SOPHOS
Cybersecurity delivered.

Sophos Firewall

Briefing del prodotto

Indice dei contenuti

Sophos Firewall

Sophos Firewall è un prodotto progettato fin dalle basi per fornire una risposta adeguata ai principali problemi dei firewall moderni. Allo stesso tempo, offre anche una vera e propria piattaforma next-gen realizzata per affrontare le difficoltà dell'attuale panorama delle connessioni internet cifrate e delle minacce in continua evoluzione. Sophos Firewall offre un approccio innovativo al modo di identificare i rischi, proteggere i sistemi dalle minacce e rispondere agli incidenti. In più, garantisce una performance ottimale. La nostra architettura Xstream per Sophos Firewall utilizza un'architettura di elaborazione dei pacchetti in grado di garantire livelli estremi di visibilità, protezione e performance.

Sophos Firewall offre una visibilità mai vista prima sugli utenti a rischio, sulle applicazioni indesiderate, sui payload sospetti e sulle minacce persistenti. Prevede la stretta integrazione di una suite completa di tecnologie di protezione contro le minacce più recenti, tutte facili da impostare e da gestire. Proprio come i firewall legacy, Sophos Firewall comunica con altri sistemi di sicurezza all'interno della rete, per diventare un punto di implementazione e contenimento delle minacce attendibile e per impedire ai malware di diffondersi o di esfiltrare dati all'esterno della rete, in maniera automatica e in tempo reale.

Sophos Firewall presenta quattro vantaggi principali rispetto agli altri firewall di rete:

1. **Mette in evidenza i rischi nascosti**: rispetto ad altre soluzioni, Sophos Firewall è molto più efficace nel mettere in evidenza i rischi nascosti, grazie alla sua dashboard visiva, alle ricche opzioni di reportistica integrata nell'appliance e nel cloud, nonché alle sue esclusive funzionalità di analisi dei rischi.
2. **Blocca le minacce sconosciute**: Sophos Firewall semplifica, ottimizza e rende più rapido il processo di blocco delle minacce, spingendosi oltre i limiti degli altri firewall, grazie alla sua suite completa di prodotti di sicurezza avanzata, tutti estremamente facili da configurare e da gestire.
3. **Risponde automaticamente agli incidenti**: Sophos Firewall con Synchronized Security risponde automaticamente agli incidenti che si verificano all'interno della rete, grazie a Sophos Security Heartbeat™, che abilita la condivisione in tempo reale dei dati di intelligence tra endpoint e firewall.
4. **Ottimizza la rete SD-WAN** : le funzionalità SD-WAN di Xstream in Sophos Firewall permettono di configurare anche le reti SD-WAN overlay più complesse in pochissimi passaggi. Inoltre, offrono opzioni molto vantaggiose, come la selezione automatica dei collegamenti WAN in base alla performance, con transizione immediata e a impatto zero dei collegamenti: questa funzionalità aiuta a ottimizzare la velocità delle applicazioni, la resilienza della rete e la continuità del business, riducendo allo stesso tempo i costi di connettività.

Smascherare i rischi nascosti

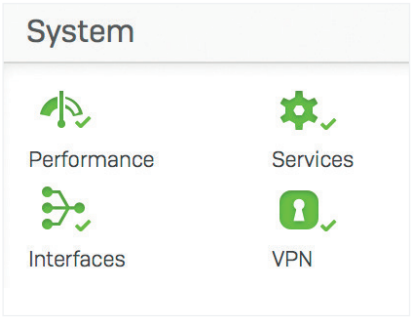
Per un firewall moderno è di vitale importanza riuscire ad analizzare la montagna di informazioni che raccoglie; deve inoltre correlare i dati, ove possibile, e mettere in evidenza solamente le informazioni più importanti che richiedono azione da parte dell'utente, possibilmente prima che sia troppo tardi.

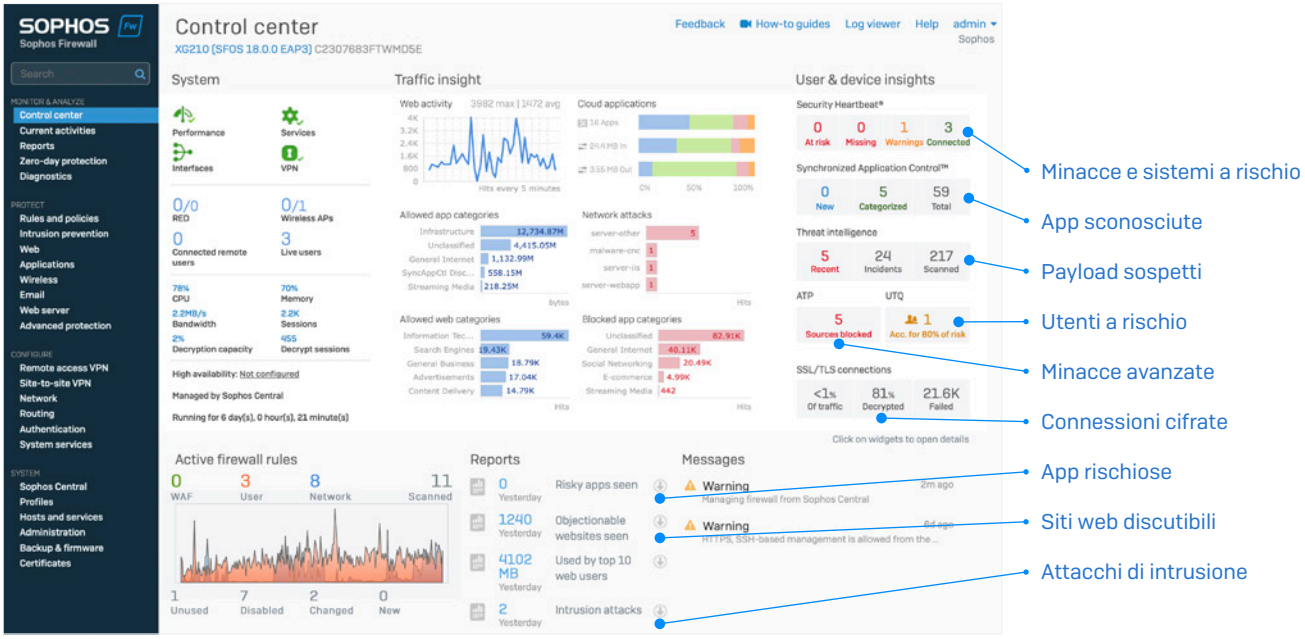
Control Center

Il Control Center di Sophos Firewall offre maggiore visibilità su attività, rischi e minacce nella rete.

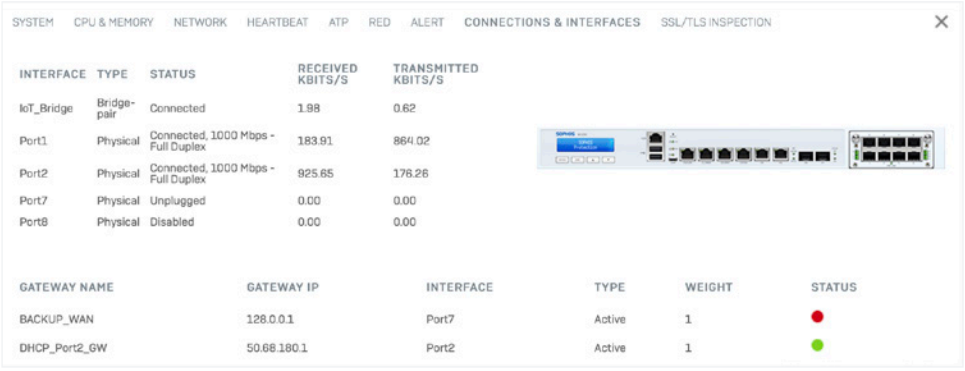
Adopera una segnaletica basata sui colori del semaforo per dirigere l'attenzione sulle questioni più importanti.

Se un elemento è rosso, richiede attenzione immediata. Il giallo indica un potenziale problema. Se tutto è verde, non è richiesta alcuna azione.

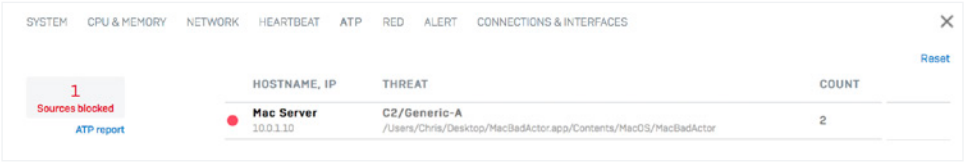




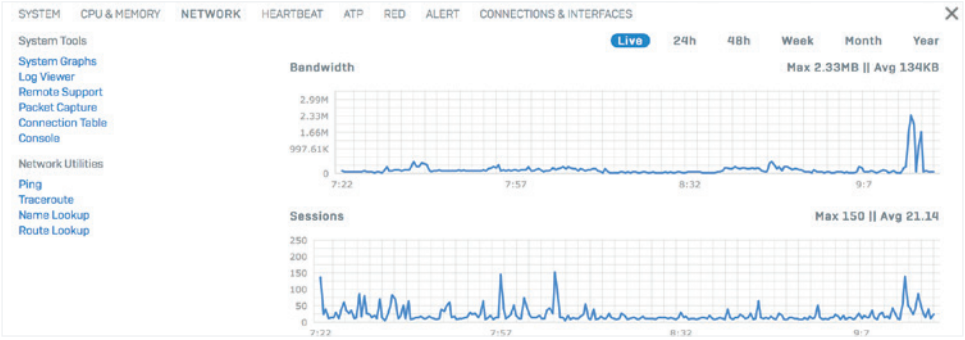
Tutti i widget del Control Center offrono informazioni aggiuntive che vengono rivelate con un semplice clic sul widget. Ad esempio, lo stato delle interfacce sul dispositivo può essere visualizzato cliccando sul widget "Interfacce" nel Control Center.



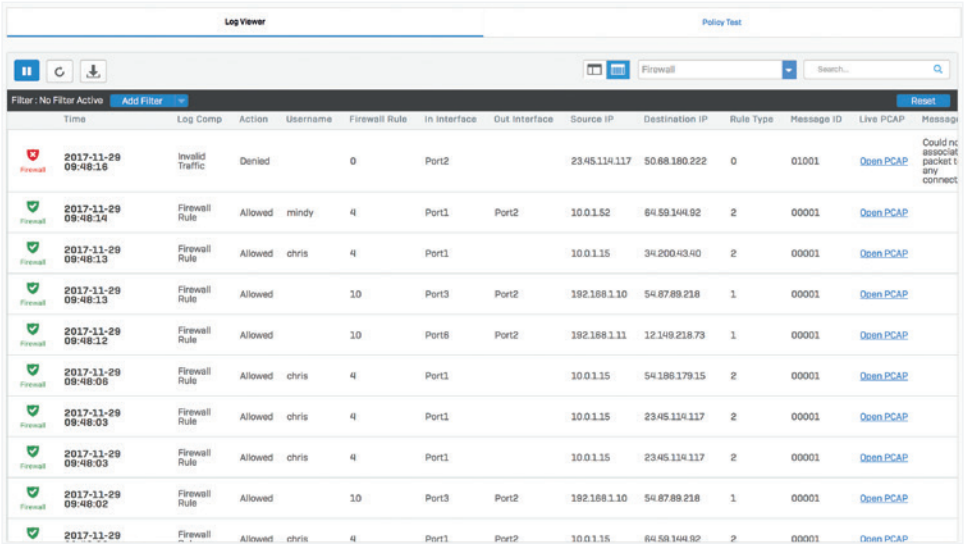
Anche host, utente e origine di una minaccia avanzata possono essere facilmente rivelati con un semplice clic nella dashboard, sul widget ATP (Advanced Threat Protection, prevenzione avanzata contro le minacce).



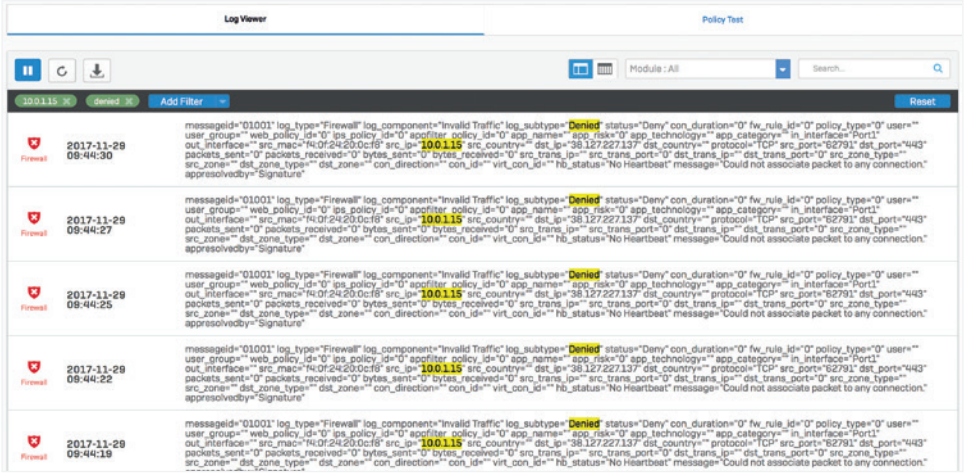
Inoltre, i grafici di sistema mostrano la performance durante orari specifici e selezionabili, sia che si desideri osservare le ultime due ore, oppure l'ultimo mese o anno. Offrono anche accesso rapido ai più comuni strumenti di troubleshooting, per risolvere eventuali problemi.



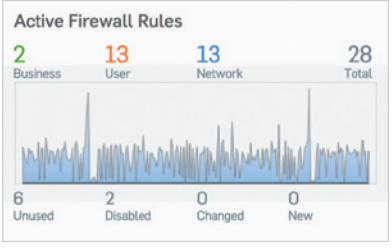
Il visualizzatore di log live è accessibile da qualsiasi schermata con un solo clic. Può essere aperto in una nuova finestra per consentire la visualizzazione del log richiesto, pur continuando a usare la console. Offre due schermate: una vista contenente un formato semplificato a due colonne, organizzato in base ai singoli moduli del firewall, e una vista unificata con informazioni più dettagliate e potenti opzioni di filtro e ordinamento, che raggruppano tutti i log del sistema in un'unica schermata aggiornata in tempo reale.



È possibile che, come la maggior parte degli amministratori di rete, vi siate chiesti se sia possibile esagerare con la quantità di regole firewall, e quali siano le regole veramente necessarie e quelle che non vengono utilizzate. Sophos Firewall elimina il bisogno di porsi queste domande.



Il widget Regole firewall attive mostra un grafico in tempo reale del traffico elaborato dal firewall, in base al tipo di regola: Regole per Applicazioni aziendali, Utenti e Rete. Inoltre, visualizza un conteggio attivo delle regole in base al relativo stato, incluse le regole inutilizzate, dandovi la possibilità di fare un po' di pulizia. Come per le altre sezioni del Control Center, cliccando su una qualsiasi di queste regole verranno fornite informazioni dettagliate, in questo caso la tabella delle regole firewall, raffigurate in base al relativo tipo o stato della regola.

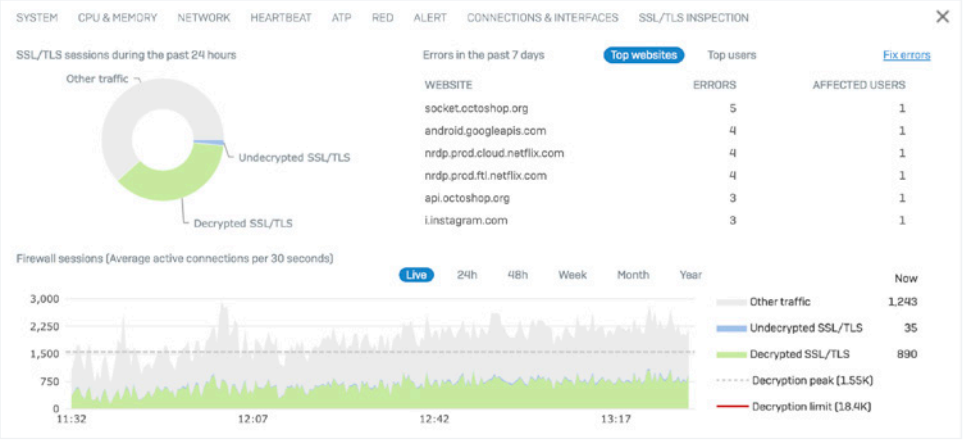


Xstream TLS Inspection

Il traffico cifrato sta per riservarci grandi sorprese. Secondo Google, il volume di traffico cifrato presente all'interno delle reti è aumentato fino a superare l'90%. Questo incremento rappresenta per i cybercriminali un'opportunità per sferrare attacchi che sono nascosti e pertanto difficili da rilevare. Dopo tutto, gli attacchi che non si notano sono impossibili da bloccare. Purtroppo, nella maggior parte dei casi le organizzazioni si trovano con le spalle al muro e non possono fare niente, perché al loro firewall attuale manca il livello di performance necessario per utilizzare l'ispezione SSL/TLS senza rallentare drasticamente i sistemi.

Sophos Firewall, con il suo nuovo motore di ispezione SSL Xstream, ha una capacità nettamente superiore di supportare connessioni simultanee, e offre strumenti flessibili per le policy che sono in grado di prendere decisioni intelligenti sugli elementi da sottoporre a scansione, ricorrendo all'offload ove sia ritenuto opportuno. Utilizzando gli strumenti SSL per le policy, le organizzazioni possono creare policy TLS/SSL di classe Enterprise, da applicare a traffico non decifrabile, certificati, opzioni di implementazione della cifratura e altro ancora. Sophos Firewall supporta TLS 1.3 e tutte le più recenti suite di cifratura per qualsiasi porta e applicazione nel sistema.

Include strumenti aggiuntivi, disponibili direttamente dalla dashboard, per permettere agli amministratori di vedere immediatamente e con estrema precisione la quantità di traffico cifrato e come viene gestito. Sophos Firewall si contraddistingue dalle altre soluzioni per il modo in cui rende subito disponibili queste informazioni, nello specifico per come evidenzia gli errori di convalida dei certificati o i siti web che non supportano i più recenti standard di cifratura.



Sophos Firewall offre informazioni dettagliate sui flussi di traffico cifrato e sui problemi che emergono dalla TLS Inspection, direttamente dal Control Center

Gli amministratori possono anche aprire una finestra contenente informazioni dettagliate, per osservare quali siti specifici stanno generando problemi e per quale motivo, con tanto di informazioni sugli utenti che riscontrano problemi. Da questa finestra, possono quindi intraprendere direttamente l'azione ritenuta più opportuna per escludere l'applicazione o il sito dalla decifratura e prevenire ulteriori problemi in futuro. Nessun'altra soluzione di ispezione SSL offre lo stesso livello di accessibilità a questo tipo di informazioni.

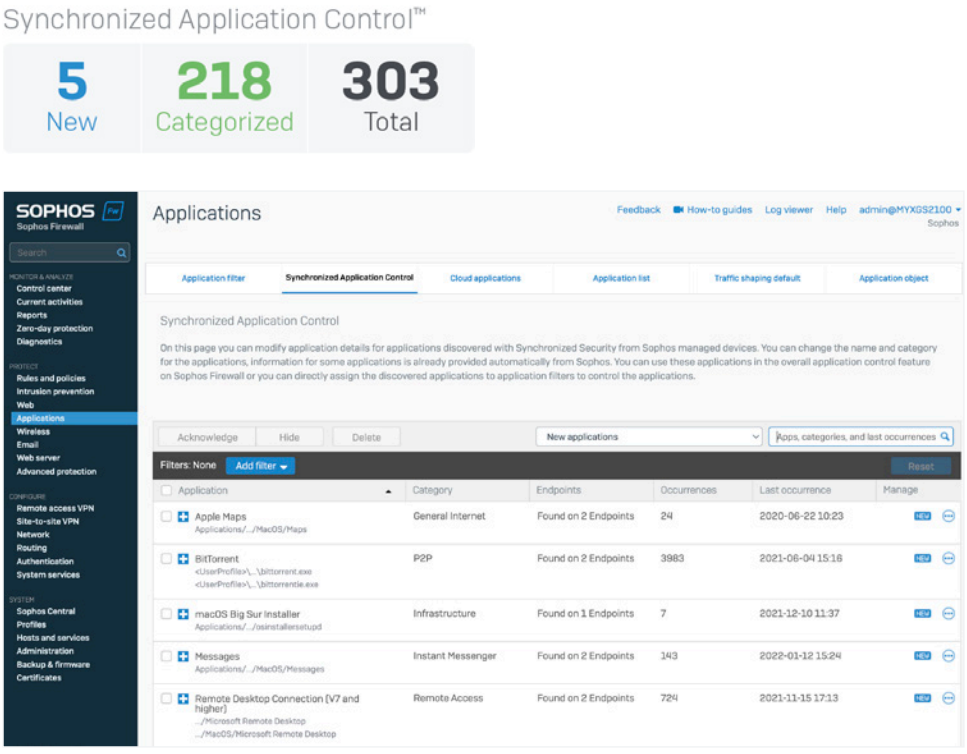
Synchronized Application Control

Il problema principale dei moderni sistemi di controllo applicazioni per qualsiasi firewall next-gen è il fatto che la maggior parte del traffico delle applicazioni rimane non identificato: si tratta di traffico non classificato o contrassegnato come sconosciuto, e di traffico HTTP o HTTPS generico.

Il motivo è semplice: tutti i motori di controllo delle applicazioni si basano su firme e pattern per identificare le applicazioni analizzate. Com'è prevedibile, le applicazioni personalizzate per i mercati verticali, quali le app utilizzate in ambito sanitario e finanziario, non avranno mai una firma. Altre app elusive, quali i client di BitTorrent e VoIP, oltre alle app di messaggistica, modificano continuamente il proprio comportamento e la propria firma per rilevare il rilevamento e il controllo. Attualmente, molte applicazioni utilizzano la cifratura per eludere il rilevamento, mentre altre ricorrono semplicemente a connessioni generiche simili a quelle dei browser web per comunicare verso l'esterno attraverso il firewall, poiché nella maggior parte dei firewall le porte 80 e 443 non sono bloccate.

Il risultato è una completa mancanza di visibilità sulle app presenti nella rete. Ed è impossibile controllare ciò che non si vede. La soluzione a questo problema, oltre ad essere estremamente efficace, è anche molto elegante: Sophos Synchronized Application Control, una funzionalità che sfrutta la nostra esclusiva connessione Synchronized Security con gli endpoint gestiti da Sophos.

Ecco come funziona. Quando Sophos Firewall rileva traffico delle applicazioni che non è in grado di identificare per mezzo delle firme, interpella l'endpoint per scoprire quale sia l'applicazione che lo ha generato.



Le applicazioni sconosciute che vengono rilevate da Synchronized Application Control possono essere classificate automaticamente o manualmente.

L'endpoint può quindi comunicarne il file eseguibile, il percorso e spesso persino la categoria, inoltrando tutte le informazioni al firewall. Nella maggior parte dei casi, il firewall sarà ora in grado di utilizzare queste informazioni per classificare e controllare automaticamente l'applicazione.

Se Sophos Firewall non dovesse essere in grado di determinare automaticamente la categoria dell'applicazione, l'amministratore potrà impostarne una oppure assegnare l'app a una policy esistente.

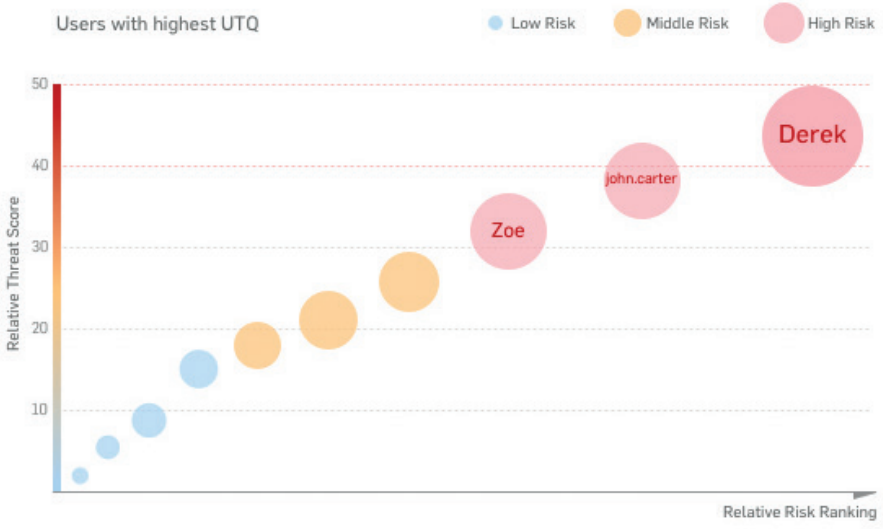
Una volta classificata (in maniera automatica o in seguito all'intervento dell'amministratore di rete), l'applicazione sarà soggetta agli stessi controlli delle policy applicabili a tutte le altre applicazioni della stessa categoria, semplificando i processi di blocco delle app indesiderate e di attribuzione di maggiore priorità alle app utili.

Synchronized Application Control è una rivoluzione nell'ambito della visibilità e del controllo sulla rete, in quanto offre massima trasparenza per tutte le applicazioni utilizzate nella rete, incluse quelle che prima potevano agire indisturbate senza poter essere identificate o controllate.

Utenti maggiormente a rischio

Da vari studi è emerso che gli utenti sono l'anello debole nella catena di sicurezza. La buona notizia è che i pattern di comportamento umano possono essere analizzati e utilizzati per prevedere e prevenire gli attacchi. Inoltre, i pattern di utilizzo possono aiutare a verificare il grado di efficienza con cui vengono adoperate le risorse aziendali, e se occorra ottimizzare le policy utente.

Il quoziente di minaccia dell'utente (User Threat Quotient, UTQ) di Sophos aiuta gli amministratori della sicurezza a individuare gli utenti che rappresentano un rischio e che vengono segnalati per via di comportamenti sospetti sul web o di una cronologia caratterizzata dalla presenza di diverse minacce e infezioni. Il punteggio UTQ di un utente potrebbe essere indizio di azioni non intenzionali (intraprese per via di una mancanza di consapevolezza sulla sicurezza), di un'infezione di malware, oppure di azioni premeditate e illecite.

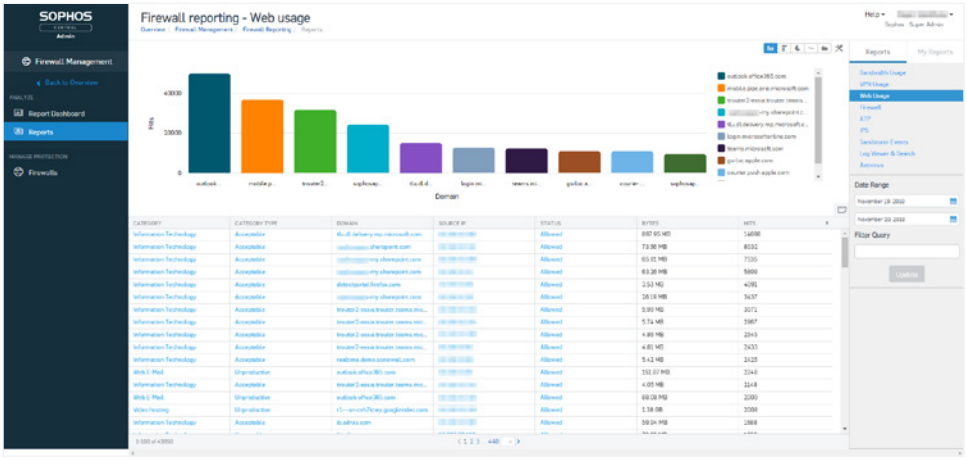


Con Sophos Firewall, gli utenti maggiormente a rischio vengono messi subito in evidenza.

Sapere quali sono gli utenti e le attività che hanno generato un rischio può aiutare gli amministratori di rete addetti alla sicurezza a intraprendere le dovute azioni, organizzando corsi di formazione per gli utenti maggiormente a rischio oppure implementando criteri più severi e adeguati per controllarne il comportamento.

Opzioni flessibili di reportistica

Sophos Firewall è un prodotto unico nel suo genere tra le soluzioni NGFW e UTM, in quanto offre flessibili opzioni di reportistica basate sul cloud o integrate nell'appliance, con un elevato livello di personalizzazione, senza costi aggiuntivi. Sophos Central Firewall Reporting (CFR) consente alle organizzazioni di svolgere analisi più approfondite sull'attività di rete, grazie ai dati raccolti. Con il suo set completo di report integrati e di strumenti per creare centinaia di varianti, CFR offre dati di intelligence pratici e fruibili sul comportamento degli utenti, sull'utilizzo delle applicazioni, sugli eventi di sicurezza e altro ancora. I report interattivi e la dashboard di reportistica a visualizzazione immediata consentono agli amministratori di svolgere un'analisi approfondita dei dati di syslog archiviati nell'account Sophos Central, per una vista granulare presentata in formato visivo per una più semplice comprensione. I dati possono quindi essere analizzati per individuare tendenze che potrebbero identificare eventuali lacune nella sicurezza, o evidenziare l'esigenza di modificare le policy.



Sophos Firewall offre ampie opzioni di reportistica sia a livello di appliance che centralizzate e basate sul cloud.

Sophos Firewall include anche ampie funzionalità di reportistica integrate nell'appliance. Le opzioni disponibili sono un set completo di report, convenientemente organizzati in base alla loro tipologia, con diverse dashboard integrate. Sono presenti centinaia di report con parametri personalizzabili per tutti gli ambiti del firewall, inclusi: attività del traffico, sicurezza, utenti, applicazioni, web, rete, minacce, VPN, e-mail e conformità. È possibile pianificare l'invio a cadenza regolare di report tramite e-mail a destinatari specifici. L'operazione è semplicissima e i report possono essere salvati in formato HTML, PDF o CSV.

Blocco delle minacce sconosciute

Per proteggere i sistemi dalle più recenti minacce della rete, occorre che tra le varie tecnologie regni la massima armonia. Devono comporre una sinfonia perfetta, sotto l'abile conduzione di un esperto direttore d'orchestra: l'amministratore di rete. Sfortunatamente, nella maggior parte dei casi i firewall sono più simili a musicisti-giocolieri di strada che si arrangiano come possono, impostando regole firewall da una parte, policy web da un'altra, effettuando un'ispezione SSL/TLS da un'altra parte ancora e gestendo il controllo delle app in una sezione completamente diversa del prodotto.

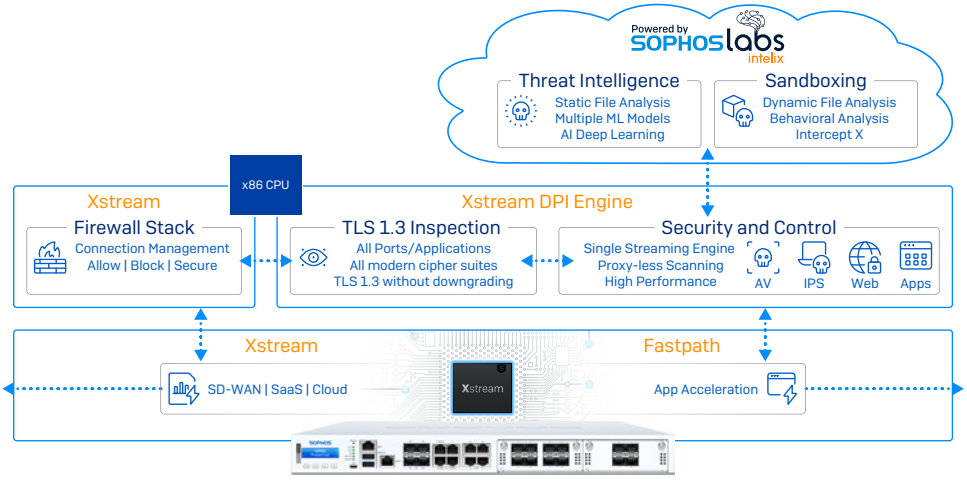
La filosofia di Sophos si basa sul concetto che, oltre alla più avanzata tecnologia disponibile sul mercato, i clienti hanno anche bisogno della massima semplicità di configurazione e gestione quotidiana, perché spesso un sistema di sicurezza configurato male può risultare peggiore di uno del tutto inesistente.

L'impegno volto a garantire la massima semplicità è sempre stato insito nel DNA di Sophos. Tuttavia, è probabilmente degna di maggior nota la propensione di Sophos ad accogliere i cambiamenti con un'attitudine aperta, affrontando impavidamente nuovi modi di agire, nell'interesse di garantire sia una protezione superiore che una migliore esperienza utente.

Con Sophos Firewall, adottiamo un approccio diverso a molte piccole cose, per fare una differenza enorme.

Protezione e performance superiori con Xstream

La performance del firewall non dovrebbe rallentare quando si attiva una sicurezza indispensabile per proteggere la rete dalle minacce. Uno degli elementi chiave dell'architettura di elaborazione dei pacchetti Xstream di Sophos Firewall è un motore di Deep Packet Inspection (DPI) ad altissima velocità. Il motore di DPI offre scansioni di sicurezza indipendenti dai proxy e a fase unica che includono IPS, AV, e controllo di web e app, oltre alla nostra ispezione SSL Xstream.



L'architettura Xstream di Sophos Firewall, con processori di flusso Xstream programmabili, garantisce protezione e performance di altissimo livello.

Quando viene stabilita una nuova connessone, viene elaborata dallo stack di firewall, che provvede a prendere decisioni in termini di autorizzazione, blocco o scansione del traffico alla ricerca di minacce. Se il traffico richiede una scansione di sicurezza, inoltrerà i pacchetti al motore di DPI di streaming indipendente dai proxy e ad alta performance, che analizzerà i pacchetti, anche se sono cifrati. Questo avviene solamente per i pacchetti iniziali. Successivamente, lo stack di firewall si fa da parte ed effettua l'offload dell'elaborazione, affidandola completamente al motore di DPI. Questo comporta un netto miglioramento in termini di latenza e performance.

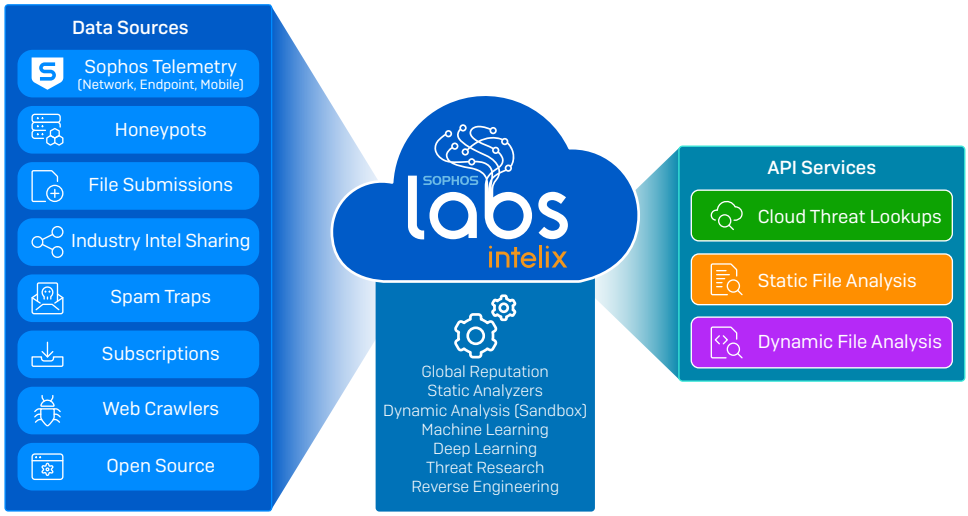
Successivamente, se lo streaming viene ritenuto sicuro e non richiede ulteriori ispezioni, il motore di DPI può affidare completamente il flusso a Sophos Network Flow FastPath, che offre un percorso più rapido per il traffico attendibile. Con questa strategia, la performance ne risulta nettamente migliorata, rendendo disponibili altre risorse che altrimenti rimarrebbero occupate nell'ispezione di traffico che non richiede questi controlli.

Protezione contro le minacce del giorno zero

Dalla presenza di minacce sempre più mirate ed elusive, come il ransomware, sorge l'esigenza critica di utilizzare sistemi predittivi di identificazione e protezione contro le minacce del giorno zero. La soluzione definitiva è composta da due elementi principali:

1. **Analisi statica di machine learning**: analisi e rilevamento predittivi con modelli di machine learning basati su reti neurali multiple e tecnologie di intelligenza artificiale, utilizzati insieme a dati di reputazione globale e scansione profonda dei file, tutto senza dover eseguire il file in tempo reale.
2. **Analisi dinamica in fase di esecuzione nella sandbox**: questa tecnologia fa detonare il malware in tempo reale in un ambiente sandbox nel cloud, fornendo informazioni dettagliate sull'attività dei file e rivelando la vera natura e i potenziali rischi delle minacce sconosciute.

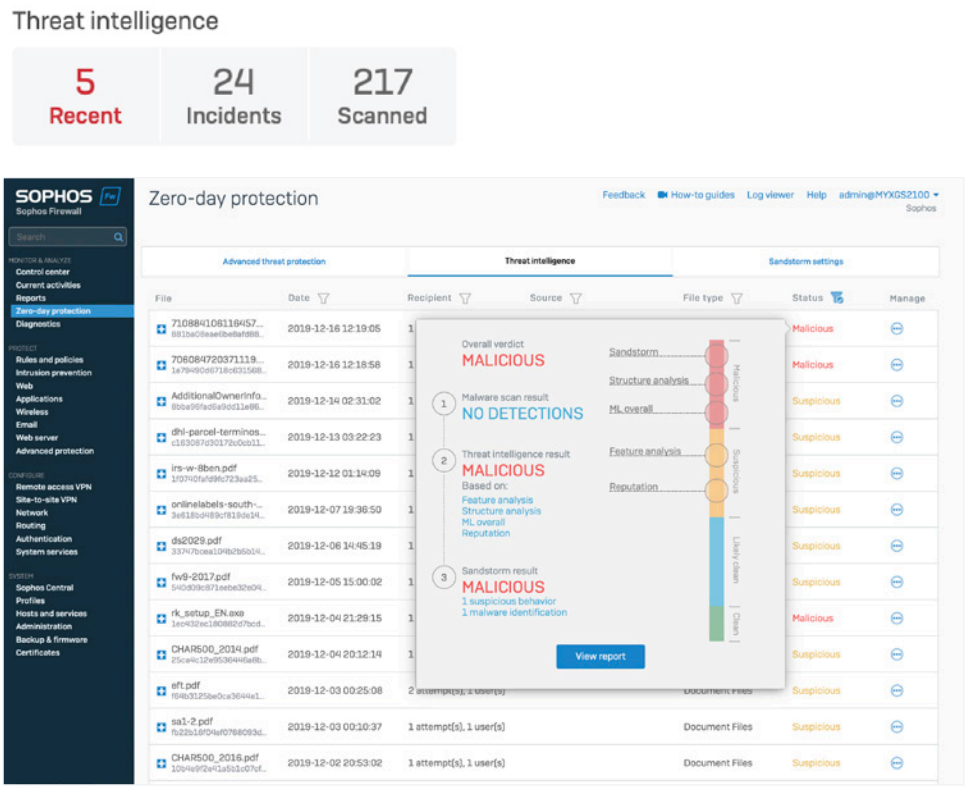
Sophos Firewall offre queste due importanti tecnologie di protezione, abbinandole alla tecnologia SophosLabs Intelix. I SophosLabs, i nostri laboratori di Livello 1 acclamati dagli esperti per il lavoro svolto nell'ambito della ricerca sulle minacce di cybersecurity, hanno sviluppato la piattaforma definitiva di analisi delle minacce e dei dati di intelligence: SophosLabs Intelix. Si basa su tecnologie innovative di machine learning, diversi decenni di esperienza maturata nella ricerca sulle minacce e vari petabyte di dati di intelligence per fornire una protezione impareggiabile contro le minacce più recenti e quelle mai osservate prima.



La protezione zero-day di Sophos Firewall si basa sulle analisi di machine learning di SophosLabs Intelix.

Quando il motore Xstream DPI di Sophos Firewall esegue l'analisi antivirus di un file che viene introdotto nella rete e stabilisce la presenza di codice attivo, trattiene il file temporaneamente e lo invia al servizio SophosLabs Intelix nel cloud per sottoporlo sia ad analisi statiche che dinamiche. Fornisce quindi un riepilogo dei risultati in Sophos Firewall Control Center mediante il widget di Intelligence sulle minacce e questo report click-through (riportato di seguito), rilasciando il file al downloader o al destinatario dell'e-mail se il file è pulito.

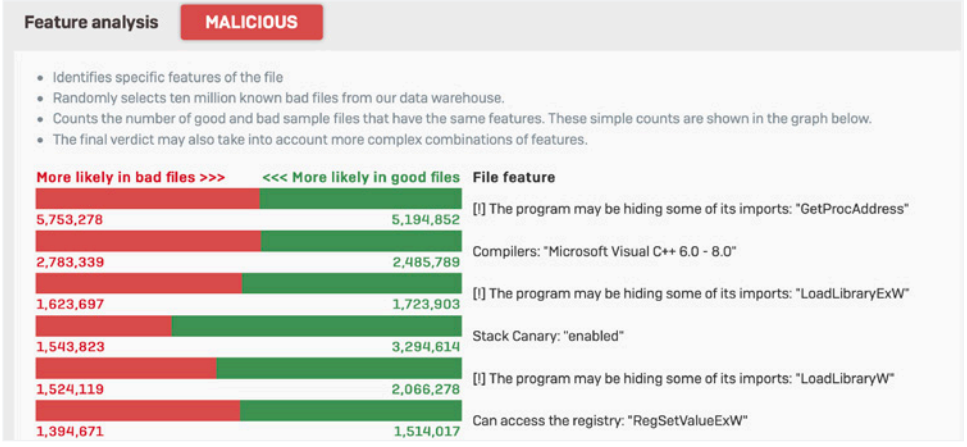
Quest'ultimo passaggio è importante, poiché molte soluzioni antimalware avanzate e basate su firewall spesso rilasciano il file all'utente finale prima che venga completata l'analisi. Il risultato in questo caso può essere una rimozione meno efficace e più costosa, qualora il file si dimostrasse pericoloso.



La protezione zero-day di Sophos Firewall identifica le minacce mai osservate in precedenza, prima ancora che riescano a infiltrarsi nella rete.

Analisi statica di machine learning

L'analisi statica dei file sfrutta modelli di machine learning multipli per analizzare i vari elementi dei file in base alle relative caratteristiche, funzionalità, strutture genetiche e reputazione. I file vengono messi a confronto con i milioni di file noti per essere innocui o pericolosi, inclusi nel database dei SophosLabs. Tutto questo permette di esprimere in pochissimi secondi un verdetto su qualsiasi file nuovo e mai osservato prima. È un sistema estremamente rapido ed efficace per identificare nuove minacce e nuove varianti di minacce esistenti, in particolar modo nel caso di minacce che non sono facilmente analizzabili in una sandbox, come i documenti protetti da password che contengono malware.



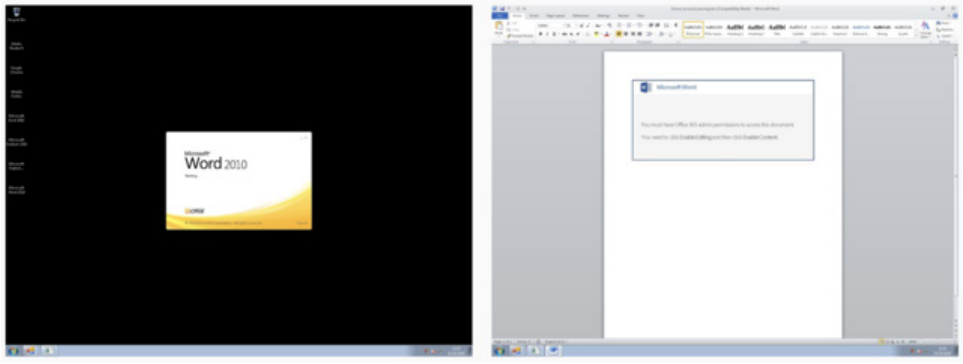
Per identificare le minacce zero-day, i file sospetti vengono analizzati con modelli di machine learning multipli.

Analisi dinamica nella sandbox in fase di esecuzione

All'inizio, le tecnologie di sandboxing avevano costi che potevano essere sostenuti solamente da aziende di grandi dimensioni. Ora invece, grazie a soluzioni di sandboxing basate sul cloud come Sophos Sandstorm, questa opzione è una possibilità concreta anche per le imprese più piccole. Per la prima volta, le piccole e medie imprese possono accedere al sandboxing con tecnologia deep learning, per usufruire di capacità che vanno ben oltre i normali tipi di soluzioni di sandboxing on-premise appositamente dedicate e utilizzate appena pochi anni fa dalle organizzazioni a un costo di vari milioni di dollari.

Siccome è basata sul cloud, non richiede alcun software o hardware aggiuntivo, e non comporta alcun impatto sulla performance del firewall. Qualsiasi file in cui il motore DPI di Xstream identifica un codice attivo (ad esempio un allegato e-mail o un download dal web) viene automaticamente caricato e fatto detonare all'interno della sandbox nel cloud di SophosLabs Intelix. Parallelamente, ne viene eseguita un'analisi statica (riportata sopra) per determinarne il comportamento in fase di esecuzione. Tutto questo avviene prima che il file possa essere autorizzato a essere introdotto nella rete.

Per identificare le minacce, i SophosLabs hanno integrato in Sophos Sandstorm le più recenti tecnologie di protezione del nostro prodotto endpoint next-gen leader di settore Intercept X, che includono deep learning, rilevamento degli exploit e CryptoGuard (rilevamento in tempo reale del ransomware attivo che effettua tentativi di cifratura dei file). Inoltre, vengono monitorati anche tutti i file, la memoria, il registro e l'attività di rete, per individuare caratteristiche che denotano intenzioni malevole e per emettere un verdetto attendibile sul file. Nessun altro firewall offre questo tipo di analisi in fase di esecuzione, svolta dalla migliore protezione contro le minacce attualmente disponibile sul mercato: Intercept X. Inoltre, nessun altro firewall offre il livello di approfondimento e reportistica di Sophos Firewall, che include una serie di screenshot che mostrano le informazioni emerse durante l'esecuzione del file.

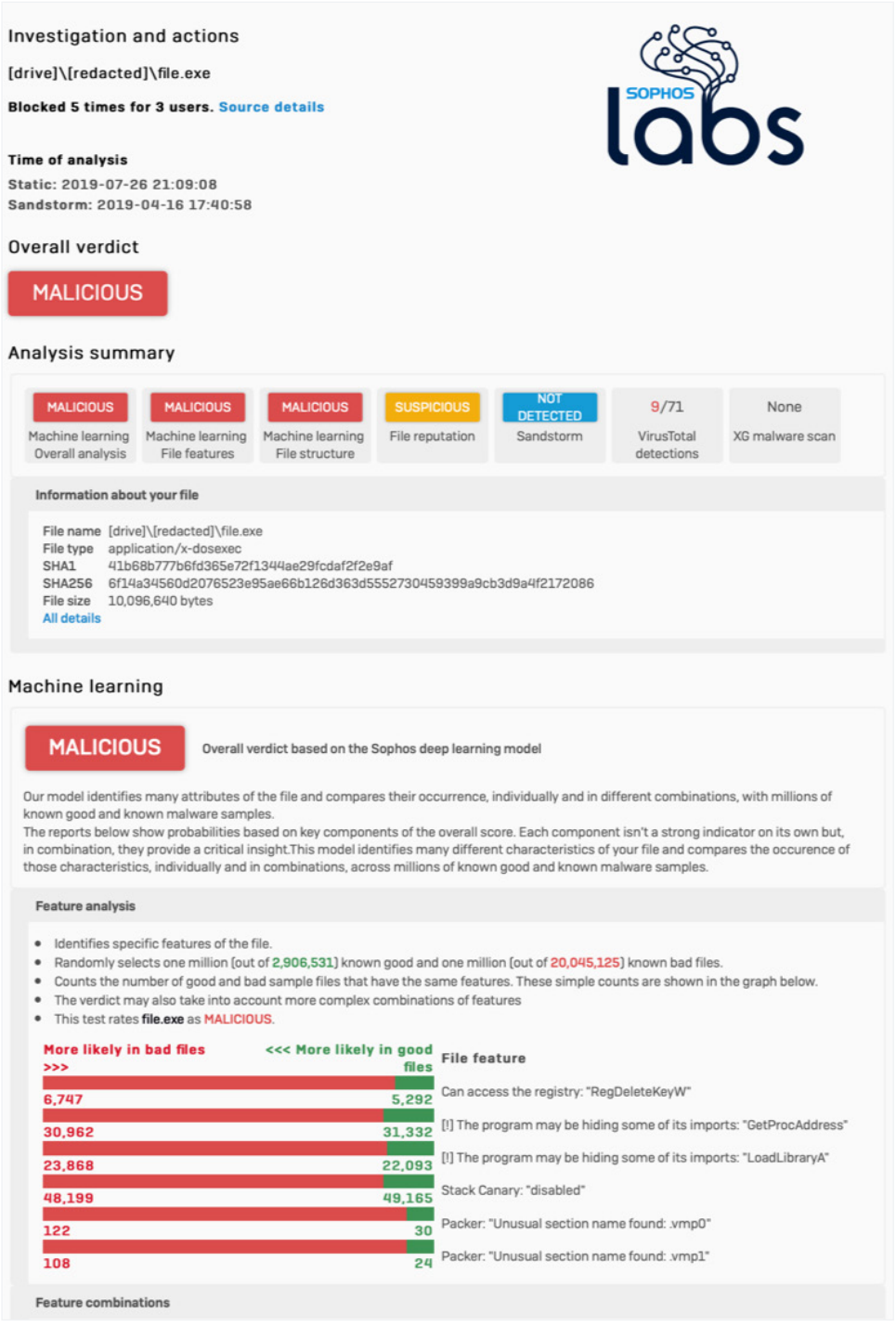


L'analisi nella sandbox in fase di esecuzione fa detonare i file in un ambiente sicuro per determinarne il comportamento; in più, fornisce screenshot che puoi valutare.

Il sandboxing è particolarmente efficace nel rilevare minacce che possono nascondersi in file normalmente innocui che potrebbero non avere caratteristiche dannose evidenti. Ad esempio, file di Office contenenti macro, oppure file eseguibili o aggiornamenti delle applicazioni legittimi che sono stati manomessi.

Report di protezione contro le minacce

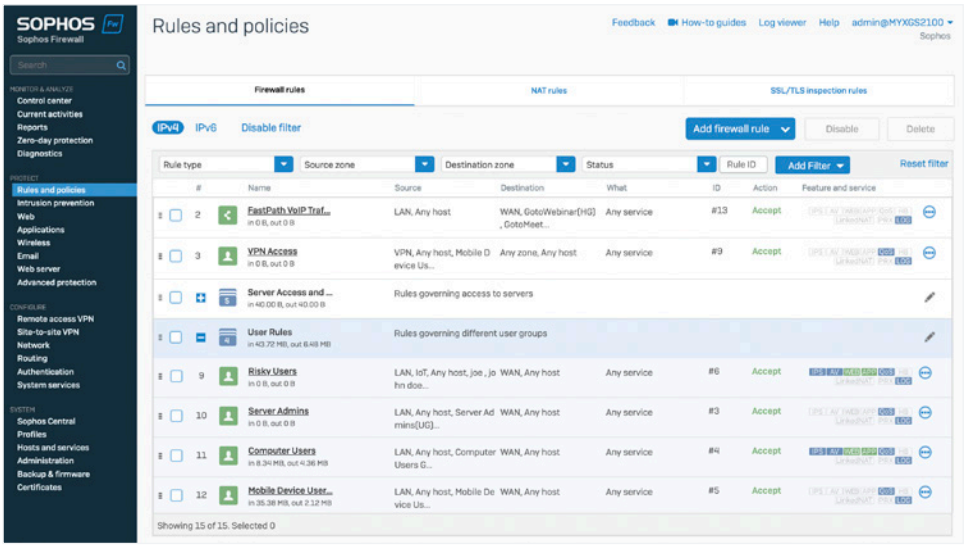
Per tutti i file analizzati da Sophos Firewall viene compilato un report che fornisce i dettagli completi dei risultati delle varie analisi, nonché i verdetti. Il report è composto da sei elementi diversi, che includono le diverse analisi di machine learning, la reputazione del file, il sandboxing e persino dati di terze parti ottenuti da VirusTotal.



Gestione unificata delle regole

Gestire un firewall può essere un'impresa ardua, con regole, policy e sistemi di sicurezza multipli suddivisi tra aree operative diverse, spesso con la necessità di impostare varie regole differenti per garantire un livello di protezione adeguato.

Con Sophos Firewall, abbiamo colto l'opportunità per rivoluzionare il modo in cui vengono organizzate le regole firewall e come viene gestita l'infrastruttura di sicurezza. Invece di costringere gli utenti a setacciare la console di gestione alla ricerca dei criteri desiderati, abbiamo riunito l'intero sistema di gestione e implementazione di regole e criteri in una singola schermata unificata. È ora possibile visualizzare, filtrare, cercare, modificare, aggiungere, cambiare e organizzare tutte le regole del firewall da un'unica vista.



Sophos Firewall visualizza in un'unica schermata tutte le regole per policy di accesso, NAT e TLS Inspection, semplificando notevolmente la gestione.

Le regole organizzate in base a utenti, applicazioni aziendali, NAT, ispezione SSL/TLS e rete semplificano la visualizzazione, mostrando solamente le policy richieste in un'unica schermata di gestione estremamente pratica.

Le icone indicatrici offrono importanti informazioni sulle policy, ad esempio il tipo, lo stato, l'implementazione e molto di più.

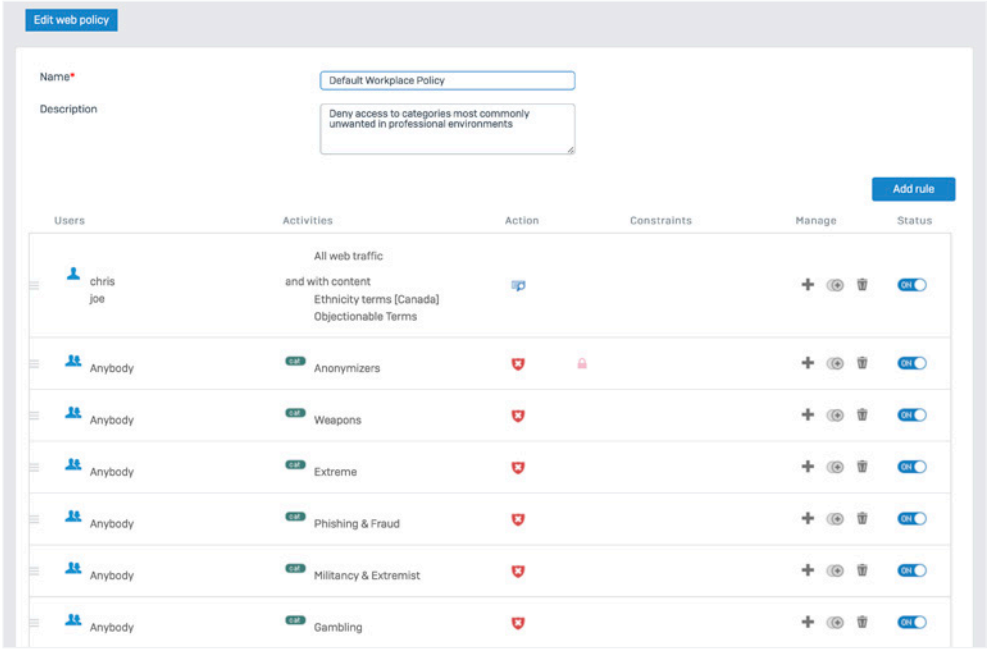
Gestione dell'infrastruttura di sicurezza in un'unica vista

Sia che si utilizzi l'account Sophos Central dal cloud oppure l'interfaccia utente di Sophos Firewall, Sophos semplifica notevolmente la configurazione e la gestione di quello che occorre per proteggere i sistemi moderni, e aiuta a fare il tutto da un'unica schermata.

Configura il tuo profilo di sicurezza completo con policy predefinite o personalizzate.

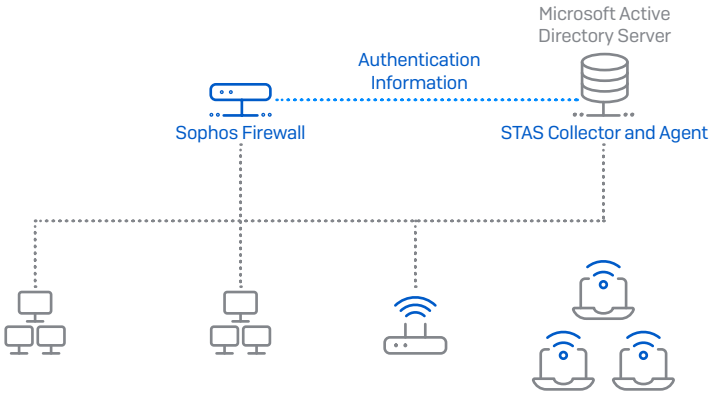
Puoi configurare e aggiungere opzioni di sicurezza e controllo per antivirus, TLS/SSL Inspection, sandboxing, IPS, shaping del traffico e controllo di web e app, nonché Security Heartbeat, NAT, instradamento e attribuzione delle priorità, tutto da un unico pannello, e tutto in base alle singole regole o ai singoli utenti e gruppi.

Per conoscere in maniera più approfondita come agiscono le policy aggiunte o per cambiare qualche impostazione, basta effettuare le modifiche direttamente dal pannello, senza bisogno di uscire dalla regola firewall e dover navigare verso un'altra sezione del prodotto.



Visualizzazione immediata dei dettagli delle policy, con possibilità di effettuare modifiche senza uscire dalla schermata delle regole firewall.

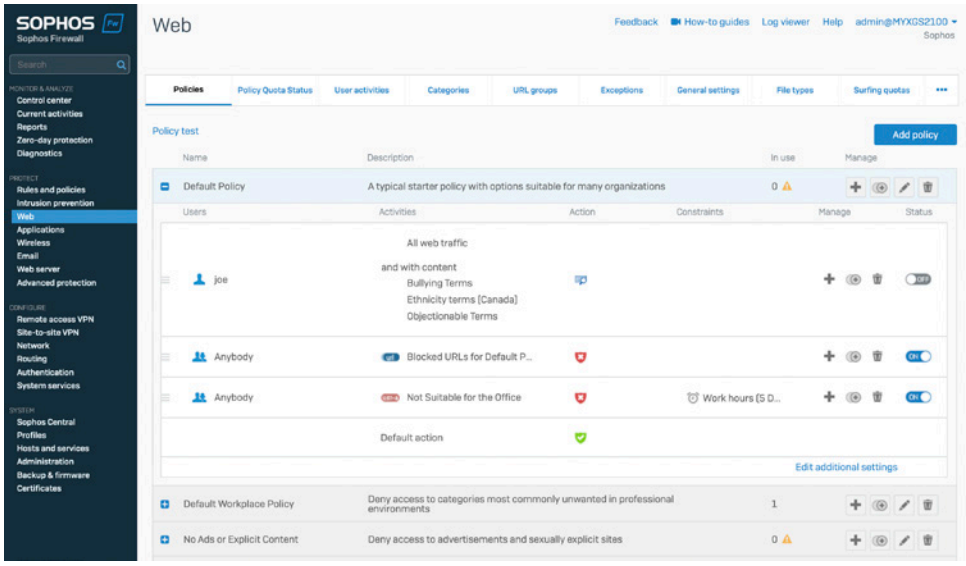
Le opzioni di autenticazione flessibili consentono di identificare facilmente i vari utenti e includono servizi di directory quali Active Directory, eDirectory, LDAP, nonché anche NTLM, Kerberos, RADIUS, TACACS+, RSA, agenti client e un captive portal. Inoltre, la Sophos Transparent Authentication Suite (STAS) offre opzioni di integrazione con servizi di directory quali Microsoft Active Directory, per fornire un sistema di autenticazione single sign-on facile, affidabile e trasparente.



No client required on devices for SSO

Un Secure Web Gateway di classe Enterprise

La protezione e il controllo del web sono elementi indispensabili per qualsiasi firewall; purtroppo però sembrano essere un elemento di importanza secondaria per la maggior parte dei sistemi firewall. L'esperienza che abbiamo maturato nel creare soluzioni di protezione web di classe Enterprise ci ha dotato delle competenze e del know-how necessari per implementare il tipo di controllo delle policy web normalmente disponibile solamente a un costo 10 volte superiore nelle soluzioni di protezione dei gateway web (SWG) per le aziende di grandi dimensioni. Abbiamo implementato un modello di policy basato sull'ereditarietà e con un elenco che viene applicato dall'alto verso il basso, per rendere semplici e intuitive anche le impostazioni di policy estremamente sofisticate. Sono inclusi modelli di policy predefinite, preimpostate e pronte per l'uso per i più comuni scenari di installazione, ad es: i tipici ambienti di lavoro, la conformità alle normative CIPA sul settore dell'istruzione, e molto altro ancora. Tutto ciò significa poter essere subito operativi, nel pieno rispetto della conformità, con opzioni di ottimizzazione e personalizzazione semplici e sempre a vostra disposizione.



Potenti policy web di classe Enterprise, per garantire controlli granulari.

Siamo infatti consci che le policy web sono uno degli elementi del firewall maggiormente soggetti a modifiche nelle attività di ogni giorno, ed è per questo motivo che abbiamo investito molto nel renderle più semplici da gestire, ottimizzando le policy in base alle esigenze di utenti e azienda. È possibile personalizzare con estrema facilità: utenti e gruppi, attività (inclusi URL, categorie, filtri dei contenuti e tipi di file), azioni (blocco, autorizzazione e avviso), e aggiunta o modifica di limitazioni in termini di ora del giorno e giorno della settimana.

Funzionalità per il settore education

Sophos Firewall offre diverse funzionalità molto utili per gli ambienti del settore education, nel quale policy web e rispetto della conformità sono requisiti critici. Le funzionalità che riguardano il settore education includono:

- Policy web preimposate per la conformità al CIPA
- Filtro dei contenuti e reportistica sulle parole chiave
- Impostazioni per SafeSearch e limitazioni per YouTube in base alle policy utente o di gruppo
- Override delle pagine di blocco, che sono gestibili dai docenti
- Opzioni complete di reportistica integrata, per identificare tempestivamente eventuali problemi

Le policy web includono ora l'opzione di registrare nel log, monitorare e persino implementare policy su contenuti dinamici in base a elenchi di parole chiave. Questa funzionalità è particolarmente importante nel settore dell'istruzione, in quanto garantisce la sicurezza on-line dei minori e offre un'analisi delle parole chiave utilizzate dagli studenti, segnalando quelle che riguardano l'autolesionismo, il bullismo, l'estremismo e contenuti inadeguati di altro genere. Gli elenchi di parole chiave possono essere caricati nel firewall e applicati a qualsiasi policy di filtro web come criteri aggiuntivi, con azioni di registrazione nel log e monitoraggio, oppure di blocco dei risultati di ricerca o dei siti web che contengono le parole chiave specificate.

Vengono offerte opzioni di reportistica complete per identificare qualsiasi corrispondenza con le parole chiave e rilevare gli utenti che cercano o utilizzano contenuti di interesse particolare, inerenti alle parole chiave. Questa strategia consente di intervenire in maniera proattiva in presenza di un utente a rischio, per evitare che si generino problemi più gravi.

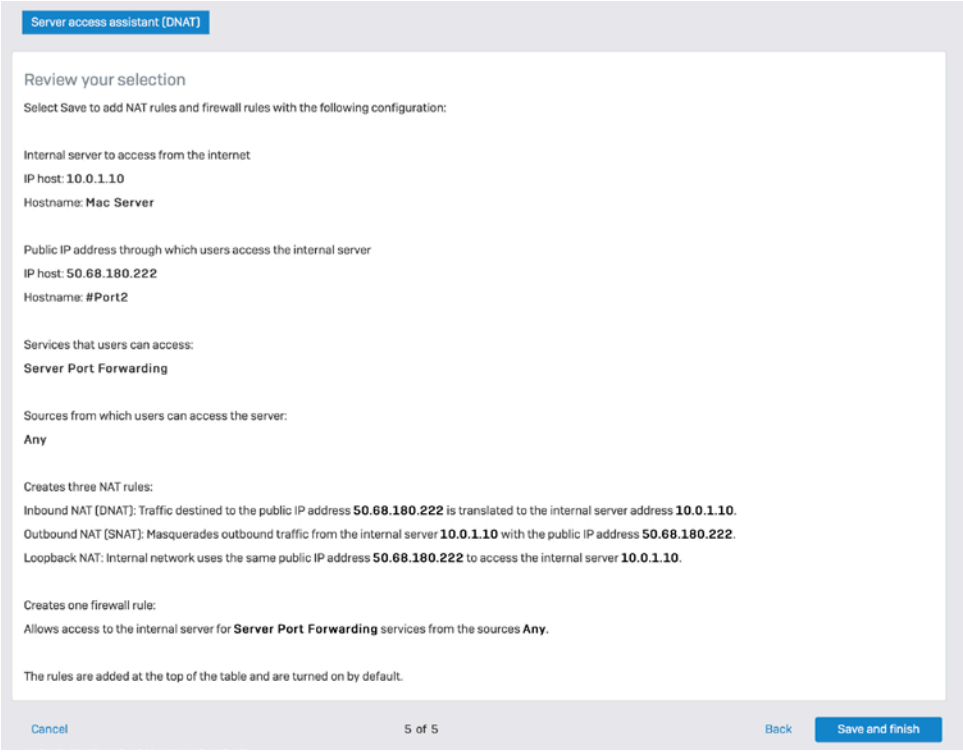
Sophos Firewall è pronto per essere subito utilizzato per la conformità alla policy CIPA, garantendone l'ottemperanza. Inoltre, offre controlli flessibili e affidabili su SafeSearch e sulle limitazioni per YouTube, in base alle policy utente/gruppi. Inoltre, gli insegnanti possono avere l'opzione di impostare e gestire i propri override delle policy, per consentire agli alunni di accedere, come parte del programma, a siti web che altrimenti sarebbero bloccati.

È la semplificazione di un approccio potente ed efficace ai criteri web.

Configurazione semplificata di NAT

Chiunque abbia mai provato a configurare regole NAT (Network Address Translation) sa quanto possa essere difficile questa operazione. Ma non deve per forza essere così. Sophos Firewall include opzioni NAT complete, per implementare potenti e flessibili configurazioni NAT, incluse Source NAT (SNAT) e Destination NAT (DNAT) in un'unica regola, con criteri di selezione estremamente dettagliati. Per semplificare ulteriormente il DNAT, è disponibile una procedura guidata di semplice utilizzo, che descrive l'intero processo di creazione di una configurazione NAT completa in pochissimi clic.

Gli amministratori possono anche usufruire della pratica opzione NAT associata, quando creano una regola firewall. La NAT associata creerà automaticamente una regola di configurazione NAT corrispondente, riducendo ulteriormente il tempo da trascorrere a creare e configurare le regole NAT.

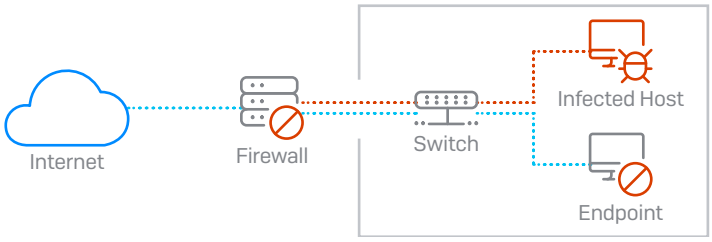


La procedura guidata di creazione delle regole NAT è semplice, ma intuitiva e permette di configurare controlli degli accessi estremamente complicati in pochissimi passaggi.

Risposta automatica agli incidenti

Una delle funzionalità firewall più richieste dagli amministratori di rete è la capacità di rispondere in maniera automatica agli incidenti di sicurezza della rete.

Sophos Firewall è l'unica soluzione di sicurezza per la rete che identifica in maniera completa l'origine di un'infezione all'interno della rete, e che risponde limitando automaticamente l'accesso del dispositivo alle altre risorse della rete dall'endpoint infettato. Tutto questo viene reso possibile dal nostro esclusivo Security Heartbeat, che abilita la condivisione di dati di telemetria e stato di integrità tra gli endpoint gestiti con Sophos e il firewall.



Sophos Firewall e Security Heartbeat sono in grado di isolare automaticamente gli host infetti presenti nella rete.

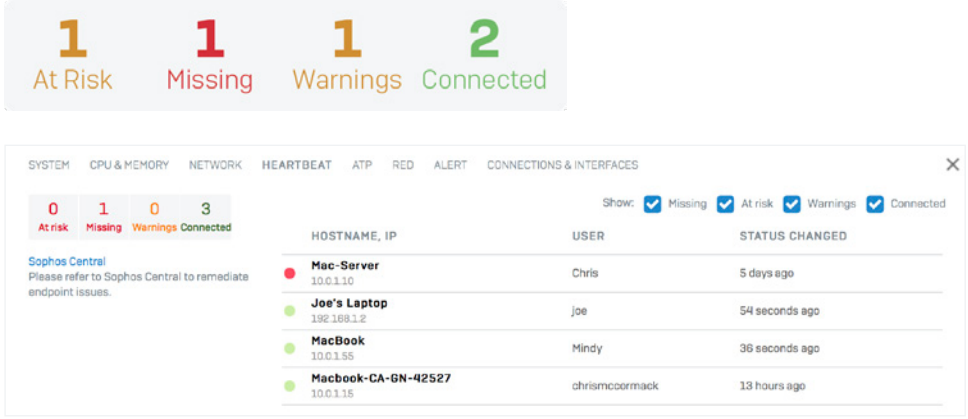
Sophos Firewall offre l'opzione esclusiva di integrare nelle regole firewall lo stato di integrità degli host connessi, abilitando la limitazione automatica dell'accesso a risorse di rete di natura sensibile da parte di tutti i sistemi compromessi, fino a quando non ne venga ripristinato lo stato sicuro.

Sophos Firewall è in grado non solo di isolare gli endpoint, impedendone l'accesso ad altre parti della rete a livello di firewall, ma anche di prelevare informazioni dagli endpoint con un ottimo stato di integrità e che si trovano all'interno della rete, al fine di isolare ulteriormente l'host compromesso a livello di endpoint.

Questo sistema è denominato Protezione contro i movimenti laterali, e agisce isolando e impedendo alle minacce o agli hacker di spostarsi lateralmente all'interno della rete per infettare altri sistemi, anche se si trovano nello stesso segmento di rete o dominio di trasmissione, dove solitamente un firewall non è in grado di intervenire. È una soluzione semplice ed efficace al problema degli active adversary presenti nella rete. Ed è un sistema possibile solamente se endpoint e firewall interagiscono reciprocamente all'interno di una difesa coordinata e sincronizzata.

Security Heartbeat

Sophos Security Heartbeat abilita la condivisione in tempo reale dei dati di intelligence utilizzando una connessione sicura tra endpoint gestiti da Sophos ed Sophos Firewall. La semplice sincronizzazione di prodotti di sicurezza che in passato agivano in maniera indipendente genera ora una protezione più efficace contro malware avanzato e attacchi mirati.



Lo stato di Security Heartbeat™ della rete è visibile nel Control Center.

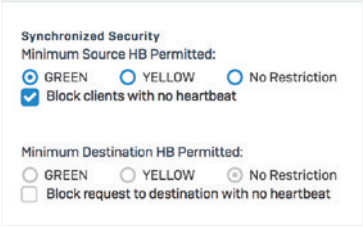
Security Heartbeat agisce identificando all'istante la presenza di minacce avanzate, ma non solo: può anche essere utilizzato per comunicare informazioni importanti sulla natura della minaccia, del sistema host e dell'utente. E per ultimo ma non per questo meno importante, Security Heartbeat può anche essere adoperato per isolare automaticamente i sistemi compromessi, oppure per limitarne l'accesso fino a quando non ne sia stata effettuata la disinfezione. È una tecnologia straordinaria che ha rivoluzionato il modo in cui le soluzioni di IT security identificano e rispondono alle minacce avanzate.

Security Heartbeat per gli endpoint gestiti, utilizzato insieme al firewall, può presentare tre stati:

Heartbeat verde: uno stato verde di Heartbeat indica che il dispositivo endpoint è in ottime condizioni, e che è autorizzato ad accedere a tutte le risorse di rete a cui ha diritto.

Heartbeat giallo: uno stato giallo di Heartbeat indica che è possibile che il dispositivo contenga applicazioni potenzialmente indesiderate (PUA) o problemi di altro genere, oppure che non rispetti la conformità. È possibile specificare le risorse a cui può accedere un sistema con stato di heartbeat giallo fino al momento della risoluzione del problema.

Heartbeat rosso: uno stato rosso di Heartbeat indica un dispositivo che è a rischio di essere infettato da una minaccia avanzata e che potrebbe effettuare tentativi di call home verso una botnet o un server di comando e controllo. Utilizzando le impostazioni delle policy di Security Heartbeat nel firewall, è possibile isolare i sistemi aventi stato di heartbeat rosso fino a quando non sia possibile risolverne i problemi, per limitare il rischio di perdita dei dati o di diffusione dell'infezione.



È possibile includere i requisiti di Security Heartbeat in qualsiasi regola firewall.

Solamente Sophos può offrire una soluzione come Security Heartbeat, perché solamente Sophos è leader di settore sia nell'ambito delle soluzioni di protezione degli endpoint che sicurezza della rete. Mentre gli altri vendor cominciano solo adesso a capire che questo è il futuro dell'IT security e fanno di tutto per escogitare qualcosa di simile, devono tutti superare un ostacolo praticamente insormontabile: non dispongono di soluzioni endpoint leader di mercato da integrare con una soluzione firewall di prima categoria.

Un mondo Zero Trust

La parola "trust" (fiducia) è diventata una parola pericolosa nel mondo dell'informatica, specialmente quando tale fiducia è implicita. La creazione di un perimetro aziendale esteso e isolato, unita alla tendenza a fidarsi di qualsiasi elemento all'interno di tale perimetro, si è dimostrata un modello fallace.

Zero Trust è un approccio olistico alla sicurezza che risolve i problemi derivati da queste novità e che aiuta le organizzazioni a rispondere alle minacce. È allo stesso tempo sia un modello che una filosofia che indica come concepire e come implementare la sicurezza.

Niente e nessuno dovrebbe meritare automaticamente la nostra fiducia, sia che si trovi all'interno o all'esterno della rete aziendale. Tuttavia, prima o poi occorre fidarsi di qualcosa. Con Zero Trust, questa fiducia è provvisoria e viene concessa solo dopo aver consultato varie fonti di dati e viene valutata di continuo.

Zero Trust consente di controllare sistemi interi, da un ufficio, fino alle piattaforme cloud più comunemente utilizzate. La mancanza di controllo all'esterno del perimetro aziendale e le difficoltà presentate dagli utenti remoti appartengono ormai al passato.

Come possiamo adottare il modello Zero Trust e usufruire di tutti i vantaggi che offre? Sebbene nessuno possa garantire Zero Trust come soluzione unica, Sophos offre una vasta gamma di tecnologie e controlli di sicurezza che velocizzano e semplificano il processo di implementazione di Zero Trust.

Sophos Central: la piattaforma di cybersecurity più attendibile a livello internazionale, che unisce in una sola console di gestione basata sul cloud un ampio spettro di tecnologie diverse che si completano a vicenda, per aiutare gli amministratori a orchestrare e monitorare la rete Zero Trust.

Synchronized Security: una cybersecurity che condivide continuamente informazioni tra endpoint, ZTNA, firewall e altri sistemi, garantendo profondità di analisi e massima visibilità per tutti i componenti del sistema di sicurezza.

Sophos ZTNA: offre una vera e propria soluzione Zero-Trust Network Access che connette in maniera sicura gli utenti alle applicazioni di rete e ai dati.

Sophos Firewall: crea segmenti o microperimetri attorno a utenti, app, reti e altro.

Server Protection e Intercept X: assegnano uno stato di integrità a ciascun dispositivo, affinché nel caso in cui un dispositivo dovesse essere compromesso, gli altri dispositivi possano isolarlo automaticamente e impedire che comunichi con altri dispositivi.

Servizio Managed Threat Response (MTR): monitora tutte le attività degli utenti all'interno della rete, identificando le credenziali utente che potrebbero essere state compromesse.

Ottimizzazione della rete SD-WAN

Sono pochi i termini relativi ai servizi di rete che sono riusciti a far parlare di sé tanto quanto la SD-WAN (ovvero i servizi di rete "Software Defined" in una "Wide Area Network"). Tutto questo discutere è stato accompagnato da una dose di informazioni molto utili, ma alcune anche poco chiare. Di conseguenza, il termine SD-WAN ha cominciato ad assumere molti significati diversi, che variano a seconda delle persone. Alcuni stanno ancora cercando di capire cosa voglia dire esattamente.

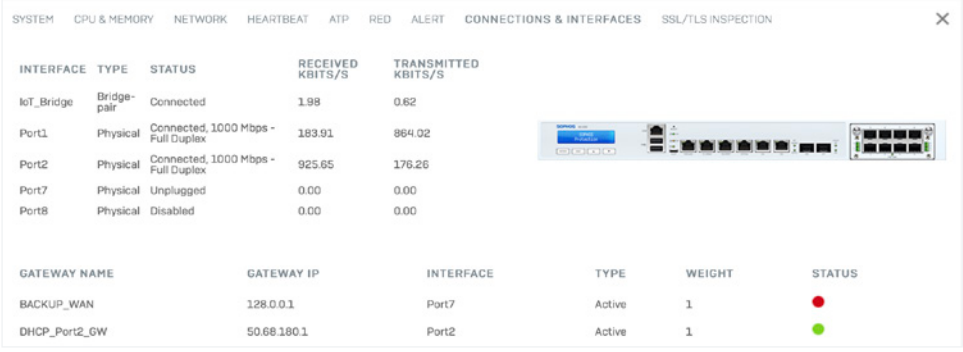
Fondamentalmente, le SD-WAN si prefiggono di raggiungere uno o più dei seguenti obiettivi di rete:

- **Riduzione dei costi di connettività**: le tradizionali connessioni MPLS (Multi-Protocol Label Switching) implicano costi molto elevati, pertanto le organizzazioni stanno passando a opzioni WAN più convenienti, basate su broadband, come ad es. quelle via cavo, DSL e 3G/4G/LTE
- **Continuità del business**: le organizzazioni hanno bisogno di soluzioni in grado di offrire ridondanza, routing, failover e di preservare la sessione nell'eventualità di un'interruzione del servizio nella WAN
- **Qualità delle applicazioni critiche**: le organizzazioni hanno bisogno di opzioni di visibilità in tempo reale sul traffico delle applicazioni e sulla performance, per mantenere la qualità della sessione per le app aziendali di tipo mission-critical
- **Orchestrazione semplificata della VPN per le filiali**: orchestrare la VPN tra le vari sedi è spesso un processo complicato che comporta un enorme dispendio di tempo, ed è per questo motivo che è essenziale poter contare su strumenti in grado di semplificare e automatizzare la distribuzione e la configurazione

Sophos Firewall con SD-WAN Xstream permette di concretizzare anche gli obiettivi più ambiziosi per la SD-WAN in maniera semplice ed economica, grazie alla sua gamma completa di opzioni di orchestrazione, gestione e ottimizzazione della performance e dell'attendibilità per la SD-WAN.

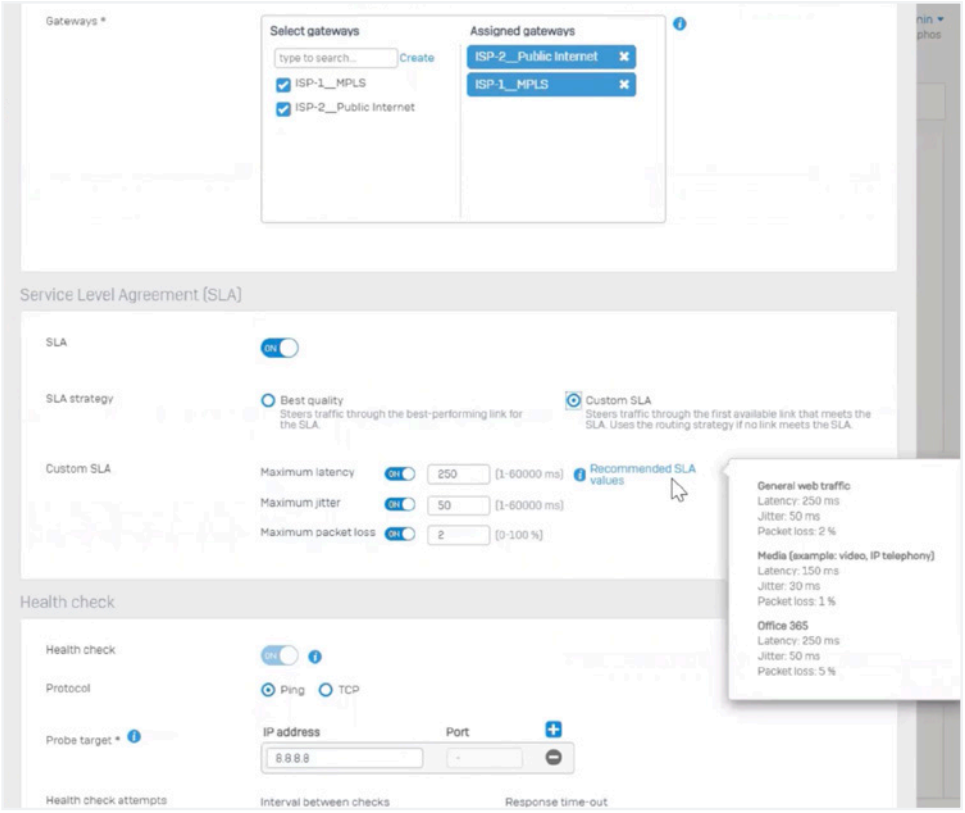
SD-WAN Xstream

La gestione del traffico delle applicazioni instradato su collegamenti WAN multipli è uno degli elementi fondamentali della SD-WAN, e Sophos Firewall con SD-WAN Xstream offre una soluzione di gestione dei collegamenti potente e flessibile, sia su connessioni MPLS multiple che su DSL, connessioni cablate o cellulari.



Lo stato dei collegamenti WAN viene visualizzato nella parte inferiore di questo widget di stato dell'interfaccia, disponibile dalla dashboard.

I profili SD-WAN definiscono una strategia di routing su gateway per collegamenti WAN multipli, garantendo il reinstradamento efficiente e invisibile delle connessioni delle applicazioni, in base alla performance dei collegamenti WAN. La transizione dei collegamenti avviene in maniera istantanea, senza alcun impatto sulle sessioni delle applicazioni e senza alcuna interruzione del servizio. Questo garantisce una perfetta continuità, con alti livelli di performance e la migliore esperienza per l'utente finale, anche negli ambienti ISP più irregolari e instabili.



Configurare profili SD-WAN in base alla performance è un processo semplice e intuitivo.

Le strategie di routing per i profili SD-WAN possono basarsi su criteri di collegamento legati alla disponibilità o alla performance. I criteri di monitoraggio della performance includono jitter, latenza e perdita dei pacchetti, e possono utilizzare target di probe multipli per probe PING e TCP.

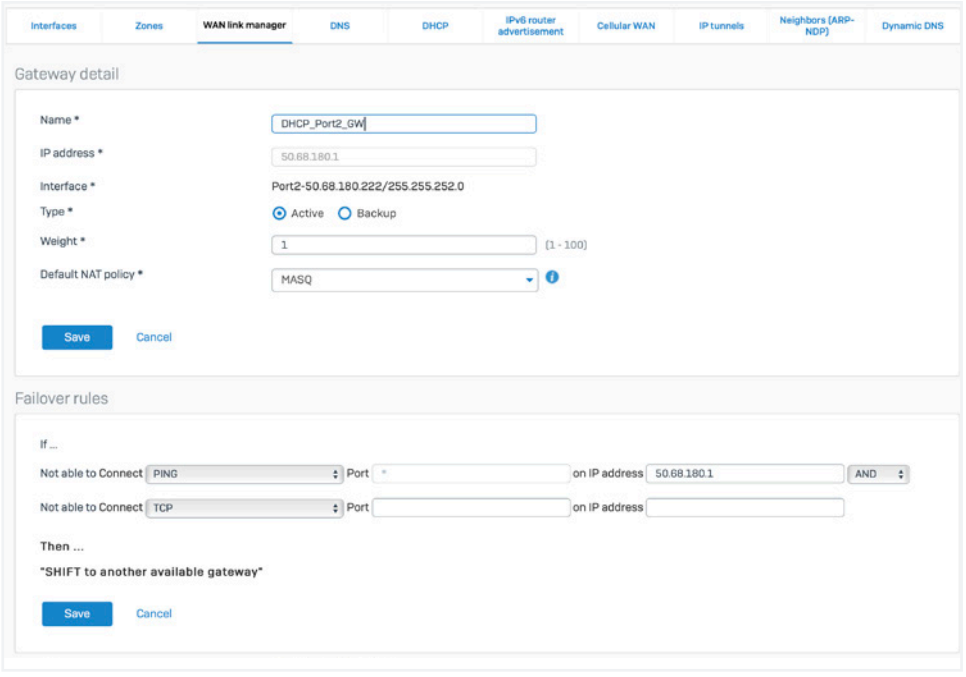
I profili SD-WAN possono selezionare automaticamente il collegamento migliore in base alla performance o secondo policy SLA personalizzate, che definiscono valori specifici per i limiti massimi accettabili di jitter, latenza o perdita dei pacchetti. Se questi valori vengono superati, si procede al reinstradamento su un collegamento caratterizzato da migliori livelli di performance, tutto senza alcun impatto sulle connessioni attive.

Monitorare la performance della rete SD-WAN è facile, grazie ai grafici in tempo reale o cronologici che mostrano latenza, jitter e perdita dei pacchetti. Le opzioni selezionabili per le tempistiche includono: in tempo reale, ultime 24 o 48 ore e ultima settimana o mese. Sono anche incluse funzionalità di log avanzate per la performance della SD-WAN e il routing.

Monitoraggio della performance dei vari collegamenti WAN in tempo reale.

Accelerazione FastPath di Xstream per il traffico VPN SD-WAN

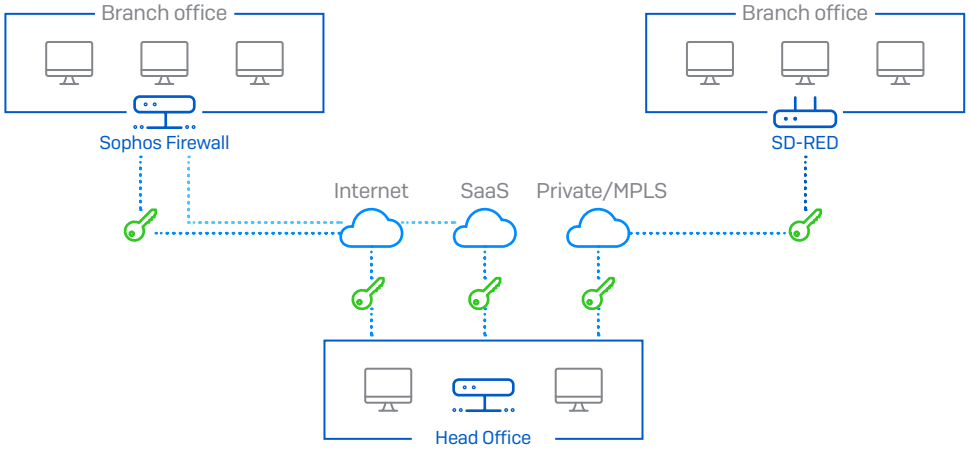
Sophos Firewall utilizza i processori di flusso Xstream integrati nelle appliance XGS per l'accelerazione hardware del traffico dei tunnel VPN IPsec. Il risultato è una performance nettamente superiore, grazie al trasferimento sul processore di flusso Xstream delle attività di elaborazione che richiedono più CPU e che sono necessarie per i tunnel IPsec, ad esempio l'incapsulamento/cifratura e la decompressione/decifratura del protocollo ESP. Questa nuova caratteristica sfrutta il pieno potenziale delle capacità di cifratura dell'hardware integrate nel processore di flusso Xstream. In più offre il vantaggio aggiuntivo di liberare più risorse CPU per altre attività, come la Deep Packet Inspection del traffico che la richiede. L'accelerazione FastPath di Xstream per il traffico IPsec è applicabile sia al traffico site-to-site che a quello VPN di accesso remoto.



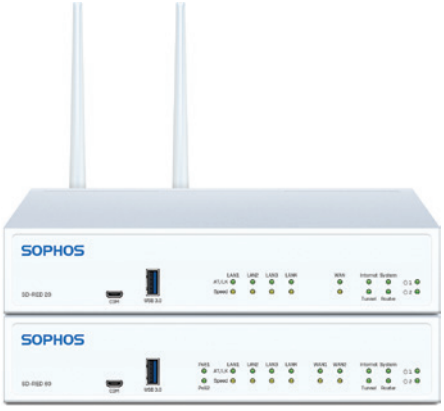
Gestione dei collegamenti WAN di Sophos Firewall, che include regole di bilanciamento e failover.

Connettività SD per le filiali

Da tempo Sophos è una delle aziende pioniere nell'ambito della distribuzione e della connettività zero touch delle filiali, grazie ai nostri esclusivi dispositivi SD-RED. Questi dispositivi sono convenienti e facilissimi da distribuire anche per i dipendenti che non hanno competenze tecniche specializzate. Permettono di stabilire un tunnel Layer 2 affidabile e sicuro tra il dispositivo e un firewall centrale.

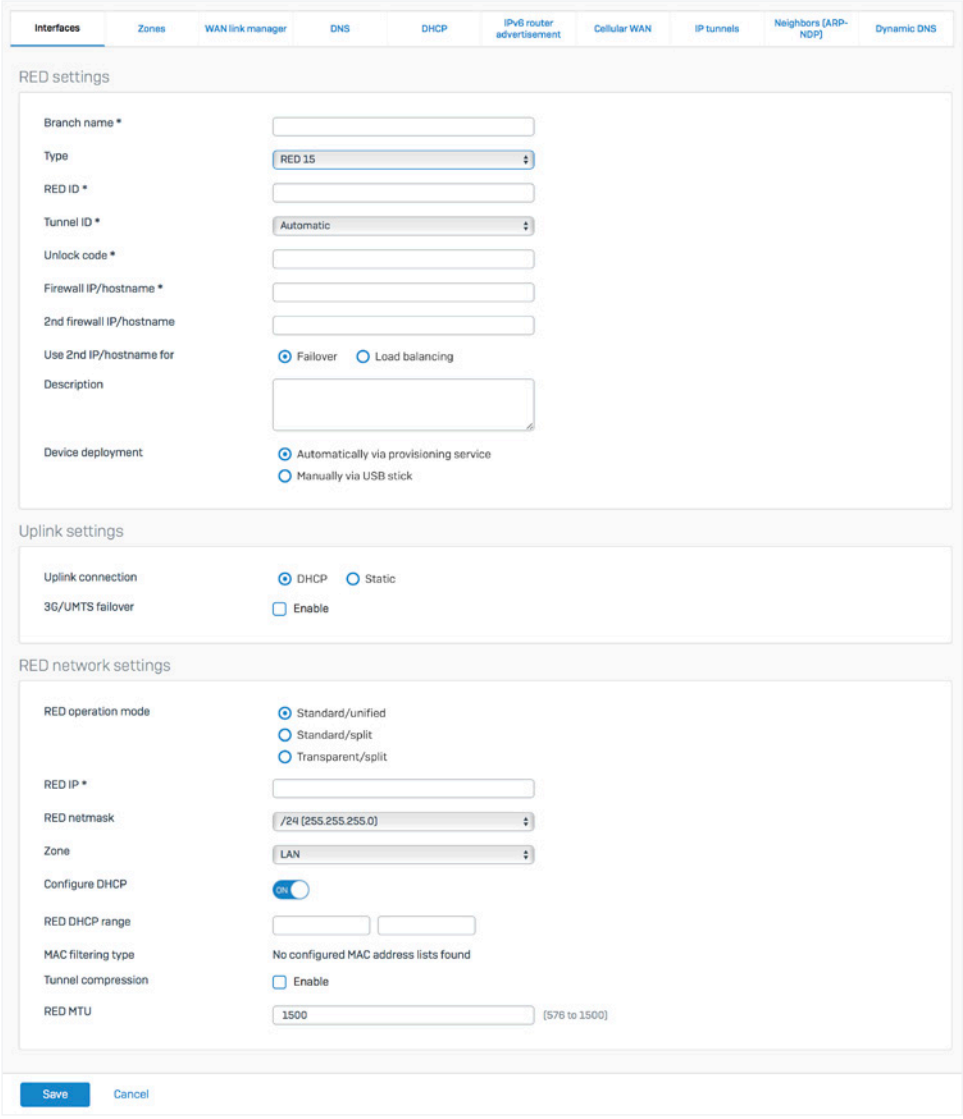


I dispositivi Sophos Firewall e SD-RED offrono opzioni di tunnelling per semplificare e connettere le filiali con SD-WAN in maniera pratica e conveniente.



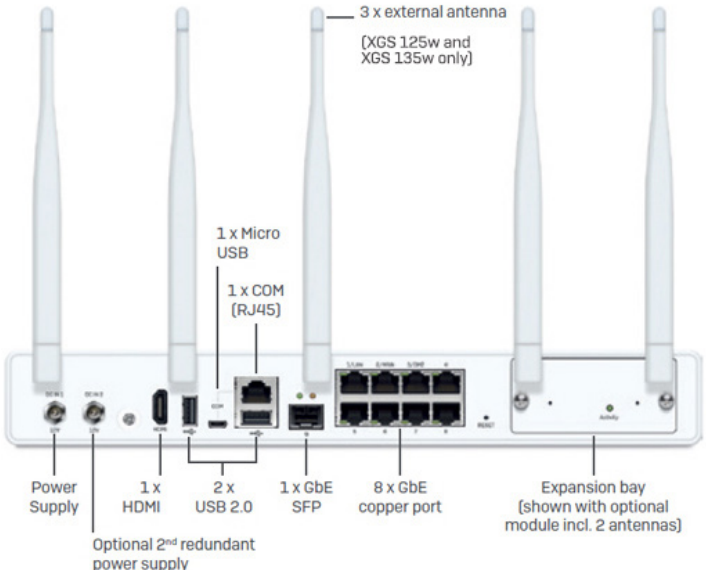
I dispositivi Sophos SD-RED offrono una soluzione zero touch pratica e conveniente per la connettività delle filiali con SD-WAN.

Distribuire i dispositivi SD-RED non potrebbe essere più semplice: basta prendere nota del numero di serie del dispositivo nel firewall e inviare il dispositivo alla sede remota. Qualsiasi dipendente (anche non dotato di particolari competenze tecniche) presso la sede remota può quindi connettere il dispositivo, e quest'ultimo contatterà il nostro servizio di provisioning su cloud, per stabilire automaticamente una connessione tunnel sicura con il tuo Sophos Firewall.



Sophos SD-RED offre una soluzione di connettività SD-WAN flessibile, sicura e conveniente per le filiali.

Anche le nostre appliance desktop XGS possono essere un'ottima soluzione di connettività SD-WAN, grazie alle loro opzioni flessibili, che includono VDSL e rete cellulare, oltre alle interfacce in rame o fibra. Inoltre, supportano anche i nostri potenti tunnel SD-RED.

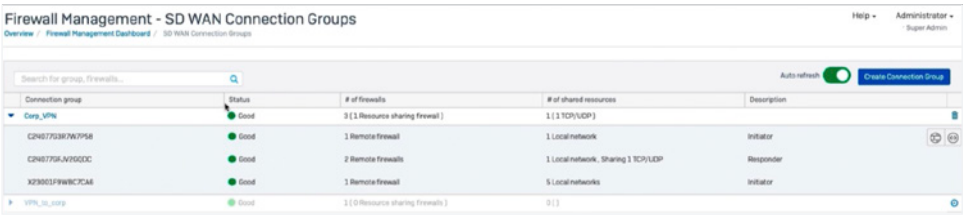


Alcuni modelli desktop (come l'XGS 135w visualizzato in questa immagine) sono dotati di opzioni di connettività WAN per LTE/rete cellulare, VDSL, rame o fibra.

Supporto e orchestrazione delle VPN

Chiunque abbia mai configurato più di due tunnel VPN tra firewall diversi sa benissimo quanto possa essere lunga e complicata questa operazione. Sophos Firewall supporta ricche funzionalità di orchestrazione della SD-WAN in Sophos Central, che semplificano e velocizzano il processo di interconnessione di tunnel multipli tra vari firewall.

Basta selezionare i firewall gestiti che si desidera includere nel gruppo di connessione SD-WAN e successivamente selezionare le risorse di rete a cui ogni sito potrà accedere. Attivando un semplice interruttore, potrai quindi assistere all'implementazione della tua rete VPN SD-WAN overlay, con la creazione automatica di tutti i tunnel e le regole di accesso necessarie per il firewall, incluse quelle per la ridondanza.



Configurazione rapida di reti SD-WAN overlay complesse in pochi passaggi, e con la possibilità di monitorarle da Sophos Central.

È possibile impostare una rete mesh completa, una topologia hub-and-spoke o un sistema ibrido. Sophos Central configura automaticamente tutte le opzioni necessarie per tunnel e firewall nel backend, per l'abilitazione della rete SD-WAN overlay.

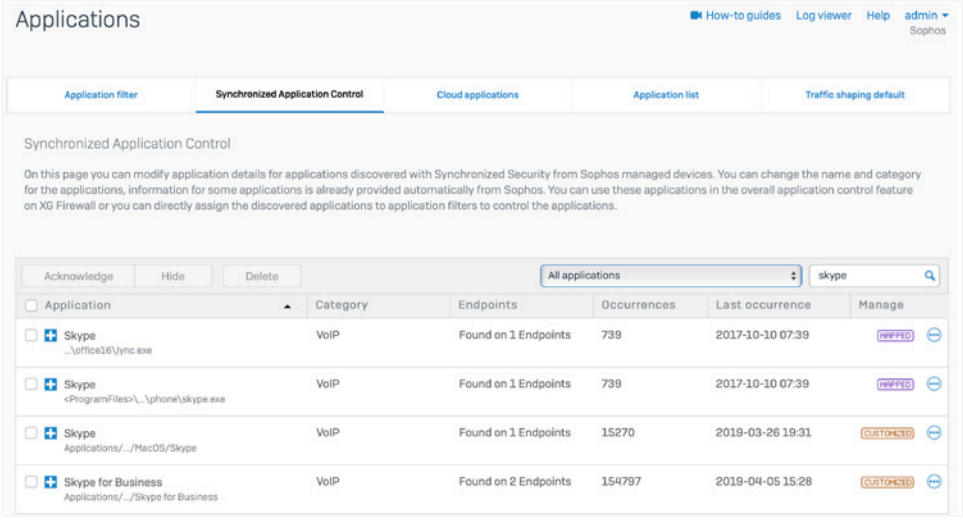
Naturalmente, Sophos Firewall supporta tutte le opzioni VPN site-to-site standard, inclusi IPsec e SSL. Offriamo anche il nostro esclusivo tunnel SD-RED Layer 2 con un routing estremamente potente e affidabile in situazioni caratterizzate da una latenza elevata, quali i collegamenti via satellite.

Visibilità e routing per le applicazioni

Un'altra opzione importante per poter raggiungere gli obiettivi delle SD-WAN è la selezione del percorso e il routing delle applicazioni, che garantiscono massima qualità e riducono la latenza per applicazioni mission-critical quali VoIP.

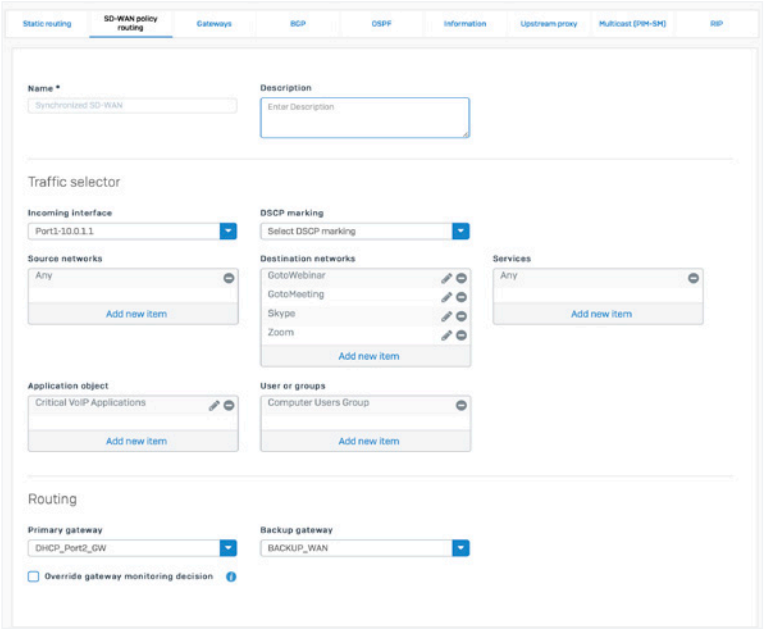
Naturalmente, è impossibile identificare quello che non si vede, per cui anche l'identificazione accurata delle applicazioni e la visibilità su queste applicazioni sono essenziali. È proprio in questo ambito che Sophos Firewall e Sophos Synchronized Security offrono un vantaggio incredibile. Il Synchronized Application Control garantisce chiarezza e visibilità al 100% su tutte le applicazioni della rete, e rappresenta un vantaggio significativo nel processo di identificazione di applicazioni mission-critical, specialmente per quanto riguarda quelle ignote o personalizzate.

Synchronized SD-WAN, una funzionalità di Synchronized Security, offre ulteriori vantaggi per il routing delle applicazioni SD-WAN. Synchronized SD-WAN sfrutta la maggiore chiarezza e attendibilità nell'identificazione delle applicazioni, grazie alla condivisione di informazioni di Synchronized Application Control tra Sophos Firewall e gli endpoint gestiti da Sophos. Ora le applicazioni precedentemente non identificate possono essere aggiunte alle policy di routing della SD-WAN, per un livello di controllo e di attendibilità del routing delle applicazioni semplicemente impensabile per gli altri firewall.



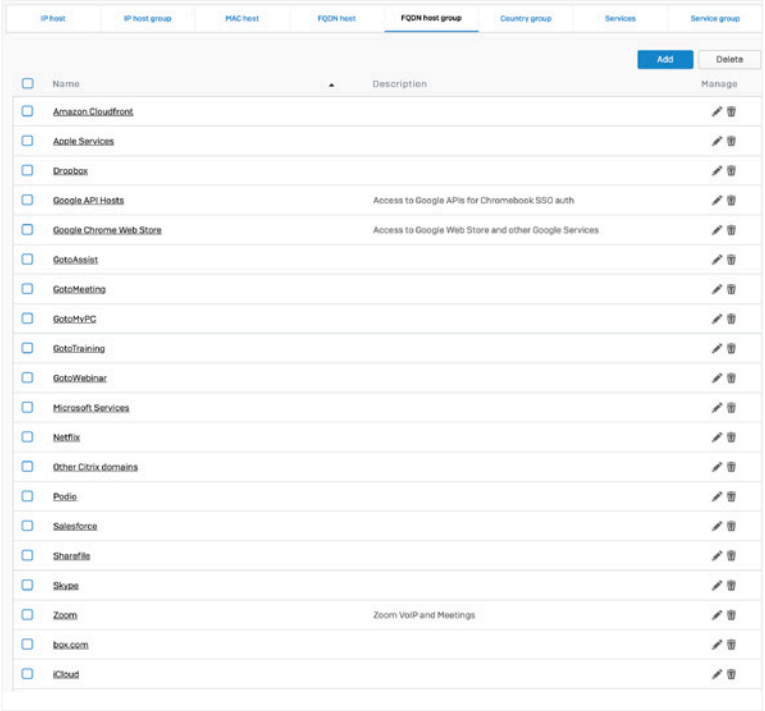
Il Synchronized Application Control identifica il 100% di tutte le applicazioni presenti all'interno della rete, semplificando l'assegnazione delle priorità e il routing delle applicazioni mission-critical.

Inoltre, Sophos Firewall abilita il routing basato sulle applicazioni e la selezione del percorso in tutte le regole del firewall, incluse quelle basate su utenti e gruppi. Il controllo del routing granulare e basato sulle policy (Granular Policy-based Routing, PBR) garantiscono la capacità di definire il routing tramite connessione WAN al gateway primario o di backup, e di configurarlo per la riproduzione della direzione. Insieme, queste funzionalità semplificano l'indirizzamento del traffico delle applicazioni importanti, in modo che utilizzino l'interfaccia WAN più idonea.



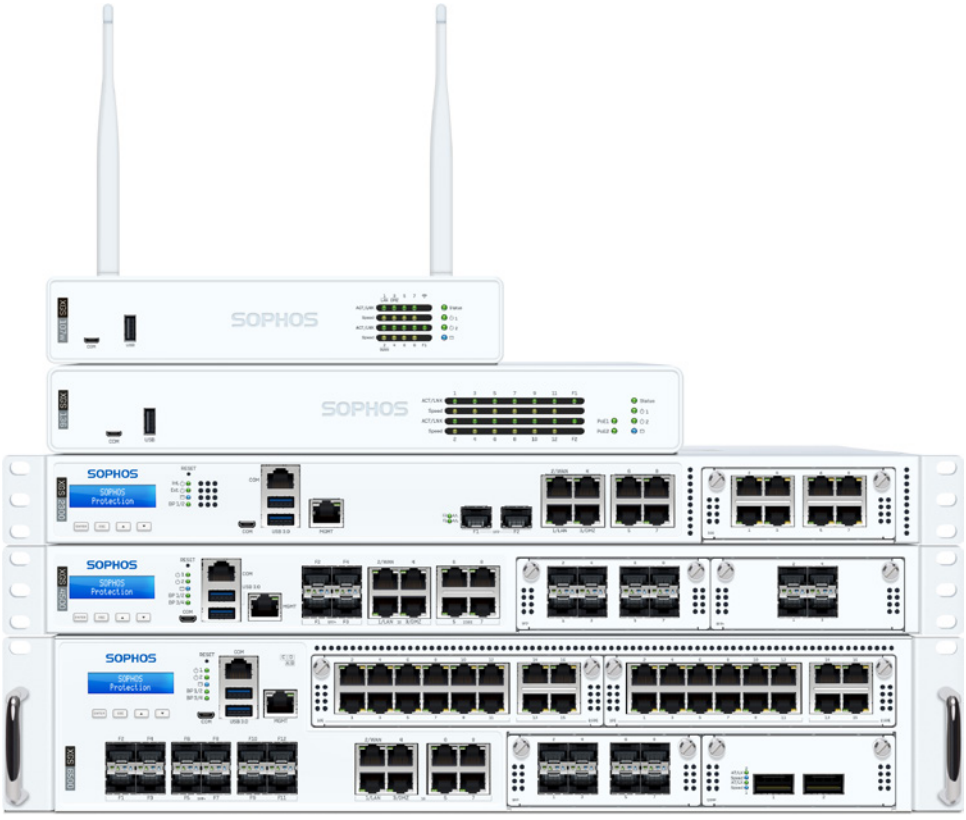
Il routing SD-WAN basato sulle policy offre strumenti flessibili per instradare il traffico delle applicazioni di natura critica.

Sophos Firewall include anche oggetti Fully Qualified Domain Name (FQDN) predefiniti per i più comuni servizi cloud SaaS, con migliaia di definizioni predefinite per gli host FQDN e l'opzione di aggiungerne altre con estrema facilità.



Gli oggetti host FQDN predefiniti semplificano la selezione del percorso e il routing in base alle applicazioni.

Aggiunta di Sophos Firewall a qualsiasi rete, con la massima semplicità



Le nostre appliance hardware Sophos Firewall offrono opzioni flessibili per la distribuzione, con porte di bypass con fail-open incluse come standard in tutti i modelli 1U e disponibili nei moduli FleXi Port per abilitare questa funzionalità anche nelle nostre appliance 2U. Le porte di bypass permettono l'installazione di Sophos Firewall in modalità bridge, in-line con firewall già esistenti. Se Sophos Firewall dovesse aver bisogno di essere arrestato o riavviato per un aggiornamento del firmware, le porte di bypass garantiranno la continuità del business, in quanto permetteranno al traffico di continuare a scorrere, evitando interruzioni del servizio nella rete. Questa funzionalità consente di introdurre nuove opzioni di distribuzione a rischio zero, senza bisogno di sostituire alcuna parte dell'infrastruttura di rete attuale. Inoltre, la nostra soluzione di protezione endpoint next-gen, Intercept X, si esegue parallelamente a qualsiasi prodotto antivirus per desktop. Questa sua caratteristica permette di installare un sistema Sophos Synchronized Security completo su qualsiasi rete, senza dover sostituire alcun componente già esistente.

Sophos Firewall: cybersecurity made simple.

Richiesta di preventivo

Per una richiesta di preventivo personalizzata e senza obbligo di acquisto, visitare: sophos.it/firewall-quote

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

22-03-30 IT (DD)