Best Practices Authpoint – Multifaktor Authentifizierung für Mobile User VPN

Thomas Fleischmann
Senior Sales Engineer CE
Thomas.Fleischmann@watchguard.com

Agenda

- Konzept von AuthPoint
- Herausforderungen bei VPN
  - Auswahl der Methoden
  - Einschränkung durch Protokolle
- Einbindung VPN in AuthPoint
  - Ressource
  - LDAP / AD Anbindung
- *Live Demo*

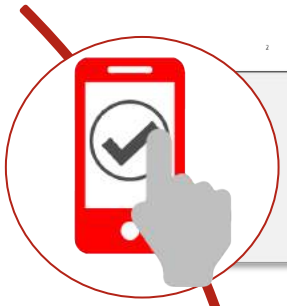
Konzept von AuthPoint

AuthPoint

- AuthPoint ist ein Multi-Faktor-Authentifizierungsdienst, der sich in ihre Firebox- und Drittanbieterdiensten integriert, um Benutzer zu authentifizieren und autorisieren, wenn sie sich bei einer Vielzahl von Anwendungen oder Diensten anmelden.

- Begriffserklärung findet man unter
  - https://de.wikipedia.org/wiki/Authentifizierung
  - https://de.wikipedia.org/wiki/Autorisierung

WatchGuard AuthPoint - MFA Das ist **wirklich** einfach



Multi-Factor Authentication

Password | Push Message | Phone Biometrics | Mobile Phone DNA

AuthPoint Mobile App

iOS & Android | 11 Sprachen | OTP | QR Code | Multiple Authenticators

WatchGuard Cloud

Visibility | Configuration | Management | Token-Zuweisung in Sekunden

Umfangreiche MFA-Abdeckung

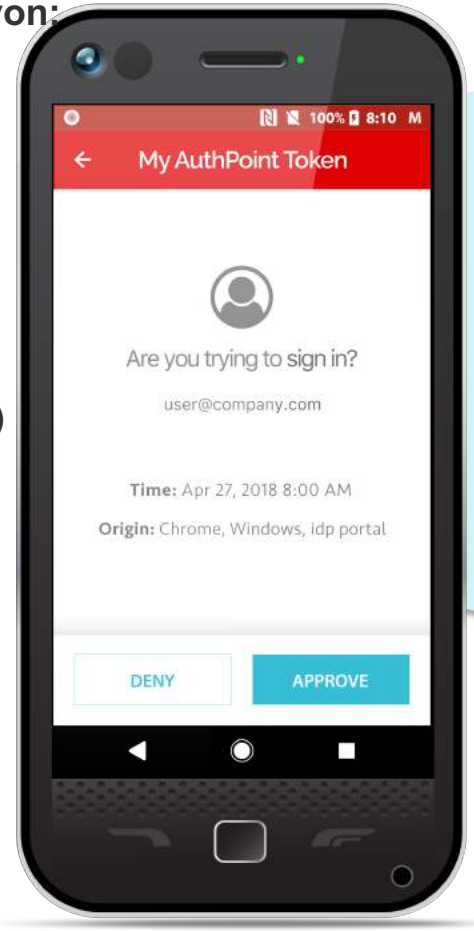
Dutzende von 3rd Party Integrationen | Web SSO | Windows/Mac Computer Logon

Was ist Multi-Faktor-Authentifizierung?

Verwendung von 2 oder mehr Authentifizierungsfaktoren von:

- **Etwas, das du kennst** (Passwort, PIN)
- **Etwas, das du hast** (Token, Handy)
- **Etwas, was du bist** (Fingerabdruck, Gesicht)

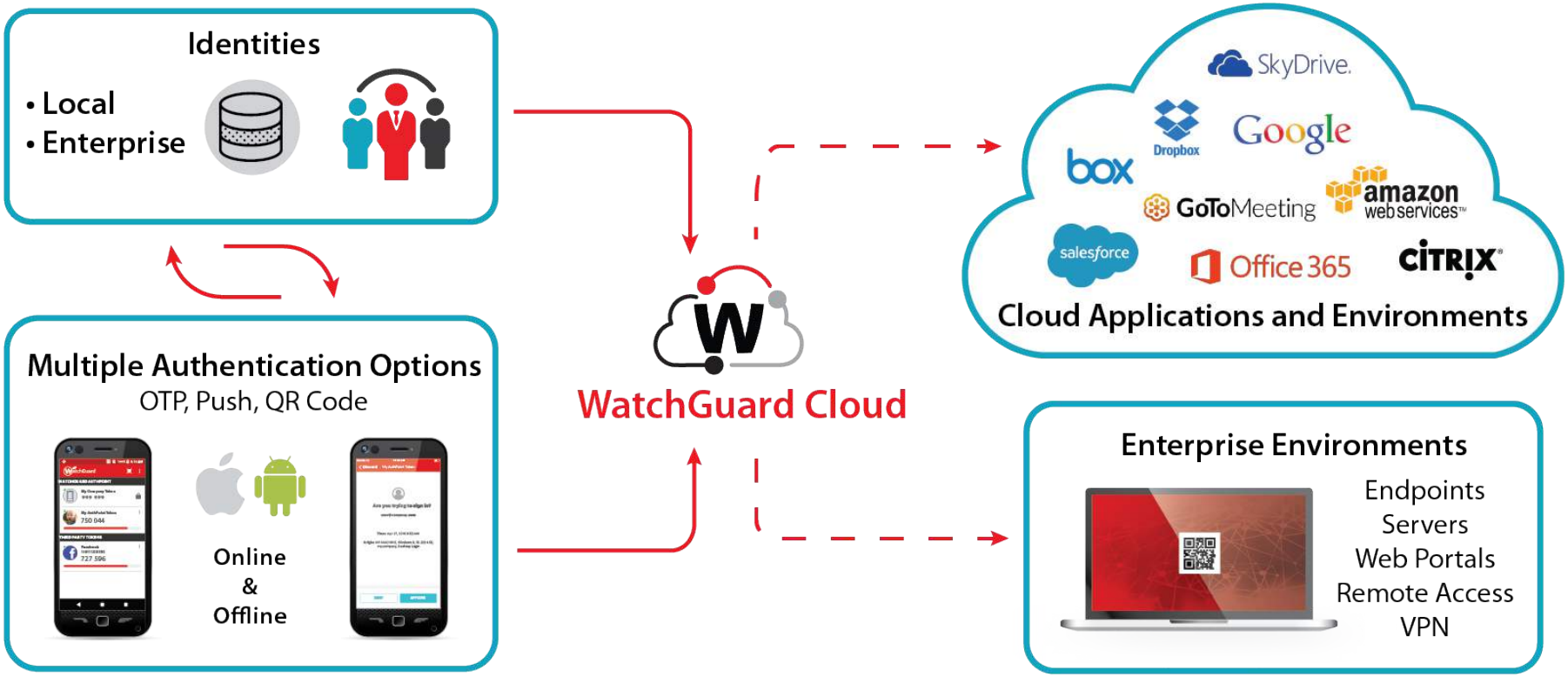
Password



AuthPoint-Faktoren:

1. **Ihr Passwort**
2. **Genehmigung für Ihren mobilen Authentifikator**
3. **Korrekte Handy-DNA**
4. **Ein Fingerabdruck für den Zugriff** (mit bestimmten Telefonmodellen)

Schützt VPNs, Web Apps, PC-Anmeldung und mehr!



AuthPoint Konzept

- Kontext User – Gruppen – Ressourcen
  - User werden über die Email Adresse eindeutig im System zugeordnet.
  - User sind immer Bestandteil einer einzigen Gruppe.
  - Die Gruppe muss vor dem User angelegt werden.
  - Die Gruppe definiert, welche Ressourcen wie verwendet werden (Access Policy).
  - In den Ressourcen werden die technischen Gegebenheiten definiert.
  - Ressourcen können sein:
    - IdP Portal
    - RADIUS
    - SAML
    - Logon-App
    - ADFS
    - ***External Identities*** *(LDAP)*

RESOURCES	RESOURCE TYPE
Access Portal	SAML
groupName	RADIUS
Salesforce	SAML
WGDCE	IDP_PORTAL
LogonApp	DESKTOP_LOGON

AuthPoint User

- Wählen Sie eine Methode aus, um AuthPoint-Benutzerkonten hinzuzufügen:
  - Manuell - Klicken Sie auf in der Users UI auf Add User
  - Automatisch - Geben Sie eine LDAP-Datenbank an, in der Benutzerkonten gespeichert und mit AuthPoint synchronisiert werden können

- Jedes Benutzerkonto:
  - Muss einer Gruppe zugewiesen sein
  - Kann nur in einer Gruppe enthalten sein
  - Muss einen eindeutigen Benutzernamen und eine E-Mail-Adresse haben

- AuthPoint sendet eine E-Mail an den Benutzer mit Anweisungen zum Aktivieren eines Authentifizierungstokens

Herausforderungen bei VPN

Auswahl der Methoden

- Bei Verwendung von AuthPoint im Bereich VPN Anmeldung sind folgende Punkte zu betrachten.

  a. Welches Authentifizierungsverfahren nutze ich für meine VPN Anmeldung?
  b. Welches Protokoll nutze ich für meine Einwahl?

Auswahl der Methoden

Welches Authentifizierungsverfahren nutze ich für meine VPN Anmeldung?

- Bei der Definierung einer RADIUS Client Ressource muss man sich bei der Erstellung einer Access Policy auf eine der beiden Anmelde Möglichkeiten entscheiden.
  - Push
  - OTP
- Was ist der Unterschied?
- Was ist der Vor- und Nachteil der Verfahren?

Welches Protokoll nutze ich für meine Einwahl?

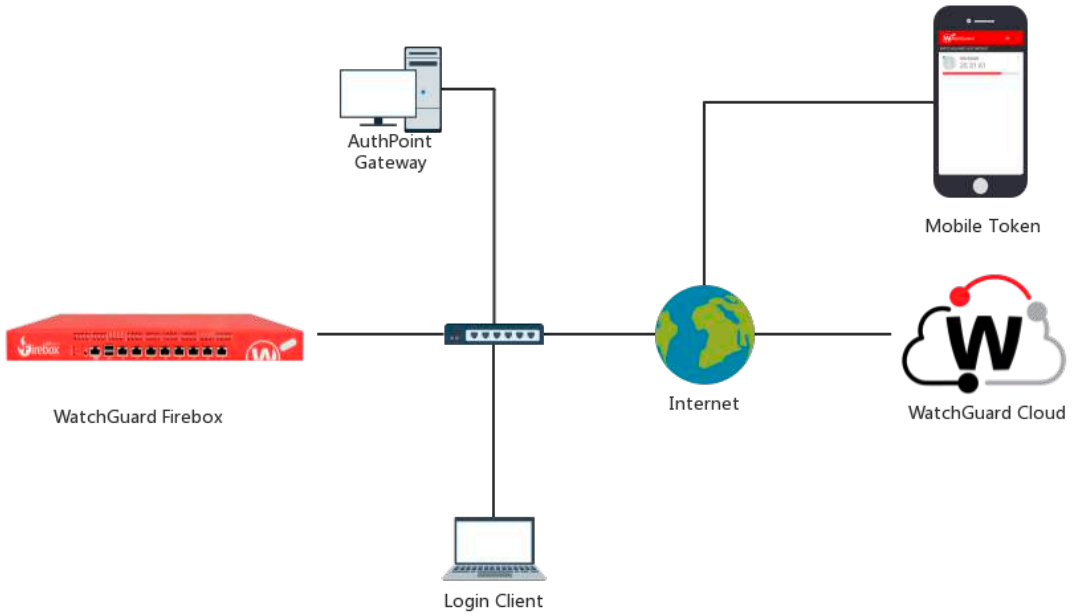
Welches Protokoll nutze ich für meine Einwahl?

- Mobile VPN with IPSec
- Mobile VPN with SSL
- Mobile VPN with L2TP
- Mobile VPN with IKEv2

Was ist der Vor- und Nachteil der Protokolle?

- Nur IPSec oder SSL können zusammen mit LDAP / AD Integration verwendet werden.

Einbindung VPN in AuthPoint



Ressourcen - RADIUS

- RADIUS-Ressourcen werden am häufigsten für Firewalls (hauptsächlich für VPNs) verwendet.

- RADIUS-Ressourcen müssen über einen gemeinsamen geheimen Schlüssel verfügen, damit der RADIUS-Server (AuthPoint Gateway) und der RADIUS-Client (die Firewall) miteinander kommunizieren können.

- RADIUS-Ressourcen müssen mit einem Gateway verknüpft sein.

External Identities

- External Identities interagieren mit externen Benutzerdatenbanken, um Benutzerinformationen zu erhalten und Passwörter zu überprüfen.

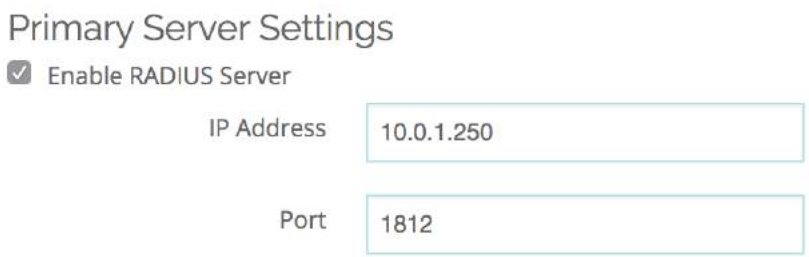
- Im Konfiguration-Menü „ **External Identities** “ können Sie die Einstellungen für Verbindungen zu Ihrem LDAP-Server konfigurieren.

External Identities

- AuthPoint sendet Abfragen an Ihre LDAP-Datenbank, um Benutzerkontoinformationen für die Authentifizierung mit AuthPoint abzurufen.
  - Das Gateway muss in der Umgebung installiert sein.
  - Sie können eine Abfrage ausführen, um LDAP-Benutzerkonten zu AuthPoint hinzuzufügen.
  - Wenn Sie die Benutzerkontoinformationen in Ihrem LDAP-Server ändern, werden sie bei einer Synchronisierung automatisch in AuthPoint aktualisiert.
  - Sie können eine Synchronisierung von Benutzerkonten manuell initiieren.

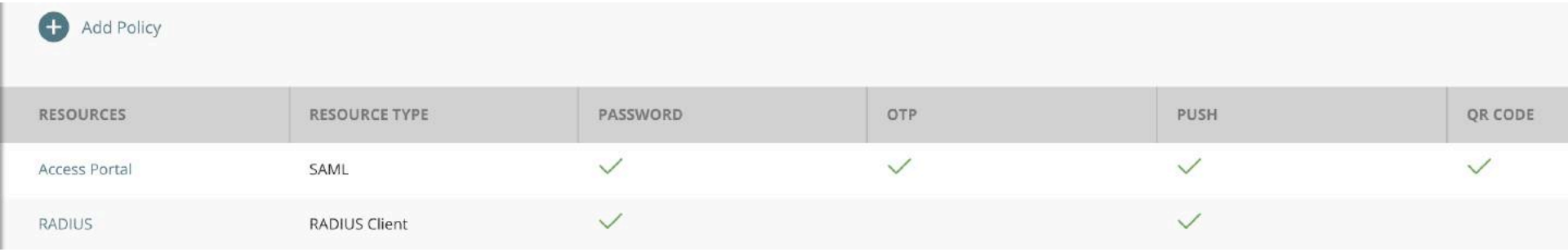
Konfigurations Schritte

- Auf der Firebox
  - Konfiguration der RADIUS Authentication
    - Wichtig: IP Adresse des AuthPoint Gateway angeben
  - Konfiguration des Mobile User VPN
    - Der Name dieser Gruppe muss mit dem Namen der AuthPoint-Gruppe oder Active Directory-Gruppe übereinstimmen, zu der Ihre Benutzer gehören.
    - Wenn Sie den Standardnamen der SSLVPN-Benutzergruppe verwenden, müssen Sie eine SSLVPN-Benutzergruppe zu AuthPoint oder Active Directory hinzufügen.



Konfigurations Schritte

- In AuthPoint
  - Eine RADIUS Ressource hinzufügen
    - Wichtig: Name !
    - Interne IP der Firebox angeben.
  - Eine Access Policy definieren
    - Wichtig: Push oder OTP
  - Die RADIUS Ressource zum Gateway hinzufügen
    - Port beachten




Live Demo


Danke