CISCO
SECURE

White Paper
Informazioni pubbliche Cisco

Il futuro del firewall

Realizzare oggi una postura più solida mentre si cerca di realizzare gli obiettivi di business e soddisfare le esigenze della sicurezza di domani

CISCO The bridge to possible

Sommario

Introduzione

Scopo di questo white paper è mostrare come sia cambiata la sicurezza della rete e discutere le strategie future per proteggere gli ambienti di lavoro.

Di pari passo a una maggiore eterogeneità delle reti, è diventato sempre più difficile gestire e applicare in modo coerente le policy o poterle monitorare tutte da un'unica console. Una rete complessa e interconnessa può indurre a passi falsi ed errori di configurazione, esponendola ancora di più a minacce sempre nuove e sofisticate.

Cosa fare per riprendere il controllo e avere policy coerenti? Possiamo iniziare da un approccio integrato alla sicurezza, che ponga il firewall al centro della nostra strategia.

I firewall sono ancora componenti imprescindibili di una strategia di sicurezza, ma così come le reti sono cambiate, è necessario che cambi anche il firewall. In passato, il firewall era una appliance situata all'ingresso/all'uscita del "perimetro" che agiva come punto di controllo basato su policy per autorizzare o rifiutare il traffico di rete. Per affermarsi nel mondo digitale di oggi, dobbiamo superare il concetto di singolo firewall e adottare una strategia di firewall diffusi, ossia adottare un metodo basato su policy in grado di coordinare strategicamente i meccanismi di sicurezza avanzati tramite più punti di controllo logici distribuiti su tutta la rete eterogenea.

L'adozione di una strategia di firewall diffusi rappresenta un passo avanti decisivo per adattare meglio la sicurezza agli obiettivi di business e alle esigenze del networking che sono in continuo mutamento. Per favorire il passaggio a questo nuovo modello, Cisco ha lavorato duramente per realizzare una piattaforma di sicurezza integrata le cui fondamenta poggiassero sul firewall.

"I firewall sono ancora componenti imprescindibili di una strategia di sicurezza, ma così come le reti sono cambiate, è necessario che cambi anche il firewall."

Adottando una strategia di firewall diffusi, le aziende che hanno intrapreso un percorso di trasformazione digitale possono conquistare una postura della sicurezza più solida per realizzare gli obiettivi di business e pensare alla sicurezza nel lungo termine.

Sezione 1 – Un po' di storia

Come è cambiata la sicurezza della rete

Il firewall è sempre stato collocato alla periferia della rete come un vero e proprio guardiano. Monitorando e controllando il traffico di rete, ha agito come un punto di controllo omnicomprensivo. Posizionato nel punto di ingresso/uscita della rete, al firewall si chiedeva soprattutto di controllare le comunicazioni. Il traffico interno alla rete era considerato per sua natura affidabile, il traffico esterno intrinsecamente pericoloso. Per autorizzare il traffico desiderato e bloccare i dati malevoli, i criteri e le policy venivano creati e applicati in questo unico punto di controllo.

Se paragoniamo il perimetro della rete a un fossato che circonda un castello, possiamo vedere il firewall come un ponte levatoio in grado di controllare chi entra e chi esce dalla fortezza.

Sicurezza della rete tradizionale

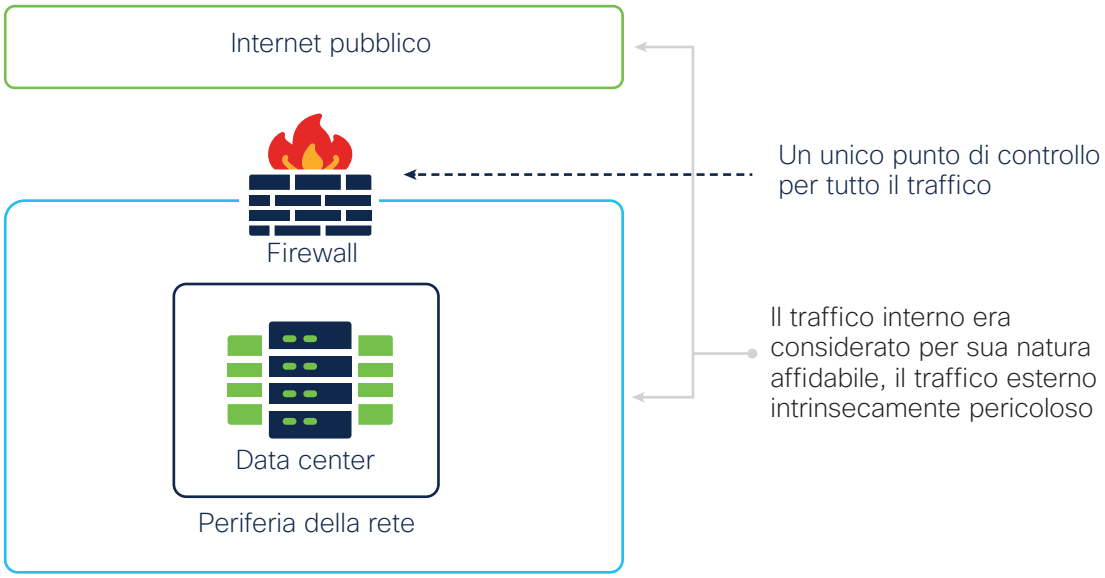


Figura 1. L'approccio tradizionale del firewall di rete

Poi è arrivato il cloud. E le applicazioni.

L'approccio alla sicurezza basato su un unico punto di controllo è stata ben presto messo in discussione. All'inizio con l'aumento degli accessi remoti e la crescita della mobilità aziendale. Ma la trasformazione è iniziata realmente con il cloud computing. Con il passaggio al cloud, i dispositivi e gli utenti hanno iniziato a migrare in massa all'esterno della rete sicura e controllata e il modello con un unico punto di controllo si è dimostrato inadeguato. I perimetri si sono moltiplicati. E tutti dovevano essere protetti. Non si poteva più scavare un fossato intorno alla rete.

Oggi le filiali, i dipendenti remoti e il crescente utilizzo dei servizi cloud stanno sempre più spostando i dati dal tradizionale "perimetro", ignorando completamente il tradizionale punto di controllo della sicurezza. Molte aziende hanno adottato un modello BYOD (Bring Your Own Device, utilizzo di dispositivi personali), che consente ai dipendenti di accedere alle applicazioni aziendali riservate dai propri computer privati o dispositivi mobili. Oltre il 67% dei dipendenti utilizza propri dispositivi al lavoro, una tendenza in aumento di cui non si vede la fine. Il modello prevalente, e ormai irrinunciabile per svolgere le attività lavorative quotidiane, è connettersi alla rete aziendale con dispositivi mobili e laptop da reti Wi-Fi pubbliche.

Inoltre, la stragrande maggioranza delle sedi e degli utenti aziendali deve poter accedere direttamente a Internet e al cloud, dove si trovano la maggior parte delle applicazioni e dei dati cruciali. Le aziende continuano a usare una molteplicità di servizi cloud, sistemi operativi, appliance fisiche, database e molto altro. Le applicazioni e i dati vengono ulteriormente decentrati e, di conseguenza, le reti diventano ancora più diversificate.

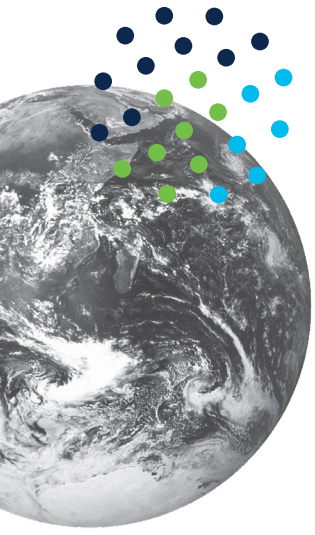
La nuova realtà

Un unico approccio per tutte le situazioni si è dimostrato inadeguato.

Figura 2. La complessità della rete e l'evoluzione delle minacce mettono a dura prova il modello tradizionale di firewall

Una realtà nuova e più complessa

Sebbene queste innovazioni favoriscano un ambiente di lavoro più interconnesso e produttivo, hanno cambiato profondamente il modo con cui lavoriamo. I tempi in cui si controllavano le applicazioni e si autorizzavano gli utenti on-premises sono tramontati e oggi i servizi e le applicazioni sono offerte alle aziende in ecosistemi dinamici e multicloud. Non è tutto, oggi anche i rapporti con le terze parti sono diventati fondamentali. L'espansione dei servizi e l'outsourcing hanno creato economie di scala ed efficienza, ma non senza qualche compromesso. Questa evoluzione delle architetture di rete ha aumentato notevolmente la superficie della rete esposta agli attacchi e ha reso più complicato il compito di proteggere le reti, i dati e gli utenti aziendali.

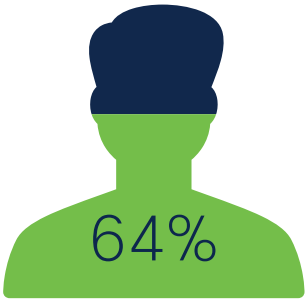


Destreggiarsi tra prodotti che soddisfano esigenze specifiche

Le aziende hanno reagito alla nuova realtà cercando la soluzione di sicurezza specifica "migliore" che potesse risolvere i singoli problemi man mano che si presentavano. Questo approccio ha creato una "proliferazione" senza precedente di dispositivi, arrivando anche a una media di 75 strumenti di sicurezza per azienda[1]. La molteplicità dei prodotti di sicurezza e dei fornitori può creare significativi problemi di gestione ai team della sicurezza. Nella maggior parte dei casi, la proliferazione di dispositivi e funzionalità di sicurezza ha comportato semplicemente un aumento del rischio di attacchi. Intervistati, il 94% dei professionisti dell'IT e della sicurezza ha dichiarato di essere preoccupato che una maggiore complessità della rete la possa rendere più vulnerabile. L'88% vuole poter cambiare le policy di sicurezza della rete con più agilità[2].

Tra gennaio e luglio 2019, sono state scoperte 3.800 violazioni, un cospicuo aumento del 54% rispetto alla prima metà del 2018[3]. Questo aumento esponenziale testimonia come anche gli hacker usino metodi sempre più sofisticati. Il crescente tasso di successo delle violazioni indica anche che i metodi tradizionali di sicurezza della rete non sono più in grado oggi di arginare e contrastare le minacce.

1 "Defense in depth: Stop spending, start consolidating", CSO, 4 marzo 2016.
2 "Navigating Network Security Complexity", report ESG Research Insights, giugno 2019.
3 "Navigating Network Security Complexity", report ESG Research Insights, giugno 2019.



L'errore umano è considerato la causa principale di un errore di configurazione

Più minacce, più interferenze, ancora più rischi

Se gli hacker usano nuovi vettori di attacco, dalle e-mail agli endpoint non verificati con policy BYOD, ai portali Web e ai dispositivi IOT, le aziende devono cercare di difendersi adottando altre strategie.

Come accennato in precedenza, la tendenza a cumulare prodotti di sicurezza per esigenze specifiche non aiuta certo la postura complessiva. Anzi, è esattamente il contrario. Crea più "interferenze" e rende difficile la gestione. Mentre i team faticano a tenere gli occhi aperti e individuare i nuovi inevitabili attacchi e malware che tentano di sfruttare qualsiasi vulnerabilità (più o meno nota), questa maggiore complessità rende ancora più difficile creare, gestire e applicare le policy di sicurezza.

Ai team che gestiscono la sicurezza della rete viene chiesto di configurare singolarmente una moltitudine di risorse cloud e ciò non fa che aumentare la possibilità di errori di configurazione e quindi di violazioni. Un controllo di sicurezza non implementato o non implementato correttamente può essere la causa di una violazione. E il 64% delle aziende afferma che gli errori di configurazione sono causati principalmente da errori umani[4]. Che l'errore comporti una violazione di conformità, un'interruzione del servizio o apra un varco per l'ingresso di un hacker, in ogni caso questi sono rischi che non possiamo permetterci.

Dobbiamo ripensare il firewall

Proteggere la rete è diventata un'impresa ardua. Oggi i team sono alla affannosa ricerca di un modo per gestire la varietà di soluzioni di sicurezza, risorse cloud e appliance. È il momento di adottare un approccio diverso.

Il momento di fondare sul firewall l'intera piattaforma di sicurezza, agile e integrata, con cui far crescere l'azienda oggi e in futuro.

Sezione 2 – Dal firewall singolo a una strategia di firewall diffusi

Perché più firewall?

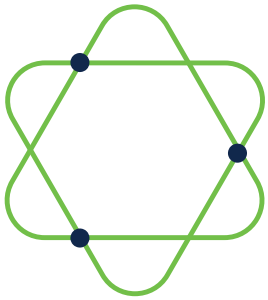
Mano a mano che le reti cambiano per adattarsi alla nuova realtà del business, anche la sicurezza della rete deve cambiare. Nel mondo attuale di risorse IT distribuite, il firewall svolge ancora un ruolo fondamentale per una solida postura della sicurezza.

Tuttavia, per rendere efficace la protezione di un'ampia varietà di infrastrutture di rete, dispositivi connessi e sistemi operativi, i requisiti che deve avere un firewall sono aumentati sensibilmente. I dispositivi firewall "tradizionali" sono stati appesantiti da un mix di appliance fisiche e virtuali, alcune integrate nella rete ma altre fornite come servizio, basate su host o incluse negli ambienti di cloud pubblico. Alcuni stanno addirittura assumendo nuovi fattori di forma, è il caso delle appliance in cluster in grado di sostenere volumi di traffico elevato, dei software dei dispositivi personali, dei router SD-WAN o dei gateway Internet sicuri. Poter condividere i risultati dell'intelligence sulle minacce in tutti i dispositivi firewall, ovunque siano situati, è essenziale per garantire una visibilità uniforme delle minacce e una postura della sicurezza solida.

Per cambiare veramente e proteggere meglio le reti moderne, è il momento di abbandonare il tradizionale approccio "perimetrale". E definire sull'intero fabric della rete i punti strategici su cui applicare le policy, il più vicino possibile alle informazioni o alle applicazioni che devono essere protette. La creazione di micro-perimetri su punti di controllo fisici e logici è diventata quindi una necessità.

Non dobbiamo più pensare al firewall come a un dispositivo di rete fisico e autonomo, ma piuttosto pensare alla funzionalità di più firewall.

4 "Cloud Security Breaches and Human Errors", Fugue, 7 febbraio 2019.



Cosa vuole dire usare più firewall?

Sgombriamo il campo da eventuali fraintendimenti: il firewall è oggi più importante che mai. E infatti, per proteggere le reti moderne abbiamo bisogno di **più** firewall **situati in più punti**. L'adozione di più firewall si differenza perché pone l'accento su **come** stabilire dei controlli basati su policy ovunque.

L'uso di più firewall può offrire un approccio agile e integrato per funzionalità di sicurezza avanzate, per coordinare le policy centralmente e applicarle in modo coerente in reti sempre più complesse ed eterogenee. Deve offrire protezione e visibilità complete e permettere di armonizzare le policy e autenticare in modo sicuro utenti e dispositivi. Un nuovo approccio al firewall deve trarre vantaggio anche dalla condivisione dell'intelligence sulle minacce in tutti i punti di controllo per avere monitoraggio e visibilità uniformi, riducendo drasticamente il tempo e lo sforzo necessari per rilevare le minacce, indagarne le cause e trovare azioni correttive.

In questo modo l'adozione di più firewall si trasforma in una vera e propria strategia in grado di proteggere reti complesse. E permette di affrontare le esigenze future dell'azienda di fronte a minacce che cambiano continuamente.

Cosa vuole dire usare più firewall?

I punti in cui erigere un firewall possono essere ovunque nelle moderne reti eterogenee.

L'adozione di più firewall permette di proteggere la rete con policy coerenti e di avere la piena visibilità delle minacce in modo da prevenire, rilevare e bloccare gli attacchi con maggiore rapidità e precisione, ovunque vengano sferrati.

In cosa consiste il nuovo approccio?

Per proteggere le risorse e i dati nel cloud, in locale o in sedi remote, i firewall devono fornire in modo coerente una protezione dalle minacce avanzate, permettere l'applicazione delle policy e usare i risultati dell'intelligence sulle minacce. Devono coordinare in modo coerente tutti i diversi ambienti in cui si usano e si implementano i dispositivi.

Le violazioni alla sicurezza possono avere origine su qualsiasi dispositivo che abbia accesso a Internet, indipendentemente da dove si trova, nella sede centrale dell'azienda, nel data center, nelle sedi remote, nei cloud pubblici o in qualunque altro luogo dove il dipendente lavora da remoto. Ecco perché è più importante che mai integrare una serie solida di punti di controllo della sicurezza in più posizioni logiche per ridurre l'esposizione ai rischi e attenuarne eventualmente le conseguenze. I controlli di sicurezza vengono applicati ove necessario, in ambienti proprietari (appliance fisiche e virtuali e dispositivi di rete come i router), in ambienti non proprietari (Security as a Service, SECaaS), nei controlli nativi e nei carichi di lavoro.

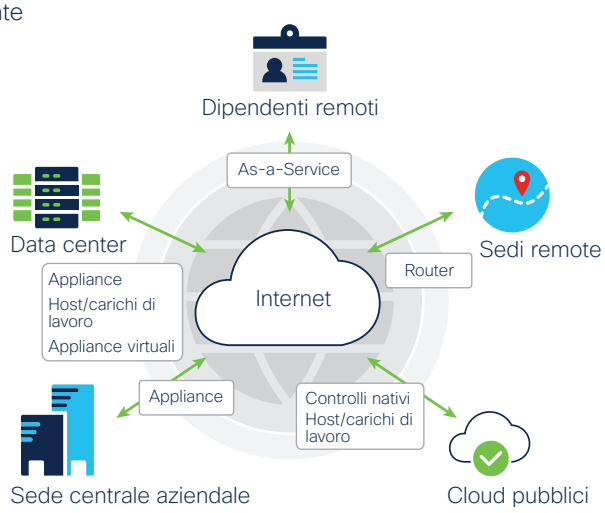


Figura 3. I principali tenant dei firewall permettono di affrontare le criticità della sicurezza delle reti moderne

Estensione dei controlli di sicurezza

Un tempo tutto il traffico interno e gli utenti autorizzati erano considerati per loro natura affidabili, al contrario del traffico esterno. Tradizionalmente, il firewall veniva collocato sul perimetro della rete. E il perimetro della rete diventava il punto di controllo logico in grado di proteggere l'intera organizzazione. Tutto il traffico di rete, ovunque fosse originato, nella sede principale, nel data center o da un lavoratore remoto, veniva incanalato in modo che passasse attraverso questo unico punto di controllo.

Negli ambienti complessi di oggi, un modello di questo tipo non sarebbe efficace. L'infrastruttura IT di un'azienda si estende a un'ampia varietà di fattori di forma e modelli di erogazione, tra cui appliance fisiche e virtuali, router o switch integrati nella rete, forniti come servizio, basati su host o inclusi in un cloud pubblico.

Adottando una strategia di firewall diffusi, è possibile implementare i controlli di sicurezza in modo coerente e fornire una visibilità completa sulle minacce e una policy unificata. Questi controlli permettono di autenticare in modo ancora più sicuro gli utenti e i dispositivi in ambienti sempre più eterogenei. E assicurano che i dispositivi soddisfino i requisiti di sicurezza predefiniti rilevando, condividendo e reagendo al contesto di utenti, sedi e dispositivi. Usando controlli di sicurezza coerenti su tutti i micro-perimetri, è possibile rendere automatiche alcune attività, come mettere in quarantena gli utenti e i dispositivi non conformi, bloccare i domini sospetti e supportare una microsegmentazione efficace. Adottare una strategia di firewall diffusi permette di avere una vista olistica di tutti gli avvisi di sicurezza e di tutti gli indicatori di compromissione e di usare i risultati dell'intelligence sulle minacce su ciascun dispositivo connesso per essere sempre aggiornati sulle nuove minacce.

Gestione nel cloud

E non basta più avere prodotti mirati e specifici. Con l'aumento esponenziale dei perimetri delle reti e delle risorse cloud sono aumentate anche le vulnerabilità. Tutelare le risorse più preziose di un ambiente cloud complesso e allo stesso tempo gestire una molteplicità di prodotti di sicurezza è compito arduo. Per ridurre al minimo l'eventualità di errori di configurazione, i team della sicurezza devono avere visibilità della rete in tempo reale e strumenti di gestione facili.

L'adozione di più firewall promuove una postura della sicurezza più solida perché supporta una gestione nel cloud centralizzata e aiuta i team della sicurezza a eliminare le complessità e applicare policy coerenti a tutta l'azienda. Con l'ausilio dei modelli è possibile definire una policy una sola volta e applicarla poi in modo coerente a decine di centinaia di punti di controllo sparsi sull'intera rete. L'uso di modelli di policy standard permette di implementare in tempi brevi i nuovi dispositivi e di ridurre gli errori di configurazione. Man mano che l'azienda cresce, le nuove implementazioni ereditano automaticamente le policy più aggiornate. Per la gestione delle policy viene usato un sistema scalabile con un'unica policy di accesso in cui sono integrate più funzionalità di sicurezza. Lo stesso sistema ottimizza le policy applicate ai dispositivi di sicurezza rilevando le incongruenze e correggendole rapidamente.

Infine, con la gestione centralizzata nel cloud le prestazioni del team aumentano notevolmente. I team possono rilevare con rapidità i rischi su tutti i dispositivi, in modo che siano tutti più sicuri e condividano le stesse policy. Sulla console di gestione unificata, possono analizzare le caratteristiche di tutti i dispositivi per scoprirne le eventuali incongruenze e ottimizzare la postura della sicurezza. La gestione delle policy può essere più semplice, l'efficienza migliorata e la sicurezza più coerente e meno complessa.

Contrastare le minacce con l'intelligence

Con l'espandersi del perimetro della rete e la proliferazione dei dispositivi connessi direttamente a Internet, aumenta anche la superficie esposta agli attacchi. Le minacce di cybersecurity che usano malware, criptovaluta, phishing e botnet

sono in rapida crescita. I criminali informatici usano l'apprendimento automatico e l'intelligenza artificiale per insinuarsi nelle vulnerabilità del software e sferrare attacchi malevoli. Sono poche le aziende che hanno le risorse adeguate per provare e confermare tutte le patch di sicurezza dei vari fornitori e respingere quindi l'assalto di minacce sempre nuove e diverse.

Ecco un altro aspetto interessante in cui una strategia di firewall diffusi può essere efficace. Con un'intelligence forte e ricerche accurate, disponibili quasi in tempo reale, è possibile avere una protezione sempre aggiornata e arginare il flusso costante di minacce. I ricercatori identificano rapidamente gli indicatori di compromissione e confermano e condividono le minacce altrettanto rapidamente. Utilizzando economie di scala, il loro obiettivo è proteggere le aziende prima che vengano attaccate. Usando i risultati condivisi dall'intelligence sulle minacce su reti, endpoint, carichi di lavoro e ambienti cloud interconnessi, i team della sicurezza possono mettere in relazione eventi che apparentemente non hanno nulla a che fare l'uno con l'altro, eliminare le interferenze e bloccare le minacce più velocemente.

Quali sono i rischi di non adottare una strategia di firewall diffusi?

Nel tentativo di adattarsi ai cambiamenti del networking, realizzare gli obiettivi di business e supportare l'operatività, le aziende hanno implementato diversi prodotti specifici. Lo stesso hanno fatto di fronte ai nuovi vettori di attacco, cumulando prodotti nel vano tentativo di proteggersi dalle nuove minacce. Coloro che fanno affidamento sul firewall tradizionale per proteggere i dispositivi connessi su più perimetri rischiano di esporre i dati e le risorse più importanti a violazioni della sicurezza. Secondo il Cybersecurity Almanac del 2019, entro il 2021 i danni causati dal crimine informatico ammonteranno a 6 trilioni di dollari l'anno[5].

Le minacce possono insinuarsi rapidamente in una rete e mettere a repentaglio l'operatività di un'azienda che non abbia una soluzione di sicurezza completa e la piena visibilità degli endpoint.

Ciò premesso rimane sicuramente un compito arduo proteggere la rete di un'azienda, gli ambienti cloud, i dispositivi e i dati ovunque si trovino.

5 "2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions And Statistics", Cybercrime Magazine, 6 febbraio 2019.

Il firewall rimane la pietra angolare su cui costruire qualsiasi nuova strategia di sicurezza a prova di futuro

In Cisco abbiamo lavorato duramente per trasformare in realtà questa visione. Collaboriamo con aziende di ogni dimensione in tutto il mondo e tutte chiedono una sicurezza più agile e integrata, che sia incorporata nella rete stessa. Ecco perché offriamo l'architettura più sicura di sempre, una piattaforma potente e completa che poggia su solide fondamenta: il firewall.

L'obiettivo della nostra strategia della sicurezza è fornire livelli di protezione elevati. Le soluzioni di sicurezza e la famiglia di firewall Cisco aiutano a prevenire le nuove minacce con controlli di sicurezza eccellenti, disponibili ovunque servano, policy e visibilità coerenti e innovazioni che migliorano la gestione operativa della sicurezza.

Oggi che le minacce sono più dinamiche che mai, Cisco offre una postura della sicurezza solida e capace di reagire anche alla sfide future, combinando tecnologie all'avanguardia e soluzioni di networking efficaci.

I firewall tradizionali offrono solo una visibilità limitata, mentre l'IT deve poter vedere ciò che accade sull'intera rete e conoscere i risultati dell'intelligence sulle minacce per rilevare e bloccare le minacce prima che danneggino irreparabilmente i sistemi. L'uso di più firewall supera l'approccio tradizionale e offre una postura della sicurezza basata su gestione unificata e sicurezza completa con funzionalità di prevenzione delle intrusioni, filtro URL e protezione dal malware avanzato usando l'automazione e l'apprendimento automatico.

Senza l'uso di firewall diffusi, la complessità della rete può portare a errori di configurazione, aumentando il rischio di una violazione della sicurezza. Secondo un report di Gartner, "fino al 2022, almeno il 95% delle falle nella sicurezza cloud sarà attribuibile a un errore umano"[6]. Adottando firewall diffusi e coordinando in modo armonico le policy di sicurezza sui vari punti di controllo, le aziende migliorano la postura complessiva.

Sezione 3 – Definire una strategia di firewall diffusi in quattro mosse

Fase 1: gettare le fondamenta per una strategia di successo con un moderno firewall di nuova generazione. Scegliere il Cisco Secure Firewall giusto permette di avere una soluzione di sicurezza integrata con policy di sicurezza coerenti, visibilità e una pronta risposta alle minacce.

Fase 2: dopo aver scelto il Cisco Secure Firewall, occorre individuare una soluzione di gestione. Tenere conto di questi fattori:

- Individuare la posizione di gestione preferita (on-premises o nel cloud) e il team responsabile (SecOps o NetOps).
- In particolare, accertarsi che la soluzione di gestione sia conforme agli obiettivi attuali e futuri dell'IT. Se si stanno spostando i carichi di lavoro nel cloud, lanciando un portale fornitori, cercando di attuare progetti di trasformazione digitale o usando applicazioni SaaS, si può scegliere una gestione nel cloud. Se l'azienda si affida ancora alle applicazioni monolitiche esistenti, la gestione on-premises può soddisfare meglio le esigenze. In genere, per funzionare correttamente nel cloud, le applicazioni esistenti devono essere aggiornate, e se non si prevede di farlo nell'immediato, è preferibile usare un sistema di gestione on-premises.
- Una soluzione di gestione nel cloud permette ai team di gestione della rete di armonizzare le policy in tutta l'azienda, ridurre la complessità e gestire tutti i punti di controllo della sicurezza da un'unica dashboard. Inoltre, semplifica l'orchestrazione e permette di gestire le policy in modo coerente da un'unica console per contrastare le nuove minacce. Con un'applicazione centralizzata nel cloud, è possibile semplificare la gestione della sicurezza, usare i modelli per implementare rapidamente i nuovi dispositivi e tenere traccia di tutte le modifiche apportate in tutto l'ambiente.

Fase 3: integrare per rafforzare la postura della sicurezza. Adottare una strategia di firewall diffusi permette di coprire tutti i micro-perimetri e garantisce protezione e controllo su tutti i dispositivi connessi e le soluzioni di sicurezza. L'integrazione della sicurezza in tutta la rete eterogenea, nelle applicazioni e nei servizi cloud, nell'e-mail aziendale e in tutti gli endpoint connessi protegge l'azienda dalle minacce in continua espansione.

In questa fase il team della sicurezza si prepara a bloccare le minacce, rispondere rapidamente ad eventi malevoli e automatizzare le attività su tutta la rete, sulle applicazioni cloud e sugli endpoint.

Fase 4: infine, accertarsi di integrare nei firewall anche le analisi delle minacce avanzate per proteggere le risorse aziendali e anticipare le

6 "Is the Cloud Secure?" Gartner, 27 marzo 2018.

nuove minacce. Una delle opzioni più semplici è scegliere una soluzione che fornisca automaticamente alla rete le informazioni più recenti sulle minacce tramite il firewall. Con l'intelligence aggiornata e una visibilità completa, ai team della sicurezza non sfuggiranno le nuove vulnerabilità. E se una minaccia si insinua all'interno, sapranno come individuarla e come risalire alla causa principale. Con la funzionalità IPS di nuova generazione integrata, i rischi e gli indicatori delle conseguenze vengono classificati automaticamente per identificare le risorse più importanti e intervenire sugli eventi in base alle priorità. I team della sicurezza possono intraprendere immediatamente azioni correttive e porre rimedio alle minacce, rimanendo concentrati sulle risorse cruciali anziché essere sopraffatti da eventi minori e rendendo la gestione della sicurezza più efficace.

Tutto dipende dal giusto firewall

Oggi i team della sicurezza hanno bisogno di:

Una sicurezza migliore supportata dall'intelligence sulle minacce per proteggere le reti complesse, rilevare tempestivamente le minacce e intervenire rapidamente.

Modalità **efficienti per configurare, scalare e armonizzare le policy di sicurezza** su tutta la rete.

Maggiore visibilità e minore complessità con una gestione e un'automazione unificate per una gestione operativa della sicurezza rapida e una migliore esperienza.

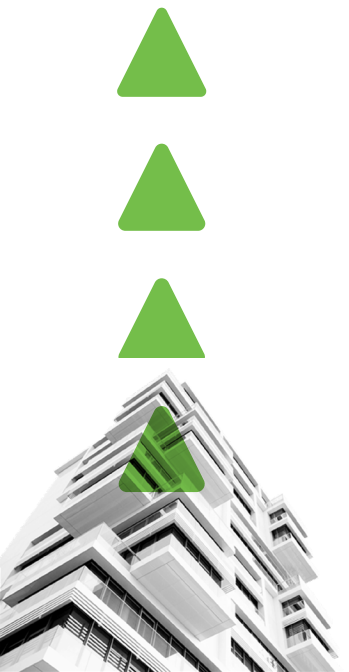
Networking e sicurezza che collaborino per trarre il massimo vantaggio dagli investimenti esistenti. La soluzione giusta dovrà quindi fornire un'integrazione profonda per una sicurezza completa che protegga tutto, ovunque.

I vantaggi di adottare una strategia di firewall diffusi con Cisco Secure Firewall

L'intera rete diventa un'estensione dell'architettura di sicurezza: condividendo la policy comune, le funzionalità di prevenzione delle intrusioni e altre funzioni principali con Cisco Secure Firewall, gli switch e i router possono applicare policy di sicurezza coerenti e integrare l'infrastruttura di rete in una soluzione di sicurezza completa. Condividi rapidamente i risultati dell'intelligence sulle minacce sull'architettura per correlare tra loro eventi apparentemente scollegati, eliminare le interferenze e bloccare le minacce più velocemente.

Controlli di sicurezza di altissimo livello: Cisco Secure Firewall è estremamente efficace contro le minacce e protegge le reti complesse dagli attacchi sempre più sofisticati di oggi. La migliore intelligence sulle minacce avanzate aiuta l'azienda a individuare nuovi domini malware e URL dannosi e a scovare vulnerabilità sconosciute o non ancora condivise per rilevare le minacce in anticipo e intervenire tempestivamente. L'IPS di nuova generazione integrato offre una visibilità completa, classifica automaticamente i rischi e gli indicatori delle conseguenze per identificare gli eventi a cui i team della sicurezza devono dare maggiore attenzione, riducendo al minimo le interferenze. La sicurezza retrospettiva ti tiene informato e analizza continuamente le minacce rilevate per individuare il malware sofisticato che potrebbe aver eluso i controlli iniziali.

Policy unificata e visibilità delle minacce: i team della sicurezza possono definire i controlli di sicurezza comuni e applicarli su tutti i dispositivi , dalle appliance della rete agli host e al cloud, e gestire così policy più coerenti e armonizzate. La gestione flessibile e centralizzata di Cisco permette di applicare controlli scalabili a molti dispositivi in modo facile e veloce per avere policy coerenti. Con funzioni di sicurezza perfettamente integrate, tra cui l'uso di più firewall per le applicazioni, NGIPS e AMP, e una gestione unificata, le complessità si riducono e gli eventi della sicurezza sono messi automaticamente in correlazione tra loro. Semplifica la gestione delle policy e dei dispositivi di sicurezza sulle reti estese e svolgi più rapidamente le attività importanti, come il rilevamento delle minacce, le indagini sulle cause principali e la ricerca di azioni correttive.



Sezione 4 – Una soluzione di sicurezza pronta per il futuro

Il nostro modo di lavorare è cambiato. Sono cambiate le nostre reti e aziende e con loro le regole di sicurezza della rete. Questi sviluppi ci impongono di ripensare il firewall e adottare una nuova strategia.

Per affrontare la nuova realtà, Cisco propone una soluzione innovativa, una piattaforma di sicurezza con controlli eccellenti e presenti ovunque ce ne sia bisogno, con policy coerenti e visibilità completa, e una intelligence sulle minacce senza eguali. Il Cisco Secure Firewall di nuova generazione rappresenta le fondamenta delle nostre soluzioni perfettamente integrate.

La principale soluzione di gestione nel cloud Cisco, **Cisco Defense Orchestrator**, permette di armonizzare le policy sui diversi prodotti di sicurezza Cisco.

Inclusa in ogni prodotto di sicurezza Cisco, **la funzionalità di risposta alle minacce Secure** permette di reagire alle minacce e ai nuovi attacchi informatici, condividendo e implementando automaticamente le contromisure sull'intera architettura di sicurezza.

Secure Endpoint offre intelligence sulle minacce globale, sandboxing avanzato e blocco del malware in tempo reale. AMP analizza senza sosta l'attività dei file sulla rete estesa per rilevare, arginare e rimuovere rapidamente il malware avanzato.

L'intelligence sulle minacce Talos è un team di ricercatori, analisti di dati e tecnici di fama mondiale che si dedicano a tempo pieno alla raccolta di informazioni sulle minacce esistenti e in via di sviluppo. Talos sostiene l'intero ecosistema di sicurezza Cisco e fornisce protezione da attacchi e malware. Permette inoltre di avere piena visibilità di tutte le nuove minacce a livello mondiale e offre dati di intelligence utili per la difesa dalle minacce e la mitigazione delle conseguenze delle conseguenze e una risposta comune per proteggere attivamente tutti i clienti Cisco.

SNORT Next-Generation Intrusion Prevention System (SNORT NGIPS) è un sistema di prevenzione delle intrusioni di nuova generazione open source che offre analisi del traffico, funzionalità di sniffing/registrazione dei pacchetti e analisi dei protocolli. Facendo affidamento sull'intelligence sulle minacce di Talos, SNORT NGIPS aiuta l'intera comunità dei professionisti della sicurezza condividendo le policy efficaci sulle nuove minacce.

Identity Services Engine (ISE) permette di accedere in modo flessibile e affidabile ovunque in base al contesto. Fornisce una protezione intelligente e integrata tramite policy basate sugli intenti e soluzioni di conformità.

Secure Access di Duo offre l'autenticazione a più fattori, la visibilità degli endpoint, un'autenticazione adattiva e l'applicazione delle policy con accesso remoto e tecnologia Single Sign-On per un accesso sicuro e proattivo alle applicazioni.

Secure Network Analytics, Secure Workload Application Centric Infrastructure (ACI) insieme tengono traccia dei siti visitati dagli utenti e dei carichi di lavoro delle applicazioni, ovunque si trovino, con tecniche come l'apprendimento automatico, la modellazione dei comportamenti, la raccolta di dati telemetrici sull'infrastruttura di rete e con la segmentazione per anticipare le nuove minacce.

Implementa la tua strategia di firewall diffusi per il futuro investendo nella piattaforma di sicurezza Cisco e in Cisco Secure Firewall. Potrai così costruire una postura della sicurezza più solida oggi ed essere preparato alle incognite del futuro.

Sezione 5 – Inizia a costruire oggi il futuro del firewall

Cisco riunisce soluzioni di networking eccellenti e una tecnologia all'avanguardia nella sicurezza per fornire l'architettura più sicura di sempre. E si impegna a innovare continuamente, per migliorare la sicurezza della rete a partire dagli investimenti esistenti o trasformando i router in firewall.

Cisco Secure Firewall rappresenta la sicurezza della rete progettata per l'azienda che sta passando al digitale dall'azienda che ha creato la rete.

Scopri di più su Cisco Secure Firewall e inizia subito a definire la nuova strategia di firewall diffusi. Per saperne di più sulle ultime tendenze per le reti di domani, leggi il Report sulle tendenze globali del networking 2020.