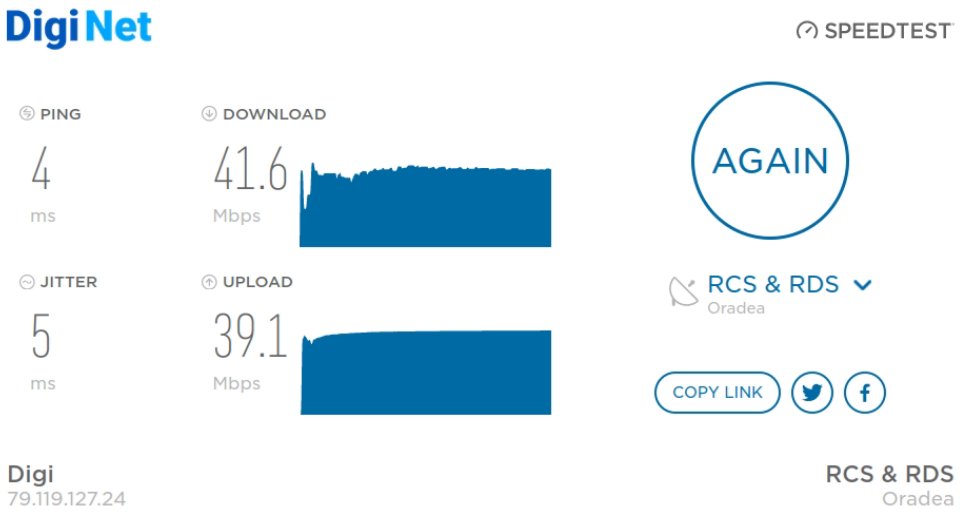
An IDS monitors a network for malicious behavior. The advantage of having this mode, is that it ensures high system performance and high network bandwidth.

Unfortunately all this has a cost; an IDS does not offer proper intrusion protection.

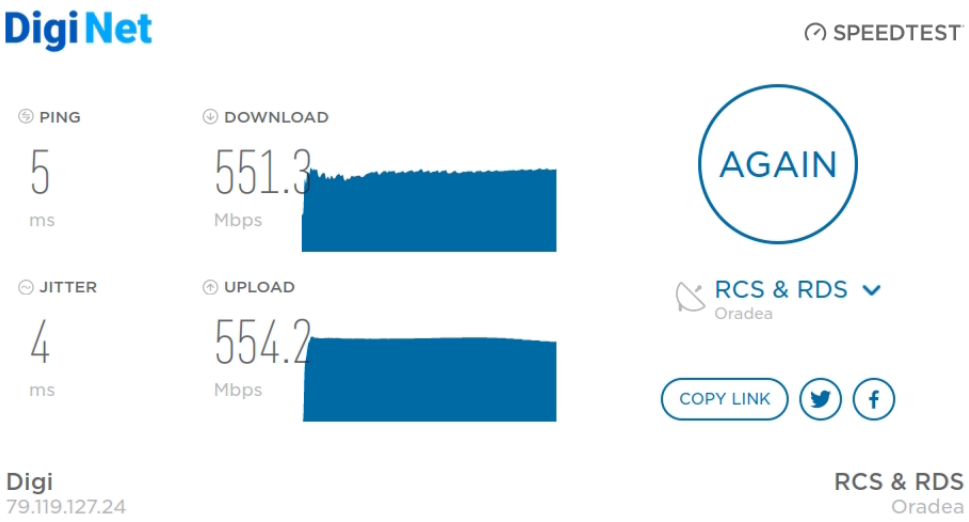
Example of network performance difference between IPS and IDS

We want to show the network performance in IDS mode compared to IPS mode. The example below is the result of one of our tests.

This is the network performance on a Endian UTM Mini 25 with IPS enabled:



This is the network performance on a Endian UTM Mini 25 with IDS enabled:



Setting IDS mode: how to proceed

Access the appliance

1. Login the appliance with root user using SSH. It can be done in two ways:
    a. directly from the Endian Network as described in the first part of this guide: https://help.endian.com/hc/it/articles/360024569533-How-to-use-Endian-Network
    b. or from a computer using Putty (Windows) or Terminal (MAC/Linux).
2. You should get a screen like this:

Root user successful login

```
  eeee      _nn_        dd   ii    _aa       _nn_
 ee""ee    _n""n_       dd   -     a"a_     _n""n_
 ee  ee    nn  nn       dd            a     nn  nn
 ee  ee    nn  nn    _dddd   ii    _aaa     nn  nn
 ee  ee    nn  nn   _d""dd   ii   _a""aa    nn  nn
 ee__ee    nn  nn   dd  dd   ii   aa  aa    nn  nn
 eeee"     nn  nn   dd  dd   ii   aa  aa    nn  nn
 ee"       nn  nn   dd  dd   ii   aa  aa    nn  nn
 ee        nn  nn   dd  dd   ii   aa  aa    nn  nn
  ee       nn  nn   dd  dd   ii   aa  aa    nn  nn
   ee      nn  nn    ddddd   ii    aaaaa    nn  nn
    _"     _"  "'     _'_"   "'     _'_"    "'  _"

 ||  ||  ||  ||  ||  ||  ||||||||||||||||||||

          Endian Firewall Enterprise

WARNING!   -  CHANGES TO SYSTEM FILES MAY AFFECT
YOUR  WARRANTY  AND DISCHARGE  ENDIAN  FROM  ANY
FURTHER  OBLIGATION  TO  PROVIDE  CUSTOMER  WITH
WARRANTY SERVICES OR SUPPORT HEREUNDER!

Have fun with your Endian Firewall!

root@efw-mini25:~ #
```

Check which mode of Intrusion System is already enabled

Please type in following command to check the current setting:

```
root@efw-mini25:~ # ds snort.settings.MODE
```

The default setting is IPS, so this is what you should get:

```
Value SNORT.SETTINGS.MODE

ips
```

If IDS was already set, the output will be:

```
Value SNORT.SETTINGS.MODE

ids
```

⚠ The network traffic between Uplink (RED Zone) and the GREEN Zone is inspected (IPS) or logged (IDS) by default even without specific settings.

Now set the correct intrusion MODE and the ZONES that have to be monitored.

Edit file: */var/efw/snort/settings* (we use **nano** editor in this guide)

```
root@efw-mini25:~ # nano /var/efw/snort/settings
```

The parameters to add/edit are two:

- MODE, which defines the way the network traffic is handled. Examples:
  - MODE=ips
  - MODE=ids
- ZONES, which defines which zone has to be monitored. Examples:
  - ZONES=UPLINK:main (the RED zone is monitored)
  - ZONES=GREEN&ORANGE (the GREEN and ORANGE zones are monitored; the separator is the symbol "&")
  - ZONES=UPLINK:main&GREEN&ORANGE&BLUE (the RED, GREEN, ORANGE and BLUE zones are monitored)

The file should look similar to the example below. The comments explain how to set the parameters.

```
# Please leave following line UNTOUCHED if it is present.
ENABLED=1
# Following line sets the MODE, which can be IPS or IDS. Here is IDS enabled.
MODE=ids
# Following line sets the ZONES. Here is Uplink and Green Zone enabled
ZONES=UPLINK:main&GREEN
```

In order to apply the changes, please execute following command:

```
root@efw-mini25:~ # jobcontrol restart snort --force
```

Now you can enable the IPS/IDS if not already enabled, directly from the web interface as described in this guide following this guide: https://help.endian.com/hc/it/articles/218144318-How-to-Enable-Configure-the-IPS

As already mentioned above, in this preview version the GUI shows only IPS, but it enables the correct settings defined via CLI.

⚠ If IDS mode is enabled, all the network traffic that goes through the interface is intercepted. It is not possible to select or exclude network traffic. This is the way SNORT works.

The high network performance of an IDS can be combined with analysis tools such as fail2ban or other AI-based tools, which allow to take countermeasures in case a malicious activity is detected.