

Progettazione esecutiva

FESRPON reti - plessi Istituto Comprensivo – Roccastrada (GR)



**Al Dirigente Scolastico
ISTITUTO COMPRENSIVO
Roccastrada (GR)**

Oggetto

Progettazione esecutiva per la realizzazione di una rete nei diversi plessi dell'Istituto - progetto 13.1.1A-FESRPON-TO-2021-308 - "Cablaggio strutturato e sicuro all'interno degli edifici scolastici" - CUP D69J21011570006.

Premessa

Il sottoscritto Alessandro Salvini, individuato come progettista con incarico del 14/03/2022 prot. 0002352/2022 a seguito della selezione di esperto interno all'istituto/dipendente da altri istituti per l'attività di Progettazione prot. 1643 del 21 febbraio 2022, ha provveduto ad effettuare le seguenti fasi preliminari dell'attività progettuale.

Presa d'atto del progetto Fondi Strutturali Europei – Programma Operativo Nazionale “Per la scuola, competenze e ambienti per l'apprendimento” 2014-2020. Asse II - Infrastrutture per l'istruzione – Fondo Europeo di Sviluppo Regionale (FESR) – REACT EU. Asse V – Priorità d'investimento: 13i – (FESR) “Promuovere il superamento degli effetti della crisi nel contesto della pandemia di COVID-19 e delle sue conseguenze sociali e preparare una ripresa verde, digitale e resiliente dell'economia” – Obiettivo specifico 13.1: Facilitare una ripresa verde, digitale e resiliente dell'economia. - Azione 13.1.1 “Cablaggio strutturato e sicuro all'interno degli edifici scolastici” – Avviso pubblico prot.n. 20480 del 20/07/2021 per la realizzazione di reti locali, cablate e wireless, nelle scuole.

Vista l'autorizzazione del progetto **13.1.1A-FESRPON-TO-2021-308**, CUP **D69J21011570006**, ove gli interventi prevedono la realizzazione o il potenziamento delle reti locali cablate e wireless degli edifici scolastici;

Visto l'obiettivo di dotare gli edifici scolastici di un'infrastruttura di rete capace di coprire gli spazi didattici nonché di consentire la connessione alla rete da parte del personale scolastico assicurando, altresì, la sicurezza informatica dei dati. Gli interventi prevedono la realizzazione o il potenziamento delle reti locali cablate e wireless degli edifici scolastici, comprensivi di fornitura di materiali e strumenti per la realizzazione di cablaggi strutturati, fornitura e installazione di apparati attivi, switch, prodotti per l'accesso wireless, dispositivi per la sicurezza delle reti e servizi, compresi sistemi di autenticazione degli utenti, nel rispetto delle norme vigenti in materia di accessibilità ai sistemi informatici e telematici della Pubblica Amministrazione, di tutela della privacy e di sicurezza informatica dei dati, nonché delle norme vigenti in materia di protezione dell'ambiente e di risparmio energetico.

Visto l'impegno di spesa totale per la realizzazione o potenziamento delle reti locali di € 70.751,15 di cui € 60.138,48 per le forniture (pari a € **49.293,83 + IVA 22%**); forniture che comprendono elementi di rete passivi e apparati di rete attivi, servizi accessori e piccoli interventi edilizi accessori alla fornitura;

Viene effettuato il sopralluogo presso le sedi interessate dall'intervento, di seguito riportate:

	PLESSI
1.	Scuola Infanzia/Primaria/Uffici Via Salvo D'Acquisto
2.	Scuola Secondaria di primo grado Via de Sanctis Roccastrada
3.	Scuola Primaria Sassofortino Via Cavour
4.	Scuola Infanzia Roccatederighi Via Gorizia
5.	Scuola Infanzia Ribolla Piazzetta della libertà
6.	Scuola Infanzia/Primaria Sticciano Via dei Mille

Preso atto della necessità di implementare la copertura di rete nelle aule dei vari plessi sopra menzionati, sia per quanto riguarda le aule tradizionali che speciali, laboratori, aula magna, ecc.

Preso atto delle necessità di rendere ottimale la fruizione dell'accesso alla rete dalle aule delle suddette sedi.

In questa sede di progettazione esecutiva, a seguito di sopralluogo, verifica delle necessità effettive dell'istituto, confronto con il personale tecnico dell'Istituto per valutare le necessità operative e le esigenze quotidiane, verifica delle apparecchiature tecnologicamente avanzate idonee e disponibili sul mercato, si predispone il presente piano, con l'indicazione dei dispositivi e degli interventi di cablaggio necessari per ciascuna sede per la realizzazione di un impianto Wireless LAN in tecnologia 802.11 ax dual radio WiFi 6.

Sede 1:

PLESSO	
Scuola Infanzia/Primaria/Uffici Via Salvo D'Acquisto	
Quantità	Descrizione
1	Armadio di Rete da 10" 6U
1	FortiGate-60F Hardware + 3 anni 24x7 FortiCare&FortiGuard
1	Switch 24 porte Gigabit 24 PoE Managed Entry level
1	Switch 24 porte Gigabit 12 PoE Unmanaged
1	Switch 8 porte Gigabit
1	Switch 8 porte Gigabit 4 PoE
7	Access Point Ruckus R350
1	Interventi di cablaggio; servizi di installazione/configurazione degli apparati

Sede 2:

PLESSO	
Scuola Secondaria di primo grado Via de Sanctis Roccastrada	
Quantità	Descrizione
1	Switch 24 porte Gigabit
7	Access Point Ruckus R350
1	FortiGate-60F Hardware + 3 anni 24x7 FortiCare&FortiGuard
1	Interventi di cablaggio; servizi di installazione/configurazione degli apparati

Sede 3:

PLESSO	
Scuola Primaria Sassofortino Via Cavour	
Quantità	Descrizione
1	Armadio Rack completo
5	Access Point Ruckus R350
1	Switch 16 porte Gigabit 16 PoE unmanaged
1	Interventi di cablaggio; servizi di installazione/configurazione degli apparati

Sede 4:

PLESSO	
Scuola Infanzia Roccatederighi Via Gorizia	
Quantità	Descrizione
1	Armadio Rack completo
1	Interventi di cablaggio; riutilizzo 4 Access Point Ubiquiti 1 Switch 24 Porte Gigabit; servizi di installazione/configurazione degli apparati

Sede 5:

PLESSO	
Scuola Infanzia Ribolla Piazzetta della libertà	
Quantità	Descrizione
1	Interventi di cablaggio; riutilizzo 3 Access Point Ubiquiti e 1 Switch 24 Porte Gigabit; servizi di installazione/configurazione degli apparati

Sede 6:

PLESSO	
Scuola Infanzia/Primaria Sticciano Via dei Mille	
Quantità	Descrizione
1	Armadio Rack completo
1	Interventi di cablaggio; riutilizzo 3 Access Point Ubiquiti e 2 Switch 24 Porte Gigabit; servizi di installazione/configurazione degli apparati

Per ciascuna delle sedi dovrà essere specificato il costo delle singole apparecchiature, il costo dell'intervento di cablaggio (almeno cat. 6/6a), installazione, configurazione apparati attivi, assistenza al collaudatore per collaudo finale, assistenza telefonica, e-mail e on-site nonché la previsione dell'assistenza specialistica a seguito dell'installazione (almeno 12 mesi, consigliato 24/36 mesi).

A seguito di opportuno e concordato sopralluogo nelle varie sedi, le aziende interessate alla realizzazione della rete dovranno produrre, unitamente all'offerta economica, un master plan specifico con l'indicazione dei locali dove dovrebbe avvenire l'intervento in modo da garantire la copertura pressoché totale dei locali stessi.

Le stesse aziende dovranno altresì fornire simulazioni basate sulle planimetrie degli edifici da coprire e l'indicazione della copertura con un segnale minimo di potenza pari a -65 dBm.

Per garantire la buona riuscita del progetto e per snellire la fase di collaudo, è necessaria la presenza, unitamente al piano, di un planning report che riporti lo studio del posizionamento degli AP WiFi nelle aree interessate tramite uno strumento software di simulazione di copertura radiofrequenza. È necessario che siano presenti mappe digitali in 2D che modellino accuratamente le aree e gli ostacoli alla propagazione e riportino sulle stesse mappe il livello di segnale RF con aree di colore differenti, allo scopo di predire il comportamento del sistema WiFi proposto dal punto di vista RF. Nel piano deve essere riportato il risultato dello studio di pianificazione radio, compresi i grafici e le mappe di copertura.

Per agevolare il concetto di "Bring Your Own Device" (BYOD) all'interno dell'Istituto, è richiesto che la rete wireless sia in grado di gestire le seguenti tecnologie:

- a. Polarization Diversity con Maximal Ratio Combining (PD-MRC) per migliorare la ricezione indipendentemente dall'orientamento del client;
- b. Low Density Parity Check (LDPC) per migliorare le performance di uplink del client;

- c. Gestione “Pre Shared Key” (PSK) dinamica associabile a ciascun dispositivo in maniera univoca e a scadenza.

Al fine di minimizzare l'impatto estetico e rendere la rete più sicura e robusta da eventuali vandalismi, è altresì richiesto che tutti gli AP forniti abbiano antenne integrate.

Gli AP forniti devono possedere uno o più pattern di antenne direzionali adattivi per reti Wi-Fi ad ALTA DENSITÀ. In questo modo l'antenna deve possedere la capacità di concentrare tutta la sua potenza verso il client in modo da ottimizzare le performance e minimizzare il livello di interferenza radio dove non serve. Il beamforming quindi non deve essere solo software, ma anche hardware, per garantire la piena compatibilità con client più vecchi rispetto allo standard 802.11ax.

Gli AP forniti devono selezionare dinamicamente il proprio canale utilizzando i seguenti metodi:

- a. Automaticamente misurando il throughput effettivo in real-time e cambiando canale automaticamente se la capacità scende sotto il livello statistico medio di quella misurata su tutti gli altri canali, senza utilizzare il background scanning come metodo di selezione automatica;
- b. automatico, utilizzando i canali più liberi;
- c. manuale selezionando i canali per AP e per radio;
- d. channel blacklisting (questo deve poter essere disponibile anche nel caso in cui si utilizzino meccanismi automatici di selezione dei canali).

Gli AP devono poter operare anche nel caso in cui non sia presente rete cablata. Devono poter raggiungere la backhaul-core network utilizzando un link radio (Wireless Mesh). La tecnologia Mesh a bordo dell'AP deve garantire:

- a. l'instaurazione di un backhaul Mesh link deve essere automatico, senza dover stabilire a priori canali o AP coinvolti nella configurazione Mesh;
- b. Nel caso in cui un link Mesh cada, data una sufficiente vicinanza di un altro AP a cui connettersi, l'AP deve automaticamente potersi riconnettere al nuovo AP senza alcun intervento manuale.

Le soluzioni che verranno proposte, intese come installazione e configurazioni richieste, dovranno rispondere ai criteri di elevata affidabilità e longevità attraverso una piattaforma di gestione di semplice utilizzo.

- Affidabilità: dal punto di vista fisico per i materiali di realizzazione, dal punto di vista logico per le tecnologie di auto-calibrazione ed i criteri di sicurezza impostabili;
- Semplicità di gestione: grazie ad un unico punto di controllo e gestione per tutta la rete.

Le specifiche tecniche, funzionali e prestazionali della rete wireless dovranno attenersi alla tecnologia Wi-Fi IEEE 802.11ax dual radio WiFi 6 nelle bande di frequenza 2,4 GHz e 5 GHz.

La rete dovrà garantire l'accesso wireless in tecnologia WiFi per gli utenti con apparati dotati di connettività IEEE 802.11ax dual radio WiFi 6 nelle bande di frequenza 2,4 GHz e 5 GHz quali computer portatili, smartphone e telefoni VoIP, lettori di codici a barre, tablet, sistemi wireless presenti nei vari edifici per rendere fruibili tutti i servizi che l'Istituto vorrà implementare.

La rete Wi-Fi dovrà comprendere i seguenti elementi:

- Centro di Controllo di Rete o Wireless Controller per la gestione e il controllo centralizzato di tutta la rete Wi-Fi;
- Access Point Wi-Fi: dispositivo che permette al client di collegarsi ad una rete wireless. L'Access Point può essere collegato fisicamente ad una rete cablata (AP Wired) oppure via radio ad un altro Access Point (AP mesh);
- Alimentatori PoE: con il termine PoE si intende Power Over Ethernet ovvero la possibilità di alimentare gli Access Point attraverso un unico cavo di collegamento.

Caratteristiche tecnico-funzionali dei componenti WiFi della rete.

La collocazione degli Access point negli edifici dell'Istituto deve essere prevista in funzione della conformazione degli elementi architettonici, ovvero prevederne l'installazione di un certo numero

in funzione degli utenti da connettere ma senza rischiare di provocare interferenze e sovrapposizione di segnale che rischiano di compromettere la copertura ed i servizi.

I dispositivi dovranno rispondere a esigenze di affidabilità e prestazioni della rete Wi-Fi. Gli Access Point devono possedere antenne adattive con controllo del segnale per evitare l'interferenza RF e consentire la selezione in tempo reale del miglior percorso del segnale per ciascuna trasmissione Wi-Fi, garantendo così la migliore connessione possibile.

Dal punto di vista del routing, l'architettura richiesta deve essere in grado di eliminare i *single point of failure* tipici di una rete centralizzata e deve essere scalabile. L'architettura proposta deve supportare elevate moli di traffico generate dalla rete di accesso Wi-Fi al crescere del numero di Access Point connessi su molteplici siti.

In particolare, deve essere evitato che si creino colli di bottiglia sulla rete, che si riducano le problematiche legate alla latenza per le applicazioni voce e al jitter per il traffico video e si offra alla rete maggior flessibilità e maggior capacità.

La tecnologia wi-fi richiesta deve essere di elevato livello, garantire l'assenza di interferenza, garantire piena scalabilità e supporto di un numero elevato di utenti in contemporanea.

Si richiede una tecnologia Wi-Fi evoluta che preveda una serie di features tra cui il controllo RF adattivo (BeamFlex), selezione predittiva del canale (ChannelFly), meshing solido e auto-ottimizzante (SmartMesh opzionale), configurazione automatica dei dispositivi degli utenti (Zero IT config) e sicurezza Wi-Fi dinamica (Dynamic Pre-shared Keys), in modo da garantire prestazioni affidabili e prevedibili, essenziali per supportare le applicazioni più esigenti.

BeamFlex, ad esempio, rappresenta l'implementazione di antenne intelligenti Wi-Fi più avanzata del settore. Grazie alla combinazione di una serie di antenne interne definite array e un software di controllo avanzato, BeamFlex classifica continuamente le configurazioni delle antenne per ciascun dispositivo di ricezione, e si riconfigura in tempo reale al fine di oltrepassare interferenze e ostacoli. BeamFlex indirizza i segnali Wi-Fi in modo tale da oltrepassare le interferenze e offrire

prestazioni prevedibili su portate più ampie. Elimina inoltre i punti morti, aumentando la portata e le prestazioni della rete Wi-Fi fino al 300%. Le antenne direzionali ad alto guadagno offrono un guadagno fino a 9 dBi e consentono un respingimento dell'interferenza fino a 17 dB. Gli elementi altamente sensibili dell'antenna garantiranno una maggiore capacità di ricezione Wi-Fi sul lungo raggio dei segnali Wi-Fi fino a -100 dBm.

Gli Access Point richiesti sono caratterizzati da dual-radio simultaneo e dual-band che utilizza la più recente tecnologia Wi-Fi 802.11ax. Questi AP vantano prestazioni leader nel settore Wi-Fi con una velocità superiore ad un Gigabit al secondo e che li rendono la soluzione perfetta per ambienti ad alta densità, come quelli scolastici.

I dispositivi richiesti offrono le seguenti funzionalità:

- Dual-band simultaneo (5 GHz / 2,4 GHz)
- Tecnologia di antenne adattive e gestione RF avanzata
- Riduzione automatica dell'interferenza, ottimizzata per gli ambienti caratterizzati da alta densità
- 1 porta ethernet di cui una Power over Ethernet (PoE) 802.3af standard
- Fino a 16 BSSID per radio con criteri di sicurezza e QoS univoci
- Smart Mesh Networking
- Array di antenne intelligenti in grado di realizzare fino a 4000 patterns al fine di garantire servizi triple-play
- esclusione delle interferenze ottimizzato per scenari ad alta densità,
- range/copertura da due a quattro volte superiore rispetto ai normali AP
- 256 client contemporanei gestibili per AP

Caratteristiche tecnico-funzionali del Controller WiFi

Il controller wifi è preposto a gestire le politiche di sicurezza del sistema, la prevenzione delle intrusioni, la gestione della parte radio, la qualità del servizio (QoS) e la mobilità. Lavora congiuntamente con gli AP per supportare le applicazioni business-critical.

Deve fornire affidabilità e controllo, ovvero tutte quelle funzioni che i gestori delle reti necessitano per costruire e mantenere reti wireless sicure e scalabili.

La scelta di apparati con controller distribuito, svolta da uno degli AP in rete in modalità Master, è tesa a evitare che un eventuale fault del controller Master, possa comportare il fault di tutta la rete wifi. Con il controller distribuito, in caso di fault del Master, un secondo AP ne prenderà le funzioni garantendo continuità di servizio.

Le principali caratteristiche del controller richiesto sono le seguenti:

- Gestione centralizzata delle configurazioni iniziali e successive degli Access Point WiFi;
- Gestione gerarchica e semplificata delle policy e dei profili degli utenti e dei dispositivi dell'infrastruttura (Access Point);
- Gestione radio. Fornisce sia informazioni storiche che in tempo reale sullo stato delle connessioni radio, su interferenze e sull'impatto che queste hanno sul funzionamento della rete wireless;
- Accesso da parte dell'amministratore di rete tramite interfaccia grafica user friendly;
- Aggiornamento firmware centralizzato degli Access Point: il Centro di Controllo supporta la creazione di profili per i vari tipi di apparati del sistema in modo da inviare aggiornamenti per gruppi di apparati oppure per tutta la rete. Il processo di aggiornamento segnala eventuali errori e fault; gli apparati hanno la possibilità di ritornare eventualmente al firmware precedente in caso di problemi con la nuova versione
- Creazione e gestione di più SSID per differenti profili di accesso ai servizi e ad internet (Docenti, Aule, Studenti, Guest).

Caratteristiche tecnico-funzionali dei Firewall

I Firewall richiesti, della serie FortiGate/FortiWiFi dovranno possibilmente essere installati in ogni plesso dell'Istituto Comprensivo di Roccastrada.

Proteggono contro le minacce informatiche con accelerazione system-on-a-chip, facile da implementare. La rete basata sulla sicurezza di Fortinet fornisce una stretta integrazione con la nuova generazione di sicurezza.

Sotto questo profilo, i firewall richiesti si basano sul filtraggio avanzato dei contenuti, identificano migliaia di applicazioni all'interno del traffico di rete per un'ispezione approfondita e un'applicazione granulare delle politiche; proteggono da malware, exploit e dannosi siti Web sia nel traffico crittografato che non crittografato; prevengono e rilevano attacchi noti e sconosciuti utilizzando l'intelligence continua sulle minacce basata sull'intelligenza artificiale.

Dal punto di vista delle prestazioni, Fortigate offre la migliore protezione dalle minacce del settore con latenza ultra-bassa utilizzando un processore di sicurezza appositamente progettato; fornisce prestazioni e protezione leader del settore del Traffico crittografato SSL; è testato e certificato in modo indipendente per essere il migliore della categoria per efficacia e prestazioni in termini di sicurezza; offre funzionalità di rete avanzate senza interruzioni con sicurezza avanzata di livello 7 e domini virtuali (VDOM) per offrire un'ampia flessibilità, multi-tenancy e utilizzo efficace di risorse; offre una combinazione flessibile e ad alta densità di vari elementi interfacce ad alta velocità per consentire il miglior TCO per implementazioni in datacenter e gestione WAN.

Include una console di gestione efficace, semplice da utilizzare e fornisce un'automazione di rete completa; fornisce l'integrazione Zero Touch; l'elenco di controllo di conformità predefinito analizza la distribuzione ed evidenzia le migliori pratiche per migliorare la sicurezza generale; abilita i prodotti dei partner Fortinet e Fabric-ready per fornire una visibilità più ampia, integrata end-to-end con rilevamento, condivisione di informazioni sulle minacce e bonifica automatizzata.

Fortinet garantisce inoltre la visibilità completa su utenti, dispositivi e applicazioni, l'intera superficie di attacco e una coerente politica di sicurezza; protegge dalle vulnerabilità sfruttabili

della rete con IPS convalidato dal settore che offre bassa latenza e prestazioni di rete ottimizzate; blocca automaticamente le minacce sul traffico decrittografato utilizzando le più alte prestazioni di ispezione SSL del settore, incluso l'ultimo standard TLS 1.3 con cifrature obbligatorie.

Infine, blocca in modo proattivo i sofisticati attacchi in tempo reale scoperti di recente basati sull'intelligenza artificiale e include servizi avanzati di protezione dalle minacce.

Il sottoscritto Alessandro Salvini, consapevole che chiunque rilascia dichiarazioni mendaci è punito ai sensi del codice penale e delle leggi speciali in materia, ai sensi e per gli effetti dell'art. 46 D.P.R. n. 445/2000

DICHIARA

di aver provveduto alla verifica di eventuali Convenzioni Consip attive e che da tale verifica è emerso che non esiste convenzione attiva in grado di fornire il materiale descritto con tutte le caratteristiche tecniche essenziali previste nella presente relazione.

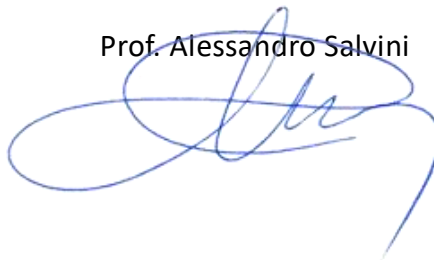
Si allegano schede tecniche dei prodotti richiesti. Successivamente verranno inviate le planimetrie con il posizionamento degli Access Points.

Il progetto è stato realizzato proponendo l'uso degli Access Point R350 Ruckus. Laddove necessario, valuteremo la possibilità di accettare l'utilizzo di apparati con caratteristiche analoghe.

Capannoli, 25 marzo 2022

In fede

Prof. Alessandro Salvini



Allegati

Firewall

Datasheet con caratteristiche tecniche dei Firewall richiesti

Hardware Specifications	
GE RJ45 WAN / DMZ Ports	2 / 1
GE RJ45 Internal Ports	5
GE RJ45 FortiLink Ports (Default)	2
Wireless Interface	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1
Console (RJ45)	1
Internal Storage	–

System Performance — Enterprise Traffic Mix	
IPS Throughput 2	1.4 Gbps
NGFW Throughput 2, 4	1 Gbps
Threat Protection Throughput 2, 5	700 Mbps

System Performance	
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps
Firewall Latency (64 byte UDP packets)	3.3 μs
Firewall Throughput (Packets Per Second)	9 Mpps
Concurrent Sessions (TCP)	700 000
New Sessions/Second (TCP)	35 000
Firewall Policies	5000
IPsec VPN Throughput (512 byte) 1	6.5 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	200
Client-to-Gateway IPsec VPN Tunnels	500
SSL-VPN Throughput	900 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200
SSL Inspection Throughput (IPS, avg. HTTPS)	630 Mbps
SSL Inspection CPS (IPS, avg. HTTPS)	400
SSL Inspection Concurrent Session (IPS, avg. HTTPS)	55 000
Application Control Throughput (HTTP 64K)	1.8 Gbps
CAPWAP Throughput (HTTP 64K)	8 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	16
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32
Maximum Number of FortiTokens	500
High Availability Configurations	Active-Active, Active-Passive, Clustering

Radio Specifications	
Multiple User (MU) MIMO	3x3
Maximum Wi-Fi Speeds	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	20 dBm
Antenna Gain	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz

FortiGate/FortiWiFi® 40F Series

Secure SD-WAN
Next Generation Firewall



La serie FortiGate / FortiWiFi 40F offre una soluzione SD-WAN veloce e sicura in un fattore di forma desktop fanless compatto per filiali aziendali e medie imprese. Protegge dalle minacce informatiche con l'accelerazione di sistema su chip e SD-WAN sicura leader del settore in una soluzione semplice, economica e facile da implementare. L'approccio di rete basato sulla sicurezza di Fortinet offre una stretta integrazione della rete con la nuova generazione di sicurezza.

Security

- Identifica migliaia di applicazioni all'interno del traffico di rete per ispezioni approfondite e applicazione granulare delle politiche
- Protegge da malware, exploit e siti Web dannosi sia nel traffico crittografato che non crittografato
- Previene e rileva dagli attacchi noti utilizzando l'intelligence continua delle minacce dai servizi di sicurezza FortiGuard Labs basati sull'intelligenza artificiale
- Blocca in modo proattivo attacchi sofisticati sconosciuti in tempo reale con il FortiSandbox integrato con Fortinet Security Fabric

Performance

- Progettato per l'innovazione utilizzando i processori di sicurezza (SPU) appositamente progettati da Fortinet per offrire le migliori prestazioni di protezione dalle minacce del settore e latenza ultra bassa
- Fornisce prestazioni e protezione leader del settore per il traffico crittografato SSL, incluso il primo fornitore di firewall a fornire un'ispezione approfondita TLS 1.3

Certification

- Migliore efficacia e prestazioni di sicurezza testate e validate in modo indipendente
- Ha ricevuto certificazioni di terze parti senza precedenti da NSS Labs, ICSA, Virus Bulletin e AV Comparatives

Networking

- Instradamento consapevole delle applicazioni con funzionalità SD-WAN integrate per ottenere prestazioni applicative coerenti e la migliore esperienza utente
- Funzionalità di routing avanzate integrate per offrire prestazioni elevate con tunnel IPSEC crittografati su larga scala

Management

- Include una console di gestione che è efficace e semplice da usare, che fornisce una rete completa di automazione e visibilità
- Fornisce il provisioning Zero Touch sfruttando il riquadro singolo della gestione del vetro fornita dal Fabric Management Center
- Elenchi di controllo di conformità predefiniti analizzano la distribuzione ed evidenziano le migliori pratiche per migliorare la posizione generale di sicurezza

Security Fabric

- Consente ai prodotti Fortinet e ai partner compatibili con Fabric di offrire una visibilità più ampia, rilevamento end-to-end integrato, condivisione delle informazioni sulle minacce e soluzioni automatizzate
- Crea automaticamente visualizzazioni della topologia di rete che scoprono i dispositivi IoT e forniscono una visibilità completa sui prodotti Fortinet e partner compatibili con Fabric

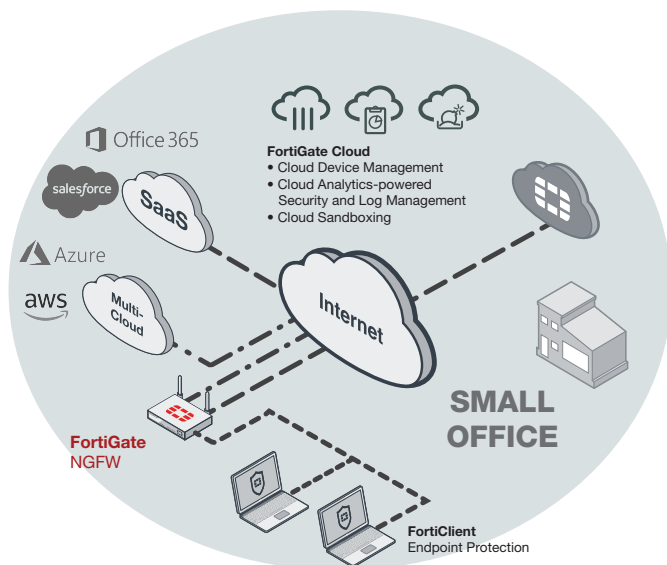
Firewall	IPS	NGFW	Threat Protection	Interfaces
5 Gbps	1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 WiFi variants

Deployment



Next Generation Firewall (NGFW)

- Riduci la complessità e massimizza il ROI integrando le funzionalità di sicurezza della protezione dalle minacce in un'unica appliance di sicurezza della rete ad alte prestazioni, alimentata dall'unità di elaborazione della sicurezza (SPU) di Fortinet
- Visibilità completa su utenti, dispositivi, applicazioni su tutta la superficie di attacco e applicazione coerente delle politiche di sicurezza indipendentemente dalla posizione delle risorse
- Proteggi dalle vulnerabilità sfruttabili della rete con IPS convalidato dal settore che offre bassa latenza e prestazioni di rete ottimizzate
- Blocca automaticamente le minacce sul traffico decrittografato utilizzando le prestazioni di ispezione SSL più elevate del settore, tra cui
- l'ultimo standard TLS 1.3 con cifre obbligatorie
- Blocca in modo proattivo attacchi sofisticati appena scoperti in tempo reale con FortiGuard Labs basato sull'intelligenza artificiale e servizi avanzati di protezione dalle minacce inclusi in Fortinet Security Fabric

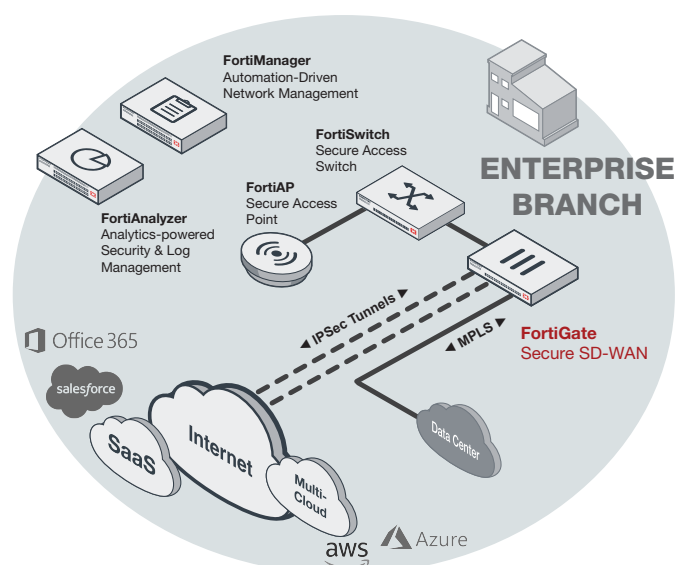


FortiWiFi 40F deployment in Small Office (NGFW)



Secure SD-WAN

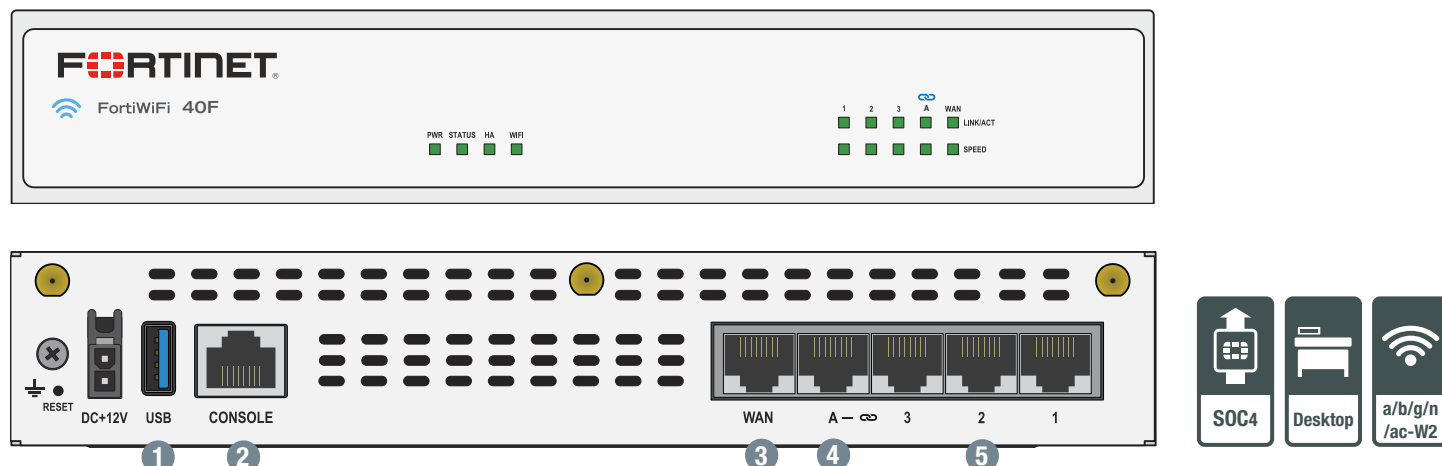
- Prestazioni coerenti delle applicazioni aziendali con rilevamento accurato, direzione e ottimizzazione dinamiche del percorso WAN
- Accesso multi-cloud per una più rapida adozione SaaS con ottimizzazione end-to-end Semplificazione con implementazione zero touch e gestione centralizzata con auto-provisioning, analisi e reportistica
- Posizione di sicurezza elevata con firewall di nuova generazione e protezione dalle minacce in tempo reale



FortiGate 40F deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate/FortiWiFi 40F Series



Interfaces

- | | |
|------------------------|------------------------------|
| 1. USB Port | 4. 1x GE RJ45 FortiLink Port |
| 2. Console Port | 5. 3x GE RJ45 Ethernet Ports |
| 3. 1x GE RJ45 WAN Port | |

Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combina una CPU basata su RISC con
- Elaborazione di sicurezza proprietaria di Fortinet
- Contenuti dell'unità (SPU) e processori di rete per prestazioni senza pari
- Offre l'identificazione delle applicazioni più veloce del settore e la gestione di operazioni aziendali efficienti
- Accelera le prestazioni della VPN IPsec per la migliore esperienza utente sull'accesso diretto a Internet
- Consente il meglio della sicurezza NGFW e ispezione SSL profonda con prestazioni elevate
- Estende la sicurezza al livello di accesso per consentire la trasformazione di SD-Branch con connettività switch e access point accelerata e integrata

3G/4G WAN Connectivity

La serie FortiGate 40F include una porta USB che consente di collegare un modem USB 3G / 4G di terze parti compatibile, fornendo ulteriore connettività WAN o un collegamento ridondante per la massima affidabilità.

Compact and Reliable Form Factor

Progettato per piccoli ambienti, è possibile posizionarlo su un desktop o montarlo a parete. È piccolo, leggero ma altamente affidabile con un MTBF (Mean Time Between Failure) superiore, riducendo al minimo la possibilità di un'interruzione della rete.

Extends Security to Access Layer with FortiLink Ports

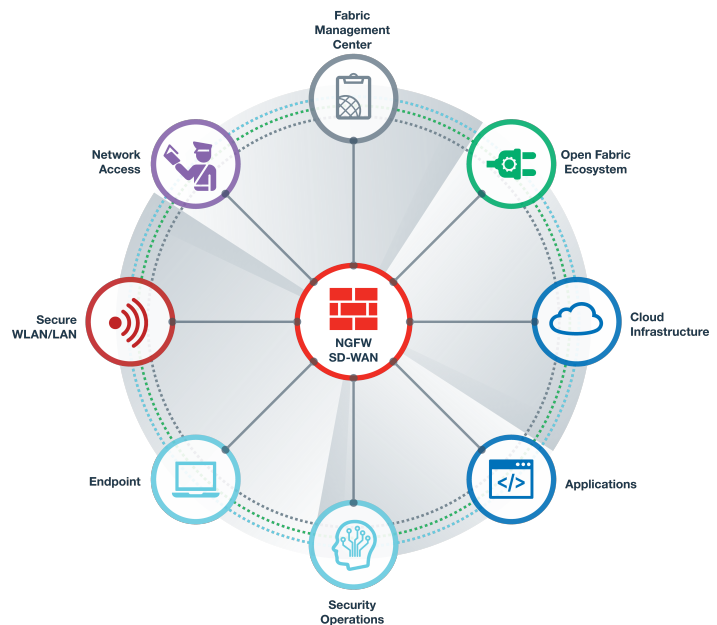
Il protocollo FortiLink consente di convertire la sicurezza e l'accesso alla rete integrando FortiSwitch in FortiGate come estensione logica di NGFW. Queste porte abilitate per FortiLink possono essere riconfigurate come porte normali secondo necessità.

Fortinet Security Fabric

Security Fabric

Security Fabric è la piattaforma di sicurezza informatica che consente innovazioni digitali. Offre un'ampia visibilità dell'intera superficie di attacco per gestire meglio il rischio. La sua soluzione unificata e integrata riduce la complessità del supporto di prodotti multipunto, mentre i flussi di lavoro automatizzati aumentano le velocità operative e riducono i tempi di risposta nell'ecosistema di implementazione di Fortinet. Fortinet Security Fabric copre le seguenti aree chiave in un unico centro di gestione:

- **Security-Driven Networking** che protegge, accelera e unifica la rete e l'esperienza utente
- **Zero Trust Network Access** che identifica e protegge utenti e dispositivi in tempo reale, dentro e fuori dalla rete
- **Dynamic Cloud Security** che protegge e controlla le infrastrutture e le applicazioni cloud
- **AI-Driven Security Operations** che previene, rileva, isola e risponde automaticamente alle minacce informatiche



FortiOS

FortiGate è il fondamento di Fortinet Security Fabric: il nucleo è FortiOS. Tutte le funzionalità di sicurezza e di rete dell'intera piattaforma FortiGate sono controllate con un sistema operativo intuitivo. FortiOS riduce complessità, costi e tempi di risposta consolidando veramente prodotti e servizi di sicurezza di prossima generazione in un'unica piattaforma.

- Una piattaforma veramente consolidata con un singolo sistema operativo e riquadro di vetro per l'intera superficie di attacco digitale.
- Protezione leader del settore: consigliati NSS Labs, VB100, comparativi AV e sicurezza e prestazioni validate ICASA.
- Sfrutta le ultime tecnologie come la sicurezza basata sull'inganno.

- Controlla migliaia di applicazioni, blocca gli exploit più recenti e filtra il traffico Web in base a milioni di valutazioni URL in tempo reale oltre al vero supporto TLS 1.3.
- Previene, rileva e mitiga automaticamente gli attacchi avanzati in pochi minuti con una sicurezza integrata basata sull'intelligenza artificiale e una protezione avanzata dalle minacce.
- Migliora e unifica l'esperienza utente con le innovative funzionalità SD-WAN con la capacità di rilevare, contenere e isolare le minacce con la segmentazione automatizzata.
- Utilizza l'accelerazione hardware SPU per migliorare le prestazioni di sicurezza della rete.

Services



**FortiGuard™
Security Services**

I FortiGuard Lab offrono informazioni in tempo reale sul panorama delle minacce, offrendo aggiornamenti di sicurezza completi su tutta la gamma di soluzioni Fortinet. Composto da ricercatori, ingegneri e specialisti forensi nelle minacce alla sicurezza, il team collabora con le principali organizzazioni mondiali di monitoraggio delle minacce e altri fornitori di reti e sicurezza, nonché con le forze dell'ordine.



**FortiCare™
Support Services**

Il nostro team di assistenza clienti FortiCare fornisce supporto tecnico globale per tutti i prodotti Fortinet. Con personale di supporto in America, Europa, Medio Oriente e Asia, FortiCare offre servizi per soddisfare le esigenze delle imprese di tutte le dimensioni.



For more information, please refer to forti.net/fortiguard and forti.net/forticare

Specifications

	FORTIGATE 40F	FORTIWIFI 40F
Hardware Specifications		
GE RJ45 WAN / DMZ Ports	1	
GE RJ45 Internal Ports	3	
GE RJ45 FortiLink Ports	1	
GE RJ45 PoE/+ Ports	—	
Wireless Interface	—	802.11 a/b/g/n/ac-W2
USB Ports	1	
Console (RJ45)	1	
Internal Storage	—	
System Performance — Enterprise Traffic Mix		
IPS Throughput ²	1 Gbps	
NGFW Throughput ^{2,4}	800 Mbps	
Threat Protection Throughput ^{2,5}	600 Mbps	
System Performance		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	5/5/5 Gbps	
Firewall Latency (64 byte UDP packets)	4 µs	
Firewall Throughput (Packets Per Second)	7.5 Mpps	
Concurrent Sessions (TCP)	700,000	
New Sessions/Second (TCP)	35,000	
Firewall Policies	5,000	
IPsec VPN Throughput (512 byte) ¹	4.4 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	250	
SSL-VPN Throughput	490 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) ³	310 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³	320	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	55,000	
Application Control Throughput (HTTP 64K) ²	990 Mbps	
CAPWAP Throughput (HTTP 64K)	3.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	8	
Maximum Number of FortiAPs (Total / Tunnel Mode)	16 / 8	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active / Active, Active / Passive, Clustering	

	FORTIGATE 40F	FORTIWIFI 40F
Dimensions		
Height x Width x Length (inches)	1.5 x 8.5 x 6.3	
Height x Width x Length (mm)	38.5 x 216 x 160	
Weight	2.2 lbs (1 kg)	
Form Factor	Desktop	
Operating Environment and Certifications		
Input Rating	12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz	
Maximum Current	100V AC / 0.2A, 240V AC / 0.1A	
Power Consumption (Average / Maximum)	12.4 W / 15.4 W	13.6 W / 16.6 W
Heat Dissipation	52.55 BTU/hr	56.64 BTU/hr
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fanless 0 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
Radio Specifications		
Multiple (MU) MIMO	–	3x3
Maximum Wi-Fi Speeds	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	–	20 dBm
Antenna Gain	–	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.

3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS, and Application Control enabled.

5. Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.

Order Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports)
FortiWiFi 40F	FWF-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2)

Bundles



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE ¹	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiGuard IoT Detection Service ²	•	•		
FortiConverter Service	•	•		
IPAM Cloud ²	•			
SD-WAN Orchestrator Entitlement ²	•			
SD-WAN Cloud Assisted Monitoring	•			
SD-WAN Overlay Controller VPN Service	•			
FortiAnalyzer Cloud	•			
FortiManager Cloud	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

DATA SHEET

FortiGate® FortiWiFi 60F Series

FG-60F, FG-61F, FWF-60F, and FWF-61F

Next Generation Firewall
Secure SD-WAN



The FortiGate/FortiWiFi 60F series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet's Security-Driven Networking approach provides tight integration of the network to the new generation of security.

Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevent and detect against known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose-built security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

Certification

- Independently tested and validated for best-in-class security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet's Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve overall security posture

Security Fabric

- Enables Fortinet and Fabric-ready partners' products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation

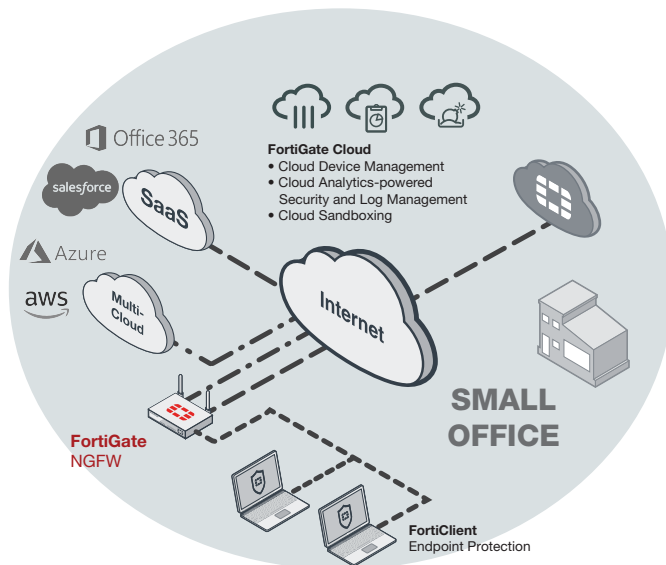
Firewall	IPS	NGFW	Threat Protection	Interfaces
10 Gbps	1.4 Gbps	1 Gbps	700 Mbps	Multiple GE RJ45 Variants with internal storage WiFi variants

DEPLOYMENT



Next Generation Firewall (NGFW)

- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

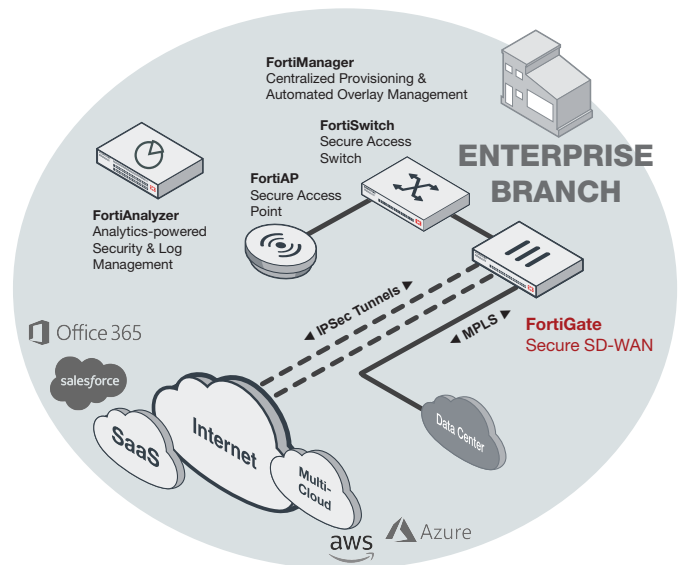


**Small Office Deployment
(NGFW)**



Secure SD-WAN

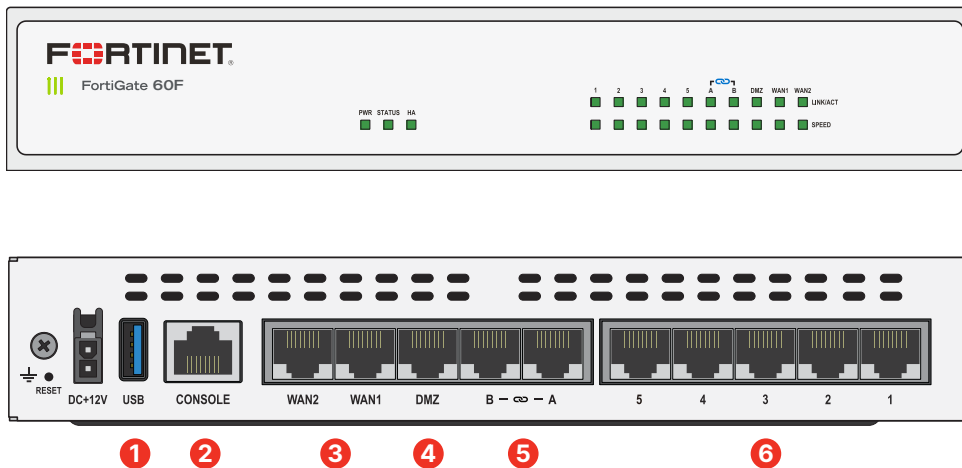
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplified and intuitive workflow with FortiManager for management and zero touch deployment
- Strong security posture with next generation firewall and real-time threat protection



**Enterprise Branch Deployment
(Secure SD-WAN)**

HARDWARE

FortiGate / FortiWiFi 60F/61F



Interfaces

1. 1x USB Port
2. 1x Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 2x GE RJ45 FortiLink Ports
6. 5x GE RJ45 Internal Ports

Hardware Features



Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

3G/4G WAN Connectivity

The FortiGate 60F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Secure Access Layer

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.



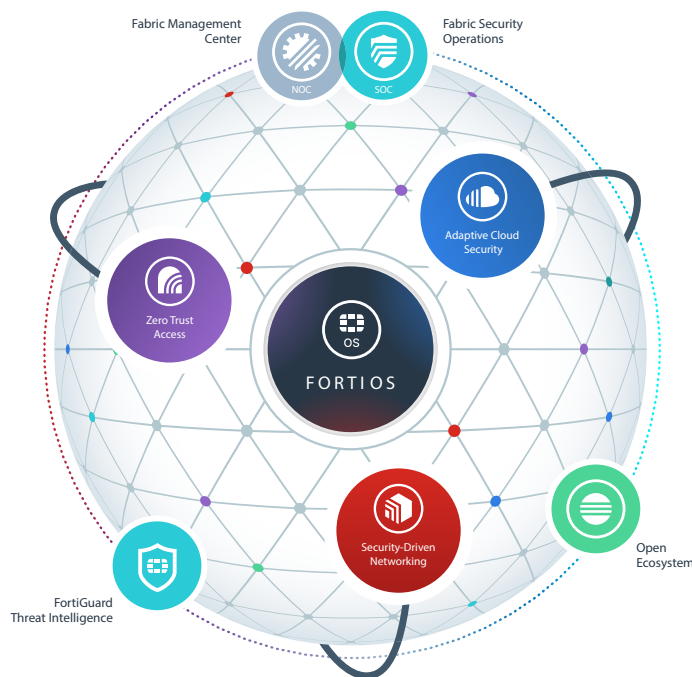
FORTINET SECURITY FABRIC

Security Fabric

The industry's highest-performing cybersecurity platform, powered by FortiOS, with a rich ecosystem designed to span the extended digital attack surface, delivering fully automated, self-healing network security.

- **Broad:** Coordinated detection and enforcement across the entire digital attack surface and lifecycle with converged networking and security across edges, clouds, endpoints and users
- **Integrated:** Integrated and unified security, operation, and performance across different technologies, location, deployment options, and the richest Ecosystem
- **Automated:** Context aware, self-healing network & security posture leveraging cloud-scale and advanced AI to automatically deliver near-real-time, user-to-application coordinated protection across the Fabric

The Fabric empowers organizations of any size to secure and simplify their hybrid infrastructure on the journey to digital innovation.



FortiOS™ Operating System

FortiOS, Fortinet's leading operating system enable the convergence of high performing networking and security across the Fortinet Security Fabric delivering consistent and context-aware security posture across network endpoint, and clouds. The organically built best of breed capabilities and unified approach allows organizations to run their businesses without compromising performance or protection, supports seamless scalability, and simplifies innovation consumption.

The release of FortiOS 7 dramatically expands the Fortinet Security Fabric's ability to deliver consistent security across hybrid deployment models consisting on appliances, software and As-a-Service with SASE, ZTNA and other emerging cybersecurity solutions.

SERVICES



FortiGuard™ Security Services

FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet's solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world's leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



FortiCare™ Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare services help thousands of organizations get the most from their Fortinet Security Fabric solution. We have more than 1000 experts to help accelerate technology implementation, provide reliable assistance through advanced support, and offer proactive care to maximize security and performance of Fortinet deployments.

SPECIFICATIONS

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIIFI 60F	FORTIWIIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput ²			1.4 Gbps	
NGFW Throughput ^{2,4}			1 Gbps	
Threat Protection Throughput ^{2,5}			700 Mbps	
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)			10/10/6 Gbps	
Firewall Latency (64 byte UDP packets)			3.3 μs	
Firewall Throughput (Packets Per Second)			9 Mpps	
Concurrent Sessions (TCP)			700 000	
New Sessions/Second (TCP)			35 000	
Firewall Policies			5000	
IPsec VPN Throughput (512 byte) ¹			6.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels			200	
Client-to-Gateway IPsec VPN Tunnels			500	
SSL-VPN Throughput			900 Mbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)			200	
SSL Inspection Throughput (IPS, avg. HTTPS) ³			630 Mbps	
SSL Inspection CPS (IPS, avg. HTTPS) ³			400	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³			55 000	
Application Control Throughput (HTTP 64K) ²			1.8 Gbps	
CAPWAP Throughput (HTTP 64K)			8 Gbps	
Virtual Domains (Default / Maximum)			10 / 10	
Maximum Number of FortiSwitches Supported			16	
Maximum Number of FortiAPs (Total / Tunnel Mode)			64 / 32	
Maximum Number of FortiTokens			500	
High Availability Configurations		Active-Active, Active-Passive, Clustering		
Dimensions				
Height x Width x Length (inches)			1.5 × 8.5 × 6.3	
Height x Width x Length (mm)			38.5 × 216 × 160 mm	
Weight			2.23 lbs (1.01 kg)	
Form Factor			Desktop	
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

Note: All performance values are “up to” and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



SPECIFICATIONS

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIIFI 60F	FORTIWIIFI 61F
Operating Environment and Certifications				
Power Rating	12Vdc, 3A			
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz			
Maximum Current	100Vac/1.0A, 240Vac/0.6A			
Power Consumption (Average / Maximum)	17.0 W / 18.5 W	17.2 W / 18.7 W	17.2 W / 18.7 W	17.5 W / 19.0 W
Heat Dissipation	63.1 BTU/hr	63.8 BTU/hr	63.8 BTU/hr	64.8 BTU/hr
Operating Temperature	32–104°F (0–40°C)			
Storage Temperature	–31–158°F (–35–70°C)			
Humidity	Humidity 10–90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN			

ORDERING INFORMATION

Product	SKU	Description
FortiGate 60F	FG-60F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port)
FortiGate 61F	FG-61F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage
FortiWiFi 60F	FWF-60F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2)
FortiWiFi 61F	FWF-61F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, and 80E/81E
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F and FG/FWF-80F series

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

BUNDLES



FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	Enterprise Protection	SMB Protection	Unified Threat Protection	Advanced Threat Protection
FortiCare	24×7	24×7	24×7	24×7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web and Video ¹ Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•			
FortiGuard IoT Detection Service	•			
FortiGuard Industrial Service	•			
FortiConverter Service	•			
FortiGate Cloud Subscription		•		

1. Available when running FortiOS 7.0



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Tecnologia

Wi-Fi

Datasheet con caratteristiche tecniche degli Access Point richiesti

Wi-Fi 6 (802.11ax) Access Point

Wi-Fi Standards	<ul style="list-style-type: none">· IEEE 802.11a/b/g/n/ac/ax
Supported Rates	<ul style="list-style-type: none">· 802.11ax: 4 to 1774 Mbps· 802.11ac: 6.5 to 867 Mbps (MCS0 to MCS9, NSS = 1 to 2 for VHT20/40/80)· 802.11n: 6.5 Mbps to 300 Mbps (MCS0 to MCS15)· 802.11a/g: 54, 48, 36, 24, 18, 12, 9, 6Mbps· 802.11b: 11, 5.5, 2 and 1 Mbps
Supported Channels	<ul style="list-style-type: none">· 2.4GHz: 1-13· 5GHz: 36-64, 100-144, 149-165
MIMO	<ul style="list-style-type: none">· 2x2 SU-MIMO· 2x2 MU-MIMO
Spatial Streams	<ul style="list-style-type: none">· 2 streams SU/MU-MIMO 5GHz· 2 streams SU/MU-MIMO 2.4GHz
Radio Chains and Streams	<ul style="list-style-type: none">· 2x2:2 (5 GHz)· 2x2:2 (2.4GHz)
Channelization	<ul style="list-style-type: none">· 20, 40, 80MHz
Security	<ul style="list-style-type: none">· WPA-PSK, WPA-TKIP, WPA2 , WPA3-Personal, WPA3- Enterprise, AES, WPA3, 802.11i, Dynamic PSK· WIPS/WIDS
Other Wi-Fi Features	<ul style="list-style-type: none">· WMM, Power Save, Tx Beamforming, LDPC, STBC, 802.11r/k/v· Hotspot· Hotspot 2.0· Captive Portal· WISPr

2.4GHZ TX POWER TARGET	
Rate	Pout (dBm)
MCS0 HT20	20
MCS7 HT20	15

5GHZ TX POWER TARGET	
Rate	Pout (dBm)
MCS0 VHT20	20
MCS7 VHT20	17
MCS0 VHT40,VHT80	17
MCS7 VHT40, VHT80	17

PERFORMANCE AND CAPACITY	
Peak PHY Rates	<ul style="list-style-type: none">· 2.4GHz: 574Mbps· 5 GHz: 1200Mbps
Client Capacity	<ul style="list-style-type: none">· Up to 256 clients per AP
SSID	<ul style="list-style-type: none">· Up to 16 per AP

RADIO MANAGEMENT	
Antenna Optimization	<ul style="list-style-type: none">· BeamFlex+· Polarization Diversity with Maximal Ratio Combining (PD- MRC)
Wi-Fi Channel Management	<ul style="list-style-type: none">· ChannelFly· Background Scan Based

Client Density Management	<ul style="list-style-type: none"> Adaptive Band Balancing Client Load Balancing Airtime Fairness Airtime-based WLAN Prioritization
SmartCast Quality of Service	<ul style="list-style-type: none"> QoS-based scheduling Directed Multicast L2/L3/L4 ACLs
Mobility	<ul style="list-style-type: none"> SmartRoam
Diagnostic Tools	<ul style="list-style-type: none"> SpeedFlex

RF	
Antenna Type	<ul style="list-style-type: none"> BeamFlex adaptive antennas Adaptive antenna that provides up to 64 unique antenna patterns per band
Antenna Gain (max)	<ul style="list-style-type: none"> Up to 3dBi
Peak Transmit Power (aggregate across MIMO chains)	<ul style="list-style-type: none"> 2.4GHz: 23 dBm 5GHz: 23 dBm
Minimum Receive Sensitivity ¹	<ul style="list-style-type: none"> -101 dBm
Frequency Bands	<ul style="list-style-type: none"> ISM (2.4-2.484GHz) U-NII-1 (5.15-5.25GHz) U-NII-2A (5.25-5.35GHz) U-NII-2C (5.47-5.725GHz) U-NII-3 (5.725-5.85GHz)

2.4GHZ RECEIVE SENSITIVITY (dBm)			
HT20		HT40	
MCS0	MCS7	MCS0	MCS7
-94	-70	-91	-72

5GHZ RECEIVE SENSITIVITY (dBm)					
VHT20		VHT40		VHT80	
MCS0	MCS7	MCS0	MCS7	MCS0	MCS7
-95	-76	-92	-73	-89	-70

NETWORKING	
Controller Platform Support	<ul style="list-style-type: none"> SmartZone ZoneDirector Unleashed2 Cloud Standalone
Mesh	<ul style="list-style-type: none"> SmartMesh™ wireless meshing technology. Self-healing Mesh
IP	<ul style="list-style-type: none"> IPv4, IPv6
VLAN	<ul style="list-style-type: none"> 802.1Q (1 per BSSID or dynamic per use based on RADIUS) VLAN Pooling Port-based
802.1x	<ul style="list-style-type: none"> Authenticator & Supplicant
Tunnel	<ul style="list-style-type: none"> L2TP, GRE, Soft-GRE
Policy Management Tools	<ul style="list-style-type: none"> Application Recognition and Control Access Control Lists Device Fingerprinting Rate Limiting

CERTIFICATIONS AND COMPLIANCE	
4	<ul style="list-style-type: none"> · Wi-Fi CERTIFIED™ a, b, g, n, ac · Wi-Fi CERTIFIED 6™ · WPA3™ -Enterprise, Personal · Wi-Fi Enhanced Open™ · Wi-Fi Agile Multiband™ · Passpoint® · Vantage · WMM
Standards Compliance5	<ul style="list-style-type: none"> · EN 60950-1 Safety · EN 60601-1-2 Medical · EN 61000-4-2/3/5 Immunity · EN 50121-1 Railway EMC · EN 50121-4 Railway Immunity · IEC 61373 Railway Shock & Vibration · UL 2043 Plenum · EN 62311 Human Safety/RF Exposure · WEEE & RoHS · ISTA 2A Transportation

SOFTWARE AND SERVICES	
Location Based Services	· SPoT
Network Analytics	· SmartCell Insight (SCI)
Security and Policy	· Cloudpath

PHYSICAL INTERFACES	
Ethernet	· 1 x 1GbE port, RJ-45
USB	· 1 USB 2.0 Port, Type A

PHYSICAL CHARACTERISTICS	
Physical Size	<ul style="list-style-type: none"> · 14.60(L) x 15.59(W) x 3.93(H) cm · 5.75(L) x 6.14(W) x 1.55(H) in
Weight	· 368g (13 oz)
Mounting	<ul style="list-style-type: none"> · Wall, Drop ceiling, Desk · Secure bracket (sold separately)
Physical Security	<ul style="list-style-type: none"> · Hidden latching mechanism · T-bar Torx
Operating Temperature	· 0 °C (32 °F) to 40 °C (104 °F)
Operating Humidity	· Up to 95%, non-condensing

RUCKUS® R350

Indoor Wi-Fi 6 (802.11ax) Access Point



Benefits

LATEST WI-FI STANDARDS

The R350 access point (AP) support the latest Wi-Fi 6 (802.11ax) technology

STUNNING WI-FI PERFORMANCE

Patented RUCKUS technologies for performance optimization and interference mitigation delivers extended coverage and superior user experience.

IoT READY

Eliminate siloed networks and unify Wi-Fi and IoT technologies into one single network by using or any future wireless technologies with the addition of an optional USB module.

MESH NETWORKING

Dynamically create self-forming, self-healing network mesh with RUCKUS patented SmartMesh technology reducing expensive cabling, and complex configurations by checking a box.

AFFORDABLE ENTERPRISE PERFORMANCE

The R350 delivers unprecedented price/performance offering extended range at an affordable price.

MULTIPLE UNIFIED MANAGEMENT OPTIONS

Manage the R350 from the cloud, with on-premises physical/virtual appliances, or without a controller.

KEEP EXISTING SWITCHES AND CABLES

Designed to operate on existing PoE switches and CAT 5e cabling to minimize costly power infrastructure upgrades.

Smaller locations can face big-time demands on their wireless infrastructure. Whether working out of a small office or connecting to a public hotspot, users are often still accessing the same high-bandwidth applications and content they'd consume anywhere else. And they expect strong, reliable connectivity. How can you provide it without breaking the bank?

The RUCKUS® R350 delivers consistent, reliable Wi-Fi 6 (802.11ax) wireless networking at an affordable price. The AP features the patented RUCKUS technologies for performance optimization and interference mitigation found in our premier access points, delivering superior user experiences at extended ranges. But it provides them in an ultra-compact form factor built for small venues—with a price tag to match.

Also, wireless requirements within enterprises are expanding beyond Wi-Fi with BLE, Zigbee and many other non-Wi-Fi wireless technologies resulting in creation of network silos. Enterprises need a unified platform to eliminate network silos. The RUCKUS R350 is equipped to solve these challenges with a USB port supporting an optional pluggable BLE and Zigbee IoT module.

The R350 is an ideal choice for low-density enterprise and hotspot environments including small and medium-size businesses, retail locations, restaurants, and multi-tenant small offices and branch offices.

The R350 Wi-Fi 6 AP incorporates patented technologies found only in the RUCKUS Wi-Fi portfolio.

- Extended coverage with BeamFlex utilizing multi-directional antenna patterns.
- Improve throughput with ChannelFly®, which dynamically finds less congested Wi-Fi channels to use.

The R350 provides an ideal combination of features and performance for smaller environments. Additionally, it supports up to 256 clients and 16 SSIDs per AP.

Whether you're deploying ten or ten thousand APs, the R350 is also easy to manage through RUCKUS' appliance, virtual, controller-less and cloud management options.

BENEFITS

- Analyzes live channel activity to determine what channels will yield the most throughput
- Automates channel selection to optimize throughput in RUCKUS® networks
- Combines with BeamFlex® to support the most demanding enterprise requirements
- Maximizes capacity by selecting channels with the fewest neighboring APs and lowest interference
- Gives IT teams the power to limit when channel changes occur

Automatic RF channel selection and interference mitigation

A feature of the SmartZone™ control and management architecture, ChannelFly® automates wireless channel planning to minimize interference from both Wi-Fi and non-Wi-Fi sources. It analyzes channel activity and uses specialized algorithms to select the best channel based on historical values. In combination with RUCKUS BeamFlex adaptive antenna technology, ChannelFly maximizes throughput in the most demanding enterprise environments. It optimizes RF channel selection based on the number of neighboring APs and the historical capacity on each channel.

ChannelFly is integrated into every RUCKUS access point. It constantly monitors the RF environment and tracks the history of devices and interference on every channel. ChannelFly uses the 802.11h protocol to advertise necessary channel changes to active clients. This helps smooth transitions from one channel to another for clients and APs.

While proper channel selection is critical for RF health, excessive channel changes can disrupt the user experience. The 802.11h protocol is inconsistently implemented on clients, and interoperability issues may arise. An automatic channel selection algorithm needs to balance seeking the best channel with preventing excessive channel changes that may disrupt the client experience. ChannelFly allows the IT admin to specify when channel changes are allowed, such as in the middle of the night when wireless usage is light. Admins can also configure how responsive ChannelFly is to interference and reductions in capacity. On each channel change, ChannelFly weighs the benefit of changing channels against the potential impact on clients to minimize disruption to the user experience.



Channel plan created by ChannelFly in an enterprise office environment (20 MHz)

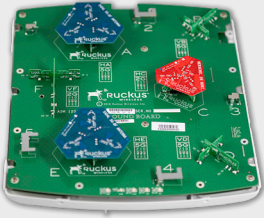
The network is idle—the optimal time for channel changes.



The network is in service—admins can choose to delay channel changes.

BeamFlex®

Smart antenna system



FEATURES

- Multiple directional high-gain elements
- Real-time optimization system
- Works with Wi-Fi 6
- Thousands of antenna patterns that are optimized via patented software to ensure the best path to the client
- Compatible with 802.11a/b/g/n networks and clients
- Continuous learning based on inputs from network layers 0 through 7
- On-the-fly antenna reconfiguration and transmission policy management per packet, per flow, per receiving device
- Up to 6 dBi signal gain and 15 dB interference mitigation

BENEFITS

- Requires fewer APs to deliver a higher capacity coverage over a greater area—delivering more reliable client connectivity
- Has a self-healing, self-optimizing antenna system proven in more than 3.5 million installations
- Mitigates interference in a high-density client and AP environment
- Extends Wi-Fi range and coverage by focusing Wi-Fi signals toward client
- Maximizes AP and client performance
- Eliminates dead spots
- Provides better reception and transmission for handheld clients that are both hard to hear and constantly change direction

The industry's only smart antenna system that delivers stable connectivity and higher performance

BeamFlex® is a combination of multiple high-gain polarized antenna elements and patented software algorithms that are combined in real time to offer an exponential increase in performance. With up to 21 high-gain, directional antenna elements, a BeamFlex smart antenna offers more than 4,200 unique antenna patterns to optimize the reception of a given client.

The RUCKUS® adaptive antenna technology also includes adaptive polarization diversity—further increasing signal gain. Translating to better reception and transmission, polarization diversity is particularly advantageous for handheld devices that are hard to hear and constantly change direction.

Completely standards based, and Wi-Fi 6, the BeamFlex smart antenna system works with any off-the-shelf 802.11a/b/g/n chipset and is integrated into every RUCKUS smart Wi-Fi access point.

How it works

Unlike omnidirectional antennas that radiate signals in all directions, BeamFlex directs transmit energy toward the best path to the receiving device. And, unlike fixed-position directional antennas, BeamFlex dynamically configures and re-configures its antenna pattern to achieve focused coverage with directional performance within a given environment—thus increasing signal gain.

The BeamFlex smart antenna is controlled by an optimization engine that automatically reconfigures the antenna patterns on a packet-by-packet basis—selecting the best performing and highest quality signal path and optimum data rate for each receiving device.

The expert software system within BeamFlex extracts important information from all 802.11 packets received, such as the sender's performance, the optimum data rate, RSSI, error rates and approximate location. It then ranks the optimum antenna patterns for each communicating device—keeping track of the best performing signal path at any time for any given client. The resulting antenna pattern shows RF energy directed toward the client, thus increasing performance while mitigating interference by removing energy where it does not need to go for each packet transmitted.

What's the big deal?

Consistent performance

By continuously steering transmissions to high-quality signal paths, BeamFlex maximizes and sustains Wi-Fi transmission speeds while minimizing transmission errors. BeamFlex stabilizes wireless network performance to enable consistent throughput at range.

Extended range

And, because BeamFlex enables high-gain, directional Wi-Fi signals to clients, it delivers up to a four-fold increase in range over any other Wi-Fi access point.

Stable connections

Through antenna diversity and dynamic adaptation, BeamFlex ensures that the best performing and most reliable signal path is used at any given time—thereby minimizing erratic Wi-Fi behavior such as dropped connections.

Interference mitigation

BeamFlex is able to select antenna patterns that focus RF energy away from the direction of interference—thereby attenuating noise to the receiving station. This enables remarkable improvements in signal gain while, at the same time, reducing interference or contention among other APs. Using these interference mitigation techniques, a single ZoneFlex AP can realize up to 6 dBi in signal gain and 15 dB in interference mitigation. An interference mitigation algorithm enables the BeamFlex software to detect the direction of interference from, for example, a neighboring network, a microwave oven, or a nearby Bluetooth device. In response, BeamFlex is able to select antenna patterns that direct energy away from the direction of interference—attenuating noise to the receiving station.

Better RF neighbor

Because BeamFlex only focuses RF energy where it's needed, it interferes less with other Wi-Fi access points and clients.

Automatic adaptation

Dynamically configuring the Wi-Fi “beam” hundreds of times each second, BeamFlex can adapt in real time to environmental changes—steering signals around obstacles, interference and other hazards that would otherwise negatively affect performance.

BeamFlex effectively allows each RUCKUS AP to deliver high-gain directional Wi-Fi signals in 360 degrees while simultaneously minimizing noise to nearby networks, devices and other APs.

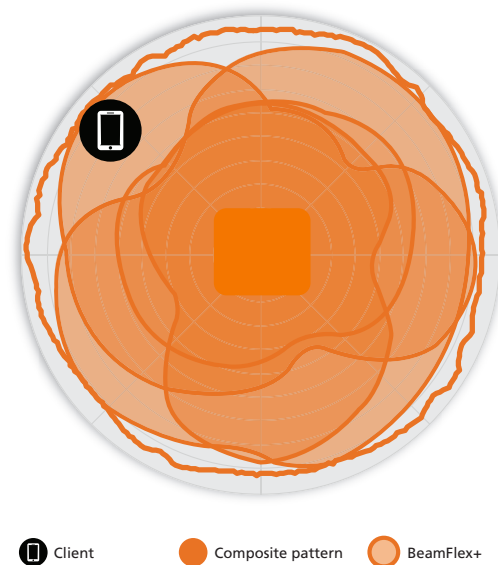


Figure 1. Example of BeamFlex+ pattern

BeamFlex not only focuses RF energy where it's needed but also mitigates interference coming from other directions. This ensures that the highest possible PHY rate is used and that the highest possible throughput is achieved for all clients.

COMMScope®

commscope.com

Visit our website or contact your local CommScope representative for more information.

© 2021 CommScope, Inc. All rights reserved.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO 9001, TL 9000, and ISO 14001.

Further information regarding CommScope's commitment can be found at www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability.

PA-115628-EN (04/21)

SCHEDA TECNICA DELLA FAMIGLIA DI PRODOTTI



VANTAGGI

Wi-Fi ULTRAVELOCE

- Garantisci agli utenti un'esperienza eccellente anche negli ambienti più complessi. La tecnologia di antenna adattiva BeamFlex+™ riconfigura in modo dinamico i diagrammi di radiazione delle antenne scegliendo tra più di 4.000 diagrammi per ottenere prestazioni superiori da qualsiasi dispositivo.
- Throughput superiore su ogni banda. La tecnologia di gestione dinamica dei canali ChannelFly™ utilizza funzionalità di apprendimento automatico per individuare in modo autonomo i canali meno congestionati.
- Costi ridotti, installazione semplificata. La tecnologia mesh wireless SmartMesh™ consente di creare in modo dinamico reti mesh autoformanti e in grado di ripristinarsi automaticamente attraverso la semplice selezione di una casella, riducendo la necessità di costosi cablaggi e configurazioni mesh complesse.

INSTALLAZIONE E GESTIONE SEMPLIFICATE

- Rete in funzione in poco meno di 5 minuti. Con Zero-Touch Mesh, puoi configurare l'intera rete Wi-Fi in pochi semplici passaggi da un dispositivo mobile o un browser grazie a un'interfaccia utente intuitiva di facile comprensione.
- Controllo totale nelle tue mani. Raccogli informazioni dettagliate sulla rete e svolgi tutte le attività amministrative chiave ovunque ti trovi grazie all'app Unleashed gratuita per iPhone e Android.

OLTRE IL WI-FI

- Rete ricca di funzionalità. Arricchisci la rete con funzionalità integrate come i servizi guest, la sicurezza DPSK, l'onboarding Zero IT e la visibilità sulle applicazioni.
- Resilienza integrata. Se la connessione a Internet non è disponibile, anche in caso di guasto a un AP, puoi continuare ad accedere alle stampanti e agli altri dispositivi di rete.

LA TUA AZIENDA È CRESCIUTA PIÙ DELLA RETE WI-FI?

Dispositivi sempre più numerosi. Applicazioni video "affamate" di larghezza di banda. Internet of Things (IoT). Costante richiesta di connettività mobile. E non dimentichiamo tutte le tendenze tecnologiche più recenti. Di fronte a tutto questo, la rete Wi-Fi non può farsi trovare impreparata. L'epoca in cui un dispositivo Wi-Fi di livello consumer poteva assolvere a tutte le richieste di una piccola azienda è finita per sempre. Oggi, anche le aziende più piccole esigono una connettività veloce, affidabile e sempre disponibile per decine o persino centinaia di dispositivi. Allo stesso tempo, le piccole e medie aziende non hanno il tempo, o spesso le competenze IT interne, di eseguire installazioni e configurazioni complesse.

Desideri una rete Wi-Fi ultraveloce? Un'installazione e una gestione semplificate? Una sicurezza e una resilienza di livello aziendale? Funzionalità di livello Enterprise? E il tutto a un costo accessibile? Ti presentiamo Ruckus Unleashed. Basati sulle nostre tecnologie brevettate, questi access point (AP) assicurano prestazioni Wi-Fi eccezionali, ma in un pacchetto progettato per le piccole e medie aziende dal costo davvero competitivo.



Wi-Fi a elevate prestazioni, di facile configurazione e gestione e dal costo contenuto

Prof. ALESSANDRO SALVINI
Progettista Progetto 13.1.1A-FESRPON-TO-2021-308

