



Zaawansowane uwierzytelnianie. Bezpieczeństwo, czy wygoda?

Dariusz Leonarski

Konsultant (senior)

Dariusz.Leonarski@microfocus.com

Rozwiązania Micro Focus



**Linux and Open
Source**



**IT Operations
Management**



**Mainframe
Solutions**



**Collaboration
& Networking**



**COBOL &
Application
Modernization**



**Identity, Access
and Security**



**Automated
Software
Quality**

Access is Secure

Every Company Knows this Fundamental Truth



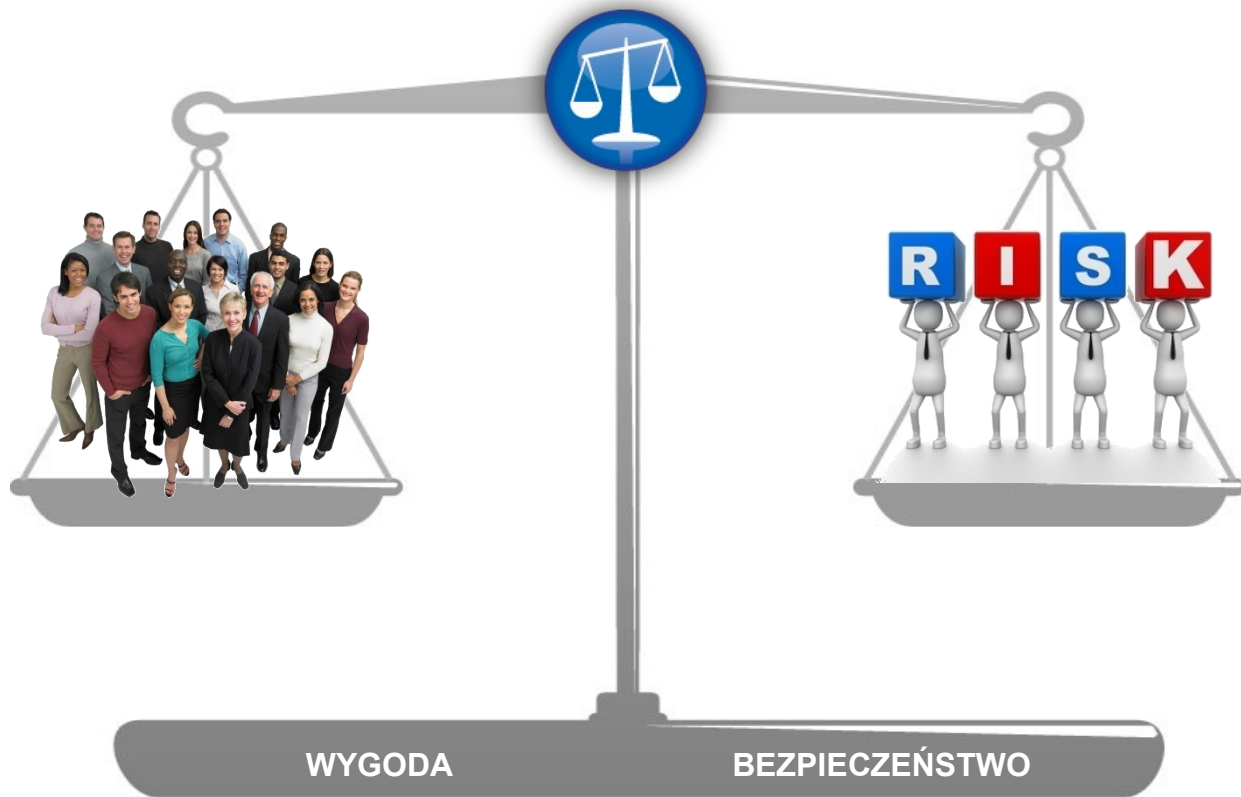
"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

Do której kategorii zalicza się Twoja firma?



Wyzwanie



Advanced Authentication

dawniej NetIQ Advanced Authentication Framework (NAAF)

Mocne uwierzytelnienie

Podstawy

Uniwersalny Model

- “Coś co wiesz”
 - Powszechnie używane
 - Hasła, frazy dostępowe, pytania bezpieczeństwa
- “Coś co posiadasz”
 - Popularne z powodu wielofunkcyjności
 - Karty, tokeny, U2F
- “Coś czym jesteś”
 - Atrybut fizyczny użytkownika
 - Odcisk palca, tęczówka, twarz, bicie serca



Hasła – wspólny problem

Users are the weakest link - Passwords are a close second

- Hasła są wszędzie
 - znakomita większość aplikacji wciąż używa haseł lub... nie używa autoryzacji
- Używanie haseł jest bolesne
 - użytkownicy używają słabych haseł
 - użytkownicy używają starych haseł lub je „synchronizują”
- Hasła są słabym zabezpieczeniem bez względu na ich złożoność
 - około roku 2000 złamanie 8-znakowego hasła zajmowało nawet 100 dni przy pomocy najlepszego sprzętu.
 - aktualnie to samo zadanie zajmuje 10 dni przy pomocy laptopa i oprogramowania znalezionej przez Google
 - czy Wasi pracownicy/użytkownicy zmieniają hasła co 9 dni?



Hasła – wspólny problem

Users are the weakest link - Passwords are a close second

- Hasła są zmorą administratorów
- Kontrola dostępu jest koszmarem z punktu widzenia zgodności z regulacjami
- Rozwiązania firmowe mają zaporowe ceny...
- ...no i nie pasują do każdej sytuacji (użytkownika, aplikacji, urządzenia, lokalizacji)



Co gorsze, administratorzy i Help Desk - ci którzy mają dbać o bezpieczeństwo - bardzo często łamią reguły, aby zadowolić użytkowników.

Advanced Authentication

Użytkownicy chcą mieć dostęp skądkolwiek, kiedykolwiek i z dowolnego urządzenia

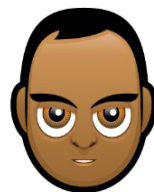


Użytkownicy:

- nie wyglądają tak samo
- nie mają takich samych ról i uprawnień
- nie korzystają z takich samych urządzeń
- nie łączą się z tego samego miejsca
- są różni i mają różne potrzeby

Advanced Authentication

Nie musimy traktować wszystkich użytkowników tak samo



Użytkownicy:

- nie wyglądają tak samo
- nie mają takich samych ról i uprawnień
- nie korzystają z takich samych urządzeń
- nie łączą się z tego samego miejsca
- są różni i mają różne potrzeby

Więc dlaczego próbujemy używać tych samych zabezpieczeń dla każdego?

Advanced Authentication

Jedna platforma z bogactwem metod



ADVANCED AUTHENTICATION SERVER v5.2

System pozwalający wykorzystać wiele różnych metod uwierzytelnienia, aby sprostać różnym wymaganiom bezpieczeństwa.

Advanced Authentication

Łatwość instalacji, administracji i konfigurowania rejestracji użytkowników

Czym jest Advanced Authentication Framework?



ADVANCED AUTHENTICATION SERVER v5.2

- Gotowa do użycia wirtualna maszyna (appliance) oparta na linuxie
- Niski koszt (licencja na użytkownika)
- Skalowalne do użytku wewnętrznego lub w chmurze
- Centralna administracja wieloma czynnikami uwierzytelniającymi
- Oparty na przeglądarce portal do inicjalizacji danych uwierzytelniających (enrollment)
- Daje możliwość wykorzystania wielu czynników uwierzytelniających w jednym rozwiązaniu

Advanced Authentication

Remote Access Edition

FIDO U2F	Voice Call	Email OTP	Smartphone	Smartphone
“Fast IDentity Online” For All Browsers	Voice Call With user PIN Validation	One Time Password Emailed	Out of Band iOS, Andriod and Windows	Geolocation Returned from Smartphone
HSM	PIN Code	Soft Token	Soft Token	Emergency
Hardware Security Module	User Enrolled PIN Code As a Factor	Time Based OTP Any OATH TOTP	Event Based OTP - Any OATH HOTP	Help Desk Assisted Password
SMS	Challenge	Hard Token	Hard Token	LDAP Password
Short Message Service	User Enrolled Question Answers	Time Based OTP Any OATH TOTP	Event Based OTP- Any OATH HOTP	User LDAP Password As a Factor

ADVANCED AUTHENTICATION SERVER v5.2

Remote Access Edition

- Obejmuje metody dla urządzeń nie podłączonych bezpośrednio
- Najczęściej wykorzystuje smartfony, tokeny i inne popularne metody
- Często używana do zabezpieczenia VPN i sieci oraz aplikacji webowych i RADIUSowych
- Zawiera możliwość integracji z NetIQ Access Manager i Cloud Access

Advanced Authentication

Enterprise Edition

FIDO U2F	Voice Call	Email OTP	Smartphone	Smartphone	Fingerprint	NFC
“Fast Identity Online” For All Browsers	Voice Call With user PIN Validation	One Time Password Emailed	Out of Band iOS, Andriod and Windows	Geolocation Returned from Smartphone	Windows Biometric Framework	13.56 MHz - Cards, Tokens, Phones, etc.
HSM	PIN Code	Soft Token	Soft Token	Emergency	Fingerprint	RFID
Hardware Security Module	User Enrolled PIN Code As a Factor	Time Based OTP Any OATH TOTP	Event Based OTP - Any OATH HOTP	Help Desk Assisted Password	Lumidigm Direct Integration	125 KHz - Cards, Tokens, Phones, etc.
SMS	Challenge	Hard Token	Hard Token	LDAP Password	Fingerprint	PKI
Short Message Service	User Enrolled Question Answers	Time Based OTP Any OATH TOTP	Event Based OTP - Any OATH HOTP	User LDAP Password As a Factor	NEXT Biometric Direct Integration	SmartCard or Other (CRL + PIN)

ADVANCED AUTHENTICATION SERVER v5.2

Enterprise Edition

- Zawiera wszystko to co Remote Access Edition
- Ponadto wspiera urządzenia podłączone (karty, biometrikę)
- Wspiera Windows Credential Provider Login
- Wspiera Mac OS X Login (przy pomocy “Remote Access”)
- Często używane do zabezpieczenia systemów i podwyższenia poziomu zabezpieczeń

Advanced Authentication

Enterprise Edition - przyszłość

FIDO U2F "Fast Identity Online" For All Browsers	Voice Call Voice Call With user PIN Validation	Email OTP One Time Password Emailed	Smartphone Out of Band iOS, Andriod and Windows	Smartphone Geolocation Returned from Smartphone	Fingerprint Windows Biometric Framework	NFC 13.56 MHz - Cards, Tokens, Phones, etc.	Fingerprint Digital Persona and Authentec Direct Integration	Kerberos Ticket checking As a Factor
HSM Hardware Security Module	PIN Code User Enrolled PIN Code As a Factor	Soft Token Time Based OTP Any OATH TOTP	Soft Token Event Based OTP - Any OATH HOTP	Emergency Help Desk Assisted Password	Fingerprint Lumidigm Direct Integration	RFID 125 KHz - Cards, Tokens, Phones, etc.	Voice Bio Voice Recognition (via Nuance)	LDAP Support for Any LDAP User Identity Store
SMS Short Message Service	Challenge User Enrolled Question Answers	Hard Token Time Based OTP Any OATH TOTP	Hard Token Event Based OTP - Any OATH HOTP	LDAP Password User LDAP Password As a Factor	Fingerprint NEXT Biometric Direct Integration	PKI SmartCard or Other (CRL + PIN)	Face Biometric Facial Recognition	Live Ensure Support of Third Party Live Ensure

ADVANCED AUTHENTICATION SERVER v5.2

Plany

- Zwiększone możliwości pracy w chmurze
- Nowe wersje aplikacji na iOS, Android i Windows Mobile
- Dodatkowe metody uwierzytelniania
- Integracja z Linux PAM
- Jeszcze więcej integracji z produktami firm trzecich

Advanced Authentication

Podnieść bezpieczeństwo nie dobijając użytkowników

Co to oznacza dla naszych klientów?

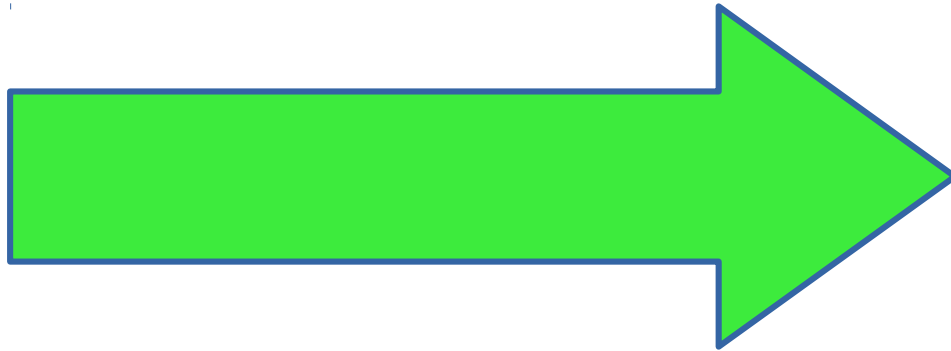
FIDO U2F 	Voice Call 	Email OTP 	Smartphone 	Smartphone 	Fingerprint 	NFC 	Fingerprint 	Kerberos 
HSM 	PIN Code 	Soft Token 	Soft Token 	Emergency 	Fingerprint 	RFID 	Voice Bio 	LDAP 
SMS 	Challenge 	Hard Token 	Hard Token 	LDAP Password 	Fingerprint 	PKI 	Face Biometric 	Live Ensure 

ADVANCED AUTHENTICATION SERVER v5.2

Szeroka paleta możliwości jest kluczem do poprawy bezpieczeństwa.
Dostarcz metody, które są efektywne, a użytkownicy je zaakceptują.

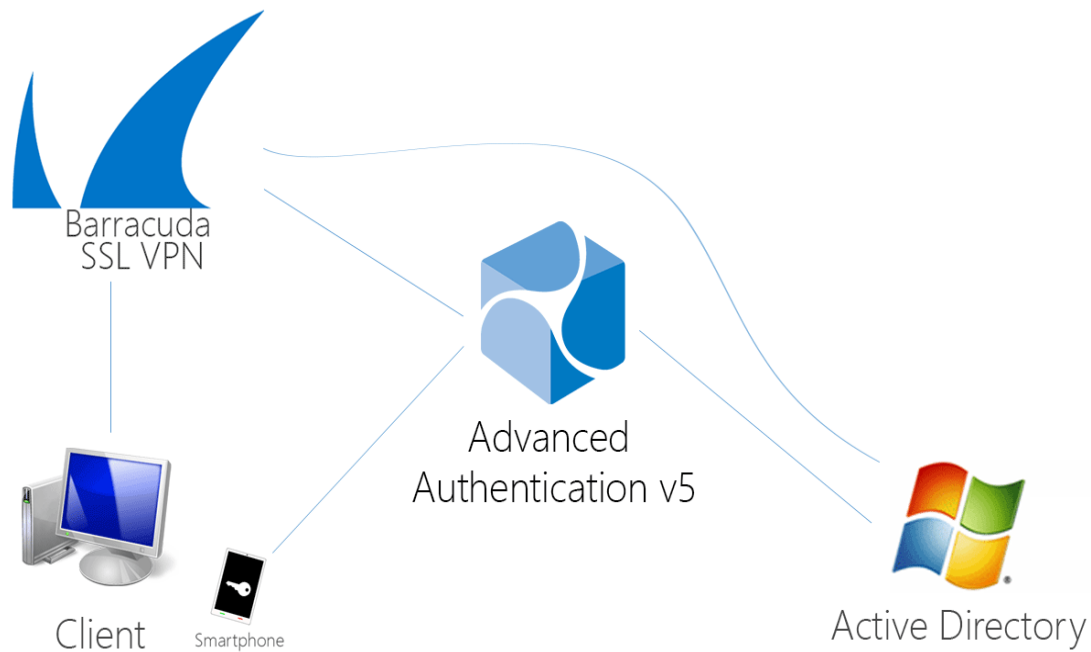
Możesz rozwiązać problemy z uwierzytelnianiem.

Zobaczmy, jak to działa



Advanced Authentication

Szczególne przypadki: Barracuda



Advanced Authentication

Szczególne przypadki: Citrix NetScaler

CITRIX
NetScaler



Client



Smartphone



Advanced
Authentication v5



Active Directory

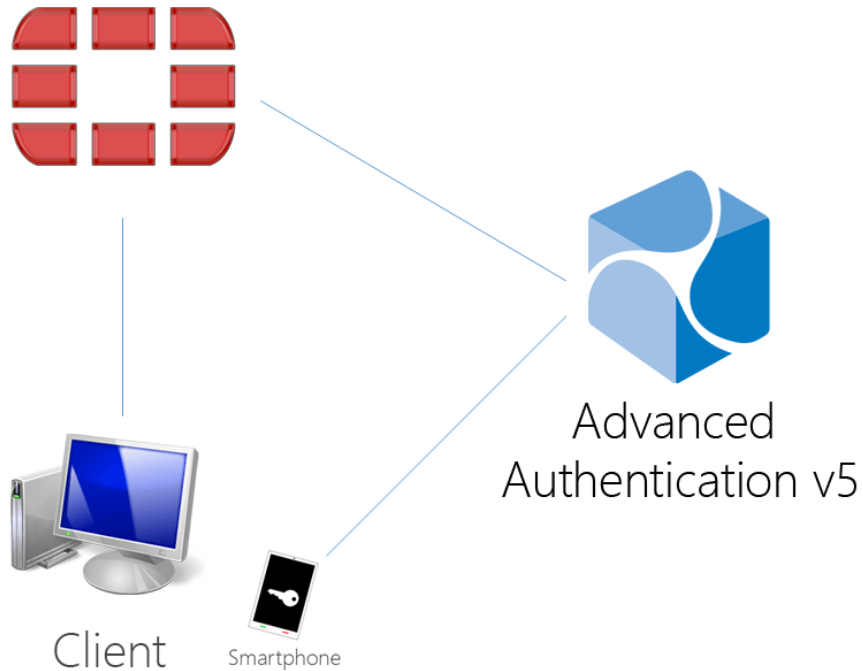
Advanced Authentication

Szczególne przypadki: Dell SonicWALL



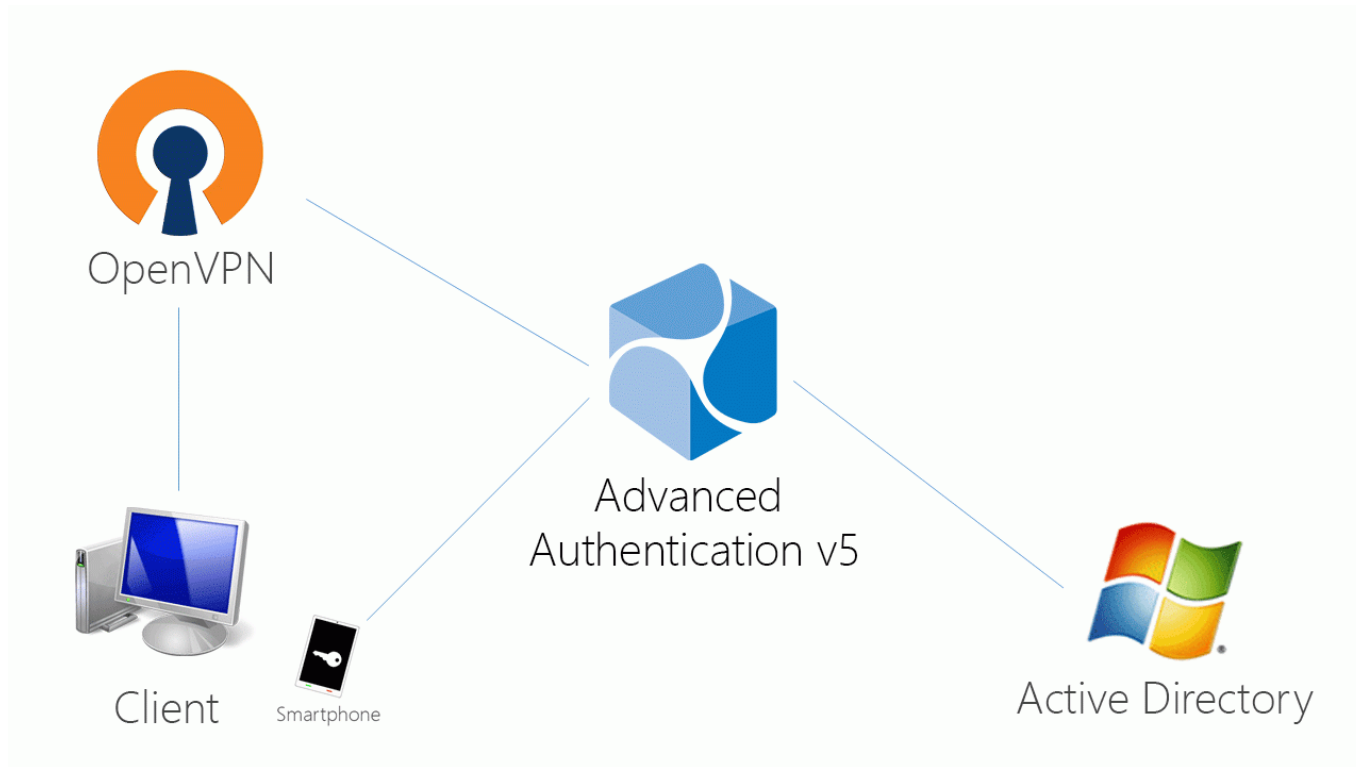
Advanced Authentication

Szczególne przypadki: FortiGate



Advanced Authentication

Szczególne przypadki: Open VPN







www.microfocus.com