

TerminET

Personlig brannmur

Brukerhåndbok

Innhold

1	INNLEDNING	3
1.1	OM TERMiNET	3
1.2	NØKKELFUNKSJONER	3
2	KOMME I GANG	3
2.1	INSTALLERE TERMiNET	3
2.2	LOGGE PÅ TERMiNET	3
2.2.1	<i>Windows 95/98</i>	3
2.2.2	<i>Windows NT/2000</i>	4
2.3	ADMINISTRATORMODUS	4
2.4	TERMiNET-GRENSESNI TTET	4
3	BRUKERE OG GRUPPER. ADMINISTRERE BRUKERE OG GRUPPER	6
3.1	LEGG E TIL BRUKERE	6
3.2	OPPRETTE GRUPPER	7
4	TRAFIKKREGLER	7
4.1	STANDARDREGLER:	7
4.2	AVANSERTE REGLER:	7
4.3	OPPRETTE REGLER:	8
5	WEBLISTER	10
5.1	SVARTE LISTER	10
5.2	HVITE LISTER	10
5.3	GLOBAL E OG LOKALE LISTER	10
6	PROBLEMER MED NETBIOS	10

1 Innledning

1.1 Om TermiNET

TermiNET er en personlig brannmur som er utviklet for å beskytte en datamaskin mot angrep fra utsiden når du er koblet til Internett, søker på webområder eller har tilgang til andre Internett-tjenester. Under installasjonen kan TermiNET konfigureres til en av følgende modi:

1. Lukket modus sperrer som standard all trafikk til og fra den lokale datamaskinen. Administratoren kan deretter åpne for selektiv tilgang, for eksempel ved å tillate bare FTP eller tillate FTP, telnet og webtilgang. Som overordnet kontroll kan tilgang begrenses til bare et bestemt sett webområder. Sidene kan oppgis direkte via spesifikke regler, eller leses fra en hvit webliste.
2. Åpen modus gir i utgangspunktet ingen sperring. Men administratoren kan senere selektivt sperre tilgang med bestemte programmer, porter og protokoller. Han/hun kan for eksempel sperre all forbindelse med telnet og FTP, all innkommende kommunikasjon på port 25 eller tilgang til et bestemt sett webområder. Dette kan oppgis via spesifikke regler eller leses fra en svart webliste eller godkjente områder.
3. Skjult modus tillater all utgående trafikk, men sperrer alle forsøk på innkommende tilkobling, hvis de ikke initieres lokalt. I denne modusen kan datamaskinen brukes som normalt til websøking, FTP og så videre, men er beskyttet mot angrep mens den er koblet til Internett.

TermiNET er en ideell sikkerhetsløsning for småbedrifter og hjemmebrukere som vil ha en sikker tilkobling til Internett, men ikke har nok ressurser til å opprette en omfattende infrastruktur for sikkerhet.

1.2 Nøkkelfunksjoner

Nøkkelfunksjonene i TermiNET inkluderer

- Standardregler og avanserte regler som med en enkel avkrysningsfunksjon kan slås **på** og **av**.
- Svarte og hvite lister som gir mulighet til å nekte tilgang til bestemte uønskede webområder, eller tillate tilgang til kjente og aksepterte områder.
- Fleksibel tilgangskontroll som lar deg spesifisere regler for bruk av IP-adresse, webadresse, port og/eller protokoll.
- Tidsbaserte regler som kan konfigureres slik at de er aktive på bestemte dager.
- Samme type grensesnitt som i Windows Utforsker, gjør det enkelt og intuitivt å konfigurere TermiNET, selv for brukere med liten eller ingen teknisk innsikt.

2 Komme i gang

2.1 Installere TermiNET

Sett inn TermiNET-CDen i CD-ROM-stasjonen på datamaskinen. Installasjonsprogrammet skal da starte automatisk. Hvis Autorun er deaktivert, klikker du Start -> Kjør og skriver D:\setup, der D: er stasjonsbokstaven for CD-ROM-stasjonen. Følg instruksjonene på skjermen for å installere produktet.

Under installasjonen kan du angi hvor installasjonen skal plasseres, og velge én av de tre standard sikkerhetsmodiene, Åpen, Lukket eller Skjult, som er beskrevet over. Når installasjonsprogrammet er ferdig, **må** datamaskinen startes på nytt for å fullføre installasjonen.

2.2 Logge på TermiNET

2.2.1 Windows 95/98

Når systemet startes, åpnes TermiNET med et sett standardregler som er definert av administratoren. Hvis det er opprettet flere TermiNET-brukerprofiler, kan brukeren logge seg på som en av de definerte brukerne på to måter. Han/hun kan enten dobbeltklikke på TermiNET-ikonet i systemkurven, eller alternativt høyreklikke på ikonet og velge Logg på. I begge tilfeller vises det et påloggingsskjerm bilde.

der brukeren blir bedt om å oppgi et brukernavn og et passord. Etter at brukernavnet og passordet er oppgitt, kan den riktige sikkerhetsprofilen for denne brukeren aktiveres.

2.2.2 Windows NT/2000

Brukere logges automatisk på TermiNET basert på NT-påloggingsprofilen.

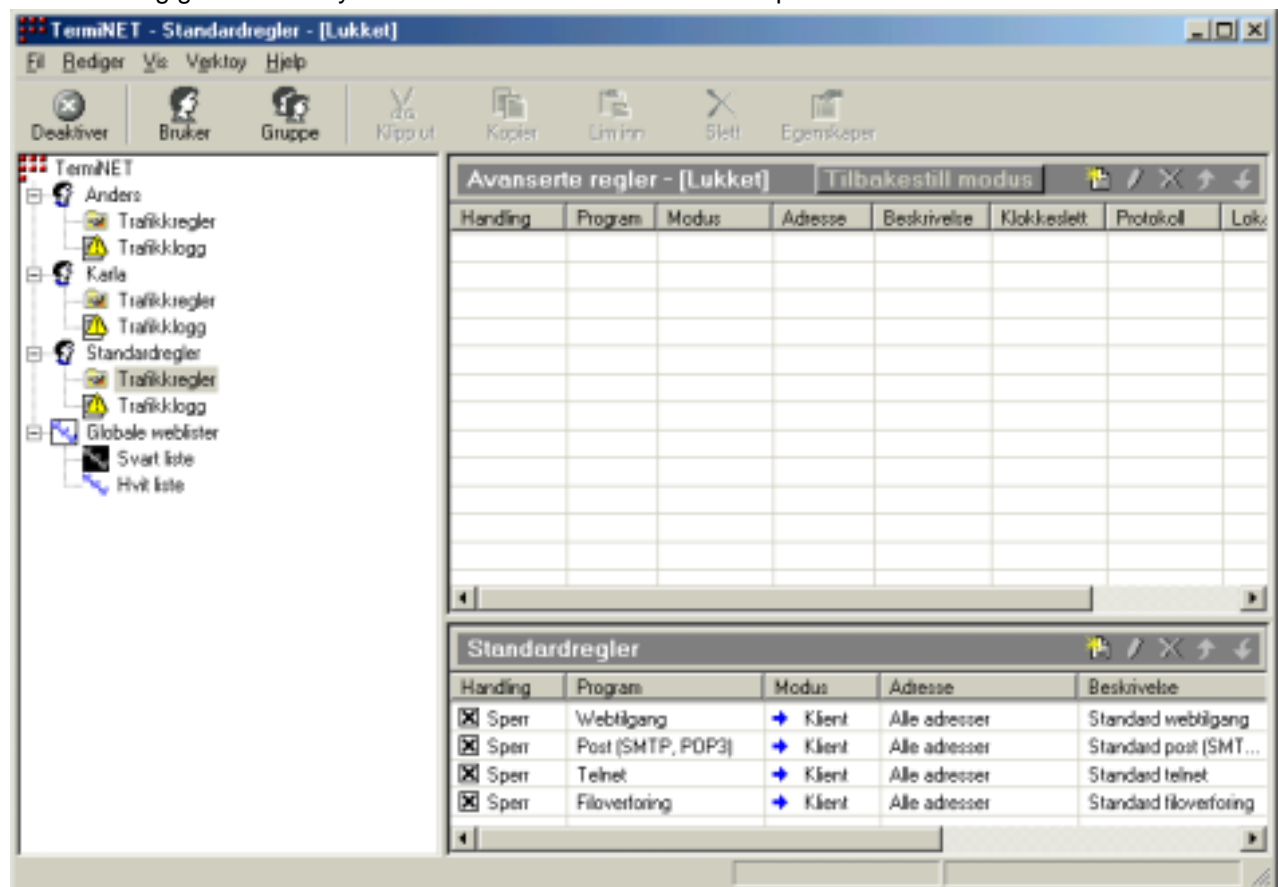
2.3 Administratormodus

I administratormodus kan du angi standard sikkerhetsprofiler for brukere, opprette nye brukerprofiler og angi avanserte regler for bestemte brukere. Administratormodus åpnes ved å høyreklikke på TermiNET-ikonet i systemkurven og velge Administratormodus. Du blir bedt om å oppgi administratorpassordet. Når passordet er oppgitt, vises konfigurasjonsskjermbildet for TermiNET og du kan utføre administrative oppgaver.

Når du vil avslutte administratormodus, lukker du bare konfigurasjonsskjermbildet med menyvalget Fil -> Avslutt Administrator.

2.4 TermiNET-grensesnittet

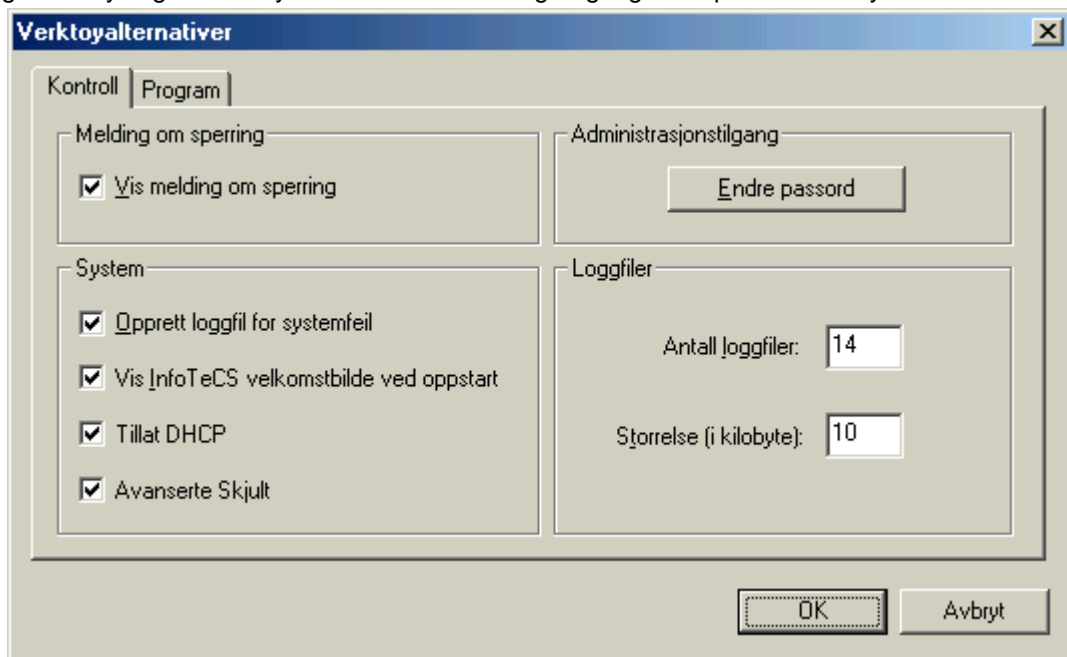
TermiNET-grensesnittet (Figur 1) kan bare åpnes ved å oppgi administratorpassordet. Dette er et brukervennlig grafisk verktøy som brukes til å definere sikkerhetsprofilene for en datamaskin.



Figur 1

Grensesnittet er delt inn i tre vinduer. Det venstre vinduet viser en trestruktur over sikkerhetssystemet som er definert. Vinduet nederst til høyre viser standardreglene som er definert av systemet på forhånd. I vinduet øverst til høyre vises eventuelle avanserte regler som er opprettet. Når du merker en bruker i det venstre vinduet, viser vinduene på høyre side statusen for denne brukerens standardregler og avanserte regler.

Grensesnittet kan tilpasses med Fil-, Rediger- og Vis-menyene i henhold til administratorens innstillinger. Menyvalget Verktøy -> Alternativer lar deg angi egenskaper for hele systemet.

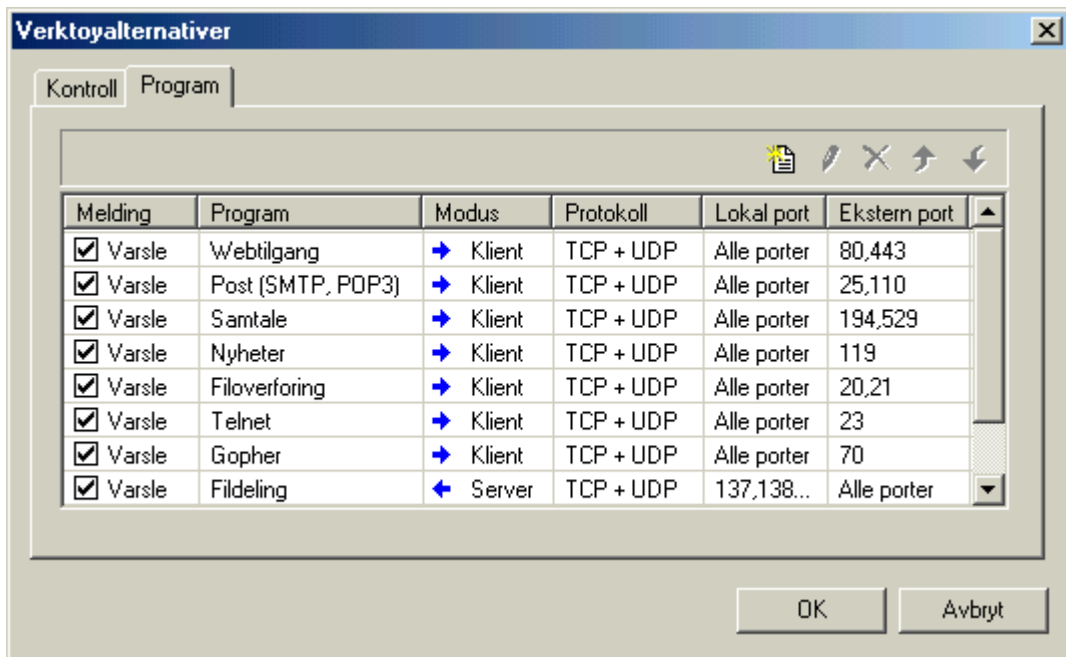


Figur 2


Kategorien Kontroll (Figur 2) gir tilgang til følgende alternativer.

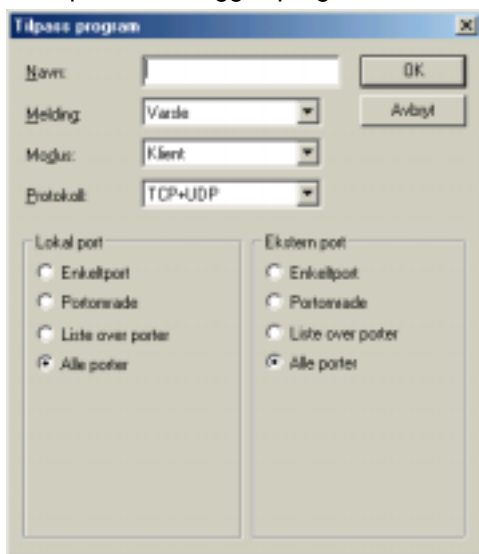
- | | |
|---|--|
| Vis melding om sperring: | Når denne er merket, viser trafikkloggen både sperret og tillatt trafikk. Når den ikke er merket, registreres bare trafikk som er tillatt. |
| Opprett loggfil for systemfeil: | Når denne er merket, skrives systemfeil til filen \Programfiler\Infotecs\Terminet\Data\errorlog.txt. |
| Vis Infotecs velkomstbilde ved oppstart: | Fjern merkingen for å hindre at Infotecs velkomstbilde vises når TermiNET starter. |
| Endre passord: | Lar deg endre administratorpassordet. |
| Antall loggfiler: | Angir antall trafikkloggfiler som skal registreres. Når den siste filen er tatt i bruk og maksimumsstørrelsen nås, overskrives den første. |
| Størrelse (i kilobyte): | Angir maksimumsstørrelsen på en trafikkloggfil. Når denne størrelsen nås, lagres filen og registreringen fortsetter i en ny fil. |

I kategorien Programmer (Figur 3) kan du opprette nye standardprogrammer.



Figur 3

Klikk på ikonet Legg til program  for å vise dialogboksen Tilpass program (Figur 4).



Figur 4

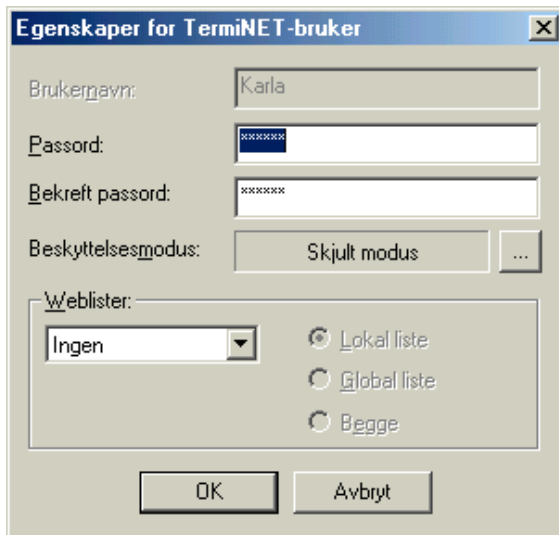
I dette vinduet kan du angi følgende alternativer.

- **Navn:** Angi navnet på programmet som skal tilpasses.
- **Protokoll:** Velg protokollen du vil bruke fra rullegardinlisten.
- **Melding:** Velg Varsle eller Ignorerer fra rullegardinlisten. Hvis du velger Varsle, vises en melding når denne typen trafikk sperrer.
- **Retning:** Velg Innkommende eller Utgående fra rullegardinlisten.
- **Ekstern port:** Angi portinnstillingene som skal gjelde for den eksterne datamaskinen for dette programmet.
- **Lokal port:** Angi portinnstillingene som skal gjelde for den lokale datamaskinen for dette programmet.

3 Brukere og grupper. Administrere brukere og grupper

3.1 Legg til brukere

Hvis du vil legge til en brukerprofil, høyreklikker du det høyeste nivået i trestrukturen i TermiNET og velger Legg til bruker fra hurtigmenyen, eller klikker på Bruker på verktøylinjen. Du får da dialogboksen Egenskaper for TermiNET-bruker (Figur 5)



Figur 5

Følgende felt finnes.

- **Brukernavn:** Brukes til å skrive inn brukernavnet til brukeren.
- **Passord:** Oppgi det aktuelle passordet for brukeren.
- **Bekreft passord:** Skriv inn passordet på nytt for å bekrefte at det er riktig.
- **Beskyttelsesmodus:** Velg standard sikkerhetsmodus for denne brukeren.
- **Webmaster:** Bestemmer om brukeren skal bruke hvit eller svart liste og global eller lokal liste eller begge disse.

3.2 Opprette grupper

Grupper kan opprettes for å organisere lister med brukere i TermiNET-vinduet som viser trestrukturen. Du kan opprette en ny gruppe ved å høyreklikke det høyeste nivået i strukturen, velge Legg til gruppe fra hurtigmenyen og skrive inn navnet du vil gi gruppen. Brukerne kan deretter plasseres i grupper ved å klikke på brukernavnet og dra det til den aktuelle gruppen. Du kan opprette en bruker i en eksisterende gruppe ved å høyreklikke på gruppen i i vinduet med trestrukturen og velge Legg til bruker fra hurtigmenyen.

4 Trafikkregler

Det kan defineres to typer trafikkregler i TermiNET.

4.1 Standardregler:

Brukes på alle IP-adresser og kan brukes globalt for å tillate eller ikke tillate tilgang til bestemte tjenester. På forhånd har systemet definert fire standardregler for henholdsvis webtilgang, FTP, telnet og post. Flere regler kan legges til ved å merke en bruker i vinduet som viser trestrukturen, høyreklikke i vinduet Standardregler og velge Legg til regel fra hurtigmenyen for å vise dialogboksen Legg til regel (Figur 6).

4.2 Avanserte regler:

Brukes på en bestemt IP-adresse eller webadresse og kan brukes til å tillate eller ikke tillate selektivt tilgang til webområder og tjenester. Regler kan legges til ved å merke brukeren som regelen skal brukes for, høyreklikke i vinduet Avanserte regler og velge Legg til regel fra hurtigmenyen for å vise dialogboksen Legg til regel (Figur 6).

Når TermiNET installeres i skjult modus, er det bare avanserte regler som kan konfigureres.

4.3 Opprette regler:

Dialogboksen Legg til regel (Figur 6) brukes til å opprette og definere nye regler.

Oppgi ny regel

Beskrivelse: []

Handling: Tillat

Program: Webtilgang

Modus: Klient

Protokoll: TCP+UDP

OK

Avbryt

Adresse | Port | Tidspunkt

Lokal adresse

Vertsadresse

Ekstern adresse

Webadresse

IP-adresse

Alle adresser

Webadresse

[]

Figur 6

Følgende felt finnes.

- **Beskrivelse:** Gi en beskrivelse av regelen som opprettes
- **Handling:** Angi om regelen skal tillate eller sperre den definerte trafikken.
- **Program:** Velg fra den forhåndsdefinerte programlisten, eller skriv inn et nytt navn på programmet som denne regelen skal gjelde for.
- **Modus:** Angi om den lokale datamaskinen skal opptre som klient eller server for denne regelen. Hvis du angir klient, betyr det at regelen brukes på utgående trafikk. Hvis du angir server, brukes den på innkommende trafikk.

Kategoriene Adresse (Figur 7), Port (Figur 8) og Tidspunkt (Figur 9) brukes til å angi de avanserte funksjonene for regelen.

Adresse:

Oppgi ny regel

Beskrivelse:

Handling: Tilført

Program: Webtligang

Modus: Klient

Protokoll: TCP+UDP

Adresse | Port | Tidspunkt

Lokal adresse

- Vertbadresse

Ekstern adresse

- Webadresse
- IP-adresse
- Alle adresser

Webadresse:

Figur 7

For standardregler vises bare alternativet Alle adresser i denne kategorien.

For avanserte regler angis hvilket webområde regelen skal brukes på, enten ved web- eller IP-adressen.

Hvis alternativet Webadresse velges, kan du oppgi en webadresse i feltet Webadresse.

Hvis du velger alternativet IP-adresse, endres navnet på adressefeltet til IP-adresse.

Port:

Oppgi ny regel

Beskrivelse:

Handling: Tilført

Program: Webtligang

Modus: Klient

Protokoll: TCP+UDP

Adresse | Port | Tidspunkt

Lokal port

- Enkeltport
- Portområde
- Liste over porter
- Alle porter

Ekstern port

- Enkeltport
- Portområde
- Liste over porter
- Alle porter

Liste over porter:

80
443

Legg til Fjern

Figur 8

Kategorien Port (Figur 8) brukes til å angi porten eller portområdet som regelen skal brukes på. Portinnstillingene må konfigureres for både lokale og eksterne datamaskiner. Følgende alternativer finnes.

- **Enkeltport:** Her kan du angi et enkelt portnummer for regelen
- **Portområde:** Her kan du angi et område med porter for regelen.
- **Liste over porter:** Her kan du angi en liste med porter for regelen.
- **Alle porter:** Fører til at regelen brukes på alle porter.

Tidspunkt:

Handling	Program	Modus	Protokoll
Tillat	Webtilgang	Klient	TCP+UDP

Adresse	Port	Tidspunkt
Tidintervall		
<input checked="" type="checkbox"/> Mandag		Pa
<input checked="" type="checkbox"/> Tirsdag		Pa
<input checked="" type="checkbox"/> Onsdag		Pa
<input checked="" type="checkbox"/> Torsdag		Pa
<input checked="" type="checkbox"/> Fredag		Pa
<input checked="" type="checkbox"/> Lørdag		Pa
<input checked="" type="checkbox"/> Søndag		Pa

I Kategorien Tidspunkt kan regelen aktiveres på bestemte dager.

Figur 9

5 Weblister

Weblister kan brukes til å tillate eller sperre tilgang til bestemte webområder. Weblister kan være enten svarte lister eller hvite lister. Svarte og hvite lister er gjensidig avhengig, det vil si at en bruker som er konfigurert til å bruke en svart liste, ikke kan konfigureres til å bruke en hvit liste, og omvendt.

5.1 Svarte lister

Svarte lister brukes til å sperre tilgang til webområder som en regel kan tillate. En standardregel kan for eksempel konfigureres til å tillate all webtilgang samtidig som en bestemt side, for eksempel www.ikketillatt.com, er oppført på den svarte listen. I dette tilfellet kan brukeren søke på alle webområder bortsett fra www.ikketillatt.com.

5.2 Hvite lister

Hvite lister brukes til å tillate tilgang til webområder som en konfigurert regel kan sperre. En standardregel kan for eksempel sperre all webtilgang samtidig som en bestemt side, for eksempel www.tillatt.com, er oppført på den hvite listen. Brukeren kan da ikke søke på andre områder enn www.tillatt.com.

5.3 Globale og lokale lister

Svarte og hvite lister kan være lokale og globale. En global liste opprettes av administratoren og kan brukes på flere brukere. Oppføringer i denne listen brukes på alle brukere som administratoren har angitt skal bruke global webliste. En lokal liste opprettes for bare en bestemt bruker. Oppføringene i denne listen brukes bare på brukeren som listen er opprettet for.

6 Problemer med NetBIOS

Under visse forhold kan du få problemer med tilgang til verter som bruker NetBIOS over TCP/IP når du er i skjult modus. Problemet oppstår når datamaskinen din bruker kringkasting til å bestemme IP-adressen til en vert i nettverket. I skjult modus sperrer TermiNET meldingene som returneres fra vertene og hindrer derfor at kommunikasjon opprettes.

Hvis dette skjer må du lage en oppføring i Hosts-filen som relaterer de aktuelle vertenes IP-adresser til deres NetBIOS-navn. Hosts er en ren tekstfil som du vanligvis finner i mappen C:\Windows i Win'98 eller c:\system32\drivers\etc i Win NT, og kan redigeres med en vanlig tekstbehandler. Eksempelfilen Hosts.sam i mappen gir informasjon om filstrukturen. En typisk vertsfil ser omtrent slik ut:

```
192.168.25.2 minserver.minorg.com  
192.168.56.10 nt_server_1
```

Hvis du vil legge til en vert med navnet nt_server_2 og IP-adressen 192.168.35.23, redigerer du filen slik:

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

Dette problemet oppstår hvis det er konfigurert en WINS-server i nettverket.