Curelan Data Sheet

Flow Protection System

Introduction:

The IPS (Intrusion Prevention System) devices are using the technology of signature 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 is not bad but when it faces the amount of packets to attack or relay attack, it will cause the performance of hardware goes down. It needs more CPU and RAM to process these analyses. Finally, it will cause the system crashed. We used the IPS products and software to simulate the DDoS attack. It generated a lot of flows/packets to attack the device. We wanted to know 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. This kind of devices used signature to compare with packets. They need to update the signature so that they can distinguish the intrusions from normal network traffic.

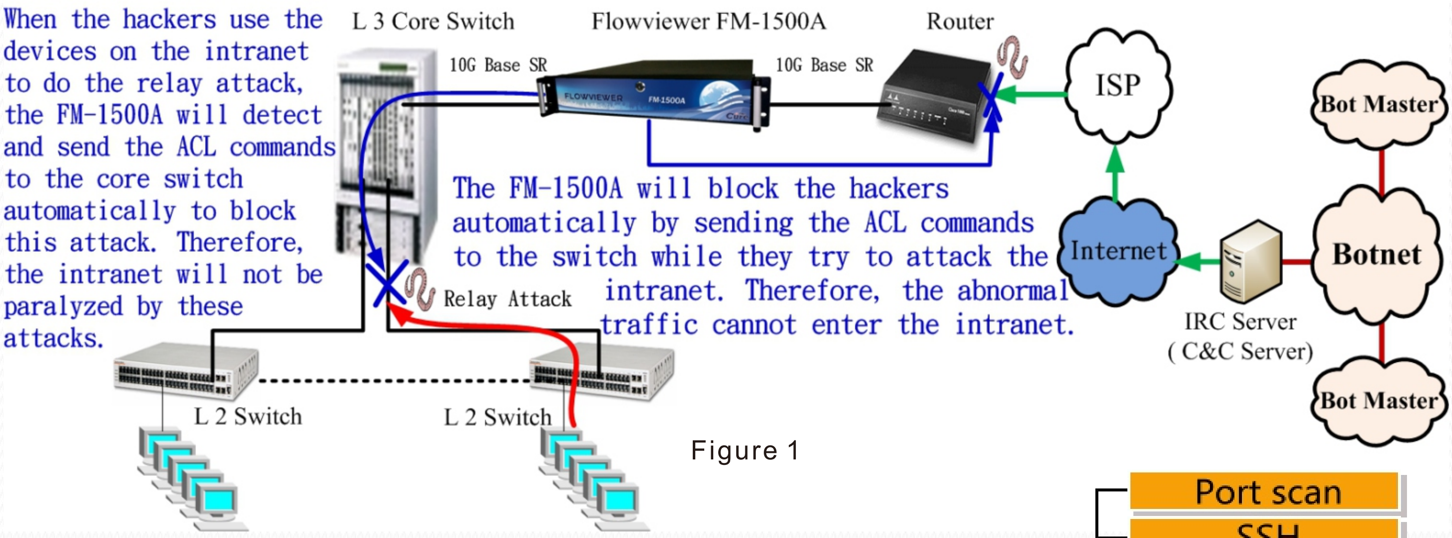
Using Netflow to find out cyber-attack and intrusion, including the source IP address, the destination IP address, the time duration, the transport protocol and port number, the number of flow, the number of packet and traffic. Just like the theory of Big Data, we can analyze those huge data to find out the regularity and then determine it is attack or not. You can find some relative papers from IEEE journals. When we want to analyze the data of Netflow, we should notice the sample rate problem. If we set the sample rate to 1:1000, that means it will choose one flow from 1000 flows. If the unit uses the device with the sample rate 1:1000, it cannot accurately detect these attacks/intrusions. Let's assume that there are one million flows, and the device only gets 1000 flows. How can this device accurately detect the attack/intrusion? Some of you may worry setting the sample rate to 1:1 will affect the hardware performance. In our experience, the network administrator told us that this setting would not cause any loading problems. The performance of the Cisco's device is not so pool. The system of the device will crash if it receives the Netflow with sample rate 1:1. Instead of blaming the product of Cisco, they should try to make their products better.

Curelan Data Sheet

Flow Protection System

Main Function: Hackers Invade Prevention & Hackers Attack Prevention

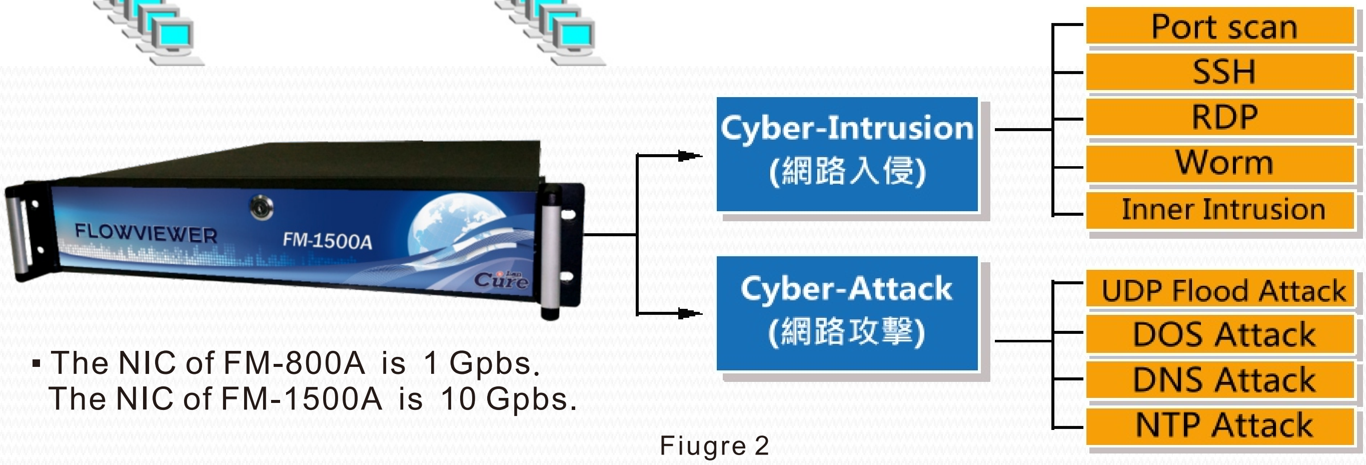
Setting the FM-1500A in inline mode (Receive Netfow / sFlow data)



When the hackers use the devices on the intranet to do the relay attack, the FM-1500A will detect and send the ACL commands to the core switch automatically to block this attack. Therefore, the intranet will not be paralyzed by these attacks.

The FM-1500A will block the hackers automatically by sending the ACL commands to the switch while they try to attack the intranet. Therefore, the abnormal traffic cannot enter the intranet.

Figure 1



Cyber-Intrusion (網路入侵)

- Port scan
- SSH
- RDP
- Worm
- Inner Intrusion

Cyber-Attack (網路攻擊)

- UDP Flood Attack
- DOS Attack
- DNS Attack
- NTP Attack

- The NIC of FM-800A is 1 Gpbs.
  The NIC of FM-1500A is 10 Gpbs.

Fiugre 2

There are two ways to automatically block the attacks from the hackers.

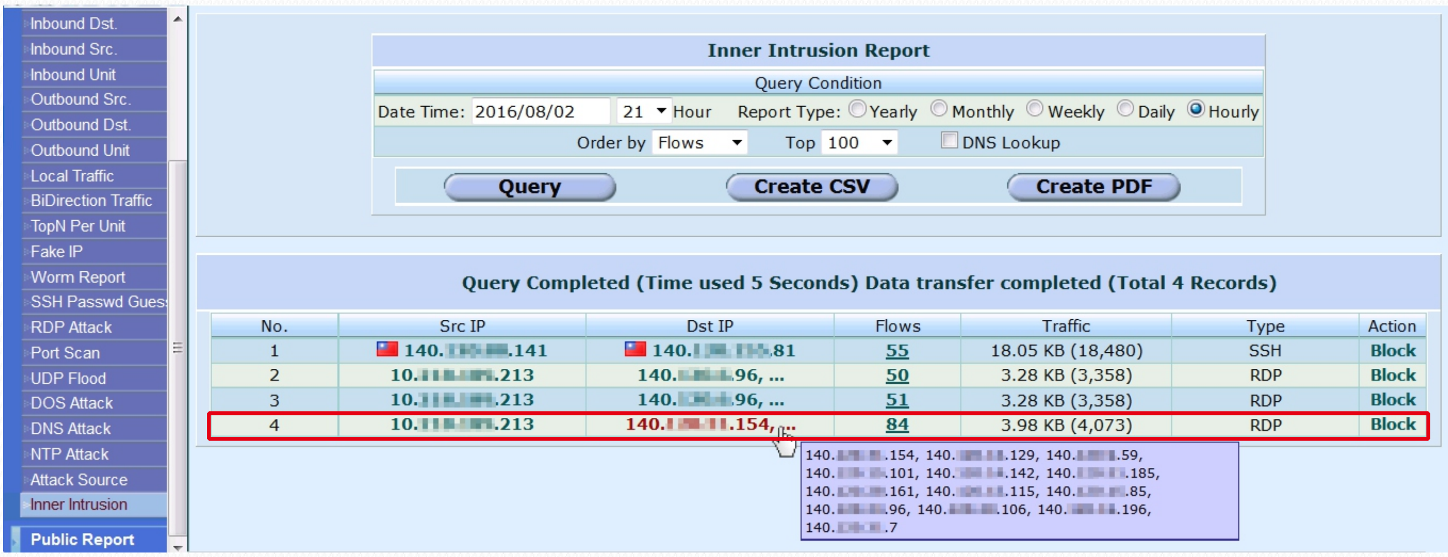
- The Flowviewer can automatically block the attacks from the hackers.
- The Flowviewer can automatically send the ACL commands to the core switch to block the attacks from the hackers.

The solution of stealing confidential data from file server by hackers.

There's no network security product which can ever protect from all attacks and invasions from hackers, for example, the Trojan horse can be hidden within in an email attachment or programs, such as P2P programs or APPs. Fortunately, the servers don't receive/send mails or automatically use P2P software to download anything; therefore, kinds of invasions are only limited on the personal computer. For example, online news had reported that the hacker-groups from Europe implanted successfully the Trojan horse program via the computers of Facebook staffs from downloading apps. Amounts of users' data were stolen that way. Let's analyze this case! The computers of Facebook staff doesn’t have the users' data on his PC. Those data must be saved in Database server. How did the hacker-groups steal those data?

It's easy! Most hacks focus on one computer and then use the intranet to invade and steal data. It’s the intranet invasion. However, all of the instruments and software are set onto the Inline Mode. That’s why the invasion of hackers would not be detected. Although Flowviewer is also set onto the Inline Mode, the Flowviewer can receive both Netflow and Sflow. Moreover, the Flowviewer receives the 1:1 random data to detect the hackers in the intranet. (Most of the hackers use the intranet and keep invading the computers until they find the server IP to steal the valuable documents. Most intranet attacks are performed via RDP. The RDP password guessing attack detection function is unique and available in FM-1500A/FM-800A. The FM-1500A/FM-800A system can detect and automatically send ACLs (Access Control List Entries) to Core Switch (Layer 3) to prevent the intranet attacks.

As the shown below, this points out that the item no.4 in the report of RDP attack was under attack. The source IP address (10.X.X.213) isn't possible to connect to thirteen computers at the same time. Maybe you'll say that it could happen when The host that owns the source IP address is used to play the role of manager. Sure! It could happen! However, Flowviewer could differentiate the illegal invasion from normal multi-computer linkage. Illegal invasion must guess the password of other users but legal log-in is not.



Inner Intrusion Report

Query Condition

Date Time: 2016/08/02 21 Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Order by Flows Top 100 □ DNS Lookup

Query Completed (Time used 5 Seconds) Data transfer completed (Total 4 Records)

No.	Src IP	Dst IP	Flows	Traffic	Type	Action
1	140.[redacted].141	140.[redacted].81	55	18.05 KB (18,480)	SSH	Block
2	10.[redacted].213	140.[redacted].96, ...	50	3.28 KB (3,358)	RDP	Block
3	10.[redacted].213	140.[redacted].96, ...	51	3.28 KB (3,358)	RDP	Block
4	10.[redacted].213	140.[redacted].154, ...	84	3.98 KB (4,073)	RDP	Block

140.[redacted].154, 140.[redacted].129, 140.[redacted].59,
140.[redacted].101, 140.[redacted].142, 140.[redacted].185,
140.[redacted].161, 140.[redacted].115, 140.[redacted].85,
140.[redacted].96, 140.[redacted].106, 140.[redacted].196,
140.[redacted].7

Figure 3 The item no.4 also shows that there are many internal hosts were under attack.

The way of hacker's invasion: hackers use invasion program through the internet — The external network hackers invade the inner users.

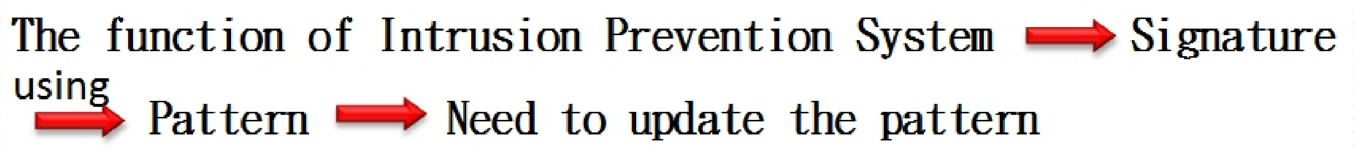
There are several methods can be used:

- Port Scanning
- SSH (by using 22 port) password guessing.
- RDP (by using 3389 port) password guessing.
- P2P, APP, Spear Phishing, Microsoft, PHP and C++ are the programs among the ones with unknown safety bug. The invasion way we mention above could only be discovered by sophisticated hackers. However, it's a situation without solution unless the administrator finds the bug himself and modify it. Hackers invade the personal computers of users through these tunnels and then keep the intra invasions till the core servers are found. This way, the confidential data could be stolen definitely.

※ Solution : Flowviewer FM-800A/FM-1500A provides with the Port Scan, SSH and RDP detection and automatically block function.

The blind spot of the IPS Equipment.

The IPS（Intrusion Prevention System) uses a feature code (Pattern; Signature) scheme to identify the external network hacker attacks by feature codes and threshold setting functions and then blocks the hacker. IPS equipment uses a feature code to detect hacker attacks and intrusion. Feature code update is slow, and the threshold value setting function error rate is very high.



The function of Intrusion Prevention System → Signature using → Pattern → Need to update the pattern

The IPS equipment is using the threshold function to detect the intrusion.
That means you need to set the value and then count the number of packets for each IP address per second. For instance, you might need to set the value of udp_src_session, the value of udp_dst_session and so on. There are lots of protocols, like voice, media stream, DNS or NTP, using the UDP packets. That is one of the reasons why the threshold function has a high false positive rate problem.

The difference between the Flowviewer and other IPS/IDS products :

	Flowviewer	**IPS/IDS products**
Architecture	InlineMode / Listen Mode	InlineMode
Analysis	Anomaly based	Signature based
Scope	WAN ⟺ LAN LAN ⟺ LAN	WAN ⟺ LAN
Technology	• **IP-NBAD** (IP-Network Behavior Anomaly Detection) Collect information of each IP address to analyze the anomalous packet in the network. • **Unique Algorithm**	• Type filters (like pattern) • OtherThreshold

The Key Technology of the Flowveiwer FM-800A / FM-1500A

The FM-800A/FM-1500A device uses self-developed mathematical algorithms that can quickly collect NetFlow or Sflow to classify and analyzes it to identify unusual or suspicious behavior. Some manufacturers develop products in this direction, but the results are far from ideal. Because almost are using the database to collect IP. Example: My SQL, Oracle and other databases. There may be a hundred million of IP data in one hour; therefore, the performance of using database to collect IP might not be efficient. The reason why we receive NetFlow or Sflow to determine the IP traffic anomaly or not, was not according to the published papers of IEEE. Instead, we use the mathematical algorithms that we developed. We combined the programs to develop mathematical algorithms, and collect all network IP data to accomplish the determining work. By identifying anomalous network data, intrusion and hacking attacks we call this way is IP NBAD (Network Behavior Anomaly Detection).

The Flowviewer takes the IP-infocollecting by receiving Netflow or sFlow data, including the source IP address, the destination IP address, time duration, transport protocol port, flows, packets and traffic.

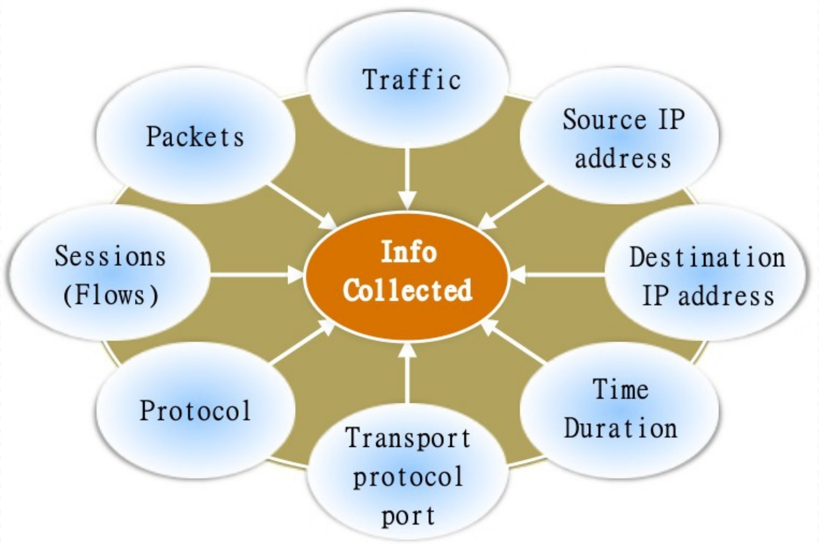
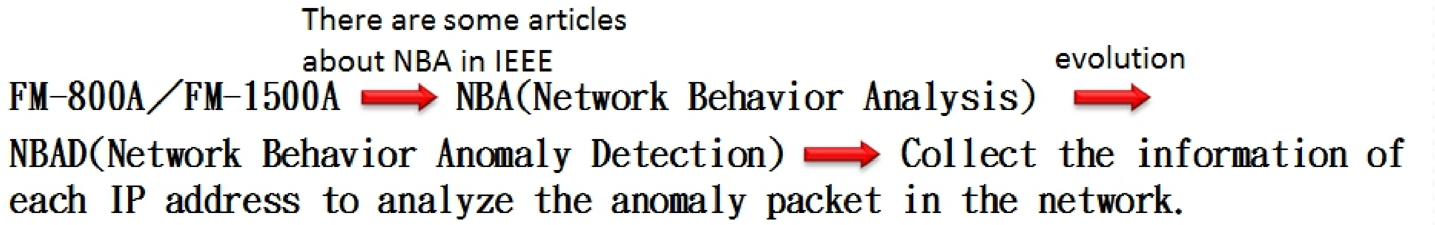


Figure 4



There are some articles about NBA in IEEE

evolution

FM-800A／FM-1500A → NBA(Network Behavior Analysis) → NBAD(Network Behavior Anomaly Detection) → Collect the information of each IP address to analyze the anomaly packet in the network.

※ The solution : The Flowviewer FM-800A/FM-1500A provides with the detection and automatically block function of DOS Attacks, UDP Flood attack, DNS attack and NTP attack.

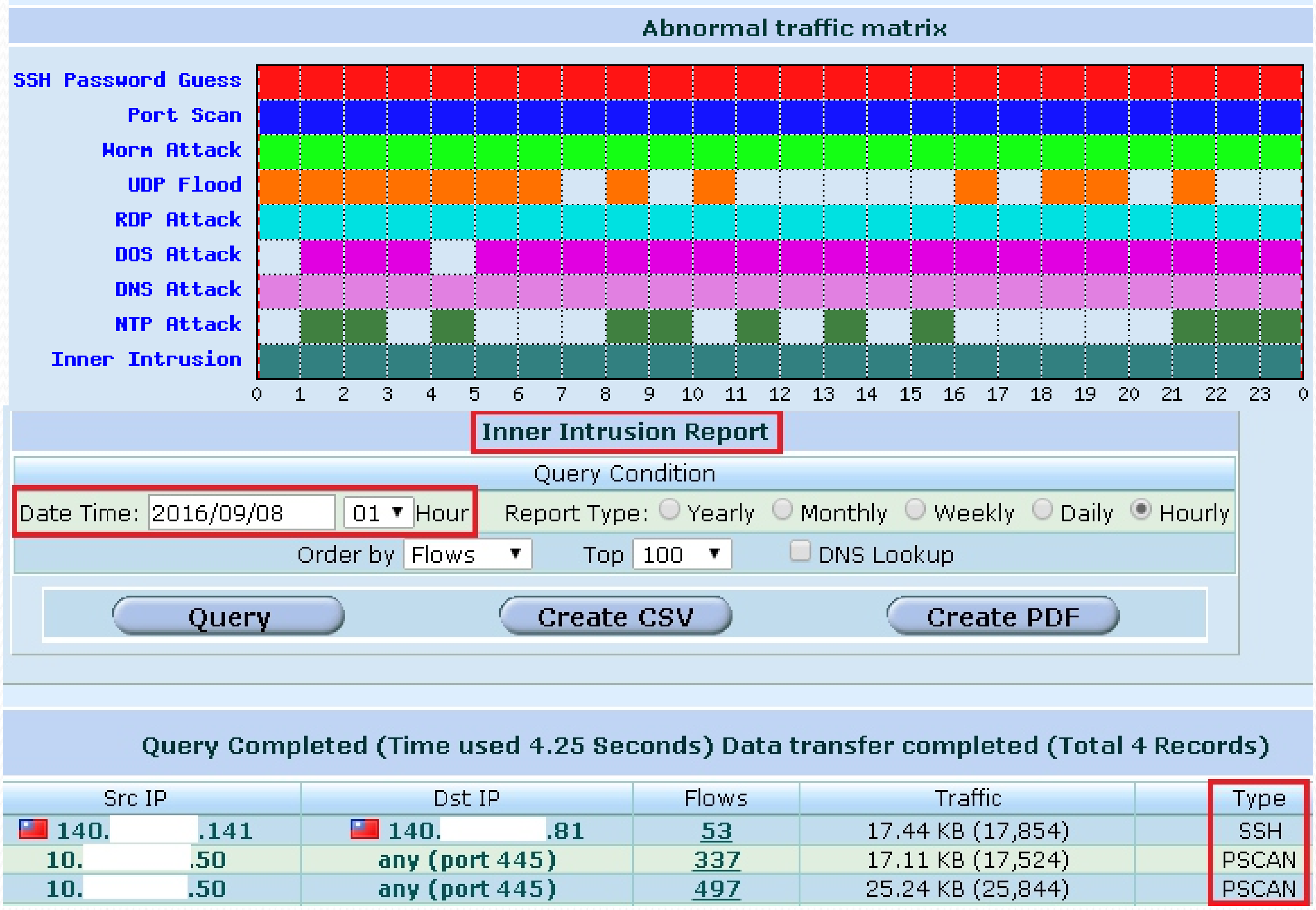
Inner Intrusion:

The Russian hacking groups steal money from banks and rigged ATMs to spew cash across the world. Because the ATM system is a closed network system, the method that they can use is intruding from intranet to intranet. Hacker will invade the device inside then use the device hacking the ATM service center. Therefore, the police cannot track down his IP address.

For government or enterprises, hackers will try to penetrate the security perimeter to steal the personal private data or the national security secrets. It may endanger national security.In Taiwan, a secret unit of government uses the closed network. They used the Flowviewer and found out the intrusion by the inner intrusion detection function.

The real case

As Figure 5 shows, the hackers tried to use the 140.X.X.141 to intrude 140.X.X.81 via SSH password guessing.



Abnormal traffic matrix

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SSH Password Guess	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Port Scan	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Worm Attack	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
UDP Flood	■	■	■	■	■	■	■		■		■						■		■	■		■		
RDP Attack	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
DOS Attack		■	■	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
DNS Attack	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
NTP Attack		■	■		■				■	■		■		■		■						■	■	■
Inner Intrusion	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

Inner Intrusion Report

Query Condition

Date Time: 2016/09/08 01 ▾ Hour

Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Order by Flows ▾ Top 100 ▾ □ DNS Lookup

Query Completed (Time used 4.25 Seconds) Data transfer completed (Total 4 Records)

Src IP	Dst IP	Flows	Traffic	Type
140.[redacted].141	140.[redacted].81	53	17.44 KB (17,854)	SSH
10.[redacted].50	any (port 445)	337	17.11 KB (17,524)	PSCAN
10.[redacted].50	any (port 445)	497	25.24 KB (25,844)	PSCAN

Figure 5

Hackers paralyzed the computer networks by:

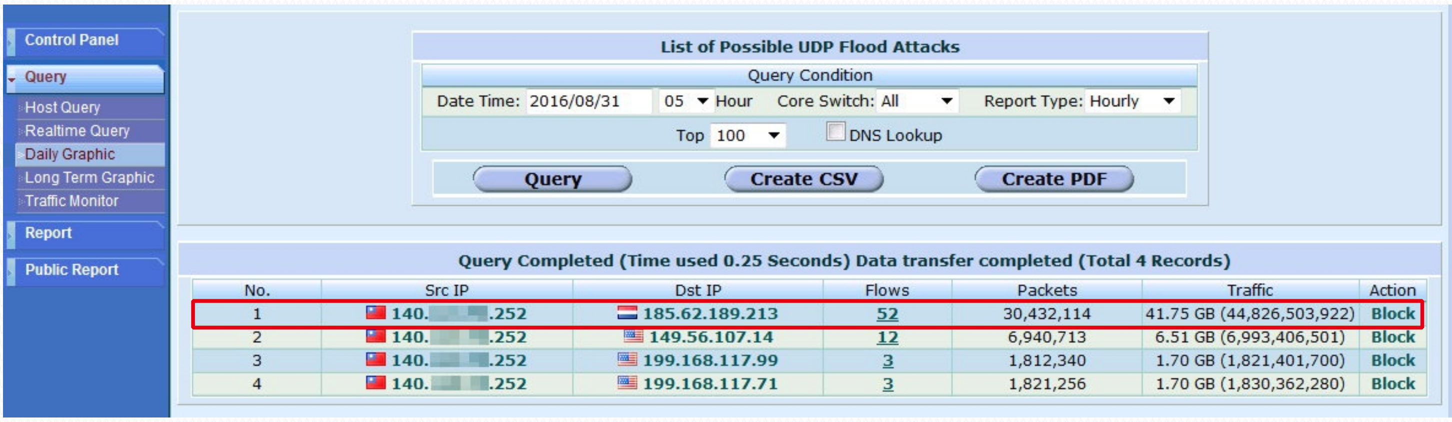
- UDP Flood Attacks: Make a large number of traffic, fake UDP packages to attack a special IP. Weaken the intranet so it cannot work normally. This IP can be the HTTP file server, Web server, DNS server and so on.

- DOS Attacks: Make a large number of Flows, fake TCP (or UDP) packages to attack a special IP. Weaken the intranet so it cannot work normally. This IP can be the HTTP file server, Web server, DNS server and so on.

The UDP Flood Attack

Real Case: UDP is a sessionless protocol(TCP protocol using the session).However, hackers use "port-jumping" method to make flows by creating a large number of udp packets to random ports.

As Figure 6 shows, the hacker relayed the 140.X.X.252 to attack 185.62.189.213, The number of the flow was 52 and the network traffic was 41.75 GB. The Flowviewer can automatically detect and block the attack IP address of attack IP. The network will NOT be paralyzed.



List of Possible UDP Flood Attacks

Query Condition

Date Time: 2016/08/31 05 Hour Core Switch: All Report Type: Hourly

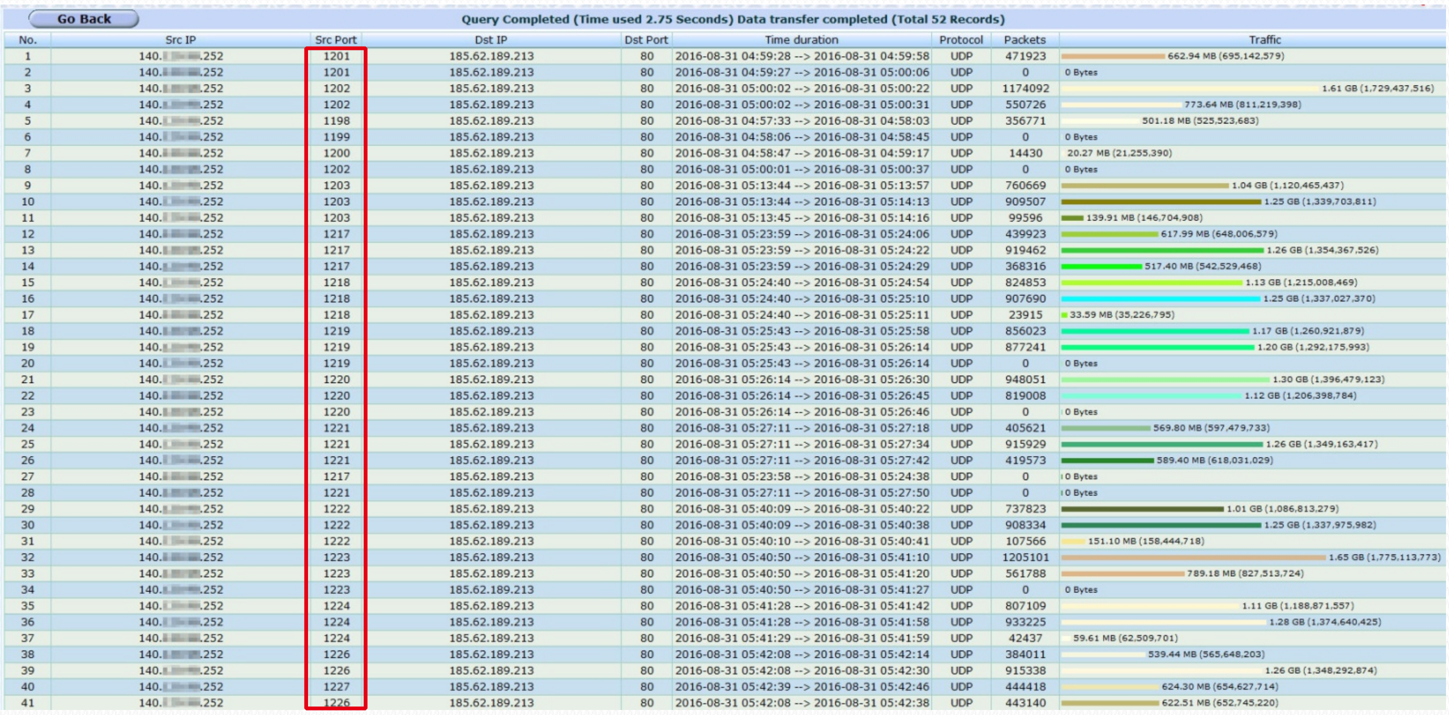
Top 100 □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 4 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic	Action
1	140.[redacted].252	185.62.189.213	52	30,432,114	41.75 GB (44,826,503,922)	Block
2	140.[redacted].252	149.56.107.14	12	6,940,713	6.51 GB (6,993,406,501)	Block
3	140.[redacted].252	199.168.117.99	3	1,812,340	1.70 GB (1,821,401,700)	Block
4	140.[redacted].252	199.168.117.71	3	1,821,256	1.70 GB (1,830,362,280)	Block

Figure 6

We can zoom in to get more detailed information by clicking the number of flows. As the shown below : The source port number was different for each item. This means that the hackers used port-jumping method to make connections. When hackers use the udp port 123 as the source port, then this is the NTP (Network Time Protocol) attack. Similarly, when the source port number changes to 53, we can tell that it is the DNS attack.



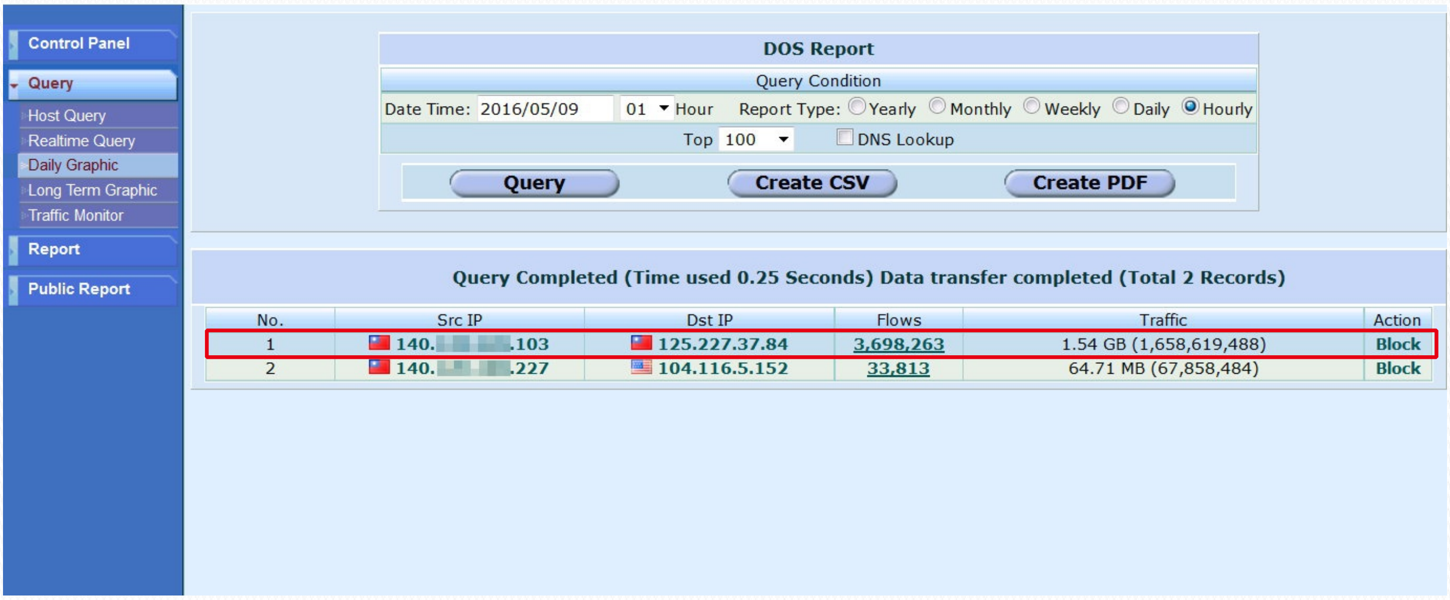
Query Completed (Time used 2.75 Seconds) Data transfer completed (Total 52 Records)

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets	Traffic
1	140.[redacted].252	1201	185.62.189.213	80	2016-08-31 04:59:28 --> 2016-08-31 04:59:58	UDP	471923	662.94 MB (695,142,579)
2	140.[redacted].252	1201	185.62.189.213	80	2016-08-31 04:59:27 --> 2016-08-31 05:00:06	UDP	0	0 Bytes
3	140.[redacted].252	1202	185.62.189.213	80	2016-08-31 05:00:02 --> 2016-08-31 05:00:22	UDP	1174092	1.61 GB (1,729,437,516)
4	140.[redacted].252	1202	185.62.189.213	80	2016-08-31 05:00:02 --> 2016-08-31 05:00:31	UDP	550726	773.64 MB (811,219,398)
5	140.[redacted].252	1198	185.62.189.213	80	2016-08-31 04:57:33 --> 2016-08-31 04:58:03	UDP	356771	501.18 MB (525,523,683)
6	140.[redacted].252	1199	185.62.189.213	80	2016-08-31 04:58:06 --> 2016-08-31 04:58:45	UDP	0	0 Bytes
7	140.[redacted].252	1200	185.62.189.213	80	2016-08-31 04:58:47 --> 2016-08-31 04:59:17	UDP	14430	20.27 MB (21,255,390)
8	140.[redacted].252	1202	185.62.189.213	80	2016-08-31 05:00:01 --> 2016-08-31 05:00:37	UDP	0	0 Bytes
9	140.[redacted].252	1203	185.62.189.213	80	2016-08-31 05:13:44 --> 2016-08-31 05:13:57	UDP	760669	1.04 GB (1,120,465,437)
10	140.[redacted].252	1203	185.62.189.213	80	2016-08-31 05:13:44 --> 2016-08-31 05:14:13	UDP	909507	1.25 GB (1,339,703,811)
11	140.[redacted].252	1203	185.62.189.213	80	2016-08-31 05:13:45 --> 2016-08-31 05:14:16	UDP	99596	139.91 MB (146,704,908)
12	140.[redacted].252	1217	185.62.189.213	80	2016-08-31 05:23:59 --> 2016-08-31 05:24:06	UDP	439923	617.99 MB (648,006,579)
13	140.[redacted].252	1217	185.62.189.213	80	2016-08-31 05:23:59 --> 2016-08-31 05:24:22	UDP	919462	1.26 GB (1,354,367,526)
14	140.[redacted].252	1217	185.62.189.213	80	2016-08-31 05:23:59 --> 2016-08-31 05:24:29	UDP	368316	517.40 MB (542,529,468)
15	140.[redacted].252	1218	185.62.189.213	80	2016-08-31 05:24:40 --> 2016-08-31 05:24:54	UDP	824853	1.13 GB (1,215,008,469)
16	140.[redacted].252	1218	185.62.189.213	80	2016-08-31 05:24:40 --> 2016-08-31 05:25:10	UDP	907690	1.25 GB (1,337,027,370)
17	140.[redacted].252	1218	185.62.189.213	80	2016-08-31 05:24:40 --> 2016-08-31 05:25:11	UDP	23915	33.59 MB (35,226,795)
18	140.[redacted].252	1219	185.62.189.213	80	2016-08-31 05:25:43 --> 2016-08-31 05:25:58	UDP	856023	1.17 GB (1,260,921,879)
19	140.[redacted].252	1219	185.62.189.213	80	2016-08-31 05:25:43 --> 2016-08-31 05:26:14	UDP	877241	1.20 GB (1,292,175,993)
20	140.[redacted].252	1219	185.62.189.213	80	2016-08-31 05:25:43 --> 2016-08-31 05:26:14	UDP	0	0 Bytes
21	140.[redacted].252	1220	185.62.189.213	80	2016-08-31 05:26:14 --> 2016-08-31 05:26:30	UDP	948051	1.30 GB (1,396,479,123)
22	140.[redacted].252	1220	185.62.189.213	80	2016-08-31 05:26:14 --> 2016-08-31 05:26:45	UDP	819008	1.12 GB (1,206,398,784)
23	140.[redacted].252	1220	185.62.189.213	80	2016-08-31 05:26:14 --> 2016-08-31 05:26:46	UDP	0	0 Bytes
24	140.[redacted].252	1221	185.62.189.213	80	2016-08-31 05:27:11 --> 2016-08-31 05:27:18	UDP	405621	569.80 MB (597,479,733)
25	140.[redacted].252	1221	185.62.189.213	80	2016-08-31 05:27:11 --> 2016-08-31 05:27:34	UDP	915929	1.26 GB (1,349,163,417)
26	140.[redacted].252	1221	185.62.189.213	80	2016-08-31 05:27:11 --> 2016-08-31 05:27:42	UDP	419573	589.40 MB (618,031,029)
27	140.[redacted].252	1217	185.62.189.213	80	2016-08-31 05:23:58 --> 2016-08-31 05:24:38	UDP	0	0 Bytes
28	140.[redacted].252	1221	185.62.189.213	80	2016-08-31 05:27:11 --> 2016-08-31 05:27:50	UDP	0	0 Bytes
29	140.[redacted].252	1222	185.62.189.213	80	2016-08-31 05:40:09 --> 2016-08-31 05:40:22	UDP	737823	1.01 GB (1,086,813,279)
30	140.[redacted].252	1222	185.62.189.213	80	2016-08-31 05:40:09 --> 2016-08-31 05:40:38	UDP	908334	1.25 GB (1,337,975,982)
31	140.[redacted].252	1222	185.62.189.213	80	2016-08-31 05:40:10 --> 2016-08-31 05:40:41	UDP	107566	151.10 MB (158,444,718)
32	140.[redacted].252	1223	185.62.189.213	80	2016-08-31 05:40:50 --> 2016-08-31 05:41:10	UDP	1205101	1.65 GB (1,775,113,773)
33	140.[redacted].252	1223	185.62.189.213	80	2016-08-31 05:40:50 --> 2016-08-31 05:41:20	UDP	561788	789.18 MB (827,513,724)
34	140.[redacted].252	1223	185.62.189.213	80	2016-08-31 05:40:50 --> 2016-08-31 05:41:27	UDP	0	0 Bytes
35	140.[redacted].252	1224	185.62.189.213	80	2016-08-31 05:41:28 --> 2016-08-31 05:41:42	UDP	807109	1.11 GB (1,188,871,557)
36	140.[redacted].252	1224	185.62.189.213	80	2016-08-31 05:41:28 --> 2016-08-31 05:41:58	UDP	933225	1.28 GB (1,374,640,425)
37	140.[redacted].252	1224	185.62.189.213	80	2016-08-31 05:41:29 --> 2016-08-31 05:41:59	UDP	42437	59.61 MB (62,509,701)
38	140.[redacted].252	1226	185.62.189.213	80	2016-08-31 05:42:08 --> 2016-08-31 05:42:14	UDP	384011	539.44 MB (565,648,203)
39	140.[redacted].252	1226	185.62.189.213	80	2016-08-31 05:42:08 --> 2016-08-31 05:42:30	UDP	915338	1.26 GB (1,348,292,874)
40	140.[redacted].252	1227	185.62.189.213	80	2016-08-31 05:42:39 --> 2016-08-31 05:42:46	UDP	444418	624.30 MB (654,627,714)
41	140.[redacted].252	1226	185.62.189.213	80	2016-08-31 05:42:08 --> 2016-08-31 05:42:38	UDP	443140	622.51 MB (652,745,220)

Figure 7

THE DOS Attack

As Figure 8 shows, the hacker attacked 125.227.37.84 by relaying 140.X.X.103. The maximum number of the flows were up to 3,698,263 and the traffic was 1.54GB.



DOS Report

Query Condition

Date Time: 2016/05/09 01 Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Top 100 □ DNS Lookup

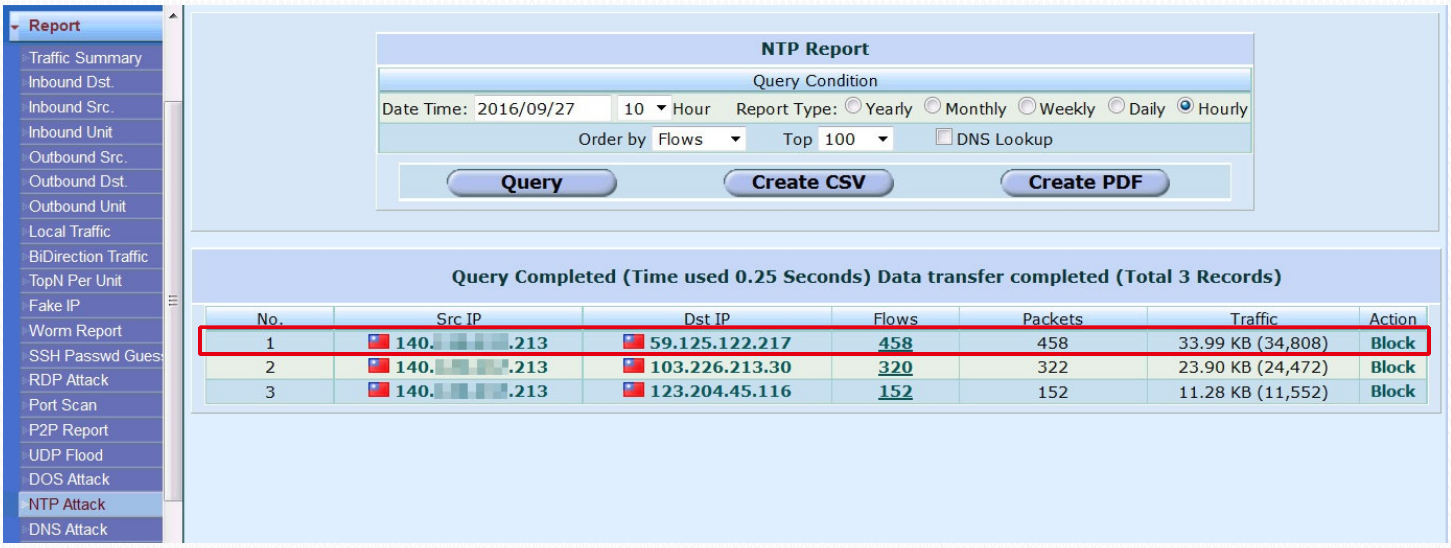
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 2 Records)

No.	Src IP	Dst IP	Flows	Traffic	Action
1	140.[redacted].103	125.227.37.84	3,698,263	1.54 GB (1,658,619,488)	Block
2	140.[redacted].227	104.116.5.152	33,813	64.71 MB (67,858,484)	Block

Figure 8

THE NTP reflection Attacks

As shown in figure 9 and 10, the hacker attacked 59.125.122.217 via port 123 by relaying 140.x.x.213. It’s was the NTP reflection attack.



NTP Report

Query Condition

Date Time: 2016/09/27 10 Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

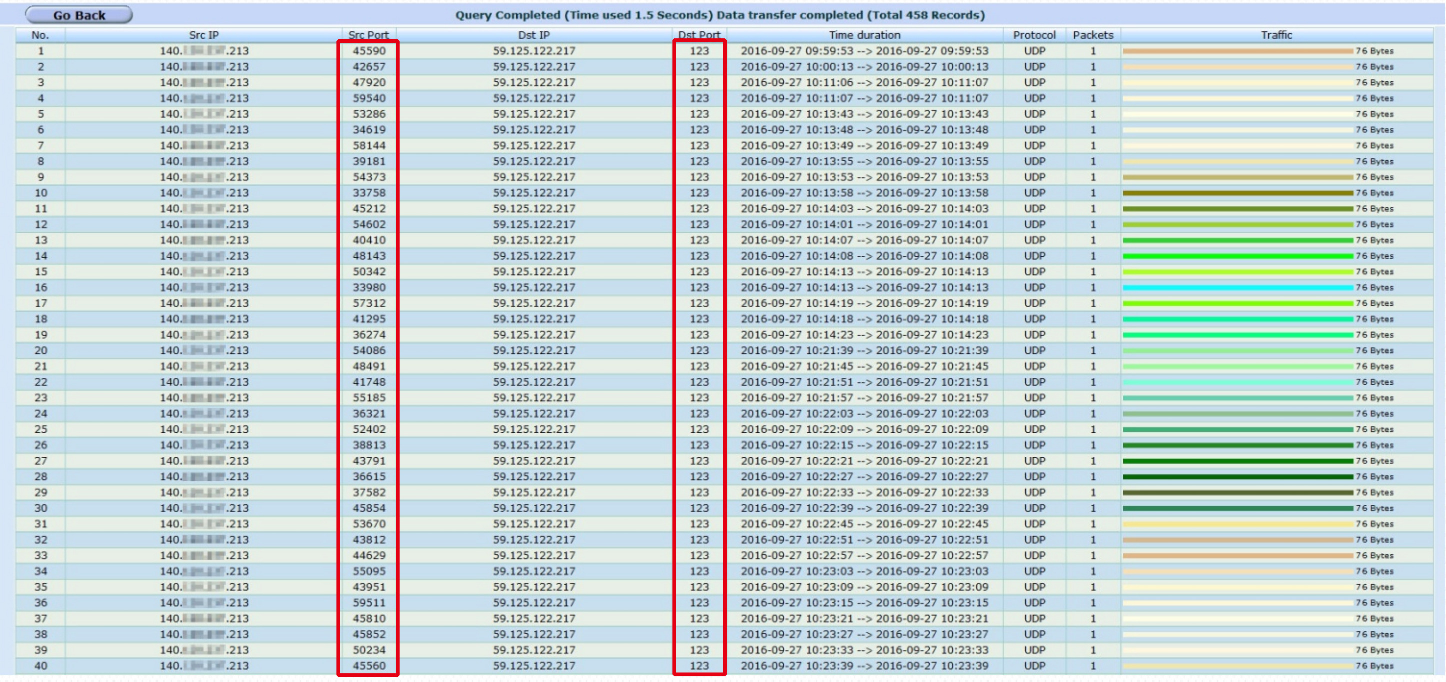
Order by Flows Top 100 □ DNS Lookup

Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 3 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic	Action
1	140.[redacted].213	59.125.122.217	458	458	33.99 KB (34,808)	Block
2	140.[redacted].213	103.226.213.30	320	322	23.90 KB (24,472)	Block
3	140.[redacted].213	123.204.45.116	152	152	11.28 KB (11,552)	Block

Figure 9

We can zoom in to get more detailed information by clicking the number of flows. As the shown below : the source port is random and the destination port is port 123. This means that hacker attacked the host by using the NTP reflection attack.



Query Completed (Time used 1.5 Seconds) Data transfer completed (Total 458 Records)

No.	Src IP	Src Port	Dst IP	Dst Port	Time duration	Protocol	Packets	Traffic
1	140.[redacted].213	45590	59.125.122.217	123	2016-09-27 09:59:53 --> 2016-09-27 09:59:53	UDP	1	76 Bytes
2	140.[redacted].213	42657	59.125.122.217	123	2016-09-27 10:00:13 --> 2016-09-27 10:00:13	UDP	1	76 Bytes
3	140.[redacted].213	47920	59.125.122.217	123	2016-09-27 10:11:06 --> 2016-09-27 10:11:07	UDP	1	76 Bytes
4	140.[redacted].213	59540	59.125.122.217	123	2016-09-27 10:11:07 --> 2016-09-27 10:11:07	UDP	1	76 Bytes
5	140.[redacted].213	53286	59.125.122.217	123	2016-09-27 10:13:43 --> 2016-09-27 10:13:43	UDP	1	76 Bytes
6	140.[redacted].213	34619	59.125.122.217	123	2016-09-27 10:13:48 --> 2016-09-27 10:13:48	UDP	1	76 Bytes
7	140.[redacted].213	58144	59.125.122.217	123	2016-09-27 10:13:49 --> 2016-09-27 10:13:49	UDP	1	76 Bytes
8	140.[redacted].213	39181	59.125.122.217	123	2016-09-27 10:13:55 --> 2016-09-27 10:13:55	UDP	1	76 Bytes
9	140.[redacted].213	54373	59.125.122.217	123	2016-09-27 10:13:53 --> 2016-09-27 10:13:53	UDP	1	76 Bytes
10	140.[redacted].213	33758	59.125.122.217	123	2016-09-27 10:13:58 --> 2016-09-27 10:13:58	UDP	1	76 Bytes
11	140.[redacted].213	45212	59.125.122.217	123	2016-09-27 10:14:03 --> 2016-09-27 10:14:03	UDP	1	76 Bytes
12	140.[redacted].213	54602	59.125.122.217	123	2016-09-27 10:14:01 --> 2016-09-27 10:14:01	UDP	1	76 Bytes
13	140.[redacted].213	40410	59.125.122.217	123	2016-09-27 10:14:07 --> 2016-09-27 10:14:07	UDP	1	76 Bytes
14	140.[redacted].213	48143	59.125.122.217	123	2016-09-27 10:14:08 --> 2016-09-27 10:14:08	UDP	1	76 Bytes
15	140.[redacted].213	50342	59.125.122.217	123	2016-09-27 10:14:13 --> 2016-09-27 10:14:13	UDP	1	76 Bytes
16	140.[redacted].213	33980	59.125.122.217	123	2016-09-27 10:14:13 --> 2016-09-27 10:14:13	UDP	1	76 Bytes
17	140.[redacted].213	57312	59.125.122.217	123	2016-09-27 10:14:19 --> 2016-09-27 10:14:19	UDP	1	76 Bytes
18	140.[redacted].213	41295	59.125.122.217	123	2016-09-27 10:14:18 --> 2016-09-27 10:14:18	UDP	1	76 Bytes
19	140.[redacted].213	36274	59.125.122.217	123	2016-09-27 10:14:23 --> 2016-09-27 10:14:23	UDP	1	76 Bytes
20	140.[redacted].213	54086	59.125.122.217	123	2016-09-27 10:21:39 --> 2016-09-27 10:21:39	UDP	1	76 Bytes
21	140.[redacted].213	48491	59.125.122.217	123	2016-09-27 10:21:45 --> 2016-09-27 10:21:45	UDP	1	76 Bytes
22	140.[redacted].213	41748	59.125.122.217	123	2016-09-27 10:21:51 --> 2016-09-27 10:21:51	UDP	1	76 Bytes
23	140.[redacted].213	55185	59.125.122.217	123	2016-09-27 10:21:57 --> 2016-09-27 10:21:57	UDP	1	76 Bytes
24	140.[redacted].213	36321	59.125.122.217	123	2016-09-27 10:22:03 --> 2016-09-27 10:22:03	UDP	1	76 Bytes
25	140.[redacted].213	52402	59.125.122.217	123	2016-09-27 10:22:09 --> 2016-09-27 10:22:09	UDP	1	76 Bytes
26	140.[redacted].213	38813	59.125.122.217	123	2016-09-27 10:22:15 --> 2016-09-27 10:22:15	UDP	1	76 Bytes
27	140.[redacted].213	43791	59.125.122.217	123	2016-09-27 10:22:21 --> 2016-09-27 10:22:21	UDP	1	76 Bytes
28	140.[redacted].213	36615	59.125.122.217	123	2016-09-27 10:22:27 --> 2016-09-27 10:22:27	UDP	1	76 Bytes
29	140.[redacted].213	37582	59.125.122.217	123	2016-09-27 10:22:33 --> 2016-09-27 10:22:33	UDP	1	76 Bytes
30	140.[redacted].213	45854	59.125.122.217	123	2016-09-27 10:22:39 --> 2016-09-27 10:22:39	UDP	1	76 Bytes
31	140.[redacted].213	53670	59.125.122.217	123	2016-09-27 10:22:45 --> 2016-09-27 10:22:45	UDP	1	76 Bytes
32	140.[redacted].213	43812	59.125.122.217	123	2016-09-27 10:22:51 --> 2016-09-27 10:22:51	UDP	1	76 Bytes
33	140.[redacted].213	44629	59.125.122.217	123	2016-09-27 10:22:57 --> 2016-09-27 10:22:57	UDP	1	76 Bytes
34	140.[redacted].213	55095	59.125.122.217	123	2016-09-27 10:23:03 --> 2016-09-27 10:23:03	UDP	1	76 Bytes
35	140.[redacted].213	43951	59.125.122.217	123	2016-09-27 10:23:09 --> 2016-09-27 10:23:09	UDP	1	76 Bytes
36	140.[redacted].213	59511	59.125.122.217	123	2016-09-27 10:23:15 --> 2016-09-27 10:23:15	UDP	1	76 Bytes
37	140.[redacted].213	45810	59.125.122.217	123	2016-09-27 10:23:21 --> 2016-09-27 10:23:21	UDP	1	76 Bytes
38	140.[redacted].213	45852	59.125.122.217	123	2016-09-27 10:23:27 --> 2016-09-27 10:23:27	UDP	1	76 Bytes
39	140.[redacted].213	50234	59.125.122.217	123	2016-09-27 10:23:33 --> 2016-09-27 10:23:33	UDP	1	76 Bytes
40	140.[redacted].213	45560	59.125.122.217	123	2016-09-27 10:23:39 --> 2016-09-27 10:23:39	UDP	1	76 Bytes

Figure 10

The Product Major Functions

- Netflow or sFlow traffic report.
- Worm detection (NBAD).
- Automatically block infected IPs from L3 Switch by ACL. (For Cisco, Foundry, Alcatel, Extreme) or automatically block by Flowviewer.
- Port Scan and SSH Password Guess Attacks Report (NBAD).
- RDP Password Guess Attacks Report (NBAD).
- List of Possible UDP Flood Attacks Report (NBAD).
- List of Possible DOS Attacks Report (NBAD).
- Port Scan and SSH Password Guess Detection and Blocking. Blocked by Flowviewer.
- RDP Password Guess Detection and Blocking. Blocking method: Blocked by Flowviewer.
- UDP Flood Attack Detection and Blocking. Blocking method: Blocked by Flowviewer or Apply ACL command to core switch.
- DOS Attack Detection and Blocking. Blocking method: Blocked by Flowviewer or Apply ACL command to core switch.
- DNS Attack Detection and Blocking. Blocking method: Blocked by Flowviewer or Apply ACL command to core switch.
- NTP Attack Detection and Blocking. Blocking method: Blocked by Flowviewer or Apply ACL command to core switch.
- Inner Intrusion Detection and Blocking. Blocking method: Blocked by Flowviewer or Apply ACL command to core switch.

Built-in standard feature with the difference functionality table

	FM-800A	FM-1500A
Netflow or sFlow traffic report	Yes	Yes
Worm Detection (NBAD)	Yes	Yes
Automatic block infected Ips from L3 Switch by ACL	Yes	Yes
SSH Password Guess Attacks Report	Yes	Yes
RDP Password Guess Attack Report	Yes	Yes
Automatic block SSH Password Guess Attacks	Yes	Yes
Automatic block RDP Attacks	Yes	Yes
UDP Flood Attack Detection and DOS Attack Report	Yes	Yes
Automatic block UDP Flood Attack and DOS Attack Detection	Yes	Yes
DNS Attack and NTP Attack Report	Yes	Yes
Automatic block DNS Attack and NTP Attack Dectection	Yes	Yes
Inner Intrusion Report	Yes	Yes
Public Report (Hyperlinks)	Yes	Yes
Report of the statistical attack source	Yes	Yes

Features	Description
HARDWARE	
Physical Dimensions	Chassis: 2U rack height Height: 3.45 inches (8.67 cm) Width: 17.4 inches (43.53 cm) Depth: 24 inches (61 cm) Weight: 41 lbs. (18.5 kg)
Environmental	Temperature, operating: 50° to 95°F (10° to 35°C) Temperature, non-operating: -40° to 158°F (-40° to 70°C) Humidity, non-operating: 95% Operating humidity: 5-85% Non-condensing at temperatures: 73° to 104°F (23° to 40°C)
Operating System	Embedded Linux operating system
Management	Web UI, role-based management
Management Interfaces	1 x 10/100/1000 Base TX
Availability	Inline bypass
MTBF	5 years
Regulatory Compliance	Complies with RoHS Directive 2002/95/EC
Web-Based GUI	Supports language: English, Traditional Chinese
Inspected Throughput	Up to 1Gbps (FM-800A) ; Up to 10Gbps (FM-1500A)
Supported Browsers	Firefox ESR 24, Firefox 24, Google Chrome 29, Internet Explorer 10, Internet Explorer 11, Safari 6
MANAGEMENT AND SECURITY	
Protected Endpoints	Unlimited
Latency	Less than 85 microseconds
Reporting	Real-time and historic traffic reporting; SSH password guess attacks reporting; RDP attack reporting; UDP flood attacks reporting; DOS attacks reporting; Worm attacks reporting; Port scan reporting; DNS attacks reporting; NTP attacks reporting; Inner Intrusion reporting
Modes	Inline, Receive Netflow; Inline, Generate Netflow itself; Listen, Receive Netflow; Listen, Generate Netflow itself
Real-Time Updates	We do NOT use Signature database so we do not need to update it.
Notifications	E-mail
Maximum NetFlow Volume	FM-800A :150,000 FPS (Flows per Second) FM-1500A : 250,000 FPS (Flows per Second) * when it be deployed in listen mode

Hardware Options

Series	FM-800A	FM-1500A
Memory	16 GB	32GB
Hard Drives	• 1 x 2.5" SSD drives with embedded system • 2 x 3 TB SATA drives in RAID 1	
Power	• 1 x AC power supplies; 520W max continuous output	
Protection Interface Options	• 2 x 10/100/1000 Base TX • 2 x Gigabit Ethernet 1000BASE SX, 850 nm	• 2 x 10 Gigabit Ethernet : SR Fiber • 2 x 10/100/1000 Base TX • 2 x Gigabit Ethernet 1000BASE:SX, 850 nm
Traffic Bypass Default	• Integrated hardware bypass • Internal “software” bypass to pass traffic without inspection	

Flowviewer appliance: All models utilize the same 2U rack height form factor.

Contact information

15F.-1, No.255, Jiuru 2nd Rd.,
Sanmin Dist., Kaohsiung City
807, Taiwan (R.O.C.)
Tel：+886-7-311-5186
Fax：+886-7-311-5178

www.curelan.com