

# **TerminET**

Henkilökohtainen palomuuuri

Käyttöopas

---

# Sisällysluettelo

<b>1</b>	<b>JOHDANTO</b>	<b>3</b>
1.1	TIETOJA TERMIŅETISTÄ	3
1.2	AVAINOMINAISUUDET	3
<b>2</b>	<b>ENNEN ALOITUSTA</b>	<b>3</b>
2.1	TERMIŅETIN ASENNUS	3
2.2	SISÄÄN KIRJOITTAUTUMINEN TERMIŅETTIIN	4
2.2.1	<i>Windows 95/98</i>	4
2.2.2	<i>Windows NT/2000</i>	4
2.3	VERKONVALVOJA-TILA	4
2.4	TERMIŅETIN LIITYNTÄ	4
<b>3</b>	<b>KÄYTTÄJÄT JA RYHMÄT. KÄYTTÄJIEN JA RYHMIEN HALLINTA</b>	<b>7</b>
3.1	KÄYTTÄJIEN LISÄÄMINEN	7
3.2	RYHMIEN LUONTI	8
<b>4</b>	<b>LIIKENNESÄÄNNÖT</b>	<b>8</b>
4.1	STANDARDISÄÄNNÖT:	8
4.2	LISÄSÄÄNNÖT:	8
4.3	SÄÄNTÖJEN LUONTI:	9
<b>5</b>	<b>WEB-LUETTELOT</b>	<b>11</b>
5.1	MUSTAT LISTAT	11
5.2	VALKOISET LISTAT	11
5.3	YLEISET JA PAIKALLISET LUETTELOT	11
<b>6</b>	<b>NETBIOS-ONGELMIA</b>	<b>11</b>

# 1 Johdanto

## 1.1 Tietoja TermiNetistä

TermiNet on henkilökohtainen palomuuuri, jonka tehtävänä on suojata tietokone ulkopuolisilta hyökkäyksiltä koneen ollessa yhteydessä internettiin, Webbiä selattaessa tai käytettäessä jotain muuta internet-palvelua. TermiNet voidaan asentaa mihin tahansa seuraavista asennustiloista:

1. "Suljettu tila" estää oletusarvoisesti kaiken paikalliseen tietokoneeseen kohdistuvan ja sieltä lähtevän liikenteen. Verkonvalvoja voi avata käytön valikoivasti - esim. sallitaan vain FTP-käyttö tai sallitaan FTP-, Telnet- ja Web-käyttö. Vanhempien valvoessa lastensa toimintaa, käyttö voidaan rajata valittuihin sivustoihin. Sivustot voidaan antaa suoraan tiettyinä sääntöinä tai ne voidaan lukea URL-osoitteistojen "Valkoiselta listalta".
2. "Avoin tila" ei aseta lähtötilanteessa estoehtoja. Verkonvalvoja voi valikoiden sulkea tietyt käytöt sovellus-, portti ja protokollakohtaisesti - esim. estää kaikki Telnet- ja FTP-käytöt, estää kaiken porttiin 25 tulevan tietoliikenteen, estää määrättyjen sivustojen käytön. Eli estot voidaan antaa määrättyinä sääntöinä tai ne voidaan lukea URL-osoitteistojen "Mustalta listalta" tai hyväksytyiltä sivustoilta.
3. "Salainen tila" sallii kaiken lähtevän liikenteen, mutta estää kaiken tulevan liikenteen paitsi jos ko. liikenne on käynnistetty paikalliselta tietokoneelta. Tässä tilassa tietokonetta voidaan käyttää Webin selaamiseen, FTP-käyttöön yms. tavalliseen tapaan, mutta kone on suojattu hyökkäyksiltä internet-yhteyden aikana.

TermiNet-tuote on ihanteellinen ja edullinen ratkaisu PK-yrityksille ja kotikäyttäjille, jotka käyttävät internettiä mutta joiden resurssit eivät riitä laajemman turvarakenteen ylläpitämiseen.

## 1.2 Avainominaisuudet

TermiNetin avainominaisuuksiin kuuluu

- Standardi- ja lisäsäännöt: Yksinkertainen valintaikkuna **päälle-** ja **pois päältä** -kytkentää varten
- Musta lista/Valkoinen lista -toiminto mahdollistaa käytön eston määrättyihin ei-suotaviin sivustoihin tai sillä voidaan mahdollistaa käyttö vain tunnettuihin hyväksyttäviin sivustoihin.
- Joustavan käytön ohjauksen ansiosta sääntöjä voidaan määrittää IP-osoitteen, URL-osoitteen, portin ja / tai protokollan mukaan
- Aikaan pohjautuvat säännöt voidaan asettaa siten, että ne ovat voimassa vain määrättyinä päivinä.
- Käytössä yksinkertaisen, "Windows Explorer" -tyylisen liitynnän ansiosta TermiNetin konfigurointi on yksinkertaista ja vaistonvaraisuuteen perustuvaa, ja onnistuu vaikka käyttäjä ei olisikaan teknisesti suuntautunut.

# 2 Ennen aloitusta

## 2.1 TermiNetin asennus

Aseta TermiNet-CD tietokoneen CD-asemaan. Asennus yleensä käynnistyy automaattisesti; jos Autorun-toiminto on valittu pois, napsauta "Käynnistys" "Suorita" ja kirjoita "D:\asennus" olettaen että D: on CD-aseman tunnuskirjain. Noudata näytölle tulostuvia asennusohjeita. Asennuksen yhteydessä voit määrittää asennuskohteen ja valita jonkin kolmesta edellä kuvatuista (kuva 1) oletusarvoisista turvavaloista: avoin, suljettu tai salainen.

Kun asennusrutiini on suoritettu, tietokone **täytyy** käynnistää uudelleen jotta asennus olisi täydellinen.

## **2.2 Sisään kirjoittautuminen TermiNettiin**

### **2.2.1 Windows 95/98**

Järjestelmän käynnistyessä TermiNet käynnistyy oletusarvoisilla säännöillä, jotka ovat verkonvalvojan asettamia. Jos on luotu useita TermiNet-käyttäjäprofiileja, on määritellyllä käyttäjällä kaksi tapaa suorittaa sisään kirjoittautuminen; joko kaksoisnapsauttamalla tehtävöpalkissa olevaa TermiNet-kuvaketta tai napsauttamalla TermiNet-kuvaketta hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla "Kirjaudu sisään".

Kummassakin tapauksessa ruudulle tulostuu sisään kirjoittautumis -näyttö, jossa kysytään käyttäjätunnusta ja salasanaa. Kun käyttäjätunnus ja salasana on annettu, määrätyn käyttäjän turvaprofiili tulee käyttöön.

### **2.2.2 Windows NT/2000**

Windows NT:n sisään kirjoittautumis -profiiliin perustuvassa TermiNETissä käyttäjän sisään kirjoittautuminen tapahtuu automaattisesti.

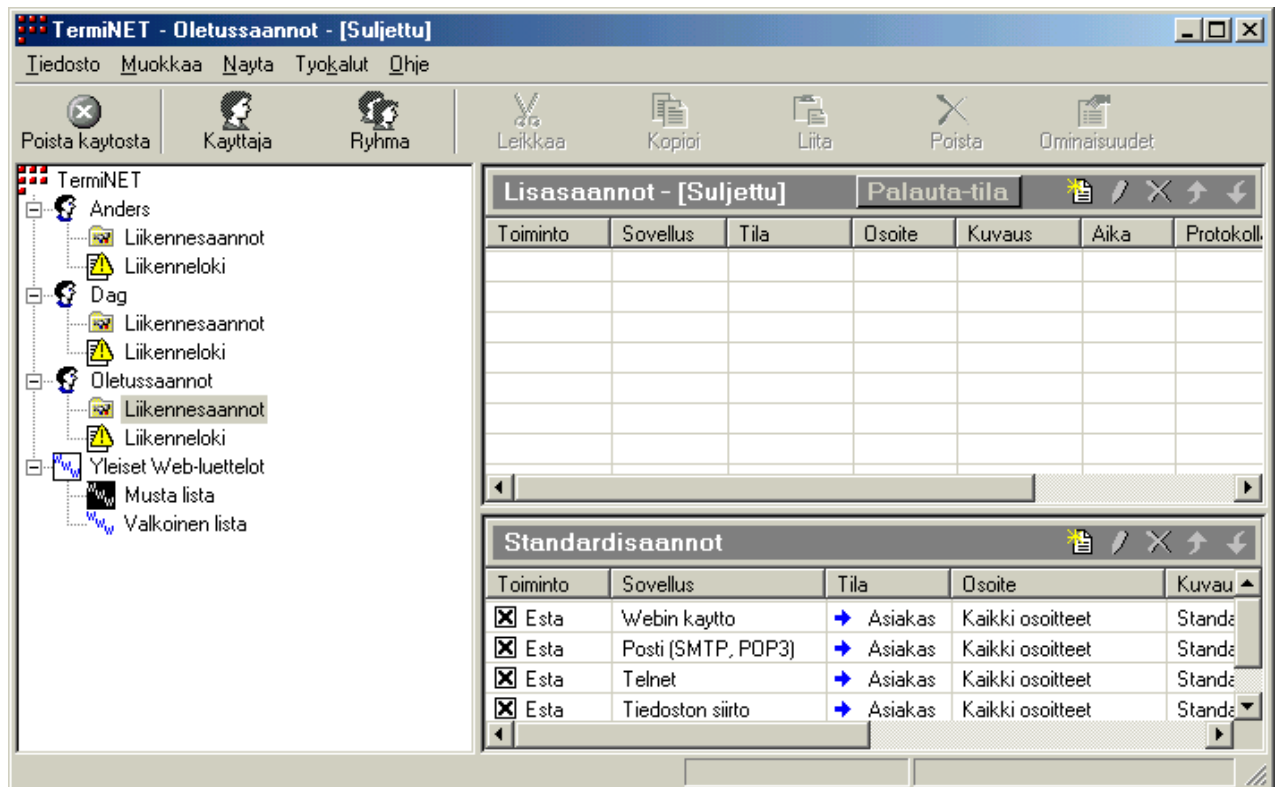
## **2.3 Verkonvalvoja-tila**

Verkonvalvoja-tila sallii seuraavat toimenpiteet: oletuskäyttäjän turvaprofiilin määrittäminen, uusien käyttäjäprofiilien luonti, ja lisäsääntöjen asettaminen määrätuille käyttäjille. Verkonvalvoja-tilaan siirrytään napsauttamalla tehtävöpalkin TermiNet-kuvaketta hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla vaihtoehdon "Verkonvalvoja-tila". Tällöin järjestelmä antaa kehoitteen, jossa pyydetään verkonvalvojan salasanaa. Salasana antamisen jälkeen ruudulle ilmestyy TermiNetin konfigurointinäyttö, jonka välityksellä hallintatoimet suoritetaan.

Poistuaksesi verkonvalvoja-tilasta, sulje konfigurointinäyttö valikkovaihtoehdosta "Tiedosto -> Poistu verkonvalvonnasta".

## **2.4 TermiNetin liityntä**

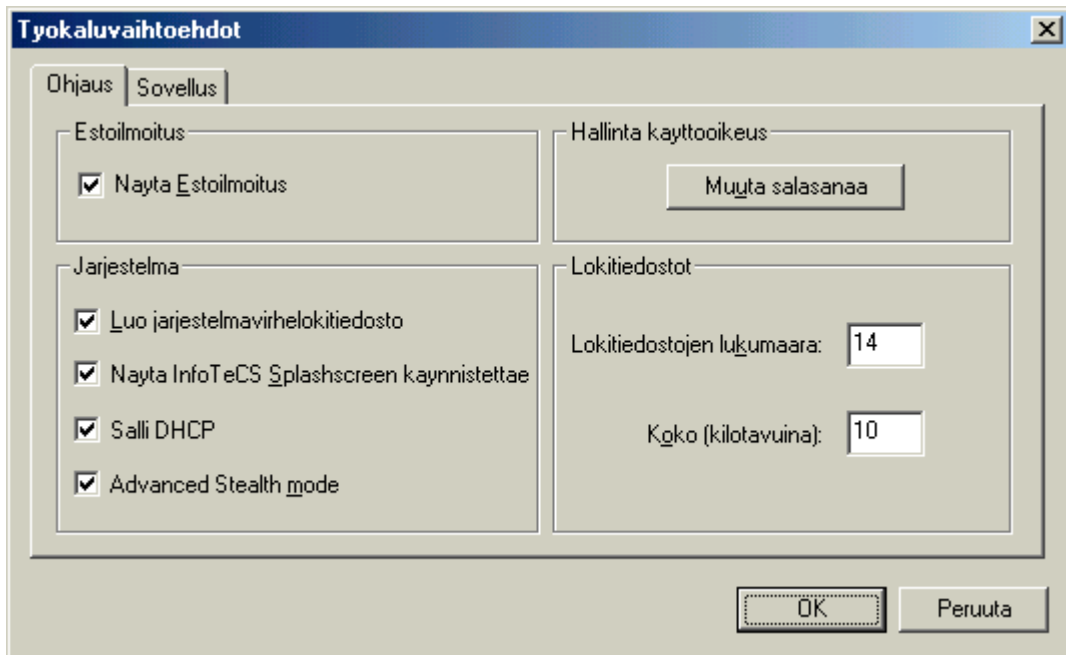
TermiNetin liityntä (Kuva 1) käyttö edellyttää verkonvalvojan salasanaa. Liityntä on käytettävyydeltään yksinkertainen graafinen työväline, jolla määritetään tietokoneen turvaprofiilit.



Kuva 1

Liityntä jakautuu kolmeen osaan; vasemmanpuoleinen osa esittää turvajärjestelmän puurakenteena. Oikeanpuoleinen osa esittää järjestelmän esimääritetyt "standardisäännöt". Ylhäällä oikealla olevassa osassa esitetään mahdolliset lisäsäännöt jos sellaisia on luotu. Kun vasemmanpuoleisessa ikkunassa valitaan käyttäjä, oikeanpuoleisista ikkunoista näkyy kyseistä käyttäjää koskevien lisä- ja standardisääntöjen tilanne.

Valikko-palkki sisältää Tiedosto-, Muokkaa- ja Näytä-valikot, joita käyttämällä liityntä on mukautettavissa verkonvalvojan tarpeisiin. "Työkalut" -> "Vaihtoehdot" -valikko sallii järjestelmänlaajuisten ominaisuuksien asettamisen.

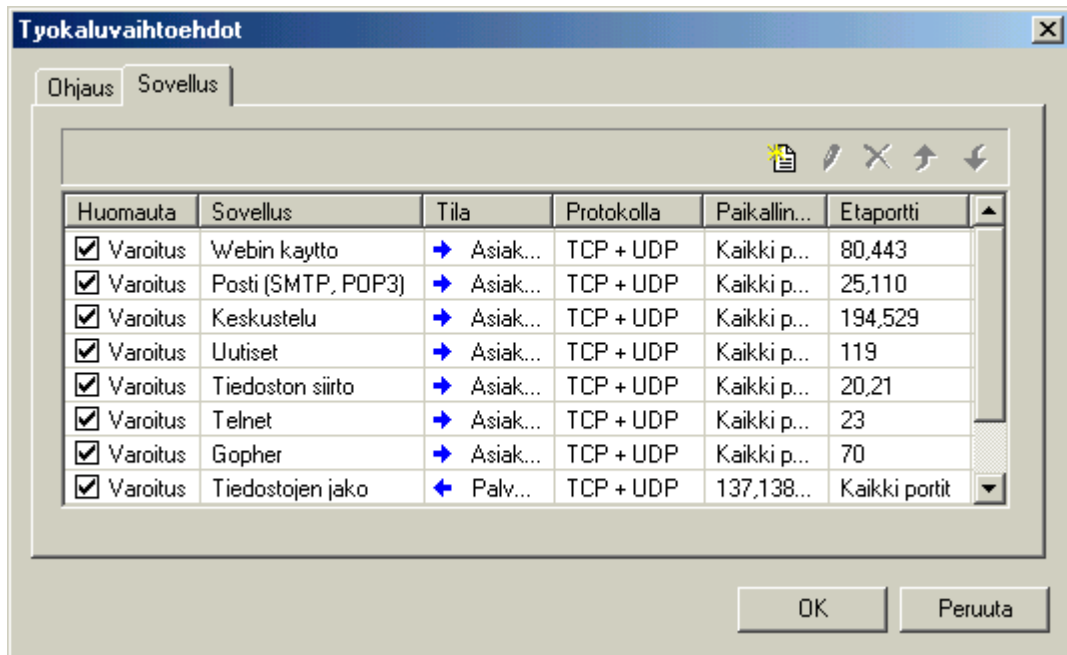


Kuva 2


Välilehti (Kuva 2) mahdollistaa pääsyn seuraaviin vaihtoehtoihin.

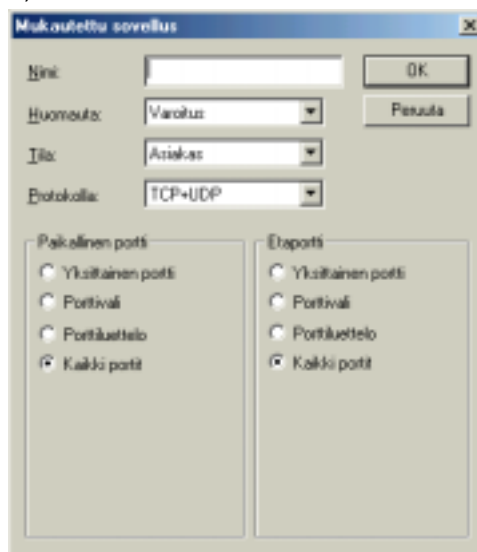
<b>Näytä estoilmoitus:</b>	Kun se on valittu, Liikennelokista käyvät ilmi sekä estetty että sallittu liikenne. Jos sitä ei ole valittu, vain sallittu liikenne kirjataan.
<b>Luo järjestelmävirhelokitiedosto:</b>	Kun valinta on voimassa, järjestelmävirheet kirjautuvat \Ohjelmatiedostot\Infotecs\Terminet\Data\errorlog.txt -tiedostoon.
<b>Näytä INFOTECS Splashscreen käynnistettäessä:</b>	Poista valinta estääksesi INFOTECS Splashscreen –näytön TerminiNetin käynnistyksen yhteydessä.
<b>Muuta salasanaa</b>	Sallii verkonvalvojan salasanan muuttamisen.
<b>Lokitiedostojen lukumäärä</b>	Asettaa kirjattavien liikennelokitiedostojen lukumäärän. Kun määrätty lokitiedostolukumäärä on saavutettu ja viimeinen tiedosto on saavuttanut enimmäiskokonsa järjestelmä kirjoittaa ensimmäinen tiedoston päälle
<b>Koko (kilotavuina):</b>	Asettaa liikennelokitiedoston koon kilotavuina johon kokoon tiedosto voi kasvaa. Kun kyseinen koko saavutetaan, tiedosto tallentuu ja toisen tiedoston kirjaaminen alkaa.

Sovellus-välilehti (Kuva 3) sallii uusien standardisovellusten luonnin.



Kuva 3

Napsautta Lisää sovellus -painiketta  jolloin ruudulle ilmestyy Mukautettu sovellus -valintaikkuna (Kuva 4).



Kuva 4

Tämän ikkunan välityksellä voidaan asettaa seuraavat vaihtoehdot.

- **Nimi:** Tässä mukautetulle sovellukselle annetaan nimi.
- **Protokolla:** Alasvetovalikosta sovellukselle valitaan haluttu protokolla.
- **Huomautus:** Alasvetovalikosta valitaan 'Varoitus' tai 'Ohita'. Mikäli valinta on 'Varoitus' järjestelmä tuottaa ilmoituksen kun kyseinen liikennetyyppi tulee estetyksi.
- **Suunta:** Alasvetovalikosta valitaan 'Tuleva' tai 'Lähtevä'.
- **Etäportti:** Määritetään sovellukselle etätietokoneen porttiasetus.
- **Paikallinen portti:** Määritetään sovellukselle paikallisen tietokoneen porttiasetus.

### 3 Käyttäjät ja ryhmät. Käyttäjien ja ryhmien hallinta

#### 3.1 Käyttäjien lisääminen

Käyttäjäprofiilin lisääminen tapahtuu napsauttamalla TermiNet-puurakenteen korkeinta tasoa hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla vaihtoehto "Lisää käyttäjä" pikakuvakevalikosta tai

napsauttamalla työkalurivin Käyttäjä-painiketta. Tämän tuloksena ruudulle ilmestyy Käyttäjän ominaisuudet -ikkuna (Kuva 5)

Kuva 5

Käytettävissä on seuraava joukko kenttiä.

- **Käyttäjän nimi:** Tässä käyttäjälle annetaan haluttu käyttäjän nimi.
- **Salasana:** Annetaan vaadittu käyttäjän salasana.
- **Vahvista salasana:** Annetaan salasana uudelleen sen vahvistamiseksi.
- **Suojaustila:** Valitaan käyttäjälle oletusarvoinen turvatila.
- **URL-luettelot:** Tässä määritetään käyttääkö käyttäjä URL-osoitteistojen 'Mustia' vai 'Valkoisia' listoja ja edelleen käyttääkö käyttäjä 'Yleistä' vai 'Paikallista' luetteloa.

### 3.2 Ryhmien luonti

Ryhmiä voidaan käyttää järjestettäessä käyttäjäluetteloita Terminetin puurakennenyöön puitteissa. Uusi ryhmä luodaan napsauttamalla puurakenteen korkeinta tasoa hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla vaihtoehdon "Lisää ryhmä" ruudulle ilmestyvästä pikakuvakevalikosta ja kirjoittamalla ryhmälle haluttu nimi. Tämän jälkeen käyttäjät voidaan sijoittaa ryhmiin napsauttamalla käyttäjän nimeä hiirellä sen oikeanpuoleista painiketta käyttäen ja vetämällä nimi haluttuun ryhmään. Käyttäjän luonti olemassa olevaan ryhmään tapahtuu napsauttamalla puurakenteessa olevaa ryhmää hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla vaihtoehdon "Lisää käyttäjä" pikakuvakevalikosta.

## 4 Liikennesäännöt

Terminetissä voidaan määrittää kahdenlaisia liikennesääntöjä.

### 4.1 Standardisäännöt:

Koskevat kaikkia IP-osoitteita ja niitä voidaan käyttää määrättyjen palveluiden yleiseen käytön sallimiseen tai kieltämiseen. Järjestelmään on esimääritelty neljä standardisääntöä: Web-käyttö, Posti, FTP ja Telnet. Lisäsääntöjä voidaan lisätä valitsemalla käyttäjä puurakenteesta, napsauttamalla 'Standardisääntö' -ruutua hiirellä sen oikeanpuoleista painiketta käyttäen ja valitsemalla vaihtoehdo "Lisää sääntö" pikakuvakevalikosta jolloin ruudulle ilmestyy Lisää sääntö -valintaikkuna (Kuva 6)

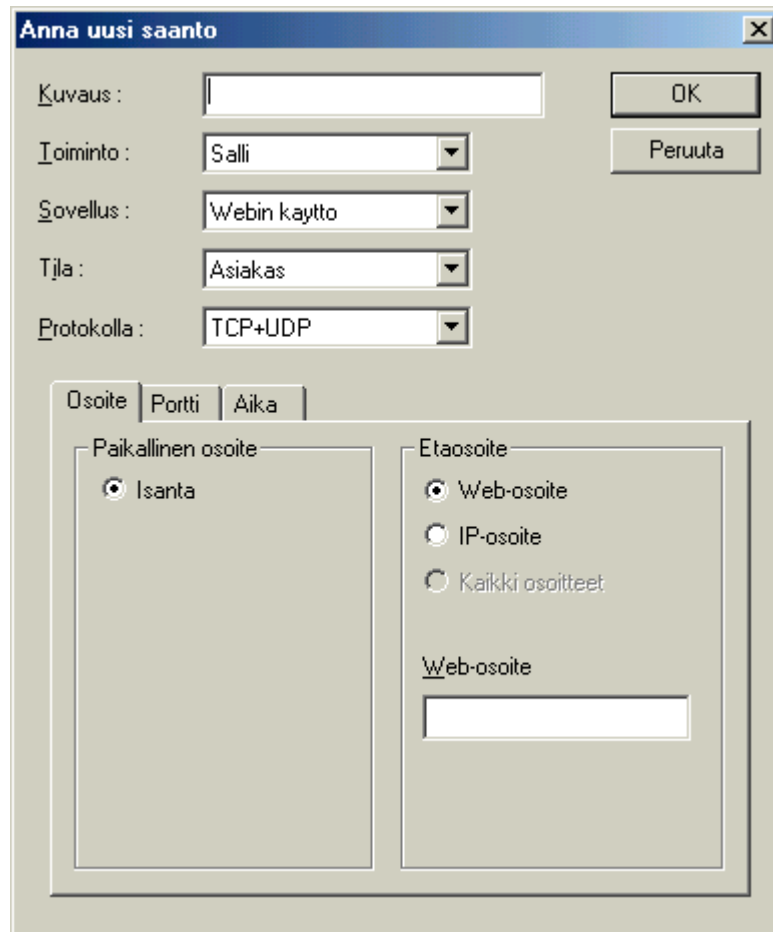
### 4.2 Lisäsäännöt:

Koskevat määrättyjä IP- tai URL-osoitteita ja käytetään kun halutaan valikoiden sallia tai estää sivustojen ja palvelujen käyttö. Sääntöjä lisätään valitsemalla käyttäjä, johon sääntöä tullaan soveltamaan, jonka jälkeen napsautetaan Lisäsäännöt-ikkunaa hiirellä sen oikeanpuoleista painiketta käyttäen ja valitaan "Lisää sääntö" pikakuvakevalikosta, jolloin ruudulle ilmestyy Lisää sääntö -valintaikkuna (Kuva 6).

Kun Terminet asennetaan toimimaan Salaisessa tilassa, voidaan konfiguroida vain lisäsääntöjä.

### 4.3 Sääntöjen luonti:

Lisää sääntö -valintaikkunaa (Kuva 6) käytetään uusien sääntöjen luomiseen ja määrittämiseen.



Kuva 6

Käytettävissä on seuraava joukko kenttiä.

- **Kuvaus:** Laaditaan kuvaus luotavasta säännöstä
- **Toiminto:** Päätetään salliiiko vai estääkö sääntö määritellyn liikenteen.
- **Sovellus:** Valitaan sovellus joko esimääritellystä sovellusluettelosta tai kirjoitetaan sovellukselle, johon sääntö kohdistuu, uusi nimi.
- **Tila:** Määritetään toimiiko paikallinen tietokone asiakkaana vai palvelimena tämän säännön osalta. Asiakkaaksi määrittäminen merkitsee että sääntöä sovelletaan lähtevään liikenteeseen; palvelimeksi määrittäminen merkitsee että sääntöä sovelletaan tulevaan liikenteeseen.

Välilehtiä Osoite (Kuva 7), Portti (Kuva 8) ja Aika (Kuva 9) käytetään määrittettäessä säännön lisätoimintoja.

## Osoite:



Kuva 7

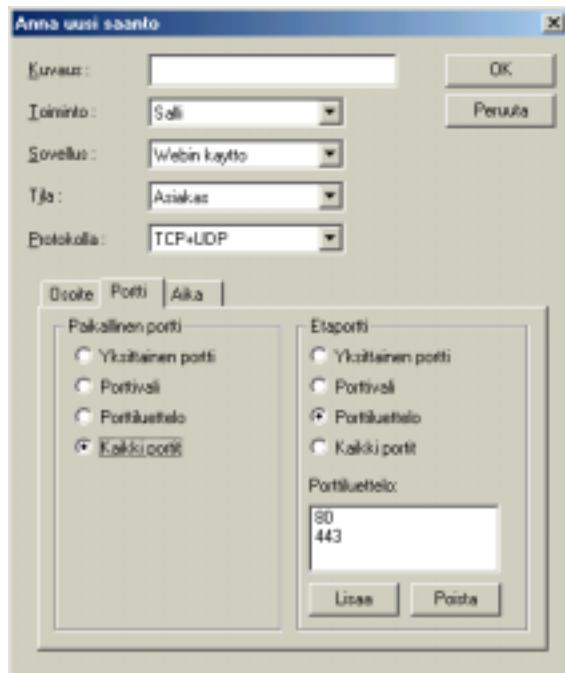
Standardisäännön kohdalla tämän välilehden ainoa käytettävissä oleva vaihtoehto on "Kaikki osoitteet"

Lisäsäännöille voidaan määrittää sivusto, johon sääntö kohdistuu, joko URL- tai IP-osoitteena.

Jos valintamerkki asetetaan URL-osoitepainikkeeseen, voidaan Osoite-kenttään antaa URL-osoite.

Jos valintamerkki asetetaan IP-osoitepainikkeeseen, muuttuu Osoite-kenttä IP-osoitteen vastaanottavaksi kentäksi.

## Portti:



Kuva 8

Portti-välilehteä (Kuva 8) käytetään määrittäessä portti tai porttiväli, johon sääntö kohdistuu. Porttiasetukset on konfiguroitava sekä paikalliselle että etätietokoneelle.

Käytettävissä on seuraava joukko kenttiä.

- **Yksittäinen portti:** Sallii yksittäisen porttinumeron määrittämisen säännölle
- **Porttiväli:** Sallii tietyllä välillä olevan porttijoukon määrittämisen säännölle.
- **Porttiluettelo:** Sallii porttiluettelon määrittämisen säännölle.
- **Kaikki portit:** Tekee säännöstä kaikkiin portteihin vaikuttavan säännön.

## Aika:

Kuvaus:	<input type="text"/>	OK
Toiminto:	Salli	Peruuta
Sovellus:	Webin käyttö	
Tyyppi:	Aziakas	
Protokolla:	TCP+UDP	
Osoite   Portti   <b>Aika</b>		
Aikajako		
<input checked="" type="checkbox"/> Maanantai		Käytössä
<input checked="" type="checkbox"/> Tiistai		Käytössä
<input checked="" type="checkbox"/> Keskiviikko		Käytössä
<input checked="" type="checkbox"/> Torstai		Käytössä
<input checked="" type="checkbox"/> Perjantai		Käytössä
<input checked="" type="checkbox"/> Lauanantai		Käytössä
<input checked="" type="checkbox"/> Sunnuntai		Käytössä

Aika-välilehden kautta voidaan säännön voimassaolo rajoittaa määrättyihin päiviin.

Kuva 9

## 5 Web-luettelot

Web-luetteloita voidaan käyttää sallimaan tai estämään määrättyjen sivustojen käyttö. URL-luettelot voivat olla Mustia listoja tai Valkoisia listoja. Mustat ja Valkoiset listat ovat toisensa pois sulkevia, ts. Mustan listan käyttäjäksi määritetty käyttäjä ei voi olla samanaikaisesti määritetty Valkoisen listan käyttäjäksi ja päinvastoin.

### 5.1 Mustat listat

Mustilla listoilla estetään sellaisten sivustojen käyttö joiden käytön sääntö saattaa sallia. Esimerkki: standardisääntö voidaan laatia sallimaan Webin käytön, mutta määrätty sivusto, esim. [www.eisallittu.com](http://www.eisallittu.com), asetetaan Mustalle listalle. Näin ollen käyttäjä voi selata kaikkia muita Web-sivustoja paitsi kohdetta [www.eisallittu.com](http://www.eisallittu.com).

### 5.2 Valkoiset listat

Valkoisilla listoilla sallitaan sellaisten sivustojen käyttö joiden käytön jokin sääntö saattaa estää. Esimerkki: standardisääntö voi olla estämässä kaiken Web-käytön mutta tietty sivusto (esim. [www.disney.com](http://www.disney.com)) on Valkoisella listalla ja niinpä käyttäjä voi selata ainoastaan sivustoa [www.disney.com](http://www.disney.com).

### 5.3 Yleiset ja paikalliset luettelot

Mustia ja Valkoisia listoja on kahdenlaisia: paikallisia ja yleisiä. Verkonvalvoja luo yleisen luettelon ja sitä voidaan soveltaa kaikkiin käyttäjiin; yleisen luettelon sisältö kohdistuu kaikkiin niihin käyttäjiin, jotka verkonvalvoja on määrittänyt yleisen URL-luettelon käyttäjiksi. Paikallinen luettelo luodaan vain määrättylle käyttäjälle; luettelon sisältöä sovelletaan vai siihen käyttäjään, jolle luettelo on luotu.

## 6 NetBios-ongelmia

Tietyissä tilanteissa voi ilmetä ongelmia toimittaessa "Salainen" -tilassa ja otettaessa yhteyttä isäntiin, jotka käyttävät NetBIOSia TCP/IP:ssä. Ongelma tulee esille kun käyttäjän tietokone käyttää lähetyksiä määrittääkseen verkossa olevan isännän IP-osoitteen. Toimiessaan "Salainen" -tilassa, TermiNET estää isänniltä palautetut sanomat ja siten myös tietoliikenneyhteyden muodostumisen.

Tällöin on käyttäjän tietokoneelle tallennettuun "HOSTS" -tiedostoon tehtävä tallennus, jossa yhdistetään tarvittavien isäntien IP-osoitteet niiden NetBIOS-nimiin. "HOSTS" on tekstitiedosto, joka yleensä löytyy hakemistosta C:\windows käyttäjärjestelmän ollessa Win'98 tai hakemistosta C:\system32\drivers\jne. kun käyttäjärjestelmä on Win NT, ja sitä voi muokata millä tahansa tekstieditorilla. Hakemistossa oleva esimerkkitiedosto nimeltä 'hosts.sam' sisältää tarkempaa tietoa tiedoston rakenteesta. Tyypillinen isäntätiedosto on seuraavankaltainen.

```
192.168.25.2 minunpalvelin.minunorg.com
192.168.56.10 nt_server_1
```

Jos esimerkiksi halutaan lisätä isännän, jonka nimi on 'nt\_server\_2' ja jonka IP-osoite on 192.168.35.23, muokataan tiedostoa näin.

```
192.168.25.2 minunpalvelin.minunorg.com
192.168.55.10 nt_server_1
192.168.35.23 nt_server_2
```

Tätä ongelmaa ei ole jos käytettyyn verkkoon on konfiguroitu WINS-palvelin