

TerminET

Personlig brandvägg

Användarhandbok

Innehåll

1	INLEDNING	3
1.1	OM TERMINET	3
1.2	HUVUDFUNKTIONER	3
2	KOMMA IGÅNG	3
2.1	INSTALLERA TERMINET	3
2.2	LOGGA IN PÅ TERMINET	3
2.2.1	<i>Windows 95/98</i>	3
2.2.2	<i>Windows NT/2000</i>	4
2.3	ADMINISTRATIONSÄGE	4
2.4	TERMINET-GRÄNSSNITTET	4
3	ANVÄNDARE OCH GRUPPER. HANTERA ANVÄNDARE OCH GRUPPER	6
3.1	LÄGGA TILL ANVÄNDARE	6
3.2	SKAPA GRUPPER	7
4	TRAFIKREGLER	7
4.1	STANDARDREGLER:	7
4.2	AVANCERADE REGLER:	7
4.3	SKAPA REGLER:	8
5	WEBBLISTOR	10
5.1	SVARTA LISTOR	10
5.2	VITA LISTOR	10
5.3	GLOBALA OCH LOKALA LISTOR	10
6	PROBLEM MED NETBIOS	11

1 Inledning

1.1 Om TermiNET

TermiNET är en personlig brandvägg som är utformad att skydda datorn från attacker utifrån medan du är ansluten till Internet, surfar på nätet eller är uppkopplad till andra Internet-tjänster. TermiNET kan installeras i något av följande startlägen:

1. "Stängt läge" blockerar som standard all trafik till och från den lokala datorn. Administratören kan sedan välja vad som ska vara åtkomligt, t ex endast en ftp-plats eller både ftp, Telnet och webbplatser. Webbåtkomst kan även begränsas till enbart vissa webbsidor. Du kan ange vilka sidor som ska tillåtas direkt som specifika regler eller hämta dem från en "vit lista" med webbadresser
2. I "öppet läge" är inget skydd aktiverat. Administratören kan sedan välja att blockera åtkomst efter tillämpning, port eller protokoll, t ex blockera all Telnet- och ftp-trafik, blockera all inkommande kommunikation till port 25 eller blockera åtkomst till en viss uppsättning med webbsidor. Detta kan göras genom att ange specifika regler eller hämta dem från en "svart lista" med webbsidor.
3. I "smygläge" tillåts all utgående trafik medan alla inkommande anslutningar blockeras, såvida de inte upprättas lokalt. I det här läget kan datorn användas som vanligt för att surfa på nätet, använda ftp, etc, medan den är skyddad från attacker utifrån.

TermiNET är en idealisk säkerhetslösning för små och medelstora företag eller enskilda användare som vill ha en säker anslutning till Internet men som inte har de resurser som krävs för att hantera en stor säkerhetsinfrastruktur.

1.2 Huvudfunktioner

TermiNET har följande huvudfunktioner:

- Standardregler och avancerade regler: Enkla kryssrutor för att aktivera/inaktivera funktioner.
- Svart lista/vit lista som medför att du kan blockera åtkomst till angivna webbplatser, eller tillåta åtkomst endast till kända, pålitliga platser.
- Flexibel åtkomstkontroll gör att du kan ange regler efter IP-adress, webbadress (URL), port och/eller protokoll
- Tidsbaserade regler som kan konfigureras så att de är aktiva enbart på vissa dagar.
- Användarvänligt gränssnitt som liknar "Windows Utforskaren" gör att det är enkelt att konfigurera TermiNET även för användare som inte är så tekniskt bevandrade.

2 Komma igång

2.1 Installera TermiNET

Stoppa in cd-skivan med TermiNET i cd-romenheten på datorn. Installationsprogrammet körs normalt automatiskt, annars klickar du på "Start" -> "Kör" och skriver "D:\setup" (där D: är enhetsbeteckningen för cd-romenheten). Följ anvisningarna på skärmen för att installera programmet. Under installationen kan du ange var programmet ska installeras och välja något av de tre startlägena Öppet, Stängt eller Smyg, som beskrivs ovan.

När installationen är klar **måste** du starta om datorn för att slutföra installationen.

2.2 Logga in på TermiNET

2.2.1 Windows 95/98

När systemet startas, öppnas TermiNET med vissa standardregler som angetts av administratören. Om flera TermiNET-användarprofiler har skapats finns det två sätt att logga in som definierad användare, antingen genom att dubbelklicka på ikonerna TermiNET i systemfältet eller genom att högerklicka på ikonerna

TermiNET och välja "Logga in". I båda fallen visas ett inloggningsfönster för användaren som frågar efter ett användar-ID och ett lösenord. När användar-ID och lösenordet har skrivits in, aktiveras säkerhetsprofilen för angiven användare.

2.2.2 Windows NT/2000

Användarna loggas in automatiskt på TerminiNET baserat på deras NT-inloggningsprofil.

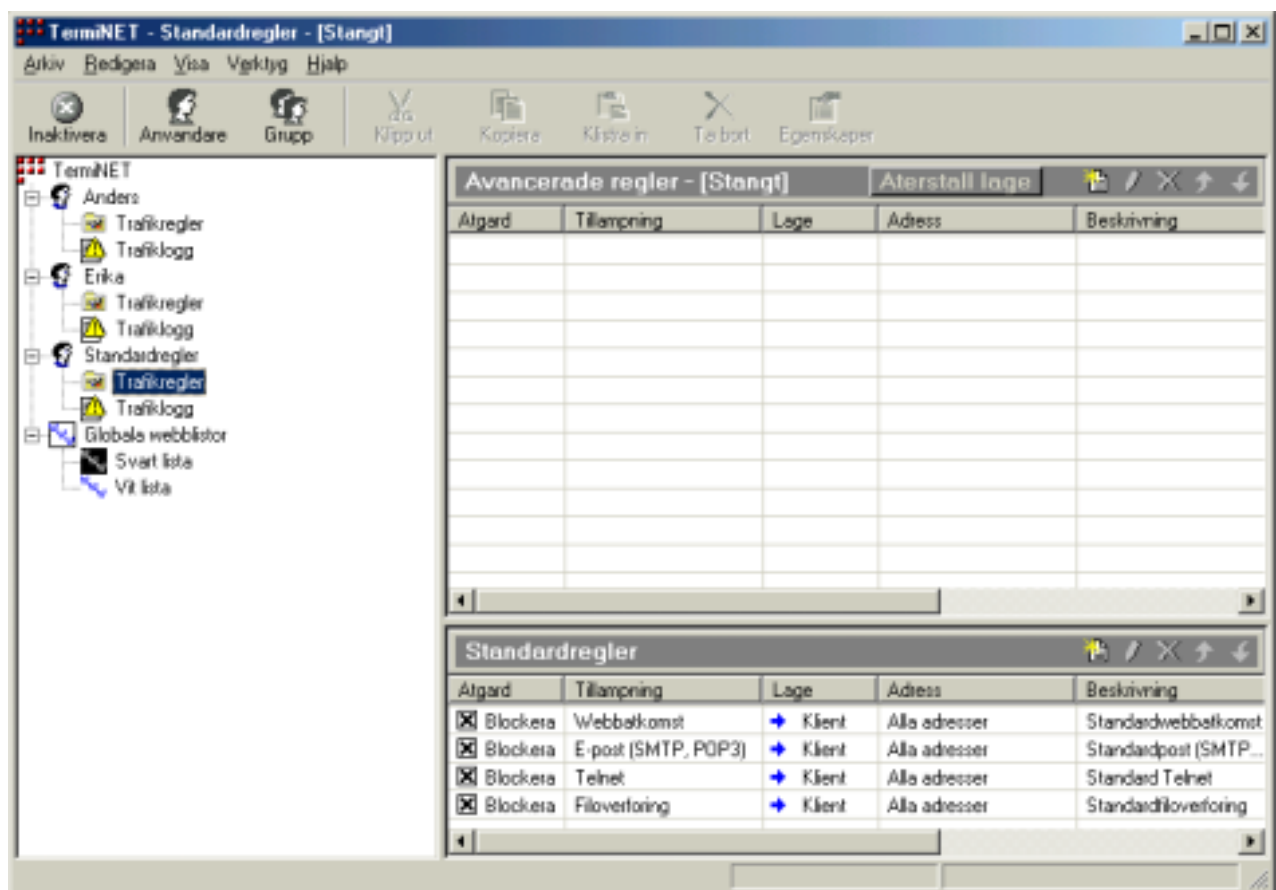
2.3 Administrationsläge

I administrationsläge kan administratören ange standardsäkerhetsprofiler för användare, skapa nya användarprofiler och ställa in avancerade regler för särskilda användare. Du aktiverar administrationsläget genom att högerklicka på ikonen TerminiNET i systemfältet och välja "Administrationsläge". Du måste ange ett administrationslösenord. När du har angett lösenordet visas konfigurationsfönstret för TerminiNET, som innehåller olika administrationsfunktioner.

När du vill avsluta administrationsläget stänger du konfigurationsfönstret genom att välja "Arkiv - >Avsluta administration".

2.4 TerminiNET-gränssnittet

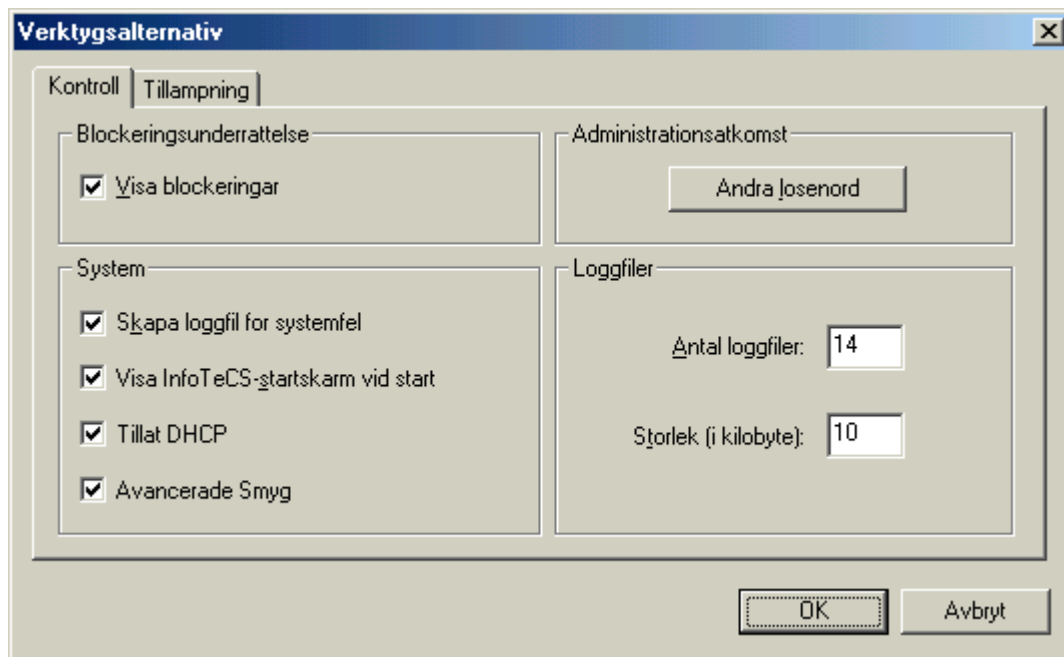
TerminiNET-gränssnittet (Figur 1) är endast åtkomligt med ett administrationslösenord. Det är ett användarvänligt, grafiskt verktyg för att definiera säkerhetsprofiler för en dator.



Figur 1

Gränssnittet är uppdelat i tre områden. På den vänstra sidan visas en trädvy av aktuellt säkerhetssystem. Längst ner till höger i fönstret visas standardregler, som är fördefinierade av systemet. Högst upp till höger visas avancerade regler om några sådana har skapats. Om du markerar en användare i den vänstra fönsterrutan visas de standardregler och avancerade regler som gäller för den användaren i den högra fönsterrutan.

På menyraden finns menyerna Arkiv, Redigera och Visa som du kan använda för att anpassa programmet (om du har administrationsbehörighet). Om du väljer "Verktyg" -> "Alternativ" kan du ställa in olika systemegenskaper.



Figur 2

Fliken Kontroll (Figur 2) innehåller följande alternativ.

Visa blockeringar:

När det här alternativet är markerat visas både blockerad och tillåten trafik i trafikloggen. Om det är avmarkerat registreras endast tillåten trafik.

Skapa loggfil för systemfel:

När det här alternativet är markerat skrivs systemfel till filen \Program\Infotecs\Terminet\Data\errorlog.txt.

Visa Infotecs-startskärm vid start:

Avmarkera det här alternativet om du inte vill att Infotecs-startskärmen ska visas varje gång TerMiNET startas.

Ändra lösenord

Gör att du kan ändra administrationslösenordet.

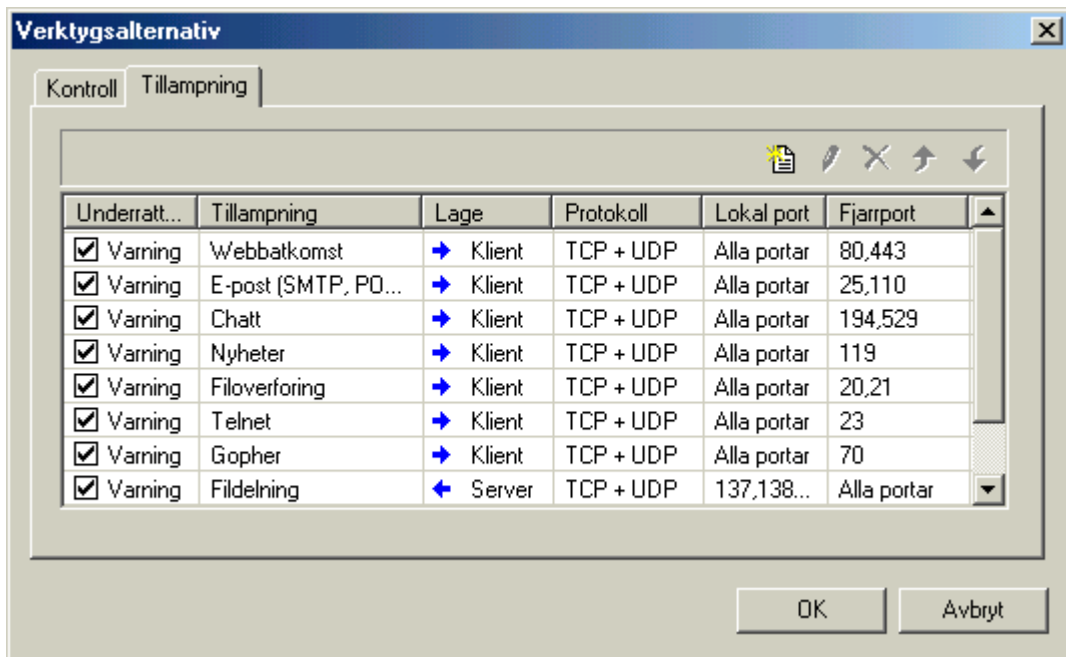
Antal loggfiler

Anger antalet trafikloggfiler som används. När angivet antal loggfiler nås och den sista filen har högsta tillåtna storlek, skrivs den första filen över


Storlek (i kilobyte):

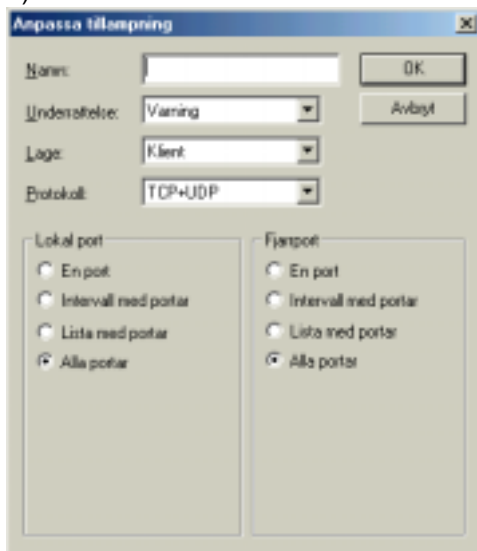
Anger hur stor en trafikloggfil får bli i kilobyte. När storleken nås, sparas filen och en annan fil registreras.

På fliken Tillämpning (Figur 3) kan du skapa nya standardtillämpningar.



Figur 3

När du klickar på knappen Lägg till tillämpning  öppnas en dialogruta där du kan anpassa en tillämpning (Figur 4).



Figur 4

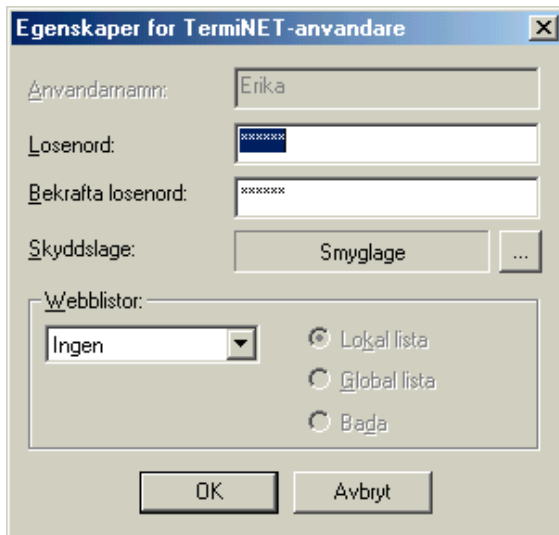
Det här fönstret innehåller följande alternativ:

- **Namn:** Ange namnet på den anpassade tillämpningen.
- **Protokoll:** Välj ett protokoll för tillämpningen i listrutan.
- **Underrättelse:** Välj Varning eller Ingen i listrutan. Om du väljer Varning visas en underrättelse när trafik av denna typ blockeras.
- **Riktning:** Välj Server (inkommande), Klient (utgående) eller Alla portar i listrutan.
- **Fjärrport:** Ange vilken portinställning som ska gälla för fjärrdatoren för denna tillämpning.
- **Lokal port:** Ange vilken portinställning som ska gälla för den lokala datorn för denna tillämpning.

3 Användare och grupper. Hantera användare och grupper

3.1 Lägga till användare

När du vill lägga till en användarprofil högerklickar du på den högsta nivån i TermiNET-trädvy och väljer "Lägg till användare" på snabbmenyn, eller klickar på knappen Användare i verktygsfältet. Då visas dialogrutan Egenskaper för TermiNET-användare (Figur 5)



Figur 5

Följande fält finns i dialogrutan.

- **Användarnamn:** Ange ett användarnamn för användaren.
- **Lösenord:** Ange ett lösenord för användaren.
- **Bekräfta lösenord:** Ange lösenordet igen för att bekräfta det.
- **Skyddsläge:** Ange standardsäkerhetsläge för användaren.
- **Webblistor:** Anger om användaren använder en svart eller vit lista med webbadresser, och om global eller lokal lista (eller båda) kommer att användas.

3.2 Skapa grupper

Du kan använda grupper för att organisera listor med användare i TermiNET-trädvyn. Du skapar en ny grupp genom att högerklicka på den högsta nivån i trädet och välja "Lägg till grupp" på snabbmenyn och sedan skriva namnet på gruppen. Sedan kan du placera användarna i grupper genom att klicka på användarnamnen och dra dem till grupperna. Du kan skapa en användare i en befintlig grupp genom att högerklicka på gruppen i trädvyn och välja "Lägg till användare" på snabbmenyn.

4 Trafikregler

Du kan definiera två olika typer av trafikregler i TermiNET.

4.1 Standardregler:

Gäller för alla IP-adresser och kan användas för att globalt tillåta åtkomst till vissa tjänster. Det finns fyra standardregler, Webbåtkomst, E-post, FTP och Telnet. Du kan lägga till fler regler genom att markera en användare i trädvyn, högerklicka i fönsterrutan Standardregler och välja "Lägg till regel" på snabbmenyn. Då öppnas dialogrutan Lägg till regel (Figur 6).

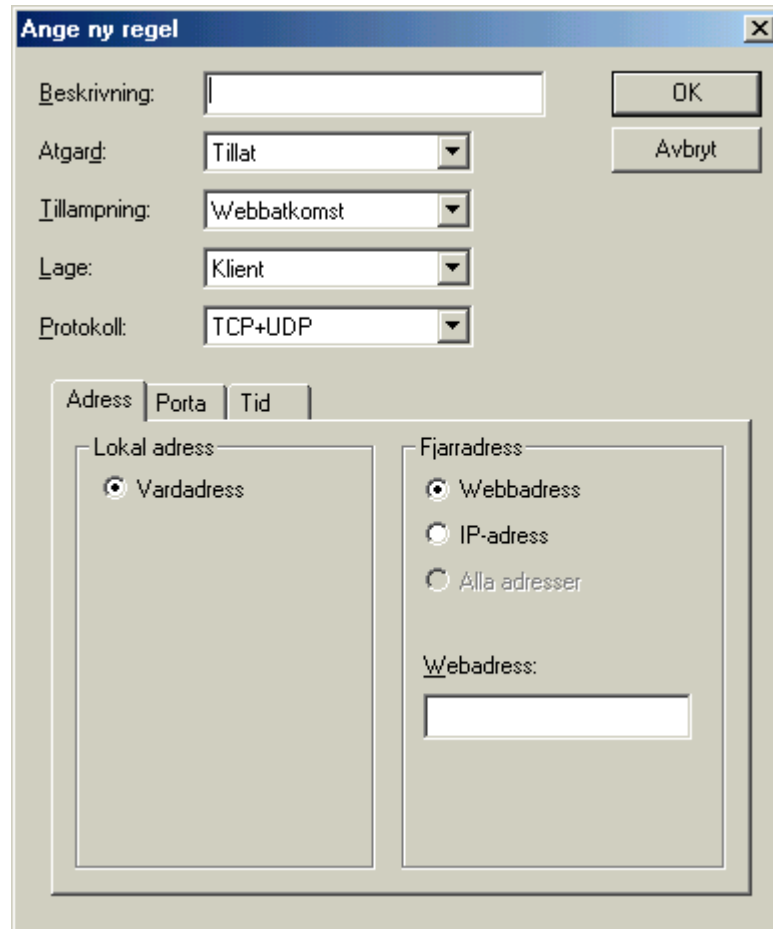
4.2 Avancerade regler:

Gäller för en specifik IP- eller webbadress (URL) och används för att tillåta eller neka åtkomst till vissa webbplatser och -tjänster. Du kan lägga till regler genom att markera användaren som regeln ska tillämpas för, högerklicka i fönstret Avancerade regler och välja "Lägg till regler" på snabbmenyn. Då öppnas dialogrutan Lägg till regel.

Om TermiNET är installerat i smygläge kan endast avancerade regler konfigureras.

4.3 Skapa regler:

Dialogrutan Lägg till regler (Figur 6) används för att skapa och definiera nya regler.



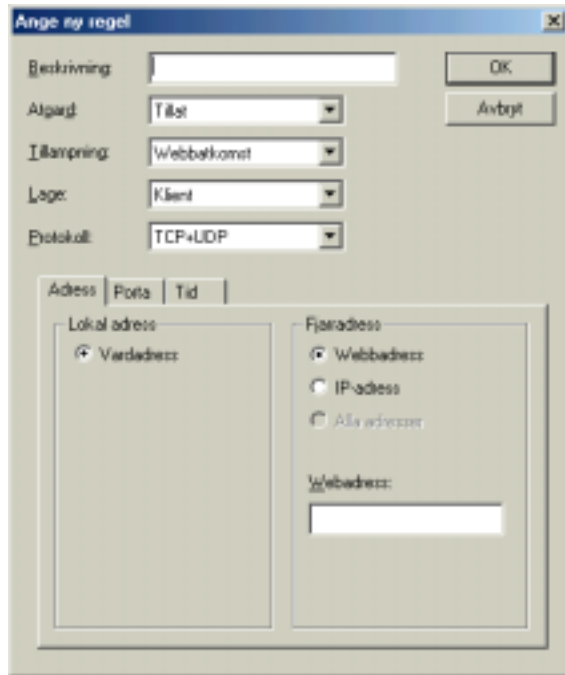
Figur 6

Följande fält finns i dialogrutan.

- **Beskrivning:** Skriv en beskrivning för regeln du skapar.
- **Åtgärd:** Ange om regeln ska tillåta eller blockera definierad trafik.
- **Tillämpning:** Välj i listan med fördefinierade tillämpningar eller ange ett nytt namn för tillämpningen som regeln ska tillämpas på.
- **Läge:** Ange om den lokala datorn ska vara klient eller server för regeln. Om du anger den som klient tillämpas regeln på utgående trafik, om du anger den som server tillämpas regeln på inkommande trafik.

Flikarna Adress (Figur 7), Port (Figur 8) och Tidsintervall (Figur 9) används för att ange avancerade funktioner för regeln.

Adress:



Figur 7

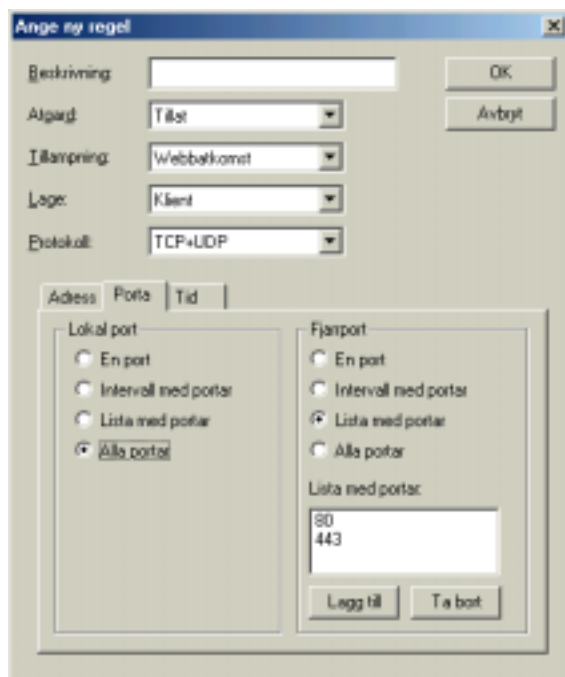
För standardregler är "Alla adresser" det enda tillgängliga alternativet.

För avancerade regler kan du ange en plats som regeln ska tillämpas på, antingen efter en webbadress (URL) eller en IP-adress.

Om du väljer alternativknappen URL-adress kan du skriva in en webbadress i adressfältet.

Om du väljer alternativknappen IP-adress ändras adressfältet så att du kan ange en IP-adress.

Port:



Figur 8

Fliken Port (Figur 8) använder du när du vill ange en port eller ett intervall med portar som regeln ska gälla för. Portinställningarna måste konfigureras för både lokala datorer och fjärdatorer. Följande alternativ finns i dialogrutan.

- **En port:** Gör att du kan ange ett enstaka portnummer för regeln.
- **Intervall med portar:** Gör att du kan ange ett intervall med portar för regeln.
- **Lista med portar:** Gör att du kan ange en lista med portar för regeln.
- **Alla portar:** Gör att regeln gäller för alla portar.

Tidsintervall:

Adress	Porta	Tid
Tidsintervall		
<input checked="" type="checkbox"/> måndag		Pa
<input checked="" type="checkbox"/> tisdag		Pa
<input checked="" type="checkbox"/> onsdag		Pa
<input checked="" type="checkbox"/> torsdag		Pa
<input checked="" type="checkbox"/> fredag		Pa
<input checked="" type="checkbox"/> lördag		Pa
<input checked="" type="checkbox"/> söndag		Pa

På fliken Tidsintervall kan du ställa in regeln så att den är aktiv på vissa dagar.

Figur 9

5 Webblistor

Webblistor använder du för att tillåta eller blockera åtkomst till vissa webbplatser. Webblistor kan vara antingen svarta listor eller vita listor. Svarta och vita listor är exklusiva, dvs en användare som är konfigurerad att använda en svart lista kan inte samtidigt vara konfigurerad att använda en vit lista, och tvärtom.

5.1 Svarta listor

Svarta listor används för att blockera åtkomst till webbplatser som kanske är tillåtna av en regel. En standardregel kan exempelvis vara konfigurerad att tillåta all webbåtkomst medan en specifik plats, t ex www.risk.com, är listad i den svarta listan. I det här fallet kan användaren visa alla webbplatser utom www.risk.com.

5.2 Vita listor

Vita listor används för att tillåta åtkomst till webbplatser som kanske är blockerade av en regel. En standardregel kan exempelvis blockerar all webbåtkomst medan en specifik plats, t ex www.disney.com, är listad i den vita listan. I detta fall kan inte användaren visa några webbplatser förutom www.disney.com.

5.3 Globala och lokala listor

Det finns två typer av svarta och vita listor: lokala och globala listor. En global lista skapas av administratören och kan gälla för alla användare. Poster i den globala listan tillämpas på alla användare för vilka administratören har angett att en global lista med webbadresser ska användas. En lokal lista skapas för en enskilda användare och poster i den här listan tillämpas enbart på användaren för vilken listan skapades.

6 Problem med NetBIOS

Under vissa omständigheter kan du få problem med att få åtkomst till värdar som använder NetBIOS över TCP/IP i smygläge. Problemet inträffar när datorn använder broadcast-meddelanden för att ta reda på IP-adressen på en värddator i nätverket. I smygläge blockerar TermiNET meddelanden som skickas tillbaka från värddatorerna, vilket gör att kommunikationen inte fungerar.

I dessa fall måste du skapa en post i filen "HOSTS" som kopplar IP-adresserna för värdarna till deras NetBIOS-namn. "HOSTS" är en textfil som vanligtvis finns i katalogen C:\Windows på Win'98 eller C:\system32\drivers\etc på Win NT och du kan redigera den med en vanlig textredigerare. Exempelfilen hosts.sam i katalogen innehåller mer information om filstrukturen.

En typisk värdfil ser ut ungefär så här:

```
192.168.25.2 minserver.minfirma.com  
192.168.56.10 nt_server_1
```

Om du vill lägga till en värd med namnet nt_server_2 med IP-adressen 192.168.35.23, redigerar du filen så här:

```
192.168.25.2 minserver.minfirma.com  
192.168.55.10 nt_server_1  
192.168.35.23 nt_server_2
```

Detta problem uppstår inte om en WINS-server är konfigurerad på nätverket.