

Project plan : Internship Actwise

By Jonas De Weerd

ACTWISE

Table of Contents

Who is the company?

User Story's

Project scope

ActWise: Securing Digital Identities

About Us

- 15 years of expertise
- Identity and Access security solutions

Our Logo

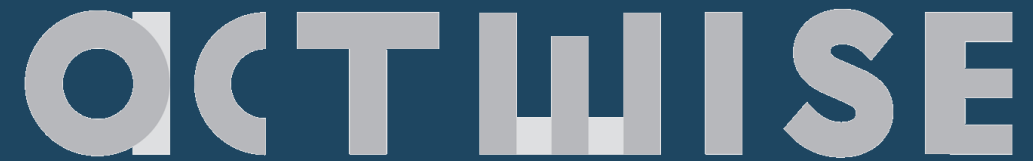
- Symbolic key: Unlocking secure access
- Binary code: Nod to the digital realm

Partnerships

- Cronos Group: Belgian tech powerhouse
- CyberArk: Leaders in privileged access management

Internship mentor

- Jelle Verreth: jelle.verreth@actwise.eu



User story's

Emergency button
for Cyber attacks

Password
recovery

Suspicious activity
detection

Approval process
for Accounts with
many rights

Temporary access

Own idea for
story

Emergency Response: Cyber Attack Mitigation

Emergency button for Cyber attacks:

- In the case of a cyber attack, swift action is required.
- Secure specific system components:
 - Block access of identified malicious users.
 - Change passwords of affected accounts.

Streamlining Account Approval Processes

Approval process for Accounts with Many Permissions:

- High-privilege accounts require meticulous approval procedures.
- Traditional approval methods can be cumbersome.
- Leveraging chat interfaces for faster approval processes:
 - Streamlines account authorization.
 - Enhances efficiency without compromising security.

Streamlined Password Recovery

Password recovery:

- Password recovery is a frequent task for users.
- Automating password recovery through a chat interface offers significant time savings.
- Simplifies the process, enhancing user experience and efficiency.

Streamlined Temporary Access Management

Temporary access:

- Occasions arise where temporary access to privileged accounts is necessary.
- Managing this process can be intricate.
- Leveraging a chat interface can significantly expedite this process, enhancing efficiency.

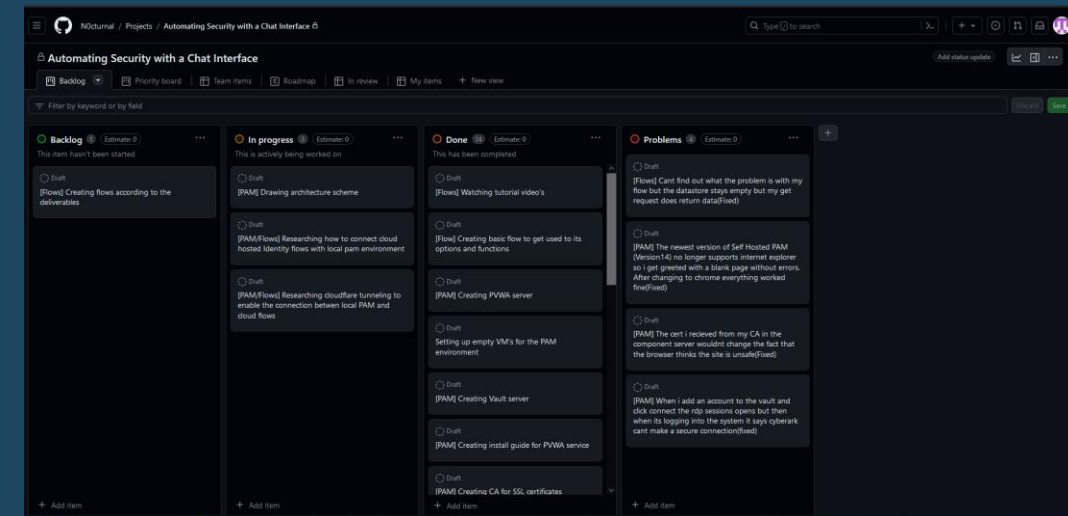
Automated Suspicious Activity Detection

Suspicious Activity Detection:

- Automated chat interfaces can play a vital role in detecting suspicious behavior.
- For instance, multiple login attempts from different locations in a short timeframe could raise alarms.
- Automatic alerts triggered by the chat interface enable rapid implementation of additional security measures.

Communication

- Kanban board on github
- Wednesday
- Weekly reporting on word/mail



Project scope

Cyberark Self-
Hosted PAM
environment

Cyberark
Identity Flows

Cyberark Self-hosted PAM environment

1.CyberArk PAM Overview:

- CyberArk Privileged Access Management (PAM) safeguards critical assets by managing and controlling who can access privileged accounts and sensitive information.

2.Components:

- **Vault:** Centralized storage for passwords and sensitive data, ensuring secure access control.
- **Session Manager:** Facilitates secure access to privileged accounts without revealing credentials, enhancing security during sessions.
- **Policy Manager:** Sets and enforces access policies, ensuring compliance and reducing security risks.

3.Key Benefits:

- **Strengthened Security:** Protects against insider threats, external attacks, and data breaches.
- **Operational Efficiency:** Streamlines privileged access management processes, reducing risks and operational overhead.
- **Auditability:** Maintains detailed logs for auditing, forensic analysis, and reporting purposes.

4.Users:

- Suitable for organizations of all sizes across various industries, including finance, healthcare, and government, requiring robust privileged access controls.

Project plan

Cyberark Self-Hosted PAM environment

Component server(CPM, PVWA, PSM)

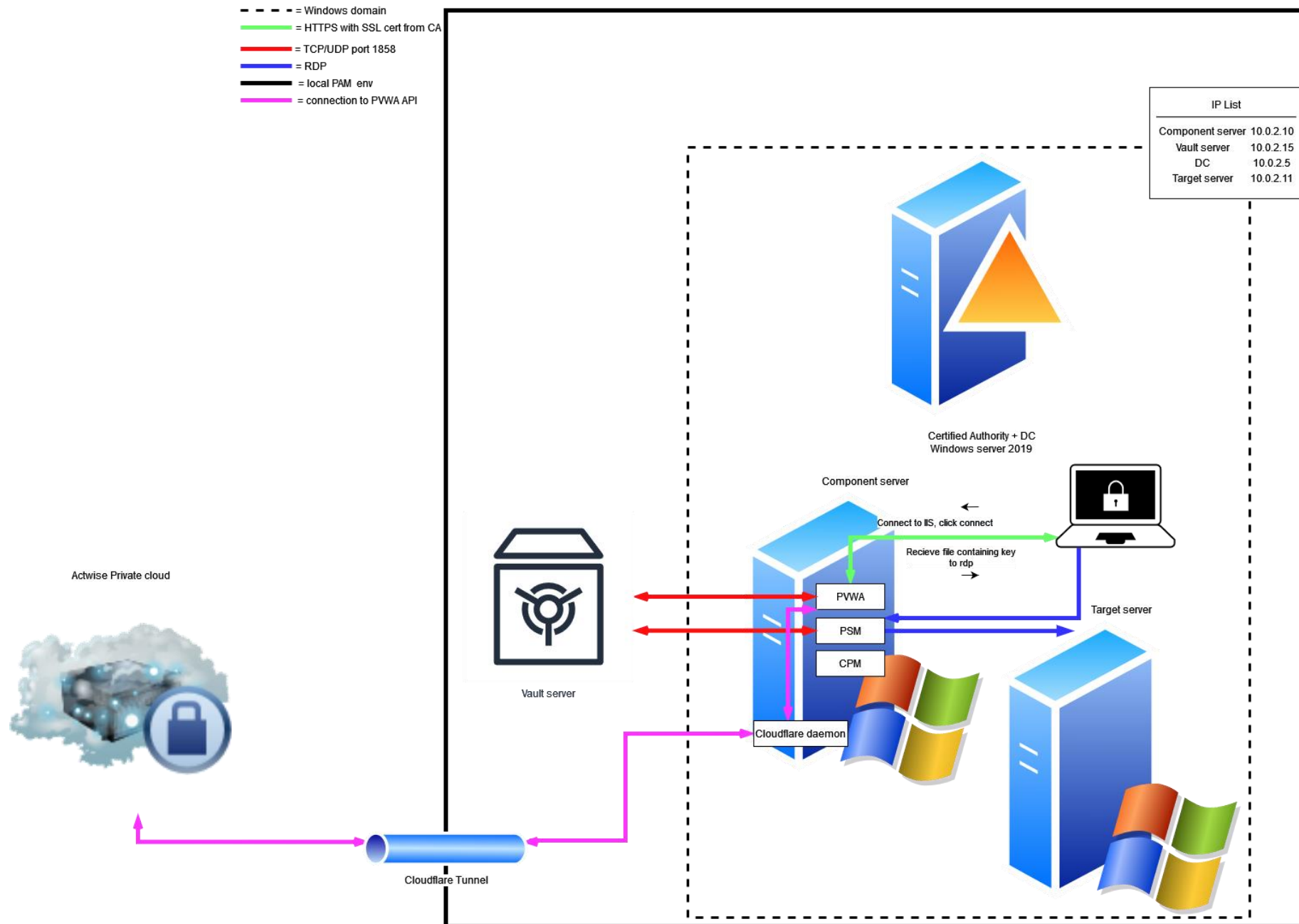
Vault server(FAT, PrivateArk server)

Windows server(DC, CA, DNS)

Target server(Windows server 2019)

PTA server(Linux RHEL)

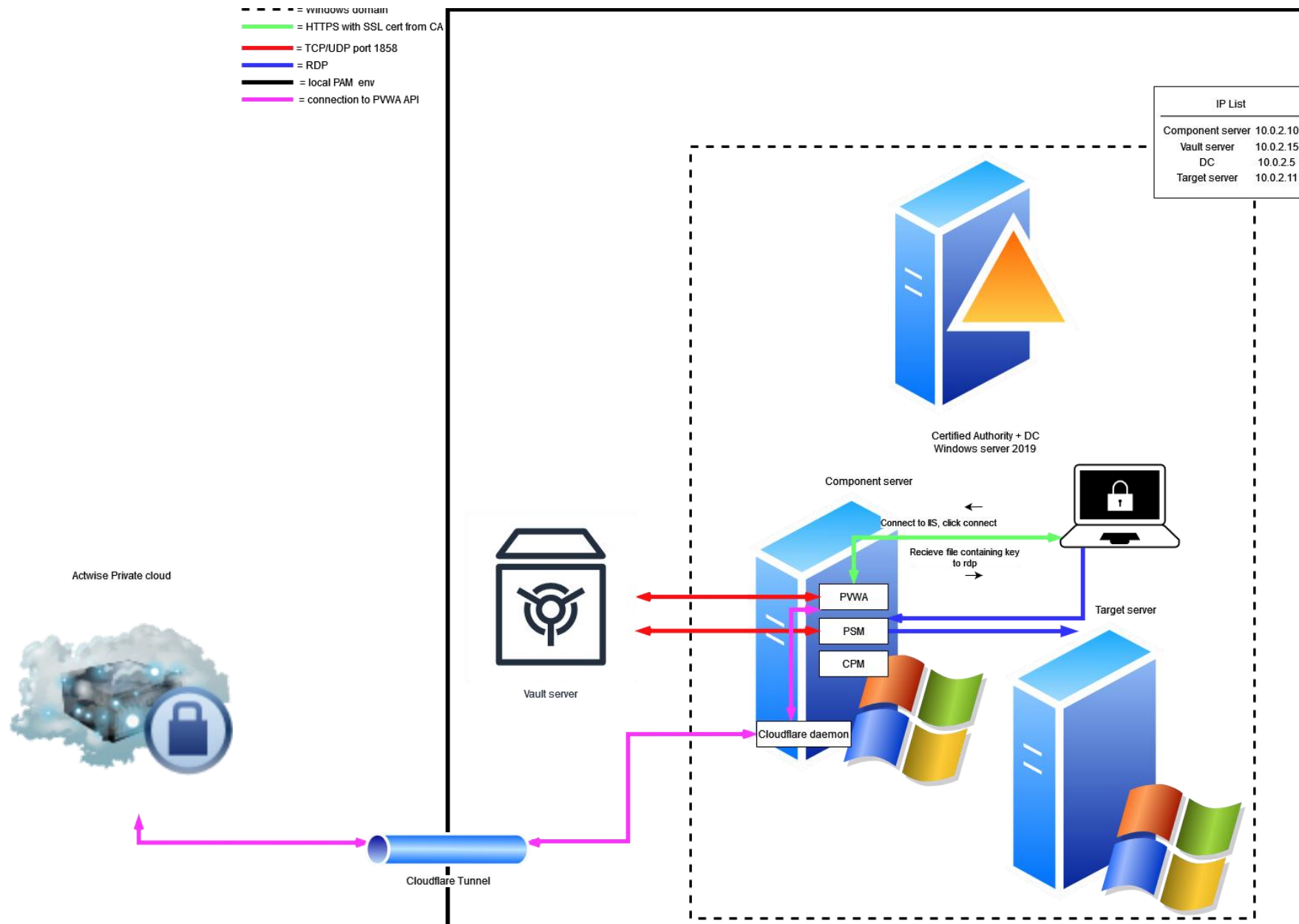




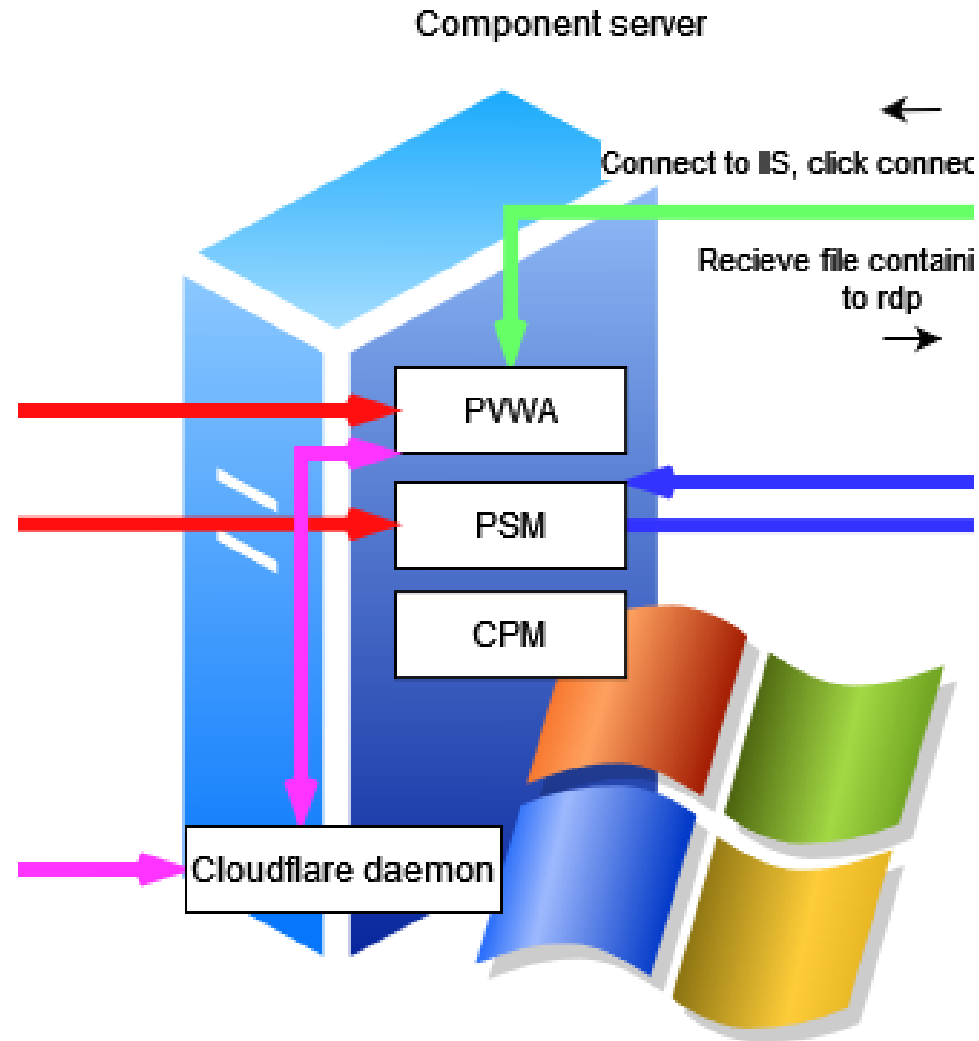
The vault server is a Windows server that holds the Cyberark vault and all of its safes. In these safes the passwords for everyone are stored



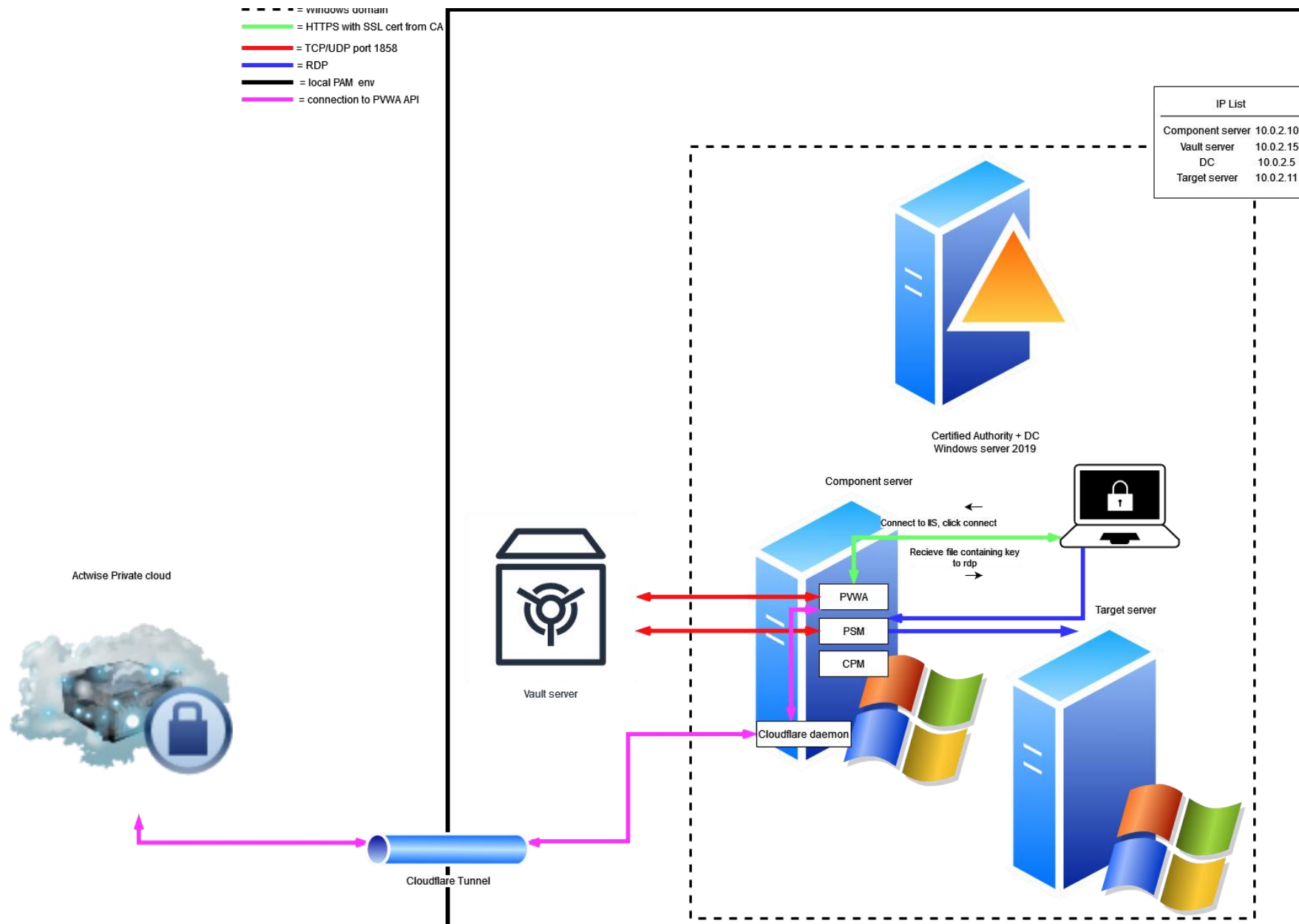
Vault server



The component server is another Windows server that holds all the services for the Cyberark environment except the vault. The PVWA(= Password vault web access) is needed to connect to the vault interface and there you will be able to connect to saved accounts/passwords. The PSM(=Privileged session manager) is used to create a secure monitored connection to the target account.



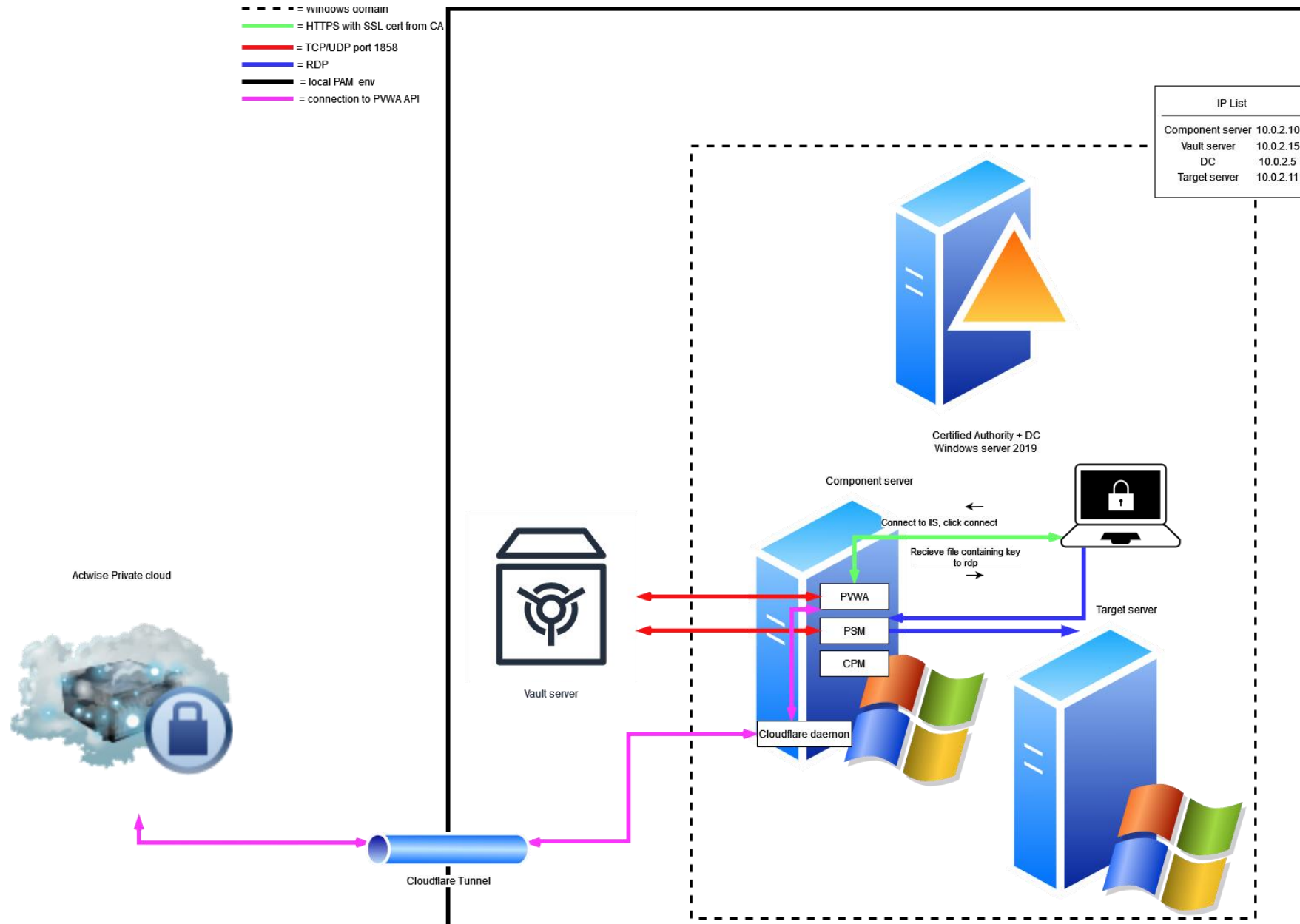
Next the CPM(=Central Policy Manager) that is a service that enforces policy's on the passwords and apply changes to passwords when its required by a policy or a manual change. And lastly the Cloudflare Daemon is required only in my environment because i need the cloud to be able to see my local environment so that identy flows can find it and use it.



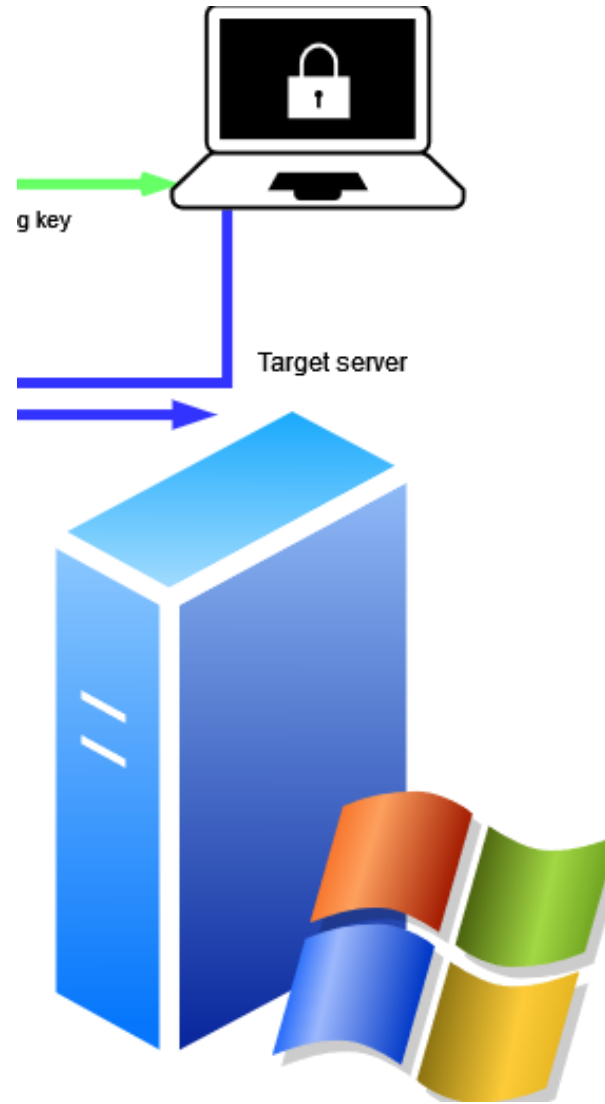
This is another windows server but its the domain controller so it creates me a domain and works as DNS server. It also has Certified Authority services installed to give out ssl cert for my https connections.



Certified Authority + DC
Windows server 2019



This is the target server. It just a windows serves as a server to add accounts into to logon to. And the laptop is there to represent how a user would normally use this system.

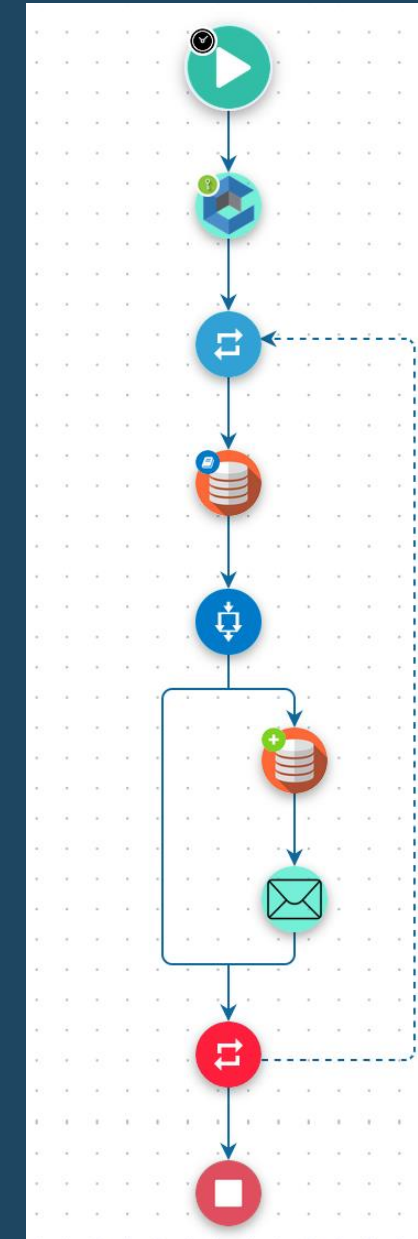


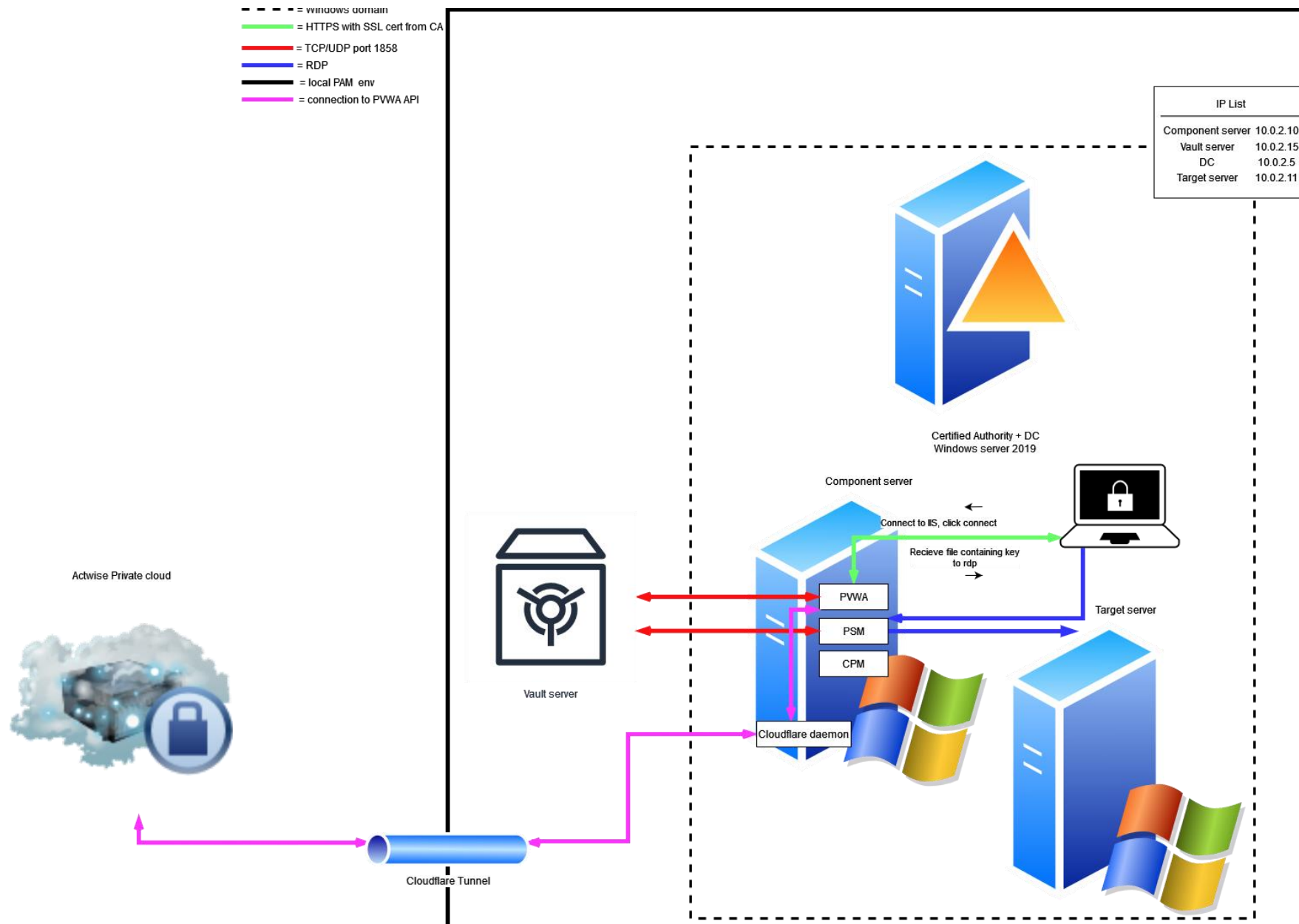
Project plan

Cyberark Identity Flows

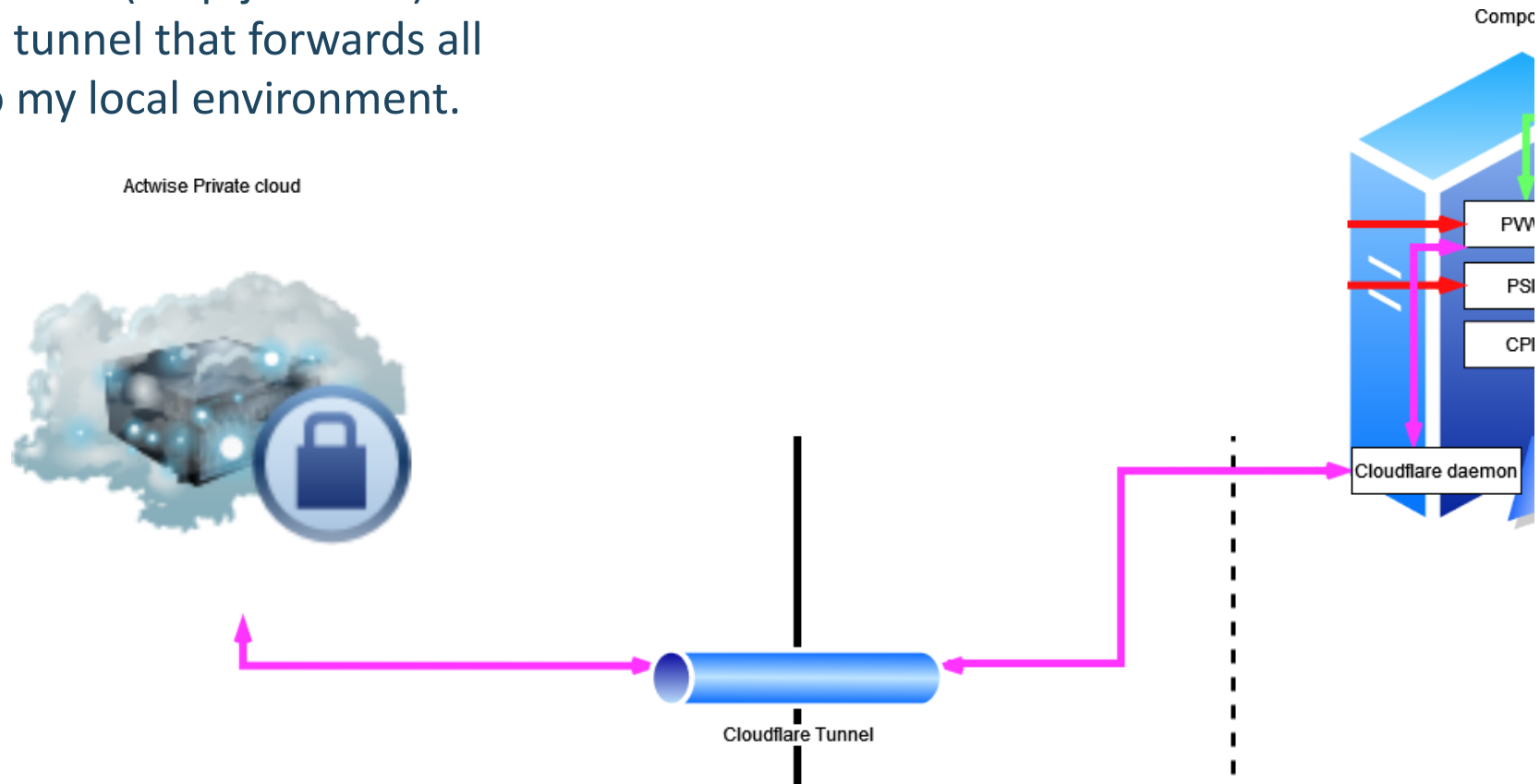
Cloud hosted Identity Flows service

Connection to local environment via cloudflared





This is the cloudflare tunnel wich helps the cloud to connect to my local PAM environment. It uses my domain name(corp-jonas.be) to create a tunnel that forwards all data to my local environment.



[← Jonas.de.weerdt@ou... ▸](#)

- Zero Trust overview
- Analytics ▾
- Gateway ▾
- Access ▾
- Networks New ▴
- Tunnels**
- Routes
- DEX ▾
- My Team ▾
- Logs ▾
- Settings

[⏪ Collapse sidebar](#)[← Back to tunnels](#)

localPAM-tunnel

[Overview](#) [Public Hostname](#) [Private Network](#)

Public hostnames

[+ Add a public hostname](#)

Public hostname			Path	Service	Origin configurations	Menu
⋮	1	pvwa.corp-jonas.be	*	https://localhost	1	⋮
⋮	2	rdp.corp-jonas.be	*	rdp://localhost	0	⋮
Catch-all rule: http_status:404 Edit						

Thank you for listening

Are there any questions?

OCTWISE