Forcepoint

Scheda dati

# Next Generation Firewall

Sicurezza di rete aziendale con funzionalità SD-WAN native

## Vantaggi principali

### Connettività per aziende SD-WAN sempre attiva

Le aziende di oggi richiedono soluzioni di sicurezza di rete totalmenteresilienti. Forcepoint Next-Gen Firewall (NGFW) offre scalabilità e disponibilità elevate a tutti i livelli.

- **Clustering misto-attivo attivo.** È possibile raggruppare fino a 16 nodi di modelli diversi in esecuzione di versioni diverse. Ciò fornisce prestazioni e resilienza di rete superiori e abilita la sicurezza come l'ispezione approfondita dei pacchetti e le VPN.
- **Aggiornamenti delle policy e aggiornamenti software senza interruzioni.** La disponibilità leader del settore di Forcepoint consente di inviare facilmente gli aggiornamenti delle policy (e persino gli aggiornamenti software) a un cluster senza interruzioni del servizio.
- Estende la copertura ad alta disponibilità alle connessioni di rete e VPN. Combina la sicurezza senza sosta con la possibilità di sfruttare le connessioni a banda larga locali per integrare o sostituire le linee costose in locazione come l'MPLS.

Forcepoint Next-Gen Firewall offre una sicurezza di rete leader del settore con una connettività SD-WAN rapida e flessibile per connettere e proteggere le persone e i dati utilizzati nelle diverse reti aziendali in continua evoluzione. Forcepoint NGFW offre sicurezza, prestazioni e operazioni uniformi su sistemi fisici, virtuali e cloud. È stato progettato da zero per garantire un'elevata disponibilità e scalabilità, oltre a una gestione centralizzata e una visibilità completa a 360 °.

**I clienti che passano a Forcepoint NGFW I clienti che passano a Forcepoint NGFW registrano un calo dell'86% degli attacchi informatici, il 53% in meno di costi IT e una riduzione del 70% dei tempi di manutenzione.***

### Rimani al passo con le mutevoli esigenze di sicurezza

Un nucleo software unificato consente a Forcepoint di gestire più ruoli di sicurezza, da firewall/VPN e ZTNA Application Connector all'Intrusion Prevention System (IPS) e al firewall di livello 2, in ambienti aziendali dinamici. Forcepoint può essere distribuito in vari modi (ad esempio, appliance fisiche, virtuali, cloud), gestendo tutto da un'unica console.

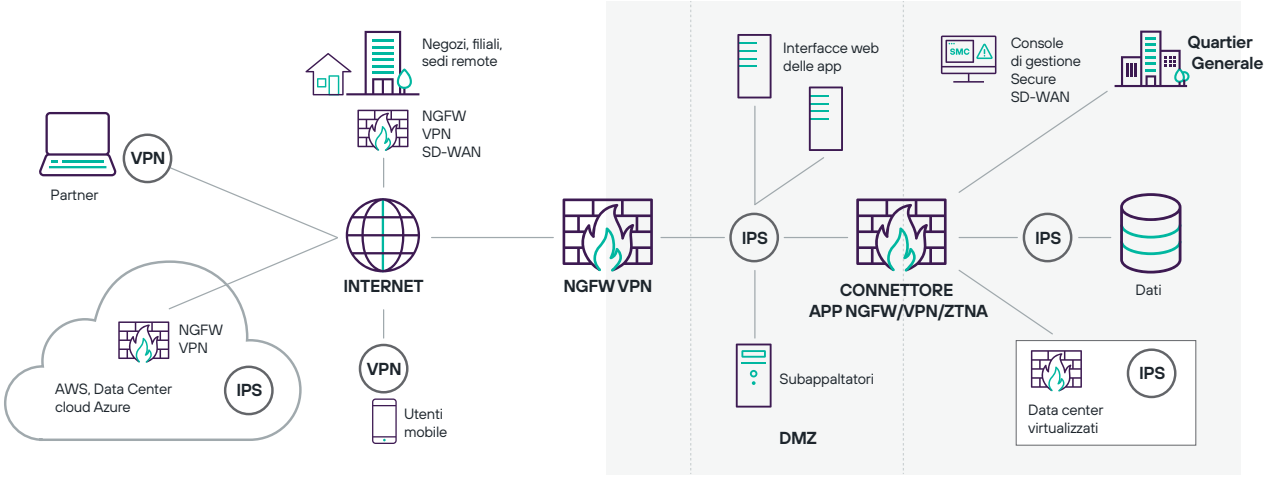
Forcepoint personalizza in modo univoco il controllo degli accessi e la deep inspection per ogni connessione al fine di fornire prestazioni e sicurezza elevate. Combina il controllo granulare delle applicazioni, le difese IPS, il controllo della rete privata virtuale (VPN) integrato e i proxy applicativi mission-critical in un design efficiente, estensibile e altamente scalabile. Le nostre potenti tecnologie anti-evasione decifrano e normalizzano il traffico di rete prima dell'ispezione e su tutti i livelli di protocollo per esporre e bloccare i metodi di attacco più avanzati.

### Blocca gli attacchi sofisticati di violazione dei dati

Le violazioni dei dati di grandi dimensioni continuano a colpire aziende e organizzazioni di ogni settore. Combatti questa minaccia prevenendo le fuoriuscite a livello di applicazione. Forcepoint consente o blocca in modo selettivo e automatico il traffico di rete proveniente da applicazioni specifiche su PC, laptop, server, condivisioni di file e altri dispositivi endpoint in base a dati contestuali di tipo endpoint altamente granulari. Prevenire le fuoriuscite di dati sensibili dagli endpoint tramite programmi non autorizzati, applicazioni web, utenti e canali di comunicazione va oltre i normali firewall.

* "Quantifying the Operational and Security Results of switching to Forcepoint NGFW", R. Ayoub & M. Marden, IDC Research, maggio 2017.

## Un'unica piattaforma con molte opzioni di distribuzione, tutte gestite da un'unica console




## Protezione senza pari

Gli aggressori sono diventati esperti nel penetrare nelle reti, nelle applicazioni, nei data center e negli endpoint aziendali. Una volta all'interno, possono rubare la proprietà intellettuale, le informazioni sui clienti e altri dati sensibili, causando danni irreparabili alle aziende e alla loro reputazione.

Le nuove tecniche di attacco possono eludere il rilevamento da parte dei dispositivi di rete di sicurezza tradizionali, tra cui molti firewall di marchi famosi, andando oltre la semplice trasmissione di exploit di vulnerabilità.

Queste strategie di evasione agiscono a più livelli per occultare exploit e malware, rendendoli invisibili all'ispezione dei pacchetti tradizionale basata su firma. Anche gli attacchi che sono bloccati da anni possono venire aggiornati mediante evasioni per compromettere i sistemi interni.

L'approccio di Forcepoint è diverso. Il nostro motore di sicurezza leader del settore è progettato per tutte e tre le fasi della difesa di rete: sconfiggere le evasioni, rilevare gli exploit di vulnerabilità e bloccare i malware. Può essere applicato in trasparenza a monte dei firewall già esistenti, per aggiungere protezione senza interferenze, oppure come firewall di fascia enterprise per una strategia di sicurezza all-in-one.

Inoltre, Forcepoint fornisce una decrittazione rapida del traffico crittografato, comprese le connessioni web HTTPS, in combinazione con controlli sulla privacy granulari per mantenre la tua azienda e gli utenti al sicuro in un mondo in rapida evoluzione. Può persino limitare l'accesso da applicazioni endpoint specifiche per bloccare i dispositivi o impedire l'uso di software vulnerabili.

### Risultati per le aziende

- → Implementazione più rapida di filiali, cloud o data center
- → Meno tempi di inattività
- → Più sicurezza, senza interferenze
- → Meno violazioni
- → Meno esposizione alle nuove vulnerabilità, mentre i team IT preparano la distribuzione delle nuove patch
- → TCO inferiore per l'infrastruttura di rete e la sicurezza

### Funzioni chiave

- → Connettività SD-WAN su scala aziendale
- → Integrazione SASE/SSE per sicurezza web, cloud e app private
- → IPS integrato con difese anti-evasione
- → Clustering ad alta disponibilità di dispositivi e reti
- → Aggiornamenti automatizzati e senza tempi di inattività
- → Gestione centralizzata basata su policy
- → Visibilità a 360° interattiva e operativa
- → Proxy di sicurezza Sidewinder per applicazioni mission-critical
- → Contesto utente ed endpoint
- → Decrittografia ad alte prestazioni con controlli granulari della privacy
- → Consenti/blocca in base all'applicazione e alla versione client
- → Monitoraggio dello stato di integrità delle applicazioni
- → Integrazione CASB e protezione Web
- → Sandboxing anti-malware
- → Software unificato per distribuzioni fisiche, AWS, Azure, e VMware
- → Meno esposizione alle nuove vulnerabilità, mentre i team IT preparano la distribuzione delle nuove patch
- → TCO inferiore per l'infrastruttura di rete e la sicurezza

Specifiche Forcepoint NGFW

| PIATTAFORME | |
|---|---|
| Appliance fisica | Diverse opzioni di appliance hardware, che vanno dalla filiale alle installazioni di data center |
| Infrastruttura cloud | Amazon Web Services, Microsoft Azure, Google, Oracle, IBM |
| Appliance virtuali | Sistemi basati su 64 bit x86; VMware ESXi, VMware NSX, Microsoft Hyper-V, KVM e Nutanix AHV |
| Endpoint | Endpoint Context Agent (ECA), client VPN |
| Contesti virtuali | Fino a 250 |
| Gestione centralizzata | Sistema di gestione centralizzata a livello aziendale con funzionalità di analisi, monitoraggio e reporting dei log. Per ulteriori dettagli, consulta la scheda tecnica del Forcepoint Security Management Center. |

| FUNZIONALITÀ DEL FIREWALL | |
|---|---|
| Ispezione profonda dei pacchetti | Normalizzazione del traffico a più livelli/Deep inspection a flusso completo, difesa anti-evasione, rilevamento dinamico del contesto, gestione/ispezione del traffico specifici per protocollo, decrittografia granulare del traffico SSL/TLS (sia TLS 1.2 che 1.3), rilevamento degli exploit delle vulnerabilità, impronte digitali personalizzate, ricognizione, anti-botnet, correlazione, registrazione del traffico, protezione DoS/DDoS, metodi di blocco, aggiornamenti automatici |
| Identificazione degli utenti | Database interno degli utenti, LDAP nativo, Microsoft Active Directory, RADIUS, TACACS+, Microsoft Exchange, Certificazioni client |
| Elevata disponibilità | › Clustering firewall attivo/attivo in standby fino a 16 nodi<br>› SD-WAN<br>› Failover stateful (incluse le connessioni VPN)<br>› Bilanciamento del carico del server<br>› Aggregazione di link (802.3ad)<br>› Rilevamento dei guasti ai link |
| Assegnazione dell'indirizzo IP | › IPv4 statico, DHCP, PPPoA, PPPoE, IPv6 statico, SLAAC, DHCPv6<br>› Servizi: Server DHCP per IPv4 e relè DHCP per IPv4 e IPv6 |
| Routing | › Rotte IPv4 e IPv6 statiche, routing basato su policy, routing multicast statico<br>› Routing dinamico: RIPv2, RIPng, OSPFv2, OSPFv3, BGP, MP-BGP, BFD, PIM-SM, PIM-SSM, IGMP proxy<br>› Routing basato sulle applicazioni |
| IPv6 | IPv4/IPv6 doppio stack, NAT44, NAT64, NAT66, ICMPv6, DNSv6, NAT, funzionalità NGFW complete |
| Reindirizzamento proxy | Reindirizzamento dei protocolli HTTP, HTTPS, FTP e SMTP a Forcepoint o a servizio di ispezione dei contenuti (CIS) di terze parti on-premise e cloud |
| Geo-protezione | Paese o continente di origine/destinazione aggiornato dinamicamente |
| Elenco di indirizzi IP | Categorie IP predefinite o elenchi di indirizzi IP personalizzati o importati |
| Filtraggio degli URL (abbonamento separato) | Elenchi di URL personalizzati o importati; supporta QUIC e HTTP/3 |
| dell'applicazione endpoint | Nome e versione |
| Applicazioni di rete | Oltre 7400 applicazioni di rete e cloud |
| Sidewinder Security Proxies | TCP, UDP, HTTP, HTTPS, SSH, FTP, TFTP, SFTP, DNS |

| INTEGRAZIONE CON SASE | |
|---|---|
| Inoltro del traffico web | Tunneling GRE e IPsec su piattaforme di Security Service Edge (SSE) come Forcepoint ONE |
| ZTNA Application Connector | Consente alle applicazioni private nei data center interni di connettersi alla Zero Trust di Forcepoint ONE |

| SD-WAN | |
|---|---|
| Protocolli | IPsec e TLS |
| VPN Site-to-Site | › VPN basata su policy e route<br>› Hub e spoke, mesh completa, mesh parziale, topologie ibride<br>› Selezione dinamica di più collegamenti ISP<br>› Condivisione dei carichi, attivo/standby, aggregazione di link<br>› Monitoraggio e reporting in tempo reale sulla qualità dei collegamenti degli ISP (ritardo, jitter, packet loss) |
| Accesso remoto | › Client VPN Forcepoint per Microsoft Windows, Android e Mac OS<br>› Qualsiasi client IPsec standard<br>› Alta disponibilità con failover automatico<br>› Controlli di sicurezza del client<br>› Accesso a portale TLS VPN |

| CONTROLLO FILE E RILEVAMENTO MALWARE AVANZATI | |
|---|---|
| Protocolli | FTP, HTTP, HTTPS, POP3, IMAP, SMTP |
| Filtraggio dei file | Filtraggio dei file basato su policy con processi di selezione efficienti.<br>Oltre 200 tipi di file supportati in 19 categorie di file |
| Reputazione dei file | Controllo della reputazione e bloccaggio di malware in cloud ad alta velocità |
| Anti-Virus | Motore di scansione antivirus locale* |
| Sandboxing zero-day | Forcepoint Advanced Malware Detection and Protection è disponibile sia come servizio cloud che on-premise |

* La scansione anti-malware locale non è disponibile con le appliance 110/115.