Network protection against DoS/DDoS attacks

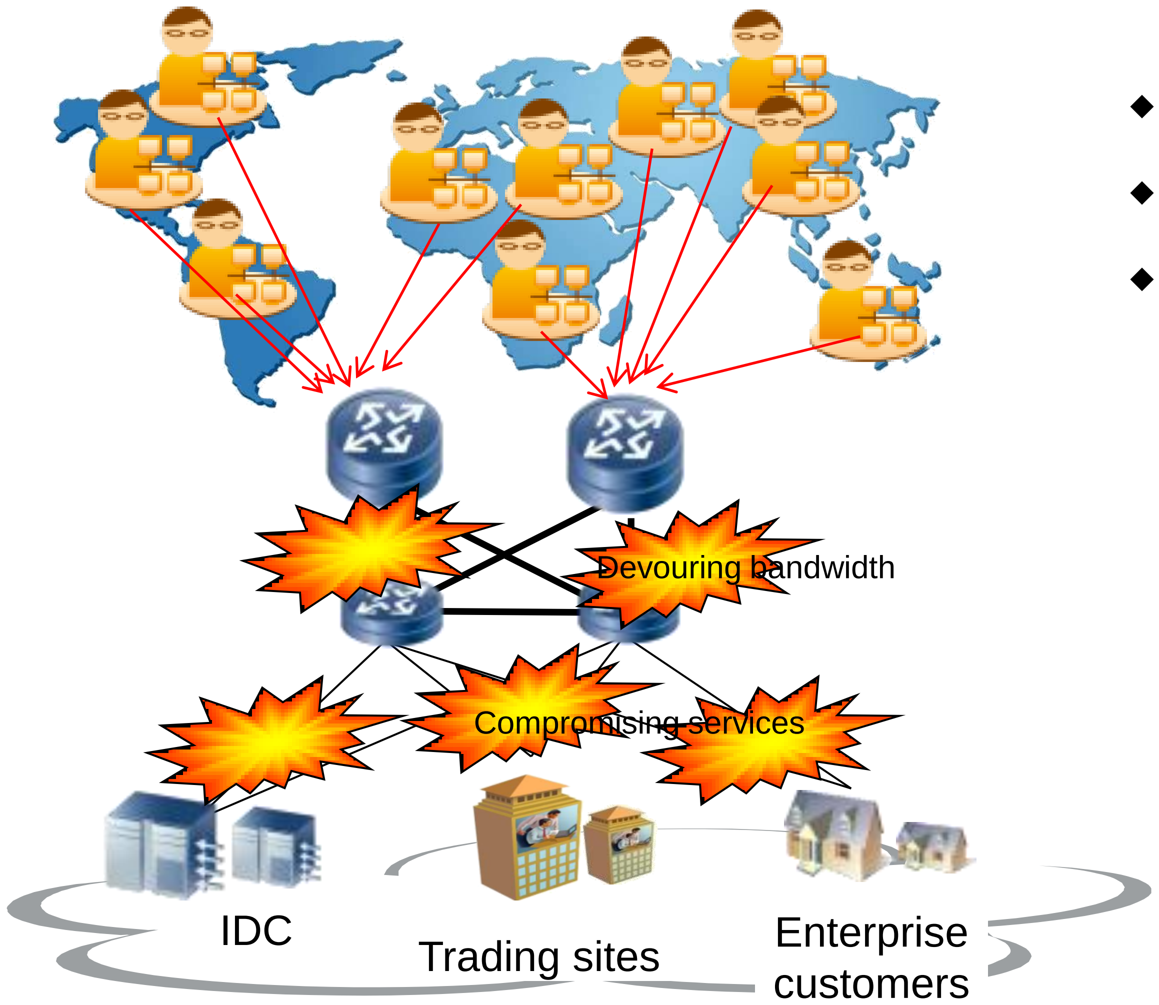
www.huawei.com

Pawel Wachelka
IP Product Manager
Huawei Enterprise Business Group, CEE & Nordic Region
Email: Pawel.Wachelka@huawei.com

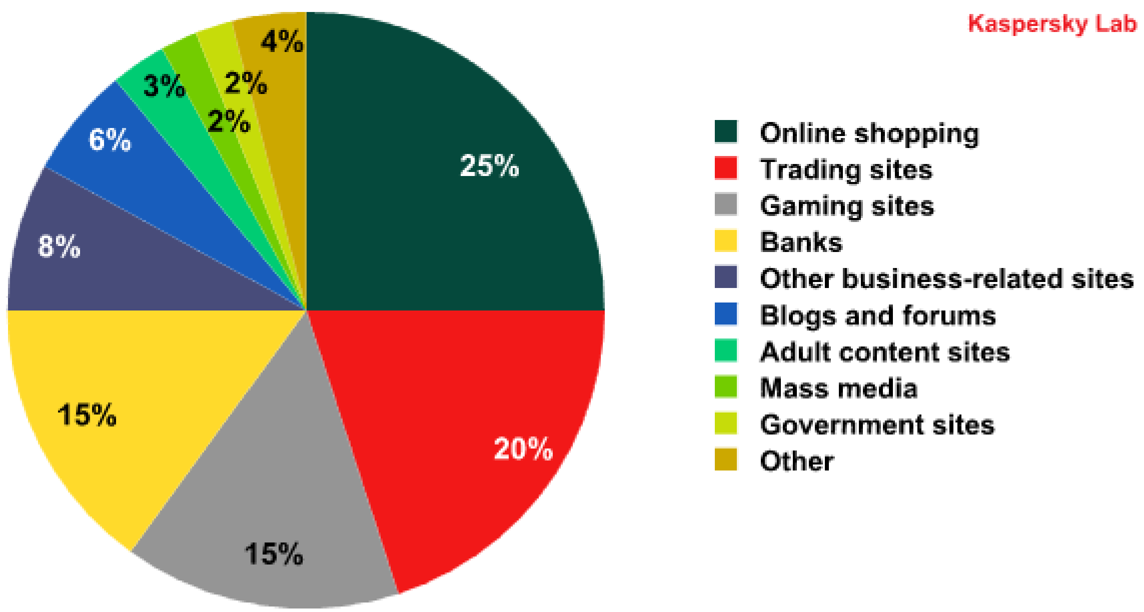
HUAWEI TECHNOLOGIES CO., LTD.

Contents

Severe Losses to Customers



- **Expenses in capacity expansion**
- **Financial losses:** $30,000,000 in the IDC industry
- **Loss of reputation**



Src: http://www.securelist.com

Evolving DDoS Attacks — Application-Layer Attacks, Rendering Conventional Flow Devices Ineffective

ID: Cyxymu	MoneyBooker	Egypt MOI	GOV

- June 2009

Many social networking Web sites were paralyzed by DDoS attacks and were unresponsive to legitimate users.

- October 2010

The official Web site of Moneybooker was paralyzed by DDoS attacks for a whole morning.

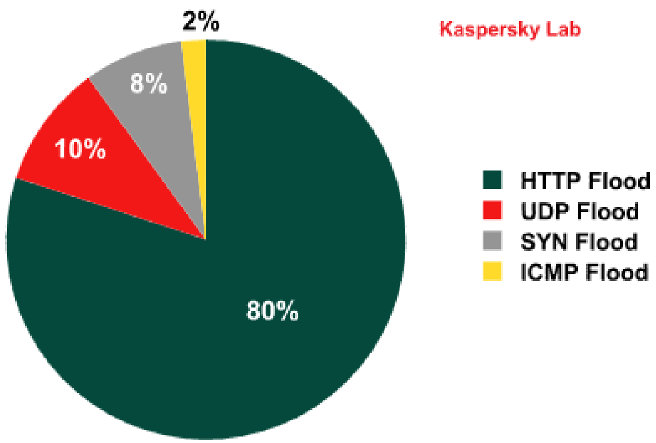
- January 2011

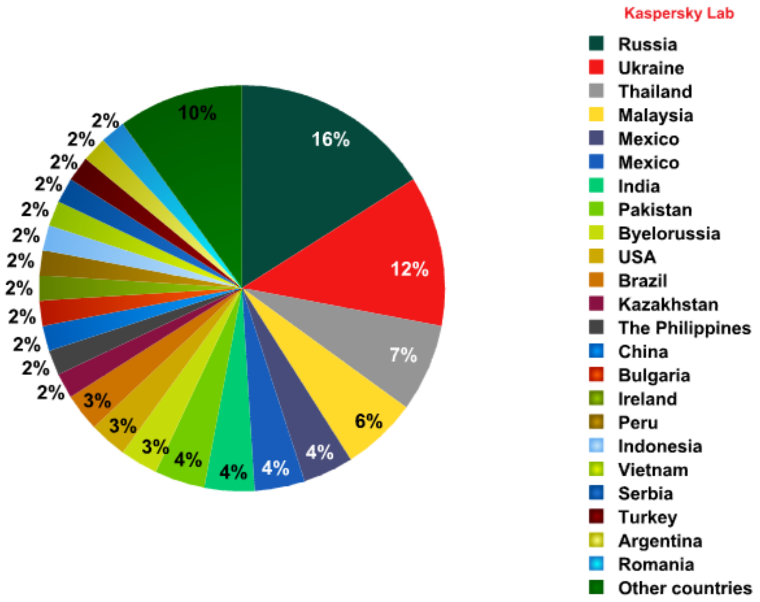
DDoS (application-layer attacks such as HTTP, TCP, and connection floods) attacks to Egypt.

- January 2012

Various Polish Government Web sites were paralyzed by DDoS attacks.

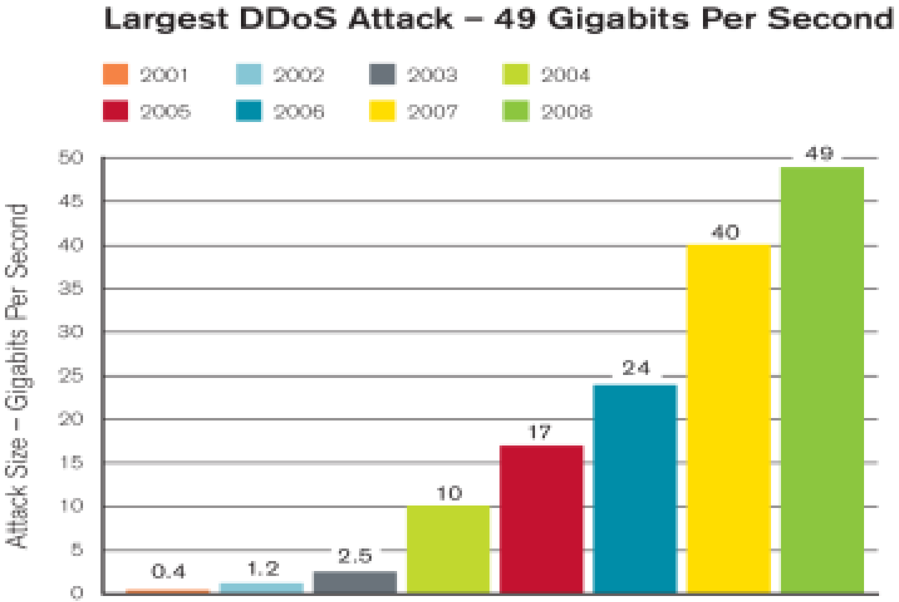
Evolving DDoS Attacks — Larger Scale, 100+ Gbit/s





In the last year, huge attacks have been of more than 120 gigabits per second, If you are on the receiving end of that much punch. It's not a pleasant place to be.

— Andy Ellis, CSO of Akamai



- Statistics about the attacks on the backbone network of Telco A the attack traffic on a single IP E1000E-D exceeds 10 Gbit/s.

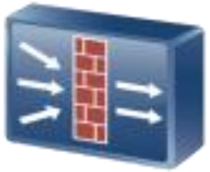
- The longest attack recorded in the second half of the 2011 year targeted a travel company and lasted for 80 days, 19 hours, 13 minutes and 5 seconds, and the average duration of DDOS attacks was 9 hours and 29 minutes.

Contents

2

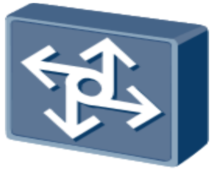
Defense Principle

Conventional Security Devices Are Hopeless and Customers Need New Solutions



• Conventional firewalls can defend against common DDoS or DoS attacks, but will be the first victim in more complicated and severe DDoS attacks.

• IPS identifies and defends against intrusion behaviors based on the signature database; however, DDoS or DoS attacks are launched through legitimate data packets, which do not meet the behavior features of intrusion.



• Based on NetFlow traffic sampling and analysis, conventional anti-DDoS or anti-DoS devices can defend against common flood attacks but cannot cope with light traffic and application-layer attacks. Moreover, conventional anti-DDoS or anti-DoS devices are slow in detecting and traffic diversion.

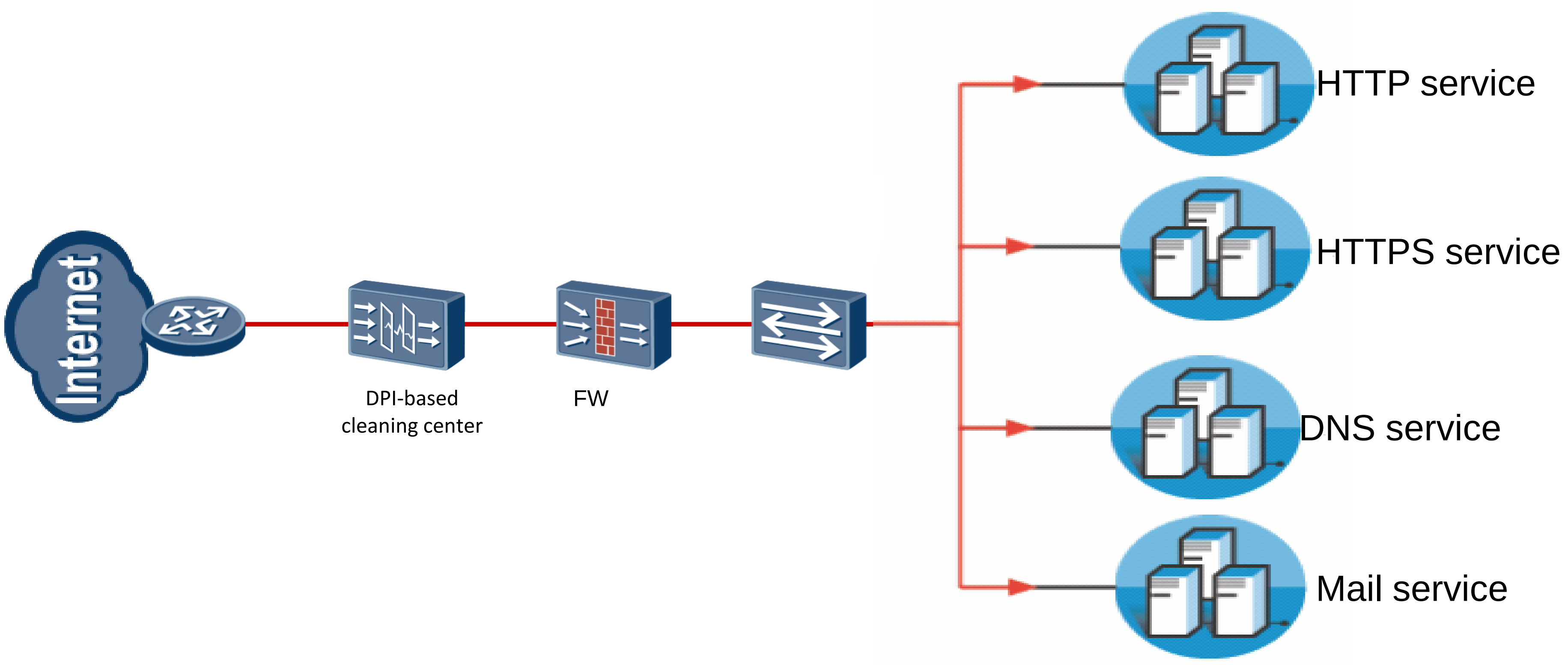
- Conventional anti-DDoS devices cannot cope with evolving DDoS attacks and cannot meet the requirements of customers.

Defending Against DDoS Attacks on the Upstream Network

Huawei anti-DDoS solution should relieve the congestion of carriers' networks first. It cleans the heavy traffic of bandwidth flood attacks .

Refined Defense for VIPs' Services — Defense at the Egress of the Downstream Network

The dedicated cleaning device is deployed at the egress of the access network to deliver refined defense for application servers. It mainly targets at application layer attacks and light traffic attacks.



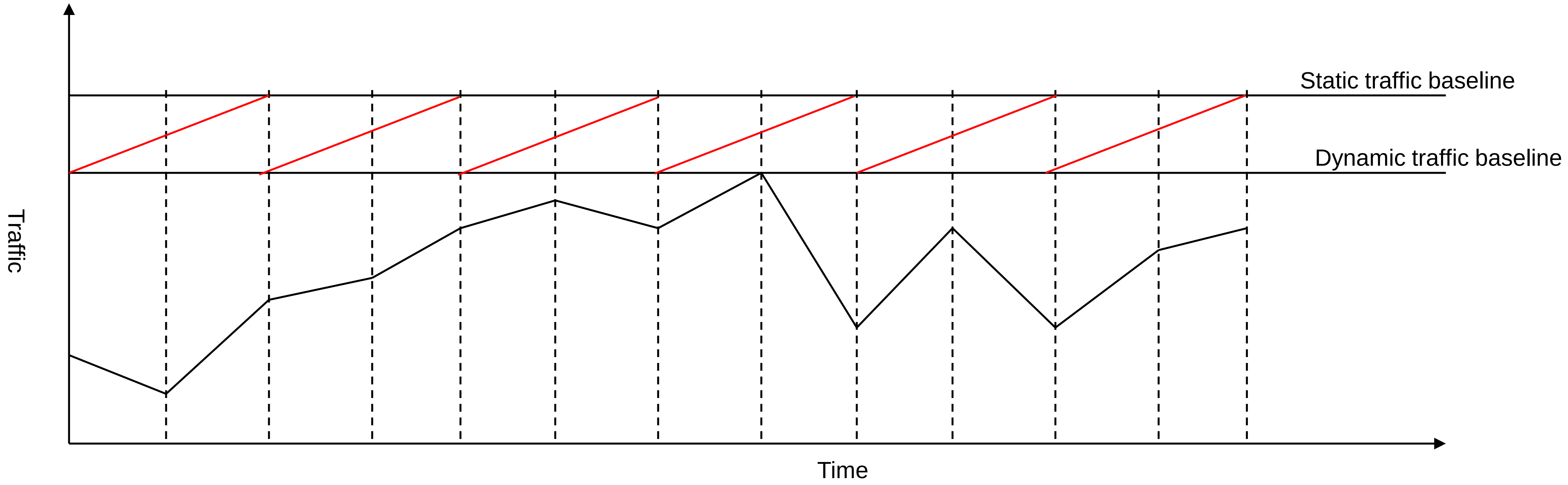
Defense Filters

1. Defends against 19% attack traffic after source authentication is performed.
2. Uses the IP address of the protected network as the attack source, resulting in reflection packet leak.

First Filter	Second Filter			Third Filter
Defense based on Interface	Defense based on services	Defense based on destination IP	Defense based on destination IP range	Defense based on source IP
syn flood syn-ack flood ack flood fin flood rst flood tcp fragment flood tcp abnormal flood http flood dns request flood dns reply flood Icmp flood	syn flood syn-ack flood ack flood fin flood rst flood IP fragment flood tcp abnormal flood http flood CC https flood dns request flood dns reply flood DNS Amplification Attacks DNS cache poisoning attack http hijacking udp flood Icmp flood SSL-DoS SSL-DDoS	syn flood syn-ack flood ack flood fin flood rst flood IP fragment flood tcp abnormal flood http flood CC https flood dns request flood dns reply flood DNS Amplification Attacks DNS cache-poisoning attack http hijacking udp flood Icmp flood SSL-DoS SSL-DDoS	syn flood syn-ack flood ack flood fin flood rst flood tcp fragment flood dns request flood dns reply flood	syn flood syn-ack flood ack flood fin flood rst flood tcp fragment flood tcp abnormal flood DNS flood

Detecting Technology: Dynamic Traffic Baseline

Currently, most anti-DDoS systems employ the single-traffic threshold for identifying attacks. The threshold should be manually configured by users according to the actual traffic on the live network. However, users experience trouble in configuring such a threshold. Under this scenario, Huawei DPI system offers the dynamic traffic baseline, through which learnt dynamic thresholds replace static ones. In so doing, detecting accuracy is improved.



2 Defense Principle

Spoofed Source Attacks: SYN Flood

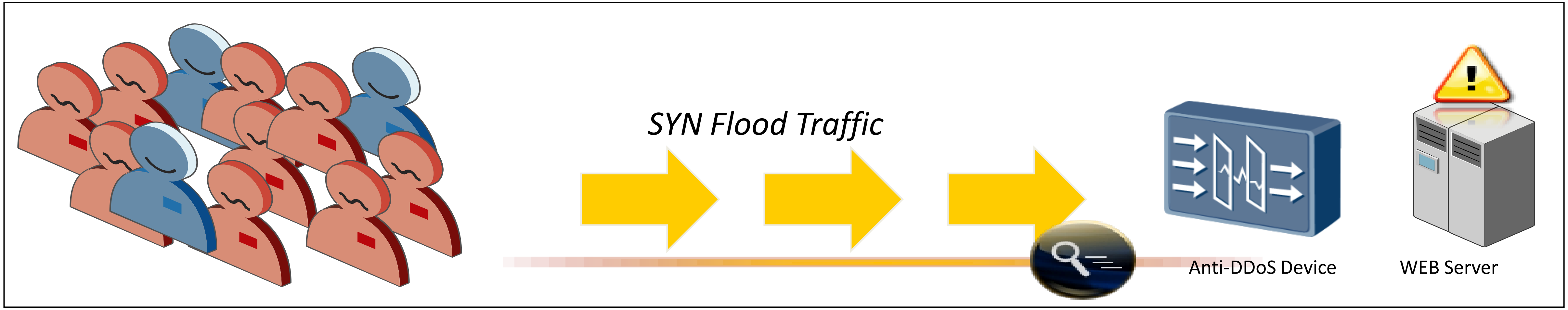
Attack Character:

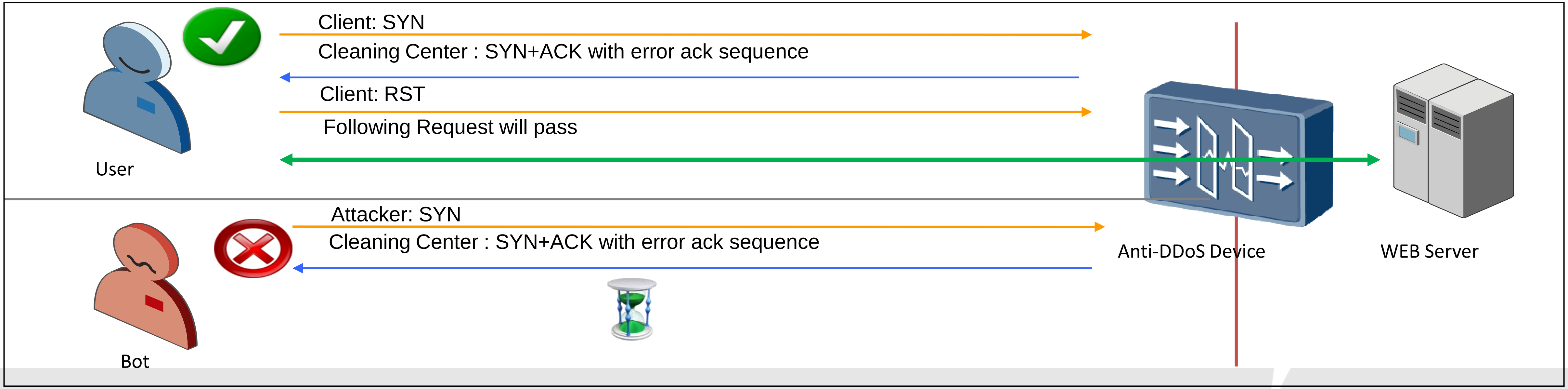
1. Spoofed source attack;
2. Defense can fail when those attack packets' source IP exist;
3. The discontinuous attack can evade the detecting.

Source Address	Dest Address	Summary	L...
100.106.126.97	210.14.67.1	TCP: 38228 > pptp [SYN] Seq=0 Ack=0 Win=65230 Len=0 MSS=1460	62
100.15.82.107	210.14.67.1	TCP: 31332 > pptp [SYN] Seq=0 Ack=0 Win=62013 Len=0 MSS=1460	62
100.2.117.79	210.14.67.1	TCP: 4155 > pptp [SYN] Seq=0 Ack=0 Win=62678 Len=0 MSS=1460	62
100.30.227.6	210.14.67.1	TCP: 21056 > pptp [SYN] Seq=0 Ack=0 Win=62535 Len=0 MSS=1460	62
100.57.126.104	210.14.67.1	TCP: 16467 > pptp [SYN] Seq=0 Ack=0 Win=62662 Len=0 MSS=1460	62
100.74.176.89	210.14.67.1	TCP: 7945 > pptp [SYN] Seq=0 Ack=0 Win=62960 Len=0 MSS=1460	62
101.114.88.6	210.14.67.1	TCP: 61545 > pptp [SYN] Seq=0 Ack=0 Win=63405 Len=0 MSS=1460	62
101.18.247.71	210.14.67.1	TCP: 64858 > pptp [SYN] Seq=0 Ack=0 Win=62116 Len=0 MSS=1460	62
101.24.162.66	210.14.67.1	TCP: 55568 > pptp [SYN] Seq=0 Ack=0 Win=63422 Len=0 MSS=1460	62
101.26.146.19	210.14.67.1	TCP: 11367 > pptp [SYN] Seq=0 Ack=0 Win=63984 Len=0 MSS=1460	62
101.52.177.30	210.14.67.1	TCP: 44103 > pptp [SYN] Seq=0 Ack=0 Win=61534 Len=0 MSS=1460	62
101.52.179.72	210.14.67.1	TCP: 47184 > pptp [SYN] Seq=0 Ack=0 Win=62635 Len=0 MSS=1460	62
101.89.8.70	210.14.67.1	TCP: 53088 > pptp [SYN] Seq=0 Ack=0 Win=63067 Len=0 MSS=1460	62
102.10.55.116	210.14.67.1	TCP: 62567 > pptp [SYN] Seq=0 Ack=0 Win=62174 Len=0 MSS=1460	62

Defense Principle: First-packet-drop can defend and report spoofing_packets log.

Defense against SYN Flood based on Application Layer-based Source Authentication





Principle of Defense against TCP Flood

Feature-based filtering	Whitelist Checking	First-packet-drop	Source Authentication	Checking Source IP	Session-checking	Traffic Shaping
1、Filtering the malformed packets; 2、Filtering packets by fingerprint;	1、Reputation IP list; 2、White-list by source authentication;	First-packet-drop can mitigate up-link stress caused by source authentication by retransmission of TCP protocol.	Defense against spoofed source attacks. Those authenticated sources are allowed to go into the following process.	Defense may fail when those attack packets' source IP exist. Defending this attack by checking the source IP's TCP packets ratio.	Drop packets without valid session.	If the traffic is still heavy and exceeds the actual bandwidth of users after previous steps, traffic shaping is used to ensure available network bandwidths.

1. Spoofed source attack packets must been dropped before building session;
2. Reputation is used to avoid affection from defense.

2

Defense Principle

Spoofed Source Attacks: UDP Flood without fingerprint

Source Address	Dest Address	Summary	Length
211.98.131.156	117.79.86.42	UDP: Source port: 12226 Destination port: 21	142
218.66.37.214	117.79.86.42	UDP: Source port: 14645 Destination port: 22	142
59.39.41.10	117.79.86.42	UDP: Source port: 20052 Destination port: 22	142
222.83.177.137	117.79.86.42	UDP: Source port: 3567 Destination port: 23	142
202.120.49.130	117.79.86.42	UDP: Source port: 62236 Destination port: 21	142
211.225.92.177	117.79.86.42	UDP: Source port: 3548 Destination port: 23	142
122.156.208.72	117.79.86.42	UDP: Source port: 1712 Destination port: 23	142
219.150.132.108	117.79.86.42	UDP: Source port: 3765 Destination port: 22	142
221.195.82.69	117.79.86.42	UDP: Source port: 2401 Destination port: 23	142
61.174.171.118	117.79.86.42	UDP: Source port: 3337 Destination port: 23	142
221.226.4.98	117.79.86.42	UDP: Source port: 1952 Destination port: 21	142

```
0000:   01 02 03 04 05 06 07 08 09 0A 0B 0C 08 00 45 00   ..............E.
0010:   00 80 51 BA 00 00 71 11 D5 3A D3 62 83 9C 75 4F   ..Q...q..:.b..uO
0020:   56 2A 2F C2 00 15 00 6C B9 10 7D 03 53 6A 00 5D   V*/....l..}.Sj.]
0030:   5D 49 31 20 4B 18 3B 5F 36 1C 1F 27 48 66 78 32   ]I1 K.;_6..'Hfx2
0040:   22 28 03 5D 7C 48 5E 5C 0B 33 10 2D 28 74 4A 4A   "(.]|H^\.3.-(tJJ
0050:   2E 05 6D 23 24 64 4B 4B 1C 6A 32 72 5A 59 27 13   ..m#$dKK.j2rZY'.
0060:   39 34 6F 6E 4B 53 54 39 40 36 25 13 09 1A 7F 39   94onKST9@6%....9
0070:   3D 4A 4B 7C 3B 38 08 73 11 4C 4B 6D 1C 7C 03 29   =JK|;8.s.LKm.|.)
0080:   71 1D 02 4A 7C 78 39 05 67 21 43 1D 3D 04         q..J|x9.g!C.=.
```

Attack Character:

1. The source IP address and source port change.
2. The packet payload changes.
3. The packet length also changes.

...ess	Summary	Length
42	UDP: Source port: 12226 Destination port: 21	142
42	UDP: Source port: 14645 Destination port: 22	142
42	UDP: Source port: 20052 Destination port: 22	142
42	UDP: Source port: 3567 Destination port: 23	142
42	UDP: Source port: 62236 Destination port: 21	142
42	UDP: Source port: 3548 Destination port: 23	142
79.86.42	UDP: Source port: 1712 Destination port: 23	142
79.86.42	UDP: Source port: 3765 Destination port: 22	142
79.86.42	UDP: Source port: 2401 Destination port: 23	142
79.86.42	UDP: Source port: 3337 Destination port: 23	142
79.86.42	UDP: Source port: 1952 Destination port: 21	142
79.86.42	UDP: Source port: 4565 Destination port: 24	142

```
0000:   01 02 03 04 05 06 07 08 09 0A 0B 0C 08 00 45 00   ..............E.
0010:   00 80 8C 3D 00 00 76 11 EC 9D DA 42 25 D6 75 4F   ...=..v....B%.uO
0020:   56 2A 39 35 00 16 00 6C 87 E7 44 7D 34 19 3E 02   V*95...l..D}4.>.
0030:   10 07 2C 50 21 23 29 24 00 33 35 12 43 04 35 77   ..,P!#)$.35.C.5w
0040:   21 01 3B 30 57 03 08 09 49 6B 4F 78 6D 6F 3C 0C   !.;0W...IkOxmo<.
0050:   65 31 35 20 6B 16 60 54 72 55 65 3E 0A 4E 75 5C   e15 k.`TrUe>.Nu\
0060:   05 1E 0B 4D 58 70 71 41 44 15 07 2F 35 58 40 46   ...MXpqAD../5X@F
0070:   6A 0B 6D 25 56 66 3E 4E 46 12 05 58 45 00 3E 65   j.m%Vf>NF..XE.>e
0080:   3C 7F 4D 54 5E 0E 06 38 43 6E 72 08 53 7C         <.MT^..8Cnr.S|
```

Defense Principle:

1. If network service-based defense, especially, access-layer defense is employed, packets not complying with the service model are directly discarded. As shown in the figure, attack packets are upon ports 21 to 24 and are directly discarded because no such services exist. If static filtering is used to discard these attack packets, the system displays "User_defined_filter".
2. If attacks are upon service ports, TCP authentication must be performed over UDP data transmission such as online games. In this case, TCP association can be used to defend against UDP flood attacks. The device displays "Spoofing_packets" for packet loss.
3. If traffic limiting is applied, the device displays "Overflow_packets" for packet loss.

Spoofed Source Attacks: UDP Flood with fingerprint

Source Address	Dest Address	Summary	Length
124.128.63.242	119.63.36.11	UDP: Source port: 51160 Destination port: 9801	569
59.56.250.88	119.63.36.11	UDP: Source port: 10289 Destination port: 9801	711
110.230.30.16	119.63.36.11	UDP: Source port: 9366 Destination port: 9801	1046
61.182.49.114	119.63.36.11	UDP: Source port: 3458 Destination port: 9801	1242
113.162.97.102	119.63.36.11	UDP: Source port: 2723 Destination port: 9801	1067
112.162.164.163	119.63.36.11	UDP: Source port: 4296 Destination port: 9801	1257
88.231.26.152	119.63.36.11	UDP: Source port: 11105 Destination port: 9801	1106
113.240.232.6	119.63.36.11	UDP: Source port: 2218 Destination port: 9801	353
121.33.201.17	119.63.36.11	UDP: Source port: 2840 Destination port: 9801	504

```
24 0B C7 D8 26 49 02 17 04 60 30 30 30 30 30 30   $...&I...`000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30   0000000000000000
```

Attack Character:

1. The source IP address and source port change.
2. The packet length also changes.
3. Packet payloads can be either the same such as Aladdin attacks or different in the case that payload bytes for the same packet are identical.

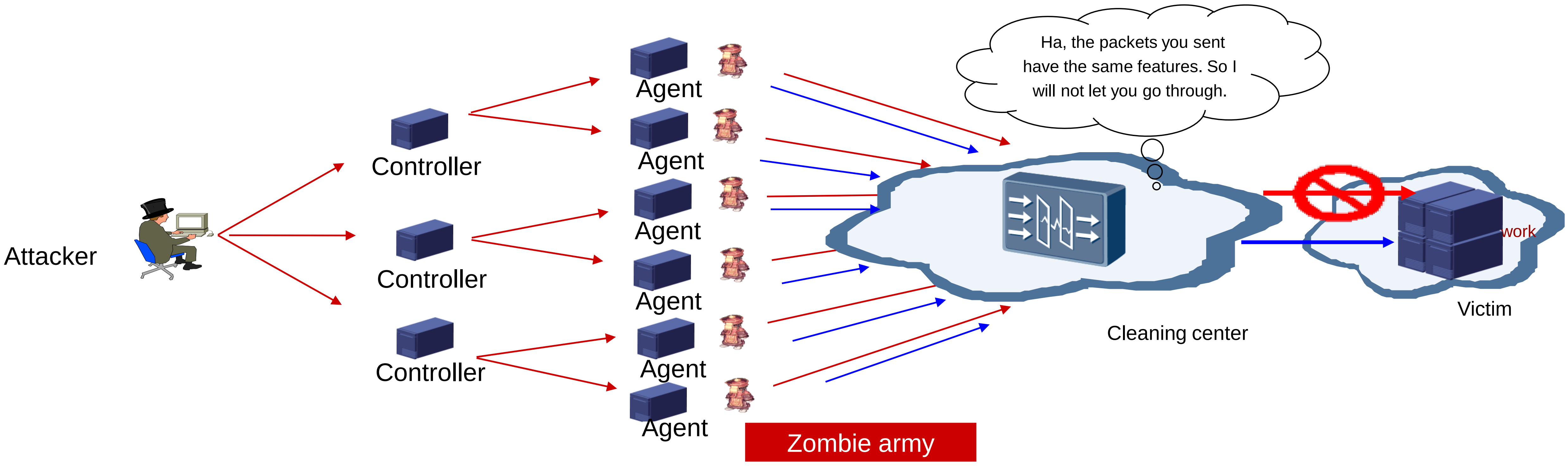
...s		Summary	Length
	...1	UDP: Source port: 51160 Destination port: 9801	569
.88	119.63.36.11	UDP: Source port: 10289 Destination port: 9801	711
0.16	119.63.36.11	UDP: Source port: 9366 Destination port: 9801	1046
.114	119.63.36.11	UDP: Source port: 3458 Destination port: 9801	1242
7.102	119.63.36.11	UDP: Source port: 2723 Destination port: 9801	1067
64.163	119.63.36.11	UDP: Source port: 4296 Destination port: 9801	1257
.152	119.63.36.11	UDP: Source port: 11105 Destination port: 9801	1106
32.6	119.63.36.11	UDP: Source port: 2218 Destination port: 9801	353
1.17	119.63.36.11	UDP: Source port: 2840 Destination port: 9801	504
.79	119.63.36.11	UDP: Source port: 12298 Destination port: 9801	1003
125.83.242.212	119.63.36.11	UDP: Source port: 3351 Destination port: 9801	977
61.167.105.146	119.63.36.11	UDP: Source port: 44330 Destination port: 9801	513

```
0000:  01 02 03 04 05 06 07 08 09 0A 0B 0C 08 00 45 68   ..............Eh
0010:  02 B9 39 56 00 00 75 11 38 9B 3B 38 FA 58 77 3F   ..9V..u.8.;8.Xw?
0020:  24 0B 28 31 26 49 02 A5 40 71 BE BE BE BE BE BE   $.(1&I..@q......
0030:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0040:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0050:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0060:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0070:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0080:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
0090:  BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE BE   ................
```

Defense Principle:

1. Such attacks can be filtered out through dynamic fingerprint learning. In this case, the device displays "Dynamic_filter" for packet loss.
2. If the locations of attack features vary randomly, you can use refined packet filtering in the case of manually extracting the attack feature of each attack. In this case, the device displays "User_defined_filter" for packet loss.

Defense against UDP Flood with Fingerprints based on Dynamic Fingerprint Learning



Principle of Defense against UDP Flood

Feature-based filtering	Whitelist Checking	First-packet-drop	Source Authentication	Behavior Analysis	Traffic Shaping
Filtering packets by fingerprint.	This method only for those UDP services needing TCP authentication first.	Drop the first packet from the source IP based on retransmission of UDP application.	Those sources authenticated are allowed to go into the following process.	Dynamic Fingerprint Learning	If the traffic is still heavy and exceeds the actual bandwidth of users after previous steps, traffic shaping is used to ensure available network bandwidths.

1. UDP-based data transmission must pass TCP authentication. Therefore, TCP association is recommeded for defending against UDP flood attacks.
2. On the live network, UDP flood attacks are mainly at four layers, because key UDP data is transmitted in encryption mode. Therefore, adding refined packet-filtering rules meets the requirements on UDP flood cleaning, except for manual intervention upon attacks. The change of each attack packet brings challenges. To resolve such a problem, use packet features as filtering ones and set the action to whilisting the source IP address if matched.
3. Many attacks bear features on the live netowrk. In this case, static filtering or dynamic fingerprint learning is recommended.

2

Defense Principle

Spoofed Source Attacks: ICMP Flood

Source Address	Dest Address	Summary
10.0.1.253	210.14.70.113	ICMP: Time-to-live exceeded
220.249.160.149	210.14.70.113	ICMP: Time-to-live exceeded
202.195.41.105	210.14.70.113	ICMP: Time-to-live exceeded
211.99.58.18	210.14.70.113	ICMP: Time-to-live exceeded
124.65.231.18	210.14.70.113	ICMP: Time-to-live exceeded
61.240.179.242	210.14.70.113	ICMP: Time-to-live exceeded
59.44.124.130	210.14.70.113	ICMP: Time-to-live exceeded
210.83.64.5	210.14.70.113	ICMP: Time-to-live exceeded
192.168.163.2	210.14.70.113	ICMP: Time-to-live exceeded
221.192.24.45	210.14.70.113	ICMP: Time-to-live exceeded
210.53.112.6	210.14.70.113	ICMP: Time-to-live exceeded
61.49.39.49	210.14.70.113	ICMP: Time-to-live exceeded
218.104.200.81	210.14.70.113	ICMP: Time-to-live exceeded
221.4.212.5	210.14.70.113	ICMP: Time-to-live exceeded
61.159.176.249	210.14.70.113	ICMP: Time-to-live exceeded
219.141.134.14	210.14.70.113	ICMP: Time-to-live exceeded
117.39.11.2	210.14.70.113	ICMP: Time-to-live exceeded
211.154.208.181	210.14.70.113	ICMP: Time-to-live exceeded
210.45.231.178	210.14.70.113	ICMP: Time-to-live exceeded
202.112.6.69	210.14.70.113	ICMP: Time-to-live exceeded

Source Address	Dest Address	Summary
10.10.5.30	210.14.70.113	ICMP: Time-to-live exceeded
218.27.16.206	210.14.70.113	ICMP: Destination unreachable
218.104.181.134	210.14.70.113	ICMP: Time-to-live exceeded
124.65.60.245	210.14.70.113	ICMP: Time-to-live exceeded
218.9.46.37	210.14.70.113	ICMP: Time-to-live exceeded
202.106.2.158	210.14.70.113	ICMP: Time-to-live exceeded
218.74.120.41	210.14.70.113	ICMP: Time-to-live exceeded
202.112.6.69	210.14.70.113	ICMP: Time-to-live exceeded
124.127.133.30	210.14.70.113	ICMP: Time-to-live exceeded
218.87.121.1	210.14.70.113	ICMP: Time-to-live exceeded
218.104.201.174	210.14.70.113	ICMP: Time-to-live exceeded
59.50.113.33	210.14.70.113	ICMP: Time-to-live exceeded
210.38.0.89	210.14.70.113	ICMP: Time-to-live exceeded
120.80.237.18	210.14.70.113	ICMP: Redirect
221.6.142.1	210.14.70.113	ICMP: Time-to-live exceeded
202.112.15.34	210.14.70.113	ICMP: Time-to-live exceeded
61.130.159.216	210.14.70.113	ICMP: Time-to-live exceeded
202.121.47.2	210.14.70.113	ICMP: Time-to-live exceeded
222.62.201.226	210.14.70.113	ICMP: Time-to-live exceeded
60.2.226.25	210.14.70.113	ICMP: Destination unreachable
58.30.14.104	210.14.70.113	ICMP: Destination unreachable

Attack Character: Spoofing source attack.

Defense Principle: First-packet-drop can defend and report spoofing_packets log.

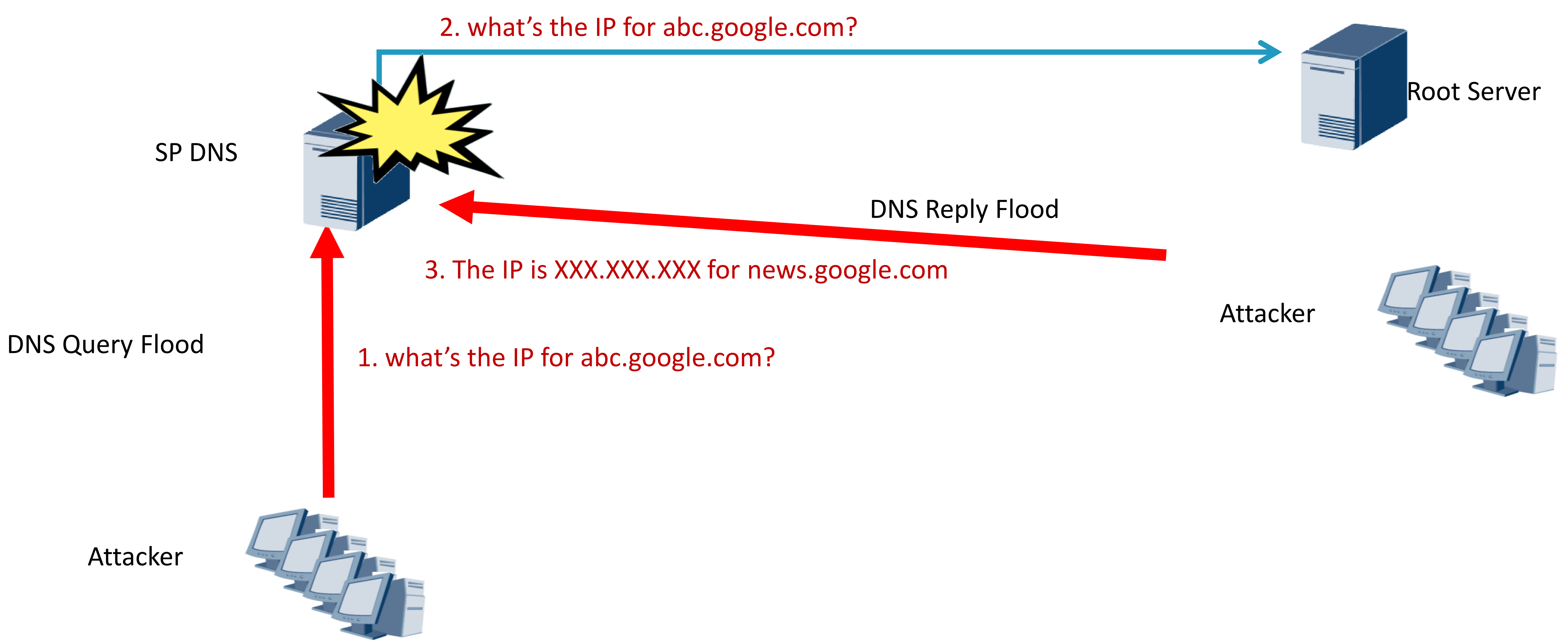
Principle of Defense against ICMP Flood

Feature-based Filtering	Whitelist Checking	First-packet-drop	Traffic Shaping
Filtering packets by fingerprint.	If service traffic exists between the client and the protected network, ICMP packets between them are allowed through; otherwise, ICMP packets enter the first packet discarding procedure.	Drop the first packet from the source IP.	If the traffic is still heavy and exceeds the actual bandwidth of users after previous steps, traffic shaping is used to ensure available network bandwidths.

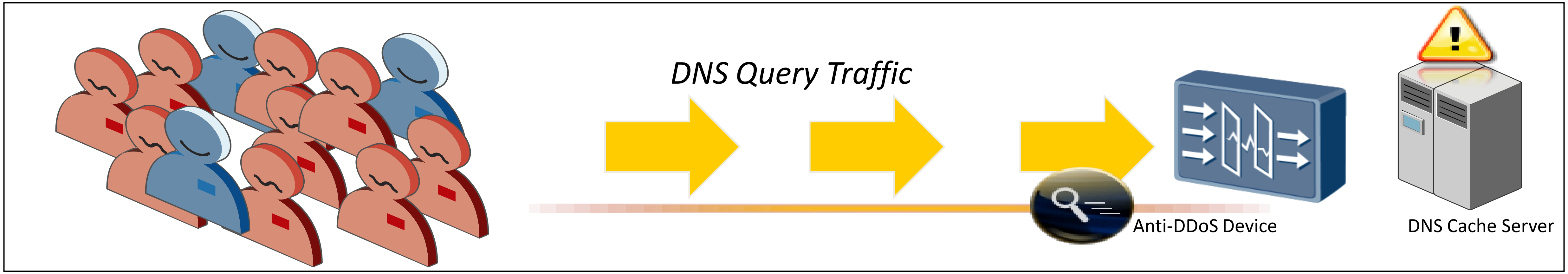
2

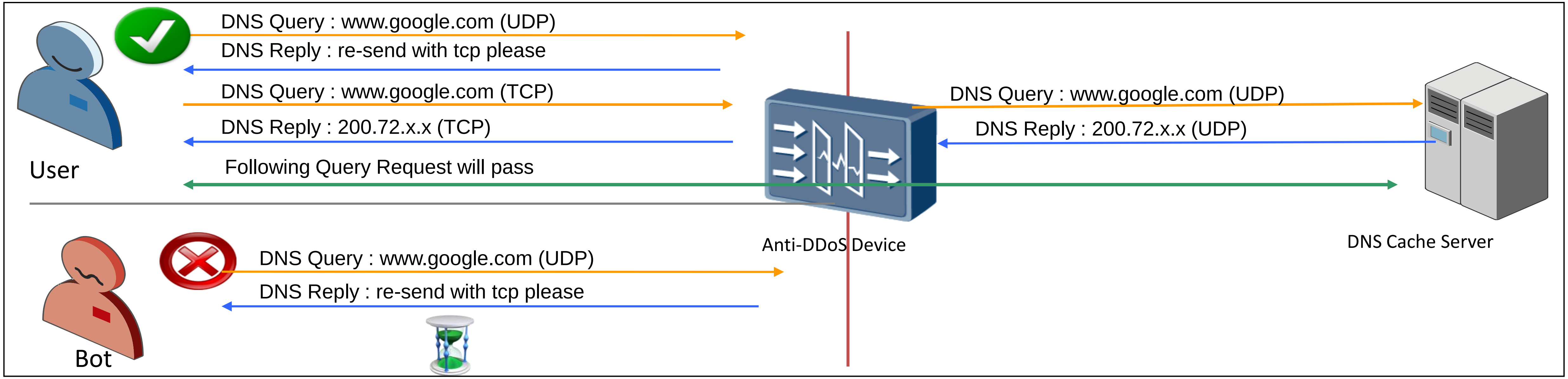
Defense Principle

DNS Query and Reply Flood Attacks

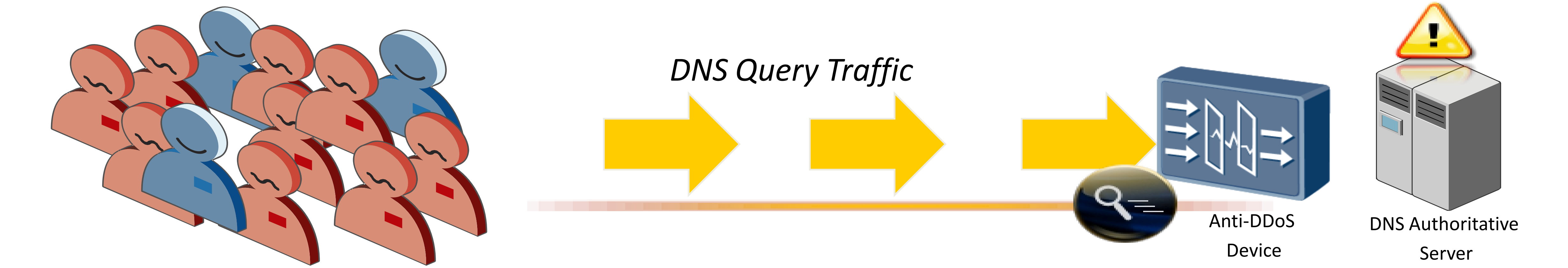


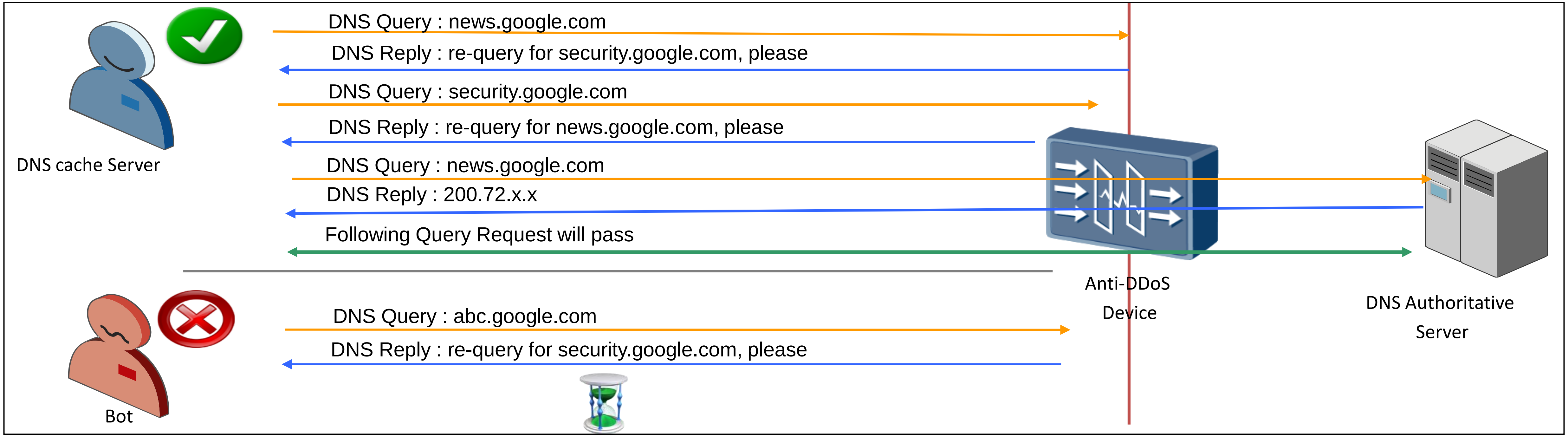
Defense against DNS Query Flood for DNS Cache Server based on Application Layer-based Source Authentication





Defense against DNS Query Flood for DNS Authoritative Server based on Application Layer-based Source Authentication





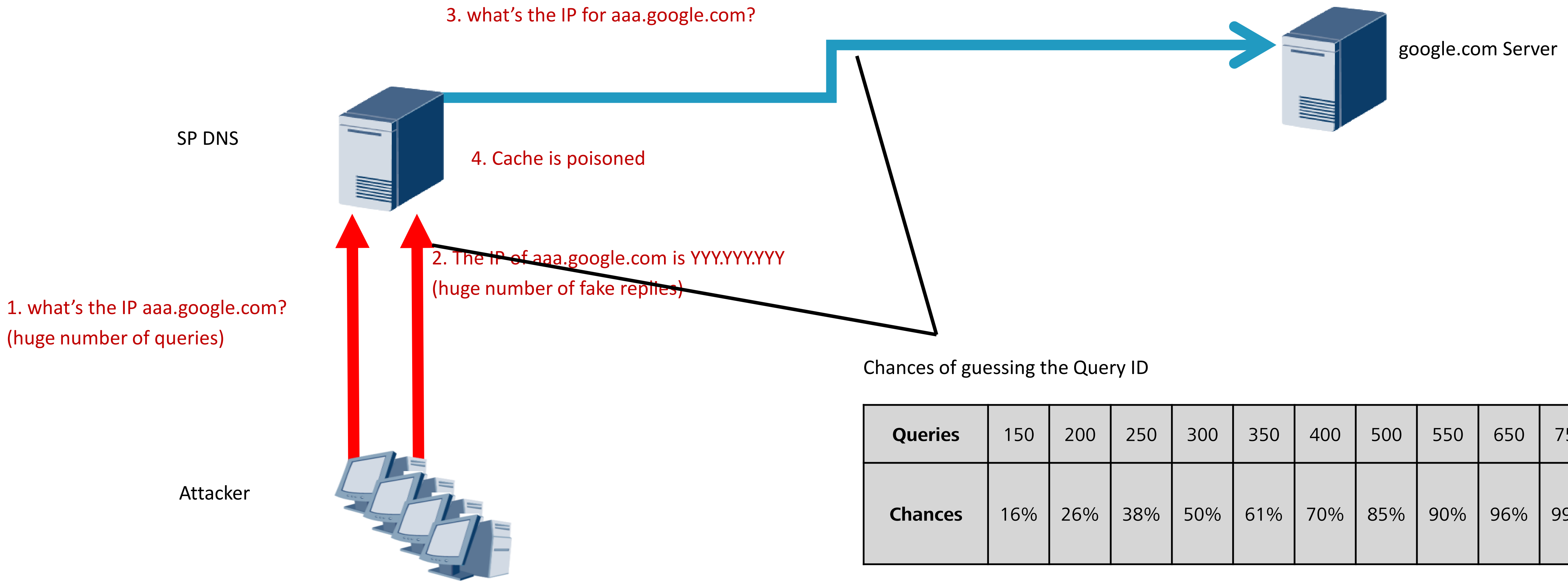
Malformed DNS Domain Attack

No.	Time	Source	Destination	length	Protocol	Info
1	0	124.114.153.221	218.30.19.40	79	DNS	Standard query A 108sz0QDg.dtywl.com
2	0	61.185.87.77	218.30.19.40	80	DNS	Standard query A ogcscy28m4.dtywl.com
3	0	113.140.72.22	218.30.19.40	77	DNS	Standard query A sk8ksu4.dtywl.com
4	0	61.185.87.77	218.30.19.40	79	DNS	Standard query A i2yc6yuk4.dtywl.com
5	0	61.185.87.77	218.30.19.40	77	DNS	Standard query A q0cm6i0.dtywl.com
6	0	61.185.87.77	218.30.19.40	77	DNS	Standard query A yy2sg0m.dtywl.com
7	0	61.185.87.77	218.30.19.40	80	DNS	Standard query A hx3xnik4er.dtywl.com
8	0	124.114.153.221	218.30.19.40	78	DNS	Standard query A Ybz6rPfJ.dtywl.com
9	0	61.185.87.77	218.30.19.40	77	DNS	Standard query A fxx9gos.dtywl.com
10	0	61.185.87.77	218.30.19.40	77	DNS	Standard query A 0o391r9.dtywl.com
11	0	61.185.87.77	218.30.19.40	81	DNS	Standard query A rectu1hny32.dtywl.com
12	0	124.114.153.221	218.30.19.40	80	DNS	Standard query A xX82Rb3glP.dtywl.com
13	0	113.140.72.22	218.30.19.40	78	DNS	Standard query A 62bzk5fz.dtywl.com
14	0	124.114.153.221	218.30.19.40	78	DNS	Standard query A 39zVShE9.dtywl.com
15	0	61.185.87.77	218.30.19.40	78	DNS	Standard query A 15f13821.dtywl.com
16	0	124.114.153.221	218.30.19.40	80	DNS	Standard query A AB7Ii5a7Bc.dtywl.com
17	0	61.185.87.77	218.30.19.40	81	DNS	Standard query A q1x1s3k4nge.dtywl.com

Attack Character: uses the forged source or real IP address on the live network as the source IP address to send massive requests for non-existent domain names. This leads to the server's continuous sending of DNS requests and exerts severe impacts.

Defense Principle: uses rate limiting based on domain name matching to filter out attacks. The device displays "User_defined_filter" for packet loss.

DNS Cache Poisoning — Malformed_connections

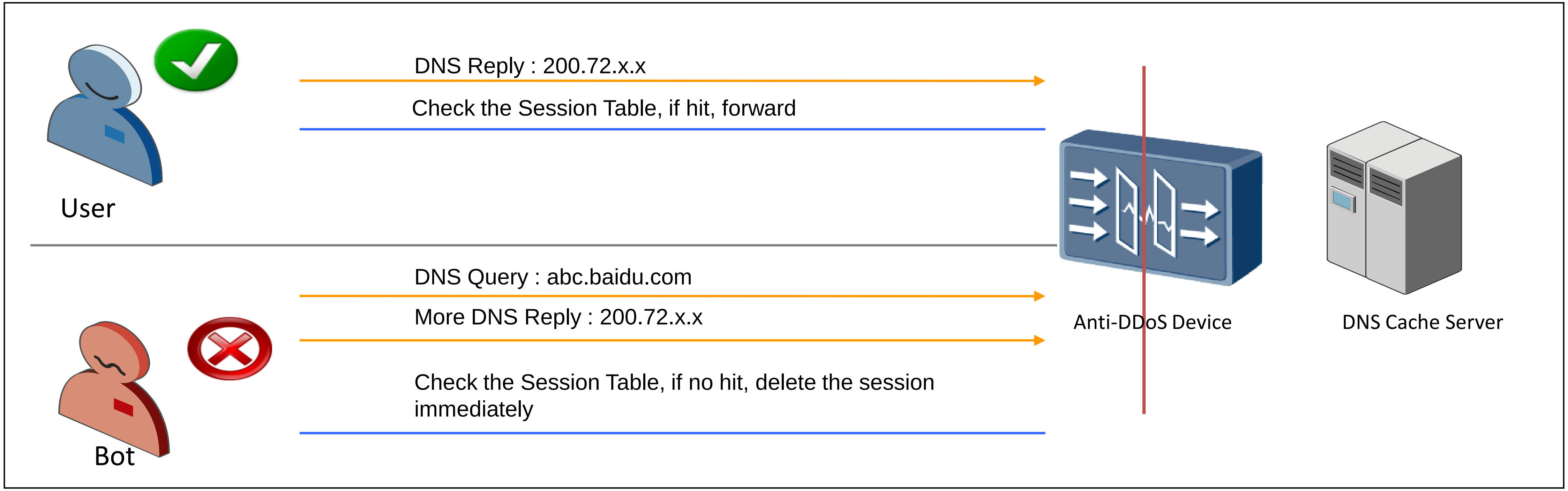


Chances of guessing the Query ID

Queries	150	200	250	300	350	400	500	550	650	750
Chances	16%	26%	38%	50%	61%	70%	85%	90%	96%	99%

Attack Character: uses the DNS session to send massive spoofed packets to match the session at possibilities within the short period. DNS cache poisoning attacks are forged source ones. This mode avoids the weakness of TCP three-way handshake.

Defense against DNS Cache Poisoning based on Session-check



Principle of Defense against DNS Flood

Principle of Defense against DNS query flood/reply flood

Whitelist Checking	First-packet-drop	Source Authenticating	Malformed packet Filtering	Malformed Domain Filtering	Source IP Rate Limiting	Session-Checking
1、Reputation IP list; 2、White-list by source authentication;	First-packet-drop can mitigate up-link stress caused by source authentication by retransmission of DNS protocol.	Defense against spoofed source attacks. Those authenticated sources are allowed to go into the following process.	Filtering malformed DNS packets.	Defense against malformed DNS request flood from real IP.	Limiting the DNS request rate on source IP.	Defense against DNS cache poisoning and DNS reflection attack based on session-check

1. Spoofed source attack packets must been dropped before building session;
2. Reputation is used to avoid affection from defense.

2

Defense Principle

TCP Retransmission Attack—Client_attacks

No.	Time	Source	Destination	Protocol	Info
4	4	222.240.187.37	118.250.201.68	HTTP	Continuation or non-HTTP traffic
5	4	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#1] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
5	4	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
7	4	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
3	4	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
9	4	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#2] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
0	4	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#3] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
1	4	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#4] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
2	5	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#5] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
3	5	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
4	5	222.240.187.37	118.250.201.68	HTTP	[TCP Previous segment lost] Continuation or non-HTTP traffic
5	5	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#6] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
6	5	118.250.201.68	222.240.187.37	TCP	[TCP Dup ACK 92#7] 4859 > http [ACK] Seq=168 Ack=26639 Win=4
7	6	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
8	6	118.250.201.68	222.240.187.37	TCP	4859 > http [ACK] Seq=168 Ack=28041 Win=46537 Len=0 TSV=9491
9	6	222.240.187.37	118.250.201.68	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic

Retransmission request

Retransmission Packets

```
+ Frame 95 (78 bytes on wire, 78 bytes captured)
+ Ethernet II, Src: HuaweiTe_2e:b9:00 (00:e0:fc:2e:b9:00), Dst: F5Networ_42:4a:35 (00:01:d7:42:4a:35)
+ Internet Protocol, Src: 118.250.201.68 (118.250.201.68), Dst: 222.240.187.37 (222.240.187.37)
- Transmission Control Protocol, Src Port: 4859 (4859), Dst Port: http (80), Seq: 168, Ack: 26639, Len: 0
    Source port: 4859 (4859)
    Destination port: http (80)
    Sequence number: 168    (relative sequence number)
    Acknowledgement number: 26639    (relative ack number)
    Header length: 44 bytes
  + Flags: 0x0010 (ACK)
    Window size: 46537
    Checksum: 0xd947 [correct]
  - Options: (24 bytes)
      NOP
      NOP
      Time stamp: tsval 94897, tsecr 6049315
      NOP
      NOP
    - SACK: 29443-30845
        left edge = 29443 (relative)
        right edge = 30845 (relative)
  + [SEQ/ACK analysis]
```

Retransmi-ssion packets

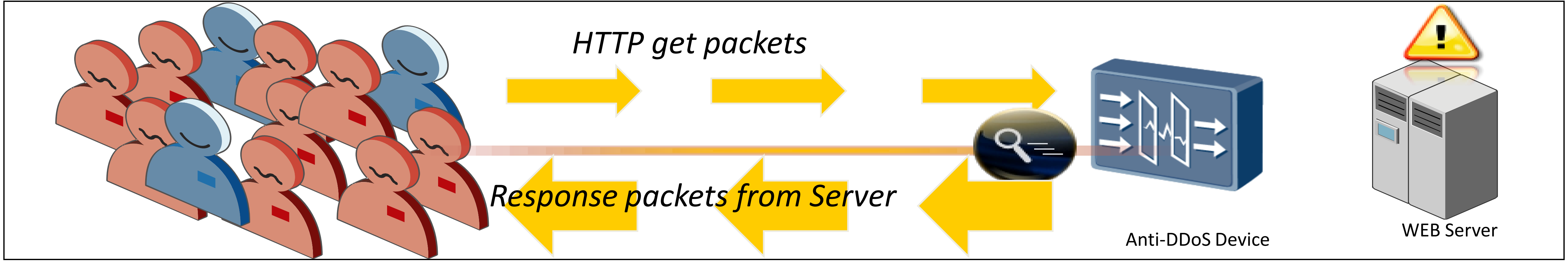
Attack Character:

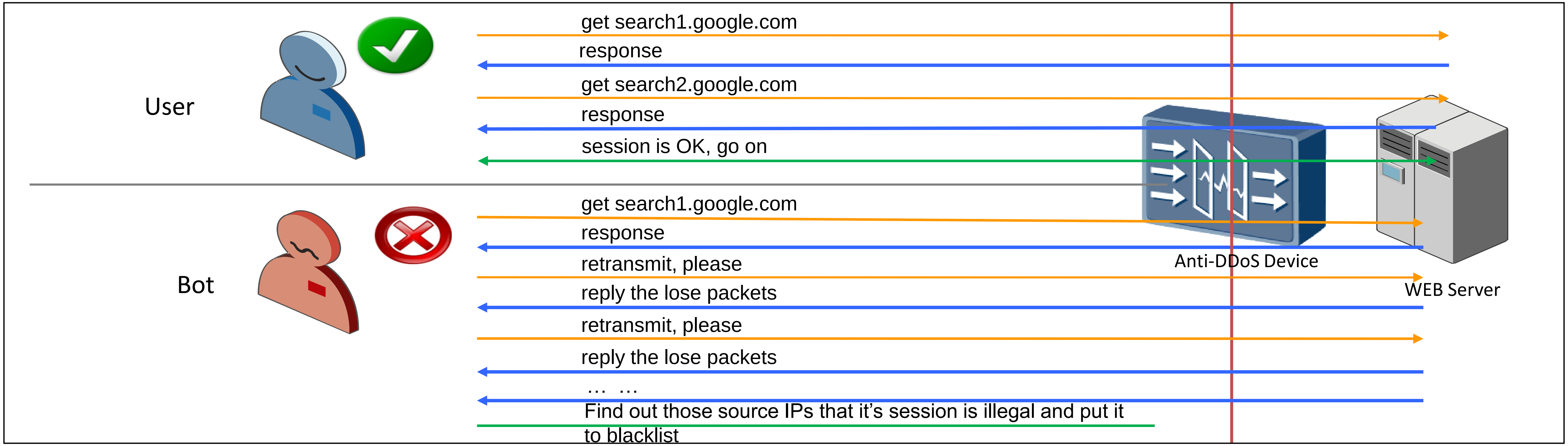
1、 Real source of attack, attack the client and server to establish a connection, a limited number of attacks on the client to send fewer messages, and as far as possible to hide the attack side; this is a common feature of Client_attacks;

2、 The same session, the attacker client kept send retransmission request message, the server that the message transmission process have discarded, non-stop to the client retransmission "discarded" message;

3、 The client IP is 118.250.201.68, the server IP is 222.240.187.37, packet capture analysis can be seen a small number of packets of the attack sent by the client, and the packet length, and the server responds with a messagerelatively large number of packets generally are larger, thus giving rise to attack the client to use a small downlink bandwidth in exchange for large upstream bandwidth overhead, leading to serious uplink congestion.

Defense against TCP Retransmission Attack based on Session-checking

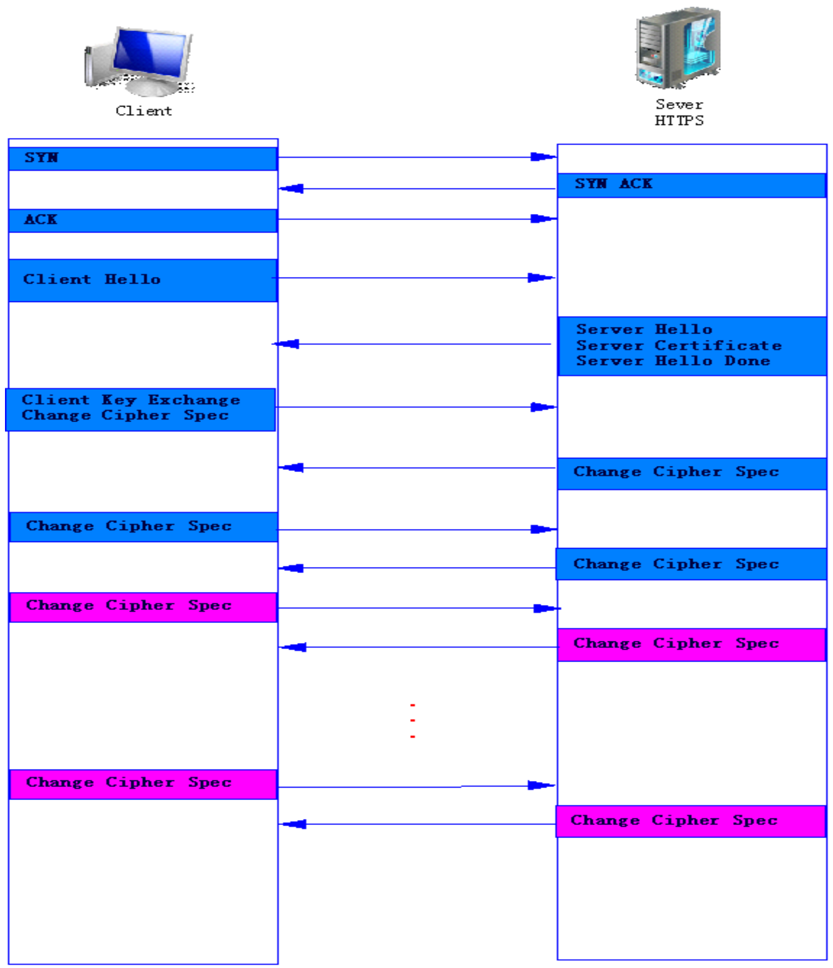




2

Defense Principle

SSL-DoS Attack on SSL Server



Source Address	Dest Address	Summary
172.16.104.201	128.18.74.201	TCP: 2341 > https [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
128.18.74.201	172.16.104.201	TCP: https > 2341 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
172.16.104.201	128.18.74.201	TCP: 2341 > https [ACK] Seq=1 Ack=1 Win=65535 Len=0
172.16.104.201	128.18.74.201	SSLv2: Client Hello
128.18.74.201	172.16.104.201	TLS: Server Hello, Certificate, Server Hello Done
172.16.104.201	128.18.74.201	TLS: Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Certificate Request[Unreassembled Packet (incorrect TCP checksum)]
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Server Hello[Unreassembled Packet (incorrect TCP checksum)]
172.16.104.201	128.18.74.201	TLS: Hello Request
128.18.74.201	172.16.104.201	TLS: Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Encrypted Handshake Message
172.16.104.201	128.18.74.201	TLS: Encrypted Handshake Message, Change Cipher Spec, Encrypted Handshake Message
128.18.74.201	172.16.104.201	TLS: Change Cipher Spec, Encrypted Handshake Message

Defense against SSL-DDoS

- Attack Character
  - **Instead it exhausts the server resources from a single host requiring only a single TCP/IP socket. This attack is a Distributed Denial of Service (DDOS) by botnet.**
  - **A single server can perform between 150-300 handshakes per second. While a single client can request up to 1000 handshakes per second.**
  - **If the botnet is consist of 1,000 hosts, it's attack result is obvious. And because a single host's connections is few, this attack can evade detecting from network security devices.**

- Defense Principle
  - A legal host sets up a ssl session to transmit data, but a illegal host only set up session to exhaust SSL **handshakes.** Check session and put those source IPs whose session is illegal to blacklist.
  - Limit the connection from IPs which doesn't exist in reputation list.

2

Defense Principle

HTTP Flood—Client_attacks

Source Ad...	Dest Address	Summary	Length
1.197.127.162	210.14.67.43	TCP: 2646 > http [ACK] Seq=0 Ack=0 Win=63888 Len=0 TSV=83017 TSER=0	66
1.202.186.37	210.14.67.43	TCP: 56060 > http [ACK] Seq=0 Ack=0 Win=63877 Len=0	54
1.205.20.94	210.14.67.43	TCP: 13158 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0	54
1.205.20.94	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1450
1.205.64.213	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1450
1.56.192.51	210.14.67.43	TCP: 1750 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1440 WS=2	66
1.60.34.129	210.14.67.43	TCP: 12616 > http [ACK] Seq=0 Ack=0 Win=46492 Len=0	54
1.60.85.79	210.14.67.43	TCP: 4777 > http [ACK] Seq=0 Ack=0 Win=65535 Len=0	54
1.61.40.89	210.14.67.43	TCP: 1380 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1440	62
1.81.6.90	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1450
1.81.6.90	210.14.67.43	TCP: 1520 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1440 WS=0	66
1.83.102.2	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1224
1.87.203.214	210.14.67.43	TCP: 64856 > http [SYN] Seq=0 Ack=0 Win=8192 Len=0 MSS=1440	62
101.71.2.68	210.14.67.43	TCP: 59970 > http [ACK] Seq=0 Ack=0 Win=65535 Len=0	54
110.17.67.31	210.14.67.43	TCP: 2058 > http [ACK] Seq=0 Ack=0 Win=53919 Len=0	54
110.18.4.115	210.14.67.43	TCP: 57169 > http [ACK] Seq=0 Ack=0 Win=16469 Len=0	54
110.185.170.60	210.14.67.43	TCP: 2565 > http [RST, ACK] Seq=0 Ack=0 Win=0 Len=0	54
110.187.147.249	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1450
110.244.97.154	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1248
110.245.203.105	210.14.67.43	HTTP: GET //p57/ HTTP/1.1	1450

Attack Character: Attack Character: This attack is a kind of http flood by botnet using a lot of open proxies. Sessions from single proxy are few to avoid detecting from security devices. The attack result is obvious when the attacked URI exhausts lots of CPU capability. “P57” directory is the attack aim.

Defense Principle: Redirection check code is used to defend against CC attack. Attacks are launched by botnet. As a result, there is no response to authentication requests and access traffic fails to be transparently transmitted to the server. The cleaning device reports client_attacks log.

CC Attack—HTTP Flood by Botnet using Proxy

Open Proxy

Source Address	Dest Address	Summary
200.65.127.161	192.168.1.57	HTTP: HTTP/1.1 400 Bad Request (text/html)
200.65.127.161	192.168.1.57	TCP: 3128 > 3553 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 ...
192.168.1.57	200.65.127.161	TCP: 3118 > http [RST, ACK] Seq=308 Ack=437 Win=0 Len=0
192.168.1.57	200.65.127.161	TCP: 3553 > 3128 [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.1.57	200.65.127.161	HTTP: GET http://www.horseb.org HTTP/1.1
203.178.133.3	192.168.1.57	TCP: 3127 > 3558 [ACK] Seq=1 Ack=307 Win=6432 Len=0
200.65.127.161	192.168.1.57	TCP: 3128 > 3483 [ACK] Seq=1 Ack=307 Win=16078 Len=0
200.65.127.161	192.168.1.57	HTTP: HTTP/1.1 400 Bad Request (text/html)
200.65.127.161	192.168.1.57	TCP: 3128 > 3483 [FIN, ACK] Seq=437 Ack=307 Win=16384 ...
200.65.127.161	192.168.1.57	TCP: http > 3484 [ACK] Seq=1 Ack=307 Win=16078 Len=0
192.168.1.57	200.65.127.161	TCP: 3483 > 3128 [ACK] Seq=307 Ack=438 Win=65099 Len=0
200.65.127.161	192.168.1.57	HTTP: HTTP/1.1 400 Bad Request (text/html)
200.65.127.161	192.168.1.57	TCP: http > 3484 [FIN, ACK] Seq=437 Ack=307 Win=16384 Le...
192.168.1.57	200.65.127.161	TCP: 3484 > http [ACK] Seq=307 Ack=438 Win=65099 Len=0
192.168.1.57	203.178.133.3	TCP: 3610 > 3127 [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS...
200.65.127.161	192.168.1.57	TCP: http > 3556 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 ...
192.168.1.57	200.65.127.161	TCP: 3556 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
192.168.1.57	200.65.127.161	HTTP: GET http://www.horseb.org HTTP/1.1
203.178.133.2	192.168.1.57	TCP: 3127 > 3561 [ACK] Seq=1 Ack=307 Win=6432 Len=0
200.65.127.161	192.168.1.57	TCP: 3128 > 3840 [ACK] Seq=1 Ack=307 Win=16078 Len=0
200.65.127.161	192.168.1.57	HTTP: HTTP/1.1 400 Bad Request (text/html)

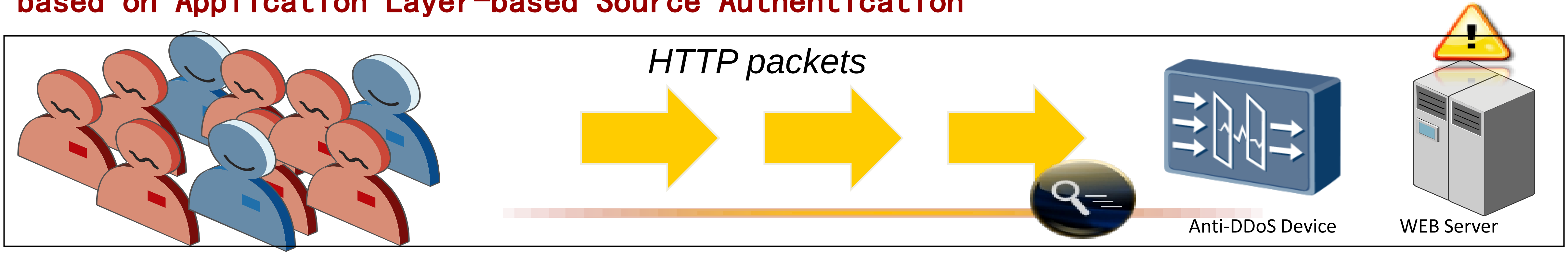
Attack destination

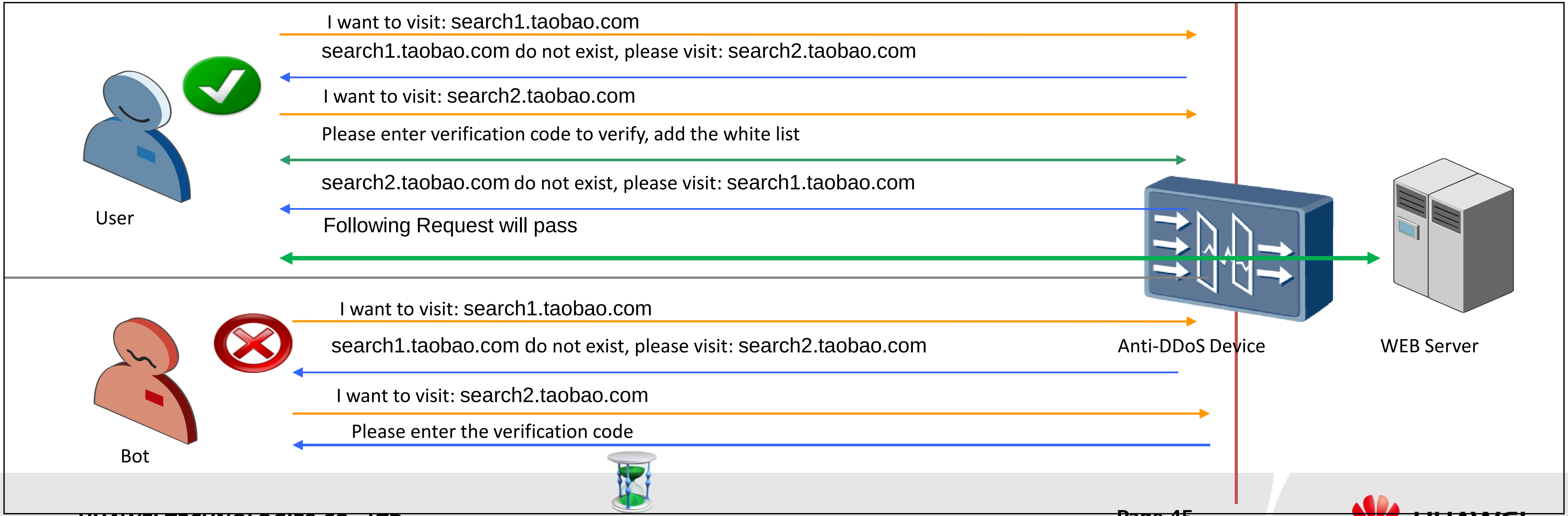
The target can’t response now.

Attack Character: This attack is a kind of http flood by botnet using a lot of open proxies. Sessions from single proxy are few to avoid detecting from security devices. The attack result is obvious when the attacked URI exhausts lots of CPU capability.

Defense Principle: Redirection check code is used to defend against CC attack. Attacks are launched by botnet. As a result, there is no response to authentication requests and access traffic fails to be transparently transmitted to the server. The cleaning device reports client_attacks log.

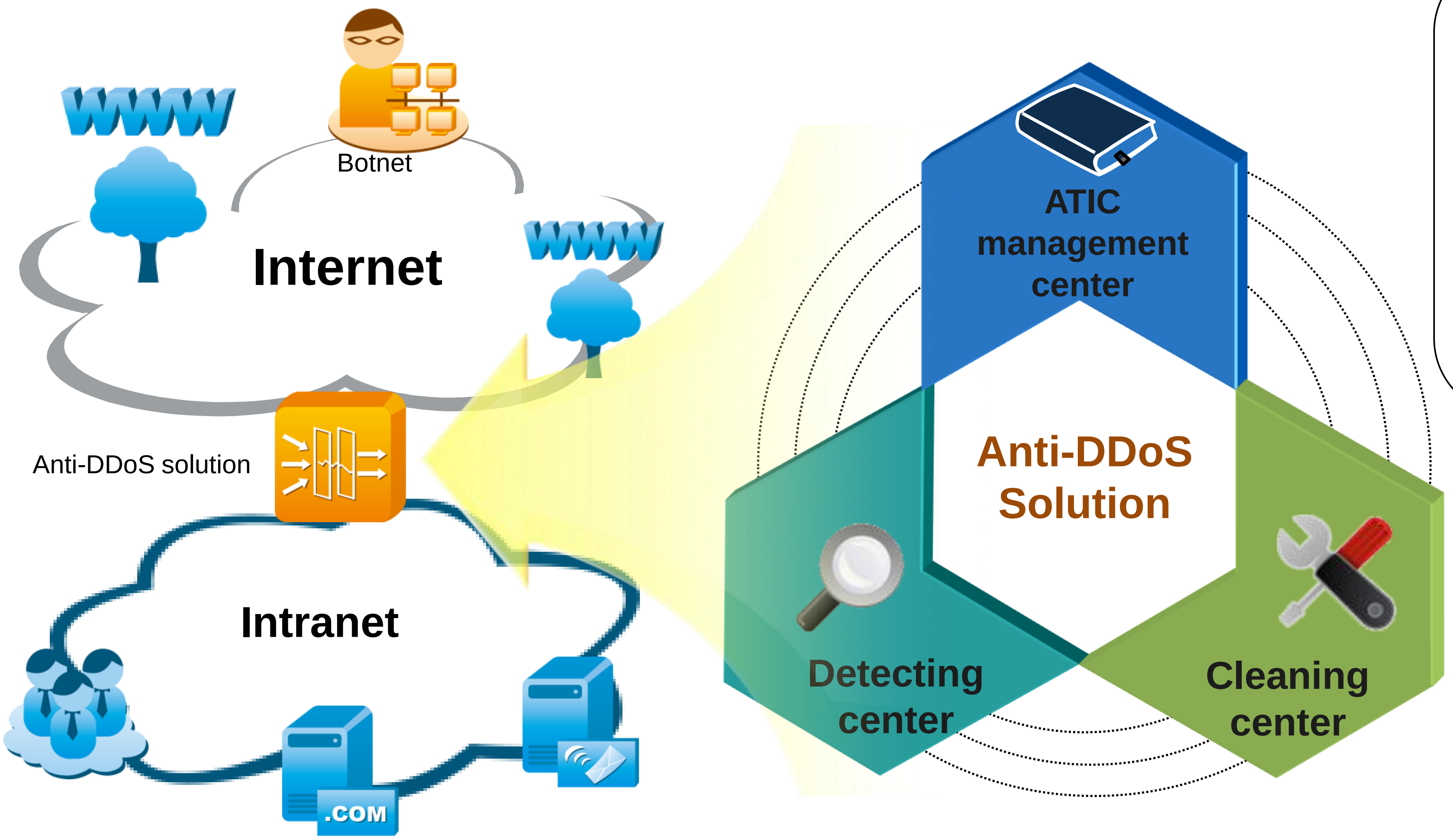
Defense against HTTP Flood based on Application Layer-based Source Authentication





Contents

Huawei Anti-DDoS Solution



Application scenario

Deployed at the egress of an IDC, enterprise network, or server network to prevent flood and application-layer attacks.

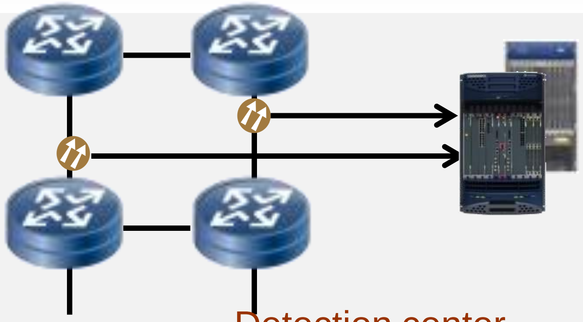
Solution objectives

Ensuring efficient bandwidth usage;
Ensuring service continuity;
Providing ease of management.

Huawei Anti-DDoS Solution

Detecting center | Cleaning center | ATIC mgmt. center

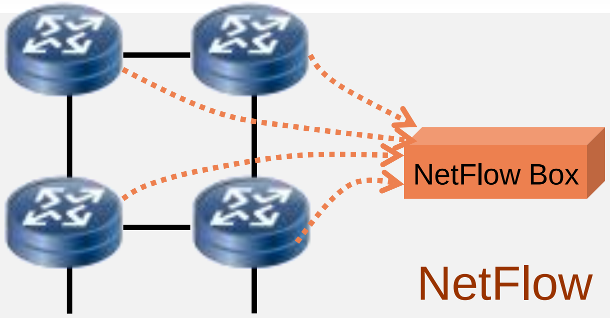
The detecting center implements the detecting policies delivered by the ATIC management center to identify abnormal traffic and sends the detecting results to the ATIC management center.



- Provides detection at fine-grained, near real-time scale
- Can detect application-layer attacks, but cannot detect routing information such as AS and next hop information
- Provides highly accurate detection, in-depth packet detection, signature matching, and session table establishment
- Centrally deployed, and difficult to scale
- Off-line deployment has no impact on network devices

Fine-grained real-time in-depth inspection

or



- Provides detection at medium-grained time scale and introduces noticeable delay
- Supports the collection and analysis of septet information, including routing information, but cannot detect application-layer attacks
- Provides low accurate detection based on sampling septet information
- Easy to deploy and scale
- Requires network devices to send NetFlow traffic to the analysis devices and has some impact on network devices

Basic and coarse-grained network-wide traffic detection

Huawei Anti-DDoS Solution

Detecting center | **Cleaning center** | ATIC mgmt. center

Cleaning center

The cleaning center receives instructions from the ATIC management center, delivers traffic diversion policies, and implement traffic cleaning. The cleaning center provides accurate protection through layered protection procedures to prevent malformed packet, DoS, and DDoS attacks with low latency.

Seven-layer filtering against attacks of all types

Static filtering
- Whitelist
- Blacklist

Malformed packet filtering
- LAND attack
- Fraggle attack
- Winnuke
- Ping of Death
- Tear Drop
- Invalid TCP flag attack
- Super large ICMP attack

Special control packet filtering
- IP Option
- ICMP redirect message
- ICMP unreachable message
- Tracert
- Packets with IP Source Routing option
- Packets with IP Timestamp option
- Packets with IP Record Route option

Source validity authentication
- TCP Fragment Flood
- SYN Flood
- SYN-ACK Flood
- HTTP Get Flood
- HTTP Post Flood
- HTTPS Flood
- DNS Query Flood
- DNS Reply Flood
- SIP Flood

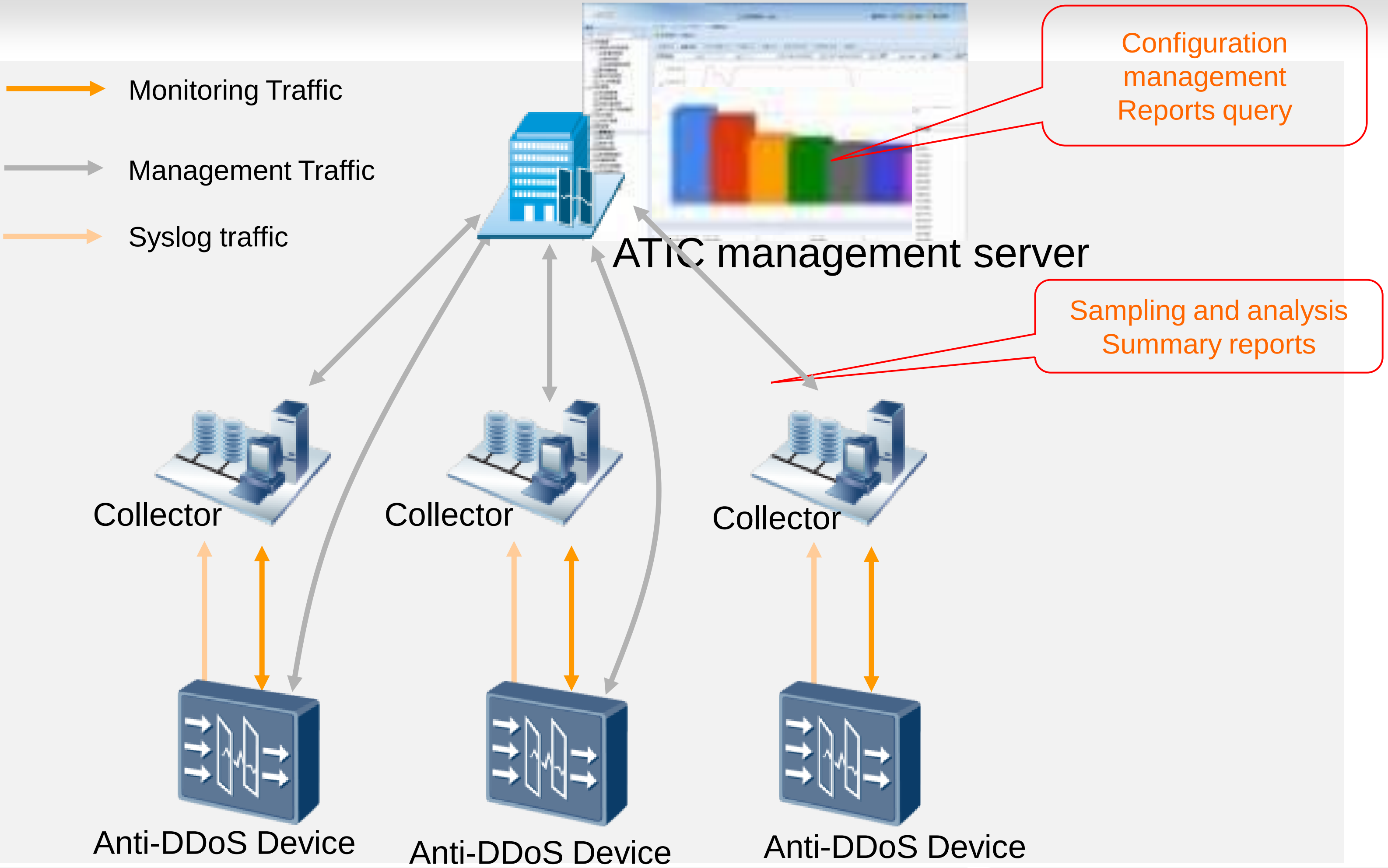
Session-based cleaning
- TCP Flood
- UDP Flood
- ICMP Flood
- Connection Flood

Signature recognition
- UDP Flood
- UDP Fragment Flood
- ICMP Flood
- CC
- HTTP Get Flood
- HTTP Post Flood

Traffic shaping
- Avoid congestion to the target

Huawei Anti-DDoS Solution

Detecting center | Cleaning center | **ATIC mgmt center**



ATIC management center

The ATIC management center is the brain of the whole solution. It provides customized detecting and cleaning policies, controls the detecting and cleaning devices, and generates attack reports and cleaning logs for query.

Layer operation mode—layer cleaning

Pipe-line level Anti-DDoS

Provider can deploy netflow detection+ E8000E-X cleaning in MAN or upper level , this can not only protect link-layer safe for provider but also give extra MSS

- Defense police is default configure and not related to application level;
- report function ；
- Charging mode：
  - A： charging on defense times, on demand cleaning mode；
  - B： charging on month, providing real-time defense；

A Mode

- Charging on cleaning times， providing on demand cleaning mode，three modes : manual cleaning、auto cleaning、interactive cleaning;
- Charging mode：XX$/IP/each cleaning or XX$/100Mbps/ IP/each cleaning
- Target user：SME（Small and medium enterprises）

B Mode

- Charge rated fee;
- Customized defense policy， providing auto cleaning;
- Charging mode： XX$/month/per IP，or XX$/ month/ 100Mbs;
- Target user： Key accounts,like IDC,NSP;

Currently, Turkey telecom, United Arab Emirates DU have been the customers of HUAWEI Anti-DDoS MSS solution

Shared-link layer Anti-DDoS

Provider deploy E8000E-X in Metro net using static traffic diversion

- Customized defense policy based on application，and provide detailed defense in application level;
- Shared cleaning device and cleaning bandwidth，in this situation, cleaning device share MAN access device;
- Report function;
- Charging mode： XX$/mode/100 Mbps， or XX$/ month/ 100Mbs ;
- Target user： SME（Small and medium enterprises, like NSP、IDC;

Owned link-layer Anti-DDoS

Provider deploy E1000E-D in customer's access point of metro net by using in-line or static traffic diversion mode，This can provide fined application level defense by customized defense policy;

- Providing fined application level defense by customized defense policy ;
- Owned cleaning device and cleaning bandwidth，detection and cleaning device can be deployed in Provider side of customer's network;
- Report function ;
- Charging mode： XX$/month ;
- Target user： Key accounts，result is that provider take care of the security issue for Key accounts，for example ,customer sold out their Anti-DDoS security to provider ,such as bank ;

Provides Up to 200 Gbit/s Performance

High performance | High availability | High detection rate | Rapid response

◆**Industry-leading architecture:** Built on the network processor (NP), multi-core CPU, and distributed architecture, breaks the performance bottleneck, and provides online capacity expansion capability.

◆**High performance:** Delivers a maximum of 160 Gbit/s processing speed per chassis, which is an industry-leading level and can cope with large scale attacks

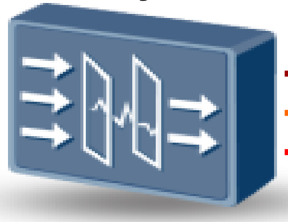
◆**High capacity:** Supports differentiated protection for a maximum of 2000 Zones; provides fine-grained protection for 10,000 IP AMS1500 resses and common protection for 1,000,000 IP AMS1500 resses

99.9999% Availability to Ensure Service Continuity

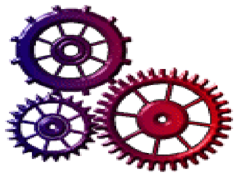
High performance | **High availability** | High detection rate | Rapid response

Delivers the industry's longest MTBF: 500,0000 hours

Delivers 500,000 hours of MTBF and 99.9999% availability with less than 1 minute of down time each year and less than 0.1 second failover time, ensuring service continuity



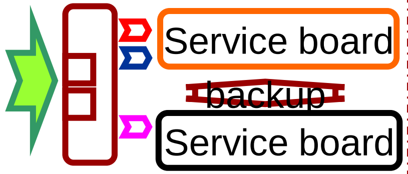
Dual-MPU multiple switching boards



- 1+1 main processing engines
- 3+1 switching boards

Delivers core-router level stability and availability

Load balancing between service boards



- Intelligent load balancing

Avoids the impact of single-board failure

Dual-system hot backup

- Multiple HA implementations
- Provides multiple paths

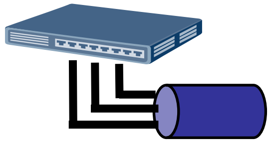
Accommodates to different HA implementations

Component redundancy

- Power redundancy
- Fan redundancy
- Hot-swappable parts

Ensures online insertion and removal of parts

Cross-board interface binding



- Evenly distributes traffic among links
- Seamlessly failover, with no impact on data forwarding

Improves link availability and increases total bandwidth

VRP platform

- Modules are independent of each other to avoid interference
- Manages 4 million devices on live networks

Provides stable and reliable software platform

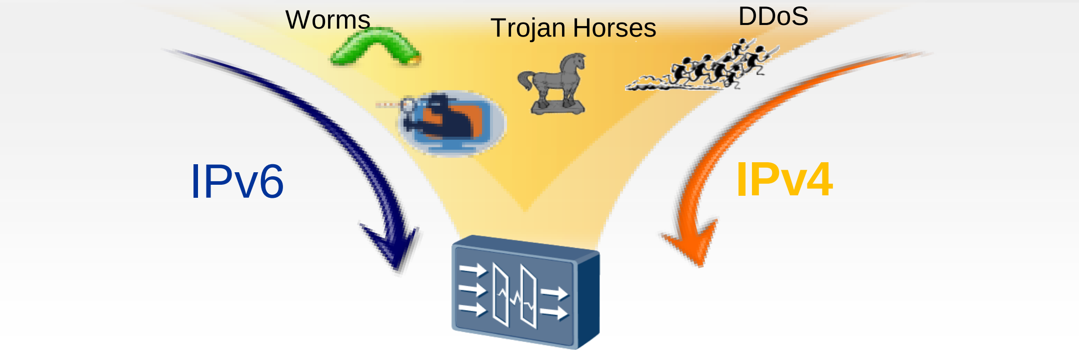
IPv6 Attack Defense to Secure IPv4-to-IPv6 Transition

High performance | High availability | High detection rate | Rapid response

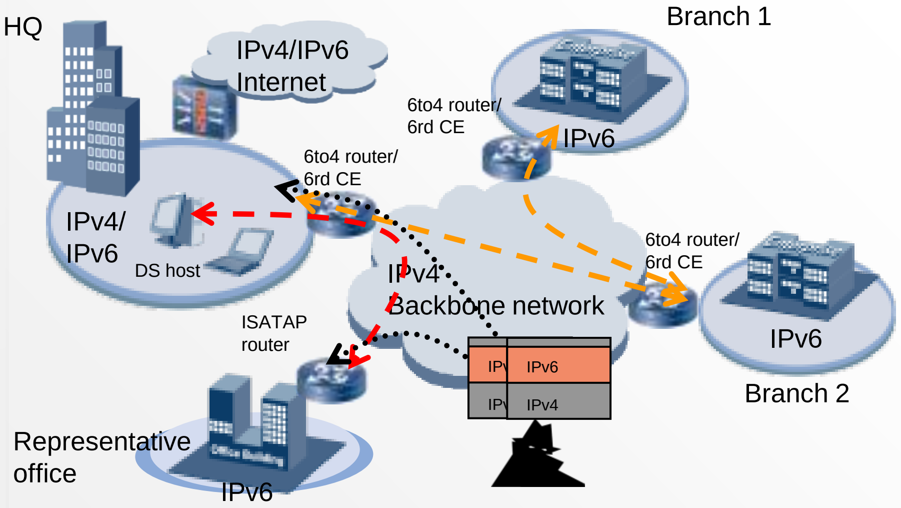
Full-scale IPv6 attack defense

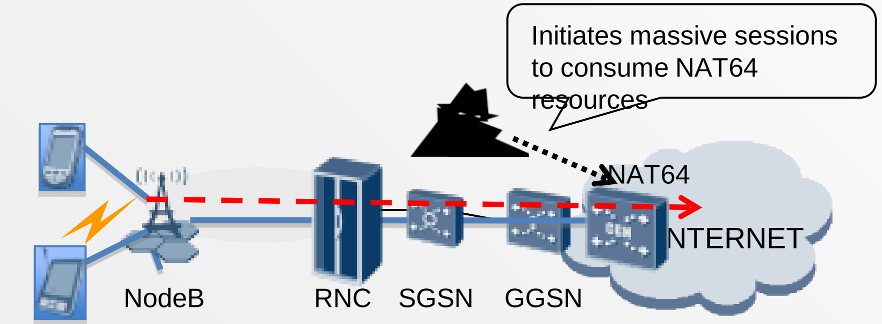
IPv6 attack defense

- IPv6/IPv4 dual stack, seven-layer defense structure
  Static IPv6 filtering
  Malformed IPv6 packet filtering
  Transport layer IPv6 source validity authentication
  Application-layer IPv6 source validity authentication
  Session-based IPv6 cleaning
  IPv6 behavior analysis
  IPv6 traffic shaping
- Defends against IPv4 and IPv6 attacks simultaneously



Threats in IPv4-to-IPv6 Transition Schemes





Detecting and Cleaning Within Seconds

High performance | High availability | High detection rate | Rapid response

	DPI technology	Conventional NetFlow technology
Detecting speed	Performs DPI packet by packet, **detects attacks within seconds**	Performs flow-based and interface-specific inspection; **detects attacks within minutes or tens of minutes**
Response speed	Leverages session and detection information synchronization; **responds to attacks within seconds**	**Diverts traffic minutes or tens of minutes after attacks**

Contents

Detection and cleaning

Suitable for refined defense on large networks

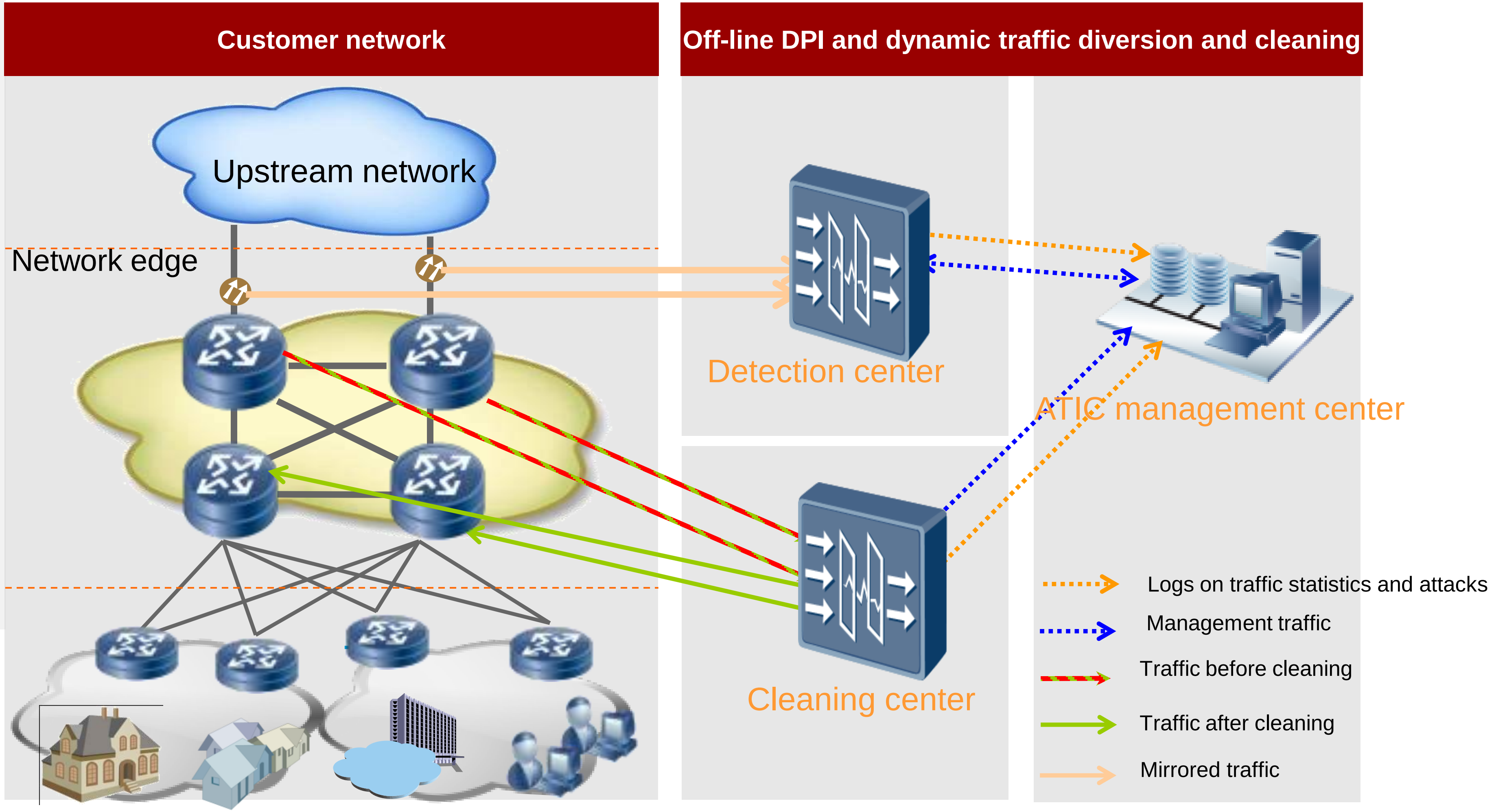
Detection and cleaning

In off-line DPI deployment, the DPI devices analyze the traffic of the entire network, automatically deliver traffic diversion policies to the core routing devices to divert the traffic for cleaning upon detecting abnormal traffic, and provide reports on attack events and cleaning results.

During deployment:

Detecting devices can be deployed outside of the cleaning devices to detect all traffic;

Detecting devices can be deployed inside of the cleaning devices to detect traffic in smaller scale to reduce costs.



Independent Cleaning

Suitable for refined defense on small and medium-sized networks

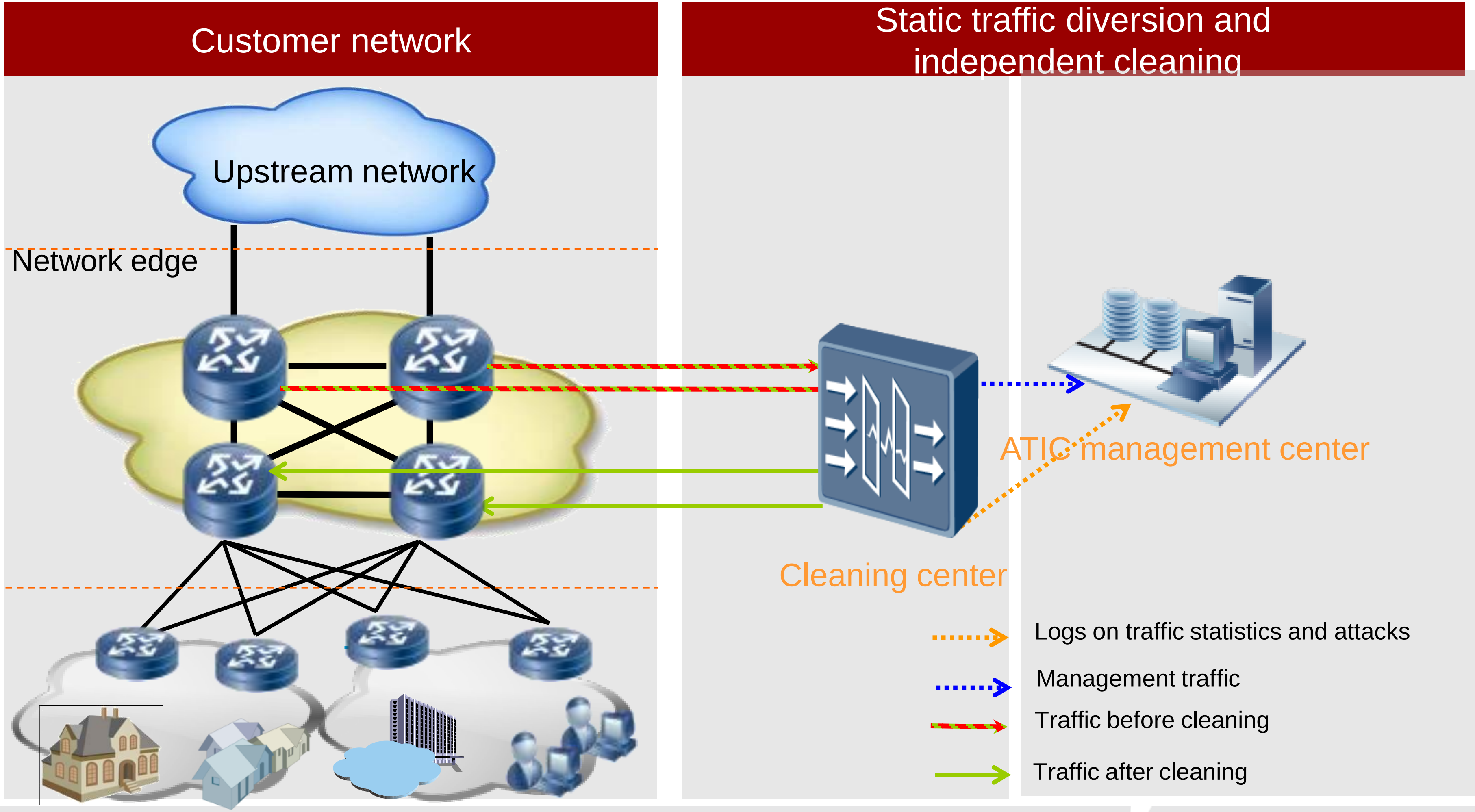
Independent cleaning

Detect specified traffic based on static rules and dynamically learn the normal traffic baseline to prevent abnormal traffic.

Independent cleaning supports the following two deployment modes:

1) In-line deployment: All traffic goes through the cleaning devices to be cleaned. In-line deployment inspects traffic in wider range, but requires high-performance hardware and is expensive.

2) Off-line deployment provides refined protection for specific customers. Off-line deployment is cheap to deploy, but inspects traffic in a smaller range.



Proportional Sampling and Cleaning

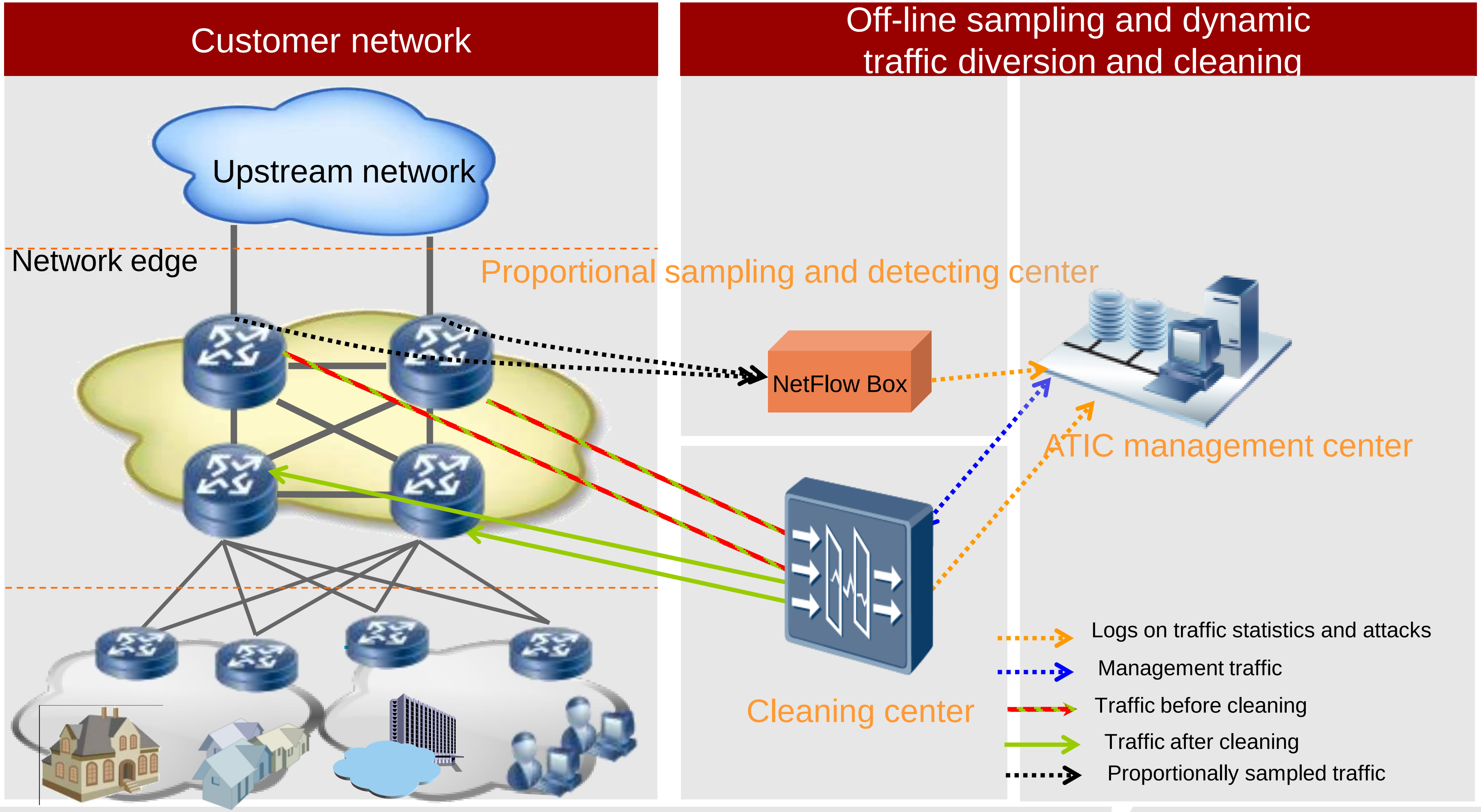
Suitable for network-wide traffic cleaning

Proportional sampling and cleaning

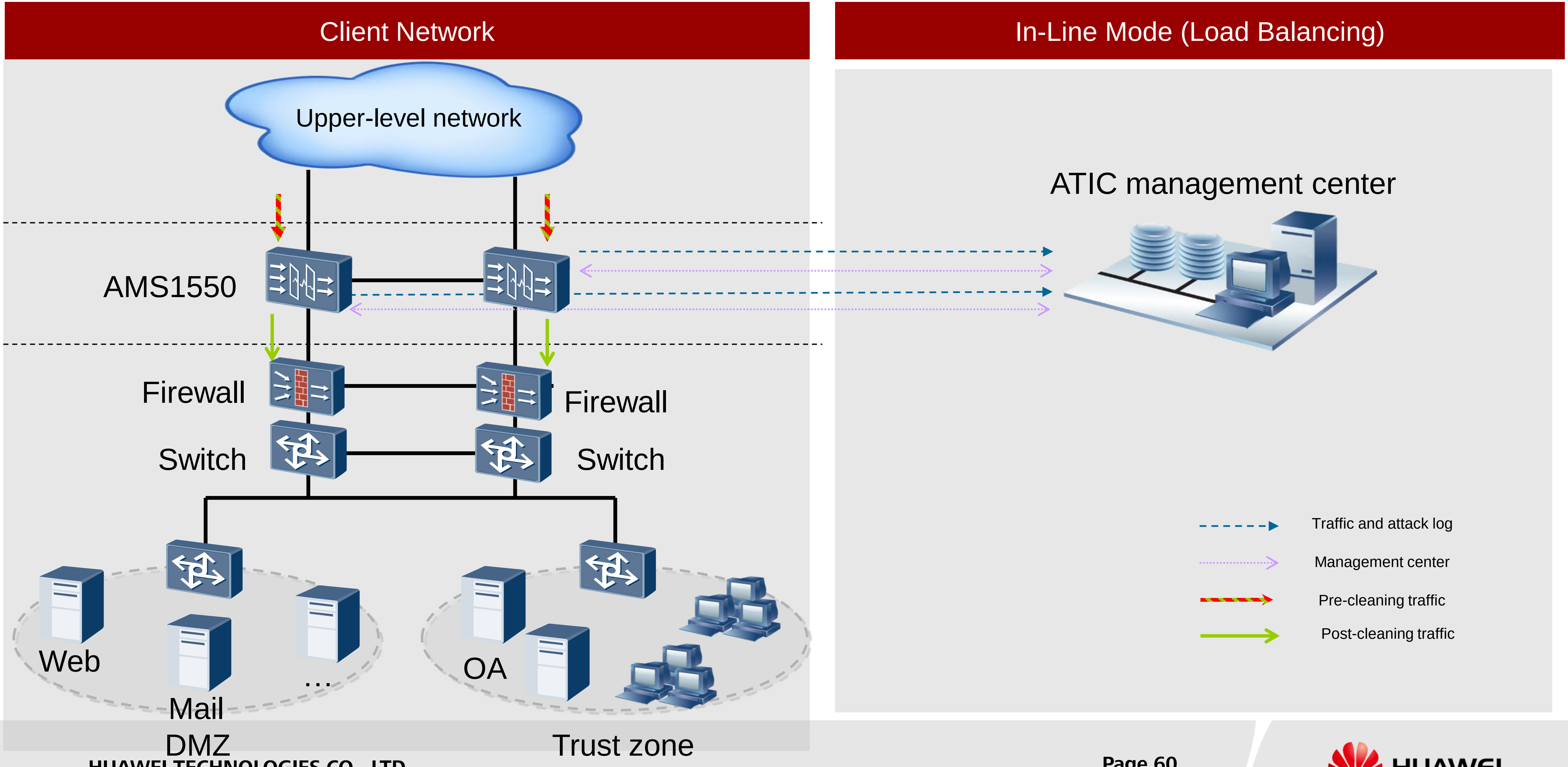
In off-line deployment, NetFlow devices sample traffic for analysis, automatically deliver traffic diversion policies to the core routing devices to divert traffic to the cleaning center for cleaning upon detecting abnormal traffic, and provide reports on attacks and cleaning results.

Pros: Low deployment cost

Cons: Slow response, low detection rate in application-layer attacks

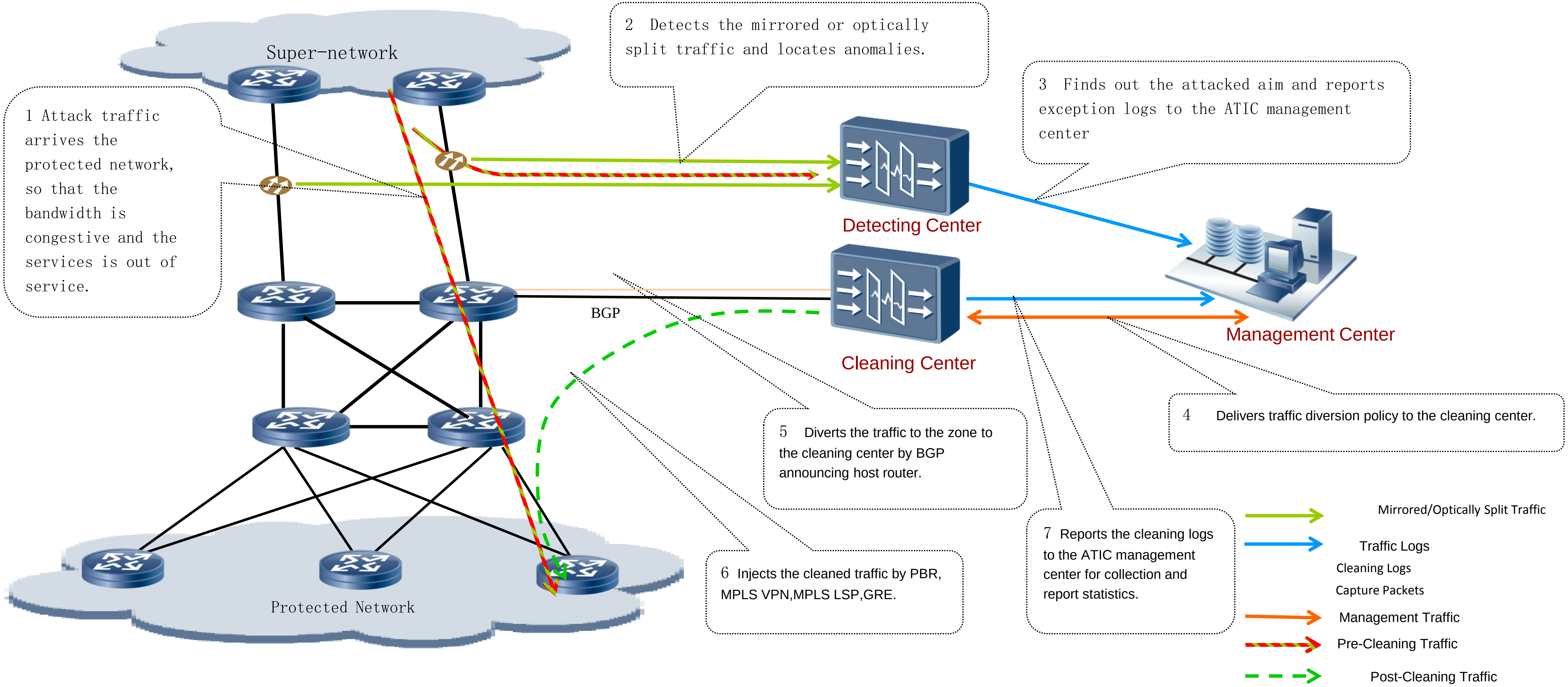


Load Balancing Cleaning Mode



Processing Flow of Anti-DDoS Solution

---Using Dynamic Traffic Diversion in Off-Line Mode as an Example



Flexible Deployments to Accommodate to Your Needs

Deployment Method

●Proportional sampling and cleaning

Network-wide traffic policing
Link congestion prevention
Customer channel cleaning

Pros and cons

Pros:
Cost-effective, suitable for backbone networks and large MANs to prevent flood attacks.

Cons:
Causes severe delay, requires the NetFlow sampling; cannot prevent application-layer attacks and light-traffic attacks.

●DPI and cleaning

Refined defense
Easy to operate

Pros and cons

Pros:
Effective to detect and prevent flood and application-layer attacks; capable of learning traffic model and delivering fine-grained detection and cleaning; rapid in response to attacks and causing small delay

Cons:
Expensive.

●Independent Cleaning

Refined defense
Low-cost deployment

Pros and cons

Pros:
Cheap to deploy; capable of detecting and preventing flood and application-layer attacks in fine-grained scale and learning traffic model; rapid in response to attacks and causing small delay.

Cons:
Static protection, suitable for only small networks.

Huawei Anti-DDoS Operation solution components

DDoS Detecting Center

Deep packet detection

<=5G

AMS1500

<=200G

AMS8000E-X

Detection

AMS1500-D

DDoS Cleanning Center

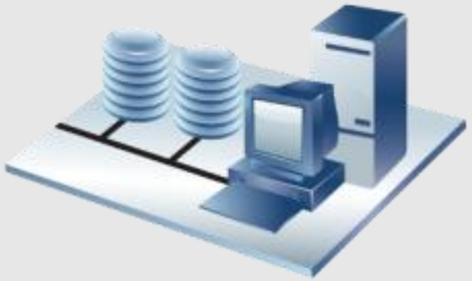
<=200G

AMS8000E-X

<=5G

AMS1500

Management Center



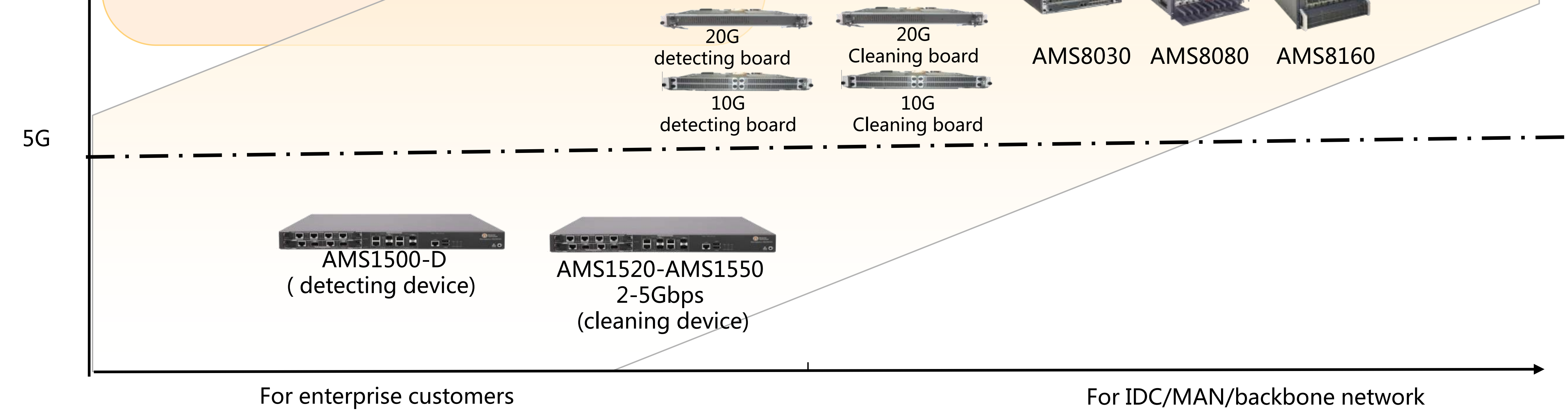
ATIC/VSM

Management Center

Including servers and software

Huawei Anti-DDoS Product

- **High performance:** Provides a maximum of 200 Gbit/s processing speed per chassis to cope with large scale attacks
- **High availability:** Delivers 500,000 hours of MTBFand 99.9999% reliability
- **High detection rate:** Provides application-layer attacks and IPv6 attacks
- **Rapid response:** Capable of detecting and cleaning within seconds to ensure service continuity



Zapraszamy do Huawei Demo Truck

ORAZ NA PREZENTACJE:

- Poniedziałek 14:55 – 16:20

  Protokół IETF TRILL – Donald E. Eastlake 3rd
- Wtorek 12:30 – 13:15

  DataCenter Interconnect – Sam Aldrin
- Wtorek 14:15 – 14:45

  Budowa przełączników modularnych – Piotr Głaska