

Anforderungen an die D3 Edgebox Kommunikation

Im Anhang zu dieser Mitteilung finden Sie die Liste der Netzanforderungen in ihrer aktuellen Fassung.

Bitte stellen Sie sicher, dass alle Ziele über die entsprechenden Ports und Applikationen erreichbar sind.

Sollten Sie eine VASEC-Firewall der VAPS einsetzen, sind die aufgeführten Freischaltungen bereits durchgeführt. Sie haben also kein To-Do mehr an Ihrer Firewall, vor der Inbetriebnahme der D3 Edgebox!

Sollten Sie Fragen oder Anmerkungen haben, wenden Sie sich bitte direkt an uns unter.

Telefonnummer: +49 5136 / 9362 200

Email: support@vaps.de



D³ Edgebox

NETZWERK ANFORDERUNGEN

Anforderung an den Internet Zugang:

Es ist ein direkter Internetzugang ohne Proxy erforderlich.

Die D3 Edgebox ist nicht für die Nutzung über eine Proxy-Umgebung freigegeben.

Anforderung an den DNS Server:

Im Rahmen der Konfiguration Ihrer D3 Edgebox wird ein DNS-Server benötigt, welcher zukünftig die DNS-Anfragen der D3 Edgebox und ihrer Dienste verarbeitet. Folgende Anforderungen muss der DNS-Server erfüllen:

- Auflösung aller Internet-FQDN, wie www.google.de
- Auflösung von CPN FQDN, wenn die CPN von einer Anwendung innerhalb der Edge-Box benötigt wird (Beispiel DMSBB)
- Auflösung interner FQDN, wenn eine interne Auflösung innerhalb der Edge-Box benötigt wird (Beispiel DMSBB)

Notwendige Firewall-Freischaltungen:

Vorbereitend zur Installation wird empfohlen, dass die Zugriffe auf die folgenden Ziele für alle IP-Adressen des Kundennetztes möglich sind!

Wenn die D3 Edgebox im Nachgang installiert ist und per DHCP die IP-Adressen für das Betriebssystem und das BMC-Interface gezogen hat, können die Firewall-Regeln auf die IP-Adressen der D3 Edgebox angepasst werden.

Edgebox Interne Firewall:

TCP/UDP/ICMP	Port(s)	Destination(s)
ICMP		8.8.8.8
UDP	53	208.91.112.52
UDP	53	208.91.112.53
UDP	500	vpn1.vw-poc.eu vpn2.vw-poc.eu vpn-lb-12.vw-poc.eu

NETZWERK ANFORDERUNGEN

UDP	4500	vpn1.vw-poc.eu vpn2.vw-poc.eu vpn-lb-12.vw-poc.eu
UDP	123	ntp1.fortinet.net
UDP	123	ntp2.fortinet.net
TCP	443, 8890	globalupdate.fortinet.net
TCP	443, 8890	usupdate.fortinet.net
TCP	443	globalregistration.fortinet.net
TCP	53, 443, 8888	globalguardservice.fortinet.net
TCP	443	usguardservice.fortinet.net

Volkswagen VM:

TCP/UDP	Port(s)	Destination(s)
TCP	443	mcm.edge.cc.europe.d3vw.com mcm.r03.cc.europe.d3vw.com
TCP	31000- 31020	ctl.ft.europe.d3vw.com bootstrap.ft.europe.d3vw.com data.ft.frankfurt.pop.europe.d3vw.com data.ft.ireland.pop.europe.d3vw.com data.ft.paris.pop.europe.d3vw.com
TCP	443	harbor.frankfurt.utilities.europe.d3vw.com
TCP	443	registry-1.docker.io
TCP	443	auth.docker.io
TCP	443	production.cloudflare.docker.com
TCP	443	storage.googleapis.com
TCP	443	k8s.gcr.io

NETZWERK ANFORDERUNGEN

TCP	443	googlecode.l.googleusercontent.com
TCP	443	git.rancher.io

Betriebssystem D3 Edgebox:

TCP	Port(s)	Destination(s)
TCP	443, 80	d3vw-com-europe-utilities-frankfurt-zededa-images.s3.amazonaws.com
TCP	443, 80	d3vw-com-europe-utilities-frankfurt-zededa-images.s3.eu-central-1.amazonaws.com

TCP	Port(s)	Destination(s)
TCP	443	zedcloud.orchid-d3vw.com
TCP	443	update.fortiguard.net
TCP	443	usupdate.fortiguard.net
TCP	443	directregistration.fortinet.com
TCP	443, 8888	securewf.fortiguard.net
TCP	443, 8888	ussecurewf.fortiguard.net
TCP	53	208.91.112.220

VAPS VM:

TCP	Port(s)	Destination(s)
TCP	443	*.synaptic-systems.com

NETZWERK ANFORDERUNGEN

TCP	4505 4506	185.71.35.173
TCP	5665	185.71.35.174 185.71.34.96
TCP	443	185.71.35.93 185.71.34.108
TCP	443	repo.vapsservices.de
TCP	9334	185.71.35.120
TCP	443	vaps-pvm-registry.sourcepark.de

Achtung!

Für eine erfolgreiche Installation und einen stabilen Betrieb ist es, neben der reinen Freischaltung der Kommunikation, unerlässlich, dass der Datenverkehr der Edgebox unverändert bleibt. Dies bedeutet, dass Security-Funktionen, wie beispielsweise **SSL-Decryption** oder **Deep-Packet-Inspection**, für die Ziele dieses Dokumentes ausgeschaltet werden.

Bitte stellen Sie dies unbedingt sicher! Die Verwendung dieser Firewall-Features kann zu Kommunikationsausfällen der Edgebox führen, welche im schlimmsten Fall einen Ausfall einer oder mehrerer Services zur Folge haben !

Setzen Sie auf eine VASEC Lösung der VAPS, haben wir dies bereits für Sie sichergestellt!

Test der Freischaltungen für VAPS Kunden

Sollten Sie einen Comserver3+, eine Provider-VM oder einen Multiserver der VAPS im Einsatz haben, können Sie nach der Konfiguration Ihrer Firewall testen, ob der Zugriff funktionieren würde. Der Verbindungstest erfolgt mit der aktuellen IP-Adresse Ihrer VAPS-Lösung, welche standardmäßig die Dritte IP-Adresse ihres VW-Netzes ist.

Zur Durchführung des Verbindungstest müssen Sie im Webbrowser Ihrer Wahl per https die Webseite ihrer VAPS-Lösung öffnen.

Beispielsweise: <https://10.40.50.3> (dies ist eine fiktive IP-Adresse)

NETZWERK ANFORDERUNGEN

Die IP-Adresse lässt sich über die Windows Eingabeaufforderung mit dem Befehl „ping mirrorserver“ herausfinden.

Auf der nun geöffneten Webseite finden sie am linken Rand folgende Kachel, hinter der sich der Test befindet:




Sobald die Kachel geöffnet wird, läuft der Kommunikationstest auf die zukünftig benötigten D3-Ziele.

Wenn Ihre Firewall korrekt konfiguriert wurde, erhalten Sie folgendes Ergebnis:

D3-EdgeBox

Allgemein

Dieser Bereich soll eine Übersicht über die benötigten Freischaltungen für eine künftige D3EdgeBox und deren aktuellem Status bieten.
Im folgenden finden Sie eine Übersicht der Komponenten und den zugehörigen Kommunikations-Anforderungen.

EVE-OS 



Fortigate Firewall 



K3S Kubernetes 



VAPS PVM3 

