Privacy & Security Essentials

Firewall

–

2019 v2

Firewall – werking, nut en noodzaak

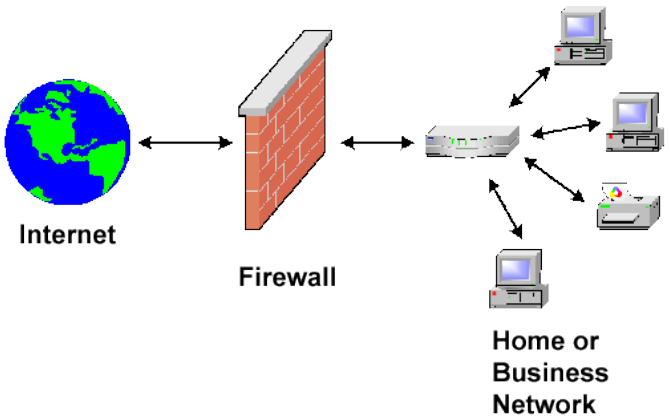
Een firewall is een app of een speciaal daartoe ingericht apparaat met firewall app erop draaiend, dat zorgt dat er een “brandscheiding” (zie links onder) bestaat tussen interne wifi/LAN netwerk en de buitenwereld het www-internet.

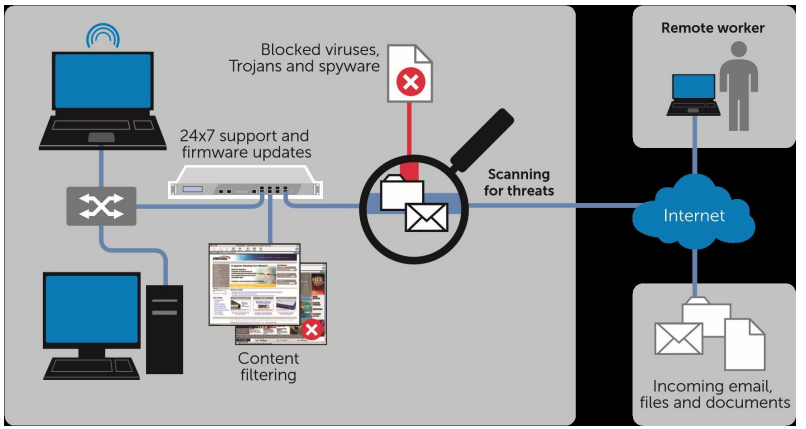
In privé situaties heeft meestal elke computer een eigen app voor Firewall. Privé personen die meer “tech-saffie” zijn installeren een firewall app op hun router, die dan als brandscheiding fungeert voor alle computers op hun wifi/LAN. Bedrijven installeren meestal een speciaal daartoe ingerichte computer/server (zie rechts onder), die de taak van firewall verricht. Laatste heeft te maken met hoeveelheid data-verkeer, diverse soorten filtering en wijze van beheer van firewall, waarover later meer.

In essentie is een firewall te vergelijken met een huis/gebouw voordeur slot:
1. als de voordeur niet op slot staat oftwel “open” is, dan kan iedereen naar binnen, zowel degene die geacht worden welkom te zijn, alsook ongenode gasten met kwalijke intenties
2. of de voordeur staat “dicht” oftewel in het slot, en alleen degene die een toegangspas hebben (ontvangen van eigenaar) kan de voordeur open doen en naar binnen; de toegangspas kan vergezeld gaan met een encrypte sleutel (toegangscode)

Waarom de vergelijking met een voordeur slot wel aardig is:
→ alleen genode gasten kunnen binnentreden, waarvoor toestemming nodig is
→ iedereen die binnen moet in principe zonder pas of encrypte sleutel naar buiten kunnen treden
In navolgende slides wordt toegansgpas en sleutel werking verder uitgewerkt

Het gebruik van een firewall is essentieel want het www-internet kent zéér veel ongenode gasten. Om nog even door te gaan op vorige beeldspraak “het www-internet is te vergelijken met een zéér slechte buurt waar iedereen zijn voordeur op slot doet.





Firewall – enable disable

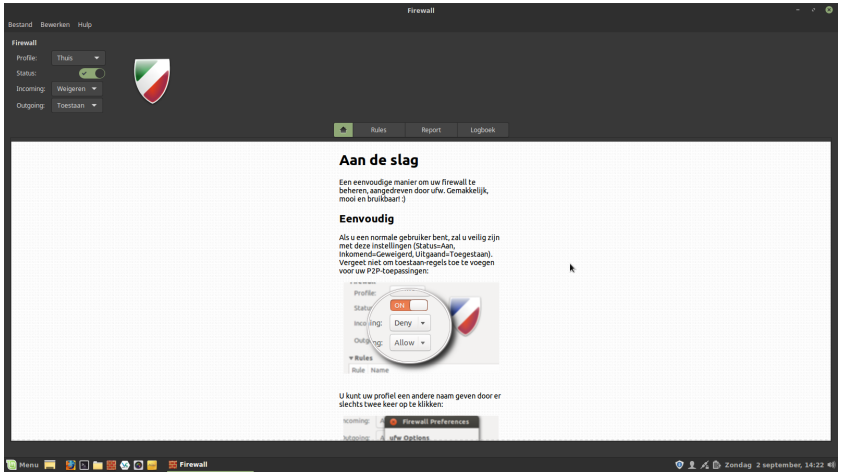
In het navolgende wordt de firewall als speciaal daartoe ingericht “apparaat” verder niet uitgewerkt, want is vakgebied van specialisten en overstijgt de reikwijdte en diepgang van onderhavige info; en het maakt verder uitleg en voorgestelde maatregelen onnodig complex. Dus uitgaand van een eenvoudige situatie het volgende:

Zowel in macOS, Windows en Linux zit standaard firewall functionaliteit: meestal wordt gebruiker geacht via de app “firewall” deze aan te zetten. Staat de firewall niet aan dan is deze disabled. Bij “aan” dan staat firewall enabled.
→ dat aan- en uitzetten kan alleen door Administrator (admin) of een account/gebruiker met admin rechten

Uit het laatste volgt dat bij iOS en Android er standaard géén app firewall aanwezig is, want smartphones worden “af-fabriek” zo geleverd dat er géén admin of gebruikers account met admin rechten mogelijk is. Even een zijspoor: er zijn tools waarbij smartphone ge-root kan worden zodat toegang tot OS wel mogelijk is; dat is niet wat men wil want dan staat de toegang van smartphone open voor elke ongenode gast.

Indachtig het voorbeeld van vorige slide over voordeur:
→ de firewall zou altijjd aan of enabled moeten zijn
→ er is geen reden waarom firewall disabled zou zijn

LET OP:
→ Google Chrome wil eigen advertentiemarkt aandeel beschermen en omzeilt bewust de firewall
→ In chrome://settings/advanced, disable the "web services" that are supposed to assist you; just uncheck these three boxes



Firewall – status inkomend

Bij status inkomend data verkeer geldt het volgende:

NIET DOEN:
→ toestaan iedereen ziet voordeur die open staat en kan naar binnen; redelijk zinloos gebruik van firewall
→ verwerpen iedereen ziet voordeur die dicht staat maar kan niet naar binnen zonder toegangspas en sleutel

Bij status “verwerpen” te weten: ongenode gasten kunnen met behulp van app “nmap” automatisch een heel postcode gebied (reeks van IP-adressen) scannen om te zien of er voordeuren / computers zijn, en zo ja, of deze open staan. Dat gaat dmv een “ping” naar doel IP-adres. Bij “verwerpen” geeft de computer antwoord op deze ping met “ja ik ben er” en als de ongenode gast dan vraagt “mag ik naar binnen” dan antwoord computer met een “algemeen – nee”. Op dat moment begint de uitdaging voor hackers om toch binnen te kunnen komen. En deze “rode vlag” is niet wat men wil.

Want: hacker ziet dat “algemeen – nee” als een indicatie dat er meer is dan niks, en gebruikt alsdan nmap om alle deuren en ramen (technische term “poorten” – Engels: “port”) binnenin het huis cq computer te checken of er toch één van de 65536 poorten open staat om dan alsnog binnen te komen. Hacker gebruikt de functie, zie onder, van “weigeren” om alsdan met een verzonnen toegangspas de sleutel “te berekenen”. Letterlijk berekenen van sleutels want sleutels zijn meestal encrypted via een formule.

Sleutels zijn dus meestal encrypted, maar niet altijd: want bijv port 23 is van oudsher bestemd voor toegang voor remote beheerder uit de tijd van “vroeger” met zonder encryptie! Dus deze “telnet”-legacy functie cq port 23 dient dicht gezet te worden want hackers kennen de port-nummers waar ze de beste kans hebben. Vandaar “firewall aan en inkomend weigeren”.

DOEN:
→ weigeren

Bij status “weigeren” is het euvel van “verwerpen” niet aanwezig, want er is geen “red flag” en ALLE poorten staan dicht!

Er zijn weinig situaties denkbaar dat wel een externe computer binnen mag komen. Deze alsdan door admin genode gasten weten precies dat ze bij specifiek bewust IP-adres willen zijn, gaan zonder signaal door voordeur. En daarachter bij specifiek vooraf aangegeven poort wordt gevraagd om toegangspas en toegekende sleutel. Moderne externe beheerders werken volgens dit principe met poort 22. Poort 22 is dan ook formeel bestemd voor SSH – secure shell login.

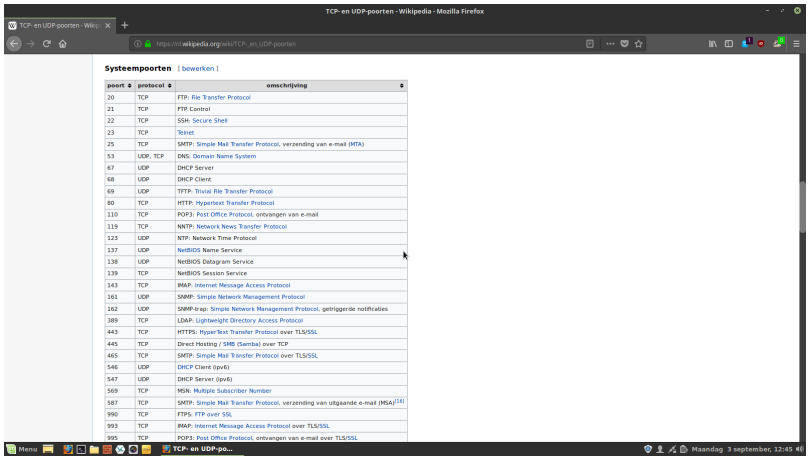
Firewall – status inkomend: toegangspas

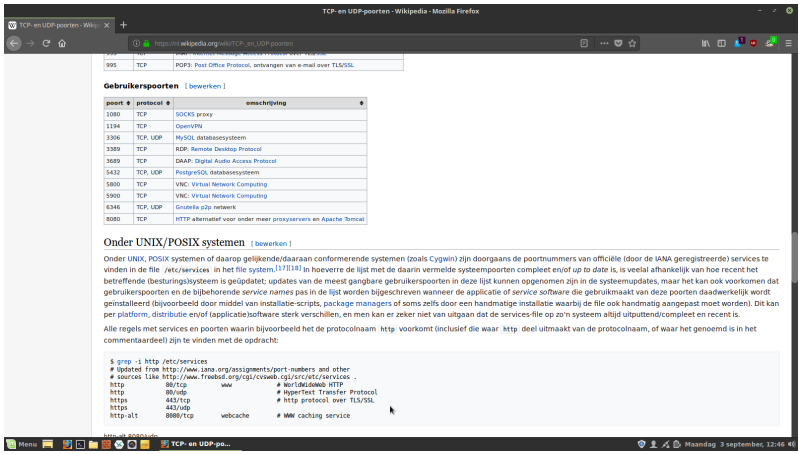
Als de instelling is zoals in vorige slide(s) geadviseerd dan is elke poort dicht gezet. Indien gewenst kan het deurbeleid aangepast worden: admin kan dus een toegangspas verlenen. Dat gaat dmv regels (rules) in te stellen bij de app firewall.

Rules: admin moet weten welke poorten waarvoor dienen om een correcte instelling te maken. En voor dat uitzoeken welke poort welke functie heeft is er een overzicht en organisatie IANA is coordinator. Iedere www-internet developer houdt zich in principe aan deze opgave. Zie: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

Resume: een poort heeft een specifiek functie en een poort kan dicht gezet worden voor inkomend data verkeer. Echter diezelfde poort kan weliswaar dicht staan voor inkomend data verkeer maar tegelijkertijd wel open staan voor uitgaand data verkeer, waarover later meer.

DOEN:
→ voor optimale privacy en security staat firewall “aan
→ status van firewall voor inkomend “weigeren”; bijgevolg
→ alle poorten voor inkomend data verkeer staan dus dicht
→ er zijn weinig redenen om een inkomende poort open te zetten
→ ingeval van twijfel – inkomend data verkeer / poort niet open zetten





Firewall – status inkomend: sleutel

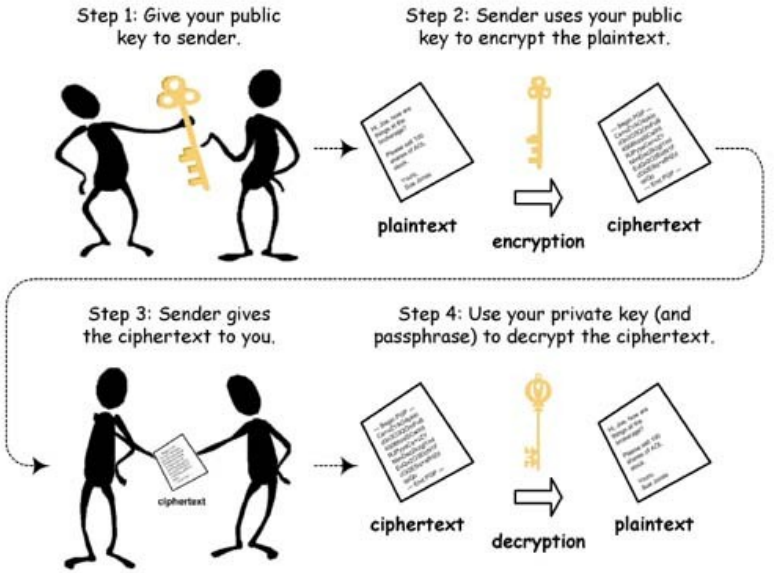
Indien advies van vorige slides gevolgd dan is deze slide over “sleutel” verder niet aan de orde. En sla dit onderdeel over.

Het door admin verlenen van sleutels is complexe materie met dito encryptie technologien. Punt is dat als admin in het genoemde voorbeeld van SSH poort 22 voor remote beheer deze open heeft gezet, dan kan een hacker dat constateren, en dus gebruiken voor snode plannen. Om ongenode gasten te weren is er dus een sleutel.

Sleutel:
→ moderne uitwisseling van sleutels gaat mbv asymetrische cryptografie oftewel “public key encryption”
→ Voor detail uitwerking van sleutels en bijbehorende encryptie, zie: https://nl.wikipedia.org/wiki/Encryptie

Het lezen, begrijpen en hanteren van “vrij geven van poort voor inkomend data verkeer met gebruik maken van sleutel” vergt meer dan normaal ontwikkeld vermogen tot “computeren”. Het is voor de normale doorsnee gebruiker geen wandeling in het park om dit proces operationeel te krijgen met alsdan “op zeker” te zijn van 100% security.
→ plaatjes zeggen soms meer dan woorden, zie (onderstaand) 4x stappen van hanteren van sleutels

DOEN:
→ naar keuze zelf uitdiepen



Firewall – status uitgaand

Bij status uitgaand data verkeer geldt het volgende:

DOEN:

→ toestaan	gebruiker kan naar het www-internet; alle 65536 poorten staan open voor uitgaand data verkeer
→ weigeren	gebruiker krijgt geen melding, kan niet naar www-internet
→ verwerpen	gebruiker krijgt wel melding, kan niet naar www-internet

Opties

Bedrijven die om privacy en security redenen géén www-internet verkeer toestaan. In dat geval doen:
→ status: “weigeren of verwerpen”

Gebruiker mag weliswaar naar www-internet maar bepaalde websites niet bezoeken. In dat geval doen:
→ status firewall toestaan
→ blokkeer domein naam “niet te bezoeken www.webadres.nl”

Een specifieke App mag niet naar www-internet. In dat geval doen:
→ status firewall toestaan
→ zoek uit welke web servers cq domein namen bewuste app zal gebruiken, en;
→ blokkeer domein naam “niet te bezoeken www.webadres.nl”
→ sommige app firewall voorzien in optie om de “app naam die geen uitgaand verkeer mag” te blokkeren
→ ivvv admin kan app “cups” blokkeren; app maakt dan geen contact meer met printer leverancier voor status doorgeven

De app DWS (zie info over Windows) plaatst dus in \etc\hosts een rij van domein namen en doet dan een dummy verwijzing naar niet bestaande server, alsdus defacto geen uitgaand data verkeer. Zéér effectieve methode!

Een ander voorbeeld met zelfde aanpak is bij Software as a Service (SaaS) er voor zorgen dat, ihkv ET phone home, bijv de app Adobe niet de fabrikant contact, voor controle van licentie-key.

Firewall – status uitgaand: domeinen blokkeren

In vervolg op vorige slide en voordeurbeleid analogie: het selectief tegengaan van uitgaand data verkeer is gelijk kinderen die niet buiten mogen spelen cq door de voordeur. Of bij een gesloten inrichting: sommigen mogen de afdeling verlaten, maar anderen weer niet. Enfin, hoe dat in computer te doen?

Gestel, ouders of bedrijf wil(len) niet dat kind / gebruiker naar bepaalde sites gaat. Admin plaats dan in /etc/hosts
0.0.0.0 www.eenofanderexreemkrantje.nl
0.0.0.0 www.pornhub.com
0.0.0.0 www.sex.com
0.0.0.0 www.spelletjesdiegeldkosten.nl

Alsdan bij surfen via web browser naar genoemde websites zal er een melding komen, zoiets als:
→ “oeps, kan geen verbinding maken met gevraagde website, controleer instellingen”

Apps die niet mogen doen aan “ET phone home” gebruiken soortgelijk techniek. Admin plaats in /etc/hosts
127.0.0.1 www.adobe.com
127.0.0.1 www.microsoft.telemetry.com
127.0.0.1 www.microsoft.store.com
127.0.0.1 www.eenofandereappdieniethetinternetmaggebruiken.nl

127.0.0.1 zorgt voor activering van bij computer “af-fabriek” ingebouwde loopback-functie: de computer verwijst naar zichzelf zonder verder acties en geen melding. Oftewel: er gebeurt niks. Behalve dan wanneer in voorbeeld van MS store, gebruiker een app wil kiezen om te installeren, dan “zegt “MS Store app” wel “oeps, etc etc”.

127: admin kan actief op www-internet zoeken naar concrete lijsten waarbij “per app” alle van toepassing zijnde domein namen op een overzicht staan. Deze overzichten zijn gemaakt door personen die dat een keer hebben uitgezocht, en doen soms aan “updates” die niet vanzelf aan admin worden geleverd! Meestal is het niet 1x domein naam maar een hele reeks.
→ admin copy paste dat overzicht in /etc/hosts
→ admin voor Windows copy paste in C:\Windows\System32\drivers\etc\hosts

Firewall – status uitgaand: domeinen blokkeren

Blokkade facebook: zowel bezoek aan die websites maar óók alle reclame cookies die staan op (bijna) alle andere websites!

DOEN:
→ admin copy en paste tekst in /etc/hosts

```
# Block Facebook Ipv4
127.0.0.1   www.facebook.com
127.0.0.1   facebook.com
127.0.0.1   login.facebook.com
127.0.0.1   www.login.facebook.com
127.0.0.1   fbcdn.net
127.0.0.1   www.fbcdn.net
127.0.0.1   fbcdn.com
127.0.0.1   www.fbcdn.com
127.0.0.1   static.ak.fbcdn.net
127.0.0.1   static.ak.connect.facebook.com
127.0.0.1   connect.facebook.net
127.0.0.1   www.connect.facebook.net
127.0.0.1   apps.facebook.com

# Block Facebook Ipv6
fe80::1%lo0 facebook.com
fe80::1%lo0 login.facebook.com
fe80::1%lo0 www.login.facebook.com
fe80::1%lo0 fbcdn.net
fe80::1%lo0 www.fbcdn.net
fe80::1%lo0 fbcdn.com
fe80::1%lo0 www.fbcdn.com
fe80::1%lo0 static.ak.fbcdn.net
fe80::1%lo0 static.ak.connect.facebook.com
fe80::1%lo0 connect.facebook.net
fe80::1%lo0 www.connect.facebook.net
fe80::1%lo0 apps.facebook.com
```

LET OP:
→ zie plaatje onderstaand: voorbeeld van Facebook track en trace
→ bij instelling firewall wordt verzenden gebruikersinfo geblokkeerd
→ (be)houden van privacy is een keuze “om er wat aan te doen”

→ dit is het script dat bijna elke commerciele website developer opneemt
→ om zo de bezoeker te tracken en tracen:

```
<!-- Facebook Pixel Code -->
<script>
!function(f,b,e,v,n,t,s){if(f.fbq)return;n=f.fbq=function(){n.cal
n.callMethod.apply(n,arguments):n.queue.push(arguments)};if(!f._f
n.push=n;n.loaded=!0;n.version='2.0';n.queue=[];t=b.createElement
t.src=v;s=b.getElementsByTagName(e)[0];s.parentNode.insertBefore(
document,'script','https://connect.facebook.net/en_US/fbevents.js
fbq('init', '858167644280778'); // Insert your pixel ID here.
fbq('track', 'PageView');
</script>
<noscript><img height="1" width="1" style="display:none"
src="https://www.facebook.com/tr?id=858167644280778&ev=PageView&n
/></noscript>
<!-- DO NOT MODIFY -->
<!-- End Facebook Pixel Code -->
```

Firewall – status uitgaand: domeinen blokkeren

Blokkade google tag manager: alle reclame cookies die staan op (bijna) alle websites, zie onder “google tag manager script”

DOEN:
→ admin copy en paste tekst in /etc/hosts

Block Google Tag Manager
127.0.0.1 www.googletagmanager.com

When Tag Manager (on website) is installed:

your website or app will be able to communicate with the Tag Manager servers. You can then use Tag Manager's web based user interface to set up tracking tags, establish triggers that cause your tag to fire when certain events occur, and create variables that can be used to simplify and automate your tag configurations.

A collection of tags, triggers, variables, and related configurations installed on a given website or mobile app is called a container. A Tag Manager container can replace all other manually-coded tags on a site or app, including tags from Google Ads, Google Analytics, Floodlight, and 3rd party tags.

→ dit is het script dat bijna elke commerciele website developer opneemt om zo de bezoeker te tracken en tracen:

```
<!-- Google Tag Manager -->
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','myNewName','GTM-XXXX');</script>
<!-- End Google Tag Manager -->
```

Firewall – status uitgaand: domeinen blokkeren

Blokkade google analytics: alle cookies die staan op (bijna) alle websites, zie onder “google analytics script”

DOEN:
→ admin copy en paste tekst in /etc/hosts

Block Google Analytics
127.0.0.1 www.google-analytics.com

What data does the tracking snippet capture?

When you add either of these tracking snippets to your website, you send a pageview for each page your users visit. Google Analytics processes this data and can infer a great deal of information including:
→ The total time a user spends on your site
→ The time a user spends on each page and in what order those pages were visited
→ What internal links were clicked (based on the URL of the next pageview)

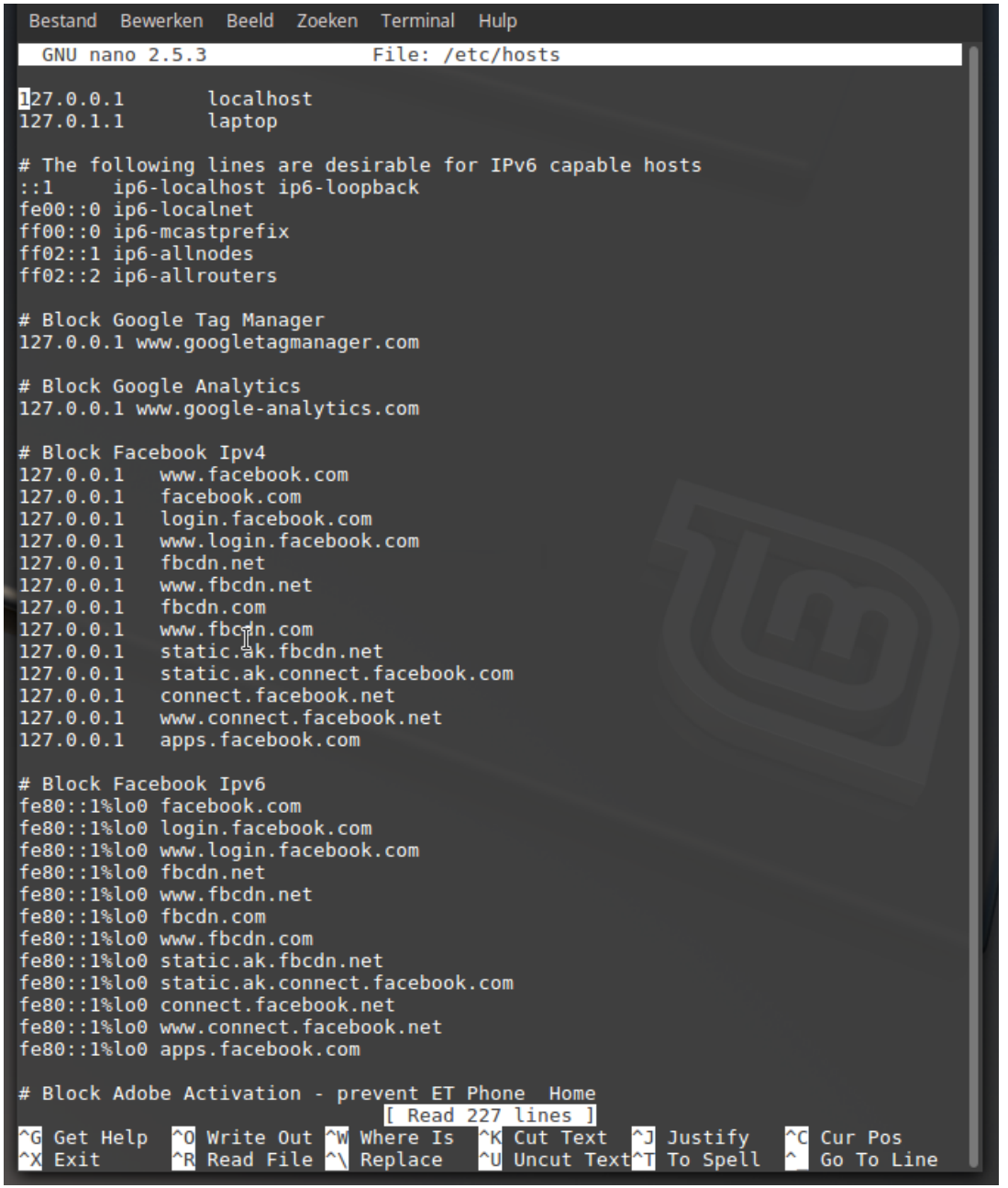
In addition, the IP address, user agent string, and initial page inspection analytics.js does when creating a new tracker is used to determine things like the following:
→ The geographic location of the user
→ What browser and operating system are being used
→ Screen size and whether Flash or Java is installed
→ The referring site

→ dit is het script dat bijna elke commerciele website developer opneemt om zo de bezoeker te tracken en tracen:

```
<!-- Google Analytics -->
<script>
(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){
(i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)
})(window,document,'script','https://www.google-analytics.com/analytics.js','ga');

ga('create', 'UA-XXXXX-Y', 'auto');
ga('send', 'pageview');
</script>
<!-- End Google Analytics -->
```

Firewall – status uitgaand: domeinen blokkeren



Firewall – verantwoording

Bronvermelding staat meestal in de screenshots en verder Wikipedia en YouTube

Het www-internet is constant in beweging en feiten en situaties zijn aan wijzigingen onderhevig, daarom:
→ Informatie is van ten tijde van vervaardigen van deze info als vermeld op voorblad – slide 1

TOOLING

Laptop	Acer – Linux Mint
VPN	protonvpn.com
Browser	Mozilla Firefox
Opmaak	LibreOffice
Website	www.summertime.tech