

What You Should Know About DDoS Incident Response

August 27, 2019 | **Adeline Zhang**



This document addresses the overall strategy and process for DDoS incident response and provides detailed analysis of and countermeasures against some typical attacks, in a bid to help organizations respond to DDoS attacks more effectively and efficiently. Therefore, we will not dwell upon specific methods of and configurations of specific mitigations against each type of DDoS attack.

0x00 Introduction

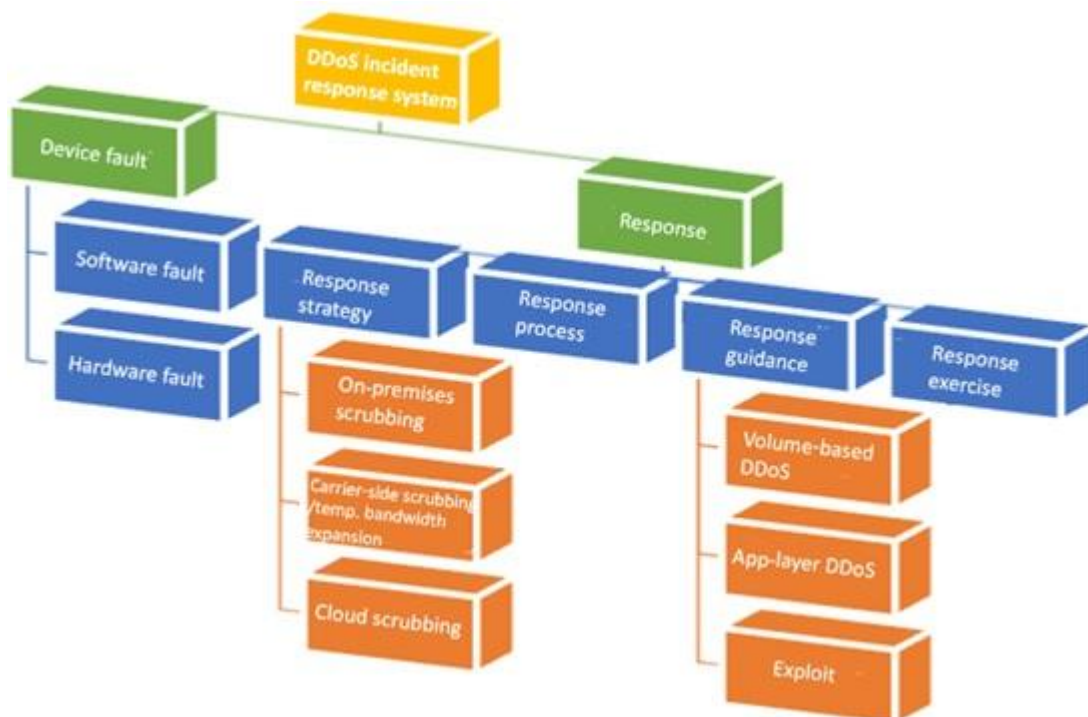
In the past several years, DDoS incidents have emerged endlessly. From DDoS analysis reports produced by security vendors, we can also find that DDoS attacks are growing by leaps and bounds in both the size and frequency. Thanks to the increasingly decreasing attack cost, the increasingly lowered technical skills required, the wide spread of attack tools, and the readily available bot machines on the Internet, it has become a piece of cake to launch a DDoS attack. Amid this trend, organizations have to input more and more in DDoS attack defenses. Naturally, with more inputs, people expect higher returns. When we say an organization does a good job in DDoS mitigation, it is largely because of its prompt and effective response to DDoS incidents.

This document is aimed at helping readers well understand DDoS incident response and stand higher to view such efforts in an all-round manner. By

reading this document, organizations are expected to handle incidents well prepared and with ease when suffering a DDoS attack, instead of being at a loss as to what to do.

0x01 Overview

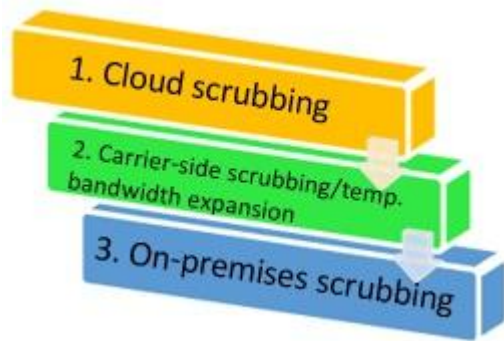
In routine operation and maintenance (O&M), incident responses are conducted either to fix device faults or to restore services carried by faulty devices or both.



Here we also list device faults. Although this component is not what we focus on in this document, it is an integral part of the overall response framework as we will be rendered helpless once anti-DDoS devices become faulty during a DDoS attack.

0x02 DDoS Incident Response Strategy

The DDoS incident response strategy can be generalized as “all-round defenses, multilevel filtering”, as shown in the following figure.



As we all know, DDoS is characterized by floods of traffic, but still there are ways to hit targets with less traffic. That is why our defense strategy is layered, as shown in the preceding figure.

During a DDoS attack, when the attack bandwidth is below 80% of the line bandwidth, on-premises anti-DDoS devices are capable enough to scrub DDoS attack traffic. In this case, external assistance is unnecessary.

However, when the DDoS attack bandwidth exceeds 100% of the line bandwidth, you have to resort to the carrier for DDoS scrubbing. Oops! The carrier owning the line under attack does not provide the DDoS scrubbing service. “What shall we do?” Take it easy. You can initiate plan B, that is, asking the carrier to expand the bandwidth for the time being. As long as the line bandwidth is greater than the attack bandwidth, on-premises devices can do their jobs effectively.

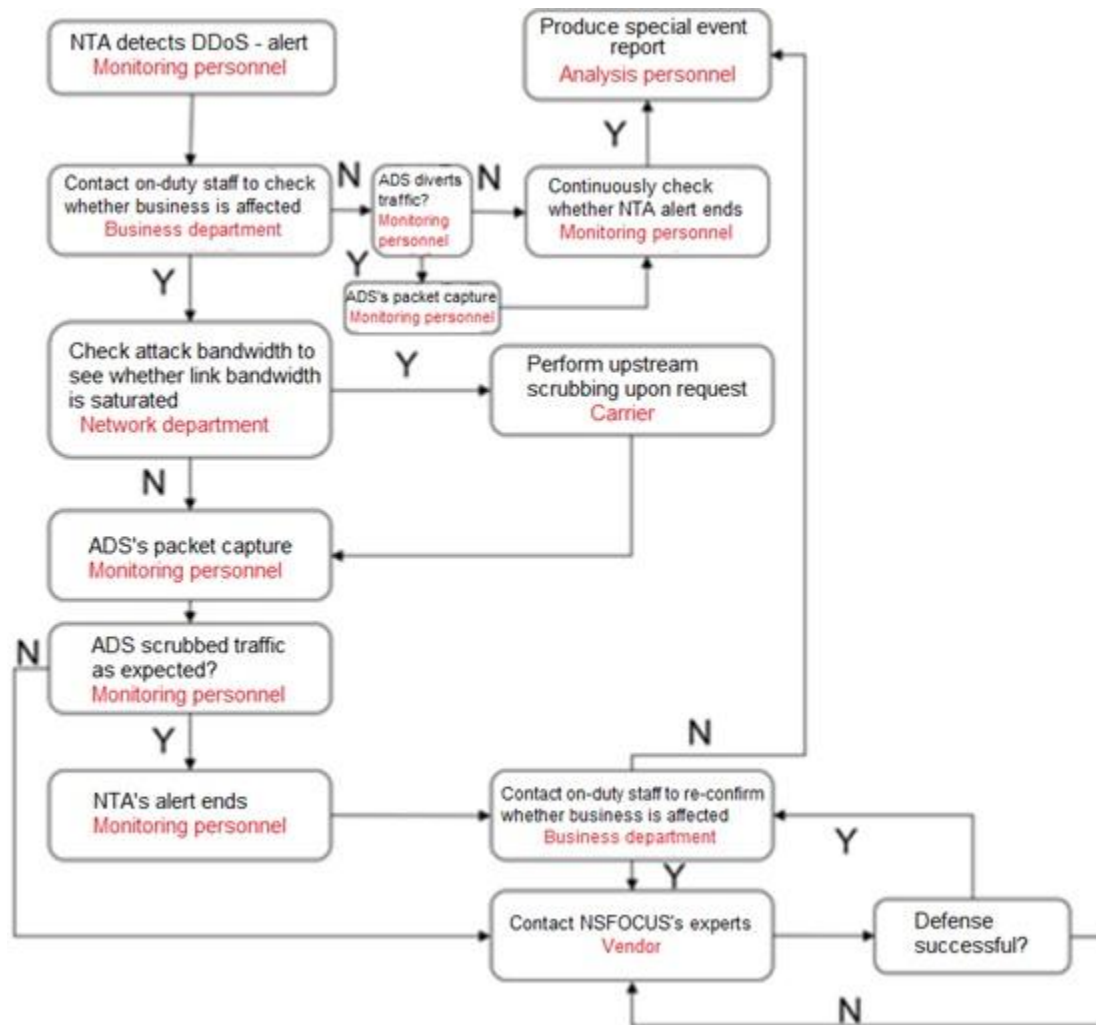
In case the carrier’s scrubbing service does not work to your satisfaction, you can play the trump card: cloud scrubbing.

Most real-life DDoS attacks are multi-vector ones (a mix of various attack types). For example, some DDoS attacks generate floods of reflective traffic as the background traffic, in which CC, connection exhaustion, and low-and-slow attack traffic is hidden. In this case, a likely option is to use the carrier-side scrubbing service (specifically for volume-based attacks) to first filter out over 80% of traffic, thereby ensuring enough line bandwidth. Among the remaining 20% of traffic, 80% is probably attack traffic (low-and-slow attack, CC attack, and so on), which needs to be further scrubbed.

0x03 DDoS Incident Response Process

The following figure illustrates a general DDoS incident response process that is suitable for most organizations. Still, there are some details needing to be clarified:

- In the case of no 24/7 onsite security O&M, the network management and monitoring center (NMMC) is usually responsible for monitoring DDoS alerts. Therefore, a collaborative handling mechanism should be in place to enable cooperation with monitoring personnel at NMMC.
- If on-premises scrubbing devices are not configured with automatic diversion, diversion needs to be manually initiated when an attack is detected. In case of emergency, who and how to do this and what kind of authorization is required should be discussed beforehand and included in the response process. Assume that a DDoS attack takes place at 2:00 a.m. If the preceding matters are well considered, emergency response personnel will be poised to do their job confidently.
- As for the carrier-side scrubbing service, a related mechanism should be established beforehand upon sufficient communication to enable effective implementation of incident responses. At least the method of reaching the contact person on the carrier's side and an authorization mode acknowledged by both sides (for example, some carriers' scrubbing service requires a fax of the request affixed with the customer's official seal) should be known to response personnel.
- For vendor's expert support, it is advisable to perform sufficient technical exchanges and communication in advance. The response personnel should at least know when this mechanism needs to be initiated. In addition, some basic information needs to be collected beforehand for second-line support personnel's ready use as it takes time for them to arrive at the site and the time to recovery is an important factor that organizations have to consider.



0x04 DDoS Incident Response Guidance

4.1 DDoS Attack Types

DDoS Attack Type Symptom

Volume-based attack (direct)	DDoS alerts on SYN, ACK, ICMP, UDP, or connection floods
Volume-based attack (reflective)	DDoS alerts on NTP, DNS, SSDP, or ICMP floods Possibly no evident traffic fluctuation, slow response to service access requests, frequent timeouts, and lots of requests for access to the same page(s)
CC	Possibly no evident traffic fluctuation, slow response to service access requests, frequent timeouts, many incomplete HTTP GET requests, and HTTP POST request packets of regular sizes (usually very small)
Low-and-slow HTTP attack	

Evident traffic fluctuations, slow response to service access requests, frequent timeouts, and many request packets with the same Referer header that indicates the same page linked to the requested resource

URL reflection Alerts possibly generated by intrusion

Various exploits detection/prevention devices, but seldom by DDoS with the DoS effect detection devices

After DDoS attacks are sorted out, the next step is to deploy defenses according to the DDoS defense guideline.

- **Volume-based attack (direct):** In the case of the attack bandwidth below the line bandwidth, on-premises scrubbing suffices to overcome this type of attack.
- **Volume-based attack (direct):** In the case of the attack bandwidth in excess of the line bandwidth, there are three options available to handle this: carrier-side scrubbing, temporary bandwidth expansion, and cloud scrubbing. After the attack bandwidth is controlled below the line bandwidth, on-premises devices can take over the remaining work.

For SYN, ACK, UDP, ICMP, and other flood attacks:

Generally, defense algorithms (for example, dropping the first packet and IP traceback) configured on on-premises devices are effective enough to cope with these attacks.

In particular circumstances, it is advisable to apply rate limits for various packets along with the preceding algorithms to at least ensure the basic availability of services during an attack.

If source IP addresses are found to be mostly located in a specific region, location-based restriction may be a good option, especially for attacks originated from foreign countries.

- **Volume-based attack (reflective):** In the case of the attack bandwidth below the line bandwidth, on-premises scrubbing suffices to overcome this type of attack.
- **Volume-based attack (reflective):** In the case of the attack bandwidth in excess of the line bandwidth, there are three options available to handle this: carrier-side scrubbing, temporary bandwidth expansion, and cloud scrubbing. After the attack bandwidth is controlled below the line bandwidth, on-premises devices can take over the remaining work.

For NTP, DNS, SSDP, and other reflection attacks:

Generally, defense algorithms (for example, drop of UDP fragments and rate limiting) configured on on-premises devices are effective enough to mitigate these attacks.

In particular circumstances, as reflection attacks are characterized by the traffic with fixed source ports and fixed destination IP addresses using over 90% of the bandwidth, a more thorough dropping rule can be configured accordingly.

- **CC attack: First on-premises devices can be used to scrub the traffic and, if the effect is not satisfactory, cloud scrubbing can step in.**

For CC attacks, if traffic scrubbing hardly works, in case of emergency, replacement with static pages can be used as a makeshift.

- **Low-and-slow HTTP attack: First on-premises devices can be used to scrub the traffic and, if the effect is not satisfactory, cloud scrubbing can step in.**

For slow HTTP body attacks, characteristics of the attack tool should be first identified and then policies should be configured on on-premises devices accordingly.

- **URL reflection: On-premises scrubbing and cloud scrubbing should be combined.**

For URL reflection attacks, it is important to identify reflectors in the attack process and then configure advanced settings on on-premises devices.

- **Various exploits with the DoS effect: Intrusion detection or prevention devices should be monitored for alerts and system vulnerabilities should be promptly fixed once discovered.**

This type of attacks, strictly speaking, does not belong to DDoS attacks, but can somewhat compare with DoS owing to the similar effect. Therefore, it is listed here only to make our classifications as exhaustive as possible.

4.2 DDoS Incident Response Guidance

4.2.1 Volume-based DDoS Attack (Direct)

Examples of this type of attacks are SYN flood, ACK flood, ICMP flood, and UDP flood attacks. When detecting a DDoS attack, the DDoS detection device immediately generates an alert. This means that we can obtain firsthand information from this device. To defend against the attack traffic, a necessary step is to divert such traffic to the DDoS scrubbing

device (not deployed in in-path mode) before being scrubbed automatically or manually. Either way, we can capture packets for further analysis to identify signatures of this attack.

Generally, when packets of a certain type account for over 80% of the total number of packets captured, an attack is believed to be in process.

No.	Time	Source	Destination	Protocol	Info
1	13:19:05.498967	110.22.126.68	5.5.5.1	TCP	56000 > http [SYN] Seq=0 win=65535 Len=0
2	13:19:05.499017	110.22.126.68	5.5.5.1	TCP	56000 > http [SYN] Seq=0 win=65535 Len=0
3	13:19:05.499100	45.61.110.120	5.5.5.1	TCP	15103 > http [SYN] Seq=0 win=65535 Len=0
4	13:19:05.499106	45.61.110.120	5.5.5.1	TCP	15103 > http [SYN] Seq=0 win=65535 Len=0
5	13:19:05.499202	168.150.250.107	5.5.5.1	TCP	53908 > http [SYN] Seq=0 win=65535 Len=0
6	13:19:05.499207	168.150.250.107	5.5.5.1	TCP	53908 > http [SYN] Seq=0 win=65535 Len=0
7	13:19:05.499293	70.125.205.44	5.5.5.1	TCP	21189 > http [SYN] Seq=0 win=65535 Len=0
8	13:19:05.499298	70.125.205.44	5.5.5.1	TCP	21189 > http [SYN] Seq=0 win=65535 Len=0
9	13:19:05.499407	21.74.6.49	5.5.5.1	TCP	61655 > http [SYN] Seq=0 win=65535 Len=0
10	13:19:05.499412	21.74.6.49	5.5.5.1	TCP	61655 > http [SYN] Seq=0 win=65535 Len=0
11	13:19:05.499482	87.101.237.116	5.5.5.1	TCP	26396 > http [SYN] Seq=0 win=65535 Len=0
12	13:19:05.499487	87.101.237.116	5.5.5.1	TCP	26396 > http [SYN] Seq=0 win=65535 Len=0
13	13:19:05.499583	134.150.46.59	5.5.5.1	TCP	44639 > http [SYN] Seq=0 win=65535 Len=0
14	13:19:05.499588	134.150.46.59	5.5.5.1	TCP	44639 > http [SYN] Seq=0 win=65535 Len=0
15	13:19:05.499706	21.225.58.74	5.5.5.1	TCP	34101 > http [SYN] Seq=0 win=65535 Len=0
16	13:19:05.499711	21.225.58.74	5.5.5.1	TCP	34101 > http [SYN] Seq=0 win=65535 Len=0

- SYN flood
- Checking the number of packets

TCP-SYN packets take up around 80% of the total packets captured.

- Checking the number of connections to the server

Run the **netstat -an | find "SYN_RECEIVED"** command to check TCP connections. If a lot of connections are in the SYN_RECEIVED state (half-open), a SYN flood attack is believed to be happening.

TCP	0.0.0.0:1025	0.0.0.0	LISTENING
TCP	0.0.0.0:1026	0.0.0.0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0	LISTENING
TCP	192.168.242.133:80	0.2.13.66:4642	SYN_RECEIVED
TCP	192.168.242.133:80	0.9.133.151:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.14.35.23:4642	SYN_RECEIVED
TCP	192.168.242.133:80	0.14.238.104:1328	SYN_RECEIVED
TCP	192.168.242.133:80	0.23.8.129:4642	SYN_RECEIVED
TCP	192.168.242.133:80	0.28.81.119:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.28.146.94:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.29.167.90:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.42.74.131:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.60.170.49:3812	SYN_RECEIVED
TCP	192.168.242.133:80	0.74.12.255:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.74.72.200:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.77.83.202:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.81.151.160:1328	SYN_RECEIVED
TCP	192.168.242.133:80	0.82.161.55:1328	SYN_RECEIVED
TCP	192.168.242.133:80	0.89.16.226:2589	SYN_RECEIVED
TCP	192.168.242.133:80	0.91.193.55:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.92.58.58:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.104.165.12:2797	SYN_RECEIVED
TCP	192.168.242.133:80	0.109.208.192:4642	SYN_RECEIVED
TCP	192.168.242.133:80	0.113.95.116:4642	SYN_RECEIVED

```
# netstat -n | awk '/^tcp/ {++S[$NF]} END {for(a in S) print a, S[a]}'
TIME_WAIT 16855
CLOSE_WAIT 21
SYN_SENT 99
FIN_WAIT1 229
FIN_WAIT2 113
ESTABLISHED 8358
SYN_RECV 48965
CLOSING 3
LAST_ACK 313
```

- ACK flood

Most ACK flood attacks are for the purpose of saturating the bandwidth. If a large proportion of packets captured are TCP-ACK packets, which do not result in setup of TCP connections and contain a large number of retransmitted TCP-ACK packets, an ACK flood attack is virtually ongoing.

- ICMP flood

Normally, ICMP packets take up a very small proportion of network traffic. When over 20% of packets captured are ICMP packets, it may be rash to determine that an ICMP flood attack is ongoing, but this symptom at least indicates that an anomaly occurs in the current network environment. Typically, when a core transport network becomes faulty, in some cases, the router encapsulates those packets that cannot reach the destination as expected via ICMP before forwarding them to the server. This will result

in a detection device generating a DDoS alert on ICMP floods. To determine whether a real ICMP flood attack is happening, we can also check the size of ICMP packets, which is usually smaller than 100 bytes (unless they are for implementing some special functions like probing). If most packets captured are ICMP packets that are larger than 1000 bytes, or sometimes there are even an overwhelming number of ICMP fragments, an ongoing ICMP flood attack is almost a surefire thing.

- UDP flood

As UDP flood attacks are mainly aimed at overwhelming the target's ability to process and respond by occupying the whole bandwidth, there must be a great number of UDP packets in a very short time. Besides, payloads of these packets are largely similar. In a UDP flood attack, we can find that, of all UDP packets captured with Wireshark, most contain similar information in the Data field although their source IP addresses and destination ports may be different.

```

> Frame 11: 432 bytes on wire (3456 bits), 432 bytes captured (3456 bits)
> Ethernet II, Src: NexcomIn_46:6b:91 (00:10:f3:46:6b:91), Dst: CiscoInc_65:69:ba (10:f3:11:65:69:ba)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 110
> Internet Protocol Version 4, Src: 121.7.58.217, Dst: 59.42.241.10
> User Datagram Protocol, Src Port: 36792 (36792), Dst Port: 28754 (28754)
+ Data (386 bytes)
  Data: 485454502f312e3120323030204f4b0d0a43414348452d43...
  [Length: 386]

```

```
> Frame 12: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on 0
> Ethernet II, Src: NexcomIn_46:6b:91 (00:10:f3:46:6b:91), Dst: CiscoInc_65:69:ba (10:f3:11:65:69:ba)
> 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 110
> Internet Protocol Version 4, Src: 190.201.156.190, Dst: 59.42.241.10
> User Datagram Protocol, Src Port: 54284 (54284), Dst Port: 33450 (33450)
+ Data (365 bytes)
  Data: 485454502f312e3120323030204f4b0d0a43414348452d43...
  [Length: 365]
```

[illegible]

For volume-based DDoS attacks (direct), common algorithms employed by most DDoS traffic scrubbing devices can work to a good effect. How to configure policies on these devices is not something this document concerns.

4.2.2 Volume-based DDoS Attack (Reflective)

The following table lists some representative volume-based DDoS attacks (reflective).

Attack Type	Amplification Factor	Vector
NTP Amplification Attack	556.9	Monlist query
DNS Amplification Attack	28 to 54	Text query
SSDP Amplification Attack	30.8	SEARCH request
Charger Amplification Attack	358.8	Character generation request
SNMP Amplification Attack	6.3	GetBulk request
NetBIOS Amplification Attack	3.8	Name resolution
QOTD Amplification Attack	140.3	Quote request

Reflective DDoS attacks have two features: (1) The attack traffic is overwhelmingly large; (2) It is difficult to trace the attack source. Owing to reflection, the real attack source is concealed, even if it is a botnet, which is actually often involved in such an attack. For this reason, hackers behind this type of attacks are especially audacious, without scruple.

These attacks have distinctive features. Experience tells us that, whether packets are captured by a cleaning device or a network probe, the attack traffic can take up over 90%, and sometimes even 99%, of the total network traffic. After all, the sole purpose of reflection attacks is to consume network bandwidth and cause congestion to the ingress line.

During a reflection attack, almost all alerts on DDoS detection devices are about UDP floods.

The following figures show signatures of various reflection attack packets.

DNS reflection attack:

No.	Time	Source	Destination	Protocol	Length	Info
254	2017-08-30 22:36:15.081344	62.157.242.7		DNS	832	Standard query response 0x0262 NS dns2.1111nets.edu NS ns1-auth.windstream.net SO NS ns
256	2017-08-30 22:36:15.089363	108.248.236.33		DNS	348	Standard query response 0x78da NS dns2.1111nets.edu NS ns2-auth.windstream.net NS dns2.
259	2017-08-30 22:36:15.090304	41.185.258.231		DNS	348	Standard query response 0x78da NS ns2-auth.windstream.net NS ns4-auth.windstream.net NS
264	2017-08-30 22:36:15.091327	108.248.236.33		DNS	348	Standard query response 0x78da NS dns2.1111nets.edu NS Fluffy.netwestleyan.edu NS ns3-a
265	2017-08-30 22:36:15.091903	213.154.20.240		DNS	348	Standard query response 0x0262 NS010 SO SO
269	2017-08-30 22:36:15.096179	195.253.201.209		DNS	734	Standard query response 0xab0d NS ns2-auth.windstream.net NS ns3-auth.windstream.net NS
270	2017-08-30 22:36:15.096745	77.87.96.243		DNS	348	Standard query response 0xab0d NS ns1-auth.windstream.net NS ns3-auth.windstream.net NS
274	2017-08-30 22:36:15.099006	72.252.205.87		DNS	278	Standard query response 0x3495 NS010
276	2017-08-30 22:36:15.100538	108.248.236.33		DNS	348	Standard query response 0x78da NS ns1-auth.windstream.net NS ns3-auth.windstream.net NS
277	2017-08-30 22:36:15.100704	187.536.335.306		DNS	333	Standard query response 0x78da NS010 SO SO
284	2017-08-30 22:36:15.104967	92.147.46.178		DNS	348	Standard query response 0xab0d NS ns1-auth.windstream.net NS dns2.1111nets.edu NS ns3-a
285	2017-08-30 22:36:15.105232	108.173.306.94		DNS	380	Standard query response 0x0262 NS dns2.1111nets.edu NS ns2-auth.windstream.net NS dns3.
289	2017-08-30 22:36:15.107466	176.124.52.5		DNS	380	Standard query response 0x3495 NS ns4-auth.windstream.net NS Fluffy.netwestleyan.edu NS
292	2017-08-30 22:36:15.109044	195.253.94.245		DNS	380	Standard query response 0x0262 NS ns2-auth.windstream.net NS ns3-auth.windstream.net NS
294	2017-08-30 22:36:15.110294	5.83.262.398		DNS	333	Standard query response 0xab0d NS NS010 SO
295	2017-08-30 22:36:15.110839	89.22.151.258		DNS	380	Standard query response 0x3495 NS ns2-auth.windstream.net NS ns3-auth.windstream.net NS
296	2017-08-30 22:36:15.111428	91.215.21.207		DNS	439	Standard query response 0x78da SO NS ns3-auth.windstream.net NS dns2.1111nets.edu NS ns
297	2017-08-30 22:36:15.111993	216.215.154.224		DNS	333	Standard query response 0xab0d NS010 SO SO
298	2017-08-30 22:36:15.112559	130.537.304.158		DNS	526	Standard query response 0x3495 SO SO NS010
305	2017-08-30 22:36:15.114233	77.87.200.186		DNS	380	Standard query response 0x78da NS Fluffy.netwestleyan.edu NS ns2-auth.windstream.net NS
307	2017-08-30 22:36:15.114873	66.42.16.82		DNS	348	Standard query response 0xab0d SO NS010 SO
309	2017-08-30 22:36:15.115388	77.80.144.122		DNS	372	Standard query response 0xab0d NS dns2.1111nets.edu NS ns3-auth.windstream.net NS ns2-a
304	2017-08-30 22:36:15.115913	62.253.238.335		DNS	333	Standard query response 0x78da NS010 SO SO
305	2017-08-30 22:36:15.116189	62.253.170.332		DNS	348	Standard query response 0x78da NS010 SO SO
306	2017-08-30 22:36:15.117084	108.248.236.33		DNS	348	Standard query response 0x78da NS ns2-auth.windstream.net NS dns2.1111nets.edu NS Fluff
307	2017-08-30 22:36:15.117699	60.242.257.12		DNS	333	Standard query response 0x0262 NS010 SO SO

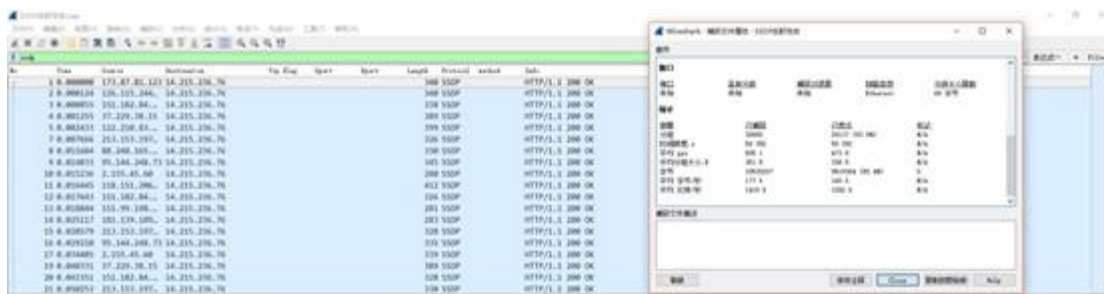
Traffic	Captured	Displayed	Marked
Packets	10000	4271	0
Between first and last packet	10143.132 sec	5.487 sec	
Avg. packets/sec	0.986	778.323	
Avg. packet size	800.381 bytes	435.261 bytes	
Bytes	8003811	1858999	
Avg. bytes/sec	789.087	338773.506	
Avg. MBit/sec	0.006	2.710	

NTP reflection attack:

No.	Time	Source	Destination	Protocol	Length	Info
34	2017-08-30 22:37:22.902110	62.157.242.7		DNS	832	Standard query response 0x0262 NS dns2.1111nets.edu NS ns1-auth.windstream.net SO NS ns
317	2017-08-30 22:37:24.904169	62.157.242.7		DNS	832	Standard query response 0x0262 NS dns2.1111nets.edu NS ns1-auth.windstream.net SO NS ns
318	2017-08-30 22:37:25.912127	62.157.242.7		DNS	832	Standard query response 0x0262 NS dns2.1111nets.edu NS ns1-auth.windstream.net SO NS ns
3457	2017-08-30 22:37:30.146623	185.58.220.335		NTP	482	NTP version 2, private
3458	2017-08-30 22:37:30.173343	185.58.220.335		NTP	482	NTP version 2, private
3459	2017-08-30 22:37:30.173808	185.58.220.335		NTP	482	NTP version 2, private
3462	2017-08-30 22:37:30.174966	185.58.220.335		NTP	482	NTP version 2, private
3475	2017-08-30 22:37:30.177538	185.58.220.335		NTP	482	NTP version 2, private
3477	2017-08-30 22:37:30.178187	185.58.220.335		NTP	482	NTP version 2, private
3478	2017-08-30 22:37:30.178655	185.58.220.335		NTP	482	NTP version 2, private
3479	2017-08-30 22:37:30.182378	185.58.220.335		NTP	482	NTP version 2, private
3483	2017-08-30 22:37:30.183309	185.58.220.335		NTP	482	NTP version 2, private
3482	2017-08-30 22:37:30.183873	185.58.220.335		NTP	482	NTP version 2, private
3483	2017-08-30 22:37:30.184437	185.58.220.335		NTP	482	NTP version 2, private
3485	2017-08-30 22:37:30.187222	185.58.220.335		NTP	482	NTP version 2, private
3486	2017-08-30 22:37:30.187787	185.58.220.335		NTP	482	NTP version 2, private
3488	2017-08-30 22:37:30.190034	185.58.220.335		NTP	482	NTP version 2, private
3489	2017-08-30 22:37:30.190764	185.58.220.335		NTP	482	NTP version 2, private
3492	2017-08-30 22:37:30.192083	185.58.220.335		NTP	482	NTP version 2, private
3496	2017-08-30 22:37:30.196336	185.58.220.335		NTP	482	NTP version 2, private
3497	2017-08-30 22:37:30.196794	185.58.220.335		NTP	482	NTP version 2, private
3498	2017-08-30 22:37:30.197335	185.58.220.335		NTP	482	NTP version 2, private
3499	2017-08-30 22:37:30.197896	185.58.220.335		NTP	482	NTP version 2, private
3495	2017-08-30 22:37:30.200284	185.58.220.335		NTP	482	NTP version 2, private
3496	2017-08-30 22:37:30.202849	77.53.247.56		NTP	482	NTP version 2, private

Traffic	Captured	Displayed	Marked
Packets	10000	8522	0
Between first and last packet	12.987 sec	12.305 sec	
Avg. packets/sec	769.984	692.582	
Avg. packet size	434.099 bytes	481.161 bytes	
Bytes	4340993	4100454	
Avg. bytes/sec	334249.512	333243.478	
Avg. MBit/sec	2.674	2.666	

SSDP reflection attack:



Reflective DDoS attacks are not difficult to mitigate. When the attack bandwidth exceeds the line bandwidth (on the web-based manager of a protection device, we often see the attack bandwidth is equal to the line bandwidth because traffic in excess of the maximum line bandwidth is already dropped by the upstream carrier), the organization should request initiation of the carrier-side DDoS scrubbing service. If the attack bandwidth does not exceed the line bandwidth, on-premises scrubbing is enough. Besides, ACLs can be configured on edge routers to filter out this type of traffic. On an on-premises DDoS traffic scrubbing device, the following policy can be configured to thoroughly filter out reflective DDoS traffic:

1	0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 123:123 drop NTP Reflect
2	
3	0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 1900:1900 drop SSDP Reflect
4	
5	0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:65535 19:19 drop CHARGEN Reflect
6	
7	0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 UDP 0:0 0:0 drop Fragment

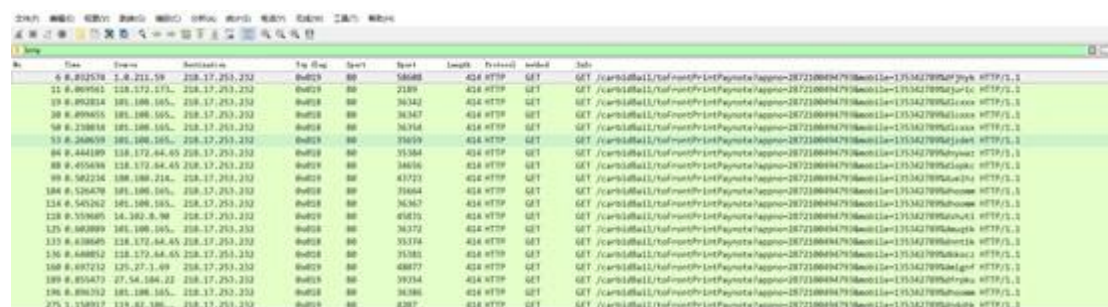
To defend against DNS reflection attacks, we can configure a DNS keyword filtering policy. Up to now, all DNS reflection attacks we have handled have the query type of 0x00ff.

4.2.3 Application-Layer DDoS Attack

Typical application-layer DDoS attacks include CC attacks and low-and-slow attacks. The most distinctive difference between these attacks and volume-based DDoS attacks is that the former can achieve the effect of the latter with small volumes of traffic. In extreme situations, no obvious traffic fluctuation is observed before services are paralyzed.

Basic algorithms employed by DDoS traffic scrubbing devices are not so competent for this type of attacks. We must capture attack signatures in real time to determine what the best cure is.

CC attacks have obvious patterns. When accessing services, users usually need to browse one after another page here and there instead of being confined to certain pages. During CC attacks, most visits are related to certain (5–10) pages. In this case, we can configure a filtering rule on the DDoS traffic scrubbing device to protect these pages.



No.	Time	Source	Destination	Type	Length	Protocol	Info
11	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
12	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
13	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
14	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
15	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
16	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
17	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
18	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
19	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html
20	0.001578	118.172.172.172	218.17.253.252	HTTP	400	GET	/carbidell/tal/mofo/IntPaymentPage-287210049479.html

Normal traffic does not contain a large number of very small packets, which is, however, the case with low-and-slow HTTP attacks, especially body-related ones. Besides, the packet size of these attacks has a pattern. After identifying these features, we can configure parameters accordingly on the DDoS scrubbing device to effectively defend against these attacks.

0x05 DDoS Incident Response Exercise

To ensure truly efficient responses to DDoS attacks, we should routinely carry out the incident response exercise. After the DDoS incident response strategy is set down, the response process established, and various DDoS attacks and related countermeasures analyzed, the next step is to conduct regular exercises, whether in sandbox mode or hands-on form. Exercises can walk us through the DDoS incident response process and help us identify what needs to be improved in our response efforts.

0x06 Must-Knows About DDoS Incident Response

What needs to be considered for DDoS incident response is listed as follows for readers' reference:

- In the current network environment, how many Internet access lines are there and what is the bandwidth of each line?
- Do the carriers owning Internet access lines support DDoS scrubbing? If yes, have we purchased this service or can we use it on a trial basis in case of emergency? Is there an emergency response process in place for initiating the carrier-side scrubbing service during DDoS attacks?
- Do the carriers owning Internet access lines support temporary bandwidth expansion in case of emergency? If yes, have we purchased the service or can we use it on a trial basis? Is there an emergency response process in place for initiating the temporary bandwidth expansion service during DDoS attacks?
- Is on-premises DDoS scrubbing available for each of the Internet access lines?
- Does the on-premises anti-DDoS device and service vendor provide an emergency response plan for DDoS attacks?
- Are all services that need to be protected included in the monitoring scope of anti-DDoS devices?
- For services that require automatic DDoS scrubbing, can automatic diversion and scrubbing work properly during a DDoS attack?
- Is there an internal guiding process for DDoS incident response?
- Is it possible that we are immediately aware of a DDoS attack taking place? And how?