

TerminET

Personal Firewall

Benutzerhandbuch

Inhalt

1	EINFÜHRUNG	3
1.1	INFO ÜBER TERMiNET	3
1.2	HAUPTMERKMALE	3
2	ERSTE SCHRITTE	3
2.1	TERMiNET INSTALLIEREN	3
2.2	ANMELDUNG IN TERMiNET	4
2.2.1	<i>Windows 95/98</i>	4
2.2.2	<i>Windows NT/2000</i>	4
2.3	ADMINISTRATORMODUS	4
2.4	DIE TERMiNET-BENUTZER OBERFLÄCHE	5
3	BENUTZER UND GRUPPEN. BENUTZER UND GRUPPEN VERWALTEN	8
3.1	BENUTZER HINZUFÜGEN	8
3.2	GRUPPEN ERSTELLEN	8
4	DATENVERKEHR-RICHTLINIEN	8
4.1	STANDARDRICHTLINIEN	8
4.2	ERWEITERTE RICHTLINIEN	9
4.3	RICHTLINIEN ERSTELLEN	9
5	WEBLISTEN	11
5.1	SCHWARZE LISTEN	11
5.2	WEIßE LISTEN	11
5.3	Globale und lokale Listen	11
6	PROBLEME MIT NETBIOS	12

1 Einführung

1.1 Info über TermiNET

TermiNET ist eine "Personal Firewall" für PCs zum Schutz vor unberechtigtem Zugriff von außen, während Ihr PC mit dem Internet verbunden ist oder das Web durchsucht oder andere Internet-Dienste in Anspruch genommen werden. TermiNET kann anfänglich in einem der folgenden Modi installiert werden:

1. Im "Geschlossenem Modus" wird der gesamte Datenverkehr zu und von dem lokalen System standardmäßig gesperrt. Der Administrator kann anschließend selektiv den Zugriff gewähren. Beispiele: nur FTP zulassen oder FTP-, Telnet- und Webzugriff zulassen. Für "Parental Control" (Sperren jugendgefährdender Inhalte) kann der Zugriff auf nur einige bestimmte Webseiten beschränkt werden. Diese Webseiten können direkt über Richtlinien eingegeben bzw. definiert oder über eine »weiße Liste« verfügbarer Webseiten (URLs) angezeigt werden.
2. Im "Offenen Modus" werden keine anfänglichen Blockierungsbedingungen auferlegt. Der Administrator kann anschließend selektiv den Zugriff sperren, und zwar je nach Anwendung, Anschluss und Protokoll. Beispiele: Blockierung des gesamten Telnet- und FTP-Datenverkehrs, Blockierung aller eingehenden Kommunikationsversuche am Anschluss 25 oder Blockierung des Zugriffs auf bestimmte Webseiten. Diese können ebenfalls als gesonderte Richtlinien definiert oder über eine »schwarze Liste« gesperrter Webseiten (URLs) angezeigt werden.
3. Im "Stealth-Modus" wird ausgehender Datenverkehr zugelassen, alle eingehenden Versuche zur Herstellung der Verbindung mit Ihrem PC werden jedoch abgelehnt, es sei denn, die Herstellung der Verbindung wird von Ihrem lokalen PC aus initialisiert. In diesem Modus kann Ihr System für Websuchen, FTP usw. verwendet werden, so wie normalerweise auch, und ist darüber hinaus bei aktiven Internetverbindungen vor unberechtigtem Zugriff geschützt.

TermiNET ist eine ideale Sicherheitslösung für KMUs (klein- und mittelständische Unternehmen) und für Benutzer von Heim-PCs, denen die notwendigen Ressourcen zur Unterstützung einer umfangreichen Sicherheitsinfrastruktur nicht zur Verfügung stehen.

1.2 Hauptmerkmale

Zu den Hauptmerkmalen von TermiNET gehören:

- Standardrichtlinien und erweiterte Richtlinien: einfache Aktivierung und Deaktivierung von Funktionen über Kontrollkästchen.
- Schwarze Listen/Weiße Listen liefern die Möglichkeit, den Zugriff auf nicht gewünschte Webseiten zu sperren oder ausgewählte bekannte Webseiten zuzulassen.
- Flexible Zugriffskontrolle über Richtlinien im Hinblick auf zugelassene/gesperrte IP-Adressen, URLs, Anschlüsse und/oder Protokolle.
- Konfiguration zeitspezifischer Richtlinien, die nur an bestimmten Tagen aktiviert werden sollen.
- Benutzerfreundliche Oberfläche, ähnlich wie der Windows Explorer, zur einfachen und intuitiven Konfiguration von TermiNET (selbst für nicht-technisch begabte Benutzer).

2 Erste Schritte

2.1 TermiNet installieren

Legen Sie die TermiNET-CD in das CD-ROM-Laufwerk des PCs ein. Setup wird automatisch gestartet und ausgeführt, sofern die Option "Autorun" in Windows aktiviert ist. Wenn "Autorun" deaktiviert ist, müssen Sie auf "Start" -> "Ausführen" klicken und "D:\setup" eingeben, wobei D: der Laufwerksbuchstabe des CD-ROM-Laufwerks ist. Folgen Sie den angezeigten Bildschirmanweisungen, um das Produkt zu installieren. Im Laufe der Installation werden Sie aufgefordert, das Installationsverzeichnis anzugeben und einen der drei verfügbaren Sicherheitsmodi (Offen, Geschlossen oder Stealth) als Standardmodus auszuwählen.

Nachdem das Installationsverfahren abgeschlossen ist, **muss** der PC neu gestartet werden, damit die Installation vollständig beendet werden kann.

2.2 Anmeldung in TermiNet

2.2.1 Windows 95/98

Beim Systemstart startet TermiNET mit den vom Administrator standardmäßig festgelegten Richtlinien. Wenn mehrere TermiNET-Benutzerprofile erstellt wurden, gibt es zwei verschiedene Möglichkeiten sich als einer der definierten Benutzer anzumelden. Sie können entweder zweimal hintereinander auf das TermiNET-Symbol in der Task-Leiste klicken (Doppelklick) oder aber mit der rechten Maustaste auf das TermiNET-Symbol klicken und dann »Anmelden" aus dem Einblendmenü wählen. In beiden Fällen erscheint ein Anmeldebildschirm, auf dem eine Benutzer-ID und ein Kennwort eingegeben werden müssen. Durch Eingabe der Benutzer-ID und des Kennworts wird das Sicherheitsprofil für den angegebenen Benutzer aktiviert.

2.2.2 Windows NT/2000

Je nach NT-Anmeldeprofil werden Benutzer automatisch in TermiNET angemeldet.

2.3 Administratormodus

Der Administratormodus erlaubt die Spezifikation des standardmäßig verwendeten Benutzersicherheitsprofils, das Anlegen neuer Benutzerprofile und das Erstellen erweiterter Richtlinien für bestimmte Benutzer. Sie schalten in den Administratormodus um, indem Sie mit der rechten Maustaste auf das TermiNET-Symbol in der Task-Leiste klicken und »Administratormodus» aus dem Einblendmenü wählen. Daraufhin werden Sie zur Eingabe des Administratorkennworts aufgefordert. Nach Eingabe des Kennworts erscheint die Anzeige zur Konfiguration von TermiNET, auf der administrative Funktionen ausgeführt werden können.

Um den Administratormodus zu beenden, schließen Sie einfach die Konfigurationsanzeige, indem Sie die Menüoption »Datei ->Administrator schließen» wählen.

2.4 Die TermiNET-Benutzeroberfläche

Die TermiNET-Benutzeroberfläche (Abbildung 1) kann nur über das Administratorkennwort angezeigt werden. Sie ist ein einfach zu verwendetes Werkzeug zur Definition der Sicherheitsprofile für ein System.

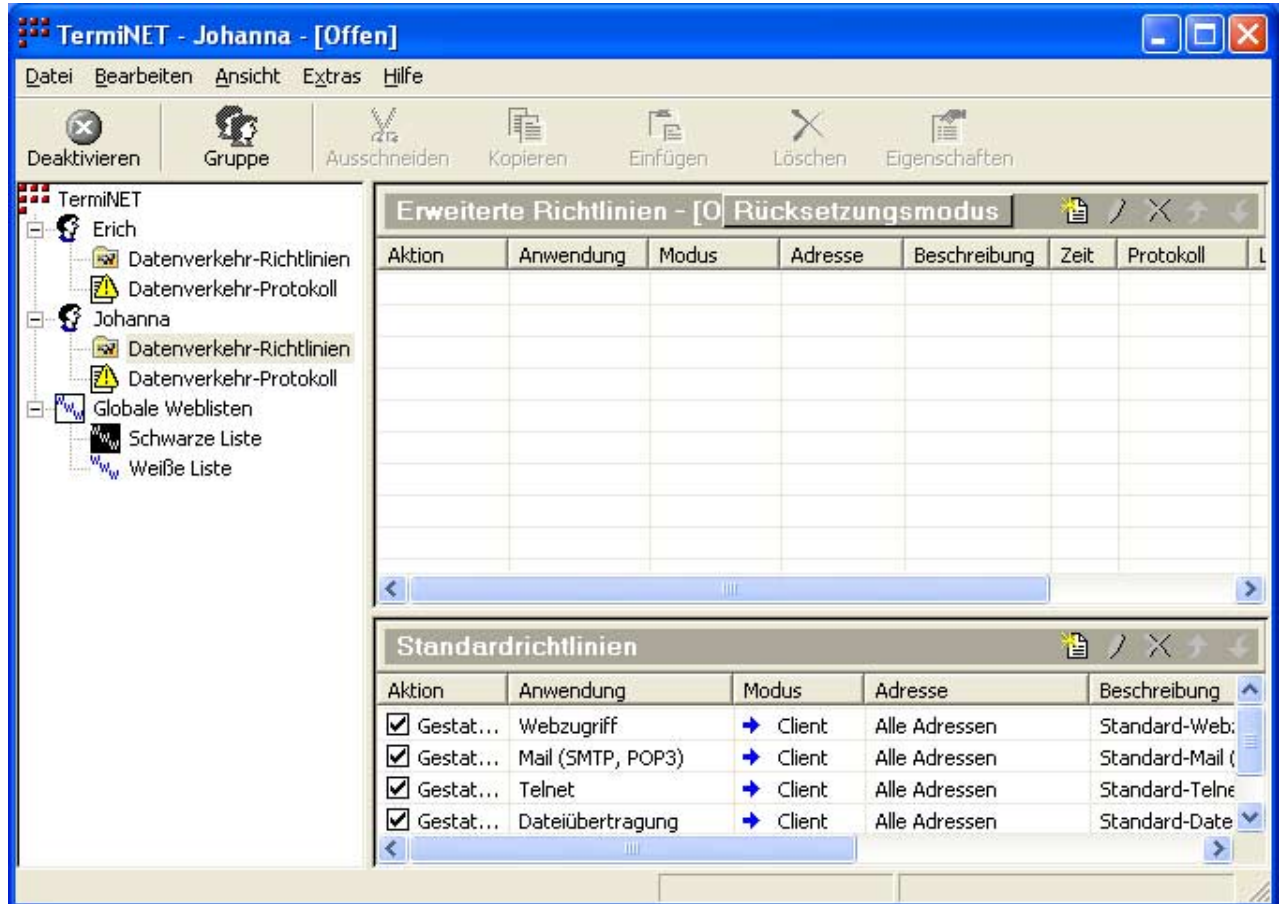


Abbildung 1

Die Benutzeroberfläche ist in drei Abschnitte unterteilt. Auf der linken Seite wird eine Baumstruktur-Ansicht des definierten Sicherheitssystems gezeigt. Unten rechts befinden sich die vom System vordefinierten »Standardrichtlinien«. Oben rechts erscheinen alle erweiterten Richtlinien, die eventuell für Ihr System erstellt wurden. Wenn auf der linken Bildschirmseite ein Benutzer ausgewählt wird, erscheinen auf der rechten Seite Statusinformationen über die erweiterten Richtlinien und die Standardrichtlinien für diesen Benutzer.

Die Benutzeroberfläche kann mit den Menüoptionen "Datei", "Bearbeiten" und "Ansicht" vom Administrator je nach Wunsch angepasst werden. Das Menü »Extras» ->»Optionen» erlaubt das Festlegen von systemweiten Eigenschaften.



Abbildung 2

Die Registerkarte "Kontrolle" (Abbildung 2) gibt Ihnen Zugriff auf folgende Optionen.

Blockierungsbenachrichtigung anzeigen:

Wenn dieses Kontrollkästchen markiert ist, werden im Datenverkehr-Protokoll gesperrter/blockierter und zugelassener/gestatteter Datenverkehr angezeigt. Wenn es nicht markiert ist, wird nur zugelassener/gestatteter Datenverkehr aufgezeichnet.

Systemfehler-Protokolldatei erstellen:

Wenn dieses Kontrollkästchen markiert ist, werden alle Systemfehler in die Datei \Programme\Infotecs\Terminet\Data\errorlog.txt geschrieben.

INFOTECS-Begrüßungsanzeige beim Start anzeigen:

Wenn dieses Kontrollkästchen nicht markiert ist, wird die INFOTECS-Begrüßungsanzeige beim Start von TerMiNET nicht angezeigt.

Kennwort ändern

Ermöglicht die Änderung des Kennworts, mit dem der Administratormodus aktiviert wird.

Anzahl der Protokolldateien

Legt die Anzahl der Datenverkehr-Protokolldateien fest, die aufgezeichnet werden sollen. Sobald diese Anzahl erreicht ist und die letzte Protokolldatei ihre maximale Größe erreicht hat, wird die erste aufgezeichnete Datei mit neuen Daten überschrieben.

Größe (in KB):

Legt die maximale Größe in Kilobytes für Datenverkehr-Protokolldateien fest. Sobald diese Größe erreicht ist, wird die Datei gespeichert und eine andere aufgezeichnet.

Die Registerkarte "Anwendung" (Abbildung 3) erlaubt das Erstellen von neuen Standardanwendungen.



Abbildung 3

Klicken Sie auf das Symbol "Anwendung hinzufügen" , um das Dialogfeld "Benutzeranwendung" anzuzeigen (Abbildung 4).



Abbildung 4

In diesem Dialogfeld können folgende Optionen eingestellt werden:

- **Name:** Geben Sie den Namen für die Benutzeranwendung ein.
- **Protokoll:** Wählen Sie das gewünschte Protokoll für die Anwendung aus der Dropdown-Liste.
- **Benachrichtigung:** Wählen Sie "Warnen" oder "Ignorieren" aus der Dropdown-Liste. Wenn "Warnen" gewählt wird, erscheint eine Benachrichtigung, wenn Datenverkehr dieses Typs blockiert/gesperrt wird.
- **Richtung:** Wählen Sie "Eingehend" oder "Ausgehend" aus der Dropdown-Liste.
- **Ferner Anschluss:** Geben Sie die Anschlusseinstellung an, die auf das entfernte System für diese Anwendung zutrifft.
- **Lokaler Anschluss:** Geben Sie die Anschlusseinstellungen an, die auf das lokale System für diese Anwendung zutrifft.

3 Benutzer und Gruppen. Benutzer und Gruppen verwalten

3.1 Benutzer hinzufügen

Um ein Benutzerprofil hinzuzufügen, klicken Sie mit der rechten Maustaste auf die oberste Ebene der TerMiNET-Baumstruktur und wählen »Benutzer hinzufügen« aus dem Einblendmenü. Sie können aber auch die Schaltfläche "Benutzer" aus der Symbolleiste wählen. Daraufhin erscheint das Dialogfeld "TerMiNET-Benutzereigenschaften" (Abbildung 5)

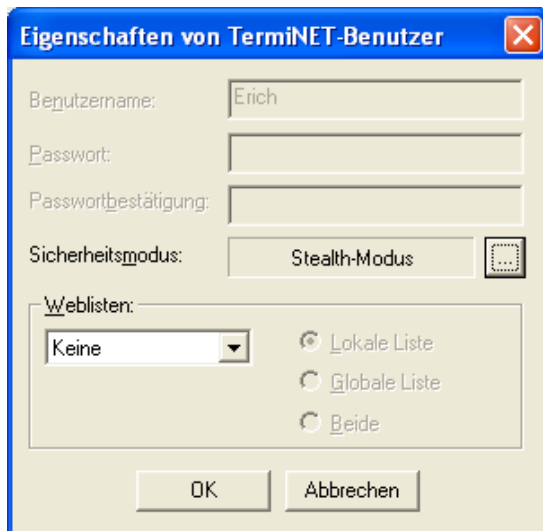


Abbildung 5

Dieses Dialogfeld enthält die folgenden Felder.

- **Benutzername:** Geben Sie den gewünschten Namen für den Benutzer ein.
- **Kennwort:** Geben Sie das gewünschte Kennwort für den Benutzer ein.
- **Kennwortbestätigung:** Geben Sie zur Bestätigung das gleiche Kennwort erneut ein.
- **Sicherheitsmodus:** Wählen Sie für diesen Benutzer den Sicherheitsmodus, der standardmäßig angewendet werden soll.
- **Weblisten:** Geben Sie an, ob der Benutzer die schwarze oder weiße Liste benutzen soll und ob die globale oder die lokale Liste oder beide Listen benutzt werden sollen.

3.2 Gruppen erstellen

Gruppen können benutzt werden, um eine Liste von Benutzern in der TerMiNET-Baumstruktur zu organisieren. Sie erstellen eine neue Gruppe, indem Sie mit der rechten Maustaste auf die oberste Ebene in der Baumstruktur klicken und »Gruppe hinzufügen« aus dem Einblendmenü wählen. Geben Sie anschließend den gewünschten Namen für die Gruppe ein. Benutzer können der Gruppe hinzugefügt werden, indem Sie die Methode Ziehen-und-Ablegen anwenden. Klicken Sie hierzu auf einen Benutzernamen, halten Sie die Maustaste gedrückt und ziehen Sie ihn auf die gewünschte Gruppe. Ein Benutzer kann auch in einer vorhandenen Gruppe erstellt werden, indem Sie mit der rechten Maustaste auf die Gruppe in der Baumstruktur klicken und »Benutzer hinzufügen« aus dem Einblendmenü wählen.

4 Datenverkehr-Richtlinien

Es gibt zwei verschiedene Typen von Datenverkehr-Richtlinien, die in TerMiNet definiert werden können:

4.1 Standardrichtlinien

Standardrichtlinien gelten für alle IP-Adressen und können benutzt werden, um den Zugriff auf bestimmte Dienste global zu gestatten oder abzulehnen. Vier Standardrichtlinien werden vom System vordefiniert: Webzugriff, Mail, FTP und Telnet. Zusätzliche Richtlinien können wie folgt hinzugefügt werden: Markieren Sie einen Benutzer in der Baumstruktur, klicken Sie mit der rechten Maustaste auf den Fensterausschnitt mit den Standardrichtlinien und wählen Sie »Richtlinie hinzufügen« aus dem Einblendmenü. Daraufhin erscheint das Dialogfeld zum Erstellen neuer Richtlinien (Abbildung 6).

4.2 Erweiterte Richtlinien

Erweiterte Richtlinien gelten für bestimmte IP-Adressen oder URLs und können benutzt werden, um den Zugriff auf Webseiten und Dienste selektiv zu gestatten oder abzulehnen. Richtlinien können wie folgt hinzugefügt werden: Markieren Sie einen Benutzer in der Baumstruktur, auf den die Richtlinie zutreffen soll, klicken Sie mit der rechten Maustaste auf den Fensterausschnitt mit den erweiterten Richtlinien und wählen Sie "Richtlinie hinzufügen» aus dem Einblendmenü. Daraufhin erscheint das Dialogfeld zum Hinzufügen neuer Richtlinien.

Wenn TermiNET im "Stealth-Modus" installiert wird, können nur erweiterte Richtlinien konfiguriert werden.

4.3 Richtlinien erstellen

Das Dialogfeld zum Erstellen/Hinzufügen von Richtlinien (Abbildung 6) wird zum Definieren von neuen Richtlinien verwendet.

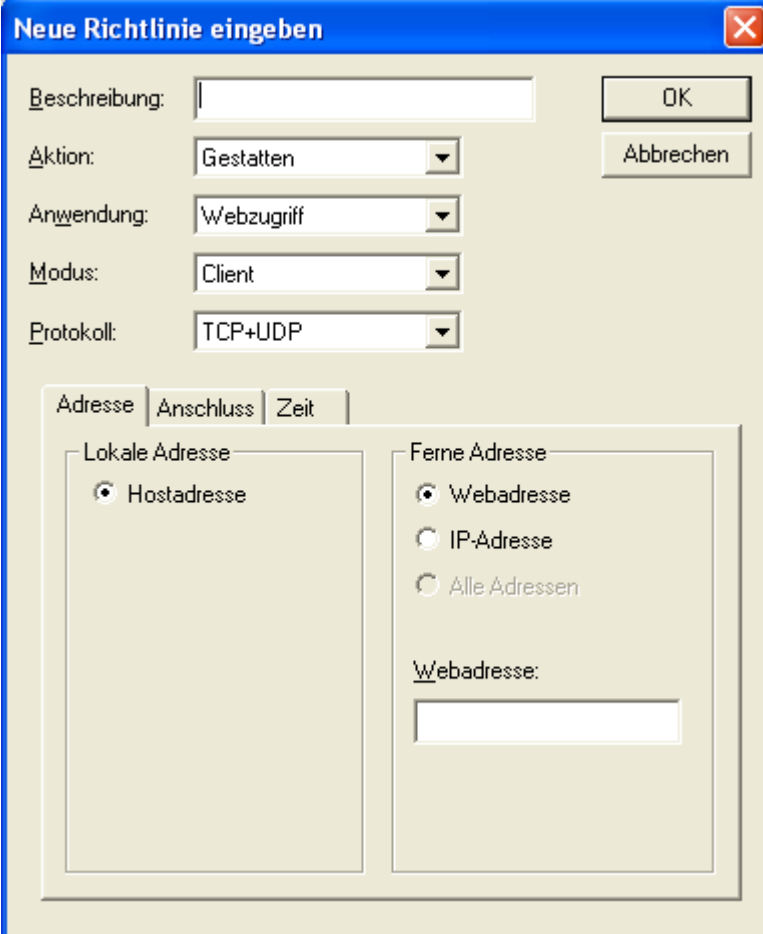


Abbildung 6

Dieses Dialogfeld enthält die folgenden Felder:

- **Beschreibung:** Geben Sie eine Beschreibung für die zu erstellende Richtlinie ein.
- **Aktion:** Geben Sie an, ob die Richtlinie den definierten Datenverkehr gestatten oder blockieren soll.
- **Anwendung:** Wählen Sie entweder eine Anwendung aus der vordefinierten Liste aus oder geben Sie einen neuen Namen für die Anwendung ein, auf die diese Richtlinie zutreffen soll.
- **Modus:** Geben Sie an, ob das lokale System ein Client oder Server für diese Richtlinie sein soll. Wenn Sie "Client" wählen, gilt die Richtlinie für den gesamten ausgehenden Datenverkehr, wenn Sie "Server" wählen, gilt sie für den gesamten eingehenden Datenverkehr.

Auf den Registerkarten "Adresse" (Abbildung 7), "Anschluss" (Abbildung 8) und "Zeit" (Abbildung 9) werden die erweiterten Funktionen der Richtlinie spezifiziert.

Adresse (Registerkarte)

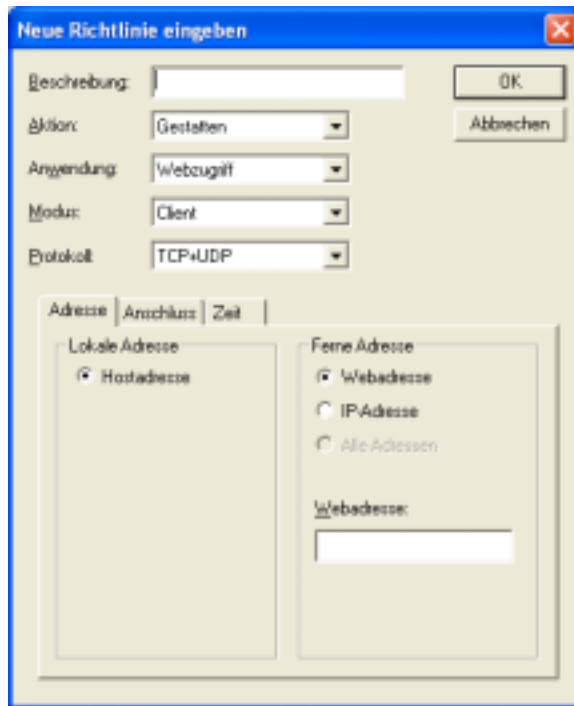


Abbildung 7

Für Standardrichtlinien gibt es auf dieser Registerkarte nur die Option »Alle Adressen«.

Für erweiterte Richtlinien kann die Webseite, auf die diese Richtlinie zutrifft, angegeben werden (entweder der URL oder die IP-Adresse).

Wenn das runde Optionsfeld "Webadresse" markiert ist, wird ein Adressfeld eingeblendet, in das die Adresse (URL) eingegeben werden kann.

Wenn Sie das Optionsfeld "IP-Adresse" wählen, ändert sich das Adressfeld in ein Adressfeld zur Eingabe der IP-Adresse.

Anschluss (Registerkarte)

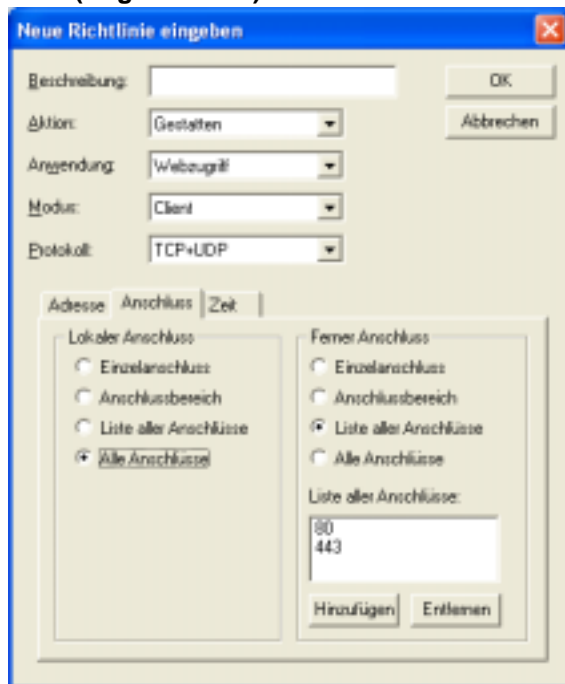
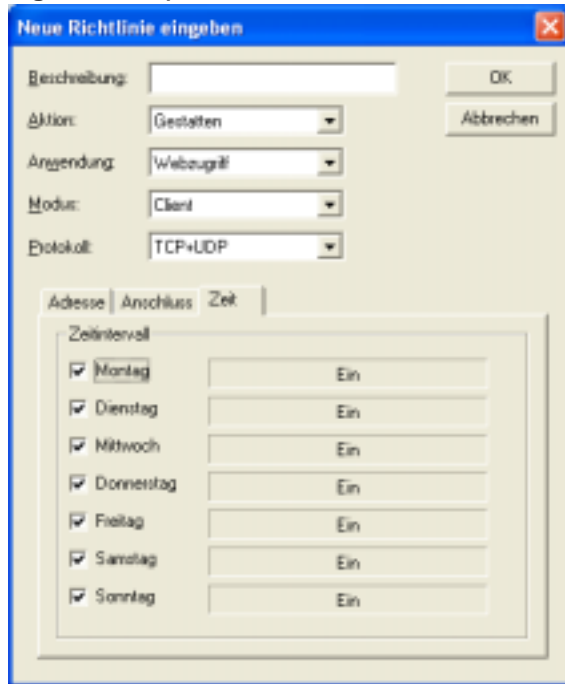


Abbildung 8

Die Registerkarte "Anschluss" (Abbildung 8) wird zur Angabe des Anschlusses oder des Anschlussbereichs benutzt, auf den die Richtlinie zutrifft. Anschlusseinstellungen müssen sowohl für das lokale als auch das ferne System konfiguriert werden. Dieses Dialogfeld enthält die folgenden Optionen:

- **Einzelanschluss:** Erlaubt die Angabe einer einzigen Anschlussnummer für die Richtlinie.
- **Anschlussbereich:** Erlaubt die Angabe eines Bereichs von Anschlüssen für die Richtlinie.
- **Liste aller Anschlüsse:** Erlaubt die Angabe einer Liste von Anschlüssen für die Richtlinie.
- **Alle Anschlüsse:** Stellt das System so ein, dass die Richtlinie auf alle Anschlüsse zutrifft.

Zeit (Registerkarte)



Die Einstellungen auf der Registerkarte "Zeit" bestimmen den Zeitpunkt, an dem die Richtlinie angewendet wird.

Abbildung 9

5 Weblisten

Weblisten werden benutzt, um den Zugriff auf bestimmte Webseiten zu gestatten oder zu blockieren/sperrern. Weblisten (auch URL-Listen genannt) können schwarze Listen oder weiße Listen sein. Beide Listen können jedoch nicht gleichzeitig ausgewählt werden, d.h. dass ein Benutzer, der für die Benutzung einer schwarzen Liste konfiguriert ist, keine weiße Liste benutzen darf (und umgekehrt).

5.1 Schwarze Listen

Schwarze Listen werden benutzt, um den Zugriff auf Webseiten zu blockieren/sperrern, die eventuell von einer Richtlinie erlaubt werden. Beispiel: Angenommen eine Standardrichtlinie erlaubt den Zugriff auf alle Webseiten und eine bestimmte Seite, z.B. www.notallowed.com, ist auf der schwarzen Liste aufgeführt. Der Benutzer kann in diesem Fall alle Webseiten anzeigen, abgesehen von www.notallowed.com.

5.2 Weiße Listen

Weiße Listen werden benutzt, um den Zugriff auf Webseiten zu erlauben, die eventuell durch eine konfigurierte Richtlinie blockiert/gesperrt werden. Beispiel: Eine Standardrichtlinie blockiert den Zugriff auf das gesamte Web und eine bestimmte Webseite, z.B. www.disney.com, ist auf der weißen Liste aufgeführt. Der Benutzer kann in diesem Fall keine Webseiten anzeigen, abgesehen von www.disney.com.

5.3 Globale und lokale Listen

Es gibt zwei Typen von schwarzen und weißen Listen: Lokale und Globale. Eine globale Liste wird vom Administrator erstellt. Die Einträge in der globalen Liste treffen auf alle Benutzer zu, für die der Administrator die Benutzung einer globalen Webliste definiert hat. Eine lokale Liste dagegen wird für einen bestimmten Benutzer erstellt und die Einträge in dieser Liste treffen nur auf den Benutzer zu, für den diese Liste erstellt wurde.

6 Probleme mit NetBIOS

Wenn "Stealth-Modus" aktiviert ist, könnten bei der Verwendung von NetBIOS über TCP/IP u.U. Probleme beim Zugriff auf Hostcomputer auftreten. Das Problem tritt auf, wenn Ihr System Broadcasts zur Bestimmung der IP-Adresse eines Hostcomputers im Netzwerk benutzt. Im Stealth-Modus blockiert TermiNET die von den Hostcomputern zurückgesendeten Meldungen und verhindert dadurch die Herstellung von Kommunikationsverbindungen.

Sie müssen in solchen Fällen einen Eintrag in Ihrer Datei "HOSTS" tätigen und den NetBIOS-Namen der gewünschten Hostcomputer die jeweilige IP-Adresse hinzufügen. Bei der Datei "HOSTS" handelt es sich um eine einfache Textdatei, die unter Windows 98 gewöhnlich im Verzeichnis C:\windows und unter Win NT gewöhnlich im Verzeichnis c: \system32\drivers\etc zu finden ist. Sie kann mit irgendeinem Texteditor bearbeitet werden. Details hinsichtlich der Dateistruktur finden Sie im selben Verzeichnis in der Beispieldatei hosts.sam. Eine typische Hostdatei enthält folgende Daten:

```
192.168.25.2 myserver.myorg.com
192.168.56.10 nt_server_1
```

Wenn Sie beispielsweise einen Hostcomputer namens nt_server_2 mit der IP-Adresse 192.168.35.23 hinzufügen möchten, müssen Sie die Datei wie folgt bearbeiten:

```
192.168.25.2 myserver.myorg.com
192.168.55.10 nt_server_1
192.168.35.23 nt_server_2
```

Beachten Sie, dass dieses Problem nicht auftritt, wenn in Ihrem Netzwerk ein WINS-Server konfiguriert ist.