1 : 1 NAT Funktion von ZeroShell

Anforderungen

Die Version und Ausgabe von ZeroShell, auf die sich dieses Dokument bezieht, lautet 1.0 beta11. Diese Dokumentation befasst sich nicht mit der Installation von ZeroShell, vielmehr wird für diese Erläuterung und Erklärung folgendes vorausgesetzt:

1 .Ein fertig installiertes und konfiguriertes System (ZeroShell)
2. Ein getestetes und abgesichertes System (ZeroShell)
3 .Ein fehlerfrei arbeitendes System (ZeroShell)

Überblick

Diese Dokumentation beschreibt die Konfiguration von ZeroShell als Router, unter Verwendung der NAT Funktion, in zwei möglichen Varianten, die wie folgt beschrieben und umgesetzt werden.

1. Eine eins zu eins Verbindung (1:1 NAT Funktion) um auf Server im lokalem Netzwerk (LAN) zugreifen zu können, beziehungsweise diese anzubinden.

2. Mehrere zu eins Verbindung (Many : 1 NAT Funktion) um auf alle anderen Netzwerkklienten (i. d. Regel Computer mit Netzwerkanschluss) im lokalen Netzwerk (LAN) zu zugreifen, beziehungsweise um diese anzubinden.

Die lokalen Netzwerkserver sind an der Netzwerkschnittstelle (Netzwerkkarte) mit dem Namen ETH02 angeschlossen. Die anderen lokalen Netzwerkteilnehmer (LAN Klienten, Computer oder Netzwerkgeräte) sind an der Netzwerkschnittstelle mit dem Namen ETH00 angeschlossen. Und an der Netzwerkschnittstelle mit dem Namen ETH01 befindet sich die Internetverbindung (WAN Schnittstelle), meistens per Modem, ISDN, ADSL oder einer Standleitung angebunden. (Siehe Abbildung 1)

Beachten Sie bitte, dass natürlich kein Zwang besteht, die Server an einer separaten Netzwerkschnittstelle (Netzwerkkarte) an das Netzwerk anzubinden.
Diese können natürlich auch zusammen mit den anderen Netzwerkklienten an der Netzwerkschnittstelle (Netzwerkkarte) mit dem Namen ETH00 angebunden werden.

ETH00 = ETH steht für Ethernet (Netzwerkkarte oder Netzwerkschnittstelle) und die Zahl dahinter nummeriert die Anzahl der Netzwerkschnittstellen durch, angefangen wird dabei immer Betriebssystem abhängig mit der Zahl 0 (null) oder doppelnull (00) was die erste Netzwerkschnittstelle (Netzwerkkarte) benennt bzw. markiert.

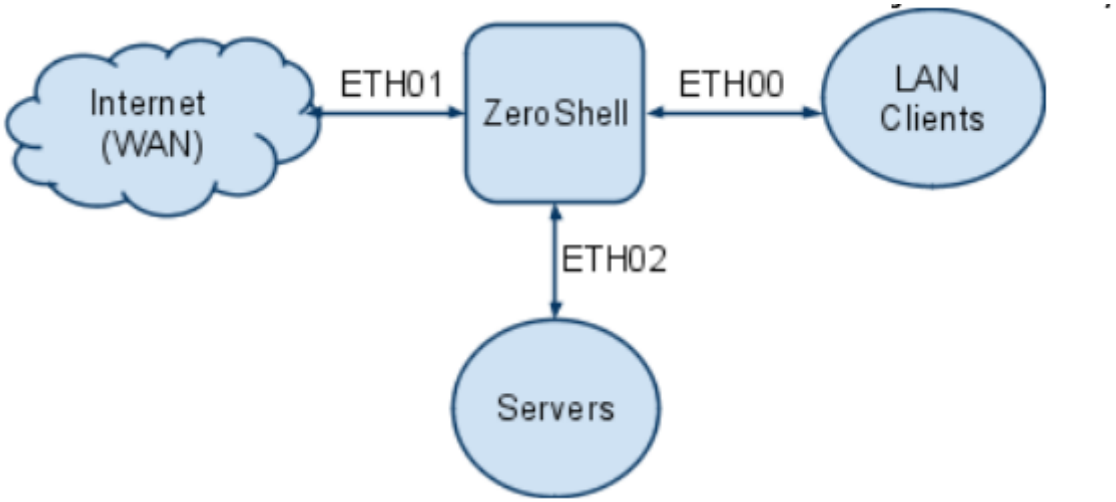


Abbildung 1

Das hier erläuterte Beispiel setzt allerdings die Verfügbarkeit von mehreren öffentlichen IP Adressen für die Internetverbindung (WAN Schnittstelle) voraus.
In dieser Dokumentation werden vier öffentliche IP Adressen benutzt, daher ist diese Dokumentation ganz klar an Administratoren von Firmennetzwerken gerichtet oder aber an Privatanwender (Home User) die sich bei DynDNS.org einige statische IP Adressen besorgt haben.

Eine dieser öffentliche IP Adresse wird von ZeroShell für die Anbindung der Netzwerkklienten an der Netzwerkschnittstelle (Netzwerkkarte) ETH00 (PC´s, Computer, Netzwerkgeräte) unter Benutzung der mehrere zu eins NAT Funktion benutzt (Viele : 1 NAT). Den Rest der öffentlichen IP Adressen benutzt ZeroShell dazu um die Server an der lokalen Netzwerkschnittstelle ETH02, unter Verwendung der eins zu eins NAT Funktion (1 : 1 NAT) anzubinden.

Die Server sind mit nicht öffentlichen, also privaten IP Netzwerkadressen des Klasse C Netzwerkes konfiguriert. In diesem Beispiel stammen die öffentlichen IP Adressen aus dem Netzwerk 216.0.0.129 mit der Subnetzmaske 255.255.255.240. Der Standardgateway für die Anbindung an das Internet ist unter der öffentlichen IP Adresse **216.0.0.129** zu erreichen.

Die Netzwerkklienten (PC´s, Computer, Netzwerkgeräte), die über die Netzwerkschnittstelle ETH00 angebunden sind,
benutzen private IP Adressen aus dem Klasse C Netzwerkbereich, beginnend mit der ersten IP Adresse 192.168.0.1 und aufwärts ansteigend.

Die Server hingegen benutzen private IP Adressen aus dem Klasse C Netzwerkbereich, beginnend mit der ersten IP Adresse 192.168.1.1 aufwärts ansteigend.

Netzwerkeinrichtung

ETH00
Rufen Sie bitte die Webschnittstelle von ZeroShell über einen Browser auf und melden sich am System an. Im Menü auf der linken Seite wählen Sie bitte den Punkt "Setup" unter "System" aus. Anschließend wählen Sie bitte den Punkt "Network" am oberen Rand aus. Die Netzwerkschnittstelle (Netzwerkkarte) ETH00 wird für die lokalen Netzwerkklienten (PC´, Computer, usw.) benutzt, jedoch müssen Sie Ihr erst eine IP Adresse zuweisen. Markieren Sie dazu den kleinen Punkt vor dem Namen ETH00 und wählen anschließen auf der rechten Seite im dazugehörigen Menü den Punkt "Add IP" durch anwählen (anklicken) mit der Maus aus. Nun öffnet sich ein kleines Fenster, bitte tragen Sie hier nun die IP Adresse 192.168.0.1 unter dem Feld "IP" und unter "Netmask" die Nummer 255.255.255.0 für das Subnetzwerk ein wie in Abbildung 2 beschrieben.

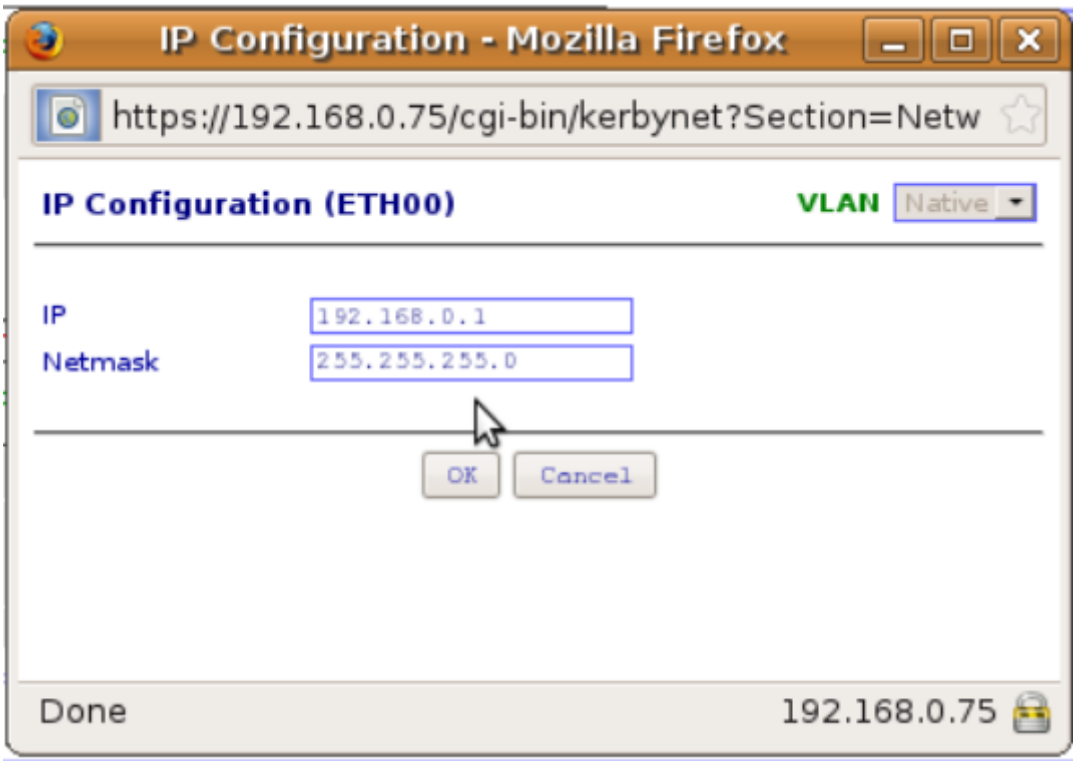


Abbildung 2

ETH01
Die Netzwerkschnittstelle (Netzwerkkarte) ETH01 wird für die Internetverbindung (WAN Schnittstelle)benutzt und wie folgt konfiguriert. Den Punkt vor dem Namen ETH01 durch anklicken markieren und auf der rechten Seite den Punkt "Add IP" durch anklicken auswählen.Als primäre öffentliche IP Adresse benutzt ZeroShell die IP Adresse 216.0.0.130 mit der Netzwerkmaske 255.255.255.240. Bitte tragen Siediese Adressen ein und bestätigen Sie Ihre Eingabe durch anklicken des Feldes "OK".

Um die eins zu eins NAT Funktion (1 : 1 NAT) nutzen zu können, benötigen wir noch zwei weitere öffentliche IP Adressen! Dazu verwenden wir die ögffentlichen IP Adressen 216.0.0.135 mittels oder in Verbindung mit der IP Adresse 216.0.0.137 jeweils mit der Subnetzmaske 255.255.255.240. Bitte tragen Sie diese nun auch unter ETH01 ein, genauso wie die anderen beiden Male vorher.

ETH02

Die Netzwerkschnittstelle (Netzwerkkarte) ETH02 soll für die Server benutzt werden. Um den Netzwerkverkehr (die Pakete) von dieser und zu dieser Netzwerkschnittstelle (Netzwerkkarte) zu leiten bzw. zu routen, muss diese Netzwerkschnittstelle (ETH02) mit einer privaten IP Adresse aus dem Klasse C Netzwerk versorgt werden.
Tragen Sie bitte dafür unter ETH02 folgende private IP Adresse “192.168.1.1“ und für das Subnetzwerk “255.255.255.0“ ein.

Wenn Sie alle Eingaben beendet haben, sollten die Einträge genau so aussehen wie auf dem folgenden Bild. (Abbildung 3)

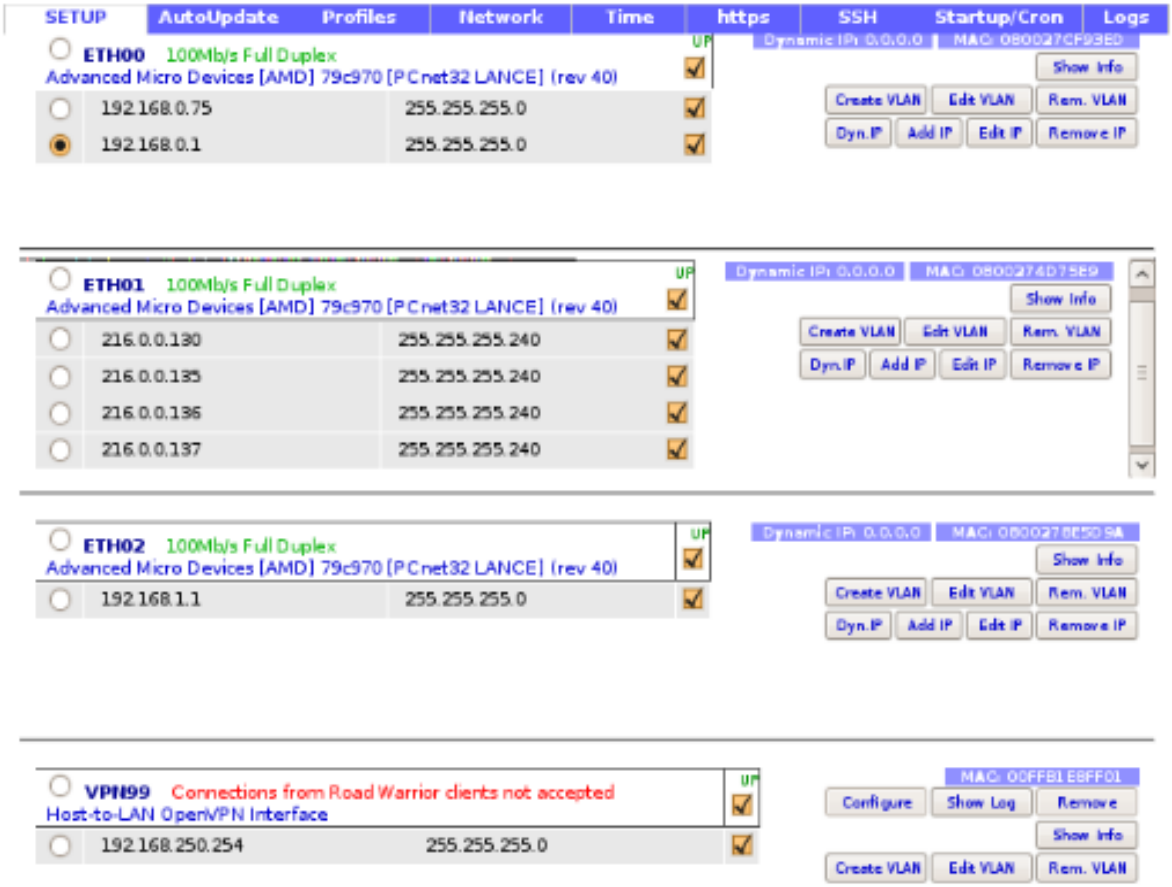


Abbildung 3

Zum Abschluss der Netzwerkkonfiguration gehen Sie bitte zum oberen Rand (unter den Einträgen in blau) in der rechten oberen Ecke und wählen durch anklicken die Option “Gateway“ aus. Und geben nun die öffentliche IP Adresse 216.0.0.129 ein. Wie in der Rubrik “Überblick“ fast am Ende bereits beschrieben.

1 : 1 NAT Einstellungen

Gehen Sie zum oberen Rand und wählen Sie bitte durch anklicken die Auswahl “Startup/Cron“ aus. Falls Sie die Eingabe bereits verlassen haben, gelangen Sie im Menü auf der linken Seite, unter System, durch das anklicken von “Setup“ wieder auf die Eingabeseite und wählen nun rechts am oberen Rand “Startup/Cron“ (in blau) Nachdem sich ein weiteres Fenster geöffnet hat, öffnen Sie bitte links neben dem Feld mit der Beschriftung “Test“ die Auswahlliste (“Drop Down Menü“) und wählen Sie mit dem Mauszeiger die Option “NAT and Virtual Servers“ aus. (Vierte Auswahlmöglichkeit von oben). Um die eins zu eins NAT Funktion (1 : 1 NAT) ordentlich und fehlerfrei nutzen zu können, müssen wir, unter Benutzung des IP Tabellen Kommandos, zwei Regelsätze (IP Vorschriften oder Anweisungen) einfügen.

Der erste Regelsatz, übersetzt bzw. leitet den eingehenden IP Verkehr, von der äußeren Internetverbindung oder der öffentlichen IP Adresse (WAN Netzwerkschnittstelle) zur internen lokalen Netzwerkschnittstelle oder privaten IP Adresse (LAN Netzwerkschnittstelle) der Server, bevor die Pakete geroutet werden.

Der zweite Regelsatz übersetzt bzw. leitet den ausgehenden IP Verkehr, von der privaten IP Adresse der Server, zurück an die Ihr zugewiesenen öffentlichen IP Adresse an der Internet Netzwerkschnittstelle (WAN Netzwerkschnittstelle).

Durch das Anlegen des zweiten Regelsatzes, wird der gesamte ausgehende IP Netzwerkverkehr über die primäre IP Adresse (216.0.0.130) geleitet.
Dieser bei dem Anlegen des zweiten Regelsatzes auftretende Fehler, wird später bei der Konfiguration der mehreren zu eins NAT Funktion (Many : 1 NAT) bereinigt.

Wir werden die Übersetzung bzw. die Verknüpfung der IP Adressen wie in der folgenden Tabelle dargestellt durchführen. (Abbildung 4)

Public (WAN) IP	Private (LAN) IP
216.0.0.135	192.168.1.35
216.0.0.136	192.168.1.36
216.0.0.137	192.168.1.37

Abbildung 4

Um diese Aufgabe zu realisieren und ab zu schließen, tippen Sie bitte den in Abbildung 5 stehenden Text genauso in das noch geöffnete Fenster (“Scripting Editor“). Bitte beachten Sie dabei die Groß –und Kleinschreibung genau um Fehler zu vermeiden.

```
# Translate incoming connections to the private server addresses
iptables -t nat -I PREROUTING 1 -d 216.0.0.135 -i ETH01 -j DNAT --to-
destination 192.168.1.35

iptables -t nat -I PREROUTING 1 -d 216.0.0.136 -i ETH01 -j DNAT --to-
destination 192.168.1.36
iptables -t nat -I PREROUTING 1 -d 216.0.0.137 -i ETH01 -j DNAT --to-
destination 192.168.1.37

# Translate outgoing connections from the private server addresses
iptables -t nat -I POSTROUTING 1 -s 192.168.1.35 -o ETH01 -j SNAT --to-
source 216.0.0.135
iptables -t nat -I POSTROUTING 1 -s 192.168.1.36 -o ETH01 -j SNAT --to-
source 216.0.0.136
iptables -t nat -I POSTROUTING 1 -s 192.168.1.37 -o ETH01 -j SNAT --to-
source 216.0.0.137
```

Abbildung 5

Testen

Wenn Sie Ihre Eingabe beendet haben, richten Sie Ihren Blick bitte an den oberen Rand und wählen Sie durch anklicken mit dem Mauszeiger das Feld “Test“ aus, um Ihren Regelsatz zu testen und Eingabefehler bereits jetzt zu erkennen. Korrigieren Sie diese bei einer Fehlermeldung bitte.

Aktiviren

Wenn Sie dies erledigt haben, gehen Sie mit dem Mauszeiger bitte in die obere rechte Ecke und wählen links vor dem Wort “Status“ durch anklicken, das kleine rechteckige Kästchen aus, um die Regelsätze zu aktivieren.

Abspeichern

Nun müssen Sie ihren kontrollierten und aktivierten Regelsatz nur noch abspeichern. Wählen Sie durch anklicken auf die Auswahl “Save“ aus, ebenfalls in der rechten oberen Ecke und schließen den “Script Editor“ durch anklicken des Feldes “Close“ rechts daneben.

Zur Erläuterung

Bei der Eingabe haben wir uns bewusst für die Option –I (Insert = Einfügen) anstatt der Option –A (Add = hinzufügen) entschieden, damit die Regelsätze bzw. Einträge später am Anfang der Tabelle stehen. Dies war für den Fall erforderlich, falls das Script abgearbeitet wird, nachdem ZeroShell seine eigenen Regelsätze aufgestellt und eingetragen hat.

Ein nicht korrigierter Fehler zu Beginn der Tabelle, kann zur Folge haben, dass sich dieser auf die gesamten eins zu eins NAT Funktion (1 : 1 NAT) und Konfiguration von ZeroShell auswirkt

Mehrere : 1 NAT Einstellungen

Bitte wählen Sie im Menü an der linken Seite, unter der Rubrik “Network“ die Auswahl “Router“ durch anklicken aus. Anschließend wählen Sie bitte am oberen Rand (blau hinterlegt) “NAT“ ebenfalls durch anklicken aus. Ein Fenster mit dem Namen “ Network Address Translation“ öffnet sich. In diesem Fenster wird festgelegt, über welche Netzwerkschnittstelle der ausgehende Netzwerkverkehr mittels NAT Funktion stattfindet.

Markieren

In unserem Fall wählen Sie bitte auf der linke Seite unter dem Namen “Available Interfaces“ die Netzwerkschnittstelle “ETH01“ durch anklicken mit dem Mauszeiger aus.

Auswählen

Anschließend fügen Sie die nun blau makierte Netzwerkschnittstelle “ETH01“ durch das anklicken, der mit diesen Pfeilen “>>>“ gekennzeichneten Taste, in der Mitte der beiden Auswahlfenster, der rechten Seite mit dem Namen “NAT Enabled Interfaces“ zu.

Sichern und schließen

Anschließend klicken Sie noch auf die als “Save“ gekennzeichnete Taste, oben rechts in der Ecke, um Ihre Auswahl dauerhaft zu abzuspeichern. Siehe Abbildung 6

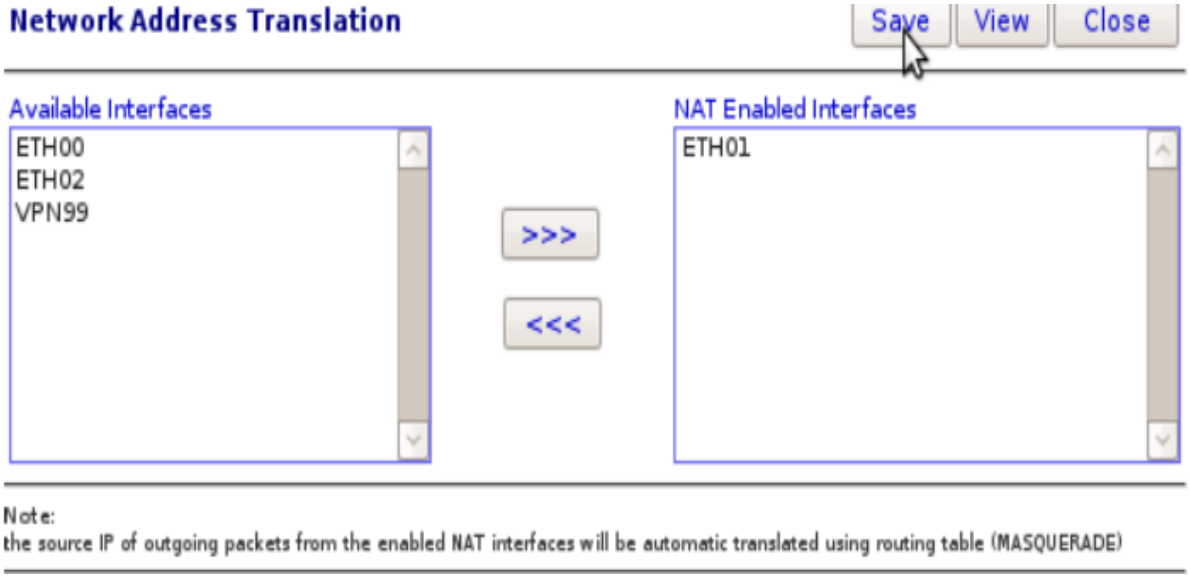


Abbildung 6

Danach drücken Sie nur noch auf die “Close“ genannte Auswahl und das Fenster schließt sich wieder.

Firewall Setup

Zu diesem Zeitpunkt, wo die NAT und Router Funktionen fertig konfiguriert sind, wenden wir uns nun den Firewall Einstellungen von ZeroShell zu.
Um unsere eben gemachten NAT Regelsätze abzusichern, werden wir nun ein paar einfache Firewall Regeln eingeben.

Wichtig
Die Regelsätze für die Firewall von ZeroShell sind manchmal sehr aufwändig umzusetzen und gestalten von Fall zu Fall sehr anspruchsvoll.
Daher werden wir nur ein paar einfache Regeln, unserer oben gemachten NAT Regelsätze betreffend eingeben.

Achtung, bei dem folgenden Beispiel für die Einstellungen der Firewall, handelt es sich nicht um eine vollständige Konfiguration der Firewall von ZeroShell.

Vorsicht, die folgenden Einstellungen für die Firewall von ZeroShell sind außerdem nicht in einer Produktionsumgebung getestet worden und auch nicht auf einem Produktivsystem.

Fehler, die bei dem erstellen von **Regeln** für die **Firewall** gemacht werden, können zur **Folge** haben, dass Sie von der Webschnittstelle (“Webinterface“) **abgemeldet werden und sich nicht wieder anmelden können!**

Zuerst werden wir Regeln erstellen, die den Zugang zum ZeroShell Router selbst, nur noch von der lokalen Netzwerkseite (LAN) aus erlauben. Das heißt für den eingehenden Netzwerkverkehr, der von der Internet Netzwerkschnittstelle (WAN) kommt, dass dieser geblockt wird. Es sei denn, er wurde vorher durch einen Netzwerkklienten (PC oder ein anderer Computer) auf der lokalen Netzwerkseite (LAN) angefordert, zum Beispiel durch das eintippen einer URL in einen Webbrowser, damit dieser eine Webseite anzeigt.

Firewall Eingangsregeln

Regel 1
Dazu gehen wir mit dem Mauszeiger auf das Auswahlmenü auf der linken Seite, unter der Rubrik “Security“ und wählen durch anklicken mit dem Mauszeiger den Punkt bzw. den Eintrag “Firewall“ aus. Wenn die Seite mit den Einstellungen für die Firewall zu sehen ist. Gehen Sie nun mit dem Mauszeiger oben in der rechten Ecke, zu dem herunterklappbaren Auswahlmenü “Pull Down Menu“ rechts neben dem Wort

“Chain“ und klicken auf den kleinen Pfeil, im aufgeklappten Menü klicken Sie jetzt bitte auf das Wort “INPUT“. Gehen Sie mit dem Mauszeiger jetzt etwas herunter auf die rechte Seite und klicken auf “Add“, ein Eingabefenster erscheint. Hier klicken Sie bitte mit dem Mauszeiger unter dem Namen “Value“, aber auf der Höhe von “Input“ am linken Rand auf den Pfeil des aufklappbaren Menüs “Pull Down Menu“, wählen bitte die Netzwerkschnittstelle “ETH00“ aus, verändern Sie sonst nichts und klicken Sie auf die Auswahl mit dem Namen “Confirm“ oben rechts in der Ecke.

Erläuterung

Diese Regel für die Firewall von ZeroShell, erlaubt nun jeglichen Netzwerkverkehr bzw. Zugriff vom lokalen Netzwerk (LAN) zum ZeroShell Router und natürlich auch auf die daran angeschlossenen Netze wie z. B. die Server und das Internet.

Regel 2

Bitte wiederholen Sie diesen Vorgang mit der Auswahl für die Netzwerkschnittstelle Mit dem Namen “ETH02“, bitte genauso wie für die Netzwerkschnittstelle “ETH00“.

Erläuterung

Diese Regel für die Firewall von ZeroShell, erlaubt nun jeglichen Netzwerkverkehr bzw. Zugriff von den Servern im lokalen Netzwerk (LAN oder auch DMZ genannt) zum ZeroShell Router und natürlich auch auf die daran angeschlossenen Netze wie z. B. die Netzwerkgeräte und Computer im lokalen Netzwerk und das Internet.

Regel 3

Für die letzte Firewall Regel, klicken Sie bitte wieder auf die Auswahl mit dem Namen “Add“ und wenn sich das Eingabefenster öffnet, wählen Sie bitte nur durch anklicken mit dem Mauszeiger, in der ziemlich Mitte des Fensters die beiden Optionen mit dem Namen “Established“ und “Related“ aus sonst bitte nichts anklicken. Ich wieder hole, bitte nichts anderes auswählen oder anklicken. Wählen Sie danach wie gewohnt durch Anklicken die Auswahl mit dem Namen “Confirm“ aus.

Erläuterung

Diese Regel für die Firewall von ZeroShell, erlaubt explizit den eingehenden Netzwerkverkehr für bereits bestehende Verbindungen zum ZeroShell Router und zu den Netzwerkteilnehmern (PC´s oder Computer) die ihn angefordert haben.

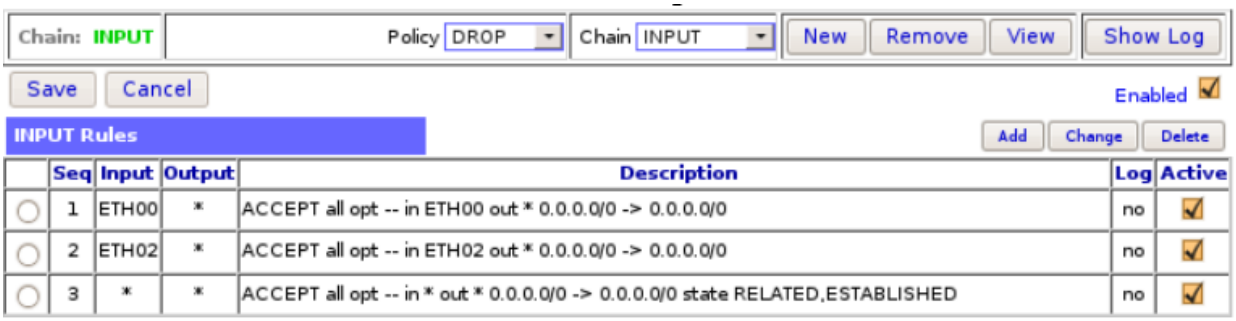
Sichern

Wählen Sie jetzt bitte durch anklicken mit dem Mauszeiger, in der oberen linken Ecke die Auswahl mit dem Namen “Safe” aus, um ihre neu angelegten Regeln zu sichern.

Aktivieren

Um diese Regeln noch zu aktivieren, gehen Sie bitte mit dem Mauszeiger etwas nach links und wählen Sie anschließend rechts neben dem Wort “Policy“ den kleinen Pfeil des aufklappbaren Menüs “Pull Down Menu“ durch anklicken aus. Markieren Sie

bitte den Eintrag “DROP“. Fertig, nun sollten die Einträge der Eingangsregeln für die Firewall von ZeroShell genau so wie in der Abbildung 7 dargestellt aussehen.



	Seq	Input	Output	Description	Log	Active
○	1	ETH00	*	ACCEPT all opt -- in ETH00 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	2	ETH02	*	ACCEPT all opt -- in ETH02 out * 0.0.0.0/0 -> 0.0.0.0/0	no	☑
○	3	*	*	ACCEPT all opt -- in * out * 0.0.0.0/0 -> 0.0.0.0/0 state RELATED,ESTABLISHED	no	☑

Abbildung 7

Firewall Weiterleitungsregeln

Jetzt werden wir die Weiterleitungsregeln für die Firewall von ZeroShell konfigurieren. Diese Regeln dienen der Absicherung der lokalen Netzwerke, in dem sich die Server und die Netzwerkklienten befinden. Sie schützen also die beiden lokalen Netzwerke vor dem unbefugten Zugriff aus dem Internet. Der Netzwerkverkehr zwischen den beiden lokalen Netzwerken mit den Servern und den Netzwerkklienten bleibt davon unberührt. Ebenso wie der Netzwerkverkehr von den beiden lokalen Netzwerken hin zum Internet.

Wir werden ein paar Regeln für die Firewall von ZeroShell eingeben und ein Netzwerkkanäle für die Server öffnen, so dass diese aus dem Internet erreicht werden können. z. B. für FTP oder email Verkehr.

Regel 1

Gehen Sie bitte mit dem Mauszeiger oben in der rechten Ecke, zu dem herunterklappbaren Auswahlmenü “Pull Down Menu“ rechts neben dem Wort “Chain“ und klicken auf den kleinen Pfeil, im aufgeklappten Menü klicken Sie jetzt bitte auf das Wort “FORWARD“. Gehen Sie mit dem Mauszeiger jetzt etwas herunter auf die rechte Seite und klicken auf “Add“, ein Eingabefenster erscheint. Wählen Sie durch anklicken im Feld mit dem Namen “INPUT“ wie vorher bei den anderen Regeln auch zuerst im aufklappbaren Menü “Pull Down Menu“ die Netzwerkschnittstelle mit dem Namen “ETH00“ aus und klicken anschließend rechts wieder auf die Auswahl mit dem Namen “Confirm“.

Erläuterung

Diese Regel für die Firewall von ZeroShell erlaubt ohne Einschränkungen den gesamten Netzwerkverkehr aus dem lokalen Netzwerk (LAN) überall dort hin (in jede Richtung) wohin der ZeroShell Rechner routen kann. z. B. in das Internet und in das lokale Server Netzwerk.

Regel 2

Wiederholen Sie diesen Vorgang und wählen nun diesmal im Feld mit dem Namen “INPUT“ die Netzwerkschnittstelle mit dem Namen „ETH02“ aus. Klicken Sie anschließend bitte wieder auf “CONFIRM“

Erläuterung

Diese Regel für die Firewall von ZeroShell erlaubt uneingeschränkten Netzwerkverkehr vom lokalen Server Netzwerk (Server LAN oder DMZ) in das Internet (WAN) und in das lokale Server Netzwerk selbst.

Regel 3

Für die letzte Firewall Regel, klicken Sie bitte wieder auf die Auswahl mit dem Namen “Add“ und wenn sich das Eingabefenster öffnet, wählen Sie bitte nur durch anklicken mit dem Mauszeiger, in der ziemlich Mitte des Fensters die beiden Optionen mit dem Namen “Established“ und “Related“ aus sonst bitte nichts anklicken. Ich wieder hole, bitte nichts anderes auswählen oder anklicken. Wählen Sie danach wie gewohnt durch Anklicken die Auswahl mit dem Namen “Confirm“ aus.

Erläuterung

Diese Regel für die Firewall von ZeroShell erlaubt eine zwei Wege Kommunikation für bestehende Verbindungen, aufgrund der vorherigen beiden Regeln.

Nun werden wir noch ein paar Netzwerkkanäle (Ports) für unsere (1 : 1 NAT) Server öffnen, so dass Sie vom Internet aus erreicht werden können.
Die folgende Tabelle zeigt welchen Netzwerkkanäle (Ports) für dieses Beispiel geöffnet werden müssen und vor allem wie Sie geöffnet werden. Abbildung 8

Public IP	Private IP	Protocol	Port
216.0.0.135	192.168.1.35	TCP	80
216.0.0.136	192.168.1.36	TCP	22
216.0.0.137	192.168.1.37	UDP	123
(all)	(all)	ICMP	(ping)

Abbildung 8

Öffnen der Netzwerkkanäle und Eintragen der Netzwerkprotokolle unter Zuweisung einer IP Adresse

Klicken Sie wieder auf “Add” und wählen unter “Input“ den Eintrag “ETH01“ aus Tragen Sie bitte bei der Empfangs IP Adresse “Destination IP“ die IP Adresse 192.168.1.35 ein und wählen am linken Rand unter dem Eintrag “Protocol Matching“ (zutreffendes Protokoll) das Protokoll “TCP“ aus dem aufklappbaren Menü aus. Nun tragen Sie bitte etwas weiter rechts, in das leere Kästchen unter der Beschriftung “Dest. Port“ (zu öffnender ankommender Netzwerkkanal) eine 80 ein und anschließend klicken Sie bitte oben rechts in der Ecke auf das Feld mit dem Namen “Confirm“

Klicken Sie wieder auf “Add” und wählen unter “Input“ den Eintrag “ETH01“ aus Tragen Sie bitte bei der Empfangs IP Adresse “Destination IP“ die IP Adresse 192.168.1.36 ein und wählen am linken Rand unter dem Eintrag “Protocol Matching“ (zutreffendes Protokoll) das Protokoll “TCP“ aus dem aufklappbaren Menü aus. Nun tragen Sie bitte etwas weiter rechts, in das leere Kästchen unter der Beschriftung “Dest. Port“ (zu öffnender ankommender Netzwerkkanal) eine 22 ein und anschließend klicken Sie bitte oben rechts in der Ecke auf das Feld mit dem Namen “Confirm“

Klicken Sie wieder auf “Add” und wählen unter “Input“ den Eintrag “ETH01“ aus Tragen Sie bitte bei der Empfangs IP Adresse “Destination IP“ die IP Adresse 192.168.1.37 ein und wählen am linken Rand unter dem Eintrag “Protocol Matching“ (zutreffendes Protokoll) das Protokoll “UDP“ aus dem aufklappbaren Menü aus. Nun tragen Sie bitte etwas weiter rechts, in das leere Kästchen unter der Beschriftung “Dest. Port“ (zu öffnender ankommender Netzwerkkanal) eine 123 ein und anschließend klicken Sie bitte oben rechts in der Ecke auf das Feld mit dem Namen “Confirm“

Klicken Sie wieder auf “Add” und wählen unter “Input“ den Eintrag “ETH01“ aus Tragen Sie bitte bei der Empfangs IP Adresse “Destination IP“ die IP Adresse 192.168.1.35-192.168.1.37 ein und wählen am linken Rand unter dem Eintrag “Protocol Matching“ (zutreffendes Protokoll) das Protokoll “ICMP“ aus dem aufklappbaren Menü aus.

Nun wählen Sie bitte auf der rechten Seite, im aufklappbarem Menü unter der Bezeichnung “ICMP Type“ den Eintrag mit dem Namen “Echo-request (ping)“ aus (der zweite Eintrag von oben) anschließend klicken Sie bitte wie gewohnt oben rechts in der Ecke auf das Feld mit dem Namen “Confirm“.

Abschließende Aufgaben

Konfigurieren Sie die Server am Netzwerkanschluss mit dem Namen “ETH02” (Server LAN) mit den dazugehörigen und benötigten IP Adressen und tragen als Sie bitte als Standard Gateway (Default Gateway), die IP Adresse vom ZeroShell Router 192.168.1.1 mit der Subnetzmaske (Subnetmask) 255.255.255.0 ein.

Konfigurieren Sie die Netzwerkklienten am Netzwerkanschluss mit dem Namen “ETH00” (Client LAN) auf die gleiche Art und Weise mit den dazugehörigen IP Adressen und tragen als Sie bitte als Standard Gateway (Default Gateway), auch wieder die IP Adresse vom ZeroShell Router 192.168.1.1 mit der Subnetzmaske (Subnetmask) 255.255.255.0 ein.

Oder konfigurieren Sie den DHCP Server von ZeroShell für die automatische IP Adresszuweisung im lokalen Netzwerk (LAN), was allerdings weit außerhalb der Tragweite dieses Dokumentes liegt.

Or, configure ZeroShell's DHCP servers to do the same (instructions for this is beyond the scope of this document).

Klicken Sie ganz am oberen Rand, fast mittig, jetzt bitte auf den Link mit dem Namen “Reboot” um ZeroShell neu zu starten (“Booten“).

Um sicher zu stellen, dass nach dem Neustart, die Hardware sowie die Software wie gewohnt funktionieren, wählen Sie bitte nach dem Neustart auf der linken Seite, unter der Rubrik mit dem Namen “Network“ das Feld mit der Bezeichnung “Router“ aus und klicken danach in der Mitte auf das Feld mit der Beschriftung “NAT“ um sich das Resultat Ihrer Bemühungen anzusehen. Siehe unten in Abbildung 9

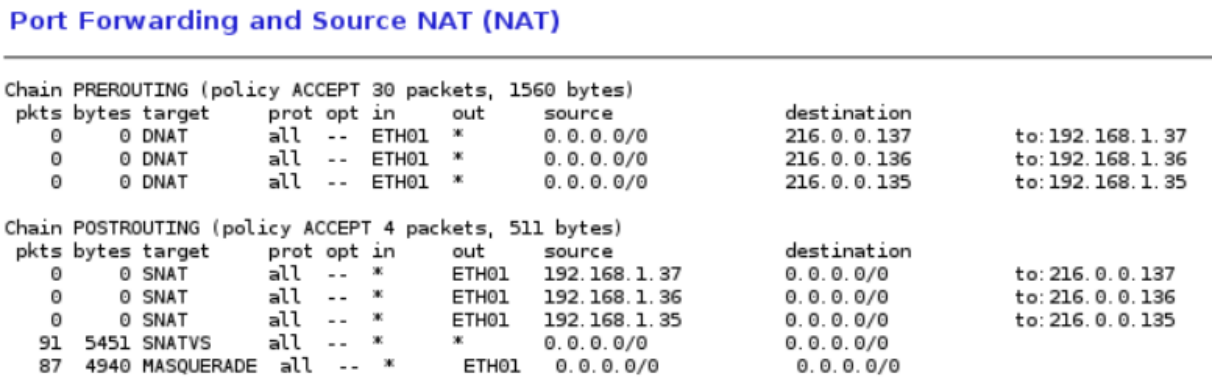


Abbildung 9

Point of origin:
The original document of this translation was written by Brian Weaver in the English language and it is reachable for comparing under the following link shown below.

Herkunftsangabe:
Das Original Dokument, auf das sich diese Übersetzung bezieht, wurde von Brian Weaver in englischer Sprache erstellt und befindet sich zum Vergleich unter folgender Internetadresse abrufbar.

http://www.zeroshell.net/listing/1_1_NAT_in_ZeroShell.pdf