



JESUÏTES El Clot
Escola del Clot

M011-SEGURETAT INFORMÀTICA i ALTA SEGURETAT

UF3- Instal·lació i Configuració d'un servidor intermediari

PRÀCTICA 1 : DE TALLAFOCS PERSONALS

Curs: 2018-19

CFGs: ASIX2

Alumne : Arnau Subirós Puigarnau

Data : 09/02/2019

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

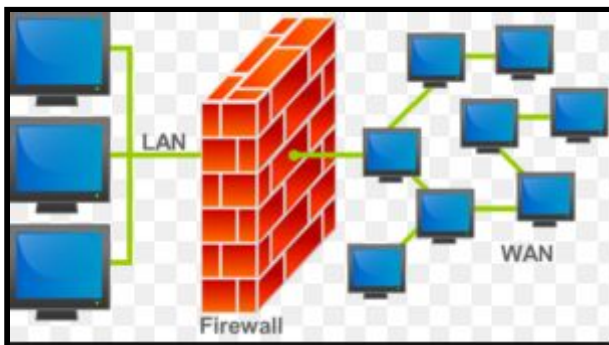
PRACTICA 1 :

De Tallafocs Personals

PART ANALÍTICA-TEÒRICA

1.Anota les diferències entre un tallafocs hardware i un de software.

Un tallafocs (Firewall) és el sistema de protecció que està entre Internet i la teva xarxa informàtica. Usat correctament previndrà l'accés no desitjat a la teva xarxa. Un servidor analitza amb deteniment les dades i brinda una barrera protectora. Aquest servidor pot ser un firewall hardware o firewall software



- **Firewall de Hardware** :Aquest tipus de sistema és col·locat sobre els dispositius (routers)usats per accedir a Internet
 - Freqüentment la instal·lació ja està realitzada quan es compra un router. En cas contrari és molt recomendable realitzar la seva instal·lació.
 - En la majoria dels casos un firewall de hardware és la solució perfecta per a les organitzacions que vulguin una única protecció per a diferents sistemes. El negatiu pot ser el car que són i el difícil a l'hora d'administrar-ho pel que necessiten de supervisió i el coneixement necessari per a la seva instal·lació, configuració i monitoratge diari

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

Exemples de Firewall de Hardware



<p>ZyXEL ATP500, 2600 Mbit/s, 900 Mbit/s, 82,23 BTU/h, 529688,2 h.</p> <p>986,85€</p>	<p>ZyXEL NSG50, 70 Mbit/s, IEEE 802.3, IEEE 802.3ab, IEEE 802.3u.</p> <p>249,41€</p>	<p>ZyXEL VPN Firewall VPN 50, 800 Mbit/s, 150 Mbit/s, Alambrico.</p> <p>512,14€</p>	<p>ZyXEL VPN Firewall VPN 300, 2600 Mbit/s, 1000 Mbit/s.</p> <p>1.073,44€</p>
--	---	--	--

- **Firewall de Software** : Podem distingir els 2 tipus :
 - **Gratuïts** : firewall, que pot ser usat amb total llibertat de manera totalment gratuïta com el seu nom indica. El seu objectiu es rastrejar i no permetre l'accés a certes dades a les computadores personals

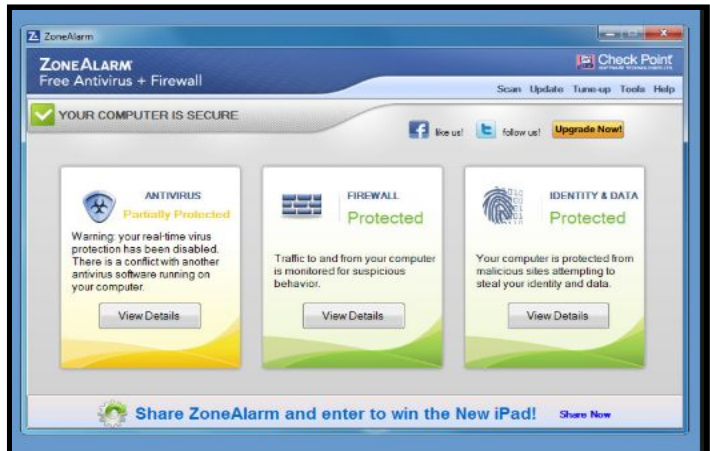
Nom i Cognoms

Arnau Subirós Puigarnau

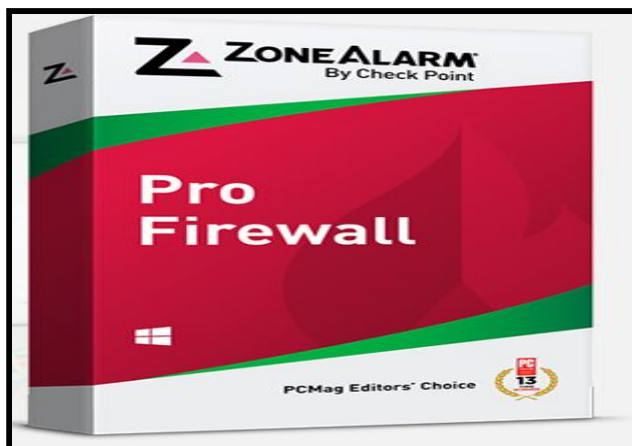
Data

09/02/2019

Exemples de Firewall de Software(gratuït)



- **Comercials** : Aquests sistemes de programari posseeixen el mateix funcionament que l'anterior i inclouen millors nivells de control i protecció. A vegades són venuts amb altres sistemes de seguretat com antivirus perquè resultin més eficients a l'hora de la protecció a la computadora



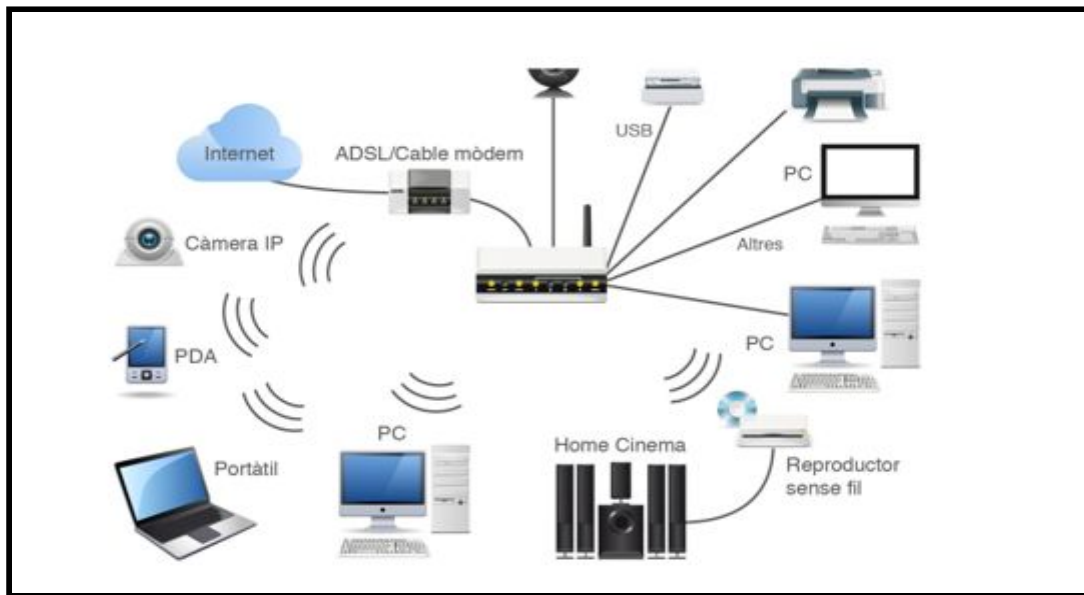
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

2.Quins tipus d'amenaçes et sugereixen el següent dibuix?



En aquesta imatge es veu un router inalàmbic on hi han alguns dispositius que utilitzen connexió via wifi i d'altres connexió ADSL.

En aquesta xarxa podem veure la gran varietat de dispositius que utilitzen connexions sense fils i gran varietat de tecnologia : PC,càmera IP, PDA Portàtil,etc

- ❖ Desconec el protocol de seguretat inalàmbic que utilitzen (WEP,WPA,WPA2..)
- ❖ **WPA2**:Una de les vulnerabilitats més freqüents té relació amb la pèrdua o el robatori de dispositius. En emprar la manera simple de compartició de clau de seguretat WPA2, el sistema aplica la mateixa clau d'accés en tota la xarxa wifi.
- ❖ Cracking de password(sin s'utilitza WEP)
- ❖ Espionatge
- ❖ Robatori de dades
- ❖ Ús inapropiat e il.legal
- ❖ Col.locació de malware

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

3.Quan avaluem la seguretat perimètrica d'un sistema o una xarxa és fonamental conèixer quines són les vulnerabilitats i les amenaces. A partir d'aquest fet busca informació sobre que és o que són els Black hat i script kiddies

BLACK HAT(hacker de barret negre) →És un hacker que viola la seguretat informàtica per raons més enllà de la malícia o per a benefici personal, els hackers de barret negre són la personificació de tot el que el públic tem d'un criminal informàtic.

- Aquest grup de hackers, busquen les falles de seguretat del programari i les aprofiten en el seu propi benefici: (malware,exploits,cucs, troians,etc)
 - Si troben un codi tancat, l'obren per la força.
 - Si tenen un programari entre les seves mans l'inspeccionen una vegada i una altra fins que troben el forat pel qual entrar (backdoor o “puerta trasera”) i inserir exploits o dur a terme atacs de dia zero.
 - Són aquesta gent que roba dades, contrasenyes, emails, números de targeta de crèdit o les teves claus d'accés al banc. Després comercien amb aquesta informació.



Nom i Cognoms

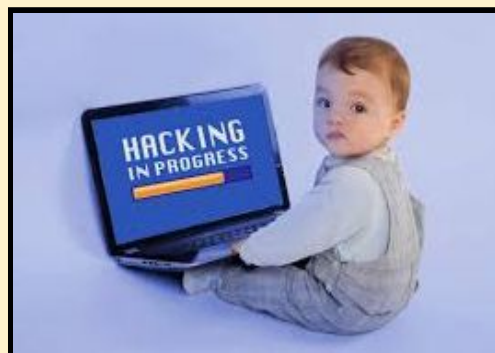
Arnau Subirós Puigarnau

Data

09/02/2019

SCRIPT KIDDIES(“script per nens”) → És un individu no qualificat que utilitza scripts o programes desenvolupats per uns altres per a atacar sistemes informàtics i xarxes i defectes de llocs web.

- És un terme pejoratiu que s'usa per a referir-se a hackers no seriosos que es creu que rebutgen els principis ètics dels **hackers professionals(white hat)**, que inclouen la cerca de coneixement, el respecte per les habilitats i un motiu d'auto-educació
 - ❑ Se suposa generalment són nens que manquen de la capacitat d'escriure programes sofisticats o exploits en els seus els propis i que el seu objectiu és intentar impressionar als seus amics o guanyar el crèdit en les comunitats
 - ❑ No obstant això, el terme no es relaciona amb l'edat real del participant.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

4. Que és una eina IDS? El Firewall es pot considerar una eina IDS?

IDS: ens referim a un sistema que s'encarregarà de monitorar el comportament d'una xarxa per a detectar i informar sobre possibles intrusions no autoritzades, amb la qual cosa es pot prevenir que es vegi afectada la integritat de la xarxa.

- També existeix el IPS, una eina molt similar però que a més d'alertar sobre les deteccions també pot bloquejar-les o prevenir-les en el moment de la seva detecció.
- Seguretat perimetral (més enllà del firewall)

FIREWALL: ens referim a firewall és l'eina de seguretat que permet controlar el trànsit d'una xarxa o que està associat amb un equip en particular.

- Generalment compleix amb la funció de filtrar el trànsit de xarxa entre Internet i un dispositiu en particular, i pot funcionar de dues maneres diferents:
 - permetent tots els paquets de xarxa i només bloquejant alguns considerats sospitosos.
 - o bé denegant tots els paquets i només permetent aquells que siguin considerats com a necessaris.
- ❖ Un **IDS** està monitorant la xarxa per a detectar quan un sistema està realitzant una activitat sospitosa a través d'examinar el trànsit de xarxa i les connexions al sistema.
- ❖ El **Firewall** establirà quan una connexió entre dos equips a través d'Internet no està d'acord amb les polítiques de seguretat establertes per a aquest entorn de xarxa.
- ❖ Un **Antivirus** es pot determinar quan en un equip o servidor, un arxiu en particular pot realitzar activitats malicioses que puguin afectar la seguretat de la informació.

Nom i Cognoms

Arnau Subirós Puigarnau

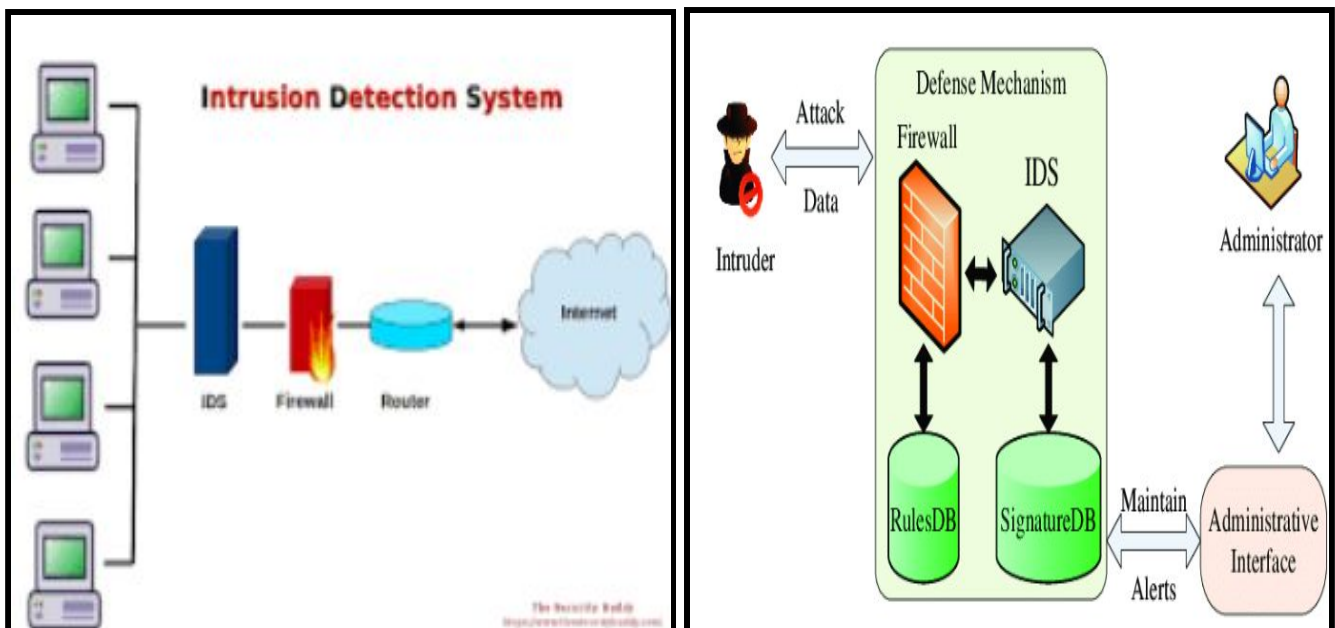
Data

09/02/2019

Podem dir que el **Firewall** no és un **IDS**, són complementaris. Si per exemple un **Black Hat** ha fet una exploració de la xarxa i ha trobat una backdoor fent un atac de DoS(denegació de servei), l'atac passaria desapercebut per el nostre Firewall, però si tenim un IDS saltarien les alarmes fent que configurem el Firewall per evitar l'atac .

Exemple teoric:

- Si un **Firewall** ben configurat bloquejaria l'accés per ports i protocols de comunicacions, **excepte aquells en els quals es desitja oferir certs serveis**. Imaginem que tenim una empresa i vengui els seus productes a través de la Web, **per al que necessitem el nostre servidor Web**. Per a donar el servei, seria necessari que el port **TCP 80** estigués obert.
- Limitacions del nostre Firewall.
 - Un hacker tindria la possibilitat d'atacar el nostre servidor Web a través d'aquest port permès.
 - Normalment les regles, si no s'ha configurat per personal expert en seguretat, bloqueja el trànsit d'entrada, no de sortida.
 -



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

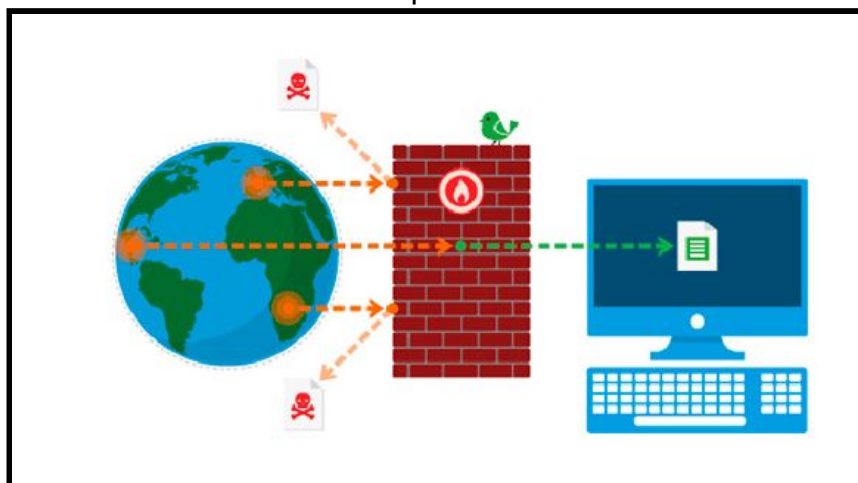
5.Fes una llista de 5 elements que poden comportar atacs a una xarxa i podem gestionar o filtrar amb un Firewall.

Elements que gestiona i filtra un FIREWALL

01. “barridos” de ports i escaneig IP
02. accés remot a estacions de treball, servidors en l' àmbit empresarial
03. Cucs, també denominats “worms”, que s'espargen de computadora en computadora via internet i després prenen el control de la teva computadora.
04. Els Hackers que desitgin entrar en la teva computadora per a prendre el control de la mateixa i fer “atacs disfressats” o robar dades personals que es troben en el disc rígid.
05. Bloqueja el trànsit de sortida per a no deixar que determinats protocols siguin utilitzats per a escampar els virus que pugui arribar a tenir la teva computadora

IMPORTANT (a tenir en compte)

- ☐ Els Firewalls no prevenen d'un atac intern(desde de la mateixa xarxa) per part d'un treballador
- ☐ Un firewall no impedeix tots els atacs, però si no tingués cap instal·lat, n'hi ha prou amb connectar-se a Internet perquè la probabilitat de ser infectat en pocs minuts sigui gran.
- ☐ Un firewall no protegeix la computadora en casos com a virus, spam i spyware. És l'última defensa quan revelem les nostres contrasenyes, o si permetem l'entrada d'agents externs com malware en aplicacions.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

PART PRÀCTICA : Firewall de Windows/configuracions

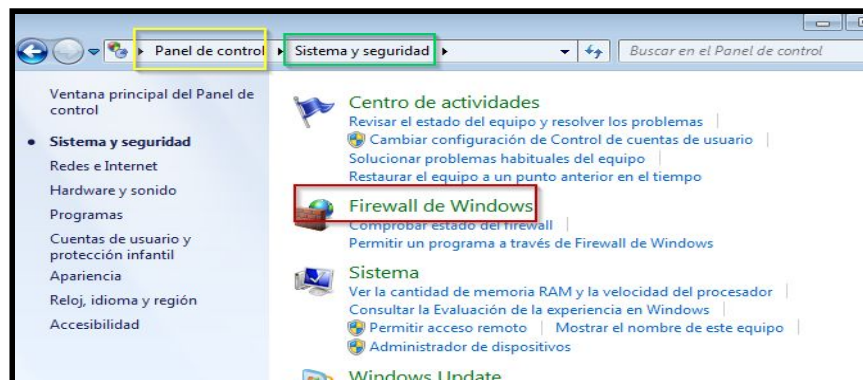
(Per realitzar la pràctica és recomana una màquina virtual de Windows 7 o Windows 10.)

1.Obre la màquina de Windows i ves al Firewall de Windows a l'apartat de configuració avançada.

1. Iniciem una màquina virtual, Windows 7 (Home Basic)



2. Podem accedir a Firewall de 2 formes
 - 2.1. Accedint al Panell de Control
 - 2.1.1. Sistemes i Seguretat
 - 2.1.1.1. Firewall de Windows



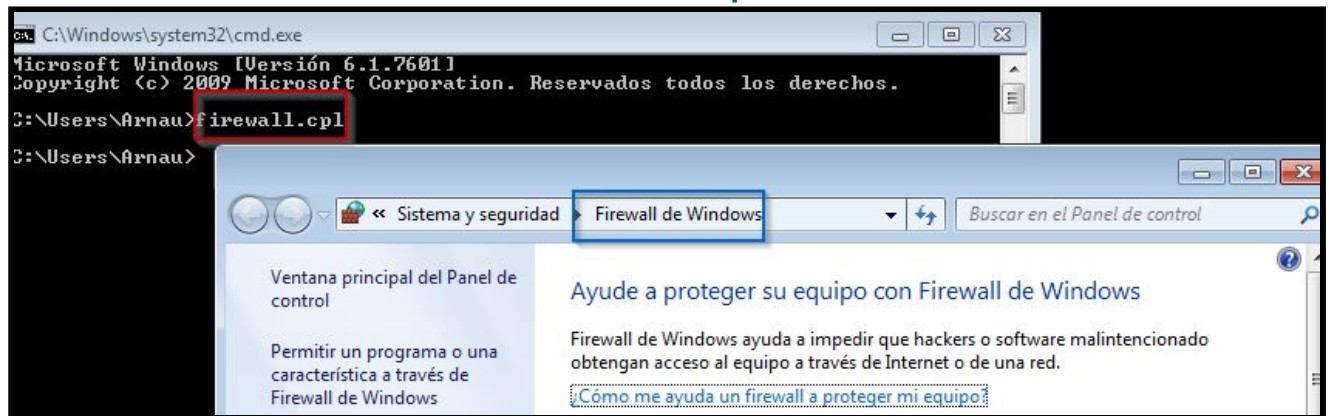
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- 2.2. Accedint al terminal (cmd)
- 2.2.1. utilitzant el comando **firewall.cpl**



3. Seleccionem “**configuració avançada**”



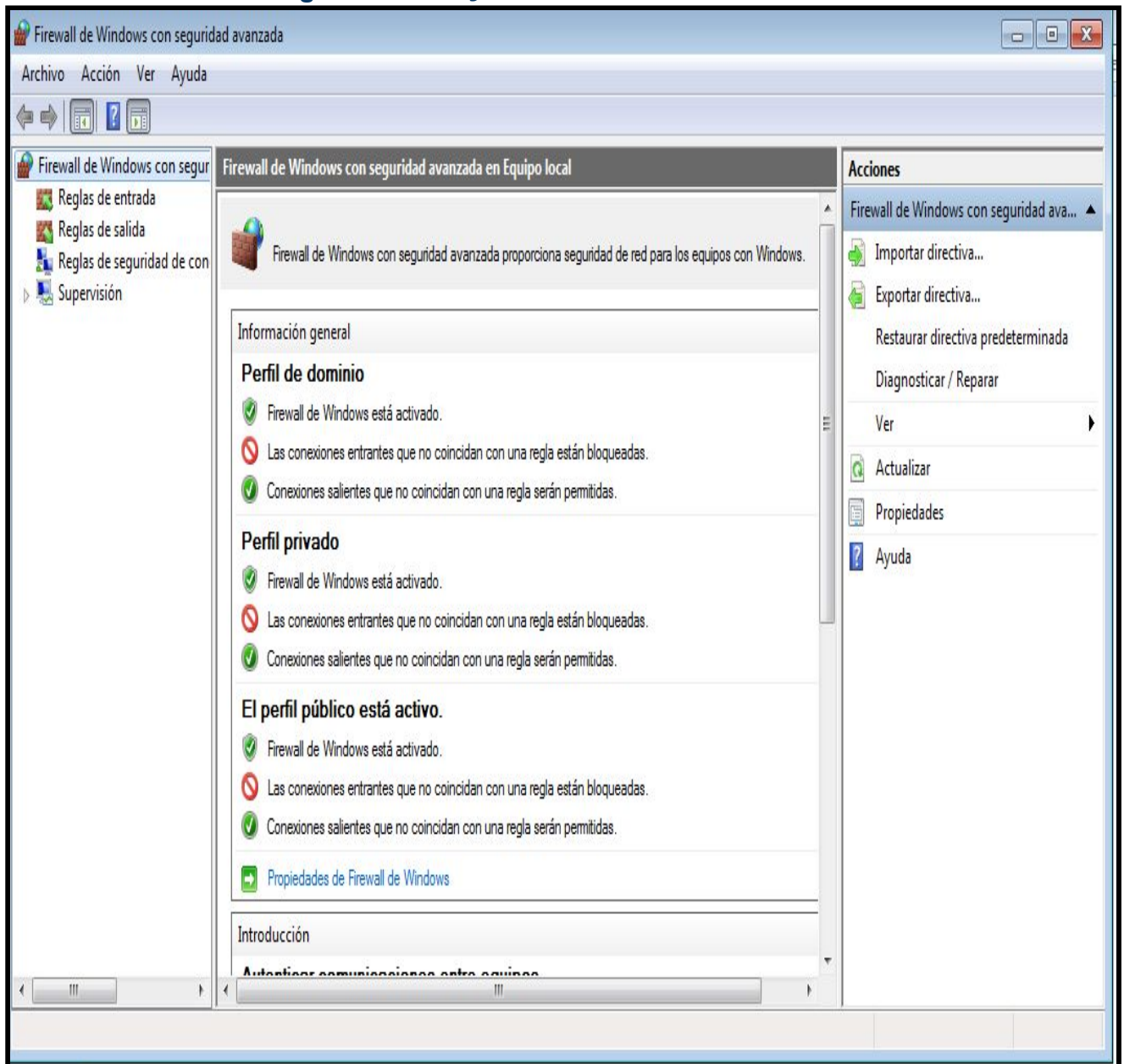
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

4. Accedim a “**configuració avançada**”



Nom i Cognoms

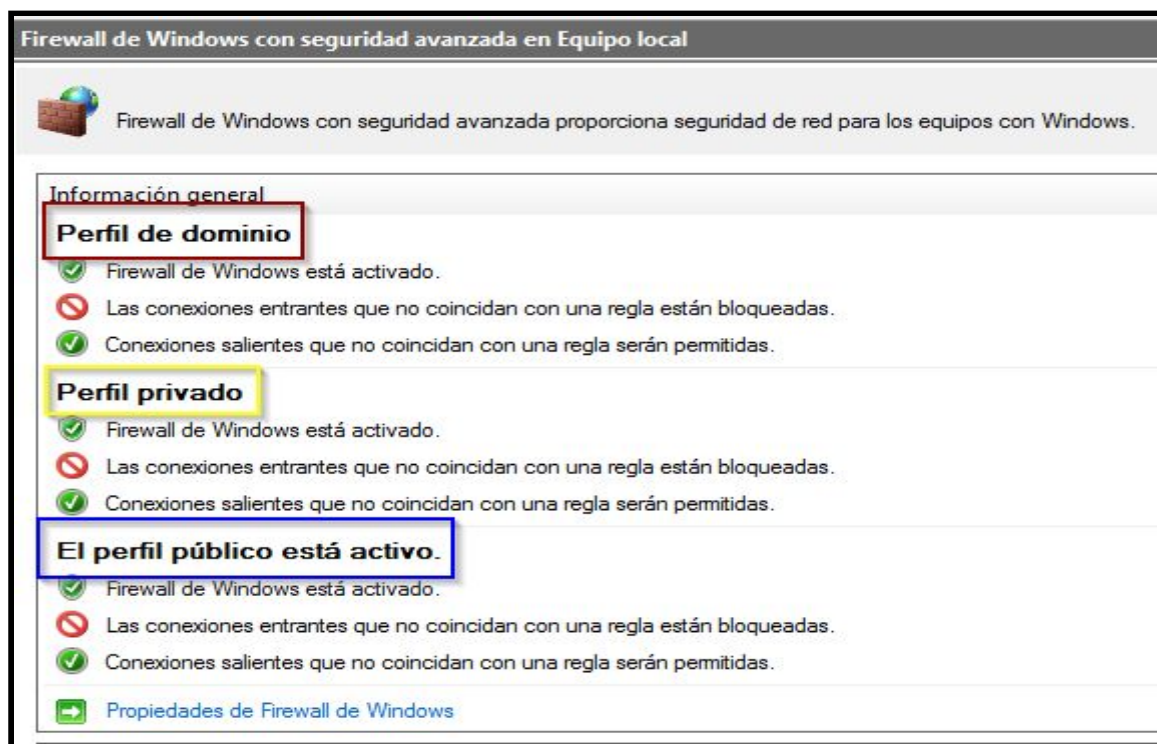
Arnau Subirós Puigarnau

Data

09/02/2019

2. Que és una regla pel que fa els firewalls? Quina diferència hi ha entre una regla d'entrada i una de sortida?

Primer de tot, al accedir a la **configuració avançada** veurem un resum dels 3 perfils : domini, privat i públic



Les regles serveixen per permetre o bloquejar el tràfic de la xarxa . Com es pot veure en la part esquerra, hi ha :

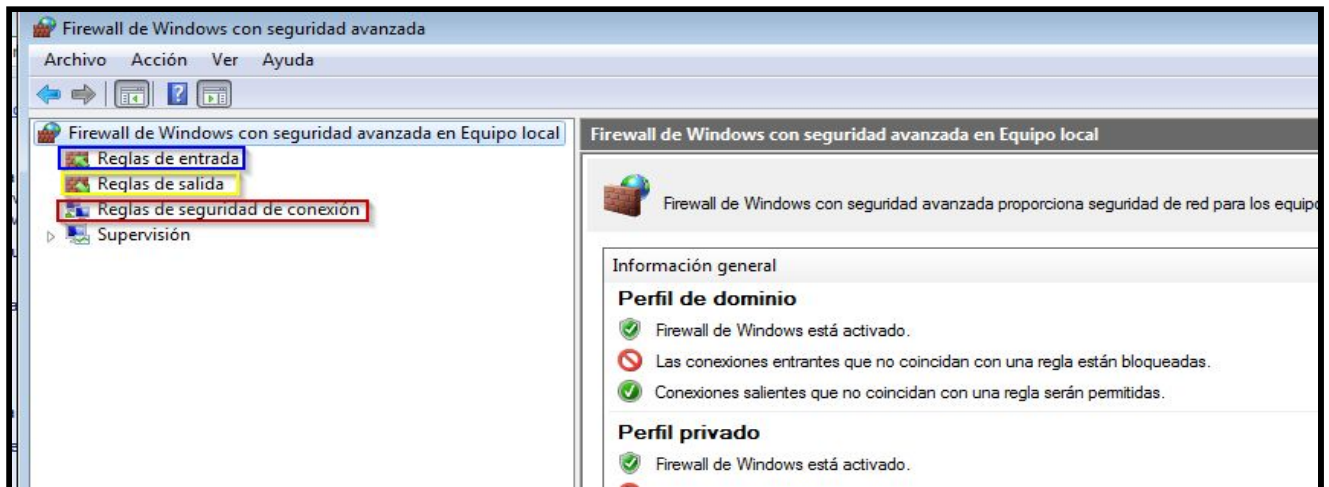
- les regles d'entrada
- les regles de sortida
- les regles de seguridad en la connexió

Nom i Cognoms

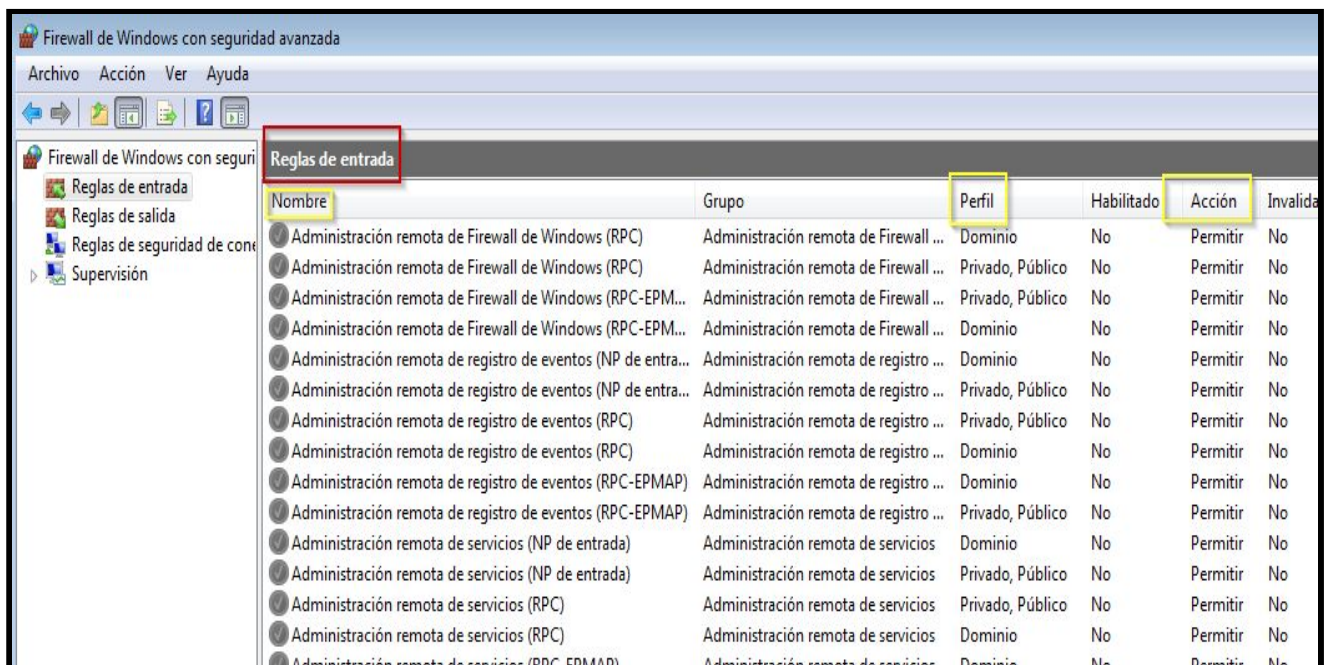
Arnau Subirós Puigarnau

Data

09/02/2019



- ❖ **Regles d'entrada:** Controlen el trànsit que es permet o bloqueja des de fonts externes, és a dir, les connexions que es generen en Internet i que arriben al nostre ordinador.



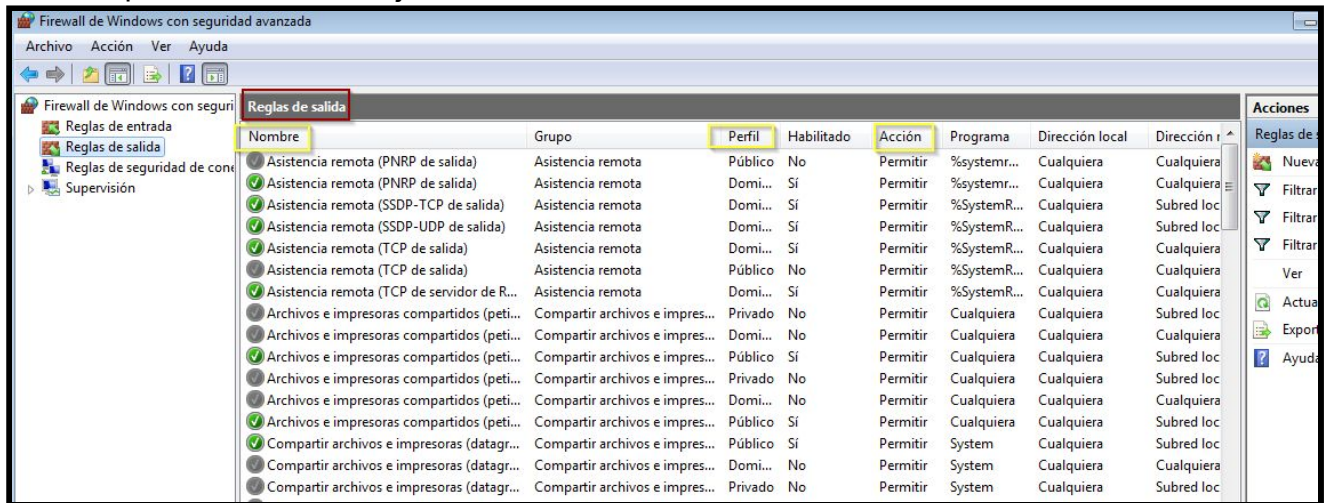
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- ❖ **Regles de sortida :** Controlen les connexions que es generen en el nostre ordinador i que tenen com a objectiu sortir a Internet



3. Quines polítiques de seguretat podem trobar en un Firewall? Indica on podem observar aquestes polítiques de seguretat al Firewall de Windows (fes una captura de pantalla i assenyala quina política de seguretat tens activada en aquell moment)

- Les polítiques d'accessos en un Firewalls s'han de dissenyar posant principal atenció en les seves limitacions i capacitats però també pensant en les amenaces i vulnerabilitats presents en una xarxa externa insegura.
- Conèixer els punts a protegir és el primer pas a l'hora d'establir normes de seguretat. També és important definir els usuaris contra els quals s'ha de protegir cada recurs, ja que les mesures diferiran notablement en funció d'aquests usuaris.
- **Per dissenyar una política de seguretat ens hauriem de fer les següents preguntes:**
 - ❖ Què s'ha de protegir?
 - S'haurien de protegir tots els elements de la xarxa interna (maquinari, programari, dades, etc.).
 - ❖ De qui protegir-se?.

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- De qualsevol intent d'accés no autoritzat des de l'exterior i contra certs atacs des de l'interior que puguin preveure's i prevenir.

❖ Com protegir-se?

➤ Paradigmes de seguretat

- Es permet qualsevol servei excepte aquells expressament prohibits.
- Es prohibeix qualsevol servei excepte aquells expressament permesos.

➤ Estratègies de seguretat

- Paranoica: es controla tot, no es permet res.
- Prudent: es controla i es coneix tot el que succeeix.
- Permissiva: es controla però es permet massa.
- Promíscua: no es controla (o es fa poc) i es permet tot.



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

POLITICAS DE SEGURETAT - Firewall Windows

Regles d'entrada (habilitades)

Nombre	Grupo	Perfil	Habilitado	Protocolo	Puerto local	Puerto remoto	Usuarios permi
Redes principales: tiempo superado (ICMPv6 de entrada)	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: Teredo (UDP de entrada)	Redes principales	Todo	Si	UDP	Cruce segur...	Cualquiera	Cualquiera
Redes principales: solicitud de enrutador (ICMPv6 de entra...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: solicitud de detección de vecinos (ICMP...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: Protocolo de configuración dinámica de ...	Redes principales	Todo	Si	UDP	546	547	Cualquiera
Redes principales: Protocolo de configuración dinámica de ...	Redes principales	Todo	Si	UDP	68	67	Cualquiera
Redes principales: Protocolo de administración de grupo d...	Redes principales	Todo	Si	IGMP	Cualquiera	Cualquiera	Cualquiera
Redes principales: problema de parámetro (ICMPv6 de entr...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: paquete demasiado grande (ICMPv6 de ...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: IPv6 (IPv6 de entrada)	Redes principales	Todo	Si	IPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: IPHTTPS (TCP de entrada)	Redes principales	Todo	Si	TCP	IPHTTPS	Cualquiera	Cualquiera
Redes principales: informe de escucha de multidifusión v2 (...)	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: informe de escucha de multidifusión (IC...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: escucha de multidifusión finalizada (ICM...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: destino inaccesible fragmentación neces...	Redes principales	Todo	Si	ICMPv4	Cualquiera	Cualquiera	Cualquiera
Redes principales: destino inaccesible (ICMPv6 de entrada)	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: consulta de escucha de multidifusión (IC...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: anuncio de enrutador (ICMPv6 de entrada)	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Redes principales: anuncio de detección de vecinos (ICMPv...	Redes principales	Todo	Si	ICMPv6	Cualquiera	Cualquiera	Cualquiera
Google Chrome (tráfico mDNS entrante)	Google Chrome	Todo	Si	UDP	5353	Cualquiera	Cualquiera
Detección de redes (WSD de entrada)	Detección de redes	Privado	Si	UDP	3702	Cualquiera	Cualquiera
Detección de redes (UPnP de entrada)	Detección de redes	Privado	Si	TCP	2869	Cualquiera	Cualquiera
Detección de redes (SSDP de entrada)	Detección de redes	Privado	Si	UDP	1900	Cualquiera	Cualquiera

Nombre	Grupo	Perfil	Habilitado	Protocolo	Puerto remoto	Puerto local	Acción	Usuarios per...
Detección de redes (Pub-WSD de entrada)	Detección de redes	Privado	Si	UDP	Cualquiera	3702	Permitir	Cualquiera
Detección de redes (nombre NB de entrada)	Detección de redes	Privado	Si	UDP	Cualquiera	137	Permitir	Cualquiera
Detección de redes (LLMNR-UDP de entrada)	Detección de redes	Privado	Si	UDP	Cualquiera	5355	Permitir	Cualquiera
Detección de redes (Eventos seguros WSD de entra...	Detección de redes	Privado	Si	TCP	Cualquiera	5358	Permitir	Cualquiera
Detección de redes (Eventos de WSD de entrada)	Detección de redes	Privado	Si	TCP	Cualquiera	5357	Permitir	Cualquiera
Detección de redes (datagrama NB de entrada)	Detección de redes	Privado	Si	UDP	Cualquiera	138	Permitir	Cualquiera
Compartir archivos e impresoras (SMB de entrada)	Compartir archiv...	Público	Si	TCP	Cualquiera	445	Permitir	Cualquiera
Compartir archivos e impresoras (sesión NB de ent...	Compartir archiv...	Público	Si	TCP	Cualquiera	139	Permitir	Cualquiera
Compartir archivos e impresoras (servicio Administ...	Compartir archiv...	Público	Si	TCP	Cualquiera	Asignador d...	Permitir	Cualquiera
Compartir archivos e impresoras (servicio Administ...	Compartir archiv...	Público	Si	TCP	Cualquiera	Puertos diná...	Permitir	Cualquiera
Compartir archivos e impresoras (nombre NB de e...	Compartir archiv...	Público	Si	UDP	Cualquiera	137	Permitir	Cualquiera
Compartir archivos e impresoras (LLMNR-UDP de ...	Compartir archiv...	Público	Si	UDP	Cualquiera	5355	Permitir	Cualquiera
Compartir archivos e impresoras (datagrama NB d...	Compartir archiv...	Público	Si	UDP	Cualquiera	138	Permitir	Cualquiera
Asistencia remota (TCP de servidor de RA de entra...	Asistencia remota	Dom...	Si	TCP	Cualquiera	Cualquiera	Permitir	Cualquiera
Asistencia remota (TCP de entrada)	Asistencia remota	Dom...	Si	TCP	Cualquiera	Cualquiera	Permitir	Cualquiera
Asistencia remota (SSDP-UDP de entrada)	Asistencia remota	Dom...	Si	UDP	Cualquiera	1900	Permitir	Cualquiera
Asistencia remota (SSDP-TCP de entrada)	Asistencia remota	Dom...	Si	TCP	Cualquiera	2869	Permitir	Cualquiera
Asistencia remota (PNRP de entrada)	Asistencia remota	Dom...	Si	UDP	Cualquiera	3540	Permitir	Cualquiera
Asistencia remota (DCOM de entrada)	Asistencia remota	Dom...	Si	TCP	Cualquiera	135	Permitir	Cualquiera
Archivos e impresoras compartidos (petición eco: I...	Compartir archiv...	Público	Si	ICMPv6	Cualquiera	Cualquiera	Permitir	Cualquiera
Archivos e impresoras compartidos (petición eco: I...	Compartir archiv...	Público	Si	ICMPv4	Cualquiera	Cualquiera	Permitir	Cualquiera

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

Regles de sortida (habilitades)

Nombre	Grupo	Perfil	Habilitado	Acción	Protocolo	Puerto local	Puerto remoto	Dirección remota	Equipos
Reglas principales: tiempo superado (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: Teredo (UDP de salida)	Reglas principales	Todo	Sí	Permitir	UDP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: solicitud de enrutador (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local, ff02::...	Cualquiera
Reglas principales: solicitud de detección de vecinos (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: Protocolo de configuración dinámica de grupo (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	UDP	546	547	Cualquiera	Cualquiera
Reglas principales: Protocolo de configuración dinámica de grupo (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	UDP	68	67	Cualquiera	Cualquiera
Reglas principales: Protocolo de administración de grupo (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	IGMP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: problema de parámetro (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: paquete demasiado grande (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: IPv6 (IPv6 de salida)	Reglas principales	Todo	Sí	Permitir	IPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: IPHTTPS (TCP de salida)	Reglas principales	Todo	Sí	Permitir	TCP	Cualquiera	IPHTTPS	Cualquiera	Cualquiera
Reglas principales: informe de escucha de multidifusión v2 (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local	Cualquiera
Reglas principales: informe de escucha de multidifusión (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local	Cualquiera
Reglas principales: escucha de multidifusión finalizada (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local	Cualquiera
Reglas principales: DNS (UDP de salida)	Reglas principales	Todo	Sí	Permitir	UDP	Cualquiera	53	Cualquiera	Cualquiera
Reglas principales: directiva de grupo (TCP de salida)	Reglas principales	Dominio	Sí	Permitir	TCP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: directiva de grupo (NP de salida)	Reglas principales	Dominio	Sí	Permitir	TCP	Cualquiera	445	Cualquiera	Cualquiera
Reglas principales: directiva de grupo (LSASS de salida)	Reglas principales	Dominio	Sí	Permitir	TCP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Reglas principales: consulta de escucha de multidifusión (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local	Cualquiera
Reglas principales: anuncio de enrutador (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local, ff02::...	Cualquiera
Reglas principales: anuncio de detección de vecinos (ICMPv6 de salida)	Reglas principales	Todo	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Detección de redes (WSD de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	3702	Subred local	Cualquiera
Detección de redes (UPnPHost de salida)	Detección de redes	Privado	Sí	Permitir	TCP	Cualquiera	Cualquiera	Subred local	Cualquiera
Detección de redes (UDP de salida)	Detección de redes	Privado	Sí	Permitir	TCP	Cualquiera	Cualquiera	Subred local	Cualquiera
Detección de redes (SSDP de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	1900	Subred local	Cualquiera
Detección de redes (Pub-WSD de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	3702	Subred local	Cualquiera
Detección de redes (nombre NB de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	137	Subred local	Cualquiera
Detección de redes (LLMNR-UDP de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	5355	Subred local	Cualquiera
Detección de redes (Eventos seguros WSD de salida)	Detección de redes	Privado	Sí	Permitir	TCP	Cualquiera	5358	Subred local	Cualquiera
Detección de redes (Eventos de WSD de salida)	Detección de redes	Privado	Sí	Permitir	TCP	Cualquiera	5357	Subred local	Cualquiera
Detección de redes (datagrama NB de salida)	Detección de redes	Privado	Sí	Permitir	UDP	Cualquiera	138	Subred local	Cualquiera
Compartir archivos e impresoras (SMB de salida)	Compartir archivos e impres...	Público	Sí	Permitir	TCP	Cualquiera	445	Subred local	Cualquiera
Compartir archivos e impresoras (sesión NB de salida)	Compartir archivos e impres...	Público	Sí	Permitir	TCP	Cualquiera	139	Subred local	Cualquiera
Compartir archivos e impresoras (nombre NB de salida)	Compartir archivos e impres...	Público	Sí	Permitir	UDP	Cualquiera	137	Subred local	Cualquiera
Compartir archivos e impresoras (LLMNR-UDP de salida)	Compartir archivos e impres...	Público	Sí	Permitir	UDP	Cualquiera	5355	Subred local	Cualquiera
Compartir archivos e impresoras (datagrama NB de salida)	Compartir archivos e impres...	Público	Sí	Permitir	UDP	Cualquiera	138	Subred local	Cualquiera
Asistencia remota (TCP de servidor de RA de salida)	Asistencia remota	Dominio	Sí	Permitir	TCP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Asistencia remota (TCP de salida)	Asistencia remota	Dominio	Sí	Permitir	TCP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Asistencia remota (SSDP-UDP de salida)	Asistencia remota	Dominio	Sí	Permitir	UDP	Cualquiera	1900	Subred local	Cualquiera
Asistencia remota (SSDP-TCP de salida)	Asistencia remota	Dominio	Sí	Permitir	TCP	Cualquiera	Cualquiera	Subred local	Cualquiera
Asistencia remota (PNRP de salida)	Asistencia remota	Dominio	Sí	Permitir	UDP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Archivos e impresoras compartidos (petición eco: ICMPv6 de salida)	Compartir archivos e impres...	Público	Sí	Permitir	ICMPv6	Cualquiera	Cualquiera	Subred local	Cualquiera
Archivos e impresoras compartidos (petición eco: ICMPv4 de salida)	Compartir archivos e impres...	Público	Sí	Permitir	ICMPv4	Cualquiera	Cualquiera	Subred local	Cualquiera
Windows Peer to Peer Collaboration Foundation (WSD de salida)	Windows Peer to Peer Colla...	Todo	No	Permitir	UDP	Cualquiera	3702	Subred local	Cualquiera
Windows Peer to Peer Collaboration Foundation (TCP de salida)	Windows Peer to Peer Colla...	Todo	No	Permitir	TCP	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Windows Peer to Peer Collaboration Foundation (SSDP de salida)	Windows Peer to Peer Colla...	Todo	No	Permitir	UDP	Cualquiera	1900	Subred local	Cualquiera
Windows Peer to Peer Collaboration Foundation (PNRP de salida)	Windows Peer to Peer Colla...	Todo	No	Permitir	UDP	Cualquiera	3540	Cualquiera	Cualquiera

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

4.Crea 3 regles amb el Firewall de Windows:

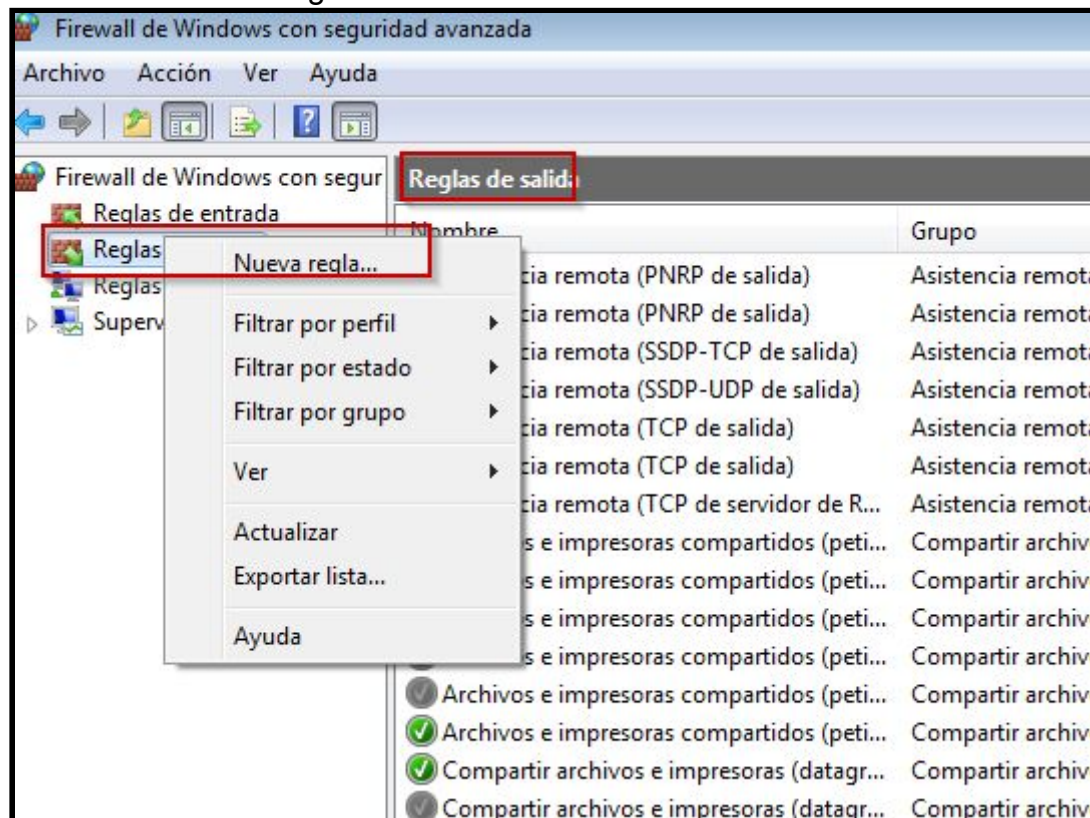
Explica quin és el procés, des d'on s'habilita i es des-habilita les regles de el següent link és un recurs interessant on es mostra com es gestionen les regles als firewalls de Windows:

<https://www.discoduroderoer.es/reglas-de-entrada-y-salida-firewall-de-windows-7/>

- Bloqueig del port 80,8080 i 443. Que creus que passa si deshabilites aquests ports?
- Bloqueig d'una pàgina web. La que vulgueu.
- Bloqueig d'una aplicació (per exemple Skype)

❖ Bloqueig del port 80,8080 i 443.

- Crearem una nova regla de sortida



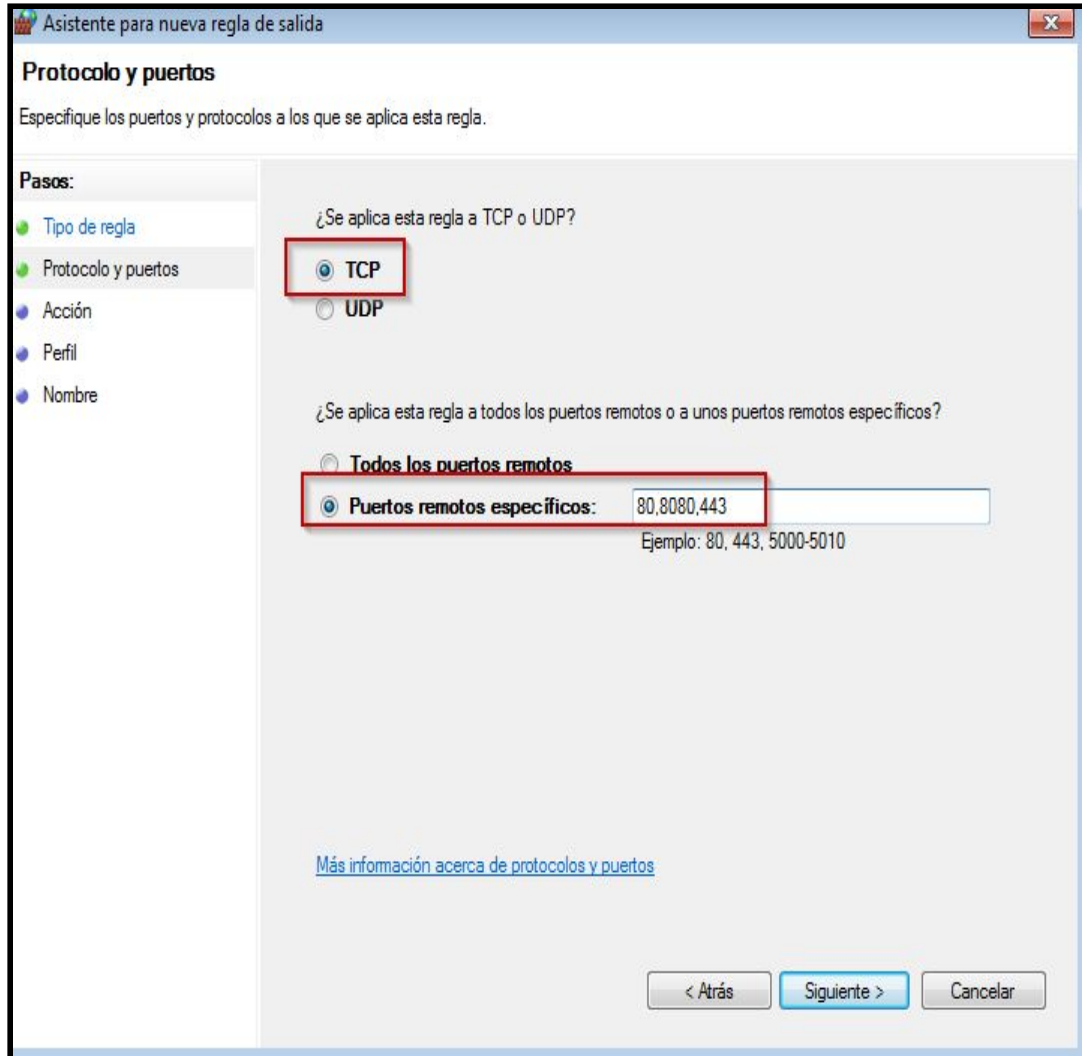
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Seleccionem la regla que controla els **ports**



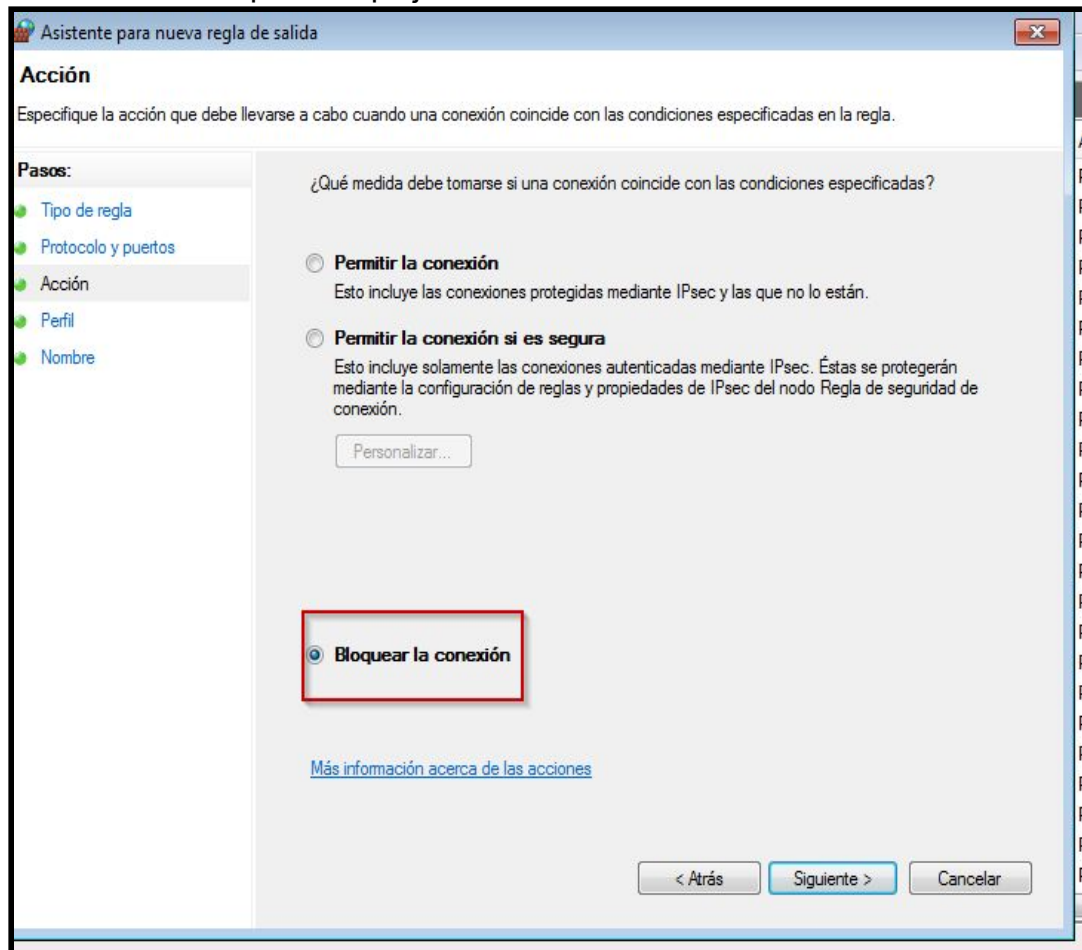
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Seleccionem la opció bloquejar la connexió



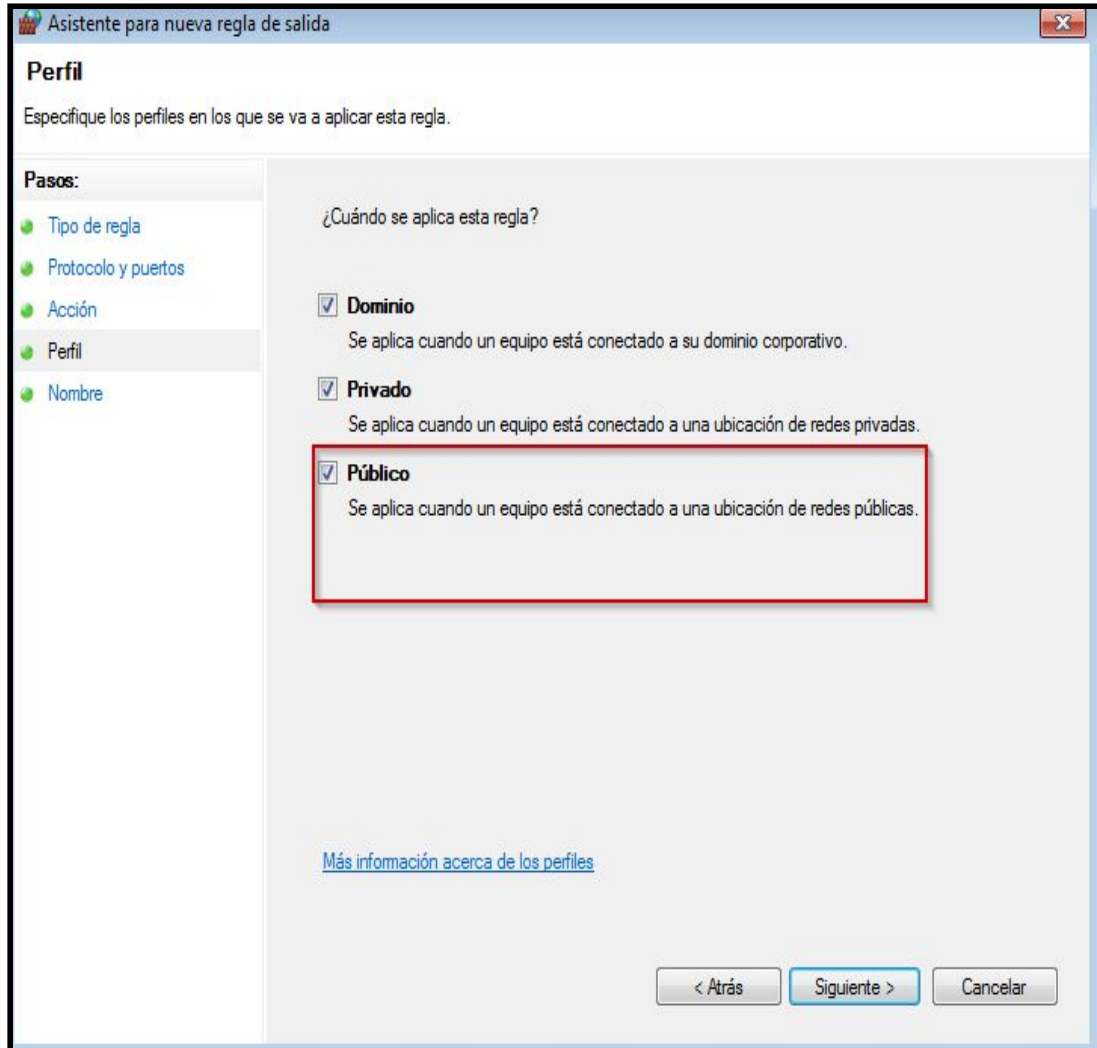
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Seleccionem el perfil tots els perfils , però realment el que ens interessa és el “**públic**”



Asistente para nueva regla de salida

Perfil

Especifique los perfiles en los que se va a aplicar esta regla.

Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil**
- Nombre

¿Cuándo se aplica esta regla?

- ☒ **Dominio**
Se aplica cuando un equipo está conectado a su dominio corporativo.
- ☒ **Privado**
Se aplica cuando un equipo está conectado a una ubicación de redes privadas.
- ☒ **Público**
Se aplica cuando un equipo está conectado a una ubicación de redes públicas.

[Más información acerca de los perfiles](#)

< Atrás Siguiente > Cancelar

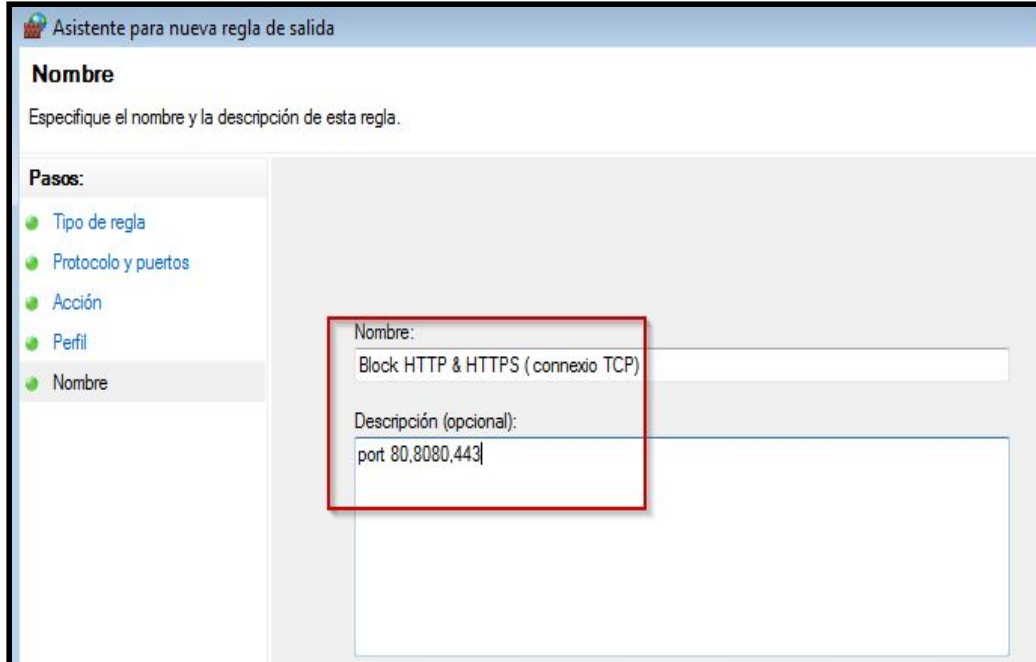
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Anotem el nom de la regla i li donem a finalitzar.



Nom i Cognoms

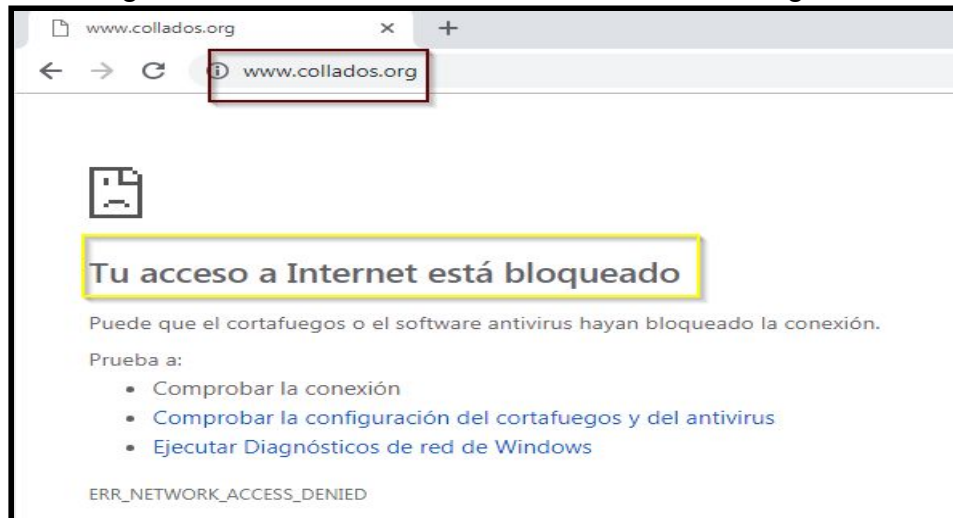
Arnau Subirós Puigarnau

Data

09/02/2019

- Ara obrim el navegador i intentem accedir a pàgines http(port80) i https(port 443)

❑ Pàgines HTTP. Intento accedir a www.collados.org



❑ Pàgina HTTPS. Intento accedir a <https://www.google.es>



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

Aquesta regla ha configurat que bloquegi les connexions TCP amb els ports 80,8080 que utilitza el protocol HTTP i el port 443 que utilitza el protocol segur HTTPS .

ANOTACIONS : realment seria recomanat afegir una altra regla (identica a l'anterior) però per connexions UDP.

Nombre	Grupo	Perfil	Habilitado	Acción	Protocolo	Puerto remoto	Puerto local	Programa	Dirección remota	Dirección local
Block HTTP i HTTPS - connexio TCP		Todo	Sí	Bloquear	TCP	80, 8080, 443	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Block HTTPS i HTTPS - connexio UDP		Todo	Sí	Bloquear	UDP	80, 8080, 443	Cualquiera	Cualquiera	Cualquiera	Cualquiera
Compartir archivos e impresoras (datagr...)	Compart...	Domini...	No	Permitir	UDP	138	Cualquiera	System	Cualquiera	Cualquiera
Compartir archivos e impresoras (datagr...)	Compart...	Público	Sí	Permitir	UDP	138	Cualquiera	System	Subred local	Cualquiera
Compartir archivos e impresoras (datagr...)	Compart...	Privado	No	Permitir	UDP	138	Cualquiera	System	Subred local	Cualquiera
Compartir archivos e impresoras (LLMNR...)	Compart...	Domini...	No	Permitir	UDP	5355	Cualquiera	%SystemR...	Subred local	Cualquiera
Compartir archivos e impresoras (LLMNR...)	Compart...	Público	Sí	Permitir	UDP	5355	Cualquiera	%SystemR...	Subred local	Cualquiera
Compartir archivos e impresoras (nombr...)	Compart...	Público	Sí	Permitir	UDP	137	Cualquiera	System	Subred local	Cualquiera
Compartir archivos e impresoras (nombr...)	Compart...	Domini...	No	Permitir	UDP	137	Cualquiera	System	Cualquiera	Cualquiera
Compartir archivos e impresoras (nombr...)	Compart...	Privado	No	Permitir	UDP	137	Cualquiera	System	Subred local	Cualquiera
Compartir archivos e impresoras (sesión ...)	Compart...	Domini...	No	Permitir	TCP	139	Cualquiera	System	Cualquiera	Cualquiera

Per acabar, seleccionem les 2 regles i les deshabilitem per comprovar que podem accedir a les 2 pàgines anteriors.

The screenshot shows the 'Reglas de salida' window with the two blocking rules disabled. Below the window, two browser windows are open:

- Internet Explorer: Address bar shows www.collados.org. The page content includes the text: *"You might be a programmer if most people say: Go To Hell, but you tell people to redirect to /dev/null" (Anonymous)*
- Google Chrome: Address bar shows <https://www.google.es>.

Nom i Cognoms

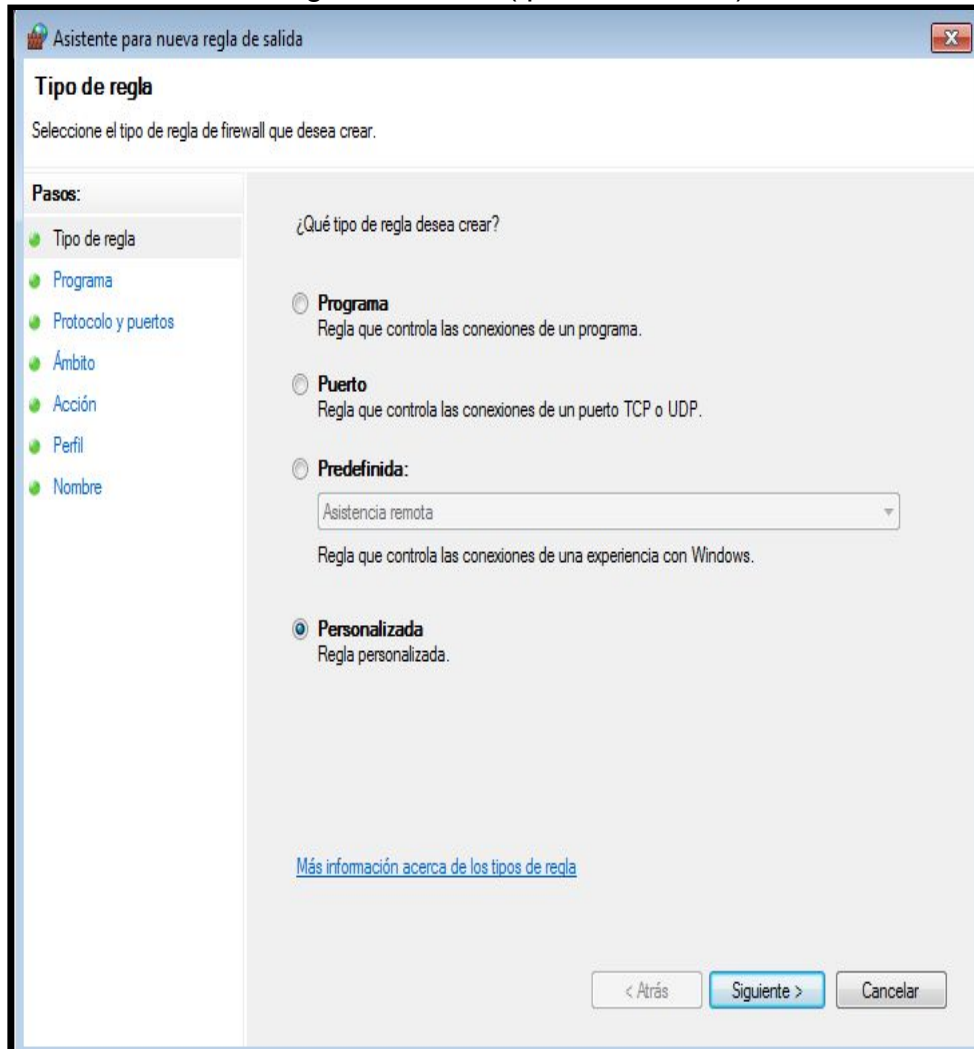
Arnau Subirós Puigarnau

Data

09/02/2019

❖ Bloqueig d'una pàgina.

- Crearem una nova regla de sortida (personalitzada)

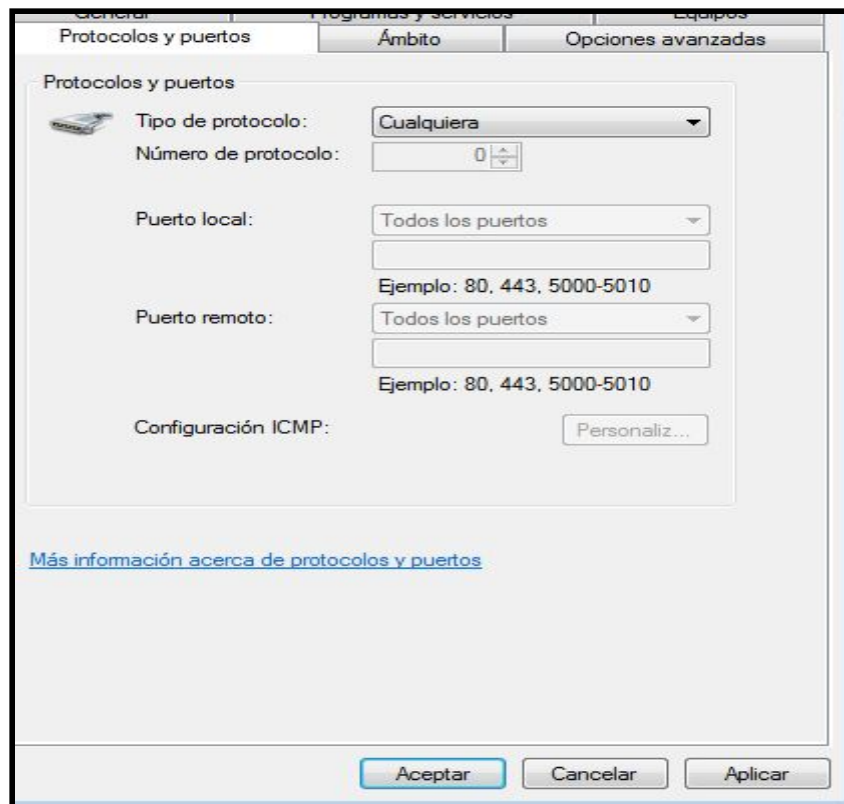


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019



- Primer obrirem el terminal i farem ping a www.collados.org (per saber la IP)

```
C:\Windows\system32\cmd.exe

G:\Users\Arnau>ping www.collados.org

Haciendo ping a collados.org [139.162.131.226] con 32 bytes de datos:
Respuesta desde 139.162.131.226: bytes=32 tiempo=53ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=60ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=52ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=53ms TTL=50

Estadísticas de ping para 139.162.131.226:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 52ms, Máximo = 60ms, Media = 54ms

G:\Users\Arnau>
```

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Anotem la IP que volem bloquejar

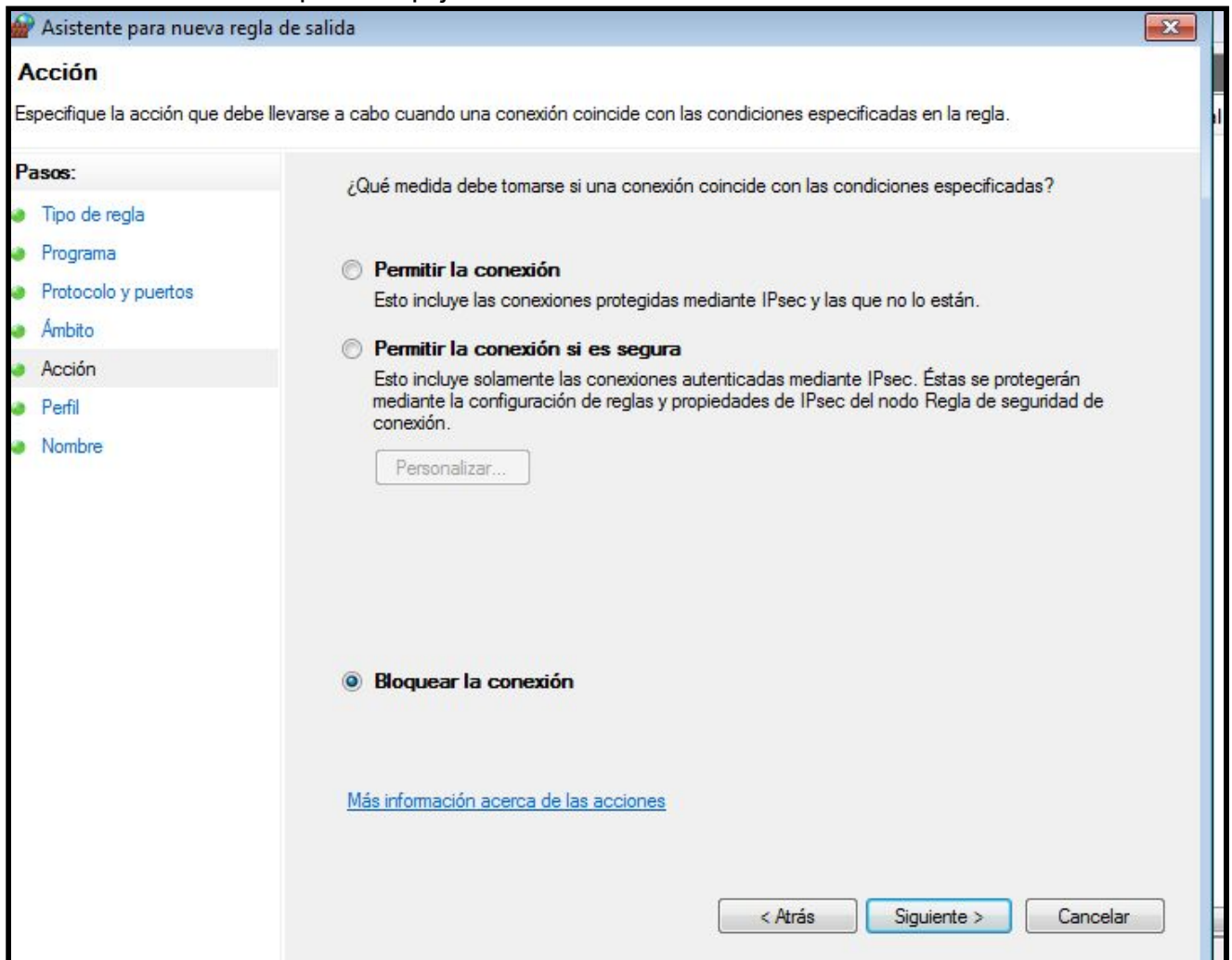
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Seleccionem l'opció bloquejar la connexió



Asistente para nueva regla de salida

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

- Tipo de regla
- Programa
- Protocolo y puertos
- Ámbito
- Acción**
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☐ **Permitir la conexión**
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

☒ **Bloquear la conexión**

[Más información acerca de las acciones](#)

< Atrás Siguinte > Cancelar

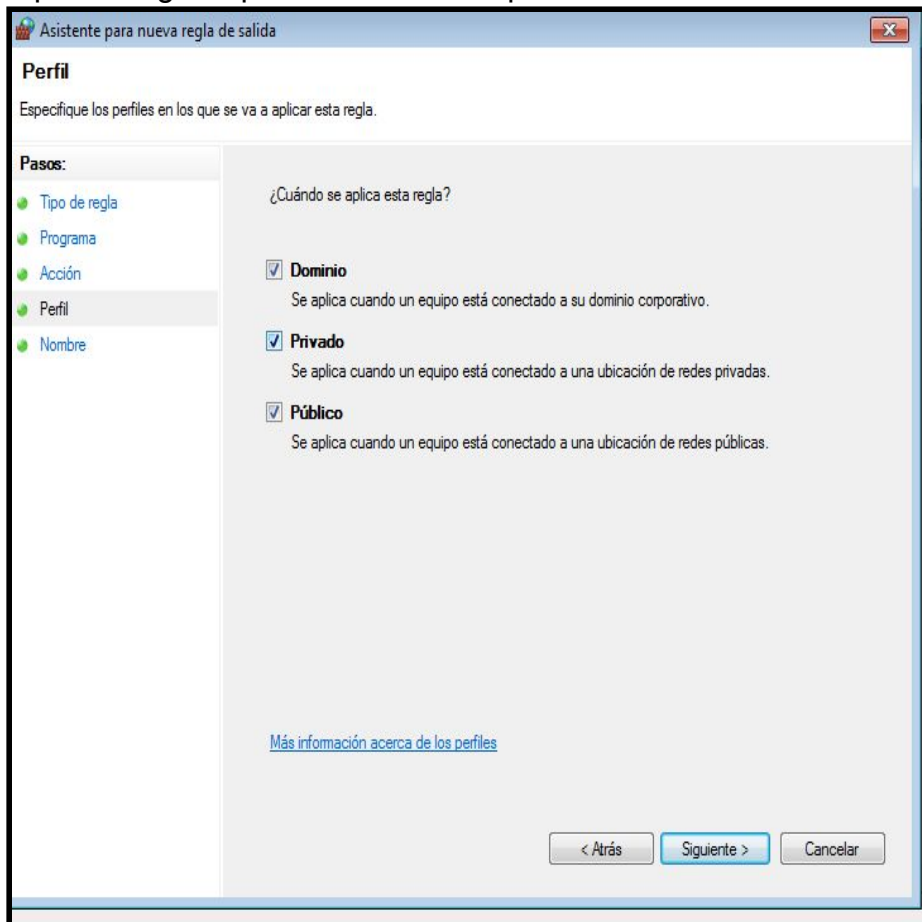
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Aquesta regla l'aplicarem a tots els perfils



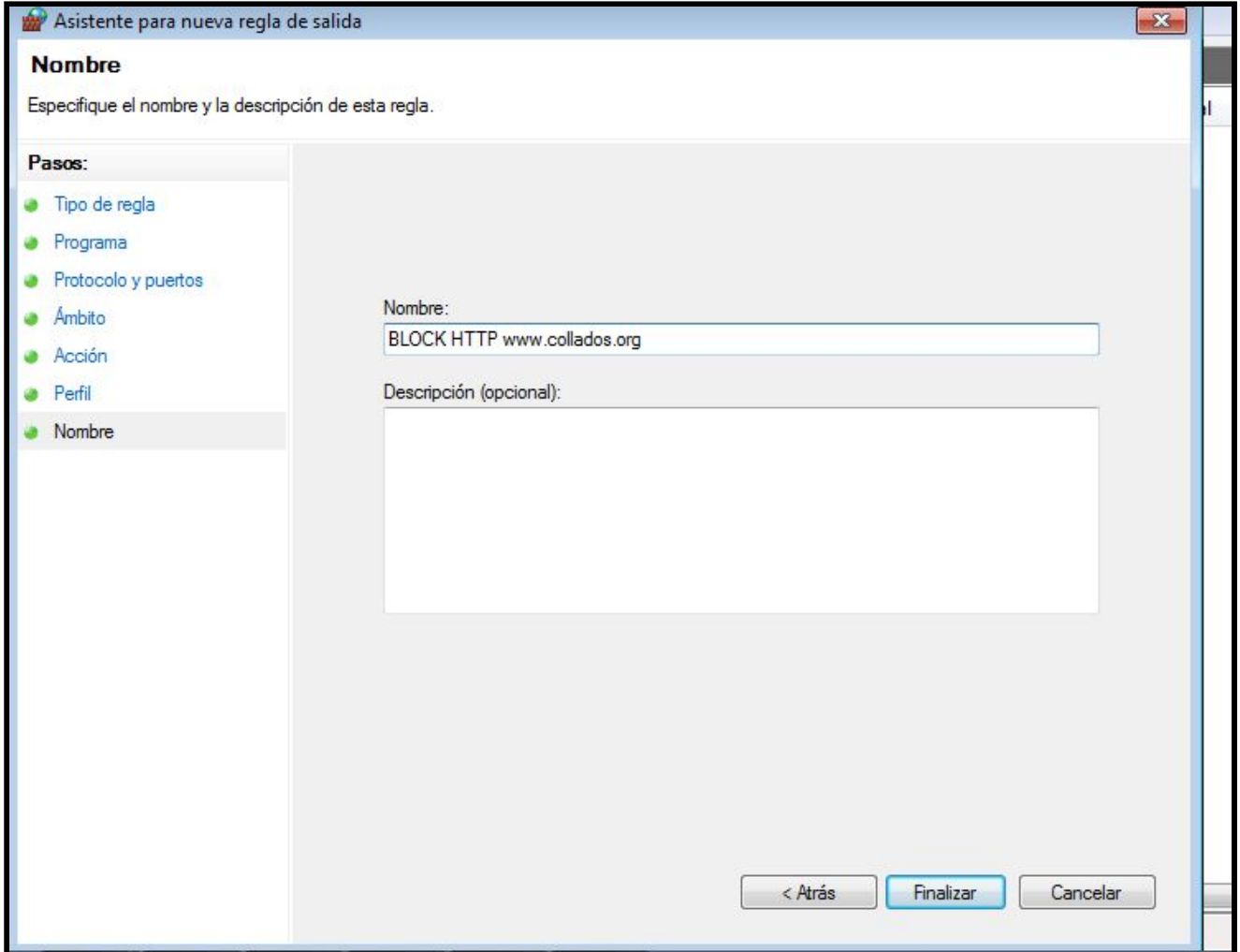
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Anotem el nom de la pàgina bloquejada



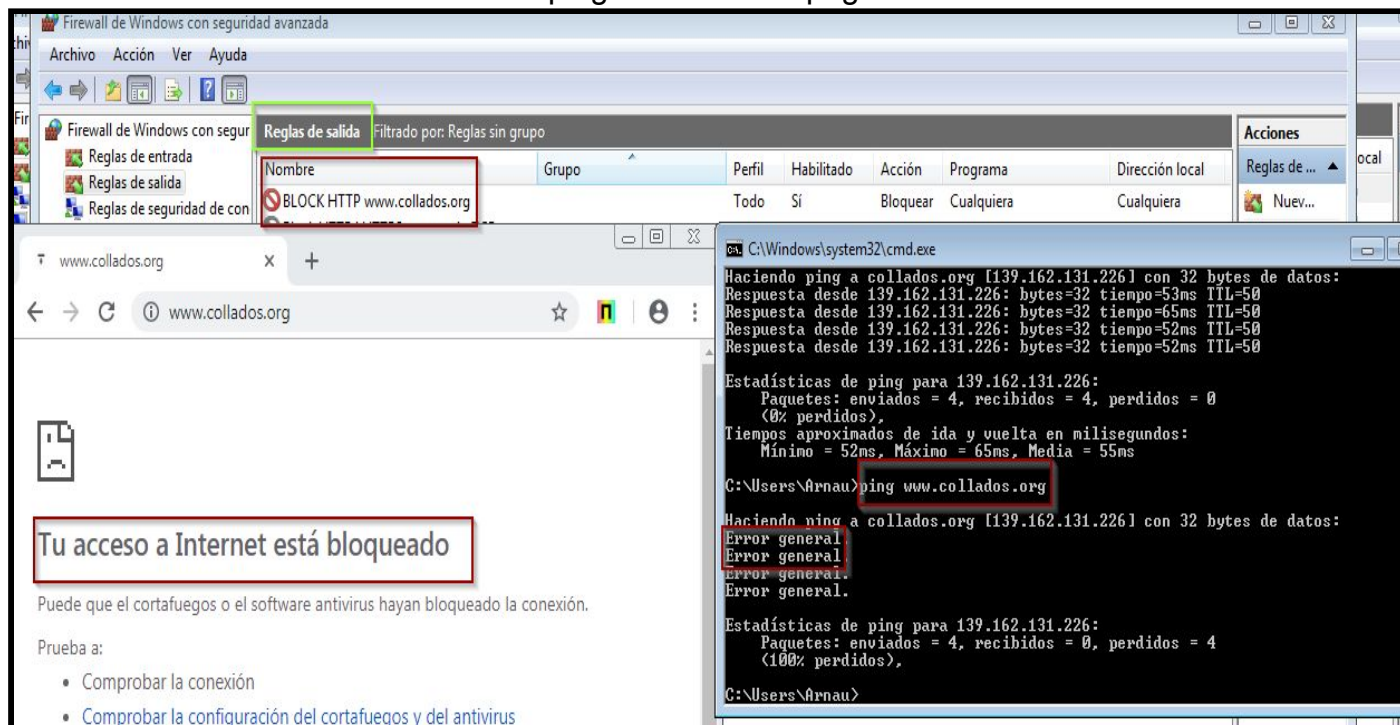
Nom i Cognoms

Arnau Subirós Puigarnau

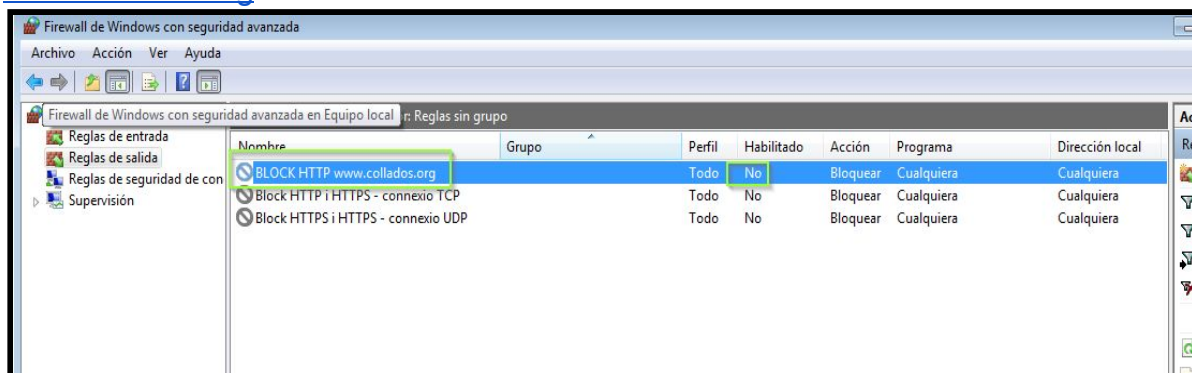
Data

09/02/2019

- Per acabar intentarem fer ping i accedir a la pàgina seleccionada



- I per finalitzar deshabilitarem la regla i confirmem que podem fer ping a www.collados.org

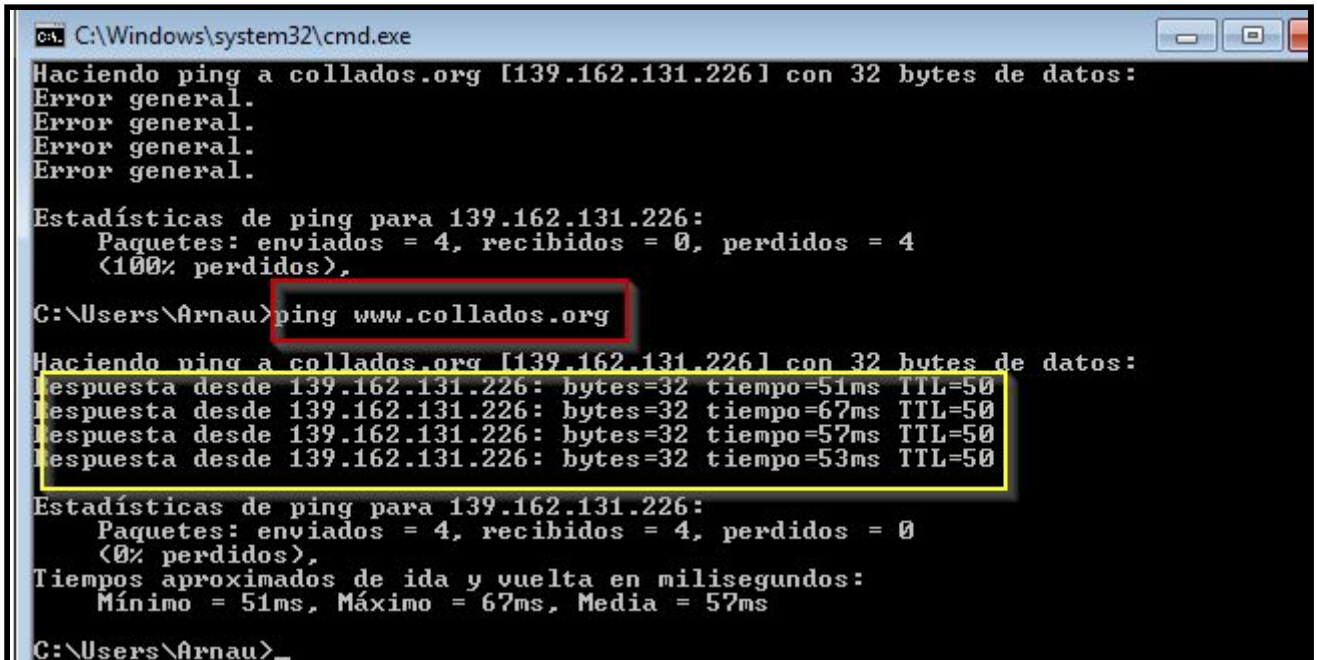


Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019



```
C:\Windows\system32\cmd.exe
Haciendo ping a collados.org [139.162.131.226] con 32 bytes de datos:
Error general.
Error general.
Error general.
Error general.

Estadísticas de ping para 139.162.131.226:
    Paquetes: enviados = 4, recibidos = 0, perdidos = 4
    (100% perdidos),

C:\Users\Arnau>ping www.collados.org
Haciendo ping a collados.org [139.162.131.226] con 32 bytes de datos:
Respuesta desde 139.162.131.226: bytes=32 tiempo=51ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=67ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=57ms TTL=50
Respuesta desde 139.162.131.226: bytes=32 tiempo=53ms TTL=50

Estadísticas de ping para 139.162.131.226:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 51ms, Máximo = 67ms, Media = 57ms

C:\Users\Arnau>_
```

Nom i Cognoms

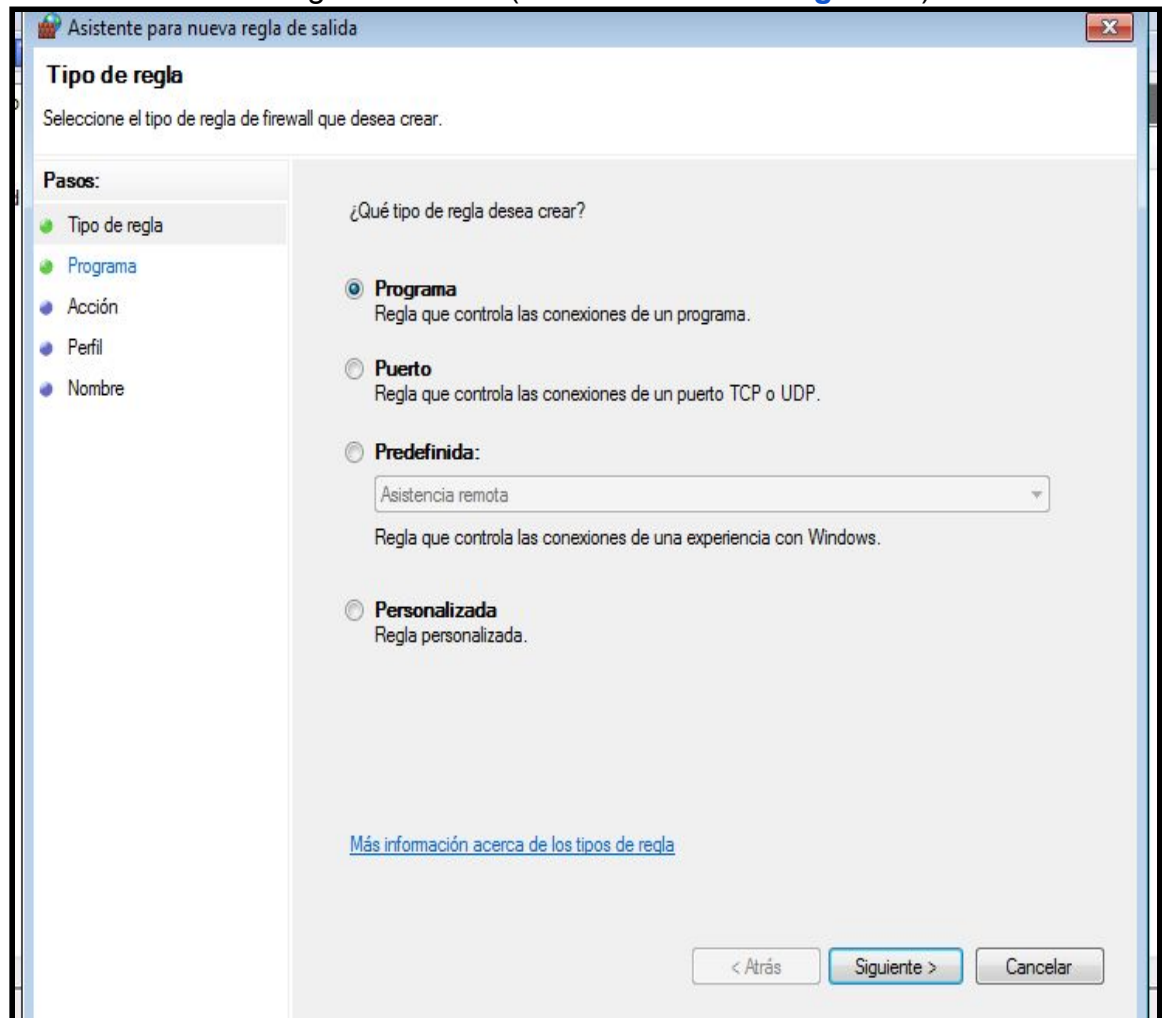
Arnau Subirós Puigarnau

Data

09/02/2019

❖ Bloqueig d'una aplicació.

- Crearem una nova regla de sortida (seleccionarem **"Programa"**)



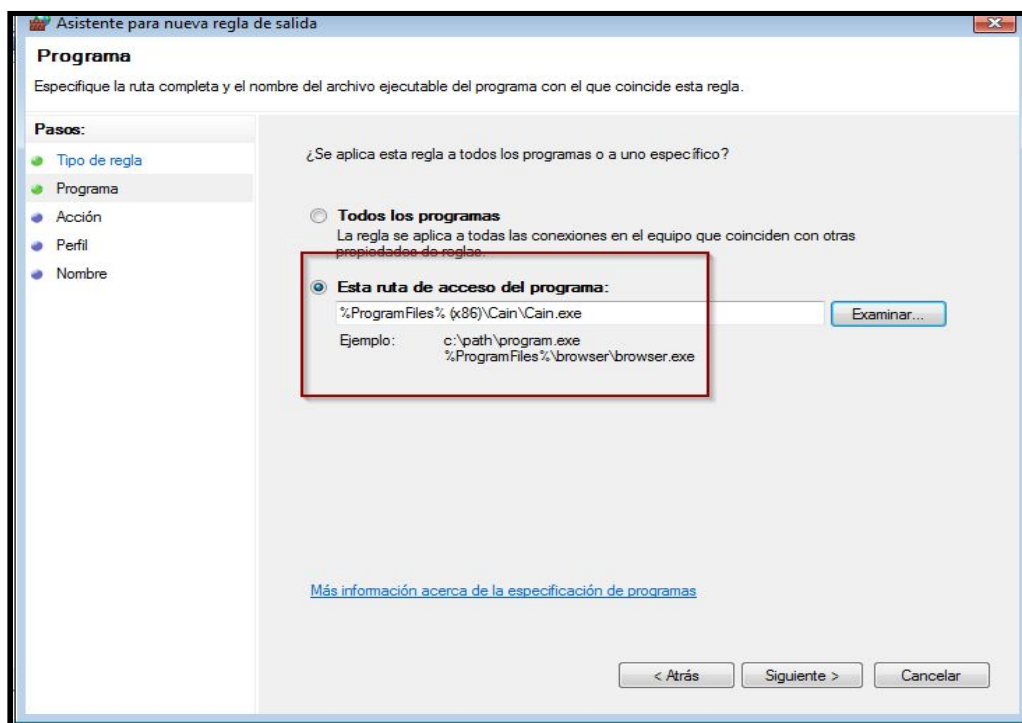
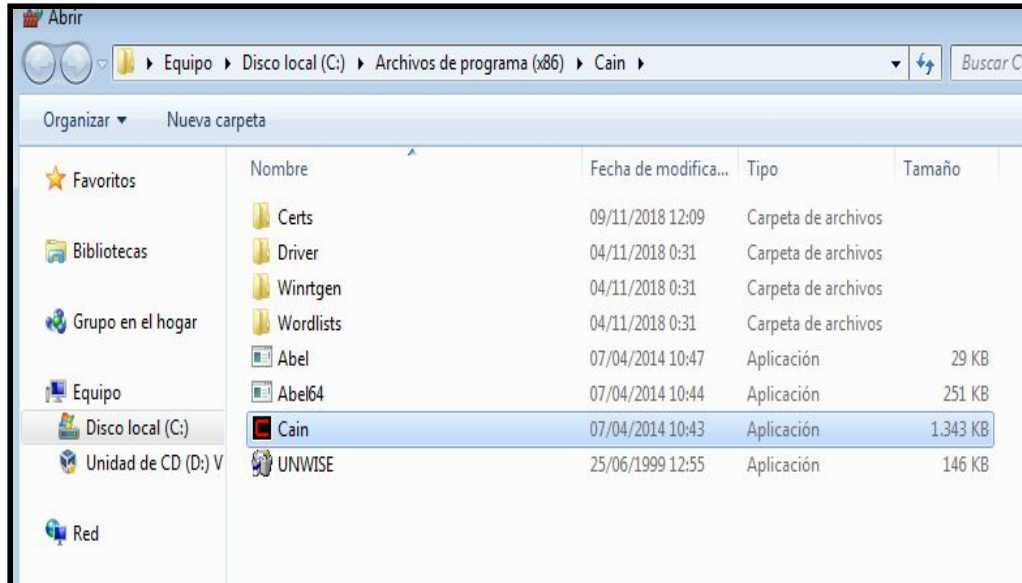
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Volem bloquejar el programa CAIN. En l'opció examinar, haurem de buscar l'arxiu executable(.exe)



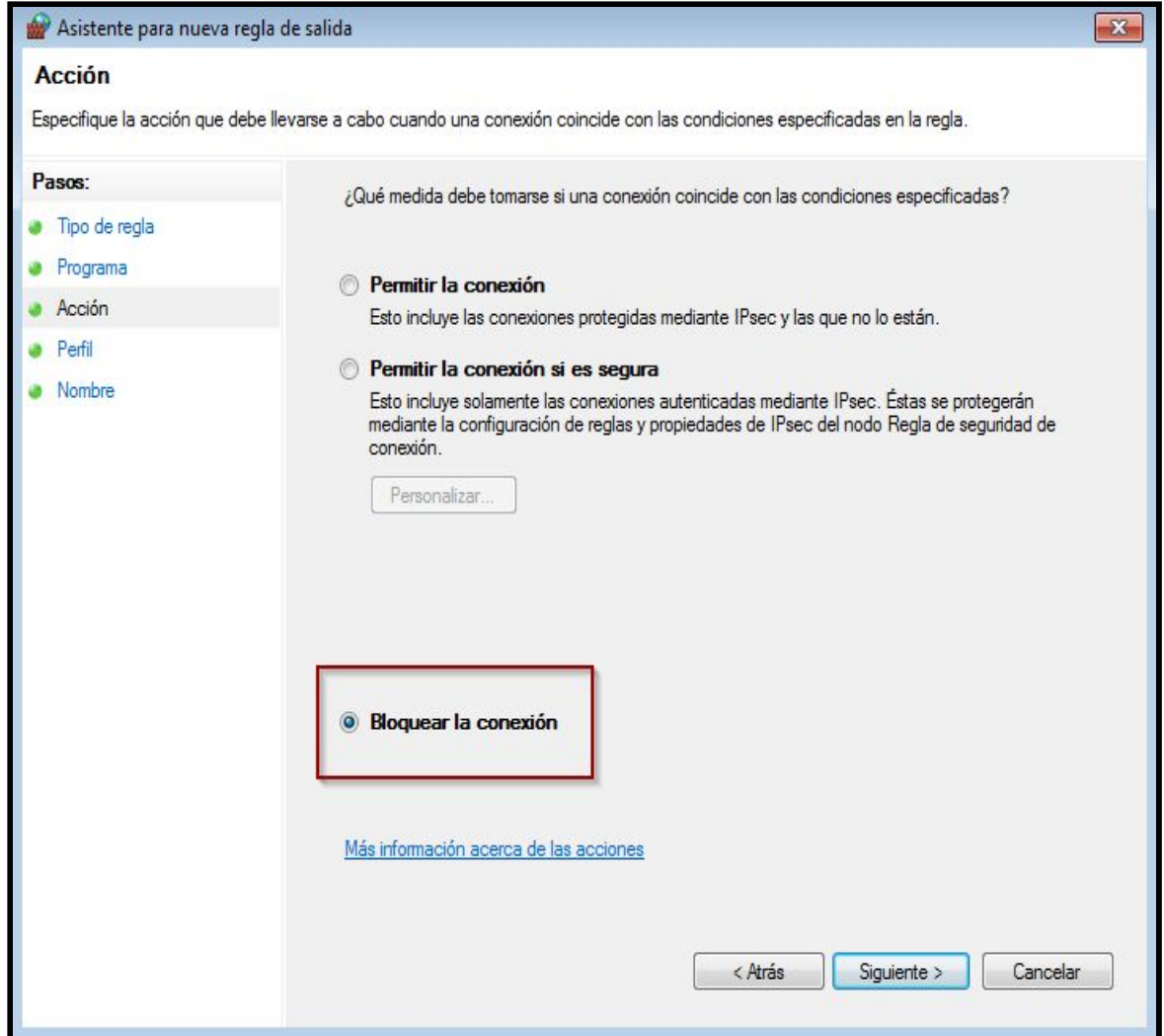
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Seleccionem l'opció de bloquejar la connexió



Asistente para nueva regla de salida

Acción

Especifique la acción que debe llevarse a cabo cuando una conexión coincide con las condiciones especificadas en la regla.

Pasos:

- Tipo de regla
- Programa
- Acción**
- Perfil
- Nombre

¿Qué medida debe tomarse si una conexión coincide con las condiciones especificadas?

☐ **Permitir la conexión**
Esto incluye las conexiones protegidas mediante IPsec y las que no lo están.

☐ **Permitir la conexión si es segura**
Esto incluye solamente las conexiones autenticadas mediante IPsec. Éstas se protegerán mediante la configuración de reglas y propiedades de IPsec del nodo Regla de seguridad de conexión.

Personalizar...

☒ **Bloquear la conexión**

[Más información acerca de las acciones](#)

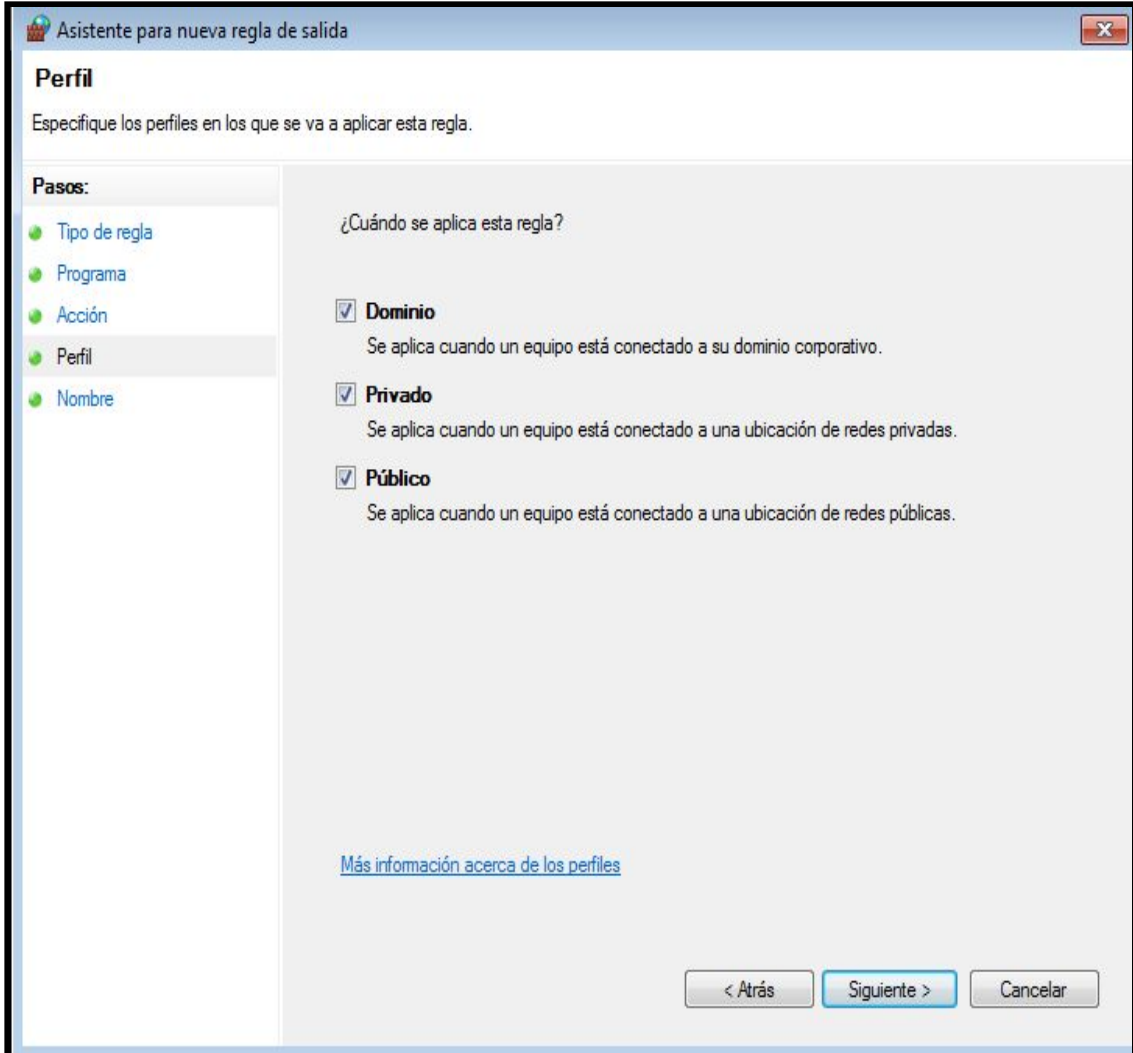
< Atrás Siguiete > Cancelar

Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019



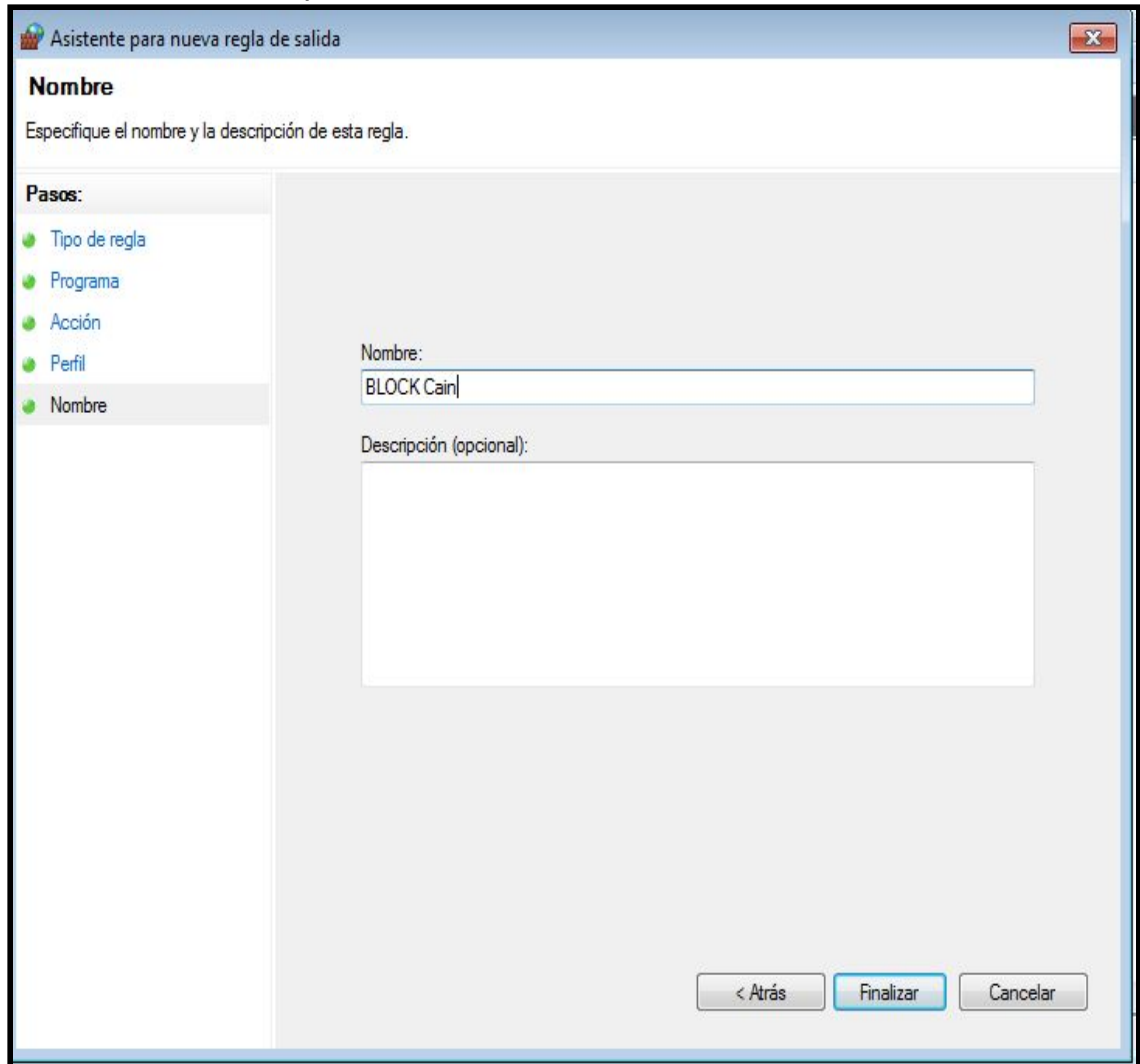
Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Anotem el nom de l'aplicació CAIN



Nom i Cognoms

Arnau Subirós Puigarnau

Data

09/02/2019

- Ara intentarem accedir al programa bloquejat.

