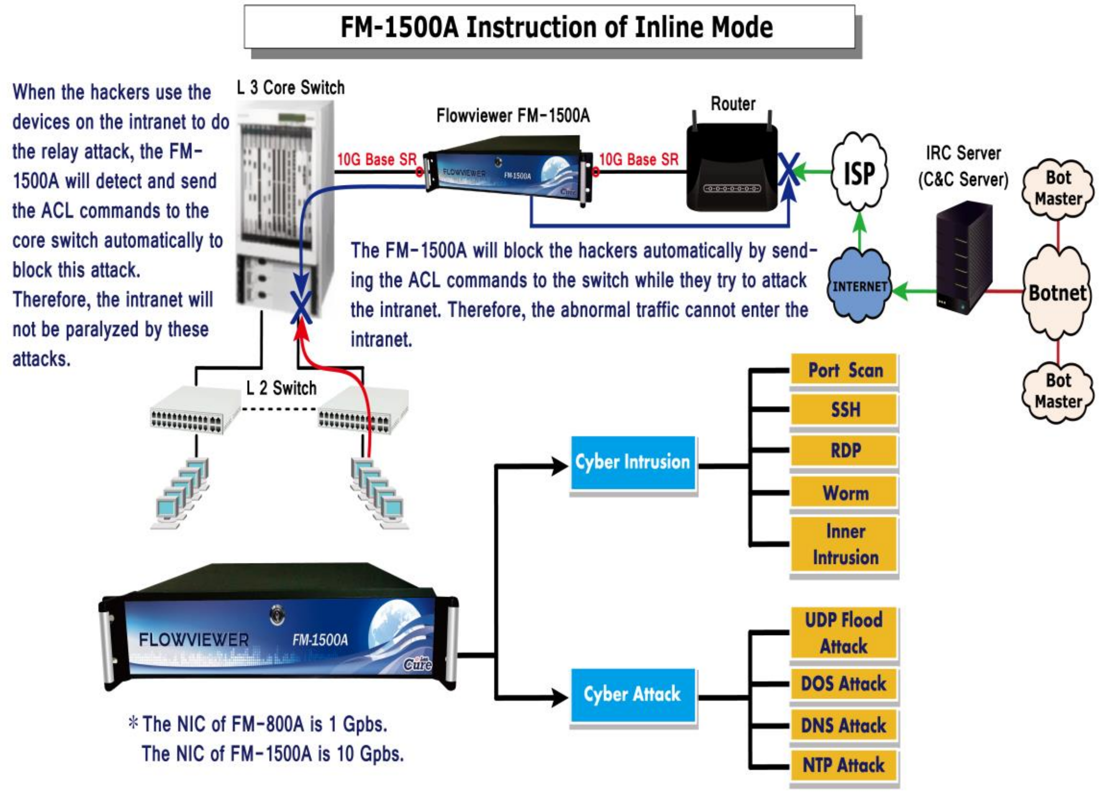
Using the collective data of Netflow to distinguish the hacking intrusion and attack from the traffic.

The IPS (Intrusion Prevention System) devices on the market 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 hardware performance goes down. It needs more CPU and RAM to process these packets. Finally, it will cause the system crashed. Besides, this technology uses signature to distinguish the cyber-attack and intrusion from the traffic. This means it needs to upgrade the newer signature so that it can know which belong to abnormal traffic. The hacker groups know this, too. That is the reason why they always use the latest version of Trojan horse to intrude the political units, the military units and the finance units..

Another way is 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 session/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.

The Flowviewer that developed by Curelan Technology Co., Ltd is using the technology of analyzing from Netflow. Because it receives the Netflow with the sample rate 1:1, it does not need to filter or analyze the huge packets with the signatures. Therefore, it can be deployed in Inline mode and will not cause any hardware problems that we just mention. Of cause, you can deploy the Flowviewer in Listen mode, too. You may ask why we deploy our product in Inline mode. It is because the hackers always try to use robot to intrude the network. According to our observation, the average number of intruded IP address is more than 300 every single day. Sometimes, it is up to 600 intruded IP addresses in one day. If you want to use the ACL (Access Control List) to block these IPs, there will be too many commands of deny. As the result, it will affect the performance of the core switch. That is the reason why we always suggest our customers to deploy the Flowviewer in Inline mode. The flowviewer has the ability to block the IP addresses that doing intrusion. The flowviewer also has the "automatic bypass" feature. If the hardware of firmware has damage, the system will switch to auto-bypass mode so that the network will not be effect by the Flowviewer. All models of the Flowviewer have this build-in feature from 2008.

Generally speaking, we will suggest our customers to deploy the Flowviewer between the router and the core switch. If they have IPS devices, we will suggest them to deploy the Flowviewer between the IPS and the core switch. It is because the most network paralysis event was caused by the relay attack from external IP addresses. We will use some real cases to prove that.



FM-1500A Instruction of Inline Mode

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.

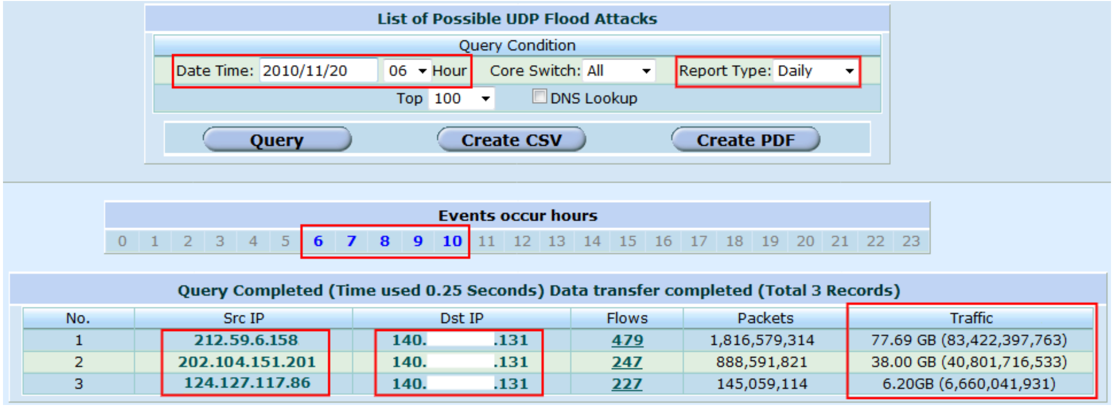
The FM-1500A will block the hackers automatically by sending the ACL commands to the switch while they try to attack the intranet. Therefore, the abnormal traffic cannot enter the intranet.

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

There are two ways that hackers can use to paralyze the network:

1. UDP Flood Attack:

   The device which be implant a Trojan horse will produce a number of UDP packets to attack the target. That will cause the network paralysis. The following figure shows a real case which happened on November 29, 2010. An internal IP of a university was attacked by three foreign IPs: 212.59.6.158 (Lithuania), 202.104.151.201 (China) and 124.127.117.86 (China) via UDP Flood Attack. This attack caused the entire campus network paralyzed.



List of Possible UDP Flood Attacks

Query Condition

Date Time: 2010/11/20 06 Hour Core Switch: All Report Type: Daily

Top 100 □DNS Lookup

Events occur hours

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

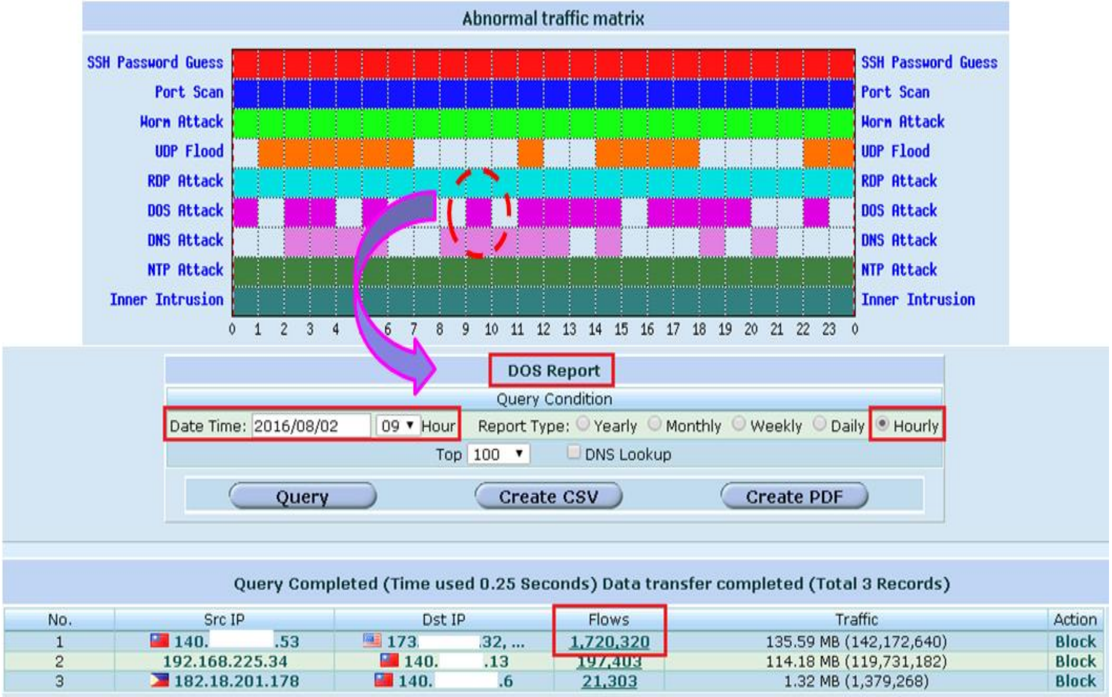
Query Completed (Time used 0.25 Seconds) Data transfer completed (Total 3 Records)

No.	Src IP	Dst IP	Flows	Packets	Traffic
1	212.59.6.158	140.[redacted].131	479	1,816,579,314	77.69 GB (83,422,397,763)
2	202.104.151.201	140.[redacted].131	247	888,591,821	38.00 GB (40,801,716,533)
3	124.127.117.86	140.[redacted].131	227	145,059,114	6.20GB (6,660,041,931)

From the report of the Flowviewer, you can see which IP launched the UDP flood attack. The only way to solve this problem is to notify your ISP to block these IP addresses so that your network bandwidth will not be consumed by those UPD packets. There is no way that your device can handle those packets do not through it. This is the only way to solve the network congestion problem.

2. DOS Attack:

The device which be implant a Trojan horse will produce a number of session to attack the target. Due to the amount of packets/requests, the device/server will end up with crashed. The following figure shows a real case. In this case, the fist entry was used to relay attack and generated 1,720,320 sessions (flows). It caused the hardware performance was consumed rapidly. For example, the high CPU usage of core switch will affect the performance of packet exchange. If the system of core switch crashes, the network will be paralyzed.



Date Time: 2016/08/02 09 Hour Report Type: ○ Yearly ○ Monthly ○ Weekly ○ Daily ● Hourly

Top 100 □ DNS Lookup

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

No.	Src IP	Dst IP	Flows	Traffic	Action
1	140.[redacted].53	173.[redacted].32, ...	1,720,320	135.59 MB (142,172,640)	Block
2	192.168.225.34	140.[redacted].13	197,403	114.18 MB (119,731,182)	Block
3	182.18.201.178	140.[redacted].6	21,303	1.32 MB (1,379,268)	Block

Once the Flowviewer detects the DoS attack, it will know which IP address launches the attack and then automatically send the ACL commands to the core switch to block it. By applying the deny commands in the inbound direction to avoid these anomalous sessions (flows) consuming the CPU resource of core switch. The device of IPS uses the threshold to determine which traffic is cyber-attack. It monitors the packets that through it and counts the number every second. For media stream, it is easy causing false positives. While the attack with the amount of session, the hardware performance will be consumed rapidly. Finally, the system will end up with crashed.

The Real-time query feature:

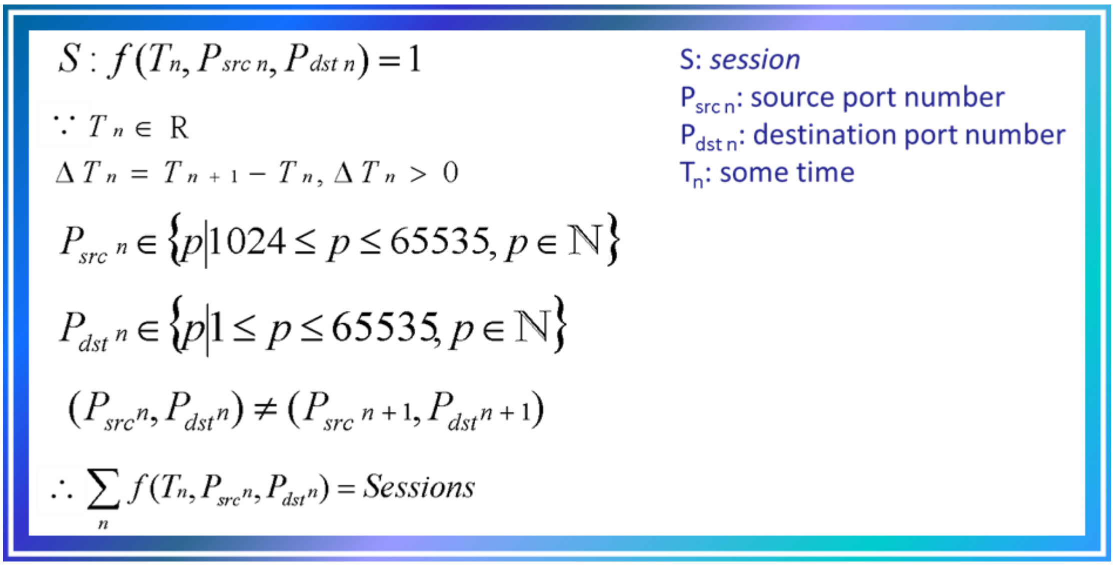
The users can use this feature to search the historical record of a specific IP within a particular period of time. It can also be used as the digital evidence. The police can use it to track down the cybercriminals. The result can be shown within 30 seconds if the time range is less than 6 hours. If you want to search the historical record of a specific IP over a very long period of time (more than 3 months) , you can use the "batch query" function to do that. Because it will take more time to complete the query, we use the queues to process the query. After the query completed, the users can click the "view" to see the result.

On the basis of those facts we can reach the following conclusion:

A. The Flowviewer which deployed in inline mode will not actively process the packets and sessions that through it. In network architecture, the Flowviewer is just like a wire. The Flowviewer takes action when it detected the port scan, worm, the intrusion of SSH/RDP and other cyber intrusions. It will block those cyber-attacks/intrusions by IP. That means it does not need to check the content of packets. That is the reason why the huge traffic will not affect it.

B. We developed the mathematical algorithms that can sort those random packets according by the IP address. The Flowviewer will analyze the collective Netflow every five minute and can distinguish it is cyber-attack or not within 1 second. If it is anomalous traffic, the Flowviewer will automatically start the blocking function.

According to our observation, the most attacks are relay attack. The hackers attack the external target with the amount of packets. As the result, these packets will saturate the bandwidth of the network. The network will be paralyzed in the end. Take the cases of NYSE and United Airlines as an example; we believe there's a high probability that their bandwidth of the network were used to do the relay attack if they did not receive the blackmail. 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.



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

$$\because T_n \in R$$

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

$$P_{src}\,n \in \{p | 1024 \le p \le 65535, p \in \mathbb{N}\}$$

$$P_{dst}\,n \in \{p | 1 \le p \le 65535, p \in \mathbb{N}\}$$

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

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

S: *session*

$P_{src\,n}$: source port number

$P_{dst\,n}$: destination port number

T_n: some time

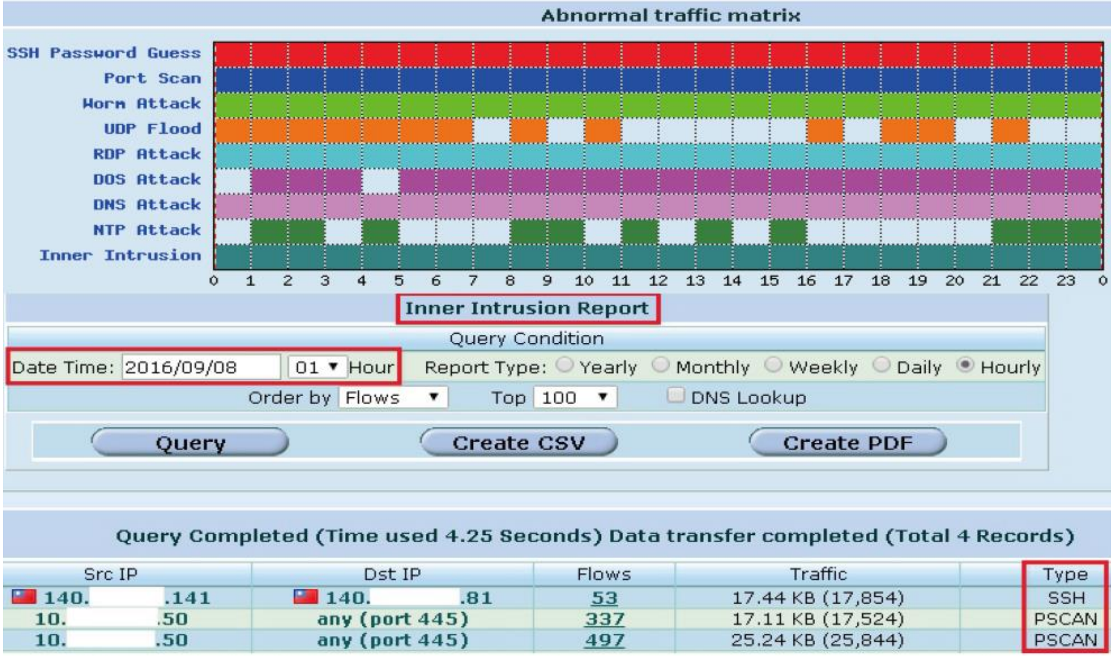
We have a simple explanation of the above equation. You can watch it on YouTube:
https://www.youtube.com/watch?v=yX_wp2oedYM
There is a video about" Simulate hacker attack_ Top 6 ways of hack attacks and how to protect".
https://www.youtube.com/watch?v=vKweWU82okI

The inner intrusion detection feature:

The Inner Intrusion detection function is unique and available only in Flowviewer. This function can guard against the intrusions from intranet to intranet. It is very useful to the units that use closed network system such as political network, military network and financial (ATM system) network. Few years ago, the user information of Facebook was stolen by hackers. The user information of Facebook was stolen because one staff who worked inside downloaded an APP which was infected by hackers. Fortunately, there is no confidential data/user information on this computer. Infect, the enterprises prefer to store these data in the specific servers, not a personal computer. So hackers would use this computer as a tool to intrude other machines in the intranet until they found the user information. Unfortunately, the most products of IPS only focus on the attack/intrusion from outside. That means the intrusion from intranet to intranet is the weakest link. We call this type of intrusions: inner intrusion. It is a very serious problem that cannot be ignored.

Take the First Commercial Bank in Taiwan heists as an example, the police traced the IP address and then found out the IP belongs to the England branch of the First Commercial Bank. This hacker/co-worker is not stupid, he must through other branches of the First Commercial Bank in other countries to do the relay intrusion so that it could make him invisible. The First Commercial Bank did not purchase the network reporting appliance with the feature that can dynamically query the information of a specific IP address. As the result, the police did not find the people who cooperate with the hacker. They can only arrest the people who took money because the CCTV shows their faces. This case shows the importance of the detecting the inner intrusion.

A unit belongs to intelligence agency in Taiwan used the Flowviewer to find out the malicious employee who worked inside. As following figure shown, it can prove that the Flowviewer has the ability to detect and block the intrusions from inside.



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

Conclusion:

To put it briefly, we can know the device with signature technology needs to compare the packet contents with the signature so that it can determine the traffic is the attack/intrusion or not. When it faces the amount of traffic, the main problem is that the performance of hardware will be consumed rapidly. Finally, the system will end up with crashed. The device that analyzes the Netflow will not cause this problem. The hackers know the weaknesses and the vulnerabilities of the IPS products. That is the reason why they always use the latest version of program to intrude/attack the network of political units, the military units and the finance units. If you want to know more about the Flowviewer, you can contact us via email: info@curelan.com