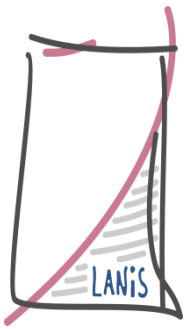
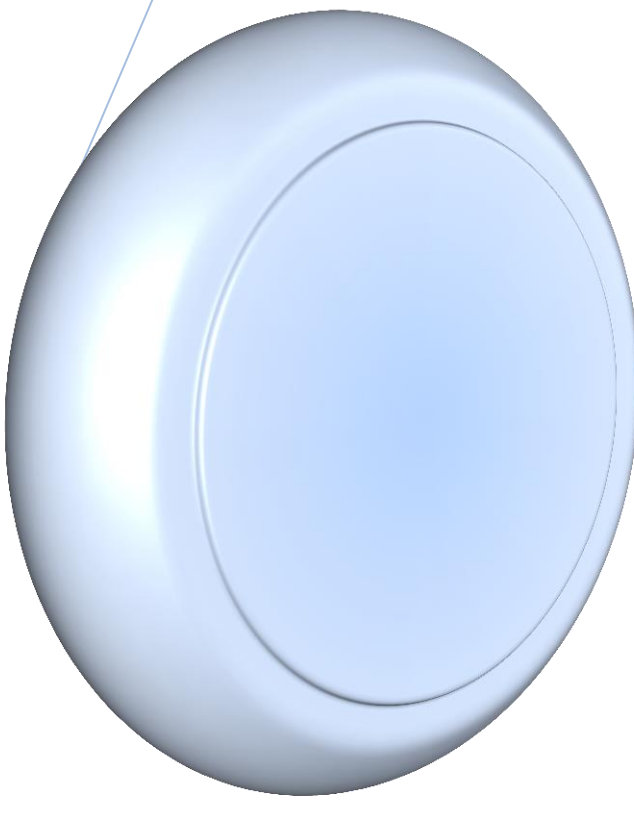


Open-Source-Firewall und –Router pfSense in schulischen Umgebungen einsetzen

Hessische Lehrkräfteakademie, Dezernat Medienbildung, Support-Center für pädagogische IT

Vorstellung und Installationsanleitung der pfSense-Firewall- und -Captive-Portal-Lösung für Netzwerke, um schuleigene mobile oder auch schulfremde Geräte (BYOD) sicher im pädagogischen Netzwerk einsetzen zu können

Christian Mehler
03.12.2015



Inhalt

Version der pfSense

Diese Anleitung basiert auf der pfSense-Version 2.1.5. Bei folgenden Versionen können sich die Angaben und Einstellungen ändern.

Installation von pfSense

Die folgende Anleitung soll zum einfachen Installieren von pfSense in einer schulischen Umgebung dienen. Bitte beachten Sie dabei, dass je nach Aufbau der Infrastruktur der Schule verschiedene Szenarien unterschieden und Einstellungen unterschiedlich eingerichtet werden müssen. Dazu kann Ihnen diese Anleitung nur Vorschläge machen, die sie auf die jeweiligen Gegebenheiten hin überprüfen müssen.

Vorabinformationen

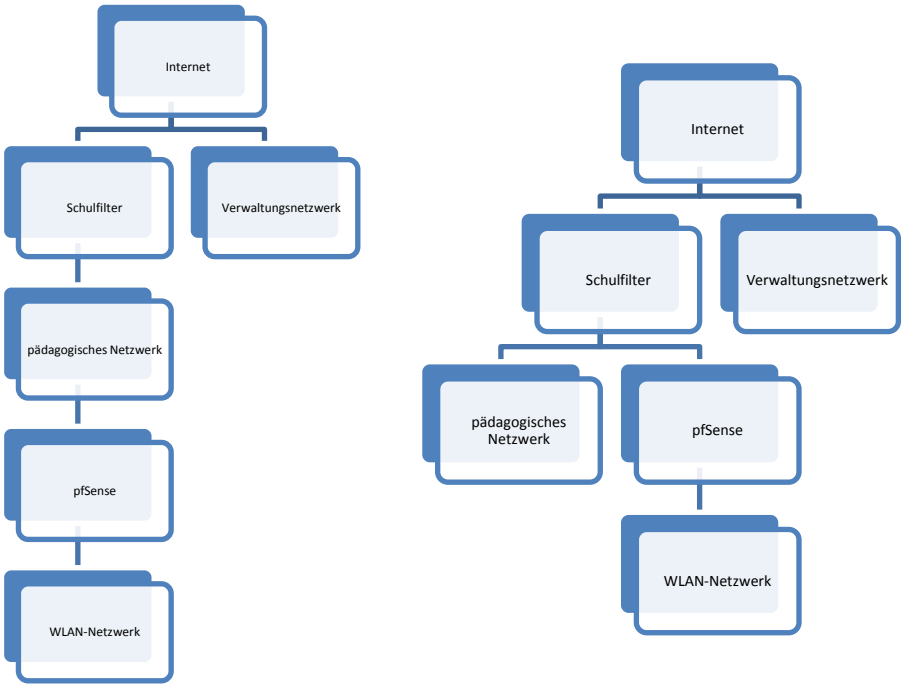
pfSense-Boxen

Hardware mit installiertem pfSense können Sie bspw. unter http://varia-store.com bekommen (Kategorie „Systeme mit Software“, Unterkategorie „pfSense“). Bitte achten Sie darauf, dass ab pfSense 2.2 mindestens 512 MB RAM vorhanden sein sollten.

Alternativ können Sie auch einen alten Rechner nehmen, in den Sie drei Netzwerkkarten einbauen und pfSense darauf selbst installieren oder direkt pfSense als VM nutzen (downloadbar unter http://www.pfsense.com/).

Einsatz von pfSense mit eigenem Internetfilter

Wenn Sie bereits einen eigenen Internetfilter betreiben, so bieten sich die beiden folgenden Anbindungsarten an. Bei der linken Einbettung können Sie den WLAN-Geräten Zugriff auf Bereiche im pädagogischen Netzwerk bieten. Im rechten Bereich ist dies nicht möglich, da die pfSense direkt mit dem Schulfilter verbunden ist. Beide Möglichkeiten bieten Vor- und Nachteile. Sie müssen sich dabei nicht zwingend jetzt entscheiden. Mit wenigen Veränderungen können Sie zwischen diesen beiden Einbindungsarten wechseln (Netzwerkkabel umstecken und LAN-Adresse ändern).

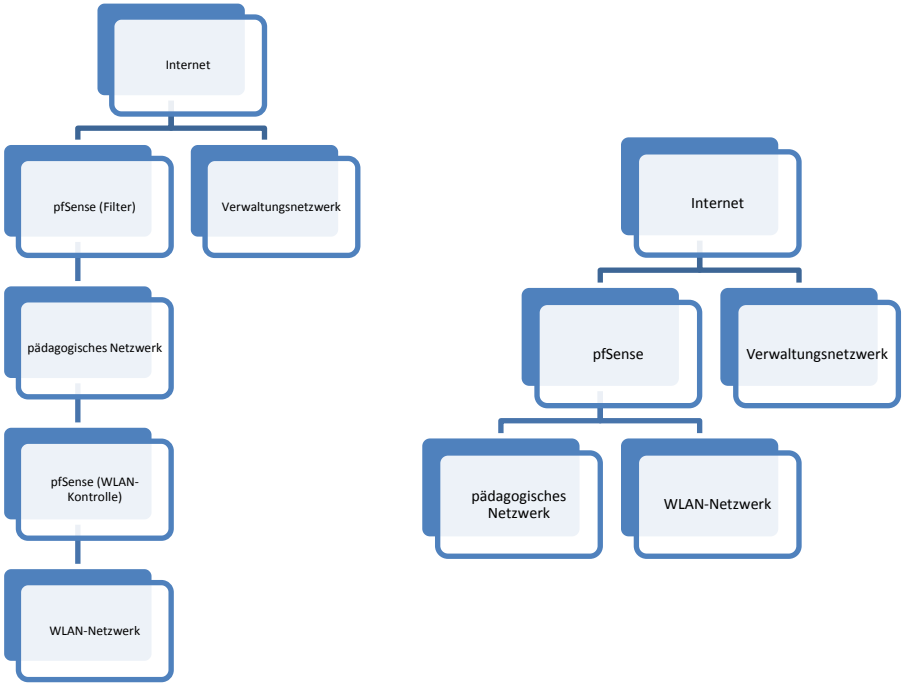


Einsatz von pfSense ohne eigenen Internetfilter

Sollten Sie bisher keinen Internetfilter einsetzen, so können Sie pfSense auch als Internetfilter einrichten. Die Einrichtung als Internetfilter wird im Dokument „pfSense als Internetfilter“ erläutert. Führen Sie bitte vorher die Installation gemäß diesem Dokument durch.

Auch hierbei gibt es zwei Möglichkeiten, wie man pfSense einbinden kann. Im linken Schaubild gewährt man allen Geräten des WLAN-Netzwerkes Zugriff auf das pädagogische Netzwerk. Man benötigt dazu nicht zwei pfSense-Boxen, sondern es müssen die zwei Komponenten aus einer pfSense für die schematische Darstellung gesondert betrachtet werden. Bei der Installation einer pfSense ist dieses Ergebnis der voreingestellte Fall.

Alternativ kann man auch hierbei wiederum den Zugriff auf das pädagogische Netzwerk verbieten. Dies kann man durch das Hinzufügen von Routing-Rules im pfSense erreichen.



Zurücksetzen der Einstellungen

Falls Sie eine pfSense-Hardware-Box gekauft haben und nichts mehr geht, so können Sie diese sehr einfach auf die Voreinstellungen zurücksetzen. Dazu die Box vom Strom trennen und den Resetknopf im Resetloch an der Vorderseite mit bspw. einer Büroklammer drücken. Strom einschalten und bis die Lampen vorne „tanzen“ gedrückt halten. Dieses Vorgehen wurde mit pfSense 2.14 geändert und funktioniert aktuell nicht mehr zuverlässig.

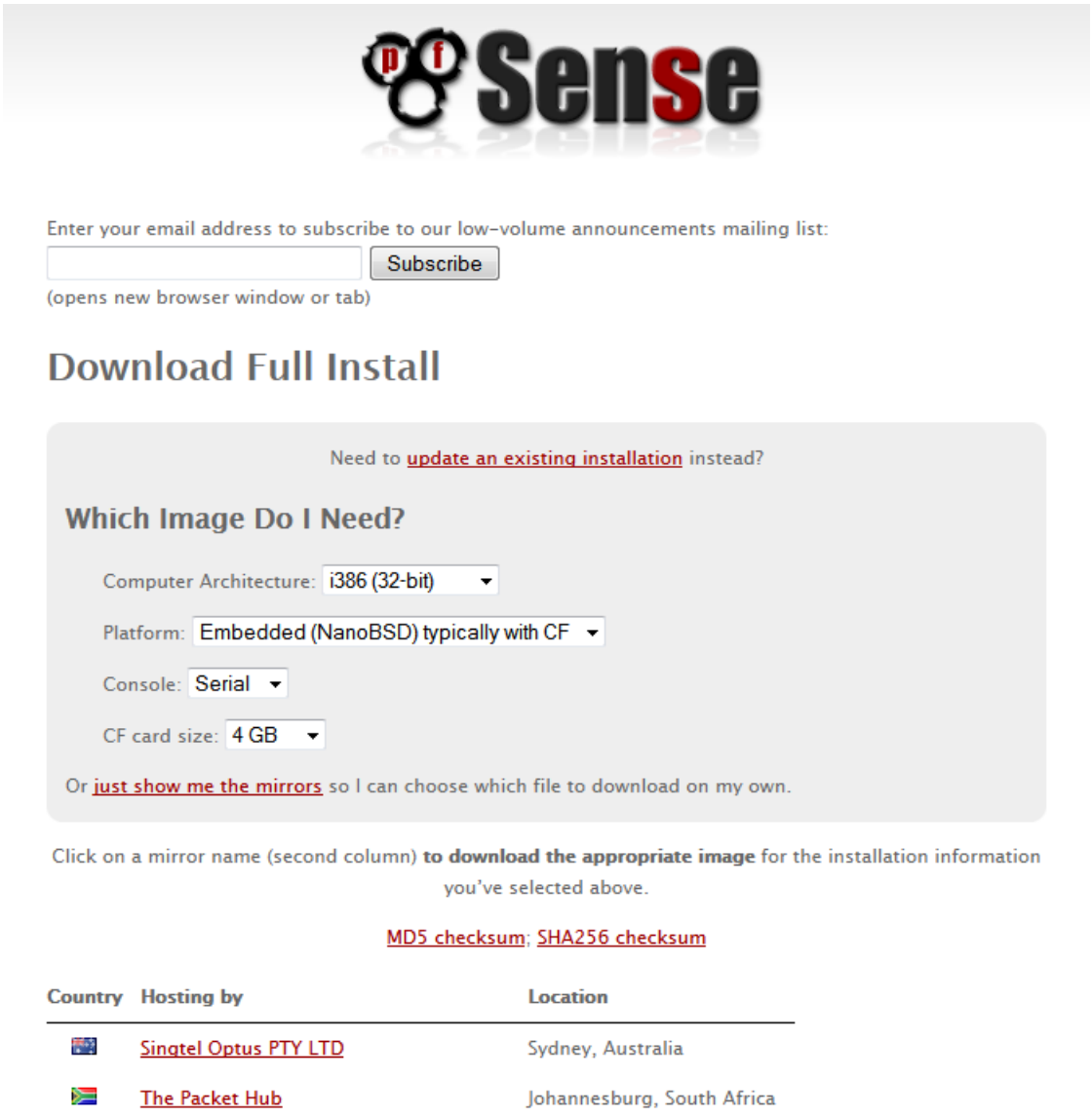
Zurücksetzen der Einstellungen II

Wenn der einfache Druck auf den Resetknopf nicht mehr hilft, so bleibt nur das Überschreiben der CF-Card mit einem neuen Image.

Möglichkeit 1: Originalimage

Dazu unter https://www.pfsense.org/download/mirror.php?section=downloads das passende Image auswählen und nach der Anweisung von *https://doc.pfsense.org/index.php/HOWTO_Install_pfSense#Embedded* mit Hilfe eines anderen Rechners die CF-Card überschreiben. Für die aktuell verwendeten ALIX.2D13-Hardware (mit 4GB CF-

Karte) des pfSense ergibt sich die folgende Image-Auswahl.



Für die „APU-1D Board"-Geräte muss hingegen in der ersten Auswahl „Computer Architecture" „AMD64" ausgewählt werden (bei größerer als 4GB-Karte trotzdem 4GB auswählen).

Das Image von dort herunterladen und einmal entpacken. Anschließend gemäß der Anleitung physdiskwrite herunterladen (die +PhysGUI-Version enthält eine grafische Oberfläche und ist daher einfacher in der Bedienung) und ebenso entpacken. Dann PhysGUI.exe *als Administrator* starten und weiter der Anleitung folgen.

Seit pfSense 2.2 muss man die LAN-Ports per seriellem Kabel manuell zuweisen. Das klappt nicht über ein Netzwerkkabel, sondern nur über ein serielles Kabel. Eine Anleitung dazu findet sich unter http://wiki.butzhammer.de/Alix-Board_mit_pfSense_CF_Karte_einrichten

Möglichkeit 2: Rident

Sollte man über kein passendes Kabel verfügen, bietet es sich an zuerst Rident (pfSense-Variation mit bereits zugewiesenen Netzwerk-Ports) zu installieren. Dieses wird ebenso mit physdiskwrite gemäß obiger Anleitung – nur mit dem passenden Image von http://www.yawarra.com.au/support/operating-system-images/#rident – auf die Karte kopiert. An-

schließend dann per Update sofort wieder zu pfSense wechseln, um die aktuellsten Updates nutzen zu können. Eine entsprechende Anleitung findet sich unter http://www.yawarra.com.au/tutorials/switch-from-rident-to-pfsense/ im Bereich „Option 1: Do a manual „Update““.

Möglichkeit 3: Aus den LANiS-Downloads

Auch wir bieten mittlerweile den Download eines pfSense-Images an, bei dem der Config- und der Wan-Port bereits zugewiesen sind. Dadurch kann man dies sehr schnell auf eine Speicherkarte überspielen und nutzen. Auf die Karten wird das Image mit Hilfe von physdiskwrite geschrieben (die +PhysGUI-Version enthält eine grafische Oberfläche und ist daher einfacher in der Bedienung). Dies wird bei Möglichkeit 1 bereits beschrieben.

Die Images werden nur sporadisch aktualisiert, können aber direkt über die Update-Funktion der pfSense auf eine neue Version gehoben werden, bei der alle Einstellungen erhalten bleiben.

Um die folgenden Links nutzen zu können, muss man einen Account für das LANiS-Schulportal haben und dort als Tooladmin für die Downloads eingetragen sein.

- pfSense 2.2.5 i386 nanobsd 4gb: https://portal.lanis-system.de/lanis-downloads.php?d=50001
- pfSense 2.2.5 amd nanobsd 8gb: https://portal.lanis-system.de/lanis-downloads.php?d=50002

Die LANiS-Images sind bereits vorkonfiguriert, so dass man direkt mit dem Schritt „Belegung der Netzwerkkarten“ starten muss.

Wichtiger Hinweis: Sicherungen erstellen

Da man sich durch falsche Konfigurationen vom pfSense komplett ausschließen kann, ist es wichtig unter dem Menüpunkt „Diagnostics“ den Punkt „Backup/Restore“ zu nutzen. Dort kann man eine Sicherung der aktuellen Konfiguration durchführen und lokal speichern. Nach dem Zurücksetzen der Einstellungen kann man unter „Diagnostics“ „Backup/Restore“ die gespeicherten Einstellungen wieder laden. Dabei startet pfSense neu und lädt auch ggf. installierte Erweiterungen (bei vorhandener Online-Verbindung) wieder herunter.

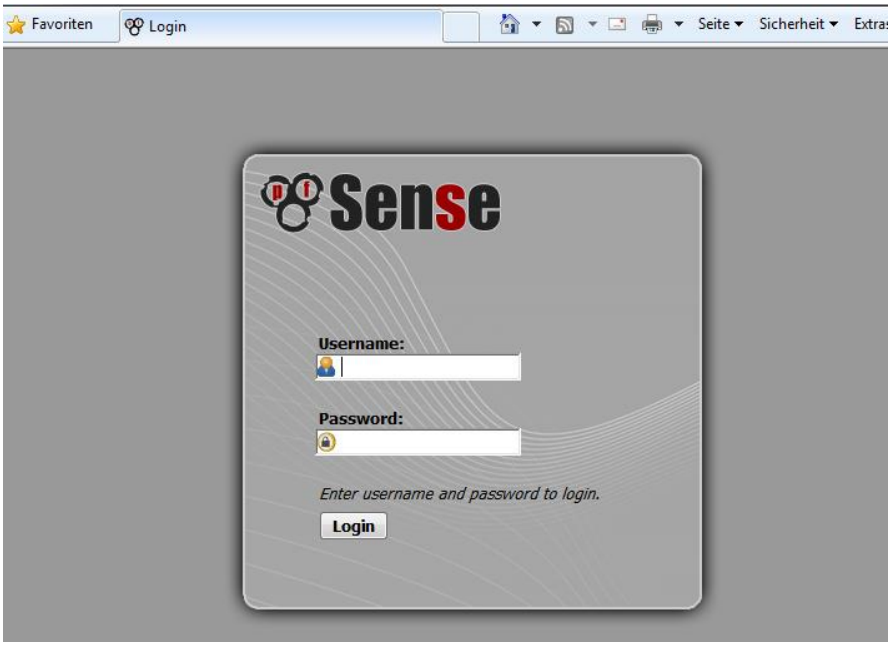
Sicherung der Speicherkarte

Nachdem pfSense vollständig installiert ist, kann man das Kartenimage ziehen und ebenso speichern. Oder schon auf einer Ersatzkarte für Notfälle bereithalten. Dazu eignet sich bspw. die Tools unter http://hddguru.com/software/HDD-Raw-Copy-Tool/ oder http://download.securepoint.de/?d=imagingtool/v2.3

Installation

Verbindung herstellen

- Box mit Netzwerkkabel (Netzwerkanschluss, der dem seriellen Anschluss am nächsten ist; als „Config Interface“ auf der Verpackung aufgedruckt) und einem PC direkt verbinden
- https://192.168.1.1/ mit einem Browser aufrufen (das „s“ bei „https“ dabei nicht übersehen – oder „pfSense“ als Adresse ausprobieren)
- Sicherheitszertifikat-Ausnahme bestätigen, dann erscheint folgende Login-Seite

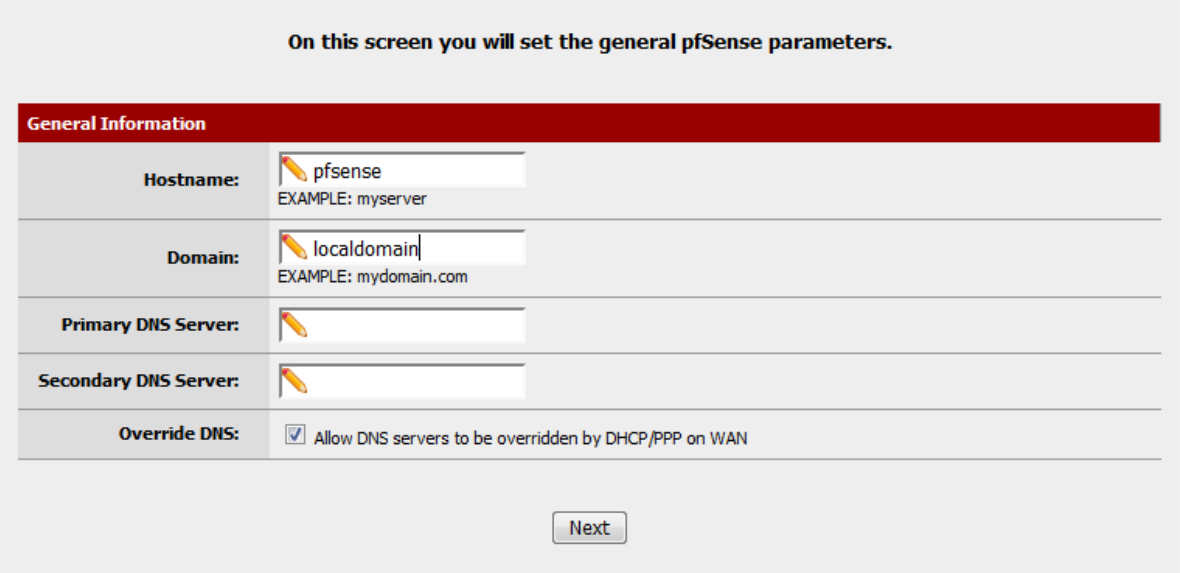


- Login mit User „admin“ und Passwort „pfsense“

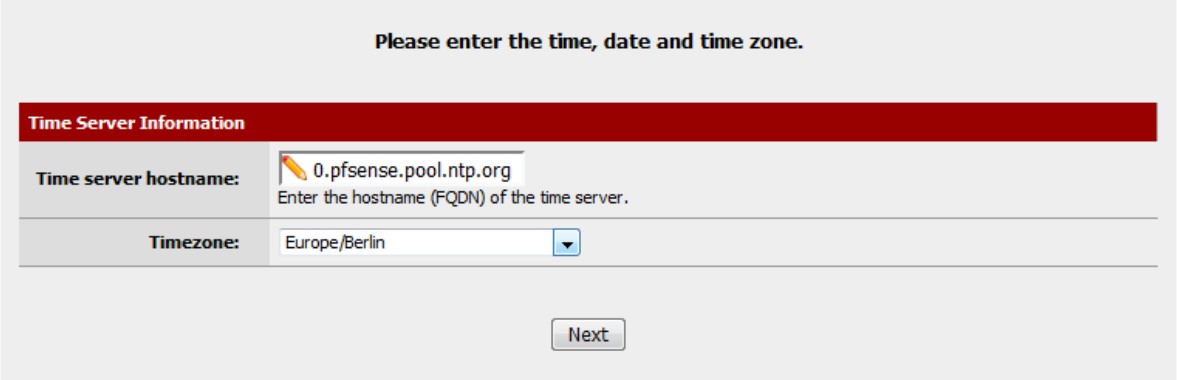
Einrichtung

- Nach kurzer Zeit startet der Installationsassistent

- Hostname „pfsense“, Domain und DNS-Server eintragen (im Zweifelsfall die Standardvorgaben bzw. frei lassen)

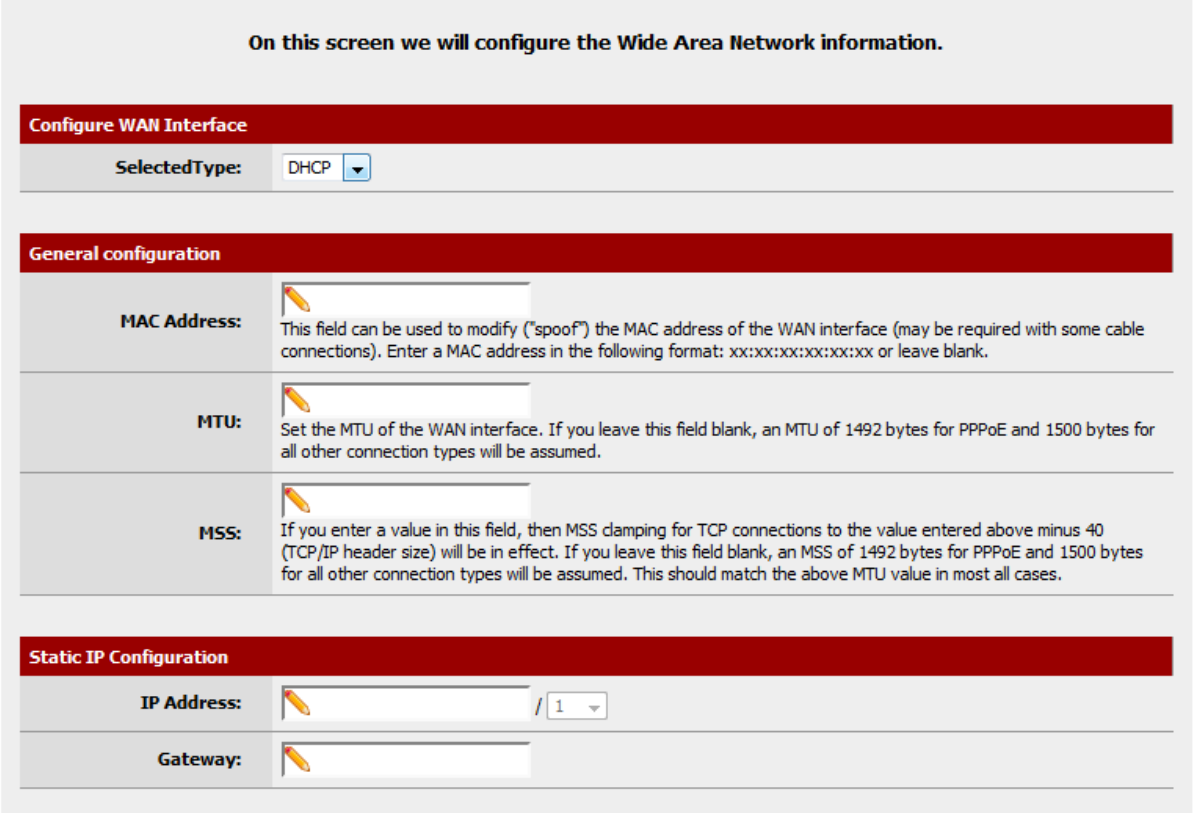


- Timezone auf „Europe/Berlin“ setzen

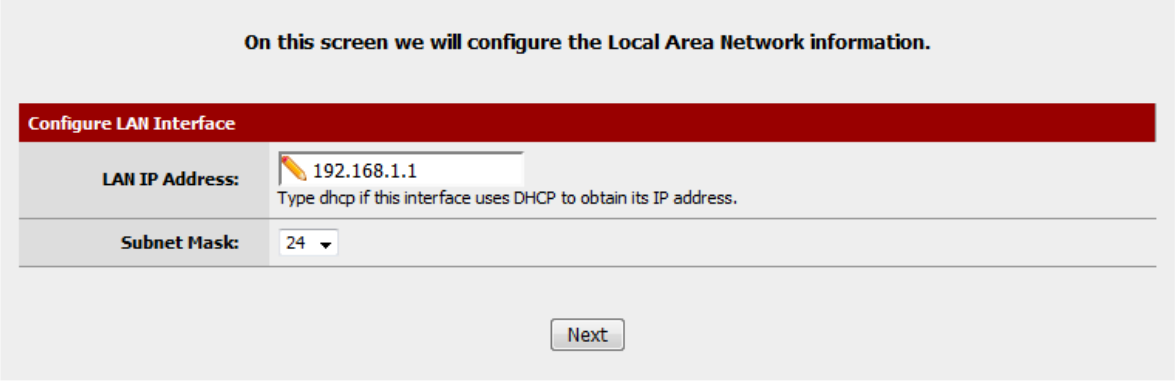


- Am besten: IP-Adresse für WAN (Wide-Area-Network) auf DCHP lassen, falls ein DHCP-Server läuft (ansonsten eine freie IP-Adresse für Zugriff aus dem WAN unter „Static IP Configurati-

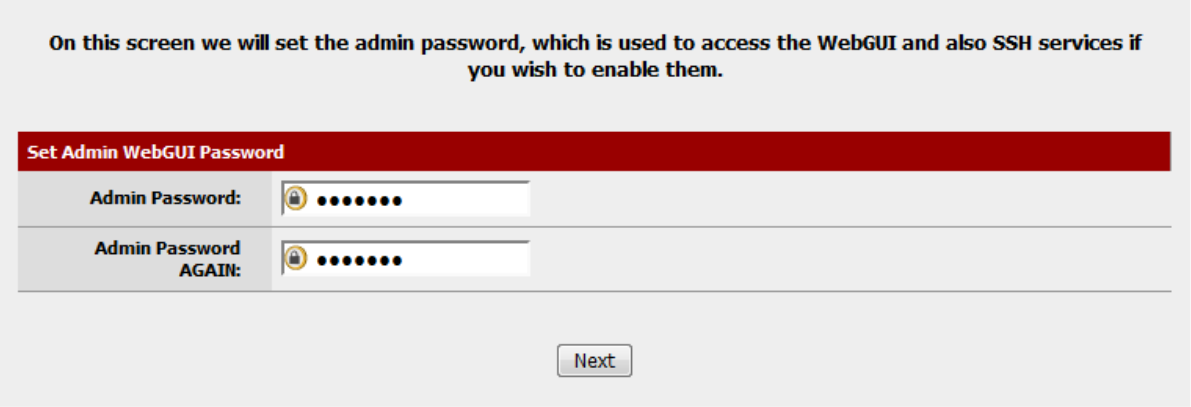
on“ eintragen, vorher den SelectedType auf „Static“ ändern)



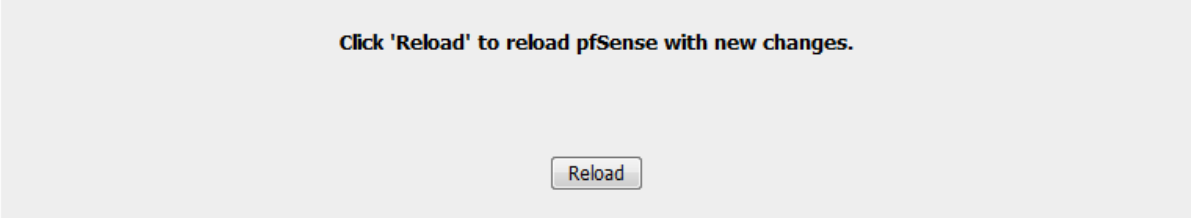
- Optional bei der vorletzte Einstellung „Block RFC198 Private Networks“ den Haken entfernen, falls hinter dem WAN entsprechende lokale IP-Adressebereiche verwendet werden (wie „10…“, „172.16….“ und „192.168….“, siehe Erklärung bei der Option)! Abschließend „next“ anklicken. An diesen Port wird hinterher die Verbindung zum Netzwerk/Internet (WAN) angeschlossen.
- Noch freie IP-Adresse für LAN-Zugriff (Local-Area-Network), entspricht der festen IP-Adresse auf dem Konfigurationsport, eintragen.



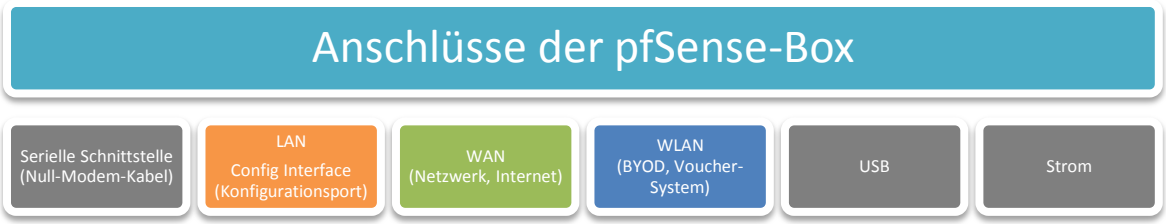
- Neues Admin-Passwort eintragen und gut merken (Es gibt keine „Passwort vergessen“-Funktion)



- Reload anklicken und Neustart abwarten.



Belegung der Netzwerkkarten



- Bei standardkonformer Einrichtung ist der linke Netzwerkport (**von hinten gesehen**) jetzt dem LAN (also der Konfiguration), der mittlere dem WAN und der linke noch nicht zugeordnet.
- Den mittleren Anschluss sollte man jetzt mit seinem Router (Internet) bzw. Netzwerk verbinden.
- Der rechte Anschluss wird mit den Geräten verbunden, die über das verkabelte Netzwerk über pfSense laufen sollen (ggf. Switches dazwischenschalten). Das ist nicht der Computer, von dem aus die pfSense gerade eingerichtet wird. Diesen bitte bis zum Schluss am aktuellem, dem „Config Interface“ lassen.
- Am sinnvollsten ist es, wenn man die Anschlüsse per Klebeetiketten beschriftet.

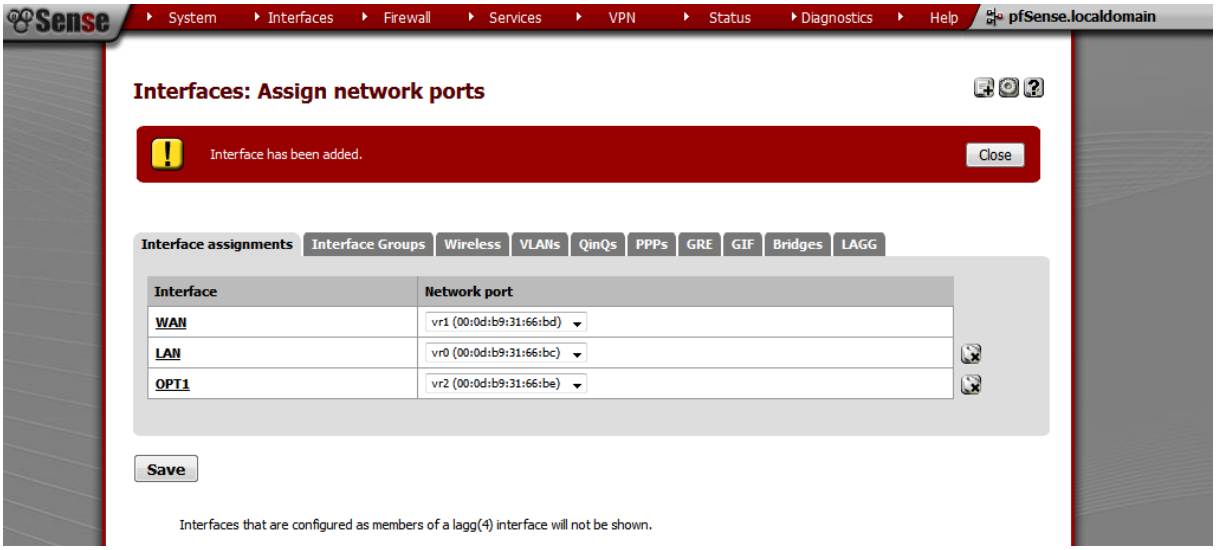
Test I

Hat man den mittleren Anschluss mit seinem Netzwerk oder dem Router verbunden und hängt der aktuell benutzte Computer noch am Konfigurationsport, so muss man jetzt bereits mit dem Rechner ins Internet kommen können.

War der Test erfolgreich, so erstellen Sie jetzt eine Sicherung der aktuellen Grundeinstellung (wie in „Wichtiger Hinweis: Sicherungen erstellen“ auf Seite 5 erklärt). Diese können Sie immer wieder nutzen, um die pfSense in einen vorkonfigurierten, aber sehr offenen Zustand zurück zu setzen.

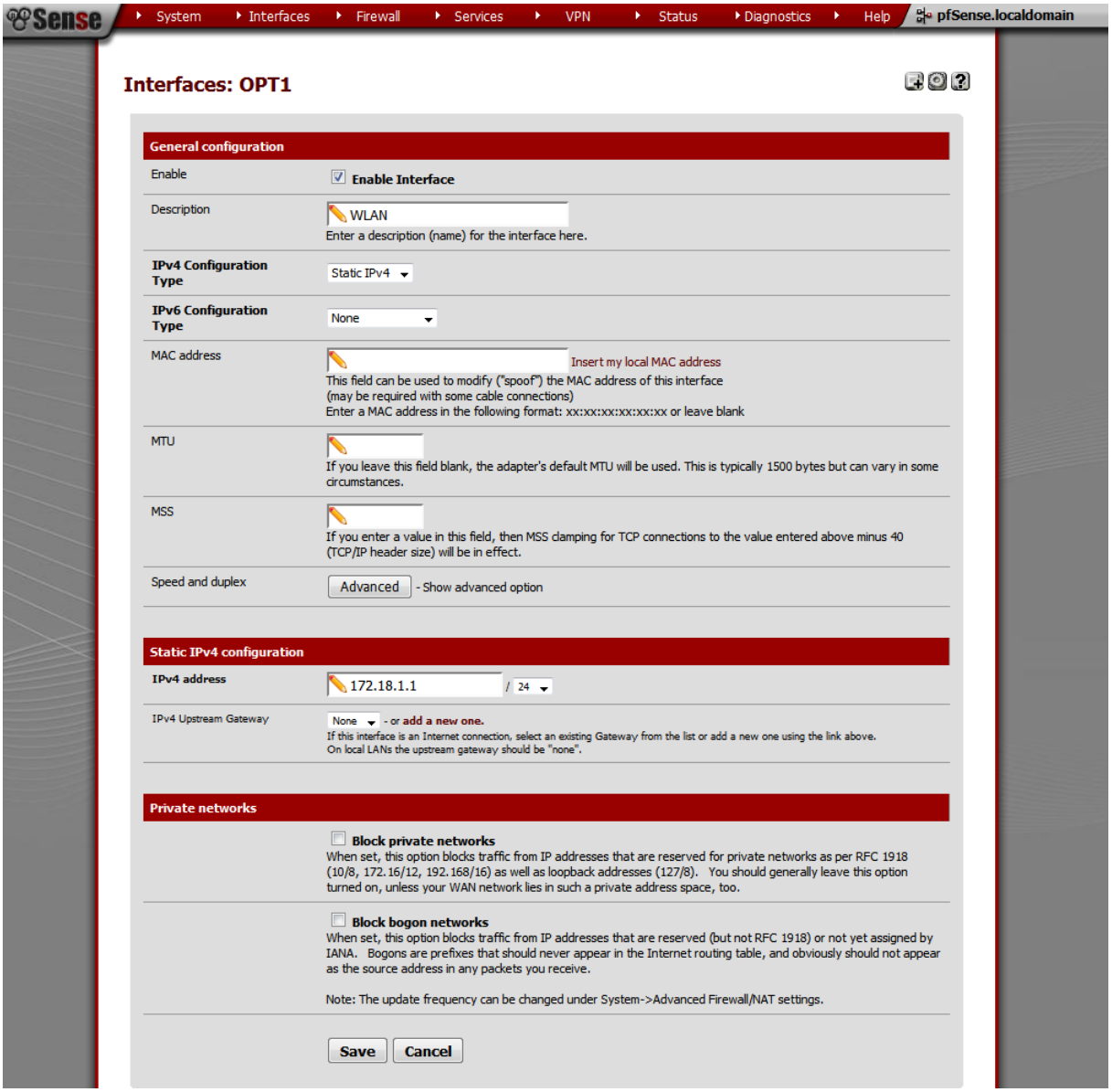
WLAN-Port einrichten

- Der rechte Anschluss (von hinten gesehen) ist noch frei und wird jetzt dem WLAN zugeordnet. Dazu im Menü „Interfaces“ „assign“ anklicken. Am Ende der Tabelle auf „+“ klicken.



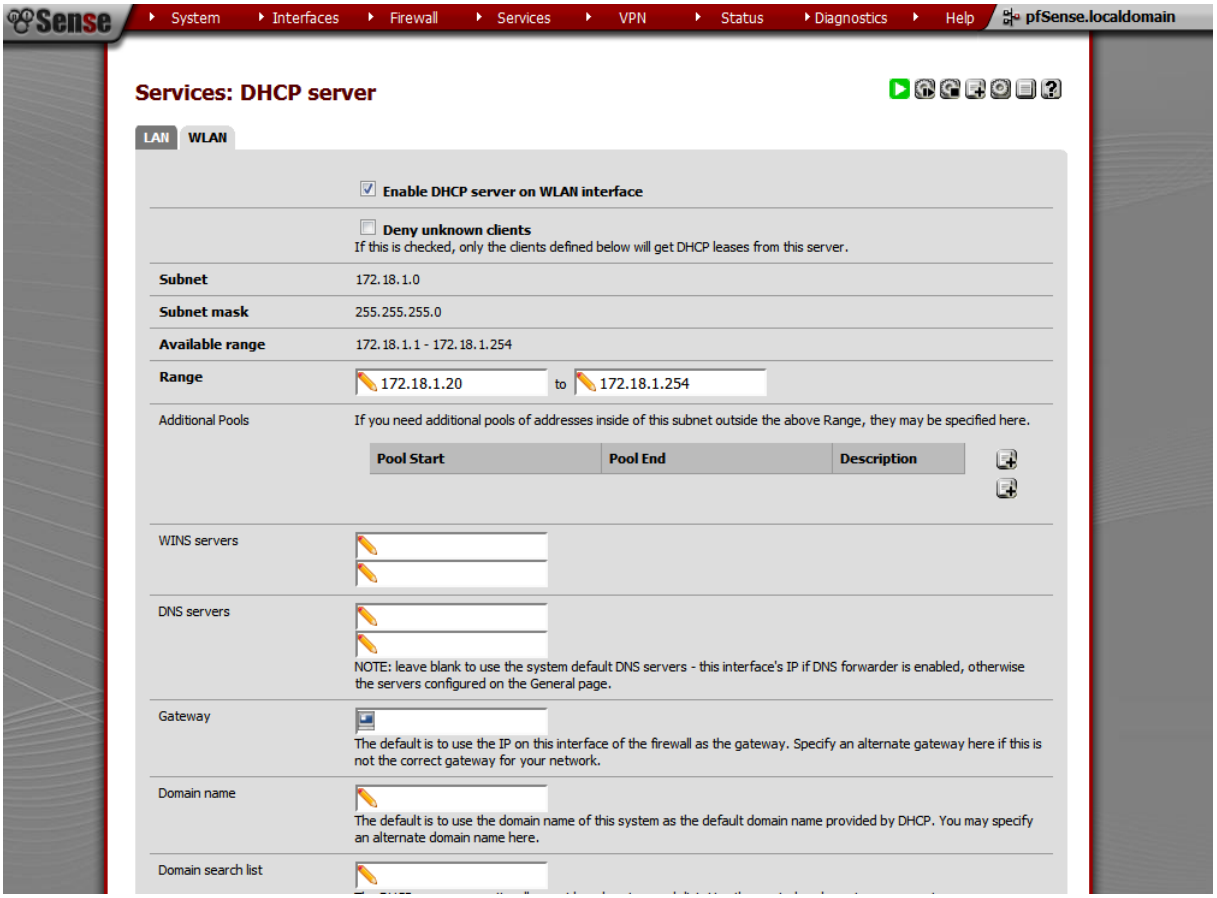
- Erneut im Menü „Interfaces“ das neue Interface „Opt1“ auswählen und per Häkchen bei „enable“ aktivieren. Dann die Description auf „WLAN“ ändern.
- Dort bei IPv4 auf „Static IPv4“ setzen und die IP-Adresse 172.18.1.1 und als Bereich /24 eintragen (falls der Bereich 172.18.1.1 bis 172.18.1.255 noch frei ist, ansonsten einen entspre-

chend anderen Bereich wählen).



- Klick auf „Save“ nicht vergessen und anschließend auf „Apply Changes“ klicken, um die Einstellungen zu aktivieren.
- Im Menü „Services“ „DHCP-Server“ auswählen und dort zum Reiter „WLAN“ wechseln. Dort das Häkchen „Enable DHCP-Server on WLAN Interface“ setzen und als Bereich (Range)

172.18.1.20 - 172.18.1.254 eingeben. Klick auf „Save“ nicht vergessen.



- Danach können die WLAN-Access-Points und -Repeater (ggf. auch über Switches zusammengeführt) an dem dritten Netzwerkanschluss angeschlossen werden.

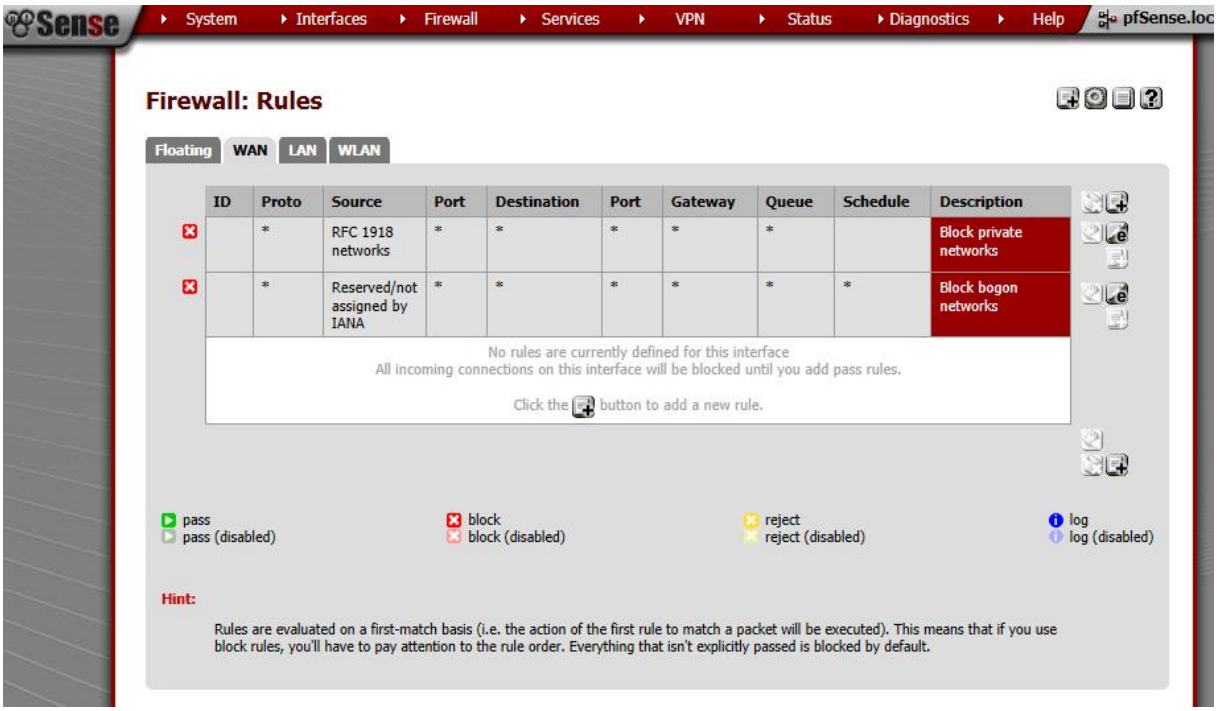
Die Firewall konfigurieren

Zwischen dem neuen WLAN-Netz und den anderen Netzen LAN und WAN müssen jetzt noch entsprechende Regeln definiert werden. Rufen Sie dazu über das Menü „Firewall“ und dann „Rules“ auf.

Es öffnet sich das Regel-Verzeichnis der Firewall. Die Regeln werden dabei immer von oben nach unten abgearbeitet. Es gilt dabei: Eine Regel, die zuerst auf den jeweiligen Traffic greift, gewinnt.

Regeln für das WAN

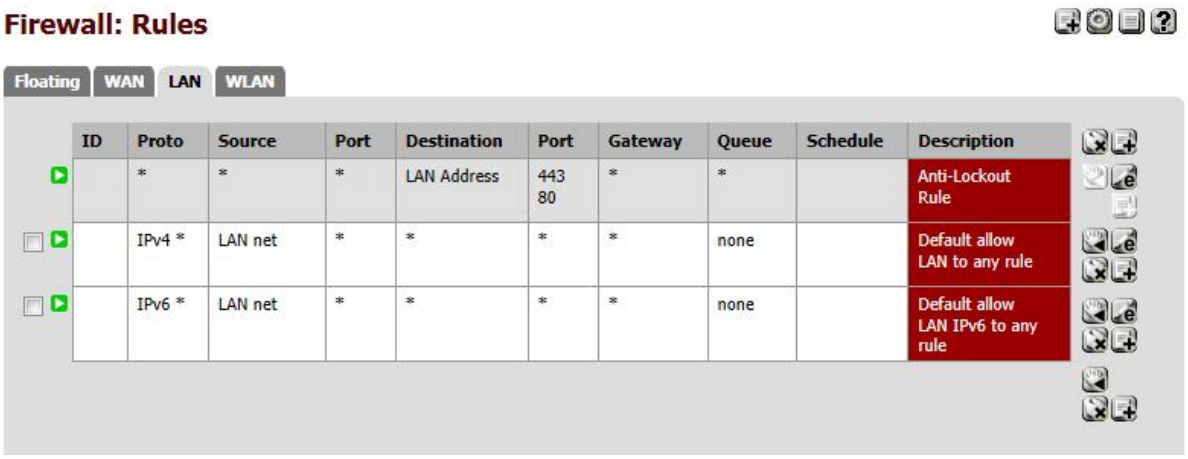
Im Reiter WAN sollten die folgenden Regeln automatisch (bzw. nur die untere, wenn der Haken bei „Block RFC198 Private Networks“ bei der WAN-Einrichtung nicht gesetzt wurde) erscheinen:



Diese blocken privaten Netzverkehr und nicht spezifizierte Adressen im Zugriff auf das WAN bzw. das lokale Netz (blockieren in beide Richtungen).

Regeln für das LAN (Konfigurationsnetzwerk)

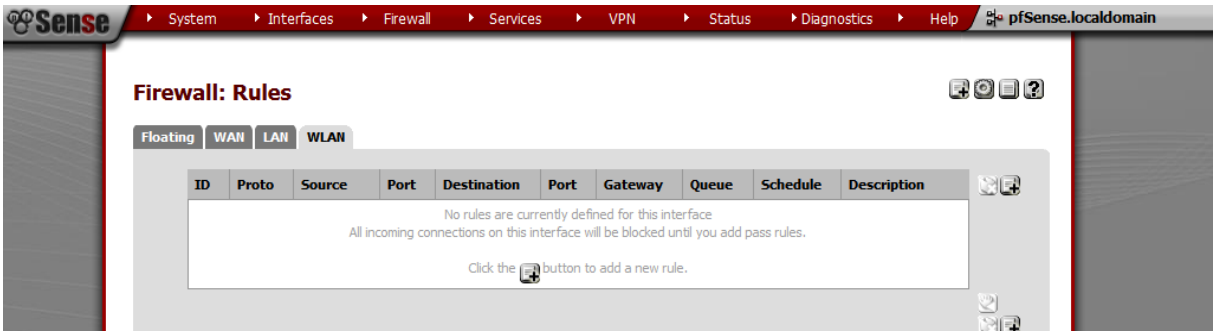
Unter dem Reiter LAN sollten die folgenden Regeln automatisch stehen:



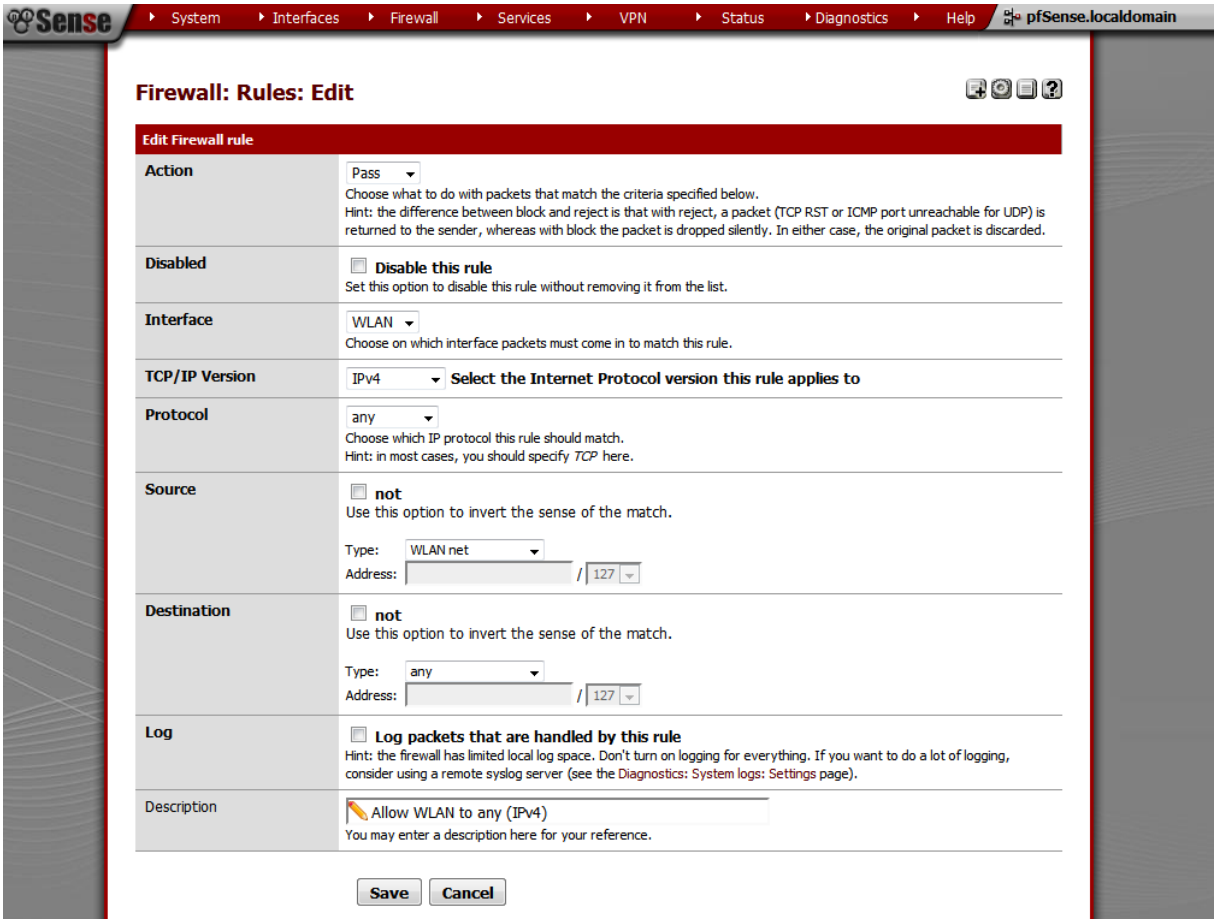
Die erste Regel verhindert, dass man sich selbst den Zugriff auf das Captive-Portal nimmt. Daher sollte diese (auch wenn ggf. weitere Regeln bei LAN eingetragen werden, immer an oberster Stelle stehen bleiben). Die beiden anderen Regeln erlauben Zugriff von dem LAN auf alles. Dabei erneut daran denken, dass das LAN unsere Konfigurationsschnittstelle ist, an der im Normalfall kein Gerät angeschlossen ist.

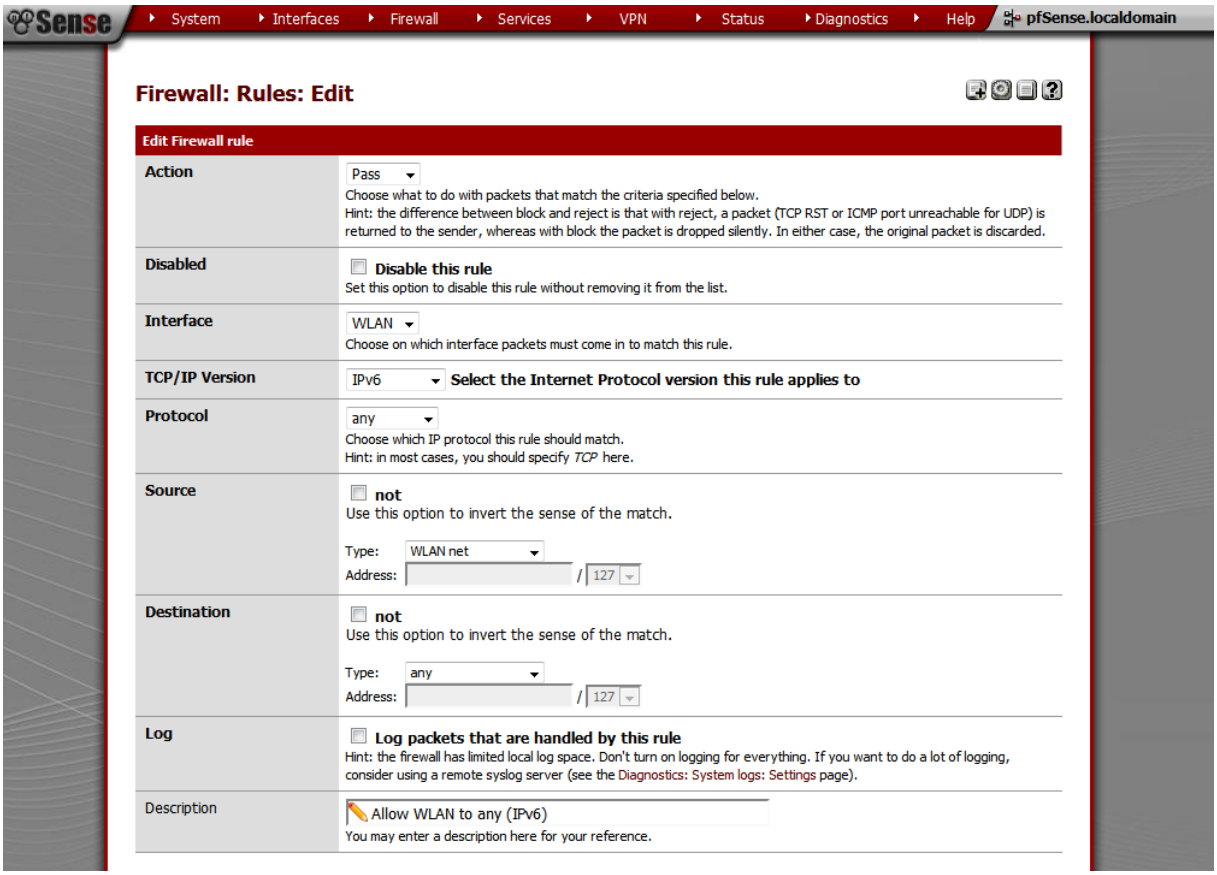
Regeln für das WLAN

Unter dem Reiter WLAN öffnet sich hingegen eine leere Regelliste. Dadurch ist aktuell alles für dieses Netzwerk verboten.

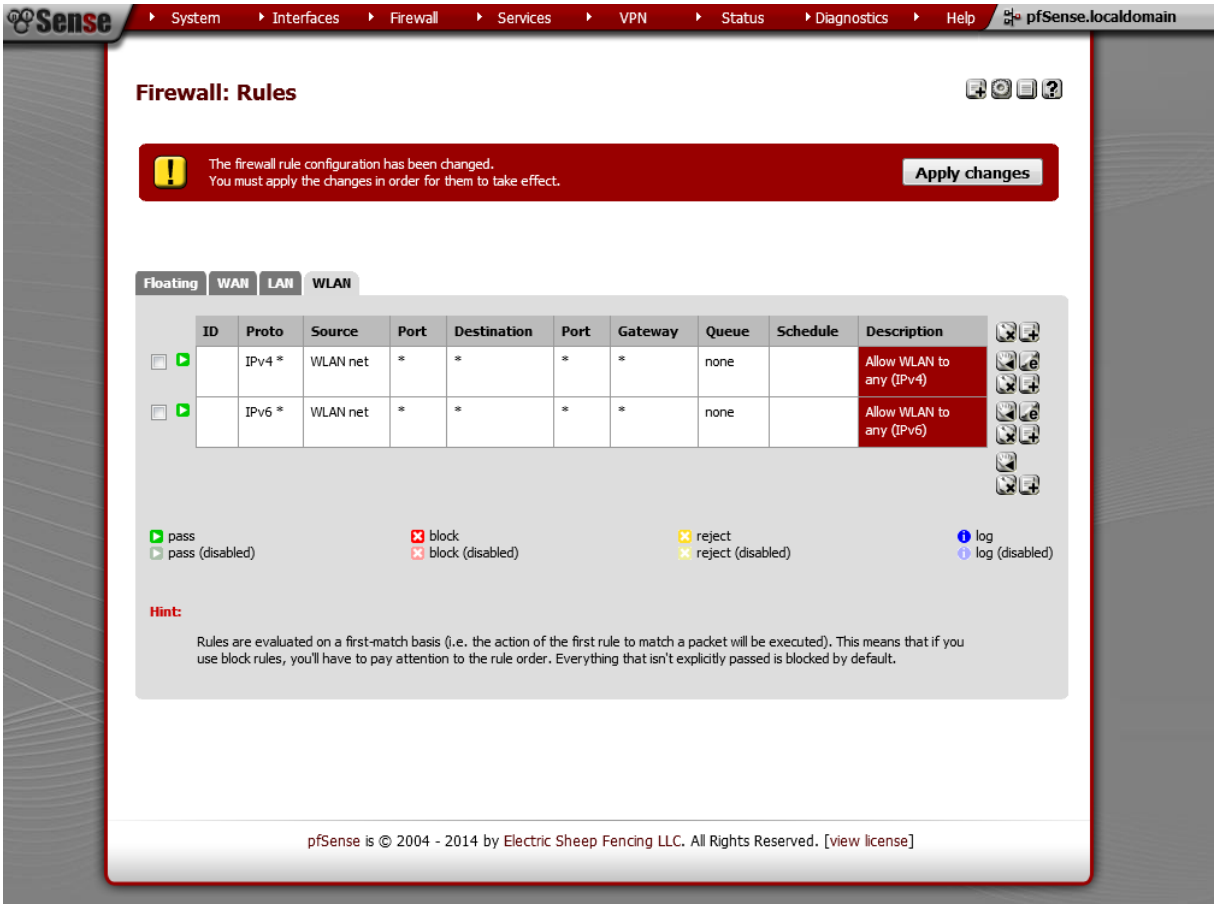


Als erstes fügen wir daher die folgenden zwei Regeln, die jeweils alles für IPv4 und IPv6 erlauben, durch Klick auf das „+“-Zeichen am Ende der Tabelle hinzu.





Dann ergibt sich folgendes Bild:



Jetzt noch auf „Apply changes“ klicken, um die Regeln anwenden zu lassen.

Test II

Schließen Sie jetzt einen weiteren Rechner (oder einfach nur den aktuellen Konfigurationsrechner) an den WLAN-Port an. Sie sollten eine IP-Adresse zugewiesen bekommen und direkt Zugriff auf das Internet haben. (Falls Sie den Konfigurationsrechner umgesteckt haben, so hängen Sie diesen abschließend wieder an den Konfigurationsport)

War der Test erfolgreich, so erstellen Sie jetzt eine Sicherung der aktuellen Grundeinstellung (wie in „Wichtiger Hinweis: Sicherungen erstellen“ auf Seite 5 erklärt).

Die Firewall für das WLAN sicherheitsbewusst konfigurieren

Je nach Einsatzsituation ergeben sich verschiedenen Regelsätze. Eine sicherheitsbedachte Konfiguration könnte wie folgt aussehen:

Firewall: Rules

Floating | WAN | LAN | WLAN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		IPv4+6 TCP/UDP	WLAN net	*	*	135	*	none		NetBIOS Block
		IPv4+6 TCP/UDP	WLAN net	*	*	137 - 139	*	none		NetBIOS Block
		IPv4+6 TCP/UDP	WLAN net	*	*	445 (MS DS)	*	none		NetBIOS Block
		IPv4+6 TCP	WLAN net	*	*	25 (SMTP)	*	none		SMTP Block
		IPv4+6 TCP	WLAN net	*	172.18.1.1	443 (HTTPS)	*	none		pfsense Web GUI Block
		IPv4 *	WLAN net	*	LAN address	*	*	none		Block LAN Subnet
		IPv6 *	WLAN net	*	LAN address	*	*	none		Block LAN Subnet
		IPv4 *	WLAN net	*	*	*	*	none		allow WLAN to any (Ipv4)
		IPv6 *	WLAN net	*	*	*	*	none		allow WLAN to any (IPv6)

pass / pass (disabled) — block / block (disabled) — reject / reject (disabled) — log / log (disabled)

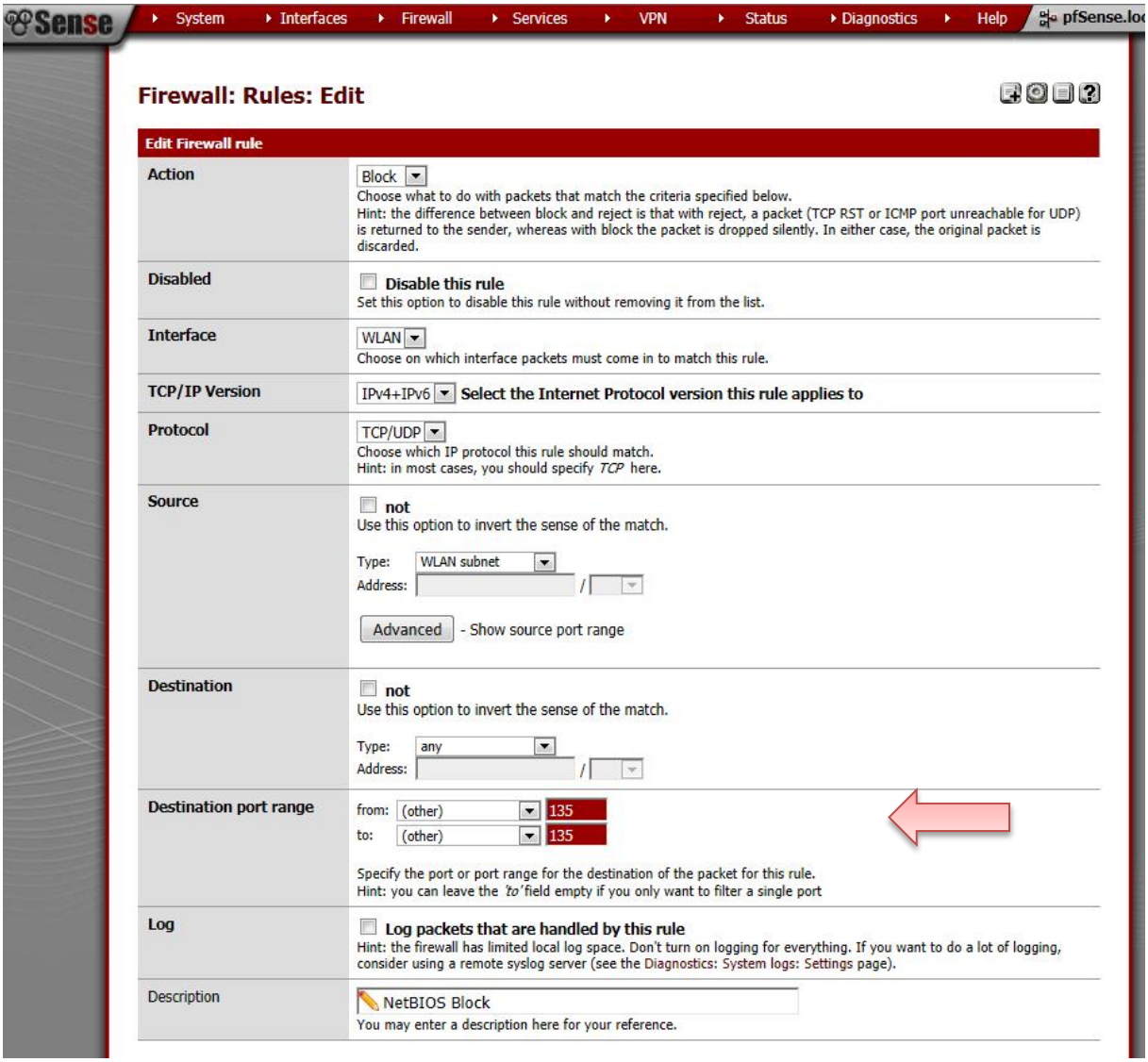
- Dabei sperren die oberen drei Regeln NetBIOS-Zugriff (bspw. notwendig für Datei- und Druckerfreigaben).
- Die Regel 4 blockiert SMTP-Zugriffe, also den Versand von e-Mails aus dem Netz durch direkten Kontakt mit SMTP-Servern (kann sinnvoll sein, um übermäßigen Traffic durch Spamversand von verseuchten Geräten zu verhindern).
- Die Regel 5 sperrt den Zugriff auf die Weboberfläche des pfSense aus diesem Netz. Dabei muss als Destination die IP-Adresse des pfSense aus diesem Netz eingetragen sein (dazu den Destination-Type auf „Single Host or Alias“ stellen).
- Regel 6 und 7 blockieren jeglichen Kontakt mit dem LAN-Netzwerk, also dem pädagogischen Netzwerk (dort beim Protokolltyp auf „any“ umstellen). Falls doch Kontakt zwischen diesen

Netzen gewünscht ist, einfach diese Regeln nicht einfügen oder durch spezifische Beschränkungen des Ports verändern.

- Die letzten beiden Regeln erlauben schließlich den grundsätzlichen Kontakt und haben wir bereits weiter oben angelegt.

Da die Regeln von oben nach unten abgearbeitet werden, ist die Reihenfolge entscheidend. Stünden die letzten beiden Regeln oben, so würde jeglicher Kontakt (auch NetBIOS, SMTP, Zugriff auf die pfSense-Weboberfläche, etc.) erlaubt sein und funktionieren.

Zum Anlegen der Regeln einfach auf den „+“-Button drücken. Es hat dabei Vorteile auf den „+“-Button der jeweils zuletzt angelegten Regel zu klicken, denn dann wird diese Regel als Vorlage benutzt und macht das Anlegen leichter. Die in der oberen Übersicht angezeigten „*“ entsprechen in dem Anlege-Formular dem Wort „any“. Als Beispiel die erste Regel:



- Zum Abschluss wieder „Apply Changes“ anklicken.

Test III

Entweder den Rechner wieder am WLAN-Port anschließen oder einen anderen Testrechner dort anschließen und versuchen auf https://172.18.1.1 oder https://pfsense zuzugreifen.

Test IV

Rechner wiederum am WLAN-Port anschließen und versuchen einen Ping auf den LANiS-Server (oder ein anderes Gerät, das nicht am WLAN-Port hängt) ausführen. Es darf keine Antwort kommen.

Abschließend ggf. den Rechner wieder an den Konfigurationsport anschließen.

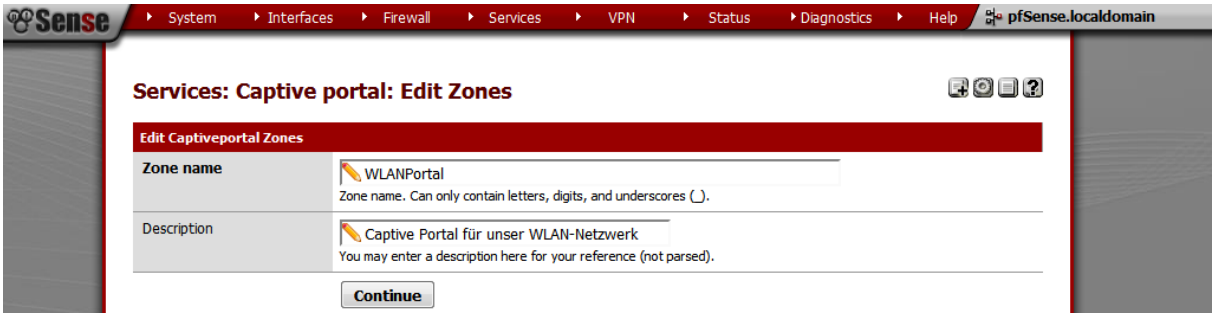
War der Test erfolgreich, so erstellen Sie jetzt eine Sicherung der aktuellen Grundeinstellung (wie in „Wichtiger Hinweis: Sicherungen erstellen“ auf Seite 5 erklärt).

Captive Portal

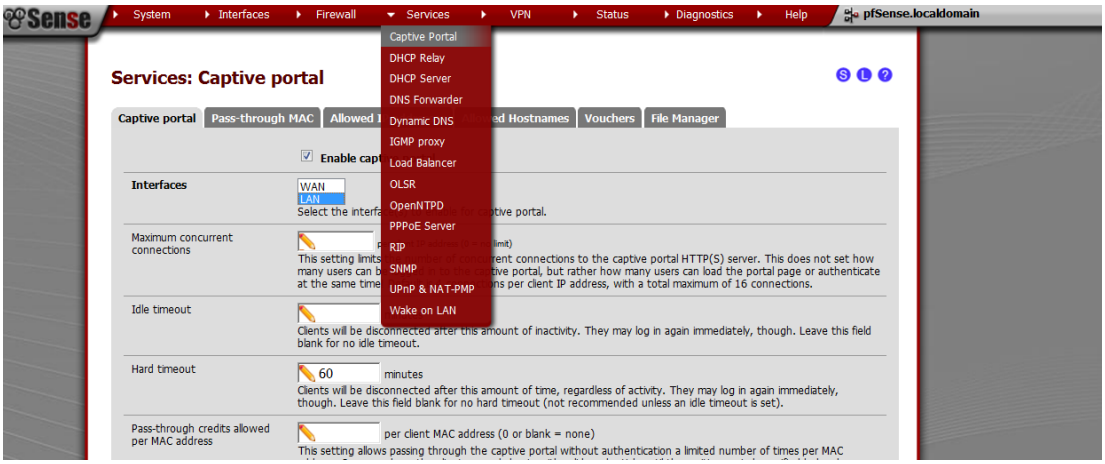
Das Captive Portal dient zum Verwalten von WLAN-Tickets bzw. WLAN-Vouchern, so dass der Internetzugriff auch nur zweitweise bzw. durch Benutzeraccounts auch dauerhaft gewährt werden kann.

Captive Portal einschalten

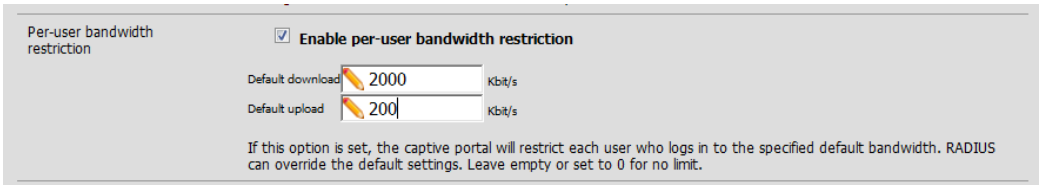
- Über „Services“ „Captive Portal“ kommt man zum Captive Portal.
- Dort muss zuerst eine neue Zone angelegt werden (+ am Ende der Tabelle). Dazu den Namen „WLANPortal“ benutzen. Nach dem Speichern landet man in der Zone.



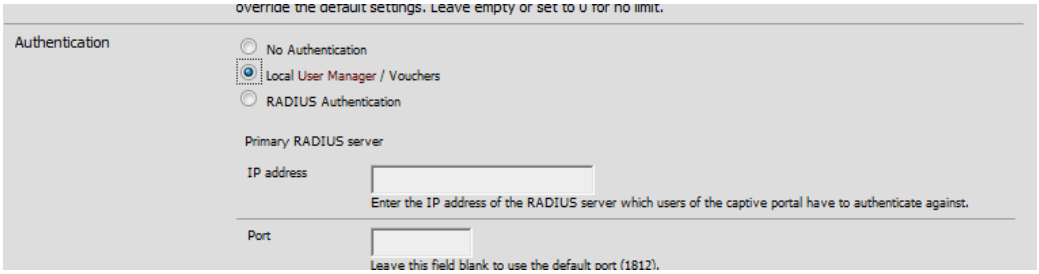
- **Achtung:** Bei den folgenden Einstellungen wird man immer wieder aus der Zone zurück zum Auswahl der Zone geleitet. Bitte immer wieder die aktuell eingerichtete Zone per „e“-Button am Ende auswählen.
- Dann das Portal per Haken bei „Enable Captive Portal“ aktivieren.
- Zuerst das Interface auswählen, für das es aktiviert werden soll (meist nur „WLAN“), alternativ auch „LAN“ möglich, falls beim Internetzugriff auch von Schulrechner ein Internet-Ticket verlangt werden soll und diese auch an der pfSense-Box hängen.



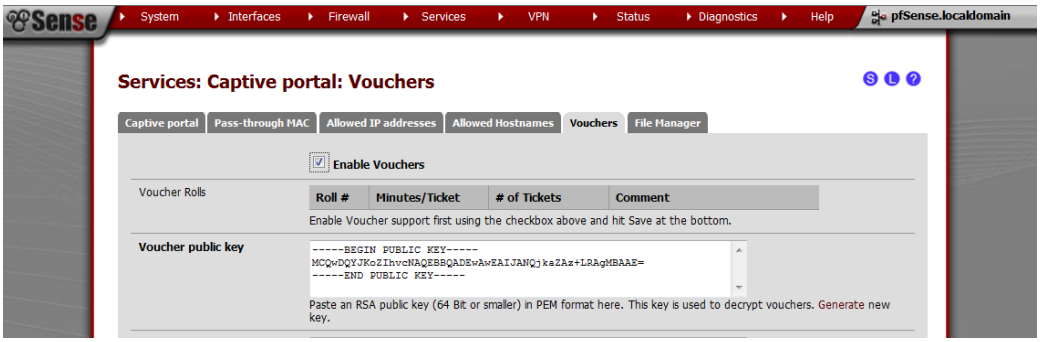
- „Idle Timeout“ und „Hard timeout“ auf 1440 (1 Tag) setzen, wenn kein Voucher länger läuft. Durch diese beiden Einstellungen lässt sich regeln, ob ein Voucher nach dem ersten Gebrauch ablaufen soll. Daher die beiden Werte zwingend größer als die längst vorgesehene Voucher-Dauer wählen.
- „Per user bandwidth restriction“ auf jeden Fall mit Werten belegen (je nach Größe der Institution und der verfügbaren Bandbreite < 5% des Maximums, bspw. 2000 für Download und 200 für Upload)



- „Authentication“ auf „Local User Manager / Vouchers“ setzen (die dort neu hinzugekommene Rollen-Recht-Angabe kann man aktiviert lassen).

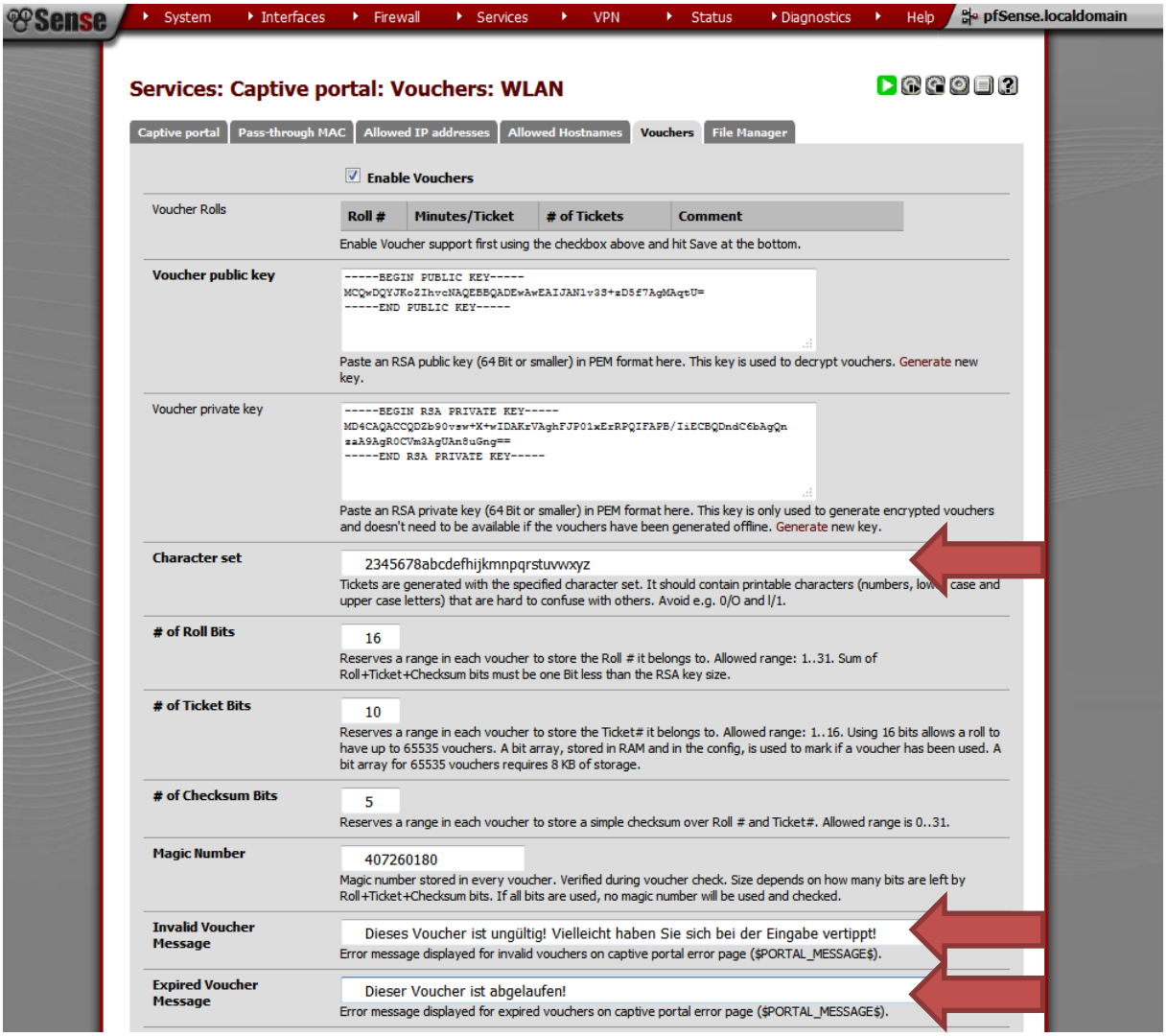


- Jetzt „Save“ anklicken und dann die Zone erneut auswählen (mit dem „e“-Button am Ende)
- Im Reiter „Vouchers“ „Enable Vouchers“ auswählen und speichern.

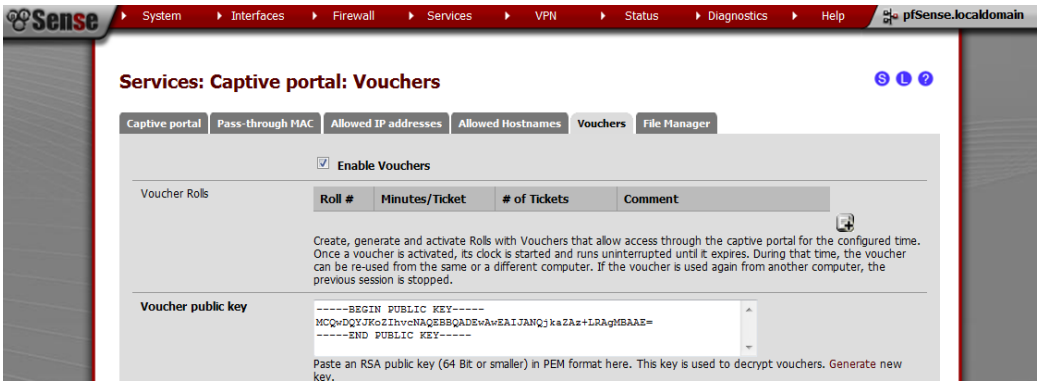


- Es kann sich dabei auch anbieten das „Character Set“, die Menge der Zeichen, aus denen Vouchers erstellt werden, noch zu verkürzen. Für eine schnelle Eingabe zu mobilen Zwecken sollte auf die Großbuchstaben verzichtet werden. Auch das Umschreiben der „Voucher Messages“ in deutsche Entsprechungen kann hilfreich sein. Alle Anpassungen kann man dem fol-

genden Bild entnehmen:

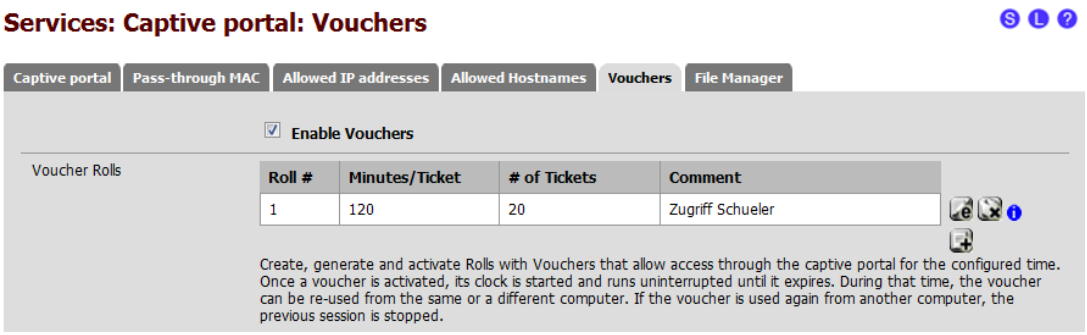


- Nach dem Speichern erscheint bei „**Voucher Rolls**“ (ganz oben) rechts das Pluszeichen.



- Über diesen Button „Voucher Rolls“ für bspw. die Zeitspannen von 50 (1 Schulstunde), 100 (2 Schulstunden), 200 (4 Schulstunden), 300 (halber Tag) sowie 500 (ganzer Tag) Minuten anle-

gen (gewünschte Anzahl an Vouchers eintragen) und speichern.



- Für Lehrer kann noch ein weiterer Voucherblock mit der Zeitspanne 525600 Minuten (1 Jahr) angelegt werden.
- Danach bei der Übersicht der „**Voucher Rolls**“ durch Klick auf das „**i**“ in jeder Zeile die Voucher generieren und herunterladen. Die Dateien zugriffsgeschützt speichern und später
    - entweder in den Ordner L:\Lehrer\config\Vouchers („L:“ ist das LANiS-Laufwerk) für die weitere Verwendung im LANiS-Lehrermodul verschieben. Dabei die Dateinamen so abändern: *Minuten-Beschreibung.csv* (als Beispiel: „30-halbe Stunde.csv“; maximal 10 verschiedene Ticketlängen konfigurierbar)
    - oder per Online-Modul über http://portal.lanis-system.de einrichten, so dass die Tickets nicht nur vom Lehrermodul ausgegeben werden können
- Achtung: Bitte dieselbe Ticket-Datei nicht in beide Systeme einstellen, da dasselbe Ticket sonst mehrfach ausgegeben werden würde.
- Die Zeit eines Vouchers fängt an zu laufen, wenn dieses das erste Mal eingesetzt wird und endet automatisch, so lange der Hard Timeout und der Idle Timeout größer als die hinterlegte Voucherdauer ist. Ein Voucher kann auch bei einem Gerätewechsel mitgenommen werden, dann wird jedoch die andere Verbindung unterbrochen. Das hat den Vorteil, dass auch Lehrer ihren Code nicht einer ganzen Klasse zur Verfügung stellen können.

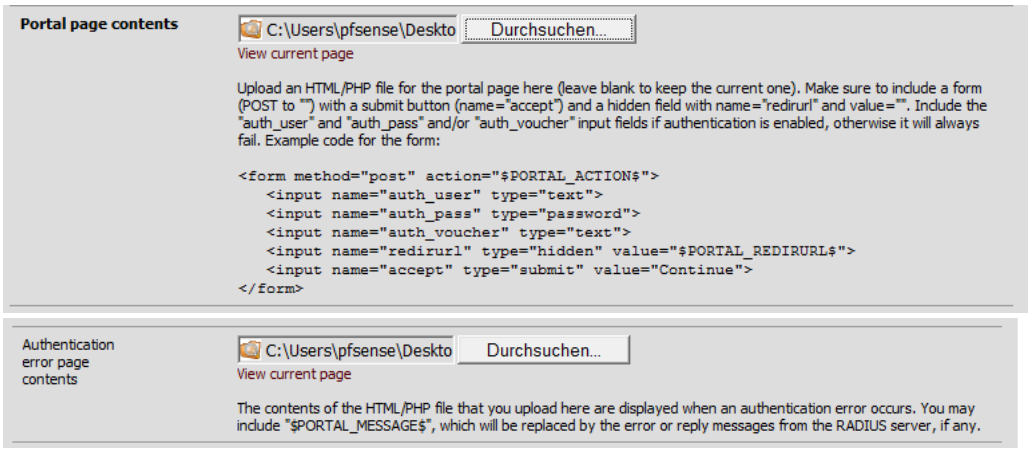
Test V

Rechner wiederum an den WLAN-Port umstecken und versuchen eine Internetseite aufzurufen. Das Captive Portal sollte aufgehen. Hier ist leider nur ein Login mit Benutzername und Passwort möglich – noch nicht per Voucher, was wir gleich nachrüsten werden.

War der Test erfolgreich, so erstellen Sie jetzt eine Sicherung der aktuellen Grundeinstellung (wie in „Wichtiger Hinweis: Sicherungen erstellen“ auf Seite 5 erklärt).

Captive Portal mit Voucher-Eingabemaske und noch schöner

- Um die vorgegebenen Login- und Error-Seiten des Captive Portals auszutauschen, gehen Sie bitte wie folgt vor.
- Upload der „login.html“ -Datei des mitgelieferten (oder unter https://support.lanis-system.de/knowledgebase.php?article=244 heruntergeladenen) Zips bei „Captive Portal“ bei „Portal page contents“ und der „error.html“-Datei bei „Authentication error page contents“. Anschließend „Save“ klicken.



- Anschließend die Bilder sowie die .css-Datei im Reiter „File Manager“ beim „Captive Portal“ hochladen.
- An der Stelle an der die HTML-Dateien hochgeladen wurden, kann man per Klick auf „View current page“ (rote Links im oberen Screenshot) eine Vorschau der Login-Seite ansehen.

Test VI

Erneut Test V ausführen und über das neue Layout freuen!

Test VII

Hier steht jetzt auch die Möglichkeit zur Verfügung eines der heruntergeladenen Voucher einzugeben und sich zu freuen, dass man jetzt im Internet surfen kann.

War der Test erfolgreich, so erstellen Sie jetzt eine Sicherung der aktuellen Grundeinstellung (wie in „Wichtiger Hinweis: Sicherungen erstellen“ auf Seite 5 erklärt).

Captive Portal verändern

- Anzeige der – schon schriftlich bestätigten – Nutzungsbedingungen als Erinnerung: https://support.lanis-system.de/knowledgebase.php?article=516
- Dauerhafte Anzeige der Account-Login-Felder beim Captive-Portal (anstatt erst noch auf „+“ klicken zu müssen, damit diese erscheinen): https://support.lanis-system.de/knowledgebase.php?article=517

Weiterführende Informationen

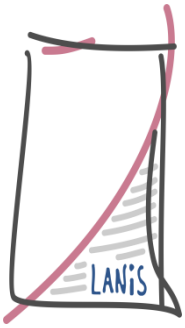
pfSense bietet sehr viele Einstellungen und kann ebenso vielen Einsatzszenarien gerecht werden. Viele hilfreiche Anleitungen finden Sie dazu bspw. unter

- In Deutsch
  - http://www.nwlab.net/tutorials/pfSense/
  - Deutsches pfSense-Forum: http://forum.pfsense.org/index.php/board,6.0.html
- In Englisch
  - Offizielle Dokumentation: http://doc.pfsense.org/
  - Forum: http://forum.pfsense.org/

Herausgeber dieser Anleitung

Diese Anleitung für die Einrichtung des pfSense in einer schulischen Umgebung ist von

Hessischer Lehrkräfteakademie
Dezernat Medienbildung
IT-Supportcenter
Stuttgarter Str. 18-24
60329 Frankfurt
Telefon: 069 / 3 89 89 - 219
Fax: 069 / 3 89 89 - 606
E-Mail: support@lanis-system.de



erstellt worden.