NetFlow y su aplicación en seguridad

NetFlow and its use in security

Chelo Malagón

Resumen

El protocolo abierto NetFlow, desarrollado por CISCO System, ha demostrado ser muy útil en el trabajo diario de los técnicos de red, ya que permite monitorizar y representar el tráfico de red en tiempo real, pero también es una herramienta esencial para los técnicos de seguridad que pueden utilizar la información de los registros NetFlow recibidos de los dispositivos capaces de exportar esta información para analizar y detectar ataques y anomalías de seguridad, aumentando así su proactividad y su capacidad de operación y respuesta.

En este artículo, se presentará brevemente el protocolo NetFlow y los elementos necesarios para establecer una infraestructura de recolección y análisis de tráfico necesaria para el uso de esta tecnología como apoyo al trabajo diario de los técnicos de seguridad.

Para finalizar, comentaremos el estado actual de la infraestructura puesta en producción en RedIRIS por el equipo de seguridad.

Palabras clave: Netflow, monitorización, análisis forense, detección, seguridad, NFSen, ataques de seguridad, anomalías de seguridad.

Summary

NetFlow, an open protocol developed by Cisco, has proven to be useful in the day to day work of network engineering given its ability to present network traffic in near real-time, as well as being an essential tool for security engineers who can use the information presented by NetFlow to analyse and detect security attacks and anomalies, helping them to be more proactive and improving their operational and response capabilities.

In this article NetFlow is presented along with the elements necessary to create the collection and analysis infrastructure to be able to use Netflow in the daily work of security engineering.

We finish by discussing the current state of the use of the technology by the RedIRIS security team.

Keywords: NetFlow, monitoring, forensic, detection, security, NFSen, security attacks, security anomalies

NetFlow es un protocolo abierto desarrollado por Darren Kerr y Barry Bruins de CISCO Systems

Esta tecnología describe la manera en la que se exportan estadísticas sobre el tráfico de red mediante registros denominados flujos

1. Tecnología NetFlow

NetFlow es un protocolo abierto desarrollado por Darren Kerr y Barry Bruins, de CISCO Systems, que permite la recolección de tráfico de red.

La tecnología NetFlow describe la manera en la que un router y/o un switch inteligente exporta estadísticas sobre el tráfico que pasa por el mismo, mediante la generación de registros NetFlow (denominados flujos) que se exportan vía datagramas UDP a un dispositivo o máquina recolectora. La capacidad de exportar flujos está disponible no sólo en la mayoría de routers CISCO, sino también en otros muchos fabricantes (Juniper, Riverstone, etc.)(1)

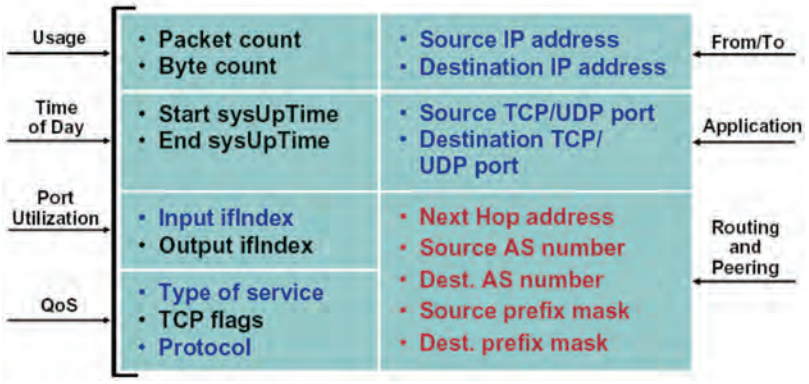
Un flujo es una secuencia unidireccional de paquetes con ciertas características comunes: dirección IP origen/destino, puerto origen/destino para TCP y UDP (tipo y código para ICMP ó 0 para otros protocolos), número de protocolo de nivel 3, ToS (Type of Service) e índice del interface de entrada.

Dependiendo de la versión de NetFlow utilizada al exportar flujos, los datagramas de exportación contendrán otros campos adicionales.

La versión de exportación NetFlow más utilizada hoy en día es la versión 5 del protocolo. Esta versión agregó información sobre sistemas autónomos (BGP) y números de secuencia a la primera versión (v1) aparecida en 1996, y ya prácticamente en desuso.(2)

La **Figura 1** muestra un ejemplo de los campos contenidos en el datagrama de exportación para la versión 5.

FIGURA 1. DATAGRAMA DE EXPORTACIÓN NETFLOW V5



Las versiones de exportación de NetFlow más utilizadas hoy en día son la versión 5 y la 9 del protocolo

Tras las versión 5, la versión más utilizada hoy en día en el mercado es la versión 9. Esta versión está basada en plantillas, permitiendo varios formatos para los registros NetFlow, siendo así mucho más flexible y extensible. Las descripción de la plantilla utilizada es pasada por el dispositivo exportador al dispositivo colector que debe ser capaz de entenderla. Además, incluye etiquetas MPLS, direcciones y puertos IPv6 y permite agregación en los routers. El RFC 3954 [1], documenta en profundidad esta versión del protocolo.

Los registros NetFlow no contienen información del usuario, sino datos de conexión, lo que permite tener una visión detallada del comportamiento de nuestra red

Aunque como hemos dicho, inicialmente el protocolo NetFlow fue implementado por CISCO, la necesidad de un protocolo estándar y universal que permita la exportación de información de flujos de red desde distintos dispositivos de red, ha hecho que NetFlow haya emergido como un estándar en la IETF (mediante el Grupo de Trabajo IPFIX (Internet Protocol Flow Information eXport) [2]). Originalmente definido en el RFC3917 [3], IPFIX se basa en la versión 9 del protocolo NetFlow, y aunque todavía no ha sido ampliamente desplegado, poco a poco los vendedores de equipamiento de red están añadiendo soporte IPFIX a sus dispositivos.

Un punto muy importante a reseñar sobre los registros NetFlow es que éstos no contienen información del usuario, sólo datos de conexión, lo que permite tener una visión detallada del comportamiento de toda nuestra red (tanto para la monitorización como para el análisis efectivo de dicho tráfico), evitando problemas relacionados con la privacidad de los usuarios.

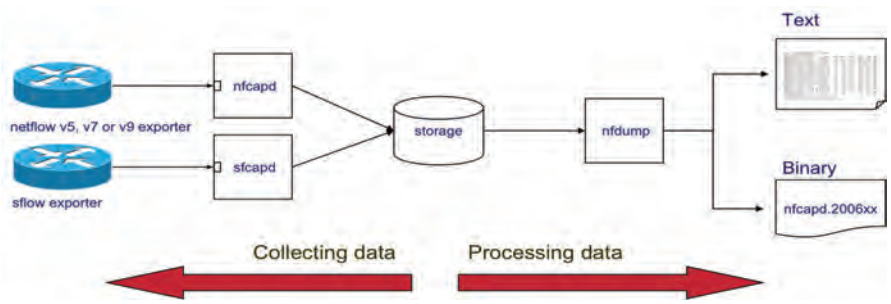
2. Componentes de una arquitectura básica para la monitorización y análisis de tráfico basada en Netflow

Se distinguen tres componentes básicos en toda arquitectura de monitorización/análisis de tráfico basada en esta tecnología:

- **Exportador.** Router o switch capaz de generar registros NetFlow, que se exportarán a un colector vía UDP.
- **Colector.** Dispositivo que escucha en un puerto UDP determinado, y que es capaz de almacenar o reenviar los flujos recibidos a otros colectores según la arquitectura definida.
- **Analizador.** Encargado de filtrar, mostrar, analizar y/o visualizar los flujos recibidos.

Exportador, Colector y Analizador son los tres componentes básicos en una arquitectura de monitorización y análisis de tráfico basada en Netflow

FIGURA 2. ARQUITECTURA DE MONITORIZACIÓN Y ANÁLISIS BASADA EN EL USO DE NFDUMP/NFSEN



Los exportadores operan construyendo una caché (flow cache) que contiene información sobre todos los flujos activos que pasan por el dispositivo. Cada flujo está representado por un registro de flujo (flow record), que contiene una serie de campos de información que luego se utilizarán para exportar datos al colector. Un registro de flujo se actualiza cada vez que se conmutan los paquetes pertenecientes al flujo, llevando una cuenta de los paquetes y bytes por flujo.

Los exportadores operan construyendo una caché que contiene información sobre todos los flujos activos que pasan por el dispositivo

Sin embargo, con las velocidades actuales en muchos casos no es posible, en cuanto a recursos, capturar y actualizar los contadores por cada paquete en cada flujo. Es por ello que para evitar la carga de la CPU en los dispositivos exportadores, en muchas ocasiones se utiliza sampleado o muestreo(3) en los routers. Sin embargo el uso de un sampling distinto a 1/1 nos proporciona una imagen inexacta del tráfico que circula por nuestra red y no es nada recomendable si vamos a usar los flujos para la detección y análisis de ataques de seguridad, aumentando además la complejidad a la hora de obtener estadísticas precisas de tráfico.

Otra solución a este inconveniente de carga de la CPU de los exportadores es la utilización de tarjetas especiales y dispositivos de monitorización pasiva de red, independientes de conmutadores y routers, como el FlowMoon Probe desarrollado por CESNET [4].

Los registros de flujo expiran de la caché según una serie de criterios, algunos de ellos configurables en el dispositivo.

Estos criterios son:

- Cuando las conexiones TCP llegan a su fin (Flag FIN) o son reseteadas (se recibe un flag RST).
- Los flujos han estado inactivos por un tiempo determinado (parámetro configurable. Normalmente 15 segundos).
- La caché se llena o el router se queda sin recursos.
- Los flujos se mantienen activos en caché por un tiempo determinado (parámetro configurable. Normalmente 30 minutos). Una vez pasado este tiempo expiran de la caché, así se asegura un reporte periódico. El envío se hace más frecuente si aumenta el tráfico de las interfaces configuradas con NetFlow.

Todos los registros de flujos que han expirado en la caché se adjuntan en un datagrama de exportación UDP, que típicamente contendrá entre 20 y 50 registros. Este datagrama se envía a un puerto determinado al dispositivo colector configurado.

Para la colección y análisis de los flujos recibidos de los dispositivos de red se pueden utilizar diversos productos disponibles en el mercado tanto de libre distribución como comerciales. SWITCH mantiene un listado bastante completo de herramientas para la recolección y análisis de flujos de red [5]. Casi todas las herramientas en el mercado dan soporte a las principales versiones del protocolo descritas anteriormente.

El uso de NetFlow es de gran utilidad para múltiples fines relacionados con la monitorización, comprobación y representación de tráfico de red y el triplete measurement, accounting y biling

3. Aplicación de la tecnología NetFlow en seguridad

El uso de NetFlow se ha demostrado de gran utilidad para múltiples fines relacionados con la monitorización, comprobación(4) y representación(5) de tráfico de red y el triplete measurement, accounting y billing.

Pero aparte de esta aplicación relacionada puramente con la operación de red, los técnicos de seguridad están continuamente haciéndose una serie de preguntas, para cuya respuesta se puede utilizar la información que nos proporciona NetFlow. Se trata de preguntas del tipo: "¿Se ha detectado en mi red este pico en el puerto X?", "¿Cómo se está propagando el malware Y en mi red?", "¿Se detecta tráfico relacionado con el incidente Z?", "¿Cómo puedo investigar este ataque de DoS?, "¿Qué hosts/subredes consumen más ancho de banda en mi red?", etc.

La tecnología NetFlow es útil para la investigación de incidentes y para la detección proactiva de ataques y anomalías de seguridad

La monitorización tradicional usando estadísticas del tráfico de los distintos enlaces (MRTG, RRD, Cricket, ect...) no es suficiente para contestar estas preguntas ya que no nos proporcionan información lo suficientemente detallada. Para contestarlas, necesitamos disponer de información a nivel de conexión (puertos, flags TCP, etc.). Esta información nos la proporciona NetFlow de una forma sencilla.

Si bien es cierto que existen diversas técnicas de monitorización y detección de ataques de seguridad (IDSs, Firewalls, etc.), la tecnología NetFlow está demostrando cada vez más su utilidad en seguridad, tanto en la investigación de incidentes (análisis forense), como en la detección proactiva de ataques y anomalías.

Frente al uso de IDSs y otros mecanismos de detección perimetrales, NetFlow proporciona una serie de ventajas entre las que podemos destacar:

- Dado que la mayoría de dispositivos de red tienen la capacidad de exportar registros NetFlow, la monitorización se puede realizar desde cualquier router de nuestra infraestructura, no sólo en los routers de acceso a Internet donde normalmente se ubican IDSs y Firewalls, teniendo así además una vista única del tráfico total de la red a nivel de infraestructura.

- A diferencia de los IDSs, en la monitorización utilizando NetFlow no se tiene acceso a información confidencial, ya que los flujos no contienen información del usuario, sólo datos de conexión. Esta es una de las mayores ventajas de esta tecnología. Además hace que la inspección de los paquetes sea mucho más rápida al contener sólo perfiles de tráfico(6) . El uso de NetFlow en entornos de redes de alta velocidad o con mucho tráfico se hace pues especialmente recomendable.

- En análisis de registros NetFlow basado en algoritmos de aprendizaje lo hace especialmente útil en la detección de ataques de "0-day" o mutaciones de ataques para los que la detección basada en firmas no es válida.

Es fundamental que los exportadores no tengan configurado muestreo de los flujos para que el almacenamiento de la información sea lo más detallado, fiel y útil posible

Lo que es necesario recalcar para la utilización de NetFlow como apoyo al trabajo diario de los técnicos de seguridad (tanto para detección como para análisis) es que es fundamental que los exportadores no tengan configurado muestreo de los flujos (o al menos que éste sea lo más cercano a 1/1) para que el almacenamiento de la información de los flujos sea lo más detallado, fiel y útil posible.

NetFlow para análisis forense

NetFlow proporciona un apoyo adicional al trabajo diario de los técnicos de seguridad a la hora de realizar análisis forense sobre incidentes(7) , ya que nos permite almacenar información adicional relativa al tráfico de red que nos ayuda en este menester.

Esta información puede estar almacenada on-line o off-line, siendo imprescindible el uso de una herramienta de recolección, almacenamiento y análisis de flujos con posibilidad de búsquedas preferiblemente vía línea de comandos para realizar consultas extensas (flow-tools, nfdump, etc. [5]). Normalmente, se programan scripts específicos que faciliten las búsquedas para este propósito.

NetFlow permite detectar, en tiempo real, ataques que se producen en la red

NetFlow para la detección de ataques y anomalías

NetFlow permite detectar, en tiempo real, ataques que se producen en nuestra red (equipos posiblemente comprometidos, conexión hacía servidores de C&C de botnets conocidas, envío de información a keyloggers, DoS/DDoS, escaneos de puertos y redes, infecciones específicas de determinados gusanos, SPAM, por poner algunos ejemplos).

Existen varios métodos de análisis de flujos para detección de ataques y anomalías de seguridad. Estos métodos se describen a continuación.

Un primer método consiste en un **análisis básico del tráfico**. Se trata de un modelo que se basa en describir qué actividad es "normal" en nuestra red(8) de acuerdo a patrones históricos de tráfico, de manera que cualquier otro tipo de tráfico se marca como malicioso. La forma más básica de realizar esta tarea es mediante el uso de estadísticas e informes de datos y sesiones (estadísticas TopN). Otras técnicas más sofisticadas y complejas son las basadas en métodos heurísticos y algoritmos de aprendizaje.

Para ilustrar este método de análisis pongamos un par de ejemplos:

- Normalmente un equipo mantiene un ritmo más o menos frecuente de conexiones a lo largo del tiempo (dependiendo de su función y los servicios que proporcione), pero si

sufre por ejemplo la infección de un gusano, su comportamiento varía drásticamente, pudiéndose observar un volumen anormalmente alto de conexiones a otro u otros equipos o redes. Esto mismo ocurre con otro tipo de ataques como escaneos de red y puertos, DoS/DDoS o SPAM, que se pueden detectar utilizando esta misma filosofía.

- La detección de grandes transferencias de tráfico en determinados periodos de tiempo desde un equipo a otro o a varios equipos, es otro ejemplo de cómo se puede realizar detección básica. Esta técnica, sin embargo puede ser bastante inexacta en entornos académicos debido al gran número de máquinas que pueden ser susceptibles de realizar estas grandes transferencias de manera legal.

Uno de los problemas asociados con el análisis básico de tráfico es precisamente determinar lo que es "normal" en nuestra red y cuales son los umbrales de sensibilidad apropiados. Esto último está relacionado con la eliminación de falsos positivos/negativos y las avalanchas de alertas difíciles de manejar y que consumen muchos recursos para su gestión y comprobación. Debemos tener en cuenta que la inspección y análisis de tráfico necesario para comprobar que un ataque no es realmente un falso positivo, es costoso y que consume recursos. Además, en la mayoría de los casos este análisis no se puede automatizar si se quiere dar un servicio de detección de calidad (9), necesitando un operador que realice esta tarea a mano.

Uno de los problemas asociados con el análisis básico de tráfico es determinar lo que es "normal" en la red y cuales son los umbrales de sensibilidad

Otro método de detección de ataques de seguridad muy extendido es el **basado en expresiones regulares**. Cualquier campo de los incluidos en los registros NetFlow es susceptible de ser utilizado en una búsqueda (normalmente incluida en un script) utilizando expresiones regulares (puertos, IPs, duración del flujo, bpp, Flags, etc.).

Por poner un ejemplo, puede ser muy útil obtener una visión más granular de la actividad anormal de nuestra red mediante un análisis más preciso de los flujos basado en los Flags TCP (por ejemplo para detectar ataques SYN, Null y/o XMAS scans) o en el tipo/código ICMP incluido en los registros.

En contraposición, la escritura de expresiones regulares para la generación de alertas no es nada trivial y necesita ser adaptado a las características específicas de nuestra red. Es por tanto todo un arte. Las expresiones regulares pueden llegar a ser realmente complejas y necesitar revisión continua para su adecuación a la evolución lógica del tráfico de nuestra red.

Otros métodos de detección de ataques de seguridad son los basados en expresiones regulares y en algoritmos de aprendizaje y data mining

Con los dos métodos descritos anteriormente es muchas veces complicado detectar infecciones y escaneos no agresivos y más silenciosos, como los que se sufren hoy en día. Para detectar este tipo de ataques es conveniente introducir otros métodos más sofisticados y complejos de detección basados también en la determinación de cual es el tráfico "normal" en nuestra red pero mediante el uso de inteligencia adicional **basada en algoritmos de aprendizaje y data mining** (por ejemplo basados en entropía). Cada vez hay más las herramientas disponibles en el mercado para la detección de anomalías basadas en esta inteligencia (Sentinel, NetReflex, QRadar, NARUS, etc., por mencionar algunos), que sin duda nos permiten una detección complementaria a la tradicional basada en sesiones/datos TopN, umbrales y expresiones regulares.

FIGURA 3. DETECCIÓN DE CANDIDATOS A PORT SCAN UTILIZANDO NETFLOW

Show port scanning candidates:

```
forth% nfdump -r /data/rx/nfcapd.200603300150 -K 123… -A srcip,dstport -s record/packets 'not proto icmp and bytes < 10(
    and bpp < 100 and packets < 5 and not port 80 and not port 53 and not port 110 and not port 123'
Aggregated flows 72506
Top 10 flows ordered by packets:
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes      bps Flows
2006-03-30 01:49:23.800   243.842 TCP      [redacted]:0     ->       0.0.0.0:4899    142172    6.5 M   223891 71151
2006-03-30 01:50:48.663   236.035 TCP      [redacted]:0     ->       0.0.0.0:5900     36452    1.6 M    56049 17232
2006-03-30 01:52:30.169   143.944 TCP      [redacted]:0     ->       0.0.0.0:41523     9982  479136    26629  5143
2006-03-30 01:49:22.650   303.173 TCP      [redacted]:0     ->       0.0.0.0:1433      4638  222624     5874  2319
2006-03-30 01:49:53.945   299.401 TCP      [redacted]:0     ->       0.0.0.0:135       3273  157104     4197  3273
2006-03-30 01:49:27.196   194.565 TCP      [redacted]:0     ->       0.0.0.0:139       1845   88560     3641  1613
2006-03-30 01:52:05.471    96.768 TCP      [redacted]:0     ->       0.0.0.0:445       1678   80544     6658   954
2006-03-30 01:49:54.012   300.038 UDP      [redacted]:0     ->       0.0.0.0:137       1471  114738     3059  1471
2006-03-30 01:49:22.970   328.838 TCP      [redacted]:0     ->       0.0.0.0:135       1432   68736     1672  1677
2006-03-30 01:53:00.822   112.524 TCP      [redacted]:0     ->       0.0.0.0:135       1254   60192     4279  1254

IP addresses anonymized
Time window: 2006-03-30 01:34:53 - 2006-03-30 01:54:57
Total flows: 1178835 matched: 245494, skipped: 0, Bytes read: 57559680
Sys: 0.634s flows/second: 1856716.7   Wall: 0.632s flows/second: 1862657.6
```

4. Monitorización de flujos de red en el área de seguridad de RedIRIS

Desde mediados del año 2006, el equipo de seguridad de RedIRIS (IRIS-CERT [6]), utiliza, entre otras tecnologías disponibles, NetFlow para el soporte en su actividad diaria, tanto para obtención de estadísticas e informes TopN, como para la realización de análisis forense sobre incidentes y la detección de ataques.

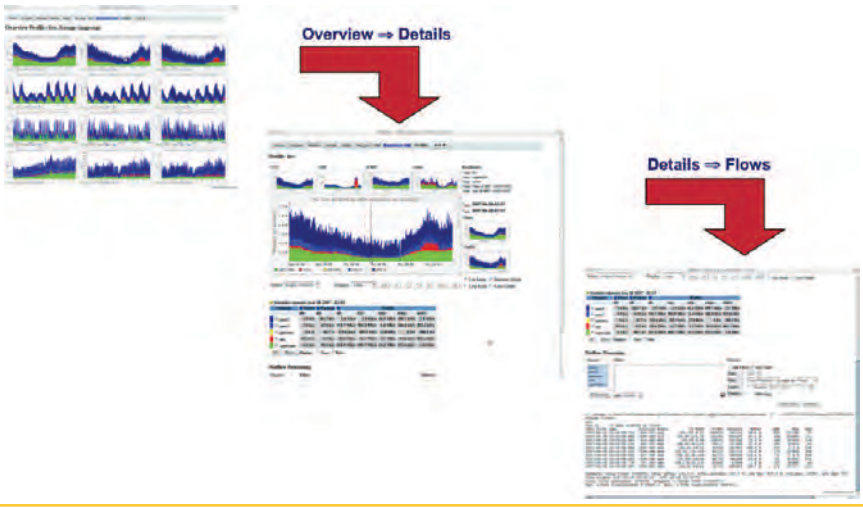
Todo comenzó con la participación de RedIRIS en el JRA2 (Security) [7] de Géant2 [8], donde estuvimos involucrados en la definición de un conjunto integrado de herramientas para la monitorización de tráfico de red para la detección de ataques y anomalías. Tras un periodo de evaluación de diversas herramientas, el NFSen, desarrollado por SWITCH [9], se eligió como parte de este ToolSet y fue puesto en producción en RedIRIS.

NFSen es una herramienta de recolección y análisis de flujos, que muestra gráficamente la situación actual de la red (desde vistas generales, por flujos/paquetes/tráfico, hasta un análisis de flujos específicos). Además, entre sus características principales se encuentran: la definición de vistas específicas sobre los datos almacenados (profiles), la realización de análisis de flujos en ventanas específicas de tiempo (vía Web y por línea de comandos), el post-procesado automático de flujos para la generación de informes y alertas, y la posibilidad de incluir extensiones flexibles usando plugins (tanto de frontend como de backend).

NfSen es una herramienta de recolección y análisis de flujos que muestra gráficamente la situación actual de la red

El NfSen recoge los flujos de todos los routers del backbone de RedIRIS almacenándose aproximadamente 4 meses de flujos en crudo para su análisis histórico

FIGURA 4. NFSEN



En la actualidad el NfSen recoge los flujos de todos los routers del backbone de RedIRIS, almacenándose aproximadamente 4 meses de flujos en crudo para su análisis histórico.

Utilizamos una máquina Dual Core AMD Opteron Processor 2210, con 1 GHz cada procesador y 8 G de memoria, con sistema operativo Red Hat Enterprise Linux. El almacenamiento de los datos en crudo se realiza en un Filer, disponiendo actualmente de 3 T de espacio.

Sobre los datos recogidos, se obtienen estadísticas internas de tráfico y utilización de la red para su uso interno. Por un lado se disponen de estadísticas diarias vía Web que muestran, por cada uno de los routers de nuestro backbone, el Top1000 de tráfico por IP fuente, IP destino, AS fuente y destino, y de clase C fuente y destino. Cada una de estas estadísticas está ordenada a su vez por bytes, flujos y paquetes, y muestran además información acerca del puesto que ocupaba una IP, red, AS en el ranking presentado el día anterior. Actualmente se guardan este tipo de estadísticas para los últimos 7 días.

En la actualidad se generan diferentes estadísticas internas de tráfico y utilización de la red que nos permiten tener una visión general de la misma

Además de éstas, se reciben por correo estadísticas top10 diarias sobre todo el tráfico de la red por clases C origen, IP origen, puerto destino y protocolo, así como un listado diario de aquellas máquinas que realizan mayores transferencias de datos y que consumen mayor ancho de banda en nuestra red.

Se dispone también de un plugin que realiza un seguimiento de los puertos más utilizados en nuestra red (PortTracker, disponible en la distribución básica del NfSen), y cuyas gráficas se pueden consultar vía Web.

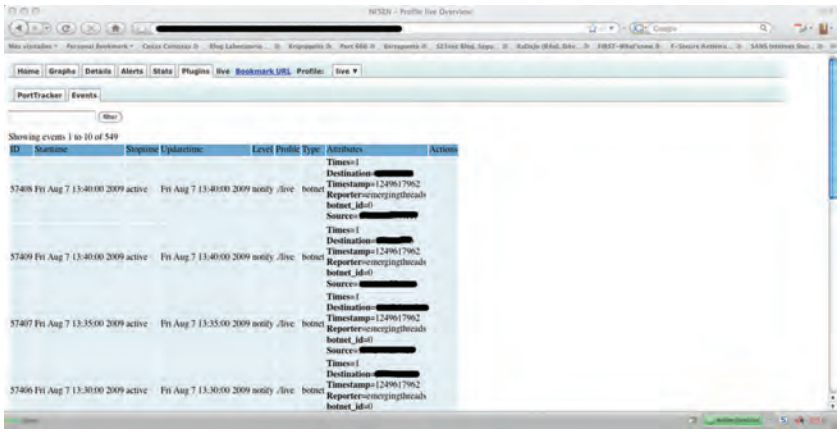
FIGURA 5. ESTADÍSTICAS DE TRÁFICO POR ROUTER DE REDIRIS

La detección de ataques y máquinas comprometidas se realiza mediante plugins específicos

La detección de ataques y máquinas comprometidas se realiza mediante plugins específicos. En la actualidad estos plugins nos permiten detectar máquinas de nuestra comunidad que realizan escaneos de puertos y redes (y que por tanto pueden estar comprometidas), así como máquinas, también en nuestra comunidad, que se conectan a servidores de Command&Control de botnets, de las que tenemos noticia desde distintas fuentes.

Los datos recogidos por estos plugins son redirigidos a un correlador denominado DesconII [10] desarrollado por la Universidad Carlos III de Madrid, que permite relacionar las alertas y determinar umbrales por encima de los cuales se considera que un conjunto de alertas puede constituir un incidente que será entonces gestionado y procesado por el CERT, vía RTIR.

FIGURA 6. NFSEN PLUGINS



Para finalizar, actualmente el equipo de seguridad de RedIRIS está inmerso en un proyecto para investigar la aplicabilidad de los flujos de red en la detección proactiva de anomalías de seguridad y ataques, estudiando y evaluando diferentes herramientas entre las que se encuentran el NetReflex, el QRadar o el módulo de análisis de flujos del DSCC (Dragon Security Command Console). Este proyecto tiene como fin el complementar la detección tradicional que en este momento se está realizando basada en los plugins que están en producción, pasando así a una detección más avanzada.

El equipo de seguridad de RedIRIS está inmerso en un proyecto para investigar la aplicabilidad de los flujos de red en la detección proactiva de anomalías de seguridad y ataques

5. Referencias

[1] *http://www.ietf.org/rfc/rfc3954.txt*
[2] *http://www.ietf.org/dyn/wg/charter/ipfix-charter.html*
[3] *http://www.ietf.org/rfc/rfc3917.txt*
[4] *http://www.flowmon.org/*
[5] *http://www.switch.ch/network/projects/completed/TF-NGN/floma/software.html*
[6] *http://www.rediris.es/cert*
[7] *http://www.geant2.net/server/show/nav.755*
[8] *http://www.geant2.net/*
[9] *http://sourceforge.net/projects/nfsen/*
[10] *http://nuberu.uc3m.es/cgi-bin/viewvc.cgi/descon2v1/*

Notas

(1) Existen otros protocolos además de NetFlow diseñados con el mismo propósito, como cflow (Juniper), sFlow (Force10) o IPFIX (estándar de IETF y basado en NetFlow).

(2) NetFlow apareció como un upgrade que añadía una serie de funcionalidades nuevas a las series 7000 de los routers CISCO.

(3) El samping o muestreo consiste en no contabilizar todos los paquetes que se conmutan perteniecientes a un flujo, sino una muestra de los mismos (1 de cada 100 (1/100), 1 de cada 200, (1/200) etc.)

(4) Por ejemplo, comprobar que por cada interface de los routers llega el tráfico que debe llegar (rangos no permitidos haciendo tránsito hacia Internet, equipos mal configurados haciendo NAT, etc.)

(5) Por ejemplo uso de distintos protocolos, intercambio de información entre distintos ASs/PoPs, volumen de tráfico, topN, mayores productores de tráfico, etc.

(6) Si bien es cierto que NetFlow no es apto para detectar ataques basados en el contenido de los paquetes.

(7) "¿Se detecta tráfico relacionado con el incidente Z?", "¿Cómo puedo investigar este ataque de DoS?", "¿Es realmente el origen del ataque el que dice ser?",...

(8) Por interface, prefijo, protocolo y puerto, pps, bps, flujos, bytes,paquetes/sg, etc., en distintos periodos de tiempo (5 mins, 30 mins, 1 hora, 12 horas, 1 semana...), etc.

(9) En realidad esto es aplicable a cualquier método autoático de detección de ataques y anomalías.

Chelo Malagón
(chelo.malagon@rediris.es)
Equipo de seguridad IRIS-CERT
Red.es/RedIRIS