Sonpo

2Element

MFA
(Multi-Factor Authentication)

Petr.Chmelik@sonpo.cz
Pavel.Novak@sonpo.cz

Arguments for MFA

- It adds another important security level to your accounts beyond the password (which can be easily misused).
- It helps to verify and ensure that anyone who signs up is really who they say they are. This significantly reduces the risk of compromising an account.
- Modern multi-factor authentication tools support methods with high user comfort and a high security level. For example, they send Push notifications to a phone with biometric protection (fingerprint, facial scan) or check the user's physical token. It is thus not necessary to overwrite numeric codes manually as with older methods.
- Recommended by security authorities (NÚKIB, CISA).

Sonpo

MFA – Factors for authentication in general

- Authentication factors are categorised into three groups:
  - Something you know (such as a password or PIN).
  - Something you have (such as a phone or a HW token).
  - Something you are (such as a fingerprint, facial scan or other biometric data).

- MFA requires the user to authenticate using two or more authentication factors from different categories (e.g. "something you know" in combination with "something you have").

- The modern method of Push notifications for smartphones with biometric authentication combines all three of these categories. Logging in with your name and password (something you know) is complemented by Push notifications on your mobile phone (something you have), which must be confirmed after biometric verification (something you are).

Sonpo

2Element – our MFA solution

- General solution for organisations and companies
- It complements problematic passwords with other factors
- MFA is mainly used for:
  - Privileged accounts (various administrator rights) – for all access types
    - VPN, server login, password administrator, …
  - User accounts – especially for Internet access to the organisation (or to the cloud)
    - VPN, remote desktops, …

- Czech and English language support (other languages can be added)
- Flexible solution for authentication – of employees, partners, customers
- On-premise installation option (entirely at the customer's site only, no cloud)

Sonpo

Typical services and applications for MFA

- VPN accesses (Fortinet, Cisco, CheckPoint, …)
- Administrator RDP accesses to MS servers
- Remote desktops (RDP) for users, incl. Terminal Server access
- Local user logins for the computer
- ADFS (Active Directory Federation Services) integration
- Cloud services (O365, …)
- Password management applications (LastPass, BitWarden, …)
- Customer's own application (Helpdesk, Intranet,…) using API, SAML
- Gateways and solutions for partners and customers
- Other integration protocols with Radius or LDAP

Sonpo

Supported second factors

- Push notifications to the application for iPhone or Android
  - (after verifying the fingerprint/face/PIN, just select "approve" or "reject")
- Hardware tokens – Yubico
- OTP codes
  - from mobile application
  - from SMS message

Sonpo

Link to AD or ADFS

- Link to Active Directory, including setting which trees or user groups to synchronise and how.
- Concurrent support for both local groups and users, as well as those transferred from AD.
- Possible operation even without link to AD. Local users can be created directly in the MFA server. Suitable for installations without AD or users who are not in AD.
- Support of other LDAP compatible directories is also possible.
- Integration into ADFS logins – this makes it easy to extend the entire ecosystem with MFA, supporting ADFS logins and also SAML as a chain-type response.

Sonpo

MFA integration options

- Open API for integration into third party applications
- Connection to ADFS and SAML (e.g. customer cloud services)
- RADIUS support (e.g. for VPN)
- SMS gateways
- Password administrator – we can deliver turnkey solutions

Sonpo

General "MFA application" for the customer

- For larger implementations, we offer a solution that is popular today, for example, in banks under the names such as – KB key, RB key, …
- This means delivering a customised mobile application to the customer that can be used for all MFA accesses.
- Appropriate consolidation of all applications that should use MFA authentication.
- “White label” customisation
  - for server (own name and design)
  - for mobile applications (own name, design and fixed connection with the customer's server)

Sonpo

Installation of MFA servers at the customer

- It is a solution installed on dedicated servers (Linux CentOS)
  - Installation into virtualisation is recommended – VMware, Hyper-V, KVM
- It includes a web interface for administrators
- Optimally divided into two sections:
  - In DMZ – web server – it communicates to the Internet (Push notifications, etc.), provides API
  - In (V) LAN – proxy server – Auth proxy, it mediates communication with AD and RADIUS
- For large installations, we deliver a scalable solution that meets the required SLAs.

Sonpo

MFA – Safety of our solution

- Detailed logging (audit log) of all processes in the whole solution.
- Registration and authorisation of mobile applications is ensured by asymmetric cryptography. Private key
  in modern mobile phones is stored in a dedicated security storage site, cannot be accessed and is protected biometrically.

- The administrator defines the required security policies for the user.
- Data transmissions are encrypted by default using *SSL / TLS*.
- Export of logs using Syslog for external processing *(SIEM support).*
- Login *(SSO)* integration with SAML or ADFS providers.
- The application is tested by penetration tests according to the OWASP methodology.
- Possibility to provide source code for audit.

Sonpo

MFA – Consultation and Demo

- We provide professional consultation in this area for customers and partners
- We will explain all concepts such as FIDO2, WebAuthn, U2F, TOTP, ...
- We can demonstrate MFA solutions using Teams or other conference platforms
- During the conference, we help analyse MFA application for the customer

Sonpo

MFA – Trial version and PoC installation

- We provide trial licences for internal testing.
- MFA server installation can be under our hosting.
- We can also install it into the customer’s infrastructure.
- Within PoC, we offer professional consultation for further integrations.

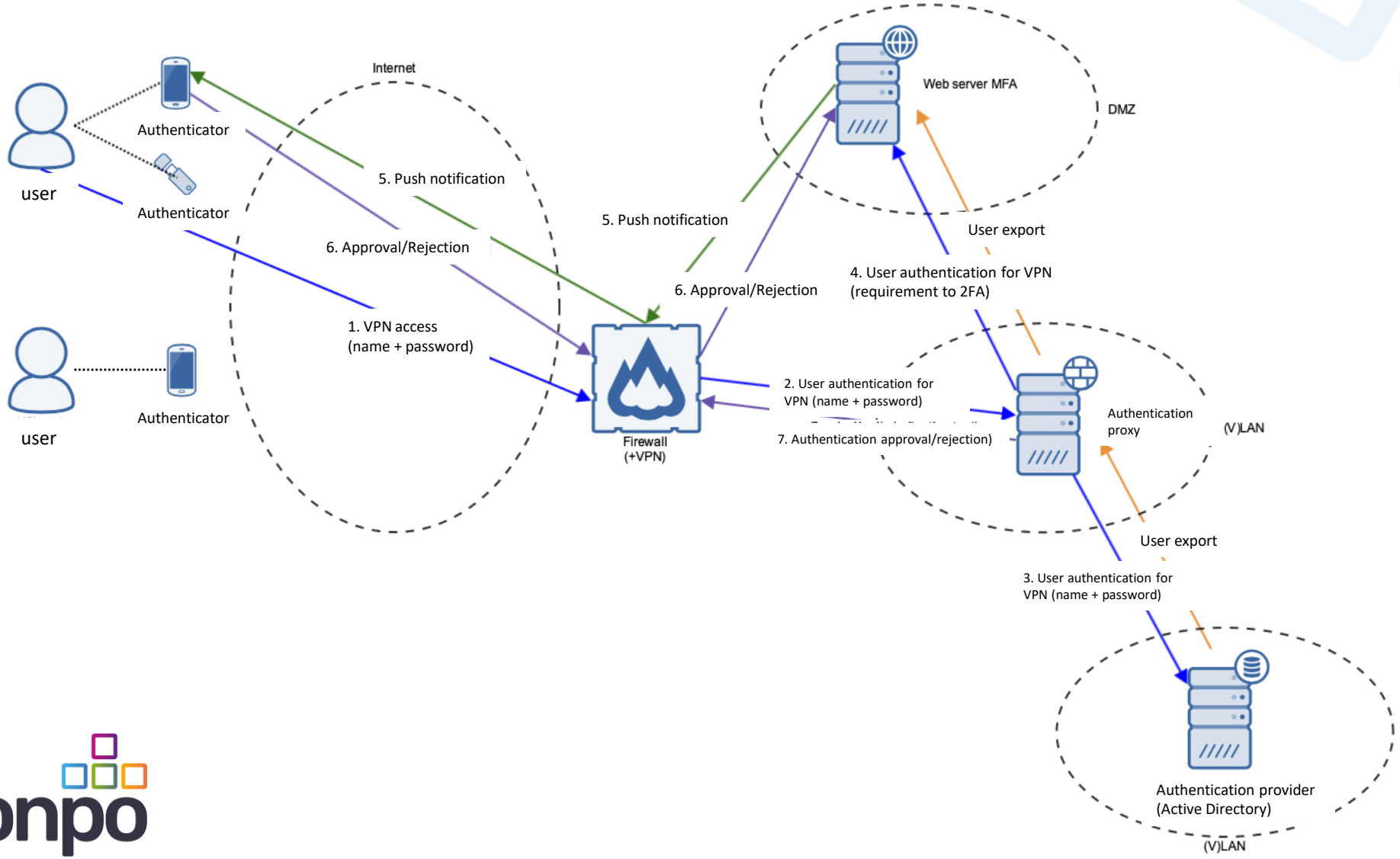
Sonpo

SONPO – Overview of services

- software development (Java, JavaScript, React, Python, .NET)
- security solution SOFiE, 2Element
- installation and administration of Fortinet security products
- installation and administration of servers (Linux, Microsoft)
- implementation of cloud services (AWS, Azure, Digital Ocean)
- infrastructure installation and administration (VMware, KVM, HyperV)
- services, monitoring and helpdesk on a 7/24 basis
- penetration tests
- security audits

Sonpo

MFA - Diagram with an example of VPN login



Sonpo