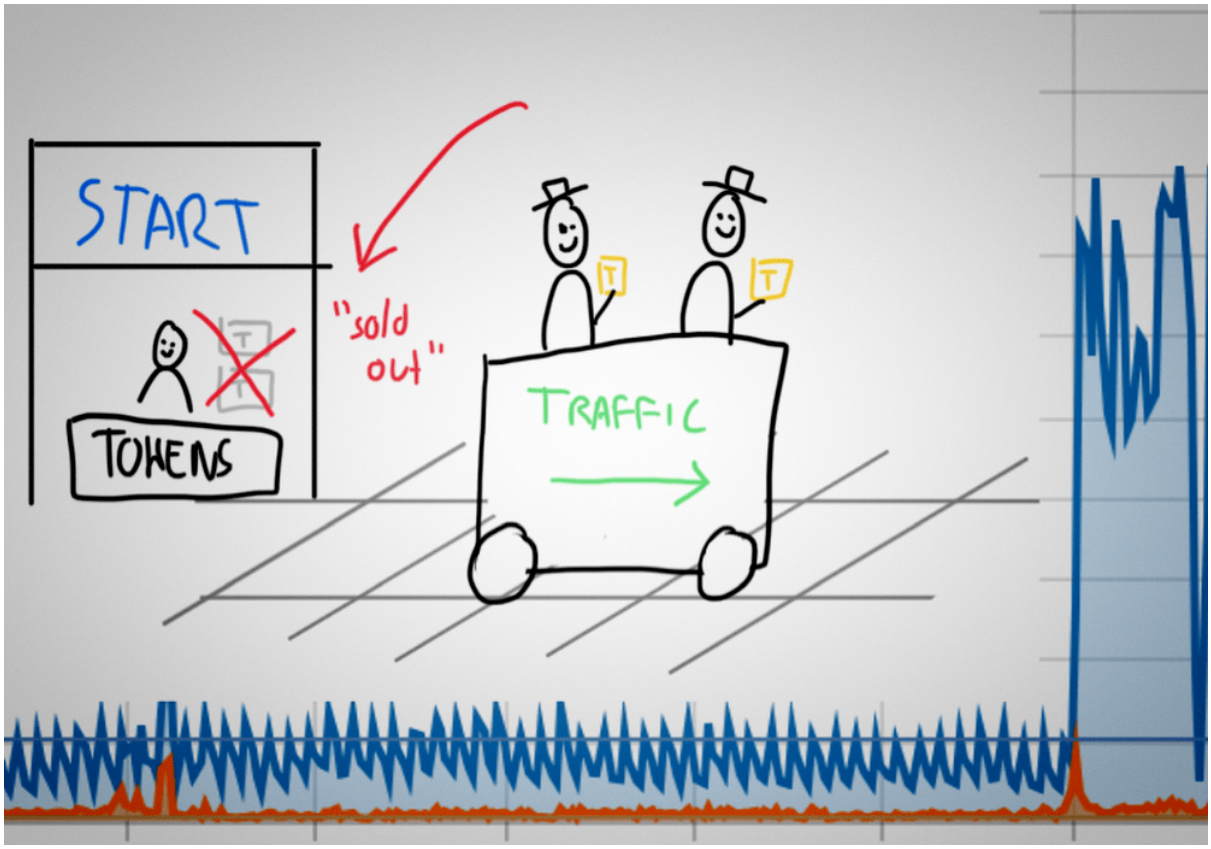
Traffic Shaping mit iptables und tc

Begrenzung der ausgehenden Netzwerkbandbreite pro Client-IP-Adresse

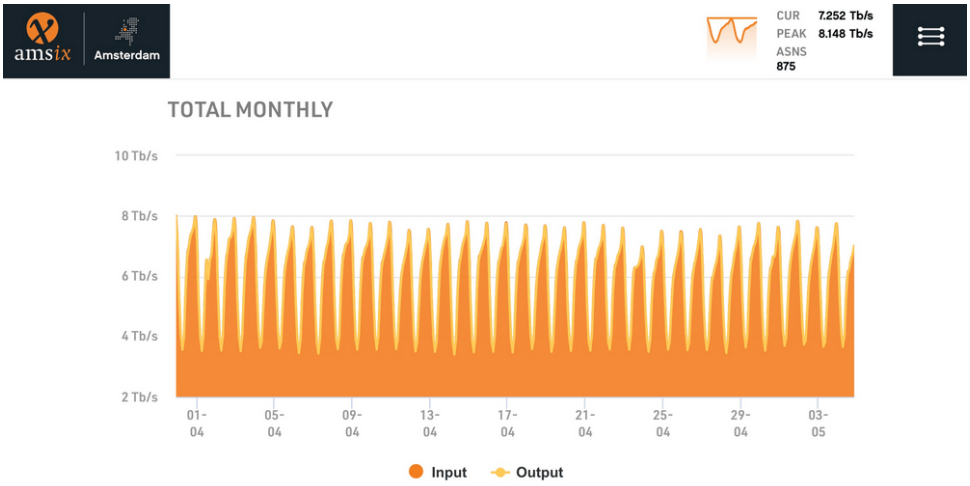
Willem L. Middelkoop
Apr. 1, 2020



Letzten Monat erhielt ich eine automatische Warnung über übermäßige Bandbreitennutzung, normalerweise ein Zeichen für Probleme. In solchen Fällen sollte man einem Standard-Störfallverfahren folgen und versuchen, die Quelle des Datenverkehrs zu isolieren, bevor man sie abschaltet. Die Ursache dieses Vorfalls war jedoch nicht das, was ich erwartet hatte... und erforderte eine andere Art der Eindämmung als eine einfache Blockade.

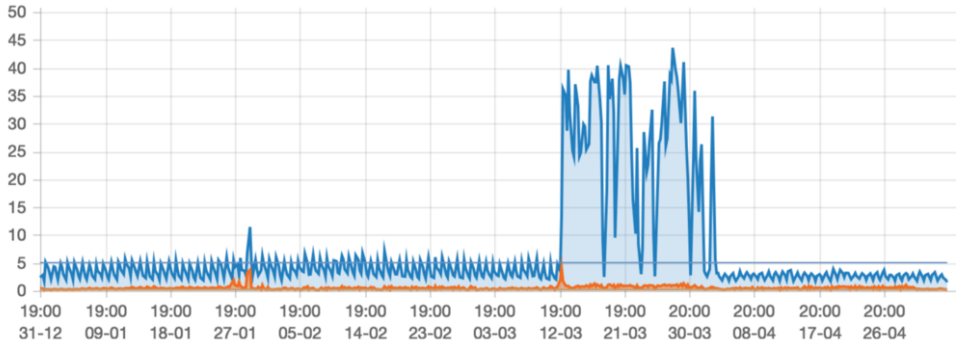
Übermäßige Bandbreitenwarnung

Wenn Sie Server verwalten, werden Sie feststellen, dass der Internetverkehr normalerweise in vorhersehbaren Mustern auftritt. Genau wie der echte Verkehr auf Straßen gibt es regelmäßige Zeiten, in denen viel und wenig los ist.



Bandbreitendiagramm von AMS-IX zeigt ein vorhersehbares Muster - beachten Sie das wellenartige Muster

Das vorhersehbare Muster ermöglicht es, Anomalien automatisch zu erkennen. So wie ein Stau auf einer Autobahn zu einer ungewöhnlichen Zeit die Folge eines Unfalls sein kann, können unerwartete Schwankungen im Internetverkehr ein Indikator für einen Vorfall im Cyberspace sein.



Bandbreitendiagramm mit ungewöhnlichem Peak, der anzeigt, dass etwas nicht stimmt - Sie müssen kein Sherlock Holmes sein, um es zu finden

Isolierung der Quelle

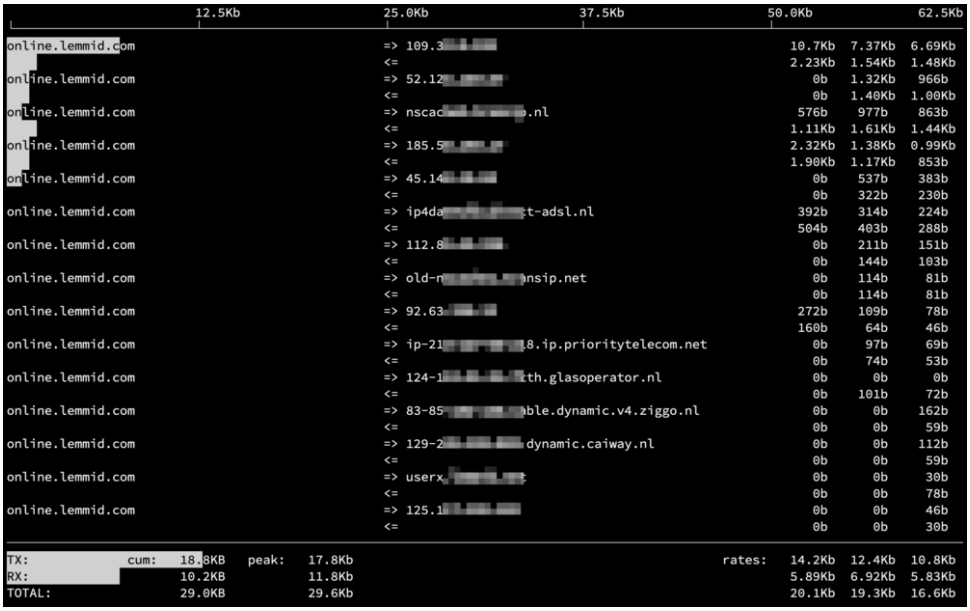
Als Erstes sollten Sie die Ursache des Problems finden. Tun Sie dies, indem Sie die Anomalie analysieren:

- Stellen Sie fest, ob der zusätzliche Verkehr eingehend oder ausgehend ist (Upload oder Download?)
- Bestimmen Sie die zugehörigen Quell- und Ziel-IP-Adressen (welcher Server ist betroffen? Wohin geht der Verkehr oder woher kommt er?)
- Bestimmen Sie die Art des Verkehrs (E-Mail, Web oder etwas anderes?)

Um dies zu tun, sollten Sie die Verkehrsdiagramme überprüfen, die normalerweise unterschiedliche Ein-/Ausgabe anzeigen. Dann sollten Sie versuchen, die betroffenen IP-Adressen zu finden. Dies kann bedeuten, dass Sie sich weitere (einzelne Server-)Diagramme und Statistiken innerhalb von Switches, Routern und Servern ansehen müssen.

Schauen Sie sich dann die CPU-Auslastung und Protokolldateien an, um festzustellen, welche Anwendung betroffen ist, z. B. Mail oder Web. Je größer die Anomalie ist, desto leichter ist sie zu finden.

Sie könnten versucht sein, die Anomalie zu beseitigen, sobald Sie sie gefunden haben, indem Sie den zugehörigen Verkehr sofort stoppen. Aber Sie sollten sie wirklich am Leben erhalten (zumindest ein wenig länger), um so viel wie möglich daraus zu lernen.



Verwendung des iftop-Tools, um die Bandbreitennutzung pro verbundener IP-Adresse anzuzeigen

Verwenden Sie ein Tool wie iftop, um eine Echtzeitübersicht der Bandbreitennutzung pro verbundener IP-Adresse zu erhalten. Es ist sehr nützlich, um einen Überblick darüber zu bekommen, was vor sich geht, insbesondere in Kombination mit Protokolldateien (Verknüpfung der IP-Adresse mit einzelnen Konten).

Ungewöhnliche Ursache

Der Server, der die übermäßige Bandbreitennutzung verursachte, war ein Mailserver. Oft werden sie von Hackern angegriffen, um sie in einen Spam-Relay-Server zu verwandeln. Dies kann auf verschiedene Weise geschehen, normalerweise indem die Spammer eine gültige Anmeldung erfassen. Dies führt zu viel ausgehendem Verkehr, da die Spammer viele E-Mails versenden. Wenn auf Ihrem Server ein Spam-Lauf stattfindet, sehen Sie dies wahrscheinlich in den Protokollen, da Spam-Nachrichten häufig zurückkommen, wodurch sich die Mail-Warteschlangen schnell füllen. Es wird schnell chaotisch, aber auf diesem Server gab es kein solches Chaos - nur eine ungewöhnlich hohe Bandbreitennutzung.

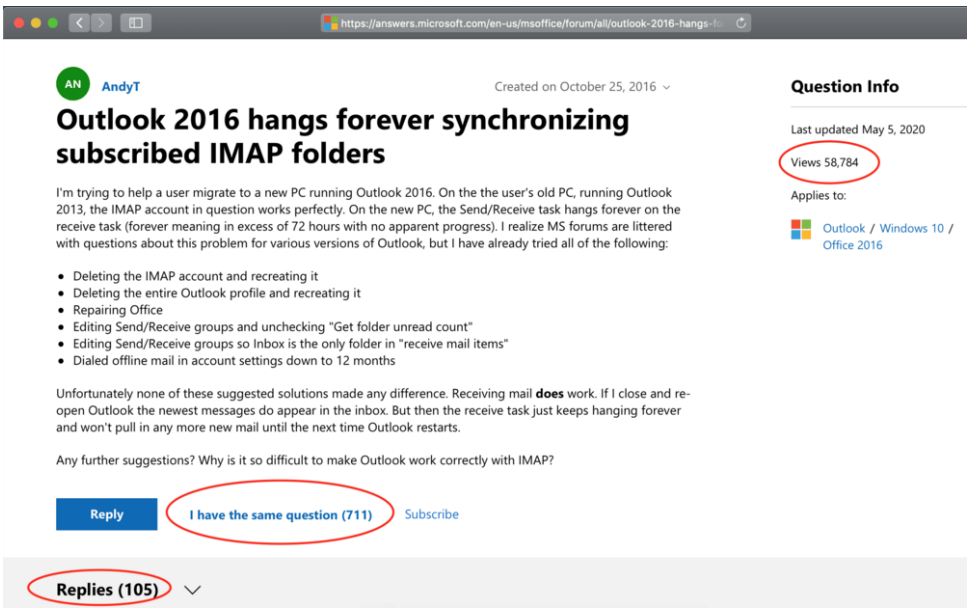
Mail (und Spam) wird über das SMTP-Protokoll versendet, aber der Verkehr auf dem SMTP-Port dieses Servers war ganz normal. Dies war sehr ungewöhnlich, da es bedeutete, dass der übermäßige Verkehr von etwas anderem stammte. Aber was? Nach der Analyse verschiedener Protokolldateien auf dem Mailserver stellte ich fest, dass das störende Protokoll IMAP war. Irgendwie verursachte ein Client, der über IMAP mit dem Mailserver verbunden war, übermäßig viel Netzwerkverkehr. IMAP ist ein Protokoll,

das zum *Lesen* von E-Mails verwendet wird, nicht zum Senden, was IMAP-bezogene Anomalien sehr selten macht.

Durch die Analyse des Protokolls des Mailservers fand ich den spezifischen Benutzer, der den Verkehr verursachte. Ich kontaktierte den Kunden, um zu fragen, ob er an seinem Ende etwas Ungewöhnliches bemerkt hatte. Es überrascht nicht, dass er bemerkte, dass sich sein Computer in letzter Zeit etwas träge anfühlte.

Microsoft Outlook Synchronisierungsschleife

Nach einigem Ausprobieren per Telefon stellten wir fest, dass etwas Microsoft Outlook dazu veranlasste, IMAP-Ordner in einer Schleife zu synchronisieren. Dies führte dazu, dass sein Computer den gesamten Inhalt seines Postfachs immer wieder herunterlud! Da sein Postfach über 40 Gigabyte groß war, verursachte dies den erheblichen Datenverkehr. Anscheinend wird dies durch einen Fehler in Microsoft Outlook verursacht, leider gibt es dafür keine einfache Lösung.



Fehler in Microsoft Outlook führen dazu, dass IMAP-Ordner ständig synchronisiert werden, ein Problem, das viele Menschen betrifft (siehe Anzahl der Aufrufe!)

Minderung durch Traffic Shaping

Ich stand vor der schwierigen Entscheidung, entweder den (normalen, legitimen, zahlenden) Kunden zu blockieren oder den übermäßigen Verkehr weiter zuzulassen (was dem Netzbetreiber erhebliche Kosten verursacht). Legitime Benutzer zu blockieren, die ihr Geschäft per E-Mail betreiben, ist eine sehr schlechte Idee, aber auch übermäßigen Verkehr zuzulassen ist schlecht. Glücklicherweise fand ich einen alternativen Weg, den übermäßigen Verkehr zu reduzieren und dem Kunden gleichzeitig den Zugriff auf seine E-Mails zu ermöglichen (mit seiner vertrauenswürdigen, aber fehlerhaften Outlook-App).

Traffic Shaping

Als Bandbreitenmanagement-Technik können Sie Traffic Shaping verwenden, um einige (oder alle) Datenpakete zu verzögern, um sie mit einem gewünschten Verkehrsprofil in

Einklang zu bringen. Wenn angewendet, formen Sie - im wahrsten Sinne des Wortes - die Verkehrsgraphen, daher der Name.

Diese Technik ist nicht unumstritten, da sie das Gegenteil des oft gepriesenen Prinzips der "Netzneutralität" ist. Mit Traffic Shaping können Sie bestimmte Arten von Verkehr absichtlich blockieren oder verlangsamen (oder extra Geld dafür verlangen). Prinzipiell bin ich gegen alles, was der Netzneutralität schadet, aber für diese spezielle Situation hatte ich keine praktikable Alternative. Ich musste den E-Mail-Verkehr für diesen bestimmten Kunden erheblich verlangsamen, um die Bandbreite zu reduzieren und gleichzeitig den Zugriff auf sein Konto zu gewährleisten.

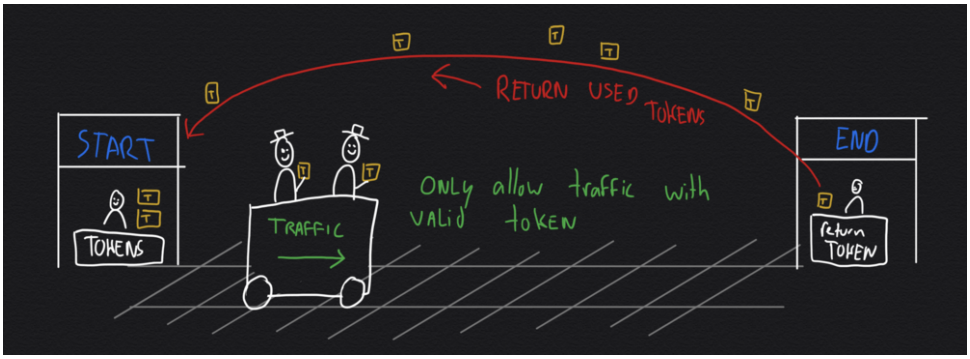
Implementierung von Traffic Shaping

Um den Verkehr zu formen, müssen Sie zwei Dinge tun:

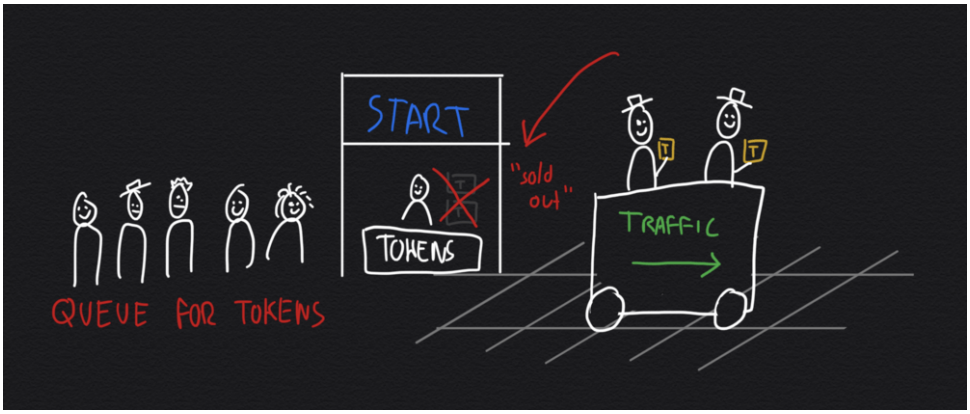
- **Verkehr markieren**: Sie möchten nur bestimmten Netzwerkverkehr beeinflussen, in diesem Fall den IMAP-Zugriff für einen bestimmten Client. Anderer Verkehr sollte nicht betroffen sein. Dies geschieht durch Markieren von Paketen, die bestimmten Merkmalen entsprechen, wie z. B. Client-IP oder Portnummern.
- **Shaping-Richtlinie durchsetzen**: Mit Traffic-Control-Tools wie 'tc' setzen Sie dann die Shaping-Richtlinie für den markierten Verkehr durch. Es gibt verschiedene Möglichkeiten, dies zu tun, aber eine gängige ist die Arbeit mit sogenannten "Hierarchy Token Buckets" oder HTBs.

Hierarchy Token Buckets (HTBs)

Im Prinzip ähnelt ein Token Bucket dem Prinzip der Begrenzung der Passagierzahl bei einer Zugfahrt, indem nur eine feste Anzahl verfügbarer Token verteilt wird. Wenn Fahrgäste (oder Datenpakete) in den Zug (oder das Netzwerk) einsteigen, nehmen sie einen Token. Wenn sie aussteigen (oder ihr Ziel erreichen), wird der Token zurückgegeben. Mit dem Token-Bucket-Prinzip können Sie die Menge des gleichzeitigen Verkehrs in einem System steuern.



Verwendung von Token zur Steuerung des Datenverkehrs - nur Passagiere (oder Datenpakete) mit einem gültigen Token sind erlaubt. Token werden zurückgegeben, sobald der Datenverkehr sein Ziel erreicht.



Datenverkehr muss warten, bis Token verfügbar werden, wenn die maximale Anzahl an Token vergeben ist, wodurch der maximale gleichzeitige Datenverkehr erzwungen wird

Sie können dieses Prinzip mit den Netzwerktools ”tc” (für Traffic Control) in Kombination mit ”iptables” implementieren. Sie können ein Skript verwenden, um die Regeln für das Markieren und Durchsetzen festzulegen. Sie können verschiedene Beispiele online finden, ich habe dieses hier von Julien Vehent verwendet.

```
#! /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
```

Beispielskript für Traffic Shaping

Schlussfolgerung

Manchmal sind Netzwerkanomalien nicht das, was Sie erwarten, deshalb sollten Sie sich immer die Zeit nehmen, sie zu untersuchen! Das blinde Blockieren von Verkehr ist stumpf, manchmal müssen Sie Ihre Methoden verfeinern, um Probleme zu entschärfen.

Die Anwendung unorthodoxer Filtertechniken ist nichts, was ich mag, aber manchmal sind sie das einzige Mittel zum Zweck. Zu wissen, was Sie tun und warum Sie es tun, ist sehr wichtig!