SOPHOS
Cybersecurity delivered.

Guida all'acquisto di soluzioni Next-Gen Firewall

In alcuni recenti sondaggi, alla richiesta di citare i principali problemi osservati nei propri firewall attuali, i responsabili IT hanno risposto come segue:

- Pessima visibilità sulle applicazioni, sui rischi e sulle minacce della rete
- Mancanza di fiducia nelle capacità di protezione contro i più recenti tipi di ransomware e di attacchi
- Risposta o assistenza inesistenti quando viene rilevata una minaccia all'interno della rete
- Difficoltà nel raggiungimento degli obiettivi di rete per la SD-WAN

Se tutto questo riflette la tua situazione, sei in buona compagnia. Il problema è che attualmente nella maggior parte dei casi i firewall Next-Gen non funzionano come dovrebbero. Non sono in grado di garantire adeguati livelli di visibilità, protezione o risposta alle minacce; inoltre, non includono opzioni di rete semplici e flessibili per la SD-WAN.

Quando si selezionano le opzioni più idonee per la scelta del prossimo firewall, anche sapere da che punto cominciare può essere un compito arduo. È consigliabile iniziare identificando le proprie esigenze principali. Una volta individuati tali requisiti, si presenta l'arduo compito di doversi districare tra i siti web e le schede tecniche dei vari vendor, nel tentativo di stabilire non solo quale sia il firewall che più si addice alle proprie esigenze, ma anche quello che mantiene le promesse fatte.

Come usare la guida

Questa guida all'acquisto è realizzata per aiutarvi a scegliere la soluzione ideale per la vostra organizzazione e per evitarvi di rimpiangere, in futuro, la scelta fatta. Descrive tutte le opzioni e le funzionalità da dover tenere in considerazione durante il processo di acquisto del vostro prossimo firewall. Abbiamo anche incluso alcune domande importanti da rivolgere al vostro vendor o partner IT per assicurarvi che il prodotto che state valutando sia veramente in grado di rispondere alle vostre esigenze. Inoltre, nelle ultime pagine troverete un pratico grafico che vi aiuterà a risparmiare tempo prezioso durante la compilazione di un primo elenco di vendor di soluzioni firewall idonee.

La tempesta perfetta nella protezione della rete: la cifratura

Il costante aumento dei flussi di traffico cifrato ha creato la tempesta perfetta, con conseguenze catastrofiche. Si considerino le seguenti statistiche:

- Il 90% del traffico Internet è ora cifrato con TLS
- Il 50% di malware, applicazioni potenzialmente indesiderate (PUA) e server degli hacker sfruttano la cifratura per eludere il rilevamento
- La maggior parte delle organizzazioni non ispeziona il traffico cifrato

Quando chiediamo alle organizzazioni perché non controllano il traffico cifrato, il motivo più frequente è la performance. L'ispezione TLS implica un utilizzo di risorse estremamente elevato e gran parte dei firewall non riesce a tenere testa all'enorme quantità di traffico cifrato. Il secondo motivo principale per evitare l'ispezione del traffico cifrato: tende a causare problemi di usabilità, rendendo inutilizzabile l'Internet.

Questa sfida di base per la cifratura, unita all'incapacità di molti firewall di affrontarla in maniera adeguata, sta generando una serie di problemi aggiuntivi: mancanza di visibilità su comportamenti e contenuti rischiosi, nonché problemi di conformità e di protezione contro ransomware, attacchi e violazioni. La cifratura è a tutti gli effetti la causa principale di molte delle principali sfide di sicurezza della rete. Purtroppo quasi tutte le reti si limitano a sorvolare su questi problemi e a ignorare gran parte del traffico. Tutto questo non è più necessario. Ora esiste un modo estremamente efficace per affrontare questa sfida.

Per scoprire di più, dai un'occhiata al nostro whitepaper: Ora che c'è la cifratura, il firewall non è più essenziale?

Principali funzionalità essenziali

Per risolvere i principali problemi di visibilità di rete, protezione e risposta alle minacce, occorre cercare nel prossimo firewall quattro funzionalità indispensabili che non sono presenti in quello attuale:

Ispezione TLS 1.3: il 90% del traffico Internet è cifrato e questa percentuale è in aumento. Pertanto, è fondamentale che il prossimo firewall includa l'ispezione TLS 1.3. Più di ogni cosa, deve offrire le capacità di intelligence e performance necessarie per svolgere questa operazione in maniera efficiente, senza causare rallentamenti e senza costringervi ad acquistare un firewall molto più caro del dovuto. Non tutto il traffico cifrato richiede ispezione e non tutto il traffico cifrato la supporta. È necessario che il prossimo firewall che acquistate supporti tutti i più recenti standard e suite di cifratura. Deve anche integrare eccezioni intelligenti, per una maggiore selettività del traffico da ispezionare. Allo stesso tempo, deve offrire gli strumenti necessari per identificare con facilità i potenziali problemi e per aggiungere eccezioni "al volo" al fine di prevenirli. Un'altra caratteristica indispensabile è un livello adeguato di performance per tenere testa a un volume di cifratura sempre più elevato, sia oggi che in futuro.

Protezione contro le minacce zero-day: le minacce si evolvono continuamente. Le varianti di ransomware utilizzate per attaccare un'organizzazione domani saranno sicuramente diverse da quelle utilizzate ieri. Questa è la natura del panorama attuale delle minacce. Il tuo prossimo firewall deve utilizzare tecnologie di intelligenza artificiale basate su modelli di machine learning multipli, oltre a sandboxing con rilevamento avanzato degli exploit e rilevamento antiransomware CryptoGuard. Con queste funzionalità, potrà identificare le più recenti minacce zero-day e bloccarle prima che possano infiltrarsi nella rete.

Accelerazione delle applicazioni con FastPath: statisticamente, è probabile che circa l'80% del traffico di rete provenga dal 20% delle app. Questi flussi di proporzioni enormi sono tipici di strumenti per riunioni e collaborazioni, streaming multimediali e VoIP. Richiedono un enorme dispendio di risorse per essere ispezionati e in più hanno bisogno di livelli di performance estremamente elevati per garantire una buona esperienza utente. La combinazione di questi fattori genera molte complicazioni. Il tuo prossimo firewall deve essere in grado di gestire in maniera adeguata questi flussi di traffico attendibili, effettuandone l'offload per garantire una performance ottimale e per liberare più risorse da dedicare al traffico che richiede un'ispezione più approfondita dei pacchetti.

Orchestrazione e gestione della rete SD-WAN: oggi come oggi la maggior parte delle organizzazioni dipende da connessioni Internet WAN ridondanti, con percorsi multipli che richiedono soluzioni SD-WAN pratiche, convenienti, resilienti e in grado di adattarsi alla rete. Chiunque abbia mai provato a configurare tunnel VPN tra firewall multipli, abbia cercato di gestire scenari di ridondanza e failover automatici, o si sia trovato alle prese con l'ottimizzazione del routing delle applicazioni su più collegamenti WAN sa benissimo che tutte queste attività sono molto complesse. Il tuo prossimo firewall deve includere opzioni SD-WAN integrate, tra cui: routing automatizzato e resiliente della SD-WAN, opzioni economiche di connettività SD per le filiali e semplicità di orchestrazione per la rete SD-WAN.

Integrazione con altri prodotti di cybersecurity: i prodotti di sicurezza che operano in maniera isolata non bastano più. Gli attacchi attuali sono molto sofisticati e per essere contrastati richiedono livelli di protezione multipli, con soluzioni che interagiscono in maniera coordinata, condividendo informazioni per orchestrare una risposta sincronizzata. Il vostro prossimo firewall deve integrarsi con altri sistemi (come la protezione antivirus per endpoint) per condividere importanti dati di telemetria e intelligence sulle minacce. Questo tipo di struttura permetterà a entrambe le soluzioni di interagire in maniera ottimale per coordinare la strategia di difesa in caso di attacco. Inoltre, i sistemi in questione devono condividere un'interfaccia di gestione comune, per semplificare la distribuzione e la gestione delle operazioni quotidiane, nonché il threat hunting e la reportistica con l'utilizzo di prodotti multipli.

Queste quattro funzionalità metteranno fine ai problemi del vostro firewall attuale, preparando la strada per una protezione della rete in grado di affrontare con successo le sfide del futuro.

Funzionalità essenziali	Domande da porre al vendor
Ispezione TLS 1.3 Offre visibilità sul volume in continuo aumento di traffico cifrato sulle reti	‣ La vostra ispezione TLS supporta il più recente standard 1.3? ‣ Funziona su tutte le porte e tutti i protocolli? ‣ È basata su streaming o su proxy? ‣ Qual è l'impatto sulla performance? ‣ Include una dashboard che offre visibilità sui flussi di traffico cifrato? ‣ Include una dashboard che offre visibilità sui siti che non supportano la decifratura? ‣ Include strumenti facili da usare per l'aggiunta di eccezioni per i siti web problematici? ‣ Include un elenco completo di esclusioni? ‣ Chi mantiene l'elenco? Lo aggiorna regolarmente?
Protezione contro le minacce mai viste prima (Zero-Day) Protezione contro le più recenti minacce inedite, con tecnologie di machine learning e sandboxing	‣ Il vostro firewall include tecnologie in grado di rilevare minacce mai osservate prima? ‣ Utilizza il machine learning per analizzare i file? ‣ Quanti modelli di machine learning vengono applicati? ‣ La vostra soluzione include il sandboxing? ‣ Il sandboxing autorizza il file mentre viene analizzato? ‣ La vostra soluzione di sandboxing si esegue on-premise o nel cloud? ‣ La vostra soluzione di sandboxing include tecnologie di protezione endpoint leader di settore, in grado di identificare minacce come il ransomware nell'ambiente sandbox? ‣ Quali tecnologie endpoint vengono utilizzare per assistere il sandboxing? ‣ Quale tipo di reportistica integrata è disponibile (a differenza di un prodotto di reportistica da acquistare separatamente)? ‣ Quale tipo di visibilità viene offerta?
Accelerazione delle applicazioni con FastPath Offload del traffico delle applicazioni attendibili su un FastPath (percorso rapido), per migliorare la performance e ridurre il carico di base	‣ Il vostro firewall supporta l'accelerazione con FastPath del traffico attendibile e dei flussi estremamente elevati? ‣ Avviene tramite software o hardware? ‣ Come vengono identificate le applicazioni per l'accelerazione con FastPath? ‣ Quali strumenti per le policy vengono forniti agli amministratori per selezionare le applicazioni di cui effettuare l'offload? ‣ Ci sono firme preimpostate per accelerare e inserire alcune applicazioni sul FastPath? ‣ I vostri processori di flusso per i pacchetti sono programmabili, predisposti per gli upgrade e in grado di seguire le evoluzioni future del panorama informatico?
Orchestrazione e gestione della rete SD-WAN Strumenti potenti e facili da usare per la gestione di collegamenti WAN multipli e reti overlay per le filiali.	‣ Il vostro firewall include opzioni SD-WAN sofisticate e integrate? ‣ Offrite routing del traffico delle applicazioni su collegamenti WAN, in base al tipo di applicazione, utente o servizio? ‣ La vostra soluzione permette di identificare e instradare il traffico di applicazioni sconosciute o personalizzate? ‣ Sono disponibili transizioni a impatto zero che mantengono le connessioni delle applicazioni quando si verifica un'interruzione del servizio dell'ISP, oppure le app devono richiedere una nuova connessione? ‣ Offrite opzioni di orchestrazione centralizzata delle reti VPN SD-WAN overlay tramite interfaccia basata sull'uso del mouse, che permettono di coordinare facilmente più firewall e posizioni? ‣ Il vostro firewall prevede l'offload e l'accelerazione hardware del traffico dei tunnel VPN SD-WAN? ‣ Includete opzioni hardware zero-touch economiche per la connessione sicura di posizioni o dispositivi remoti?
Integrazione con altri prodotti di sicurezza L'integrazione è essenziale per garantire un'adeguata protezione a livelli multipli e per consentire la condivisione di informazioni tra i prodotti a scopo di risposta alle minacce o di indagine approfondita e threat hunting	‣ Il vostro firewall è integrato con una tecnologia endpoint? ‣ Quali informazioni vengono condivise tra i due prodotti? ‣ Quando uno dei prodotti identifica una minaccia, condivide questa informazione con l'altro? ‣ In che cosa consiste la risposta in caso di rilevamento di una minaccia? È in grado di isolare automaticamente le minacce? Come procede per farlo? ‣ La tecnologia endpoint fornisce al firewall informazioni sugli utenti o sull'utilizzo delle applicazioni? ‣ Le soluzioni firewall ed endpoint possono essere gestite dalla stessa console? Si tratta di una console basata sul cloud? ‣ È possibile condurre threat hunting con prodotti multipli (Extended Detection and Response, XDR)? ‣ Il vendor offre un servizio di monitoraggio della rete e risposta alle minacce completamente gestito? ‣ Il firewall si integra con altri prodotti quali soluzioni Wi-Fi, ZTNA, dispositivi edge o switch di rete?

Principali funzionalità firewall

Anche le seguenti tecnologie sono componenti essenziali per qualsiasi soluzione firewall. Molte sono elementi fondamentali e consolidati per qualsiasi firewall, per cui spesso la selezione dei vendor si basa sulla semplicità di gestione e sul livello di visibilità pratica che offrono.

Assicuratevi che il vostro prossimo firewall non si limiti a includere queste funzionalità, ma che garantisca soprattutto maggiore visibilità sui rischi e sui problemi in ciascuno di questi ambiti.

Funzionalità principali	Domande da porre al vendor
Ispezione approfondita dei pacchetti e protezione dalle intrusioni Includono decifratura e ispezione per individuare minacce ed exploit	‣ La vostra ispezione TLS supporta il più recente standard 1.3? ‣ Funziona su tutte le porte e tutti i protocolli? ‣ È basata su streaming o su proxy? ‣ Qual è l'impatto sulla performance? ‣ Include una dashboard che offre visibilità sui flussi di traffico cifrato? ‣ Include una dashboard che offre visibilità sui siti che non supportano la decifratura? ‣ Include strumenti facili da usare per l'aggiunta di eccezioni per i siti web problematici? ‣ Include un elenco completo di esclusioni? ‣ Chi mantiene l'elenco? Lo aggiorna regolarmente?
Protezione avanzata contro le minacce Identifica bot e altre minacce o malware di tipo avanzato che cercano di effettuare il call-home o di comunicare con server di comando e controllo	‣ Il vostro firewall include tecnologie in grado di rilevare minacce mai osservate prima? ‣ Utilizza il machine learning per analizzare i file? ‣ Quanti modelli di machine learning vengono applicati? ‣ La vostra soluzione include il sandboxing? ‣ Il sandboxing autorizza il file mentre viene analizzato? ‣ La vostra soluzione di sandboxing si esegue on-premise o nel cloud? ‣ La vostra soluzione di sandboxing include tecnologie di protezione endpoint leader di settore, in grado di identificare minacce come il ransomware nell'ambiente sandbox? ‣ Quali tecnologie endpoint vengono utilizzare per assistere il sandboxing? ‣ Quale tipo di reportistica integrata è disponibile (a differenza di un prodotto di reportistica da acquistare separatamente)? ‣ Quale tipo di visibilità viene offerta?
Protezione web e filtro degli URL Offrono protezione contro malware basato sul web, siti web compromessi e download pericolosi dal web	‣ Il vostro firewall supporta l'accelerazione con FastPath del traffico attendibile e dei flussi estremamente elevati? ‣ Avviene tramite software o hardware? ‣ Come vengono identificate le applicazioni per l'accelerazione con FastPath? ‣ Quali strumenti per le policy vengono forniti agli amministratori per selezionare le applicazioni di cui effettuare l'offload? ‣ Ci sono firme preimpostate per accelerare e inserire alcune applicazioni sul FastPath? ‣ I vostri processori di flusso per i pacchetti sono programmabili, predisposti per gli upgrade e in grado di seguire le evoluzioni future del panorama informatico?
Controllo delle applicazioni Visibilità e controllo sul traffico delle applicazioni per modellare o bloccare il traffico indesiderato e accelerare e attribuire massima priorità al traffico delle applicazioni essenziali	‣ Quali fonti di informazioni vengono utilizzate per identificare le applicazioni? ‣ Il motore delle applicazioni è in grado di utilizzare i dati ottenuti dalla soluzione endpoint per migliorare l'identificazione delle applicazioni oppure è limitato alle informazioni che riesce a recuperare dal pacchetto? ‣ Le applicazioni possono essere assegnate al FastPath e instradate su collegamenti WAN preferiti con l'uso di regole delle policy? ‣ Il sistema include una dashboard che offre analisi approfondite sulle app cloud e sullo shadow IT?

Prodotti firewall complementari

I seguenti prodotti complementari possono essere fondamentali per estendere la rete e la protezione dove necessario. Assicuratevi che il vendor che selezionate offra questi prodotti aggiuntivi e che tali prodotti siano facili da integrare con il firewall mediante gestione diretta oppure dalla stessa console di gestione centralizzata del firewall.

Prodotti complementari	Domande da porre al vendor
Dispositivi perimetrali SD-WAN per le filiali Dispositivi facili da distribuire e convenienti, per la connessione delle filiali remote più piccole	‣ Avete un dispositivo in grado di connettere le sedi remote al firewall principale con una VPN dedicata? ‣ Prevede la distribuzione senza intervento manuale? ‣ Quanto costa? ‣ Supporta sia tunnel dedicati che split-tunnel? ‣ Quali opzioni di connettività modulare supporta (ad es. Wi-Fi o LTE)?
Access point wireless Estensione della rete per includere il wireless	‣ Il firewall include un controller wireless integrato? ‣ Quanto costa? ‣ I vostri access point wireless sono subito pronti per l'uso? ‣ Supportano radio e SSID multipli? ‣ Supportano le reti mesh?
ZTNA Zero-Trust Network Access per connettere in maniera sicura gli utenti remoti alle applicazioni e ai dati	‣ Offrite una soluzione ZTNA? ‣ Si integra con il firewall e/o con la protezione endpoint? ‣ Viene gestita insieme al firewall dalla stessa console di gestione centralizzata? ‣ La distribuzione dell'agente ZTNA avviene insieme a quella dell'agente endpoint? ‣ Come viene integrato lo stato del dispositivo con la soluzione ZTNA?
Protezione delle e-mail Protezione dei messaggi e-mail contro spam, phishing e posta indesiderata	‣ Offrite una soluzione di protezione delle e-mail integrata e pronta per l'uso? ‣ Offrite la gestione dal cloud per la protezione delle e-mail? ‣ Include il sandboxing degli allegati sospetti? ‣ Supporta la cifratura della posta elettronica e la prevenzione contro la perdita dei dati (DLP)? ‣ Offre routing in base al dominio e una modalità MTA completa? ‣ Offre un portale utente per la gestione della quarantena?
Web Application Firewall Web Application Firewall (WAF) per la protezione tramite proxy inverso dei server on-premise connessi a Internet	‣ Offrite opzioni WAF integrate e pronte per l'uso? ‣ Semplificano la configurazione con modelli preimpostati per le più comuni applicazioni in hosting? ‣ La soluzione include protezione avanzata, CSS e blocco della manomissione dei cookie? ‣ Offre l'offload dell'autenticazione tramite reverse proxy?

Funzionalità di gestione

Spesso la differenza principale tra i vari prodotti firewall è la semplicità con cui possono essere gestiti. Molti firewall disponibili sul mercato da anni sono stati strutturati aggiungendo nuove opzioni al prodotto nel corso del tempo, utilizzando schemi grafici diversi per varie parte dell'interfaccia, dando così l'impressione che ogni sezione del prodotto sia in realtà una soluzione completamente diversa. Le funzionalità indicate di seguito possono essere significative nella distribuzione e nella gestione quotidiana delle soluzioni.

Funzionalità di gestione	Domande da porre al vendor
Gestione centrale Gestione di firewall o prodotti di IT security multipli	‣ Offrite una soluzione di gestione dal cloud? ‣ Come vengono gestiti firewall multipli con questa soluzione? ‣ Quali altri prodotti vengono gestiti dalla stessa console cloud? ‣ I dati di intelligence sulle minacce vengono condivisi tra i vari prodotti ed è possibile eseguire threat hunting con informazioni provenienti da prodotti multipli?
Reportistica Le opzioni di reportistica incluse	‣ Il firewall include archiviazione integrata per i dati di log? Quanto spazio prevede? ‣ È inclusa la reportistica integrata nell'appliance? Quanto costa? ‣ È supportata la reportistica per il cloud? Quanto costa? ‣ È possibile creare, salvare, esportare e pianificare report personalizzati? ‣ È supportata l'esportazione dei dati di syslog? ‣ Sono supportati la reportistica e il threat hunting con prodotti multipli?
Esperienza di gestione Il livello di efficacia del firewall in termini di come semplifica le operazioni di gestione quotidiana e quanto mette in evidenza le informazioni importanti	‣ Il vostro prodotto offre una dashboard dettagliata con la possibilità di approfondire sui risultati? ‣ Le policy per web, controllo delle app, IPS e shaping del traffico si trovano tutte nella stessa schermata oppure occorre configurare questi elementi in parti diverse del prodotto? ‣ L'esperienza utente è coerente tra le varie sezioni del prodotto? ‣ Sono disponibili guide approfondite, integrate e contestuali, nonché documenti, video e altri contenuti utili per chi utilizza un firewall per la prima volta?
Portale utenti Portale di autosupporto per gli utenti	‣ Il firewall offre un portale da cui gli utenti possono scaricare client VPN o impostazioni e dove possono gestire le e-mail in quarantena?

Opzioni di distribuzione

Un altro fattore importante da considerare per il tuo prossimo firewall è se sia semplice da integrare nella struttura della rete attuale e futura. Quello che occorre è un firewall in grado di inserirsi perfettamente nella rete esistente, non un prodotto che ne richieda la modifica. Assicuratevi che il vostro vendor abbia una vasta gamma di opzioni di distribuzione, incluso il supporto di piattaforme cloud pubbliche quali AWS e Azure, oltre ad altre comuni piattaforme di virtualizzazione. Inoltre, deve offrire appliance hardware flessibili e modulari.

Opzioni di distribuzione	Domande da porre al vendor
Appliance hardware Assicuratevi che il vostro prossimo firewall sia in grado di seguire le evoluzioni future del panorama informatico	‣ Quanti modelli di appliance offrite per i miei requisiti? ‣ Quali sono le opzioni di connettività incluse? ‣ Quali sono le opzioni modulari di connettività incluse? ‣ Sono disponibili alimentatori ridondanti? ‣ Quali sono le opzioni di disponibilità elevata? ‣ Gli upgrade del firmware sono inclusi nelle licenze? ‣ Quale garanzia è prevista per l'hardware?
Modalità cloud, virtuale, software Il supporto del cloud pubblico e di opzioni virtuali per reti ibride potrebbe essere importante per la struttura attuale o futura	‣ Il vostro firewall è disponibile nel marketplace di piattaforme cloud pubbliche quali AWS e Azure? ‣ Sono supportate tutte le più comuni piattaforme di virtualizzazione? ‣ La vostra appliance è disponibile anche in versione software per l'esecuzione su hardware X86?

Elenco delle funzionalità firewall

	Sophos	Meraki	Fortinet	PAN	SW	WG
Principali funzionalità firewall						
Simulatore di prova per regole firewall e policy web	✓		✓	✓		✓
Ottimizzazione dei pacchetti FastPath	✓		✓	✓		
Sistema di protezione dalle intrusioni	✓	✓	✓	✓	✓	✓
Controllo delle applicazioni	✓	Limitata	✓	✓	✓	✓
Doppio motore antivirus	✓					✓
Visibilità sulle app cloud illecite ("Shadow IT")	✓		✓	✓	✓	✓ - OEM
Blocco delle applicazioni potenzialmente indesiderate (PUA)	✓		✓	✓	✓	
Protezione e controllo web	✓	✓	✓	✓	✓	✓
Monitoraggio e implementazione di parole chiave sul web	✓		✓	✓	✓	✓
Motore DPI: streaming, proxy o entrambi?	✓	Flusso	✓	Flusso	Streaming	Proxy
Visibilità sul rischio per utenti e app (Quoziente di minaccia dell'utente)	✓		Limitata			
Protezione avanzata contro le minacce	✓	✓	✓	✓	✓	✓
Log e report storici integrati	✓		Limitata	Limitata		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Protezione per server ed e-mail						
WAF a funzionalità complete integrato	✓		Extra*			
Protezione e-mail integrata: antivirus, antispam, cifratura, prevenzione della perdita dei dati	✓					

	Sophos	Meraki	Fortinet	PAN	SW	WG
SD-WAN e VPN						
VPN di accesso remoto gratuita, illimitata e a funzionalità complete	✓	Extra*	✓	Extra*	Extra*	Extra*
VPN site-to-site IPSEC e SSL	✓	✓	✓	✓	✓	✓
VPN site-to-site con SD-RED Layer-2	✓					
Orchestrazione SD-WAN gestita dal cloud	✓	✓	Extra*		✓	
Routing SD-WAN e gestione dei collegamenti	✓	✓	✓	✓	✓	✓
Transizione failover SD-WAN a impatto zero	✓		✓	✓		
Identificazione e routing del traffico di app sconosciute o personalizzate per la SD-WAN	✓			✓		
Accelerazione hardware e offload del traffico VPN	✓		✓			
Dispositivi zero-touch economici per i tunnel VPN	✓					

	Sophos	Meraki	Fortinet	PAN	SW	WG
Ispezione TLS						
Ispezione TLS 1.3	✓		✓	✓	✓	✓
Dashboard con visibilità sui problemi relativi al traffico cifrato	✓					
Creazione di eccezioni TLS dalla dashboard	✓					

* Queste opzioni sono disponibili pagando un extra

	Sophos	Meraki	Fortinet	PAN	SW	WG
Protezione contro le minacce del giorno zero						
Analisi dei file sospetti con modelli di machine learning multipli	✓	✓	✓	✓	✓	
Sandboxing dinamico dei file sospetti	✓	✓	✓	✓	✓	✓
Analisi dei file basata sul cloud	✓	✓	✓	✓	✓	✓
Reportistica sulle analisi delle minacce estesa e integrata	✓	✓			✓	

	Sophos	Meraki	Fortinet	PAN	SW	WG
Ottimizzazione dei pacchetti FastPath						
Offload tramite FastPath del traffico SD-WAN, cloud e SaaS	✓		✓	✓		
Policy e offload automatico tramite FastPath	✓		✓	✓		
Offload e accelerazione dell'hardware	✓		✓	✓		
Processori di flusso programmabili per i pacchetti	✓			✓		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Funzionalità di integrazione della protezione endpoint						
Identificazione degli host compromessi	✓	✓	Extra*	✓	✓	✓
Isolamento automatico degli host a livello di firewall per proteggere le altre parti della rete	✓		Extra*			✓
Isolamento automatico degli host a livello di endpoint per prevenire i movimenti laterali	✓			Extra*		✓
Identificazione delle applicazioni di rete sconosciute (controllo sincronizzato delle app)	✓			✓		
Abilitazione del threat hunting con prodotti multipli (XDR)	✓			✓		
Abilitazione di un servizio di risposta alle minacce completamente gestito	✓			✓		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Integrazione di una gamma di prodotti di accesso alla rete						
Access point con controller wireless integrato	✓	✓	✓		✓	✓
Integrazione con una soluzione ZTNA	✓	✓	✓	✓	✓	
Integrazione con switch di rete	✓	✓	✓		✓	
Integrazione con dispositivi perimetrali per l'accesso remoto ai servizi (SD-RED)	✓					

* Queste opzioni sono disponibili pagando un extra

	Sophos	Meraki	Fortinet	PAN	SW	WG
Gestione dal cloud						
Gestione del firewall a funzionalità complete dal cloud, senza costi aggiuntivi	✔	✔	Extra*		Extra*	✔
Console di gestione unificata per endpoint, server, dispositivi mobili, e-mail, cifratura e firewall	✔					✔
Gestione dei gruppi di firewall dal cloud	✔	✔	Extra*		✔	
Pianificazione degli aggiornamenti del firmware dal cloud	✔	✔	✔		✔	✔
Distribuzione dei nuovi firewall dal cloud (senza intervento manuale)	✔	✔	Extra*		✔	✔
Reportistica del firewall basata sul cloud	✔	✔	✔		✔	✔
Threat hunting con prodotti multipli e gestione dal cloud (XDR)	Extra*			Extra*		

	Sophos	Meraki	Fortinet	PAN	SW	WG
Opzioni di distribuzione cloud e virtuali						
AWS	✔	✔	✔	✔	✔	✔
Azure	✔	✔	✔	✔	✔	✔
Google	In futuro	✔	✔	✔		
Nutanix	✔		✔	✔	✔	
FWaaS	In futuro		✔	✔		
Piattaforme virtuali	✔	✔	✔	✔	✔	✔
Appliance software (x86)	✔					

* Queste opzioni sono disponibili pagando un extra

Sophos Firewall

Per scoprire di più sulle opzioni e sulle funzionalità di Sophos Firewall, vi invitiamo a dare un'occhiata anche queste risorse:

- Briefing sulla soluzione Sophos Firewall
- Elenco delle funzionalità di Sophos Firewall
- Brochure di Sophos Firewall

Effettua subito una prova gratuita

Per una prova on-line gratuita di Sophos Firewall, visita la pagina: sophos.it/demo

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

22-03-31 IT (PC)

SOPHOS