PRITUNL VPN-Server

Für den VPN-Zugriff auf die internen Dienste, wird der Server OS auf ABDOMEN ausgeführt. Dieser betreibt das System PRITUNL, welches die Benutzerzugriffe und OpenVPN-Server verwaltet. Der Server ist über den Domainnamen https://vpn.drk-cannstatt.de/ erreichbar.

Zugriffssteuerung

Die Benutzer authentifizieren sich über ihren ActiveDirectory-Account am VPN Server. Dieser verlangt zusätzlich eine OTP-Authentifizierung.

Benutzer für VPN freigeben

Um einen Benutzer für den VPN-Zugriff freizugeben, muss dieser im ActiveDirectory einer der unten aufgelisteten Benutzergruppen hinzugefügt werden. Dem Benutzer stehen dann automatisch die entsprechenden Server zur Verfügung.

Benutzergruppe	**Erreichbare VPN-Server**
VPN_Admin	Alle
VPN_Einsatzleitung	Einsatzleitung
VPN_Material	Material

Sollte ein Benutzer einer anderen Benutzergruppe hinzugefügt werden, welche mehr Server beinhaltet, muss der Benutzer erneut seinen Profillink im PRITUNL-Client eingeben. Erst danach stehen die weiteren Server zur Verfügung.

Benutzer für VPN sperren

Die Sperrung für den VPN-Zugriff kann auf unterschiedlichen Wegen erfolgen.

1. Entzug der Benutzergruppe im ActiveDirectory
2. Sperren des Benutzers im ActiveDirectory (CAVE: Der Benutzer kann sich an keinem Dienst mit AD-Authentifizierung mehr anmelden)
3. Sperren des Benutzers im PRITUNL-Webinterface (Der Benutzer muss sich hierfür bereits ein mal angemeldet haben, sonst wird er nicht angezeigt)

Somit muss je nach Situation die richtige Methode ausgewählt werden. Grundsätzlich empfiehlt es sich Änderungen lieber im ActiveDirectory (1) vorzunehmen, da das Webinterface eher zur Verwaltung der verschiedenen VPN-Server dient.

VPN-Server

Um die Zugriffe gezielt in der Firewall steuern zu können, stehen den Benutzern den Aufgaben

angepasste Server zur Verfügung.

Server	IP-Range	Firewall
Admin	10.8.10.0/24	Alle Bereiche
Einsatzleitung	10.8.200.0/24	» src_VPN-Einsatzleitung
Material	10.8.20.0/24	» src_MatWLAN

Routen

Server	Route	Beschreibung
Admin	10.10.0.0/16	Quelle
	10.4.0.0/16	WaWa
	10.41.0.0/16	Wilhelm
	10.69.0.0/16	PA
	10.9.0.0/16	WaSa
Einsatzleitung	10.4.110.0/24	WaWa SRV-VLAN
Material	10.4.110.0/24	WaWa SRV-VLAN

Konfiguration

Die Server sind so eingestellt, dass jede Verbindung mit Zwei-Faktor-Authentifizierung stattfinden muss. Wird eine Verbindung mit dem PRITUNL eigenen Client hergestellt, prüft dieser beim Aufbau der Verbindung ob Änderungen an der Konfiguration vorgenommen wurden und aktualisiert diese bei Bedarf.

Zur Sicherstellung des korrekten Routings wurde die VM in ein eigenes VLAN eingebunden. Die verbundenen Clients nutzen kein NAT, wodurch sich der Client immer mit seiner zugewiesenen IP am Router meldet.

Mobile Nutzung

Es ist möglich OpenVPN-Benutzerprofile herunterzuladen. Diese Funktion ist für den Endnutzer gesperrt. Über das Admin-Interface können diese bei Bedarf für den entsprechenden Nutzer heruntergeladen werden.

Da wir davon ausgehen, dass die meisten Arbeiten sowieso mit einem Computer erledigt werden müssen, wurde diese Funktion deaktiviert. Desweiteren aktualsiert sich die heruntergeladene Konfiguration bei änderungen nicht automatisch. Der Benutzer muss also erst eine neue Konfiguration über die Admins anfordern.

PRITUNL-Webinterface

Über das Webinterface können sich sowohl die Benutzer ihre entsprechenden Konfigurationen herunterladen, als auch die administrativen Änderungen vorgenommen werden.

Für Endnutzer

Über den AD-Benutzer können sich berechtigte Personen einloggen. Folgende Funktionen stehen dann zur Verfügung:

- OTP-QR-Code für die Zwei-Faktor-Authentifizierung
- Download des PRITUNL-Clients
- Profillink zum hinzufügen im PRITUNL-Client

Für Administratoren

Über gesonderte Benutzer kann über das Webinterface auf die Administration zugegriffen werden. Folgende Funktionen stehen hier zur Verfügung:

- Verwaltung der VPN-Server sowie neustarten dieser
- Einsehen der Zugriffslogs
- Benutzerverwaltung (Einstellungen, OTP-QR-Code, Sperren/Freigeben)

Admin-Accounts werden im Webinterface gesondert angelegt und sollen zusätzlich mit einer Zwei-Faktor-Authentifizierung geschützt werden. Dieser Code kann über das Webinterface auch für Admin-Accounts eingesehen werden. Ein Zugriff ist im Regelbetrieb eigentlich nicht erforderlich.

Fallback Zugriff

Falls die RADIUS-Authentifizierung ausfällt, beispielsweise wenn COR ausfällt, gibt es einen Benutzer als Rückfallebene.
Dieser ist standardmäßig deaktiviert und muss vorher über das Webinterface aktiviert werden.

Anschließend kann mit diesem Benutzer über VPN auf das Netzwerk zugegriffen werden.