JORNADAS DE SEGURIDAD INFORMÁTICA
3ª EDICIÓN | 2019

CHACO Gobierno del Pueblo

Monitoreo de trafico de red

Ing. Alberto Cisneros
bcisneros@ecomchaco.com.ar

ECOM

POLICÍA DEL CHACO
División Cibercrimen

POLICÍA DEL CHACO

Ministerio de Seguridad Pública
Gobierno del Pueblo del Chaco

Subsecretaría de Niñez, Adolescencia y Familia
Gobierno del Pueblo del Chaco

Ministerio de Desarrollo Social
Gobierno del Pueblo del Chaco

Dirección General de Tecnologías de Información y Comunicación
Gobierno del Pueblo del Chaco

Subsecretaría de Modernización del Estado
Gobierno del Pueblo del Chaco

Secretaría General de Gobierno y Coordinación
Gobierno del Pueblo del Chaco

IPAP CHACO

CHACO Gobierno del Pueblo

Análisis de Tráfico de Red

Existen dos formas:

- Análisis de paquetes.
- Análisis de flujo.

Algunos Protocolos

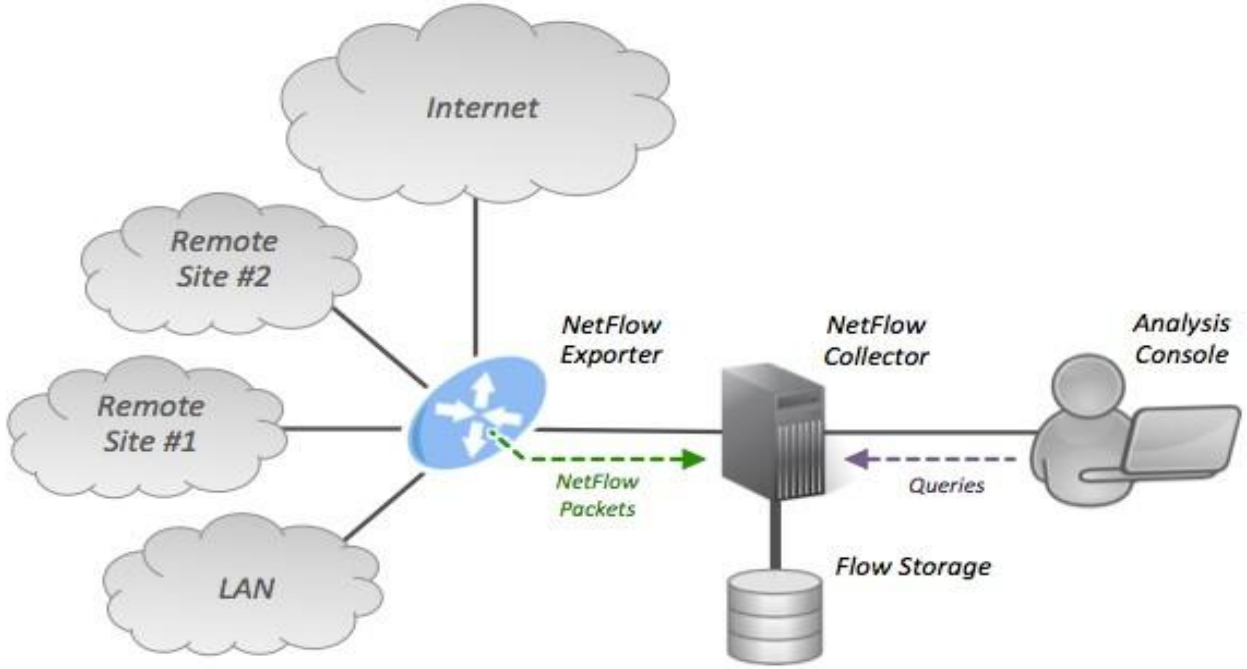
- **Netflow de Cisco**
- Jflow de Juniper
- NetStream de Huawei Technology
- Cflowd de Alcatel-Lucent
- Rflow de Ericsson
- AppFlow Citrix
- IPFIX (IETF – Pretende estandarizar el protocolo)
- sFlow (RFC 3176: recaba muestras)

Flujo de Red

Cisco: una clave séptuple en que el flujo se define como una secuencia unidireccional de paquetes que comparten los siguientes 7 valores:

Dirección IP de origen.
Dirección IP de destino.
Puerto UDP o TCP de origen.
Puerto UDP o TCP de destino.
Protocolo IP.
Interfaz (SNMP ifIndex)
Tipo de servicio IP

Arquitectura de Netflow



Análisis de Flujo de Red

- Recabar Metadatos
  - Almacenar y procesar la información.
- Análisis estadístico
- Basado en un grupo de protocolos específicos
  - Procesos de generación, almacenaje, transporte y procesamiento de los datos.
- Evaluar el trafico de la red en funcion de características comunes
- No se almacenan los datos (payload)

Netflow de Cisco

- Flujos unidireccionales.
- IPv4 unicast y multicast.
  - (IPv6 en Netflow v9)
- Flujos exportados utilizando UDP.
  - No existe un estándar en particular, aunque son de uso común 2055 y 9996.

Contabilidad de flujos

- Un resumen de todos los paquetes que se observan en un flujo (hasta el momento).
  - Identificación del flujo: protocolo, IP origen/ destino, puerto, etc
  - Conteo de paquetes.
  - Conteo de Bytes.
  - Tiempos de inicio/finalización.
  - Información adicional, como por ejemplo; números de Sistemas Autónomos (AS), máscaras de red.
- Registrar el volumen de trafico, no el contenido.

Configuración de Netflow

1) Activar el protocolo en el dispositivo de red compatible (**NetFlow Exporter**).
2) Configura qué parámetros queremos agrupar en un flujo.
3) Establece un destino a enviar los datos **'NetFlow Collector'** (nuestra herramienta de monitorización compatible con el protocolo elegido).
4) Configurar nuestro 'Netflow Collector' para recibir los datos del dispositivo de red ajustando los parámetros de versión, protocolo, etc.

Generacion de Flujos

1) En un router u otro dispositivo de red:

- Si el dispositivo lo soporta.
- No se requiera hardware adicional.
- Podría tener algún impacto en el rendimiento.

2) Colector pasivo (por lo general Unix):

- Recibe una copia de cada paquete y genera los flujos.
- Requiera un puerto espejo.
- Muchos recursos.

Recopilación en el enrutador

- Con este método se pueden observar todos los flujos en la red:
  - Pero el enrutador tiene más carga porque tiene que procesar y exportar los flujos
- Opcionalmente se pueden seleccionar para cuales interfaces se habilitara la generación de flujos, y no activarlo para las demás.
- Además, si hay enrutadores en cada segmento de red local, se puede habilitar la recopilación y exportación de flujos en esos enrutadores, y así reducir la carga en el enrutador central.

Colector Pasivo

- El colector sólo verá los flujos desde el punto de vista de la red donde se encuentra

- Tiene la ventaja de que releva al enrutador del trabajo de generar y exportar los flujos

- Útil para enlaces con un solo punto de entrada a la red, o donde sólo se requiere observar un segmento de la red.

- Se puede implementar en conjunto con un IDS.

- Ejemplos: softflowd (Linux/BSD), pfflowd (BSD),

ng_netflow (BSD)

Usos y Aplicaciones

- Puede responder a preguntas como:
  - ¿Que usuario o departamento ha estado cargando o descargando mas?
  - ¿Cuáles son los protocolos más utilizados en la red?
  - ¿Qué dispositivos están enviando más tráfico SMTP, y para dónde?
- Identificación de anomalías y ataques.
- Visualización mas minuciosa (representación grafica) que se puede hacer a nivel de interfaz.

Que mas podemos ver?

- Porcentaje de Uso de la Red.
- Distribución de los protocolos presentes en la red: Identificar los protocolos que están en uso dentro de la red.
- Consumo de los dispositivos de red.
- Tamaño de datos enviados entre dos dispositivos (MB/GB).

Que mas podemos ver?

- Equipos con más envío o recepción de paquetes.
- Protocolos mas utilizados.
- Analizar problemas en las redes, y conocer las causas y efectos de dichos problemas, verificando los datos que viajan por la red.
- Descubrir las fuentes de tráfico no deseado.

Razones para analizar el tráfico

- Monitorear la performace de la red.
- Verificar la seguridad de la red.
- Verificar las transacciones de las comunicaciones en la red.
- **Mantener un registro del tráfico (Conocer el estado “normal” de nuestra red).**

Qué necesitamos conocer para comprender los resultados de un análisis de tráfico?

- Diagrama de la red.
- Información sobre los servidores (nombre, ip, servicios, etc).
- Información sobre aplicaciones y servicios.
- Información sobre el direccionamiento.

Donde aplicar el análisis de trafico de red

A nivel WAN:

- Análisis de tráfico de ancho de banda (recurso escaso)
  - Análisis de del trafico sobre aplicaciones publicadas.
  - Detección de ataques de DoS.
  - Mal uso del ancho de banda.

A nivel LAN:

- Monitoreo y revisión del uso de recursos.
- Detección de virus o fallas internas (broadcast excesivos).
- Utilización del ancho de banda interno.

Monitoreo de trafico de red

CONSULTAS...