10-12-2021

Deliverable D8.7
Best Practices for DDoS Mitigation Strategies

Deliverable D8.7

Contractual Date:	31-12-2021
Actual Date:	10-12-2021
Grant Agreement No.:	856726
Work Package	WP8
Task Item:	Task 3
Nature of Deliverable:	R (Report)
Dissemination Level:	PU (Public)
Lead Partner:	DFN
Document ID:	GN4-3-21-514979
Authors:	H. Nussbacher (IUCC), J. Schönfelder (DFN-CERT), A. Moens (GÉANT Association), T. Coulouarn (DeIC), R. Mooi (GÉANT Association)

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).

Abstract

This deliverable provides an overview of current methods of detecting and mitigating Distributed Denial of Service (DDoS) attacks, to help NRENs identify areas for potential change or enhancement within their organisation, and presents the findings of a survey on the systems and processes used by NRENs to battle DDoS.

Table of Contents

Executive Summary 1

1 Introduction 2
1.1 Document Structure 2
1.2 Information Sources and Sensitivity 2
1.3 Scope 2

2 Detecting a DDoS Attack 4
2.1 Mechanisms for Detecting DDoS Attacks 4
2.1.1 NetFlow 4
2.1.2 Taps 7
2.1.3 Router CLI 7
2.1.4 Instinct 9
2.2 False Positives 10
2.2.1 Firewall Anomalies 10
2.2.2 State Table 10
2.2.3 Routing Loops 10

3 Mitigations 11
3.1.1 RTBH 11
3.1.2 ACL 12
3.1.3 Anti-Spoofing 12
3.1.4 Rate Limiting 13
3.1.5 Application/Server-Level Mitigation 13
3.1.6 Flowspec 14
3.1.7 BGP Diversion 14
3.1.8 Distribute Assets 14
3.1.9 Reduce Attack Surface 15
3.1.10 External DDoS Mitigation Provider 15

4 Workflow and Communication 17

5 Status at NRENs 19
5.1 Survey 19
5.2 Categories 24
5.2.1 NRENs Who Have GÉANT as their Single Upstream 24
5.2.2 NRENs Who Also Cater to Governments 25
5.2.3 NRENS Who Service Schools and School Systems 25
5.2.4 NRENs with a Diverse Peering Strategy 25

6 Conclusions 26
References 27
Glossary 29

Table of Figures

Figure 2.1: Example of a NetFlow-based DDoS report: Flowmon 5
Figure 2.2: Example of a NetFlow-based DDoS report: FastNetMon 6
Figure 2.3: Example of a NetFlow-based DDoS report: DFN-NeMo 7
Figure 2.4: CLI query and results example: Cisco IOS XE 8
Figure 2.5: CLI query example: Cisco IOS XR 9
Figure 2.6: CLI query results example: Cisco IOS XR 9
Figure 5.1: Responses to Survey Q3: number of DDoS attacks detected per month 19
Figure 5.2: Responses to Survey Q4: type of monitoring system used 20
Figure 5.3: Responses to Survey Q5: DDoS protection system on NREN network 20
Figure 5.4: Responses to Survey Q6: systems used locally 21
Figure 5.5: Responses to Survey Q7: use of GÉANT FoD 21
Figure 5.6: Responses to Survey Q8: use of GÉANT DDoS Cleansing and Alerting service 22
Figure 5.7: Responses to Survey Q9: frequency of detection for different types of attack 22
Figure 5.8: Responses to Survey Q10: worst effect of DDoS attack 23
Figure 5.9: Responses to Survey Q12: interest in DDoS mitigation collaboration 23
Figure 5.10: Responses to Survey Q13: DDoS mitigation expenditure 24

Executive Summary

This document provides an overview of current methods of detecting and mitigating Distributed Denial of Service (DDoS) attacks, to help National Research and Education Networks (NRENs) identify areas for potential change or enhancement within their organisation's DDoS mitigation strategy. It also presents the findings of a survey on the systems and processes used by NRENs to battle DDoS.

The primary mechanisms for detecting DDoS attacks are systems based on NetFlow (or comparable technologies, e.g. sFlow and IPFIX), network taps (physical and logical), and router command-line interface (CLI) queries. There will always be false positive alerts, possible causes of which could be firewall anomalies, state table and routing loops.

There are numerous techniques for mitigating a DDoS attack, including remotely triggered black hole (RTBH), access control list (ACL), anti-spoofing, rate limiting, application/server-level mitigation, flowspec, Border Gateway Protocol (BGP) diversion, distribute assets, reduce attack surface and external DDoS mitigation, such as cloud-based solutions.

Factors to consider in order to decide the most appropriate solution(s) include the proposed grade of automation as well as the size of the attacks to be mitigated within different points of the network.

Whatever the technical solution(s) selected, an organisation needs to set up, in advance, processes for who gets notified and who does what when a DDoS attack occurs. This involves pre-identifying stakeholders and knowing how to contact them.

During June 2021, a survey was sent to all GÉANT NRENs to gauge the systems and processes they use to battle DDoS; 20 NRENs responded. The findings indicate a diverse situation, which could be related to the different types of NREN. An attempt has therefore been made to categorise the various NREN types and assess the impact that type/category has on the solutions they might prefer for combatting DDoS attacks. The four categories are: NRENs who have GÉANT as their single upstream, NRENs who also cater to governments, NRENs who service schools and school systems, and NRENs with a diverse peering strategy.

As most NRENs fall into multiple categories, a differentiated strategy might be the best way forward at this time, together with enough trained personnel to successfully handle the workflows and communication that are required for effective DDoS attack handling.

1 Introduction

With Distributed Denial of Service (DDoS) attacks having long been a common network security threat, the GÉANT project tries to help the National Research and Education Network (NREN) community by summarising the best current practices adopted by members of the community for handling these attacks within the field of research networks.

This document is intended to provide an overview of the current methods of detecting, handling and mitigating DDoS attacks. By introducing the different aspects of DDoS-attack handling, it enables NRENs to identify areas in which there might be potential for change and enhancement within their organisation's DDoS mitigation strategy.

1.1 Document Structure

This document first addresses the monitoring aspects of DDoS and how an organisation can determine whether it is under DDoS attack (Section 2). It then covers the technical aspects of how to mitigate a DDoS attack (Section 3). Next it considers workflow and communication aspects: who needs to be kept in the loop and who needs to be notified when a DDoS attack occurs (Section 4). Finally, the document presents the situation at NRENs and what they have in place to handle DDoS attacks (Section 5), before drawing some general conclusions (Section 6).

1.2 Information Sources and Sensitivity

All the contents of this document are either based on discussions within the NREN community and the GÉANT project and Association or are outcomes of surveys within this community. Due to the sensitive topic as well as the proposed public dissemination of this document, no matching between techniques, mitigations, workflows and individual NRENs or research organisations is provided.

1.3 Scope

In line with the intended purpose of this document, while it presents an overview of all relevant methods to mitigate DDoS attacks, it does not aim to discuss what a DDoS attack is or what types of DDoS attacks exist in the wild. In addition, no detailed in-depth guides for specific situations are given. However, the overview of the different aspects of DDoS-attack handling provided here should offer NRENs starting points for further implementation, and suggestions for further reading, including a good basic explanation of DoS attacks and the difference between DoS and DDoS attack techniques [Wiki_DoSA], are provided in the References section at the end of this document.

2 Detecting a DDoS Attack

Almost all DDoS mitigation systems have some component which is intended to detect that the organisation is under DDoS attack. The challenge for an NREN, university or institution is determining a baseline of what is normal. For a bank or insurance company, that is easily done, but in academia a researcher could start downloading a 10TB dataset from 2–3 repositories which would be flagged as a DDoS attack. There will always be false positive alerts in any system and the trick is bringing down the level of false positives to a bare minimum without missing the real attacks.

This section covers primary mechanisms for detecting DDoS attacks, and some common causes of false positive alerts.

2.1 Mechanisms for Detecting DDoS Attacks

The primary mechanism for determining whether an organisation is experiencing a DDoS attack is via anomalies in data traffic patterns – usually in relation to volume, but for certain types of attacks there are also other changes in the patterns. These changes in traffic patterns can often be observed using whatever network monitoring system is in place, usually fed with data from the routers. This data can take the form of SNMP data, NetFlow (sFlow/IPFIX) exports, mirroring (via taps/SPAN ports), etc. This section covers:

- NetFlow.
- Taps.
- Router command-line interface.

2.1.1 NetFlow

The primary system for determining whether an organisation is under DDoS attack is via a NetFlow (or comparable technology) based system. Numerous NetFlow-based systems exist, some built into a commercial DDoS solution and some standalone.

NetFlow was created by Cisco in 1996 and is a proprietary technology [NetFlow]. In general there are netflow exporters, typically routers; netflow collectors, which merge and process all the flow data arriving from all the different devices; and netflow analysis tools, which display the data in a manageable form – in the present case, DDoS analysis engines.

NetFlow does not export payload data, only metadata. This would include the standard tuple fields (including source IP address, destination IP address, source port number, destination port number), as well as some other parts depending on the version of NetFflow being used. NetFlow is already up to v9 (created in 2009), although the most common NetFlow version is v5. Due to the high volume of flows, most organisations will do “netflow sampling” – 1:10, or 1:100 and sometimes even 1:1000.

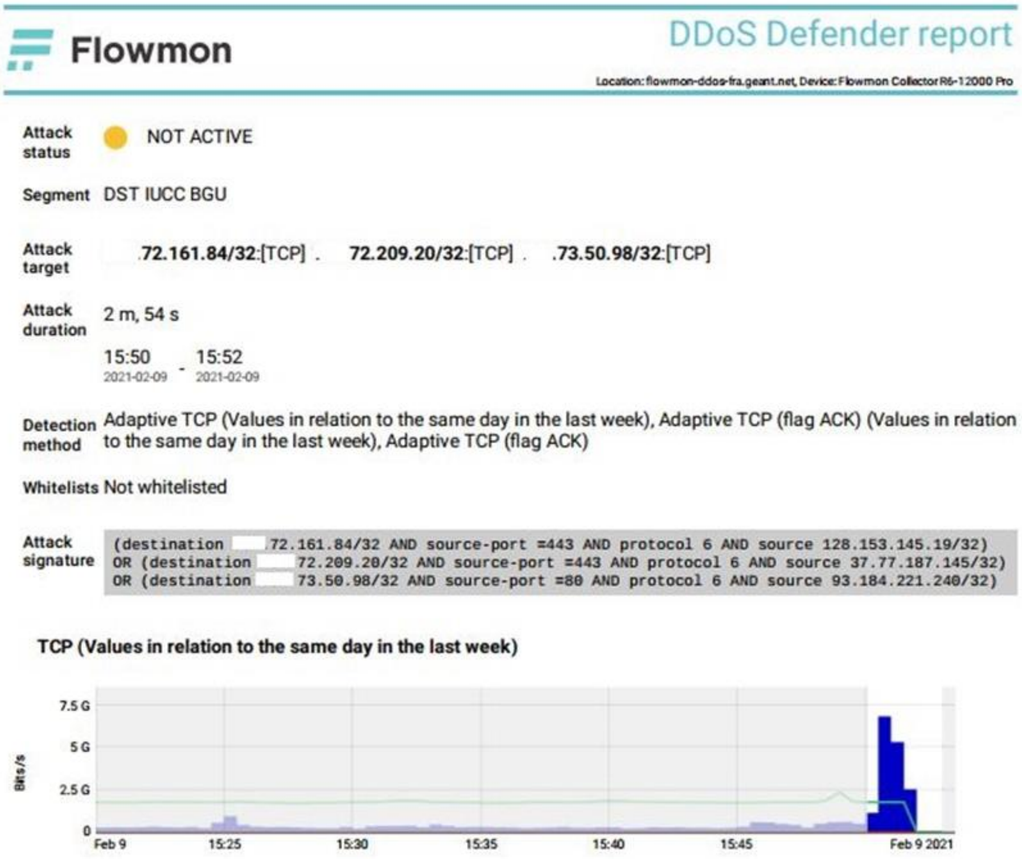
sFlow, which stands for sampled Flow, is a technology created and owned by the sflow.org consortium [sFlow]. sFlow is limited in that it cannot handle 1:1 sampling. Sampling is an integral part of sFlow.

Internet Protocol Flow Information Export (IPFIX) is an IETF protocol [IPFIX]. Both sFlow and IPFIX were created because people did not like the monopoly that Cisco has over export flow technology. Drafted in 2002–2003 and created in 2004, IPFIX used NetFlow v9 as a basis for the design.

Nowadays, due to these three competing technologies, most router vendors support all three common flow technologies.

NetFlow-based detection is obviously only possible when one has access to flow data relevant to the to-be-protected network. This might limit the use for systems hosted outside the organisation.

One example of a NetFlow-based DDoS report is shown in Figure 2.1 below:



Flowmon

DDoS Defender report

Location: flowmon-ddos-fra.geant.net, Device: Flowmon Collector R6-12000 Pro

Attack status ● NOT ACTIVE

Segment DST IUCC BGU

Attack target .72.161.84/32:[TCP] . 72.209.20/32:[TCP] . .73.50.98/32:[TCP]

Attack duration 2 m, 54 s

15:50 2021-02-09 - 15:52 2021-02-09

Detection method Adaptive TCP (Values in relation to the same day in the last week), Adaptive TCP (flag ACK) (Values in relation to the same day in the last week), Adaptive TCP (flag ACK)

Whitelists Not whitelisted

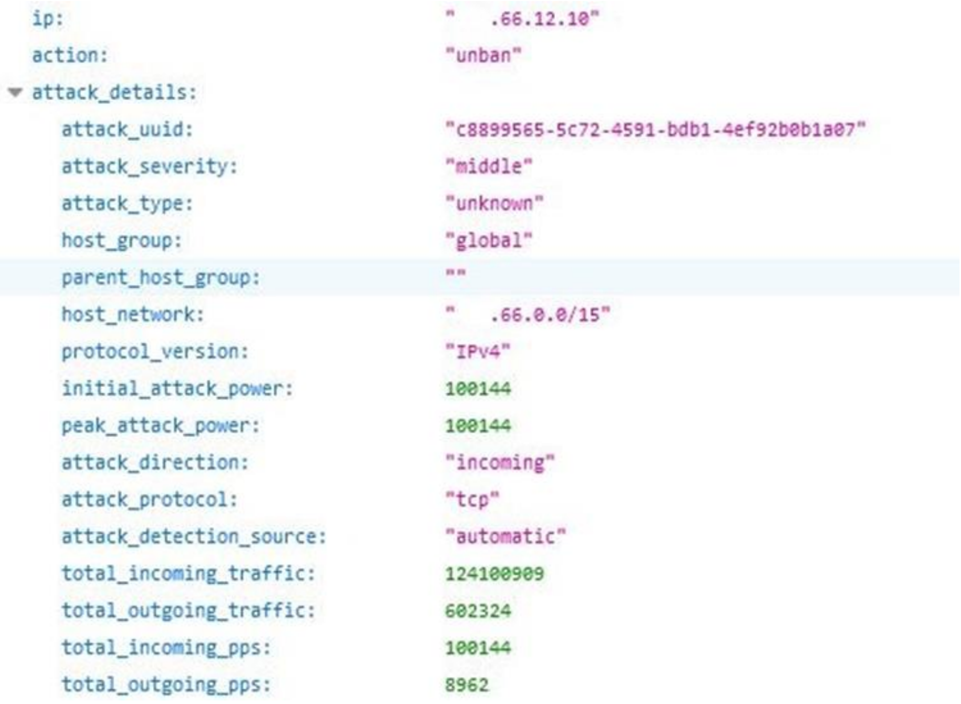
Attack signature

```
(destination     .72.161.84/32 AND source-port =443 AND protocol 6 AND source 128.153.145.19/32)
OR (destination     72.209.20/32 AND source-port =443 AND protocol 6 AND source 37.77.187.145/32)
OR (destination     73.50.98/32 AND source-port =80 AND protocol 6 AND source 93.184.221.240/32)
```

TCP (Values in relation to the same day in the last week)

Figure 2.1: Example of a NetFlow-based DDoS report: Flowmon

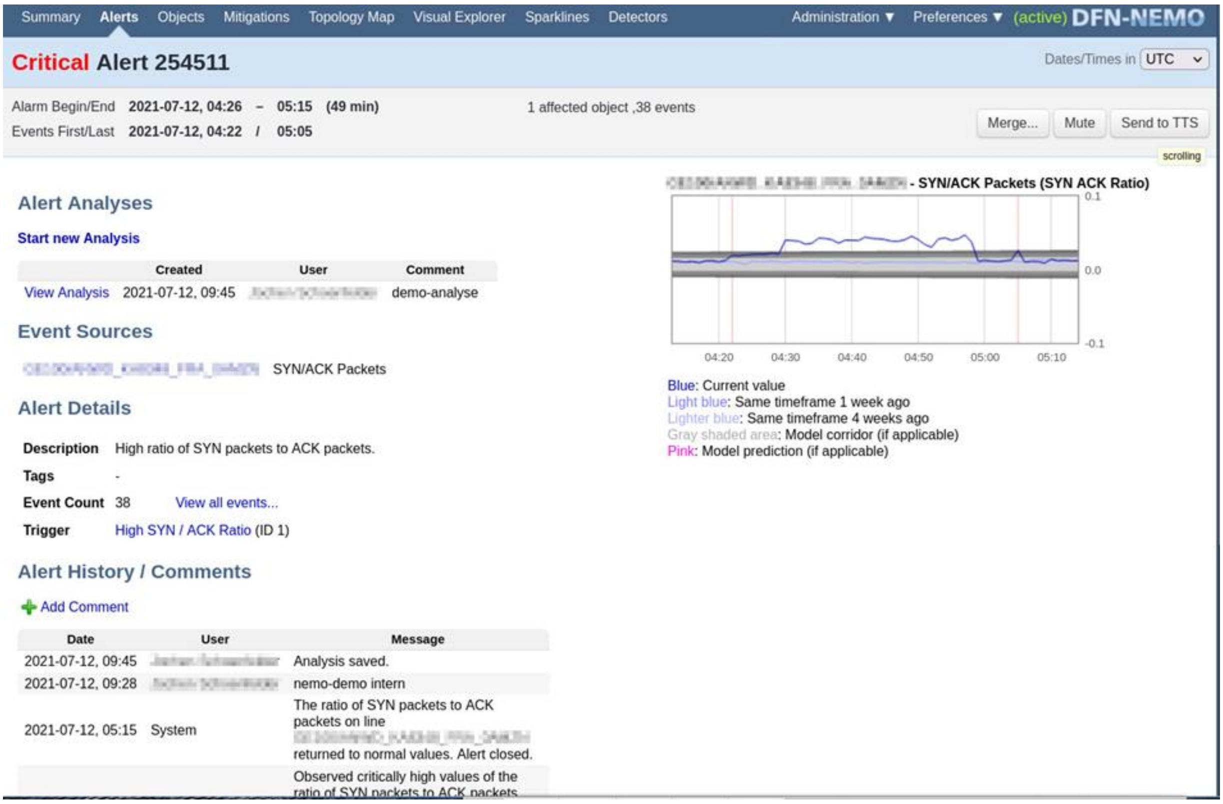
Another example is FastNetMon, which sends out emails with JSON:



```
ip:                              "   .66.12.10"
action:                          "unban"
▾ attack_details:
    attack_uuid:                 "c8899565-5c72-4591-bdb1-4ef92b0b1a07"
    attack_severity:             "middle"
    attack_type:                 "unknown"
    host_group:                  "global"
    parent_host_group:           ""
    host_network:                "   .66.0.0/15"
    protocol_version:            "IPv4"
    initial_attack_power:        100144
    peak_attack_power:           100144
    attack_direction:            "incoming"
    attack_protocol:             "tcp"
    attack_detection_source:     "automatic"
    total_incoming_traffic:      124100909
    total_outgoing_traffic:      602324
    total_incoming_pps:          100144
    total_outgoing_pps:          8962
```

Figure 2.2: Example of a NetFlow-based DDoS report: FastNetMon

A final example of a NetFlow processing system is the DFN-NeMo system, an open source detection and analysis tool developed by DFN to address the needs of a large NREN [NeMo]:



Critical Alert 254511

Alarm Begin/End 2021-07-12, 04:26 – 05:15 (49 min)
Events First/Last 2021-07-12, 04:22 / 05:05

1 affected object ,38 events

Alert Analyses

Start new Analysis

	Created	User	Comment
View Analysis	2021-07-12, 09:45	[redacted]	demo-analyse

Event Sources

[redacted] SYN/ACK Packets

Alert Details

Description	High ratio of SYN packets to ACK packets.
Tags	-
Event Count	38 View all events...
Trigger	High SYN / ACK Ratio (ID 1)

Alert History / Comments

Add Comment

Date	User	Message
2021-07-12, 09:45	[redacted]	Analysis saved.
2021-07-12, 09:28	[redacted]	nemo-demo intern
2021-07-12, 05:15	System	The ratio of SYN packets to ACK packets on line [redacted] returned to normal values. Alert closed.
		Observed critically high values of the ratio of SYN packets to ACK packets

[redacted] - SYN/ACK Packets (SYN ACK Ratio)

Blue: Current value
Light blue: Same timeframe 1 week ago
Lighter blue: Same timeframe 4 weeks ago
Gray shaded area: Model corridor (if applicable)
Pink: Model prediction (if applicable)

Figure 2.3: Example of a NetFlow-based DDoS report: DFN-NeMo

2.1.2 Taps

A network tap comes in two flavours: physical and logical. A physical tap would be a simple box which takes a fibre and, using tiny micro-mirrors, splits the traffic to one or more output ports. This way, numerous copies can be made of the incoming traffic so that it can be processed out of band. The logical method would be via what is known as a Switched Port Analyser (SPAN) or mirror port, whereby the router itself duplicates the traffic and sends the duplicated traffic to a destination port.

By diverting one of these “splits” to a packet sniffer system which uses tcpdump or Wireshark (packet analysers), a network administrator can try to understand what is happening in the network. However, that is like trying to drink from a firehose. That is why it is customary to send the duplicated traffic to a dedicated, customised DDoS analysis engine similar to those mentioned in Section 2.1.1 above.

The difference is that, with a network tap, there is no sampling and the traffic is 1:1.

2.1.3 Router CLI

Before the existence of the dozens of different NetFlow analysis engines with their user-friendly graphs and automated emails, the network administrator had to use the router command-line interface (CLI) as a tool to retrieve flow data and process it.

An example of a Cisco IOS XE CLI query and its results is show in Figure 2.4:

```
OpenRtr#sho ip cache flow
IP packet size distribution (502617M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .001 .372 .040 .029 .018 .011 .012 .004 .005 .006 .006 .003 .002 .006 .001

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .001 .002 .003 .026 .441 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 0 bytes
  199479 active, 521 inactive, 2239582258 added
  76834381 ager polls, 3106410521 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total     Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows      /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet  2361180720     549.7         1    41    704.2       0.6      30.3
TCP-FTP      171036528      39.8         1    41     45.3       0.1      30.3
TCP-FTPD      24532091       5.7         1    40      6.3       0.0      30.3
TCP-WWW      880401483     204.9        46   991   9543.4       1.6      30.1
TCP-SMTP      97436137      22.6        22   657    519.1       1.2      30.2
TCP-X         89896411      20.9         1    43     22.2       0.0      26.3
TCP-BGP       15801472       3.6         1    42      4.0       0.0      30.0
TCP-NNTP      15615027       3.6         1    41      3.9       0.0      30.3
TCP-Frag          6151       0.0         3   425      0.0       2.3      30.3
TCP-other  65716212591   15300.7         5   597  89697.1       0.3      28.9
UDP-DNS      678311665     157.9         1    79    202.2       0.0      30.4
UDP-NTP      266747550      62.1         1   117     74.0       0.0      30.4
UDP-TFTP      26970325       6.2         1    43      6.9       0.0      30.2
UDP-Frag        524851       0.1       111   227     13.6       6.9      29.8
UDP-other   4546731789    1058.6        14  1181  15266.8       0.1      27.8
ICMP         344160447      80.1         2    64    182.8       0.7      30.2
IGMP            699867       0.1         1    44      0.1       0.0      30.4
IPINIP              15       0.0         1    25      0.0       0.7      30.1
IPv6INIP        639793       0.1         1    87      0.2       0.7      30.6
GRE            3740993       0.8         1   320      1.4       3.0      30.1
IP-other      13388401       3.1         2    97      7.0       4.3      29.0
Total:     75254034307   17521.4         6   700 116301.4       0.3      28.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
te0/3/0.1     195.54.161.152  NULL          12.233.78.126   06 ce48 aa3a     1
te0/3/0.1     193.27.229.207  NULL          12.233.122.55   06 bec7 4b51     1
te0/3/0.1     195.54.161.152  NULL          12.233.150.14   06 ce48 1cad     1
te0/3/0.1     45.141.84.30    NULL          12.233.71.113   06 d78f 857a     1
te0/3/0.1     45.141.84.30    NULL          12.233.217.127  06 d78f 6a9b     1
te0/3/0.1     193.27.229.207  NULL          12.233.185.231  06 bec7 4930     1
te0/3/0.1     185.40.4.132    NULL          147.233.24.214  11 13ce 0401     1
…
```

Figure 2.4: CLI query and results example: Cisco IOS XE

The problem is that the list of individual flows can go on for many tens of thousands of lines, so some sort of scripting would be needed to aggregate results.

Larger Cisco routers, which use IOS XR, have a slightly different CLI syntax to query flows. An example query is shown in Figure 2.5 below:

```
show flow monitor fmp-nfsen cache  match ipv4 destination-address eq 128.139.0.0/16
incl ipv4 protocol  source-address destination-address layer4 source-port-overloaded
destination-port-overloaded eq 53 counters  packets sort counters packets top 100
location 0/0/CPU0
```

Figure 2.5: CLI query example: Cisco IOS XR

The resulting output would be as follows:

```
Cache summary for Flow Monitor fmp-nfsen:
Cache size:                          12000
Current entries:                     12000
Flows added:                    2701572382
Flows not added:              231027930651
Ager Polls:                       14195856
  - Active timeout               382405957
  - Inactive timeout            2219156568
  - TCP FIN flag                  99997857
  - Emergency aged                       0
  - Counter wrap aged                    0
  - Total                       2701560382
Periodic export:
  - Counter wrap                         0
  - TCP FIN flag                         0
Flows exported                  2701560382

IPV4SrcAddr      IPV4DstAddr      L4SrcPort  L4DestPort IPV4Prot PacketCount
95.211.31.219    128.139.251.9    443        24497      tcp      3527
85.17.233.108    128.139.251.9    443        6792       tcp      2979
37.77.187.142    128.139.225.226  443        64083      tcp      2921
162.159.192.1    128.139.225.226  2408       51399      udp      1879
95.211.219.143   128.139.251.9    443        24163      tcp      1460
216.58.214.10    128.139.17.40    443        62159      tcp      1358
142.250.179.170  128.139.17.40    443        62128      tcp      1330
37.77.187.142    128.139.225.246  443        55754      tcp      1220
…
```

Figure 2.6: CLI query results example: Cisco IOS XR

Clearly a CLI cannot be used for constantly determining whether an organisation is under DDoS attack, but it does give the ability to quickly determine packet flows when no functioning NetFlow analysis tool is available.

2.1.4 Instinct

Occasionally, one just has to rely on one’s instinct. It could be that the DDoS attack has started and the organisation’s monitoring system requires 15–30 minutes to report on the attack. It could be that some new-style DDoS attack is taking place and the organisation’s monitoring system is not tuned to pick it up. It could be that the DDoS attack is flying just under the thresholds needed for the organisation’s system to send out an alert.

In these cases, a trained and experienced network administrator will start suspecting a DDoS attack. Unfortunately, the number of tools available to the network administrator to quickly determine whether an actual DDoS attack is taking place is limited.

2.2 False Positives

There are many times when it seems a DDoS is taking place when in fact it is not a DDoS at all but rather something that looks and feels like a DDoS attack. Possible causes of these false positives include firewall anomalies, state tables and routing loops. Each of these is described below.

2.2.1 Firewall Anomalies

It may happen that something causes a firewall to act up. The users believe they are under DDoS attack and the network administrators will believe they are under DDoS attack when it is just a matter of a firewall that has failed. This can be caused by simply encountering a massive external port scan on a large number of IP addresses which causes the state table in the firewall to have issues. Improper protocol implementations can also cause unexpected issues. Often, a simple reboot of the firewall will clear out any stalled processes.

2.2.2 State Table

It may not be only the firewall that has issues but any server – such as a web server – which can display DDoS-like issues simply because its state table has filled up [STF]. This phenomenon can also be caused by port table exhaustion [PTE].

2.2.3 Routing Loops

A simple error with regard to routing can cause packets to loop, which will be perceived as a DDoS attack.

3 Mitigations

There are numerous techniques a network administrator can use to try to mitigate a DDoS attack. Factors to consider in order to decide between them include the proposed grade of automation as well as the size of the attacks to be mitigated within different points of the network.

From discussions in the NREN community there seems to be a current consensus that the further away from the end user a mitigation takes place, the less automation is needed. One could justify this view by considering that an attack mitigation within the backbone of an NREN most possibly might affect more network traffic and most possibly would be done with less knowledge about the attacked service than a countermeasure within a system placed directly in front of the attacked service.

In addition, an NREN might decide that most brief DDoS attacks would not disturb the functionality of its backbone in a way that would justify intercepting the network traffic by a mitigation, which could – as a side effect – even affect security research itself.

The relevant mitigation techniques are as follows:

- Remotely triggered black hole (RTBH).
- Access control list (ACL).
- Anti-spoofing.
- Rate limiting.
- Application/server-level mitigation.
- Flowspec.
- Border Gateway Protocol (BGP) diversion.
- Distribute assets.
- Reduce attack surface.
- External DDoS mitigation.

Each of these is described below.

3.1.1 RTBH

Remotely triggered black hole (RTBH) was first documented via RFC3882 “Configuring BGP to Block Denial-of-Service Attacks” [RFC3882] but was presented in 2004 at North American Network Operators’ Group (NANOG) 30 in a presentation called “Customer-Triggered Real-Time Blackholes” [CTRTB].

RTBH is based on Border Gateway Protocol (BGP) and requires setup prior to being attacked by DDoS. With RTBH, the customer triggers the RTBH activity via their BGP session with their ISP. There is a specific BGP community that has to be used, as detailed in RFC7999 “Blackhole Community” [RFC7999]. The customary community to use would be 65535:666, where 65535 means “no-export” (since only the upstream needs to hear the RTBH and no one else) and 666 is the registered RTBH number.

In general, most ISPs will only want to accept a /32 (prefix length) as an RTBH and no larger prefix. Once the customer encounters the DDoS attack, they need to announce the victim IP (/32) via RTBH to their upstream, which has been pre-set to know what to do with such an announcement. The upstream ISP now drops all traffic destined to the victim. This then becomes “destination-based RTBH”.

Note that in 2004 this was considered state of the art, even though it meant that the victim was effectively removed from the Internet. This was considered necessary in order to protect the other IPs which were not being DDoSed at the time.

There is an additional variant known as “source-based RTBH” [SBRTBH], in which by combining the standard RTBH with Unicast Reverse Path Forwarding (uRPF) loose-checking on edge interfaces, the blackholing system can be utilised to block source IPs. Unfortunately, this was not widely implemented on the Internet, primarily because of the high level of difficulty.

3.1.2 ACL

Access control lists (ACLs) should be considered an organisation’s first line of defence. It is possible to pre-define preventative ACLs as well as on-demand specific ACLs.

As an example of preventative ACLs, an organisation might consider blocking udp/0 and tcp/0. Each organisation can decide which ports should be blocked. Some might block external NetBIOS (tcp+udp 137–139), since this protocol should not be coming in from outside your organisation. Some might pre-block defunct protocols such as Finger (tcp/79). Again, it is up to each organisation to determine which ports it wishes to pre-block and to inform its clientele.

However, ACLs are usually used to block an existing attack. If the network administrator sees certain IPs or IP ranges DDoSing their network, they can institute an ACL to block all traffic from those specific IPs. But that will only work under certain, very limited circumstances.

In general, when a DDoS happens, it will be coming from thousands of random IP addresses. It is quite difficult to quickly build an ACL to block 3,000 IP addresses. The organisation can therefore decide to block the victim IP via an ACL, and if the attack is targeted to a specific port on the victim IP, then an ACL for a specific IP and destination port makes it an easy option to quickly block the attack.

3.1.3 Anti-Spoofing

In order to cut down the attack footprint, anti-spoofing measures can be defined. An easy one to define would be to not allow the organisation’s own network IPs to enter the network from abroad, as clearly someone has spoofed the organisation’s IPs and is using those spoofed IPs to be part of the DDoS attack. The technology used is called Reverse Path Forwarding (RPF) [RPF] and was initially defined in RFC2287 in 2000 [RFC2287]. Since then it has undergone a number of changes and uRPF

(Unicast Reverse Path Forwarding) is now defined via RFC8704, "Enhanced Feasible-Path Unicast Reverse Path Forwarding" [RFC8704].

There are other anti-spoofing measures an organisation can take. No private IP addresses (RFC1918) [RFC1918] should be entering the network from abroad, so these too should be blocked. An organisation can also refer to the IANA table of special and reserved IP addresses [IANA_SPAR] and some of these, too, should be pre-blocked as an anti-spoofing method.

3.1.4 Rate Limiting

DDoS attacks come in many flavours and styles. Many ports can be used for amplification attacks, such as udp/123 (NTP), tcp+udp/19 (CHARGEN), tcp+udp/17 (QOTD), which are known to have a high amplification factor. There are also tcp-syn floods, tcp-ack floods, syn-rst floods and any other combination the imagination can conjure. All of these can be pre-rate-limited. If an organisation knows that the maximum bandwidth incoming for CHARGEN is 1 Mb/sec, it can rate-limit CHARGEN to 5 Mb/sec. If an organisation knows that the maximum bandwidth ever seen for tcp-syns was 500 Mb/sec, it can pre-set a rate-limit for 1.5 Gb/sec for tcp-syns. It is very popular to rate-limit ICMPs. An organisation can select a target number and apply a rate limit to ICMP and not just ICMP echo requests.

Rate limits can be defined based on source or destination. Destination rate limiting for a single IP may lead to unknown issues. Equally, rate limiting based on a single source IP first needs to be checked to ensure that the IP is not some multi-use system and that by rate limiting it some service of which the network administrator is not aware is hurt.

Baselining and benchmarking are key to determining what thresholds to place on rate limiting – especially when based on ports. That is why it is difficult, since traffic patterns change over time. Most network administrators try to avoid using rate limiters when mitigating DDoS attacks and will just use an ACL to block the source or destination.

3.1.5 Application/Server-Level Mitigation

In general, a DDoS attack will affect an organisation's entire network, not just one specific server. However, there are cases where the attackers target just one specific server via a DDoS attack. In that case, pre-planning can help mitigate the attack. Any server needs to have all the necessary resources to be able to function, such as an increased buffer size or many more threads than under normal conditions. The key is to over-provision the organisation's critical servers so that even when hit with massive numbers of requests they will not buckle.

Occasionally, a load balancer can be inserted into the solution so as to distribute the increased load among multiple servers or even among different geographies. Another technique would be to employ a firewall that is capable of geo-blocking. If the attack is coming from one specific country, then geo-blocking is any easy solution to the DDoS attack.

In general, however, DDoS attacks are not against specific servers but can be targeted against dorm-room IPs or even non-allocated IP addresses within an organisation. When an organisation has thousands of IP addresses, each and every one of them needs to be protected from DDoS attack.

3.1.6 Flowspec

Flowspec was created by the IETF back in 2009 (in RFC5575) but has undergone many revisions and is now up to RFC8955, which came out in December 2020 [RFC8955]. Flowspec may be thought of as the next generation of RTBH.

Flowspec allows the matching of flows based on numerous fields, including src-ip, dst-ip, src-port, dest-port, ICMP code, packet length, DSCP, TCP flags and more. There is usually a primary Flowspec router which distributes flowspec rules to all the other routers in its ASN. The edge routers can be directed to rate-limit, mark, redirect or drop traffic.

In general, Flowspec is operated and managed within a specific ASN. Network operators do not yet feel comfortable allowing Flowspec to cross ASN boundaries as they do with RTBH or using a specific community to signal to drop traffic. A case in point would be the five-hour outage of one of the largest ISPs in the world, CenturyLink/Level 3, which was caused by something related to Flowspec [CLL3O].

3.1.7 BGP Diversion

Diversion of traffic for the purposes of analysis, cleaning of malicious traffic and reinsertion into the Internet has been a game changer for handling DDoS attacks. In order to divert traffic, BGP announcements are usually played with. One method is to announce a shorter prefix (for example, /24) than the announcement appearing on the Internet (for example, a /22). Another method is to use AS prepending in order to fictitiously lengthen the AS-path of the original victim. Another method is to simply withdraw the prefix and allow the “diverter” to announce the original prefix. The most common method is the first method – using a more specific prefix length.

The easy part is diverting the traffic; the harder part is reinjecting the cleaned traffic back into the Internet. This requires delivering the traffic to the intended target and bypassing the diversion that is taking place on the Internet. This is usually accomplished via a GRE tunnel from the diverter to the victim network whereby all the cleaned traffic can be sent, unaffected by the diversion. See Section 3.1.10 for how this method is used commercially.

This concept was first documented and patented in 2000 [BGPDP]; the patent was awarded to Cisco in 2006, and expires in 2022.

3.1.8 Distribute Assets

One of the system vulnerabilities that allow a DDoS attack to be effective is when an organisation has all its IP assets in one spot, which is 99% the case with every organisation. It is difficult for a university in Rome, for example, to divide its IP assets and place some of them in different countries and in different continents. However, that is exactly what cloud computing can accomplish. Many critical servers and services (DNS, ERP, CRM, etc.) can be placed within various cloud providers, thereby making it more difficult to DDoS a specific service, although purchasing anti-DDoS mitigation from a cloud provider can be costly.

Another common way to distribute assets is to use IP anycast, which nowadays is primarily used for DNSs and Content Delivery Networks (CDNs). However, this requires that the owner purchase or acquire access to multiple servers worldwide and advertise all those servers to the Internet via the exact same IP address, as well as synchronise the data behind each instance.

3.1.9 Reduce Attack Surface

A DDoS mitigation approach not commonly used by network administrators is to reduce the attack surface by limiting the prefixes announced. If an organisation has a /16 (65,536 IPs), there is a high probability that not all 65K IP addresses are in use or even allocated. It is a painstaking exercise but one that can be accomplished by going through all IP allocations and only announcing /24s that are in use rather than the easily announced /16s.

Another, similar method is to switch as many public IP addresses to using Network Address Translation (NAT) as possible. Rather than announce a /16, an organisation can switch to NAT and only announce a /24 to the Internet. Again, this is painstaking and requires time and effort but can be done to reduce the IP attack surface. A comparable reduction could be achieved by setting a stateful firewall between the organisation and the Internet.

However, the complexity of managing this firewall or NAT device for a larger organisation, as well as these devices then being an attack target themselves, has to be considered.

3.1.10 External DDoS Mitigation Provider

The basic concept of an external, cloud-based solution for DDoS mitigation is for the DDoS cloud mitigator to announce the organisation’s “under attack” network prefix via their numerous points of presence (PoPs) scattered throughout the world (using BGP), divert all the traffic destined to the organisation’s local victim to their PoPs, clean out the attack traffic and then pass only the clean traffic onward to the intended victim.

As with almost all DDoS mitigation techniques, this involves advance setup and pre-planning and cannot be performed when under attack. The two different types of mitigation that the cloud providers offer are “always on” or “on demand”.

“Always on” means that the cloud mitigator is always announcing your prefix, which means all your traffic is always flowing via the mitigator. This introduces an extra amount of delay as well as cost. Moreover, it is only suitable for 1–2 fixed servers and not for an entire network. The other option is “on demand”, whereby the customer alone decides when it considers itself to be under attack and, via some signalling method, informs the DDoS mitigator to start announcing the prefix of the to-be-protected attack targets. This means the DDoS attack can last at least 5–15 minutes before it gets mitigated.

Some ISPs provide this as part of a service for their customers but there are a few companies that specialise in providing this type of cloud DDoS mitigation:

- Akamai
- F5
- Radware
- Neustar

- Imperva
- Cloudflare
- Netscout (Arbor).

Each of the above companies creates its own “scrubbing centre”, either using custom-designed hardware and software or using one or more of the following specialised boxes that handle the scrubbing aspect:

- Radware DefensePro
- FortiDDoS
- F5 Advanced Firewall Manager
- A10 Thunder APS
- Arbor TMS.

After scrubbing the traffic for the customer, the cloud mitigator needs to deliver that cleaned traffic back to the customer, which is usually done via some sort of GRE tunnel, thereby bypassing the diversion that would normally create a routing loop.

One of the reasons why many organisations opt to use a cloud-based solution for DDoS mitigation is because they do not want to spend money on purchasing a box that would have to sit in-line (which is always an issue for network administrators) and would need to be upgraded and managed in a similar way to a local firewall.

However, an important aspect when examining this type of vendor, in order to achieve the optimum benefit, is to determine how many points of presence (PoPs) they have worldwide and how much inbound capacity they can handle (measured in Tb/sec).

Lastly, all vendors count the number of IP addresses under mitigation and charge accordingly. Most organisations have a /24 (255 IP addresses) and some larger organisations might even have a /22 (1,024 IP addresses). In the world of NRENs, almost all NRENs have in excess of 1M IP addresses (GARR – 2.7M, IUCC – 1.1M, Jisc – 7.3M), which vastly affects the pricing for this service.

4 Workflow and Communication

Up to this point, the document has covered numerous technical aspects of detection and mitigation. However, even if an organisation implements the best technical solutions the market has to offer, it will still end up with disrupted services and impacted users when a DDoS attack occurs. The organisation needs to set up, in advance, processes for who gets notified and who does what when a DDoS attack occurs. This involves pre-identifying stakeholders and knowing how to contact them.

Assume the organisation's system identifies that three universities are under DDoS attack. Who is contacted? What if the attack is at 2 a.m. on a Saturday? Who would know the consequences in case an attack or a countermeasure restricts the traffic to a certain network? Sending an email will not work reliably since the contact person may not be online and even if they are, the email may not get through since they are under DDoS attack. Therefore, it is imperative that for every client for which the organisation provides DDoS mitigation, some sort of Out Of Band (OOB) method to contact them (messenger service or phone, preferably mobile, as Voice over IP (VOIP) components might be affected by the DDoS as well) on a 24x7 basis has been agreed and is in place.

However, during daytime hours, when students and faculty are dependent on the Internet, merely notifying the technical contact may not be enough. When the entire access to the Internet is down for three hours due to a DDoS attack and students are taking online tests, there needs to be contact with upper management (such as the rector, president, CEO) of the university. In addition, since phone explanations in a situation like this can take 10–15 minutes per person, the organisation will need staff whose sole task is to maintain a line of communication with the upper management of its clients. The person handling the hands-on CLI cannot stop for 30 minutes and start explaining what is being done to mitigate the attack.

Within NRENs who offer DDoS protection, the following workflow building blocks seem to be common ground:

- Definition of which attacks can be mitigated without previous end-user / end-user organisation communication. This might be all attacks where the NREN's backbone functionality is at risk, as well as any well-known attacks.
- Definition of who to contact within affected organisations and how, in case of attack detection or mitigation.
- Definition of which authorisations are needed in the different cases of attacks (mostly dependent on whether they are relevant to the backbone) and how to obtain them.
- Definition of communication channels over which DDoS-affected organisations can notify the NREN and ask for support.

While some NRENs might consider the DDoS-related workflows to be part of the established services performed by Network Operations Centre (NOC) or Computer Security Incident Response Team (CSIRT) personnel, this also might be part of a separate service where separate communication channels are used.

5 Status at NRENs

This section presents the situation at NRENs with regard to DDoS detection and mitigation. It describes the survey by which the status information was obtained, and, based on findings and feedback, attempts to categorise types of NRENs to help them identify preferred solutions.

5.1 Survey

During June 2021 a survey was sent to all GÉANT NRENs. Its purpose was to gauge the systems and processes all NRENs use to battle DDoS. A simple Google form was used and was sent to targeted network administrators in each NREN. The graphs below represent the responses from 20 NRENs: ACOnet, CARNET, CESNET, CyNet, DFN, EENet, FCCN, GARR, GRENA, GRNET, HEAnet, IUCC, KIFÜ, PIONIER, RASH, RedIRIS, RENAM, RENATER, SWITCH and URAN.

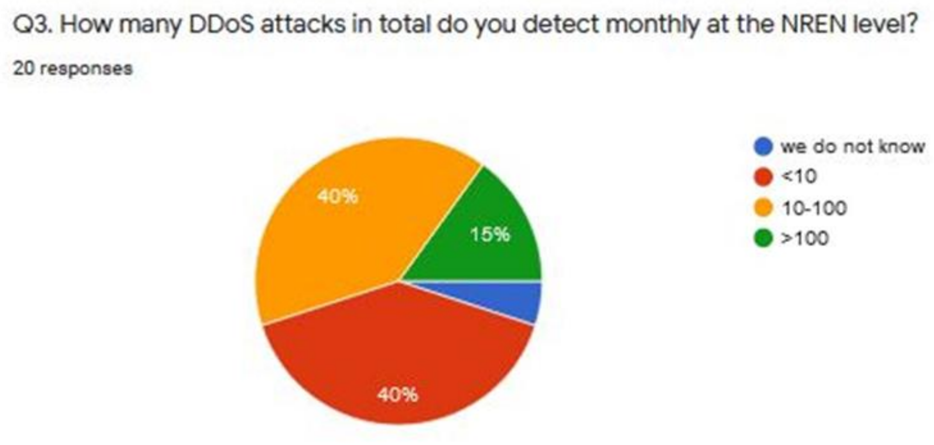


Figure 5.1: Responses to Survey Q3: number of DDoS attacks detected per month

Figure 5.1 shows that almost every NREN undergoes some sort of DDoS attack, although from this graph it is not possible to know whether the attacks had an adverse effect on the NREN or not.

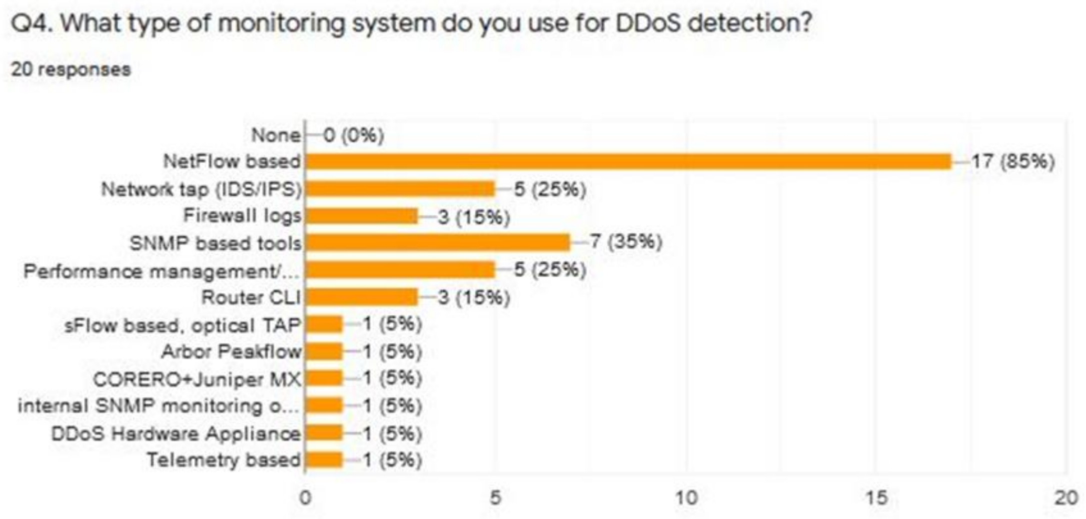


Figure 5.2: Responses to Survey Q4: type of monitoring system used

Figure 5.2 shows that 85% of all NRENs use some sort of NetFlow-based system for determining whether they are under attack or not. It can also be deduced that many NRENs use more than one system for alerting them to DDoS attacks, although NetFlow is the primary system used.

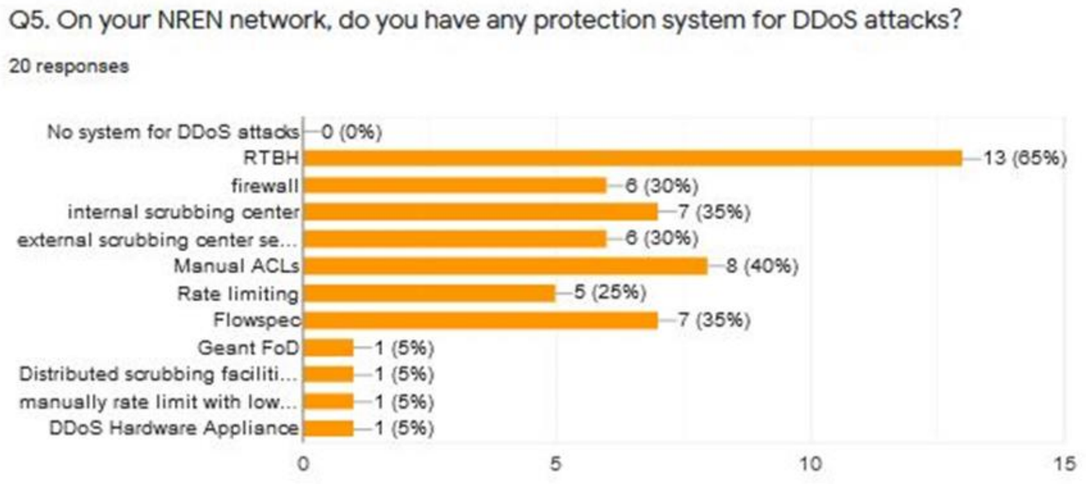


Figure 5.3: Responses to Survey Q5: DDoS protection system on NREN network

Figure 5.3 reveals the perhaps surprising finding that most NRENs still use an RTBH process to handle DDoS attacks, indicating that more mature solutions (RTBH is a 17-year-old technology) continue to be valid and useful. It can also be deduced that all NRENs use multiple technologies to mitigate DDoS attacks. In addition, the figure shows that 13 NRENs use either an internal or external scrubbing centre service – a number that will probably increase every year.

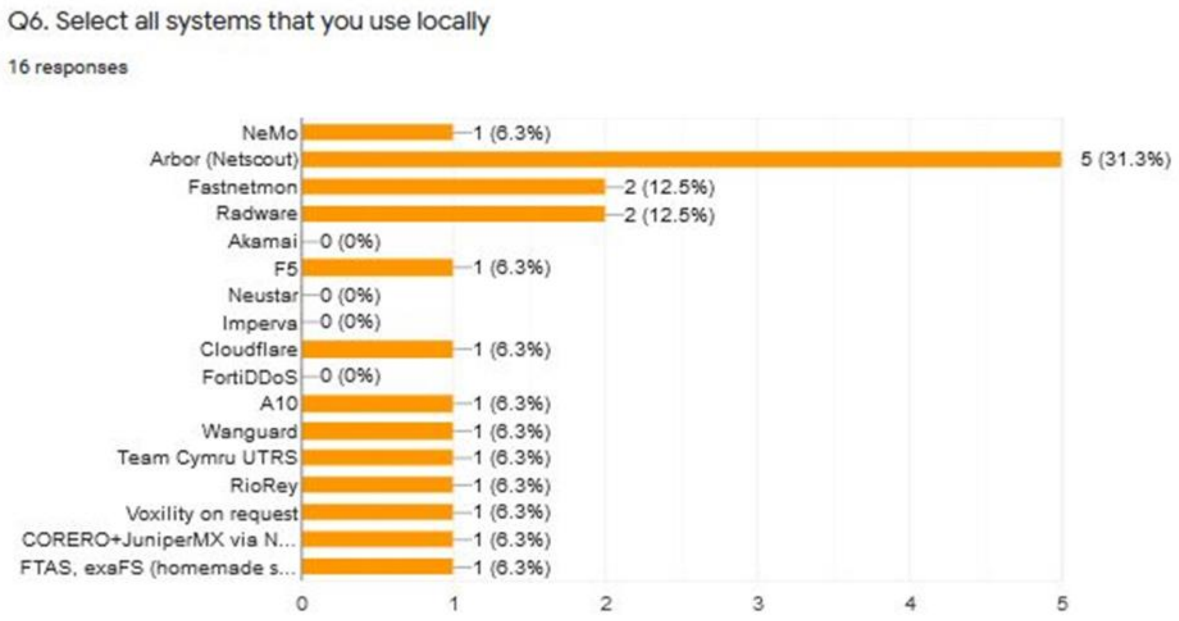


Figure 5.4: Responses to Survey Q6: systems used locally

From Figure 5.4 it can be seen that the most popular system in use is an external commercial system known as Netscout (previously known as Arbor), which is an external scrubbing service, although there is no clear popular system in use by a majority of NRENs.

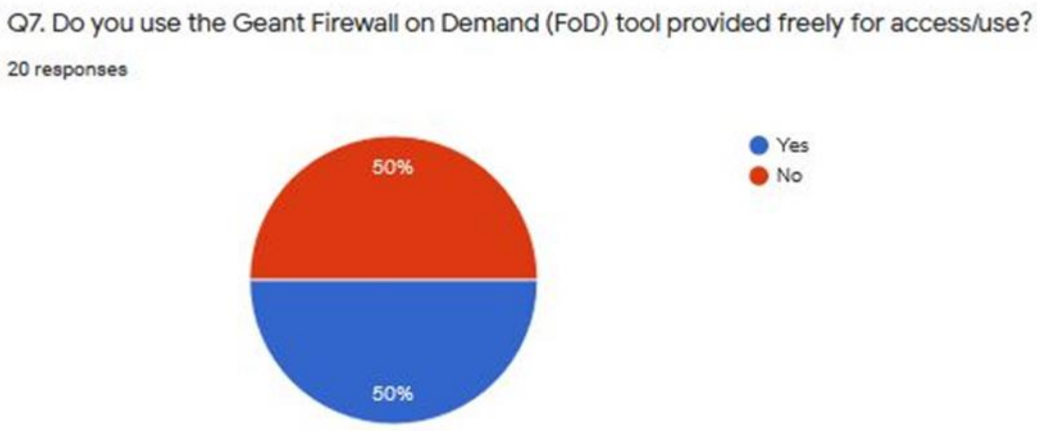


Figure 5.5: Responses to Survey Q7: use of GÉANT FoD

Of the 20 NRENs polled, half stated that they use the free[1] GÉANT Firewall on Demand (FoD) service (Figure 5.5).

[1] FoD is a no-cost option for all GÉANT peering users and remains available to support DDoS mitigation for other users and for inter-NREN DDoS attacks [FoD].

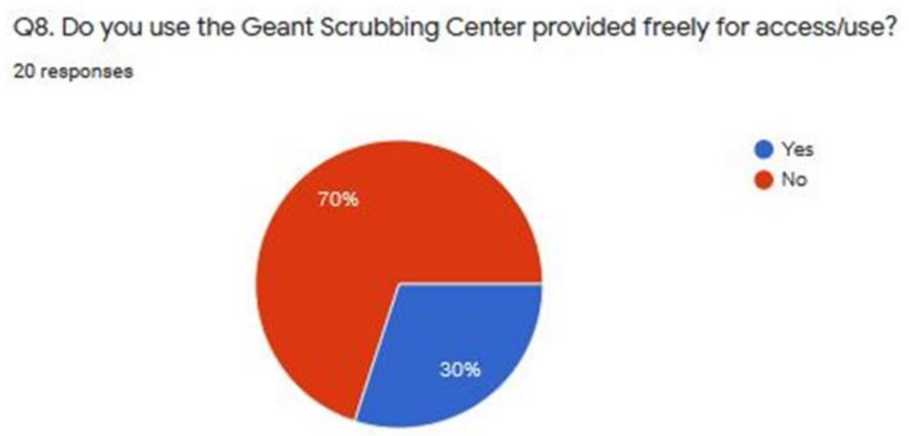


Figure 5.6: Responses to Survey Q8: use of GÉANT DDoS Cleansing and Alerting service

Even less than the 50% of NRENs that use FoD, only 30% make use of the free[2] GÉANT DDoS Cleansing and Alerting service, referred to in the survey as the GÉANT Scrubbing Centre (Figure 5.6).

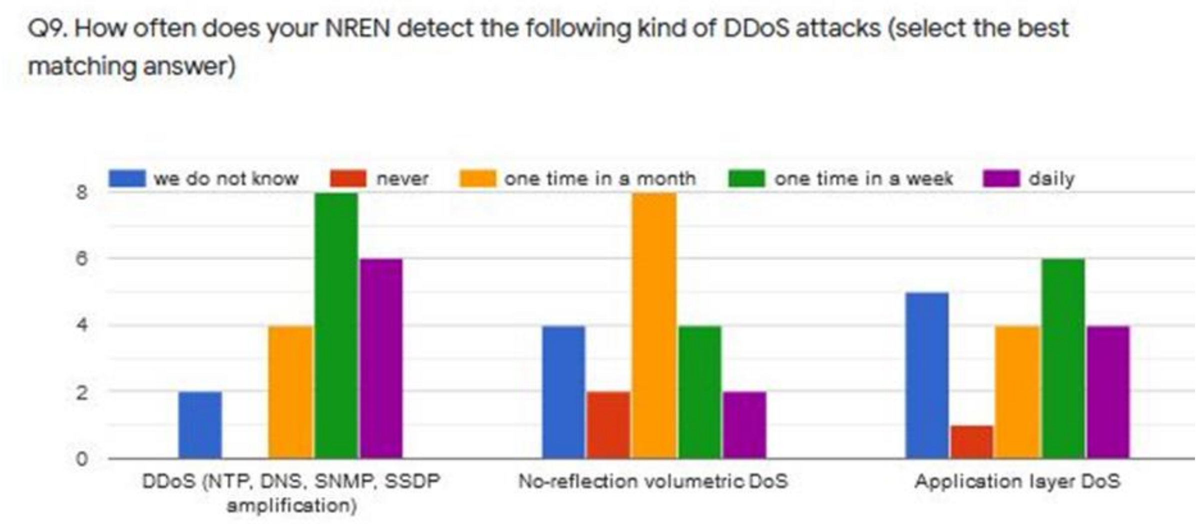


Figure 5.7: Responses to Survey Q9: frequency of detection for different types of attack

Figure 5.7 shows that the type of DDoS attack encountered is across the board, with no obvious discernible pattern.

[2] As with FoD, the service is a no-cost option for all GÉANT peering users [DDoSC&A].

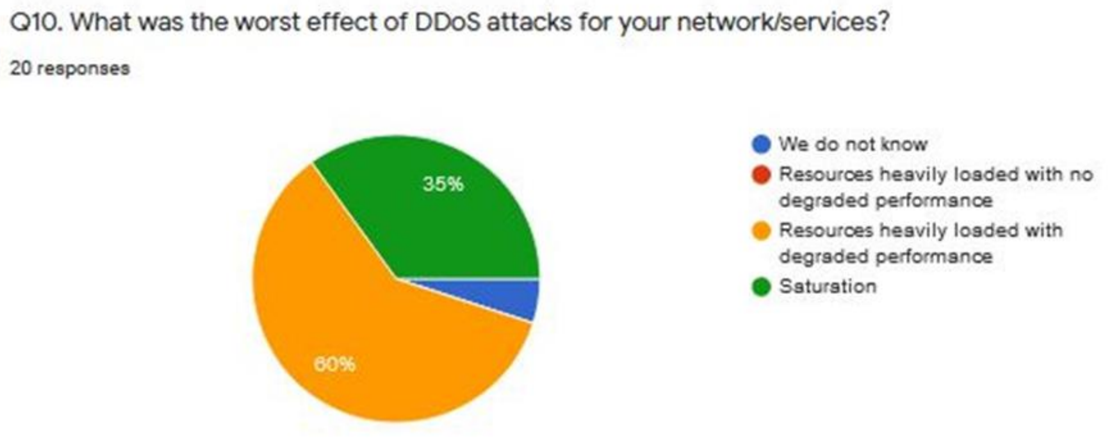


Figure 5.8: Responses to Survey Q10: worst effect of DDoS attack

From Figure 5.8 it can be seen that NRENs suffer from DDoS attacks, yet Figure 5.6 above shows that many do not use the free GÉANT DDoS Cleansing and Alerting service. This might be a result of the differences in their peering and upstream strategy.

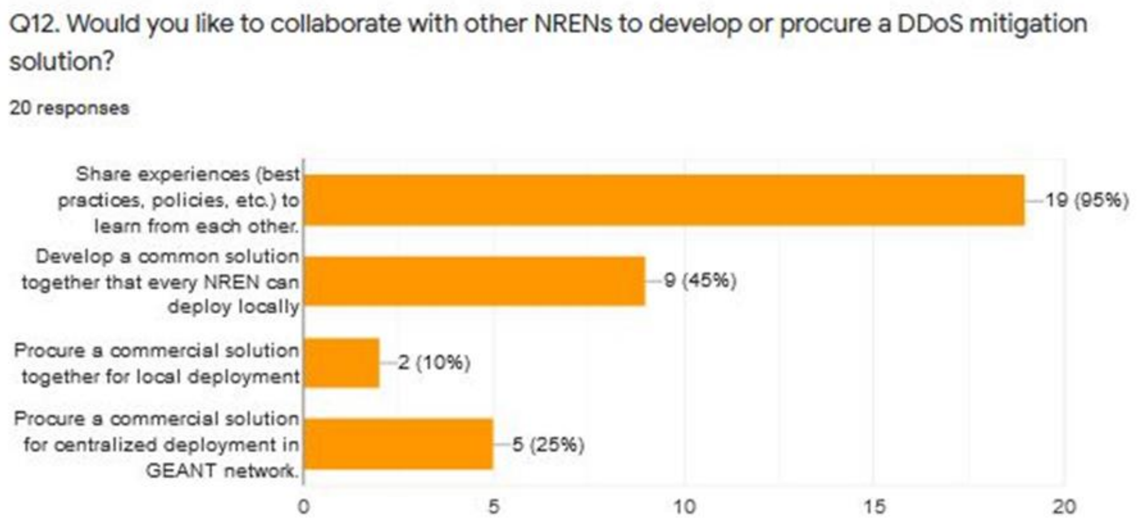
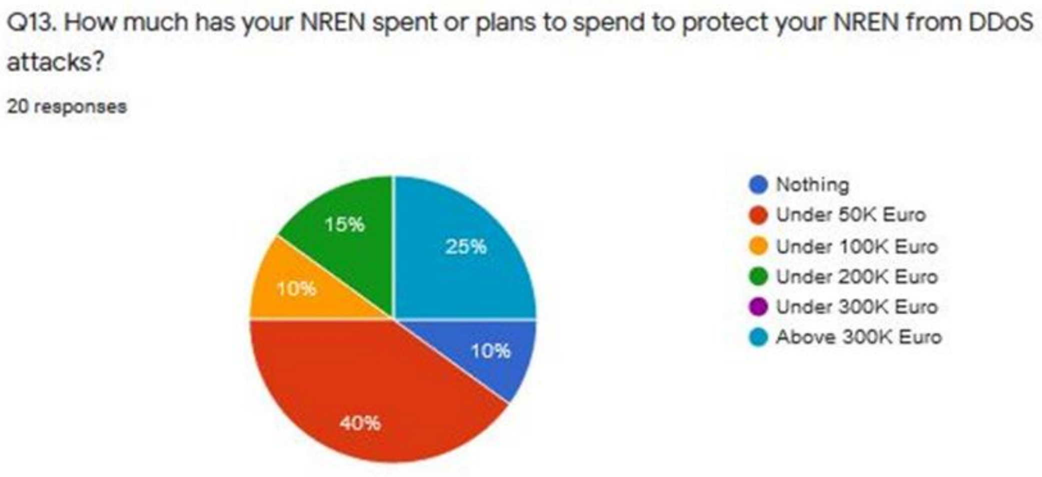


Figure 5.9: Responses to Survey Q12: interest in DDoS mitigation collaboration

Figure 5.9 shows that NRENs are interested in sharing experiences with regard to DDoS attacks but only 25% wish to procure a centralised DDoS mitigation system upstream in GÉANT.



Q13. How much has your NREN spent or plans to spend to protect your NREN from DDoS attacks?

20 responses

Figure 5.10: Responses to Survey Q13: DDoS mitigation expenditure

As can be seen in Figure 5.10, very few NRENs (10%) plan to spend nothing to mitigate DDoS attacks, whereas at the other end of the scale, 25% of NRENs plan to spend in excess of 300K Euro on systems to mitigate DDoS attacks. This shows that NRENs experience DDoS attacks very differently from each other.

5.2 Categories

The feedback received via the survey questionnaires, as well as direct feedback, indicates a diverse situation within the current NREN world, which might be based upon the different NREN types.

An attempt has therefore been made to categorise the various types of NREN and assess the impact that type/category has on the solutions they might prefer for combatting DDoS attacks. As most NRENs fall into multiple categories, often a differentiated strategy might be needed, as is reflected in the answers to Q4 to Q9 above.

The categories are:

- NRENs who have GÉANT as their single upstream.
- NRENs who also cater to governments.
- NRENs who service schools and school systems.
- NRENs with a diverse peering strategy.

Each of these is described below.

5.2.1 NRENs Who Have GÉANT as their Single Upstream

In this scenario, the next outside hop of the NREN is always the GÉANT network and using the freely available GÉANT DDoS Cleansing and Alerting service might be of interest to the NREN, at least for solving any larger-scale attacks. (Further information about this service is provided at [DDoSC&A]. To order the service you will need to access the Partner Portal [PP]. The service requires prior setup during "peacetime" via the form at [PP].)

Systems for mitigating medium to minor attacks might still be added within the NREN to better handle situations that just affect certain universities or even single servers.

5.2.2 NRENs Who Also Cater to Governments

Governments by nature attract numerous DDoS attacks, far in excess of what academia might sustain, therefore NRENs who support government access need to have a robust DDoS mitigation plan in place.

However, as most governmental network activity is more limited in its use of different Internet protocols than research network usage, it might be useful to add specialised solutions for network areas used by government institutions and agencies.

5.2.3 NRENS Who Service Schools and School Systems

Schools are sometimes targets of DDoS attacks with totally different motivation – such as kids having attack wars – but rarely are the attacks of a political nature. Most often, attacks are also directly related to school activities, so that a good network segmentation, as well as direct protection of a small number of services, might be helpful.

In addition, several NRENs report that they block most of the UDP protocol range for school systems, as this is rarely used and minimises the attack surface.

5.2.4 NRENs with a Diverse Peering Strategy

NRENs who follow a diverse peering strategy are less likely to be affected by full network outages during DDoS attacks, as these most possibly will just fill several, but not all, peerings or uplinks. This makes internal mitigation strategies within the NREN more effective, and fewer outside services are needed. In this scenario, a NREN would probably need its own internal scrubbing centre service.

Most of these NRENs are also only mildly interested in a centralised GÉANT DDoS Cleansing and Alerting service, as they use this peering only to reach other NRENs and do not expect to get significant attacks over this peering. They still might be interested in the visibility aspects such a service might provide.

6 Conclusions

Mitigation of DDoS attacks is not easy. Certainly there is no single solution, and while an organisation might think that a combination of numerous techniques as detailed above can minimise the attack, in the end, if someone wants to DDoS the organisation they will. The most effective and powerful DDoS mitigation method for a lot of services is often to redirect the attack traffic outside the organisation's own network via the external cloud-based mitigators, but even then there are no guarantees and, in the end, the service might still be affected to some degree.

A further complication is added to NREN networks, as research traffic patterns can be very diverse, resulting in lower efficiency of strict thresholds for DDoS detection or mitigation techniques, and higher efforts needed for network-related configuration and documentation. In addition, there may also be research activities in the field of DDoS itself, which might complicate the NREN's abilities in this field.

Given this situation, it is expected that the best way to address DDoS attacks is to take them into account in all aspects of network and capacity planning ahead of the implementation phases. In addition, rapid communication between the affected responsible parties, as well as a good overall awareness of the general network topology, are needed.

As most NRENs do, using a mixture of several services and techniques might be the best way forward at this time. Whatever the solutions selected, enough trained personnel are needed to successfully handle the workflows and communication that are required for effective DDoS attack handling.

References

[BGPDP]	https://patents.google.com/patent/US7225270
[CLL3O]	https://www.thousandeyes.com/blog/centurylink-level-3-outage-analysis/
[CTRTB]	https://archive.nanog.org/meetings/nanog30/presentations/morrow.pdf
[DDoSC&A]	https://www.geant.org/Services/Trust_identity_and_security/Pages/DDoS.aspx
[FoD]	https://www.geant.org/Networks/Network_Operations/Pages/Firewall-on-Demand.aspx
[IANA_SPAR]	https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml
[IPFIX]	https://en.wikipedia.org/wiki/IP_Flow_Information_Export
[NeMo]	https://security.geant.org/nemo-ddos-software/
[NetFlow]	https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-netflow/index.html
[PP]	https://geantprojects.sharepoint.com/sites/partner/Lists/Services%20with%20forms/AllItems.aspx?viewpath=%2Fsites%2Fpartner%2FLists%2FServices%20with%20forms [login required]
[PTE]	https://docs.microsoft.com/en-us/windows/client-management/troubleshoot-tcpip-port-exhaust
[RFC1918]	https://tools.ietf.org/html/rfc1918
[RFC2287]	https://tools.ietf.org/html/rfc2827
[RFC3882]	https://tools.ietf.org/html/rfc3882
[RFC7999]	https://tools.ietf.org/html/rfc7999
[RFC8704]	https://tools.ietf.org/html/rfc8704
[RFC8955]	https://tools.ietf.org/html/rfc8955
[RPF]	https://en.wikipedia.org/wiki/Reverse-path_forwarding
[SBRTBH]	https://packetlife.net/blog/2010/aug/23/source-based-rtbh/
[sFlow]	https://sflow.org/
[STF]	https://community.checkpoint.com/t5/Management/Limit-of-concurrent-connections/td-p/31881
[Wiki_DoSA]	https://en.wikipedia.org/wiki/Denial-of-service_attack

Further Reading

AWS. “What is a DDoS Attack?”
https://aws.amazon.com/shield/ddos-attack-protection/

IETF. BCP 38. “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”. May 2000.
https://tools.ietf.org/rfc/bcp/bcp38.txt

Kartch, Rachel. “Distributed Denial of Service Attacks: Four Best Practices for Prevention and Response”. 21 November 2016. Carnegie Mellon University Software Engineering Institute blog. https://insights.sei.cmu.edu/sei_blog/2016/11/distributed-denial-of-service-attacks-four-best-practices-for-prevention-and-response.html

NIST. “Advanced DDoS Mitigation Techniques”. 15 August 2016. https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

NSA. “National Security Agency Cybersecurity Report: A Guide to Border Gateway Protocol (BGP) Best Practices”. 10 September 2018. https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/ctr-guide-to-border-gateway-protocol-best-practices.pdf

Wikipedia. “Denial-of-service attack” https://en.wikipedia.org/wiki/Denial-of-service_attack

Wikipedia. “DDOS mitigation” https://en.wikipedia.org/wiki/DDoS_mitigation

Glossary

ACL	Access Control List
APS	Application Provisioning System
AS	Autonomous System
ASN	Autonomous System Number
AWS	Amazon Web Services
BCP	Best Current Practice (IETF)
BGP	Border Gateway Protocol
CDN	Content Delivery Network
CEO	Chief Executive Officer
CHARGEN	Character Generator Protocol
CLI	Command-Line Interface
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DNS	Domain Name System
DSCP	Diffserv Code Point
ERP	Enterprise Resource Planning
FoD	Firewall on Demand
GRE	Generic Routing Encapsulation
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IOS	Internetwork Operating System
IP	Internet Protocol
IPFIX	Internet Protocol Flow Information Export
ISP	Internet Service Provider
JSON	JavaScript Object Notation
NANOG	North American Network Operators' Group
NAT	Network Address Translation
NeMo	Network Monitoring
NetBIOS	Network Basic Input/Output System
NIST	National Institute of Standards and Technology
NOC	Network Operations Centre
NREN	National Research and Education Network
NTP	Network Time Protocol
OOB	Out of Band
PoP	Point of Presence
QOTD	Quote of the Day

RFC	Request for Comments (IETF)
RPF	Reverse Path Forwarding
RTBH	Remotely Triggered Black Hole
sFlow	sampled NetFlow
SNMP	Simple Network Management Protocol
SPAN	Switched Port Analyser
T	Task
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
uRPF	Unicast Reverse Path Forwarding
WP	Work Package
WP8	Work Package 8 Security
WP8 T3	WP8 Task 3 Products and Services