Windows firewall



context

dit document beschrijft de Windows firewall

nut

elke firewall die je krijgt, moet je gebruiken. Je kan nooit genoeg security hebben.

profielen

1. public:publieke netwerken (hotspots oa)
2. private: private of thuis netwerken
3. domain: voor hosts die deel uitmaken van een Windows domein

Maak een firewall rule aan voor alle profielen en activeer daarna enkel de profielen die je nodig hebt. Je kan firewall regels instellen op basis van

- **uitgaand** en
- **inkomend** verkeer

en dat voor

- **poort**
- **programma**
- **protocol**

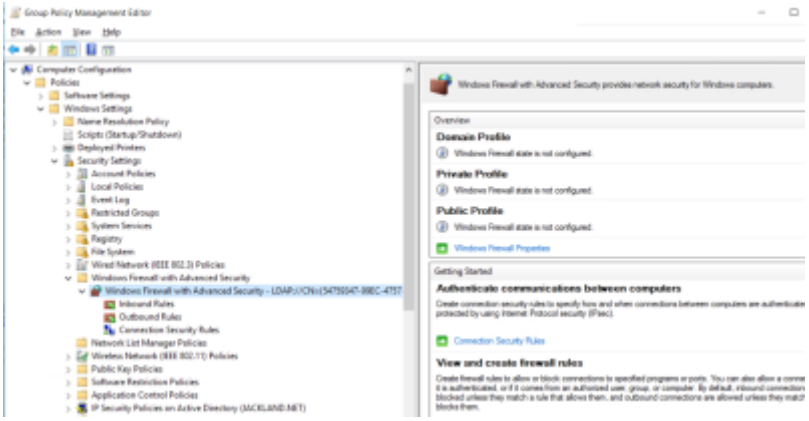
Dit artikel geeft aan hoe je het actieve firewall profiel nakijkt.

regels aanmaken

maak alleen regels aan via group policy! Dit doe je als volgt:

1. meld aan op de **Domein controller**
2. start **Group Policy Editor**
3. maak een nieuwe GPO aan

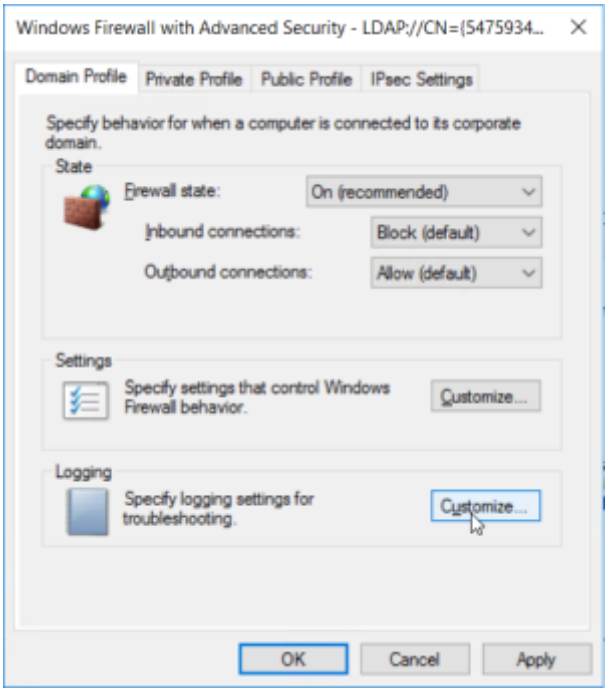
4. open: **Computer configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Firewall with Advanced Security** > **Windows Firewall with Advanced Security - LDAP://...**:



5. kies **in-/outbound rule**, **rechter** klik: **New Rule...**
6. kies het rule type: **poort**, **programma** of **Predefined**
   Predefined bevat regels voor veelgebruike Windows programma/services
7. kies afhankelijk van type, de juiste instellingen
8. kies
   1. **“Allow the connection”** OF:
   2. **“Allow the connection if it is secure”**: beperking op gebruikers/computers
9. dubbel-klik nu op de aangemaakte regel om die te **verfijnen**:
   1. profile
   2. eventueel geauthenticeerde gebruiker/computer
   3. restricties op ip adressen
10. **koppel de GPO** nu aan servers/computers.

firewall activeren

1. meld aan op de **Domein controller**
2. start **Group Policy Editor**
3. maak een nieuwe GPO aan of bewerk bovenstaande
4. open: **Computer configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Windows Firewall with Advanced Security** > **Windows Firewall with Advanced Security - LDAP://...**: **Windows Firewall Properties**:



5. **State**:
    1. **Firewall State** naar **On(recommended)**
    2. **inbound connections**: Block(default)
    3. **outbound connections**: Allow(default)
6. **Logging: Customize**:
    1. **Name**: vink uit: **Not configured**.
       stel in op: pfirewall<profile>.log
    2. **Size**: vink uit: **Not configured**
    3. **Log dropped packets**: Yes

problemen, problemen

logboeken

- standaard: %systemroot%\system32\logfiles\firewall\pfirewall<profile>.log
  je kan die echter ook zetten waar je wil.

meer info

- firewall regels aanmaken
- Windows firewall logging activeren
- Windows firewall configureren via GPO
- ICMP verkeer doorlaten

windows, firewall

From:
https://louslab.be/ - **Lou's lab**

Permanent link:
https://louslab.be/doku.php?id=windows:firewall

Last update: **2024/11/16 18:14**