

Il bisogno di una security fabric per orchestrare i firewall

Scomparendo il perimetro aziendale occorre ridefinire l'architettura di firewalling per rispondere a minacce sempre più mirate. Un'urgenza per le imprese distribuite

Avvertenze

Pubblicato nel 2016

Tutti i marchi contenuti in questo white paper sono registrati e di proprietà delle relative società. Tutti i diritti sono riservati. Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale.

Copyright Reportec – 2016

www.reportec.it

Sicurezza senza confini: il nuovo ruolo del firewall per l'enterprise

I modelli architetturali sono inadeguati a proteggere un perimetro aziendale che non esiste più. Il bisogno di una security fabric nella risposta allo scenario evolutivo delle minacce.

Dagli albori della sicurezza informatica, il firewall rappresenta, insieme all'antivirus, l'elemento base per la protezione delle informazioni aziendali. Sviluppato agli inizi degli anni Novanta, si è occupato per oltre un ventennio di proteggere il perimetro aziendale. Inizialmente, il compito era relativamente semplice ed è sempre stato svolto con efficienza negli anni, evolvendo in risposta alle nuove minacce, anche se, talvolta, con poca efficacia. Non di rado, infatti, firewall mal configurati o impostati su policy di base hanno dato e danno un illusorio senso di sicurezza.

Oggi siamo a una svolta sostanziale, tanto che il firewall, così come è stato interpretato finora, non ha più ragione d'essere, perché, semplicemente, non esiste più un "perimetro" aziendale. Più precisamente, non esiste più un perimetro disegnato dalla rete aziendale a protezione della quale sono stati finora posti i firewall e gli IPS (Intrusion Prevention System). Già i cosiddetti NXGF (Next Generation Firewall) hanno introdotto una serie di funzionalità tese a rispondere a nuove forme di attacco via Internet, ma la questione è che una quantità sempre maggiore di dati, anche critici, non è più dietro la rete aziendale.

Smart working, mobility, Internet of things, public e hybrid cloud, applicazioni SaaS, digital transformation: sono gli ambiti tecnologici e organizzativi che trainano l'innovazione dei processi nelle imprese, ma dal punto di vista della sicurezza diventano un grande problema. Un altro aspetto da considerare è l'obsolescenza di un approccio semplicemente basato sul tradizionale risk assessment, che potrebbe portare a trascurare punti di un'infrastruttura sempre più "allargata", classificandoli come a basso rischio, salvo poi scoprire





che costituiscono un accesso per la rete attraverso un percorso, magari tortuoso ma mirato.

La prima difficoltà, in questo scenario, è definire la superficie d'attacco, che si è estesa a dismisura, rispetto al passato, quando proprio il firewall rappresentava il baluardo del "castello". Questa metafora non può più rappresentare le variegate realtà aziendali e, in particolare, non ha alcun riscontro con le aziende distribuite, le quali, oltre a essere quelle più esposte alle minacce, sono anche le più a rischio, in quanto perlopiù appartenenti a settori storicamente presi di mira dai cyber criminali, come finanziario, retail, sanità. Attacchi mirati e persistenti sono certamente una piaga per le grandi organizzazioni, che si dotano di numerosi livelli di controllo, ma poi accade che un ospedale si vede bloccare gli apparati da un ransomware penetrato nel sistema grazie a un "click distratto" su una mail.

Ma una costante opera di educazione alla sicurezza, per quanto fondamentale, non è sufficiente, proprio perché confini aziendali si sono estesi: il link malevolo per il download del suddetto ransomware, per esempio, potrebbe arrivare non tramite una mail di spear phishing, ma all'interno di un messaggio di LinkedIn o di un altro social, sul quale è complicato attuare una qualche forma di controllo. Come accennato, i cyber criminali hanno imparato a sfruttare i punti deboli, considerati a basso rischio dallo staff IT, utilizzandoli a guisa di un ponte. Ha fatto scuola il caso di Target, il retailer cui nel 2014 sono stati rubati i dati delle carte di credito dalla rete Pos: gli hacker ci sono arrivati penetrando la rete di un fornitore che monitorava il funzionamento dei frigoriferi. Un punto di accesso trascurato e un sistema vulnerabile, quello del fornitore, fuori dal

controllo dell'azienda.

A complicare la situazione contribuisce la crescita disordinata del sistema di sicurezza, cui negli anni si vanno sommando componenti di diversi fornitori, magari perché si persegue la logica del best of breed o perché sono state effettuate acquisizioni. La gestione di tali sistemi comporta oneri operativi dovuti all'uso di console diverse e porta a una riduzione della sicurezza effettiva, perché risulta spesso difficile contare su un controllo integrato e si rimane vincolati a segmentazione a silos altamente inefficiente in un contesto caratterizzato da una superficie di attacco dinamica. Peraltro, anche laddove si è consolidato la sicurezza su sistemi di ultima generazione, come i firewall NGFW, si ripresenta la questione della loro gestione, che in contesti distribuiti non è banale, ancora una volta generandosi conflitti tra dispositivi diversi o, più semplicemente, creandosi l'esigenza di utilizzare console di management non integrabili fra loro.

Per superare tali problematiche, alcune aziende della sicurezza stanno proponendo servizi e soluzioni più efficaci ed efficienti, soprattutto in termini di compatibilità tra diversi fattori di forma, consolidamento delle aree di sicurezza, più alte prestazioni e affidabilità della rete. Non ultimo, soluzioni caratterizzate da una gestione semplificata realizzata attraverso una singola console di management. Restano però delle criticità, finanche nell'approccio.

Firewall packet filtering

Nei primi anni '90 è stata commercializzata una delle prime tecnologie firewall (filtraggio dei pacchetti), che veniva integrata principalmente nei router e negli switch per filtrare determinati protocolli e indirizzi IP. Quindi è stata sviluppata una versione migliorata del filtraggio dei pacchetti, detta stateful inspection.

Firewall Stateful Inspection

A differenza del semplice filtraggio dei pacchetti, il firewall stateful inspection era in grado di mantenere informazioni sullo stato, che gli permettevano una maggiore sicurezza nella metodologia di ispezione. Anche se la tecnologia stateful inspection eseguiva controlli efficaci sui livelli inferiori dello stack OSI, non era altrettanto affidabile quando si trattava di capire e proteggere i dati al livello applicativo.



La protezione delle imprese distribuite

Come si è avuto modo di osservare, le imprese distribuite presentano delle specificità che le rendono particolarmente soggette ad attacchi da parte di organizzazioni cyber criminali e vulnerabili.

Le suddette difficoltà implicite nella gestione di soluzioni eterogenee sono una delle questioni che devono affrontare le imprese distribuite: si pensi alle acquisizioni e fusioni che, negli anni recenti e ancora oggi, si registrano nel settore bancario e in quello della grande distribuzione. A queste si aggiungono le scelte dettate dalle diverse teorie sviluppatesi per seguire l'evoluzione delle reti e delle architetture progettate per i sistemi di protezione. In particolare, si è partiti concentrando l'intelligence di sicurezza nella sede principale, dove risiedeva storicamente il CED (Centro Elaborazione Dati) e tutte le strutture più importanti che andavano quindi salvaguardate. Il nucleo della rete era l'elemento attorno al quale "ruotava" l'architettura, ma, con l'evolversi delle reti geografiche (WAN) si sono sviluppate due impostazioni: da un lato, si è pensato di mantenere un'infrastruttura centralizzata sempre più estesa, che supportasse le esigenze di sicurezza dal centro fino alla periferia o "edge" della rete. Sul fronte opposto, si è realizzato un modello decentralizzato che replicava le funzioni di sicurezza presso ogni sede distaccata.



Application Firewall, IPS e Web Filtering

Alcuni anni dopo sono stati realizzati i firewall applicativi, in grado di capire determinati protocolli e applicazioni comuni negli ambienti aziendali. Anche se i firewall applicativi sono in grado di capire e decifrare il traffico di tipo HTTP (web) o SMTP (email), possono incidere pesantemente sulle prestazioni di rete e richiedono molti interventi di ottimizzazione e aggiornamento per funzionare correttamente. La necessità di comprendere il contesto applicativo ha inoltre portato allo sviluppo di soluzioni di sicurezza

specializzate, come i sistemi di intrusion prevention (IPS) e i prodotti di web filtering, che sono infine diventati prodotti di sicurezza con una propria area specifica di applicazione.

Spesso i responsabili della sicurezza nelle aziende distribuivano sia firewall stateful inspection che applicativi per la difesa del perimetro principale. Ciò portava a una complessità elevata e a sfide collegate alla gestione e configurazione delle svariate tecnologie di sicurezza di rete.



I due approcci hanno ben presto mostrato limiti e svantaggi, nessuno dei due permettendo di garantire un'adeguata sicurezza nelle sedi distaccate. Nel primo caso, ciò si verifica sia per problematiche prestazionali sia perché l'architettura non permette di estendere tutte funzioni di protezioni a sedi che sono, di fatto, al di là della periferia di rete.

Nell'approccio decentralizzato, la sicurezza viene meno per i costi di acquisto di numerosi apparati per la protezione per quelli derivanti dalla loro gestione. Tra l'installazione e le operazioni distribuite su tanti dispositivi, il rischio più che probabile è quello di veder aumentare i punti di vulnerabilità a causa degli errori umani, inevitabili, per l'installazione e configurazione.

Le esigenze di mobilità

A complicare ulteriormente questi aspetti architetture, è intervenuto il boom della mobility, cioè la diffusione esponenziale dei dispositivi mobili, dal notebook al tablet, dallo smartphone a un crescente numero di apparati dalle caratteristiche mutevoli. Le reti wireless sono nate inizialmente per superare problematiche strutturali che rendevano difficoltoso o molto costoso installare la rete cablata: per esempio in edifici storici, dove non era possibile svolgere opere murarie, oppure in estese aree esterne con presenza di ostacoli naturali, come corsi d'acqua. Ma la presenza di

Firewall Unified Threat Management

Intorno agli anni 2000 entrò sulla scena la tecnologia Unified Threat Management (UTM), che consentiva di combinare, elaborare e gestire i controlli stateful e applicativi da una singola piattaforma. Il firewall UTM (coniato da IDC) si riferiva a un prodotto di sicurezza all-inclusive che combinava firewall di rete e altre tecnologie di ispezione a livello applicativo, come IPS, web filtering, antisipam e antivirus, in un unico fattore di forma. Dal momento che i firewall UTM all-inclusive richiedevano risorse di elaborazione massicce,

vennero adottati nelle piccole e medie imprese, dove i requisiti di larghezza di banda erano minori. A causa di considerazioni economiche e di esigenze consolidamento di diverse tecnologie di sicurezza a livello di applicazione, le imprese IT all'interno di questi mercati vincolati dal budget adottarono questa soluzione su larga scala.

Dal momento che i firewall UTM mancavano della granularità e del controllo necessari per alcune delle funzioni di sicurezza più avanzate (ad esempio





numerosi dispositivi ha spostato le criticità sulla scalabilità e sulla segmentazione delle aree coperte e/o della tipologia di utenti. Per questo, i network manager hanno impostato reti di overlay wireless con regole per la sicurezza degli accessi diverse da quelle definite per l'infrastruttura cablata esistente. Con conseguenti complessità gestionali e, soprattutto con un aumento delle vulnerabilità. Tutto a discapito del livello di sicurezza raggiungibile. Per di più, si pone la questione della Quality of Service da rendere generalmente omogenea e coerente agli SLA storni, in una rete ibrida composta da collegamenti aziendali, wireless e cablati, e da collegamenti WAN pubblici e/o privati.

Aumentano le complicazioni sia sulle architetture centralizzate sia su quelle decentralizzate. Si pone, quindi, un scelta diversa rappresentata da una nuova architettura di sicurezza distribuita che deve rispecchiare le esigenze della moderna impresa distribuita, ma non solo. Più in generale, infatti, è necessario garantire insieme alla sicurezza le massime prestazioni possibili e la disponibilità della rete. Da un lato, dunque occorre impostare un'architettura che prevede i diversi dispositivi di protezione, a partire ovviamente dal firewall, essere inseriti inline, per consentire di applicare al traffico di rete tutti i controlli necessari a prevenire gli attacchi. Questo, però, significa rischiare che il traffico possa restare bloccato dalle operazioni di uno qualsiasi di tali dispositivi.

IPS, web filtering, antispam), le imprese più grandi continuarono con il modello di difesa tradizionale, che prevedeva sia un firewall stateful che diverse forme di tecnologie di sicurezza a livello applicativo distribuiti lungo il perimetro aziendale esteso. La separazione e la scarsa comunicazione tra i diversi controlli di sicurezza non contribuivano a risolvere il problema della complessità di gestione e manutenzione di soluzioni di più fornitori.

Next Generation Firewall

La terminologia NGFW (firewall di nuova generazione), conosciuta da Gartner, è emersa intorno alla fine degli anni 2000. Partendo dall'idea UTM di una soluzione di sicurezza all-in-one, se ne guidò l'evoluzione orientandola più verso i requisiti di scalabilità degli ambienti aziendali più grandi. Per diversi anni la tecnologia NGFW ha ampliato le funzioni di sicurezza a livello di applicazione, aumentando la quantità di controlli e la granularità per rispondere alle esigenze prospettate dagli esperti di sicurezza aziendale. Oltre



Si dovrebbero, quindi, accelerare i controlli, ma questo non può avvenire a scapito della sicurezza. Piuttosto è opportuno aumentare le prestazioni per non congestionare la rete e garantire l'affidabilità dei dispositivi per mantenere elevata la disponibilità delle connessioni. C'è da considerare che ci sono tanti motivi per cui un dispositivo potrebbe smettere di funzionare e, spesso, non si tratta di attacchi informatici. È anche un semplice calcolo matematico, perché l'MTBF (Mean Time Between Failure) di configurazioni seriali si ottiene moltiplicando gli MBTF di ciascun dispositivo nella serie e il risultato potrebbe semplicemente essere eccessivo da tollerare, anche senza arrivare alla congestione totale, probabilmente i tempi di risposta penalizzerebbero l'experience degli utenti e la loro produttività.

Per questo si sta affermando un nuovo approccio basato su una security fabric. Si tratta di un nuovo approccio, che fa tesoro dell'esperienza maturata nella lotta agli attacchi mirati, anche chiamati persistenti (APT – Advanced Persistent Threats), la cui caratteristica principale è quella di utilizzare più tecniche di attacco e diversi tipologie di malware e tool, combinandoli e aggiungendo manovre “evasive”.

In questi tipi di attacco sono spesso identificabili delle fasi, ciascuna delle quali potrebbe essere bloccata, ma il cui disegno complessivo sfugge alle singole soluzioni di protezione messe in campo.

Occorre dunque un approccio collaborativo, che sappia anche sfruttare l'intelligence disponibile in cloud (cioè le informazioni aggiornate in tempo reale sullo stato delle minacce). La security fabric si deve occupare proprio della coordinazione delle attività di controllo, in modo che collaborino in maniera molto più efficiente di quanto finora realizzato dai firewall NGFW.

Nel seguito del white paper esaminiamo la security fabric messa a punto da Fortinet e le soluzioni di Enterprise Firewall, che la società statunitense ha basato su tale fabric.

a ulteriori controlli di sicurezza, il firewall NGFW ha inoltre integrato una maggiore potenza di elaborazione per la sicurezza di rete, per stare al passo con gli elevati requisiti di throughput degli ambienti più grandi.



La Security Fabric di Fortinet e l'Enterprise firewall

La Security Fabric consiste in framework che rappresenta il “tessuto” (fabric appunto in inglese) della sicurezza. Questo unisce tutte le soluzioni fornite dai firewall di Fortinet, i Fortigate, i Web application firewall e così via, inclusi nei vari segmenti della rete.

Di fatto consente di far comunicare tutti i dispositivi tra loro, realizzando un'intelligence interna, altresì esportabile nella global intelligence che aggiorna i sistemi su scala mondiale.

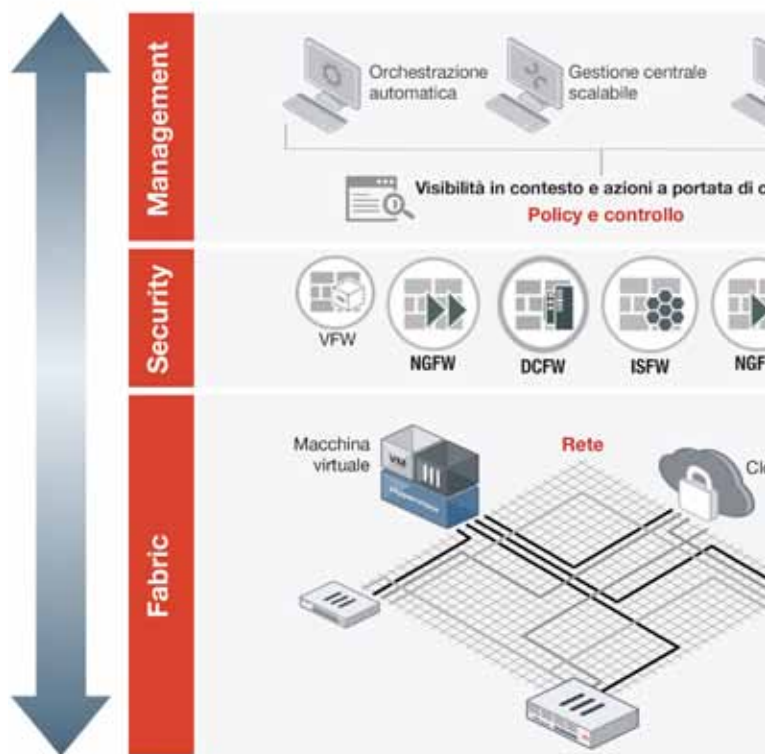
In questo modo si realizza un Enterprise Firewall che protegge l'infrastruttura nel suo complesso, comprese le sedi periferiche, in funzione delle strategie aziendali.

L'Enterprise Firewall definisce di fatto tre domini che cooperano come un unicum per eliminare la complessità e aumentare la sicurezza.

Il primo è il dominio di gestione: un'unica console fornisce ai responsabili della sicurezza un punto di riferimento fisso per la registrazione, la configurazione e la generazione di report relativi alla sicurezza. Grazie a delle API, vengono condivisi i dati di Threat Intelligence ed è possibile unificare la configurazione delle policy di sicurezza in tutta l'infrastruttura.

Al dominio di sicurezza, invece attengono le funzioni per ridurre o prevenire gli incidenti di sicurezza mediante sistemi di sicurezza multilivello. Per quanto profondi i controlli siano, le prestazioni sono assicurate dagli ASIC di Fortinet. Le configurazioni di sicurezza dipendono dalla distribuzione scelta e dalla segmentazione.

Infine il dominio della fabric è l'interfaccia di comunicazione e collaborazione che determina i punti in cui condividere la network e threat intelligence nell'azienda. Security Fabric può estendere i controlli di sicurezza oltre il livello della rete



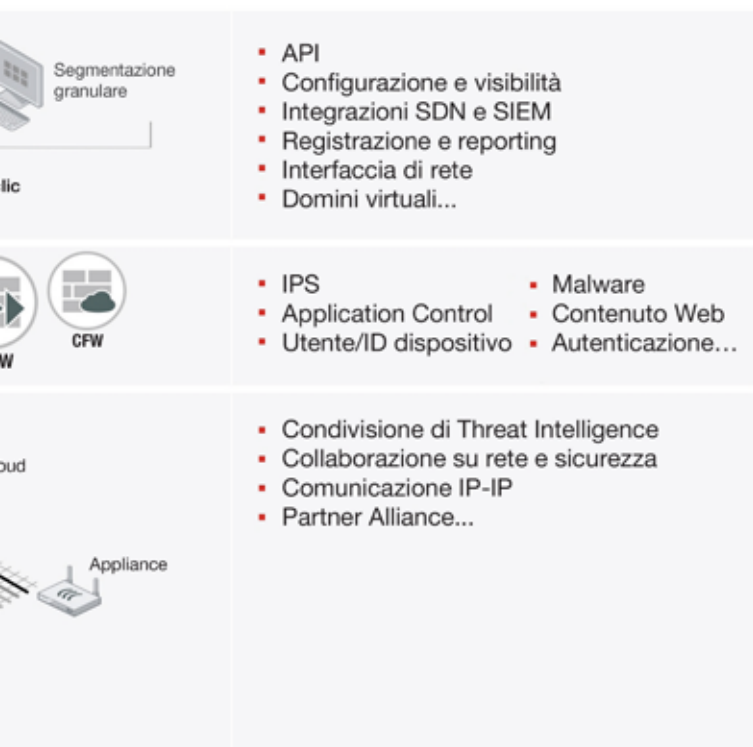
fino al livello degli accessi in cui è ubicato l'endpoint e al livello delle applicazioni in cui vengono presentati i servizi di dati e informazioni. Quando Enterprise Firewall rileva un evento lo segnala a Fortinet Security Fabric, che determina quali informazioni dovranno essere condivise in tutta l'azienda. Per esempio, se in una determinata area vengono rilevati dei malware, Security Fabric condivide informazioni di Threat Intelligence con il resto dell'infrastruttura aziendale. Similmente, quando viene definita una policy in una sezione, Security Fabric la applica contestualmente all'intera infrastruttura. Per non penalizzare le prestazioni, le funzionalità di personalizzazione flessibile del firewall consentono di adattare la condivisione di quanto connesso alla sicurezza con le esigenze specifiche di un particolare punto dell'organizzazione. Tutti i dispositivi firewall della soluzione Fortinet Enterprise Firewall sono interconnessi tramite Security Fabric. L'interconnessione ha il duplice scopo di fornire una protezione più efficace e allo stesso tempo semplificare la distribuzione riducendo l'esigenza di disporre a livello di azienda di più punti

di intervento e policy.

In pratica, ai fini operativi Fortinet Enterprise Firewall è una soluzione che, tramite un'unica piattaforma, un unico sistema operativo per la sicurezza di rete, una gestione delle policy unificata e una singola console di gestione, fornisce una sicurezza di rete end-to-end atta a garantire una elevatissima protezione contro le minacce più avanzate e gli attacchi mirati.

Le funzioni della soluzione Enterprise Firewall di Fortinet

FortiGate Next-Generation Firewall è, come evidenziato, una soluzione con cui Fortinet si è prefissata di perseguire l'obiettivo di assicurare una elevatissima protezione dalle minacce più



avanzate, con prestazioni ultraveloci ma senza per questo rinunciare alla semplicità operativa.

La piattaforma, che opera avendo alle spalle i FortiGuard Labs, fornisce un'ampia serie di servizi integrati. Tra questi:

- Stateful Firewall
- Intrusion Prevention
- Application Control
- Gestione e autenticazione delle identità di utenti/dispositivi
- Antimalware
- Sandboxing
- Web Filtering
- IP Reputation
- Ispezione SSL
- VPN IPsec/SSL
- Networking (LAN, WAN, Wi-Fi)
- Gestione e reporting

Singola console di gestione

Indipendentemente dalla posizione o dalla piattaforma (hardware, virtualizzata, cloud pubblico o ibrido) di distribuzione dei dispositivi Fortinet Enterprise Firewall, la visibilità e il controllo della sicurezza della rete avviene tramite un unico sistema operativo, il FortiOS.

FortiOS provvede a consolidare tutti i servizi di rete forniti dalla soluzione e a dare una visibilità a 360° del traffico che sulla rete si sviluppa. Il responsabile, con un solo clic, ha la possibilità di prendere visione del traffico con un'analisi che permette di esplorare cosa avviene per la singola applicazione, il tipo di minaccia, un particolare dispositivo, una determinata nazione e altri parametri di selezione.

Enterprise Firewall
distribuiti

Livello s

Firewall cloud



Next Generation Firewall (NGFW)

Firewall per data center



Internal Segmentation Firewall

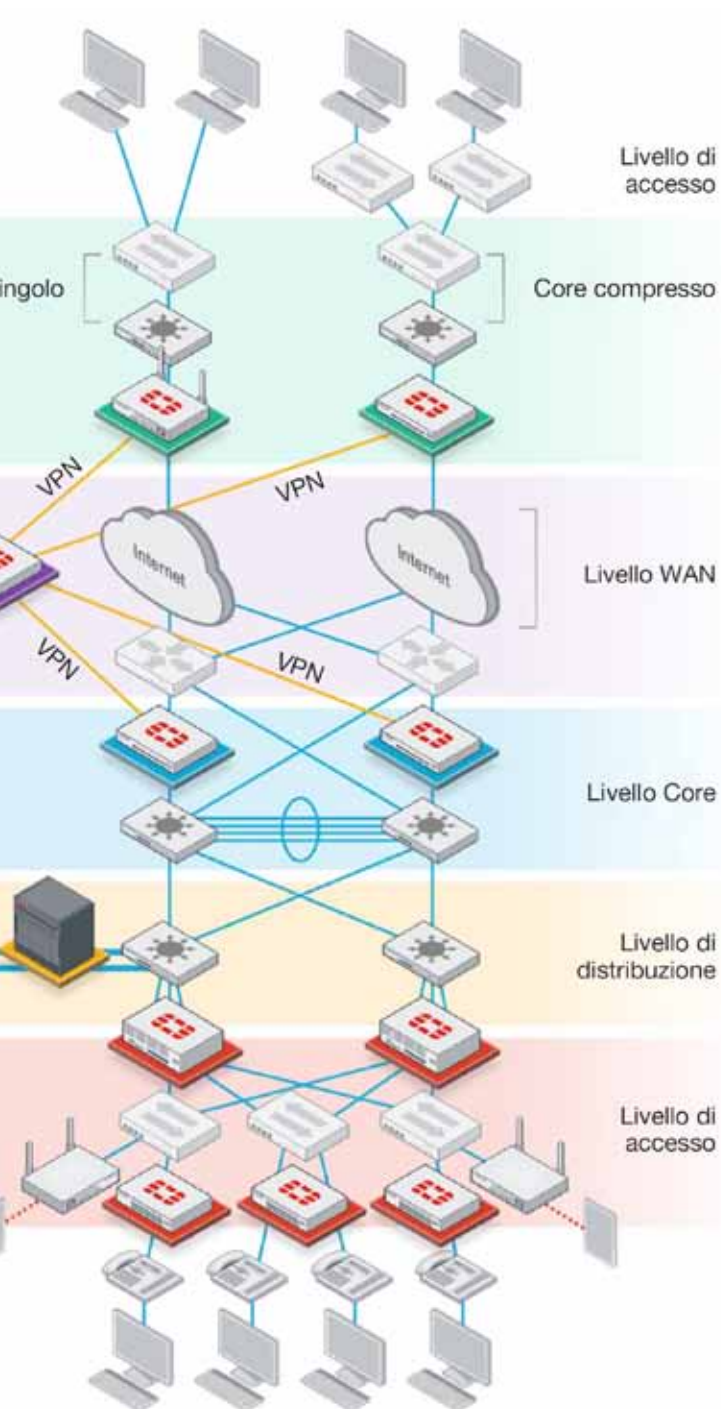
Parimenti, per quanto concerne le policy, i responsabili della sicurezza hanno la possibilità di prendere visione del traffico di rete e impostare policy consolidate che includono controlli di sicurezza granulari. Una singola console di gestione fornisce ai responsabili della sicurezza visibilità e controllo attraverso l'intera impresa per

una registrazione, reporting e gestione centrale scalabili.

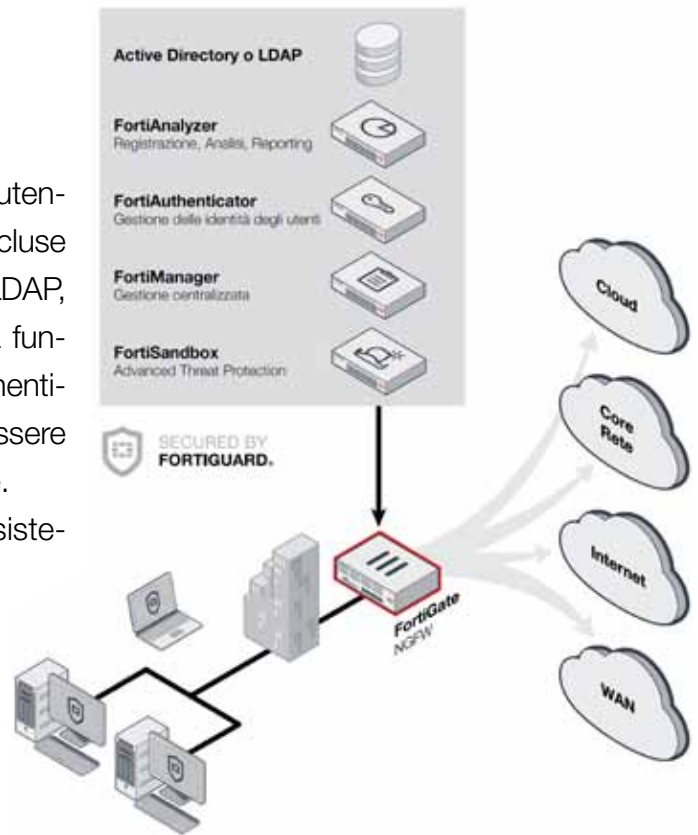
L'approccio adottato da Fortinet nello sviluppo della soluzione FortiGate, basato sul concetto di piattaforma singola, offre il beneficio di assicurare una protezione che può essere estremamente capillare, semplice da acquistare, distribuire e gestire. La visualizzazione intuitiva di applicazioni, utenti, dispositivi, minacce e l'uso dei servizi cloud e di ispezioni realizzabili in profondità presentano il beneficio congiunto di poter meglio comprendere cosa accade nella rete. È una visione strategica che permette di creare e gestire facilmente policy di sicurezza a elevata granularità concepite per ottimizzare la protezione e l'allocazione delle risorse di rete.

Ai fini operativi e del controllo diventa possibile:

- **Identificare migliaia di applicazioni** diverse con l'ausilio dell'Application Control (con funzione di controllo in profondità specifica per i servizi cloud). Tramite policy application-aware e altre sue caratteristiche FortiGate può esaminare il traffico SSL crittografato ed elusivo, così come il traffico in esecuzione sui protocolli più recenti e di nuova concezione. Questa capacità, abbinata ad altre funzioni di sicurezza, ha l'obiettivo di intercettare attacchi avanzati che si nascondono dentro applicazioni o sessioni crittografate.



- **Impostare policy granulari** per diversi tipi di utenti, tramite le funzioni di gestione delle identità incluse nel FortiGate e grazie alla integrazione con AD/LDAP, RADIUS, Exchange e altre fonti. È una coesiva funzionalità NGFW che, con l'aggiunta di FortiAuthenticator per reti diverse di grandi dimensioni, può essere espansa a molte altre soluzioni di autenticazione.
- **Identificare i tipi di dispositivi**, con relativi sistemi operativi, usati in rete, senza la necessità di ricorrere a specifici agenti o prodotti aggiuntivi. È una funzionalità che permette di impostare policy di sicurezza più rigorose atte a proteggere i dispositivi a maggiore rischio
- **Accelerare i tempi di risposta** agli incidenti tramite avanzati strumenti di visualizzazione, quali le mappe personalizzate delle minacce specifiche della propria organizzazione e le policy one-click per la messa in quarantena dei dispositivi e altre funzioni.
- **Ridurre il carico di lavoro amministrativo** tramite il supporto di un'ampia gamma di servizi di sicurezza di livello enterpris, I servizi disponibili includono informazioni sul malware per dispositivi mobili e sulle sandbox locali, tutti consolidati e gestiti da un'unica console.



Architettura integrata a elevate prestazioni

Le elevate caratteristiche funzionali e le prestazioni di FortiGate gli derivano dall'essere basato su FortiASIC, un'architettura integrata dedicata che permette di disporre del throughput estremamente elevato e della bassa latenza che lo caratterizzano.

L'elevata capacità elaborativa fornita dai processori FortiASIC dedicati permette di effettuare ispezioni approfondite del traffico di nuova generazione e di consolidare sulla medesima piattaforma più funzioni di sicurezza. Agli Asic dedi-

cati si affianca una architettura software che sfrutta l'elaborazione parallela dei percorsi in modo da ottimizzare le risorse hardware e software ad alte prestazioni che gestiscono il flusso dei pacchetti, in modo da massimizzare le capacità di throughput e ridurre al minimo la latenza

La famiglia di appliance FortiGate include poi un insieme di piattaforme flessibili che possono essere distribuite sul perimetro, come Next Generation Firewall (NGFW), sul perimetro del data center, come Firewall per data center (DCFW), presso i segmenti interni (ISFW) o presso i siti remoti di aziende distribuite. Gestite da un unico sistema operativo per la sicurezza della rete, le appliance permettono di consolidare una policy di sicurezza unificata che copra le diverse ubicazioni dei siti da proteggere.



Reportec

2016

