

FortiGate™ -50-100 Series

Uffici Periferici/Filiali
Small-Medium Business
Customer Premise Equipment

Datasheet

Soluzioni di Unified Threat Management

Le minacce alla Sicurezza all'interno delle Piccole e Grandi Aziende

La criminalità informatica e gli attacchi alla rete rappresentano una grave minaccia per le piccole imprese. Proprietà intellettuale, fatturati, dati clienti e altre risorse mission-critical sono a rischio. Più le Grandi imprese lavorano per rendere sicure le loro reti, e più le minacce alla sicurezza vengono dirette alle imprese più piccole. L'ambiente Small Office/Home Office (SOHO) spesso manca di infrastrutture dedicate a rispondere alle più complesse ed attuali tecniche di attacco e gli uffici Remoti/Filiali (ROBO) spesso sono carenti di competenze in loco per affrontare le complesse questioni di sicurezza. I dispositivi di sicurezza point-based sono insufficientemente equipaggiati di adeguata protezione contro questi tipi di attacchi a causa della moltitudine di vettori di attacco utilizzati.

La gamma di strumenti di sicurezza Fortinet FortiGate dedicate a SOHO e ROBO integrano un'elevata protezione multi-minaccia su una piattaforma progettata appositamente per bloccare efficacemente attacchi alla rete e ad applicazioni.

Piattaforma di Sicurezza Conveniente

La gamma di strumenti di sicurezza Fortinet Fortigate offre prestazioni elevate e protezione multi-minaccia ad un costo interessante, ideale per rendere sicuri i piccoli ambienti di lavoro.

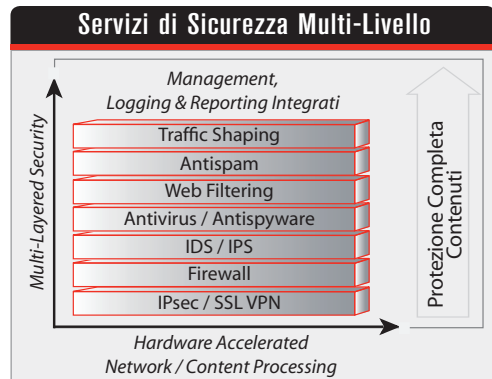
Caratteristiche di Unified Threat Management (UTM) quali Firewall, VPN, Intrusion Prevention, Web Filtering, Antispam, Antivirus, Antispyware, Traffic Shaping e Controllo IM/P2P permettono di prevenire attacchi combinati o utilizzi non autorizzati finalizzati a bloccare le attività aziendali. Tutti i dispositivi Fortinet supportano le configurazioni in High Availability (HA) per assicurare la massima disponibilità dei servizi. Gli strumenti Fortinet, oltre ad operare in modalità transparent e routing, sono disponibili in configurazioni che integrano switch, modem, access point WiFi e slot Pccard per modem 3G/UMTS, tutti elementi che consentono ai dispositivi FortiGate di adattarsi a qualsiasi tipologia di rete.

Inoltre, grazie ai servizi Fortinet FortiGuard Security Subscription, la serie FortiGate-50, fino alla serie 100, diventa una soluzione di sicurezza dedicata a uffici periferici e filiali di aziende, conveniente e facile da gestire, sia per fornitori di servizi di Customer Premise Equipment (CPE) sia quale soluzione All-in-one per le piccole e medie imprese.

Principali Problemi	Soluzioni	
<ul style="list-style-type: none"> Gli Small Office e Home Office (SOHO) sono particolarmente vulnerabili agli attacchi informatici a causa della mancanza di risorse e budget necessari ad affrontare reti complesse e minacce content-based. 	Un sistema di Unified Threat Management (UTM) All-in-one che fornisce protezione multi-livello dalle minacce tramite aggiornamenti automatici, il tutto in un pacchetto conveniente	<p>FortiGate-50B</p>
<ul style="list-style-type: none"> L'utilizzo di prodotti provenienti da diversi produttori non fornisce una protezione integrata dalle minacce di tipo combinato ed è costoso e complesso da mantenere 	Una soluzione di sicurezza UTM che offre servizi restrittivi di protezione con un'interfaccia unificata di gestione, logging e reportistica	<p>FortiWiFi-50B</p>
<ul style="list-style-type: none"> L'adozione di tecnologie wireless Wi-Fi apre nuove possibilità di attacco dall'interno della rete 	L'integrazione del WiFi Wireless assicura il medesimo livello di protezione sia sulla rete cablata sia su quella wireless	<p>FortiGate-60B</p>
<ul style="list-style-type: none"> La conformità ai requisiti SOX e PCI aggiunge una nuova dimensione di complessità di logging e reportistica 	Tools unificati da un'interfaccia utente comune per semplificare l'analisi, la reportistica e la conformità di gestione	<p>FortiWiFi-60B</p>
		<p>FortiGate-100A</p>

La Soluzione di Fortinet

La soluzione di sicurezza multi-livello Fortinet offre una serie di servizi di sicurezza integrata, efficiente e conveniente, tutto questo con un unico dispositivo ad alte prestazioni, facile da gestire e in grado di supportare una vasta gamma di scenari di implementazione. Inoltre i Servizi FortiGuard Subscription, coprono ogni necessità: supporto tecnico, aggiornamenti Antivirus, Antispam e Web Content Filtering, per assicurare che il vostro ambiente di sicurezza resti attuale e le vostre risorse aziendali siano protette contro le ultime minacce. Tutti i sistemi FortiGate sono in possesso di un anno di garanzia limitata sull'hardware e 90 giorni di garanzia limitata sul software.



Le appliance FortiGate 50-100 series sono state progettate per rendere sicure le reti di piccoli uffici ed imprese

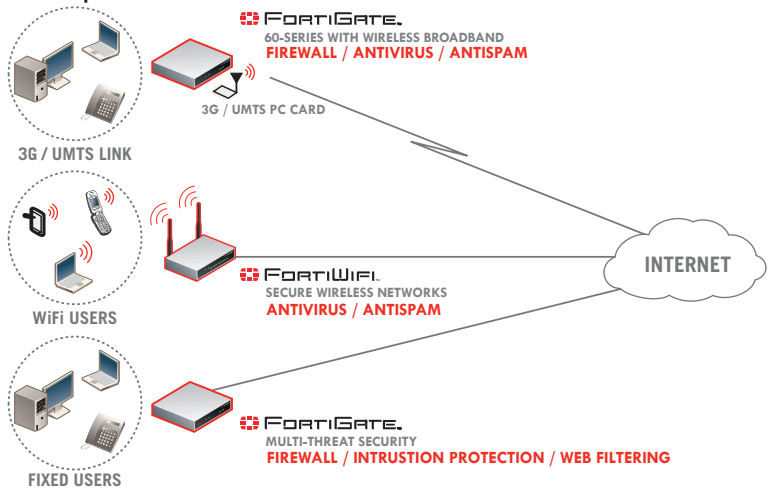
Gateway di sicurezza per reti cablate e wireless per le piccole imprese

Firewall + Antivirus + Antispam + Intrusion Prevention + Web Filtering

Attraverso l'integrazione di tecnologie essenziali in materia di sicurezza, Fortinet protegge sia i lavoratori mobili, sia le postazioni di lavoro in ambiente SOHO e ROBO.

Per mantenere al sicuro le risorse, i sistemi avanzati Antivirus, Antispyware, Antispam e Intrusion Prevention, Fortinet utilizza il processore integrato FortiASIC ed una combinazione di signature e motori di rilevamento euristico multi-livello, per una protezione real-time da una moltitudine di attacchi.

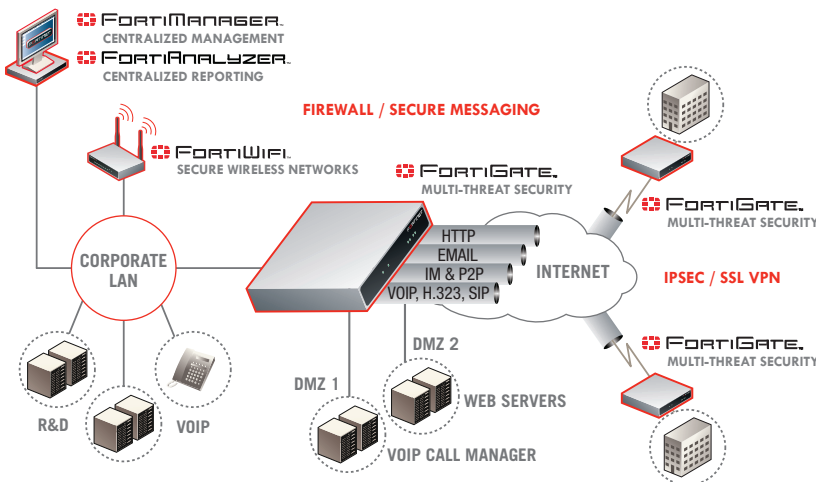
La gamma FortiWifi offre la possibilità di trasmettere SSID (Service Set Identifiers) multiple, massimizzando la flessibilità di infrastrutture multi-provider e limitando lo spettro. Inoltre, possono essere impostate differenti policy di sicurezza per ciascun SSID, aumentando la flessibilità di sicurezza. Per garantire una connettività di rete sicura i modelli della serie FortiGate-60 implementano uno slot PC Card che consente di utilizzare una PC Card 3G/UMTS



Installazione ROBO in ambienti Enterprise

Firewall + VPN + Messaggistica Sicura (Email, IM e P2P)

I lavoratori presenti in uffici remoti spesso eseguono compiti diversi tramite differenti processi aziendali: alcuni utilizzano applicazioni di messaggistica, mentre altri utilizzano applicazioni database. Gli uffici vendite, ad esempio, utilizzano e-mail e applicazioni di messaggistica istantanea e saranno protetti dalle minacce combinate che utilizzano più metodi per attaccare i sistemi: virus, che generano trojan dormienti, quali rootkit e bot. La combinazione delle tecnologie Fortinet Antivirus e Antispam e dei Controlli IM e P2P, permetteranno di proteggere gli utilizzatori di programmi di posta elettronica e di messaggistica immediata, impedendo perdite di fatturato o perdite dati. Gli utenti di applicazioni e database, presenti in un sito remoto di produzione, avranno una connettività sicura, tramite Firewall e VPN, verso i server applicativi da utilizzare presso la sede centrale. Infine, Fortinet offre una soluzione completa di gestione centralizzata per il monitoraggio, reporting, logging e analisi al fine di garantire il funzionamento di tutti gli uffici remoti.

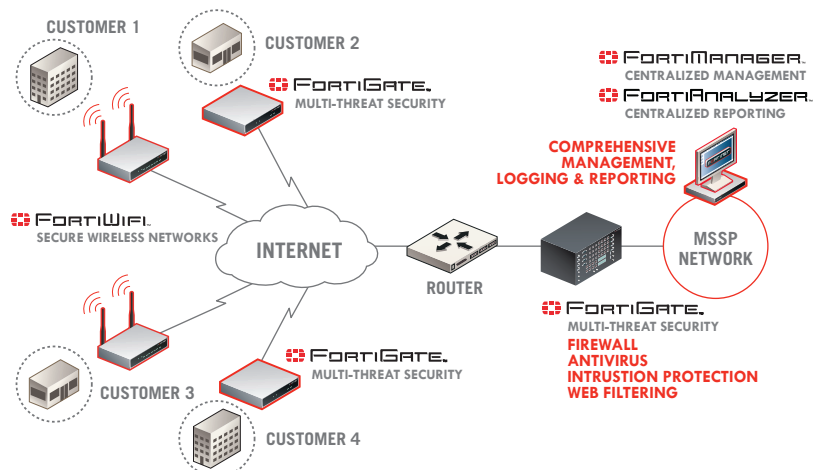


Distribuzione Managed Security Service Provider

Firewall + Antivirus + Intrusion Prevention + Web Filtering

Grazie alla vasta gamma di opzioni di connettività e all'architettura di sicurezza modulare, i Managed Security Service Providers (MSSP) possono distribuire le appliance FortiGate unitamente alle installazioni dei loro Customer Premise Equipment (CPE).

Clienti differenti possono essere protetti in modi diversi ed in base alle loro esigenze. Per esempio, un gruppo di clienti può essere protetto con un firewall ed un sistema di intrusion prevention, mentre un altro può essere protetto con un Firewall e Web Content Filtering. Gli MSSP possono controllare e gestire centralmente tutti i clienti che utilizzano FortiManager e FortiAnalyzer, ottenendo una reportistica end to end, il logging e l'analisi forense degli eventi legati alla sicurezza.



Specifiche Tecniche



SPECIFICHE HARDWARE	FortiGate-50B	FortiWiFi-50B	FortiGate-60B	FortiWiFi-60B	FortiGate-100A
LAN Switching					
Interfacce	3	3	6	6	4
WAN Interfacce	2	2	2	2	2
DMZ Interfacce			1	1	2
Modem analogico			Si	Si	
Wireless LAN					
802.11a/b/g		802.11 b/g		802.11 a/b/g	
Porte USB	2	2	2	2	2
Power Over Ethernet (PoE)		Si			
Slot PC Card*			Si	Si	
VDOMs supportati	10	10	10	10	10

* la PC card viene venduta separatamente

PERFORMANCE SISTEMA *

Throughput Firewall	50 Mbps	50 Mbps	100 Mbps	100 Mbps	100 Mbps
Throughput VPN 3DES	48 Mbps	48 Mbps	64 Mbps	64 Mbps	40 Mbps
Throughput Antivirus	19 Mbps	19 Mbps	20 Mbps	20 Mbps	20 Mbps
Throughput IPS	30 Mbps	30 Mbps	60 Mbps	60 Mbps	70 Mbps
Tunnel IPSec VPN Dedicati	20	20	50	50	80
Licenze User illimitate	Si	Si	Si	Si	Si
Sessioni contemporanee	25,000	25,000	70,000	70,000	200,000
Nuove Sessioni/Secondo	2,000	2,000	3,000	3,000	4,000
Policies	2,000	2,000	2,000	2,000	2,000

* La performance dell'antivirus è misurata sulla base di traffico HTTP con 32Kbyte di file allegati e le prestazioni IPS sono misurate sulla base del traffico UDP con 512 byte di dimensioni del pacchetto
Le prestazioni effettive possono variare a seconda del traffico sulla rete e l'ambiente

DIMENSIONI	FortiGate-50B	FortiWiFi-50B	FortiGate-60B	FortiWiFi-60B	FortiGate-100A
(H, W, L, weight)	1.38 pollici 8.63 pollici 5.8 pollici 1.5 libbre	1.38 pollici 8.63 pollici 5.8 pollici 1.5 libbre	1.75 pollici 10.87 pollici 6.13 pollici 5.5 libbre	1.75 pollici 10.87 pollici 6.13 pollici 5.5 libbre	1.75 pollici 10.87 pollici 6.13 pollici 3.35 libbre

AC POWER 100-240 VAC, 50-60 Hz, 8.0 Amp (Max)

CONSUMO ALIMENTAZIONE (MEDIO) 6W 6W 15W 15W 14W

AMBIENTALI Temperatura Operativa: da 0° to 40° C
Temperatura Stoccaggio: -13 to 158 deg F (-25 to 70 deg C)
Umidità: 5 to 95% non-condensante

CONFORMITA' FCC Class A Part 15 (FG-100A), FCC Class B Part 15 (FG-50-60),
UL/CUL, C Tick, CE, VCCI

CERTIFICAZIONI Certificazioni ICSA Labs: Firewall, Antivirus, IPS, IPSec VPN, SSL-VPN
NSS Labs Approved (UTM), Common Criteria (EAL 4+), FIPS 140-2

(Si prega di contattare il vostro account vendite Fortinet per un elenco completo delle certificazioni prodotto)

Soluzioni Unified Security Fortinet

- All-inclusive, soluzione di sicurezza conveniente**
 Fortinet offre un basso TCO (total cost of ownership) con il più completo set di funzioni tra cui: Antivirus, Intrusion Prevention, Antispyware, Web Content Filtering e Antispam
- Aggiornamenti automatici di Antivirus/Antispyware e Sicurezza IPS**
 Protezione a 360° contro le più recenti minacce. Enciclopedia virus e intrusioni, copre più di 60.000 diverse minacce
- Contenuti personalizzati ad alte prestazioni hardware**
 Fortinet FortiASIC offre prestazioni superiori e affidabilità, garantendo che le applicazioni di sicurezza non diventino il collo di bottiglia della rete
- Switch multi-porta integrato**
 Elimina la necessità di switch esterni e fornisce maggiori opzioni di connettività
- Interfaccia utente sicura per una facile implementazione e gestione**
 Procedura di configurazione guidata rapida e facile: guida gli amministratori di rete attraverso la configurazione iniziale o l'interfaccia grafica utente che permette il controllo delle performance e gli eventi di sicurezza in un colpo d'occhio
- Sistema Operativo (OS) di personalizzato e security hardened**
 Il sistema operativo FortiOSTM è certificato ICSA Labs e offre anche una completa interfaccia a linea di comando

I vantaggi dell'ASIC Fortinet

FortiASIC è il fondamento dell'esclusiva tecnologia hardware Fortinet. FortiASIC è una famiglia di processori di rete e contenuti ad alte prestazioni appositamente progettati per accelerare i calcoli altamente intensivi dei servizi di sicurezza, che utilizzano un motore intelligente di scansione di contenuti e di algoritmi multipli. FortiASIC fornisce le prestazioni necessarie per fornire servizi UTM di classe enterprise e carrier. Associato con FortiOS sistema operativo security hardened, FortiASIC offre prestazioni e sicurezza estreme.

FortiOS: Sviluppato per la Sicurezza

FortiOS è il software alla base della piattaforma di sicurezza multi-minaccia FortiGate. Sviluppato esclusivamente per la sicurezza, le prestazioni e l'affidabilità, FortiOS è un sistema operativo appositamente progettato per sfruttare la potenza dei processori di rete e contenuti FortiASIC. FortiOS gestisce una completa suite di servizi di sicurezza - Firewall di ispezione contenuti, IPS, Antivirus, Web Filtering, Antispam, IM/P2P, Sicurezza di Reti virtuali e Bandwidth Shaping. FortiOS è una suite completa di servizi di sicurezza UTM ed è certificato Common Criteria EAL 4 +

FortiGate-50-100 Series



Le piattaforme FortiGate-50-100-series forniscono le seguenti caratteristiche di sicurezza:

FIREWALL

ICSA Labs Certified (Enterprise Firewall)
NAT, PAT, Transparent (Bridge)
Routing Mode (RIP v1 & v2, OSPF, BGP, & Multicast)
Policy-Based NAT
Virtual Domains (NAT/Transparent mode)
VLAN Tagging (802.1Q)
User Group-Based Authentication
SIP/H.323 NAT Traversal
WINS Support
Customized Protection Profiles

VIRTUAL PRIVATE NETWORK (VPN)

ICSA Labs Certified (IPSec & SSL)
PPTP, IPSec, and SSL
Dedicated Tunnels
DES, 3DES, and AES Encryption Support
SHA-1/MD5 Authentication
PPTP, L2TP, VPN Client Pass Through
Hub and Spoke VPN Support
IKE Certificate Authentication
IPSec NAT Traversal
Dead Peer Detection
RSA SecurID Support

INTRUSION PREVENTION SYSTEM (IPS)

ICSA Labs Certified (NIPS)
Protection From Over 3000 Threats
Protocol Anomaly Support
Custom Signature Support
Automatic Attack Database Update

ANTIVIRUS

ICSA Labs Certified (Gateway Antivirus)
Includes AntiSpyware and Worm Prevention
HTTP/SMTP/POP3/IMAP/FTP/IM and Encrypted VPN Tunnels
Automatic "Push" Virus Database Update
File Quarantine Support
Block by File Size or Type

WEB FILTERING

URL/Keyword/Phrase Block
URL Exempt List
Content Profiles
Blocks Java Applet, Cookies, Active X
FortiGuard Web Filtering Support

ANTISPAM

Real-Time Blacklist/Open Relay Database Server
MIME Header Check
Keyword/Phrase Filtering
IP Address Blacklist/Exempt List
Automatic Real-Time Updates From FortiGuard Network

TRAFFIC SHAPING

Policy-based Traffic Shaping
Differentiated Services (DiffServ) Support
Guarantee/Max/Priority Bandwidth

NETWORKING/ROUTING

Multiple WAN Link Support
PPPoE Support
DHCP Client/Server
Policy-Based Routing
Dynamic Routing (RIP v1 & v2, OSPF, BGP, & Multicast)
Multi-Zone Support with Routing Between Zones
Route Between Virtual LANs (VDOMS)

MANAGEMENT/ADMINISTRATION OPTIONS

Console Interface (RS-232)
WebUI (HTTP/HTTPS) and Command Line Interface
Telnet / Secure Command Shell (SSH)
Role-Based Administration
Multi-language Support
Multiple Administrators and User Levels
Upgrades and Changes Via FTP and WebUI
System Software Rollback
Central Management via FortiManager (optional)

LOGGING/MONITORING

Internal Logging
Log to Remote Syslog/WELF server
Graphical Real-Time and Historical Monitoring
SNMP
Email Notification of Viruses And Attacks
VPN Tunnel Monitor
Optional FortiAnalyzer Logging

USER AUTHENTICATION OPTIONS

Local Database
Windows Active Directory (AD) Integration
External RADIUS/LDAP Integration
IP/MAC Address Binding
Xauth over RADIUS for IPSEC VPN
RSA SecurID Support

VIRTUAL DOMAINS (VDOMS)

Separate Firewall/Routing domains
Separate Administrative domains
Separate VLAN interfaces
10 VDOMS (standard)

HIGH AVAILABILITY (HA)

Active-Active, Active-Passive
Stateful Failover (FW and VPN)
Device Failure Detection and Notification
Link Status Monitor
Link failover

INSTANT MESSENGER /

PEER-TO-PEER ACCESS CONTROL

AOL-IM	Yahoo	MSN
ICQ	Gnutella	BitTorrent
WinNY	Skype	eDonkey
KaZaa		

Servizi FortiGuard Security Subscription

Con l'abilitazione dei servizi FortiGuard™ Security Subscription, i clienti possono essere certi che le loro piattaforme di sicurezza Fortinet performano ottimamente tutelando i beni aziendali con la più recente intelligenza di sicurezza. I servizi FortiGuard forniscono i contenuti di sicurezza più aggiornati direttamente ai prodotti Fortinet. Fortinet offre quattro servizi standard di abbonamento: Antivirus, Intrusion Prevention, Web Filtering e Antispam, servizi di protezione contro tipologie molteplici di nuove ed emergenti minacce. I servizi FortiGuard sono aggiornati dal Fortinet Global Threat Research Team, un team di esperti che opera 24 ore su 24 per mantenere al sicuro i clienti Fortinet. Il Team Fortinet Global Threat Research di Fortinet consente di fornire una completa protezione multi-minaccia, compresa una protezione "zero-day" da nuove ed emergenti minacce. Il FortiGuard Network è una rete globale di centri dati che fornisce aggiornamenti automatici per i prodotti Fortinet in modo rapido e affidabile.

Per i clienti che richiedono tempi di risposta garantiti in caso di sospette minacce e malware, Fortinet offre una versione di servizio di abbonamento premier per FortiGuard protezione Antivirus. Insieme con il Service Level Agreement (SLA), il servizio premier fornisce al cliente un rapporto diretto con il Team Fortinet Global Threat Research. Fortinet, offre anche una versione premier del servizio di sicurezza abbonamento FortiGuard Web Filtering. Questo più elevato livello di servizio garantito comprende lo SLA e una più ampia quota di rating URL sottomesse a Team Fortinet Global Threat Research.

Servizi di Supporto FortiCare

Include:

- Supporto FortiCare 24/7/365 basato su Web
- Supporto tecnico telefonico 8x5 (24x7 - opzionale)
- 1 anno di garanzia limitata hardware
- Disponibilità del servizio di gestione tecnica
- Disponibilità di servizi professionali
- Garanzia limitata 90-giorni sul software



FORTINET

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com/sales

EMEA SALES OFFICE-FRANCE

Fortinet Incorporated
120 Rue Albert Caquot
06560 Sophia Antipolis, France
Tel +33-4-8987-0510
Fax +33-4-8987-0501

APAC SALES OFFICE-HONG KONG

Fortinet Incorporated
Room 2429-2431, 244F Sun Hung Kai Centre
No.30 Harbour Road, WanChai, Hong Kong
Tel +852-3171-3000
Fax +852-3171-3008