FICHE SOLUTION

FortiAuthenticator™

Gestion des identités utilisateurs et authentification unique

Les systèmes de gestion des identités utilisateurs FortiAuthenticatorTM renforcent la sécurité des entreprises en simplifiant et en centralisant la gestion et le stockage des identifiants.

Politiques d'identité des réseaux professionnels

Au sein d'une entreprise, tous les collaborateurs - ou presque - ont besoin d'accéder au réseau interne et à internet. Ces besoins impliquent des risques qu'il convient de gérer. L'accès au réseau doit être sécurisé et contrôlé, pour permettre à chaque professionnel de disposer des bons accès au bon moment, sans compromettre la sécurité.

Fortinet Single Sign-On permet de fournir une identification sécurisée et un accès au réseau Fortinet adapté aux besoins de chacun. Grâce à son intégration aux systèmes d'authentification Active Directory ou LDAP existants, cette solution protège les identités sans entraver l'expérience utilisateur ni générer de travail supplémentaire pour les administrateurs réseau. FortiAuthenticator reprend les bases de Fortinet Single Sign-on, en intégrant davantage de méthodes d'identification utilisateurs et une plus grande évolutivité. FortiAuthenticator est le gardien de votre réseau professionnel sécurisé Fortinet. Il identifie les utilisateurs, interroge les autorisations d'accès des systèmes tiers et communique ces informations aux appareils FortiGate, pour la mise en place de politiques de sécurité des identités.

FortiAuthenticator mobilise un large éventail de méthodes d'identification :

- Sondage de contrôleur de domaine Active Directory ;
- Intégration avec l'agent de mobilité FortiAuthenticator Single Sign-On, qui détecte les ouvertures de session, les changements d'adresse IP et les déconnexions ; • SAML SP/IdP Web SSO
- Authentification via le portail FSSO avec widgets de suivi, pour moins d'authentifications répétées ;
- Monitoring des enregistrements RADIUS Accounting Start.

FortiAuthenticator Fonctionnalités FSSO

- Mise en place de politiques de sécurité basées sur l'identité et sur les fonctions de chaque professionnel au sein du réseau sécurisé Fortinet, sans authentification supplémentaire, grâce à l'intégration Active Directory
- Simplification et centralisation de la gestion des informations relatives aux identités des utilisateurs, pour une sécurité renforcée

Fonctionnalités complémentaires FortiAuthenticator

- Authentification sécurisée à deux facteurs/OTP avec prise en charge complète des FortiTokens
- Authentification RADIUS et LDAP
- Gestion des certificats pour le déploiement de VPN
  IEEE 802.1X : prise en charge de la sécurisation des réseaux câblés et sans fil

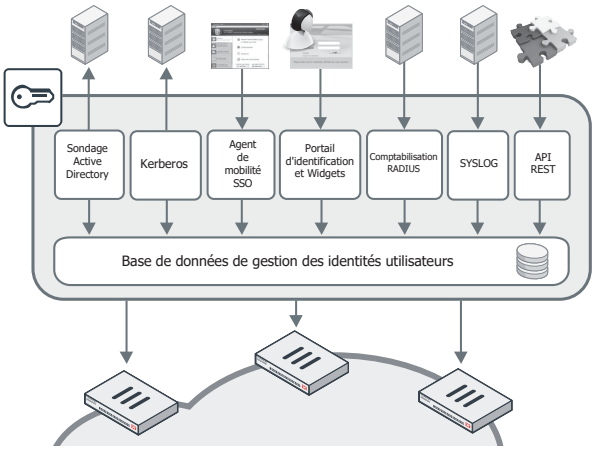
Fonctionnalités

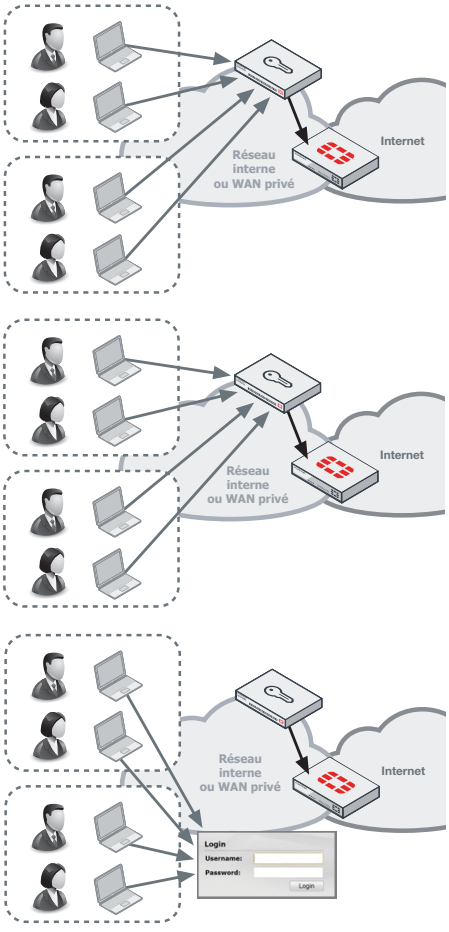
Fonctions-clés

Identification utilisateur FSSO	Aucun impact pour les utilisateurs au sein de l'entreprise.
Intégration LDAP et AD pour (données relatives aux groupes)	Utilise les systèmes existants pour les informations relatives aux autorisations réseau, pour la réduction des délais de déploiement et pour la rationalisation des processus de gestion. Intégration avec les procédures existantes pour la gestion des utilisateurs.
Large éventail de méthodes d'identification utilisateurs	Méthodes souples d'identification pour une intégration dans les environnements professionnels les plus variés.
Activation de la sécurité en fonction de l'identité et les attributions de chacun	Permet à l'administrateur de la sécurité de donner aux utilisateurs l'accès aux ressources réseau et ressources applicatives dont ils ont besoin, tout en conservant le contrôle et en minimisant les risques.

FortiAuthenticator - Identification via l'authentification unique

FortiAuthenticator peut identifier les utilisateurs via plusieurs méthodes. Il peut s'intégrer à des systèmes LDAP ou Active Directory externes pour appliquer des données (relatives aux groupes ou à des rôles) à un utilisateur et transmettre ensuite ces données à FortiGate pour qu'elles soient utilisées dans le cadre des politiques de sécurité. FortiAuthenticator est totalement flexible et peut recourir à plusieurs méthodes différentes. Par exemple, dans une grande entreprise, le sondage AD ou l'agent de mobilité SSO FortiAuthenticator peuvent être choisis comme méthode principale d'authentification, et un basculement vers le portail peut être mis en place pour les systèmes non liés au domaine ou pour les utilisateurs invités.





Sondage Active Directory

L'authentification des utilisateurs sur un répertoire Active Directory est détectée par des contrôleurs de domaine régulièrement interrogés. Lorsqu'une connexion utilisateur est détectée, le nom d'utilisateur, l'IP et les détails du groupe sont ajoutés à la base de données de gestion des identités utilisateurs de FortiAuthenticator. En fonction des politiques de sécurité locales, ces données peuvent être partagées avec plusieurs appareils FortiGate.

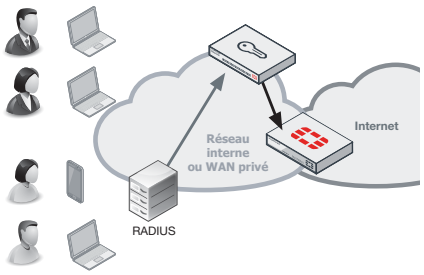
Agent de mobilité FortiAuthenticator SSO

Pour les architectures de domaines distribués complexes où le sondage des contrôleurs de domaine n'est pas possible ou pas souhaitable, le client SSO FortiAuthenticator sert d'alternative. Distribué via FortiClient ou via des installations autonomes pour les PC Windows, ce client communique au FortiAuthenticator les événements liés aux connexions, aux déconnexions et aux changements de couche IP (Câblé > Sans fil, itinérance sur le réseau sans fil), supprimant ainsi la nécessité de sondage.

Portail et widgets FortiAuthenticator

Pour les systèmes ne prenant pas en charge le sondage Active Directory et pour lesquels le recours au client n'est pas possible, FortiAuthenticator fournit un portail d'authentification explicite. Les utilisateurs peuvent ainsi s'authentifier manuellement au niveau du FortiAuthenticator, puis au niveau du réseau. Pour limiter le nombre de connexions répétées nécessaires via l'authentification manuelle, un ensemble de widgets peuvent être intégrés au réseau intranet de l'entreprise, pour connecter automatiquement les utilisateurs via des cookies navigateur, chaque fois qu'ils accèdent à la page d'accueil de l'intranet.

Fonctionnalités



Identification via l'accounting RADIUS

Dans un réseau utilisant l'authentification RADIUS (par exemple, l'authentification sans fil ou VPN), l'accounting RADIUS peut être utilisé comme méthode d'identification. Il permet d'initier la connexion et fournit des informations concernant l'IP et le groupe, ce qui permet de ne pas exiger un second niveau d'authentification.

Fonctionnalité complémentaire

L'authentification à deux facteurs, pour une protection renforcée

FortiAuthenticator procure l'authentification à deux facteurs aux appliances FortiGate ainsi qu'aux appliances tierces prenant en charge l'authentification RADIUS ou LDAP. Les informations relatives à l'identité des utilisateurs de FortiAuthenticator, combinées aux informations d'authentification de FortiToken, garantissent que seules les personnes autorisées puissent accéder aux informations sensibles de votre entreprise. Ce niveau de sécurité supplémentaire réduit considérablement les risques de fuites de données tout en vous aidant à satisfaire aux exigences des réglementations gouvernementales et commerciales en matière de confidentialité. FortiAuthenticator prend en charge la plus large gamme de tokens qui soit, pour répondre aux besoins de vos utilisateurs. Avec FortiToken 200 basé sur le temps, FortiToken Mobile (pour iOS et Android) et les tokens emails/SMS, FortiAuthenticator propose des options pour tous les utilisateurs, pour tous les scénarios. L'authentification à deux facteurs peut être utilisée pour contrôler l'accès à des applications telles que la gestion FortiGate, les VPN SSL et IPsec, les connexions au portail captif sans fil et les équipements réseau tiers conformes aux normes RADIUS. Pour rationaliser la gestion locale des utilisateurs, FortiAuthenticator comprend des fonctions d'auto-enregistrement des utilisateurs et de récupération des mots de passe.

Des VPN reposant sur les certificats

Les VPN site à site permettent d'accéder directement au cœur du réseau depuis de multiples emplacements extérieurs. Souvent, ces VPN sont simplement sécurisés par une clé pré-partagée. Pourtant, si elle est piratée, cette clé peut donner accès à l'ensemble du réseau. FortiOS prend en charge les VPN utilisant les certificats. L'utilisation de ces VPN sécurisés par certificat est souvent limitée, principalement en raison de la complexité de gestion des certificats. FortiAuthenticator élimine ces contraintes en rationalisant les déploiements en masse de certificats. L'utilisation des VPN en environnement FortiGate, en association avec FortiManager, permet la configuration et la délivrance automatisée des certificats sécurisés via le protocole SCEP. Pour les VPN clients, les certificats peuvent être créés et stockés sur le FortiToken 300 USB Certificate store. Cette base de stockage sécurisée des certificats est compatible avec FortiClient et peut être utilisée pour renforcer la sécurité des connexions VPN clients en association avec FortiAuthenticator.

Fonctionnalités complémentaires

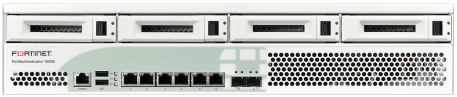
Authentification des utilisateurs RADIUS et LDAP	La base de données d'authentification locale centralise, avec les interfaces RADIUS et LDAP, la gestion des utilisateurs.
Large choix de méthodes d'authentification renforcées	L'authentification renforcée fournie par FortiAuthenticator au moyen de tokens matériels, de courriers électroniques, de SMS, d'e-mails et de certificats numériques contribue à renforcer la sécurité des mots de passe et à minimiser le risque de divulgation, de relecture ou de forçage brutal des mots de passe.
Auto-enregistrement de l'utilisateur et récupération du mot de passe	Réduit les besoins d'intervention de la part de l'administrateur en permettant à l'utilisateur d'effectuer son propre enregistrement et de résoudre ses propres problèmes de mot de passe. La satisfaction des utilisateurs s'en trouve également améliorée.
Intégration avec Active Directory et LDAP	L'intégration avec le répertoire existant simplifie les déploiements, accélère les installations et tire profit des travaux de développement déjà réalisés.
Gestion des certificats	La gestion rationalisée des certificats permet un déploiement rapide et rentable des méthodes d'authentification via certificats, comme les VPN.
Authentification 802.1X	Fournit un contrôle d'accès permettant de valider la connexion des utilisateurs au réseau local et au réseau local sans fil, afin d'empêcher tout accès non-autorisé au réseau.

Spécifications

	FORTIAUTHENTICATOR 200E	FORTIAUTHENTICATOR 400E	FORTIAUTHENTICATOR 1000D
Hardware			
Interfaces 10/100/1000 (Cuivre, RJ-45)	4	4	4
Interfaces SFP	0	0	2
Stockage local	Disque dur 1x 1 To	Disque dur 2x 1 To	Disque dur 2x 2 To
Alimentation électrique	Plage automatique unique 250W (100V-240V)	Plage automatique double (1+0) 300W (100V-240V)	Plage automatique double (1+0) 300W (100V-240V)
Performances système			
Nombre total d'utilisateurs (locaux + distants)	500	2000	10000
FortiTokens	1000	4000	20000
Clients RADIUS (dispositifs NAS)	166	666	3333
Groupes d'utilisateurs	50	200	1,00
Certificats CA	10	10	50
Certificats utilisateurs	2500	10000	50000
Dimensions			
Hauteur x Largeur x Longueur (pouces)	1,75 x 17,05 x 13,86	1,73 x 17,24 x 16,38	3,50 x 17,24 x 14,49
Hauteur x Largeur x Longueur (mm)	45 x 433 x 352	44 x 438 x 416	89 x 438 x 368
Poids	6,1 kg (13,4 lbs)	11,0 kg (25,0 lbs)	12.5 kg (27,6 lbs)
Environnement			
Format	Montable en rack (1RU)	Montable en rack (1RU)	Montable en rack (2 RU)
Source d'alimentation	90–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Courant maximum	4A / 110V, 2A / 220V	5A / 110V, 3A / 220V	5A /110V, 3A /220V
Consommation d'énergie (moyenne)	60 W	102 W	115 W
Dissipation de la chaleur	280 BTU/h	482 BTU/h	471 BTU/h
Température de fonctionnement	0–40°C (32–104°F)	32–104°F (0–40°C)	32–104°F (0–40°C)
Température de stockage	-25–70°C (-13–158°F)	-25–75°C (-13–167°F)	-25–70°C (-13–158°F)
Humidité	5–95% sans condensation	5–95% sans condensation	5–95% sans condensation
Système			
Normes prises en charge	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), Révocation de certificat (RFC3280), Importation de certificat PKCS#12, Importation CSR PKCS#10 (RFC2986), Protocole de statut de certificat en ligne (RFC 2560), EAP-TLS (RFC2716), Protocole d'inscription de certificat simple (SCEP)		
Gestion	CLI, Console directe DB9 CLI, HTTPS	CLI, Console directe DB9 CLI, HTTPS	CLI, Console directe DB9 CLI, HTTPS
Haute disponibilité (HA)	HA active-passive et HA config. sync.	HA active-passive et HA config. sync.	HA active-passive et HA config. sync.
Conformité			
Sécurité	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

FortiAuthenticator 200E

FortiAuthenticator 400E



FortiAuthenticator 1000D

FortiAuthenticator 2000E

FortiAuthenticator 3000E

Appliance virtuelle FortiAuthenticator

Spécifications

	FORTIAUTHENTICATOR 2000E	FORTIAUTHENTICATOR 3000E
Hardware		
Interfaces 10/100/1000 (Cuivre, RJ-45)	4	4
Interfaces SFP	2	2
Stockage local	2x 2 To SAS Drive	2x 2 To SAS Drive
Alimentation électrique	Plage automatique double (1+1) 740W (100V-240V)	Plage automatique double (1+1) 1000W (100V-240V)
Performances système		
Nombre total d'utilisateurs (locaux + distants)	20 000	40 000
FortiTokens	40 000	80 000
Clients RADIUS (dispositifs NAS)	6 666	13 333
Groupes d'utilisateurs	2 000	4 000
Certificats CA	50	50
Certificats utilisateurs	100 000	200 000
Dimensions		
Hauteur x Largeur x Longueur (pouces)	3,50 x 17,20 x 25,50	3,50 x 17,20 x 25,50
Hauteur x Largeur x Longueur (mm)	89 x 437 x 647	89 x 437 x 647
Poids	14,5 kg (32,0 lbs)	18,6 kg (40.0 lbs)
Environnement		
Format	Montage en rack (2 RU)	Montage en rack (2 RU)
Source d'alimentation	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Courant maximum	10A /110V, 4A /220V	10A /110V, 5A /220V
Consommation d'énergie (moyenne)	189 W	347 W
Dissipation de la chaleur	781 BTU/h	1325 BTU/h
Température de fonctionnement	5–35°C (41–95°F)	10–35°C (50–95°F)
Température de stockage	-40–60°C (-40–140°F)	-40–70°C (-40–158°F)
Humidité	8–90% sans condensation	8–90% sans condensation
Système		
Normes prises en charge	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, NTP Client (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), révocation de certificat (RFC3280), importation de certificat PKCS#12, importation CSR PKCS#10 (RFC2986), protocole de statut de certificat en ligne (RFC 2560), EAP-TLS (RFC2716), protocole d'inscription de certificat simple (SCEP)	
Gestion	CLI, Console directe DB9 CLI, HTTPS	CLI, Console directe DB9 CLI, HTTPS
Haute disponibilité (HA)	HA active-passive et HA config. sync.	HA active-passive et HA config. sync.
Conformité		
Sécurité	FCC, ICES, CE, RCM, VCCI, BSMI, UL, CB	FCC Partie 15 Classe A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

APPLIANCES VIRTUELLES	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG	FAC-VM-100000-UG
Capacité					
Utilisateurs locaux	100	+100	+1000	+10 000	+100 000
Utilisateurs à distance	100	+100	+1000	+10 000	+100 000
FortiTokens	200	+200	+2000	+20 000	+200 000
Dispositifs NAS	33	+33	+333	+3333	+33 333
Groupes d'utilisateurs	10	+10	+100	+1000	+10 000
Certificats CA	5	+5	+50	+500	+500
Certificats utilisateurs	100	+100	+1000	+10 000	+100 000
Machine virtuelle					
Hyperviseurs pris en charge	VMware ESXi / ESX 4 / 5 / 6, Microsoft Hyper-V Server 2010, 2012 R2 et 2016, KVM, Xen, Microsoft Azure, AWS				
Nombre maximum de CPU virtuels pris en charge	64				
NIC virtuels requis (minimum / maximum)	1 / 4				
Stockage des machines virtuelles (minimum / maximum)	60 Go / 16 To				
Mémoire de machine virtuelle requise (minimum / maximum)	2 Go / 1 To				
Prise en charge haute disponibilité	HA active-passive et HA config. sync.				

Informations relatives aux commandes

Produit	Référence (SKU)	Description
FortiAuthenticator 200E	FAC-200E	4 ports GE RJ45, 1x 1 To HDD.
FortiAuthenticator 400E	FAC-400E	4 ports GE RJ45, 2x 1 To HDD.
FortiAuthenticator 1000D	FAC-1000D-E07S	4 ports GE RJ45 ports, 2 ports GE SFP, 2x 2 To HDD.
FortiAuthenticator 2000E	FAC-2000E	4 ports GE RJ45, 2 ports GE SFP, 2x 2 To SAS Drive.
FortiAuthenticator 3000E	FAC-3000E	4 ports GE RJ45, 2 ports GE SFP, 2x 2 To SAS Drive.
FortiAuthenticator-VM License	FAC-VM-Base	Machine virtuelle FortiAuthenticator-VM de base avec une licence 100 utilisateurs. VCPU illimité.
	FAC-VM-100-UG	Mise à jour de la licence FortiAuthenticator-VM 100 utilisateurs.
	FAC-VM-1000-UG	Mise à jour de la licence FortiAuthenticator-VM 1000 utilisateurs.
	FAC-VM-10000-UG	Mise à jour de la licence FortiAuthenticator-VM 10 000 utilisateurs.
	FAC-VM-100000-UG	Mise à jour de la licence FortiAuthenticator-VM 100 000 utilisateurs.
	FC1-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-500 utilisateurs).
	FC2-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-1100 utilisateurs).
	FC3-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-5100 utilisateurs).
	FC4-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-10 100 utilisateurs).
	FC8-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-25 100 utilisateurs).
	FC5-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-50 100 utilisateurs).
	FC6-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-100 100 utilisateurs).
	FC9-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-100 100 utilisateurs).
	FC7-10-0ACVM-248-02-12	1 an de contrat FortiCare 24h/24, 7j/7 (1-1 million d'utilisateurs).
Accessoires optionnels		
Alimentation électrique	SP-FAD700-PS	Alimentation en courant alternatif pour FAC-400E.
	SP-FXX1000D-PS	Alimentation en courant alternatif pour FAC-1000D.
	SP-FML2000E-PS	Alimentation en courant alternatif pour FAC-2000E.
	SP-FML3000E-PS	Alimentation en courant alternatif pour FAC-3000E.

www.fortinet.com