FortiAuthenticator™

Správa identít používateľov a jediné prihlásenie

Zariadenia na správu identít používateľov FortiAuthenticator posilňujú podnikovú bezpečnosť zjednodušením a centralizovaním správy a ukladania informácií o identitách používateľov.

Pravidlá správy identít v podnikovej sieti

Prístup k sieti a na internet je rozhodujúci pre takmer každú rolu v rámci spoločnosti. Táto požiadavka však musí byť vyvážená rizikom, ktoré sa s tým spája. Kľúčovým cieľom každej spoločnosti je poskytovať bezpečný, ale zároveň kontrolovaný prístup k sieti, ktorý umožňuje správnej osobe získať správny prístup v správnom čase bez toho, aby sa tým ohrozila bezpečnosť.

Fortinet Single Sign-On je spôsob poskytovania zabezpečeného prístupu k prepojenej sieti Fortinet na základe identít a rol. Integrácia s existujúcimi overovacími systémami Active Directory alebo LDAP umožňuje poskytovať podnikové zabezpečenie založené na identitách používateľov bez obmedzovania používateľa alebo dodatočnej práce pre správcov siete. FortiAuthenticator stavia na základoch systému Fortinet Single Sign-On, rozširuje ponuku spôsobov identifikácie používateľov a zvyšuje úroveň škálovateľnosti. FortiAuthenticator je správca oprávnení pre prístup k zabezpečenej podnikovej sieti Fortinet. Identifikuje používateľov, overuje prístupové práva v systémoch tretích strán a posiela takto získané informácie do zariadení FortiGate, kde sa používajú v rámci politík založených na identitách.

FortiAuthenticator poskytuje transparentnú identifikáciu viacerými spôsobmi:

- posielaním výzvy do radiča domény služby Active Directory,
- integrovaním s funkciou FortiAuthenticator Single Sign-On Mobility Agent, ktorá deteguje prihlásenie, zmeny adresy IP a odhlásenie,
- overením cez portál FSSO s miniaplikáciami sledovania, ktoré znižujú potrebu opakovať overenia,
- monitorovaním záznamov začiatku účtovania pre protokol RADIUS.

Vlastnosti služby FortiAuthenticator FSSO

- Umožňuje používať politiky zabezpečenia na základe identít a rol v zabezpečenej podnikovej sieti Fortinet bez potreby dodatočného overenia cez integráciu so službou Active Directory.
- Posilňuje podnikovú bezpečnosť zjednodušením a centralizovaním správy a ukladania informácií o identitách používateľov.

Ďalšie vlastnosti zariadenia FortiAuthenticator

- Zabezpečené dvojúrovňové alebo OTP overenie s úplnou podporou pre aplikáciu FortiToken
- Overenie RADIUS a LDAP
- Správa certifikátov pre zavedenie podnikovej siete VPN
- Podpora štandardu IEEE802.1X na zabezpečenie káblovej a bezdrôtovej siete
- Webové prihlásenie SAML SP/IdP SSO

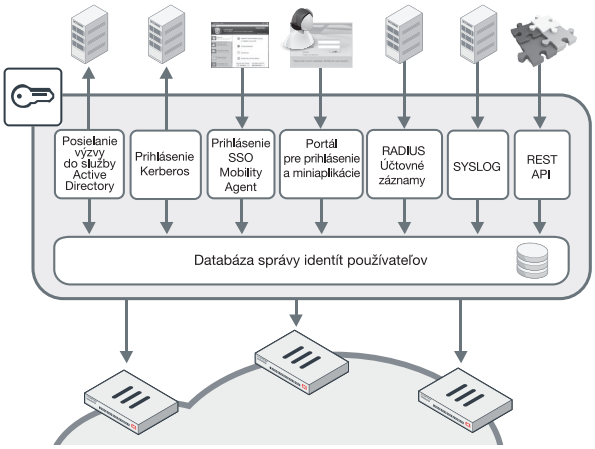
ZÁKLADNÉ VLASTNOSTI

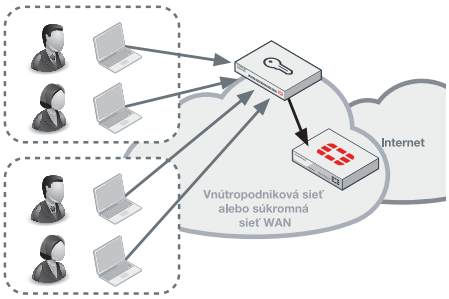
Kľúčové vlastnosti a prínosy

Transparentná identifikácia používateľov FSSO	Nulový dosah na podnikových používateľov.
Integrácia s LDAP a AD pre členstvo v skupine	Využíva existujúce systémy na získavanie informácií o sieťových oprávneniach, skracuje čas nasadenia a zefektívňuje riadiace procesy. Integrácia s existujúcimi postupmi na správu používateľov.
Rôzne spôsoby identifikácie používateľov	Flexibilné spôsoby identifikácie používateľov na integráciu do najrôznejších podnikových prostredí.
Zapnutie zabezpečenia na základe identít a rol	Umožňuje správcovi zabezpečenia poskytnúť používateľom prístup k príslušným sieťovým a aplikačným zdrojom, ktoré sú vhodné pre ich rolu, pri zachovaní kontroly a minimalizovaní rizika.

Spôsoby identifikácie používateľov s jediným prihlásením FortiAuthenticator Single Sign-On

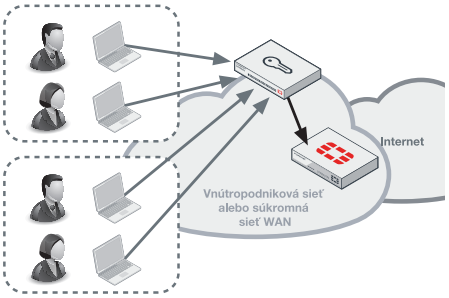
FortiAuthenticator dokáže identifikovať používateľov rôznymi spôsobmi a môže sa integrovať do systémov LDAP alebo Active Directory tretích strán s cieľom použiť údaje o skupine alebo role používateľa a komunikovať so zariadením FortiGate na účely použitia takto získaných informácií v politikách založených na identitách. Zariadenie FortiAuthenticator poskytuje úplnú flexibilitu a dokáže používať tieto možnosti súčasne. Napríklad, vo veľkej spoločnosti môže byť posielanie výzvy do služby AD alebo FortiAuthenticator SSO Mobility Agent nastavené ako hlavný spôsob pre účely transparentného overenia s núdzovým prístupom k portálu pre nedoménové systémy alebo hostí.





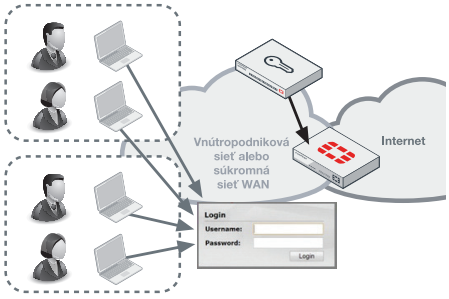
Posielanie výzvy do služby Active Directory

Overenie používateľov v službe Active Directory je detegované pravidelným posielaním výzvy do radičov domény. Po detegovaní prihlásenia používateľa sa meno používateľa, adresa IP a informácie o skupine vložia do databázy na správu identity používateľov FortiAuthenticator a v závislosti od lokálnej politiky sa môžu zdieľať s viacerými zariadeniami FortiGate.



FortiAuthenticator SSO Mobility Agent

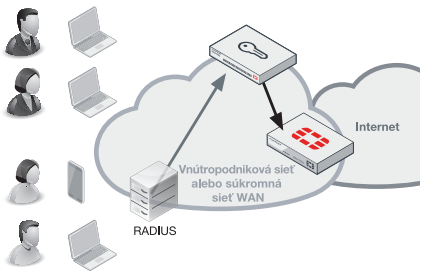
Pri zložitých distribuovaných doménových architektúrach, pri ktorých nie je posielanie výzvy do radičov domény uskutočniteľné alebo žiaduce, je alternatívnym riešením klient FortiAuthenticator SSO. Klient je distribuovaný ako súčasť systému FortiClient alebo ako samostatná inštalácia pre osobné počítače so systémom Windows a posiela informácie o prihlásení, zmene súboru protokolov IP (káblové pripojenie > bezdrôtové pripojenie, roaming v bezdrôtovej sieti) a udalostiach odhlásenia do zariadenia FortiAuthenticator, čím sa eliminuje potreba posielať výzvy.



Portál FortiAuthenticator a miniaplikácie

V prípade systémov, ktoré nepodporujú posielanie výzvy do služby AD, prípadne ak použitie klienta nie je uskutočniteľné, FortiAuthenticator poskytuje explicitný overovací portál. Používateľom umožňuje manuálne overiť svoju identitu v zariadení FortiAuthenticator a následne v sieti. S cieľom minimalizovať vplyv opakovaných prihlásení, ktoré sú vyžadované pri manuálnom overovaní, je dostupný balík miniaplikácií, ktoré sa začlenia do intranetu organizácie a automaticky prihlasujú používateľov pomocou súborov cookie prehliadača pri každom otvorení domovskej stránky na intranete.

ZÁKLADNÉ VLASTNOSTI



Prihlásenie sa pomocou služby RADIUS Accounting

V sieti, kde sa používa overenie RADIUS (napríklad overenie v bezdrôtovej sieti alebo v sieti VPN), sa služba RADIUS Accounting môže používať ako spôsob identifikácie používateľov. Tieto údaje sa používajú na aktivovanie prihlásenia používateľov a na poskytnutie informácie o adrese IP a skupine, čím sa eliminuje potreba druhej úrovne overenia.

Ďalšie funkcie

Silná používateľská identita s dvojúrovňovým overením

FortiAuthenticator rozširuje funkciu dvojúrovňového overenia na niekoľko zariadení FortiGate a na riešenia tretích strán, ktoré podporujú overenie RADIUS alebo LDAP. Informácie o identite používateľa zo zariadenia FortiAuthenticator v spojení s informáciou o overení z aplikácie FortiToken sú zárukou, že prístup k citlivým informáciám spoločnosti bude poskytnutý iba oprávneným osobám. Táto dodatočná vrstva zabezpečenia výrazne znižuje riziko úniku údajov a zároveň pomáha spoločnostiam spĺňať požiadavky na audit v súvislosti s vládnymi a internými predpismi týkajúcimi sa ochrany osobných údajov. FortiAuthenticator podporuje najširšiu ponuku tokenov pre rôzne potreby používateľov. FortiAuthenticator spolu s fyzickým časovým zariadením FortiToken 200, aplikáciou FortiToken Mobile (pre iOS a Android), e-mailovými a SMS tokenmi poskytuje rôzne tokeny pre akéhokoľvek používateľa a scenár. Dvojúrovňové overenie sa môže používať na riadenie prístupu k aplikáciám, ako sú napríklad správa zariadení FortiGate, SSL a IPsec VPN, prihlásenie do systému Wireless Captive Portal a sieťové zariadenia tretích strán s podporou protokolu RADIUS.

FortiAuthenticator ponúka funkcie na vlastnú registráciu používateľov a obnovenia hesla, ktoré zjednodušujú správu lokálnych používateľov.

Podnikové siete VPN založené na certifikátoch

Siete VPN spájajúce lokality často poskytujú prístup priamo do jadra podnikovej siete z mnohých vzdialených miest. Takéto siete VPN sú často zabezpečené iba vopred poskytnutým kľúčom, ktorý môže v prípade prezradenia poskytnúť prístup do celej siete. FortiOS podporuje siete VPN založené na certifikátoch. Siete VPN zabezpečené certifikátom sa však využívajú iba v obmedzenej miere, najmä z dôvodu réžie a zložitosti súvisiacej so správou certifikátov. FortiAuthenticator odstraňuje takúto réžiu zjednodušením hromadného nasadenia certifikátov na použitie so sieťami VPN v prostredí FortiGate prostredníctvom spolupráce so zariadením FortiManager na konfiguráciu a automatizáciu zabezpečeného doručovania certifikátov cez protokol SCEP.

Pre siete VPN s klientskymi certifikátmi sa certifikáty môžu vytvárať a uložiť na USB kľúč pre certifikáty FortiToken 300. Kľúč je chránený kódom PIN, kompatibilný s formátom FortiClient a v spojení so zariadením FortiAuthenticator sa používa na zvýšenie bezpečnosti pripojenia klientov k sieti VPN.

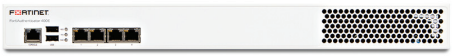
Ďalšie vlastnosti a prínosy

Overenie používateľov cez službu RADIUS a LDAP	Lokálna databáza overovania s rozhraniami RADIUS a LDAP centralizuje správu používateľov.
Rôzne spôsoby silného overovania	Silné overovanie poskytované zariadením FortiAuthenticator pomocou hardvérových tokenov, e-mailu, SMS a e-mailových a digitálnych certifikátov pomáha zvýšiť bezpečnosť hesiel a znižuje riziko prezradenia hesla, opakovaného prehrávania alebo útoku hrubou silou.
Vlastná registrácia a obnovenie hesla používateľov	Znižuje potrebu zásahov správcu tak, že umožňuje používateľom vykonať registráciu a vyriešiť vlastné problémy s heslom, čo zároveň vedie aj k zvýšeniu spokojnosti používateľov.
Integrácia so službami Active Directory a LDAP	Integrácia s existujúcim adresárom zjednodušuje nasadenie, skracuje čas inštalácie a umožňuje využívať existujúce zdroje.
Správa certifikátov	Zjednodušená správa certifikátov umožňuje rýchle a nákladovo efektívne nasadenie spôsobov overovania založených na certifikátoch, ako je napríklad VPN.
Overenie 802.1X	Rozhodnite sa pre podnikové riadenie prístupu k portom na overenie pripojenia používateľa k sieti LAN a bezdrôtovej sieti LAN s cieľom zabrániť nepovolenému prístupu k sieti.

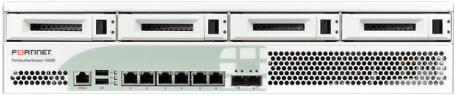
ŠPECIFIKÁCIE

	FORTIAUTHENTICATOR 200E	FORTIAUTHENTICATOR 400E	FORTIAUTHENTICATOR 1000D
Hardvér			
Rozhrania 10/100/1000 (medené, RJ-45)	4	4	4
Rozhrania SFP	0	0	2
Lokálne úložisko	1x pevný disk s kapacitou 1 TB	2x pevný disk s kapacitou 1 TB	2x pevný disk s kapacitou 2 TB
Zdroj napájania	Jeden 480 W s automatickou detekciou napätia (100 V – 240 V)	Dva 480 W s automatickou detekciou napätia (100 V – 240 V)	Dva 480 W s automatickou detekciou napätia (100 V – 240 V)
Výkonové údaje systému			
Celkový počet používateľov (lokálni + vzdialení)	500	2 000	10 000
Tokeny FortiToken	1 000	4 000	20 000
Klienti služby RADIUS (zariadenia NAS)	166	666	3 333
Skupiny používateľov	50	200	1 000
Certifikáty CA	10	10	50
Používateľské certifikáty	2 500	10 000	50 000
Rozmery			
Výška × šírka × dĺžka (v palcoch)	1,75 × 17,05 × 13,86	1,73 × 17,24 × 16,38	3,50 × 17,24 × 14,49
Výška × šírka × dĺžka (v mm)	45 × 433 × 352	44 × 438 × 416	89 × 438 × 368
Hmotnosť	13,4 libier (6,1 kg)	25,0 libier (11,0 kg)	27,6 libier (12,5 kg)
Prostredie			
Veľkosť	Stojanový (1 RU)	Stojanový (1 RU)	Stojanový (2 RU)
Napájanie	90 – 240 V~, 50 – 60 Hz	100 – 240 V~, 50 – 60 Hz	100 – 240 V~, 50 – 60 Hz
Maximálny prúd	4 A pri 110 V, 2 A pri 220 V	5 A pri 110 V, 3 A pri 220 V	5 A pri 110 V, 3 A pri 220 V
Spotreba energie (priemerná)	60 W	102 W	115 W
Odvádzanie tepla	280 BTU/hod.	482 BTU/hod.	471 BTU/hod.
Pracovná teplota	32 – 104 °F (0 – 40 °C)	32 – 104 °F (0 – 40 °C)	32 – 104 °F (0 – 40 °C)
Teplota uskladnenia	-13 – 158 °F (-25 – 70 °C)	-13 – 167 °F (-25 – 75 °C)	-13 – 158 °F (-25 – 70 °C)
Vlhkosť	5 – 95 % bez kondenzovania	5 – 95 % bez kondenzovania	5 – 95 % bez kondenzovania
Systém			
Podporované štandardy	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, klient NTP (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), zrušenie certifikátu (RFC3280), importovanie certifikátu PKCS#12, importovanie PKCS#10 CSR (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP)		
Správa CLI, HTTPS	CLI, priame pripojenie ku konzole DB9 CLI, HTTPS	CLI, priame pripojenie ku konzole DB9 CLI, HTTPS	CLI, priame pripojenie ku konzole DB9 CLI, HTTPS
Vysoká dostupnosť (VD)	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie
Súlad s predpismi			
Bezpečnosť	FCC, časť 15, trieda A, C-Tick, VCCI, CE, UL/cUL, CB	FCC, časť 15, trieda A, C-Tick, VCCI, CE, UL/cUL, CB	FCC, časť 15, trieda A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

FortiAuthenticator 200E



FortiAuthenticator 400E



FortiAuthenticator 1000D

FortiAuthenticator 2000E

FortiAuthenticator 3000E

Virtuálne zariadenie FortiAuthenticator

ŠPECIFIKÁCIE

	FORTIAUTHENTICATOR 2000E	FORTIAUTHENTICATOR 3000E
Hardvér		
Rozhrania 10/100/1000 (medené, RJ-45)	4	4
Rozhrania SFP	2	2
Lokálne úložisko	2x disk SAS s kapacitou 2 TB	2x disk SAS s kapacitou 2 TB
Zdroj napájania	Dva 480 W s automatickou detekciou napätia (100 V – 240 V)	Dva 480 W s automatickou detekciou napätia (100 V – 240 V)
Výkonové údaje systému		
Celkový počet používateľov (lokálni + vzdialení)	20 000	40 000
Tokeny FortiToken	40 000	80 000
Klienti služby RADIUS (zariadenia NAS)	6 666	13 333
Skupiny používateľov	2 000	4 000
Certifikáty CA	50	50
Používateľské certifikáty	100 000	200 000
Rozmery		
Výška × šírka × dĺžka (v palcoch)	3,50 × 17,20 × 25,50	3,50 × 17,20 × 25,50
Výška × šírka × dĺžka (v mm)	89 × 437 × 647	89 × 437 × 647
Hmotnosť	32,0 libier (14,5 kg)	40,0 libier (18,6 kg)
Prostredie		
Veľkosť	Stojanový (2 RU)	Stojanový (2 RU)
Napájanie	100 – 240 V~, 50 – 60 Hz	100 – 240 V~, 50 – 60 Hz
Maximálny prúd	10 A pri 110 V, 4 A pri 220 V	10 A pri 110 V, 5 A pri 220 V
Spotreba energie (priemerná)	189 W	347 W
Odvádzanie tepla	781 BTU/hod.	1 325 BTU/hod.
Pracovná teplota	41 – 95 °F (5 – 35 °C)	50 – 95 °F (10 – 35 °C)
Teplota uskladnenia	-40 – 140 °F (-40 – 60 °C)	-40 – 158 °F (-40 – 70 °C)
Vlhkosť	8 – 90 % bez kondenzovania	8 – 90 % bez kondenzovania
Systém		
Podporované štandardy	10/100/1000 Base-TX (GE), IP, Telnet, HTTP 1.0/1.1, SSL, RS232, klient NTP (RFC1305), RADIUS (RFC2865), LDAP (RFC4510), x.509 (RFC5280), zrušenie certifikátu (RFC3280), importovanie certifikátu PKCS#12, importovanie PKCS#10 CSR (RFC2986), Online Certificate Status Protocol (RFC 2560), EAP-TLS (RFC2716), Simple Certificate Enrollment Protocol (SCEP)	
Správa	CLI, priame pripojenie ku konzole DB9 CLI, HTTPS	CLI, priame pripojenie ku konzole DB9 CLI, HTTPS
Vysoká dostupnosť (VD)	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie
Súlad s predpismi		
Bezpečnosť	FCC, ICES, CE, RCM, VCCI, BSMI, UL, CB	FCC, časť 15, trieda A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

VIRTUÁLNE ZARIADENIA	FAC-VM BASE	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG	FAC-VM-100000-UG
Kapacita					
Lokálni používatelia	100	+100	+1 000	+10 000	+100 000
Vzdialení používatelia	100	+100	+1 000	+10 000	+100 000
Tokeny FortiToken	200	+200	+2 000	+20 000	+200 000
Zariadenia NAS	33	+33	+333	+3 333	+33 333
Skupiny používateľov	10	+10	+100	+1 000	+10 000
Certifikáty CA	5	+5	+50	+500	+500
Používateľské certifikáty	100	+100	+1 000	+10 000	+100 000
Virtuálny počítač					
Podporovaní hypervízori	VMware ESXi/ESX 3.5/4.0/4.1/5.0/5.5/6.0, Microsoft Hyper-V Server 2008 R2, 2012 a 2012 R2, KVM				
Maximálny podporovaný počet virtuálnych procesorov	64				
Požadované virtuálne NIC (min./max.)	1 / 4				
Úložisko virtuálneho počítača (min./max.)	60 GB / 16 TB				
Požadovaná pamäť virtuálneho počítača (min./max.)	512 MB / 1 TB				
Podpora pre vysokú dostupnosť (VD)	VD s aktívnym a pasívnym zariadením a VD synchronizácie konfigurácie				

INFORMÁCIE O OBJEDNÁVANÍ

Produkt	SKU	Opis
FortiAuthenticator 200E	FAC-200E	4x port GE RJ45, 1x pevný disk s kapacitou 1 TB.
FortiAuthenticator 400E	FAC-400E	4x port GE RJ45, 2x pevný disk s kapacitou 1 TB.
FortiAuthenticator 1000D	FAC-1000D-E07S	4x port GE RJ45, 2x GE SFP, 2x pevný disk s kapacitou 2 TB.
FortiAuthenticator 2000E	FAC-2000E	4x port GE RJ45, 2x GE SFP, 2x disk SAS s kapacitou 2 TB.
FortiAuthenticator 3000E	FAC-3000E	4x port GE RJ45, 2x GE SFP, 2x disk SAS s kapacitou 2 TB.
Licencia pre FortiAuthenticator-VM	FAC-VM-Base	Základné zariadenie FortiAuthenticator-VM s licenciou pre 100 používateľov. Virtuálne procesory bez obmedzenia.
	FAC-VM-100-UG	FortiAuthenticator-VM s rozšírením licencie pre 100 používateľov.
	FAC-VM-1000-UG	FortiAuthenticator-VM s rozšírením licencie pre 1 000 používateľov.
	FAC-VM-10000-UG	FortiAuthenticator-VM s rozšírením licencie pre 10 000 používateľov.
	FAC-VM-100000-UG	FortiAuthenticator-VM s rozšírením licencie pre 100 000 používateľov.
	FC1-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 500 používateľov).
	FC2-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 1 100 používateľov).
	FC3-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 5 100 používateľov).
	FC4-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 10 100 používateľov).
	FC8-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 25 100 používateľov).
	FC5-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 50 100 používateľov).
	FC6-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 100 100 používateľov).
	FC9-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 500 100 používateľov).
	FC7-10-0ACVM-248-02-12	1-ročná zmluva 24x7 FortiCare (1 až 1 mil. používateľov).

CELOSVETOVÁ CENTRÁLA
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
USA
Tel.: +1 408 235 77 00
www.fortinet.com/sales

OBCHODNÉ ZASTÚPENIE
PRE KRAJINY EMEA
905 rue Albert Einstein
06560 Valbonne
Francúzsko
Tel.: +33 4 89 87 05 00

OBCHODNÉ ZASTÚPENIE
PRE KRAJINY APAC
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapur 038988
Tel.: +65 63 95 27 88

OBCHODNÉ ZASTÚPENIE
PRE LATINSKÚ AMERIKU
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
USA
Tel.: +1 954 368 99 90

FST-PROD-DS-FAUM

FAC-DAT-R18-201902