

Inhalt

Einleitung	2
Zielsetzung	2
Bereitgestellte Services	2
Web Application Proxy (WAP) & Active Directory Federation Service (ADFS)	2
Network Policy Service (NPS).....	2
VPN-Service	2
Planung der Migration.....	2
Umstellung von Web Application Proxy auf HAProxy (2019-10-27!)	3
Vorgeschichte und IST-Zustand	3
HAProxy für Exchange.....	4
IST-Zustand.....	4
Umbau	6
HAProxy für RDS.....	18
HAProxy für PRTG.....	22
Testlauf HA	26
Bereinigung WAP	28
Entfernung von ADFS und WAP	28
Vorbereitung	28
Entfernen von WAP auf WS-RA1	30
Entfernen von WAP auf WS-RA2	31
Entfernen von ADFS auf WS-DC2 (Slave).....	32
Entfernen von ADFS auf WS-DC1 (Master)	35
Bereinigung in der PFSense	36

Einleitung

Zielsetzung

Meine Serverumstellung auf Windows Server 2019 geht in die nächste Runde. Dieses Mal sind die beiden Server WS-RA1 und WS-RA2 dran. Beide laufen aktuell unter Windows Server 2016 als virtuelle Maschinen. Im folgenden Abschnitt prüfe ich, welche Services auf den Servern laufen und wie ich diese migrieren werde.

Bereitgestellte Services

Web Application Proxy (WAP) & Active Directory Federation Service (ADFS)

Früher nutzte ich sie für die Bereitstellung eines Web Application Proxy (**WAP**) Clusters. Mit diesem konnte ich eingehende Verbindungsanfragen von außen über HTTPS nach dem SNI auf die richtigen, internen Server aufteilen. Dies war notwendig, da ich von meinem Provider nur eine öffentliche IPv4-Adresse bekommen habe, aber mehrere Anwendungen von außen über den Port 443 erreichbar sein sollten.

Beide Server stellten das Frontend des Services bereit. Das Backend sind 2 ADFS-Services, die im Farm-Mode auf meinen Domain Controllern laufen.

Wie vor jeder Migration eines Servers überlege ich auch in diesem Fall, ob die Services so noch benötigt werden. Mittlerweile habe ich WAP durch einen HA-Proxy in meiner Firewall-Appliance unter PFSense abgelöst. Damit würde eine komplette Deinstallation von WAP genügen. Durch den Wegfall wäre dann auch die ADFS-Farm auf meinen Domain Controllern überflüssig. Das erleichtert dann später auch deren Migration.

Die Umstellung auf den HAProxy habe ich in dieses WSHoWto als eigenen Punkt integriert. Die Arbeiten dazu habe ich aber schon im Oktober ausgeführt.

Network Policy Service (NPS)

Dazu stellt der Server WS-RA1 noch einen Network Policy Service (**NPS** – auch als Radius Server bekannt) bereit. Diesen nutzt ein WLAN-Accesspoint für WPA2-Enterprise-Anmeldungen meiner Clients. Die Funktion wird weiter benötigt und muss daher auf einen neuen Server migriert werden. Dabei halte ich mir eine Erweiterung auf eine hochverfügbare Lösung offen.

Die Migration wird mittels Wipe & Load vorgenommen, da ich aktuell keine Hochverfügbarkeitsanforderung gestellt habe. Für den Wechsel ist eine Downtime erforderlich.

Diesen Teil der Migration führe ich separat aus, da der Artikel sonst zu lang wird.

VPN-Service

Die Namen der beiden Server habe ich aus dem Servicennamen RemoteAccess abgeleitet. Ich nutzte die Server als VPN-Server für die Einwahl von extern.

Die Formulierung in der Vergangenheitsform deutet es schon an: Ich nutze seit Ewigkeiten kein VPN mehr für die Arbeiten von außen. Diese Funktion bilde ich über meine Remote Desktop Services dank des RD-Gateways ab. Der Service VPN wird also nicht mehr benötigt und kann einfach entfernt werden.

Diesen Teil der Migration führe ich separat aus, das der Artikel sonst zu lang wird.

Planung der Migration

Dieser Artikel befasst sich mit der Entfernung des Web Application Proxy Cluster und der ADFS-Farm. Dazu habe ich vorher ausgeführte Konfiguration de PFSense HAProxies integriert. Die Migration des NPS wird in einem anderen Artikel beschrieben.

Damit sind die Arbeitsschritte für die komplette Migration klar:

- Schritte in diesem Artikel
 - Zuerst entferne ich alle nicht mehr benötigten Services und deren Konfigurationen in der richtigen Reihenfolge.
- Schritte im nächsten Artikel

- Danach migriere ich den Service NPS auf einen neuen Windows Server 2019 mit dem Namen WS-NPS1.
- Zuletzt entferne ich die beiden alten Server aus meiner Infrastruktur.

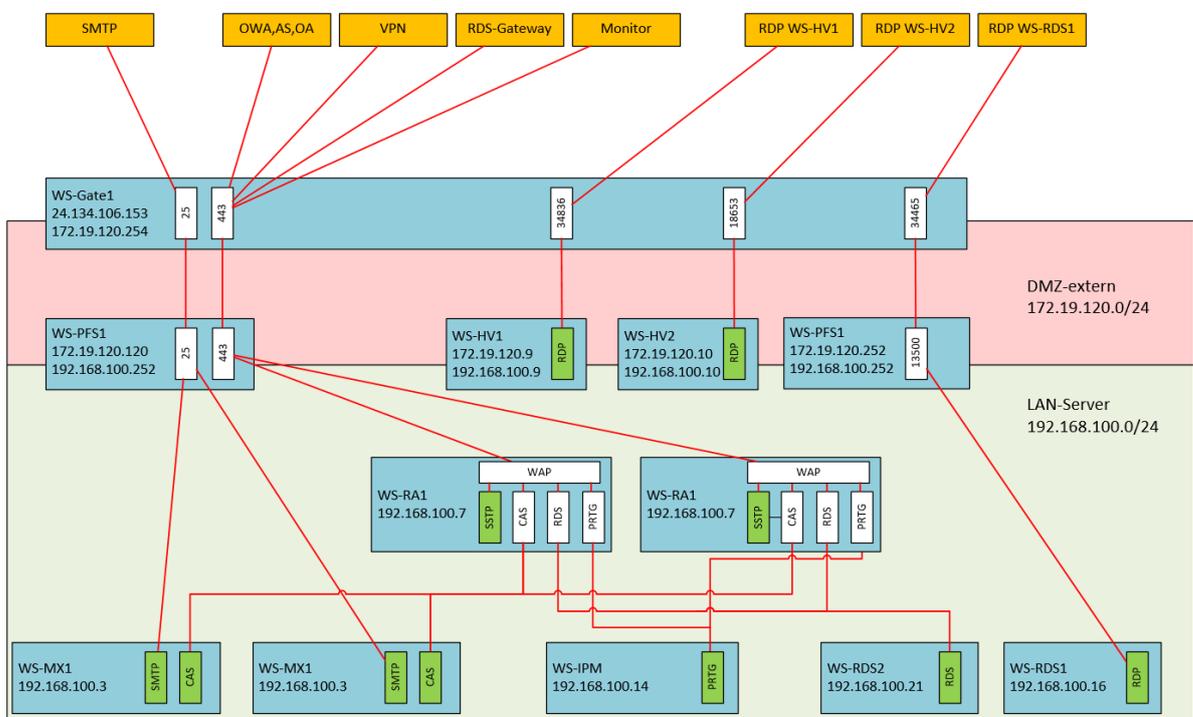
Für die Migration des NPS werde ich den neuen Server neben dem alten synchron aufbauen. Der eigentliche Austausch wird durch die Übergabe der alten IPv4-Konfiguration an den neuen Server vorgenommen. Denn nur über diese IPv4 findet der WLAN-AccessPoint den NPS-Server. Damit spare ich mir die Rekonfiguration des WLAN-AccessPoints und die Anpassung der Firewall-Ausnahmen. Und ich könnte auch schnell wieder auf den alten Server zurückschwenken, indem ich die IP-Änderung wieder zurücknehme. Ein Rollback-Szenario ist immer gut.

Umstellung von Web Application Proxy auf HAProxy (2019-10-27!)

Dieses Kapitel hatte ich bereits vor 2 Monaten geschrieben und administrativ bearbeitet. Damals hat es aber nirgends richtig reingepasst. Daher füge ich es hier an diese Stelle ein.

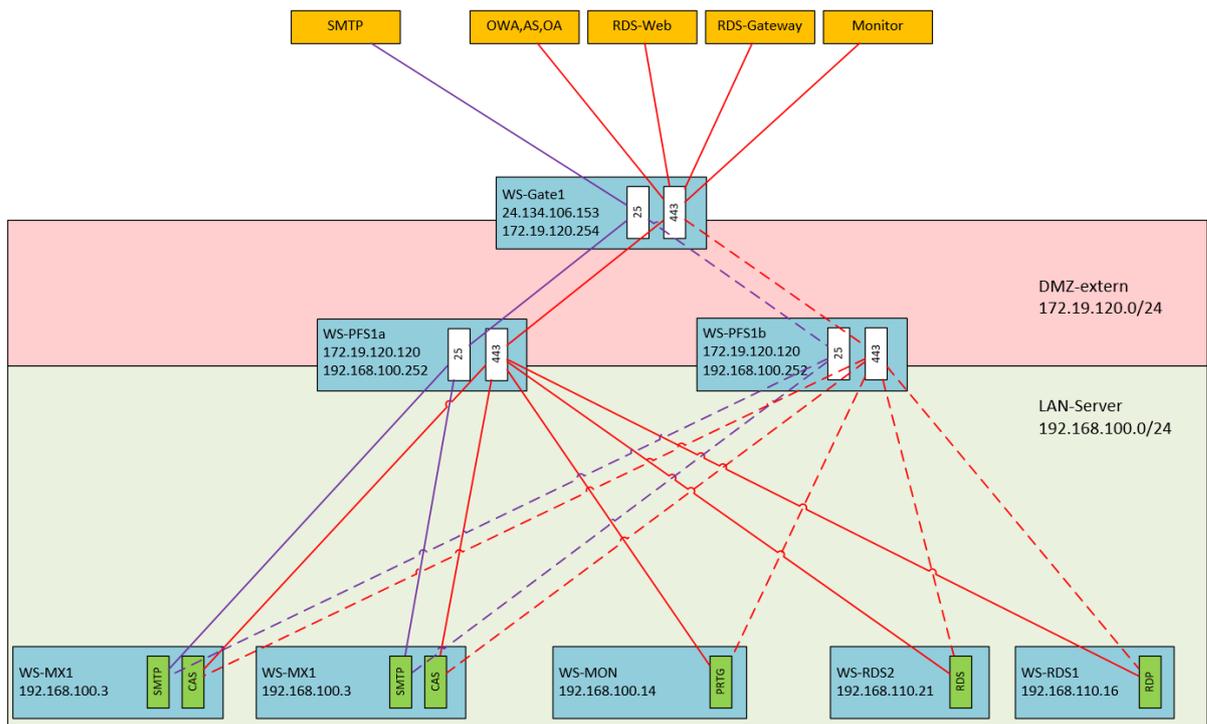
Vorgeschichte und IST-Zustand

Ich wollte meinen Web Application Proxy durch einen HAProxy ablösen. Das Konstrukt ist kompliziert und fehleranfällig geworden. Ursprünglich wollte ich einfach mehrere Webanwendungen mit https auf dem gleichen Port (443) auf der gleichen externen IPv4-Adresse veröffentlichen. Dazu nutzte ich 2 Web Application Proxy Server – beides sind virtuelle Maschinen, verteilt auf 2 Hyper-V-Hosts. Primär arbeiteten beide mit einem Windows Network Loadbalancer Feature unter einer virtuellen IP-Adresse. Für diese erstellte ich in meinen Internetrouter ein Portforwarding. Aber NLB unter Windows ist einfach schlecht. Und da kam mir eine Funktion meiner Linux Firewall gelegen: der HAProxy. Dieser kann als intelligenter Loadbalancer die eingehenden Verbindungen verteilen und Fehler ausgleichen. Das sah dann so aus (diese Zeichnung stammt aus meiner Infrastruktur-Dokumentation 😊). Man erkennt hoffentlich im oberen Bereich die verschiedenen, extern verfügbaren Anwendungen und deren Weg nach intern. Die beiden Server WS-RA1 und WS-RA2 konnten die vom Client angesprochenen Namen auswerten und danach die Verbindung an das richtige Backend leiten. Und vor diesen beiden Servern befindet sich meine PFSense WS-PFS1 und deren HAProxy:



Das geniale an dem HAProxy ist, dass er die Funktion des Web Application Proxies direkt übernehmen kann. Damit wird die Abhängigkeitskette für meine externen Anwendungen deutlich schlanker: ich benötige die beiden RemoteAccess-Server WS-RA1 und WS-RA2 nicht mehr. Und WAP benötigt im Backend ein Active Directory Federation Service. Diesen Service hatte ich ebenfalls hochverfügbar auf 2 Servern installiert. Diese kann ich damit ebenfalls verschlanken.

Das wird dann meine Infrastruktur für externe Services:

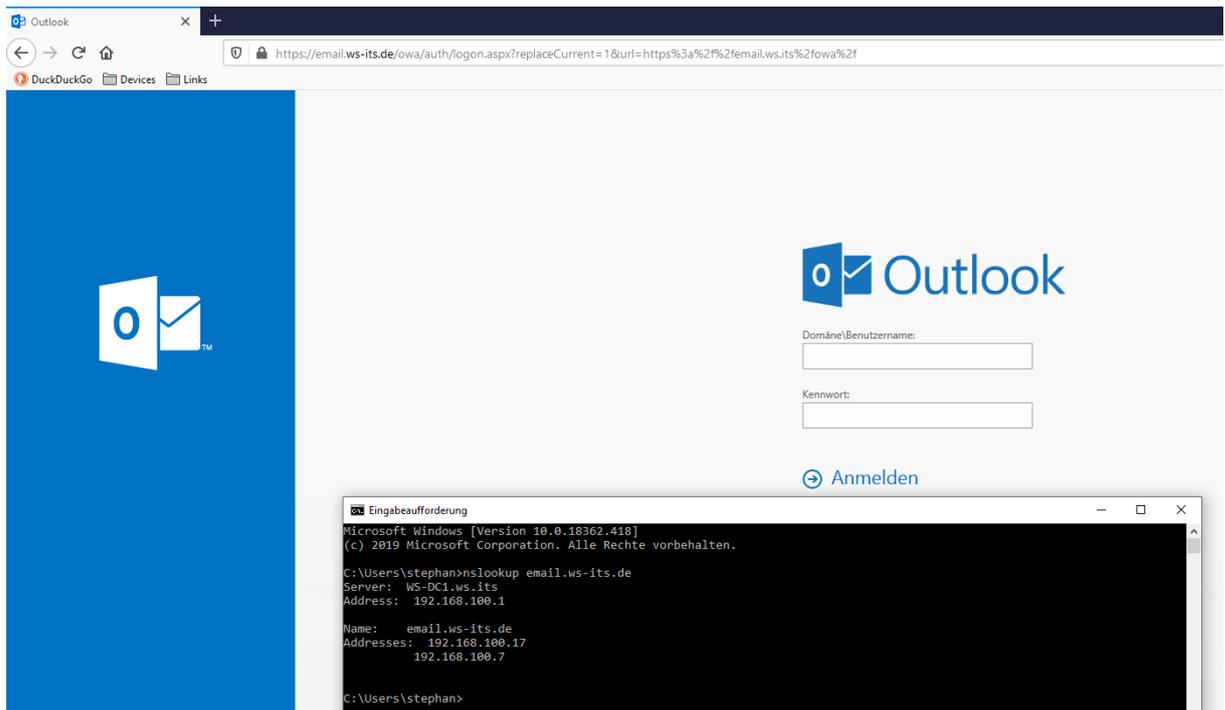


Sieht doch gleich viel einfacher aus, oder? Zwei PFSense-Systeme als virtuelle Maschinen auf unterschiedlichen Hyper-V-Hosts arbeiten als CARP-Cluster und stellen darüber einen hochverfügbaren HAProxy bereit, der vom Internetrouter weitergeleitete Pakete auf Port 443 erhält. Und diese Pakete werden nach ihrem Ziel analysiert und intern an die richtigen Systeme weitergereicht.

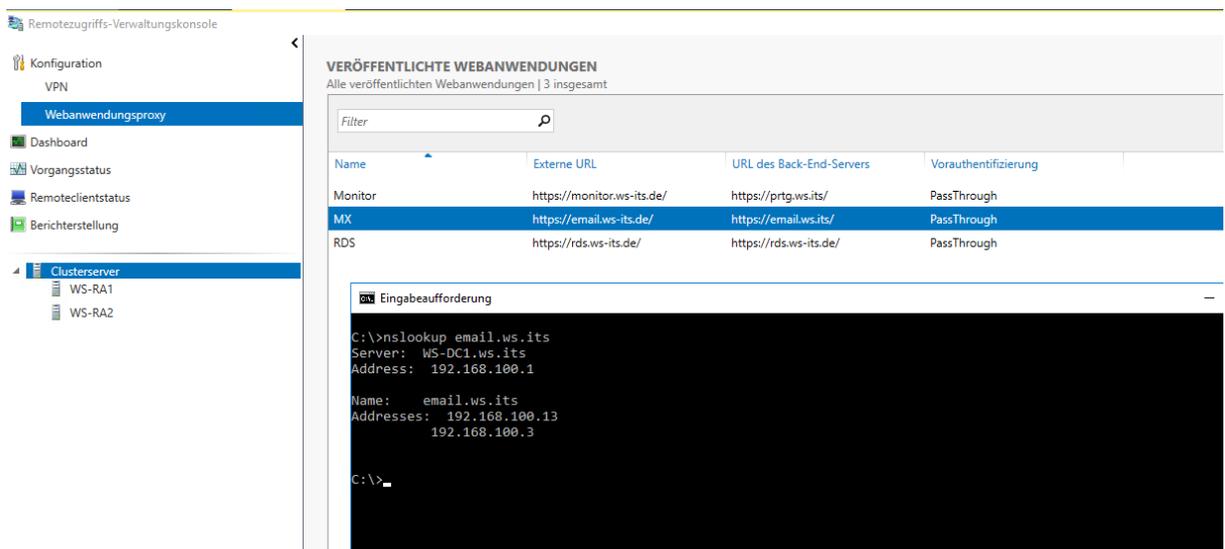
HAProxy für Exchange

IST-Zustand

Ein für mich sehr wichtiger Service ist der Zugriff auf meine Mailserver. Aktuell unterscheide ich zwei unterschiedliche Zugriffswege: den Zugriff von intern und den Zugriff von extern. Für beide verwende ich den gleichen Namespace email.ws-its.de. Meine interne Domain heißt aber ws.its. Ich muss also einen Trick anwenden. Greife ich von intern zu, dann löst mein eigener DNS-Server auf die beiden IP-Adressen der RemoteAccess-Server auf:

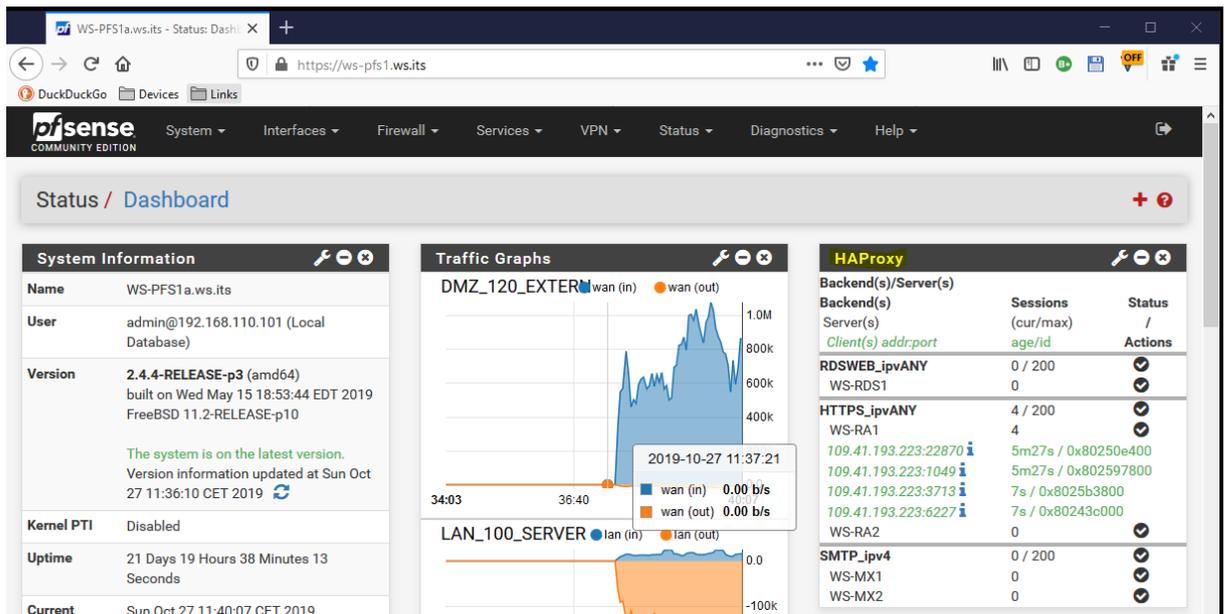


Der Benutzer kommt also erst einmal an einem der beiden Web Application Proxies raus. Die Verteilung läuft dabei über DNS-Roundrobin. Am WAP findet dann der Redirect auf den Namen der beiden Mailserver statt – ebenfalls über DNS-Roundrobin:

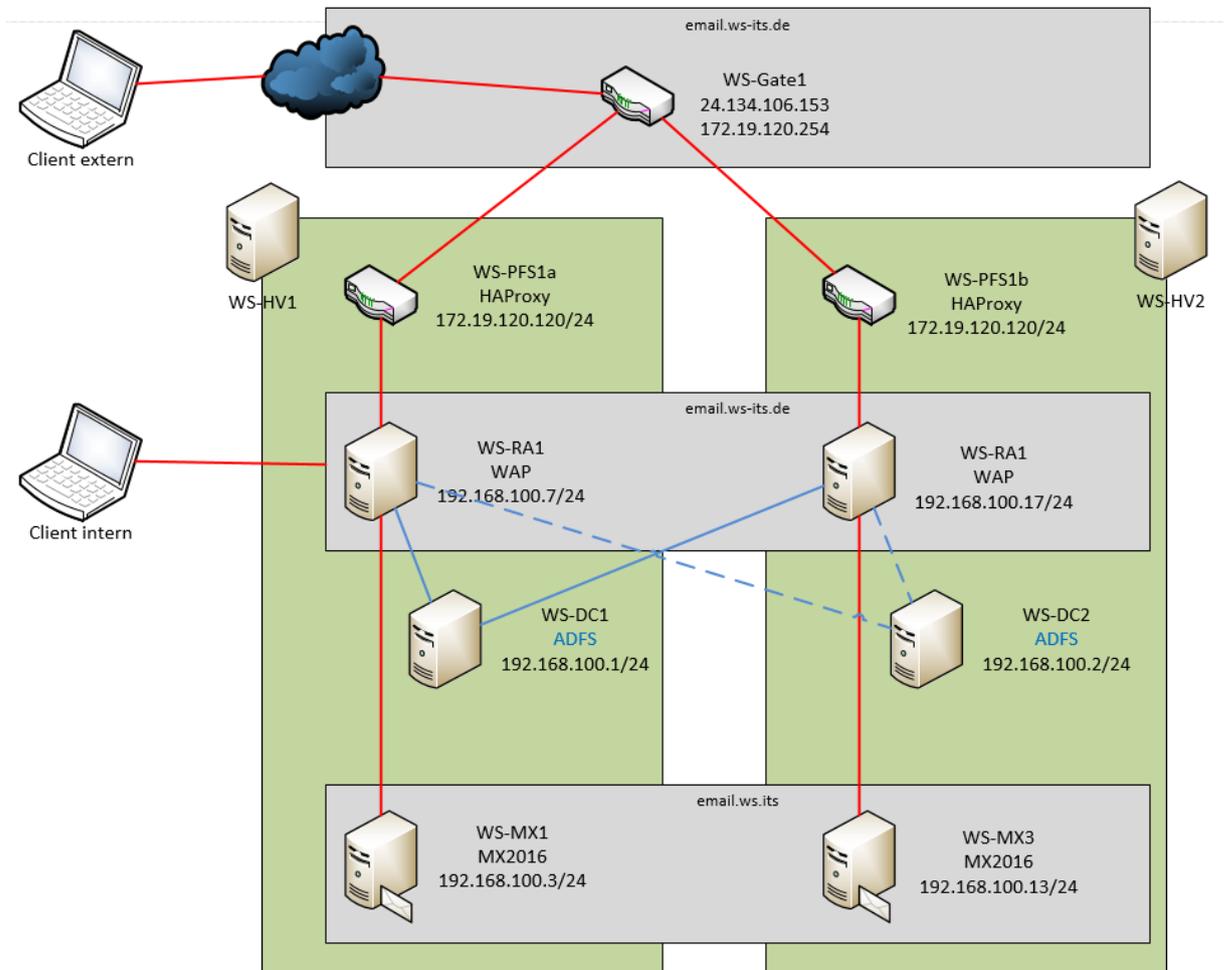


Das hat den Nachteil, dass bei einem Ausfall eines der 4 Servern (WS-MX1, WS-MX2, WS-RA1, WS-RA2) oder beim Ausfall eines darunterliegenden Hyper-V-Hosts ggf. lange Verbindungszeiten zu erwarten sind. Clients benötigen einige Zeit für den DNS-Timeout, bevor sie auf den nächsten DNS-Roundrobin-Wert springen.

Und damit nicht genug: Von extern kommt die Verbindung über meinen HAPoxy auf die WAP-Server rein. Also ein weiterer Hop bzw. eine weitere Technologie, welche die Business Continuity nicht gerade verbessern:

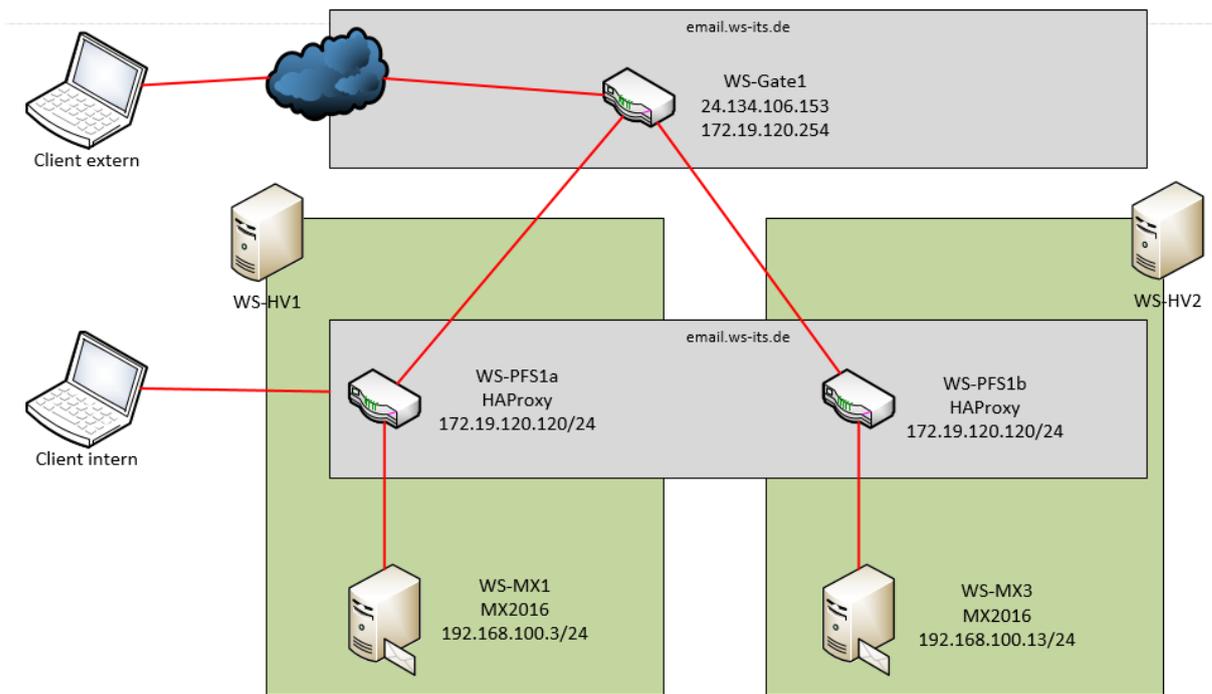


So schaut die Konstruktion schematisch aus. Und die ADFS-Server hab ich als Abhängigkeit mal mit dazu genommen:



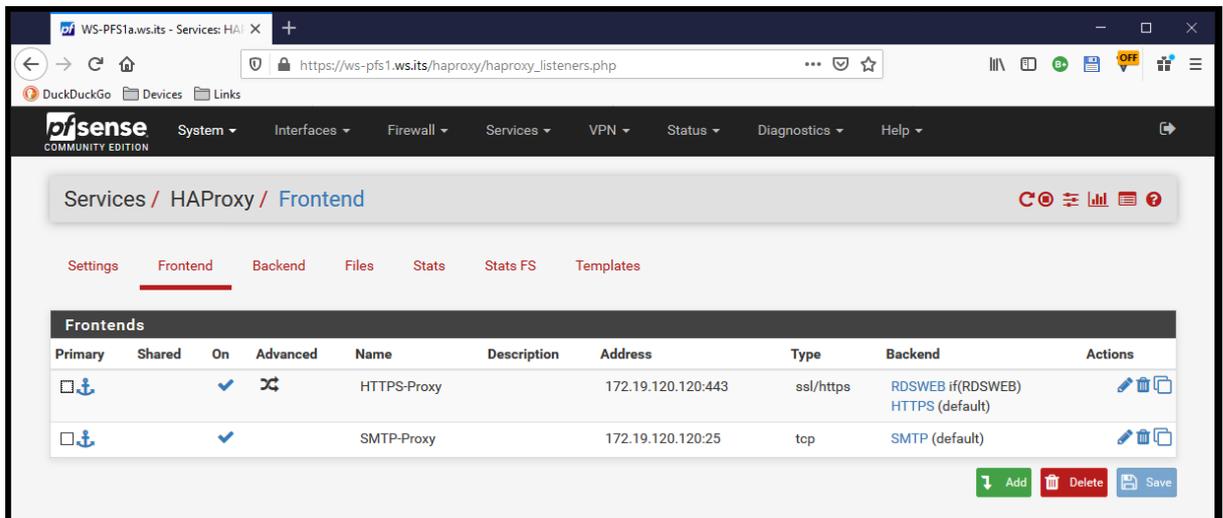
Umbau

Und so wird die Konstruktion nach dem Umbau aussehen:

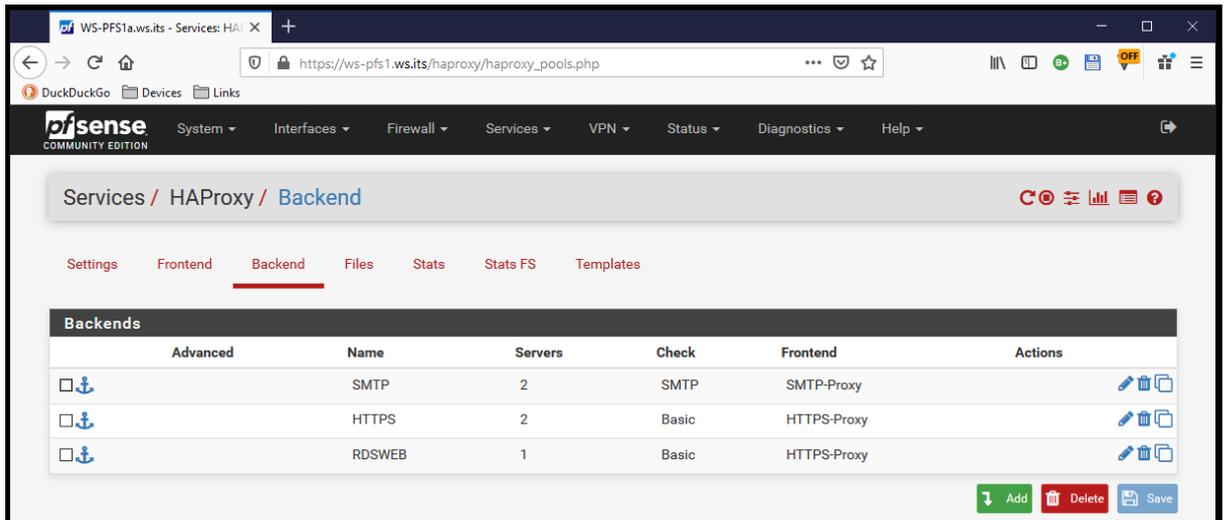


Das ist eine deutliche Vereinfachung, oder?

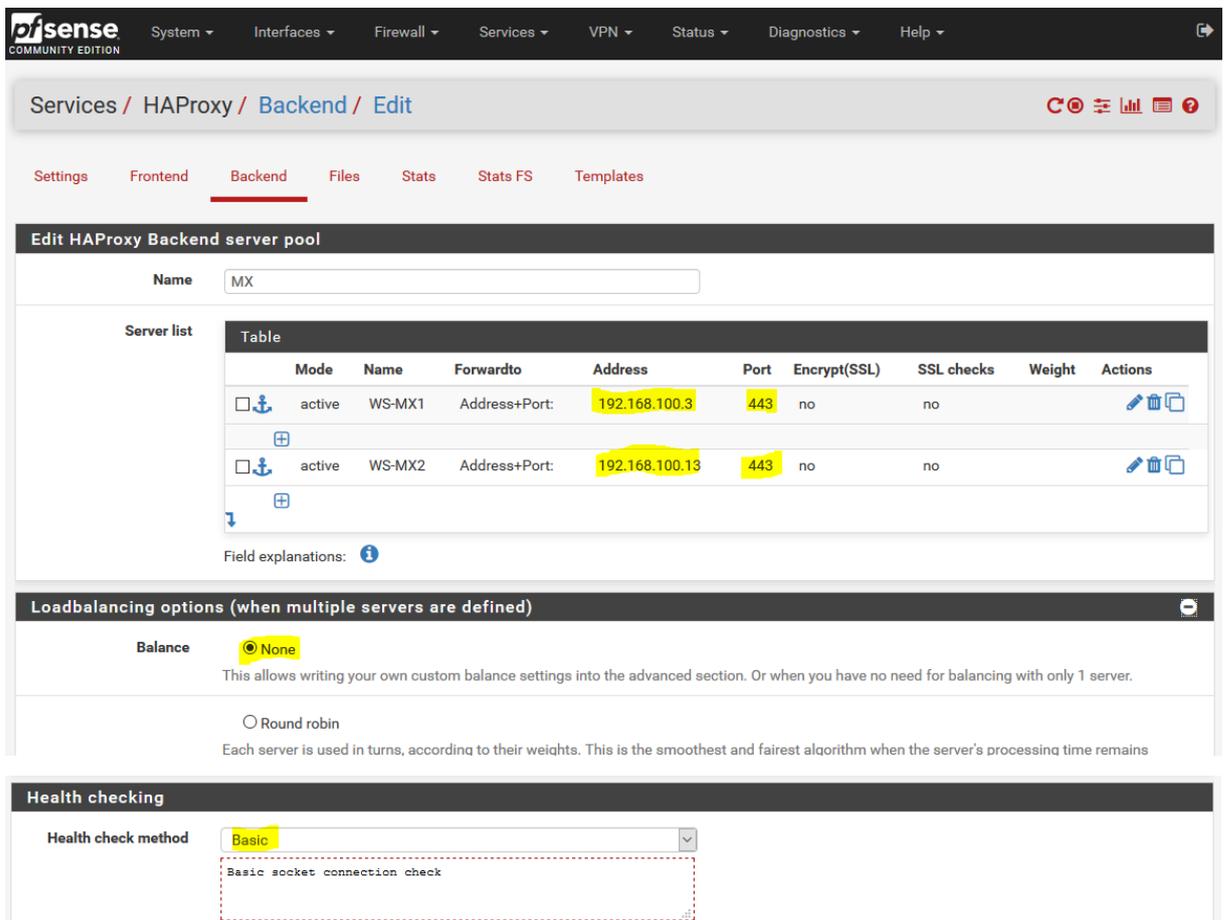
Zuerst editiere ich in meiner primären PfSense das Modul HAProxy. Von der Hauptseite mit den Frontends geht es zu den Backends:



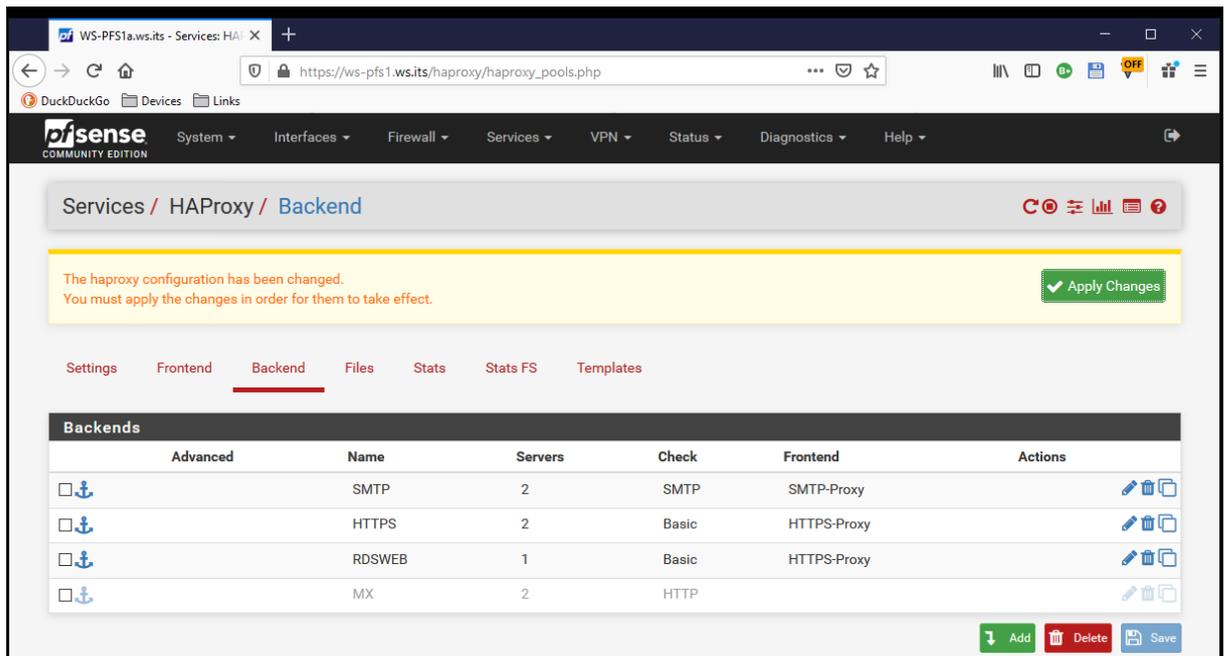
Dort erstelle ich ein neues Backend für die Kommunikation mit meinen beiden Mailservern. Über den Schalter add ist das recht einfach:



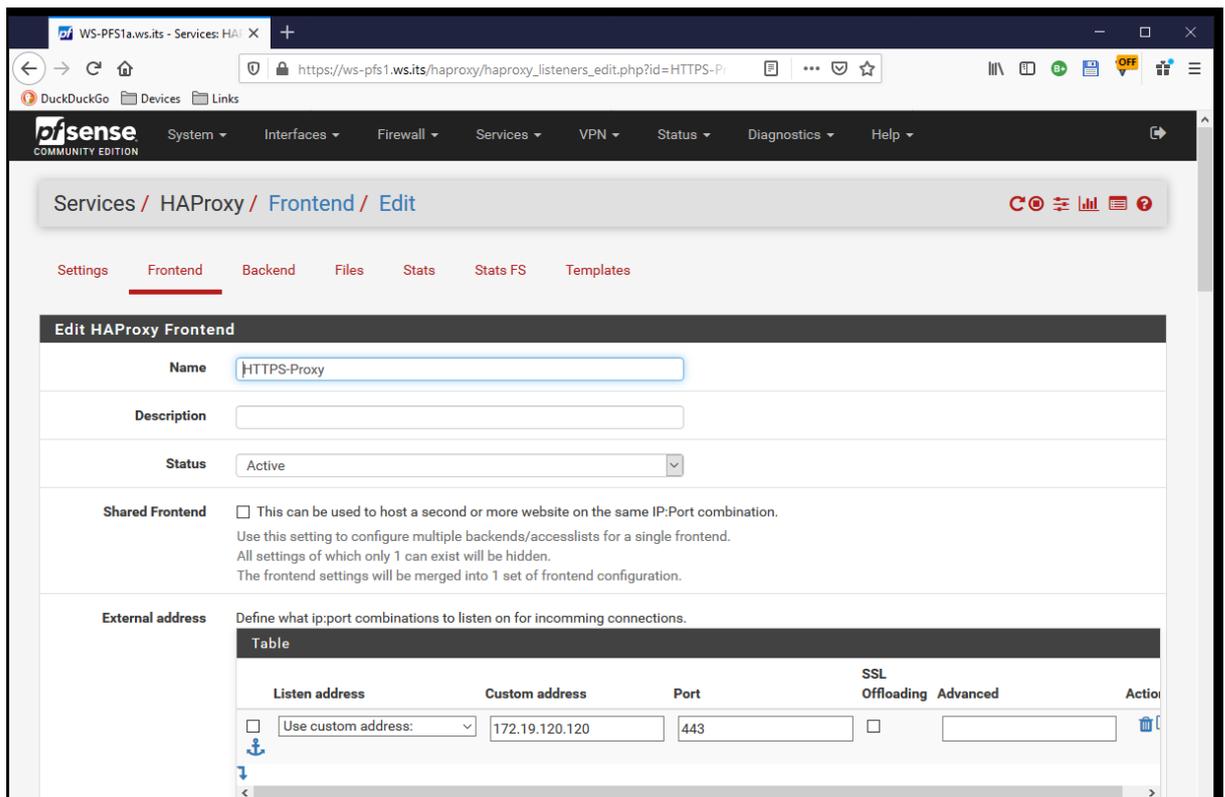
Die Mailserver werden von den Clients über https angesprochen. Daher wähle ich eine passende Validierung für die Verfügbarkeit aus. So kann mein HAProxy erkennen, wenn ein Exchange Server offline geht und die Clients auf den anderen Server umleiten:



Das Backend ist fertig, wird aber von keinem Frontend verwendet:



Das Frontend existiert ja schon. In meinem Fall reagiert der HAProxy auf eingehende Verbindungen auf der IPv4-Adresse 172.19.120.120 und dem Port 443:



Aber nun muss er noch eine Differenzierung zur Backend-Weiterleitung erhalten. Dazu nutze ich den SNI (Server Name Indikation) – also den FQDN, den ein Client anspricht. Meine Smartphones und Outlooks verwenden den Namen email.ws-its.de. Erkennt der HAProxy diesen SNI, dann soll er an das neue Backend weiterleiten. Gesteuert wird das Verhalten im Frontend in so genannten Access Control Lists. Hier füge ich eine neue hinzu:

NOTE: You must add a firewall rules permitting access to the listen ports above.
 If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define **Virtual IP** addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections
 Sets the maximum amount of connections this frontend will accept, may be left empty.

Type
 This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

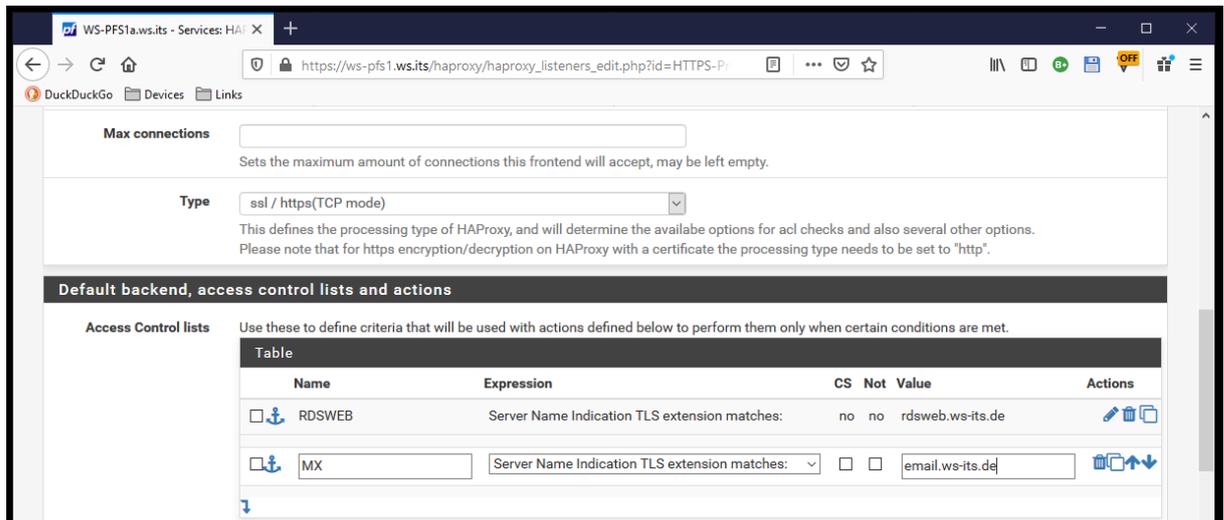
Table						
	Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/>	RDSWEB	Server Name Indication TLS extension matches:	no	no	rdsweb.ws-its.de	 
<input type="checkbox"/>						

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld will not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched

Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

Die neue ACL bekommt einen passenden Namen bzw. ein Kürzel und natürlich die Regel für die Bedingung:

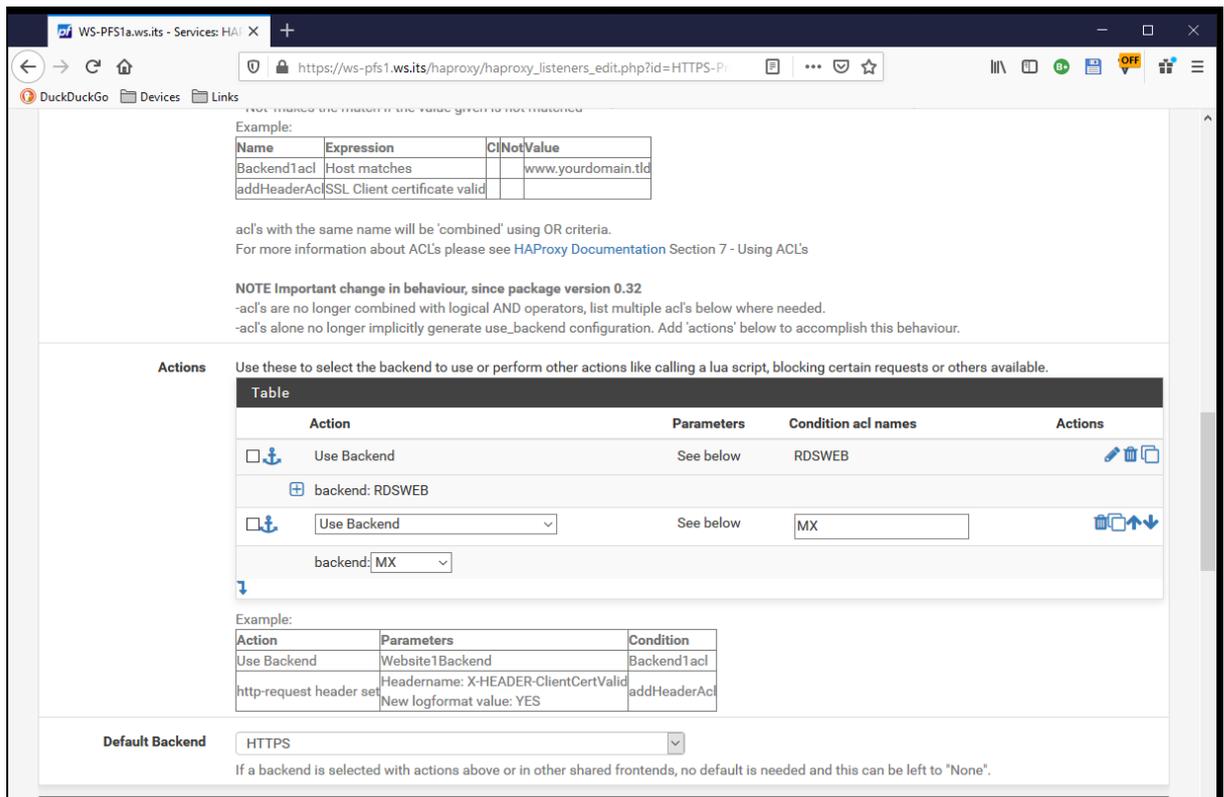


The screenshot shows the HAProxy configuration interface with the following details:

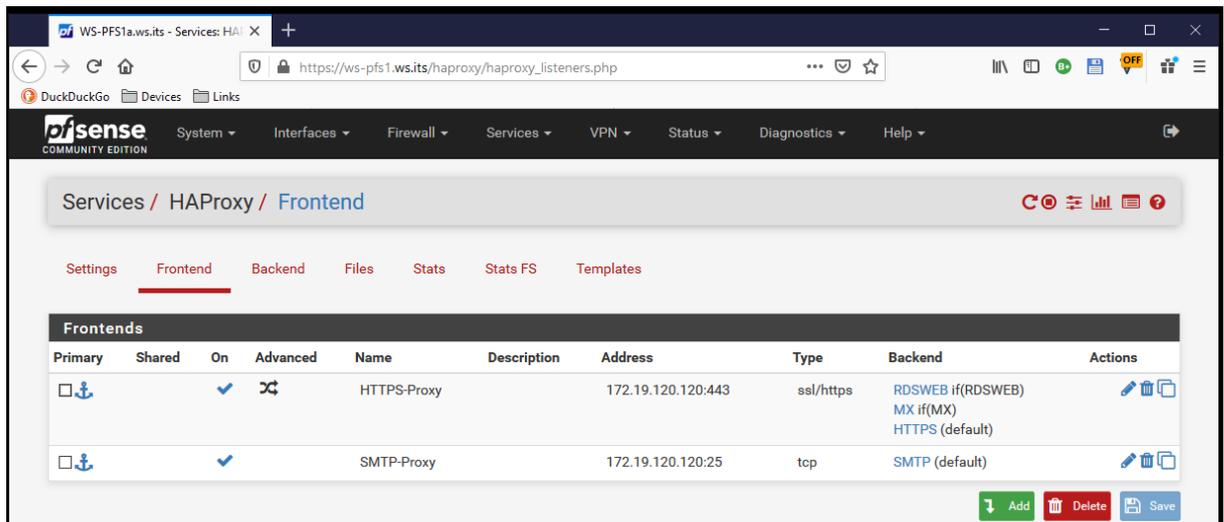
- Max connections:**
- Type:**
- Access Control lists table:**

	Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/>	RDSWEB	Server Name Indication TLS extension matches:	no	no	rdsweb.ws-its.de	 
<input type="checkbox"/>	MX	Server Name Indication TLS extension matches:	<input type="checkbox"/>	<input type="checkbox"/>	email.ws-its.de	  

Die ACL ist aber nur ein Bestandteil. Zusätzlich muss weiter unten im Frontend noch die action für eine positive Bedingungsprüfung definiert werden. In meinem Fall soll das Backend „MX“ angesprochen werden:



Ein Apply später ist diese Regel aktiv:



Auf dem Dashboard meiner PfSense sieht man den neuen Eintrag. Bisher ging der Traffic durch das https_ipvany-Frontend an die beiden WAP-Server WS-RA1 und WS-RA2. Ab jetzt wird vorher direkt auf die Exchange Server umgeleitet:

The screenshot shows the pfSense Status Dashboard. The 'System Information' section displays the name 'WS-PFS1a.ws.its', user 'admin@192.168.110.101', version '2.4.4-RELEASE-p3', and uptime of 21 days. The 'Traffic Graphs' section shows two graphs: 'DMZ_120_EXTER' for WAN traffic and 'LAN_100_SERVER' for LAN traffic. The 'HAProxy' section lists several backends and servers:

Backend(s)/Server(s)	Sessions (cur/max)	Status
RDSWEB_ipvANY	0 / 200	✓
WS-RDS1	0	✓
MX_ipvANY	0 / 200	✓
WS-MX1	0	✓
WS-MX2	0	✓
HTTPS_ipvANY	0 / 200	✓
WS-RA1	0	✓
WS-RA2	0	✓
SMTP_ipv4	0 / 200	✓
WS-MX1	0	✓
WS-MX2	0	✓

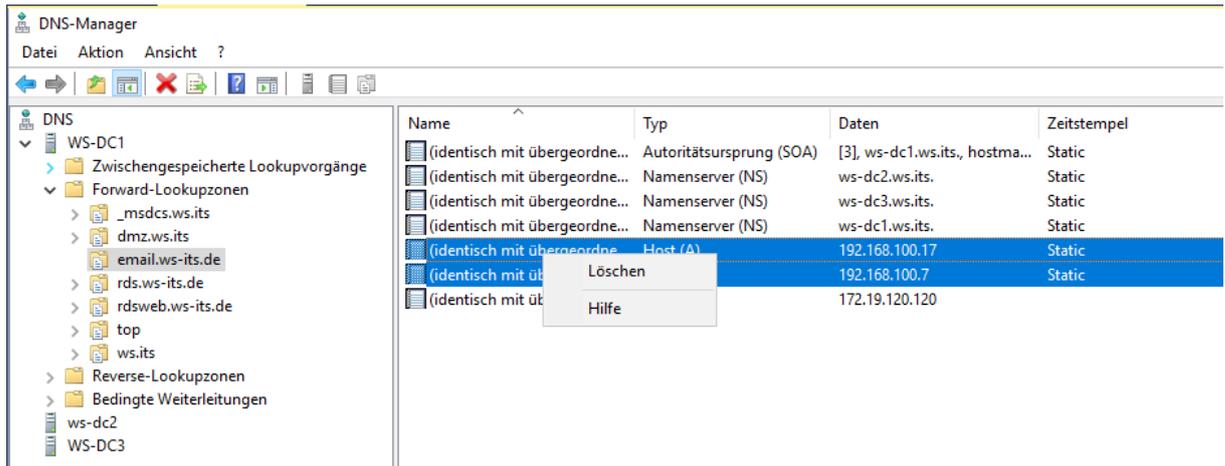
Damit funktioniert der externe Aufruf ohne weitere Konfiguration. Intern haben meine Clients aber die Exchange Server über den Namespace email.ws-its.de angesprochen. Im internen DNS hatte ich dazu eine Zone erstellt und direkt auf beide WAP-Server verwiesen. Jetzt kommen die Clients direkt zum HAProxy. Also erstelle ich einen neuen Record. Wichtig dabei: ich gebe keinen Namen an. Damit ist der Record direkt für die Zone gültig – also für email.ws-its.de:

The screenshot shows the Windows DNS Manager interface. A 'Neuer Host' dialog box is open, showing the configuration for a new host record:

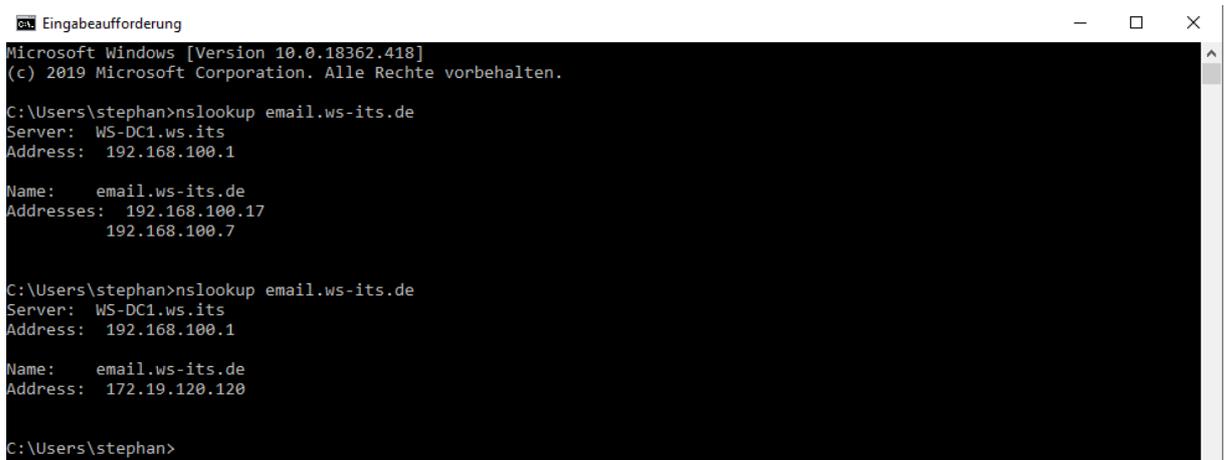
- Name (bei Nichtangabe wird übergeordneter Domänenname verwendet):
- Vollqualifizierter Domänenname: email.ws-its.de.
- IP-Adresse: 172.19.120.120
- Verknüpften PTR-Eintrag erstellen
- Authentifizierte Benutzer können DNS-Einträge mit demselben Besitzernamen aktualisieren
- Gültigkeitsdauer (TTL): 0 :0 :2 :0 (TTTT:HH.MM.SS)

Buttons at the bottom: 'Host hinzufügen' and 'Abbrechen'.

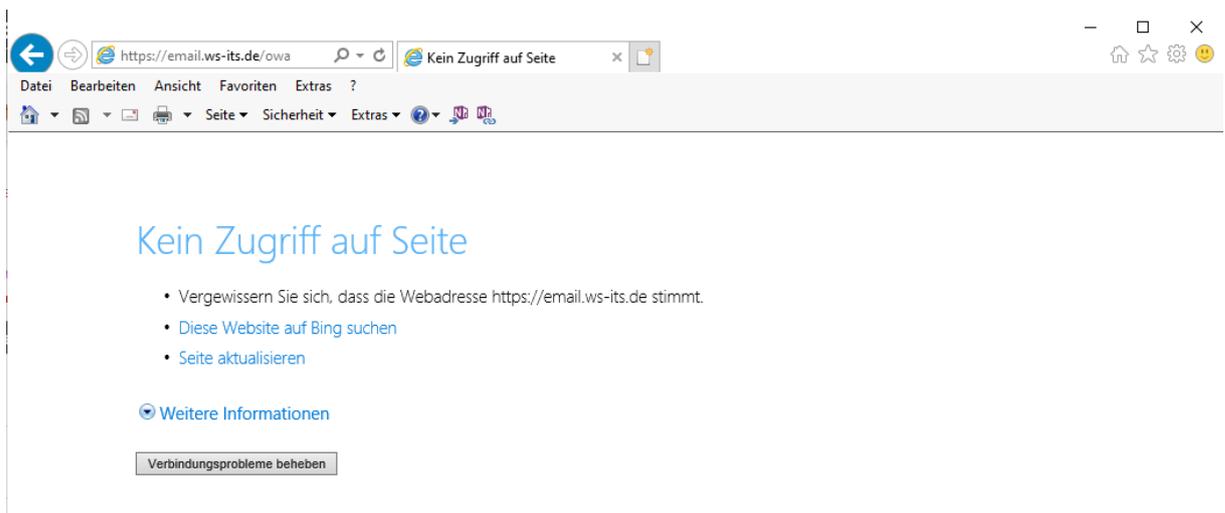
Danach kann ich die beiden alten Records zu den WAP-Servern löschen:



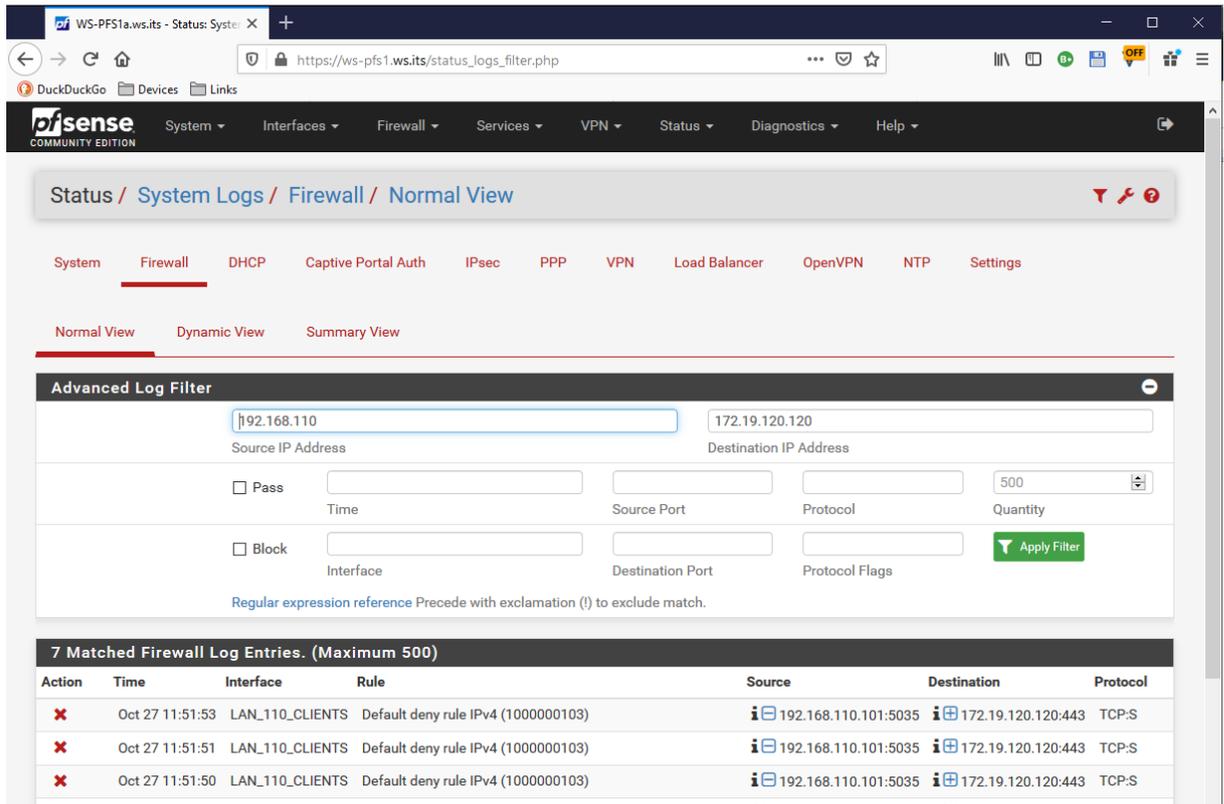
Die Clients lernen bei mir recht schnell diese Änderung, da ich alle DNS-Record mit 2 Minuten TimeToLive erstellt habe:



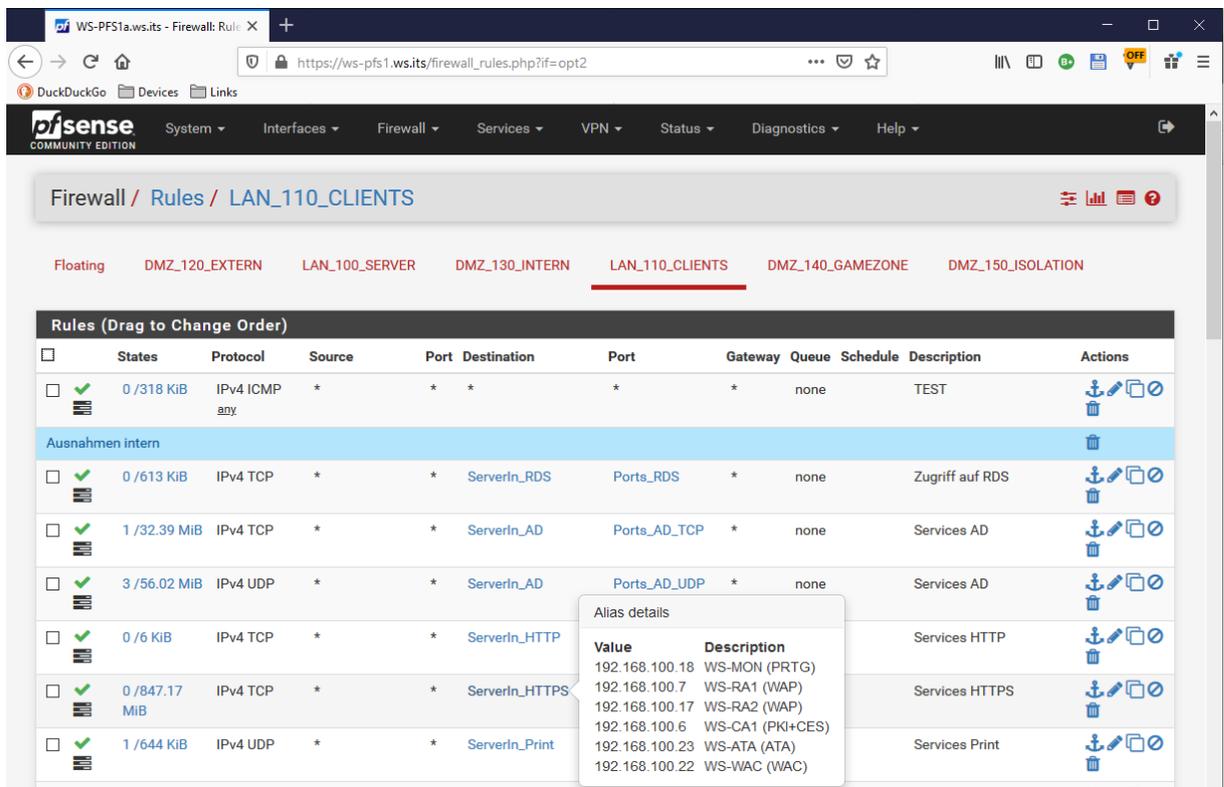
Also wird es Zeit für einen Test. Ich öffne einen Browser auf einem internen Client und navigiere zum OWA-Portal des Exchange Servers. Aber das scheint noch nicht durchzugehen:



Die Ursache des Problems ist schnell gefunden: Meine Clients haben nicht das Recht, den HAProxy von intern anzusprechen. Das verhindert die Firewall der PFSense. Bisher war das ja auch nicht erforderlich. Im Firewall-Log sieht man sehr schön die Blocks:



Meine Regeln habe ich durch Alias-Definitionen etwas strukturiert. So kann ich sehr bequem die Erweiterung vornehmen. Meine Clients dürfen HTTPS nur zu folgenden internen Servern verwenden. Natürlich stehen hier die beiden alten WAP-Server drin:



Ein Klick auf den Hyperlink des Alias bringt mich zur Konfiguration. Ich nehme die IPv4 des HAProxy mit auf:

Firewall / Aliases / Edit

Properties

Name ServerIn_HTTPS
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description Services mit HTTPS
A description may be entered here for administrative reference (not parsed).

Type Host(s)

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	Service	Action
192.168.100.18	WS-MON (PRTG)	Delete
192.168.100.7	WS-RA1 (WAP)	Delete
192.168.100.17	WS-RA2 (WAP)	Delete
192.168.100.6	WS-CA1 (PKI+CES)	Delete
192.168.100.23	WS-ATA (ATA)	Delete
192.168.100.22	WS-WAC (WAC)	Delete
172.19.120.120	HAProxy	Delete

Save Add Host

Die beiden WAP-Server belasse ich noch, da es noch weitere Anwendungen gibt, die ich vorab umstellen muss. Die Firewall-Ausnahme greift sofort. Mein Browser kann eine Verbindung aufbauen. Aber die Fehlermeldung zeigt ein weiteres Problem:

https://email.ws-its.de/owa

Diese Website ist nicht sicher.

Dieses Problem deutet eventuell auf den Versuch hin, Sie zu täuschen bzw. Daten abzufangen, die Sie an den Server gesendet haben. Die Website sollte sofort geschlossen werden.

[Diese Registerkarte schließen](#)

[Weitere Informationen](#)

Der Hostname im Sicherheitszertifikat der Website unterscheidet sich von der Website, die Sie besuchen möchten.

Fehlercode: DLG_FLAGS_SEC_CERT_CN_INVALID

Bisher war mein öffentliches Zertifikat für email.ws-its.de auf den WAP-Servern installiert. Die Mailserver hatten nur ein internes Zertifikat. Dessen Name passt natürlich nicht mehr. Also editiere ich noch die Zertifikatverwendung auf beiden Mailservern. Das öffentliche Zertifikat hatte ich bereits für SMTP-TLS installiert. Ich muss also nur noch die IIS-Bindung nachtragen:

Exchange Admin Center

Server auswählen: WS-MX1.ws.its

NAME	STATUS	GÜLTIG BIS	
MX-2018-01-07-intern	Gültig	07.01.2020	
CN=WS-ITS-Zertifizierungsstelle-CA1, DC=ws, DC=...	Gültig	05.04.2020	
Microsoft Exchange Server ACS Certificate	Gültig	14.09.2021	
MX-2019-10-20-extern	Gültig	18.01.2022	MX-2019-10-20-extern
Microsoft Exchange	Gültig	02.04.2022	Von einer Zertifizierungsstelle signiertes Zertifikat Aussteller: CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
WMSVC-SHA2	Gültig	29.03.2027	Status Gültig Gültig bis: 18.01.2022 Erneuern

Diensten zugewiesen
SMTP

Das geht sehr einfach:

Exchange Admin Center

Exchange-Zertifikat - Mozilla Firefox

MX-2019-10-20-extern

Allgemein

Dienste

- SMTP
- Microsoft Exchange Unified Messaging
- Unified Messaging-Anrufrouter
- IMAP
- POP
- IIS

Alternativ kann das auch mit der PowerShell erledigt werden. Den zweiten Server stelle ich mit diesen 2 Zeilen um:

```

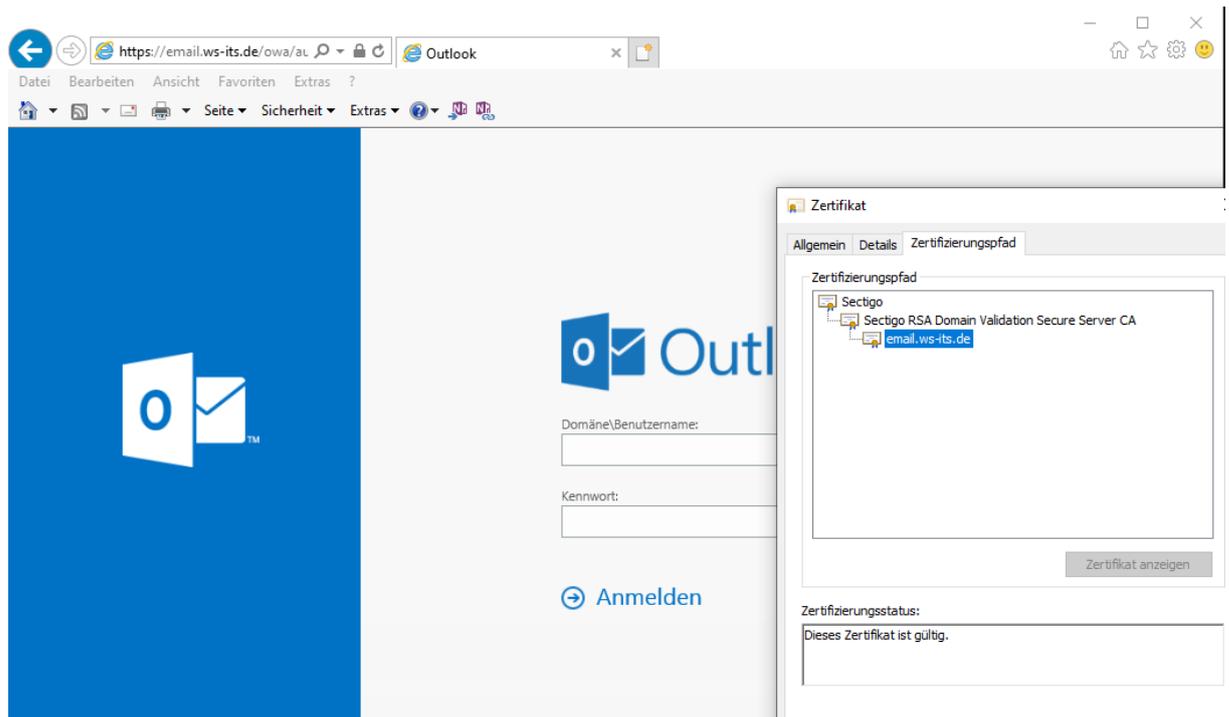
Computer: WS-MX2.ws.its
[PS] C:\>Get-ChildItem -Path Cert:\LocalMachine\my

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\my

Thumbprint                                     Subject
-----
F862AF15D5E97017B71FF895EDC832F88137E33E    CN=WS-MX2
DF056FFE19F31F22A7AC56AB6A8A54E720C93A7F    CN=Microsoft Exchange ACS Certificate
76EC10561160E217E8C93E2B7151221D315B3F61    CN=email.ws.its, OU=IT-Services, O=WS IT-Solutions, L=Ergoldsbach, S=Bayer...
70CA8162910B7E261245ABA4A818A869AC897DFE    CN=WMSvc-SHA2-WS-MX2
69521BE172C1083C6F68F5607EC2DB3E12D70847    CN=email.ws-its.de, OU=Domain Control Validated
458498173DCF5F4EAB94FDED5BE4A4D8C6825D7B    CN=WS-MX2, OU=MX, OU=Server, OU=WS, DC=ws, DC=its

[PS] C:\>Enable-ExchangeCertificate -Thumbprint 69521BE172C1083C6F68F5607EC2DB3E12D70847 -Services IIS
[PS] C:\>
    
```

Ein weiterer OWA-Test wird nun zu einem der Mailserver durchgereicht. Der Client möchte mit <https://email.ws-its.de> sprechen. Und beide Server präsentieren dafür das richtige Zertifikat:

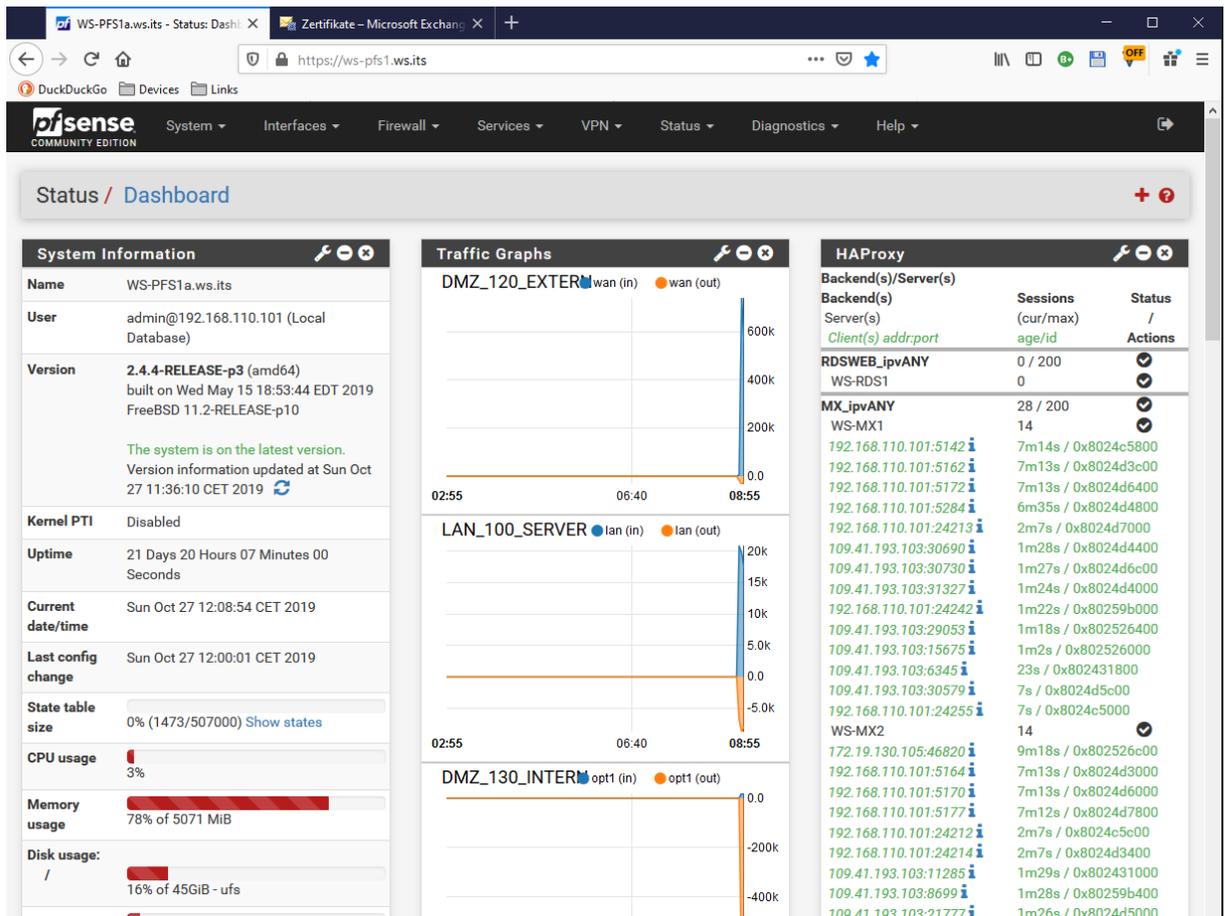


Natürlich geht es einem internen Outlook gleich. In der Verbindungsanzeige von Outlook kann man schön die Servernamen erkennen. Und natürlich die erfolgreiche Verbindung über den HAProxy zum Mailserver:

The screenshot shows the 'Outlook-Verbindungsstatus' window with the 'Allgemein' tab selected. It displays a table of connection activities:

VID	SMTP-Adres...	Anzeigena...	Proxyserver	Servername	Status	Protokoll	Authn	Versc...	RPC-Port	Typ	Anfr/Fehler	Reaktio...	Bearb (0)	Sitzungstyp	Sd ^
22	Stephan.W...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	3/0	31	7	Hintergrund	Etl
31	Stephan.W...	Onlinearch...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	88/0	17	4	Hintergrund	Etl
34	Stephan.W...	Stephan.W...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	84/0	20	6	Cache	Etl
36	stephan@j...	Onlinearch...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	63/0	16	2	Hintergrund	Etl
40	stephan@j...	stephan@j...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	46/0	13	3	Cache	Etl
42	stephan@w...	stephan@...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	40/0	20	3	Cache	Etl
45	Stephan.W...	Stephan.W...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	99/0	27	7	Hintergrund	Etl
48	stephan@j...	stephan@j...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	64/0	13	2	Hintergrund	Etl
52	stephan@w...	stephan@j...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	29/0	18	2	Hintergrund	Etl
56	stephan@j...	Öffentliche...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	8/0	25	11	Cache	Etl
64	Stephan.W...	Öffentliche...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	24/0	19	5	Cache	Etl
67	stephan@w...	Öffentliche...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	8/0	25	12	Cache	Etl

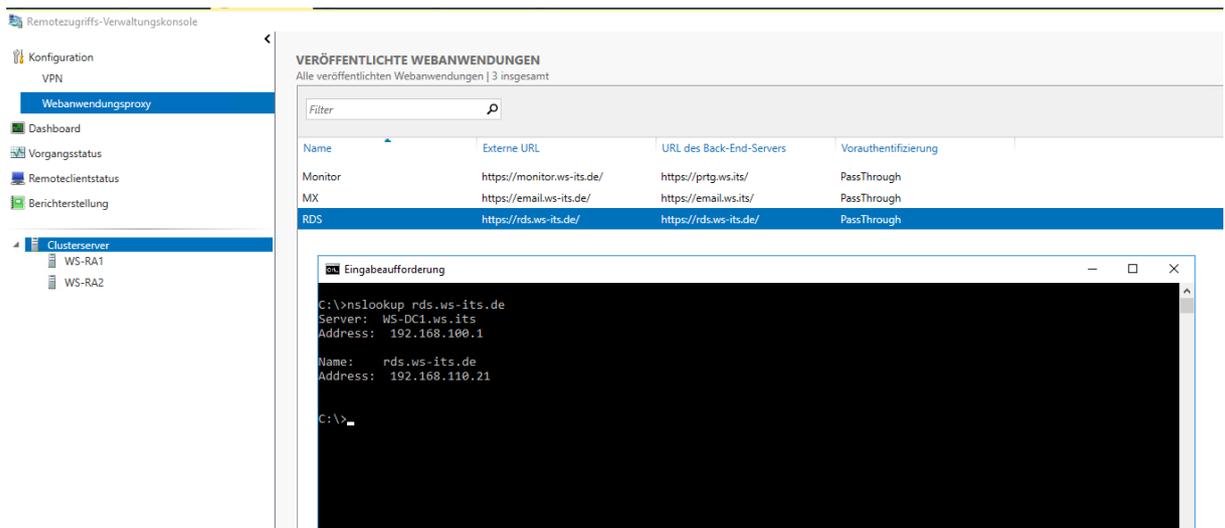
Doch mit welchem Server reden meine Clients aktuell? Der HAProxy zeigt die Verbindungen im Dashboard der PFSense an:



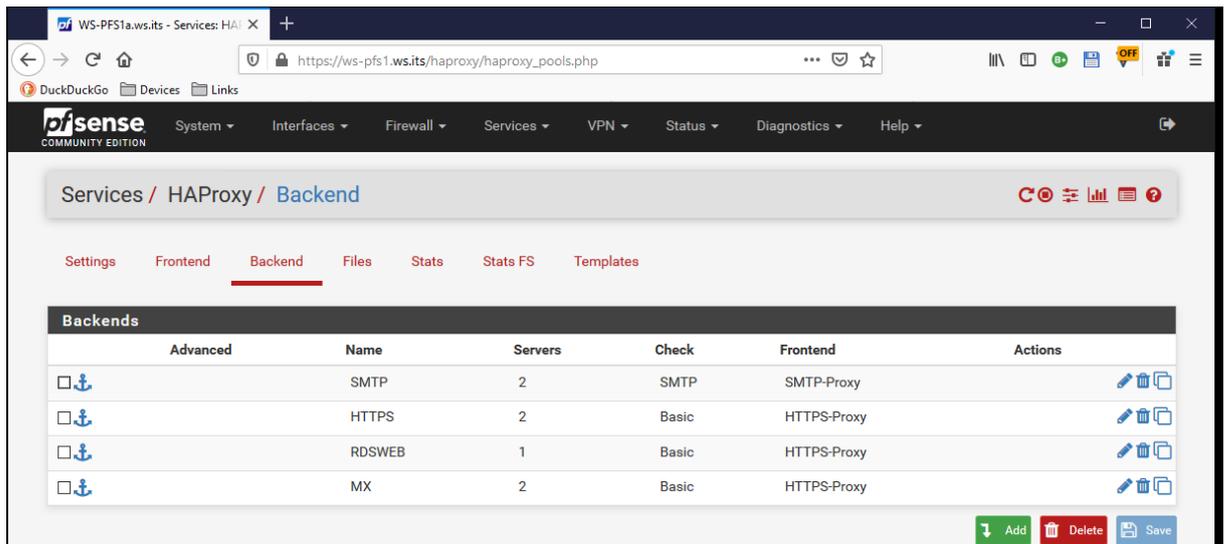
Damit benötige ich WAP nicht mehr für den Zugriff auf meine Exchange Server.

HAProxy für RDS

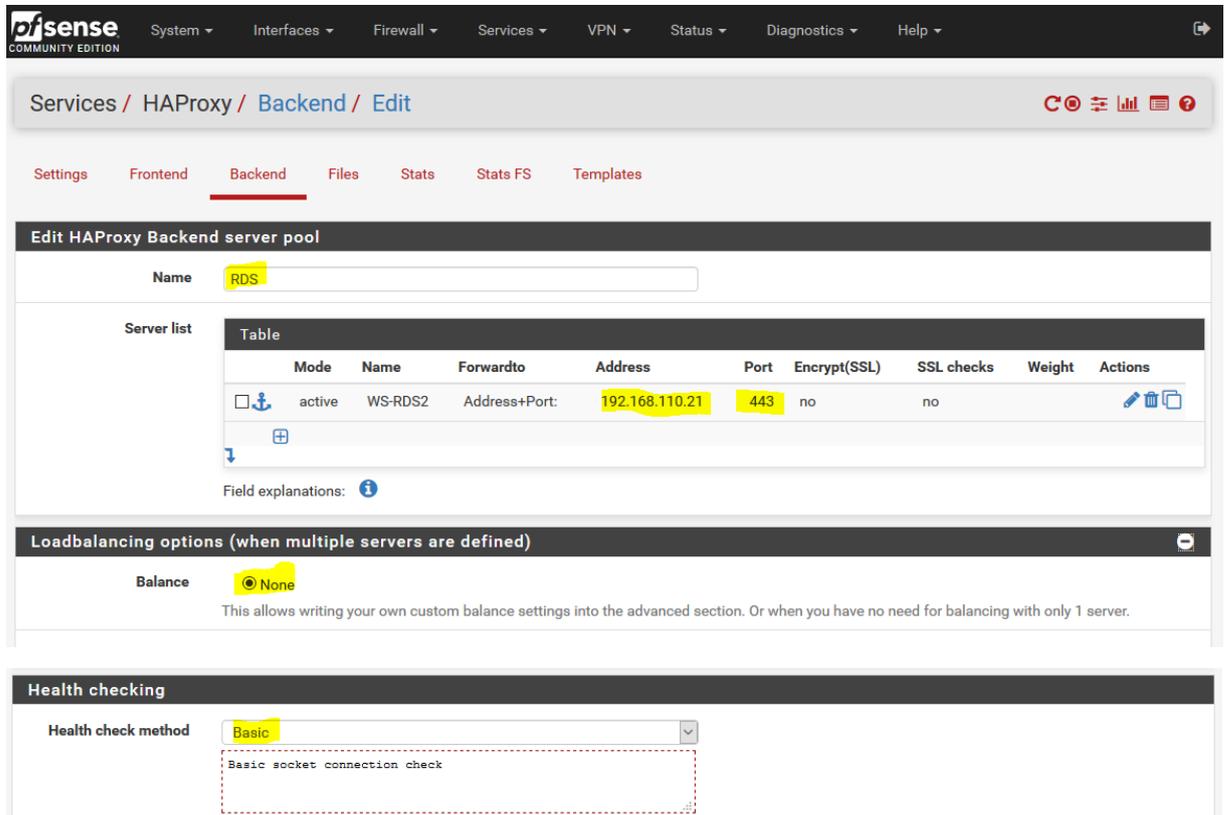
Die WAP-Server leiten externe Anfragen auf den SNI rds.ws-its.de auf meinen RD-Gateway weiter. Dieser verwendet mit dem gleichen DNS-Trick wie beim Exchange Server intern den gleichen Namen:

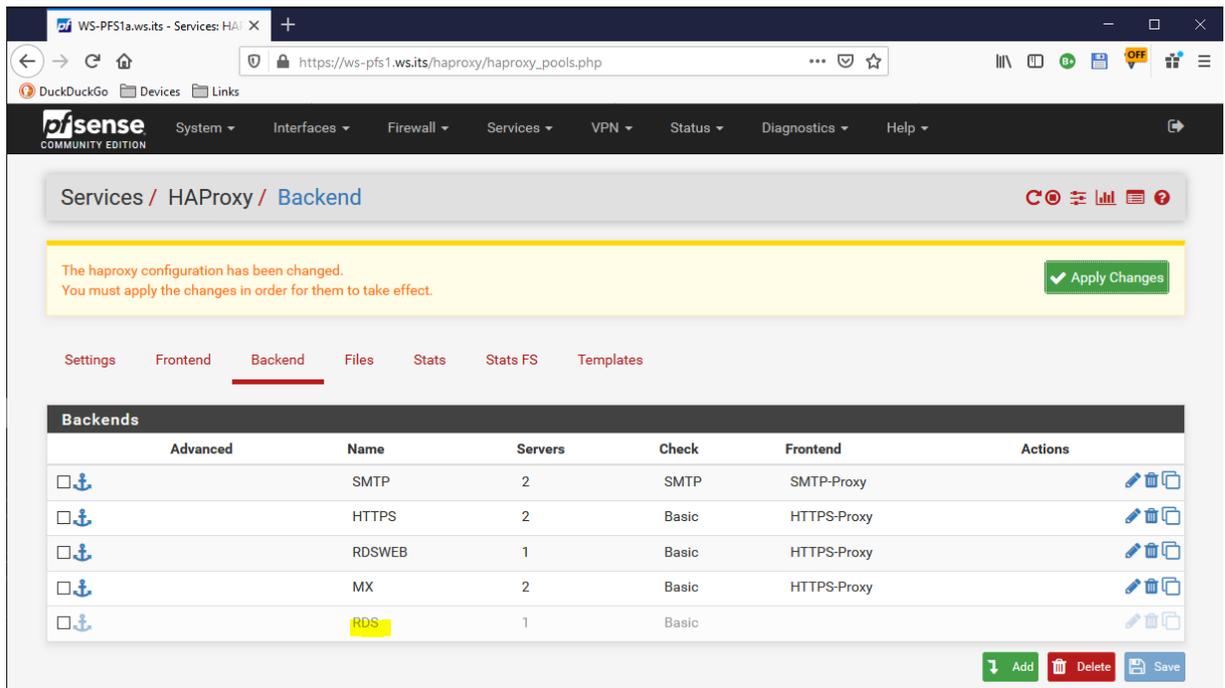


Damit ist die Rekonfiguration fast identisch zu der vom Exchange Service. Im HAProxy erstelle ich zuerst ein passendes Backend, dass auf meinen RD-Gateway verweist. Dieses ist nicht zu verwechseln mit dem Backend rdsweb. Dieses leitet zu einem anderen RDS-Server mit dem HTML5-Client um:



Das neue Backend hat nur ein einziges Ziel. RDS ist damit nicht hochverfügbar:

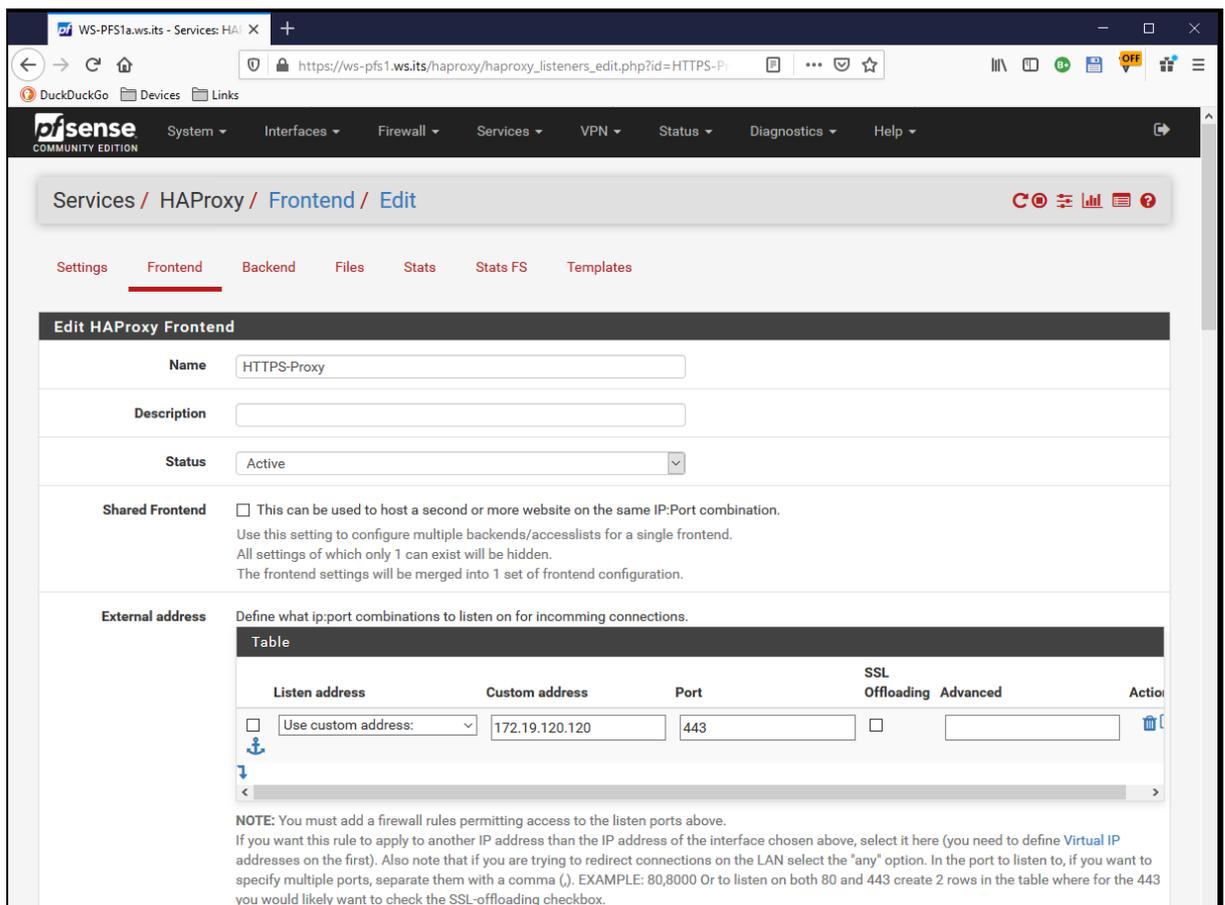




The screenshot shows the pfSense HAProxy configuration interface. A notification at the top states: "The haproxy configuration has been changed. You must apply the changes in order for them to take effect." Below this, the "Backends" section is active, displaying a table of configured backends.

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	SMTP	2	SMTP	SMTP-Proxy	
<input type="checkbox"/>	HTTPS	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDSWEB	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	MX	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDS	1	Basic		

Im HTTPS-Frontend erstelle ich wieder eine ACL mit dem SNI-Filter für die neue Anwendung:



The screenshot shows the pfSense HAProxy Frontend configuration page for "HTTPS-Proxy". The "External address" section is expanded, showing a table for listening addresses.

External address Define what ip:port combinations to listen on for incoming connections.

Listen address	Custom address	Port	SSL Offloading	Advanced	Action
<input type="checkbox"/> Use custom address: <input type="text"/>	172.19.120.120	443	<input type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define Virtual IP addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/> RDSWEB	Server Name Indication TLS extension matches:	no	no	rdsweb.ws-its.de	
<input type="checkbox"/> MX	Server Name Indication TLS extension matches:	no	no	email.ws-its.de	
<input type="checkbox"/> RDS	Server Name Indication TLS extension matches:	<input type="checkbox"/>	<input type="checkbox"/>	rds.ws-its.de	

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld will not be the same as WWW.domain.TLD
- 'Not' makes the match if the value given is not matched
Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld

Die neue ACL leitet dann auf das neue Backend:

Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.
For more information about ACL's please see [HAProxy Documentation Section 7 - Using ACL's](#)

NOTE Important change in behaviour, since package version 0.32
-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
-acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
<input type="checkbox"/> Use Backend	See below	RDSWEB	
<input type="checkbox"/> backend: RDSWEB			
<input type="checkbox"/> Use Backend	See below	MX	
<input type="checkbox"/> backend: MX			
<input type="checkbox"/> Use Backend	See below	RDS	
<input type="checkbox"/> backend: RDS			

Ein Apply später ist die Anwendung bereit:

WS-PFS1a.ws-its - Services: HAProxy

https://ws-pfs1a.ws-its/haproxy/haproxy_listeners.php

System Interfaces Firewall Services VPN Status Diagnostics Help

Services / HAProxy / Frontend

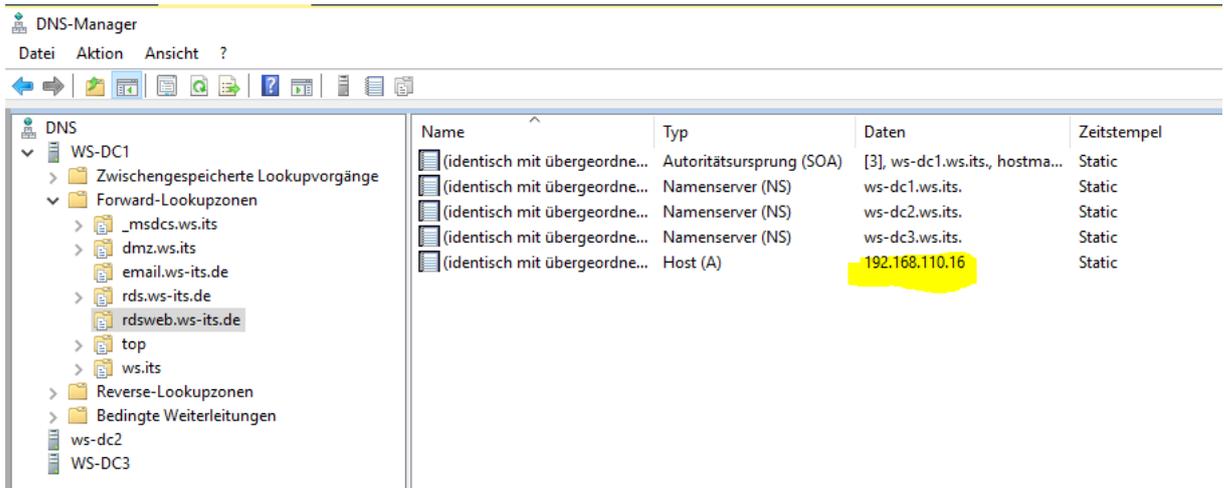
The haproxy configuration has been changed. You must apply the changes in order for them to take effect. Apply Changes

Settings Frontend Backend Files Stats Stats FS Templates

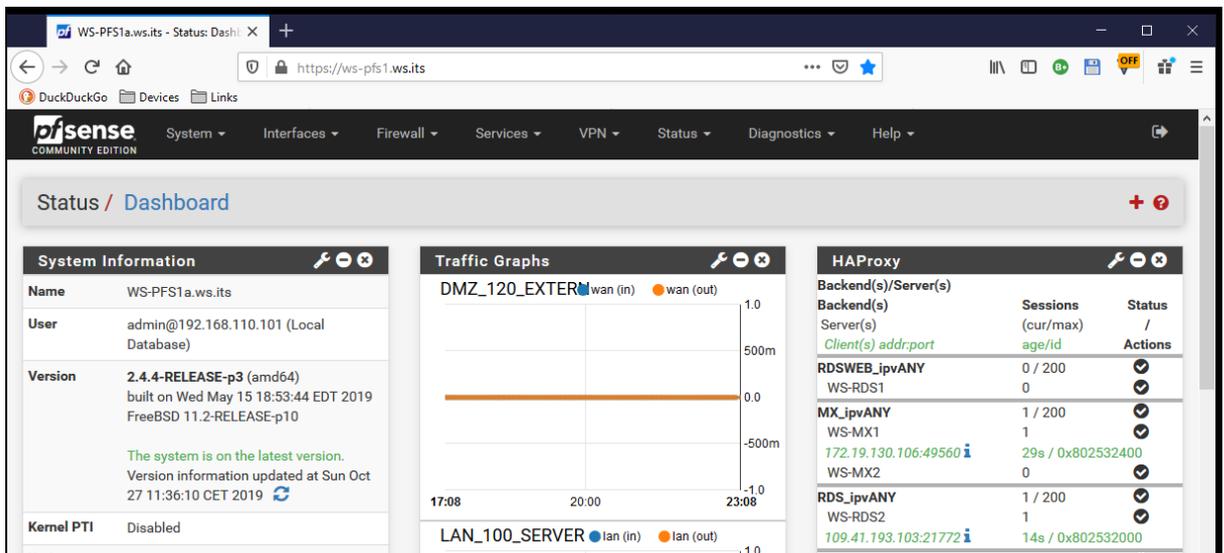
Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>		<input checked="" type="checkbox"/>		HTTPS-Proxy		172.19.120.120:443	ssl/https	RDSWEB if(RDSWEB) MX if(MX) RDS if(RDS) HTTPS (default)	
<input type="checkbox"/>		<input checked="" type="checkbox"/>		SMTP-Proxy		172.19.120.120:25	tcp	SMTP (default)	

Add Delete Save

Intern dürfen meine Clients weiter direkt mit dem RDS-Broker sprechen und so den HAProxy umgehen. Keep it simple, oder?

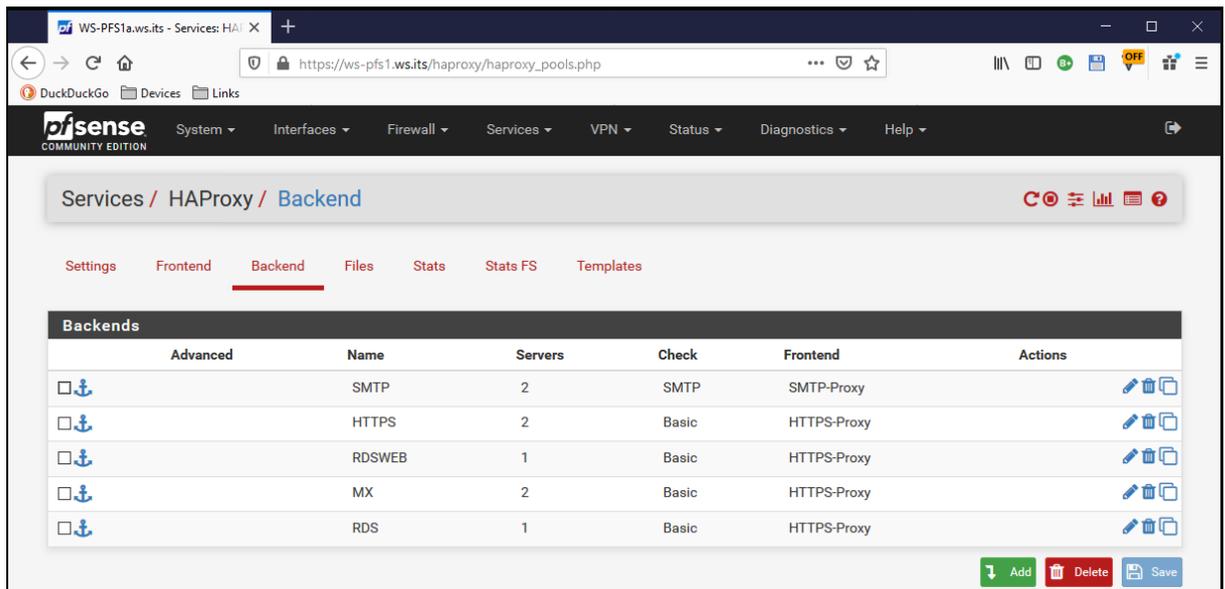


Die neue App zeigt sich wie gewohnt im Dashboard der PfSense. Und ein Einwahlversuch von außen wird erfolgreich auf meinen RDS-Server geleitet:

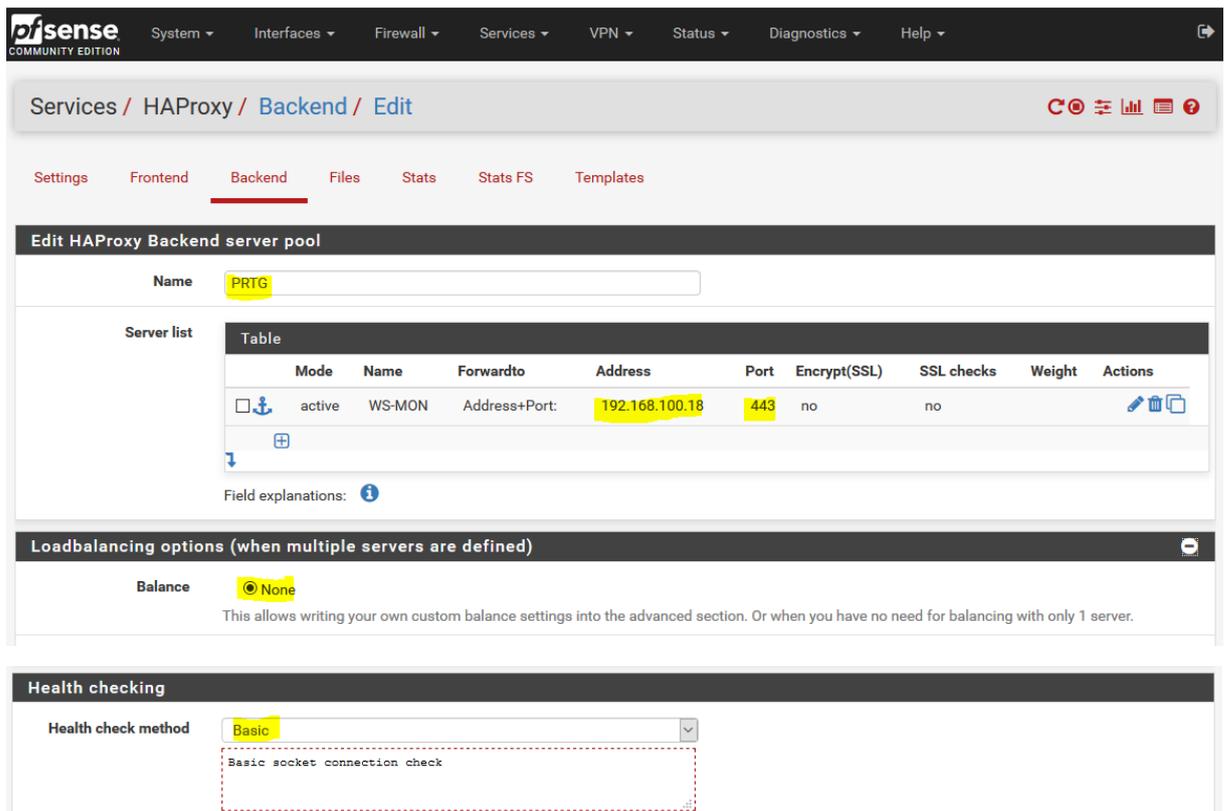


HAProxy für PRTG

Meine letzte Anwendung im Web Application Proxy ist mein PRTG-Monitor. Mit diesem Zugriffspunkt erhalte ich Push-Benachrichtigungen auf mein Smartphone, wenn es Probleme in meiner Infrastruktur gibt. Die Vorgehensweise ist gleich mit der meines RDS-Servers. Ich erstelle wieder ein Backend im HAProxy. Ein Klick auf add und es geht los:



Das Ziel ist mein WS-MON, auf dem die PRTG-Installation läuft. Ich benötige kein Load Balancing und als Prüfmechanismus genügt der Standardtest:



Ein Apply später ist das Backend einsatzbereit:

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	SMTP	2	SMTP	SMTP-Proxy	
<input type="checkbox"/>	HTTPS	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDSWEB	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	MX	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDS	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	PRTG	1	Basic		

Und ein letztes mal editiere ich mein HAProxy-Frontend und erstelle die ACL und die Weiterleitung:

Listen address	Custom address	Port	SSL Offloading	Advanced	Action
<input type="checkbox"/> Use custom address:	172.19.120.120	443	<input type="checkbox"/>		

NOTE: You must add a firewall rules permitting access to the listen ports above.
If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define **Virtual IP** addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (,). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/> RDSWEB	Server Name Indication TLS extension matches:	no	no	rdsweb.ws-its.de	
<input type="checkbox"/> MX	Server Name Indication TLS extension matches:	no	no	email.ws-its.de	
<input type="checkbox"/> RDS	Server Name Indication TLS extension matches:	no	no	rds.ws-its.de	
<input type="checkbox"/> <input type="text" value="PRTG"/>	Server Name Indication TLS extension matches: <input type="text" value=""/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="monitor.ws-its.de"/>	

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched
 Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.
 For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
<input type="checkbox"/> Use Backend	See below	RDSWEB	
<input type="checkbox"/> Use Backend	See below	MX	
<input type="checkbox"/> Use Backend	See below	RDS	
<input type="checkbox"/> <input type="text" value="Use Backend"/>	See below	<input type="text" value="PRTG"/>	

backend:RDSWEB
 backend:MX
 backend:RDS
 backend:

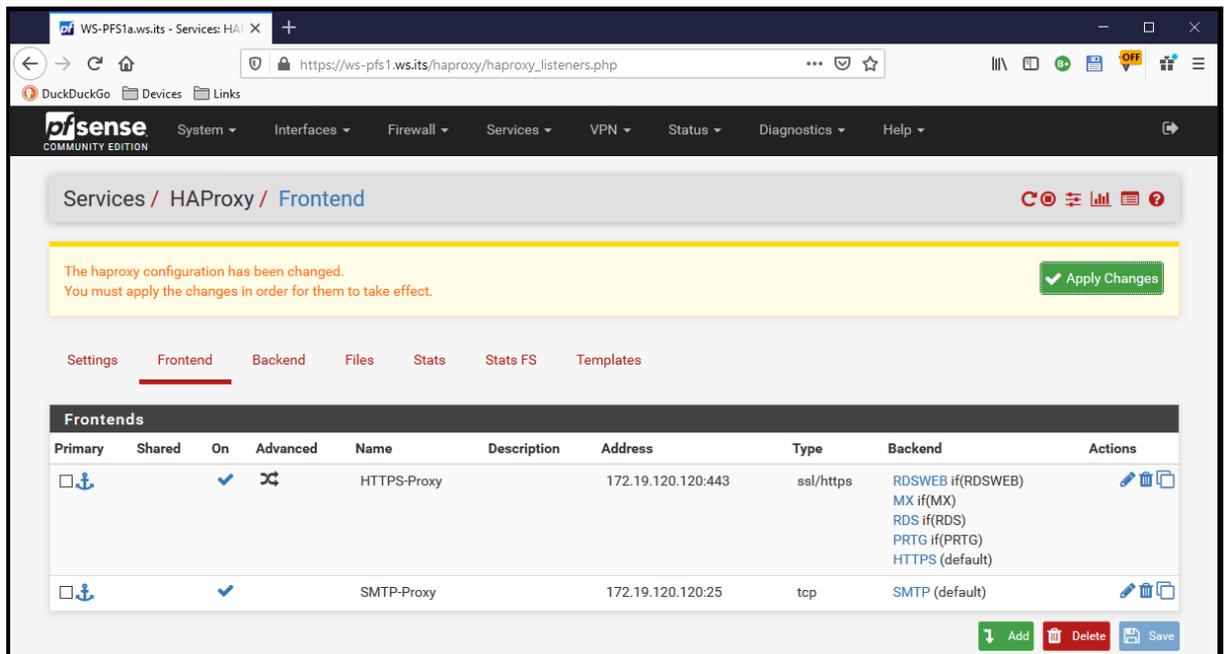
Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

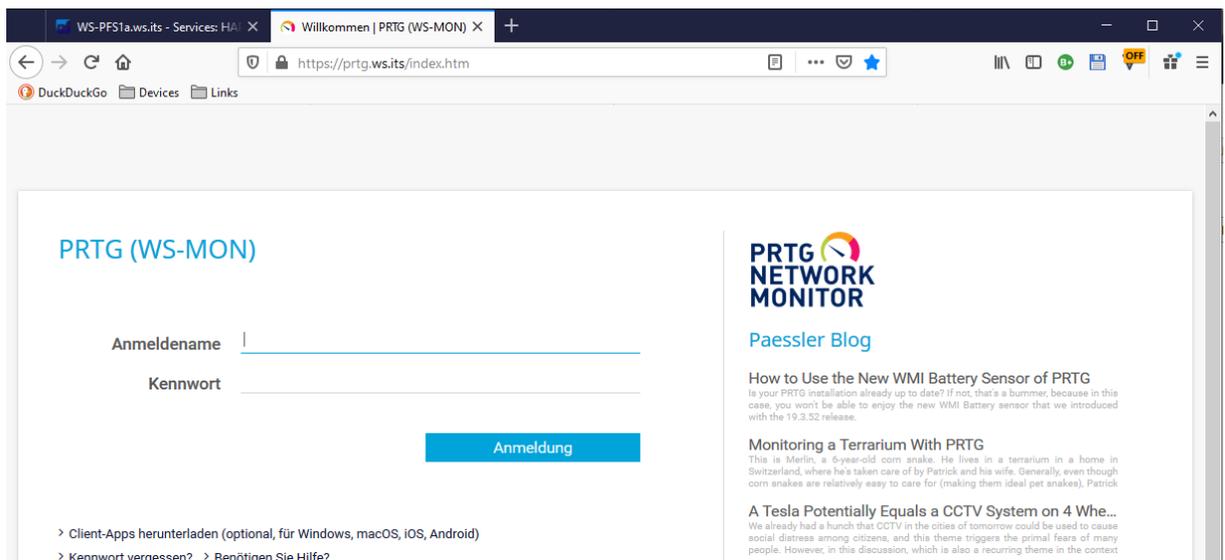
Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

Ein finales Apply später ist auch diese Anwendung umgestellt:



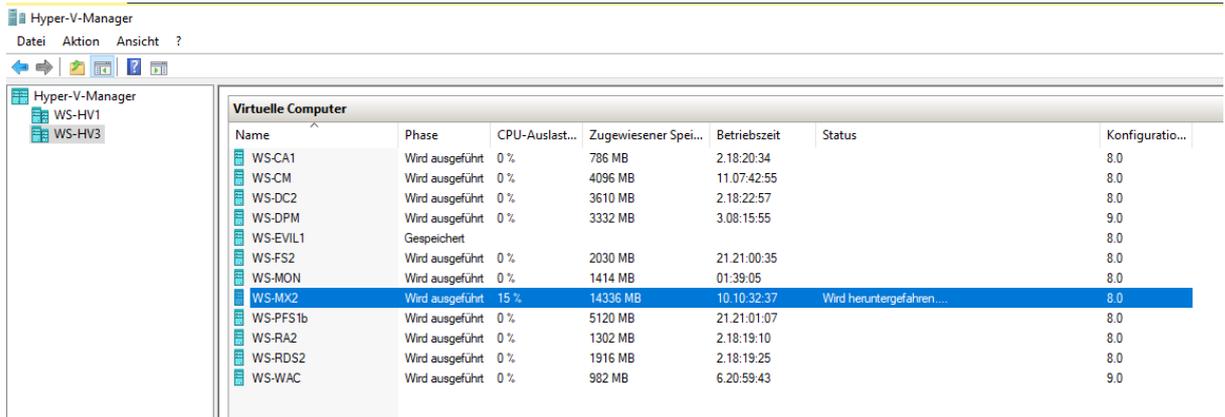
Intern spreche ich meine PRTG-Installation direkt an. Das funktioniert davon unabhängig. Meine App im Smartphone zeigt eine kurze Zertifikatbestätigung an und ist danach wieder verbunden:



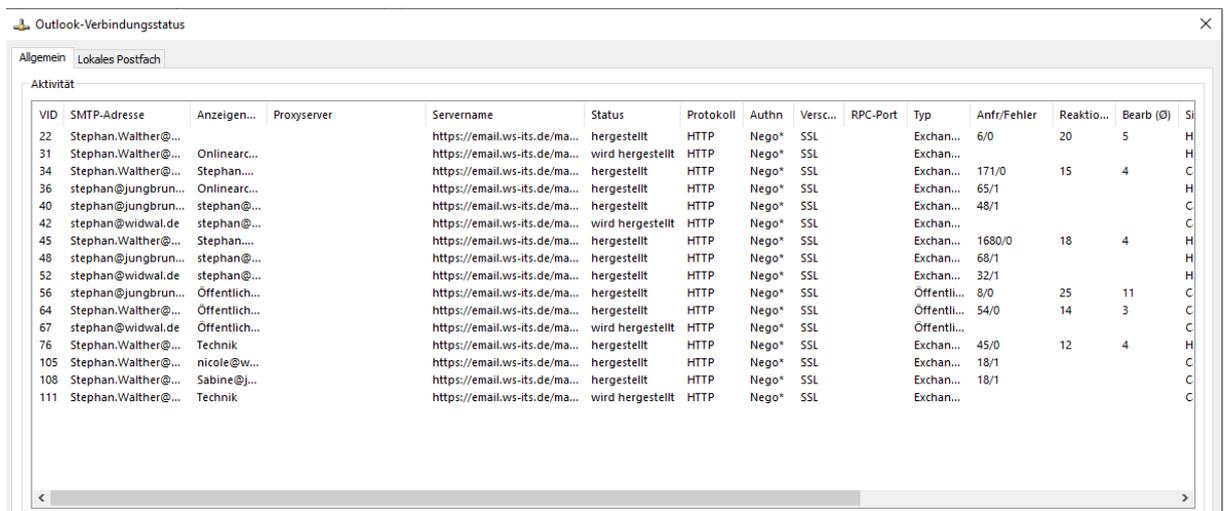
Testlauf HA

Bevor ich meinen Web Application Proxy abreiße möchte ich die neue Lösung gerne testen. Dafür werde ich nun verschiedene Server ausschalten und danach bzw. währenddessen von der zugehörigen Anwendung aus prüfen, ob der Schwenk funktioniert.

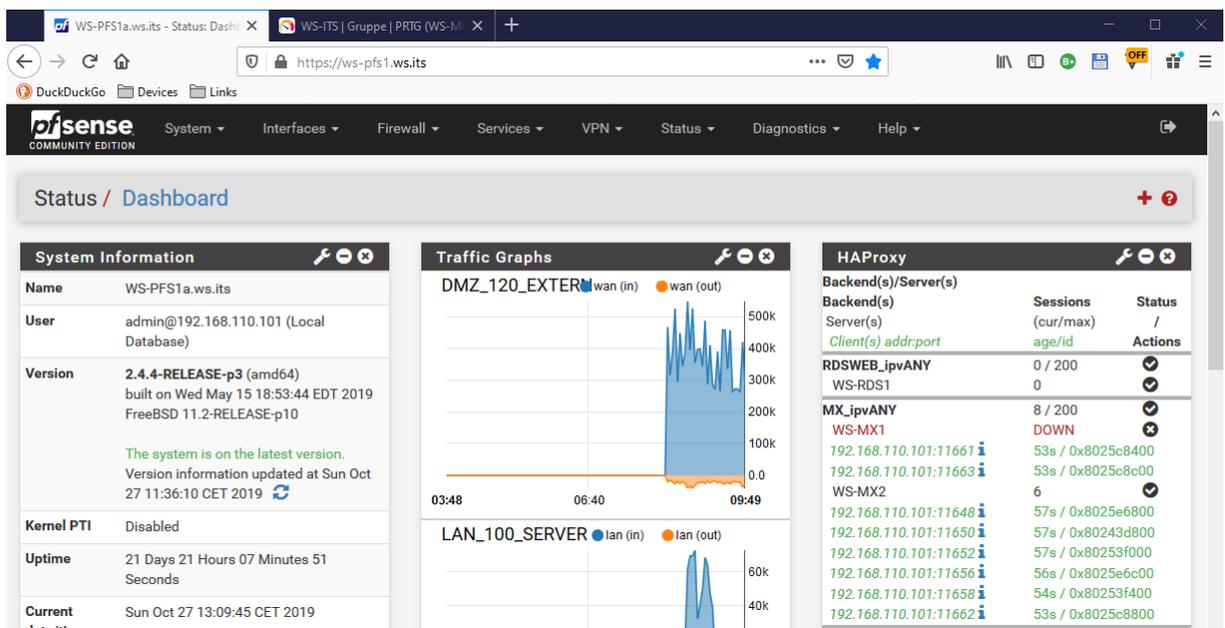
Zuerst fahre ich einen der Exchange Server herunter:



Dabei beobachte ich in meinem Outlook-Verbindungsstatus, wie einige Verbindungen schwenken:



Die gleiche Information erhalte ich auch in der PfSense. Das HAProxy-Modul hat erkannt, dass der Server nicht mehr einsatzbereit ist und die Verbindungen schwenken zum anderen Server:



Der Prozess dauert nur wenige Sekunden. In der Outlook-Verbindungsanzeige sind alle Verbindungen wieder hergestellt. Ohne die Anzeige hätte ich als Benutzer nichts bemerkt:

Outlook-Verbindungsstatus

Allgemein Lokales Postfach

Aktivität

VID	SMTP-Adresse	Anzeigen...	Proxyserver	Servername	Status	Protokoll	Authn	Versc...	RPC-Port	Typ	Anfr/Fehler	Reaktio...	Bearb (D)	Si
22	Stephan.Walther@...			https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	6/0	20	5	H
31	Stephan.Walther@...	Onlinearc...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	92/1			H
34	Stephan.Walther@...	Stephan...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	171/0	15	4	C
36	stephan@jungbrun...	Onlinearc...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	65/1			H
40	stephan@jungbrun...	stephan@...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	48/1			C
42	stephan@widwal.de	stephan@...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	52/1			C
45	Stephan.Walther@...	Stephan...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	1680/0	18	4	H
48	stephan@jungbrun...	stephan@...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	68/1			H
52	stephan@widwal.de	stephan@...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	41/2			H
56	stephan@jungbrun...	Öffentlich...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	8/0	25	11	C
64	Stephan.Walther@...	Öffentlich...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	58/1			C
67	stephan@widwal.de	Öffentlich...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Öffentli...	11/2			C
76	Stephan.Walther@...	Technik		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	45/0	12	4	H
105	Stephan.Walther@...	nicole@w...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	18/1			C
108	Stephan.Walther@...	Sabine@j...		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	18/1			C
111	Stephan.Walther@...	Technik		https://email.ws-its.de/ma...	hergestellt	HTTP	Nego*	SSL		Exchan...	124/1			C

Auch der Schwenk des HAProxy auf die zweite PfSense geschieht nahezu transparent. Das sieht gut aus.

Bereinigung WAP

Also kann ich jetzt die im WAP veröffentlichten Anwendungen entfernen:

Remotenzugriffs-Verwaltungskontrolle

Konfiguration

- VPN
- Webanwendungsproxy**
- Dashboard
- Vorgangstatus
- Remoteclientstatus
- Berichterstellung
- Clusterverserver
 - WS-RA1
 - WS-RA2

VERÖFFENTLICHTE WEBANWENDUNGEN
Alle veröffentlichten Webanwendungen | 3 insgesamt

Filter

Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung
Monitor	https://monitor.ws-its.de/	https://prtg.ws.its/	PassThrough
MX	https://email.ws-its.de/	https://email.ws.its/	PassThrough
RDS	https://rds.ws-its.de/	https://rds.ws-its.de/	PassThrough

Bearbeiten
Basierend auf dieser Anwendung veröffentlichen
Entfernen

Damit wird mein Web Application Proxy Cluster nicht länger verwendet.

Dieses Kapitel habe ich bereits im Oktober geschrieben. Es gehört aber thematisch in diesen Artikel. Ab jetzt geht es wieder im Dezember 2019 weiter...

Entfernung von ADFS und WAP

Vorbereitung

Beide WAP-Server bilden einen WAP-Cluster. Dieser ist aber seit einigen Tagen gestört:

Remotenzugriffs-Verwaltungskontrolle

Konfiguration

- VPN
- Webanwendungsproxy
- Dashboard**
- Vorgangstatus
- Remoteclientstatus
- Berichterstellung
- Clusterverserver
 - WS-RA1
 - WS-RA2

Remotenzugriffs-Dashboard

Serverstatus

Vorgangstatus

- Clusterverserver
 - WS-RA1.ws.its
 - WS-RA2.ws.its

Status von DirectAccess- und VPN-Clients

Aktive Clients (insgesamt): 0 Übertragene Daten (gesamt): 0 Bytes eingehend/0 Bytes ausgehend

Aktive DirectAccess-Clients (insgesamt): 0 Maximale Anzahl von Clientverbindungen: 0

Aktive VPN-Clients (insgesamt): 0

Kumulierte Verbindungen (insgesamt): 0

Seite "Remoteclientstatus"

In den Details der Administrationsoberfläche sieht man, dass die Services nicht laufen. Diese lassen sich auch nicht mehr starten. Das Eventlog des Servers ist voll mit Fehlermeldungen. Die Ursache ist mir aber nach dem Entschluss der Service-Entfernung egal:

Es sind im WAP-Cluster keine Webanwendungen mehr veröffentlicht. Die habe ich alle in meinen HA-Proxy der PfSense integriert. Sonst gäbe es an dieser Stelle noch ein paar offene Löschaktionen:

Hier sieht man rechts im Bild meinen Nachfolger des WAP-Clusters:

Backend(s)/Server(s)	Sessions (cur/max)	Status / Actions
RDSWEB_ipvANY	0 / 200	✓
WS-RDS1	0	✓
MX_ipvANY	19 / 200	✓
WS-MX1	10	✓
172.19.130.105:46566	25m39s / 0x8025da400	
172.19.130.105:46607	24m58s / 0x80242bc00	
192.168.110.101:1142	5m11s / 0x8025da000	
192.168.110.101:1243	5m11s / 0x80242f000	
192.168.110.101:1322	4m11s / 0x8025da800	
172.19.130.105:46698	3m53s / 0x802476000	
192.168.110.101:20033	3m23s / 0x802476c00	
192.168.110.101:1430	1m11s / 0x80253f000	
192.168.110.101:1498	20s / 0x802480800	
192.168.110.101:1510	11s / 0x80242f400	
WS-MX2	9	✓
172.19.130.105:46546	26m30s / 0x80242fc00	
172.19.130.105:46574	25m39s / 0x8025d9400	
192.168.110.101:1140	5m11s / 0x802477800	
192.168.110.101:1323	4m11s / 0x80253f800	
172.19.130.105:46690	3m54s / 0x80242f800	
192.168.110.101:1429	1m11s / 0x802480400	
192.168.110.101:1499	20s / 0x8025d9800	
192.168.110.101:1500	20s / 0x802477000	
192.168.110.101:1513	9s / 0x80243a000	
RDS_ipvANY	0 / 200	✓
WS-RDS2	0	✓
PRTG_ipvANY	0 / 200	✓
WS-MON	0	✓
HTTPS_ipvANY	0 / 200	✓
WS-RA1	0	✓
WS-RA2	0	✓
SMTP_ipv4	0 / 200	✓
WS-MX1	0	✓
WS-MX2	0	✓

Natürlich wurde ich von meinem Monitoring über den Ausfall des Services auf WS-RA1 informiert:

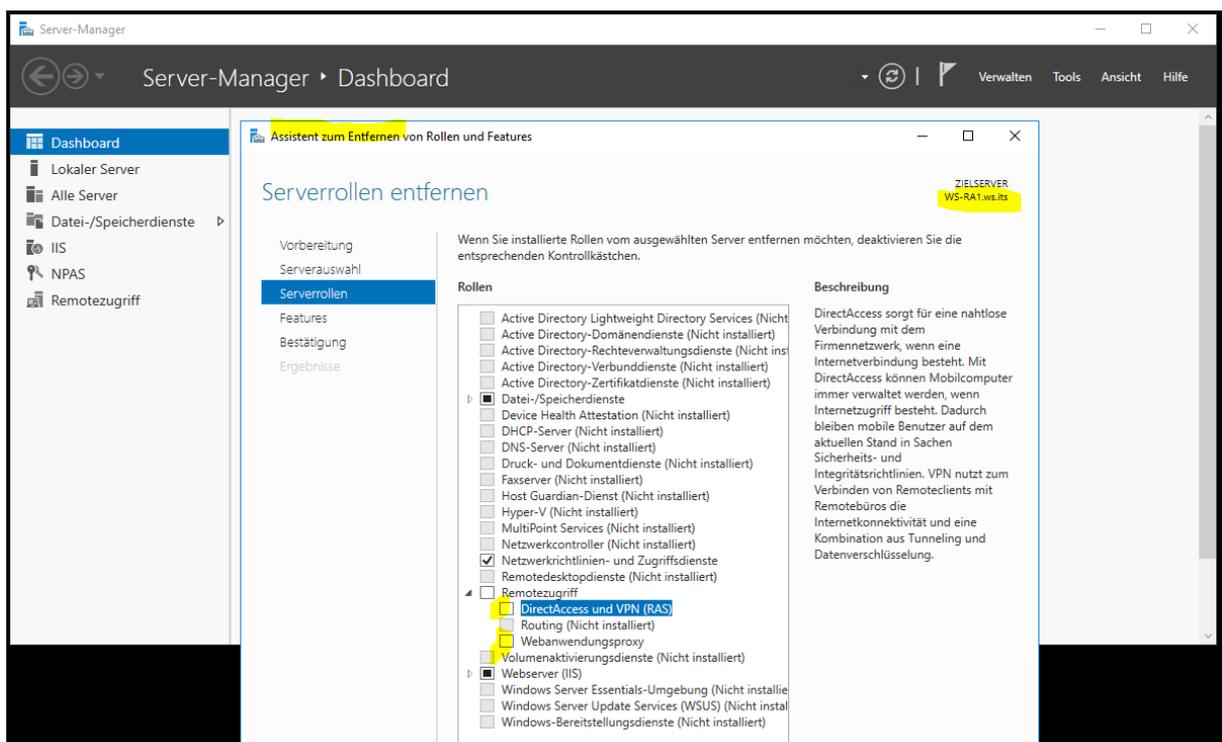


Eine Entfernung der Services WAP und ADFS sind problemlos möglich, da es keine Abhängigkeiten mehr gibt. Bleibt nur die Reihenfolge der Deprovisionierung:

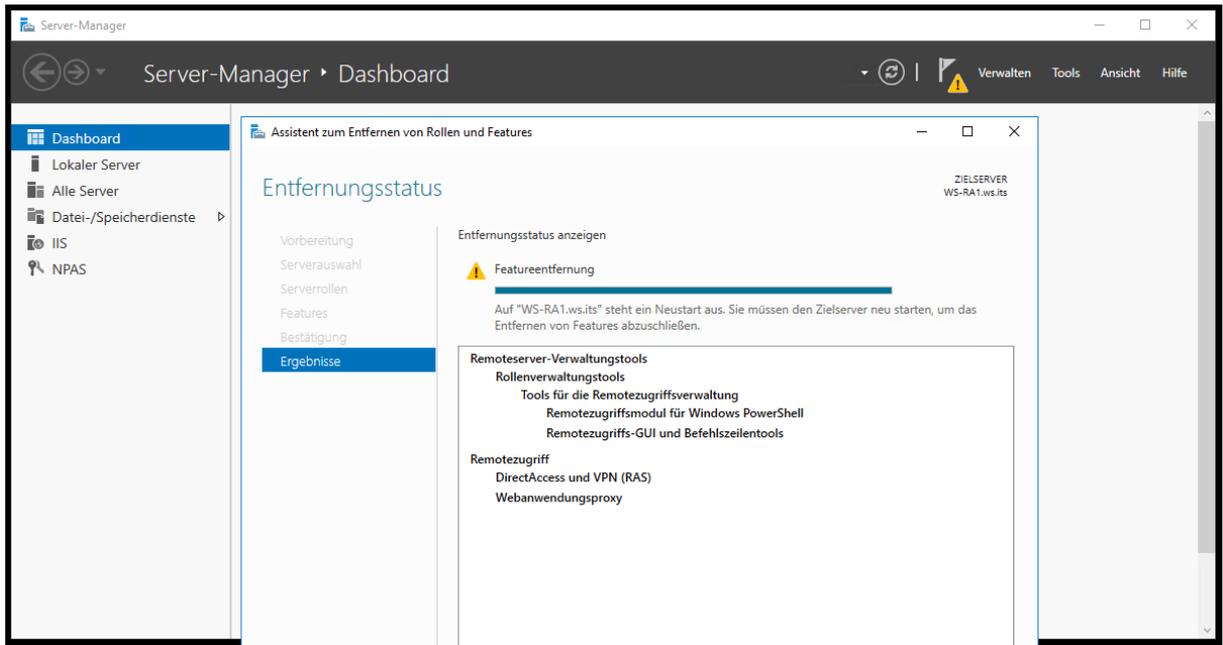
- Ich werde zuerst den defekten WAP-Service auf WS-RA1 löschen
- Dann kann ich WAP auf WS-RA2 korrekt im ADFS löschen.
- ADFS besteht bei mir aus 2 Farm-Mitgliedern: WS-DC1 und WS-DC2. Dabei ist ein Server der Master, alle anderen sind im Slave-Mode. Zuerst entferne ich den Slave.
- Zuletzt entferne ich den ADFS-Master.

Entfernen von WAP auf WS-RA1

Den defekten WAP-Server WS-RA1 kann ich nicht sauber deregistrieren. Daher entferne ich die Rolle und hoffe, dass damit ein positiver Effekt erzielt wird. Nebenbei entferne ich auch das Feature für die VPN-Services:



Der Abschluss ist ein einfacher Neustart:



Entfernen von WAP auf WS-RA2

Auf dem aktiven Server WS-RA2 entferne ich die Rolle mit der PowerShell. Warum? Weil ich es kann!

```

Administrator: Windows PowerShell
PS C:\> Get-WindowsFeature | where installed
-----
Display Name                                     Name                                     Install State
-----
[X] Datei-/Speicherdienste                       FileAndStorage-Services                Installed
[X] Datei- und iSCSI-Dienste                     File-Services                          Installed
[X] Datei- und iSCSI-Dienste                     FS-FileServer                          Installed
[X] Speicherdienste                             Storage-Services                        Installed
[X] Remotezugriff                               RemoteAccess                            Installed
[X] Remotezugriff                               DirectAccess-VPN                        Installed
[X] Remotezugriff                               Web-Application-Proxy                  Installed
[X] Webserver (IIS)                             Web-Server                              Installed
[X] Webserver                                   Web-WebServer                          Installed
[X] Webserver                                   Web-Common-Http                        Installed
[X] Webserver                                   Web-Http-Errors                        Installed
[X] Webserver                                   Web-Default-Doc                        Installed
[X] Webserver                                   Web-Static-Content                     Installed
[X] Webserver                                   Web-Dir-Browsing                       Installed
[X] Leistung                                     Web-Performance                        Installed
[X] Leistung                                     Web-Stat-Compression                   Installed
[X] Sicherheit                                  Web-Security                            Installed
[X] Sicherheit                                  Web-Filtering                           Installed
[X] Sicherheit                                  Web-IP-Security                         Installed
[X] Systemzustand und Diagnose                  Web-Health                              Installed
[X] Systemzustand und Diagnose                  Web-Http-Logging                       Installed
[X] Verwaltungsprogramme                         Web-Mgmt-Tools                          Installed
[X] Verwaltungsprogramme                         Web-Mgmt-Console                       Installed
[X] Verwaltungsprogramme                         Web-Scripting-Tools                    Installed
[X] .NET Framework 4.6-Funktionen                NET-Framework-45-Fea...                 Installed
[X] .NET Framework 4.6                          NET-Framework-45-Core                  Installed
[X] WCF-Dienste                                  NET-WCF-Services45                     Installed
[X] WCF-Dienste                                  NET-WCF-TCP-PortShar...                 Installed
[X] Gruppenrichtlinienverwaltung                 GPMC                                    Installed
[X] Interne Windows-Datenbank                    Windows-Internal-Dat...                 Installed
[X] RAS-Verbindungs-Manager-VerwaltungsKit (CMAK) CMAK                                    Installed
[X] Remoteserver-Verwaltungstools                RSAT                                    Installed
[X] Remoteserver-Verwaltungstools                RSAT-Role-Tools                        Installed
[X] Remoteserver-Verwaltungstools                RSAT-AD-Tools                          Installed
[X] Remoteserver-Verwaltungstools                RSAT-AD-PowerShell                     Installed
[X] Remoteserver-Verwaltungstools                RSAT-RemoteAccess                       Installed
[X] Remoteserver-Verwaltungstools                RSAT-RemoteAccess-Mgmt                 Installed
[X] Remoteserver-Verwaltungstools                RSAT-RemoteAccess-Po...                 Installed
[X] Unterstützung für die SMB 1.0/CIFS-Dateifreigabe FS-SMB1                                 Installed
[X] Windows Defender-Features                    Windows-Defender-Fea...                 Installed
[X] Windows Defender                             Windows-Defender                        Installed
[X] GUI für Windows Defender                     Windows-Defender-Gui                    Installed
[X] Windows PowerShell                           PowerShellRoot                           Installed
[X] Windows PowerShell 5.1                       PowerShell                                Installed
[X] Windows PowerShell ISE                       PowerShell-ISE                           Installed
[X] Windows Server-Sicherung                       Windows-Server-Backup                   Installed
[X] WoW64-Unterstützung                           WoW64-Support                           Installed

PS C:\> Remove-WindowsFeature -Name DirectAccess-VPN,Web-Application-Proxy

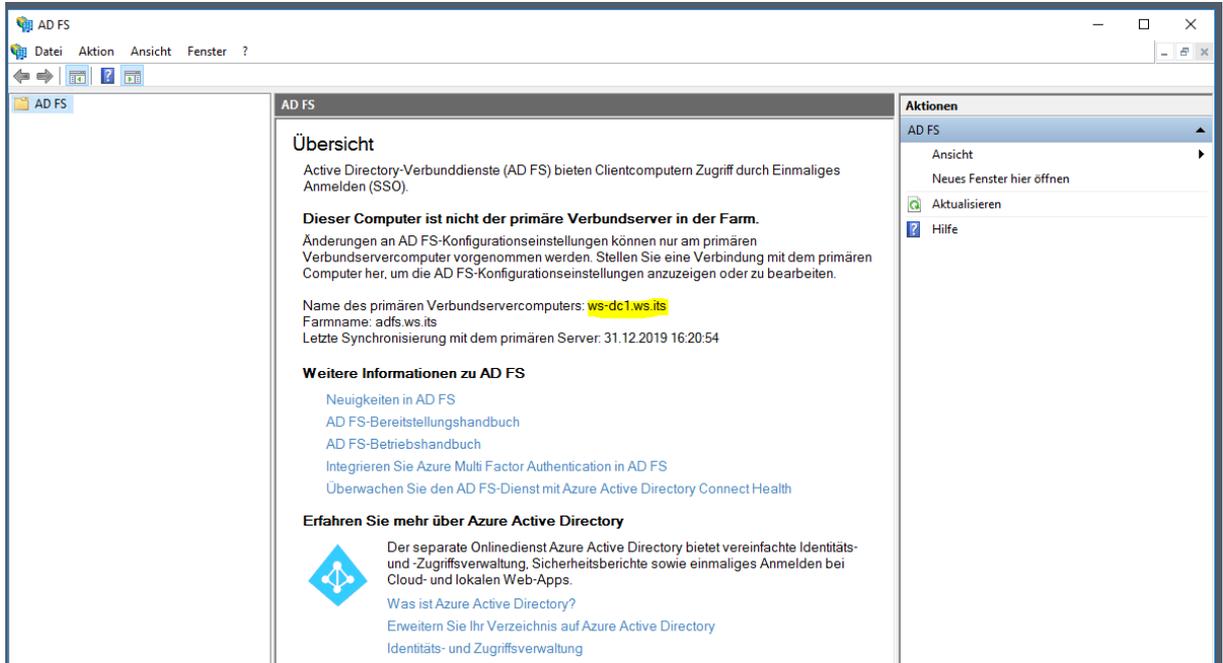
Success Restart Needed Exit Code      Feature Result
-----
True   Yes           SuccessRest... {DirectAccess und VPN (RAS), Remotezugriff...
WARNUNG: Sie müssen den Server neu starten, um das Entfernen abzuschließen.

PS C:\>
    
```

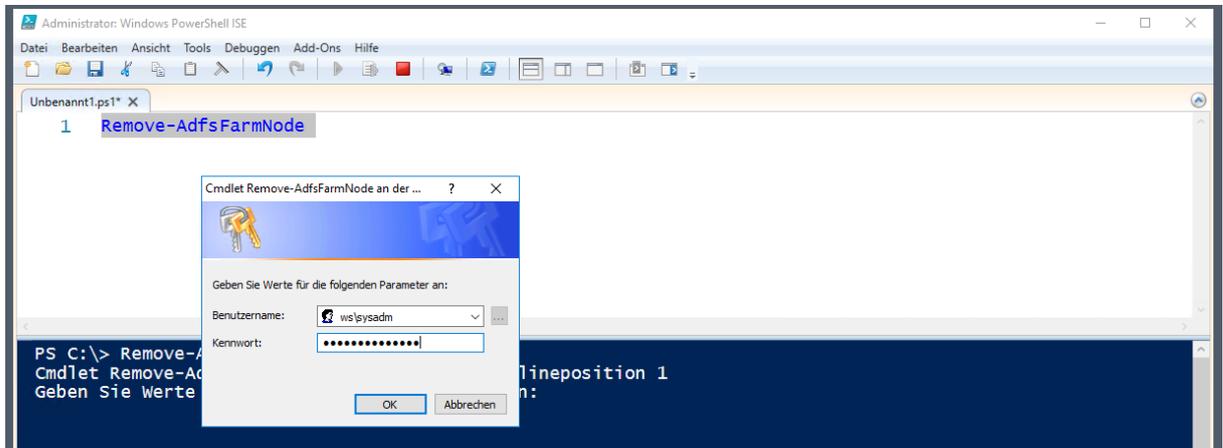
Damit ist der letzte WAP bereinigt.

Entfernen von ADFS auf WS-DC2 (Slave)

Weiter geht es im ADFS. Der Slave-Server ist mein Domain Controller WS-DC2. Ein ADFS auf einer solchen Maschine ist alles andere als optimal. Aber „damals“ hatte ich kaum noch Systemressourcen frei... Das würde ich heute nicht mehr so umsetzen. In der ADFS-Konsole kann ich den Mode des Servers prüfen:



Bevor ich die Rolle deinstallieren kann, entferne ich WS-DC2 als FarmNode aus der ADFS-Farm. Das geht mit der PowerShell:



```

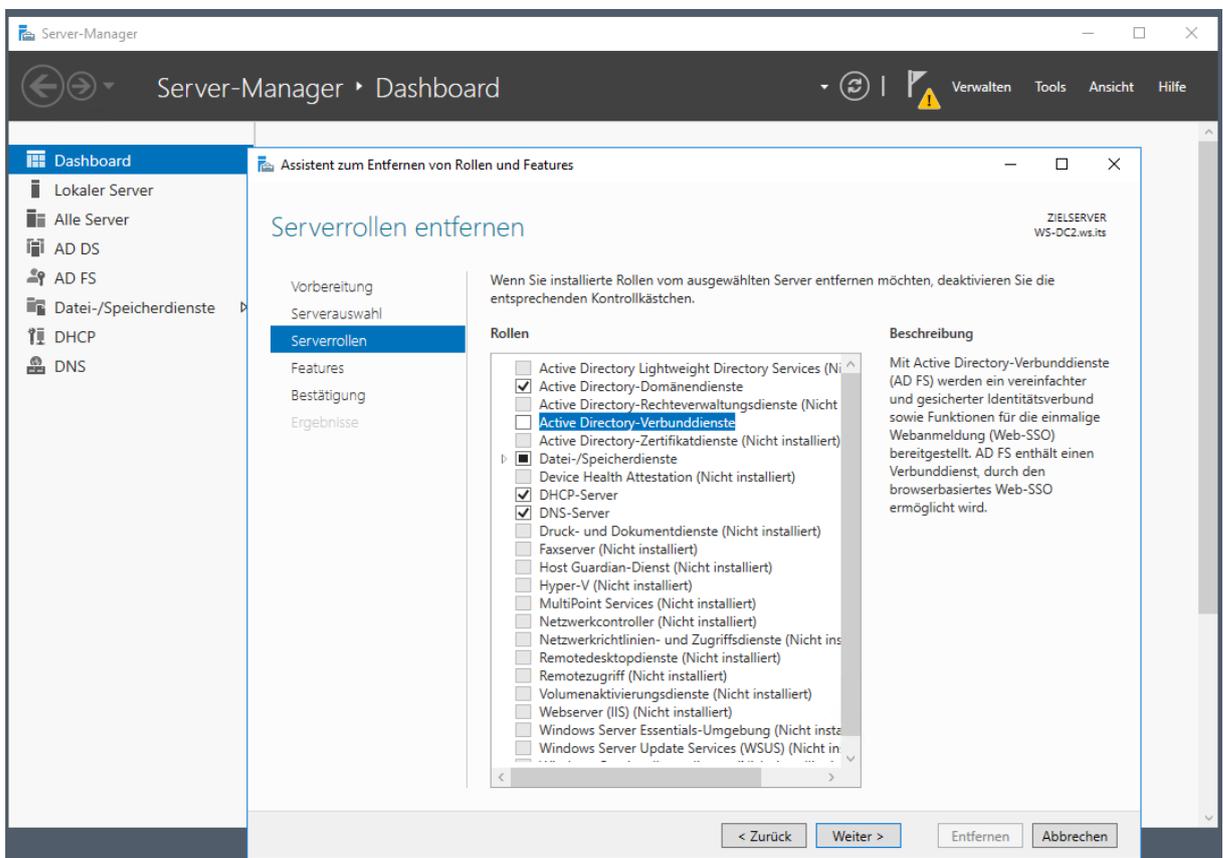
Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1* X
1 Remove-AdfsFarmNode

PS C:\> Remove-AdfsFarmNode
Cmdlet Remove-AdfsFarmNode an der Befehlspipelineposition 1
Geben Sie Werte für die folgenden Parameter an:

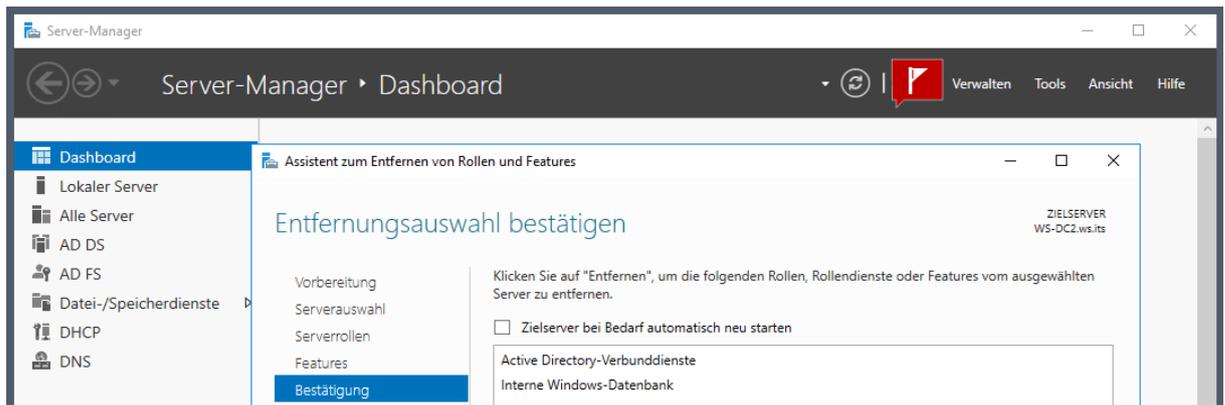
Message                                     Context                                     Status
-----                                     -
Die Konfiguration wurde erfolgreich abgeschlossen. DeploymentSucceeded Success

PS C:\>
    
```

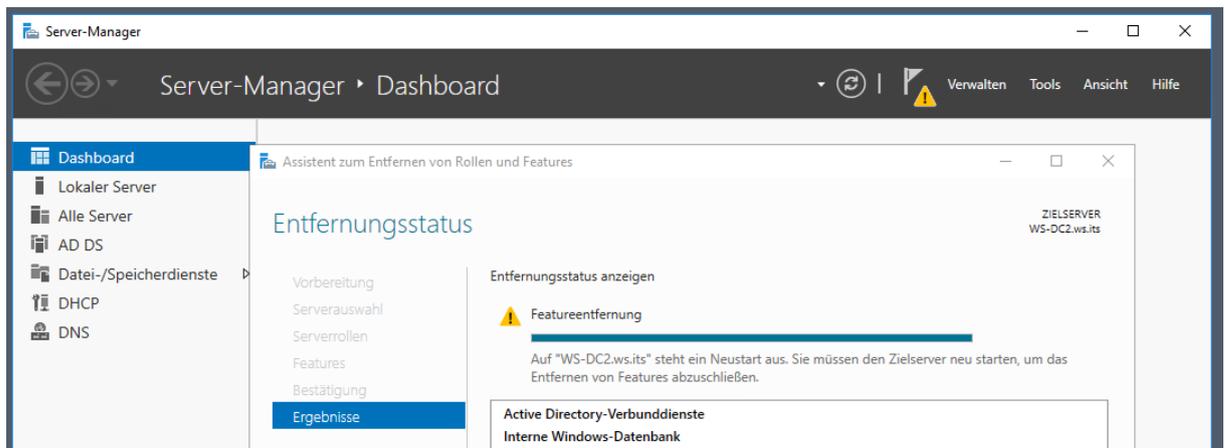
Nun ist die Rolle kein Problem mehr. Ich wähle die Deinstallation im Server Manager aus:



Auch die Windows Internal Database des ADFS wird nicht mehr benötigt:



Die Entfernung muss mit einem Neustart abgeschlossen werden. Da ich 2 Domain Controller einsetze, kann ich einen davon einfach durchstarten:



Ein kurzer Blick in die Ereignisprotokolle nach dem Neustart zeigt keine Fehler oder Warnungen. Das hat funktioniert:

Ereignisanzeige (Lokal)

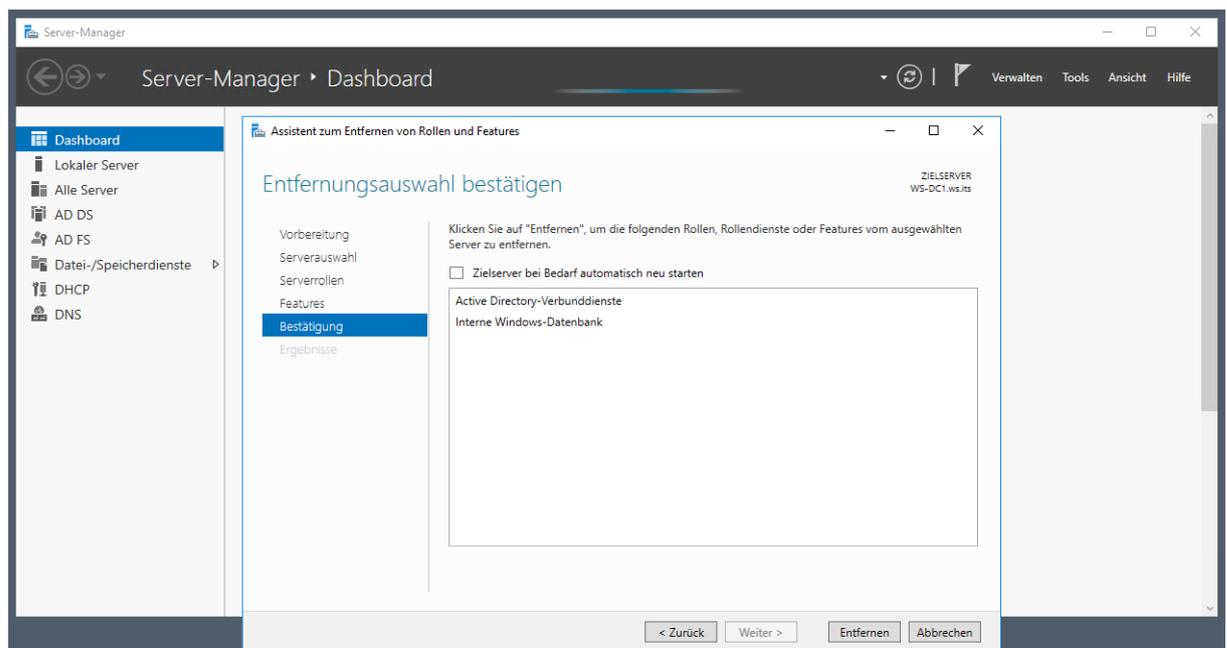
Übersicht und Zusammenfassung

Zusammenfassung der administrativen Ereignisse

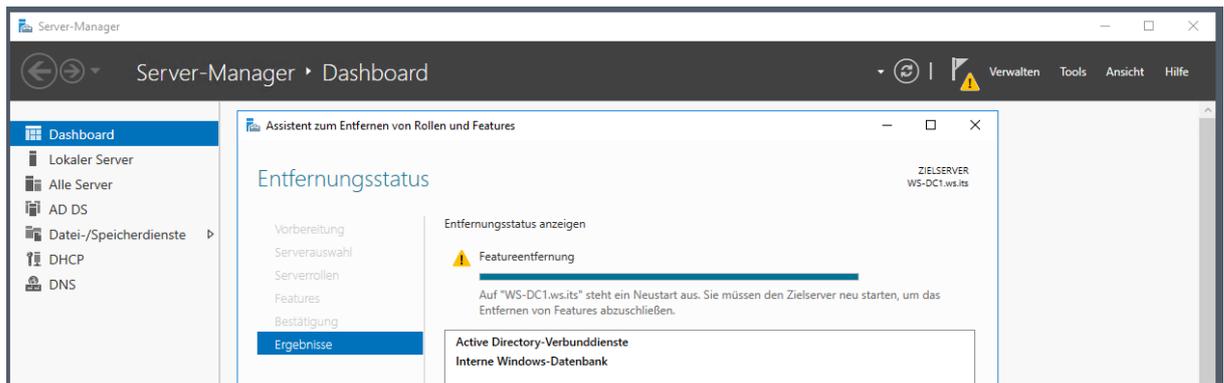
Ereignistyp	Ereignis...	Quelle	Protokoll	Letzte Stu...	24 Stunden	7 Tage
Kritisch	-	-	-	0	0	0
<input checked="" type="checkbox"/> Fehler	-	-	-	95	1.421	9.763
2	Kernel-EventTracing	Microsoft...		0	1	3
3	FilterManager	System		0	0	4
6	CertificateServicesClient-AutoEnrollment	Anwendu...		0	0	1
11	Kerberos-Key-Distribution-Center	System		1	1	2
19	Security-Kerberos	System		1	1	2
67	CertificateServicesClient-CertEnroll	Anwendu...		0	0	1
68	CertificateServicesClient-CertEnroll	Anwendu...		0	0	1
304	User Device Registration	Microsoft...		3	3	3
307	User Device Registration	Microsoft...		3	3	3
513	CAPI2	Anwendu...		0	5	15
1008	Perflib	Anwendu...		6	6	21
2004	PerfNet	Anwendu...		2	2	6
5002	DFSR	DFS-Repli...		1	1	1
7000	Service Control Manager	System		1	1	2
7001	Service Control Manager	System		2	2	4
7023	Service Control Manager	System		1	1	1
7031	Service Control Manager	System		1	1	3
7038	Service Control Manager	System		1	1	2
8193	VSS	Anwendu...		1	1	3
10010	DistributedCOM	System		1	1	1
10016	DistributedCOM	System		50	1360	9564
10028	DistributedCOM	System		16	16	16
20252	DHCP-Server	Microsoft...		1	1	1
20255	DHCP-Server	Microsoft...		1	1	1
20318	DHCP-Server	Microsoft...		1	6	51

Entfernen von ADFS auf WS-DC1 (Master)

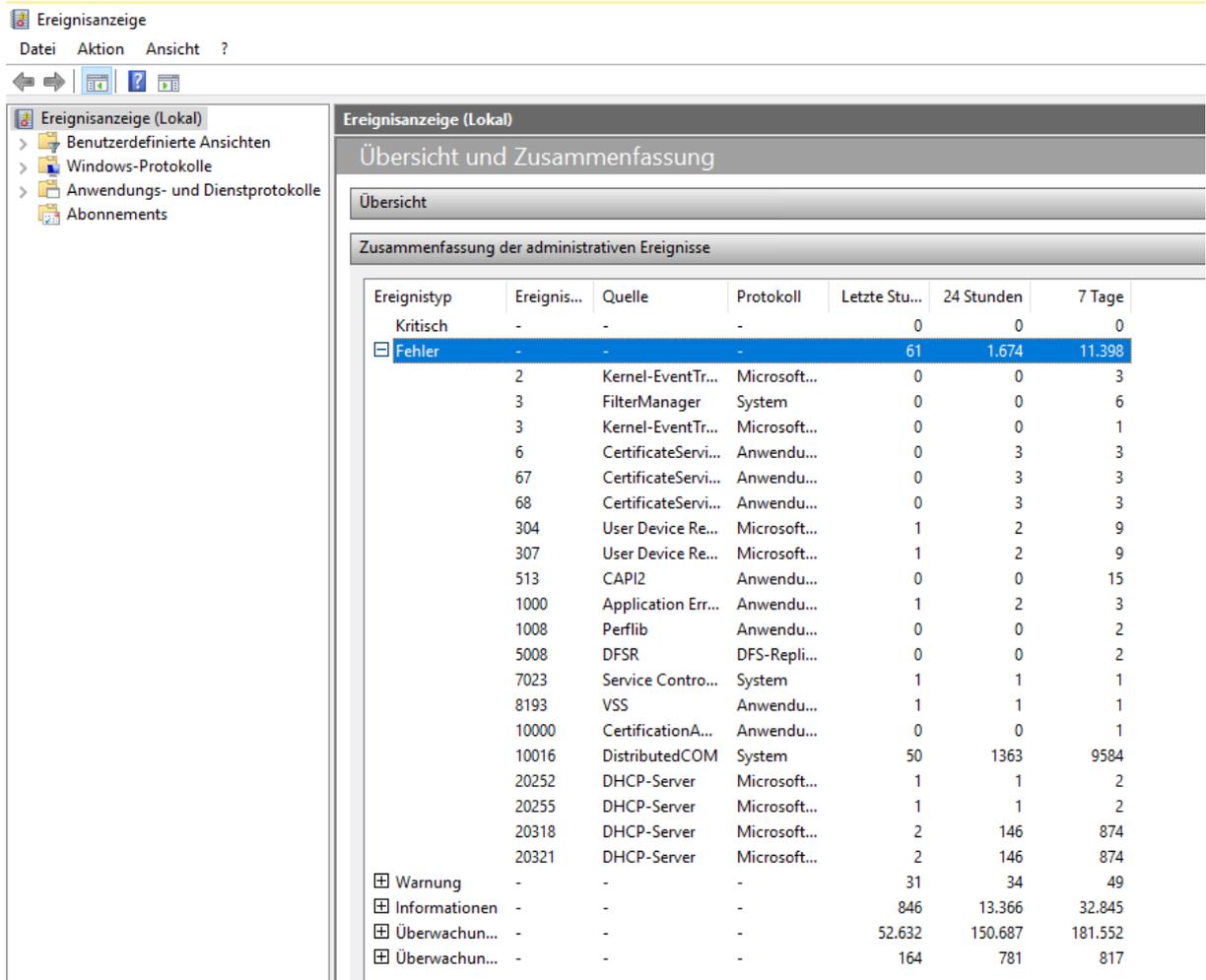
So bleibt nur noch der ADFS-Masternode über. Also geht's auf zum WS-DC1. Hier kann ich die Deinstallation direkt starten. Der letzte ADFS-Node macht sprichwörtlich das Licht aus:



Der Neustartwunsch kommt erwartet und wird umgesetzt:



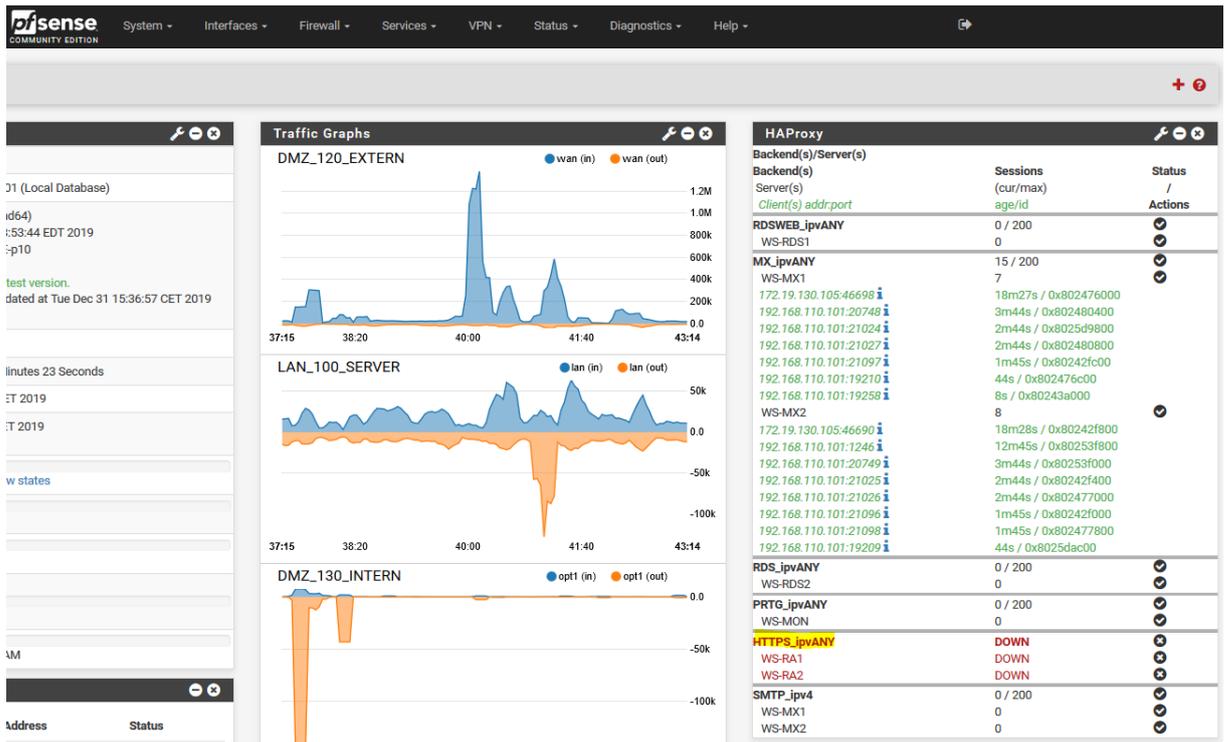
Nach dem Neustart kontrolliere ich wieder die Eventlogs. Auch hier gibt es keine Probleme im Bezug auf die vorherige Entfernung:



Damit sind WAP und ADFS entfernt. Falls ich diese Services morgen wieder benötige, dann installiere ich auf separaten Servern neu.

Bereinigung in der PFSense

Ich habe WAP zwar nicht mehr verwendet, aber der Endpunkt war noch in meiner PFSense registriert. Der HA-Proxy, der die Funktion des WAP übernahm, hat die WAP-Clusternodes damals vorgelagert angesprochen. Diesen Endpunkt benötige ich nicht mehr:



Also entferne ich das hinterlegte Backend für den WAP-Cluster aus dem Frontend des HAProxy:

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	HTTPS-Proxy		172.19.120.120:443	ssl/https	RDSWEB if(RDSWEB) MX if(MX) RDS if(RDS) PRTG if(PRTG) HTTPS (default)	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SMTP-Proxy		172.19.120.120:25	tcp	SMTP (default)	

WAP war bis zu diesem Zeitpunkt der Default-Endpunkt. Da alle Verbindungen gezielt umgeleitet werden, setze ich den Default auf NONE:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend: **None**

Stats options: HTTPS, MX

Separate sockets: PRTG, RDS

Logging options: RDSWEB

Don't log null: SMTP

Die Konfiguration muss in der PFSense bestätigt werden:

Services / HAProxy / Frontend

The haproxy configuration has been changed.
You must apply the changes in order for them to take effect.

Settings Frontend Backend Files Stats Stats FS Templates

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	HTTPS-Proxy		172.19.120.120:443	ssl/https	RDSWEB if(RDSWEB) MX if(MX) RDS if(RDS) PRTG if(PRTG)	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SMTP-Proxy		172.19.120.120:25	tcp	SMTP (default)	

Add Delete Save

Nun ist das HAProxy-Backend frei und kann ebenfalls gelöscht werden:

Services / HAProxy / Backend

Settings Frontend Backend Files Stats Stats FS Templates

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	SMTP	2	SMTP	SMTP-Proxy	
<input checked="" type="checkbox"/>	HTTPS	2	Basic		
<input type="checkbox"/>	RDSWEB	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	MX	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDS	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	PRTG	1	Basic	HTTPS-Proxy	

Add Delete Save

Und dann ist auch hier nichts mehr vom WAP über:

Services / HAProxy / Backend

Settings Frontend Backend Files Stats Stats FS Templates

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	SMTP	2	SMTP	SMTP-Proxy	
<input type="checkbox"/>	RDSWEB	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	MX	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDS	1	Basic	HTTPS-Proxy	
<input type="checkbox"/>	PRTG	1	Basic	HTTPS-Proxy	

Add Delete Save

The screenshot displays the Mikrotik WinBox interface with the following components:

- System Menu:** System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, Help.
- Left Panel:**
 - 01 (Local Database)
 - id64
 - i:53:44 EDT 2019
 - :p10
 - test version.
 - dated at Tue Dec 31 15:36:57 CET 2019
 - minutes 10 Seconds
 - ET 2019
 - ET 2019
 - w states
- Traffic Graphs:**
 - DMZ_120_EXTERN:** Graph showing wan (in) and wan (out) traffic. The y-axis ranges from -500m to 1.0. The x-axis shows time from 42:01 to 48:01.
 - LAN_100_SERVER:** Graph showing lan (in) and lan (out) traffic. The y-axis ranges from -500m to 1.0. The x-axis shows time from 42:01 to 48:01.
- HAProxy Configuration Table:**

Backend(s) Server(s)	Sessions (cur/max)	Status / Actions
RDSWEB_ipvANY WS-RDS1	0 / 200 0	⊗
MX_ipvANY WS-MX1	5 / 200 3	⊗
192.168.110.101:19540 i	51s / 0x80242ac00	
192.168.110.101:13369 i	29s / 0x80242b800	
192.168.110.101:13370 i	29s / 0x80242bc00	
WS-MX2	2	⊗
192.168.110.101:13368 i	29s / 0x80242b400	
172.19.130.106:49124 i	3s / 0x80242b000	
RDS_ipvANY WS-RDS2	0 / 200 0	⊗
PRTG_ipvANY WS-MON	0 / 200 0	⊗
SMTTP_ipv4 WS-MX1	0 / 200 0	⊗
WS-MX2	0	⊗