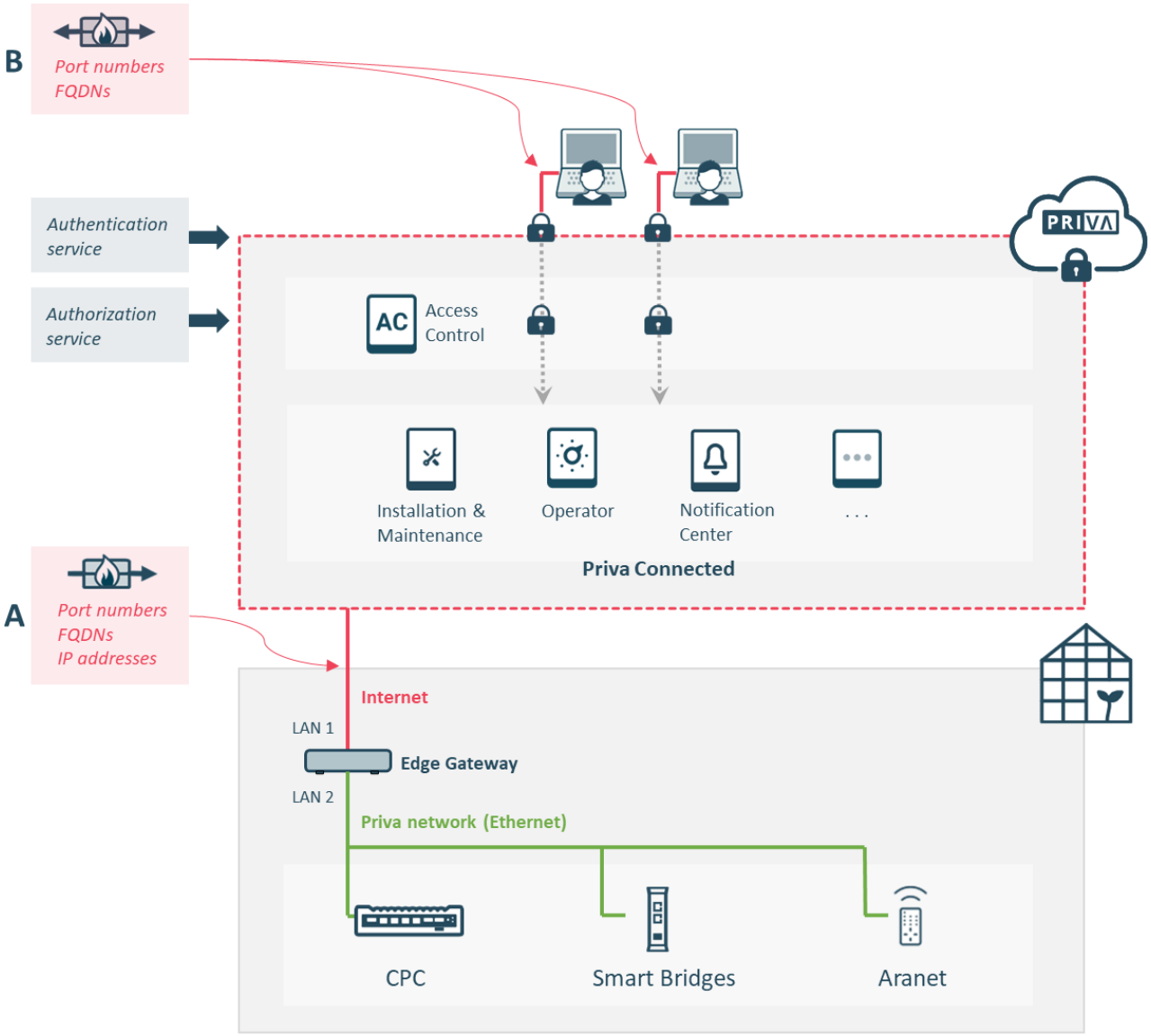
> ICT-INFORMATIE

Hoe beschermt Priva de data van uw kas? En wat moet u doen om communicatie tussen de Priva hardware en software op een veilige manier mogelijk te maken?

Netwerkoverzicht

De afbeelding toont de aangeraden netwerkconfiguratie waarbij het Priva-netwerk gescheiden is van het internet. Houd er rekening mee dat het veiligheidsrisico's met zich meebrengt als het Priva-netwerk niet van het internet gescheiden is.



A Zie: A) Communicatie tussen gateway en Priva Cloud (pag. 3)

B Zie: B) Communicatie tussen browsers en Priva Cloud (pag. 5)

Functie Edge Gateway / Priva Gateway

Procesbeheersystemen mogen nooit op een netwerk met internettoegang draaien omdat dit veiligheidsrisico's met zich meebrengt. Priva adviseert daarom dringend om het Priva-netwerk en het internet gescheiden te houden. Om cloud services te kunnen gebruiken, is natuurlijk wel communicatie tussen het beheersysteem en de Priva Cloud nodig. De Edge Gateway is een gateway die dit op een veilige manier mogelijk maakt. De Edge Gateway is de opvolger van de Priva Gateway.

De gateway staat alleen uitgaande verbindingen toe. Zo beschermt het het Priva-netwerk tegen toegang door onbevoegden via het internet. Inkomende verbindingen staat de gateway niet toe. Als de gateway de verbinding naar buiten toe opzet, zal inkomend verkeer binnen die actieve sessie wel worden toegestaan. Dit maakt het mogelijk om met een applicatie/dienst van buitenaf waarden aan te passen.

De data die wordt overgedragen tussen de gateway en de cloud is beveiligd aan de hand van versleuteling. In tegenstelling tot andere methoden voor toegang tot het Priva-netwerk, zoals een VPN, maakt deze architectuur gebruik van een systeem op basis van berichten, dus is er geen volledige datalink tussen het Priva-netwerk en de buitenwereld. Er wordt slechts in heel beperkte mate data uitgewisseld.

Updates van Linux op de Edge Gateway worden uitgevoerd in Installation & Maintenance (module FirmwareUpdater).

Support van Priva

Bij gebruik van de Priva Gateway kan Priva eenvoudig support op afstand leveren via TeamViewer. Hiervoor moet poort 5938 open staan.

Bij gebruik van de Edge Gateway kan Priva support op afstand leveren via Remote Monitor. Remote Monitor is beschikbaar vanaf firmwareversie 2.13.1. Voor Remote Monitor hoeven geen extra poorten open gezet te worden, de communicatie gaat via HTTPS en WebSocket Secure (WSS) (poort 443). Wel is FQDN edge-status.priva.com nodig.

Wat is Remote Monitor?

Remote Monitor is een service van Priva die bestaat uit twee onderdelen:

- dienst die op de Edge Gateway draait,
- server in Microsoft Azure.

Remote Monitor heeft twee functies:

- Priva kan inzien welke gateways online zijn. De gateway stuurt periodiek een bericht naar de server via een API. Deze API geeft een lijst terug van alle online gateways en gateways die eerder online waren maar momenteel offline zijn.
- Priva kan support leveren voor uw gateway via een gecodeerde SSH-verbinding.

De communicatie met de gateway is volledig veilig en afgeschermd:

- Communicatie tussen gateway en cloud wordt geïnitieerd door de gateway.
- Alle communicatie is beveiligd via TLS.
- Gateways hebben een clientcertificaat nodig dat is uitgegeven door Priva om te authenticeren met de cloudserver. Op deze manier kunnen alleen echte Priva Edge Gateways verbinding maken met de server.
- Alle communicatie is afgeschermd met specifieke wachtwoorden en tokens per gateway die alleen toegankelijk zijn voor specifieke Priva-medewerkers.
- Wachtwoorden en tokens worden gegenereerd door Azure KeyVault.

Remote Monitor draait als een aparte service onafhankelijk van IoT Edge en blijft daarom werken in het geval dat er problemen zijn met IoT Edge.

Beveiligingsmaatregelen van Microsoft

Alle Digital Services zijn vormgegeven op basis van het cloudplatform van Microsoft Azure. De services van Priva maken gebruik van de standaardcomponenten IoT-hub en Service Bus van Microsoft Azure voor de communicatie tussen het Priva-netwerk en de cloud. Gedetailleerde informatie over de beveiliging van Microsoft vindt u in het Microsoft Trust Center.

A) Communicatie tussen gateway en Priva Cloud

Om de communicatie tussen de gateway en de Priva Cloud mogelijk te maken, moeten specifieke poorten open staan in de firewall. Daarnaast moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's of op basis van IP-adressen.

Zie **A** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (gateway - Priva Cloud)

In de tabel hieronder staan de poortnummers die nodig zijn voor communicatie tussen de Edge Gateway of Priva Gateway en de Priva Cloud. Alle poorten maken alleen gebruik van uitgaande communicatie.

Poort	Details	Transport-protocol	
123	NTP	UDP	[1]
443	HTTPS	TCP	[1]
5671	AMQP	TCP	[1]
5672	AMQP	TCP	[1]
8883	MQTT	TCP	[1]

= uitgaand

[1] LAN-poort aangesloten op internet

FQDN's (gateway - Priva Cloud)

In de tabellen hieronder staan de Fully Qualified Domain Names (FQDN) weergegeven die nodig zijn voor communicatie tussen de gateway en de Priva Cloud. U heeft de keus om wildcards (adressen startende met *) te gebruiken of de volledige FQDN's vrij te geven. De lijst van volledige FQDN's is echter wel dynamisch; er kunnen in de toekomst FQDN's toegevoegd worden en ze kunnen gewijzigd worden. Het gebruik van wildcards is meer onderhoudsvriendelijk omdat de lijst van wildcards minder vaak zal wijzigen dan de lijst van volledige FQDN's.

We raden aan om ten minste de wildcard *.priva.com te whitelisten omwille van toekomstige ontwikkelingen.

FQDN's: van Edge Gateway naar cloud

FQDN	Service
***.blob.core.windows.net** (HTTPS)	
coprdfrontend2sawe.blob.core.windows.net	Gateway services[1]
edgegatewayfirmware.blob.core.windows.net	Gateway services[1]
prddevicemetadatasa.blob.core.windows.net	Gateway services[1]
prdfileuploadersa.blob.core.windows.net	Gateway services[1]
prdhdptsgwtelemetrysa.blob.core.windows.net	Cloud History
prdprivaauditlogs.blob.core.windows.net	Gateway services[1]
***.priva.com** (HTTPS)	
cr.priva.com	Gateway services[1]
cr-data-westeurope.priva.com	Gateway services[1]
data-gateway-fileuploader.priva.com	Gateway services[1]
edge-remote.priva.com	Gateway services[1]
edge-status.priva.com (HTTPS, WSS)	Gateway service Remote Monitor
local-auth-provisioning.priva.com	Gateway services[1]
***.pool.ntp.org** (NTP)	
Landsafhankelijk, bijv.: 0.nl.pool.ntp.org	NTP-server
***.oms.opinsights.azure.com** (HTTPS)	Gateway services[1]
Overige	
aka.ms [2] (HTTPS)	Gateway services[1]
global.azure-devices-provisioning.net (HTTPS)	Gateway services[1]
mcr.microsoft.com (HTTPS)	Gateway services[1]
prd-priva-generic-ih.azure-devices.net (HTTPS, MQTT, AMQP)	Gateway services[1]
priva.azurecr.io (HTTPS)	Gateway services[1]

FQDN	Service
priva.westeurope.data.azurecr.io (HTTPS)	Gateway services[1]
westeurope.data.mcr.microsoft.com (HTTPS)	Gateway services[1]

[1] Services van de gateway (configuratie van de gateway, gateway updates, authorisatie, metadata, ...)

[2] Bij het uitvoeren van de connectivity check (in de lokale configuratieapplicatie) zal aka.ms omleiden naar andere endpoints: raw.githubusercontent.com/* (aan verandering onderhevig).

FQDN's: van Priva Gateway naar cloud

FQDN	Service
***.priva.com** (HTTPS)	
accesscontrolapi.priva.com	Gateway services[1]
assetapi.priva.com	Gateway services[1]
auth.priva.com	Gateway services[1]
authorization.priva.com *(verouderd)*	Gateway services[1]
connect.priva.com *(verouderd)*	Gateway services[1]
gps.priva.com	Gateway services[1]
state.priva.com	Gateway services[1]
tenantapi.priva.com	Gateway services[1]
Overige	
prdinstallupdatesa.blob.core.windows.net (HTTPS)	Gateway services[1]

[1] Services van de gateway (configuratie van de gateway, gateway updates, authorisatie, metadata, ...)

IP-adressen (gateway - Priva Cloud)

Priva gebruikt de "EuropeWest" en "EuropeNorth" IP-adresreeksen van Microsoft die nodig zijn voor Priva Digital Services. Deze reeksen worden dynamisch gebruikt door Microsoft en kunnen daarom niet specifiek genoemd worden. De reeksen die Microsoft gebruikt, zijn te vinden op hun website: ga naar https://www.microsoft.com/en-us/download/details.aspx?id=56519 en download het json-bestand.

Dit bestand wordt wekelijks bijgewerkt. Nieuwe reeksen die in het bestand worden toegevoegd, worden gedurende ten minste één week niet gebruikt in Azure. Indien u gebruik maakt van de IP-adres beperkingslijst, download dan elke week het nieuwe json-bestand en voer de nodige wijzigingen uit op uw locatie om diensten die in Azure worden uitgevoerd correct te identificeren.

Maak geen gebruik van IP-adresreeks 172.23.105.0/24. Deze reeks wordt namelijk al intern in de Edge Gateway gebruikt.

Internetverbinding

Alle Priva Digital Services vereisen een breedband-internetverbinding met een minimale upload- en downloadsnelheid van 10 Mbps.

B) Communicatie tussen browsers en Priva Cloud

Om de communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud mogelijk te maken, moet poort 443 open staan in de firewall en moet de communicatie met de Priva Cloud toegestaan worden op basis van FQDN's.

Zie **B** in de afbeelding in Netwerkoverzicht (pag. 1).

Poortnummers (browser - Priva Cloud)

In de tabel hieronder staat het poortnummer dat nodig is voor communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud.

Poort	Details	Transport-protocol	
443	HTTPS, WSS[1]	TCP	

[1] WSS staat voor WebSocket Secure. In tegenstelling tot HTTP maakt het WebSocket-protocol full-duplex communicatie mogelijk tussen browsers en de Priva Cloud (die wordt gebruikt om real-time waarden te verkrijgen zonder HTTP-polling).

 = in- en uitgaand

FQDN's (browser - Priva Cloud)

In de tabel hieronder staat de Fully Qualified Domain Names (FQDN) weergegeven die nodig is voor communicatie tussen de browsers van de Priva Digital Services-gebruikers en de Priva Cloud. De tabel toont alleen de wildcard (adres startende met *).

FQDN's: van browser naar cloud

FQDN wildcard	Service
***.priva.com** (HTTPS, WSS[1])	Priva Digital Services
***.azurewebsites.net** (HTTPS, WSS[1])	API Access

[1] WSS staat voor WebSocket Secure. In tegenstelling tot HTTP maakt het WebSocket-protocol full-duplex communicatie mogelijk tussen browsers en de Priva Cloud (die wordt gebruikt om real-time waarden te verkrijgen zonder HTTP-polling).

Internetverbinding

Alle Priva Digital Services vereisen een breedband-internetverbinding met een minimale upload- en downloadsnelheid van 10 Mbps.

Priva (hoofdkantoor)
Zijlweg 3
2678 LC De Lier
Nederland

Zie www.priva.com voor contactgegevens van een Priva kantoor of partner voor uw regio.