Firewall on Demand v1.5
New features supported

Evangelos Spatharas

September 2019
Contents

- Introduction
- FoD Capabilities
- FoD Requirements, Constraints and Limitations
- How to Subscribe to FoD
- New Features on v1.5 release
  - REST API
  - Multi-port Range Support
  - Attack History Graph
- How to Contact us
Firewall on Demand – Introduction

• Firewall on Demand, abbreviated as FoD, is an application with a WEB front which allows subscribed users to disseminate firewall filters easily without any hassle.

• FoD’s key features are:
  • Precision – specific malicious flows can be targeted
  • Speed - Time to disseminate/withdraw firewall filters is sub 10 seconds
  • Convenience - NREN users can use web portal themselves, or make request by phone or e-mail.
  • Simplicity - The web portal uses intuitive, non-vendor specific GUI-based wizard to configure router firewall filters.
  • No interaction* (e-mail, phone call) with GEANT NOC is required. NREN user can add/remove filters at its own discretion.
  • No special knowledge of router-language is required. The WEB based app offers a very friendly scheme for applying the filter.

• The magic of FoD is powered on by the cutting edge flowspec technology as described by the RFC 5575.

*NOC/CERT users can still contact GEANT CERT using the traditional methods to request blocking
Why Flowspec?

- Speed
- Effectiveness
- Efficiency
Why Firewall on Demand?

- Value add tool part of the NSHaRP service
- Easier audit of flowspec filters
- Easier removal (auto-expire)
- Cleaner traditional filters without "temp" terms that pile up with time
- Less tickets on the OTRS queue
- Reporting (to be supported)
FoD Capabilities

- Propagate flowspec filters across GEANT network
- Filters CAN have DST address from YOUR administrative IP space
- Have an e-mail sent to yourself or ticketing system for tracking after rule submission/edit/withdrawn
- Historical record – users can view all rules (active and de-activated) created by themselves or their colleagues
Requirements, Constraints and Limitations

- Only affects flows transiting GÉANT core routers
- IPv6 is not currently supported
- Propagate a filter with a DST subnet bigger than /29
- Access FoD platform from an IP space other than your NOC’s/GEANT network’s space

![Diagram showing DDoS attack launched from compromised systems (bots) and attack that originates from the direct IX peering still passes through NREN.]
All GÉANT member NRENs may subscribe. The subscription process is as follows:

1. NREN APM completes form on [https://partner.geant.org/sites/main/Pages/fod-request.aspx](https://partner.geant.org/sites/main/Pages/fod-request.aspx) or contacts [partner-relations@geant.org](mailto:partner-relations@geant.org) if issues

2. Authorized NREN user, using host in NOC subnet, accesses [https://fod.geant.net](https://fod.geant.net) and clicks at “Shibboleth Login” button. Log in using standard eduGAIN method.

3. New user’s account will be activated within 1 business day or less (assuming login details match info provided by APM)
Shibboleth Attributes

• FoD’s Shibboleth module requires the release of the following attributes:

• givenName
• Mail
• Persistent-id
• principalName
• Surname
• UniqueID
REST API – Token creation

• API Token Creation Process
  • Click on the “My Profile” tab and then from the right side click “Generate one” next to Api Token.
  • You will use that token in order to make calls to the REST API
  • Don’t worry about losing that token once generated. It will always be there.
    • However, keep it safe from “shoulder surfers”
REST API – Reading rule examples with curl

- Reading all rules
- Reading specific rule with ID of 1 (ID can be retrieved from above query)
• Deleting a specific rule with ID of 18
  • curl -X DELETE 'https://prod-fod.geant.net/api/routes/18/' -H 'Authorization: Token <your token>‘ | python -m json.tool
  • Again, the ID of a rule can be retrieved by reading all rules with “curl –X GET. From the example previously”
  • As always, the rule above now will enter the “deactivated” state, and not deleted. I.e. it will still be visible on your dashboard for later use if needed.
REST API – Submitting new rule requirements

- Submitting a new rule requires that first we have defined protocols, and “then actions” at minimum
  - Some ports, protocols and “then actions” are already defined. Let’s see which protocols are defined:
    
    ```
    [{
      "id": 1,
      "protocol": "icmp"
    },
    {
      "id": 2,
      "protocol": "tcp"
    },
    {
      "id": 3,
      "protocol": "udp"
    }]
    ```

As you can see, ICMP, TCP and UDP protocols are defined. Those are enough for most of the attacks we know.
Finally let us see what are the defined “then actions” already in place:

```bash
```

```json
[
  {
    "action": "discard",
    "action_value": "",
    "id": 3
  },
  {
    "action": "rate-limit",
    "action_value": "10000k",
    "id": 27
  }
]
```

If we want to add new action of rate-limit 1k:

```bash
curl -X POST https://prod-fod.geant.net/api/thenactions/ -F "action=rate-limit" -F "action_value=1k" -H 'Authorization: Token xxxxx' | python -mjson.tool
```

```json
{
  "action": "rate-limit",
  "action_value": "1k",
  "id": 28
}
```
We submit new rules using the POST method. Additionally, we must add more control to our flows by using foreign keys with the –F parameter. The required keys are the following:

- Name
- Source
- Destination
- Status (which have to be active when submitting new rule)
- Then

Some optional keys are:

- Comments
- Protocol
- Port
- Destination port
- Source port

Submitting a new rule:

Notice that “then” and “protocol” keys below take the whole path of the ID of the action and protocol. This is mandatory.

```
curl -X POST https://prod-fod.geant.net/api/routes/ -F "comments=My first rule from REST" -F "source=10.100.10.4/32" -F "destination=192.168.1.5/32" -F "name=Test1" -F "then=https://uat-fod.geant.net/api/thenactions/27/" -F "destinationport=89" -F "protocol=https://uat-fod.geant.net/api/matchprotocol/2/" -F "status=ACTIVE" -H 'Authorization: Token xxxx' | python -m json.tool
```
REST API – Having issues with REST API?

• Don’t forget that:
  • Field “name” does not accept spaces
  • The trailing slash ‘/’ in the end of each field. E.g. https://prod-fod.geant.net/api/routes/
  • To put the CIDR notation on the source/destination fields
  • Field “status” has to take ACTIVE in capital
Multi-port Range Support

- Historically, FoD users have to insert ports one by one to form a range on the FoD GUI

Now, it is possible that one can insert ranges
Now, it is also possible that one can see number of packets and bytes for a specific rule he applied.

There are two views, absolute and relative depicting traffic for the last 60 minutes.

In order to see history graph, one would need to click on the “rule name” from within “Rules” tab.
In case you have any issues or queries in relation to FoD, please contact GÉANT Infrastructure & Security team at security@geant.org