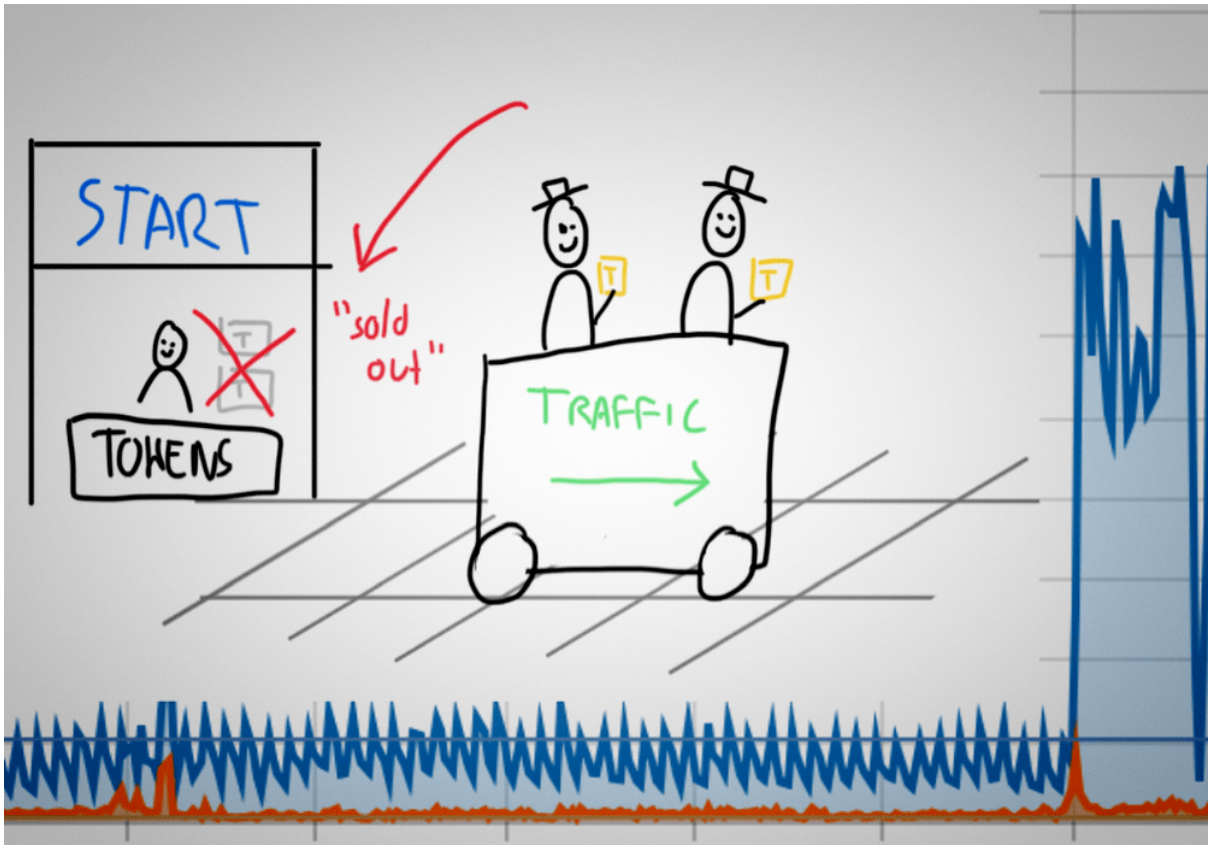
Modelado de tráfico usando iptables y tc

Limitando el ancho de banda de red saliente por dirección IP de cliente

Willem L. Middelkoop
Apr. 1, 2020



El mes pasado recibí una alerta automatizada que indicaba un uso excesivo de ancho de banda, normalmente una señal de problemas. Cuando esto sucede, se debe seguir un procedimiento estándar de incidentes, tratando de aislar la fuente del tráfico antes de cerrarlo. Sin embargo, la causa de este incidente no fue lo que esperaba... requiriendo un tipo de mitigación diferente a un simple bloqueo.

Alerta de ancho de banda excesivo

Cuando administras servidores, notarás que el tráfico de internet generalmente ocurre en patrones predecibles. Al igual que el tráfico real en las carreteras, hay momentos regulares en los que está ocupado y tranquilo.

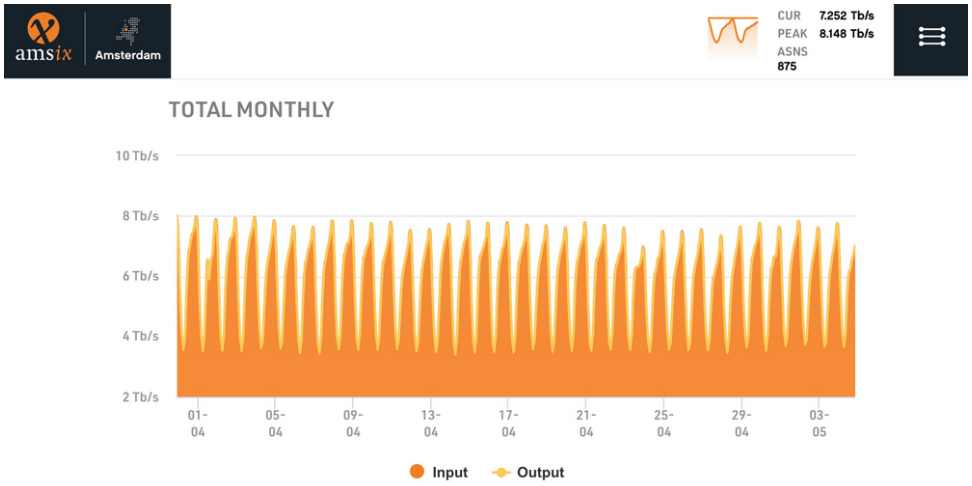


Gráfico de ancho de banda de AMS-IX muestra un patrón predecible - observe el patrón ondulatorio

El patrón predecible permite detectar anomalías automáticamente. Al igual que un atasco de tráfico en una carretera a una hora inusual puede ser el resultado de un accidente, las fluctuaciones inesperadas en el tráfico de internet pueden ser un indicador de un incidente en el ciberespacio.

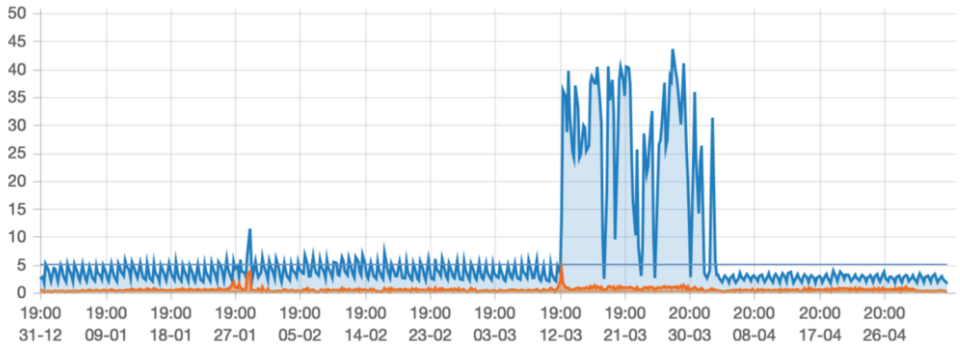


Gráfico de ancho de banda con un pico inusual que indica que algo está mal - no necesitas ser Sherlock Holmes para encontrarlo

Aislando la fuente

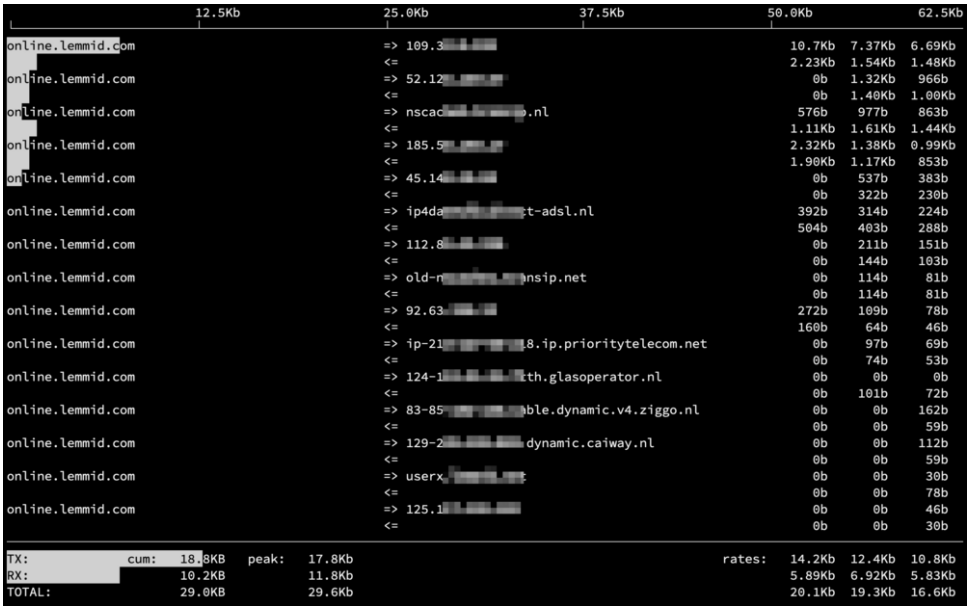
Lo primero que debes hacer es encontrar la fuente del problema. Haz esto analizando la anomalía mediante:

- Determinar si el tráfico adicional es entrante o saliente (¿subida o descarga?)
- Determinar las direcciones IP de origen y destino asociadas (¿qué servidor está afectado? ¿A dónde va o de dónde viene el tráfico?)
- Determinar el tipo de tráfico (¿correo electrónico, web o algo más?)

Para hacer esto, debes inspeccionar los gráficos de tráfico, que generalmente indican entradas/salidas distintas. Luego, debes intentar encontrar las direcciones IP afectadas. Esto podría implicar mirar más gráficos (de servidor individual) y estadísticas dentro de conmutadores, enrutadores y servidores. Luego, observa el uso de la CPU y los archivos

de registro para determinar qué aplicación está afectada, como correo o web. Cuanto mayor sea la anomalía, más fácil será encontrarla.

Puede que tengas la tentación de eliminar la anomalía una vez que la hayas encontrado, deteniendo inmediatamente el tráfico asociado. Pero realmente deberías mantenerla viva (al menos un poco más) para aprender todo lo que puedas de ella.



Usando la herramienta iftop para ver el uso de ancho de banda por dirección IP conectada

Utiliza una herramienta como iftop para ver una descripción general en tiempo real del uso del ancho de banda por dirección IP conectada. Es muy útil para comprender lo que está sucediendo, especialmente en combinación con los archivos de registro (vinculando la dirección IP a cuentas individuales).

Causa inusual

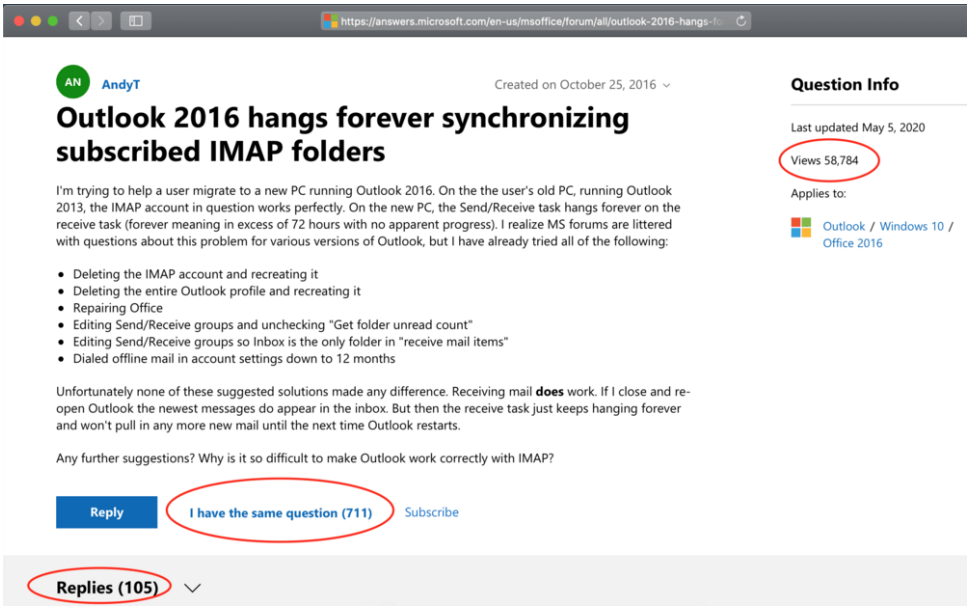
El servidor que produjo el uso excesivo de ancho de banda era un servidor de correo. A menudo, los piratas informáticos los atacan para convertirlos en un servidor de retransmisión de spam. Esto puede suceder de varias maneras, generalmente cuando los spammers capturan un inicio de sesión válido. Esto resulta en mucho tráfico saliente, ya que los spammers enviarán muchos correos electrónicos. Si se produce una ejecución de spam en tu servidor, probablemente lo veas en los registros, ya que los mensajes de spam rebotan con frecuencia, lo que hace que las colas de correo se llenen rápidamente. Se vuelve un desastre rápidamente, pero en este servidor no hubo tal desastre, solo mucho uso inusual de ancho de banda.

El correo (y el spam) se envía utilizando el protocolo SMTP, pero el tráfico en el puerto SMTP de este servidor era muy normal. Esto fue muy inusual, ya que significaba que el tráfico excesivo provenía de algo más. ¿Pero qué? Después de analizar varios archivos de registro en el servidor de correo, determiné que el protocolo infractor era IMAP. De alguna manera, un cliente conectado al servidor de correo mediante IMAP estaba causando cantidades excesivas de tráfico de red. IMAP es un protocolo que se utiliza para *leer* correo electrónico, no para enviarlo, lo que hace que las anomalías relacionadas con IMAP sean muy raras.

Al analizar el registro del servidor de correo, encontré el usuario específico que causó el tráfico. Me comuniqué con el cliente para preguntarle si había notado algo extraño de su parte. No es sorprendente que notara que su computadora se sentía un poco lenta últimamente.

Bucle de sincronización de Microsoft Outlook

Después de algunas pruebas y errores por teléfono, determinamos que algo causó que Microsoft Outlook siguiera sincronizando las carpetas IMAP en un bucle. ¡Esto provocó que su computadora descargara todo el contenido de su buzón una y otra vez! Como su buzón tenía un tamaño de más de 40 gigabytes, esto causó el tráfico sustancial. Aparentemente, esto es causado por un *bug en Microsoft Outlook*, desafortunadamente no hay una solución fácil para ello.



Errores en Microsoft Outlook hacen que siga sincronizando carpetas IMAP, un problema experimentado por mucha gente (¡vea el número de vistas!)

Mitigación mediante la conformación del tráfico

Me enfrenté a la difícil decisión de bloquear al cliente (normal, legítimo, que paga) o permitir que el tráfico excesivo continuara (incurriendo en costos serios para el proveedor de la red). Bloquear a los usuarios legítimos que operan su negocio utilizando el correo electrónico es una muy mala idea, pero permitir que continúe el tráfico excesivo también es malo. Afortunadamente, encontré una forma alternativa de reducir el tráfico excesivo y al mismo tiempo permitir que el cliente acceda a su correo (utilizando su aplicación Outlook confiable, pero defectuosa).

Conformación del tráfico

Como técnica de gestión del ancho de banda, puedes utilizar la conformación del tráfico para retrasar algunos (o todos) los paquetes de datos para que cumplan con un perfil de tráfico deseado. Si se aplica, estás, literalmente, dando forma a los gráficos de tráfico, de ahí el nombre.

Esta técnica no está exenta de controversia, ya que es todo lo contrario del principio a menudo aclamado de "*neutralidad de la red*". Con la conformación del tráfico, puedes bloquear o ralentizar intencionalmente (o cobrar dinero extra) por tipos específicos de tráfico. Por principio, estoy en contra de cualquier cosa que perjudique la neutralidad de la red, pero para esta situación particular no tenía una alternativa viable. Necesitaba ralentizar seriamente el tráfico de correo electrónico para este cliente en particular, reduciendo la cantidad de ancho de banda y al mismo tiempo brindándole acceso a su cuenta.

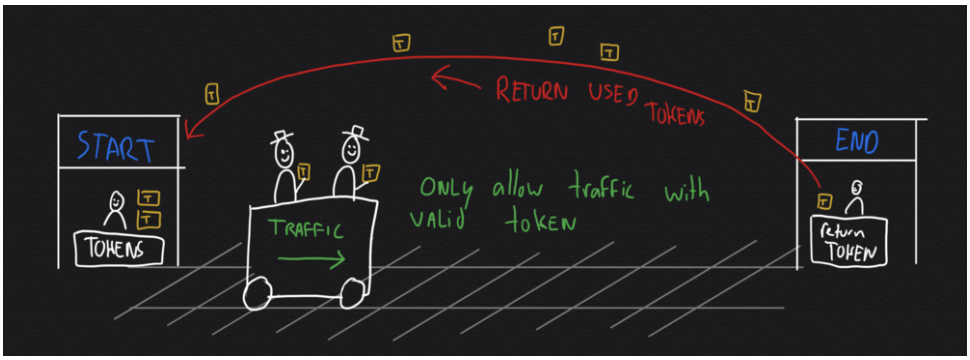
Implementación de la conformación del tráfico

Para conformar el tráfico, necesitas hacer dos cosas:

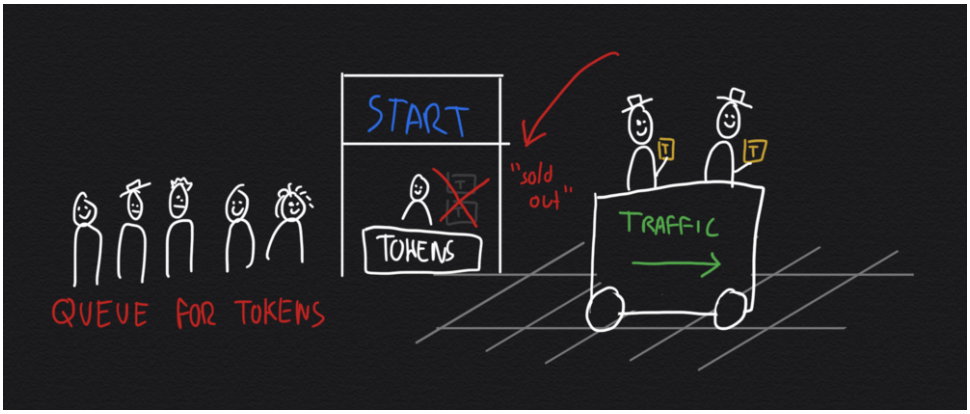
- **marcar el tráfico**: solo deseas afectar el tráfico de red particular, en este caso el acceso IMAP para un cliente determinado. El resto del tráfico no debería verse afectado. Esto se hace marcando los paquetes que coinciden con características particulares, como la IP del cliente o los números de puerto.
- **aplicar la política de conformación**: utilizando herramientas de control de tráfico como 'tc', aplicas la política de conformación al tráfico marcado. Hay diferentes maneras de hacer esto, pero una común es trabajar con los llamados "Hierarchy Token Buckets" o HTB.

Hierarchy Token Buckets (HTB)

En principio, un cubo de tokens es similar al principio de limitar la cantidad de pasajeros en un viaje en tren distribuyendo solo un número fijo de tokens disponibles. Cuando los pasajeros (o paquetes de datos) entran al tren (o red), toman un token. Cuando desembarcan (o llegan a su destino), el token se devuelve. Utilizando el principio del cubo de tokens, puedes controlar la cantidad de tráfico concurrente en un sistema.



Usando tokens para controlar el tráfico - solo los pasajeros (o paquetes de datos) con un token válido están permitidos. Los tokens se devuelven cuando el tráfico llega a su destino.



El tráfico debe esperar a que los tokens estén disponibles cuando se entrega el número máximo de tokens, lo que aplica el tráfico concurrente máximo

Puedes implementar este principio utilizando las herramientas de red ”tc” (para el control del tráfico) en combinación con ”iptables”. Puedes utilizar un script para establecer las reglas para marcar y aplicar. Puedes encontrar varios ejemplos en línea, yo usé *este* *por Julien Vehent*.

```
#! /bin/bash
NETCARD=eth0
MAXBANDWIDTH=100000  # choose a number that is high enough for non-shaped traffic      default

# reinit
tc qdisc del dev $NETCARD root handle 1
tc qdisc add dev $NETCARD root handle 1: htb default 9999

# create the default class, this is "all the other traffic"
tc class add dev $NETCARD parent 1:0 classid 1:9999 htb rate $(( $MAXBANDWIDTH ))kbit ceil $(( $MAXBANDWIDTH ))kbit burst 5k prio 9999

# control bandwidth per IP       DEFINING POLICY PER IP
declare -A ipctrl
# define list of IP and bandwidth (in kilo bits per seconds) below
ipctrl[192.168.1.101]="128"             # limited to 128 kilobits per second      policy per client IP
ipctrl[192.168.1.102]="512"             # limited to 512 kilobits per second
ipctrl[192.168.1.103]="32"              # limited to just 32 kilobit per second

mark=0
for ip in "${!ipctrl[@]}"  SHAPING TRAFFIC BY IP
do
    mark=$(( mark + 1 ))          Setting up Firewall rules to enforce rules
    bandwidth=${ipctrl[$ip]}

    # traffic shaping rule
    tc class add dev $NETCARD parent 1:0 classid 1:$mark htb rate $(( $bandwidth ))kbit ceil $(( $bandwidth ))kbit burst 5k prio $mark

    # netfilter packet marking rule
    iptables -t mangle -A INPUT -i $NETCARD -s $ip -j CONNMARK --set-mark $mark

    # filter that bind the two
    tc filter add dev $NETCARD parent 1:0 protocol ip prio $mark handle $mark fw flowid 1:$mark

    echo "IP $ip is attached to mark $mark and limited to $bandwidth kbps"
done

#propagate netfilter marks on connections
iptables -t mangle -A POSTROUTING -j CONNMARK --restore-mark
```

Script de ejemplo para la gestión del tráfico

Conclusión

A veces, las anomalías de la red no son lo que esperas que sean, ¡por lo tanto, siempre debes tomarte el tiempo para investigarlas! Bloquear el tráfico a ciegas es brusco, a veces necesitas refinar tus métodos para mitigar los problemas.

Aplicar técnicas de filtrado poco ortodoxas no es algo que me guste, pero a veces son el único medio para lograr un fin. ¡Saber lo que estás haciendo y por qué lo estás haciendo es muy importante!