

Konfiguration pfSense FireWall für WAN GUI Zugriff

Ersteller: System-Clinch IT Servcies – www.MiaTel.ch
Author: Manuel Magnin, MMagnin@Clinch.ch
Datum: 04.04.2019

Um die Firewall von extern via WAN Zugriff managen zu können, muss dieser freigegeben werden. Sinn macht es wenn nicht die ganze Welt auf das GUI Login kommt, sondern wenn nur der Zugriff von den Netzwerken des Supportes freigegeben ist. Dafür müssen auf der pfSense ein paar Einstellungen vorgenommen werden.

Hier ein Beispiel mit einer pfSense 2.4.4 und GUI Zugriff für HTTPS

Firewall / Regeln / WAN

Übergreifend **WAN** LAN

Regeln (Ziehen, um die Anordnung zu ändern)

<input type="checkbox"/>	States	Protokoll	Quelle	Port	Ziel	Port	Gateway	Queue	Zeitplan	Beschreibung	Aktionen
<input type="checkbox"/>	✓ 2 /12.70 MIB	IPv4 TCP	CLINCH_NET	*	Diese Firewall	443 (HTTPS)	*	nicht gesetzt		CLINCH-NET-Management	
<input type="checkbox"/>	✓ 0 /1 KiB	IPv4 ICMP any	CLINCH_NET	*	Diese Firewall	*	*	nicht gesetzt		ICMP-CLINCH-OK	

Hinzufügen Hinzufügen Löschen Speichern Trenner

Die Quelladresse CLINCH_NET kann auch ein * sein, mit einem Objekt mit z.B. dem Namen CLINCH_NET wird erreicht, dass nicht das ganze Internet Zugriff auf die pfSense Firewall bekommt!

Firewall / Aliase / IP

IP **Ports** URLs Alle

Firewall Aliase IP

Name	Werte	Beschreibung	Aktionen
CLINCH_NET	11.22.33.44	CLINCH.NET	

Hinzufügen Importieren

Der Zugriff auf den Drucker ist ab der IP 11.22.33.44 zugelassen (kann auch durch weitere ergänzt werden)

Firewall / Aliase / Bearbeiten

Eigenschaften

Name: CLINCH_NET
Der Name des Aliases darf nur aus den folgenden Zeichen bestehen "a-z, A-Z, 0-9 und _".

Beschreibung: CLINCH.NET
Hier kann eine Beschreibung zu administrativen Zwecken eingetragen werden (wird nicht intern verarbeitet).

Typ: Netzwerke

Netzwerke

11.22.33.44 / 32 SupportNET Löschen

[System](#) ▾ [Schnittstellen](#) ▾ [Firewall](#) ▾ [Dienste](#) ▾ [VPN](#) ▾ [Status](#) ▾ [Diagnose](#) ▾ [Hilfe](#) ▾

Firewall / [Regeln](#) / [Bearbeiten](#)

[🔍](#) [📊](#) [📄](#) [?](#)

Firewall Regel bearbeiten

Aktion Erlauben ▾
 Wähle aus, was mit Paketen geschieht, die die u.g. Kriterien erfüllen.
 Hinweis: Der Unterschied zwischen blockieren und zurückweisen besteht darin, dass beim Zurückweisen das Paket (TCP, RST or ICMP Port für UDP nicht erreichbar) an den Versender zurückgeschickt wird, während beim Blockieren das Paket still verschwindet. In jedem Fall wird das Paket verworfen.

Deaktiviert Diese Regel deaktivieren
 Wählen Sie diese Option, um diese Regel zu deaktivieren ohne sie aus der Liste zu löschen.

Schnittstelle WAN ▾
 Wählen Sie die Schnittstelle, aus deren Richtung Pakete kommen müssen, um von dieser Regel verarbeitet zu werden.

Adressfamilie IPv4 ▾
 Wählen Sie das Internet Protokoll, welches dieser Regel entsprechen soll.

Protokoll TCP ▾
 Wählen Sie das IP-Protokoll, welches dieser Regel entsprechen soll.

Quelle

Quelle Negieren Einzelner Host oder Alias ▾ CLINCH_NET / ▾

Der **Source Port Range** ist in der Regel zufällig und in nahezu allen Fällen nicht identisch mit dem Zielport. Daher belässt man diese Einstellung normalerweise auf ihrem Standardwert, any.

Ziel

Ziel Negieren Diese Firewall (selbst) ▾ Ziel Address / ▾

Bereich der Zielports HTTPS (443) ▾ Benutzerdefiniert Bis HTTPS (443) ▾ Benutzerdefiniert

Wählen Sie den ziel Port oder den Portbereich für diese Regel. Das 'Bis'-Feld darf leer bleiben, wenn nur ein einzelner Port gemappt wird.

Zusätzliche Optionen

Protokollieren Von dieser Regel erfasste Pakete protokollieren
 Tipp: Die Firewall hat nur einen begrenzten Platz für die lokale Speicherung von Protokollen. Benutzen Sie diese Option sparsam. Für umfangreicheres Protokollieren empfiehlt sich die Einrichtung eines externen Syslog Servers ([Status](#) : [System Logs](#): [Einstellungen](#) Seite).

Beschreibung CLINCH-NET-Management
 Beschreibung für administrative Zwecke eingeben. Ein Maximum von 52 Buchstaben wird im Regelsatz benutzt und im Firewall Log angezeigt.

Erweiterte Optionen

Als **Quelle** [CLINCH_NET](#) kann auch das ganze Internet zugelassen werden, mit einem Objekt mit z.B. dem Namen [CLINCH_NET](#) wird erreicht, dass nicht die ganze Welt Zugriff auf den Drucker bekommt! Dies da die Drucker meistens ohne Passwort betrieben werden!

Mit **diese Firewall (selbst)** als **Ziel** wird der Zugriff auf die Firewall aktiviert.

PS: Wir aktivieren jeweils auch ICMP / Ping, für diese Quelle, auf die Firewall. So kann wenn das Web-GUI nicht geht, mit Ping festgestellt werden, ob das WAN Interface der Firewall Online ist.

Wenn Sie den Dienst HTTPS (Port 443) für andere Services benötigen, so können Sie extern Port 444 verwenden und intern 443. Beim Zugriff muss dann der Port angegeben werden z.B. <https://12.34.56.78:444>