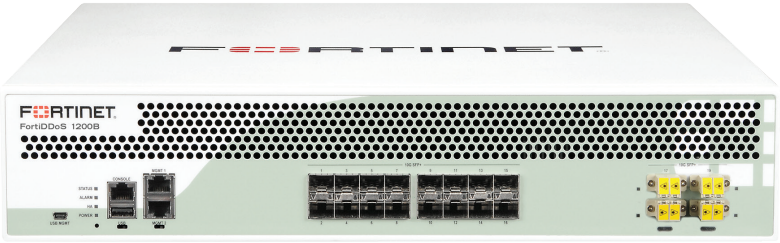
FortiDDoS™

FortiDDoS 200B, 400B, 600B, 800B, 900B, 1000B, 1000B-DC a 1200B



Distributed Denial of Service (DDoS) útoky zostávajú naďalej najvyššou hrozbou pre bezpečnosť IT a vyvinuli sa takmer vo všetkých smeroch, aby robili to, čo robia najlepšie: aby vypli vaše dôležité online služby. Problém nebol nikdy taký dynamický a široký bez toho, aby bol viazaný na jednu konkrétnu technológiu.

Existuje takmer neobmedzená škála nástrojov, ktoré môžu používať hektivisti a kyberteroristi, aby zabránili prístupu do vašej siete. Sofistikované útoky DDoS vytvárajú nielen objemové útoky vrstvy 4, ale aj cielené služby vrstvy 7 a DNS, kde oveľa menšie veľkosti útokov môžu skrývať útoky pred metódami zmierňovania cloudu. Na boj s týmito útokmi potrebujete riešenie, ktoré je rovnako dynamické a široko založené. Zariadenia Fortinet na zmierňovanie útokov FortiDDoS využívajú metódy detekcie útokov založené na správaní a detekciu a zmierňovanie 100 % hardvéru pomocou bezpečnostných procesorových jednotiek (SPU), ktoré poskytujú na dnešnom trhu najpokročilejšie a najrýchlejšie zmiernenie útokov DDoS.

Iný a lepší prístup k DDoS Zmierňovanie útoku

Iba spoločnosť Fortinet využíva 100 % prístup SPU k produktom DDoS bez ohrozenia výkonu hybridného systému CPU alebo CPU/ASIC. Transakčné procesory SPU-TP2 kontrolujú 100 % prichádzajúcich aj odchádzajúcich prevádzok vrstvy 3, 4 a 7, čo má za následok najrýchlejšiu detekciu a zmiernenie a najnižšiu latenciu v priemysle. FortiDDoS používa 100 % heuristickú metódu správania na identifikáciu hrozieb v porovnaní s konkurentmi, ktorí sa spoliehajú predovšetkým na podpisovú zhodu. Namiesto vyžadovania preddefinovaných podpisov na identifikáciu modelov útokov FortiDDoS využíva masívne paralelnú výpočtovú architektúru na vytvorenie adaptačnej základne normálnej aktivity zo stoviek tisíc parametrov a potom monitoruje prevádzku proti tejto základnej línii. Ak by sa začal útok, FortiDDoS ho považuje za abnormálny a okamžite podnikne kroky na jeho zmiernenie.

Hlavné výhody

- 100 % identifikácia a zmiernenie útokov na hardvér v rámci vrstvy 3, 4 a 7 DDoS.
- 100 % detekcia DDoS založená na správaní.
- Úplne neviditeľné pre útočníkov bez IP a MAC adries v dátovej dráhe. FortiDDoS nepredstavuje smerovanie ani ukončenie zariadenia vrstvy 3.
- Rozšírené zmiernenie DNS DDoS pre väčšinu modelov.
- Dostupné hybridné On-premise/Cloud zmierňovanie s Open Signaling.
- Kontinuálne vyhodnocovanie hrozieb na minimalizáciu falošných pozitívnych detekcií.
- Jednoduchá architektúra súčasne sleduje státisíce parametrov – masívne paralelné výpočty portálu MSSP pre zákaznícky predaj.

Celosvetová nepretržitá podpora FortiCare

support.fortinet.com

HLAVNÉ VÝHODY

FortiDDoS vás chráni pred známymi útokmi a útokmi typu „zero-day", pretože nemusí čakať na aktualizované podpisové súbory. FortiDDoS spracúva zmiernenie útoku inak než iné riešenia. Pri iných zariadeniach na zmiernenie útoku DDoS, len čo sa útok začne, je na 100 % zablokované, alebo miera návštevnosti je obmedzená na cieľovú IP adresu, ktorá má negatívny vplyv aj na „dobrú" prevádzku. Ak ide o udalosť typu „falošný poplach", potom je ovplyvnená celá prevádzka a vyžaduje zásah. FortiDDoS používa operatívnejší prístup, kde sleduje bežnú prevádzku a potom používaním Source Tracking zistí až 6 miliónov zdrojov IP adries, ktoré spôsobujú problém.

FortiDDoS blokuje nepriaznivé adresy IP zdroja a potom prehodnotí útok v intervaloch, ktoré používateľ definuje. Ak sú zdrojové IP adresy pre každé z týchto období prehodnotenia naďalej hrozbou, doba blokovania sa predlžuje, až kým sa útok nepotlačí. Cieľové IP adresy sú zriedka obmedzené rýchlosťou a platné IP adresy sú vždy povolené.

Flexibilné obranné mechanizmy

FortiDDoS chráni pred každým útokom DDoS vrátane útokov typu Bulk Volumetric, Layer 7 Application, DNS a SSL/HTTPS. FortiDDoS má pokrytú oblasť od najstaršieho triku v zozname až po najnovšie v pokročilých vrstvách útokov.

Volumetrické objemové útoky naďalej predstavujú významné hrozby. Zatiaľ čo poskytovatelia internetových služieb môžu zabrániť jednoduchým útokom tohto typu, útoky sa čoraz častejšie používajú na maskovanie zložitejších útokových metód na úrovni aplikácií. Sledovanie zdroja FortiDDoS naďalej umožňuje „dobrú" návštevnosť počas blokovania zdrojových adries IP, ktoré spôsobujú problém. Tento proces nielenže poskytuje ochranu, ktorú potrebujete, ale minimalizuje aj účinky „falošného poplachu" od pozastavenia dobrej klientskej návštevnosti.

Cieľové útoky na vrstve 7 sú rýchlo rastúcim zdrojom útokov DDoS. Pokúšajú sa zneužiť zraniteľnosti v rámci služby alebo servera, aby vyčerpali svoje zdroje, čím sa stávajú nedostupnými. Tieto typy útokov sa takmer vždy vyhýbajú zmierňovaniu ISP vrstvy 3 a 4 a prechádzajú priamo do vašej siete. Útoky na vrstve 7 spôsobia zmeny na úrovni služby, ktoré FortiDDoS identifikuje a zmierni.

Útoky založené na protokole SSL sú zvyčajne jednorazové útoky DoS, ktoré sú navrhnuté tak, aby injektovali škodlivý softvér. Útoky SSL DDoS sú zriedkavé, pretože viacnásobné SSL útoky vyžadujú viac zdrojov útočníkov a odkryjú zdrojové IP adresy serverov alebo botov útočníka, ktoré môžu byť trvale zablokované. FortiDDoS vidí DDoS útoky založené na protokole SSL pre zmeny správania z parametrov ako Nové pripojenia, Pripojenia/Zdroj, SNI Host Floods, Pomalé pripojenia alebo Počet jedinečných zdrojov, ktoré nie sú šifrované parametre.

Spoločnosť Fortinet je presvedčená, že je nedostatočnou bezpečnostnou praxou umiestniť svoje certifikáty SSL mimo ochranu brány firewall a webovej aplikácie a ukončiť relácie v zariadení na zmiernenie DDoS na dešifrovanie a tým poskytnúť priestor útoku na zariadenie. Spoločnosť Fortinet vždy odporúča úplný bezpečnostný systém, ktorý zahŕňa FortiGate a FortiWeb, aby bol chránený pred všetkými úrovňami útokov na vašu infraštruktúru.

Útoky založené na protokole DNS sú zamerané na všetky typy serverov DNS ako obete alebo ako príčiny útokov DDoS. Podniky a prevádzkovatelia, ktorí hostia servery DNS, sú ohrození útokmi DDoS, ktoré využívajú nedostatky v spôsobe, akým servery DNS spracúvajú otázky a odpovede. FortiDDoS je jediná platforma na zmierňovanie DDoS, ktorá kontroluje 100 % všetkých návštev DNS na ochranu proti všetkým typom útokov DDoS smerovaných na servery DNS, vrátane záplav DNS Reflection/Response, NXDomain, záplava otázok, Náhodné subdomény a anomálie DNS. FortiDDoS podporuje službu reputácie domén FortiGuard na ochranu DNS serverov a klientov pred známymi škodlivými doménami. Zvýšená ochrana DNS je k dispozícii na väčšine modelov FortiDDoS.

Botnety typu IoT - „Internet vecí", ako Mirai, sú schopné viacerých vektorových GRE, náhodných subdomén, DNS reflexií, UDP a TCP útokov, pričom robia spoofing celého priestoru adries IPv4. Malé paketové záplavy zdôrazňujú schopnosť mnohých zariadení DDoS v reálnom čase, čo zabraňuje úplnej kontrole a bez vyspelých techník na zisťovanie DNS, náhodné útoky na subdomény vyzerajú ako bežné návštevnosti dopytu pri vyčerpávajúcich zdrojoch servera DNS. Hardvérová architektúra systému FortiDDoS a veľký počet monitorovaných parametrov vás budú naďalej chrániť, pretože tieto útoky sa vyvíjajú.

Hybridné zmierňovanie On-premise/Cloud DDoS

Zatiaľ čo FortiDDoS môže zmierniť akýkoľvek útok DDoS na hranicu prichádzajúcej šírky pásma, veľké útoky môžu nasýtiť prichádzajúce odkazy. Partneri FortiDDoS so spoločnosťou Baffin Bay Networks OpenFSP™ vám poskytnú možnosť výberu najlepších zmierňovačov CPE/Cloud DDoS v triede, keď útoky ohrozujú nahromadenie vzostupných zdrojov. Signalizačné rozhranie FortiDDoS API je otvorené a zdokumentované. FortiDDoS kontroluje prichádzajúcu čistú prevádzku GRE od poskytovateľov služby Cloud, aby sa zabezpečila kontinuita nahlasovania a úplné zmiernenie hrozieb. FortiDDoS na zariadeniach prevádzkovaných v dátových centrách podniku môžu spolupracovať priamo s vysokokapacitnými modelmi FortiDDoS v sieti poskytovateľa služieb pomocou našej technológie cloud signalizácie a môžu poskytovať vášmu poskytovateľovi internetových služieb aj skripty Flowspec, ktoré podporujú zneužitie a zablokovanie útokov.

Hlavné vlastnosti a výhody

100 % detekcia správania	FortiDDoS sa nespolieha na podpisové súbory, ktoré je potrebné aktualizovať s najnovšími hrozbami, takže ste chránení pred známymi aj neznámymi útokmi typu „zero-day".
100 % hardvérová ochrana DDoS	Transakčný procesor SPU-TP2 poskytuje 100 % kontrolu paketov s obojstrannou detekciou a zmierňovaním útokov DDoS na vrstve 3, 4 a 7 pre špičkový výkon.
Priebežné hodnotenie útokov	Minimalizuje riziko zisťovania „falošného poplachu" prostredníctvom prehodnotenia útoku, aby sa zabezpečilo, že nie je narušená „dobrá" prevádzka.
Zvýšená ochrana DNS	FortiDDoS poskytuje 100 % kontrolu nad celou prevádzkou DNS na ochranu pred širokou škálou objemových, aplikačných a anomálnych útokov na báze DNS.
Automatizovaný proces učenia	Pri minimálnej konfigurácii FortiDDoS automaticky vytvára bežné profily správania a zdrojov, čo vám ušetrí čas a zdroje IT správy.
Podpora hybridného On-premise/Cloudu	Open API umožňuje integráciu s poskytovateľmi zmierňovania cloudu DDoS z tretích strán pre flexibilné možnosti nasadenia a ochranu pred rozsiahlymi útokmi DDoS.

VLASTNOSTI FORTIDDOS

Technológia kontroly paketov
- Prediktívna behaviorálna analýza
- Heuristická analýza
- Kontrola granulárnych hĺbkových paketov
- Priebežné obmedzenie adaptívnej rýchlosti
- Monitorovanie stavu pre konkrétne útokové vektory
- 100 % kontrola paketov
- Plná podpora IPv4/IPv6 pre jednu IP podsieť
- Úplná neviditeľnosť bez MAC a IP adries v dátovej dráhe

Behaviorálne riadenie prahových hodnôt
- Odporúčanie systému založené na nepretržitej štatistike návštevnosti
- Adaptívny odhad prahových hodnôt

Proces viacnásobného overovania
- Dynamické filtrovanie
- Aktívna verifikácia
- Rozpoznanie anomálií
- Protokolová analýza
- Biely zoznam, čierny zoznam, nezosilnené podsiete
- Rozpoznávanie stavu anomálií
- Filtrovanie tajných útokov
- Lokálna adresa proti spoofingu (BCP-38)
- Sledovanie zdroja
- Legitímna zhoda IP adresy (Anti-Spoofing)
- Zvýšená liečba protokolov IP Proxy — zistená na základe hlavičky a počtu súbežných pripojení

100 % kontrola anomálií
- L3/L4/L7 HTTP/DNS

Zmierňovanie flood na úrovni 3
- Flood protokoly (všetky 256)
- Zloženie floodov
- Zdrojové floody
- Kontrola GRE

Zmierňovanie flood na úrovni 4
- TCP porty (všetky 65k)
- UDP porty (všetky 65k)
- UDP herné porty
- Typ/kódy ICMP (všetky 65k)
- SYN, flood spojenie
- Záplava SYN paketov
- Záplavy typu Out-Of-State, RST/FIN/ACK
- Pripojenie/sekundu
- Floody na zdrojovú frekvenciu (zdroje 6M)
- Záplavy typu Zombie
- Pomalé pripojenia
- TCP flood poruchy

Zmierňovanie flood na úrovni 7
- HTTP URL
- Metóda HTTP Flood (všetkých 8 METÓD)
- Používateľ agent Flood
- Referrer Flood
- Cookie Flood
- Host Flood

Mechanizmy flood prevencie
- SYN Cookie, ACK Cookie, retranslácia SYN, retransmisia DNS/TC = 1
- Legitímna IP validácia/zhoda
- Sledovanie zdroja
- Obmedzenie zdrojov
- Agresívne starnutie

Zoznamy prístupu L3-L7
- Reputácia IP
- Reputácia domény
- Dĺžka paketu/protokol/port
- Geolokalizácia
- Čierny zoznam/Biely zoznam IP/podsiete
- Hromadné nahranie zákazníkov na čiernu listinu IPv4
- Hromadná registrácia zákazníkov na čiernu listinu
- Rozšírená verifikácia zdrojovej adresy BCP38/ lokálna adresa proti spoofingu
- Protokol, fragment, fragment DNS, port L4, typ/kód ICMP
- DNS RR ACLs
- Metódy HTTP, URL, Host, Referrer, User Agent
- Generovanie skriptu Flowspec

Zmierňovanie útoku DNS
- Predchádzanie anomáliám záhlavia DNS
- Zhoda odpovede dotazu DNS
- DNS dotaz/MX/ALL/ZT/ fragment/na flood zdroj
- Overenie zdroja DNS dotazu
- Neočakávaný dopyt DNS
- Nevyžiadaná reakcia na flood DNS
- Vyrovnávacia pamäť DNS odpovedí na flood
- Kontroly TTL DNS dotazu
- ACL špecifické pre DNS
- Odber predplatného na doméne

VLASTNOSTI FORTIDDOS

Komplexné zabudované nahlasovanie

- Filtrovateľný/exportovateľný protokol útoku
- Súhrnné grafy a logy pre:
  - Najčastejšie útoky/najčastejší útočníci
  - Top ACL vyčleňovanie
  - Najčastejšie napadnuté podsiete a adresy IP
  - Najčastejšie napadnuté protokoly
  - Najčastejšie napadnuté porty TCP a UDP
  - Najčastejšie napadnuté typy/kódy ICMP
  - Najčastejšie napadnuté webové adresy, hostitelia HTTP, referenční používatelia, súbory cookie, zástupcovia používateľov
  - Najčastejšie napadnuté servery DNS
  - Najčastejšie napadnuté DNS anomálie
  - Štatistiky SPP: Monitorovanie mbps/pps a vyradenie
  - Štatistika podsiete: Monitorovanie prevádzky mbps/pps
- Vlastné, na vyžiadanie, podľa plánu a/alebo v správach o prahu útoku
- 1000 vstavaných grafov na vykazovanie v reálnom čase a forenznej analýzy

Centralizované hlásenie udalostí

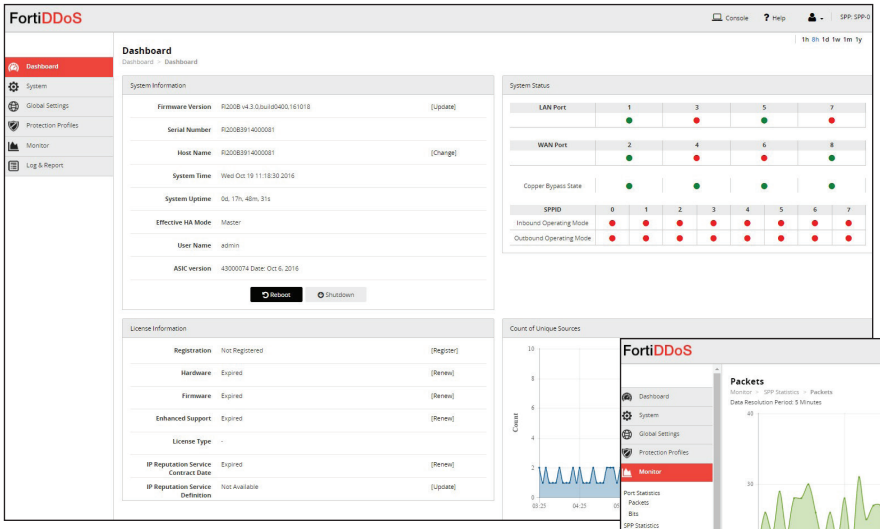
- SNMP v2/v3
- Mailové upozornenia a správy
- Otvorené rozhranie RESTful API
- Syslog podpora FortiAnalyzer,
- FortiSIEM a tretia strana

Trasy auditu a prístupu

- Prihlásenie na audit
- Konfigurácia auditu

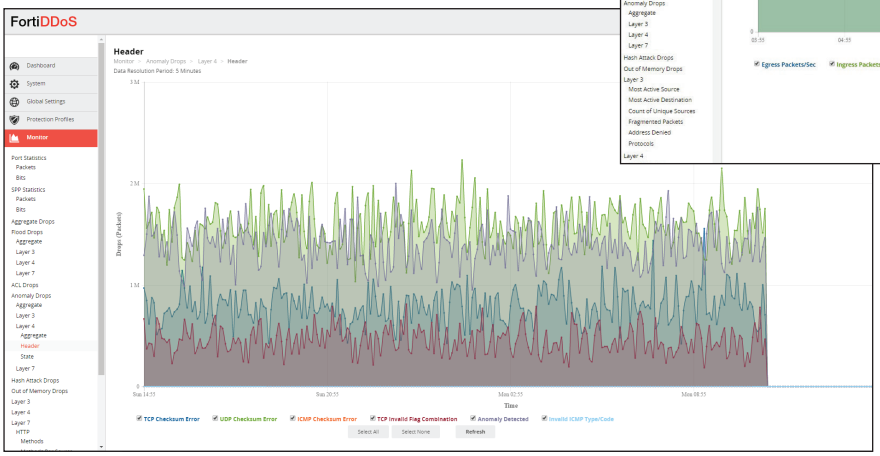
Riadenie

- GUI pre správu SSL
- CLI
- Otvorené rozhranie RESTful API
- Overenie RADIUS, LDAP, a TACACS+
- Portál MSSP pre viacerých používateľov
- Vytvorenie skriptov Flowspec
- Aktuálne upozornenia útoku
- Otvorenie signalizácie zmiernenia cloudu



Dashboard zobrazenie stavu a udalostí

Štatistiky SPP: Monitorovanie paketov



Vyčleňovanie anomálií hlavičky na vrstve 4

TECHNICKÉ ÚDAJE

	FORTIDDOS 200B	FORTIDDOS 400B	FORTIDDOS 600B	FORTIDDOS 800B
Technické vybavenie zariadenia				
LAN rozhrania Copper GE so zabudovaným premostením	4	8	8	8
WAN rozhrania Copper GE so zabudovaným premostením	4	8	8	8
LAN rozhrania SFP GE	4	8	8	8
WAN rozhrania SFP GE	4	8	8	8
LAN rozhrania SFP+ 10 GE / SFP GE	—	—	—	—
WAN rozhrania SFP+ 10 GE / SFP GE	—	—	—	—
LAN rozhrania LC (850 nm, 10 GE) so zabudovaným premostením	—	—	—	—
WAN rozhrania LC (850 nm, 10 GE) so zabudovaným premostením	—	—	—	—
Úložisko	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Mierka formy	Zariadenie 1U	Zariadenie 1U	Zariadenie 1U	Zariadenie 1U
Napájací zdroj	Jednoduché (voliteľné externé Dual Hot-Swappable)	Jednoduché (voliteľné externé Dvojitá výmena počas prevádzky)	Jednoduché (voliteľné externé Dvojitá výmena počas prevádzky)	Jednoduché (voliteľné externé Dvojitá výmena počas prevádzky)
Výkon systému				
Priepustnosť (Enterprise Mix — Gbps)	3	6	12	12
Priepustnosť paketov (Mpps)	4	8	16	16
Oneskorenie (ps) maximum/štandard	<50/<10	<50/<10	<50/<10	<50/<10
Reakčný čas na zmiernenie DDoS (s)	<2	<2	<2	<2
Rozšírené zmiernenie DNS (Firmware v4.2.0)	Áno	Áno	Nie	Áno
DNS dotazy za sekundu (M)	1	2	N/A	4
Otvorená podpora hybridného zmierňovania cloudov	Áno	Áno	Áno	Áno
Prostredie				
Vstupné napätie AC	100–240V AC, 50-60 Hz	100–240V AC, 50-60 Hz	100–240V AC, 50-60 Hz	100–240V AC, 50-60 Hz
Vstupné napätie DC	—	—	—	—
Spotreba energie (priemerne)	156 W	156 W	174 W	174 W
Spotreba energie (maximálne)	260 W	260 W	285 W	285 W
Maximálny prúd AC	110V/5,29A, 120V/2,2A	110V/5,29A, 120V/2,2A	110V/5,29A, 220V/2,2A	110V/5,29A, 120V/2,2A
Maximálny prúd DC	—	—	—	—
Rozptyl tepla (BTU/hr) / (kjoules/hr)	887/936	887/936	972/1026	972/1026
Prevádzková teplota	32–104 °F (0–40 °C)	32–104 °F (0–40 °C)	32–104 °F (0–40 °C)	32–104 °F (0–40 °C)
Teplota skladovania	-13–158 °F (-25–70 °C)	-13–158 °F (-25–70 °C)	-13–158 °F (-25–70 °C)	-13–158 °F (-25–70 °C)
Vlhkosť	5–95 % bez kondenzácie	5–95 % bez kondenzácie	5–95 % bez kondenzácie	5–95 % bez kondenzácie
Dodržiavanie predpisov				
Bezpečnostné certifikáty	FCC Trieda A Časť 15, UL/CB/cUL, C-Tick, VCCI, CE			
Rozmery				
Výška x šírka x dĺžka (palce)	1,77 x 17 x 16,32	1,77 x 17 x 16,32	1,77 x 17 x 16,32	1,77 x 17 x 16,32
Výška x šírka x dĺžka (mm)	45 x 432 x 414,5	45 x 432 x 414,5	45 x 432 x 414,5	45 x 432 x 414,5
Hmotnosť	17,2 lbs (7,8 kg)	17,2 lbs (7,8 kg)	17,2 lbs (7,8 kg)	17,2 lbs (7,8 kg)

FortiDDoS 200B

FortiDDoS 400B

FortiDDoS 600B

FortiDDoS 800B

TECHNICKÉ ÚDAJE

	FORTIDDOS 900B	FORTIDDOS 1000B / FORTIDDOS 1000B-DC	FORTIDDOS 1200B
Technické vybavenie zariadenia			
LAN rozhrania Copper GE so zabudovaným premostením	—	—	—
WAN rozhrania Copper GE so zabudovaným premostením	—	—	—
LAN rozhrania SFP GE	—	—	—
WAN rozhrania SFP GE	—	—	—
LAN rozhrania SFP+ 10 GE / SFP GE	8	8	8
WAN rozhrania SFP+ 10 GE / SFP GE	8	8	8
LAN rozhrania LC (850 nm, 10 GE) so zabudovaným premostením	—	—	2
WAN rozhrania LC (850 nm, 10 GE) so zabudovaným premostením	—	—	2
Úložisko	1x 480 GB SSD	1x 480 GB SSD	1x 480 GB SSD
Mierka formy	Zariadenie 2U	Zariadenie 2U	Zariadenie 2U
Napájací zdroj	Dvojitá výmena počas prevádzky	Dvojitá výmena počas prevádzky	Dvojitá výmena počas prevádzky
Výkon systému			
Priepustnosť (Enterprise Mix — Gbps)	18	18	36
Priepustnosť paketov (Mpps)	24	24	48
Oneskorenie (ps) maximum/štandard	<50/<10	<50/<10	<50/<10
Reakčný čas na zmiernenie DDoS (s)	<2	<2	<2
Rozšírené zmiernenie DNS (Firmware v4.2.0)	Nie	Áno	Áno
DNS dotazy za sekundu (M)	N/A	6	12
Otvorená podpora hybridného zmierňovania cloudov	Áno	Áno	Áno
Prostredie			
Vstupné napätie AC	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz
Vstupné napätie DC	—	40,5-57V DC	—
Spotreba energie (priemerne)	253 W	253 W	311 W
Spotreba energie (maximálne)	422 W	422 W	575 W
Maximálny prúd AC	110V/10,0A, 220V/5,0A	110V/10,0A, 120V/5,0A	110V/10,0A, 120V/5,0A
Maximálny prúd DC	—	24 A	—
Rozptyl tepla (BTU/hr) / (kjoules/hr)	1440/1420	1440/1420	1962/2070
Prevádzková teplota	32-104 °F (0-40 °C)	32-104 °F (0-40 °C)	32-104 °F (0-40 °C)
Teplota skladovania	-13-158 °F (-25-70 °C)	-13-158 °F (-25-70 °C)	-13-158 °F (-25-70 °C)
Vlhkosť	5-95 % bez kondenzácie	5-95 % bez kondenzácie	5-95 % bez kondenzácie
Dodržiavanie predpisov			
Bezpečnostné certifikáty		FCC Trieda A Časť 15, UL/CB/cUL, C-Tick, VCCI, CE	
Rozmery			
Výška x šírka x dĺžka (palce)	3,5 x 17,24 x 22,05	3,5 x 17,24 x 22,05	3,5 x 17,24 x 22,05
Výška x šírka x dĺžka (mm)	88 x 438 x 560	88 x 438 x 560	88 x 438 x 560
Hmotnosť	36,0 lbs (16,2 kg)	36,0 lbs (16,2 kg)	36,0 lbs (16,2 kg)

FortiDDoS 900B

FortiDDoS 1000B

FortiDDoS 1200B

INFORMÁCIE O OBJEDNÁVKE

PRODUKT	SKU	POPIS
FortiDDoS 200B	FDD-200B	DDoS Protection Appliance — 4 páry x Zdieľané médiá DDoS Obranné porty (vrátane 4 párov x GE RJ45 s ochranou premostenia, 4 páry x GE SFP sloty), 2x GE RJ45 Manipulačné porty, napájací zdroj s redundantným napájaním. Obsahuje úložisko 480 GB SSD, priepustnosť 3 Gbps, podporuje Advanced DNS Mitigation,
FortiDDoS 400B	FDD-400B	DDoS Protection Appliance — 8 párov x Zdieľané médiá DDoS Obranné porty (vrátane 8 párov x GE RJ45 s ochranou premostenia, 8 párov x GE SFP sloty), 2x GE RJ45 Manipulačné porty, napájací zdroj s redundantným napájaním, vrátane úložiska 480 GB SSD, priepustnosť 6 Gbps, podporuje Advanced DNS Mitigation,
FortiDDoS 600B	FDD-600B	DDoS Protection Appliance — 8 párov x Zdieľané médiá DDoS Obranné porty (vrátane 8 párov x GE RJ45 s ochranou premostenia, 8 párov x GE SFP sloty), 2x GE RJ45 Manipulačné porty, napájací zdroj s redundantným napájaním, vrátane úložiska 480 GB SSD, priepustnosť 12 Gbps, podporuje Advanced DNS Mitigation,
FortiDDoS 800B	FDD-800B	DDoS Protection Appliance — 8 párov x Zdieľané médiá DDoS Obranné porty (vrátane 8 párov x GE RJ45 s ochranou premostenia, 8 párov x GE SFP sloty), 2x GE RJ45 Manipulačné porty, napájací zdroj s redundantným napájaním, vrátane úložiska 480 GB SSD, priepustnosť 12 Gbps, podporuje Advanced DNS Mitigation,
FortiDDoS 900B	FDD-900B	DDoS Protection Appliance — 8 párov x 10 GE SFP+ DDoS Obranné porty (tiež podpora GE SFP), 2x GE RJ45 Manipulačné porty, dvojitý napájací zdroj, vrátane úložiska 480 GB SSD a 2x 10 GE SR SFP+, priepustnosť 18 Gbps, bez podpory Advanced DNS Mitigation,
FortiDDoS 1000B	FDD-1000B	DDoS Protection Appliance — 8 párov x 10 GE SFP+ DDoS Obranné porty (tiež podpora GE SFP), 2x GE RJ45 Manipulačné porty, dvojitý napájací zdroj, vrátane úložiska 480 GB SSD a 2x 10 GE SR SFP+, priepustnosť 18 Gbps, podpora Advanced DNS Mitigation,
FortiDDoS 1000B-DC	FDD-1000B-DC	DDoS Protection Appliance — 8 párov x 10 GE SFP+ DDoS Obranné porty (tiež podpora GE SFP), 2x GE RJ45 Manipulačné porty, dvojitý napájací zdroj, vrátane úložiska 480 GB SSD a 2x 10 GE SR SFP+, priepustnosť 18 Gbps, podpora Advanced DNS Mitigation,
FortiDDoS 1200B	FDD-1200B	DDoS Protection Appliance — 8 párov x 10 GE SFP+ DDoS Obranné porty (tiež podpora GE SFP), 2 páry x 10 GE LC porty s optickým premostením, 2x GE RJ45 Manipulačné porty, dvojitý napájací zdroj, vrátane úložiska 480 GB SSD a 2x 10 GE SR SFP+, priepustnosť 36 Gbps, podpora Advanced DNS Mitigation,
Kompatibilné transceivery FortiDDoS		
Transceivery FortiDDoS	FG-TRAN-LX	1 Modul transceiver GE SFP LX pre všetky systémy so SFP a SFP/SFP+
	FG-TRAN-GC	1 Modul transceiver GE SFP RJ45 pre všetky systémy so SFP a SFP/SFP+
	FG-TRAN-SX	1 Modul transceiver GE SFP SX pre všetky systémy so SFP a SFP/SFP+
	FG-TRAN-SFP+SR	10 Modul transceiver GE SFP, krátky dosah pre všetky systémy so SFP a SFP/SFP+
	FG-TRAN-SFP+LR	10 Modul transceiver GE SFP+, dlhý dosah pre všetky systémy so SFP a SFP/SFP+
	SP-CABLE-ADASFP+	10 GE SFP+ aktívny kábel, 10 m / 32,8 stôp pre všetky systémy so SFP+ a SFP/SFP+
Voliteľné príslušenstvo		
Externý redundantný napájací zdroj	FRPS-100	Externý redundantný napájací zdroj až pre 4 jednotky: FG-300C, FG-310B, FS-348B a FS-448B. Až pre 2 jednotky: FG-200B, FG-200D, FG-240D and FG-300D, FG-500D, FDD-200B, FDD-400B, FDD-600B a FDD-800B. Nepodporuje: FG-200D-POE/240D-POE

HLAVNÉ SÍDLO
Fortinet Inc.
899 KIFER ROAD
Sunnyvale, CA 94086
USA
Tel: +1 408 235 7700
www.fortinet.com/sales

POBOČKA EMEA
905 Rue Albert Einstein
06560 Valbonne
Francúzsko
Tel: +33 4 8987 0500

POBOČKA APAC
8 Temasek Boulevard
#12-01 Suntec Tower Three
Singapur 038988
Tel: +65 6395 2788

POBOČKA LATINSKÁ AMERIKA
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
USA
Tel: +1 954 368 9990