

Remote-Authentifizierung – sicher und komfortabel

Mit FortiAuthenticator lanciert Fortinet eine zentrale Instanz für «User Identity Management» und «User Access Control». Die Appliance unterstützt Funktionen wie 2-Faktor-Authentifizierung, Identitätsverifikation und Netzwerkzugriffskontrolle (NAC).

Traditionelle Authentifizierungs- und Autorisierungsmechanismen basieren in der Regel auf der Verwendung von User-Name und Passwort – angesichts des laschen Umgangs mit den persönlichen «Credentials» ein höchst unsicheres Verfahren. Selbst die Verwendung komplexer Passwörter löst das Problem nicht nachhaltig. Sie lassen sich schwer merken, weshalb viele User dieselben Zugangsdaten auf unterschiedlichen Plattformen und Applikationen verwenden. Wird eine dieser Sites gehackt, sind Angriffe auf die verbleibenden Anwendungen ein Leichtes.

Um eine sichere User-Authentifizierung (Überprüfung der Echtheit der berechtigten Person) und User-Autorisierung (Freigabe von Anwendungen gemäss individuell vergebenen Rechten) zu gewährleisten, sind intelligentere Login-Verfahren notwendig («Strong Authentication»). Dazu stellt Fortinet mit FortiAuthenticator eine wegweisende Plattform zur Verfügung. FortiAuthenticator ist eine



FortiAuthenticator erweitert das Security-Produkte-Portfolio von Fortinet mit einem zentralen «User Identity Management» sowie mit «User Access Control»-Funktionen.

zentrale Instanz für die Zugriffssteuerung auf FortiGate-Appliances, auf Systeme von Drittanbietern, Websites und VPN-Zugänge. Sie unterstützt Funktionen wie 2-Faktor-Authentifizierung, Identitätsverifikation und Netzwerkzugriffskontrolle (NAC). Dank der Unterstützung von LDAP und RADIUS, der nahtlosen AD- (Active Directory-) Einbindung sowie der Integration von «Fortinet Single Sign On» in Active Directory stehen umfangreiche Funktionen zur Zugriffskontrolle der Anwender zur Verfügung.

2-Faktor-Authentifizierung mit unterschiedlichen Token

FortiAuthenticator ermöglicht eine wahlweise Unterstützung von Hardware-, Mobile-, SMS- und E-Mail-OTP-Token, die zeitbasierende Einmalpasswörter (OTP) generieren. Da für die Anmeldung eine Kombination aus Wissen (Zugangsdaten) und Besitz (Token) erforderlich ist, verhindern OTPs den unerlaubten Zugriff auf Netzwerk und Applikationen durch Dritte. Zudem bilden sie aufgrund des nur kurzzeitig gültigen Zugangscodes (max. 60 Sek.) einen wirksamen Schutz gegen Keylogger und ähnliche Attacken.

FortiToken Mobile

«FortiToken Mobile», eine App-basierende Client-Software von Fortinet, macht Smartphones und Tablets (iOS, Android) zum mobilen OTP-Token bzw. zum persönlichen Authentifizierungs-Device. Die Open-Authentication-(OATH-)konforme Lösung weist gegenüber herkömmlichen Hardware-Token markante Vorteile auf. Dazu gehören das einfache Rollout und die komfortable Aktivierung von Token bzw. Lizenz ebenso wie die Tatsache, dass keine zusätzliche Hardware notwendig ist. Der Software-Token unterstützt sämtliche Benutzer-Authentifizierungsfunktionen wie VPN (SSL, IPsec), User-Administration und Captive-Portale.

FORTIAUTHENTICATOR-HIGHLIGHTS – EIN AUSZUG

- Starke Authentifizierung und Autorisierung mittels 2-Faktor-Authentifizierung
- AD-Synchronisation (Modifikationen und Zugangsrechte müssen nicht doppelt erfasst werden)
- Einbindung von Drittsystemen via RADIUS und LDAP
- Integration in existierende AD-Infrastrukturen ermöglicht Nutzung identitätsbasierter Regelwerke (Zugriff in Abhängigkeit von Gruppenzugehörigkeiten und Attributen)
- Integrierte CA (Certificate Authority)
- Zertifikatsbasiertes VPN; Unterstützung von USB-Smartcard-Token für die Verwaltung und Speicherung von PKI-Zertifikaten sowie die dazugehörigen privaten Schlüssel
- Fortinet Single Sign On (FSSO) zur Reduktion der Anzahl erforderlicher Logins
- Port Access Control (NAC) verhindert unerlaubte Netzwerk-Zugriffe
- Aufbau von sicheren Wireless-LANs (WPA Enterprise / 802.1x)
- Komfortables Gäste-Management mit Funktionen wie zeitlimitierte Zugriffe und Multi-Site-Unterstützung
- Self-Service-Portal
- Erhältlich als Hardware-Appliance oder VM-Lösung



Firmenname

BOLL Engineering AG,
 Jurastrasse 58, 5430 Wettingen
 Tel. 056 437 60 60,
 info@boll.ch, www.boll.ch