OPNsense Central Management

Einleitung

Mit der stetig wachsenden Verbreitung von OPNsense Firewalls, steigt dementsprechend auch der Bedarf an einer zentralen Übersicht und Verwaltung der eigenen Systeme, aber auch kleine Systemhäuser müssen immer einen schnellen Überblick auf die zu verwalteten Kundenfirewalls haben.

Das von Deciso verwaltete Plugin OPNcentral bietet diese Möglichkeit für die Business Edition, nicht aber die Community Edition, was im Gegenzug bedeutet, dass für die Verwaltung von 50 Firewalls jährlich Kosten von ca. 7.500 EUR zu bezahlen sind, während unsere Plugins in dieser Staffel noch bei unter 1.000 EUR liegen. Zusätzlich lassen sich über OPNcentral Aliase und Firewallregeln nur über ALLE Firewalls ausrollen, was v.a. im MSP-Umfeld absolut ungeeignet ist.

Unser Central Management geht hier einen eigenen Ansatz, bei dem Firewalls gruppiert werden und and diese, ausgewählte Aliase und Regeln ausgerollt werden können. Eine zentrale Regel, dass alle LANs auf Google DNS auflösen dürfen, kann z.B. an alle Firewalls deployt werden, während der Zugriff auf einen Proxy nur für einzelne ausgewählte Systeme gewährt wird.

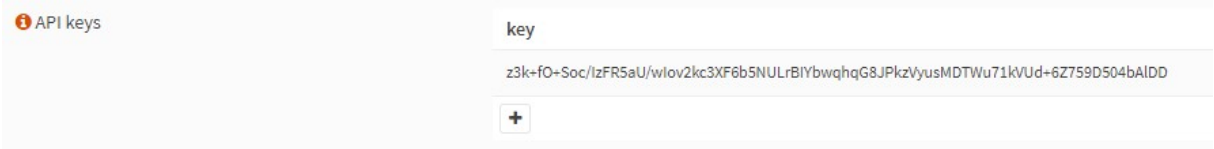
Das Ausrollen von Plugins und geplante Upgrades sind auch ein zentraler Punkt, den unser Plugin einzigartig auf dem Markt macht.

Vorbereitung

Für die Installation des Plugins muss erst unser Repository aktiviert werden. Eine Anleitung dazu findet man hier: https://opnsense.max-it.de/professional-content/freie-videos/

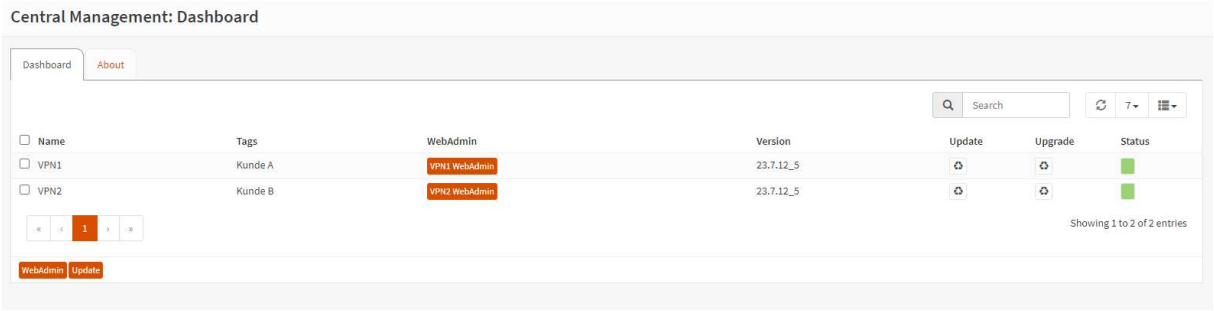
Bevor die ersten Systeme aufgenommen werden können, muss auf dem Zielsystem sichergestellt sein, dass die IP vom Central Management Zugriff auf die Web GUI hat (Firewall : Rules : WAN)!

Authentifiziert wird über API Keys, dazu muss auf dem Zielsystem in System : Access : Users ein Adminuser bearbeitet und im Bereich API auf „+“ geklickt werden. Es wird eine Textdatei mit Key und Secret geladen und nur der Key (public) bleibt mit dem Drücken auf „Save“ lokal gespeichert.

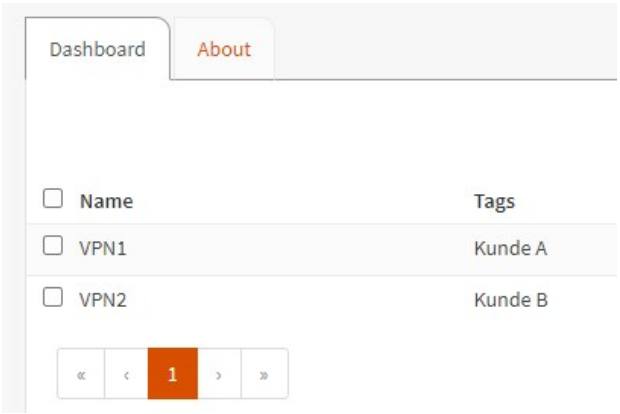


Dashboard

Das Dashboard listet alle inventarisierten Firewalls auf und verschafft einen schnellen Überblick welche Systeme erreichbar sind, auf welcher Version sie laufen, Tags nach Kunden oder Funktion und alles auch durchsuchbar.

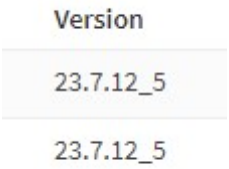


1. In den ersten beiden Spalten findet man den Namen der Firewall und optional Tags, um die Geräte zu verschlagworten, z.B. nach Kundennamen oder auch Funktion wie „Cloud“ oder „Proxy“.



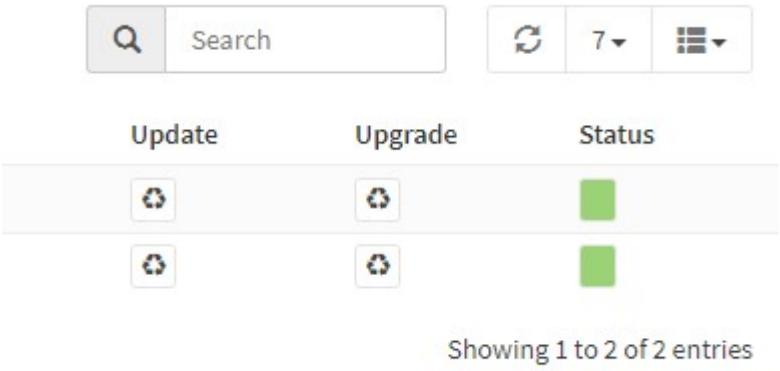
2. Über die Inventarisierung geben hinterlegen wir die IP des Systems und das Dashboard baut dazu einen Button, um direkt auf die jeweilige Firewall zu springen

3. Über regelmäßige API-Calls wird die Version der Firewalls geprüft



4. Für jedes System wir auch ein Button für Minor- und Major Upgrade angeboten und ein Statussymbol (rot/grün) für die Erreichbarkeit des Systems. Falls die Firewall offline ist, wird

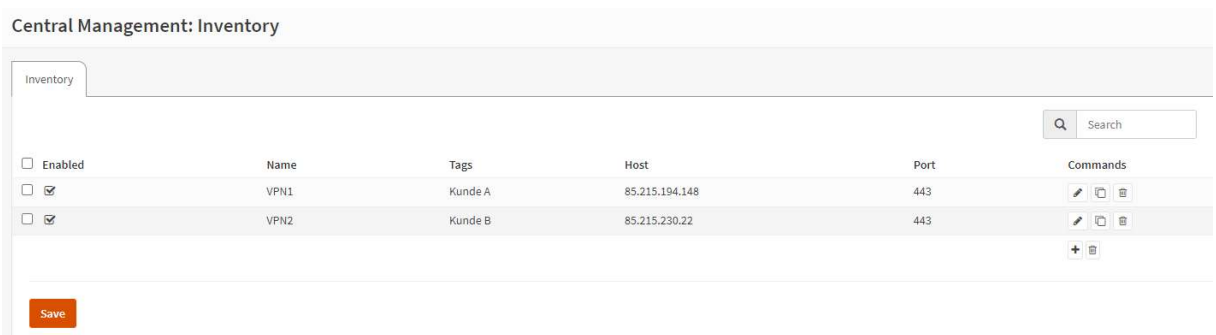
der Button für das Upgrade natürlich ausgegraut. Über das Suchfeld kann nach allen Feldern (bis auf Status) gesucht werden.



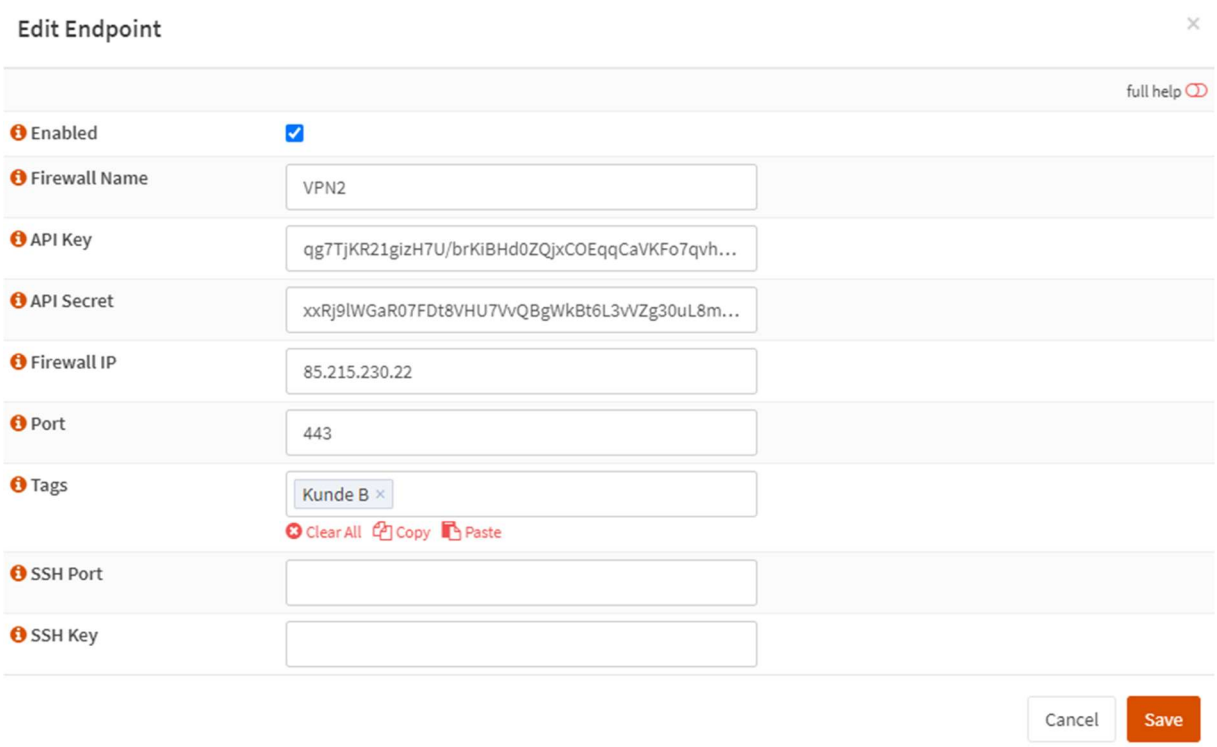
5. Lins neben dem Hostnamen können mehrere Firewalls ausgewählt und der Web GUI und Update Befehl an die ausgewählten Systeme gesendet werden.

Inventory

Über das Inventory können die zu verwaltenden Firewalls gepflegt werden. Das Dashboard greift über die hier hinterlegten Daten auf die jeweiligen Systeme zu. Über den „Klon-Button“ können bequem auch Cluster hinzugefügt werden.



In der Tabelle unten rechts auf das „+“ zum Hinzufügen klicken



Enabled: Aktiviert oder deaktiviert die Firewall für diverse Tasks

Firewall Name: Name der Firewall

API Key: Der Key des jeweiligen Systems

API Secret: Das Secret des jeweiligen Systems

Firewall IP: IP des Zielsystems, die lokale Firewall muss den Zugriff des Central Management zulassen

Port: Port auf dem die Web GUI läuft

Tags: Hinzufügen einer oder mehrerer Tags

SSH Port: Derzeit ohne Verwendung, für zukünftige Features

SSH Key: Derzeit ohne Verwendung, für zukünftige Features

Aliase

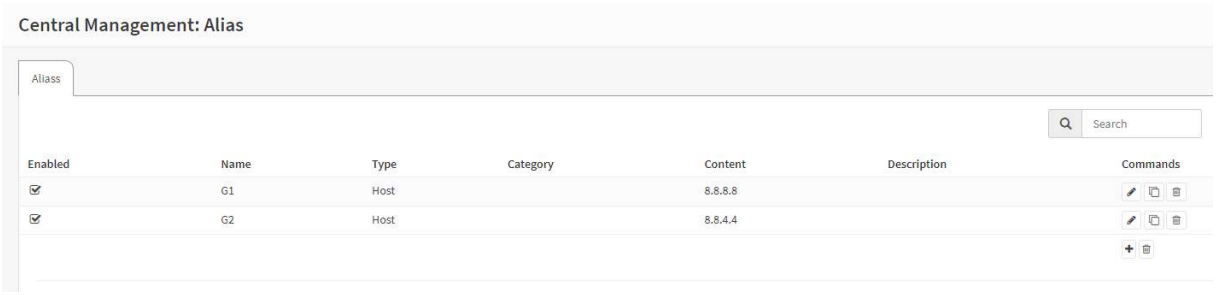
Allgemein

Seit März 2024 können auch Aliase zentral gepflegt werden. Wir legen viel Wert darauf, dass bestehende Installationen mit aufgenommen werden können und somit bestehende Aliase nicht überschrieben werden. Dazu habt es pro Firewallgruppe (z.B. ein Kunde) die Möglichkeit, einen Aliaspräfix mit anzugeben. Dieser wird dann automatisch an den Aliasnamen vorangestellt.

Legt man z.B. den Alias G1 (für Google DNS) mit der IP 8.8.8.8 an und hat in der Gruppe den Präfix BDEMO gewählt, so wird auf allen Firewalls in dieser Gruppe ein Alias „BDEMOG1“ angelegt und kann auch so in den Firewallregeln verwendet werden.

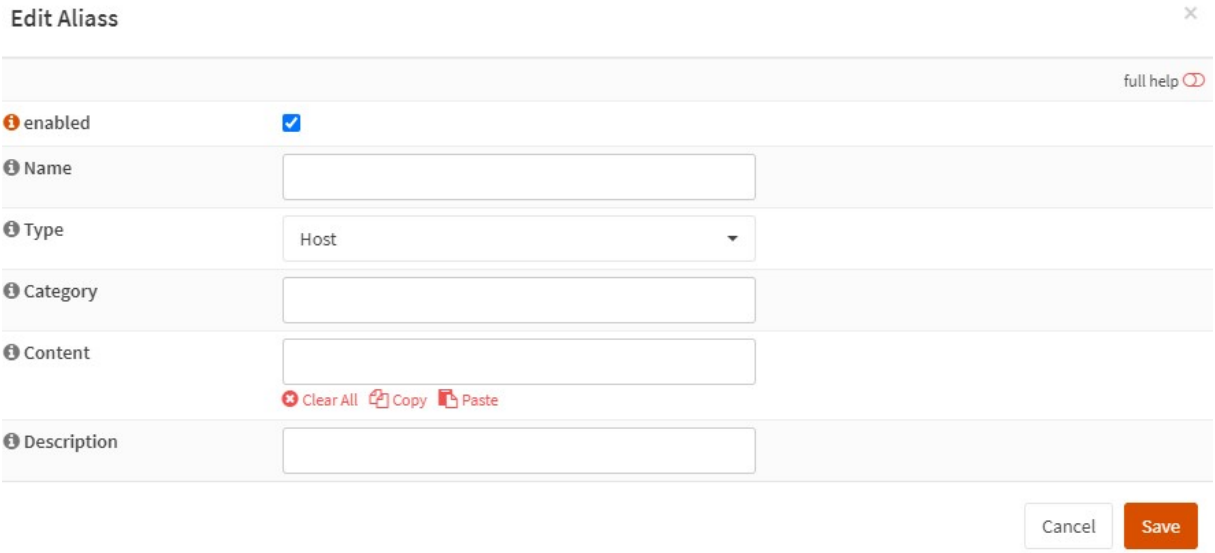
Übersicht

Wie bei OPNsense üblich werden alle Aliase in Tabellenform angezeigt und die Hauptfunktionen (Name, Typ, Kategorie, Inhalt und Beschreibung) gleich in der Übersicht abgebildet.



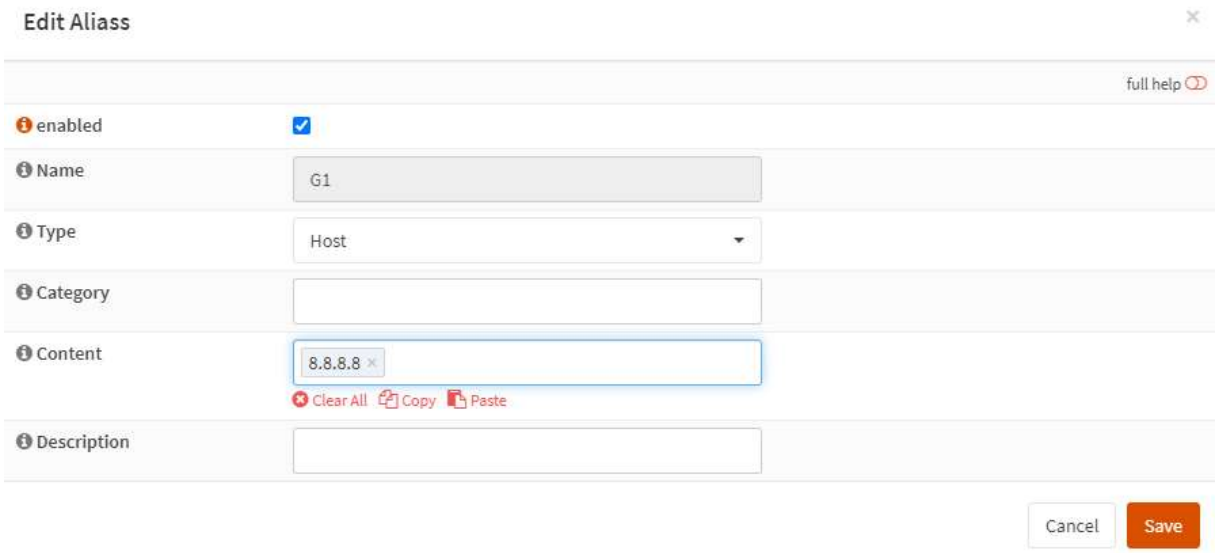
Eintrag

Beim Klicken auf „+“ öffnet sich Dialog für das Hinzufügen eines neuen Alias



Momentan werden nur die Aliastypen „Host“, „Network“, und „Port“ unterstützt. Die Funktionsweise ist identisch wie mit dem Handling lokaler Aliase.

Wichtig zu beachten ist, dass der Aliasename nachträglich NICHT geädert werden kann, da die Zuordnung, die den Firewallregeln über den Namen und nicht eine UUID geregelt wird.



Firewallregeln

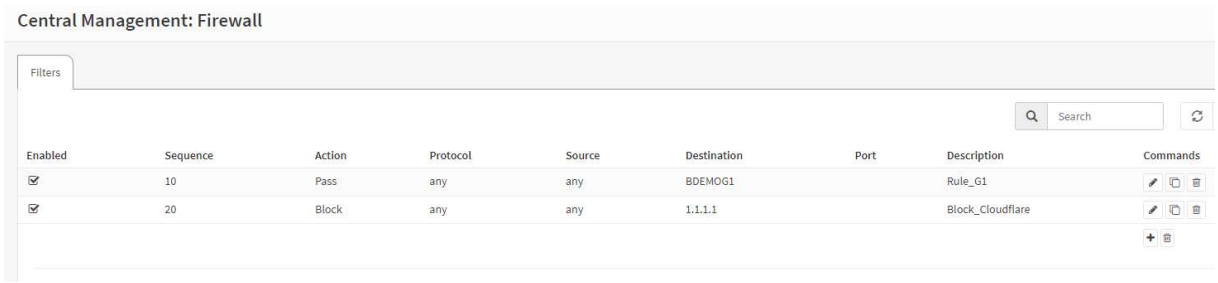
Allgemein

Die Verwaltung von Firewallregeln werden über die API gesteuert und tauchen ab OPNsense Version 24.1 im Untermenü „Automations“ auf. In Versionen vor 24.1 musste noch das Plugin „os-firewall“ nachinstalliert werden, hierauf muss dringend geachtet werden und in den Gruppen bietet das Central Management zusätzlich die Option Plugins zentral auszurollen.

Übersicht

Wie auch bei den Aliasen werden Regeln in einer Standardtabelle gepflegt und nicht wie im legacy Format auf der Firewall lokal.

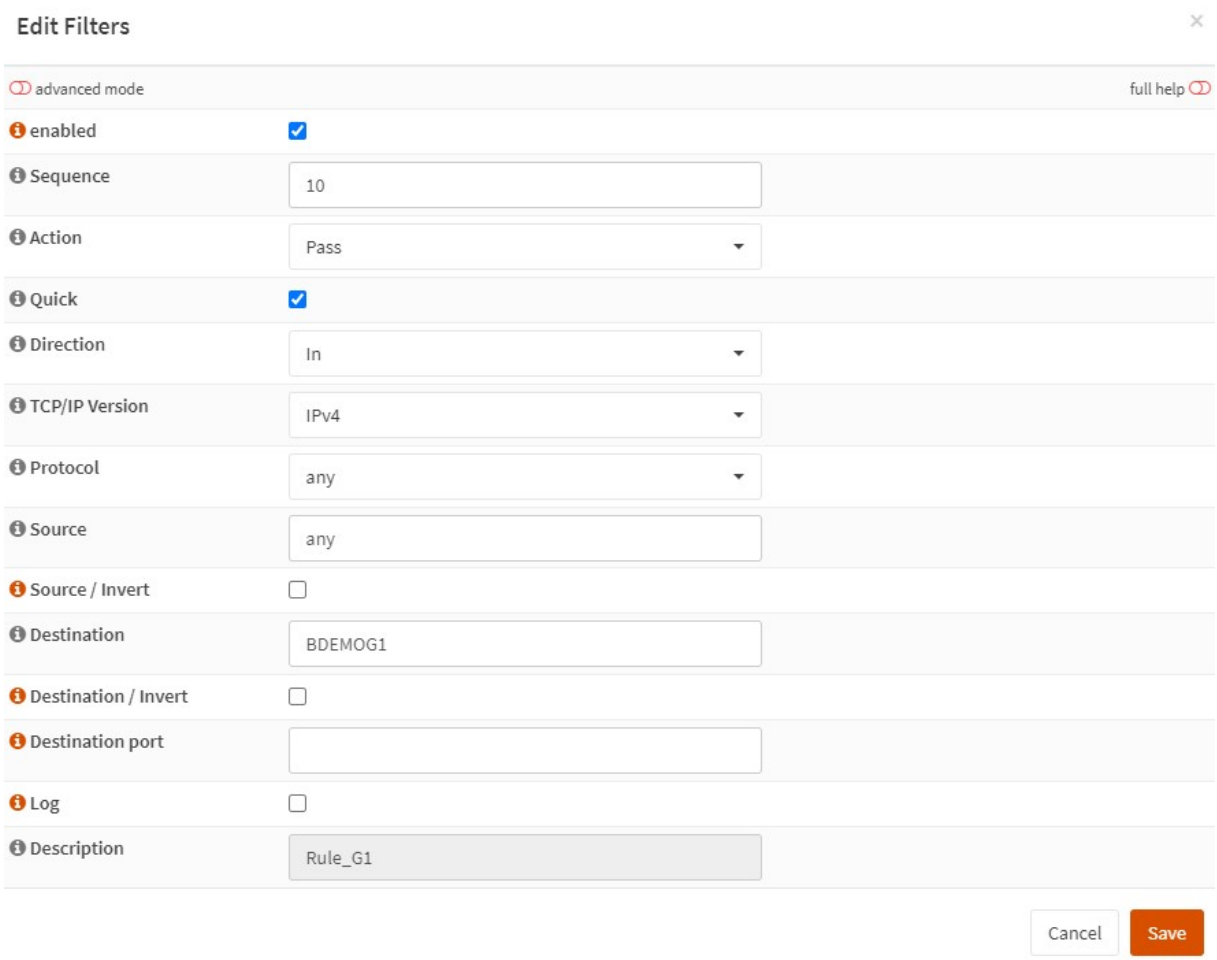
Wichtig: Auch hier kann die Description im Nachhinein nicht geändert werden, da lokale UUIDs und die auf der entfernten Firewall sich unterscheiden. Der eindeutige Identifier ist also auch hier der Name.



Eintrag

Die neue Art über die API Firewallregeln zu pflegen, bietet einen ähnlichen Funktionsumfang und erlaubt es, dank erweiterter Validierung auch frei Aliase zu benennen, sofern sie auch auf der jeweiligen Firewall hinterlegt sind.

Sollte also eine Gruppe Bestandsysteme mit aufgenommen werden und haben diese bereits den Alias „FirmenLAN1“, kann dieser im Textfeld für „Source“ und „Destination“ verwendet werden (Bei Gruppenpräfix diesen voranstellen, siehe Gruppen).



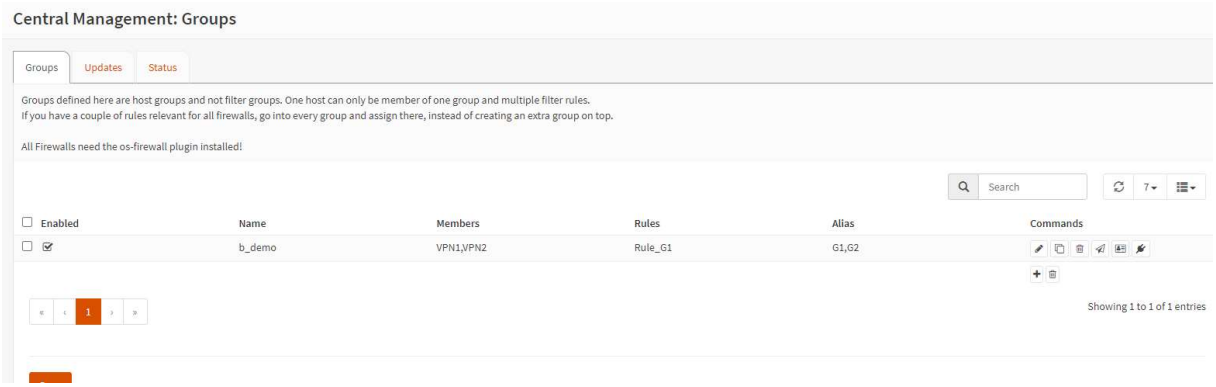
- **Enabled**: Aktivieren oder deaktivieren, die Verteilung erfolgt aber über die Gruppen
- **Sequence**: Positionsnummer, es wird empfohlen in 10er-Schritten zu arbeiten, da so nachträglich Regeln eingefügt werden können
- **Action**: Pass, Block oder Reject; bei „Block“ wird still verworfen, „Reject“ sendet ein „Port unreachable“ an das Quellsystem
- **Quick**: First Match, ohne den Haken werden nachfolgende Regeln ebenfalls überprüft
- **Direction**: Richtung, in der Regel immer „in“
- **TCP/IP Version**: IP-Version
- **Protocol**: IP-Protokoll
- **Source**: Quell-IP oder -Netz, auch Aliase möglich, entweder zentral oder lokal (Name muss bekannt sein)
- **Source / Invert**: Negieren/Umkehren der Quelle
- **Destination**: Ziel-IP oder -Netz, auch Aliase möglich, entweder zentral oder lokal (Name muss bekannt sein)
- **Destination / Invert**: Negieren/Umkehren des Ziels
- **Log**: Soll der Eintrag geloggt werden, taucht mit dem Regelname im „Live View“ auf
- **Description**: Name der Regel, muss eindeutig sein und kann nicht geändert werden, keine Leerzeichen erlaubt

Gruppen

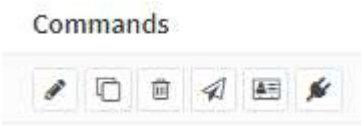
Allgemein

Gruppen sind das neue Herzstück des Central Management. Hier werden mehrere Firewalls zu Gruppen zusammengefügt. Es handelt sich hierbei um Hostgruppen und nicht Funktionsgruppen. Das bedeutet eine Firewall sollte nicht in mehreren Gruppen sein, sofern diese Gruppe auch zum Verteilen von Aliasen und Firewallregeln verwendet wird, um Überschneidungen auf den jeweils lokal gepflegten Aliasen und Regeln zu vermeiden.

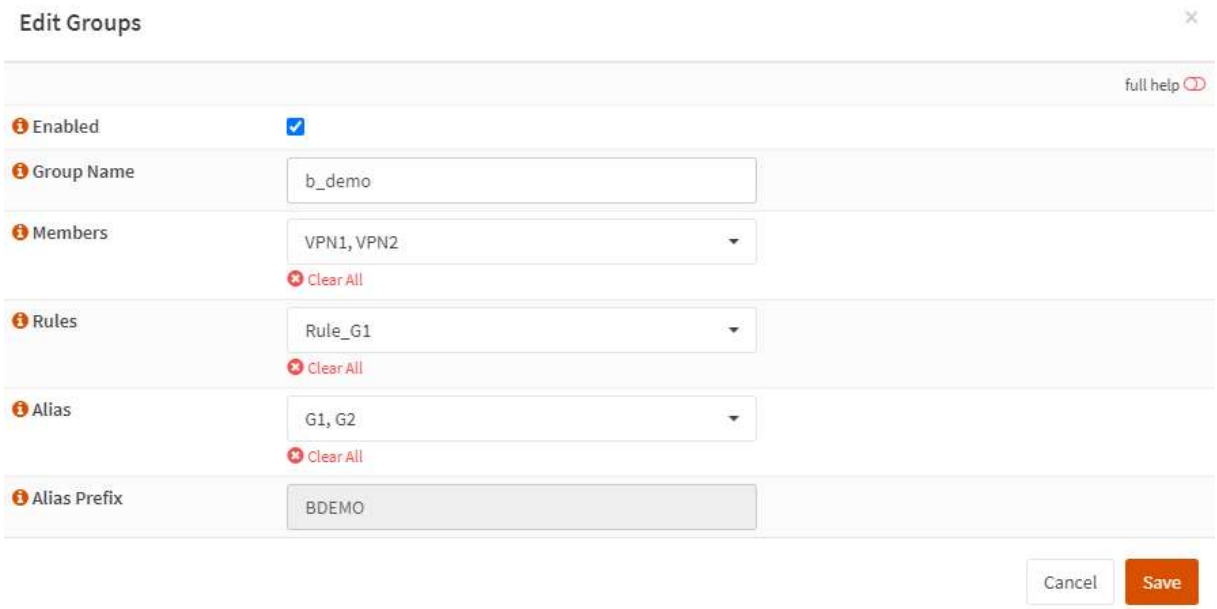
Übersicht



Anders als bei den Aliasen und Regeln sind in der Spalte Commands noch weitere Funktionen hinterlegt auf die später im Detail eingegangen wird.



Eintrag



Enabled: Aktivieren oder Deaktivieren einer Gruppe

Group Name: Gruppenname, der die Firewalls beinhaltet, wie üblich keine Leerzeichen erlaubt

Members: Hier werden die Firewalls über ein multi-select Feld ausgewählt. Bitte darauf achten, dass eine Firewall zwar in mehreren Gruppen sein kann, aber dann jeweils immer die Aliase und Regeln der anderen Gruppe beim Deploy gelöscht werden.

Rules: Die einzelnen Regeln die auf die jeweilige Gruppe ausgerollt werden. Die Reihenfolge wird innerhalb der Regel über die Sequence Number geregelt

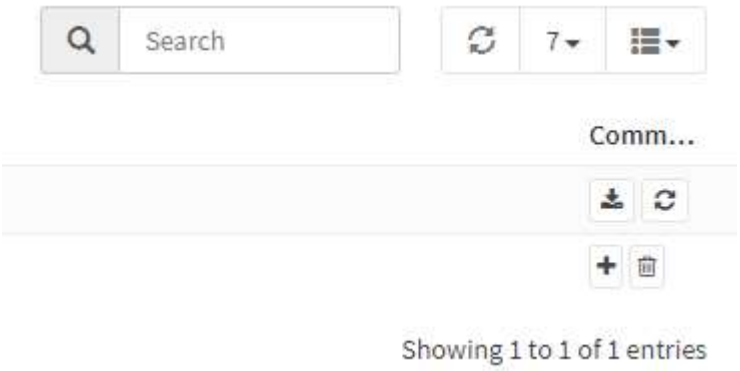
Alias: Der auszurollende Alias. Bei einem Alias Präfix wird der Präfixname direkt an den Alias vorangestellt. Auf dem Central Management wird er zwar ohne das Präfix angezeigt, falls er in einer Regel zum Einsatz kommt, muss in der Firewallregel auch das Präfix angegeben werden.

Alias Präfix: Der Alias Präfix dient dazu, dass Aliase die zentral gepflegt werden, nicht die lokalen Aliase überschreiben. Wird z.B. der Portalias „HTTP_HTTPS“ mehrfach in lokal gepflegten Regeln verwendet, kann dies auch weiterhin zentral geschehen, ohne dass der lokale Alias überschrieben wird. Der Wert kann aus Sicherheitsgründen im Nachhinein nicht geändert werden.

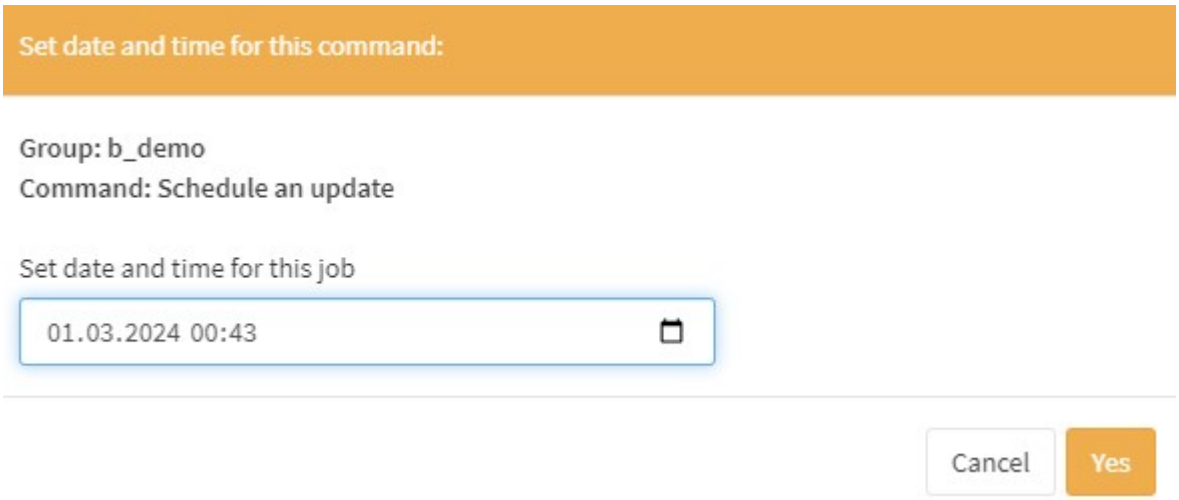
Update

Im Reiter „Update“ könnte Updates und Major-Upgrades geplant werden. Die Sortierung im Reiter „Groups“ und „Update“ kann am Anfang abweichen, Empfehlung ist, in beiden Tabs nach Namen zu sortieren und die Einstellung wird dauerhaft im Browser gespeichert.

Je Gruppe stehen 2 Commands mit jeweils Update und Upgrade zur Verfügung



Nach einem Klick öffnet sich ein Popup mit der Auswahl von Datum und Uhrzeit



Mit den Buttons „Show all jobs“ und „Clear all jobs“ werden die aktuell geplanten Aufgaben angezeigt und können bei Bedarf wieder entfernt werden.

Der Reiter „Status“ liefert die Ausgabe der jeweiligen Kommandos zurück.

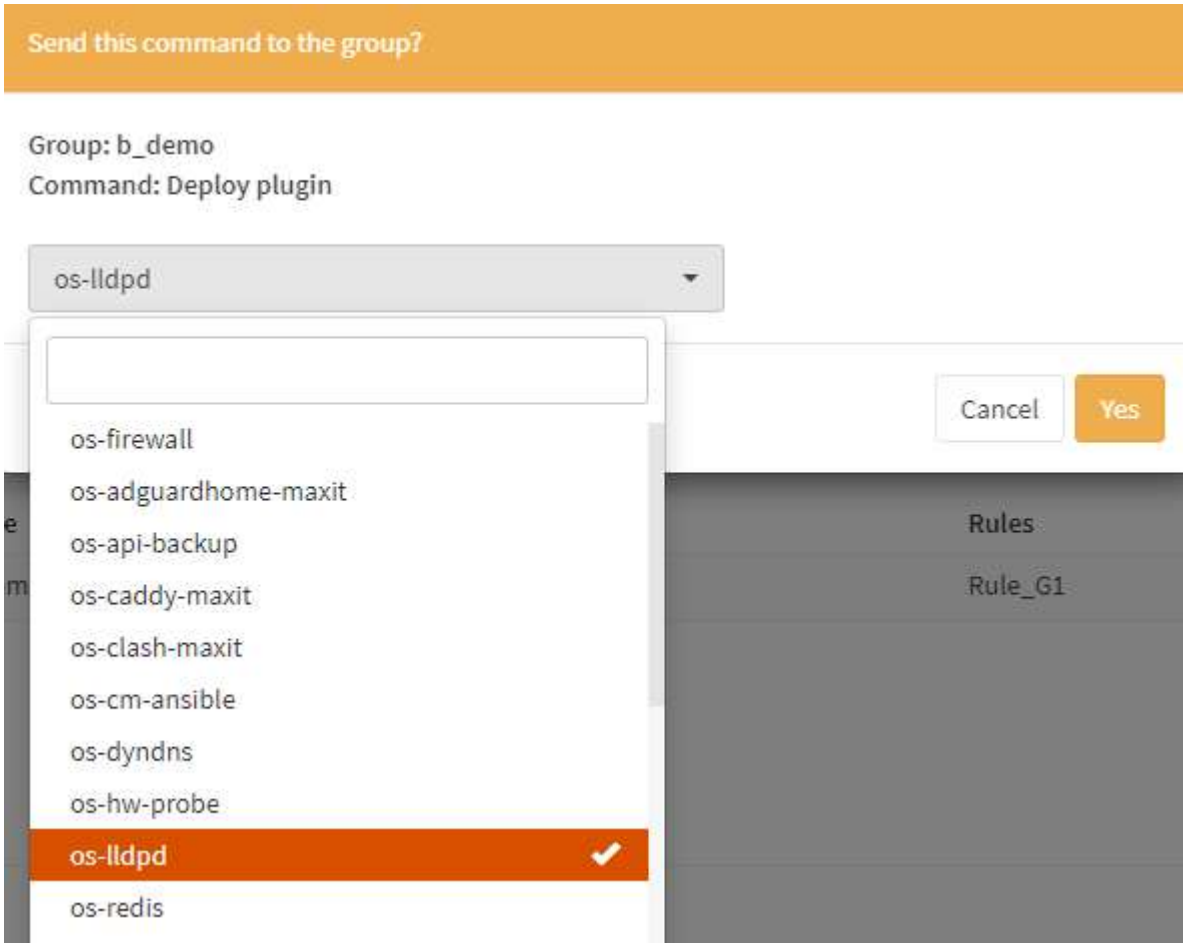
Commands

In der Spalte „Commands“ sind alle relevanten Buttons zum Steuern der Gruppen.

Die ersten 3 sind wie üblich „editieren“, „klonen“ und „löschen“. Der Papierflieger dient zum Ausrollen von Firewallregeln. Falls in neu angelegten Firewallregeln auch neue Aliase enthalten sind, müssen erst die Aliase über die Karteikarte ausgerollt werden. Sowohl bei Regeln als auch bei Aliasen

werden beim deployen erst alle Einträge gelöscht und dann neu hinzugefügt. Erst im Anschluss folgt der virtuelle Klick auf „Apply“.

Über den Stromstecker kann über die ganze Gruppe hinweg auch Plugins installiert werden. Voraussetzung dafür ist eine aktuelle OPNsense Version auf den jeweiligen Firewalls:



Troubleshooting


```
TASK [opnsense-fw-rules : Get existing rules at VPN1] *************************
fatal: [VPN1 -> localhost]: FAILED! => {"cache_control": "no-store, no-cache, must-revalidate", "changed": false, "connection": "close", "content_length": "89", "content_security_policy": "default-src 'self' ;img-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;style-src 'self' 'unsafe-inline' 'unsafe-eval' ;", "content_type": "application/json", "date": "Thu, 29 Feb 2024 20:08:03 GMT", "elapsed": 0, "expires": "Thu, 19 Nov 1981 08:52:00 GMT", "json": {"message": "controller OPNsense\\Firewall\\Api\\FilterController not found", "status": 400}, "msg": "Status code was 400 and not [200]: HTTP Error 400: Bad Request", "pragma": "no-cache", "redirected": false, "referrer_policy": "same-origin", "server": "OPNsense", "set_cookie": "PHPSESSID=993773270599949e78c3dc3c83d58294; path=/; secure; HttpOnly", "status": 400, "url": "https://85.215.194.148:443/api/firewall/filter/searchrule", "x_content_type_options": "nosniff", "x_frame_options": "SAMEORIGIN", "x_xss_protection": "1; mode=block"}
ok: [VPN2 -> localhost]
```


Die Meldung wie oben „"controller OPNsense\\Firewall\\Api\\FilterController not found"“ kommt in der Regel, wenn die Firewall älter als Version 24.1 und das Plugin os-firewall nicht installiert ist.

Beim ersten Aufruf vom Dashboard kann bei einer großen Anzahl am Anfang noch die Version auf Timeout stehen, wenn der API Call nicht rechtzeitig beantwortet wird (z.B. wegen höherer Latenz). Die Versionsabfrage läuft im Hintergrund jede Minute und pendelt sich dann in 2-3 Wiederholungen ein.

failed: [TK_DEMO_FW2 -> localhost] (item={'key': 'Rule_G1', 'value': {'enabled': 1, 'sequence': 10, 'action': 'pass', 'quick': 1, 'interface': None, 'direction': 'in', 'ipprotocol': 'inet', 'protocol': 'any', 'source_net': 'any', 'source_port': None, 'source_not': 0, 'destination_net': 'BDEMOG1', 'destination_not': 0, 'destination_port': None, 'gateway': None, 'log': 0, 'description': 'Rule_G1'}}) => {"ansible_loop_var": "item", "attempts": 3, "changed": false, "connection": "close", "content_length": "111", "content_type": "application/json; charset=UTF-8", "cookies": {}, "cookies_string": "", "date": "Mon, 04 Mar 2024 16:58:28 GMT", "elapsed": 0, "item": {"key": "Rule_G1", "value": {"action": "pass", "description": "Rule_G1", "destination_net": "BDEMOG1", "destination_not": 0, "destination_port": null, "direction": "in", "enabled": 1, "gateway": null, "interface": null, "ipprotocol": "inet", "log": 0, "protocol": "any", "quick": 1, "sequence": 10, "source_net": "any", "source_not": 0, "source_port": null}}, "json": {"result": "failed", "validations": {"rule.destination_net": "BDEMOG1 is not a valid source IP address or alias."}}, "msg": "OK (111 bytes)", "redirected": false, "server": "OPNsense", "status": 200, "url": "https://157.97.111.246:443/api/firewall/filter/addRule"}

Die obige Meldung kommt beim Deploy von Regeln wo noch kein Alias ausgerollt wurde. Falls so ein Fehler auftritt, wird auf dem betroffenen System das Regelwerk auch nicht ausgeführt.