The advantages and benefits of Flowviewer

Technical principle

The Flowviewer used an optimized system and the network card with auto-bypass feature. The optimized system contained the abnormal detection feature which with our anomalous traffic detecting algorithm and the driver that can collect the packets rapidly. It can collect and deal with the packets rapidly via multi-thread processing. With the concept of multicore processing, it would increase the processing speed. The Flowviewer can block the abnormal traffic on itself or used the ACL (Access Control List) commands to block the abnormal traffic. Now, the Flowviewer can support the core-switch of Alcatel, Cisco, Foundtry and Extreme. When IPS (Intrusion Prevention System) equipment faced the resource-draining attack or bandwidth-consuming attack, it might have the hardware failure problem. Due to the hardware and software were integrated well, the Flowviewer would not have this problem.

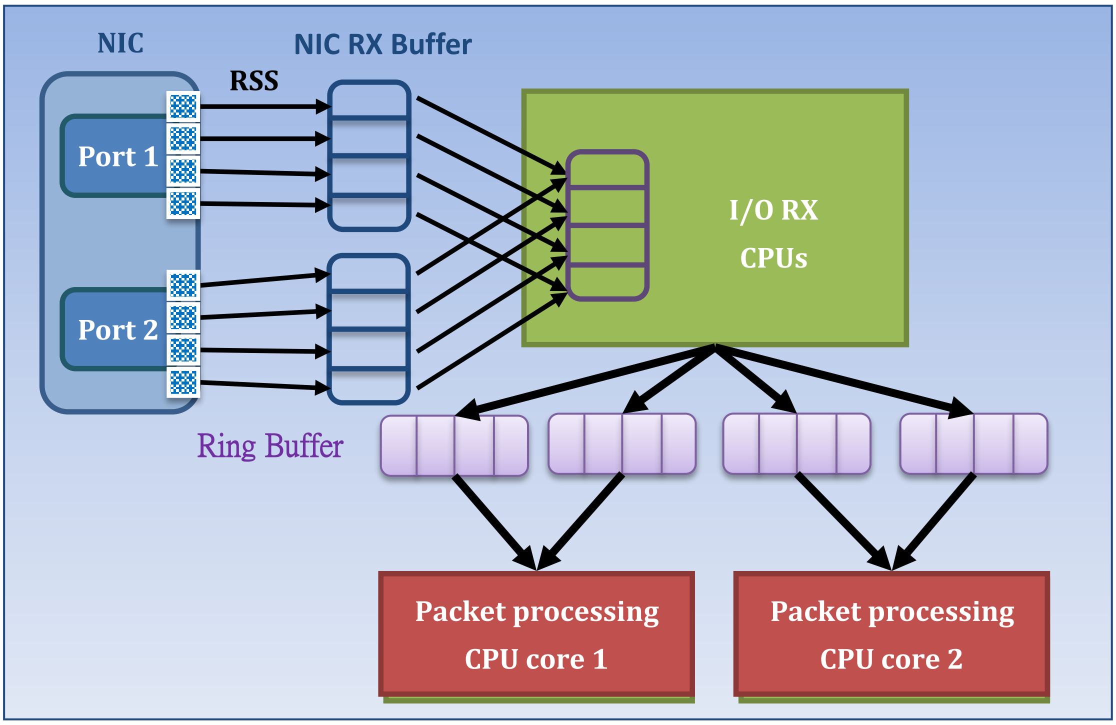


Figure 1

Using multi-cure and multi-thread to improve the effect of packet processing

Compared the technology of the Flowviewer with IPS (Intrusion Prevention System)

The IPS equipment is using the technology of deep packet inspection to filter or compare the packet that through itself with the signature. It also uses the function of threshold to distinguish cyber-attack from the traffic. This technology must contain the principle of session. It also uses the function of threshold to distinguish cyber-attack from the traffic. It needs to calculate how many packets and session will through itself. The number of threshold is setting by the user. That technology also contains the principle of session.

This technology of using session has a weakness. When it faces the DDoS attack, the amount of sessions will cause the performance of CPU goes down. Finally, it will cause the system crashed. Although the company of IPS claimed that they used ASIC chips to prevent this difficult situation. ASIC is just a general term for a microchip. CPUs are technically ASICs, but much simpler devices can be implemented on an ASIC too. You can use the IPS products and software to simulate the DDoS attack if you don't believe it. That DDoS attack would generate a lot of flows/packets to attack the device. You can observe the proportion of the rate of CPU-usage to the number of flow/packet. The X-axis is the number of flow/packet and the y-axis is the usage of CPU-usage. We used the data to plot a graph and found the usage of CPU-usage is linear relation with the number of flow/packet. If we used the more data to plot the graph, the result is approximately linear dependency. On the base of the two degrees of space, we can use the time as the z-axis to find out when will the device crash.

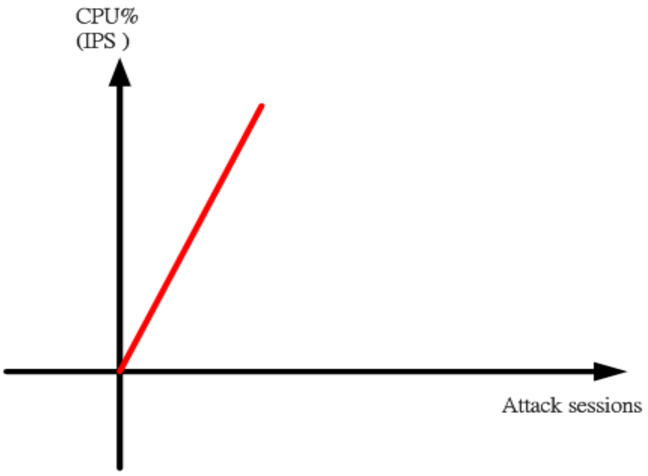


Figure 2

The schematic diagram of the number of session and CPU utilization

Why can the Flowviewer use the architecture of non-session? The Flowviewer can receive the Netflow or sFlow with sampling rate 1:1 so that it can use the architecture of non-session. The Flowviewer can find out the anomalous traffic by analyzing the data of the source IP address, the destination IP address, the time duration, the transport protocol and port number, the number of session/flow, the number of packet and traffic. Just like the theory of Big Data, the Flowviewer can analyze those huge data to find out the regularity and then determine it is attack or not. It can accurately detect the cyber-attack and intrusion by the full sampling-and-analysis processing. You can find some relative papers from IEEE journals. On the basis of the above reasons, we will suggest our customers to redirect the Netflow with sample rate 1:1 to the Flowviewer. The Flowviewer can use this data to find out the malicious traffic. The full sampling-and-analysis is the best solution. However, not every device can receive the huge data in the real world. That is another problem that you should consider. This is the reason why this technology cannot be applied to the products on the market. The Flowviewer used the mathematical formula and algorithm that developed by the Curelan Technology Co., Ltd. to analyze data. By our experience, the product of brand A can only receive the Netflow with sample rate 1:1000. In other words, it would choose 1000 packets from one million packets to be analyzed. How can this device accurately detect the attack/intrusion? That means the cyber security companies agree to this idea, but they cannot find the solution to this bottleneck of that technology.

The Flowviewer has a feature that can restrict the unauthorized accessing specific domains. All you have to do is entering the domain name and then save it. This feature just needs to analyze one packet to know the domain name. Unlike the deep packet inspection technology, it is possible to use the non-session technology.

The IPS equipment that used sessions to block the abnormal traffic would use deep packet inspection technology to analyze the packets that through it. That means the hardware failure problem would happen when it faced the huge packets. The hardware performance would be consumed by these packets. As the result of this issue, it would cause the hardware failure. The Flowviewer uses the non-session technology to prevent that problem.

Real case

A hacking group declared a DDoS attack which hit the campus network of a private university in New Taipei, Taiwan. The TV programs in Taiwan and the network news reported this event at the time. The hackers announced that they would launch another attack for another day. This university is one of our clients. The network administrator complained to us about the campus network paralysis. He could not understand why the DDoS attack would be succeeded. There is an edge router at the boundary of their network. The IPS device is downstream of the edge router; the IPS device is upstream of the Flowviewer; the core switch is downstream of the Flowviewer. Because the Flowviewer could receive the Netflow which was transferred from the core switch, that meant the core switch was not failed when the campus network was paralyzed. You can see the internal communication IP data had been recorded in the Flowviewer but you cannot find any IP data from external network to internal network or data from internal network to external network. That means the Flowviewer was not failed at that time. From the above mentioned, we can know the sticking point of network paralysis is the router or the IPS device. We would rather believe that the router is not so vulnerable. We advised using another Flowviewer to replace the IPS device. The Flowviewer had succeeded in blocking the attacking IP address at the second time. If the hackers succeeded in attacking the university, there might be another cyber-attack. The network administrator did not put the IPS device online again. You can use the huge number of sessions to attack the IPS devices. You might get a graphic like figure 2.

The IPS (Intrusion Prevention System) / IDS (Intrusion Detection System) devices are using the technology of signature to filter or compare the packet that through itself with the signature. You need to upgrade the signatures so that the device can make the most of it. This kind of device is not optimal solution when it faces the unknown attack or the zero-day attack because the hackers will change the signature of the attack every two or three days. **In fact, the hackers will use the hacking tools to intrude the machines. It will guess the password of the internal devices. Once it succeeded in intruding, it will implant the Trojan horse on the device and use specific ports to do the intrusion. Some of the services will use the fixed port number so the hackers can guess the password via these port services. Some of the port services are used to do the intrusions because they are easier than others. The Trojan horse program will spread itself and then make the botnet grow bigger than**

before. The IPS devices use the collected signatures to compare and the packet and filter the malicious traffic. Even the user can block the outcoming attacks/intrusions, the hackers will try to steal the military/financial confidential information from inside. The most famous case is the facebook data breach. The security experts in America did not talk about the insider intrusion. They only talk about how hackers found the vulnerabilities of software. They made a conclusion about that event: It was caused by one of the employees who downloaded an APP software and then made the hacker had a change to reach the internal network. Did the user data store in the employee’s computer? Of course NOT! The hacker must use the latest Trojan horse to intrude the network and escape the detection of IPS. The equipment of IPS did not have the patterns/signatures so it is easy to escape from its detection and steal the user data. If it is not true, the Equifax data breach in 2017 will not happen again. I guess that the Sanrio, the Japanese owner of the Hello Kitty brand, was hacked and private information on 3.3 million users was exposed by the same method. You will use the similar method to steal the confidential information if you know it will be succeed. Besides, it is not difficult to hacker to create a new Trojan horse program. The corporate spy/ military spy will use the hacking program with the latest signature to do the intrusions. The device that used signature to filter or compare the packet can do nothing about this kind of attacks/intrusions. Using the technology of signature to filter or compare the packet is not bad but when it faces the amount of packets to attack or relay attack, it will cause the hardware performance goes down. We had mentioned it above. Some of IPS/IDS devices use threshold function to distinguish the cyber-attack. The low threshold value will cause the false positive problem, so the network administrator will not set a low threshold value. As the result, it gives the hackers a chance to launch the attack.

On the other hand, most of IPS/IDS devices focus on the attacks and intrusions from the external network to the internal network or from the internal network to the external network. They pay little attention to the insider intrusions or attacks. The financial and military network usually used closed network to protect themselves. The network administrator ignored the the seriousness and threatening of insider intrusion because the network had no external connectivity. When the Flowviewer analyzed the traffic from the Netflow, the insider traffic was included. Therefore, the Flowviewer can use the unique feature: inner intrusion to find out the insider intrusion.

Flowviewer used the behavior of packets to distinguish the cyber-attack and intrusion

We also created the relative equations to distinguish hacking intrusion and attack from the traffic. With the practical applications, we will modify the equations until the unit does not get the false positive results.

$$S : f(T_n, P_{src\,n}, P_{dst\,n}) = 1$$

$$\because T_n \in \mathrm{R}$$

$$\Delta T_n = T_{n+1} - T_n,\ \Delta T_n > 0$$

$$P_{src\,n} \in \{p \mid 1024 \le p \le 65535, p \in \mathrm{N}\}$$

$$P_{dst\,n} \in \{p \mid 1 \le p \le 65535, p \in \mathrm{N}\}$$

$$(P_{src}n, P_{dst}n) \neq (P_{src}\,n+1, P_{dst}n+1)$$

$$\therefore \sum_n f(T_n, P_{src}n, P_{dst}n) = Sessions$$

S: *session*
$P_{src\,n}$: source port number
$P_{dst\,n}$: destination port number
T_n: some time

Figure 3
The Flowviewer used mathematical formula to distinguish the cyber-attack and intrusions

We have a simple explanation of the above equation. You can watch it on YouTube: https://www.youtube.com/watch?v=yX_wp2oedYM

There is a video about" Simulate hacker attack_ Top 6 ways of hack attacks and how to protect". https://www.youtube.com/watch?v=vKweWU82okI

Real case

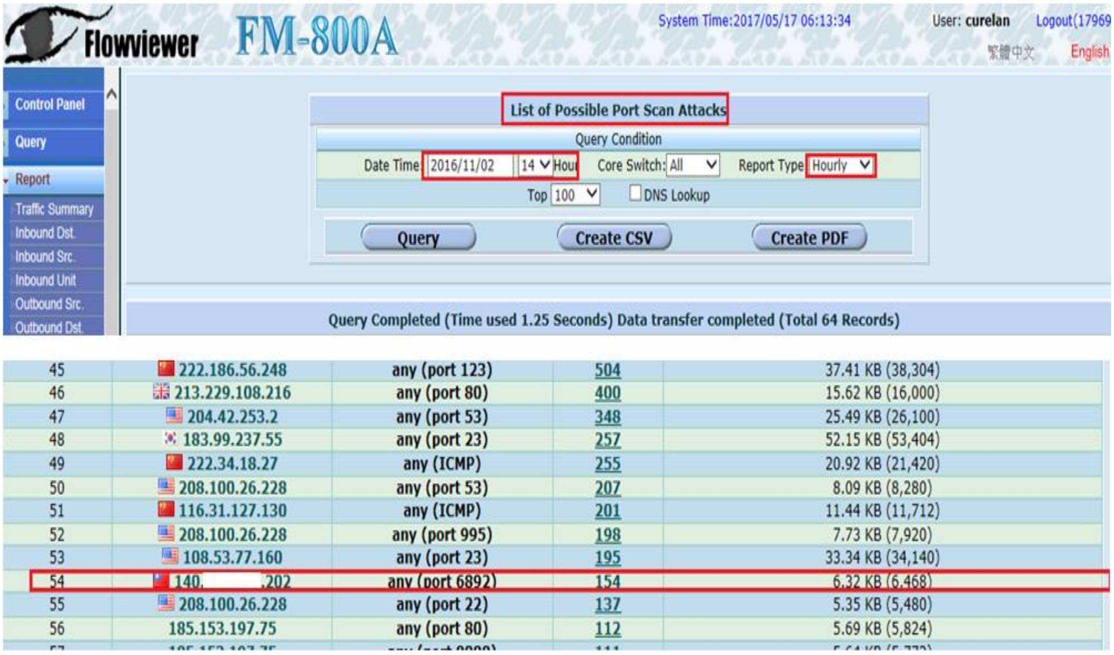
Case 1：WannaCry ransomware attack

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WsnnaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operation system. It used the exploit of Windows' SMB protocol to spread itself. It can gain the access, and automatically spread itself via port 445 or port 139. Beside update the latest released patches, it was suggested that using the firewall to close the port 445. However, closing the port 445 may influence other normal services or other executed problems. After we observed some of Flowviewer, we found the number of intrusion/attack via port 445 has risen significantly. This can prove that the Flowviewer has the ability to detect and stop the attack spreading.

A Unit		B Unit	
Date	The number of attack / per day	Date	The number of attack / per day
2017/5/1	6	2017/5/1	69
2017/5/2	14	2017/5/2	75
2017/5/3	19	2017/5/3	82
2017/5/4	24	2017/5/4	80
2017/5/5	29	2017/5/5	84
2017/5/6	25	2017/5/6	118
2017/5/7	20	2017/5/7	60
2017/5/8	15	2017/5/8	85
2017/5/9	18	2017/5/9	61
2017/5/10	18	2017/5/10	83
2017/5/11	18	2017/5/11	75
2017/5/12	**309**	2017/5/12	**328**
2017/5/13	286	2017/5/13	278
2017/5/14	94	2017/5/14	140
The average number of attack IP address via 445 before May 12 ：19 *The number of attack IP address via 445 on May 12* ：309		*The average number of attack IP address via 445 before May 12* ：80 *The number of attack IP address via 445 on May 12* ：328	

Table 1 the number of intrusion IP addresses via 445 port in A unit and B unit from May 1 to May 14.

Even closed the port 445, the ransomware like WannaCry will use other ports to do the intrusion. Example: The Flowviewer detected the intrusion in a private university in Taiwan on November 2 2016. The intrusion was launched by the infected host from inside. It did the intrusion on a large-scale via port 6892. As figure 4 and 5 shown, the Flowviewer detected that intrusion. From this experience, we can know that it is ineffective in stopping the intrusions and attacks by controlling the specific port number.



System Time:2017/05/17 06:13:34 User: curelan Logout(17969

List of Possible Port Scan Attacks

Query Condition

Date Time 2016/11/02 14 Hour Core Switch: All Report Type Hourly

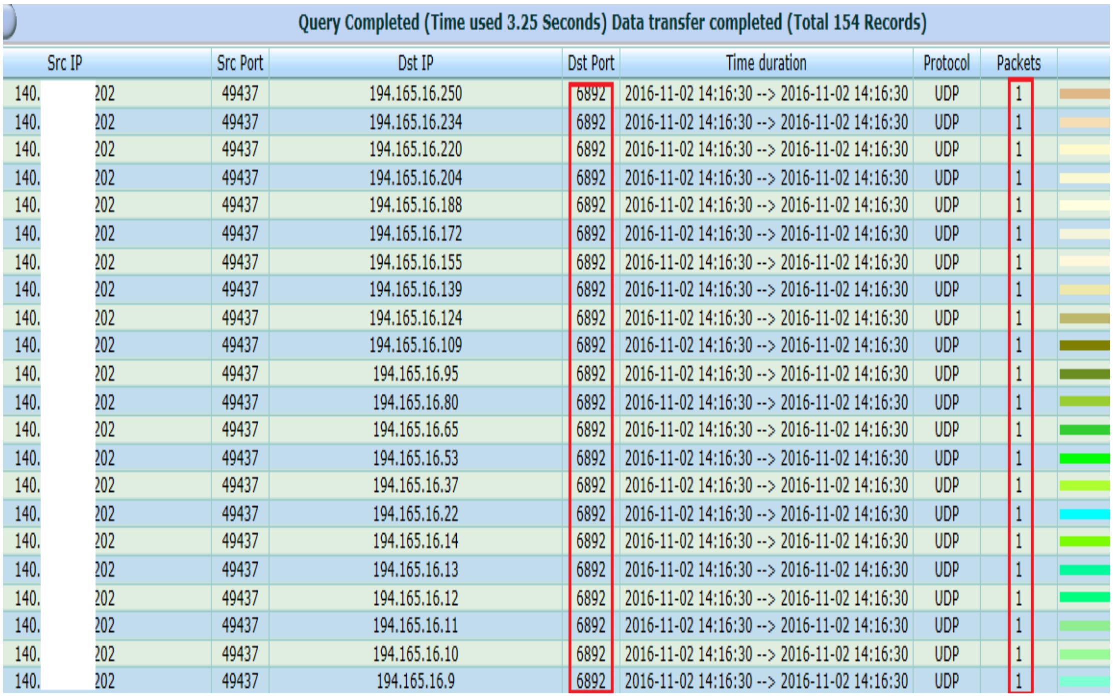
Top 100 □DNS Lookup

Query Completed (Time used 1.25 Seconds) Data transfer completed (Total 64 Records)

45	222.186.56.248	any (port 123)	504	37.41 KB (38,304)
46	213.229.108.216	any (port 80)	400	15.62 KB (16,000)
47	204.42.253.2	any (port 53)	348	25.49 KB (26,100)
48	183.99.237.55	any (port 23)	257	52.15 KB (53,404)
49	222.34.18.27	any (ICMP)	255	20.92 KB (21,420)
50	208.100.26.228	any (port 53)	207	8.09 KB (8,280)
51	116.31.127.130	any (ICMP)	201	11.44 KB (11,712)
52	208.100.26.228	any (port 995)	198	7.73 KB (7,920)
53	108.53.77.160	any (port 23)	195	33.34 KB (34,140)
54	140.[redacted].202	any (port 6892)	154	6.32 KB (6,468)
55	208.100.26.228	any (port 22)	137	5.35 KB (5,480)
56	185.153.197.75	any (port 80)	112	5.69 KB (5,824)

Figure 4

The Flowviewer detected the infected host in the inside



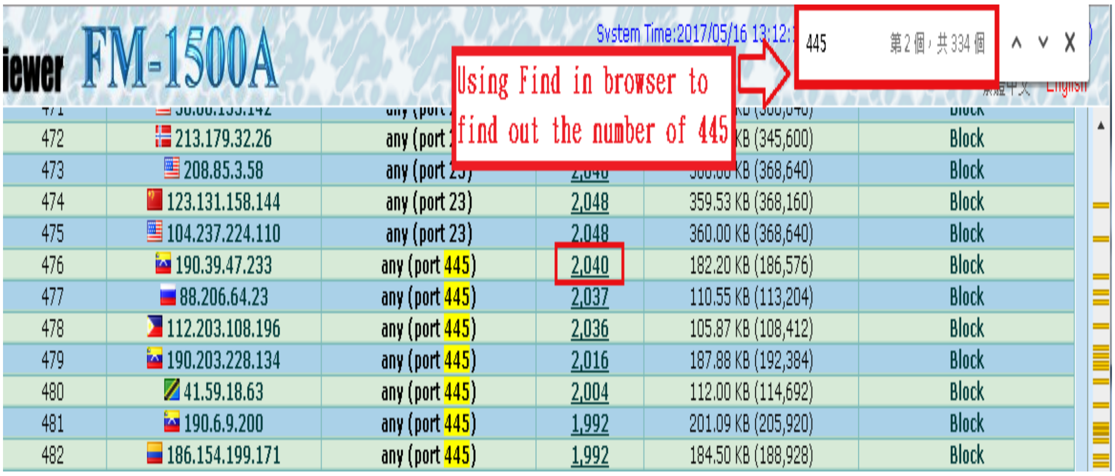
Query Completed (Time used 3.25 Seconds) Data transfer completed (Total 154 Records)

Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets
140.[redacted]202	49437	194.165.16.250	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.234	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.220	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.204	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.188	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.172	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.155	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.139	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.124	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.109	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.95	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.80	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.65	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.53	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.37	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.22	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.14	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.13	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.12	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.11	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.10	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1
140.[redacted]202	49437	194.165.16.9	6892	2016-11-02 14:16:30 --> 2016-11-02 14:16:30	UDP	1

Figure 5

The detailed report of specific IP address

The Flowviewer has the ability to detect and block the intrusions and attacks. In addition, it can provide the relative report. The figure 6 and 7 showed the detailed report of port scan for a specific IP address (190.39.47.233).



iewer FM-1500A

System Time:2017/05/16 13:12:

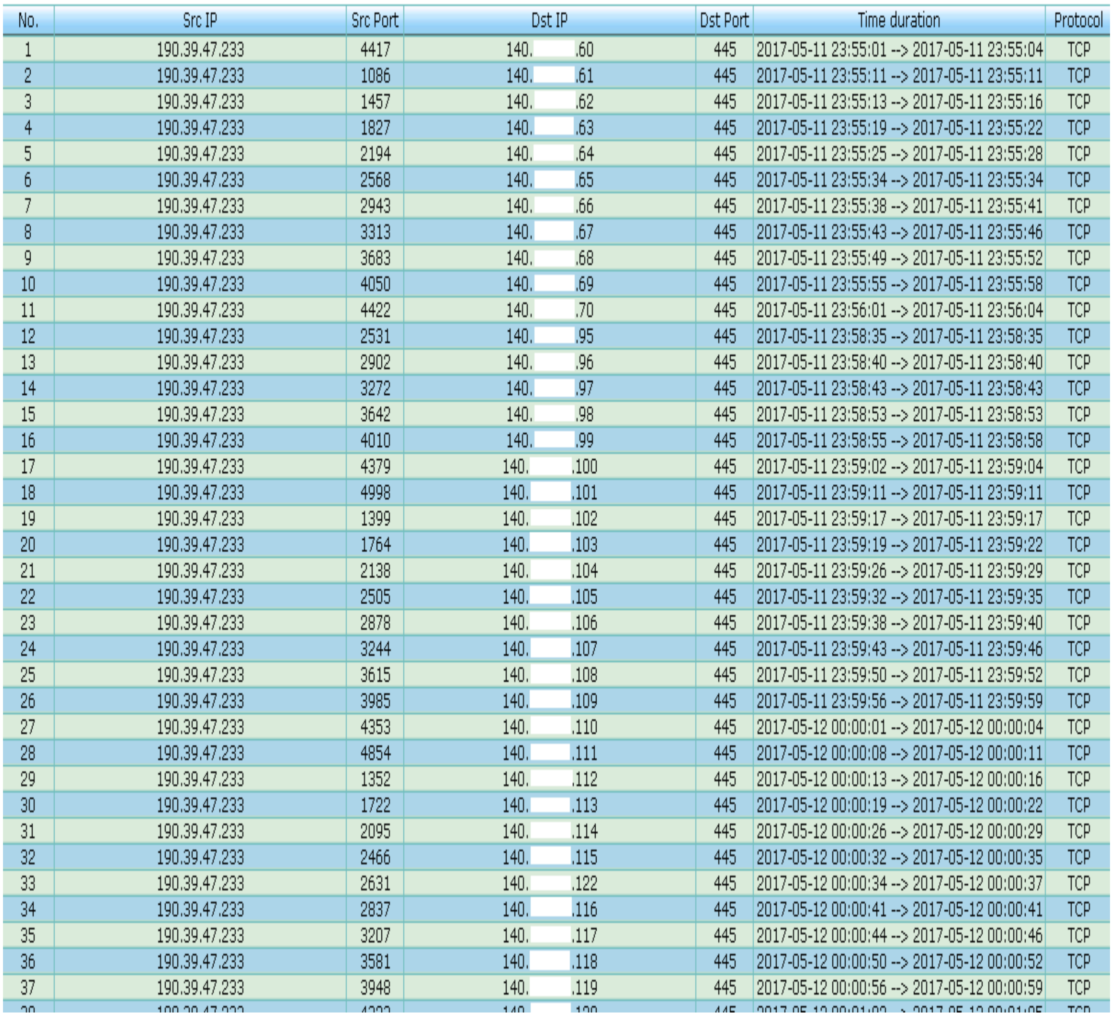
445 第2個，共334個

Using Find in browser to find out the number of 445

471	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
472	213.179.32.26	any (port [illegible]	[illegible]	KB (345,600)	Block
473	208.85.3.58	any (port [illegible]	[illegible]	[illegible] KB (368,640)	Block
474	123.131.158.144	any (port 23)	2,048	359.53 KB (368,160)	Block
475	104.237.224.110	any (port 23)	2,048	360.00 KB (368,640)	Block
476	190.39.47.233	any (port 445)	2,040	182.20 KB (186,576)	Block
477	88.206.64.23	any (port 445)	2,037	110.55 KB (113,204)	Block
478	112.203.108.196	any (port 445)	2,036	105.87 KB (108,412)	Block
479	190.203.228.134	any (port 445)	2,016	187.88 KB (192,384)	Block
480	41.59.18.63	any (port 445)	2,004	112.00 KB (114,692)	Block
481	190.6.9.200	any (port 445)	1,992	201.09 KB (205,920)	Block
482	186.154.199.171	any (port 445)	1,992	184.50 KB (188,928)	Block

Figure 6

The portscan report on the 12 May 2018



No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol
1	190.39.47.233	4417	140.[redacted].60	445	2017-05-11 23:55:01 --> 2017-05-11 23:55:04	TCP
2	190.39.47.233	1086	140.[redacted].61	445	2017-05-11 23:55:11 --> 2017-05-11 23:55:11	TCP
3	190.39.47.233	1457	140.[redacted].62	445	2017-05-11 23:55:13 --> 2017-05-11 23:55:16	TCP
4	190.39.47.233	1827	140.[redacted].63	445	2017-05-11 23:55:19 --> 2017-05-11 23:55:22	TCP
5	190.39.47.233	2194	140.[redacted].64	445	2017-05-11 23:55:25 --> 2017-05-11 23:55:28	TCP
6	190.39.47.233	2568	140.[redacted].65	445	2017-05-11 23:55:34 --> 2017-05-11 23:55:34	TCP
7	190.39.47.233	2943	140.[redacted].66	445	2017-05-11 23:55:38 --> 2017-05-11 23:55:41	TCP
8	190.39.47.233	3313	140.[redacted].67	445	2017-05-11 23:55:43 --> 2017-05-11 23:55:46	TCP
9	190.39.47.233	3683	140.[redacted].68	445	2017-05-11 23:55:49 --> 2017-05-11 23:55:52	TCP
10	190.39.47.233	4050	140.[redacted].69	445	2017-05-11 23:55:55 --> 2017-05-11 23:55:58	TCP
11	190.39.47.233	4422	140.[redacted].70	445	2017-05-11 23:56:01 --> 2017-05-11 23:56:04	TCP
12	190.39.47.233	2531	140.[redacted].95	445	2017-05-11 23:58:35 --> 2017-05-11 23:58:35	TCP
13	190.39.47.233	2902	140.[redacted].96	445	2017-05-11 23:58:40 --> 2017-05-11 23:58:40	TCP
14	190.39.47.233	3272	140.[redacted].97	445	2017-05-11 23:58:43 --> 2017-05-11 23:58:43	TCP
15	190.39.47.233	3642	140.[redacted].98	445	2017-05-11 23:58:53 --> 2017-05-11 23:58:53	TCP
16	190.39.47.233	4010	140.[redacted].99	445	2017-05-11 23:58:55 --> 2017-05-11 23:58:58	TCP
17	190.39.47.233	4379	140.[redacted].100	445	2017-05-11 23:59:02 --> 2017-05-11 23:59:04	TCP
18	190.39.47.233	4998	140.[redacted].101	445	2017-05-11 23:59:11 --> 2017-05-11 23:59:11	TCP
19	190.39.47.233	1399	140.[redacted].102	445	2017-05-11 23:59:17 --> 2017-05-11 23:59:17	TCP
20	190.39.47.233	1764	140.[redacted].103	445	2017-05-11 23:59:19 --> 2017-05-11 23:59:22	TCP
21	190.39.47.233	2138	140.[redacted].104	445	2017-05-11 23:59:26 --> 2017-05-11 23:59:29	TCP
22	190.39.47.233	2505	140.[redacted].105	445	2017-05-11 23:59:32 --> 2017-05-11 23:59:35	TCP
23	190.39.47.233	2878	140.[redacted].106	445	2017-05-11 23:59:38 --> 2017-05-11 23:59:40	TCP
24	190.39.47.233	3244	140.[redacted].107	445	2017-05-11 23:59:43 --> 2017-05-11 23:59:46	TCP
25	190.39.47.233	3615	140.[redacted].108	445	2017-05-11 23:59:50 --> 2017-05-11 23:59:52	TCP
26	190.39.47.233	3985	140.[redacted].109	445	2017-05-11 23:59:56 --> 2017-05-11 23:59:59	TCP
27	190.39.47.233	4353	140.[redacted].110	445	2017-05-12 00:00:01 --> 2017-05-12 00:00:04	TCP
28	190.39.47.233	4854	140.[redacted].111	445	2017-05-12 00:00:08 --> 2017-05-12 00:00:11	TCP
29	190.39.47.233	1352	140.[redacted].112	445	2017-05-12 00:00:13 --> 2017-05-12 00:00:16	TCP
30	190.39.47.233	1722	140.[redacted].113	445	2017-05-12 00:00:19 --> 2017-05-12 00:00:22	TCP
31	190.39.47.233	2095	140.[redacted].114	445	2017-05-12 00:00:26 --> 2017-05-12 00:00:29	TCP
32	190.39.47.233	2466	140.[redacted].115	445	2017-05-12 00:00:32 --> 2017-05-12 00:00:35	TCP
33	190.39.47.233	2631	140.[redacted].122	445	2017-05-12 00:00:34 --> 2017-05-12 00:00:37	TCP
34	190.39.47.233	2837	140.[redacted].116	445	2017-05-12 00:00:41 --> 2017-05-12 00:00:41	TCP
35	190.39.47.233	3207	140.[redacted].117	445	2017-05-12 00:00:44 --> 2017-05-12 00:00:46	TCP
36	190.39.47.233	3581	140.[redacted].118	445	2017-05-12 00:00:50 --> 2017-05-12 00:00:52	TCP
37	190.39.47.233	3948	140.[redacted].119	445	2017-05-12 00:00:56 --> 2017-05-12 00:00:59	TCP
[illegible]	190.39.47.233	[illegible]	140.[redacted].120	445	[illegible]	TCP

Figure 7

The detailed report of specific IP address (190.39.47.233)

Case 2：Memcached amplification attack

In February 2018, an American content delivery network (CDN) and cloud services provider announced the memcached amplification attack via UDP port 11211. The amplification factor is over 50000. The GitHub, which commonly used to host open-source software projects, is one of the victims. It had suffered roughly 1.35 Tbps, more than twice the size of the September 2016. It was the biggest record since 2016. When you face this kind of attack, the defense methods such as Flow Cleaning cannot solve the physical bandwidth congestion problem. The most effective solution is blocking the anomalous traffic from upstream ISP or the Network Regional Center. We posted this idea in a security magazine: SECURITY in September 2017. I think it would be better if we can block it before the traffic was amplified. As the following figure shown, role A acts as the attackers, role B acts as the exposed memcached servers, and role C acts the victims. Is it possible to find a solution to block the anomalous traffic between A and B. The answer is pretty clearly yes. When we checked one of our Flowviewer, we found that the algorithm is still valid. It can be used to detect the abnormal traffic which is not amplified. From the report of Flowviewer, you can know that the amplification factor would not more than 50000 in the first 5 minutes.

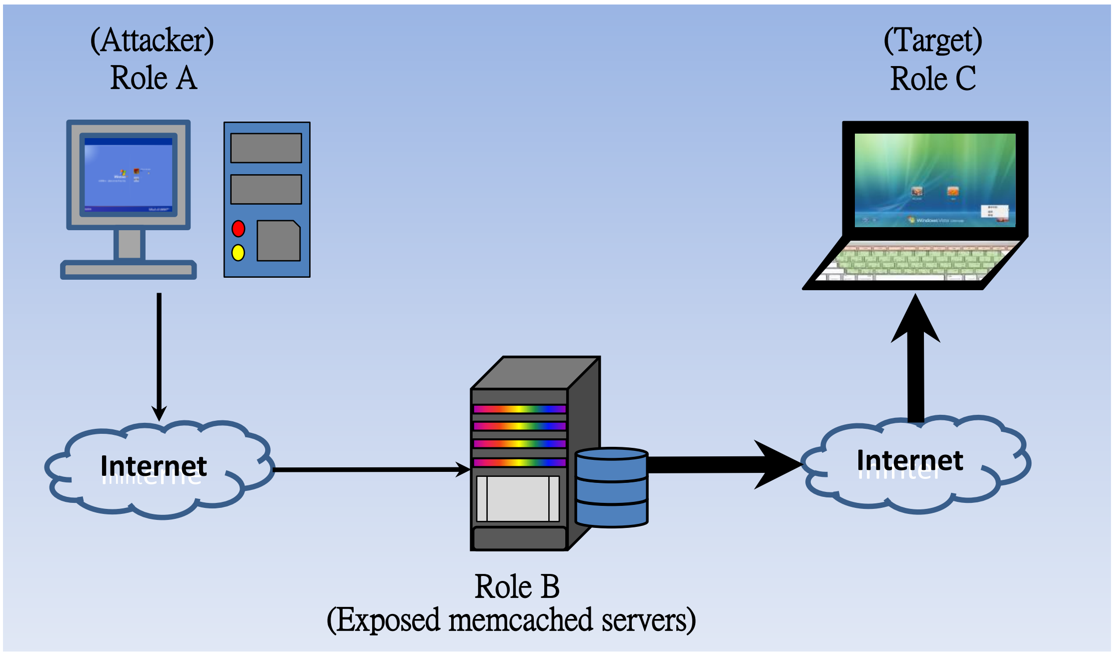
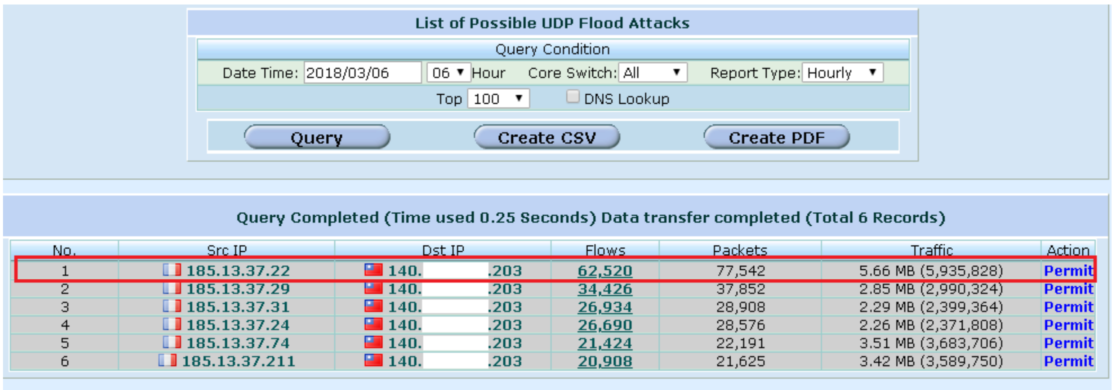


Figure 8

The schematic diagram of the memcached servers deliver amplified DDoS attack

As figure 9 shown, the Flowviewer can detect and block that abnormal traffic. You can click the number of flows to zoom in and check the detailed information. As the figure10 shown, the behavior of attack was regularly.



List of Possible UDP Flood Attacks

Query Condition

Date Time: 2018/03/06 06 Hour Core Switch: All Report Type: Hourly

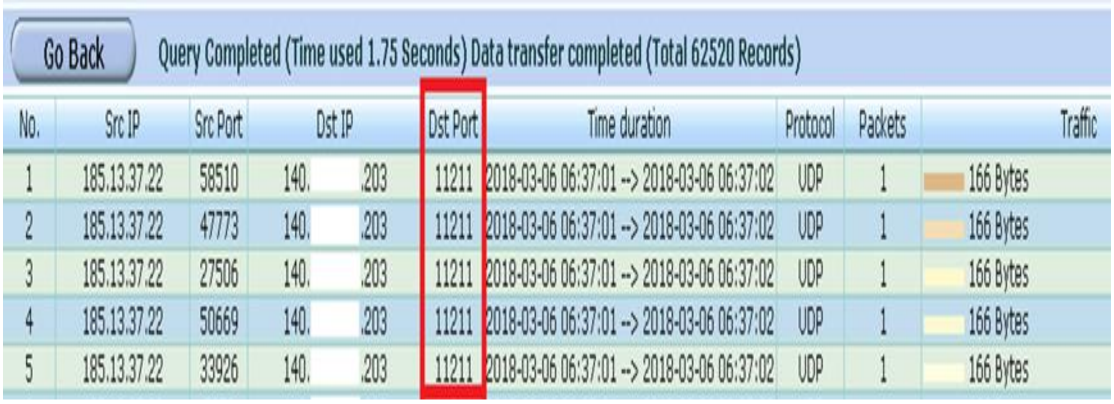
Top 100 □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 6 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic	Action
1	185.13.37.22	140.[redacted].203	62,520	77,542	5.66 MB (5,935,828)	Permit
2	185.13.37.29	140.[redacted].203	34,426	37,852	2.85 MB (2,990,324)	Permit
3	185.13.37.31	140.[redacted].203	26,934	28,908	2.29 MB (2,399,364)	Permit
4	185.13.37.24	140.[redacted].203	26,690	28,576	2.26 MB (2,371,808)	Permit
5	185.13.37.74	140.[redacted].203	21,424	22,191	3.51 MB (3,683,706)	Permit
6	185.13.37.211	140.[redacted].203	20,908	21,625	3.42 MB (3,589,750)	Permit

Figure 9

The attacker delivered a number of packets that contained small network traffic to the memcached server



Query Completed (Time used 1.75 Seconds) Data transfer completed (Total 62520 Records)

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets	Traffic
1	185.13.37.22	58510	140.[redacted].203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
2	185.13.37.22	47773	140.[redacted].203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
3	185.13.37.22	27506	140.[redacted].203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
4	185.13.37.22	50669	140.[redacted].203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes
5	185.13.37.22	33926	140.[redacted].203	11211	2018-03-06 06:37:01 --> 2018-03-06 06:37:02	UDP	1	166 Bytes

Figure 10

You can find out the regularity from the detailed report

Conclusion

As mentioned above, the advantages and benefits of Flowviewer included:

1. The flexible deployment: the Flowviewer provides four kinds of deployment architecture for network administrator. According to the network administrator's needs, the Flowviewer can be deployed rapidly in their network. The Flowviewer has the user-friendly user interface. It is easy to learn how to use the Flowviewer.

2. The Flowviewer can collaborate with other network security devices. The network administrator can choose to block the abnormal traffic on the Flowviewer or send ACL commands to core switch to block the malicious traffic.

3. The Flowviewer can use the behavior of packets to distinguish the cyber-attack and intrusion. The Flowviewer can find out the anomalous traffic by analyzing the data of the source IP address, the destination IP address, the time duration, the transport protocol and port number, the number of session/flow, the number of packet and traffic in 5 minutes. It can accurately detect the cyber-attack and intrusion by this method. You don't have to pay any extra fees for the signature updating.

4. The Flowviewer can provide many reports as the cyber-crime evidence. It also provides the dynamic select feature to the administrator so that they can retrieve the data for specific conditions.