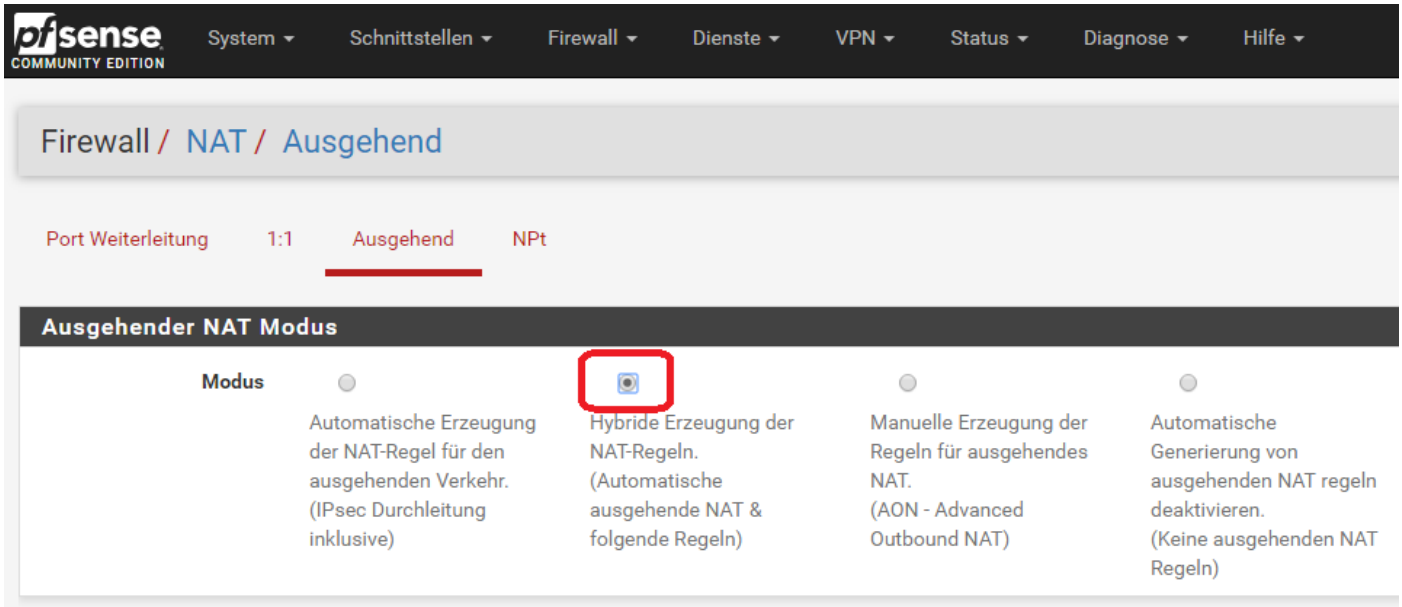
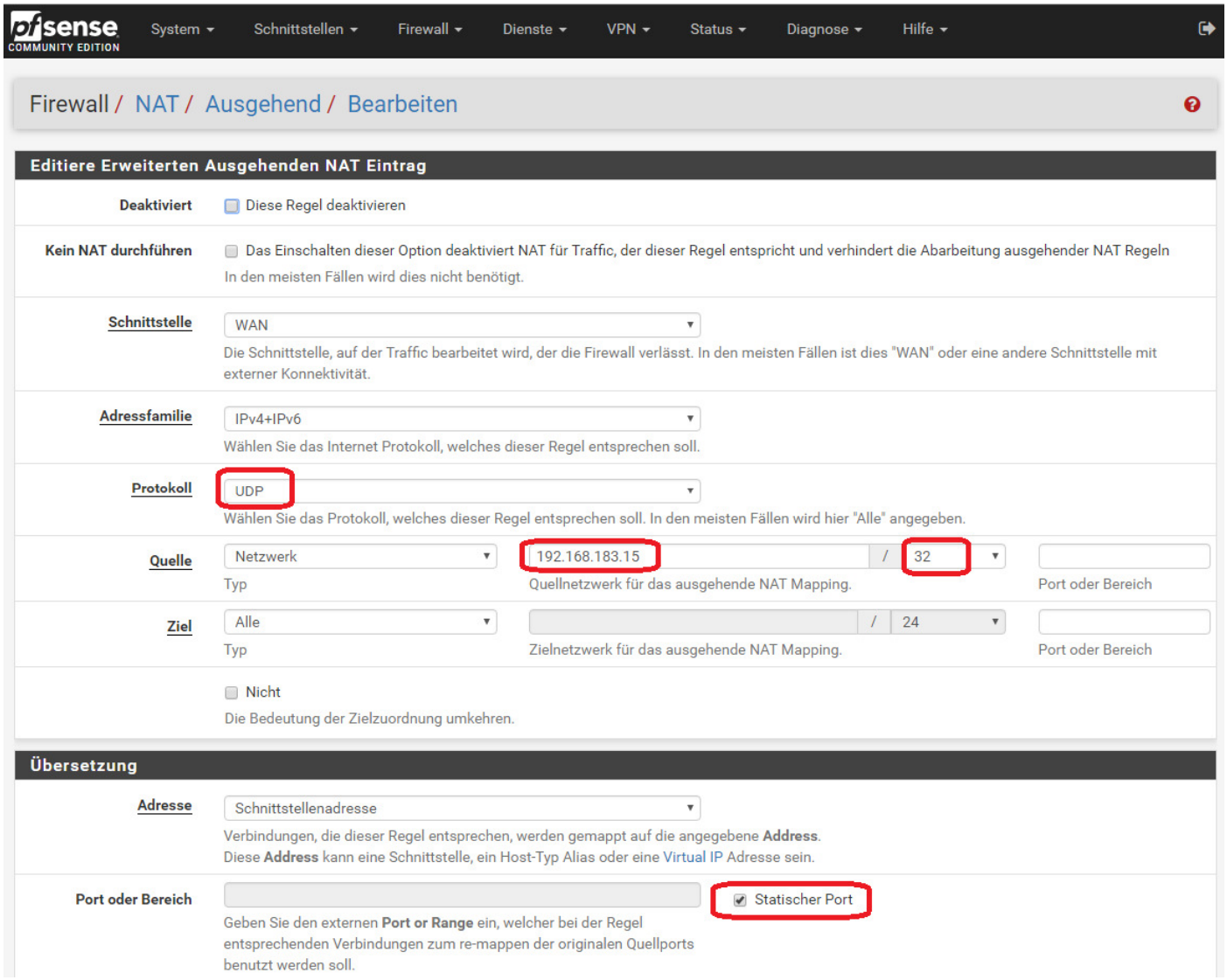
Konfiguration pfSense FireWall für SIP

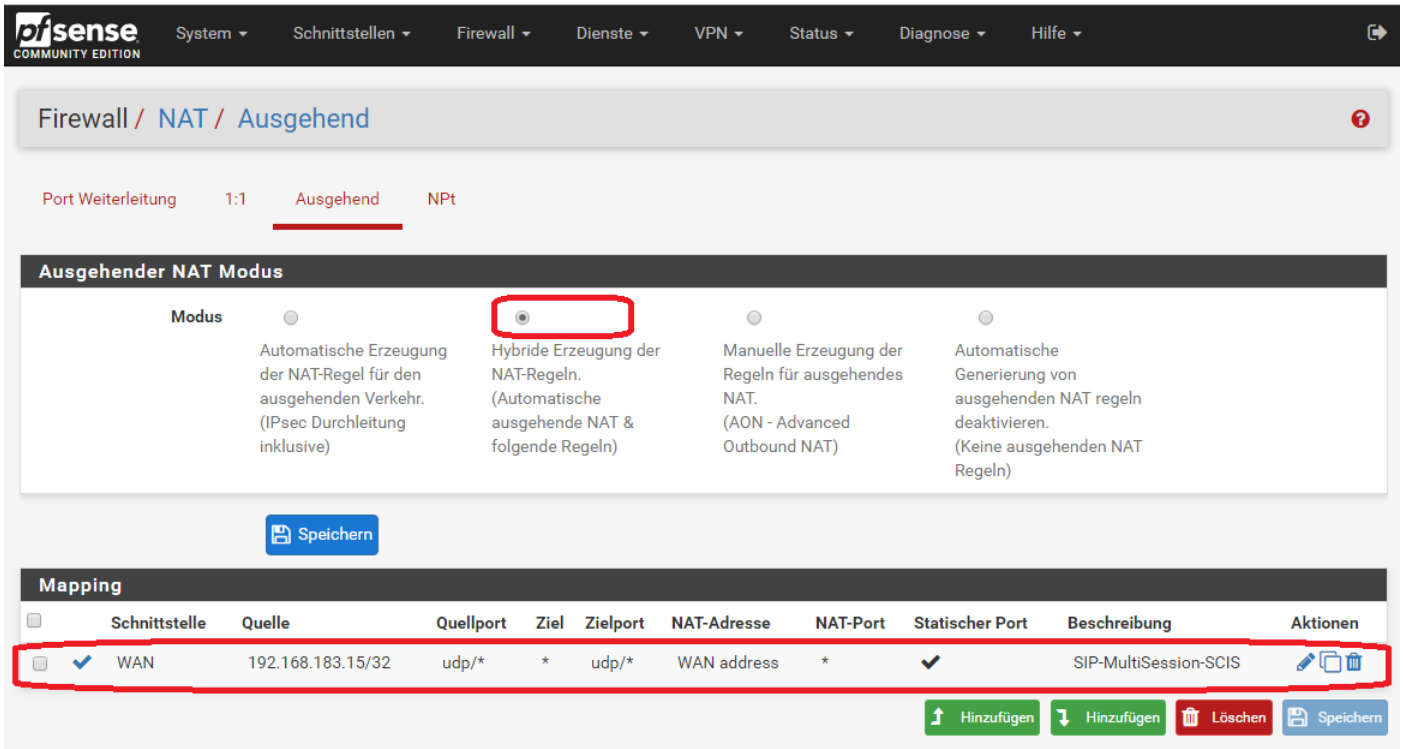
Ersteller: System-Clinch IT Servcies – www.MiaTel.ch
Author: Manuel Magnin, MMagnin@Clinch.ch
Datum: 28.02.2019

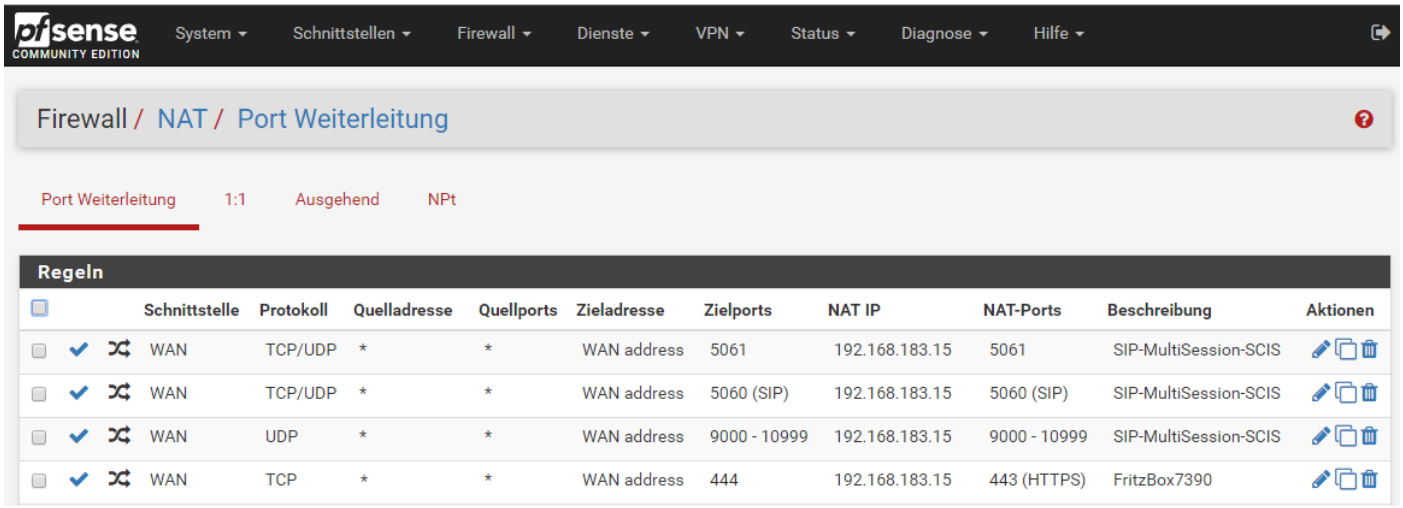
Leider unterstützt pfSense in der Auslieferkonfiguration nur eine SIP Registrierung zugleich (Im Firewall Betrieb LAN zu WAN). Moderne SIP Clients bekommen das Problem mit der Registration in den Griff in dem für die zweite Registration ein anderer Port verwendet wird. Jedoch sind weiterhin keine zwei Sprachkanäle per RTP möglich. Zusätzlich sind die NAT Timeouts zu klein, so dass ausgehende Anrufe immer gehen, jedoch eingehende Anrufe funktionieren nur sporadisch. Dann ist die Ursache, die NAT Timeout Zeit. Die pfSense hat einen NAT-Timeout von Standard mässig 60 Sekunden, SIP sollte 600 Sekunden haben.
Um mehrere Registrationen und mehrere Sprachkanäle zugleich nutzen zu können, müssen auf der pfSense ein paar Einstellungen vorgenommen werden.

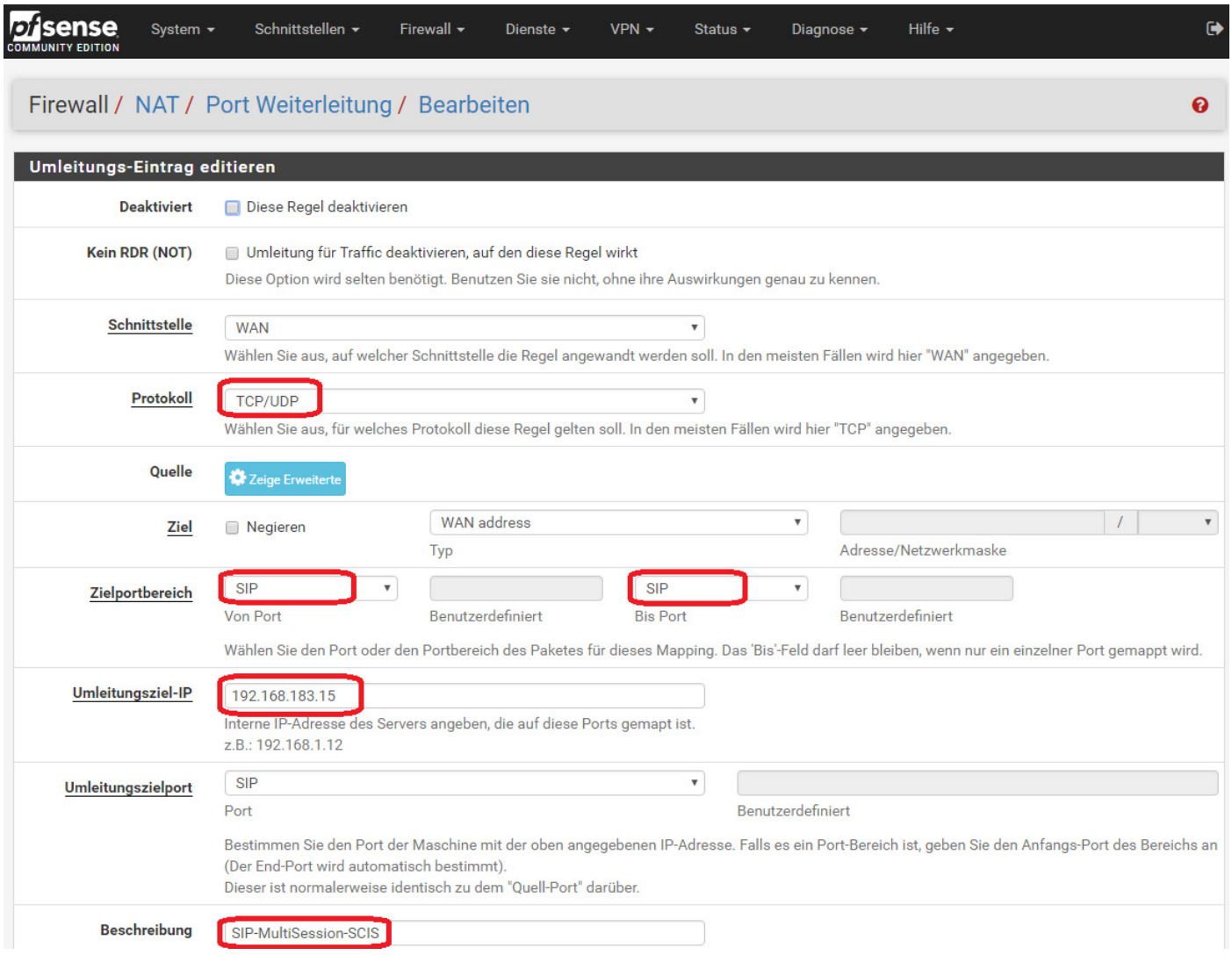
Hier ein Beilspiel mit einer pfSense 2.4.4 und einer FritzBox 7490 mit der IP: 192.168.183.15

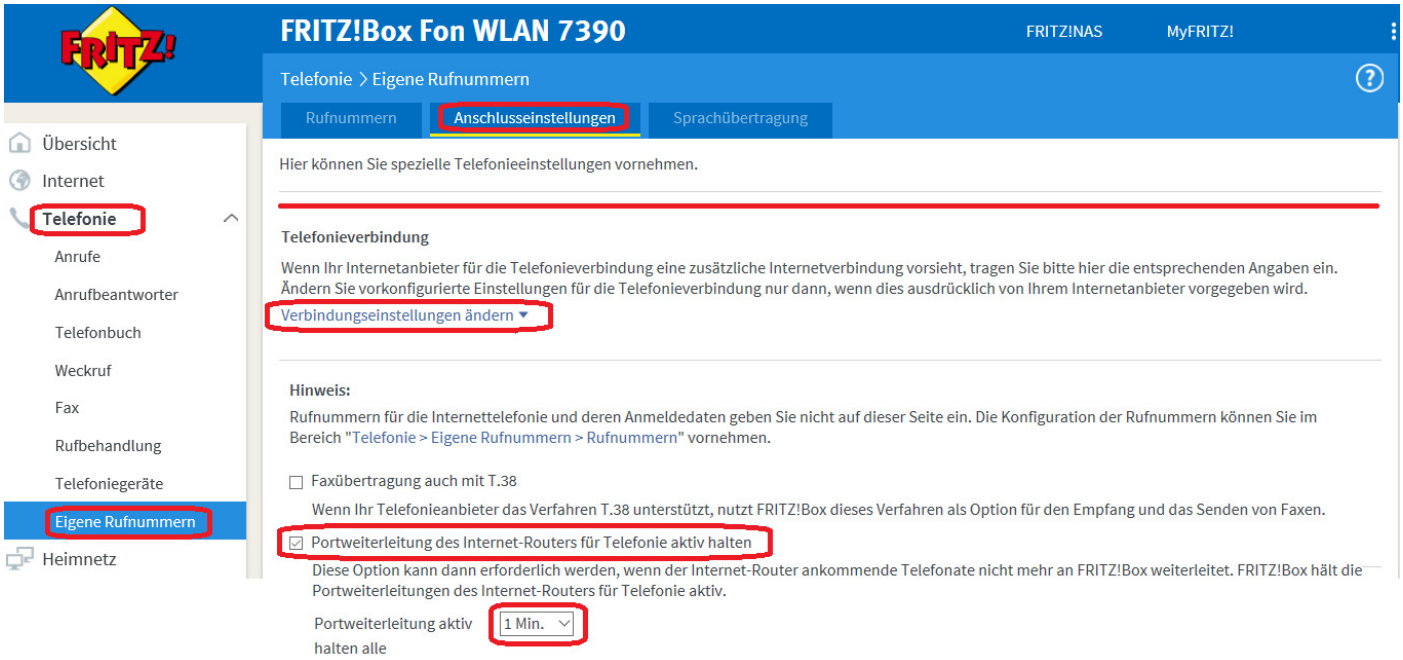



pfsense COMMUNITY EDITION
System
Schnittstellen
Firewall
Dienste
VPN
Status
Diagnose
Hilfe
Firewall / NAT / Ausgehend / Bearbeiten
Editiere Erweiterten Ausgehenden NAT Eintrag
Deaktiviert
Diese Regel deaktivieren
Kein NAT durchführen
Das Einschalten dieser Option deaktiviert NAT für Traffic, der dieser Regel entspricht und verhindert die Abarbeitung ausgehender NAT Regeln
In den meisten Fällen wird dies nicht benötigt.
Schnittstelle
WAN
Die Schnittstelle, auf der Traffic bearbeitet wird, der die Firewall verlässt. In den meisten Fällen ist dies "WAN" oder eine andere Schnittstelle mit externer Konnektivität.
Adressfamilie
IPv4+IPv6
Wählen Sie das Internet Protokoll, welches dieser Regel entsprechen soll.
Protokoll
UDP
Wählen Sie das Protokoll, welches dieser Regel entsprechen soll. In den meisten Fällen wird hier "Alle" angegeben.
Quelle
Netzwerk
Typ
192.168.183.15
/ 32
Quellnetzwerk für das ausgehende NAT Mapping.
Port oder Bereich
Ziel
Alle
Typ
/ 24
Zielnetzwerk für das ausgehende NAT Mapping.
Port oder Bereich
Nicht
Die Bedeutung der Zielzuordnung umkehren.
Übersetzung
Adresse
Schnittstellenadresse
Verbindungen, die dieser Regel entsprechen, werden gemappt auf die angegebene Address.
Diese Address kann eine Schnittstelle, ein Host-Typ Alias oder eine Virtual IP Adresse sein.
Port oder Bereich
Statischer Port
Geben Sie den externen Port or Range ein, welcher bei der Regel entsprechenden Verbindungen zum re-mappen der originalen Quellports benutzt werden soll.


pfsense COMMUNITY EDITION
System
Schnittstellen
Firewall
Dienste
VPN
Status
Diagnose
Hilfe
Firewall / NAT / Ausgehend
Port Weiterleitung
1:1
Ausgehend
NPt
Ausgehender NAT Modus
Modus
Automatische Erzeugung der NAT-Regel für den ausgehenden Verkehr. (IPsec Durchleitung inklusive)
Hybride Erzeugung der NAT-Regeln. (Automatische ausgehende NAT & folgende Regeln)
Manuelle Erzeugung der Regeln für ausgehendes NAT. (AON - Advanced Outbound NAT)
Automatische Generierung von ausgehenden NAT regeln deaktivieren. (Keine ausgehenden NAT Regeln)
Speichern
Mapping
Schnittstelle
Quelle
Quellport
Ziel
Zielport
NAT-Adresse
NAT-Port
Statischer Port
Beschreibung
Aktionen
WAN
192.168.183.15/32
udp/*
*
udp/*
WAN address
*
SIP-MultiSession-SCIS
Hinzufügen
Hinzufügen
Löschen
Speichern


pfsense COMMUNITY EDITION
System
Schnittstellen
Firewall
Dienste
VPN
Status
Diagnose
Hilfe
Firewall / NAT / Port Weiterleitung
Port Weiterleitung
1:1
Ausgehend
NPt
Regeln
Schnittstelle Protokoll Quelladresse Quellports Zieladresse Zielports NAT IP NAT-Ports Beschreibung Aktionen
WAN TCP/UDP * * WAN address 5061 192.168.183.15 5061 SIP-MultiSession-SCIS
WAN TCP/UDP * * WAN address 5060 (SIP) 192.168.183.15 5060 (SIP) SIP-MultiSession-SCIS
WAN UDP * * WAN address 9000 - 10999 192.168.183.15 9000 - 10999 SIP-MultiSession-SCIS
WAN TCP * * WAN address 444 192.168.183.15 443 (HTTPS) FritzBox7390


pfsense COMMUNITY EDITION
System
Schnittstellen
Firewall
Dienste
VPN
Status
Diagnose
Hilfe
Firewall / NAT / Port Weiterleitung / Bearbeiten
Umleitungs-Eintrag editieren
Deaktiviert
Diese Regel deaktivieren
Kein RDR (NOT)
Umleitung für Traffic deaktivieren, auf den diese Regel wirkt
Diese Option wird selten benötigt. Benutzen Sie sie nicht, ohne ihre Auswirkungen genau zu kennen.
Schnittstelle
WAN
Wählen Sie aus, auf welcher Schnittstelle die Regel angewandt werden soll. In den meisten Fällen wird hier "WAN" angegeben.
Protokoll
TCP/UDP
Wählen Sie aus, für welches Protokoll diese Regel gelten soll. In den meisten Fällen wird hier "TCP" angegeben.
Quelle
Zeige Erweiterte
Ziel
Negieren
WAN address
Typ
Adresse/Netzwerkmaske
Zielportbereich
SIP
Von Port
Benutzerdefiniert
SIP
Bis Port
Benutzerdefiniert
Wählen Sie den Port oder den Portbereich des Paketes für dieses Mapping. Das 'Bis'-Feld darf leer bleiben, wenn nur ein einzelner Port gemappt wird.
Umleitungsziel-IP
192.168.183.15
Interne IP-Adresse des Servers angeben, die auf diese Ports gemapt ist.
z.B.: 192.168.1.12
Umleitungszielport
SIP
Port
Benutzerdefiniert
Bestimmen Sie den Port der Maschine mit der oben angegebenen IP-Adresse. Falls es ein Port-Bereich ist, geben Sie den Anfangs-Port des Bereichs an
(Der End-Port wird automatisch bestimmt).
Dieser ist normalerweise identisch zu dem "Quell-Port" darüber.
Beschreibung
SIP-MultiSession-SCIS


FRITZ!Box Fon WLAN 7390
FRITZ!NAS
MyFRITZ!
Telefonie > Eigene Rufnummern
Rufnummern
Anschlusseinstellungen
Sprachübertragung
Übersicht
Internet
Telefonie
Anrufe
Anrufbeantworter
Telefonbuch
Weckruf
Fax
Rufbehandlung
Telefoniegeräte
Eigene Rufnummern
Heimnetz
Hier können Sie spezielle Telefonieeinstellungen vornehmen.
Telefonieverbindung
Wenn Ihr Internetanbieter für die Telefonieverbindung eine zusätzliche Internetverbindung vorsieht, tragen Sie bitte hier die entsprechenden Angaben ein. Ändern Sie vorkonfigurierte Einstellungen für die Telefonieverbindung nur dann, wenn dies ausdrücklich von Ihrem Internetanbieter vorgegeben wird.
Verbindungseinstellungen ändern
Hinweis:
Rufnummern für die Internettelefonie und deren Anmeldedaten geben Sie nicht auf dieser Seite ein. Die Konfiguration der Rufnummern können Sie im Bereich "Telefonie > Eigene Rufnummern > Rufnummern" vornehmen.
Faxübertragung auch mit T.38
Wenn Ihr Telefonieanbieter das Verfahren T.38 unterstützt, nutzt FRITZ!Box dieses Verfahren als Option für den Empfang und das Senden von Faxen.
Portweiterleitung des Internet-Routers für Telefonie aktiv halten
Diese Option kann dann erforderlich werden, wenn der Internet-Router ankommende Telefonate nicht mehr an FRITZ!Box weiterleitet. FRITZ!Box hält die Portweiterleitungen des Internet-Routers für Telefonie aktiv.
Portweiterleitung aktiv halten alle
1 Min.