

## <u>Inhalt</u>

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
Enffernung 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	



## <u>Einleitung</u>

## <u>Zielsetzung</u>

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 Servicenamen 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 <sup>(C)</sup>). 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 PFSene 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.wsits.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-Rounrobin. Am WAP findet dann der Redirect auf den Namen der beiden Mailserver statt – ebenfalls über DNS-Roundrobin:

Remotezugriffs-Verwaltungskonsole					
🕌 Konfiguration VPN	VERÖFFENTLICHTE V     Alle veröffentlichten Web	VEBANWENDUNGEN anwendungen   3 insgesamt			
Webanwendungsproxy	Filter	م			
Dashboard					
Vorgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung	
🜉 Remoteclientstatus	Monitor	https://monitor.ws-its.de/	https://prtg.ws.its/	PassThrough	
Rerichterstellung	MX	https://email.ws-its.de/	https://email.ws.its/	PassThrough	
	RDS	https://rds.ws-its.de/	https://rds.ws-its.de/	PassThrough	
Clusterserver	C:\>nslookup e Server: WS-DC Address: 192. Name: email Addresses: 192. 192.	erung mail.ws.its 1.ws.its 168.100.1 1.ws.its 22.168.100.13 168.100.3			_

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:

🗾 WS-PI	FS1a.ws.its - Status: Dashb 🗙 🕂					
÷) → C'	ⓓ ▲ https://ws-pfs1.w	s.its		··· 🖂 🚖	III\ 🗉 🚯 💾	<mark>, off</mark> ∰
DuckDuckGo	🗀 Devices 📋 Links					
	Se System - Interfaces - Fire ।गा००	wall → Services → VPN →	Status 🕶 Diagnos	stics ▼ Help ▼		•
Status /	/ Dashboard					+ 0
System I	nformation 🛛 🗲 🖨 😸	Traffic Graphs	۶۵۵	HAProxy		<b>₽</b> ⊖ 8
Name	WS-PFS1a.ws.its	DMZ_120_EXTER wan	(in) 😑 wan (out)	Backend(s)/Server(s)	Cassiana	Chatrus
User	admin@192.168.110.101 (Local Database)		1.0M	Server(s) Client(s) addr:port	(cur/max) age/id	/ Actions
Version	2.4.4-RELEASE-p3 (amd64)		600k	RDSWEB_ipvANY WS-RDS1	0 / 200 0	0
	FreeBSD 11.2-RELEASE-p10		400k	HTTPS_ipvANY WS-RA1	4 / 200 4	00
	The system is on the latest version. Version information updated at Sun Oct		2019-10-27 11:37:21	109.41.193.223:22870 <b>i</b> 109.41.193.223:1049 <b>i</b>	5m27s / 0x802 5m27s / 0x802	250e400 2597800
	27 11:36:10 CET 2019 🔁	34:03 36:40	wan (in) 0.00 b/s	109.41.193.223:3713	7s / 0x8025b3	800
Kernel PTI	Disabled	LAN_100_SERVER Ian	(in) lan (out)	109.41.193.223:6227 <b>1</b> WS-RA2	7s / 0x80243c 0	000
Uptime	21 Days 19 Hours 38 Minutes 13 Seconds		0.0	SMTP_ipv4 WS-MX1	0 / 200 0	00
Current	Sun Oct 27 11:40:07 CET 2019		-100k	WS-MX2	0	0

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



#### <u>Umbau</u>

WS IT-Solutions

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:

) → C' <b>G</b>	ť		🛛 🔒 https:	://ws-pfs1. <b>ws.i</b> '	.its/haproxy	y/haproxy_liste	ners.php		🖂 1	☆ III	\ 🗉 💿 💾	OFF i
DuckDuckGo	Devices	Links										
	C Sys	stem 🕶	Interfaces	s <del>▼</del> Firew	wall <del>-</del>	Services 🕶	VPN 🗸	Status 🕶	Diagnostics 👻	Help 🕶		C
Service	es / HA	Prox	y / Fronte	end							Со 🗄 🎹	. 🗖 🕄
Settings	Fronte	nd	Backend	Files S	Stats	Stats FS	Templates					
Settings Frontend	Fronte	nd	Backend	Files S	Stats	Stats FS	Templates					
Settings Frontence Primary	Fronte d s Shared	nd On	Backend Advanced	Files S Name	Stats	Stats FS Description	Templates Address	3	Туре	Backend	Act	ions
Settings Frontence Primary	Fronte ds Shared	end On	Backend Advanced	Files S Name HTTPS-Pr	Stats 'roxy	Stats FS Description	Templates Address 172.19	<b>;</b> 120.120:443	<b>Type</b> ssl/https	Backend RDSWEB if(RDSW HTTPS (default)	Act EB)	ions

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

of WS-PFS1a.ws.its -	Services: HAF × +					- 0
→ C' 🏠	0	https://ws-pfs1.ws.its/hapr	oxy/haproxy_pools.php		⊠ ☆	III\ 🗉 💿 💾 👎 👬
)uckDuckGo  🗎 Device	es 🗎 Links					
	System - Inter	faces 👻 Firewall 👻	Services - VP	N → Status →	Diagnostics 👻 Help 👻	e
Services / I	HAProxy / Ba	ickend				С⊚ 幸 Ш 🗏 8
Settings Fro	ontend Backend	d Files Stats	Stats FS Temp	plates		
Backends						
	Advanced	Name	Servers	Check	Frontend	Actions
		SMTP	2	SMTP	SMTP-Proxy	e 🖉 🛍 🗋
-						
□.₺		HTTPS	2	Basic	HTTPS-Proxy	e 🖉 🛍 🗠
□± □±		HTTPS RDSWEB	2	Basic	HTTPS-Proxy HTTPS-Proxy	◢ֿײַ עַּיּהַר

Die Mailserver werden von den Clients über https angesprochen. Daher wähle ich eine 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:

	System -	Interfaces 🗸	Firewall 🗸	Services 🕶	VPN 👻 Sta	atus <del>-</del> D	iagnostics <del>-</del>	Help 🗸		¢
Services	/ HAProx	ky / Backend	I / Edit						Co	≢ III 🔲 0
Settings	Frontend	Backend Fi	es Stats	Stats FS	Templates					
Edit HAPr	oxy Backend	l server pool								
	Name	MX								
	Server list	Table								
		Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
		active 🔒	WS-MX1	Address+Port:	192.168.100.3	3 <mark>443</mark>	no	no		e 🖉 🖉 🖉
		Ð								
		□ 📩 active	WS-MX2	Address+Port:	<mark>192.168.100.</mark>	443	no	no		e 🖉 🛍 🗋
		÷.								
		Field explanations	•							
Loadbalar	ncing option	s (when multip	e servers a	re defined)						Θ
	Balance	None		t t i ini						
		This allows writing	your own cust	om balance setting	s into the advanced	i section. Or w	nen you nave no	need for balancing	) with only 1	server.
		O Round robin								
		Each server is use	d in turns, acco	ding to their weigh	ts. This is the smo	othest and fair	est algorithm wh	en the server's pro	cessing time	remains
Health che	ecking									
Health ch	eck method	Basic			`	·				
		Basic socket cor	nection check			1				

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

WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

WS-PFS1a.ws.its - Services: H/	AF × +				
→ C' û	🛛 🔒 https://ws-pfs1.ws.it	ts/haproxy/haproxy_pools.php	)	⊠ ☆	III\ 🗊 💿 💾 👎 👬
JckDuckGo 🗎 Devices 🗎 Link	5				
Sense System -	- Interfaces <del>-</del> Firew	rall <del>→</del> Services <del>→</del> V	PN - Status -	Diagnostics → Help →	•
Services / HAProx	xy / Backend				С⊚ ≆ Ш 🗏 0
The haproxy configuration h	as been changed.				🗸 Apply Changes
You must apply the changes	s in order for them to take effec	ct.			
You must apply the changes Settings Frontend	s in order for them to take effer Backend Files S	ct. Xats Stats FS Ten	nplates		
You must apply the changes Settings Frontend Backends	s in order for them to take effer Backend Files S	ct. Nats Stats FS Ten	nplates		
You must apply the changes Settings Frontend Backends Advanced	s in order for them to take effer Backend Files S Name	ct. Xats Stats FS Ten Servers	nplates Check	Frontend	Actions
You must apply the changes Settings Frontend Backends Advanced	Backend Files S Name SMTP	ct. Stats Stats FS Ten Servers 2	nplates Check SMTP	Frontend SMTP-Proxy	Actions
You must apply the changes Settings Frontend Backends Advanced	Backend Files S Name SMTP HTTPS	ct. Stats Stats FS Ten Servers 2 2 2	nplates Check SMTP Basic	Frontend SMTP-Proxy HTTPS-Proxy	Actions
You must apply the changes Settings Frontend Backends Advanced 	Backend Files S Name SMTP HTTPS RDSWEB	ct. Stats Stats FS Ten Servers 2 2 2 1	nplates Check SMTP Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy	Actions

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:

WS-PFS1a.ws.its - Services: I	+ × 14	- 🗆 ×
$\overleftarrow{\leftarrow}$ > C $\textcircled{a}$	🛛 🔒 https://ws-pfs1. <b>ws.its</b> /haproxy/haproxy_listeners_edit.php?id=HTTPS-Pr	III\ 🗉 💿 🖺 👎 👬 =
🕡 DuckDuckGo 🗎 Devices 🗎 Lir	ks	
COMMUNITY EDITION	Interfaces • Firewall • Services • VPN • Status • Diagnostics • Help •	€ •
Services / HAPro	xy / Frontend / Edit	С⊚ 幸 Ш 🗏 6
Settings Frontend	Backend Files Stats Stats FS Templates	
Edit HAProxy Fronten	i	
Name	HTTPS-Proxy	
Description		
Status	Active	
Shared Frontend	☐ This can be used to host a second or more website on the same IP:Port combination. Use this setting to configure multiple backends/accesslists for a single frontend. All settings of which only 1 can exist will be hidden. The frontend settings will be merged into 1 set of frontend configuration.	
External address	Define what ip:port combinations to listen on for incomming connections.	
	SSL	
	Listen address Custom address Port Offloading Adv	vanced Action
	□ Use custom address: ✓ 172.19.120.120 443 □	<b>m</b> (
	1 <	>

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.wsits.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:

## WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

	If you want this rule t	apply to another IF	address than the IP address	ess of the interface ch	osen above	, select	it here (you need to defi	ine Virtual IP
	addresses on the firs	t). Also note that if y	ou are trying to redirect co	onnections on the LAN	select the	any" op	tion. In the port to listen	n to, if you want to
	you would likely want	to check the SSL-of	floading checkbox.	ou,ouou or to listen on	1 DOLTI OU AL	ia 445 c	reate z rows in the table	e where for the 445
Max connections								
	Sets the maximum a	mount of connection	ns this frontend will accept	t, may be left empty.				
Туре	ssl / https(TCP mo	de)		~				
	This defines the proc	essing type of HAPr	oxy, and will determine the	availabe options for a	acl checks a	and also	several other options.	
	Please note that for h	ittps encryption/dec	ryption on HAProxy with a	certificate the process	sing type ne	eds to b	be set to "http".	
	r leade note that for i	inpo enoryphon, dee	sphon on the loxy mana	ber and are proceed	ong type ne		o det to map.	
for the second second		- 1 1						
efault backend, acc	ess control lists a	nd actions						
efault backend, acc	ess control lists a	nd actions	a durith antique defined by	lau de se franchese			dui	
efault backend, acc Access Control lists	use these to define c	nd actions riteria that will be us	ed with actions defined be	elow to perform them a	only when c	ertain co	onditions are met.	
efault backend, acc Access Control lists	use these to define c Table	nd actions riteria that will be us	ed with actions defined be	elow to perform them o	only when c	ertain co	onditions are met.	
efault backend, acc Access Control lists	ess control lists a Use these to define o Table Name	nd actions riteria that will be us Expression	ed with actions defined be	elow to perform them o	only when c CS	ertain co Not	onditions are met. Value	Actions
efault backend, acc Access Control lists	Use these to define of Table	nd actions riteria that will be us Expression Server Name	ed with actions defined be Indication TLS extension 1	elow to perform them o matches:	only when c CS no	ertain co Not no	onditions are met. Value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table Name	nd actions riteria that will be us Expression Server Name	ed with actions defined be Indication TLS extension	elow to perform them o matches:	only when c CS no	ertain co Not no	onditions are met. Value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table Table RDSWEE Table	nd actions riteria that will be us Expression Server Name	ed with actions defined be Indication TLS extension :	How to perform them of the second sec	only when c CS no	ertain co Not no	onditions are met. Value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table Name C trable Name C trable Name C trable Name C trable Name C trable Name C trable C trable	nd actions riteria that will be us Expression Server Name g matches 'Case Ser	ed with actions defined be Indication TLS extension i nsitive' so www.domain.tld	Now to perform them of matches:	only when c CS no	ertain co Not no main.TL	value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table Name Table RDSWEE T ToCS' makes the strin - 'Not' makes the mat	nd actions riteria that will be us Expression Server Name g matches 'Case Set ch if the value given	ed with actions defined be Indication TLS extension i nsitive' so www.domain.tld is not matched	alow to perform them of matches:	no cs no	ertain co Not no main.TL	Value rdsweb.ws-its.de	Actions I to C
efault backend, acc	Use these to define of Table RDSWEE C'S' makes the strin - 'CS' makes the mat Example:	nd actions riteria that will be us Expression Server Name g matches 'Case Ser ch if the value given	ed with actions defined be Indication TLS extension in insitive' so www.domain.tld is not matched	alow to perform them of matches:	CS no	ertain co Not no main.TL	value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table RDSWEE C'CS' makes the strin - 'CS' makes the mat Example: Name Expres	nd actions riteria that will be us Expression Server Name g matches 'Case Set ch if the value given sion	ed with actions defined be Indication TLS extension i nsitive' so www.domain.tld is not matched CiNotValue	elow to perform them of matches:	CS no	ertain co Not no main.TL	Value rdsweb.ws-its.de	Actions
efault backend, acc	Use these to define of Table Name Table Name C'CS' makes the strin - 'CS' makes the strin - 'Not' makes the mat Example: Name Expres Backend1acl Host m	nd actions riteria that will be us Expression Server Name g matches 'Case Ser ch if the value given sion natches	ed with actions defined be Indication TLS extension i nsitive' so www.domain.tld is not matched CINOtValue www.yourdomain.tld	elow to perform them of matches:	only when c CS no	ertain co Not no main.TL	Value rdsweb.ws-its.de	Actions

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

WS-PFS1a.ws.its - Service	es: HAF 🗙 🛛 🗕	F											- 0	
(←) → ⊂ ⊕	0	https://ws-pfs1	.ws.its/haproxy	y/haproxy_listen	ers_edit.php?	id=HTTPS-Pn	Ē	©	9 ☆	lii\			OFF	# ≡
🚺 DuckDuckGo 🛅 Devices 🗎	Links													
Max connections														
	Sets the	maximum amou	nt of connecti	ons this fronten	d will accept	, may be left e	mpty.							
Туре	ssl / ht	ttps(TCP mode)				$\sim$								
	This defi	ines the processi	ng type of HA	Proxy, and will d	letermine the	availabe opti	ons for ac	l checks	and al	so several other opti	ons.			
	Please n	ote that for https	encryption/d	ecryption on HA	Proxy with a	certificate the	e processi	ing type	needs t	o be set to "http".				
Default backend, ac	cess cont	trol lists and	actions											
Access Control lists	Use thes	se to define criteri	ia that will be	used with action	ns defined be	low to perforr	n them or	nly when	certain	conditions are met.				
	Table	9												
		Name		Expression				С	S Not	Value		Act	tions	
	□♣	RDSWEB		Server Name I	Indication TL	S extension m	natches:	r	io no	rdsweb.ws-its.de		4	✐₫	)
	<b>•</b>	MY		Server Name	Indication T	S extension r	natches:	~ [		omoil wo ito dol		<b>1</b> m̂	╔╖ <b>ѧ╶</b> ╻	
		WIA		ocreat Name	marcation	Lo extension i	natories.	- 1		email.ws-its.de			· • •	-
	Ţ													

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:



worrona.waita berricea.	HAF × +						- 🗆	
€) → ୯ û	🛛 🔒 https://ws-pfs1	l.ws.its/haproxy/hap	roxy_listeners_edit.ph	p?id=HTTPS-Pr		III\ 🗊 🚯	🗎 💔 i	1 ≡
🗿 DuckDuckGo  🗎 Devices 🗎 Li	inks							
	Example:	r the value given to h	normatorica					
	Name Expressio	n CIN	lotValue					
	Backend1acl Host mate	hes	www.yourdomain.	tld				
	addHeaderAclSSL Client	certificate valid						
	acl's with the same name	e will be 'combined' r	using OR criteria.					
	For more information abo	out ACL's please see	e HAProxy Document	ation Section 7 - Using	ACL's			
				_				
	-acl's are no longer comb	in behaviour, since   pined with logical AN	package version 0.3 D operators, list mul	2 tiple acl's below where	needed			
	-acl's alone no longer imp	plicitly generate use.	_backend configurati	on. Add 'actions' below	v to accomplish this behaviour.			
	Action			Parameters	Condition acl names	Ac	tions	
	Action			Parameters	Condition acl names	Ac	ctions	
	Use Backen	d		See below	RDSWEB			
	Use Backen	d )SWEB		See below	RDSWEB		<i>₽</i> ₩ L	
	Use Backen	d DSWEB	~	See below See below	RDSWEB	1	<ul><li>✓ 前 ()</li><li>前() 小 小</li></ul>	
	Use Backen	d DSWEB	~	See below See below	RDSWEB	]	╱ฃ∪ ©∩≁↓	
	Use Backend: RL backend: RL Use Backerd: ML	d DSWEB nd X ~	~	See below See below	RDSWEB	]	◢ֿ ₽ ₽	
	Use Backen backend: Rt Use Backer backend: Mt	id DSWEB Ind X ~	~ ·	See below See below	RDSWEB	]	╱ <sup>₩</sup> □	
	Use Backen backend: Rt Use Backer backend: Mt Example:	d DSWEB nd X ~	×.	See below	RDSWEB	]	₽````	
	Use Backend: RE backend: RE backend: M backend: M backend: M comple: Action P	d DSWEB Ad X V arameters		See below See below	RDSWEB	]	ℰш	
	Use Backend: M Use Backend: M backend: M	d DSWEB Ad X V arameters Vebsite1Backend		See below See below ondition ackend1acl	RDSWEB	]	✓ ± (-) ± (-)	
	Use Backend: Use Backend: Use Backend: Lxample: Action P Use Backend M http-request header set N	d DSWEB nd X Varameters Vebsite1Backend feadername: X-HEAL few logformat value:	C DER-ClientCertValid v: YES	See below See below ondition ackend1acl ddHeaderAcl	RDSWEB MX	]	✓ ± □	
Default Backend	Use Backend: RE backend: RE backend: M backend: M backend: M backend: M backend: M backend: M backend W http-request header set H http-request header set H http-request header set H https	d DSWEB nd X v arameters Vebsite1Backend leadername: X-HEAD leaw logformat value:	v E DER-ClientCertValid 2: YES	See below See below	RDSWEB MX		✓ ± (_)	
Default Backend	Use Backend: Rt Use Backend: Rt Use Backend: M Complete Backend: M Use Backend M http-request header set N HTTPS If a backend is salested u	d DSWEB A A A A A A A A A A A A A A A A A A A	V C C C C C C C C C C C C C C C C C C	See below See below	RDSWEB	]	✓ ± · · · · · · · · · · · · · · · · · ·	

#### Ein Apply später ist diese Regel aktiv:

MS-PFS	51a.ws.its - Sen	vices: HAP	× +						- 0
→ C' 1	ŵ		🗊 🔒 https:	://ws-pfs1. <b>ws.its</b> /hapr	oxy/haproxy_listen	ers.php	🛛 1	☆ lii\ 0	🗊 🚯 💾 💔
uckDuckGo	Devices	🗎 Links							
	SE Sy	stem 🝷	Interfaces	s → Firewall →	Services -	VPN 👻 Status 🕶	Diagnostics 👻	Help 🗸	
Servic	ces / HA	Prox	y / Fronte	end				c	C® ≆ 🔟 🗏 6
Settings	Fronte	end	Backend	Files Stats	Stats FS	Templates			
Settings Fronten	Fronte	end	Backend	Files Stats	Stats FS	Templates	Ture	Deshard	Anima
Settings Fronten Primary	Fronte nds Shared	end On	Backend	Files Stats	Stats FS Description	Templates Address	Туре	Backend	Actions
Settings Fronten Primary	Fronte nds Shared	on On	Backend Advanced	Files Stats Name HTTPS-Proxy	Stats FS Description	Templates Address 172.19.120.120:443	Type ssl/https	Backend RDSWEB if(RDSWEB) MX if(MX) HTTPS (default)	Actions
Settings Fronten Primary	Fronte nds Shared	on On	Backend Advanced	Files Stats Name HTTPS-Proxy SMTP-Proxy	Stats FS Description	Templates Address 172.19.120.120:443 172.19.120.120:25	Type ssl/https tcp	Backend RDSWEB if(RDSWEB) MX if(MX) HTTPS (default) SMTP (default)	Actions P 11 P 11

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:

🗾 WS-PI	FS1a.ws.its - Status: Dashb × +						- 0
-) → C	D A https://ws-pfs1.	vs.its			··· 🖂 🚖	III\ 🗉 🔒	🗎 💔 👬
DuckDuckGo	Devices Links						
	SC System ▼ Interfaces ▼ Fire	wall - Services - VPN -	Status 🗸	Diagnos	tics <del>▼</del> Help <del>▼</del>		€
Status /	/ Dashboard						+ 0
System I	nformation 🛛 🗲 🗢 😣	Traffic Graphs	) عمر	<b>&gt;</b> 8	HAProxy		3
Name	WS-PFS1a.ws.its	DMZ_120_EXTER wan (in)	🛑 wan (out)	4.0	Backend(s)/Server(s)		<b>e</b>
User	admin@192.168.110.101.(Local			1.0	Server(s)	Sessions (cur/max)	Status /
	Database)			500m	Client(s) addr:port	age/id	Actions
largian	244 051 5455 -2 (			50011	RDSWEB_ipvANY	0 / 200	0
rsion	2.4.4-RELEASE-p3 (amd04) huilt on Wed May 15 18:53:44 EDT 2010			0.0	WS-RDS1	0	0
	FreeBSD 11.2-RELEASE-p10			0.0	MX_ipvANY	0 / 200	0
				-500m	WS-MX1	0	0
	The system is on the latest version.			50011	WS-MX2	0	•
	Version information updated at Sun Oct			10	HTTPS_ipvANY	0 / 200	0
	27 11:36:10 CET 2019 🛃	<b>45:24</b> 46:40	50:00 51	:24	WS-RA1	0	<b>S</b>
Kernel PTI	Disabled		lon (out)	_	WS-RA2	U	<u> </u>
Un Alexan	01 5 10 11 40 14 1 00	LAN_IOU_SERVER Ian (in)	-ian (out)	1.0	SMTP_ipv4	0 / 200	<b>S</b>
optime	21 Days 19 Hours 49 Minutes 28				WS-MX1	U	Sec. 1
	Seconds			500m	VVS-IVIX2	U	<b>v</b>

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:

La DNS-Manager				
Datei Aktion Ansicht ?				
⊨ →   <u>≈</u>   🗊 🔍 🖳   📰 🗮	j.			
DNS WS-DC1 WS-DC1 Convard-Lookupzonen Convard	Name         [ (identisch mit übergeordne]         [ Neuer Host         Name (bei Nichtangabe wi verwendet):         [	Typ Autoritätsursprung (SOA) Namenserver (NS) Namenserver (NS) Host (A) Host (A) Host (A) ag erstellen er können DNS-Einträge mit de ieren (TTTTT:HH.MM.SS) Host hinzufügen Abt	Daten [3], ws-dc1.ws.its., hostma ws-dc2.ws.its. ws-dc1.ws.its. 192.168.100.17 192.168.100.7	Zeitstempel Static Static Static Static Static Static

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

**VS IT-Solutions** 

**NS IT-Solutions** 

🏯 DNS-Manager				
Datei Aktion Ansicht ?				
🗢 🔿 🙍 📰 🗙 🗟 🛛 🖬 📋 🛱				
<ul> <li>DNS</li> <li>WS-DC1</li> <li>Zwischengespeicherte Lookupvorgänge</li> <li>Forward-Lookupzonen</li> <li></li></ul>	Name (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne (identisch mit üt (identisch mit üt Hilfe	Typ Autoritätsursprung (SOA) Namenserver (NS) Namenserver (NS) Host (A) en	Daten [3], ws-dc1.ws.its., hostma ws-dc2.ws.its. ws-dc1.ws.its. 192.168.100.17 192.168.100.7 172.19.120.120	Zeitstempel Static Static Static Static Static Static
W3-DC3				

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:

**NS IT-Solutions** 

🖬 WS-	PFS1a.ws.its - Status: Sj	yster × +									-	
$\rightarrow$ C	ŵ	🗊 🔒 https://v	vs-pfs1. <b>ws.its</b> /stat	us_logs_filte	r.php			⊠ ☆	•	\ ⊡	🕒 💾	ÇFF 📫
DuckDuckG	io 🗎 Devices 🗎 Li	inks										
of ser	ISE System	✓ Interfaces ✓	Firewall 👻	Services	- V	PN <del>-</del>	Status 👻 Diag	gnostics 👻	Help 🛨			
DMMUNITY E	EDITION											
Statu	Is / System	Loas / Firewa	all / Norma	l View							T	10
System	i Firewall	DHCP Captive	e Portal Auth	IPsec	PPP	VPN	Load Balancer	OpenVPN	NTP	Settings		
-,												
Norma	l View Dynam	iic View Summ	ary View									
	the sector											
Advan	iced Log Filter	Character										
		192.168.110					172.19.12	20.120				
		Source IP Address					Destination	n IP Address				
		Pass								500		÷
		Tim	10			Source	e Port	Protocol		Quantity		
		□ Block								T Apply	Filter	
		Inte	erface			Destin	ation Port	Protocol Fla	gs			
		Regular expression	reference Preced	de with excla	amation (!)	to exclud	e match.					
7.14	1 1 1 1 1 1 1	F /	. 500)	_	_	_	_	_	_	_	_	_
/ Mat	Time	log Entries. (Ma)	amum 500)				Sam		Dev	dination	Due	da se l
Action	I Ime	Interrace	Rule				sour	rce	Des	stination	Pro	tocol
×	Oct 27 11:51:53	LAN_110_CLIENTS	Default deny ru	le IPv4 (100	0000103)		iE	192.168.110.10	1:5035	172.19.120.12	0:443 TC	P:S
×												
	Oct 27 11:51:51	LAN_110_CLIENTS	Default deny ru	le IPv4 (100	0000103)		iE	192.168.110.10	1:5035	172.19.120.12	0:443 TC	P:S
×	Oct 27 11:51:51 Oct 27 11:51:50	LAN_110_CLIENTS	Default deny ru Default deny ru	le IPv4 (100 le IPv4 (100	10000103) 10000103)		i E	) 192.168.110.10 ) 192.168.110.10	1:5035 1 1:5035 1	172.19.120.12 172.19.120.12	0:443 TC 0:443 TC	P:S

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:

→ CI	ŵ	0	https://ws-pfs1.w	vs.its/firew	/all_rules.php?if=opt	2		(	⊴ ב	III\ 🗉	) 🕒	CFF V	1
ckDuckGo	🗎 Devices 📋	Links											
	SC Systen	n <del>v</del> Inter	rfaces 👻 🛛 Fire	ewall 👻	Services -	VPN 🗸 Status	← Diag	nostics 👻	Help 👻				C
													_
Firewa	all / Rules	/ LAN_1	10_CLIENT	S							₽l	<u>lıl</u> 🔳 (	0
Floating	DMZ_120	_EXTERN	LAN_100_SERV	'ER I	DMZ_130_INTERN	LAN_110_CLIE	NTS DI	MZ_140_G	AMEZONE DM2	Z_150_ISOI	ATION		
Dulas (				_				_				_	
Rules (I	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule Descriptio	n	۵	ctions	
] 👱	0 /318 KiB	IPv4 ICMP	*	*	*	*	*	none	TEST		5	£∥⊡	0
		any									T		
												-	
usnahme	en intern										ť	Ì	
usnahme	en intern 0 /613 KiB	IPv4 TCP	*	*	ServerIn_RDS	Ports_RDS	*	none	Zugriff au	IF RDS	t t	〕 ₽∕© 〕	0
xusnahme	en intern 0 /613 KiB 1 /32.39 MiB	IPv4 TCP IPv4 TCP	*	*	ServerIn_RDS ServerIn_AD	Ports_RDS Ports_AD_TCP	*	none	Zugriff au Services /	if RDS AD	t i	Ì ₽/© Ì ₽/©	0
usnahme	en intern 0 /613 KiB 1 /32.39 MiB 3 /56.02 MiB	IPv4 TCP IPv4 TCP IPv4 UDP	* * *	* * *	ServerIn_RDS ServerIn_AD ServerIn_AD	Ports_RDS Ports_AD_TCP Ports_AD_UDP	*	none none none	Zugriff au Services / Services /	IF RDS	t t	〕 ₺ / ि 〕 ₺ / ि ₺	0
usnahme	en intern 0 /613 KiB 1 /32.39 MiB 3 /56.02 MiB	IPv4 TCP IPv4 TCP IPv4 UDP	* * *	* * *	ServerIn_RDS ServerIn_AD ServerIn_AD	Ports_RDS Ports_AD_TCP Ports_AD_UDP Alias details	*	none none none	Zugriff au Services / Services /	if RDS AD AD	t t t	〕 ₺ / ि ₺ / ि 〕 ₺ / ि	0
usnahme	en intern 0 /613 KiB 1 /32.39 MiB 3 /56.02 MiB 0 /6 KiB	IPv4 TCP IPv4 TCP IPv4 UDP IPv4 TCP	* * *	* * * *	Serverin_RDS Serverin_AD Serverin_AD Serverin_HTTP	Ports_RDS Ports_AD_TCP Ports_AD_UDP Alias details Value 192 168 100 18	* * * Description WS-MON (P	none none none none	Zugriff au Services / Services / Services /	AD AD HTTP		〕 ₺ / © 〕 ₺ / © 〕 ₺ / © 〕	0 0 0
	en intern 0 /613 KiB 1 /32.39 MiB 3 /56.02 MiB 0 /6 KiB 0 /847.17 MiB	IPv4 TCP IPv4 TCP IPv4 UDP IPv4 TCP IPv4 TCP	* * * *	* * * * *	ServerIn_RDS ServerIn_AD ServerIn_AD ServerIn_HTTPS	Ports_RDS Ports_AD_TCP Ports_AD_UDP Alias details Value 192.168.100.7 192.168.100.7	* * Description WS-MON (P WS-RA1 (W WS-RA2 (W	none none none RTG) AP) AP)	Zugriff au Services / Services / Services   Services	AD AD HTTP HTTPS			0 0 0 0

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

**VS IT-Solutions** 

of WS-PFS1a.ws.its - Firewall: Ali	a: × +			-	
) → C ŵ	🛛 🔒 https://ws-pfs1.ws.its/firewall_aliases_edit.php?id	=84	⊠ ☆	III\ 🗉 🛯 💾	OFF 📫
DuckDuckGo 🗎 Devices 🗎 Link	5				
COMMUNITY EDITION	Interfaces <del>▼</del> Firewall <del>▼</del> Services <del>▼</del> V	PN ✔ Status ✔ Diagnost	ics 🕶 Help 🕶		•
Firewall / Aliases /	Edit				0
Properties					
Name	ServerIn_HTTPS	a-7 A-7 0-9 and "			
Description	Services mit HTTPS	a 2, A 2, V 3 and			
	A description may be entered here for administrative refer	ence (not parsed).			
Туре	Host(s)	~			
Host(s)					
Hint	Enter as many hosts as desired. Hosts must be specified re-resolved and updated. If multiple IPs are returned by a I as 192.168.1.16/28 may also be entered and a list of indiv	by their IP address or fully qualified NS query, all are used. An IP range idual IP addresses will be generate	domain name (FQDN). FQDI such as 192.168.1.1-192.16 d.	N hostnames are per i8.1.10 or a small sul	iodically bnet such
IP or FQDN	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:



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:





#### Das geht sehr einfach:



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



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:



C () () () () () () () () () () () () ()	tras 🕶 🔞 🗸 💭 🐘	- □ × ☆☆ <sup>(2)</sup>
	Domăne\Benutzername: Kennwort:	Image: Certifikat         Algemein Details         Zertifizierungspfad         Image: Sectigo         Zertifikat anzeigen         Zertifikat ist gultig.

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:

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

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

WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

🗾 WS-PF	S1a.ws.its - Status: Dashl: 🗙 🛛 😹 Zertifikate – Micro	soft Exchang × +					- 0
_) → C'		ws.its			🗵 🚖	III\ 🗉 🕕 💾	eff 👬
DuckDuckGo	Devices Links						
							~
	SC System - Interfaces - Fire	ewall 👻 Services 🕶	VPN - Stat	us 👻 Diagno:	stics ▼ Help ▼		
Status /	Dachboard						10
Status /	Dashboard						ŦŪ
			_	600		_	600
System In	nformation 🖉 🖯 😵	Traffic Graphs			HAProxy		~00
Name	WS-PFS1a.ws.its	DMZ_120_EXTE	Ralwan (in) 🛛 😑 wai	n (out)	Backend(s)/Server(s)	Constant	Chatan
lleor	admin@102.168.110.101.(Local				Socier(s)	Sessions (our/max)	Status
2361	Database)			600k	Client(s) addr.nort	age/id	/ Actions
						0 / 200	
Version	2.4.4-RELEASE-p3 (amd64)			400k	WS-RDS1	07200	ĕ
	built on Wed May 15 18:53:44 EDT 2019				MY invANV	28 / 200	
	FreeBSD 11.2-RELEASE-p10			2004	WS-MX1	20/200	ĕ
	The surface is an the latest constant			2006	102 168 110 101:51/2	7m1/ls / 0v80	24c5800
	Version information undeted at Sun Oct				102 168 110 101 5162	7m13s / 0x80	2400000
	27 11:36:10 CET 2010			0.0	192.168.110.101:5172	7m13s / 0x80	24d6400
	27 11.00.10 021 2017	02:55	06:40	08:55	192.168.110.101:5284	6m35s / 0x80	24d4800
ernel PTI	Disabled	LAN 100 SERV	ER 🔵 Ian (in) 🛛 🔴 Iai	n (out)	192.168.110.101:24213	2m7s / 0x802	4d7000
Intime	21 Days 20 Hours 07 Minutes 00			N 20k	109.41.193.103:30690	1m28s / 0x80	24d4400
punc	Seconds				109.41.193.103:30730	1m27s / 0x80	24d6c00
				15k	109.41.193.103:31327 i	1m24s / 0x80	24d4000
urrent	Sun Oct 27 12:08:54 CET 2019			10k	192.168.110.101:24242	1m22s / 0x80	259b000
ate/time					109.41.193.103:29053	1m18s / 0x80	2526400
ast config	Sun Oct 27 12:00:01 CET 2019			5.0K	109.41.193.103:15675	1m2s / 0x802	526000
hange				0.0	109.41.193.103:6345	23s / 0x8024	31800
tata tabla				5.0%	109.41.193.103:30579	7s / 0x8024d	5c00
izo	0% (1473/507000) Show states			-5.0K	192.168.110.101:24255	/s / 0x8024c	0000
120		02:55	06:40	08:55	WS-MX2	14	0506-00
PU usage					1/2.19.130.105:40820	9m10s / 0xou	2320000
	3%	DMZ_130_INTE	R 🎽 opt1 (in) 🛛 🛑 opt	1 (out)	192.100.110.101.5104	7m13s / 0x80	2405000
<b>Nemory</b>				0.0	192.100.110.101:5170	7m12s / 0x80	240000
isage	78% of 5071 MiB				192 168 110 101-24212	2m7s / 0x802	4c5c00
)isk usane:				-200k	192.168.110.101:24214	2m7s / 0x802	4d3400
/					109.41.193.103:11285	1m29s / 0x80	2431000
	16% of 45GiB - ufs			-400k	109.41.193.103:8699	1m28s / 0x80	259b400
					109 41 193 103 21777	1m26s / 0x80	24d5000

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:

Semotezugriffs-Verwaltungskonsole						
👫 Konfiguration VPN	VERÖFFENTLICHTE V     Alle veröffentlichten Web	VEBANWENDUNGEN anwendungen   3 insgesamt				
Webanwendungsproxy	Filter	م				
Dashboard						
W Vorgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung		
💻 Remoteclientstatus	Monitor	https://monitor.ws-its.de/	https://prtg.ws.its/	PassThrough		
Berichterstellung	MX	https://email.ws-its.de/	https://email.ws.its/	PassThrough		
	RDS	https://rds.ws-its.de/	https://rds.ws-its.de/	PassThrough		
<ul> <li>Clustesever</li> <li>WS-RA1</li> <li>WS-RA2</li> </ul>	C:\>nslookup n Server: WS-DC Address: 192. Name: rds.v Address: 192. C:\>_	erung rds.ws-its.de 1.ws.its 168.100.1 vs-its.de 168.110.21				

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:

🛃 WS-PFS1a.ws.its - Services: HAF 🗙	: +				-
$\rightarrow$ C' $\textcircled{0}$	https://ws-pfs1.ws.its/hapro	pxy/haproxy_pools.php		··· 🗵 🏠	III\ 🗊 💿 💾 <mark>977</mark> 👬
uckDuckGo 🗎 Devices 🗎 Links					
	Interfaces 👻 Firewall 👻	Services - VPN		Diagnostics 👻 Help 👻	<b>C</b>
Services / HAProxy	/ Backend				C⊚ 幸 Ш 🗏 0
Settings Frontend B Backends Advanced	Sackend Files Stats	Stats FS Temple	tes Check	Frontend	Actions
Settings Frontend E Backends Advanced	Backend Files Stats Name SMTP	Stats FS Templa	tes Check SMTP	Frontend SMTP-Proxy	Actions
Settings Frontend E Backends Advanced	Backend Files Stats Name SMTP HTTPS	Stats FS Templa Servers 2 2	tes Check SMTP Basic	Frontend SMTP-Proxy HTTPS-Proxy	Actions          Image: Constraint of the second s
Settings Frontend E Backends Advanced	Sackend Files Stats Name SMTP HTTPS RDSWEB	Stats FS Temple Servers 2 2 1	tes Check SMTP Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy	Actions Act
Settings Frontend E Backends Advanced	Sackend Files Stats Name SMTP HTTPS RDSWEB MX	Stats FS Templa Servers 2 2 1 2 2	tes Check SMTP Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions Action

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

WS IT-Solutions

	System -	- Interf	faces 🔻	Firewall 🗸	Services -	VPN 👻	Status <del>-</del>	Diagnostic	s → Help →		l
Services	/ HAPro	xy / Ba	ckend	/ Edit						Ce	) 🗄 🔟 🚍 🔞
Settings	Frontend	Backend	File	s Stats	Stats FS	Templates					
Edit HAPr	oxy Backen	d server j	pool								
	Name	RDS									
	Server list	Table									
			Mode	Name	Forwardto	Address		Port Encryp	t(SSL) SSL	checks Weight	Actions
		□₺	active	WS-RDS2	Address+Port:	<mark>192.168.</mark>	110.21	443 no	no		e 🖉 🖉 🖉
		Ð	)								
		Field expl	anations:	6							
Loadbalar	ncing option	ıs (when	multiple	servers a	e defined)						e
	Balance	Non	e		,						
		This allow	s writing y	our own custo	om balance setting	js into the adva	nced section	. Or when you h	nave no need for l	palancing with only i	l server.
Health che	ecking										
Health ch	eck method	Basic					~				
		Basic so	cket conn	ection check							
		Dabie So	CACO COIII	ccoron check							

## WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

🚮 WS-PFS1a.ws.its - Services: HAF 🗙 🚽	+				- 0
→ C û	https://ws-pfs1.ws.its/hapro	oxy/haproxy_pools.php		⊠ ☆	III\ 🗊 🚯 💾 <mark>07</mark> i
ckDuckGo 🛅 Devices 🛅 Links					
Sense System - Ir	nterfaces 👻 Firewall 👻	Services - VPN	I <del>-</del> Status -	Diagnostics 👻 Help 👻	G
Services / HAProxy / I	Backend				С⊚ ≆ Ш 🗏 0
The haproxy configuration has been You must apply the changes in orde	changed. r for them to take effect.				Apply Changes
The haproxy configuration has been You must apply the changes in order Settings Frontend Back	changed. r for them to take effect. end Files Stats	Stats FS Templ	ates		Apply changes
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends	changed. r for them to take effect. end Files Stats	Stats FS Templ	ates		Apply Changes
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends Advanced	changed. r for them to take effect. end Files Stats Name	Stats FS Templ	ates Check	Frontend	Apply Changes
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends Advanced	changed. r for them to take effect. end Files Stats Name SMTP	Stats FS Templ	ates Check SMTP	<b>Frontend</b> SMTP-Proxy	Apply Changes
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends Advanced	changed. r for them to take effect. end Files Stats Name SMTP HTTPS	Stats FS Templ Servers 2 2 2	ates Check SMTP Basic	Frontend SMTP-Proxy HTTPS-Proxy	Actions
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends Advanced	r for them to take effect. end Files Stats Name SMTP HTTPS RDSWEB	Stats FS Templ Servers 2 2 1	ates Check SMTP Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy	Actions
The haproxy configuration has been You must apply the changes in order Settings Frontend Back Backends Advanced	r for them to take effect.  end Files Stats  Name  SMTP  HTTPS  RDSWEB  MX	Stats FS Templ Servers 2 2 1 2	ates Check SMTP Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions

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

0 WS-PFS1a.ws.its - Services: H	AF× +					- 0
← → C <sup>u</sup> ŵ <sup>(3)</sup> DuckDuckGo 🗎 Devices 🗎 Link	■ https://ws-pfs1.ws.its/hapro	xy/haproxy_listeners_edit.ph	np?id=HTTPS-Pr	… ⊠ ☆	\ 🗊 🖪	) 🖺 👎 👬
COMMUNITY EDITION	Interfaces 🗸 🛛 Firewall 🗸	Services - VPN -	Status 👻 Diagr	nostics <del>-</del> Help <del>-</del>		•
Services / HAProx	xy / Frontend / Edit				Co :	E 🔟 🔲 😧
Settings Frontend	Backend Files Stats	Stats FS Templates				
Edit HAProxy Frontend	ł					
Name	HTTPS-Proxy					
Description						
Status	Active		~			
Shared Frontend	☐ This can be used to host a second Use this setting to configure multiple All settings of which only 1 can exist The frontend settings will be merged	l or more website on the sar backends/accesslists for a will be hidden. into 1 set of frontend config	ne IP:Port combination. single frontend. juration.			
External address	Define what ip:port combinations to li	sten on for incomming con	nections.			
	Table					
	Listen address	Custom address	Port	SSL Offloading	Advanced	Actio
	Use custom address:	× 172.19.120.120	443			<b>m</b> (
	1					
	NOTE: You must add a firewall rules p If you want this rule to apply to anoth addresses on the first). Also note that specify multiple ports, separate them	ermitting access to the liste er IP address than the IP ad t if you are trying to redirect with a comma (,). EXAMPL	en ports above. dress of the interface ch connections on the LAN E: 80,8000 Or to listen of	osen above, select it here select the "any" option. I both 80 and 443 create	e (you need to define ' n the port to listen to, 2 rows in the table wl	Virtual IP if you want to here for the 443



Туре	ssl / https(TCP mode)	~				
	This defines the processing t	ype of HAProxy, and will determine the availabe options for acl ch	hecks a	nd als	so several other options.	
	Flease note that for https en	cryption/decryption on HAProxy with a certificate the processing	type ne	eus t	o be set to http.	
efault backend, acc	ess control lists and act	tions				
Access Control lists	Use these to define criteria th	nat will be used with actions defined below to perform them only v	when ce	ertain	conditions are met.	
	Table		Willen et	, can	conditions are met.	
	Name	Expression	CS	Not	Value	Actions
	□ 📩 RDSWEB	Server Name Indication TLS extension matches:	no	no	rdsweb.ws-its.de	e 🖉 🖉
	Ð					
	□ 🚠 MX	Server Name Indication TLS extension matches:	no	no	email.ws-its.de	e 🖉 🛍 🔽
	÷					
		Server Name Indication TLS extension matches:	~		rds.ws-its.de	<b>₫</b> [] <b>↑</b> \
	KD3					
	1					
	- 'CS' makes the string match	es 'Case Sensitive' so www.domain.tld wil not be the same as WV	WW.don	nain.1	٢LD	

#### Die neue ACL leitet dann auf das neue Backend:

	Backend1acl Host matches www.yourdon addHeaderAclSSL Client certificate valid	nain.tld		
	acl's with the same name will be 'combined' using OR criteria For more information about ACL's please see HAProxy Docur	ı. mentation Section 7 - Using	g ACL's	
	NOTE Important change in behaviour, since package versior -acl's are no longer combined with logical AND operators, list -acl's alone no longer implicitly generate use_backend config	<b>10.32</b> t multiple acl's below where uration. Add 'actions' below	e needed. w to accomplish this behaviour.	
Actions	Use these to select the backend to use or perform other action Table	ons like calling a lua script,	blocking certain requests or others av	ailable.
	Action	Parameters	Condition acl names	Actions
	Use Backend	See below	RDSWEB	e 🖉 🛍 🗋
	🖶 backend: RDSWEB			
	Use Backend	See below	МХ	e 🖉 🛍 🗋
	🖶 backend: MX			
	Use Backend ~	See below	RDS	₫⊡≁↓
	backend: RDS 🗸			

### Ein Apply später ist die Anwendung bereit:

MS-PFS	1a.ws.its - Servio	ces: HAF	× +							- 0	
) ) → C' 1	۵		🛛 🔒 http:	s://ws-pfs1. <b>ws.its</b> /hapro	oxy/haproxy_lister	ners.php	··· ⊠ ੯	ז ווו	🗈 🕑 🚦	e off	ľ
DuckDuckGo	🗎 Devices 🗎	Links									
	SC Syst	tem 👻	Interface	es ▼ Firewall <del>▼</del>	Services <del>-</del>	VPN 👻 Status 👻	Diagnostics 👻	Help 🗸		e	•
Servic	es / HAI	Proxy	/ Front	end					C® ≇	<u>III</u> 🔲 🕢	
The hapro You must	oxy configurat apply the cha	tion has anges ir	been change order for the	ed. em to take effect.					🗸 Appl	y Changes	
Settings	Fronten	nd	Backend	Files Stats	Stats FS	Templates					
Fronten	ıds										
Primary	Shared	On	Advanced	Name	Description	Address	Туре	Backend	A	ctions	1
□.₺		~	X;	HTTPS-Proxy		172.19.120.120:443	ssl/https	RDSWEB if(RDSWE MX if(MX) RDS if(RDS) HTTPS (default)	B)	<b>₽</b> ₩.	1
□ᡱ		×		SMTP-Proxy		172.19.120.120:25	tcp	SMTP (default)		<b>/ 🛍 </b>	נ
								1 /	Add <u> Î</u> Dele	te 💾 Save	



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

🛔 DNS-Manager				
Datei Aktion Ansicht ?				
🔶 🌩 🖉 📰 🖾 😖 🛛 🖬 📋 🛱	1			
<ul> <li>DNS</li> <li>WS-DC1</li> <li>Zwischengespeicherte Lookupvorgänge</li> <li>Forward-Lookupzonen</li> <li>Imsdcs.ws.its</li> <li>Imsdcs.ws.its</li> <li>Imsdrs.ws.its.de</li> <li>Inds.ws-its.de</li> <li>Inds.ws-its.de</li> <li>Inds.ws-its.de</li> <li>Inds.ws.its</li> <li>Inds.ws.its.de</li> <li>Inds.ws.its.de</li> <li>Imsdrs.ws.its.de</li> <li>Imsdrs.ws.its.d</li></ul>	Name (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne (identisch mit übergeordne	Typ Autoritätsursprung (SOA) Namenserver (NS) Namenserver (NS) Host (A)	Daten [3], ws-dc1.ws.its., hostma ws-dc1.ws.its. ws-dc2.ws.its. ws-dc3.ws.its. 192.168.110.16	Zeitstempel Static Static Static Static Static

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:

WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

					- 0
→ C' û 🛛 🗎	https://ws-pfs1. <b>ws.its</b> /hapr	oxy/haproxy_pools.php		… 🖂 ☆	III\ 🗉 💿 💾 👎 👬
ickDuckGo 🗎 Devices 🗎 Links					
SENSE System - Int	erfaces 🔻 🛛 Firewall 🔫	Services - VPN	I <del>▼</del> Status <del>▼</del>	Diagnostics 👻 Help 👻	•
Services / HAProxy / B	ackend				С⊚ 幸 Ш 🗏 0
Settings Frontend Backe	nd Files Stats	Stats FS Templ	ates		
Jettings Frontend Ducito	nu meo etato	otato i o i o inpi	ateo		
Backends					
Backends Advanced	Name	Servers	Check	Frontend	Actions
Backends Advanced	Name SMTP	Servers 2	Check SMTP	Frontend SMTP-Proxy	Actions
Backends Advanced	Name SMTP HTTPS	Servers 2 2	Check SMTP Basic	Frontend SMTP-Proxy HTTPS-Proxy	Actions
Advanced	Name SMTP HTTPS RDSWEB	Servers 2 2 1	Check SMTP Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy	Actions
Advanced	Name SMTP HTTPS RDSWEB MX	Servers 2 2 1 2	Check SMTP Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions
Advanced	Name SMTP HTTPS RDSWEB MX RDS	Servers 2 2 1 2 1 2 1	Check SMTP Basic Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions

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

	System <del>-</del>	Interf	aces 🔻	Firewall 👻	Services -	VPN 🗸	Status 🕶	Diagnostics 👻	Help 🗸		•
Services	HAProx	y/Bao	ckend /	Edit						Co	± III ■ 6
Settings	Frontend	Backend	Files	Stats	Stats FS	Templates					
Edit HAProx	xy Backend	server p	ool					_			
	Name	PRTG									
	Server list	Table									
			Mode	Name	Forwardto	Address	ſ	Port Encrypt(SS	SL) SSL checks	Weight	Actions
		□₺	active	WS-MON	Address+Port:	192.168.1	00.18	<mark>443</mark> no	no		e 🖉 🛍 🗋
		I									
		Field expla	inations:	0							
Loadbalanc	ing options	when r	nultinle	servers a	re defined)						8
Loudbulune					le definied)						
	Balance	None     This allow:	e s writing vo	our own custo	om balance setting	us into the advar	nced section.	Or when you have	no need for balancin	a with only 1	server.
						, 					
Health chec	king										
Health chec	k method	Basic					×				
		Basic so	ket conne	ction check							
		·									

Ein Apply später ist das Backend einsatzbereit:

## WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

of WS-PFS1a.ws.its - Services: HA	F× +				
→ Cª 🏠 .ckDuckGo 🗎 Devices 🗎 Links		roxy/haproxy_pools.php		⊌ ☆	III\ 🗉 💿 🗎 👎 👬
Sense System -	Interfaces <del>→</del> Firewall <del>→</del>	Services - VPN		Diagnostics 👻 Help 👻	e
Services / HAProx	ky / Backend				C⊚ ≑ Ш 🗏 0
The haproxy configuration ha You must apply the changes	as been changed. in order for them to take effect.				✔ Apply Changes
Settings Frontend	Backend Files Stats	Stats FS Templa	ates		
Settings Frontend Backends Advanced	Backend Files Stats	Stats FS Templa Servers	ates Check	Frontend	Actions
Settings Frontend Backends Advanced	Backend Files Stats Name SMTP	Stats FS Temple Servers 2	ates Check SMTP	Frontend SMTP-Proxy	Actions
Settings Frontend Backends Advanced	Backend Files Stats Name SMTP HTTPS	Stats FS Templa Servers 2 2	ates Check SMTP Basic	Frontend SMTP-Proxy HTTPS-Proxy	Actions I to Consultation of
Settings Frontend Backends Advanced	Backend Files Stats Name SMTP HTTPS RDSWEB	Stats FS Temple Servers 2 2 1	ates Check SMTP Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy	Actions
Settings Frontend Backends Advanced	Backend Files Stats Files Stats Name SMTP HTTPS RDSWEB MX	Stats FS Temple Servers 2 2 1 2 2	ates Check SMTP Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions Act
Settings Frontend Backends Advanced	Backend Files Stats Files Stats Name Name Name NTP RDSWEB MX RDS	Stats FS Templa Servers 2 2 1 1 2 1 1	Check SMTP Basic Basic Basic Basic	Frontend SMTP-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy HTTPS-Proxy	Actions

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

of WS-PFS1a.ws.its - Services: H	IAF × +							
← → ♂ ☆	🛛 🔒 https://ws-pfs1.ws.its/haproxy,	/haproxy_listeners_edit.php?i	d=HTTPS-Pri 🗏 🚥 🗵	7 ☆	III\ 🗊	🗈 💾 😲	<sup>6</sup> 17	Ξ
🜔 DuckDuckGo 🗎 Devices 🗎 Linl	ks							
COMMUNITY EDITION	Interfaces 🗸 Firewall 🕇 S	Services - VPN -	Status - Diagnostics -	Help 🗕			۵	
Services / HAProx	xy / Frontend / Edit				Co	≆ 🔟 🗖	0	
Settings Frontend	Backend Files Stats S	Stats FS Templates						
Edit HAProxy Frontend	ł							÷
Name	HTTPS-Proxy							
Description								
Status	Active		~					
Shared Frontend	☐ This can be used to host a second or Use this setting to configure multiple ba All settings of which only 1 can exist wil The frontend settings will be merged int	r more website on the same ckends/accesslists for a sin l be hidden. o 1 set of frontend configura	IP:Port combination. gle frontend. tion.					
External address	Define what ip:port combinations to liste	en on for incomming connec	tions.					
	Table Listen address	Custom address	Port	SSL Offloading	Advanced	,	Actio	
	Use custom address: ~	172.19.120.120	443				<b>m</b> (	
	1 1 1						>	
	NOTE: You must add a firewall rules perr If you want this rule to apply to another I addresses on the first). Also note that if specify multiple ports, separate them wi you would likely want to check the SSL-c	mitting access to the listen p P address than the IP addre you are trying to redirect cor th a comma (,). EXAMPLE: 8 offloading checkbox.	orts above. ss of the interface chosen abov nections on the LAN select the 0,8000 Or to listen on both 80 a	e, select it here any" option. In and 443 create	e (you need to defir n the port to listen 2 rows in the table	ne <b>Virtual IP</b> to, if you wan where for the	t to 2 443	



Туре	ool / https(TCP mode)	~		
-	This defines the processing f	type of HAProxy, and will determine the availabe options for ac	ol checks and also several other options.	
	Please note that for https en	cryption/decryption on HAProxy with a certificate the processi	sing type needs to be set to "http".	
ofault backend, aco	case control lists and ac	tions		
Access Control lists	Use these to define criteria tr	nat will be used with actions defined below to perform them or	nly when certain conditions are met.	
			co. u e velue	Antione
	Name	Expression	CS Not Value	Actions
	C t RDSWEB	Server Name Indication 1LS extension matches:	no no rdsweb.ws-its.ae	or ш ч
		Constitution TLC extension matches	meil we ite de	<b>*</b> m [
	□ ♣ MX	Server Name Indication 1LS extension matches.	no no email.ws-its.ue	or ш ч
		2	te un ite do	<b>≈</b> m̂ [
	L t. RDS	Server Name Indication 1LS extension matches.	no no rds.ws-its.ae	<i>₽</i> ш ч
		Contraction TLS extension matches		
		Server Name Indication 1L5 extension matches.	LI LI [monitor.ws-its.ae]	W4*** •
	1			
	- 'CS' makes the string match	nes 'Case Sensitive' so www.domain.tld wil not be the same as	s WWW.domain.TLD	
	- 'Not' makes the match if the	e value given is not matched		
	Example:			
	Name Expression	CINotValue		
	Backend1acl Host matches	www.wourdomain.tld		
	Line Lange Client out			
	addHeaderAclSSL Client cer	tificate valid		
	addHeaderAclSSL Client cer	I be 'combined' using OR criteria.		
	addHeaderAclSSL Client cer acl's with the same name wil For more information about A	I be 'combined' using OR criteria. ACL's please see HAProxy Documentation Section 7 - Using AC	CL's	
	addHeaderAclSSL Client cer acl's with the same name wil For more information about /	The 'combined' using OR criteria. ACL's please see HAProxy Documentation Section 7 - Using AC	CĽs	
	addHeaderAcCSSL Client cer acl's with the same name wil For more information about / NOTE Important change in bo	If the 'combined' using OR criteria.  ACL's please see HAProxy Documentation Section 7 - Using AC  ehaviour, since package version 0.32	CĽs	
	addHeaderAcCSSL Client cer acl's with the same name wil For more information about <i>i</i> <b>NOTE Important change in b</b> -acl's are no longer combinec -acl's alone no longer implicit	www.yourdonnain.tod           tifficate valid           II be 'combined' using OR criteria.           ACL's please see HAProxy Documentation Section 7 - Using AC           ehaviour, since package version 0.32           1 with logical AND operators, list multiple acl's below where ne           ily generate use_backend configuration. Add 'actions' below to	CL's зeded. ว accomplish this behaviour.	
	addHeaderAclSSL Client cer acl's with the same name wil For more information about <i>i</i> <b>NOTE Important change in b</b> -acl's are no longer combiner -acl's alone no longer implicit	Il be 'combined' using OR criteria.     ACL's please see HAProxy Documentation Section 7 - Using AC     ehaviour, since package version 0.32     d with logical AND operators, list multiple acl's below where ne     thy generate use_backend configuration. Add 'actions' below to	CL's eeded. 5 accomplish this behaviour.	
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about , <b>NOTE Important change in b</b> -acl's are no longer combinee -acl's alone no longer implicit Use these to select the backet	If the analysis of the actions like calling a lua script, bloc	CL's seded. o accomplish this behaviour. 	le
Actions	addHeaderAc(SSL Client cer acl's with the same name wil For more information about . NOTE Important change in b -acl's are no longer combinec -acl's alone no longer implicit Use these to select the backor Table	If the analysis of the actions of the action of the a	CL's seded. o accomplish this behaviour. 	le.
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about . <b>NOTE Important change in b</b> -acl's are no longer combiner -acl's alone no longer implicit Use these to select the back Table Action	Il be 'combined' using OR criteria. ACL'a please see HAProxy Documentation Section 7 - Using AC whaviour, since package version 0.32 d with logical AND operators, list multiple acl's below where ne tly generate use_backend configuration. Add 'actions' below to end to use or perform other actions like calling a lua script, blo Parameters	CL's eeded. o accomplish this behaviour. ocking certain requests or others availabl <b>Condition acl names</b>	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about . NOTE Important change in b -acl's are no longer combined -acl's alone no longer implicit Use these to select the back Table Action	If in the second s	CL's eeded. o accomplish this behaviour. coking certain requests or others availabl Condition acl names RDSWEB	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about . NOTE Important change in b -acl's are no longer combined -acl's alone no longer implicit Use these to select the back Table Action : Use Backend : backend: RDSW	ACL's please see HAProxy Documentation Section 7 - Using AC with Joint Control of the section 2 - Using AC with logical AND operators, list multiple acl's below where nee thy generate use_backend configuration. Add 'actions' below to be and to use or perform other actions like calling a lua script, blo     Parameters     See below EB	CL's eeded. o accomplish this behaviour. coking certain requests or others availabl Condition acl names RDSWEB	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about . NOTE Important change in b -acl's are no longer combined -acl's alone no longer combined -acl's alone no longer implicit Use these to select the backet Table Action : Use Backend : backend: RDSW	If in the second s	CL's eeded. o accomplish this behaviour. coking certain requests or others availabl Condition acl names RDSWEB	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about. NOTE Important change in b -acl's are no longer combined -acl's alone no longer combined -acl's alone no longer implicit Use these to select the backer Table Action Backend: RDSW	inficiate valid     inficiate valid       II be 'combined' using OR criteria.       ACL's please see HAProxy Documentation Section 7 - Using AC       wehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       ty generate use_backend configuration. Add 'actions' below to       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below	CL's eeded. o accomplish this behaviour. ocking certain requests or others availabl Condition acl names RDSWEB MX	le. Actions ک ش (ر
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about. NOTE Important change in b -acl's are no longer combinet -acl's alone no longer combinet -acl's alone no longer implicit Use these to select the back Table Action	If in the set of	CL's eeded. o accomplish this behaviour. cking certain requests or others available Condition acl names RDSWEB MX	le. Actions I I I I I I I I I I I I I I I I I I I
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about. NOTE Important change in b -acl's are no longer combine -acl's alone no longer implicit Use these to select the back Table Action	Il be 'combined' using OR criteria.           ACL's please see HAProxy Documentation Section 7 - Using AC           why Galderman           why Object	CL's eeded. o accomplish this behaviour. bcking certain requests or others available Condition acl names RDSWEB MX RDS	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wil For more information about. NOTE Important change in b -acl's are no longer combine -acl's alone no longer implicit Use these to select the back Table Action	Il be 'combined' using OR criteria.       ACL'a please see HAProxy Documentation Section 7 - Using AC       rehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       thy generate use_backend configuration. Add 'actions' below to       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       See below	CL's eeded. o accomplish this behaviour. condition acl names RDSWEB MX RDS	le. Actions I to C I to
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about. NOTE Important change in b -acl's are no longer combine -acl's alone no longer implici Use these to select the back Table Action	Il be 'combined' using OR criteria.       ACL'a please see HAProxy Documentation Section 7 - Using AC       rehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       type generate use_backend configuration. Add 'actions' below to       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       EB       See below       See below	CL's eeded. o accomplish this behaviour. condition acl names RDSWEB MX RDS PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about. NOTE Important change in b -acl's are no longer combine -acl's alone no longer implici Use these to select the back Table Action	Il be 'combined' using QR criteria.       ACL'a please see HAProxy Documentation Section 7 - Using AC       rehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       ty generate use_backend configuration. Add 'actions' below to       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       'EB       See below       See below	CL's eeded. o accomplish this behaviour.  cocking certain requests or others availabl Condition acl names RDSWEB MX RDSWEB RDS PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi. For more information about. NOTE Important change in b -acl's are no longer combiner -acl's alone no longer implici Use these to select the back Table Action	Il be 'combined' using QR criteria.       ACL'a please see HAProxy Documentation Section 7 - Using AC       rehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       tygenerate use_backend configuration. Add 'actions' below to       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       'EB       See below             See below	CL's eeded. o accomplish this behaviour.  condition acl names RDSWEB MX RDSWEB RDS PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about. NOTE Important change in b -acl's are no longer combine -acl's alone no longer implici Use these to select the back Table Action Action Deckend: RDSW Deckend: RDSW Deckend: RDS Deckend: RDS Deckend: RDS Deckend: RDS Deckend: RDS Deckend: PRTG Fxample:	Image: Second	CL's eeded. o accomplish this behaviour. condition acl names RDSWEB MX RDS PRTG PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about . NOTE Important change in b -acl's are no longer combine -acl's alone no longer implici Use these to select the back Table Action	inficiate valid     inficiate valid       II be 'combined' using OR criteria.       ACL's please see HAProxy Documentation Section 7 - Using AC       wehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       'EB       See below       'See below       'See below       'See below       'See below	CL's eeded. o accomplish this behaviour.  condition acl names RDSWEB MX RDS PRTG PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about. NOTE Important change in b -acl's are no longer combiner -acl's alone no longer combiner -acl's alone no longer combiner -acl's alone no longer implici Use these to select the back Table Action	inficiate valid     inficiate valid       II be 'combined' using OR criteria.       ACL's please see HAProxy Documentation Section 7 - Using AC       wehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       end to use or perform other actions like calling a lua script, blo       Parameters       EB       See below       'EB       See below       'See below       'actions' See below       'actions' See below       'actions' See below       'actions' See below	CL's eeded. o accomplish this behaviour.  cocking certain requests or others availabl Condition acl names RDSWEB MX RDS RDS PRTG	le. Actions
Actions	addHeaderAclSSL Client cer acl's with the same name wi For more information about. NOTE Important change in b -acl's are no longer combiner -acl's alone no longer combiner -acl's alone no longer implici Use these to select the back Table Action Backend: RDSW Backend: MX Backend: MX Backend: RDS Backend: PRTG Backend: PRTG Example: Action Para Use Backend Webs	inficiate valid     inficiate valid       Il be 'combined' using OR criteria.       ACL's please see HAProxy Documentation Section 7 - Using AC       wehaviour, since package version 0.32       d with logical AND operators, list multiple acl's below where ne       end to use or perform other actions like calling a lua script, blo       Parameters       end to use or perform other actions like calling a lua script, blo       Parameters       See below       'EB       See below       See below	CL's eeded. o accomplish this behaviour.  cocking certain requests or others availabl Condition acl names RDSWEB MX RDS RDS PRTG PRTG	le. Actions

Ein finales Apply später ist auch diese Anwendung umgestellt:

💋 WS-PFS1a	a.ws.its - Services	HAFX +											
→ C' û	) Devices 🗀 !	U A ht	tps://ws-pfs1. <b>ws.</b> i	its/haproxy/	/haproxy_liste	ners.php		··· @	) ☆	lii\	E 🚯		OFF 1
	C System	n <del>-</del> Interfa	ices <del>-</del> Firev	wall <del>-</del>	Services -	VPN <del>-</del>	Status 🕶	Diagnostics 🗸	Help 🗸				C
Service	es / HAPi	roxy / Fro	ntend								C® ≣	e lad I	• •
The haprox	xy configuratio	n has been cha	nged.								✓ A	pply Ch	anges
You must a	apply the chan	ges in order for	them to take effe	ect.									
You must a Settings	apply the chan Frontend	ges in order for Backend	Files	stats	Stats FS	Templates							
You must a Settings Frontend	Frontend	ges in order for Backend	Files	Stats	Stats FS	Templates							
You must a Settings Frontend Primary	Frontend	ges in order for Backend )n Advance	Files S	Stats	Stats FS Description	Templates Address		Туре	Backend			Actio	ns
Settings Frontend Primary	Frontend ds Shared C	Backend Din Advance	Files -	Stats	Stats FS Description	Templates Address 172.19.120	0.120:443	<b>Type</b> ssl/http	Backend B RDSWEE MX if(M) RDS if(R PRTG if( HTTPS (	B if(RDSWEE X) DS) PRTG) default)	3)	Actio	ns 🖋 🏛 🗍

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:

WS-PFS1a.ws.its - Services: HAF >	K 🕥 Willkommen   PRTG (WS-MON) X	+			-		×
$\leftarrow \rightarrow$ C $\textcircled{a}$	🛛 🔒 https://prtg. <b>ws.its</b> /index.htm		▣ ••• 🖂 📩	III\ 🗊 🔒		V	1 ≣
🗿 DuckDuckGo  Devices 🗎 Links							
PRTG (WS-MON)	)		PRTG O NETWORK MONITOR				
Anmeldename			Paessler Blog				
Kennwort			How to Use the New WMI Batt Is your PRTG installation already up to date? If case, you won't be able to enjoy the new WM with the 19.3.52 release.	tery Sensor of PR not, that's a bummer, becau Il Battery sensor that we in	FG use in this ntroduced		
		Anmeldung	Monitoring a Terrarium With P This is Merlin, a 6-year-old corn snake. He Switzerland, where he's taken care of by Patrick corn snakes are relatively easy to care for (ma	RTG lives in a terrarium in a c and his wife. Generally, ev Iking them ideal pet snake	home in en though s), Patrick		
<ul> <li>Client-Apps herunterladen (optic</li> <li>Kennwort vergessen?</li> <li>Benötig</li> </ul>	onal, für Windows, macOS, iOS, Android) gen Sie Hilfe?		A Tesla Potentially Equals a CC We already had a hunch that CCTV in the cities social distress among citizens, and this them people. However, in this discussion, which is a	CTV System on 4 of tomorrow could be used te triggers the primal feare also a recurring theme in th	Whe to cause of many te context		

#### **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:



2 📰 👔 🖬							
per-V-Manager WS-HV1	Virtuelle Computer						
WS-HV3	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
	WS-CA1	Wird ausgeführt	0 %	786 MB	2.18:20:34		8.0
	WS-CM	Wird ausgeführt	0 %	4096 MB	11.07:42:55		8.0
	WS-DC2	Wird ausgeführt	0 %	3610 MB	2.18:22:57		8.0
	🗑 WS-DPM	Wird ausgeführt	0 %	3332 MB	3.08:15:55		9.0
	WS-EVIL1	Gespeichert					8.0
	WS-FS2	Wird ausgeführt	0 %	2030 MB	21.21:00:35		8.0
	WS-MON	Wird ausgeführt	0 %	1414 MB	01:39:05		8.0
	WS-MX2	Wird ausgeführt	15 %	14336 MB	10.10:32:37	Wird heruntergefahren	8.0
	WS-PFS1b	Wird ausgeführt	0 %	5120 MB	21.21:01:07		8.0
	WS-RA2	Wird ausgeführt	0 %	1302 MB	2.18:19:10		8.0
	WS-RDS2	Wird ausgeführt	0 %	1916 MB	2.18:19:25		8.0
	WS-WAC	Wird ausgeführt	0 %	982 MB	6.20:59:43		9.0

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

tivit	it												
D	SMTP-Adresse	Anzeigen	Proxyserver	Servername	Status	Protokoll	Authn	Versc	RPC-Port	Тур	Anfr/Fehler	Reaktio	Bearb (Ø)
	Stephan.Walther@			https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	6/0	20	5
	Stephan.Walther@	Onlinearc		https://email.ws-its.de/ma	wird hergestellt	HTTP	Nego*	SSL		Exchan			
	Stephan.Walther@	Stephan		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	171/0	15	4
	stephan@jungbrun	Onlinearc		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	65/1		
	stephan@jungbrun	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	48/1		
	stephan@widwal.de	stephan@		https://email.ws-its.de/ma	wird hergestellt	HTTP	Nego*	SSL		Exchan			
	Stephan.Walther@	Stephan		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	1680/0	18	4
	stephan@jungbrun	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	68/1		
	stephan@widwal.de	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	32/1		
	stephan@jungbrun	Öffentlich		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Öffentli	8/0	25	11
	Stephan.Walther@	Öffentlich		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Öffentli	54/0	14	3
	stephan@widwal.de	Öffentlich		https://email.ws-its.de/ma	wird hergestellt	HTTP	Nego*	SSL		Öffentli			
	Stephan.Walther@	Technik		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	45/0	12	4
5	Stephan.Walther@	nicole@w		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	18/1		
8	Stephan.Walther@	Sabine@j		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	18/1		
1	Stephan.Walther@	Technik		https://email.ws-its.de/ma	wird hergestellt	HTTP	Nego*	SSL		Exchan			

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:



mein	Lokales Postfach												
tivit	at												
/ID	SMTP-Adresse	Anzeigen	Proxyserver	Servername	Status	Protokoll	Authn	Versc	RPC-Port	Тур	Anfr/Fehler	Reaktio	Bearb (Ø)
2	Stephan.Walther@			https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	6/0	20	5
1	Stephan.Walther@	Onlinearc		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	92/1		
4	Stephan.Walther@	Stephan		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	171/0	15	4
6	stephan@jungbrun	Onlinearc		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	65/1		
0	stephan@jungbrun	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	48/1		
2	stephan@widwal.de	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	52/1		
5	Stephan.Walther@	Stephan		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	1680/0	18	4
8	stephan@jungbrun	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	68/1		
2	stephan@widwal.de	stephan@		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	41/2		
6	stephan@jungbrun	Öffentlich		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Öffentli	8/0	25	11
4	Stephan.Walther@	Öffentlich		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Öffentli	58/1		
7	stephan@widwal.de	Öffentlich		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Öffentli	11/2		
6	Stephan.Walther@	Technik		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	45/0	12	4
05	Stephan.Walther@	nicole@w		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	18/1		
08	Stephan.Walther@	Sabine@j		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	18/1		
11	Stephan.Walther@	Technik		https://email.ws-its.de/ma	hergestellt	HTTP	Nego*	SSL		Exchan	124/1		

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:

Remotezugriffs-Verwaltungskonsole				
Konfiguration VPN	<     VERÖFFENTLICHTE     Alle veröffentlichten We	WEBANWENDUNGEN banwendungen   3 insgesamt		
Webanwendungsproxy	Filter	م		
Dashboard				
Vorgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung
💻 Remoteclientstatus	Monitor	https://monitor.ws-its.de/	https://prtg.ws.its/	PassThrough
Berichterstellung	MX	https://email.ws-its.de/	https://email.ws.its/	PassThrough
	RDS	https://rds.ws-its.de/	https://rds.ws_its.de/	DareThrough
A E Churtemanne		Bearbeite	n	
WS-PA1		Basierend	l auf dieser Anwendung veröffentliche	en
		Entfernen		
WS-KA2				

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:

Remotezugriffs-Verwaltungskonsole				
Konfiguration VPN	Remotezugriffs-Dashboard			
Webanwendungsproxy	h Serverstatus			^
Dashboard				
W Vorgangsstatus	vorgangsstatus	<u>.</u>		
💻 Remoteclientstatus	WS-RA1.ws.its	^		
Berichterstellung	<ul> <li>Ws-RA2.ws.its</li> <li>Vorgangsstatusseite</li> </ul>			
Clusterserver WS-RA1 WS-RA2	Status von DirectAccess- und VPN-Client			^
	Aktive Clients (insgesamt):	0 Übertragene Daten (gesar	mt): 0 Bytes eingeh	end/0 Bytes ausgehend
	Aktive DirectAccess-Clients (insgesamt):	0 Maximale Anzahl von Clie	ntverbindungen:	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:

💐 Remotezugriffs-Verwaltungskonsole			
👫 Konfiguration VPN	Remotezugriffs-Dashboard		
Webanwendungsproxy	🐻 Serverstatus		^
🛅 Dashboard	Vorgangsstatus	•	
W Vorgangsstatus	WE BAL with		
arr Remoteclientstatus	VIS-KA LWS-ITS	^	
Berichterstellung	Services     VPN connectivity     Web Application Proxy     Xeb Application Proxy     Web Application Proxy     Web Application Proxy Core     Vorgangsstatusseite	n ent	^
	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"		

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:

Signal Remotezugriffs-Verwaltungskonsole	
<	
👫 Konfiguration	VERÖFFENTLICHTE WEBANWENDUNGEN
VPN	Alle veröffentlichten Webanwendungen   0 insgesamt
Webanwendungsproxy	
Dashboard	Derzeit sind keine Webanwendungen veröffentlicht. Klicken Sie zum Veröffentlichen einer Webanwendung auf Veröffentlichen'.
W Vorgangsstatus	
📕 Remoteclientstatus	
📴 Berichterstellung	
Clusterserver	
WS-RA1	
WS-RA2	

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

	System - Interf	aces - Firewall -	Services - VPN	<ul> <li>Status -</li> </ul>	Diagnostics - Hel	p -	•	
								+
	8	Traffic Graphs	_	_	<b>₽</b> ⊖8	НАРгоху		۶۹
		DMZ_120_EXT	RN	🔵 wan (in)	🛑 wan (out)	Backend(s)/Server(s)		
						Backend(s)	Sessions	Status
(Local Database	e)				10k	Server(s)	(cur/max)	/
4)					y al	Client(s) addr:port	age/id	Action
		~ ~ ~			0.0	RDSWEB_ipvANY	0 / 200	0
0			$\sim$			WS-RDS1	0	
-					-10k	MX_ipvANY	19 / 200	0
t version.						WS-MX1	10	$\bigcirc$
ed at Tue Dec 3	1 15:36:57 CET 2019			V	-20k	172.19.130.105:46566	25m39s / 0x8025da400	
				Y	2011	172.19.130.105:46607	24m58s / 0x80242bc00	
		22:39 23:20	25:00	26:40	28:40	192.168.110.101:1142	5m11s / 0x8025dac00	
		22.00 20.20	20.00	20.40	20.10	192.168.110.101:1243	5m11s / 0x80242f000	
tas 52 Seconds		LAN_100_SERV	'ER	🔵 lan (in)	lan (out)	192.168.110.101:1322	4m11s / 0x8025da800	
02 0000103		A				172.19.130.105:46698	3m53s / 0x802476000	
2019					100k	192.168.110.101:20033	3m23s / 0x802476c00	
						192.168.110.101:1430	1m11s / 0x80253f000	
019					501	192.168.110.101:1498	20s / 0x802480800	
					SUK	192.168.110.101:1510	11s / 0x80242f400	-
			$\sim$			WS-MX2	9	$\bigcirc$
tates			·	~~~	0.0	172.19.130.105:46546	26m30s / 0x80242fc00	
			$\sim$			172.19.130.105:46574	25m39s / 0x8025d9400	
					501	192.168.110.101:1140	5m11s / 0x802477800	
					-SUK	192.168.110.101:1323	4m11s / 0x80253f800	
		22:39 23:20	25:00	26:40	28:40	172.19.130.105:46690	3m54s / 0x80242f800	
		DM7 130 INTE	RN	ant1 (in)	ent1 (out)	192.168.110.101:1429	1m11s / 0x802480400	
			4	- opti (iii)		192.168.110.101:1499	20s / 0x8025d9800	
						192.168.110.101:1500	20s / 0x802477000	
					0.0	192.168.110.101:15131	9s / 0x80243a000	
					-2.0k	RDS_ipvANY	0 / 200	Ø
						WS-RDS2	0	<b>v</b>
					-4.0k	PRTG_ipvANY	0 / 200	0
	0.8				0.01	WS-MON	0	0
			1		-6.0k	HTTPS_ipvANY	0 / 200	0
ress	Status				-8.0k	WS-RA1	0	0
			V			WS-RA2	0	0
9.120.120	MASTER	22:39 23:20	25:00	26:40	28:40	SMTP_ipv4	0 / 200	0
68 100 252	MASTER	LAN 110 OUE	ATS STA	ant2 (in)	ent2 (out)	WS-MX1	0	Ö
55.100.202	WING LER	LAN_TTU_CLIEF		- opi2 (in)	- opi2 (Out)	WS-MX2	0	0
0 120 252	MASTER							-

Seite 29 von 39

## WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

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

SSL Se Only St	acurity II WAP	+ S hin	lensor zufügen		
🗉 📼 WS-RA2 🏳					
SSL Se Only St	ecurity rong Prot	396 ms + S	lensor zufügen		
🖻 📼 WS-DC1 🏳					
			Disastas ADEC		Carrow
V DNS	2 ms	0 #	0 #	203 ms	hinzufüg

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

- Ich werden 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!

2	Administrator: Windows PowerShell			_	$\times$
PS (	C:\> Get-WindowsFeature   where installed				 ^
Dis	play Name	Name	Install State		
[X]	Datei-/Speicherdienste [X] Datei- und iSCSI-Dienste [X] Dateiserver [X] Speicherdienste Remotezugriff XI Dietetterse und VDV (DAC)	FileAndStorage-Services File-Services FS-FileServer Storage-Services RemoteAccess	Installed Installed Installed Installed Installed		
~~~	[X] Webanwendungsproxy	Web-Application-Proxy	Installed		
[X]	Webserver (IIS) [X] Webserver [X] Allgemeine HTTP-Features [X] HTTP-Fehler	Web-Server Web-WebServer Web-Common-Http Web-Http-Frors	Installed Installed Installed Installed		
	[X] Standarddokument [X] Statischer Inhalt [X] Verzeichnis durchsuchen	Web-Default-Doc Web-Static-Content Web-Dir-Browsing	Installed Installed Installed Installed		
	<ul> <li>[X] Leistung</li> <li>[X] Komprimierung statischer Inhalte</li> <li>[X] Sicherheit</li> <li>[X] Andersteit</li> </ul>	Web-Performance Web-Stat-Compression Web-Security	Installed Installed Installed		
	[X] IP- und Domäneneinschränkungen [X] Systemzustand und Diagnose [X] HTTP-Protokollierung	Web-IP-Security Web-Health Web-Http-Logging	Installed Installed Installed Installed		
	[X] Verwaltungsprogramme [X] IIS-Verwaltungskonsole [X] IIS-Verwaltungsskripts und -tools	Web-Mgmt-Tools Web-Mgmt-Console Web-Scripting-Tools	Installed Installed Installed		
[X]	.NET Framework 4.6-Funktionen [X] .NET Framework 4.6 [X] WCF-Dienste [X] TCP-Portfreigabe	NET-Framework-45-Fea NET-Framework-45-Core NET-WCF-Services45 NFT-WCF-TCP-PortShar	Installed Installed Installed Installed		
[X] [X] [X]	Gruppenrichtlinienverwaltung Interne Windows-Datenbank RAS-Verbindungs-Manager-Verwaltungskit (CMAK)	GPMC Windows-Internal-Dat CMAK	Installed Installed Installed		
[X]	Remoteserver-Verwaltungstools [X] Rollenverwaltungstools [X] AD DS- und AD LDS-Tools [X] Active Directory-Modul für Windows P [X] Tools für die Remotezugriffsverwaltung [X] Remotezugriffs-GUI und Befehlszeilen	RSAT RSAT-Role-Tools RSAT-AD-Tools RSAT-AD-PowerShell RSAT-RemoteAccess RSAT-RemoteAccess -Mgmt	Installed Installed Installed Installed Installed Installed		
[X] [X]	[X] Kemotezugriffsmodul für Windows Powe Unterstützung für die SMB 1.0/CIFS-Dateifreigabe Windows Defender-Features [X] Windows Defender	KSAI-REMOTEACCESS-PO FS-SMB1 Windows-Defender-Fea Windows-Defender Windows-Defender-Gui	Installed Installed Installed Installed		
[X]	Windows PowerShell [X] Windows PowerShell 5.1 [X] Windows PowerShell ISE	PowerShell PowerShell PowerShell	Installed Installed Installed Installed		
[X] [X]	Windows Server-Sicherung WoW64-Unterstützung	Windows-Server-Backup WoW64-Support	Installed Installed		
PS (	C:\> Remove-WindowsFeature -Name DirectAccess-VPN,Web	b-Application-Proxy			
Suc	cess Restart Needed Exit Code Feature Result				
Tru WAR	e Yes SuccessRest {DirectAccess und NUNG: Sie müssen den Server neu starten, um das Entf	VPN (RAS), Remotezugriff ernen abzuschließen.			
PS (	∑:\> _				×

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:

State AD FS		_			
输 Datei Aktion Ansicht Fenster ?			_ & ×		
ad FS	AD FS	Aktionen			
		AD FS			
	Ubersicht	Ansicht	•		
	Active Directory-Verbunddienste (AD FS) bieten Clientcomputern Zugriff durch Einmaliges Anmelden (SSO).	Neues Fenster hier öffnen			
	Dieser Computer ist nicht der primäre Verbundserver in der Farm	Aktualisieren			
	Anderungen an AD FS-Konfigurationseinstellungen können nur am primären Verbundservercomputer vorgenommen werden. Stellen Sie eine Verbindung mit dem primären Computer her, um die AD FS-Konfigurationseinstellungen anzuzeigen oder zu bearbeiten.	Hilfe			
	Name des primären Verbundservercomputers: <mark>ws-dc1.ws its</mark> Farmname: adfs.ws.its Letzte Synchronisierung mit dem primären Server: 31.12.2019 16:20:54				
	Weitere Informationen zu AD FS				
	Neuigkeiten in AD FS				
	AD FS-Bereitstellungshandbuch				
	AD FS-Betriebshandbuch				
	Integrieren Sie Azure Multi Factor Authentication in AD FS				
	Überwachen Sie den AD FS-Dienst mit Azure Active Directory Connect Health				
	Erfahren Sie mehr über Azure Active Directory				
	Der separate Onlinedienst Azure Active Directory bietet vereinfachte Identitäts- und -Zugriffsverwaltung. Sicherheitsberichte sowie einmaliges Anmelden bei Cloud- und Iokalen Web-Apps.				
	Was ist Azure Active Directory?				
	Erweitern Sie Ihr Verzeichnis auf Azure Active Directory				
	Identitäts- und Zugriffsverwaltung				

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

🛃 Administrator: Windows Powe	Shell ISE	-	$\times$
Datei Bearbeiten Ansicht Too	Is Debuggen Add-Ons Hilfe		
1 🧀 📙 🠇 🕒 🗎			
Unbenannt1.ps1* ×			
1 Remove-Ad	fsFarmNode		
	Cmdlet Kemove-AdfsFarmNode an der ? X		
	Geben Sie Werte für die folgenden Parameter an:		
	Benutzername: 🙍 wsjsysadm 🗸		
	Kennwort:		- -
Cmdlet Remove-A	linenosition 1		
Geben Sie Werte	OK Abbrechen		

Administrator: Windows PowerShell ISE			-	×
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe				
1 🙆 🔒 🠇 🕒 🔪 🎽 🕫 🕒 🕒 📾 🖉 🖂 🗖	🗖 🖻 📮			
Unbenannt1.ps1* ×				
1 Remove-AdfsFarmNode				
				2
PS C:\> Remove-AdfsFarmNode				^
Cmdlet Remove-AdtsFarmNode an der Betehlspipelinepo Geben Sie Werte für die folgenden Parameter an:	sition 1			
Message	Context	Status		
Die Konfiguration wurde erfelgreich abgeschlessen		 Succoss		
bre Konfiguration wurde erforgreich abgeschlossen.	DeproymentSucceeded	Success		

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:

🔁 Server-Manager			- 0	×
Server-l	Manager • Dashbo	ard 🔹 🕫 🖡	Verwalten Tools Ansicht I	Hilfe
🗰 Dashboard	🔁 Assistent zum Entfernen von R	ollen und Features	X	
Lokaler Server Alle Server	Entfernungsstatu	S	ZIELSERVER WS-DC2.ws.its	
Datei-/Speicherdienste	Vorbereitung Serverauswahl	Entfernungsstatus anzeigen		
min UNS		Auf "WS-DC2.ws.its" steht ein Neustart aus. Sie müssen den Ziels Entfernen von Features abzuschließen.	erver neu starten, um das	
	Ergebnisse	Active Directory-Verbunddienste Interne Windows-Datenbank		

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



🚪 Ereignisanzeige								
Datei Aktion Ansic	:ht ?							
Þ 🔶   🖬   🗗 🖬								
🛃 Ereignisanzeige (Lo	kal) Erei	ignisanzeige (Lok	al)					
<ul> <li>Benutzerdefinie</li> <li>Windows-Proto</li> </ul>	rte Ansichter	Jbersicht un	d Zusamr	menfassung				
> Anwendungs- u Abonnements	ind Dienstprc	bersicht						
	Z	usammenfassung	der administr	rativen Ereignisse				
		Ereignistyp	Ereignis	Quelle	Protokoll	Letzte Stu	24 Stunden	7 Tage
		Kritisch	-	-	-	0	0	0
		E 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	DESR	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
			10078	DistributedCOM	System	16	16	16
			20252	DHCD-Sen/er	Microsoft	10	10	10
			20252		Microsoft	1	1	1
			20233	Drick-Server	IVIICIOSOIT			

## 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:

Server-Manager · Dashboard       • ② I V vervaten       Tools       Ansicht       Hilfe         Bashboard       • ○ I V vervaten       Tools       Ansicht       Hilfe         I Dashboard       • ○ I V vervaten       Tools       Ansicht       Hilfe         I Lokaler Server       • Ansicht       Besterver       • ○ I V vervaten       ×         I AD DS       • ○ O I V vervaten       Vervaten       ×       • O I Vervaten       ×         Vorbereitung       Serverauswahl       Serverauswahl       Serverauswahl       Serverauswahl       • ○ I Vervaten       • I Vervaten         I DHCP       • DNS       • O I Vervaten       • O I	📥 Server-Manager		- 🗆 X
Image: Dashboard   Image: Lokaler Server   Image: Lokaler Server <th>Server-Ma</th> <th>anager • Dashboard</th> <th>🕶 😥   🚩 Verwalten Tools Ansicht Hilfe</th>	Server-Ma	anager • Dashboard	🕶 😥   🚩 Verwalten Tools Ansicht Hilfe
	Image: Dashboard         Image: Lokaler Server         Image: AD DS         Image: AD FS         Image: Datei-/Speicherdienste         Image: DhCP         Image: DNS	Assistent zum Entfernen von Rollen und Features  Entfernungsauswahl bestätigen Vorbereitung Serverauswahl Serverrollen Features  Bestätigung Ergebnisse  Cative Directory-Verbunddienste Interne Windows-Datenbank  Cative Directory-Verbundelenste Cative Dir	- C X  ZELSERVER WS-DCLwsite r Features vom ausgewählten  Entfernen Abbrechen

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:

🛃 Ereignisanzeige									
Datei Aktion Ansicht ?									
Ereignisanzeige (Lokal)     Eei     Benutzerdefinierte Ansichten     Windows-Protokolle     Anwendungs- und Dienstprotokolle     Abonnements	Ere Ú Ű	ignisanzeige (Lokal Übersicht und Ibersicht (usammenfassung d	))   Zusamr     der administr	menfassung ativen Ereignisse					
	I	Ereignistyp	Ereignis	Quelle	Protokoll	Letzte Stu	24 Stunden	7 Tage	
		Kritisch	-	-	-	0	0	0	
		E Fehler	-	-	-	61	1.674	11.398	
			2	Kernel-EventTr	Microsoft	0	0	3	
			3	FilterManager	System	0	0	6	
			3	Kernel-EventTr	Microsoft	0	0	1	
			6	CertificateServi	Anwendu	0	3	3	
			67	CertificateServi	Anwendu	0	3	3	
			68	CertificateServi	Anwendu	0	3	3	
			304	User Device Re	Microsoft	1	2	9	
			307	User Device Re	Microsoft	1	2	9	
			513	CAPI2	Anwendu	0	0	15	
			1000	Application Err	Anwendu	1	2	3	
			1008	Perflib	Anwendu	0	0	2	
			5008	DFSR	DFS-Repli	0	0	2	
			7023	Service Contro	System	1	1	1	
			8193	VSS	Anwendu	1	1	1	
			10000	CertificationA	Anwendu	0	0	1	
			10016	DistributedCOM	System	50	1363	9584	
			20252	DHCP-Server	Microsoft	1	1	2	
			20255	DHCP-Server	Microsoft	1	1	2	
			20318	DHCP-Server	Microsoft	2	146	874	
			20321	DHCP-Server	Microsoft	2	146	874	
		🗄 Warnung	-	-	-	31	34	49	
		$\pm$ Informationen	-	-	-	846	13.366	32.845	
		🗄 Überwachun	-	-	-	52.632	150.687	181.552	
		🗄 Überwachun	-	-	-	164	781	817	

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:

WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

System - Interfac	es • Firewall • Services • VPN	- Status - Diagnostics - He	łp -	•	
Commont's Conton					+ 0
£00	Traffic Graphs	600	HAProxy		600
	DMZ 120 EXTERN		Backend(s)/Server(s)		
	DIVIZ_120_EXTERN	wan (in)	Backend(s)	Sessions	Status
01 (Local Database)		1.2M	Server(s)	(cur/max)	1
100		1 OM	Client(s) addr:port	age/id	Actions
1004) 152:44 EDT 2010			RDSWEB_ipvANY	0 / 200	0
un10		800k	WS-RDS1	0	<b>O</b>
		600k	MX_ipvANY	15 / 200	0
test version.		400k	WS-MX1	7	0
dated at Tue Dec 31 15:36:57 CET 2019		200k	172.19.130.105:46698	18m27s / 0x802476000	
			192.168.110.101:20748	3m44s / 0x802480400	
	37:15 38:20 40:00	41:40 43:14	192.168.110.101:21024	2m44s / 0x8025d9800	
			192.168.110.101:21027	2m44s / 0x802480800	
linutes 23 Seconds	LAN_100_SERVER	🔵 lan (in) 🛛 🛑 lan (out)	192.168.110.101:210971	1m45s / 0x80242fc00	
		50k	192.168.110.101:192101	44s / 0x8024/6c00	
ET 2019			192.168.110.101:19258	8s / 0x80243a000	
T 2019			172 10 120 105:46600	0 19m28c / 0x90242f900	•
		0.0	102 169 110 101:1246	12m/5s / 0x80253f800	
	· · · · · · · · · · · · · · · · · · ·	~ ~ ~	192 168 110 101 20740	3m44s / 0x80253f000	
w states		-50k	192,168,110,101,21025	2m44s / 0x80242f400	
			192.168.110.101:21026	2m44s / 0x802477000	
		-100k	192.168.110.101:21096 i	1m45s / 0x80242f000	
			192.168.110.101:21098 i	1m45s / 0x802477800	
	37:15 38:20 40:00	41:40 43:14	192.168.110.101:19209 i	44s / 0x8025dac00	
	DMZ 100 INTERN		RDS_ipvANY	0 / 200	0
	DMZ_130_INTERN	opti (in) epti (out)	WS-RDS2	0	0
		0.0	PRTG_ipvANY	0 / 200	0
			WS-MON	0	0
			HTTPS_ipvANY	DOWN	0
AM		-50k	WS-RA1	DOWN	8
			WS-RA2	DOWN	8
● ⊗		4001	SMTP_ipv4	0 / 200	0
		-100k	WS-MX1	0	0
Address Status			WS-MX2	0	0

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

	SE Sy	stem <del>+</del>	Interface	es∓ F	Firewall +	Services -	VPN -	Status <del>-</del>	Diagnostics <del>-</del>	Help +		۲
Servic	es / H/	AProx	y / Front	end							C⊚ ≑ Ш 🔳	0
Settings	Front	end	Backend	Files	Stats	Stats FS	Templates					
Fronten	ıds											
Primary	Shared	On	Advanced	Name		Description	Address		Туре	Backend	Actions	
		~	X\$	HTTF	PS-Proxy		172.19.1	120.120:443	ssl/https	RDSWEB if(RDSWE MX if(MX) RDS if(RDS) PRTG if(PRTG) HTTPS (default)	B) 🥜 🕯	10
⊐₺		~		SMT	P-Proxy		172.19.1	120.120:25	tcp	SMTP (default)	Ø 1	0 t

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

	Example:			
	Action	Parameters	Condition	]
	Use Backend	Website1Backend	Backend1acl	
	http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc	
Default Backend	HTTPS		~	
	None		no de	fault is needed and this can be left to "None".
	HTTPS			
Stats options	MX			
Separate sockets	PRTG			
	RDS			
Logging options	RDSWEB			
Don't log null	SMTP		đ.	
	To skip logging probes	from monitoring systems that otherwise	would pollute	the logging. (It is generally recommended not to use this option in

Die Konfiguration muss in der PFSense bestätigt werden:

WSHowTo – Migration des HAProxy & Entfernung ADFS und WAP 2019-12-31 Migration auf Windows Server 2019

	SE Sy	stem +	Interfaces	- Firewall -	Services -	VPN -	Status +	Diagnostics +	Help +	۵
Servic	es / HA	AProx	y / Fronte	end					с	:0 ≑ Ш 🗏 0
The hapro You must	oxy configur t apply the c	ation ha hanges i	s been change n order for the	d. m to take effect.						✓ Apply Changes
Settings	Fronte	end	Backend	Files Stats	Stats FS	Templates				
Fronter Primary	Shared	On	Advanced	Name	Description	Address		Туре	Backend	Actions
□.₺		~	<b>x</b> ;	HTTPS-Proxy		172.19.12	20.120:443	ssl/https	RDSWEB if(RDSWEB) MX if(MX) RDS if(RDS) PRTG if(PRTG)	<i>₽</i> ∰ ()
⊔₽		~		SMTP-Proxy		172.19.12	20.120:25	tcp	SMTP (default)	e 🖉 🛍 🗋
									3 Add	前 Delete 📙 Save

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

	System <del>-</del>	Interfaces +	Firewall <del>-</del>	Services -	VPN +	Status +	Diagnostics <del>-</del>	Help +		۲
Services	/ HAProxy /	Backend							С⊚ ≑ Ш	•
Settings	Frontend Ba	a <mark>ckend</mark> Files	s Stats	Stats FS	Templates					
Backends										
	Advanced	Nar	ne	Servers	1	Check	Frontend		Actions	
□.₺		SM	ITP	2		SMTP	SMTP-Prox	у		<b>/ 🛍 </b>
<b>⊠</b> £		HT	TPS	2		Basic				<b>/ D</b>
□♣		RD	SWEB	1		Basic	HTTPS-Pro:	xy		<b>/ 🛍 </b>
□♣		M	<b>K</b>	2		Basic	HTTPS-Pro:	xy	•	Ø 🛍 🗋
□.₺		RD	s	1		Basic	HTTPS-Pro:	ку		e 🖞 🖗
□♣		PR	TG	1		Basic	HTTPS-Pro	xy		<b>/ 🖻</b> 🗋
									🕽 Add 🛅 Delete	🖺 Save

Und dann ist auch hier nichts mehr vom WAP über:

	System +	Interfaces 🗸	Firewall +	Services -	VPN -	Status +	Diagnostics +	Help +	(r)
Services	/ HAProx	y / Backend							C⊚ ≑ Ш 🗏 0
Settings	Frontend	Backend File	s Stats	Stats FS	Templates				
Backends									
	Advanced	Na	me	Servers		Check	Frontend		Actions
□ <b>≟</b>		SI	MTP	2		SMTP	SMTP-Prox	у	e 🖞 🖗 🖓
□ᡱ		R	DSWEB	1		Basic	HTTPS-Pro:	ху	e 🛍 🗋
□₺		М	х	2		Basic	HTTPS-Pro:	ху	e 🛍 🗋
□₺		R	DS	1		Basic	HTTPS-Pro:	ху	Ø 🛍 🗋
□±		Pf	RTG	1		Basic	HTTPS-Pro:	ху	e 🛍 🗋
									🕽 Add 🛍 Delete 🖺 Save



COMMUNITY EDITION	aces + Firewall + Services + VPI	N ≠ Status ≠ Diagn	ostics - Help	) +	•	
						+ 6
۶٥٥	Traffic Graphs		۵ ې ۶	HAProxy		8
	DMZ_120_EXTERN	🔵 wan (in) 🛛 🔴 wan	(out)	Backend(s)/Server(s)	0	Obstan
01 (Local Database)			1.0	Server(s)	(cur/max)	Status /
			500m	Client(s) addr:port	age/id	Actions
1064)			30011	RDSWEB_ipvANY	0 / 200	0
-n10			0.0	WS-RDS1	0	0
				MX_ipvANY	5 / 200	0
test version.			-500m	WS-MX1	3	$\bigcirc$
dated at Tue Dec 31 15:36:57 CET 2019				192.168.110.101:19540	51s / 0x80242ac00	
			-1.0	192.168.110.101:13309	295 / 0X802420800 29s / 0x802420800	
	<b>42:01</b> 43:20 45:	00 46:40	48:01	WS-MX2	2	0
Visutes 10 Occardo	LAN 100 SERVER	🔵 lan (in) 🛛 🛑 lan	(out)	192.168.110.101:13368 i	29s / 0x80242b400	
inutes to seconds		•	1.0	172.19.130.106:49124	3s / 0x80242b000	
ET 2019				RDS_ipvANY	0 / 200	0
-T 2019			500m	WS-RDS2	0	0
				PRTG_ipvANY	0 / 200	0
			0.0	WS-MON	0	0
w states				SMTP_ipv4	0 / 200	0
			-500m	WS-MX1	0	ğ
				WS-MX2	0	0