



Windows Firewall & Remote Management



Windows Client



Microsoft Defender Firewall



Firewall with Advanced Security



Remote Desktop



Remote Assistance



WinRM Service

Microsoft Windows Firewall

= Eenvoudige firewall binnen Windows

- ➔ Eenvoudige regels om netwerkverkeer toe te laten of blokkeren
 - Gebonden aan programma of service
 - Kunnen manueel geconfigureerd worden of bij melding dat programma/service wordt geblokkeerd
- ➔ Minimum aan regels geconfigureerd bij installatie



Microsoft Defender Firewall

- Gebruikt “Full Stealth”, “Boot Time Filtering” en “Statefull Firewall”

Full Stealth

- ➔ Blokkeert OS fingerprinting
 - Techniek om te bepalen welk OS een host heeft

Boot Time Filtering

- ➔ Kan niet uitgeschakeld worden

Statefull Firewall

Microsoft Defender Firewall

- Gebruikt “Full Stealth”, “Boot Time Filtering” en “Statefull Firewall”

Full Stealth

Boot Time Filtering

Statefull Firewall

➔ Zorgt dat firewall werkt van zodra de netwerkkkaart actief is

- Bij oude systemen werd de firewall pas actief nadat het OS volledig was opgestart

Microsoft Defender Firewall

- Gebruikt “Full Stealth”, “Boot Time Filtering” en “Statefull Firewall”

Full Stealth

Boot Time Filtering

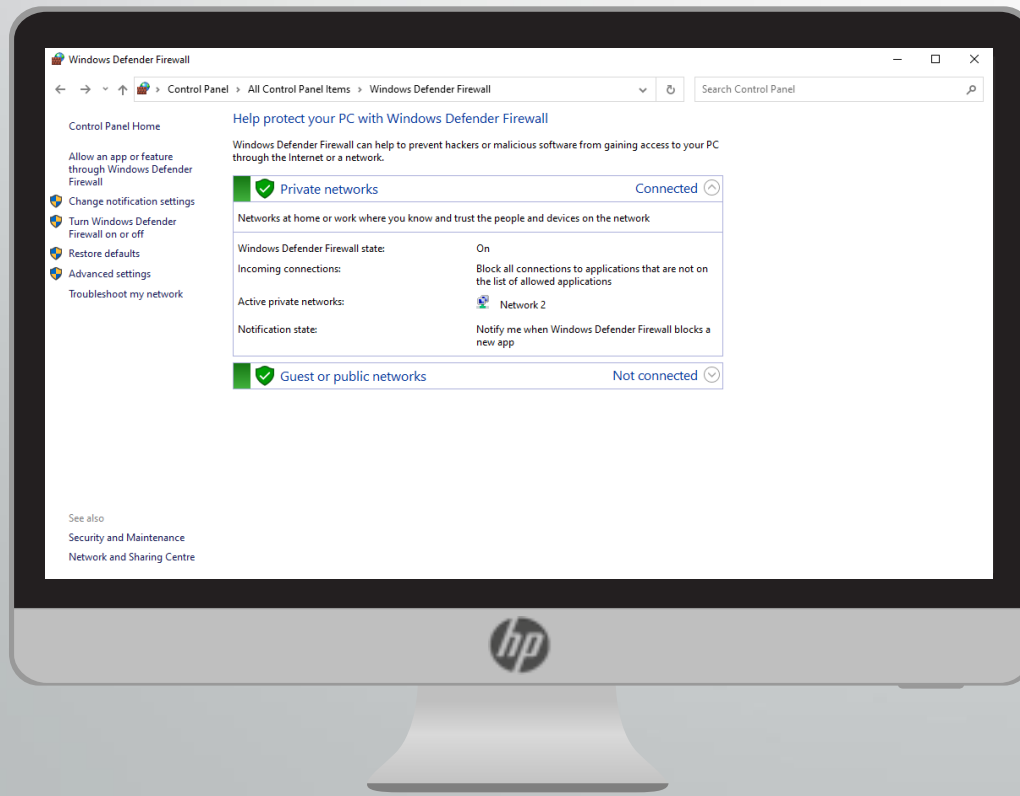
Statefull Firewall

➔ Controleert of het pakketje waarvan het afkomstig is wel degelijk pakketjes mocht sturen, ook al gaat het over een opengelaten poort

Microsoft Defender Firewall

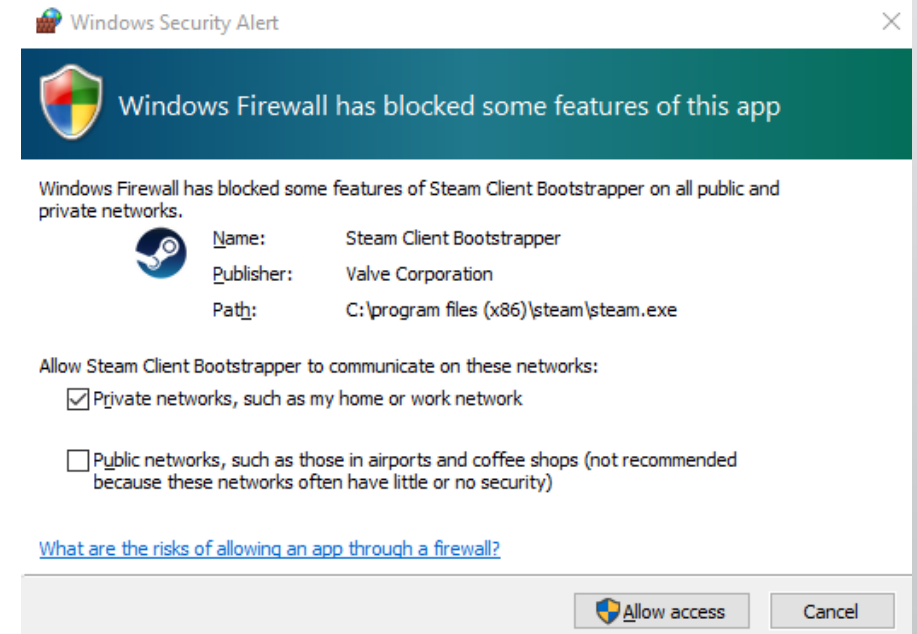
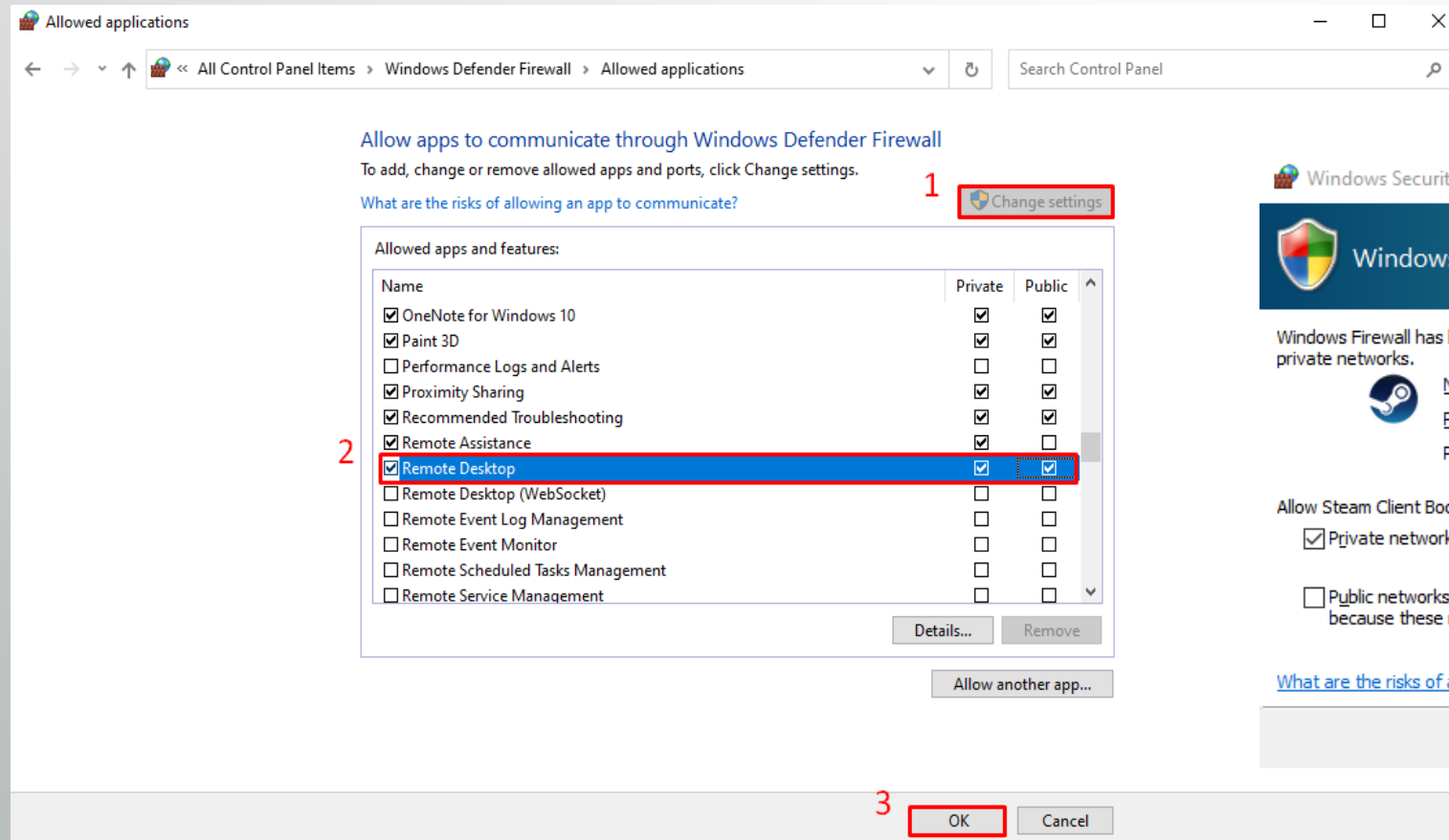
FUTURE-PROOF

PEOPLE-CENTRIC



- ➔ Applicatie toelaten
- ➔ Meldingen aanpassen
 - Bvb. als een applicatie geblokkeerd wordt
- ➔ Firewall aan-/uitzetten
- ➔ Advanced settings
 - ⇒ Windows Firewall with Advanced Security

Microsoft Defender Firewall



Microsoft Defender Firewall

- Network Location Awareness (NLA)
 - ➔ Toekennen netwerkprofiel a.d.h.v. de eigenschappen van netwerkverbinding
 - ➔ 3 netwerkprofielen



Domain



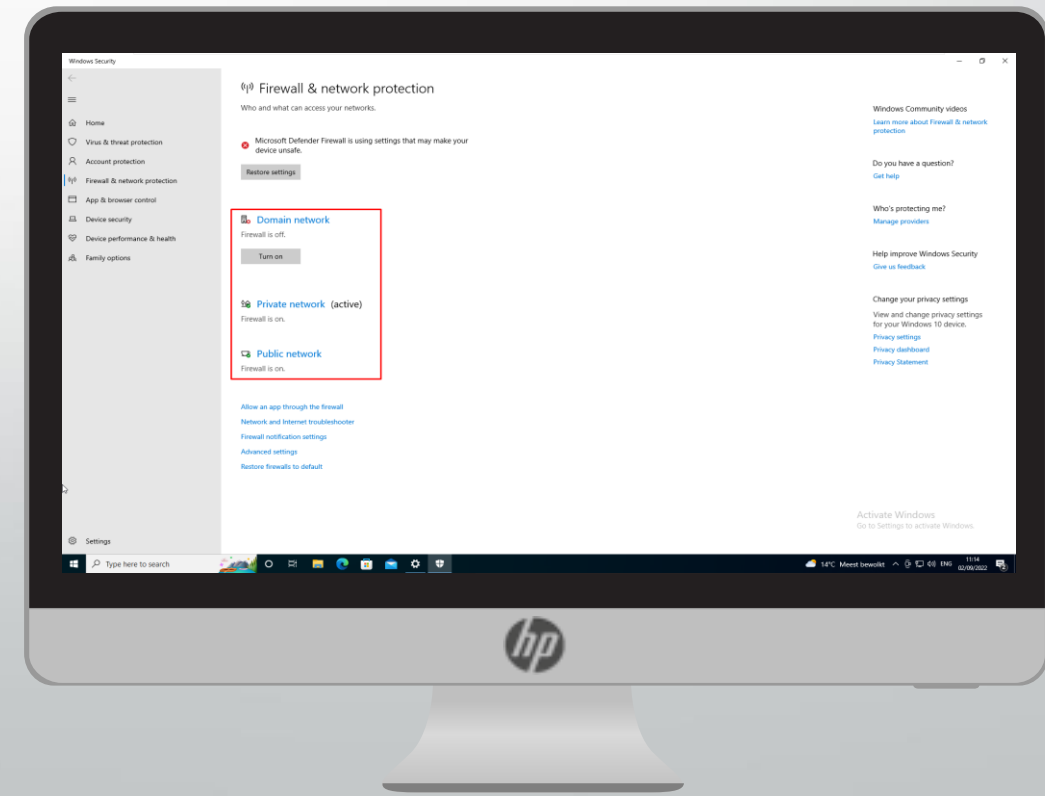
Private
(Home or Work)



Public

Microsoft Defender Firewall

- ➔ Aan elke netwerkprofiel zijn firewall regels verbonden
- ➔ Werkt ook per netwerkadapter
 - 1 NIC kan het profiel "Domain" krijgen
 - 1 WNIC kan het profiel "Public" krijgen
- ➔ Firewall per profiel in- of uitschakelen is mogelijk



Windows Firewall with Advanced Security

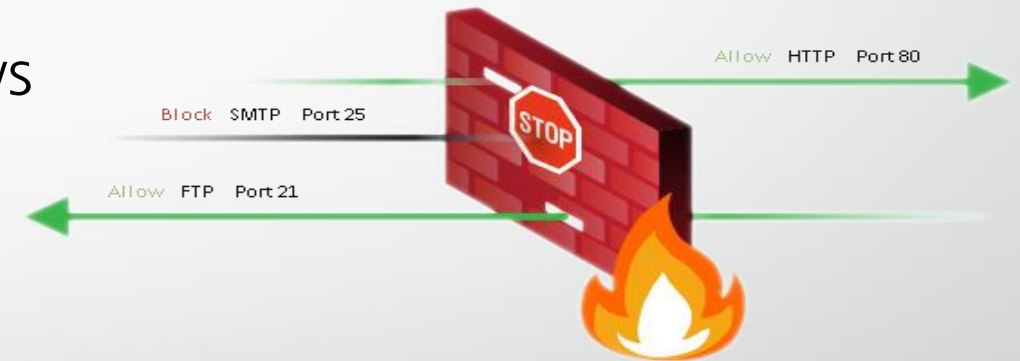
= Geavanceerde firewall binnen Windows

➔ Regels aanmaken volgens

- ✓ Inkomend verkeer (Inbound)
- ✓ Uitgaand verkeer (Outbound)
- ✓ Protocol of poort

➔ Aanmaken van Connection Security Rules

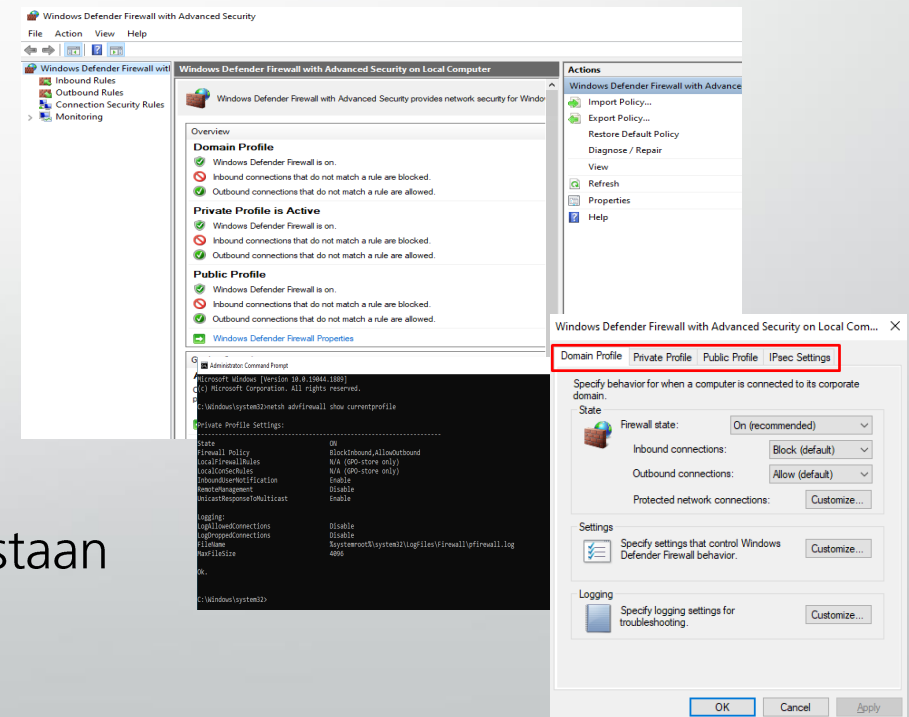
- Vereenvoudigen IPSec-verbinding



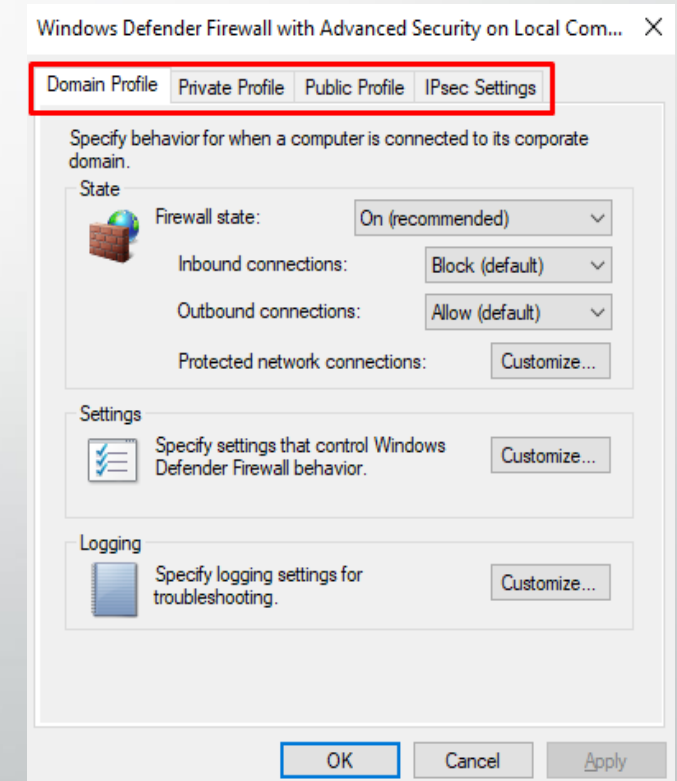
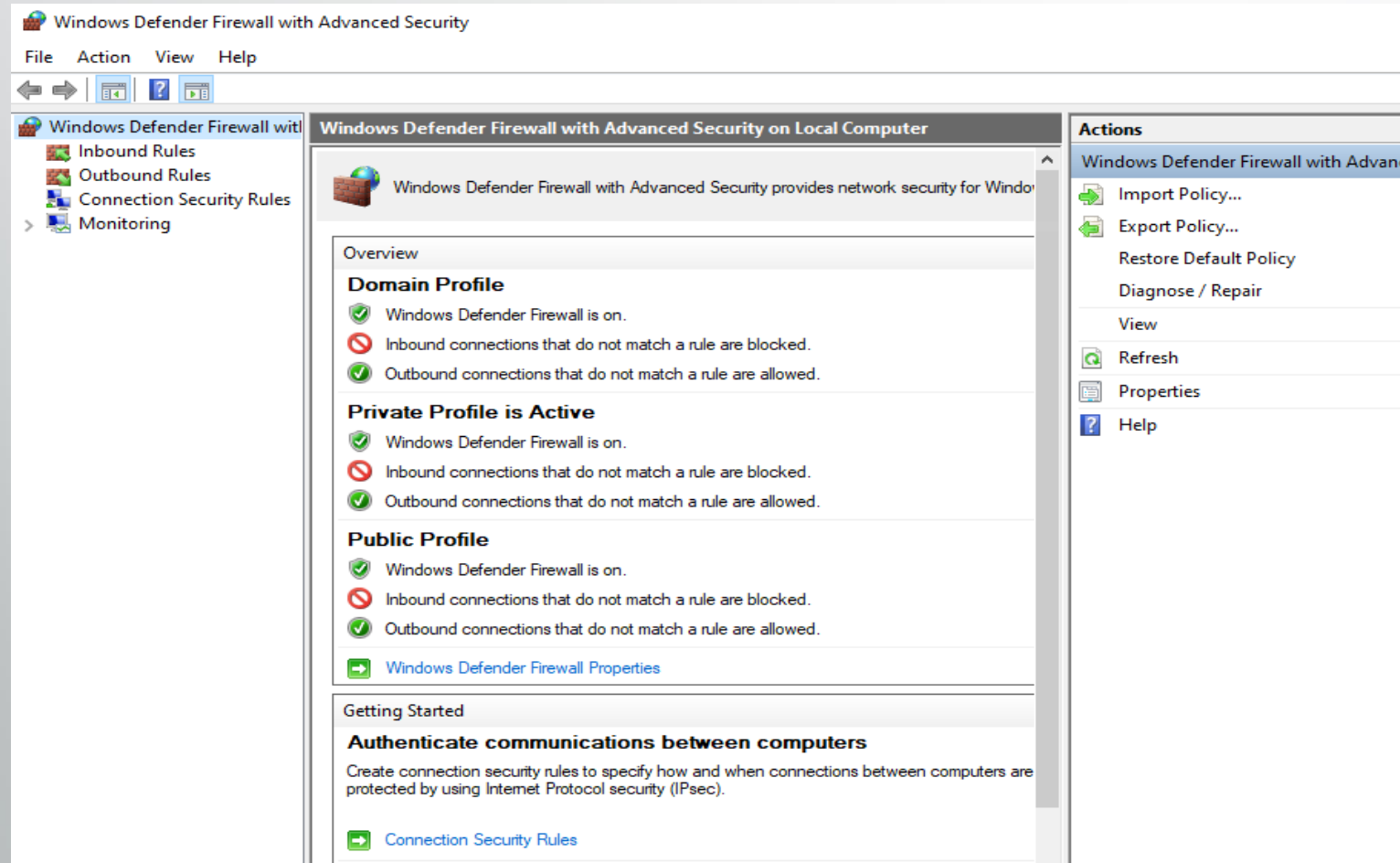
- ✓ Verkeer voor specifieke services
- ✓ Authenticatie (dan pas verkeer toelaten)

Windows Firewall with Advanced Security

- ➔ Openen via commando "wf.msc"
- ➔ Beheren via
 - Group Policies
 - Commando "netsh"
- ➔ Mogelijkheid om scopes in te stellen
 - Bepalen vanaf/naar waar traffic is toegestaan
- ➔ Mogelijkheid om regels/configuraties te importeren of exporteren



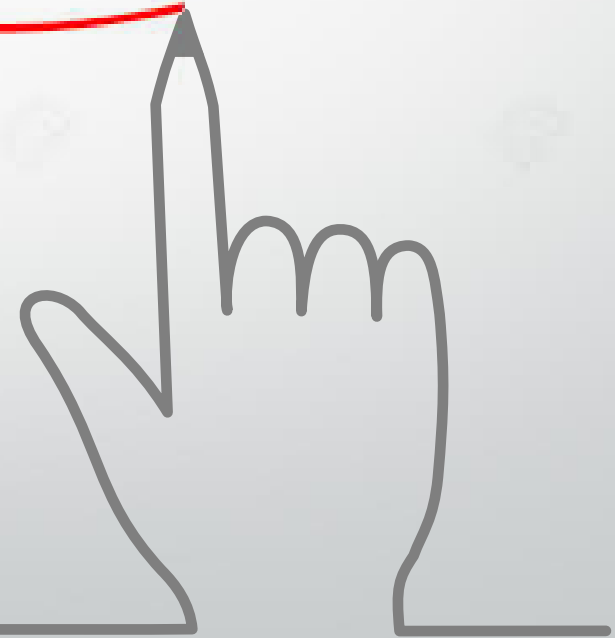
Windows Firewall with Advanced Security



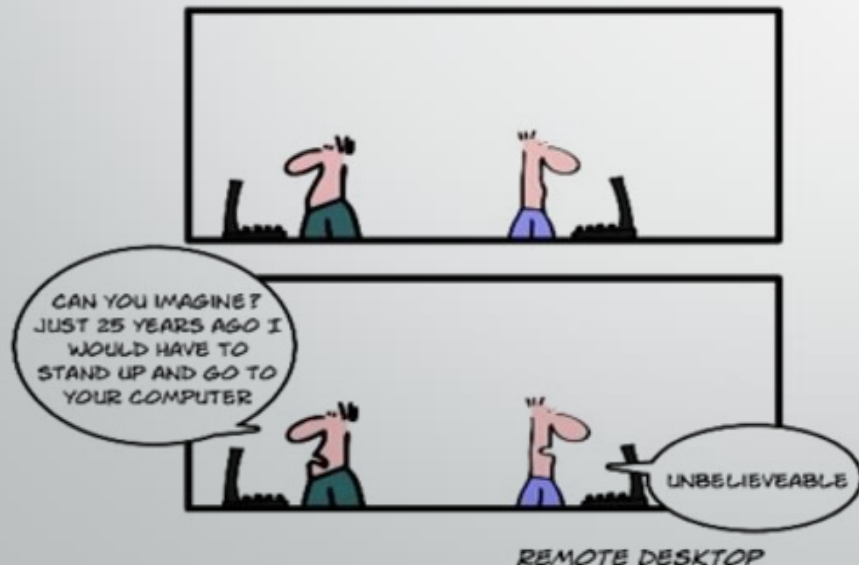


LAB – Windows Firewall

Practice
Makes Perfect



Remote Desktop



- = Vanop afstand aanmelden en scherm overnemen
- Remote Desktop starten
 - ➔ Start\All Programs\Windows Accesories\Remote Desktop Connection
 - ➔ Commando "mstsc.exe"
 - MSTSC = MicroSoft Terminal Services Client

Remote Desktop

- Kan ook gebruikt worden voor beheer van clients of servers
- Zowel lokale als remote apparaten kunnen gebruikt worden in een RDP-sessie
- Gebruikt protocol RDP
 - ➔ Poort 3389

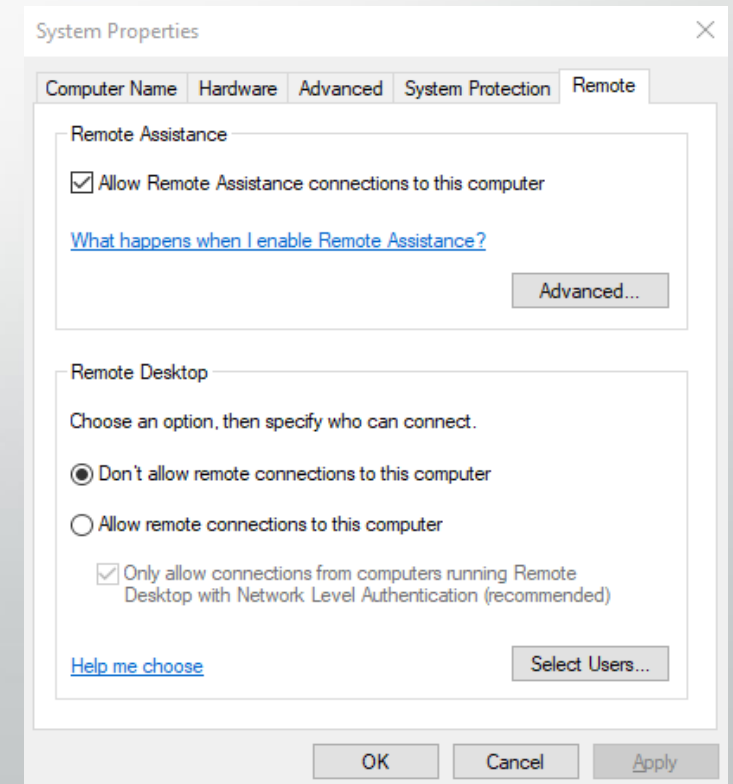
Aantal gelijktijdige sessies:

- Client: 1 console of 1 RDP
- Server: 1 console en 2 RDP's



Remote Desktop

- Standaard uitgeschakeld in Windows
 - ➔ Windows Firewall blokkeert standaard inkomend RDP-verkeer
- Remote Desktop inschakelen
 1. System Properties
 2. Tabblad "Remote"
 - ➔ "Allow remote connections to..." aanvinken



Remote Desktop



- RDP with NLA (= Network Level Authentication)
 - = Authenticatie vooraleer er wordt aangemeld
 - ⇒ Meer veiligheid tussen “client” en “server”
- ➔ Vereist:
 - Client heeft minimum Remote Desktop Connection 6.0
 - Vanaf Windows XP SP3 of Server 2008

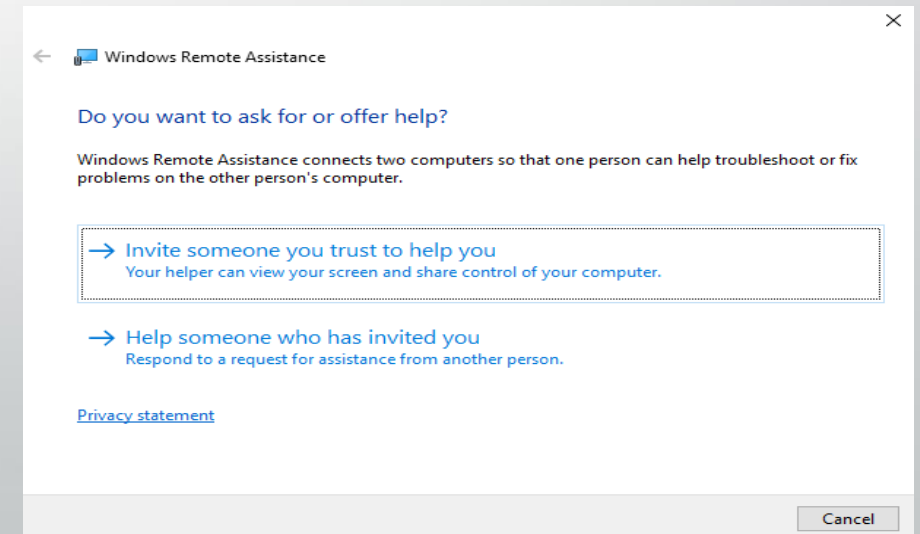
Remote Desktop

- Poortnummer RDP aanpassen ???
 - ⇒ Meer veiligheid creëren
 - ⇒ Verschillende RDP-sessies van buitenaf toelaten
 - Port forwarding kan RDP maar naar 1 IP-adres doorsturen
 - ➞ Hoe aanpassen?
 - Via Registry of Powershell



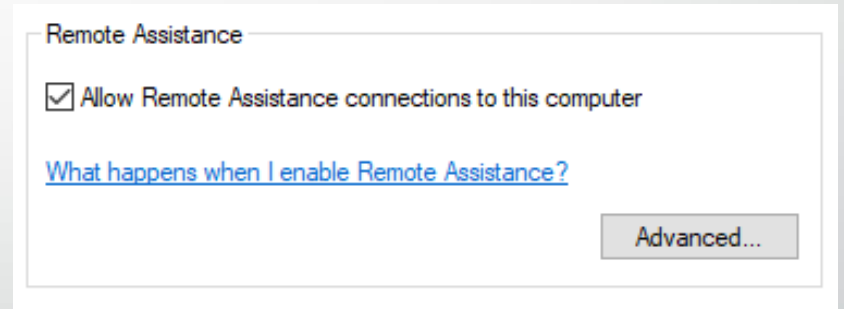
Remote Assistance

- = Tool voor support-/helpdeskmedewerker om scherm te zien van gebruiker
 - ⇒ Zowel klant als support zien het scherm
- Remote Assistance starten starten
 - ➔ Start\All Programs\Windows Accesories\Remote Assistance
 - ➔ Commando "msra.exe"




Remote Assistance

- Standaard ingeschakeld in Windows
- Kan extra geconfigureerd worden
 - ➔ Bepalen hoe lang een sessie kan duren
 - ➔ Bepalen vanaf welke machines een connectie tot stand kan gebracht worden



Remote Assistance



Heb ik zomaar
volledige controle
?

- Rechten van Remote Assistance
 - ➔ Standaard kan men enkel het scherm zien
 - ➔ Extra rechten nodig om interactie te hebben

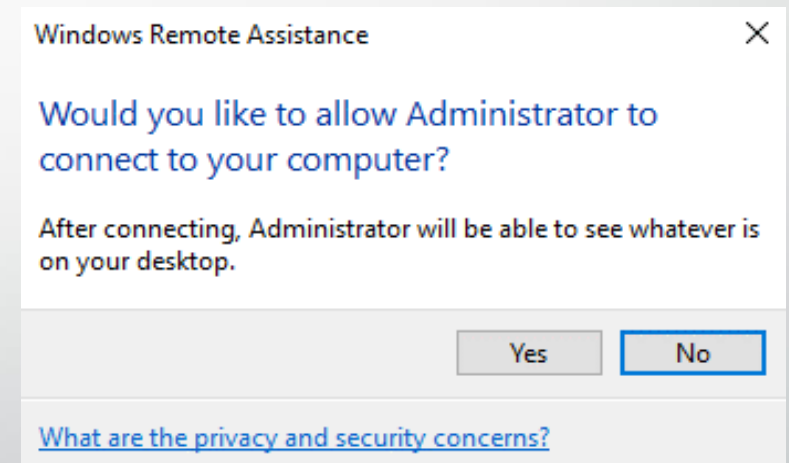
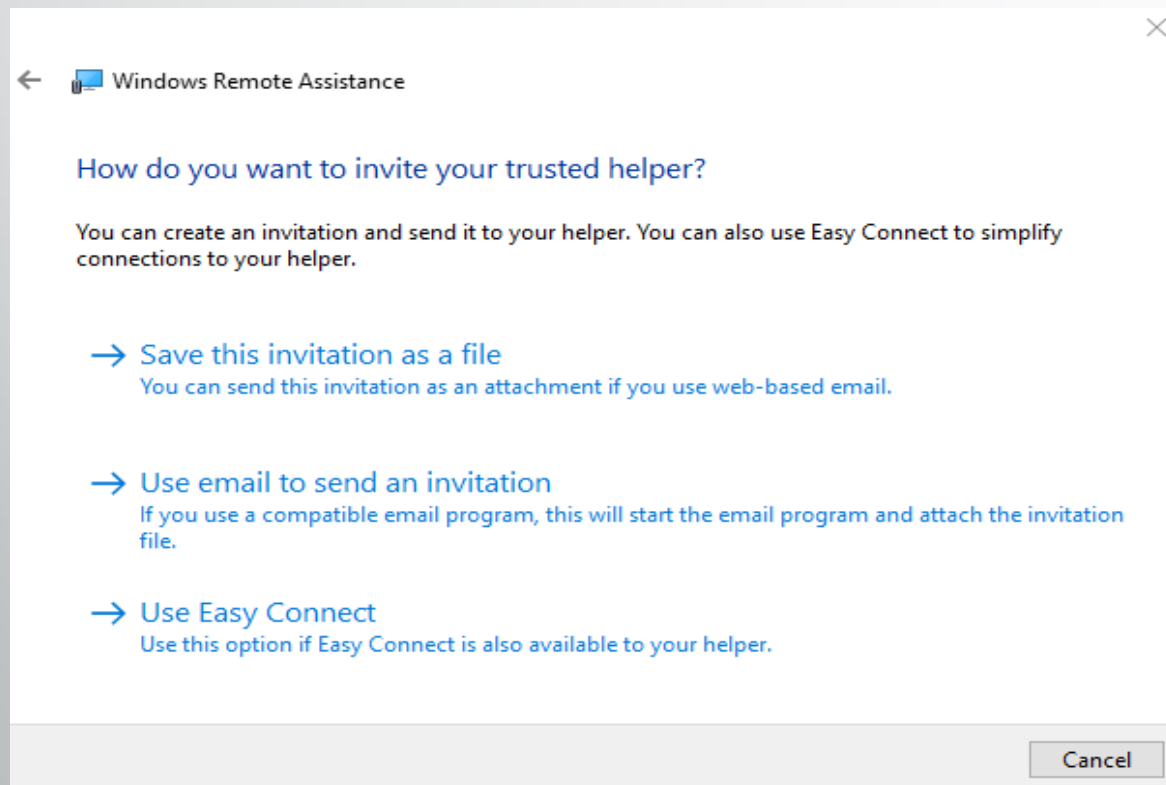


Klant bepaalt de rechten voor support !!

Remote Assistance

- Proces:
 1. Klant moet zelf een uitnodiging sturen voor hulp
 - Via een bestand verstuurd via e-mail (web-based of lokale mailapplicatie)
 - Via Easy Connect (enkel in LAN met PEER Name Resolution Protocol aanwezig)
 2. Support open Remote Assistance
 - Bestand openen ⇒ Connectie via Remote Assistance gestart
 3. Klant geeft toegang tot computer

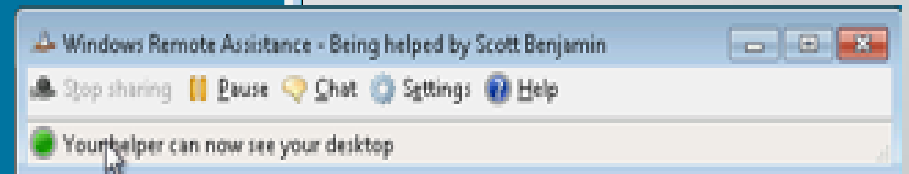
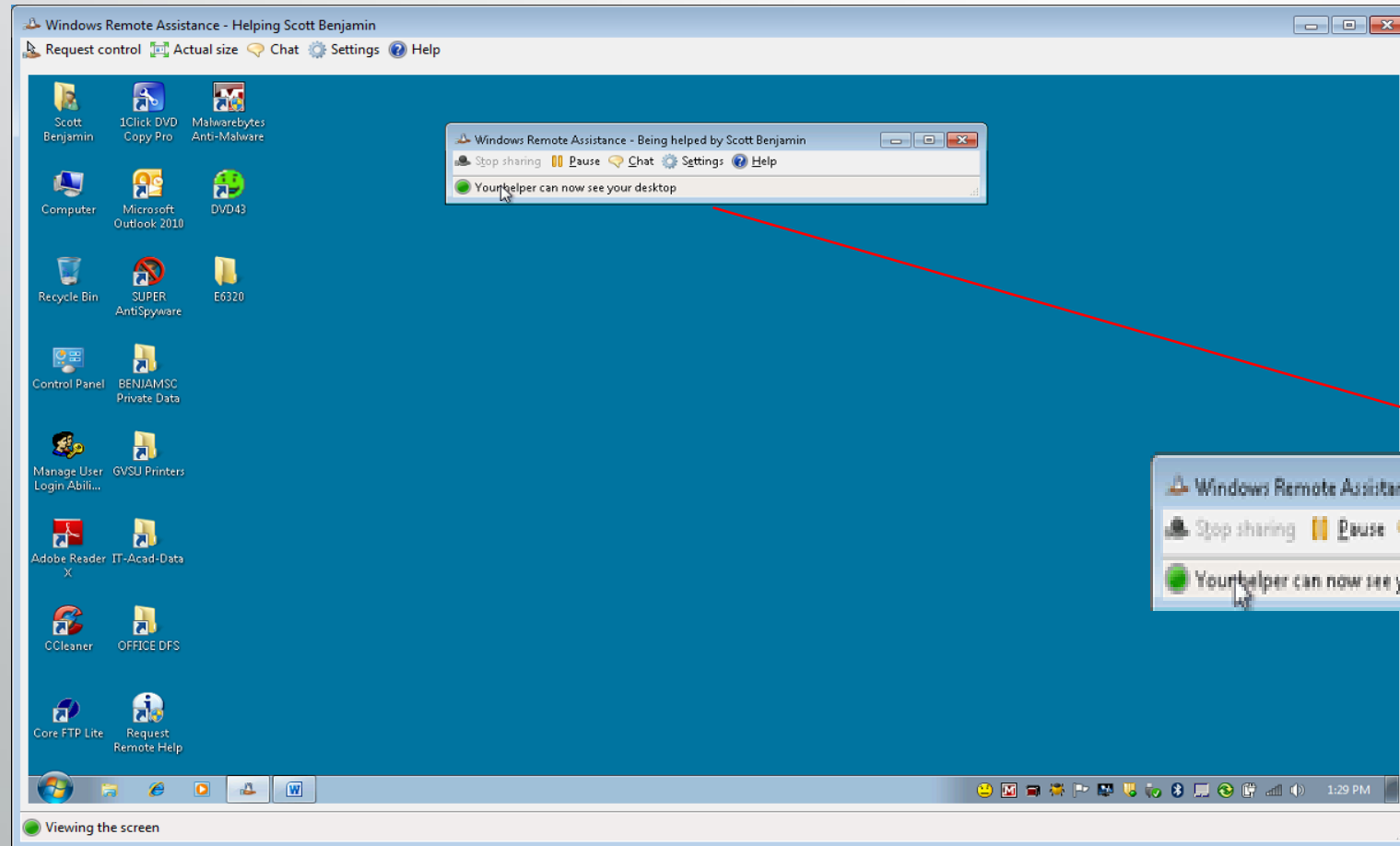
Remote Assistance



Remote Assistance

FUTURE-PROOF

PEOPLE-CENTRIC



WinRM Service

- = Windows Remote Management Service
- ⇒ Remote command's kunnen uitgevoerd worden
 - ➔ Via commando "*winrs*"
 - ➔ Via Powershell
- Inschakelen op de doelcomputer
 - ➔ Via commando "*WinRM QuickConfig*"



WinRM Service

```
Administrator: Command Prompt - winrm quickconfig
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>winrm quickconfig
WinRM is not set up to receive requests on this machine.
The following changes must be made:

Start the WinRM service.
Set the WinRM service type to delayed auto start.

Make these changes [y/n]?
```

- WinRM QuickConfig doet het volgende:
 1. Start de service "WinRM"
 2. Verandert startup type van WinRM Service
 3. Maakt een regel aan in de firewall



Interessant bij servers en bij gebruik van Powershell



LAB – Windows Remote

Practice
Makes Perfect

