Realsoft Firewall

Wichtige Hinweise zur Inbetriebnahme

V. 1.1 – APU2C4W

Inhaltsverzeichnis

Einleitung

Vielen Dank für den Einsatz unserer Firewall. Sie halten ein kompaktes und bereits fertig konfiguriertes Stück Technologie in der Hand, welches Ihnen modernste Funktionalität für Ihre Netzwerkzentrale bietet. Sowohl die Hardware, ein APU 2C4 mit Quad Core Prozessor und 4 GB Speicher, als auch die Software, pfSense in der Version 2.3.2, garantieren Funktionalität, Geschwindigkeit und vor allem anderen Sicherheit.

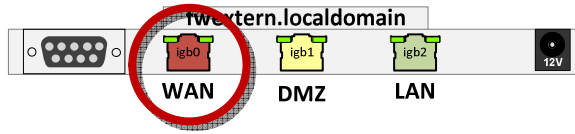
Die Firewall bietet vielfältige Anschlussmöglichkeiten und die Unterstützung modernster Protokolle und Dienste. Neben der an sich schon umfangreichen Firewall Funktionalität bietet sich die Nutzung als Router an, als VPN mit Ipsec und OpenVPN, als Proxy Server oder als Unterstützung für DynDNS Dienste.

Eine Firewall ist eine recht komplexe Technologie. Sie bildet das Eingangstor zu Ihrem Netzwerk und muss somit sorgfältig konfiguriert sein, damit keine ungewollten Zugriffe von außen möglich sind. Daher sollte grundsätzlich an der Konfiguration nur jemand mit dem entsprechenden Fachwissen arbeiten.

Überblick

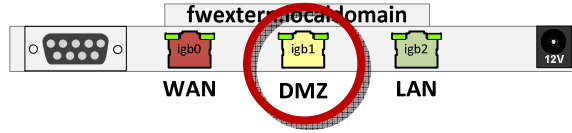
Die ausgelieferte Firewall ist bereits vorkonfiguriert. Die nachfolgenden Charakteristika geben einen kurzen Einblick in die Konfiguration und mögliche Anschlussoptionen.

Netzwerkanschlüsse der Realsoft Firewall



Der **WAN Anschluss** (die Verbindung in das Internet, linker Netzanschluss, direkt neben der seriellen Schnittstelle) ist für DHCP konfiguriert. Hiermit wird die sofortige Inbetriebnahme hinter einem Router oder an einem typischen Anschluss mit dynamischer IP Adresse ermöglicht.

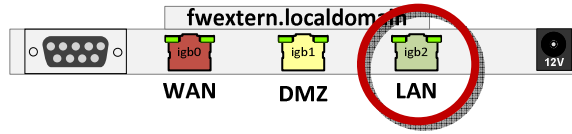
Sollten Sie die Firewall mit einer fixen IP Adresse betreiben, so müssen die entsprechenden Einstellungen vorgenommen werden.



Die **DMZ**, die Demilitarisierte Zone (Netzsegment mit Servern, die von außen erreichbar sein sollen, mittlerer Netzanschluss) ist auf das Netzsegment 192.168.70.0/24 konfiguriert. Dort läuft ein DHCP Server mit dem Adressbereich 192.168.70.30-99.

Wenn Sie einen Webserver, Mailserver oder ähnliches in der DMZ betreiben wollen, müssen Sie entsprechende Regeln in der Firewall eintragen. Derzeit ist keine Regel eingetragen, so dass kein Netzwerkverkehr vom Internet in die DMZ weitergeleitet wird.

Möchten Sie mehrere Webserver auf dem gleichen Port (80, 443) in der DMZ betreiben, so müssen Sie einen Reverse Proxy Server (Squid, HA-Proxy) nutzen. Diesen können Sie über die Paketverwaltung installieren und entsprechend Ihren Anforderungen konfigurieren.



Der **LAN Anschluss** (rechter Netzanschluss neben der USB Anschlüssen) schließlich hat keine eigene Adresse, da er mit dem WLAN gemeinsam über eine Bridge (LANBridge) geführt wird.

Das **WLAN** ermöglicht den Kontakt zur LAN Zone und wird mit dem LAN Anschluss gemeinsam über die LANBridge konfiguriert.

Die **LANBridge** ist eine Zusammenfassung aus LAN Anschluss und WLAN. Diese ist auf das Netzsegment 192.168.76.254 konfiguriert. Dort läuft ein DHCP Server mit dem Adressbereich 192.168.76.30-99. Somit wird jedes angeschlossene Gerät sofort mit einer IP Adresse und den notwendigen Daten versorgt.

Das LAN Segment ist das sicherste Segment. Die Firewall Regeln sind so festgelegt, dass von außen (WLAN, also Internet und DMZ) initiierter Netz-

werkverkehr vollständig blockiert wird. Die im LAN Segment angeschlossenen Geräte dürfen hingegen ohne Einschränkungen auf das Internet oder die DMZ zugreifen.

Anschlussoptionen für die Realsoft Firewall

Um Server mit der Realsoft Firewall mit dem Internet zu verbinden, brauchen Sie einen entsprechenden Anschluss. Während in Privathaushalten im Regelfall Anschlüsse mit einer dynamischen Adressvergabe vergeben werden, können im Business Bereich auch Anschlüsse mit festen IP Adressen existieren. Für beide Variationen ist die Realsoft Firewall geeignet und kann entsprechend konfiguriert werden. Sämtliche notwendigen Einstellungen werden dazu in der Firewall vorgenommen. Einige Beispiele sollen dies verdeutlichen. Die Beispiele basieren auf den Realsoft Kombiserver, der mit der gleichen Firewall ausgeliefert wird.

Anschluss mit einer dynamischen IP Adresse

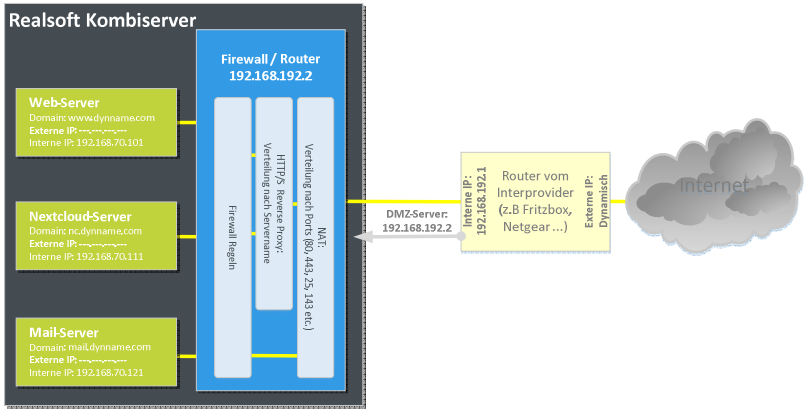
Die für Privatpersonen und Freiberufler wohl gebräuchlichste Anschlussvariante ist die mit einer dynamischen Adresszuordnung.

Dies bedeutet, dass der Provider (Unitymedia, 1 und 1, Telekom oder andere) nach einer festgelegten Zeit (z. B. nach 24 Stunden) dem Anschluss eine neue IP Adresse zuordnet. Zudem wird im Regelfall vom Provider ein entsprechender Router gestellt, hinter dem erst die Realsoft Firewall eingehängt wird. Dies hat mehrere Auswirkungen.

Zunächst muss die Zuordnung zwischen einem Domain-Namen (z.B. dyn-name.com) und der IP Adresse genauso oft angepasst werden, wie die Adresse durch den Provider gewechselt wird. Hierzu gibt es eigene, teilweise kostenlose Dienste, die diese Zuordnung übernehmen. Dort wird ein Konto eröffnet und die entsprechenden Namen eingetragen. Das Ändern der Adresse kann dann im Regelfall direkt im Router des Providers oder im Router der Realsoft Firewall konfiguriert werden.

Beispiel: Dynamische Adresse (Privatanschluss, DSL etc.)

Adresse wird vom Provider dynamisch gewechselt. Provider stellt Router zur Verfügung.
Bei einem „DynDNS-Provider" wird mit einem Account ein Domainname reserviert.



Anschluss mit einer festen IP Adresse

Wie bei der Konfiguration mit einer dynamischen IP Adresse bekommen bei einer festen IP Adresse sämtliche an die Firewall angeschlossenen Server im Prinzip die gleiche externe Adresse. Anders hingegen wird die Firewall über die immer gleiche Adresse angesprochen. Daher ist ein Update einer sich ändernden Adresse bei einem DynDNS Anbieter nicht mehr erforderlich.

Das Prinzip der Zuordnung der Server zu der IP Adresse funktioniert aber wiederum gleich. Es werden entweder bestimmte Ports – mit denen wiederum bestimmte Dienste verknüpft sind – auf entsprechende Server geleitet oder, im Falle, dass zwei Server auf dem gleichen Port Dienste anbieten, es wird anhand der entsprechenden Domainnamen unterschieden. Hierzu ist in der Firewall eine zusätzliche Komponente (der sg. Reverse-Proxy) notwendig, die Sie unter der Paketverwaltung finden. Dieser Reverse Proxy erledigt alle Arbeiten, die mit Verteilung der Kommunikationsdaten an die richtigen Adressaten zu tun haben.

Für den täglichen Einsatz ist diese Software völlig transparent und wird vom Anwender nicht bemerkt. Bei der Installation von Zertifikaten (z.B. mit LetsEncrypt) für verschlüsselte Kommunikation ist hier aber ein besonderes

Augenmerk drauf zu richten, da durch den Proxy nur Teile einer vollautomatischen Installation möglich sind.

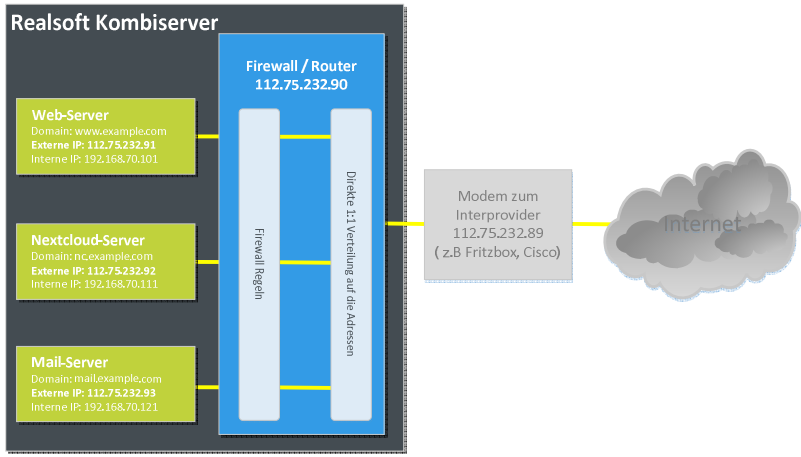
Anschluss mit mehreren festen IP Adressen

Selbstverständlich können auch unterschiedliche, feste IP Adressen für einzelne Server genutzt werden. Dann entfällt neben dem DynDNS Dienst auch der Zwang zu einem Reverse Proxy, da eine eindeutige Zuordnung von IP Adresse zu Server möglich ist. Die Konfiguration der Firewall vereinfacht sich entsprechend.

Anstelle eines Reverse Proxies kann über eine direkte NAT Zuordnung und entsprechende Portweiterleitungen jeder angeschlossene Server direkt adressiert werden. Selbstverständlich lassen sich die verschiedenen Vorgehensweisen auch kombinieren. Die nebenstehende Abbildung zeigt die vereinfachte Struktur.

Beispiel: Unitymedia Paket mit 5 festen IP Adressen

Vom Provider zugewiesener Adressblock:	**112.75.232.90 – 112.75.232.94**
Automatisch zugewiesene zusätzliche Adressen:	**112.75.232.89 – UM Gatewayadresse (Modem)**
	112.75.232.88 – UM Netzwerkadresse
	112.75.232.95 – UM Broadcastadresse



Inbetriebnahme

Um die Firewall in Betrieb zu nehmen reicht es, die oben erwähnten Kabel zu verbinden und das Stromkabel anzuschließen. Da die Firewall bereits konfiguriert ist, nimmt sie sofort Ihre Tätigkeit auf. Der Startvorgang benötigt eine kleine Weile.

Schließen Sie Ihre neue Firewall wie auf der nebenstehenden Abbildung an.

Verbinden das **rote Kabel** mit Ihrem Internetanschluss. Dies kann hinter einem Router sein (typisch für dynamische Adresszuordnung in privaten Haushalten) oder direkt hinter einem Modem (typisch für feste Adressen bei gewerblich genutzten Anschlüssen).

Das **gelbe Kabel** ist der Anschluss für die DMZ, schließen Sie hier die Server an, die vom Internet aus erreichbar sein sollen, also Webserver, Mailserver etc.

Das **grüne Kabel** schließlich ist ebenso wie er WLAN Zugang für das interne LAN gedacht. Hier werden Geräte angeschlossen, die nur intern erreichbar sein sollen, aber einen Zugang zum Internet haben.

Wenn Sie nur ein Gerät an DMZ oder LAN-Kabel anschließen, können Sie dieses direkt an die Firewall anschließen. Benötigen Sie hingegen mehr als ein Gerät, dann können Sie problemlos die Firewall mit einem entsprechend Switch verbinden und so beliebig viele Anschlüsse bereitstellen. Achten Sie aber darauf, dass DMZ und LAN in jedem Fall über physisch getrennte Switche gehen, damit die Sicherheit gewahrt bleibt.

Schließen Sie am Ende schließlich das mitgelieferte Netzteil an. Die Firewall startet. Der Startvorgang selbst nimmt etwas Zeit in Anspruch. Sobald die Firewall bereit ist, zeigt sie dies über einen entsprechenden Ton an.

Hardware

Die Basis bildet eine APU.2C4 Platine von PCEngines, welche das Nachfolgemodell der sehr erfolgreichen APU.1D4 ist. Mit einem leistungsstärkeren Prozessor, Intel Netzwerk Controller und einer deutlichen Verringerung der Wärmeentwicklung konnte PCEngines nahtlos an das Erfolgsmodell anknüpfen.:

- CPU: AMD Embedded G series GX-412TC, 1 GHz quad Jaguar core mit 64 bit
- DRAM: 4 GB DDR3-1066 DRAM
- Speicher:30 GB mSATA SSD
- 12V DC, zwischen 6 und 10W, abhängig von der CPU Last
- Verbindung: 3 Gigabit Ethernet Anschlüsse (Intel i210AT)
- I/O: DB9 Serial Port, 2 USB 3.0 extern + 2 USB 2.0 intern, drei Front LEDs
- Erweiterung: 2 MiniPCI Express (eine mit SIM Sockel), LPC Bus, GPIO Header, I2C Bus, COM2 (3.3V RXD / TXD)

Software

Die Software der Firewall, pfSense ist bereits installiert und vorkonfiguriert (siehe oben). pfSense basiert auf dem Betriebssystem FreeBSD. pfSense ist eine Weiterentwicklung der Firewall- und Router-Distribution monowall. Die Software selbst ist lizenzkostenfrei. Es haben sich aber eine Vielzahl von Unternehmen gebildet, die kostenpflichtigen Support und Wartung liefern.

Mit der gelieferten Hardware und Software sind Sie in der Lage, eine Vielzahl von Einsatzmöglichkeiten zu nutzen.

- Multi-WAN, Bündelung mehrerer Verbindungen, Load Balancing, Fail Over
- Redundanz auf der LAN-Seite mit Common Address Redundancy Protocol CARP
- pfsync zur Synchronisierung der State-Tables mehrerer Firewalls
- Transparente Layer 2 Firewall

- Statefull Firewall auf Layer 3
- VPN mit IPsec, OpenVPN und PPTP
- Erkennung von Betriebssystemen (pof) und Filterung
- Reporting und Monitoring, RRD Graphs
- DynDNS-Unterstützung
- Captive Portal
- Proxy und Webfilter mit Squid und SquidGuard
- Reverse Proxy mit Squid oder HAProxy
- Es lassen sich Funktionen wie AntiVirus, netIO, nmap und Snort und weitere nachrüsten.

Der Aufruf der Firewallkonfiguration erfolgt im Browser je nach dem, an welchem Anschluss sich der aufrufende Rechner befindet.

- Hat er eine Verbindung zum LAN Anschluss erfolgt der Aufruf mit: http://192.168.76.254
- Hat er eine Verbindung zum DMZ Anschluss erfolgt der Aufruf mit: http://192.168.70.254

Die Firewall ist derzeit auf HTTP eingestellt, sollte aber später auf HTTPS umgestellt werden. In der Konfiguration ist nur ein Minimalset an Regeln hinterlegt. Dies dient dem anfänglichen, problemlosen Nutzen der Maschine. Sollten Sie später restriktiver vorgehen wollen, können Sie die Regeln über die Konfiguration im Browser problemlos erweitern. Dies sollte man nur mit notwendigen Fachwissen tun, da es sonst schnell passieren kann, dass die einzelnen Server kompromittiert werden oder man sich selbst vom Zugriff aussperrt.

Lieferumfang

- Firewall/Router auf Basis des APU.2C4 Boards inkl. WLAN Access Point und pfSense Software, fertig eingebaut in Metallgehäuse
- SSD eingebaut
- Passendes Netzteil mit 12 V-, max. 2,5 A
- 3 x Cat.5e Ethernetkabel, 2x RJ45 (je 1 x rot / gelb / grün)
- Installierte Software: pfSense, vorkonfiguriert und bereits mit WLAN eingerichtet

Userdaten und Kennwörter der Firewall

Die nachfolgende Tabelle gibt Ihnen eine Übersicht über die derzeit konfigurierten Einstellungen, User und deren Passworte. Da es sich um von uns vergebene Standardpasswörter handelt, sollten diese möglichst schnell neu vergeben werden.

Wichtig!

Verlieren Sie diese Information nicht, da Sie sonst keinen Zugriff auf Ihr System haben.

System	User	Passwort	Anmerkung
Zugang via Web-Oberfläche	admin	2016!AFw#01	Dies ist der uneingeschränkte Systemzugang. Hiermit lassen sich alle Änderungen durchführen inkl. Das Anlegen neuer Benutzer und deren Berechtigung.

Bereich	Inhalt	Anmerkung
Zugriff auf die Konfiguration via Web-Browser	http://192.168.76.254	Um den Zugang nutzen zu können, muss das Gerät mit dem Web-Browser mit dem LAN-Bereich der Firewall verbunden sein. Dies kann direkt über den grünen Anschluss (siehe oben) geschehen oder via Switch, der mit dem grünen Kontakt verbunden ist. Das Gerät sollte sich via DHCP konfigurieren um sicherzustellen, dass es die richtige Adresse für den Zugriff hat.

Hostname.Domain	fwextern.localdomain	Dies ist nur ein exemplarischer Standardwert von unserer Seite. Im Produktionsbetrieb sollte dies entsprechend angepasst werden.
DNS-Server	8.8.8.8, 8.8.4.4	Voreingestellt sind die beiden DNS-Server von Google, da diese schnell und sicher sind. Selbstverständlich können hier andere oder eigene DNS-Server eingetragen werden.
WLAN Access Point	5 GHz Band, SSID: fwextern PWD: 2016FW#01	Der WLAN Access Point kommuniziert auf dem 5 GHZ Band. Ein Wechsel auf 2,4 GHz ist per Konfiguration möglich. SSID und Passwort sind voreingestellt und sollten entsprechend geändert werden. Das WLAN ist über eine Bridge direkt mit dem LAN Bereich (grün) verbunden. Dies bedeutet, dass via WLAN die gleichen Rechte (Interzugang, DMZ Zugang) vorhanden sind, wie bei einem Kabelanschluss mit dem grünen Kontakt.
LAN-Kontakt / LAN-Bridge grün	IP: 192.168.76.254 DHCP-Bereich: 192.168.76.30-99	Der LAN Bereich ist der sicherste Bereich innerhalb der Firewall. Für alle Geräte, die hier angeschlossen werden gilt, dass eine unaufgeforderte Kontaktaufnahme aus dem Internet oder der DMZ vollständig unterbunden wird.

		Der LAN Anschluss ist mit dem WLAN über eine LAN-Bridge verbunden, so dass für beide Bereiche die gleichen Sicherheitsmechanismen greifen. Die IP Adressen (wie links nebenstehend) gelten demnach auch für beide Bereiche, da sie der LAN Bridge zugeordnet sind.
DMZ Kontakt gelb	IP: 192.168.70.254 DHCP-Bereich: 192.168.70.30-99	Die Demilitarisierte Zone (DMZ) ist der Bereich, in dem Server angesiedelt werden, die über das Internet von außen erreichbar sein müssen. Dies trifft zum Beispiel für Web-Server, Mail-Server oder andere Server zu. Dies bedeutet, dass mit diesen Maschinen jederzeit über die in den Firewallregeln freigegeben Ports (z.B. 80 und 443 für Webserver) Kontakt mit diesen Servern aufgenommen werden kann Daher gelten hier besonders strenge Sicherheitsregeln. Die DMZ liegt in einem eigenen Netzsegment (192.168.70.0), welches ausschließlich hierfür reserviert ist. Sie bringt ebenfalls einen DHCP Server, so dass sich auch hier angeschlossene Geräte selbständig mit einer gültigen Adresse versorgen können, wenngleich dies für Server eher unüblich ist.
WAN Kontakt rot	DHCP	Der WAN Anschluss schließlich ist die „Leitung zum ISP", also zum Internet Service Provider. Dies kann je nach Einsatzszenario direkt hinter einem Modem sein,

		so dass die Firewall direkt aus dem Internet erreichbar ist. Die Firewall kann aber auch hinter einem Router liegen. Hierbei ist darauf zu achten, dass die Ports und Adressen zum Durchreichen der Daten auch im Router entsprechend freigegeben werden.

Wichtig!

Verlieren Sie diese Information nicht, da Sie sonst keinen Zugriff auf Ihr System haben.

Perfekte Lösungen für Ihren Erfolg

Wir vertreiben nicht nur Standards, sondern wir fertigen individuelle Maschinen und Konfigurationen für unsere Kunden. Ganz gleich ob Sie einfache Lösungen benötigen, umfangreiche Cluster oder Spezialhardware, die außer Ihnen niemand hat. Nutzen Sie unseren Service von der Planung bis zur Inbetriebnahme und darüber hinaus.

Für Neuigkeiten und interessante Themen rund um die IT in Mittelstand, Vereinen und privatem Umfeld schauen Sie doch gerne bei uns herein oder nehmen Sie direkt Kontakt mit uns auf.

Realsoft GmbH
Am Hangelstein 20
65812 Bad Soden

Telefon +49 6196 921 8299
Fax +49 6196 921 6616

Web www.realsoft.de
Email info@realsoft.de