Zum Hauptmenü

Weitere Netzwerke konfigurieren

Wenn Sie weitere Netzwerke haben, so können sie diese an eigene Netzwerkverbindungen anschließen. In der Vorkonfiguration sind die weiteren Netzwerke deaktiviert. Um sie zu aktivieren gehen Sie auf den jeweiligen Menüpunkt und drücken Sie ENTER. Sie können nun auswählen, ob das Netzwerk aktiviert werden soll. Wenn Sie ja auswählen und die Eingabe bestätigen öffnet sich das Konfigurationsmenü für das jeweilige weitere Netzwerk.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das jeweilige Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Zusatz-Netzwerke

Die Konfiguration des weiteren Netzwerkes erfolgt analog zur Konfiguration des ersten Netzwerks. Vgl. Sie bitte den Abschnitt Internes Netzwerk.

Zusätzlich zu den Einstellungen können Sie noch angeben, ob das Netzwerk den Squid oder Mail-Zugang sowie unbegrenztes Masquerading über die Firewall nutzen soll.

Fallback-Netzwerk

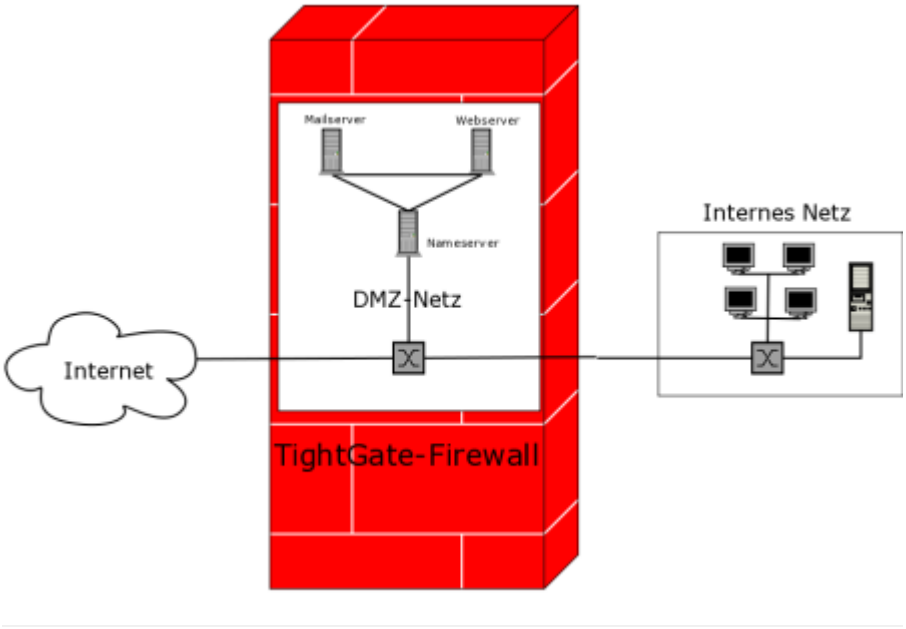
Die Konfiguration für das Fallback-Netzwerke erfolgt analog zur Konfiguration des externen Netzwerks.

Zusätzlich können Sie einstellen, welches Netzwerk immer das Fallback-Netzwerk nutzen soll.

Grundsätzlich wird vom gesamten System aber nur eine DSL-Verbindung unterstützt. Folglich muss für eine zweite DSL-Verbindung ein separater Router eingesetzt werden.

Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ, deutsch: entmilitarisierte Zone) bezeichnet einen geschützten Rechnerverbund, der sich zwischen zwei Computernetzwerken befindet. Die gesamte Kommunikation vom und zum Rechnerverbund wird dabei durch die Firewall geschützt.



Der Sinn der DMZ ist es, möglichst auf sicherer Basis Dienste des Rechnerverbundes sowohl dem einem als auch dem anderem Netz zur Verfügung zu stellen. Ein typisches Anwendungsbeispiel ist das Betreiben eines eigenen TightGate-Pro Servers.

Diese Server sind Teile der DMZ und müssen von außen erreichbar sein, da ansonsten Anfragen nicht bearbeitet werden können. Anderseits sollen die Clients, die im internen Netz angeschlossen sind, auch auf die Server zugreifen können. Die Server selber können jedoch von sich aus keine Verbindungen ins interne Netz aufbauen.

Vorteil einer solchen Lösung ist, dass im Falle einer Kompromittierung eines Servers in der DMZ das interne Netzwerk trotzdem noch geschützt bleibt. Wären die Server nicht in einer DMZ, sondern direkt im internen Netzwerk, so wäre auch das gesamte Netzwerk durch eine Kompromittierung betroffen. Gerade weil öffentlich angebotene Dienste oft ein nicht unerhebliches Angriffsziel darstellen, kann man durch eine DMZ das Gesamtrisiko erheblich minimieren.

Um das DMZ Netzwerk zu konfigurieren, melden Sie sich bitte als Benutzer *config* an und wählen Sie aus dem Menü den Menüpunkt *Einstellungen>DMZ Netzwerk* aus. Aktivieren Sie den Schalter DMZ-Netzwerk. Sie haben folgende Einstellungsmöglichkeiten:

Ende	Verlassen des Menüs.
DMZ Netzwerk aktiviert	An- oder Abschalten des DMZ-Netzwerks.
Interfaces	Anzeige aller im System verfügbaren Netzwerkinterfaces.
—	
Netzwerk-Treiber (DMZ)	Auswahl des Netzwerkkarten-Treibers für das DMZ Netzwerkinterface.
MAC-Adresse (DMZ)	Auswahl der zugehörigen MAC-Adresse für das Netzwerkinterface.
IP-Adresse (DMZ)	Die IP-Adresse der für das DMZ Netz. Über diese IP-Adresse kommuniziert die Firewall mit den Servern in der DMZ.
IP-Netzwerk-Valid-Bits (DMZ)	Anzahl der gültigen IP-Netzwerk-Bits des DMZ Netzes.
IP-Netzwerk-Maske (DMZ)	Entsprechend dem IP-Adressbereich die IP-Netzwerkmaske für das DMZ Netz.
IP-Netzwerk (DMZ)	IP-Adressbereich für das DMZ Netzwerk.
IP-Broadcast (DMZ)	DMZ Broadcast-Adresse für das IP-Netzwerk dieser Firewall.

IP-Netzwerk rückwärts (DMZ)	IP-Netzwerk der DMZ rückwärts ohne die Hosts.
IP-Netzwerk Hostanteil (DMZ)	Hostanteil der IP-Adresse des DMZ-Netzes.
—	
Aus der DMZ maskierte TCP-Ports	Legen Sie hier fest, welche TCP-Ports maskiert in das Internet durchgeleitet werden sollen.
Ping ICMP aus der DMZ durchleiten	Legt fest, ob eine PING-Anfrage aus der DMZ weitergeleitet wird.
Von der DMZ offene Firewall-TCP-Ports	Auswahl diejenigen TCP-Ports, über die Server aus dem DMZ-Netz auf Dienste der mp-Firewall zugreifen sollen. Z.B. Freischaltung des TCP-Ports 53, wenn ein Server aus der DMZ die mp-Firewall als DNS-Server benutzen soll.
Von der DMZ offene Firewall-UPD-Ports	Auswahl diejenigen UDP-Ports, über die Server aus dem DMZ-Netz auf Dienste der mp-Firewall zugreifen sollen.
DMZ-Server 1-4	IP-Adresse des jeweiligen in der DMZ stehenden Server.
Externe TCP-Ports zum DMZ-Server 1-4	Einstellung derjenigen Ports, über die aus dem externen Netzwerk Verbindungen direkt an den jeweiligen in der DMZ stehenden Server weiterzuleiten sind. Es werden nur TCP-Verbindungen über einen Proxy in die DMZ weitergeleitet. Sollen andere Protokolle in die DMZ durchgeleitet werden, so ist die über den Menüpunkt Custom-Settings vorzunehmen. Achtung: Wenn eigene Durchleitungen eingestellt werden, werden diese u.U nicht protokolliert!

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Virtuelle Adressen

Die mp-Firewall kann zusätzliche Adressen aus dem externen Netzwerk verwenden und alle zugehörigen Verbindungen an ein anderes System in der DMZ weiterleiten. Dabei werden die verwendeten Adressen automatisch angepasst, dieser Vorgang nennt sich Network Address Translation (NAT).

Um neue virtuelle Adressen zu erstellen oder bestehende zu konfigurieren melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>Virtuelle Adressen* aus. Wählen Sie den Menüpunkt *Neu* aus, um eine neue Virtuelle Adresse zu erstellen. Sie werden nun durch ein Menü geführt, welches Ihnen bei der Erstellung der Virtuellen Adresse behilflich ist. Hierbei können Sie auch festlegen, welche Protokolle und Ports vom Paketfilter der Firewall zum Zielsystem durchgelassen werden sollen.

Für virtuelle Adressen, die direkt auf dem System liegen und nicht zu einem anderen System weiter geleitet werden sollen, können auch lokale Ports definiert werden. Hierfür ist es nicht mehr nötig eine eigene *Custom Input Rule* zu definieren.

Um bestehende virtuelle Adressen zu ändern wählen Sie die jeweilige Adresse aus. Es öffnet sich das Bearbeitungsmenü, wo Sie alle Einstellungen ändern können.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben verlassen die das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt

Sanft Anwenden an. Erst nach dem Anwenden werden die neuen Einstellungen wirksam.

Zum Hauptmenü