

TermiNET

Persoonlijke firewall

Gebruikshandleiding

Inhoud

| | | |
|----------|--|-----------|
| 1 | INLEIDING | 3 |
| 1.1 | INFO TERMINET | 3 |
| 1.2 | BELANGRIJKSTE FUNCTIES | 3 |
| 2 | AAN DE SLAG | 3 |
| 2.1 | TERMINET INSTALLEREN | 3 |
| 2.2 | AANMELDEN BIJ TERMINET | 4 |
| 2.2.1 | <i>Windows 95/98</i> | 4 |
| 2.2.2 | <i>Windows NT/2000</i> | 4 |
| 2.3 | BEHEERDER-MODUS | 4 |
| 2.4 | DE TERMINET-INTERFACE | 5 |
| 3 | GEBRUIKERS EN GROEPEN. BEHEER VAN GEBRUIKERS EN GROEPEN | 7 |
| 3.1 | GEBRUIKERS TOEVOEGEN | 7 |
| 3.2 | NIEUWE GROEPEN MAKEN | 8 |
| 4 | VERKEERSREGELS | 8 |
| 4.1 | STANDAARD REGELS: | 8 |
| 4.2 | GEAVANCEERDE REGELS: | 8 |
| 4.3 | NIEUWE REGELS MAKEN: | 9 |
| 5 | WEBLIJSTEN | 11 |
| 5.1 | ZWARTE LIJSTEN | 11 |
| 5.2 | WITTE LIJSTEN | 11 |
| 5.3 | Globale en lokale lijsten | 11 |
| 6 | PROBLEMEN MET NETBIOS | 11 |

1 Inleiding

1.1 Info TermiNET

TermiNET is een persoonlijke 'firewall' die bedoeld is om uw pc tijdens verbindingen met het Internet te beschermen tegen aanvallen van buitenaf terwijl u op het net surft of andere internet-diensten gebruikt. TermiNET kan eerst in één van de volgende modi worden geïnstalleerd:

1. In de modus Gesloten wordt standaard alle verkeer van en naar de lokale computer geblokkeerd. +De beheerder kan vervolgens selectief bepaalde diensten openstellen - bijvoorbeeld alleen FTP toestaan of tegelijk FTP, Telnet en webtoegang toestaan. Ouders kunnen voor hun kinderen de toegang beperken tot een vaste serie pagina's. . De pagina's kunnen rechtstreeks worden ingevoerd als specifieke regels of worden ingelezen vanaf een URL «Witte lijst».
2. In de modus Open worden er om te beginnen geen blokkerende voorwaarden gesteld. De beheerder kan vervolgens beslissen om selectief bepaalde toegangen te blokkeren, per toepassing, poort of protocol, bijvoorbeeld: Telnet en FTP totaal blokkeren, alle inkomend verkeer op poort 25 blokkeren, toegang blokkeren tot een bepaalde serie webpagina's. Ook hier kunnen deze maatregelen worden ingevoerd in de vorm van specifieke regels of worden ingelezen vanaf een URL «Zwarte lijst» of accepteerbare websites.
3. In de modus Afgeschermd is al het uitgaande verkeer mogelijk, maar worden alle inkomende verbindingen geblokkeerd, behalve als deze lokaal zijn gestart. In deze modus kan de computer gewoon worden gebruikt voor het surfen op het net, voor FTP, enz., maar is beschermd tegen aanvallen tijdens verbindingen met het Internet.

TermiNET is de ideale beveiligingsoplossing voor middelgrote en kleine bedrijven en voor particulieren die het Internet willen gebruiken, maar die niet over de middelen beschikken om een grote beveiligingsstructuur te onderhouden.

1.2 Belangrijkste functies

De belangrijkste functies van TermiNET zijn:

- Standaard en geavanceerde regels: Dit zijn series eenvoudige aankruisvakjes die kunnen worden **ingeschakeld** of **uitgeschakeld**.
- De zwarte-lijst / witte-lijst functie, waarmee de toegang tot bepaalde ongewenste websites kan worden geweigerd of waarmee alleen toegang kan worden verleend aan bekende acceptabele websites.
- Het flexibele toegangsbeheer maakt het mogelijk om regels op te stellen die gelden per IP-adres, URL, poort en/of protocol.
- Ook kunnen tijdgebonden regels worden geconfigureerd die alleen actief zijn op bepaalde dagen.
- Door de simpel te gebruiken interface in de stijl van Windows Verkenner is TermiNET eenvoudig en intuïtief te configureren, zelfs voor een niet technisch onderlegde gebruiker.

2 Aan de slag

2.1 TermiNET installeren

Plaats de TermiNET-cd in het cd-rom-station van de pc. Normaal start het installatieprogramma automatisch. Als de functie Autorun is uitgeschakeld, klikt u op «Start» -> «Uitvoeren» en typt u «D:\setup» waarin D: de letter voorstelt van het cd-rom-station. Volg de aanwijzingen op het scherm om het product te installeren. Het is tijdens de installatie mogelijk om het pad aan te geven waar het programma moet worden geïnstalleerd en om een van de drie standaard beveiligingsmodi te kiezen, Open, Gesloten of Afgeschermd, die hierboven zijn beschreven.

Aan het einde van de installatieprocedure **moet** de pc opnieuw worden gestart om de installatie te voltooien.

2.2 Aanmelden bij TermiNET

2.2.1 Windows 95/98

Bij het opstarten van het systeem begint TermiNET met een standaard serie regels, zoals dat door de beheerder is vastgelegd. Als er meerdere profielen voor TermiNET-gebruikers zijn gemaakt, zijn er twee manieren om zich aan te melden als één van de gedefinieerde gebruikers: dubbelklik op het pictogram TermiNET in de systeemwerkbalk of klik met de rechtermuisknop op het pictogram TermiNET en kies de opdracht Aanmelden. In beide gevallen wordt een aanmeldingsscherm geopend waarin u wordt gevraagd om een gebruikers-id en een wachtwoord. Door het invoeren van de gebruikers-id en het wachtwoord wordt het beveiligingsprofiel geactiveerd voor de opgegeven gebruiker.

2.2.2 Windows NT/2000

Gebruikers worden automatisch aangemeld bij TermiNET op basis van het NT-aanmeldingsprofiel.

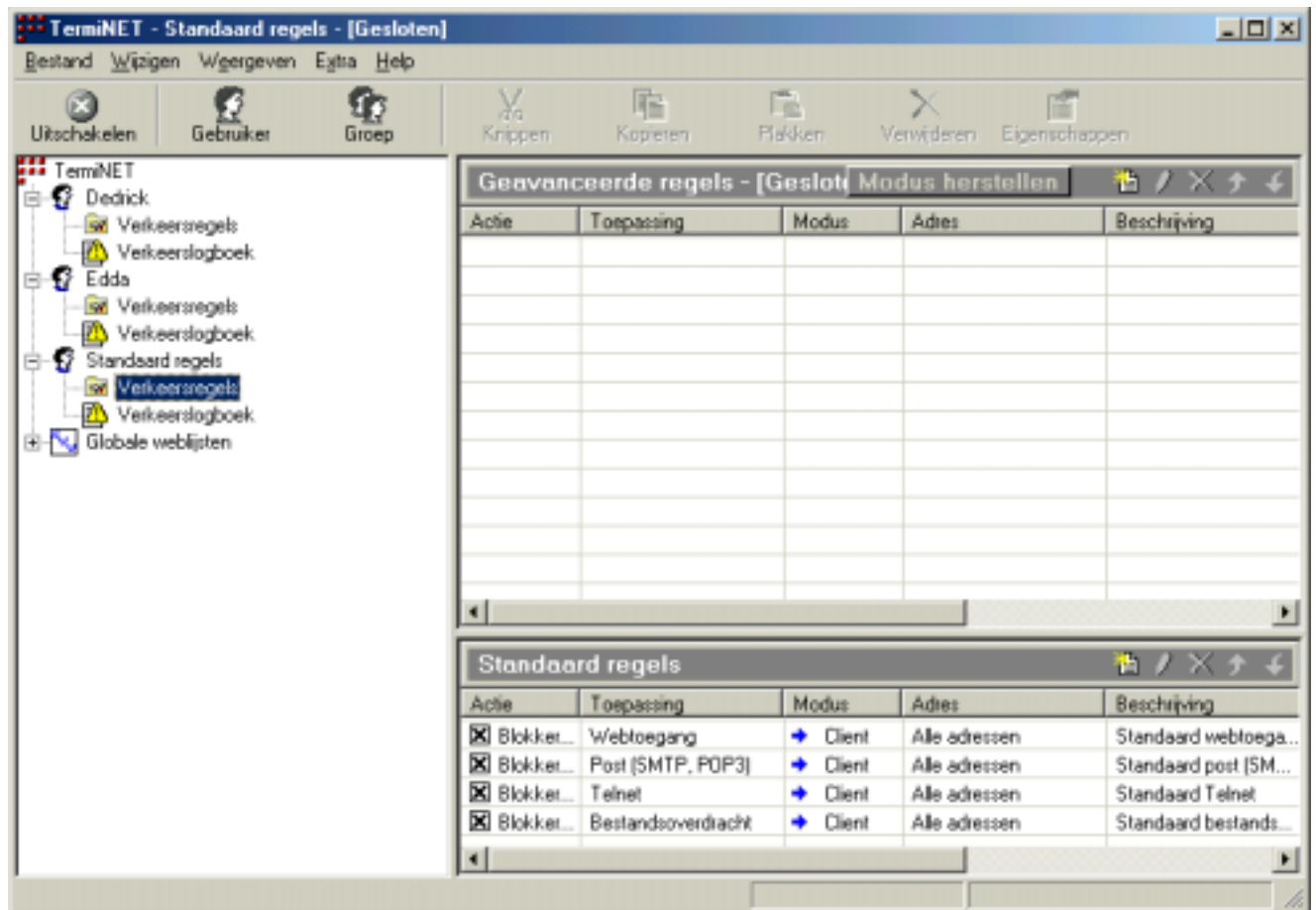
2.3 Beheerder-modus

In de -modus Beheerder kunt u het standaard gebruikerbeveiligingsprofiel bepalen, nieuwe gebruikersprofielen maken en geavanceerde regels instellen voor bepaalde gebruikers. U roept de modus Beheerder op door met de rechtermuisknop te klikken op het pictogram TermiNET in de systeemwerkbalk en de opdracht Beheerder-modus te kiezen. U wordt dan gevraagd om het beheerderswachtwoord. Na het invoeren van het wachtwoord wordt het configuratiescherm van TermiNET weergegeven waarmee u beheerdersfuncties kunt uitvoeren.

Door gewoon het configuratiescherm te sluiten via de opdracht "Bestand -> Beheerder sluiten", verlaat u de modus Beheerder.

2.4 De TerMiNET-interface

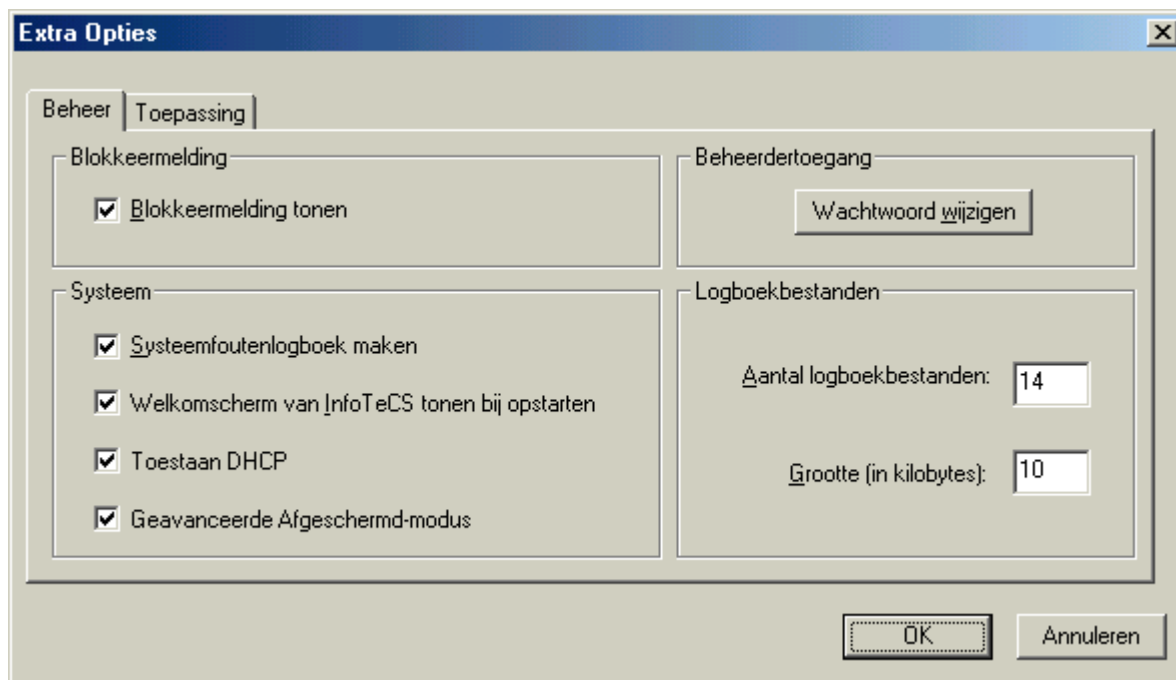
De TerMiNET-interface (Figuur 1) is alleen toegankelijk via het beheerderswachtwoord. Dit is een eenvoudig te gebruiken grafisch hulpmiddel om beveiligingsprofielen te definiëren voor een computer.



Figuur 1

De interface bestaat uit drie secties, waarvan de linkse sectie het gedefinieerde beveiligingssysteem weergeeft in de vorm van een boomstructuur. De sectie rechts onder toont de standaard regels die zijn voorgedefinieerd door het systeem. De sectie rechts boven toont de geavanceerde regels, voor zover die zijn aangemaakt. Door in het linker venster een gebruiker te selecteren wordt in de rechter vensters de status weergegeven van de geavanceerde en standaard regels voor die bepaalde gebruiker.

Met behulp van de menu's Bestand, Bewerken en Weergeven kan de interface volgens de wensen van de beheerder kan worden aangepast. Via het menu "Extra" ->"Opties" kunnen globale systeemeigenschappen worden ingesteld.

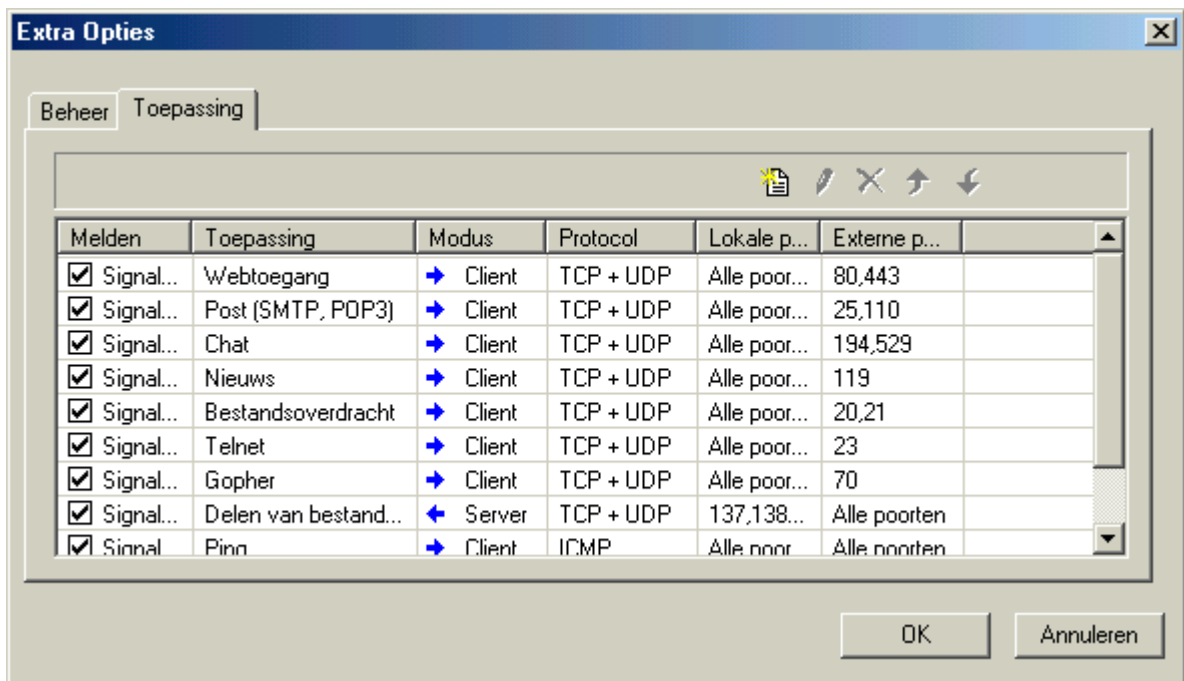


Figuur 2


Op het tabblad Beheer (Figuur 2) kunnen de volgende opties worden ingesteld.

| | |
|---|---|
| Blokkeermelding tonen: | Indien aangekruist, wordt in het verkeerslogboek zowel het geblokkeerde als het toegelaten verkeer vermeld. Indien leeg, wordt alleen het toegelaten verkeer geregistreerd. |
| Systeemfoutenlogboek maken: | Indien aangekruist, worden systeemfouten in het bestand \Programmabestanden\Infotecs\Terminet\Data\errorlog.txt geschreven. |
| Welkomscherm van Infotecs tonen bij opstarten: | Maak dit vakje leeg als u wilt niet wilt dat het welkomscherm van Infotecs wordt weergegeven bij het opstarten van TerMiNET. |
| Wachtwoord wijzigen: | Dit maakt het mogelijk om het beheerderswachtwoord te wijzigen. |
| Aantal logboekbestanden: | Hiermee wordt het aantal verkeerslogboekbestanden ingesteld die worden geregistreerd. Als het opgegeven aantal logboekbestanden is bereikt en zodra het laatste bestand zijn maximumgrootte bereikt, wordt het eerste bestand overschreven. |
| Grootte (in kilobytes): | Hiermee stelt u de maximumgrootte in voor een verkeersbestand. Zodra deze grootte is bereikt, wordt het bestand opgeslagen en begint de registratie in een ander bestand. |

Met het tabblad Toepassing (Figuur 3) kunt u nieuwe standaard toepassingen maken.



Figuur 3

Klik op de knop Toepassing toevoegen  om het dialoogvenster Aangepaste toepassing (Figuur 4) te openen.



Figuur 4

In dit venster kunt u de volgende opties instellen:

- **Naam:** Geef de naam op van de aangepaste toepassing.
- **Protocol:** Selecteer in de vervolgkeuzelijst het gewenste protocol voor de toepassing.
- **Melden:** Selecteer Signaleren of Negeren in de vervolgkeuzelijst. Als u Signaleren kiest, wordt er een melding weergegeven wanneer dit type verkeer wordt geblokkeerd.
- **Richting:** Selecteer Inkomend of Uitgaand in de vervolgkeuzelijst.
- **Externe poort:** Geef de instelling van de poort op die van toepassing is op de externe computer voor deze toepassing.
- **Lokale poort:** Geef de instellingen van de poort op die van toepassing zijn op de lokale computer voor deze toepassing.

3 Gebruikers en groepen. Beheer van gebruikers en groepen

3.1 Gebruikers toevoegen

Voeg een gebruikerprofiel toe door met de rechtermuisknop te klikken op het hoogste niveau van de TermiNET-boom en selecteer Gebruiker toevoegen uit het pop-upmenu of klik op de knop Gebruiker in de werkbalk. Dit opent het dialoogvenster Gebruikerseigenschappen (Figuur 5)



Figuur 5

Dit venster bevat de volgende velden.

- **Gebruikersnaam:** Vul hier de naam die u hebt gekozen voor de gebruiker.
- **Wachtwoord:** Vul hier het vereiste wachtwoord in voor de gebruiker.
- **Bevestig wachtwoord:** Vul hier een tweede maal het wachtwoord in om dit te bevestigen.
- **Beveiligingsmodus:** Selecteer de standaard beveiligingsmodus voor deze gebruiker.
- **URL-lijsten:** Hiermee bepaalt u of de gebruiker de URL zwarte of witte lijsten gaat gebruiken en of de globale lijst, de lokale lijst of beide worden gebruikt.

3.2 Nieuwe groepen maken

U kunt groepen gebruiken om binnen het venster met de Terminet-boomstructuur lijsten van gebruikers te organiseren. Maak een nieuwe groep door met de rechter muisknop te klikken op het hoogste niveau van de boomstructuur en kies Groep toevoegen in het pop-upmenu en typ de voor de groep gekozen naam. U kunt gebruikers in groepen plaatsen door op de gebruikersnaam te klikken en deze vervolgens naar de gekozen groep te slepen. U kunt een nieuwe gebruiker aanmaken in een bestaande groep door met de rechter muisknop op de groep te klikken in het venster met de boomstructuur en dan Gebruiker toevoegen te kiezen in het pop-upmenu.

4 Verkeersregels

U kunt in Terminet twee typen verkeersregels definiëren.

4.1 Standaard regels:

Deze zijn van toepassing op alle IP-adressen en kunnen worden gebruikt om de toegang tot specifieke diensten globaal toe te staan of te weigeren. Er bestaan vier voorgedefinieerde standaard regels in het systeem: Webtoegang, Post, FTP en Telnet. U kunt meer regels toevoegen door in het venster met de boomstructuur een gebruiker te selecteren, met de rechtermuisknop in het venster Standaard regels te klikken en vervolgens in het pop-upmenu de opdracht Regel toevoegen te kiezen om het dialoogvenster Regel toevoegen (Figuur 6.) te openen.

4.2 Geavanceerde regels:

Deze zijn van toepassing op specifieke IP-adressen of URL's en worden gebruikt om op een selectieve manier de toegang tot websites en diensten toe te staan of te weigeren. U kunt regels toevoegen door de gebruiker op wie de regel moet worden toegepast te selecteren, met de rechtermuisknop in het venster Geavanceerde regels te klikken en vervolgens in het pop-upmenu de opdracht Regel toevoegen te kiezen om het dialoogvenster Regel toevoegen te openen.

Indien Terminet is geïnstalleerd in de modus Afgeschermd, kunnen alleen geavanceerde regels worden geconfigureerd.

4.3 Nieuwe regels maken:

Het dialoogvenster Regel toevoegen (Figuur 6) wordt gebruikt om nieuwe regels te maken en te definiëren.

The dialog box 'Nieuwe regel invoeren' contains the following fields and options:

- Beschrijving:** Text input field.
- Actie:** Dropdown menu with 'Toestaan' selected.
- Toepassing:** Dropdown menu with 'Webtoegang' selected.
- Modus:** Dropdown menu with 'Client' selected.
- Protocol:** Dropdown menu with 'TCP+UDP' selected.
- Buttons:** 'OK' and 'Annuleren'.
- Adres tab:**
 - Lokaal adres:** Radio button for 'Host-adres' (selected).
 - Extern adres:** Radio buttons for 'Webadres' (selected), 'IP-adres', and 'Alle adressen'.
 - Webadres:** Text input field below the 'Extern adres' section.

Figuur 6

Dit venster bevat de volgende velden.

- **Beschrijving:** Typ een beschrijving voor de nieuw te maken regel
- **Actie:** Geef aan of de regel het gedefinieerde verkeer toestaat of blokkeert.
- **Toepassing:** Selecteer een applicatie uit de voorgedefinieerde lijst van applicaties of typ een nieuwe naam voor de applicatie waarop deze regel van toepassing is.
- **Modus:** Geef aan of de lokale computer een client of een server wordt voor deze regel. Door 'client' te antwoorden geeft u aan dat de regel wordt toegepast op uitgaand verkeer, terwijl 'server' betekent dat de regel wordt toegepast op inkomend verkeer.

De tabbladen Adres (Figuur 7), Poort (Figuur 8) en Tijd (Figuur 9) worden gebruikt om de geavanceerde functies van de regel te bepalen.

Adres:

The screenshot shows the 'Nieuwe regel invoeren' dialog box with the 'Adres' tab selected. The 'Lokaal adres' section has 'Host-adres' selected. The 'Extern adres' section has 'Webadres' selected, and a text box below it is empty. The 'Adres' tab is highlighted in the tab bar at the top of the dialog.

Figuur 7

Voor een standaard regel is op deze tab alleen de optie "Alle adressen" mogelijk.

Voor geavanceerde regels geeft u hier aan hoe de website wordt aangeduid, via zijn URL of via zijn IP-adres.

Door het keuzerondje URL in te schakelen kunt u een URL in het adresveld invoeren.

Door het keuzerondje IP-adres in te schakelen verandert u het adresveld in een IP-adresveld.

Poort:

The screenshot shows the 'Nieuwe regel invoeren' dialog box with the 'Poort' tab selected. The 'Lokale poort' section has 'Alle poorten' selected. The 'Externe poort' section has 'Lijst van poorten' selected, and a text box below it contains the numbers '80' and '443'. The 'Poort' tab is highlighted in the tab bar at the top of the dialog.

Figuur 8

Op het tabblad Poort (Figuur 8) kunt u de poort of de poorten opgeven waarop de regel van toepassing is. Poortinstellingen moeten zowel voor lokale als voor externe computers worden geconfigureerd. Deze tab bevat de volgende opties.

- **Eén poort:** Hiermee kunt u een enkel poortnummer opgeven voor de regel.
- **Poortbereik:** Hiermee kunt u een reeks poorten opgeven voor de regel.
- **Lijst van poorten:** Hiermee kunt u een lijst van poorten opgeven voor de regel.
- **Alle poorten:** Hiermee maakt u dat de regel wordt toegepast op alle poorten.

Tijd:

The screenshot shows the 'Nieuwe regel invoeren' (New Rule Wizard) dialog box. The 'Tijd' (Time) tab is active, displaying a table for scheduling the rule. The table has three columns: 'Tijdinterval' (Time interval), a checkbox, and a 'Uit' (Out) button. All days of the week are checked.

| Tijdinterval | | |
|---|--|-----|
| <input checked="" type="checkbox"/> maandag | | Uit |
| <input checked="" type="checkbox"/> dinsdag | | Uit |
| <input checked="" type="checkbox"/> woensdag | | Uit |
| <input checked="" type="checkbox"/> donderdag | | Uit |
| <input checked="" type="checkbox"/> vrijdag | | Uit |
| <input checked="" type="checkbox"/> zaterdag | | Uit |
| <input checked="" type="checkbox"/> zondag | | Uit |

Met het tabblad Tijd kunt u zorgen dat de regel alleen wordt geactiveerd op bepaalde dagen.

Figuur 9

5 Weblijsten

U kunt weblijsten gebruiken om de toegang tot specifieke websites toe te staan of te blokkeren. URL-lijsten kunnen zwarte lijsten of witte lijsten zijn. Zwarte lijsten en witte lijsten zijn wederzijds exclusief, dat wil zeggen dat een gebruiker die is geconfigureerd om een zwarte lijst te gebruiken, niet kan worden geconfigureerd om een witte lijst te gebruiken en viceversa.

5.1 Zwarte lijsten

Zwarte lijsten worden gebruikt om toegang tot websites te blokkeren die eventueel wel door een regel zijn toegestaan. Er kan bijvoorbeeld een standaard regel zijn geconfigureerd om toegang tot alle websites toe te staan, maar een specifieke website, bijvoorbeeld www.niettoegestaan.com, staat op de zwarte lijst. In deze situatie mag de gebruiker alle websites bezoeken, behalve www.niettoegestaan.com.

5.2 Witte lijsten

Witte lijsten worden gebruikt om toegang tot websites toe te staan die eventueel door een regel zijn geblokkeerd. Een standaard regel kan bijvoorbeeld de toegang tot alle websites blokkeren, maar een specifieke website, bijvoorbeeld www.disney.com, staat op de witte lijst. Daarom kan de gebruiker geen enkele website bezoeken, behalve www.disney.com.

5.3 Globale en lokale lijsten

Er bestaan twee typen zwarte en witte lijsten: lokale en globale. Een globale lijst wordt aangelegd door de beheerder en kan worden toegepast op alle gebruikers; de adressen in de globale lijst zijn van toepassing op alle gebruikers voor wie de beheerder heeft bepaald dat een globale URL-lijst wordt gebruikt. Een lokale lijst wordt alleen voor een specifieke gebruiker aangelegd; de adressen in deze lijst zijn alleen van toepassing op de gebruiker voor wie de lijst is gemaakt.

6 Problemen met NetBIOS

In bepaalde situaties kunt u problemen verwachten bij het verkrijgen van toegang tot hosts via NetBIOS over TCP/IP wanneer u in de modus Afgeschermde bent. Het probleem treedt op wanneer uw

computer pakketten moet uitzenden om het IP-adres te bepalen van een host op het netwerk. In de modus Afgeschermd zal TerMiNET de door de server teruggezonden berichten blokkeren waardoor het tot stand komen van verbindingen onmogelijk wordt gemaakt.

In deze situatie is het noodzakelijk om een item toe te voegen aan uw "HOSTS"-bestand waarin de adressen van de benodigde hosts worden verbonden aan hun NetBIOS-namen. "HOSTS" is een gewoon tekstbestand dat gewoonlijk kan worden gevonden in de directory c:\windows in Windows98 of in de directory c:\system32\drivers\etc in Windows NT en dat kan worden gewijzigd met behulp van een willekeurige tekstverwerker. In het voorbeeldbestand hosts.sam in de directory vindt u details over de bestandsstructuur. Een typisch host-bestand ziet er ongeveer als volgt uit.

```
192.168.25.2 mijnserver.mijnorg.com  
192.168.56.10 nt_server_1
```

Als u een host wilt toevoegen met de naam nt_server_2 met het IP-adres 192.168.35.23, dient u het bestand als volgt te wijzigen:

```
192.168.25.2 mijnserver.mijnorg.com  
192.168.55.10 nt_server_1  
192.168.35.23 nt_server_2
```

Dit probleem bestaat niet als op uw netwerk een WINS-server is geconfigureerd.