

FortiManager

Bezpečnostné tímy zaostávajú v novodobom náročnom prostredí kybernetických hrozieb kvôli obmedzeným zdrojom a neschopnosti držať krok s najnovšími hrozbami. Zložitosť a neznáme hrozby znižujú efektivitu zabezpečenia – NOC-SOC pomáha omladiť a zvýšiť silu zabezpečenia.

Centralizovaná správa zabezpečenia pomáha spoločnostiam **sprevádzkovať a automatizovať zabezpečenie** s cieľom skrátiť čas odozvy a zlepšiť povedomie a **Security Fabric od spoločnosti Fortinet** je základom tohto nového prístupu. FortiManager poskytuje jednu konzolu na správu siete pre úplnú kontrolu nad zariadeniami Fortinet so správou podnikovej triedy.

Centralizovaná správa zabezpečenia

Správa operácií NOC-SOC v rámci zariadenia

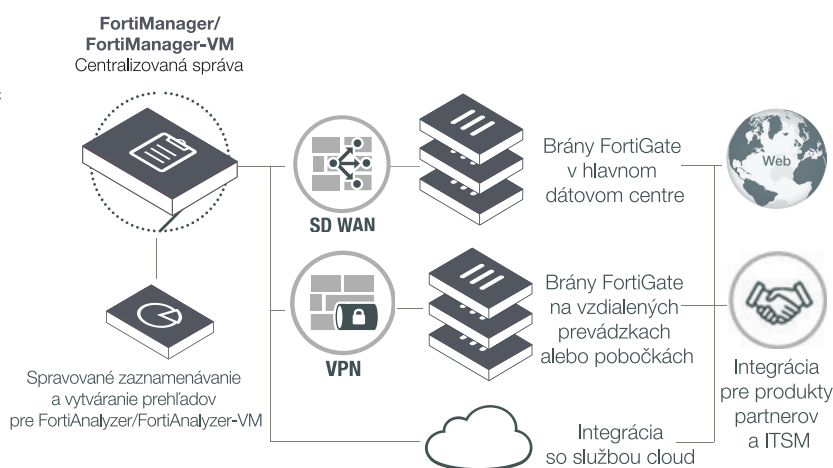
FortiManager poskytuje zabezpečenú prevádzkovú viditeľnosť naprieč celou vrstvou Fortinet Security Fabric pre sledovanie zabezpečenia v reálnom čase, identifikovanie a elimináciu hrozieb a zraniteľných miest.

Informácie zo systému pre kvantifikovateľné zabezpečenie

ako sú napríklad zrelosť zabezpečenia a hodnotenia zabezpečenia, stanovujú merateľnú mieru zodpovednosti, ktorú môžete použiť na stanovenie vnútornej pripravenosti v oblasti zabezpečenia a jej porovnanie s inými riešeniami v odvetví.

Integrácia pracovného toku so službou ITSM

(ServiceNow) na zmiernenie udalostí zabezpečenia a použitie zmien konfigurácie a aktualizácií pravidiel.



Obr. 1: Nasadenie zariadenia FortiManager

Hlavné vlastnosti

- Centralizovaná správa zariadení: Jediná konzola na správu všetkých prepínačov brány firewall, bezdrôtovej infraštruktúry a koncových bodov Fortinet.
- Centralizovaná správa politík a objektov: rýchlo vytvárajte a prispôbujete politiky alebo objekty s konsolidovaným náhľadovým editorom s prostredím podporujúcim presun myšou.
- Podrobné sledovanie revízií a výkonné funkcie auditu.
- Spravujte zariadenia v skupine vrstvy Security Fabric, ako keby išlo o jediné zariadenie, a zobrazte topológiu vrstvy Security Fabric.
- Integrácia pracovného toku na správu riadenia zmien.
- Centralizované poskytovanie a monitorovanie siete SD-WAN.
- Centralizovaná správa siete VPN: komunity siete VPN, správa tunelov, topológie.
- Automatizácia – šablóny a skripty na automatizáciu poskytovania zariadení a inštaláciu politík pomocou rozhraní API JSON alebo rozhraní API XML na zníženie administratívneho zaťaženia a prevádzkových nákladov.
- Granulované spravovanie na základe zariadení a rol pre veľké spoločnosti a nasadenia s podporou niekoľkých nájomníkov.
- Centralizované inovácie softvéru a aktualizácie zabezpečenia pre spravované zariadenia.

Správa pomocou konsolidovanej tably

Fortinet Security Fabric prináša sofistikovanú správu zabezpečenia pre zjednotenú ochranu medzi koncovými zariadeniami. Nasadením bezpečnostnej infraštruktúry založenej na platforme Fortinet na boj s vyspelými hrozbami a pridaním zariadenia FortiManager na poskytovanie správy pomocou konsolidovanej tably v rámci celej spoločnosti získate prehľad o prenosoch a hrozbách v rámci celej siete.

FortiManager ponúka funkcie podnikovej triedy na zastavenie vyspelých hrozieb. FortiManager prináša aj najlepšiu škálovateľnosť v odvetví na správu až 100 000 zariadení Fortinet. FortiManager spolu so skupinou zariadení FortiAnalyzer na centralizované zaznamenávanie a vytváranie prehľadov poskytuje komplexnú a výkonnú centralizovanú správu pre vašu organizáciu.

Základné vlastnosti

Centralizované nasadenie a monitorovanie siete SD-WAN

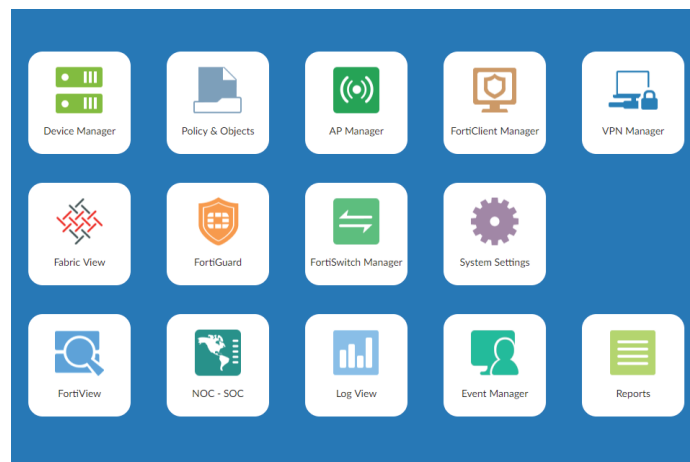
Centrálne monitorujte výkony siete SD-WAN. Monitorujte vlastné zariadenia na mape s farebne označenými ikonami a nastavením sa myšou na položku si zobrazte štatistické informácie o stave každého článku siete SD-WAN. Tabuľkové zobrazenie poskytuje podrobnejšie informácie o každom článku siete SD-WAN vrátane stavu pripojenia, výkonov aplikácie a využívania šírky pásma.

Spravované zariadenia FortiAP, FortiSwitch a FortiExtender

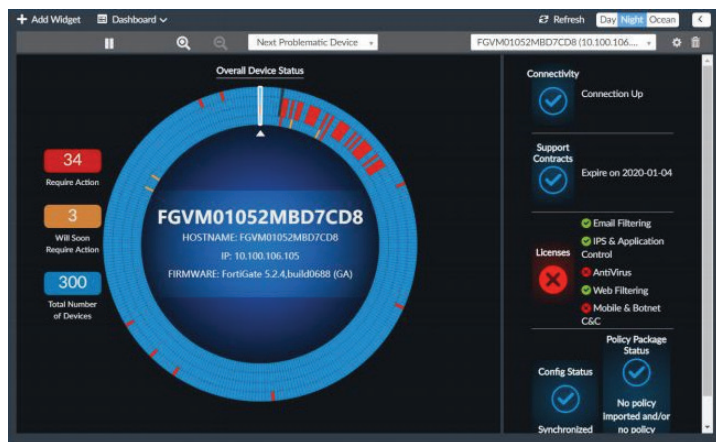
Centrálne spravujte bezdrôtové siete, vytvárajte šablóny pre WiFi, profily prístupových bodov, SSID a WIDS. Spravujte celú infraštruktúru FortiSwitch.

Konfigurácia a správa nastavení

Hromadne konfiguruje nastavenia zariadení, objekty a politiky v celej sieti z jedného používateľského rozhrania. Správca siete VPN zjednodušuje nasadenie a umožňuje spravovať komunitu VPN s centrálnym poskytovaním a monitorovať pripojenia VPN v službe Mapy Google. Správca FortiAP umožňuje konfigurovať, nasadzovať a monitorovať prístupové body FortiAP z jedinej konzoly so zobrazením v službe Mapy Google. Správca FortiClient umožňuje centralizovanú konfiguráciu, nasadenie a monitorovanie klientov FortiClient.



Obr. 3: Tabuľka zariadenia FortiManager



Obr. 2: Tabuľka so stavom zariadení NOC-SOC

Integrácia a Security Fabric

Integrácia so službou ITSM (ServiceNow) na zmiernenie udalostí zabezpečenia a použitie zmien konfigurácie a aktualizácií pravidiel. Bezproblémová integrácia so zariadeniami FortiAnalyzer poskytuje hĺbkové zisťovanie, analýzu, stanovenie priority a hlásenie udalostí zabezpečenia siete.

Pracovný postup pre audit a zabezpečovanie súladu

FortiManager umožňuje vykonať kontrolu, schválenie a audit zmien politiky z centrálného miesta vrátane používania automatizovaných procesov, ktoré uľahčujú dodržiavanie pravidiel, riadenia životného cyklu politik a vynútenia pracovného toku s cieľom znížiť riziko zmien politiky.

Monitorovanie a prehľady pre hlbokú viditeľnosť

Získajte prístup k vitálnym bezpečnostným a sieťovým štatistickým údajom, monitorovaniu v reálnom čase a vstavaným prehľadom pre viditeľnosť v súvislosti so sieťovou aktivitou a aktivitou používateľov. Ak chcete používať výkonné analytické funkcie, pridajte zariadenie FortiAnalyzer, ktoré umožňuje dolovať údaje a vytvárať grafické prehľady.

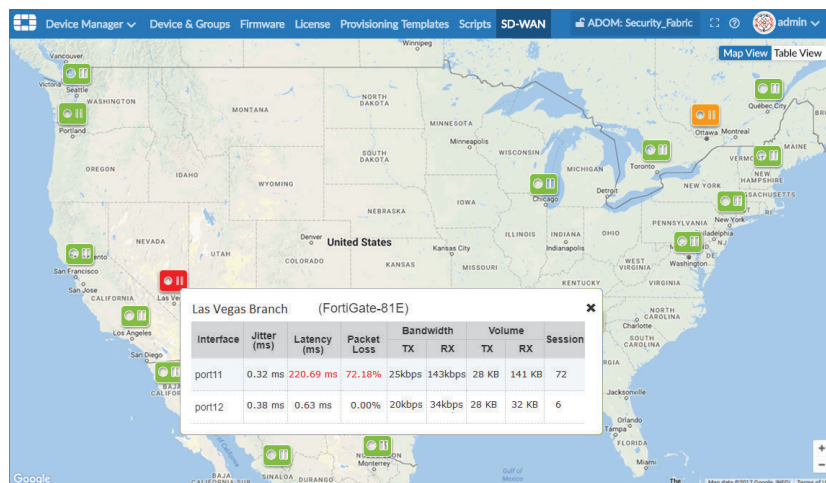
Základné vlastnosti

Lokálne hostovaný obsah zabezpečenia FortiGuard Labs

Hostujte obsah zabezpečenia lokálne pre väčšiu kontrolu nad aktualizáciami obsahu zabezpečenia a kratšie časy reakcie databázy hodnotení. Zahŕňa podporu pre nasledovné funkcie: aktualizácie pre riadenie aplikácií a prevenciu neoprávnených vniknutí, správu zraniteľných miest, antispam, antivírus a webové filtrovanie.

Podpora pre niekoľko nájomníkov a hierarchická štruktúra – administratívne domény (ADOM)

FortiManager poskytuje databázu hierarchických objektov, ktorá uľahčuje opätovné použitie spoločných konfigurácií, a architektúru s podporou pre niekoľko nájomníkov na súčasné poskytovanie služieb viacerým zákazníkom. Grafické rozhranie uľahčuje zobrazenie, vytváranie a správu ADOM. ADOM sa môžu použiť na správu nezávislých prostredí zabezpečenia, kde každá ADOM má vlastné politiky zabezpečenia a konfiguračnú databázu. FortiManager umožňuje združovať zariadenia logicky alebo geograficky pre flexibilnú správu a pri Zero-Touch nasadení sa používajú šablóny na poskytovanie zariadení pre rýchle hromadné nasadenie. Definujte globálne objekty, ako sú napríklad objekty brány firewall, politiky a bezpečnostné profily, ktoré sa môžu zdieľať medzi viacerými ADOM. Granulárne povolenia umožňujú prideliť ADOM, zariadenia a politiky používateľom na základe rol a povinností.



Obr. 4: SD-WAN Monitor

API pre automatizáciu a zosúladenie

API RESTful umožňuje poskytovateľom spravovaných služieb zabezpečenia (MSSP) a veľkým spoločnostiam vytvárať prispôbené vlastné webové portály na správu politik a objektov. Automatizujte bežné úlohy, ako sú napríklad poskytovanie nových brán FortiGate a konfigurácia existujúcich zariadení. Staňte sa členom siete Fortinet Developer Network (FNDN) a získajte prístup k exkluzívnym článkom, návodom na automatizáciu a prispôbenie, nástrojom od komunity, skriptom a ukážkam kódov.

FortiManager VM

Spoločnosť Fortinet ponúka zariadenie FortiManager VM v rámci modelu s možnosťou rozšírenia licencie. Model vám umožní rozšíriť riešenie VM s rastom vášho prostredia. FortiManager-VM je softvérová verzia fyzického zariadenia FortiManager na báze technológie virtualizácie. Aplikácia je navrhnutá tak, aby sa mohla spúšťať pod rôznymi virtualizačnými platformami. Ponúka všetky funkcie fyzického zariadenia FortiManager.

Rad virtuálnych zariadení FortiManager minimalizuje úsilie potrebné na monitorovanie a správu prijateľných politík používania a identifikovanie znakov útokov. Získané informácie sa môžu použiť na doladenie politiky zabezpečenia a prekazenie ďalších útokov.

Špecifikácie

VIRTUÁLNE ZARIADENIA FORTIMANAGER	FMG-VM-BASE	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG
KAPACITA					
Počet zariadení/VDOM (maximálny) ^{1,4}	10	10 +	100 +	1 000 +	5 000 +
Kapacita úložiska ²	100 GB	200 GB	1 TB	4 TB	8 TB
GB/deň pre záznamy ³	1	2	5	10	25
Správa rámov	✓	✓	✓	✓	✓
VIRTUÁLNY POČÍTAČ					
Podpora pre hypervizorov	VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/6.7, Microsoft Hyper-V 2008 R2/2012 R2/2016, Citrix XenServer 6.0+ a Open Source Xen 4.1+, KVM so systémami Redhat 6.5+ a Ubuntu 17.04, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP), Oracle Cloud Infrastructure (OCI), AliCloud				
Podporovaný počet v CPU (minimálny/maximálny)	2 / bez obmedzenia				
Podporované sieťové rozhrania (min./max.)	1 / 4				
Podporované úložisko (minimálne/maximálne)	100 GB / 16 TB				
Podporovaná pamäť (minimálna/maximálna)	4 GB / bez obmedzenia so 64-bitovou verziou				
Podpora pre vysokú dostupnosť (VD)	Áno				

¹ Každá virtuálna doména (VDOM) prevádzkovaná na fyzickom alebo virtuálnom zariadení sa považuje za jedno (1) licencované sieťové zariadenie.

³ Kapacita úložiska a GB/deň pre protokoly nie sú rozšíriteľné. Tieto údaje predstavujú maximálne dostupné hodnoty so zakúpenou licenciou.

² Obmedzené softvérom na 10 000 zariadení/VDOM.

⁴ Uvádza dostupnú prídavnú licenciu pre zariadenie.

Informácie o objednávaní

PRODUKT	SKU	OPIS
FortiManager	FMG-200F	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 2x RJ45 GE, 2x SFP, úložný priestor 8 TB, max. 30 zariadení Fortinet alebo virtuálnych domén
	FMG-300F	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 4x GE RJ45, 2x SFP, úložný priestor 16 TB, max. 100 zariadení Fortinet alebo virtuálnych domén
	FMG-400E	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 2x GE RJ45, úložný priestor 24 TB, max. 300 zariadení Fortinet alebo virtuálnych domén
	FMG-2000E	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 4x GE RJ45, 2x zásuvka 10 GE SFP+, úložný priestor 36 TB, dva zdroje napájania, spravuje max. 1 200 zariadení Fortinet alebo virtuálnych domén
	FMG-3000F	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 4x GE RJ45, 2x zásuvka 10 GE SFP+, úložný priestor 48 TB, dva zdroje napájania, spravuje max. 4 000 zariadení Fortinet alebo virtuálnych domén
	FMG-3700F	Zariadenie na centralizovanú správu, zaznamenávanie do denníka a analýzu – 2x 10 GbE SFP+, 2x zásuvka 1 GbE RJ-45, úložný priestor 240 TB, dva zdroje napájania, spravuje max. 10 000 zariadení Fortinet alebo virtuálnych domén
FortiManager Rozšírenie počtu zariadení	FMG-DEV-100-UG	Licencia pre FortiManager na rozšírenie počtu zariadení prídávajúc 100 zariadení Fortinet alebo VDOM (od radu 3000 – iba pre fyzické zariadenia)
FortiManager VM	Vstavaná skúšobná licencia	Vstavaná 15-dňová skúšobná licencia, nevyžaduje sa aktivácia.
	Plnohodnotná skúšobná licencia (60 dní)	Skúšobná licencia. Vyžaduje sa licencia a aktivácia.
	FMG-VM-Base	Základná licencia pre rozšíriteľné zariadenie FortiManager-VM Umožňuje spravovať až 10 zariadení Fortinet alebo virtuálnych domén, 1 GB/deň pre protokoly a 100 GB kapacita úložiska. Určené pre všetky podporované platformy.
	FMG-VM-10-UG	Rozširujúca licencia na pridanie 10 zariadení Fortinet alebo virtuálnych domén. Pre celkovo 2 GB/deň pre protokoly a 200 GB kapacitu úložiska.
	FMG-VM-100-UG	Rozširujúca licencia na pridanie 100 zariadení Fortinet alebo virtuálnych domén. Pre celkovo 5 GB/deň pre protokoly a 1 TB kapacitu úložiska.
	FMG-VM-1000-UG	Rozširujúca licencia na pridanie 1 000 zariadení Fortinet alebo virtuálnych domén. Pre celkovo 10 GB/deň pre protokoly a 4 TB kapacitu úložiska.
Doplnky pre FortiManager	FC-10-FNDN1-139-02-12	Obnovenie ročného prístupu k sieti Fortinet Developer Network pre 1 používateľa.
	FC-10-FNDN2-139-02-12	Ročný prístup k sieti Fortinet Developer Network pre neobmedzený počet používateľov.
	FMG-SDNS	Licencia na prevádzkovanie zariadenia FortiManager ako vyhradený server Secure DNS (od radu 3000 – iba pre fyzické zariadenia).



CELOSIVETOVÁ 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
Singapore 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

Copyright© 2019 Fortinet, Inc. Všetky práva vyhradené. Fortinet®, FortiGate®, FortiCare® a FortiGuard® a niektoré ďalšie ochranné známky sú registrované ochranné známky spoločnosti Fortinet, Inc. v USA a iných jurisdikciách a iné názvy spoločnosti Fortinet, ktoré sú použité v tomto dokumente, môžu byť tiež registrované a/alebo bežné ochranné známky spoločnosti Fortinet. Všetky ostatné názvy produktov alebo spoločností môžu byť ochrannými značkami príslušných vlastníkov. Výkonové údaje a iné parametre uvedené v tomto dokumente boli získané v rámci interných laboratórnych testoch v ideálnych podmienkach a skutočný výkon aj ďalšie výsledky sa môžu líšiť. Sieťové premenné, rôzne sieťové prostredia a iné podmienky môžu ovplyvniť výsledné výkonové údaje. Nič z toho, čo je uvedené v tomto dokumente, nepredstavuje záväzok spoločnosti Fortinet. Spoločnosť Fortinet odmieta akékoľvek záruky, či už výslovné alebo implicitné, s výnimkou prípadov, keď uzavrie záväznú písomnú zmluvu, ktorú podpísal právny zástupca spoločnosti Fortinet s kupujúcim a ktorá výslovné zaručuje, že príslušný produkt bude poskytovať výkony v súlade s určitými výslovné stanovenými výkonovými parametrami. V takom prípade budú pre spoločnosť Fortinet záväzné konkrétne výkonové parametre, ktoré sú výslovné uvedené v príslušnej záväznej písomnej zmluve. Z dôvodu absolútnej prehľadnosti bude každá takáto záruka poskytovaná iba na výkony v rovnakých ideálnych podmienkach, v akých spoločnosť Fortinet vykonala interné laboratórne testy. Spoločnosť Fortinet v žiadnom prípade neakceptuje žiadne záväzky týkajúce sa budúcich dodávok, funkcií ani vývoja. Okolnosti sa môžu zmeniť natoľko, že žiadne vyhlásenia týkajúce sa plánov, ktoré sú uvedené v tomto dokumente, nemusia byť presné. Spoločnosť Fortinet sa v celom rozsahu zrieka akýchkoľvek dohôd, vyjadrení a záruk podľa tohto dokumentu, či už výslovných alebo implicitných. Spoločnosť Fortinet si vyhradzuje právo zmeniť, upraviť, previesť alebo inak korigovať túto publikáciu bez predchádzajúceho upozornenia, pričom v takom prípade platí najnovšia verzia publikácie.

FST-PROD-DS-MGR

FMG-DAT-R43-201902