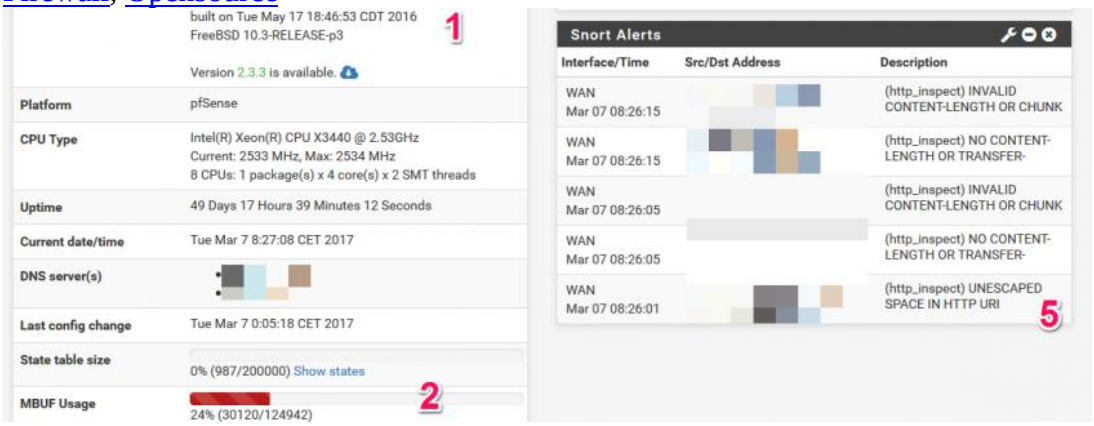
Pfsense Firewall installieren und konfigurieren

Firewall, Opensource



Was ist eine pfsense Firewall?

Pfsense ist eine Opensource Firewall-Software. D.h. die Software wird von vielen Entwicklern weltweit „kostenlos“ programmiert und kann von jedem (sowohl Einzelpersonen als auch Firmen) genutzt werden. Pfsense basiert auf FreeBDS – einem Linux Derivat. Im Gegensatz zu den meisten Linux-Systemen auf denen das Programm „iptables“ für Firewall-Regel zum Einsatz kommt, nutzt FreeBSD zur Steuerung von Netzwerk-Verkehr einen Paket-Filter. Das „pf“ von PFsense steht für Paket-Filter.
PFsense kann unter https://www.pfsense.org/download/ herunter geladen werden. Auf der Website von pfsense.org kann auch direkt Firewall-Hardware gekauft werden. Für unsere Zwecke reicht aber bereits ein älterer PC. Dazu gleich mehr.

Neben pfsense gibt es noch eine Anzahl weiterer Firewalls die auf Opensource basieren.
– IPCOP (mittlerweile veraltet), http://www.ipcop.org/
– M0n0wall: http://m0n0.ch
– Endian http://www.endian.com/de/
– OPNsense: https://opnsense.org/about/about-opnsense/ (Fork von pfsense)

Pfsense ist unter den Opensource Firewalls das zur Zeit (Stand 2017) bekannteste Projekt und hat dabei die größte aktive Anzahl an Entwickler bzw. Supportern.

2 Virtuelle Maschine anlegen / PC vorbereiten

Um eine pfsense zu installieren benötigen Sie meistens wenig echte Hardware-Ressourcen. Wich-tig sind 2 Netzwerk-Karten. Ohne zweite Netzwerk-Karte macht der Firewall wenig Sinn, da er ja nun mal zwei Netze (das interne und das externe) voneinander trennt.

Wenn die pfsense physisch installiert werden soll: 2- Kerne, 2 GB RAM, 10 -15 GB HDD. Oft ge-nügt ein alter PC (auf Celeron Basis), in den eine zweite Netzwerkkarte eingebaut wird. Wichtiger als die Leistung des Geräts ist die Zuverlässigkeit und Stabilität der Firewall. Schließlich soll die pfsense Firewall ja viele Monate bzw. Jahre zuverlässig ihren Dienst tun.

Für die pfsense gibt es fertige Distributionen für so genannte Appliances. Das sind fertige Geräte (meist auf Basis einer kleineren CPU – Atom bspw.) bei denen neben wenig RAM eine Flash-Speicherkarte eingebaut ist. Diese sind oft sehr genügsam was den Stromverbrauch angeht und reichen für kleine Firmen oder Home-Offices meistens aus.

Ebenso genügsam sind die Anforderungen wenn die pfsense z.B. unter VMWare virtualisiert wird. Hierbei wieder wichtig: 2 NICs mit je einem Bein im LAN und einem Bein im WAN.

3 Pfsense einrichten

3.1 Installation

Zur Installation einer pfsense legen Sie die CD ins Laufwerk, booten und folgen anschließend dem Assistenten (engl. Wizard). Auf Geräten, die von USB booten können, reicht oft auch ein bootbarer USB-Stick auf dem Sie vorher das ISO-Image von pfsense entpackt haben. Download: https://www.pfsense.org/download/

Der Installations-Screen der pfsense

Die Fragen des Installations-Assistenten bestätigen Sie mit „ok“ und lassen die Installation durch-laufen. Der Reihe nach werden nun erst die notwendigen File-Systeme angelegt, anschließend formatiert und danach mit den Bits und Bytes der pfsense-Distribution bestückt.

Bei der Installation werden die Filesysteme neu formatiert – daher vorher Daten sichern!

Der Vorgang ist je nach Geschwindigkeit der Hardware – insb. Der Festplatte – nach einigen, we-nigen Minuten fertig. Danach werden Sie aufgefordert die neu installierte Firewall neu zu booten.

Am Ende der Installation folgt der obligatorische Reboot

Bestätigen Sie das, entfernen Sie die CD-ROM (egal ob physisch oder virtuelle) und rebooten die Firewall.

3.2 Konfiguration

Nach dem Reboot meldet sich die pfsense Firewall mit dem Einrichtungs-Bildschirm. Hier müssen Sie zunächst die Zuweisung der Netzwerk-Interfaces durchführen.
Tipp: Sofern Sie eine virtuelle pfsense einrichten: Schauen Sie unter VMWare nach den MAC-Adressen und notieren sich diese (meist reichen die letzten 3-4 Stellen um die Anschlüsse ausei-nander zu halten). Bei physischen Maschinen schauen Sie vorher auf die Interface-Karten oder notieren sich die MAC-Adresse im Bios.

Der wichtigste Punkt der Konfiguration: Zuweisung der Netzwerk-Schnittstellen

Wählen Sie im obigen Screen (1) um die Zuordnung des externen (WAN) und internen (LAN) Inter-faces durchzuführen. Mit (2) ändern Sie direkt danach mindestens die LAN-Adresse der Firewall auf ihr Netzwerk ab.

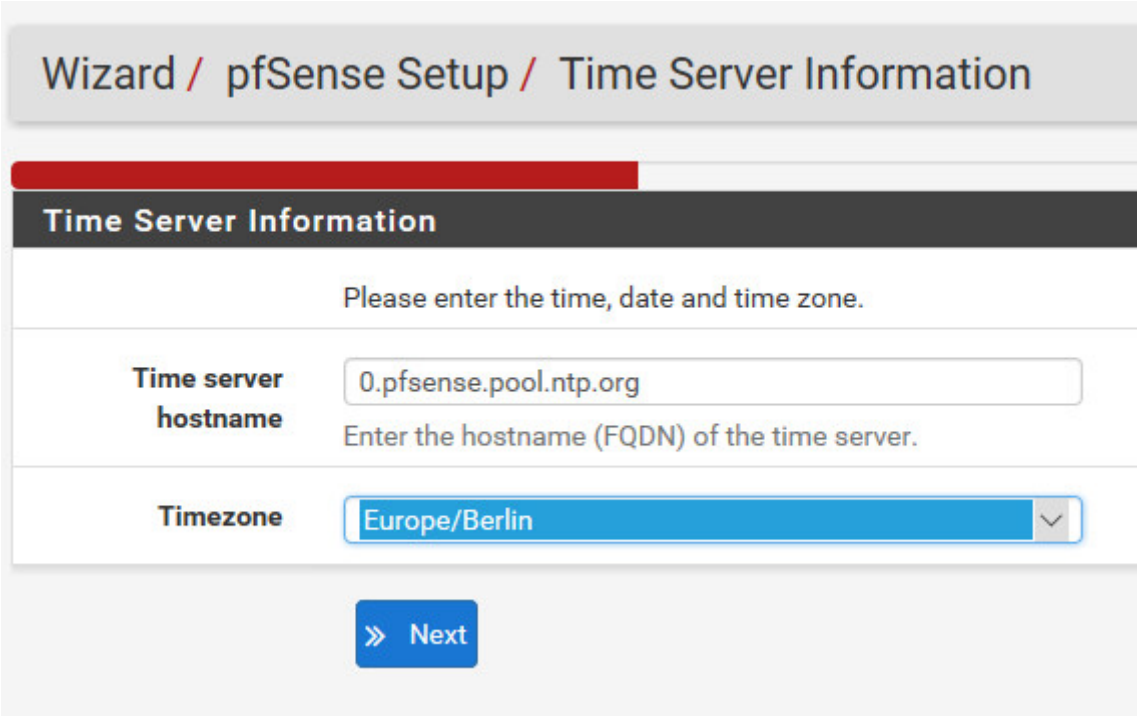
Direkt danach müssen Sie von einem PC/Server im internen LAN die IP-Adresse der Firewall pin-gen können (hier im Beispiel 192.168.1.254). Sofern der Ping auf das LAN-Interface der pfsense erfolgreich isrt, wechseln Sie für alle weiteren Arbeiten auf einen PC/Notebook/Server im internen LAN.

Melden Sie sich dort mit einem Browser an der LAN-Adresse des Firewalls an. URL: https://192.168.1.254
Das initiale Passwort für die erste Anmeldung lautet „pfsense“. Der Username ist „admin“.

3.3 Wizard starten

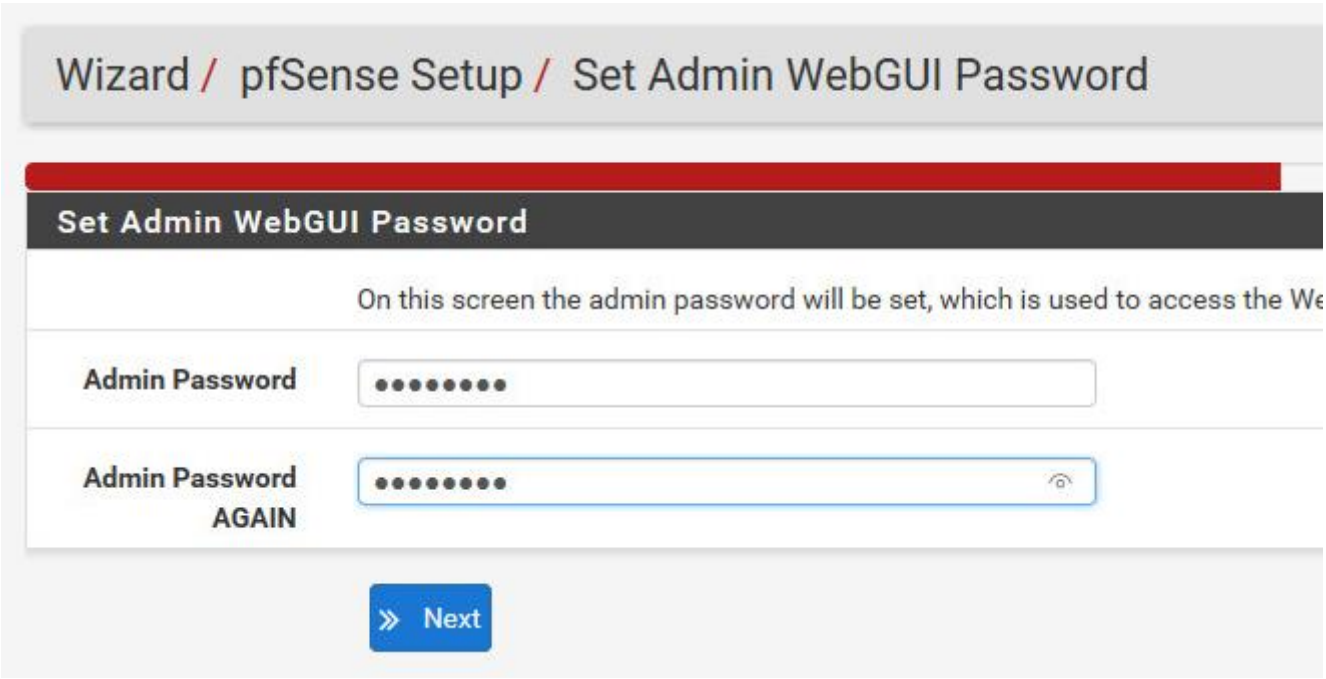
Starten Sie im Web-Browser anschließend den Wizard, mit dem Sie DNS, Zeitzone und die Zeit-Server einrichten:

Die Einstellungen sind an sich fast selbst erklärend:



Einstellen der korrekten Zeitzone für die pfsense Firewall

Zum Schluß ändern Sie die WAN-Adresse des externen Interfaces und ändern das Passwort für den Web-Benutzer „admin“ ab.



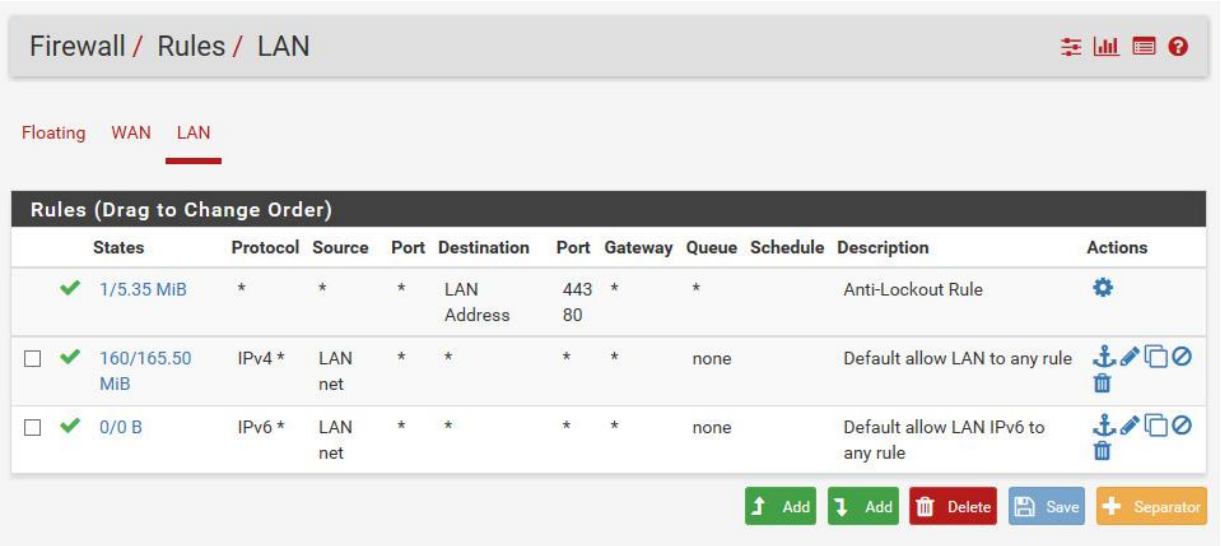
Last but not least: Ein sicheres Passwort für die Web-Oberfläche der pfsense

Damit ist der Wizard abgeschlossen und die Firewall fast betriebsbereit.

Lesetipp: Wie Sie sich selbst schwierige Passwörter gut merken können.

3.4 Minimal-Regeln

Die pfsense Firewall hat in ihrer Grund-Einstellung folgenden Regeln (siehe Screenshot weiter unen). Diese finden Sie unter Firewall => Rules.



Die Standard-Regeln für die Firewall nach der ersten Installation.

Aller Netzwerk-Verkehr aus dem LAN kann von intern nach extern ist erlaubt und wird mit Network Adress Translation (NAT) von internen IP-Adressen auf externe gemappt. (Tab bzw. Rei-ter „LAN“)
Aller Netzwerkverkehr von außen nach innen wird blockiert. (Tab bzw. Reiter „WAN“)

Bitte testen Sie nun von einem Endgerät aus dem LAN heraus ob Sie eine öffentliche Adresse pingen können.
Test: Ping zu 8.8.8.8 geht? Gut. Dann machen Sie weiter

4 Update der pfsense / weitere Anpassungen

4.1 Software-Updates

Jetzt ist ein guter Zeitpunkt, um die pfsense auf den aktuellen Stand der Software zu bringen.
Sie erhalten die SW-Updates online aus dem Repository von pfsense:
System -> Updates -> durchlaufen lassen. => Reboot.

Achtung: Beim Reboot werden je nach Update Umfang mehrere Pakete entpackt und installiert.
Das kann ein paar Minuten dauern. Halten Sie durch – bitte nicht die Nerven verlieren. Sofern

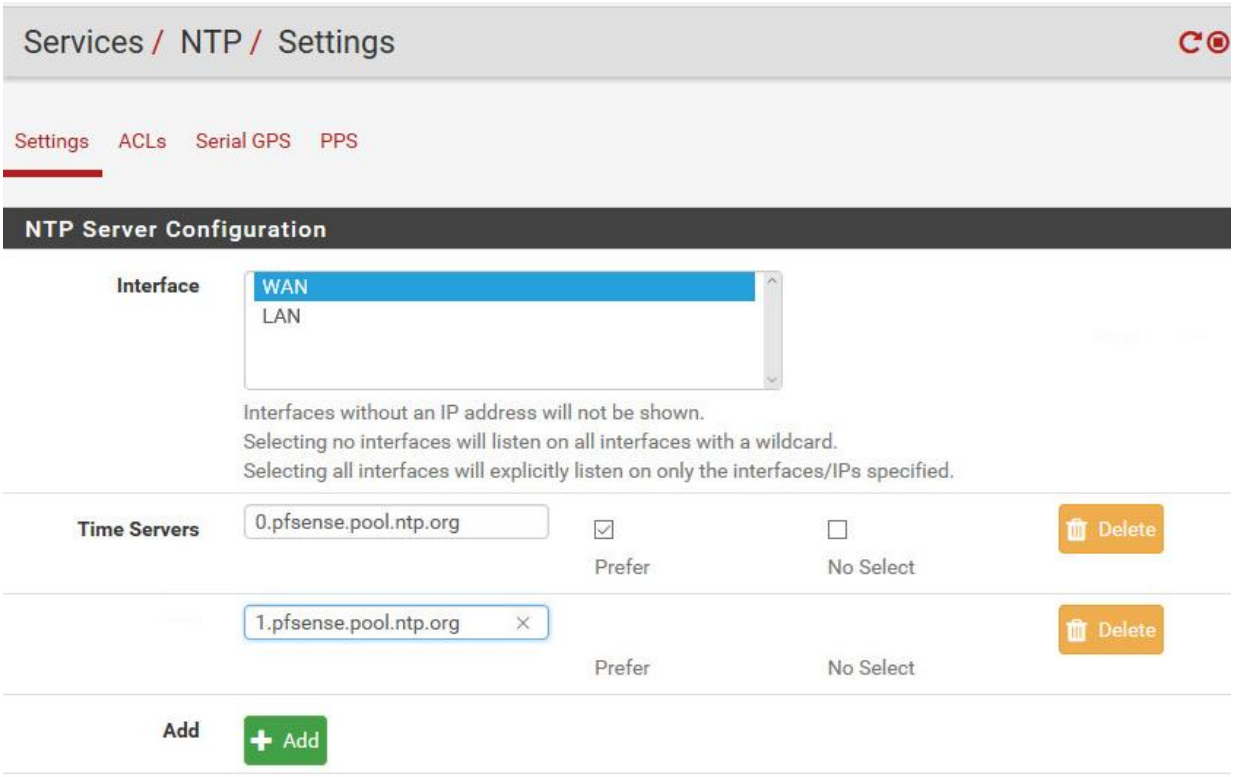
Sie die pfsense virtuell auf VMWare oder Hyper-V installiert haben, können Sie sich den Fortschritt der Installation direkt auf der System-Konsole anschauen.

4.2 DNS einstellen

Per Default ist auf der pfsense ein DNS-Resolver eingestellt. Das kann man so lassen oder den DNS-Resolver aus machen und DNS-Forward (empfohlen) einstellen.
Ein DNS-Resolver ist dabei der eigentliche DNS-Dienst. Die pfsense übernimmt also normale DNS-Aufgaben.
Beim DNS-Forwarder werden DNS Anfragen von der pfsense direkt an einen erreichbaren DNS-Server weiter geleitet.

4.3 NTP einstellen

Beim NTP-Service binden Sie den NTP-Dienst bitte an das LAN-Interface und setzen zusätzlich zum Eintrag „0.pfsense.pool.ntp.org“ den zweiten „1.pfsense.pool.ntp.org“.



Bindung des NTP-Dienstes an den internen LAN-Port

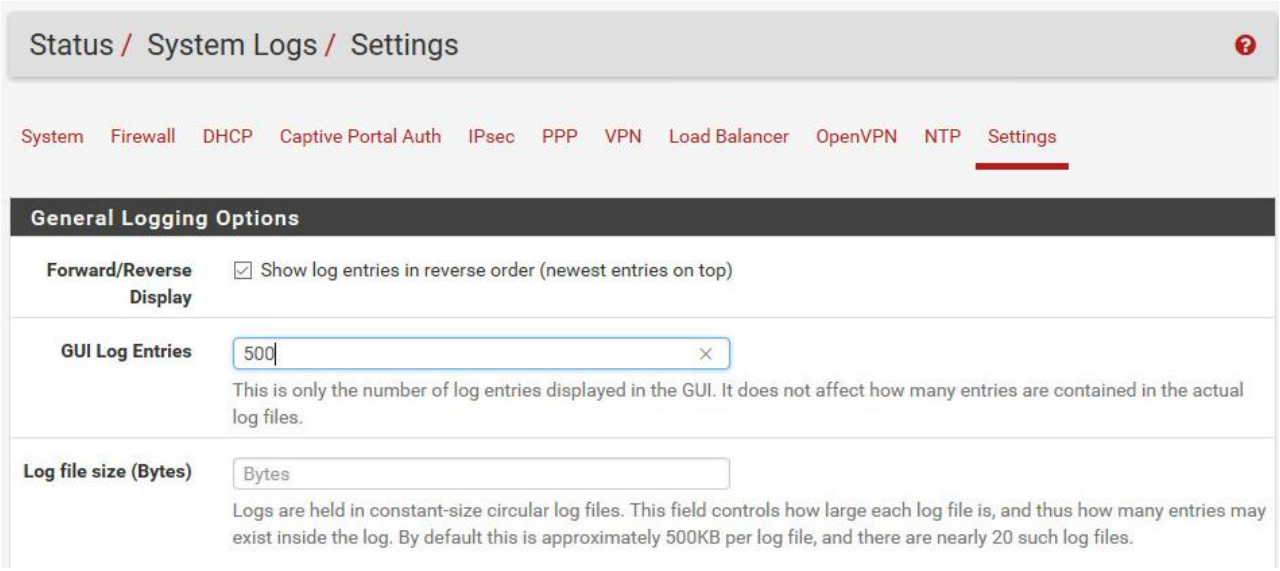
4.4 SSH Dienst

Die pfsense sollte nur intern via ssh zu erreichen sein. Dazu müssen Sie den ssh-Dienst aber erst frei schalten: System -> advanced => Ssh erlauben.
In diesem Zusammenhang macht es Sinn, die „System Console“ mit einem Passwort zu schützen.

4.5 Weitere Services auf einer pfsense

Wer mag kann nun noch SNMP ermöglichen. Ebenso hat die pfsense die Möglichkeit einen Wake-On LAN Dienst zu betreiben. Auch ein DHCP Services ist vorhanden.

4.6 Log Einstellungen



Einstellen der Protokollierung auf der pfsense Firewall

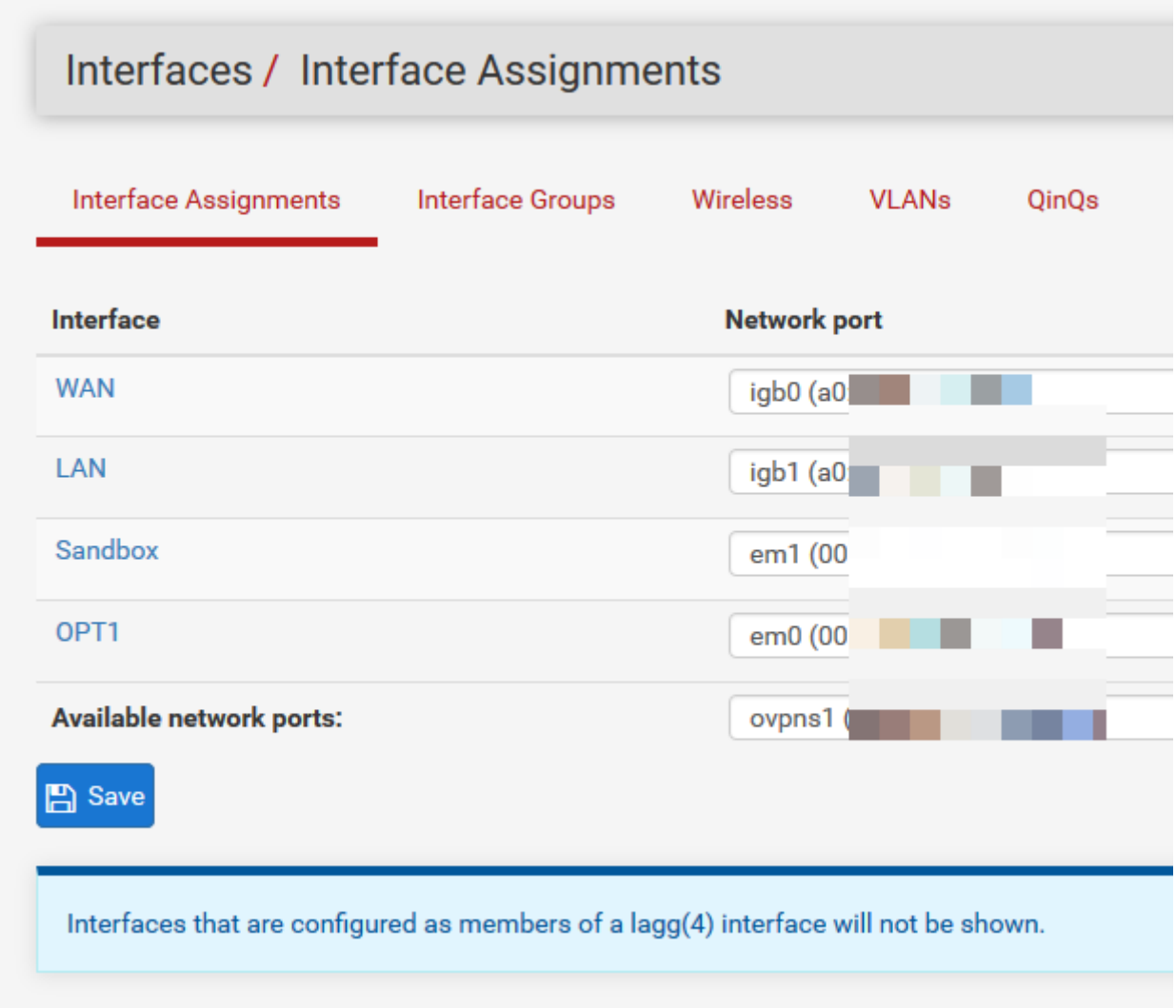
Um später in den Auswertungen und Protokollen der pfsense immer die aktuellen Einträge oben zu haben, setzen Sie unter Status => System Logs => Settings den Haken bei „… show log entries in reverse order“.

5 Weitere Setup-Punkte auf der pfsense Firewall

Hier nur der Reihe nach weitere Einstellungen, die auf einer pfsense möglich sind.

5.1 Weitere Interfaces.

Die pfsense kann weitere Interfaces haben. Bspw. eines für eine DMZ (demilitarisierte Zone) oder für ein WLAN. Sobald die pfsense das Interface als solches erkannt hat, können Sie den Anschluss auch konfigurieren. Sofern im verbauten PC ein WLAN-Chip vorhanden ist, mit dem die pfsense bzw. Free-BSD etwas anfangen kann, so aktivieren Sie diesen unter =>Interfaces => „assign“ => Wireless.
Unter => Interfaces => „assign“ können Sie generell die weiteren Interfaces einem physischen Netzwerk-Anschluss zuweisen.



Zuweisung weiterer Interfaces z.B. für eine DMZ oder das WLAN

Die eigentliche Einrichtung des zusätzlichen Interfaces machen Sie danach unter => Interfaces => „Interface-Name“.

5.2 Weitere IP-Adressen

Für bestimmte Einsatzfälle können weitere externe IP-Adressen interessant sein. Diese werden der pfsense unter => Firewall => Virtual IPs eingetragen und können anschließend genutzt werden.
Einsatzfall: Die Mails an den internen Mail-Server sollen über eine zweite IP-Adresse angenommen werden.

5.3 VLANs

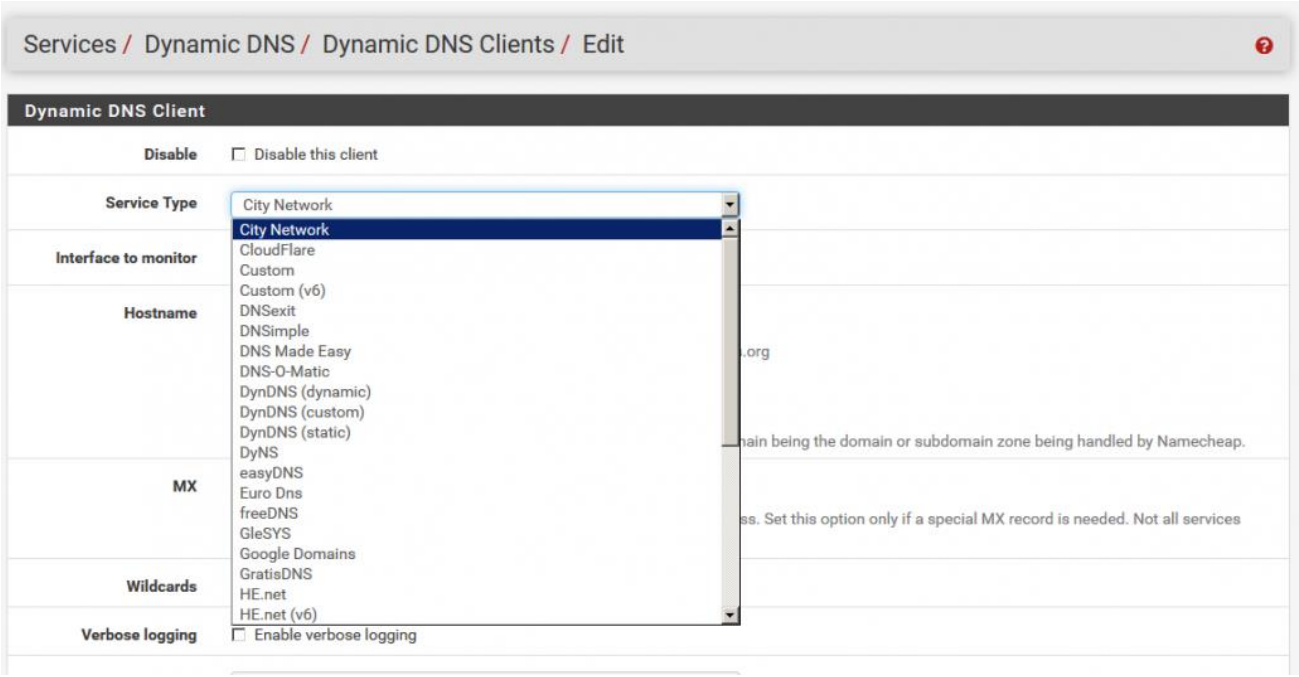
Für den Fall, daß Sie mehr Anschlüsse an der pfsense benötigen als Sie Adapter haben, können Sie VLANs einsetzen. Voraussetzung dafür ist allerdings, daß Sie einen VLAN-fähigen Switch nut-zen und dieser entsprechend konfiguriert ist.

5.4 Carp / pfsync

Sofern man zwei pfsense Firewalls als redundante Lösung einsetzen möchte, so bietet die pfsense auch hier eine entsprechende Funktion an. Dazu benötigen Sie zwei baugleiche Geräte – die in jedem Fall die gleiche Anzahl an Interface-Anschlüssen haben müssen. Damit pfsync funktioniert, benötigt jede Firewall ein weiteres Interface mit dem es sich mit der Nachbar-Firewall austauschen kann. Über dieses Netzwerk wird dann ein so genannter Heartbeat ausgetauscht über den die Firewalls ermitteln welche Firewall im Moment das „führende“ System ist.

5.5 Dynamic DNS / DynDNS & Co

Nur für den Fall, daß die pfsense keine feste (=statische) IP für das WAN-Interface hat: die pfsense kann mit mehreren Dutzend Anbietern von DynDNS Lösungen umgehen. Diese tragen Sie unter => Services => Dynamic DNS ein.



DynDNS Einstellung in der Konfig der pfsense

Die pfsense meldet dann jeweils beim Update des WAN-Interfaces die neue externe IP an den Service-Anbieter (z.B. DynDNS).
Wichtig dabei zu wissen: Ein zuverlässiger Betrieb von Inhouse-Servern, die über das Internet erreichbar sein sollen, ist auf diesem Weg nicht zu erreichen.

5.6 Traffic Shaper

Mit dem Traffic Shaper kann Netzwerk-Verkehr priorisiert werden. Dazu gibt es grob gesagt zwei Einsatzfälle:

5.6.1 Internen Netzwerk-Verkehr nach extern priorisieren.

Der Netzwerkverkehr einiger Geräte soll hoch oder runter priorisiert werden.
Bsp.: Der Traffic der Kinder (im LAN) die ständig auf Youtube Videos schauen soll gegenüber dem restlichen Zugriffen aufs Internet runter priorisiert werden, damit die Eltern

flüssig arbeiten können.
Oder: VoIP-Verkehr wird gegenüber Daten-Verkehr hoch priorisiert.

5.6.2 Verkehr nach extern über mehrere Leitungen priorisieren.

Für den Fall dass an der pfsense mehrere WAN-Anschlüsse vorhanden sind, kann der ausgehende und eingehende Verkehr über eben diese Anschlüsse intelligent verteilt werden.

Für beide Fälle empfiehlt sich die Nutzung des Wizards, mit dem die ersten Regeln für den Netz-werk-Verkehr erstellt werden.

5.7 Virtual Private Network (VPN)

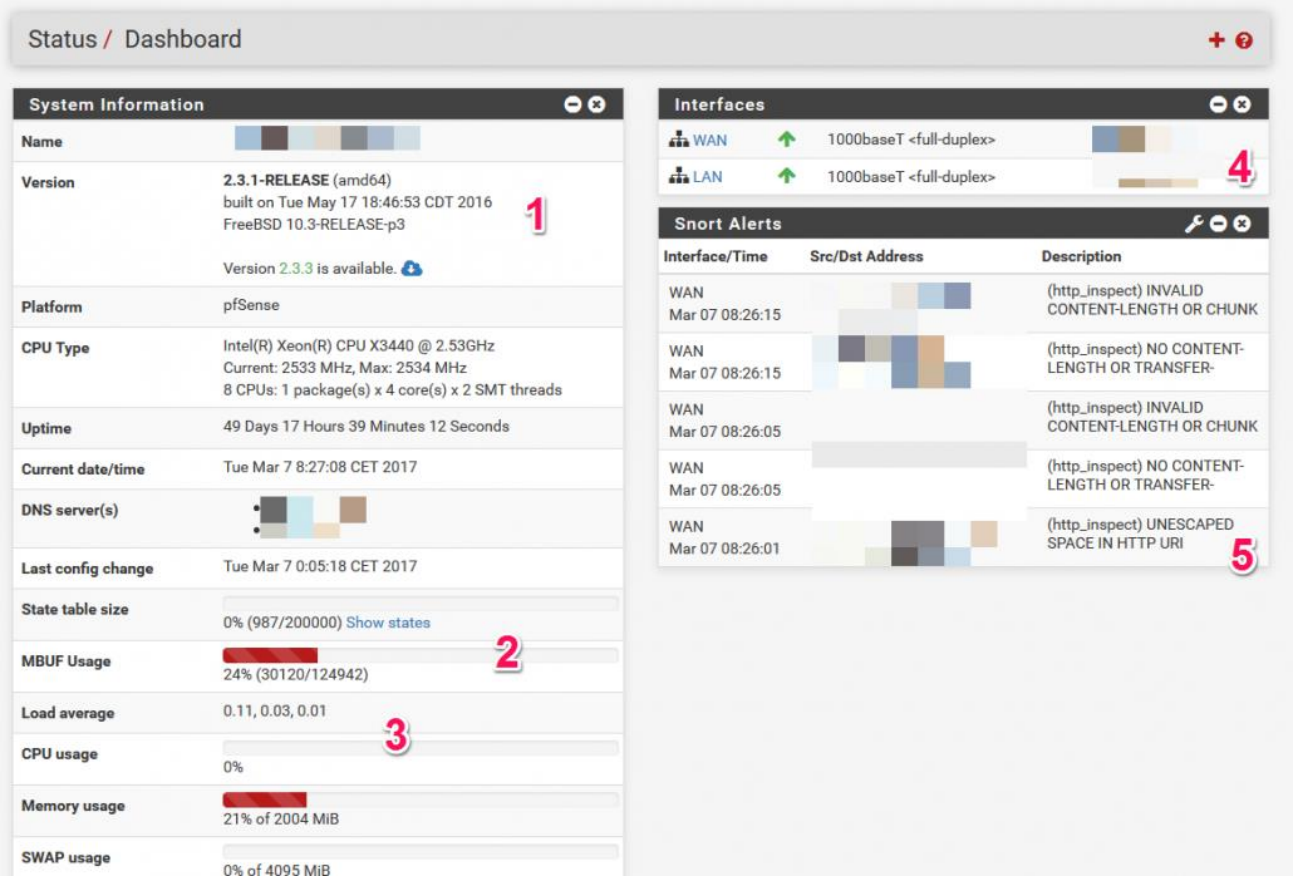
Die pfsense kann mit anderen Firewalls über die folgenden Protokolle verbunden werden:
– IPSEC
– OpenVPN
– L2TP (Layer 2 Tunnel Protokoll)
Wir verwenden bei der Biteno
– IPSEC um Standorte zwischen zwei Firewalls miteinander zu vernetzen
– OpenVPN für die Einwahl von Benutzern.

In begründeten Ausnahmen kann man auch OpenVPN für die Standort-Vernetzung verwenden oder IPsec für die Einwahl von Benutzern.

Die ausführliche Beschreibung eines VPN für Benutzer auf Basis von OpenVPN auf einer pfsense haben wir im Blog des IT Dienstleisters Biteno GmbH schon einmal hier beschrieben.

6 Status / Log-Files / Was tut die pfsense

Die pfsense gibt über eine Art Dashboard direkt nach der Anmeldung in der Weboberfläche bereits einen guten Überblick über den aktuellen Zustand der Firewall:

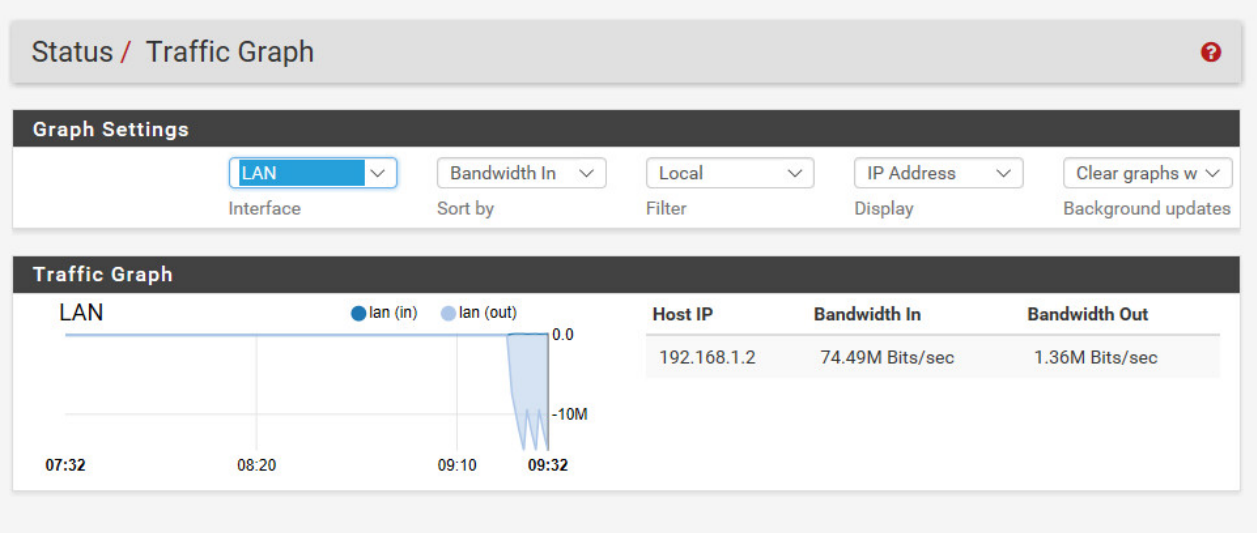


Das Dashboard gibt direkt nach der Anmeldung via Web eine Übersicht über den Status der pfsense

Unter (1) erkennen Sie ob ein neues SW-Release vorhanden ist und installiert werden kann.
Unter (2) und (3) erkennen Sie auf einen Blick wie ausgelastet die pfsense ist.
Rechts oben bei (4) haben Sie alle Interfaces im Blick.
Sofern Sie weitere Software wie etwa Snort installiert haben, sehen Sie dessen letzte Meldungen unter (5).

6.1 Aktuellen Netzwerk Verkehr beobachten

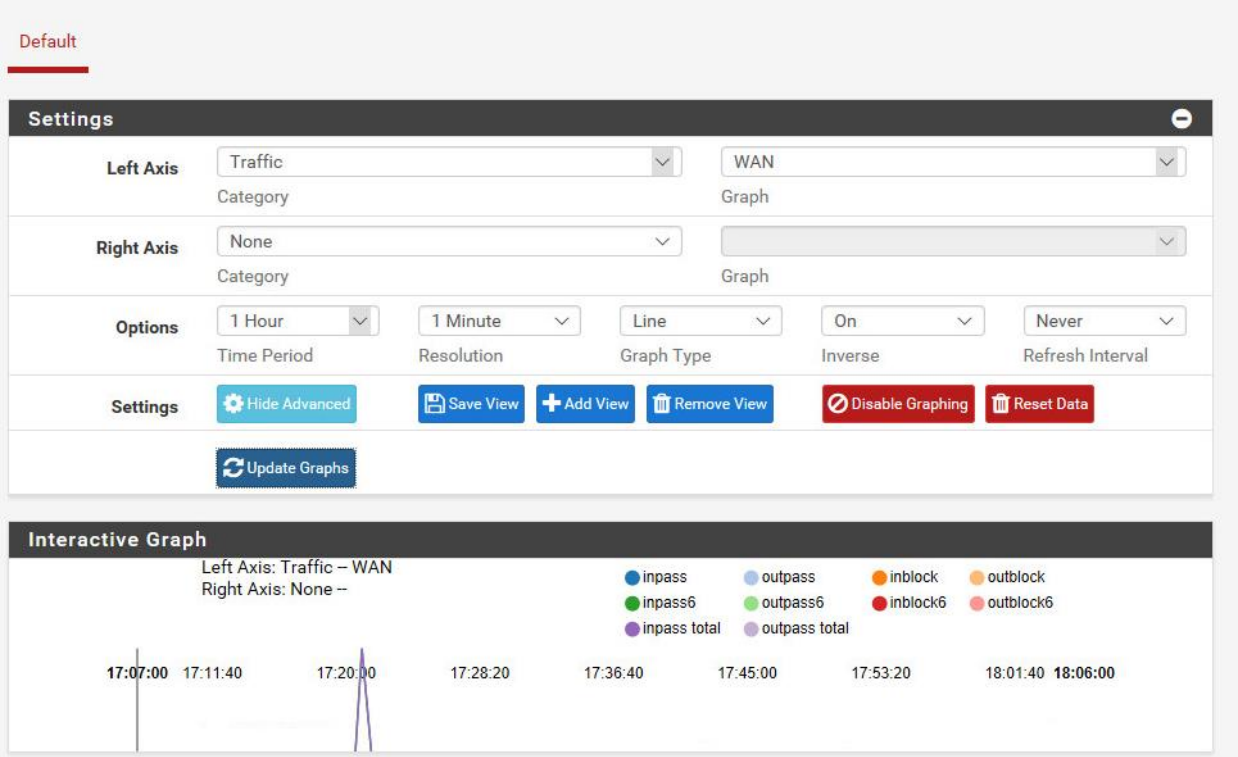
Die aktuelle Auslastung der pfsense sehen Sie unter => Status => Traffic Graph. Hier sehen Sie wer in diesem Moment welche Bandbreite nutzt.



Traffic Graph in der pfsense

6.2 Historische Verbrauchs / Traffic-Daten

Um die vergangene Auslastung der pfsense einzusehen gab es in der Version 1.x unter => Status => RRD Graphs eine Darstellung des vergangener Auslastung der Interfaces. Seit der Version 2.x der pfsense ist das Tool etwas versteckt. Sie finden es nun unter => Status => Monitoring.



Historische Traffic-Darstellung (ehemals RRD Graph)

Dort müssen Sie allerdings oben links „left axis“ zuerst „Traffic“ im Drop-Down Menü auswählen.
Danach können Sie unter „Time Period“ die gewünschte Dauer einstellen.

7 Weitere Regeln für die Firewall

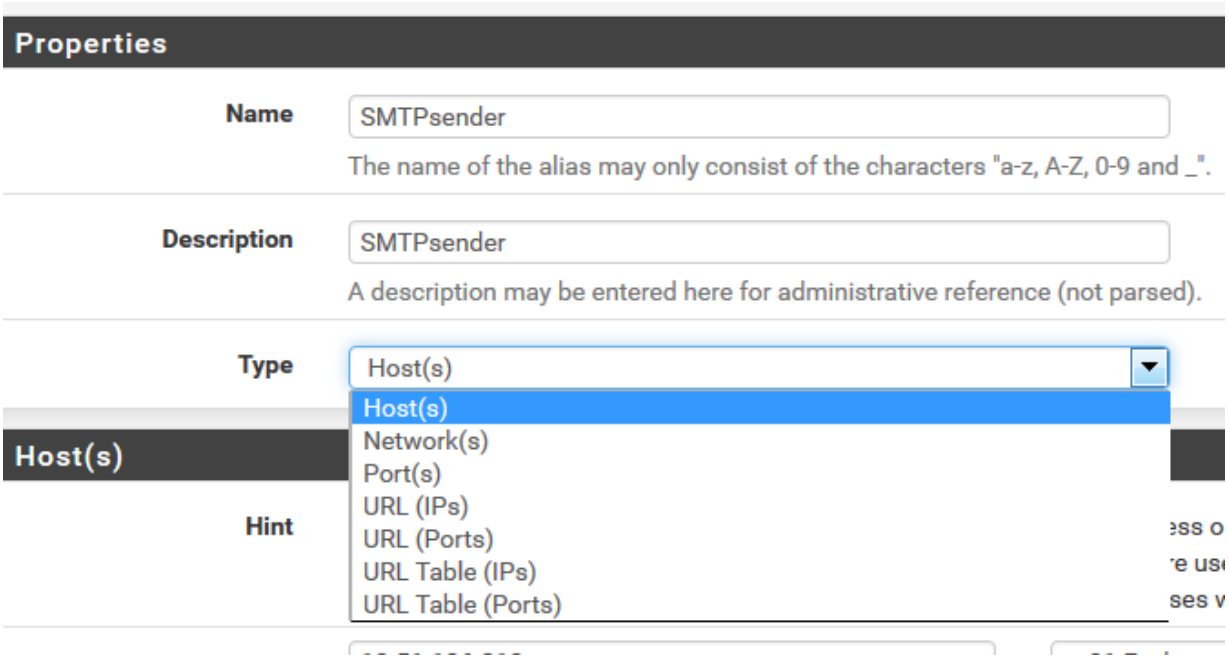
In den meisten Fällen möchten Sie den vorhandenen Regel-Satz für den Netzwerk-Verkehr auf der pfsense abändern.
Egal ob Sie von bestimmten PCs aus nur eingeschränkte Internet-Nutzung erlauben wollen, oder Mails von außen nach innen durchlassen möchten. Sie müssen dazu entweder eine neue Regel anlegen oder eine bestehende Regel verändern.

7.1 Ein gut gemeinter Rat zur Verwaltung von Regeln auf der Firewall

Wiederstehen Sie bitte unbedingt der Versuchung direkt in einzelne Firewall-Regeln direkt IP-Adressen einzutragen. Auf Dauer werden Sie mit wachsender Anzahl von Regeln ihr eigenes Re-gelwerk nicht mehr durchschauen. Nutzen Sie unbedingt Aliases für die Gruppierung von Hosts, Netzen oder einzelnen Ports.

7.2 Alias-Liste anlegen

Bevor Sie Regeln auf einer pfsense erstellen, sollten Sie sich kurz die Sektion Firewall => Aliases anschauen. Hier können Sie beliebige Gruppen (Aliase) bilden. Eine Gruppe kann dabei aus Hosts-Einträgen (in der Regel IP-Adressen), ganzen Netzwerken oder einzelnen TCP-Ports bestehen.
Legen Sie als Beispiel einmal eine neue Gruppe mit dem Namen SMTPSender an.



Einen Alias anlegen auf der Firewall

Sie müssen dazu lediglich einen möglichst sprechenden Namen wählen und die Art (Type) der Liste. Wählen Sie hier „Host(s)“ aus.

Fügen Sie der Liste nun einzelne Server oder Endgeräte zu, die Mails versenden dürfen. Das ist im Zweifel der eigene Exchange-Server – einzelne PCs (die das wirklich brauchen) und etwa der Multifunktions-Scanner der Scan-2-Email beherrscht.
Speichern Sie die Alias-Liste nun ab.

7.3 Ausgehenden SMTP Verkehr einschränken

Eine der größten Gefahren ist nach wie vor der unbemerkte Versand von Mail von infizierten PCs aus. Diese Gefahr kann man mit der pfsense aber sehr einfach eindämmen.
Als erstes Klicken Sie auf Firewall => Rules => Reiter „LAN“ und dann auf „Add“

Unter (1) haben Sie die Möglichkeit Netzwerk-Verkehr zu blockieren oder durchzulassen. Im Bild oben wir der Traffic blockiert. Weiter unten bei (2) stellen Sie das Interface ein, auf das sich die Regel bezieht und bei (3) das Netzwerk-Protokoll.
Weiter unten im Bereich Source können Sie nun einstellen, wer etwas darf oder eben auch nicht.
Im obigen Beispiel unterbinden wir bei (1) zunächst allen Traffic von intern nach extern der als Quelle (Source Port Range) SMTP – also E-Mail – aufweist.
Mit dem Haken bei „invert match“ (4) erlauben wir aber ausgesuchten Hosts, die rechts bei (5) mit SMTPSender angegeben sind, dennoch Mails zu senden.

Mit dieser Regel erlauben wir also nur ausgesuchten Einträgen der Alias-Liste „SMTPSender“ Mails auf Port 25 nach extern zu senden. Mit dieser einfachen Regel können wir sicher stellen, daß ein mit Schadcode oder einem Computer-Virus infizierter PC nicht direkt per SMTP-Protokoll Teil eines Bot-Netzwerks wird.

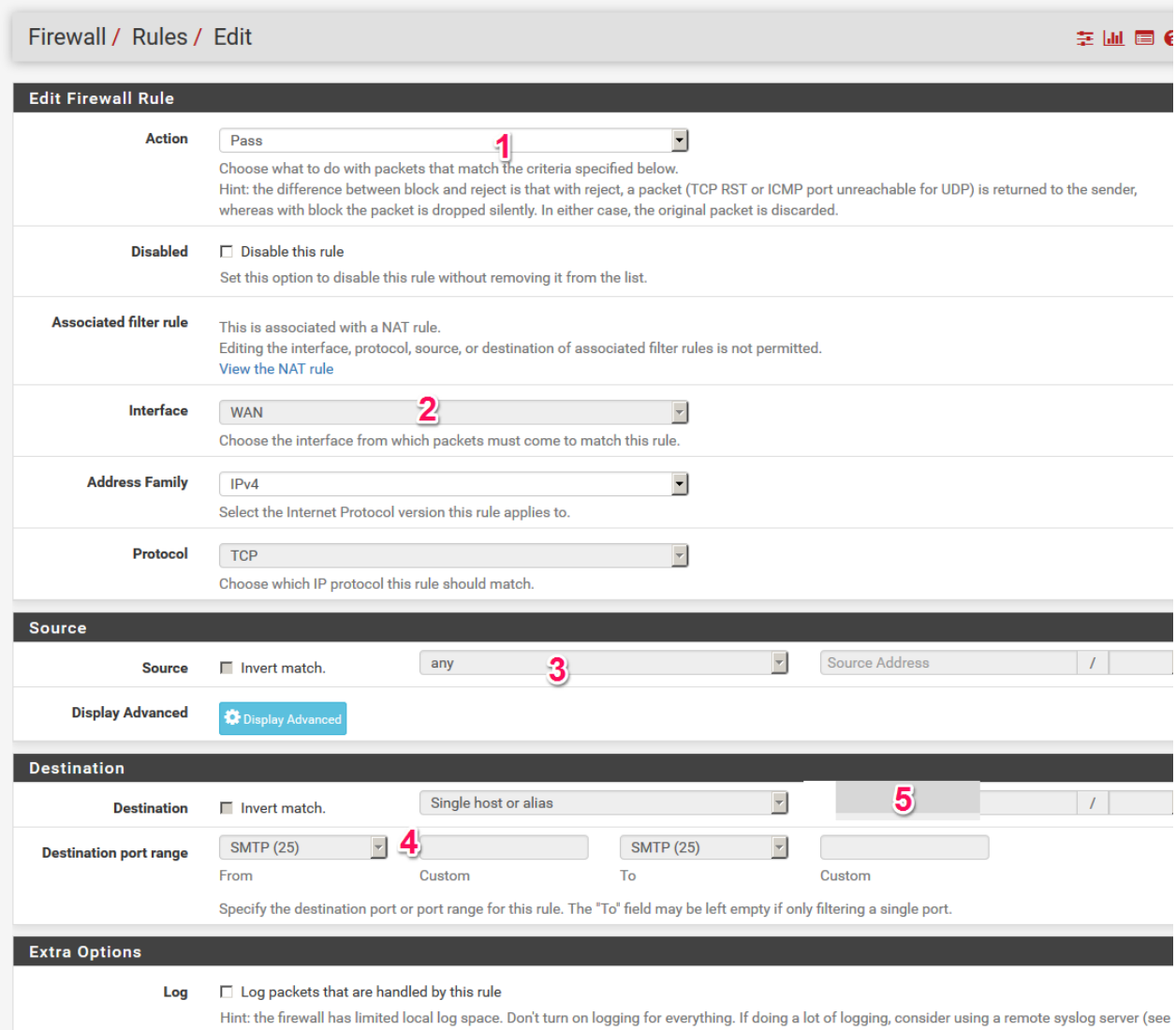
7.4 Emails ins Netz lassen

In vielen Fällen betreiben Kunden in ihren lokalen Netzen einen Mail-Server. Egal ob das auf einem Small Business-Server oder mit einem MS-Exchange Server realisiert wird: Dieser Server muss Mails senden können und auf spezifischen Ports mit der Außenwelt kommunizieren können.

Um das zu realisieren, benötigen wir zwei Dinge:
– Die Weiterleitung von Netzwerk-Traffic auf die interne IP des Mailservers
– Eine Regel, die diesen Traffic auch erlaubt.

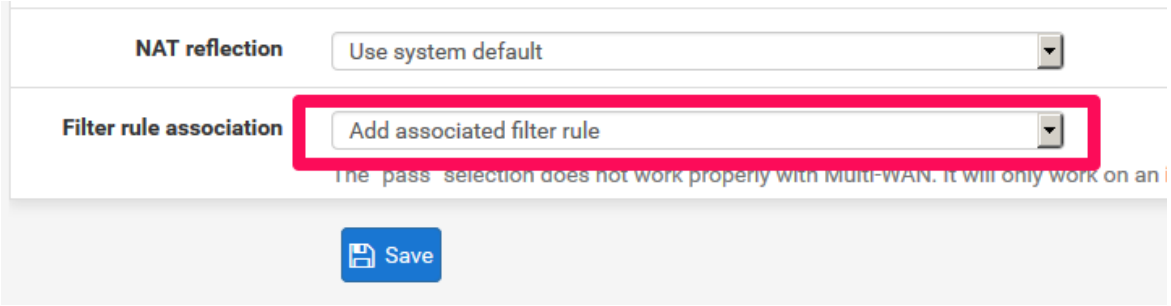
7.4.1 Weiter-Leitung von eingehendem Traffic

Die Weiterleitung von Traffic wird unter => • Firewall => NAT => Port Forward eingerichtet. Klicken Sie auf „Add“.



Eine Weiterleitungs-Regel auf der pfsense einrichten

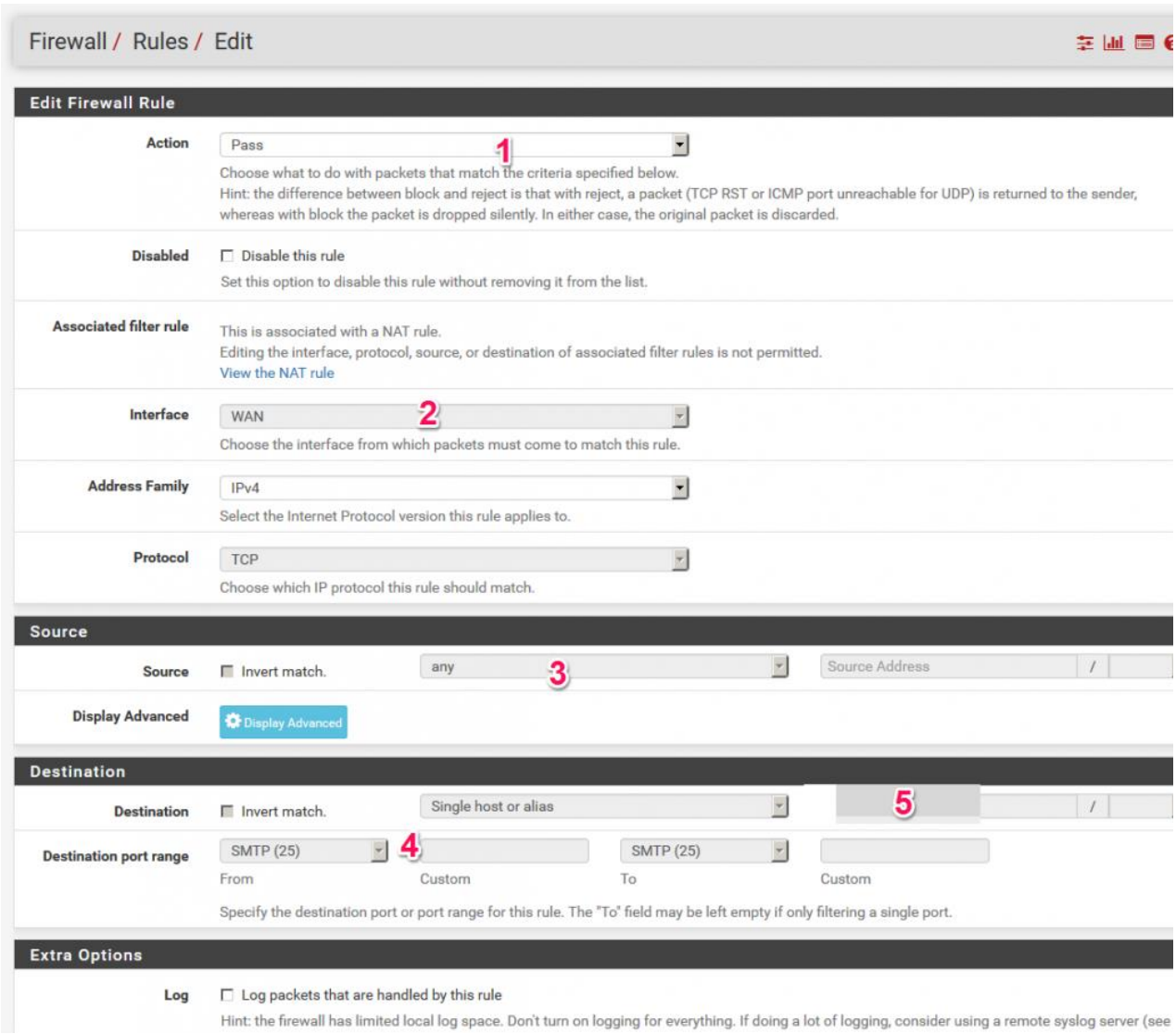
Unter (1) wählen Sie den Neztwerkanschluss auf dem der Netzwerkverkehr von außen ankommt. Das ist im Zweifel „WAN“. Sofern Sie lediglich eine WAN-IP-Adresse haben steht unter (2) „WAN Address“. Beim Einsatz von mehreren IP-Adressen auf dem WAN Internface müssen Sie hier die richtige IP auswählen.
Unter (3) und (5) legen Sie den Port bzw. den Portbereich fest, dessen Verkehr weiter geleitet werden soll. In unserem Beispiel ist das Port 25 (also SMTP).
Im Feld „redirect target IP“ (4) legen Sie die interne IP-Adresse fest an die der Netzwerk-Verkehr gesendet werden soll.
Tipp: Sie können in jedem Feld in das Sie eine IP-Adresse eintragen können auch einen Alias verwenden, den Sie vorher unter => Firewall => Alias angelegt haben.



Wenn Sie im letzten Feld den Eintrag bei „Filter rule association“ so lassen wie abgebildet, so wird von der pfsense die für das Port-Forwarding notwendige Regel gleich mit erstellt.

7.4.2 Erlauben des Traffic

Wie schon erwähnt, benötigt das Port-Forwarding eine eigene Regel, die den Traffic erlaubt. Das ist insofern „logisch“ da die Standard-Regel für eingehenden Verkehr auf „block“ steht. D.h. nichts kommt rein. Daher müssen Sie entweder die Regel beim Port-Forwarding mit erstellen lassen oder nachher selbst von Hand anlegen.



Die für den SMTP-Verkehr notwendige Regel

Die für unser Beispiel notwendige Regel zum Weiterleiten von SMTP-Traffic sieht dann z.B. so aus: Unter (1) ist definiert, daß der nachfolgend beschriebene Verkehr durchgelassen wird („pass“).
Unter (2) definieren Sie wieder das Interface, auf dem der Traffic auf die pfsense trifft – hier „WAN“. Unter (3) könnten Sie die Herkunft noch einschränken, was in unserem Fall aber wenig Sinn macht. Bei „destination port range“ (4) wählen wir wieder bewußt nur „SMTP“ also Port 25 aus. Unter (5) „Destination“ muss dann wieder die IP-Adresse oder der Alias des Mail-Servers stehen.

Lesetipp: Wie Sie Microsoft Exchange (Version 2010) auf Windows Server R2 richtig installieren.

8 Software auf der pfsense installieren

Grundsätzlich gilt: Auf einer Firewall sollte nur Software laufen, die zum Betrieb der Firewall not-wendig ist. Sonst nichts.

Auf die pfsense Firewall können unterschiedliche Software-Pakete aus dem Repository von pfsen-se installiert werden. So kann die pfsense etwa um einen Web-Proxy wie squid oder ein Intrusion-Preventions System wie snort erweitert werden.

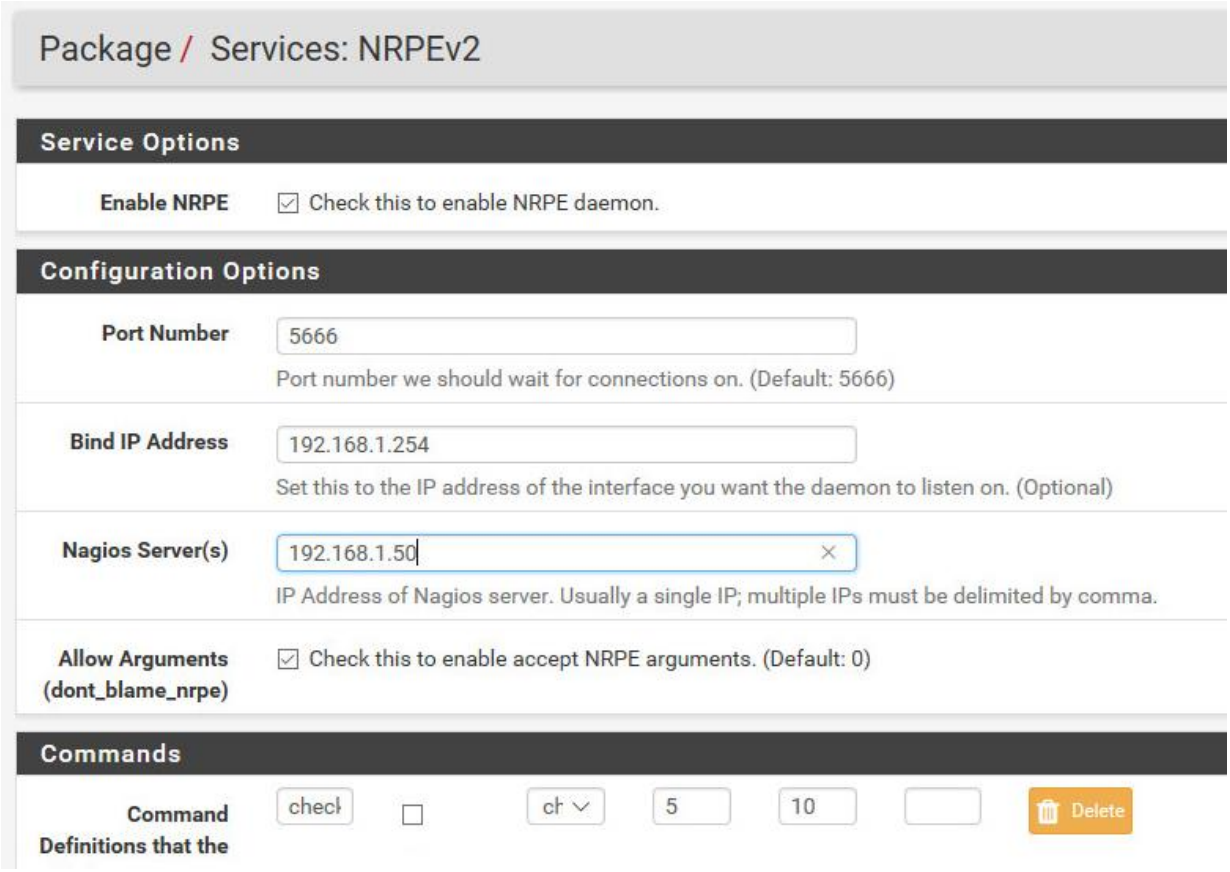
8.1 Open-VM Tools

Sofern die pfsense virtuell auf VMWare läuft: Open-VM-Tools verbessern die Performance der pfsense unter VMWare und ermöglichen es einen kontrollierten Shutdown der virtuellen pfsense vom vSphere Client aus.

8.2 NRPE

Der Nagios Remote Plugin Executor ist dann hilfreich, wenn im Monitoring der Status der pfsense Firewall abgefragt werden soll. NRPE läßt sich sowohl in Nagios als auch in Icinga(2) Umhgebun-gen nuzten.

Die Installation ist einfach: Paket nrpe suchen und installieren.
Wichtig: Anschließend muss NRPE konfiguriert werden, so daß möglichst nur der Monitoring-Server (namentlich per IP) auf die NRPE Installation auf der pfsense zugreifen kann.
Services => NRPE2



Das NRPE Plugin auf der pfsense richtig konfigurieren

Wichtig hier: Bindung nur an die LAN Adresse und immer (den richtigen) Monitoring Server ange-ben. Das kann Nagios, Icinga oder Icinga2 (Satellit oder Master) sein.

8.3 OpenVPN Client Export

Wer später die pfsense zur Einwahl mit OpenVPN nutzen möchte, wird das Paket „openvpn-Client-export“ installieren wollen. Damit ist es sehr bequem und einfach den Remote-Benutzern ihre VPN Konfiguration und Zugangs-Informationen zukommen zu lassen.

8.4 pfBlockNG

Seit der Version 2.2.x kann die pfsense Firewall um eine Software namens pfBlockNG (NG steht für next generation) erweitert werden. Im Wesentlichen lädt die SW Listen von geographischen IP-Bereichen herunter. Auf Basis dieser alle paar Stunden aktualisierten Listen können dann Regeln erstellt werden, um bspw. bestimmte IP-Adress-Bereiche bestimmter Regionen grundsätzlich aus-zusperren.
Kurzübersicht mit Version 2.2.x https://www.youtube.com/watch?v=6rjbTxKsoBE
Tutorial zur Einrichtung unter 2.3.x https://www.youtube.com/watch?v=M81kFLEhhZQ

8.5 Squid

Squid ist ein Web-Proxy. D.h. er übernimmt die Aufgabe Webseiten aus dem Internet zu cachen und kann als Reverse-Proxy genutzt werden.
Vorteil: Mehrfach-Downloads werden vermieden. Dazu müssen aber alle Benutzer im lokalen

Netz den Web-Proxy nutzen.
Aber Achtung: Der Squid speichert viel und oft auf der lokalen Festplatte der pfsense. Den Squid sollte man nur einsetzen, wenn auf der pfsense Firewall echte Platten verbaut wurden.
Nach der Installation muss der Squid Proxy konfiguriert werden. Das ist in 1-2 Minuten erledigt.
Services -> Squid
Schritt 1: Local Cache festlgen , d.h. wo und wie speichert der squid die Dateien
Schritt 2: (Tab General): Squid enablen
In der Regel wird man der Einfachheit halber den transparent mode des Squid einschalten. Dabei schaltet sich der squid zwischen den Browser des Nutzers und den Web-Server der abgefragt wird. Der Benutzer merkt davon nichts.

8.6 SquidGuard

Hier kann ein Inhaltsfilter für den Zugriff auf Webseiten eingebaut werden. Damit können dann bspw. Zugriffe auf nicht erlaubte oder nicht gewollte Inhalte unterbunden werden.

8.7 Snort auf pfsense

Snort ist ein Intrusion Detection bzw. Intrusion Prevention System. Snort ist (wie pfsense und squid auch) Opensource und kann sowohl auf einer pfsense als auch auf anderen Plattformen eingesetzt werden. Zu Snort sind weiter reichende Einstellungen auf der pfsense notwendig, so daß wir dazu eine separate Anleitung erstellen.

9 Pfsense aktualisieren / Upgrade

Die pfsense zu aktualisieren ist innerhalb der 2.3.x Reihe kein Problem. Von 2.3.1 ist der Upgrade auf 2.3.x per Web-GUI möglich. Der Update von einer alten Version 1.2.x auf 2.x sollte vorher ge-testet werden.

10 Downloads / Links

Pfsense Download: https://www.pfsense.org/download/
Pfsense Docu: https://doc.pfsense.org/index.php/Main_Page
Pfsense Forum: https://forum.pfsense.org/

Das Buch zu pfsense ist zwar schon aus dem Jahr 2009 und bezieht sich auf die 1.2er Version. Da die Konzepte darin aber grundsätzlich noch richtig sind, lohnt auch hier ein Blick hinein.
https://www.amazon.de/Pfsense-Definitive-Christopher-M-Buechler/dp/0979034280

Falls Sie bis hierhin noch nicht von der pfsense überzeugt sind, finden Sie auf Wikipedia eine Liste aller bekannten Firewall-Distributionen

https://en.wikipedia.org/wiki/List_of_router_and_firewall_distributions