Panoramica del firewall di nuova generazione Palo Alto Networks

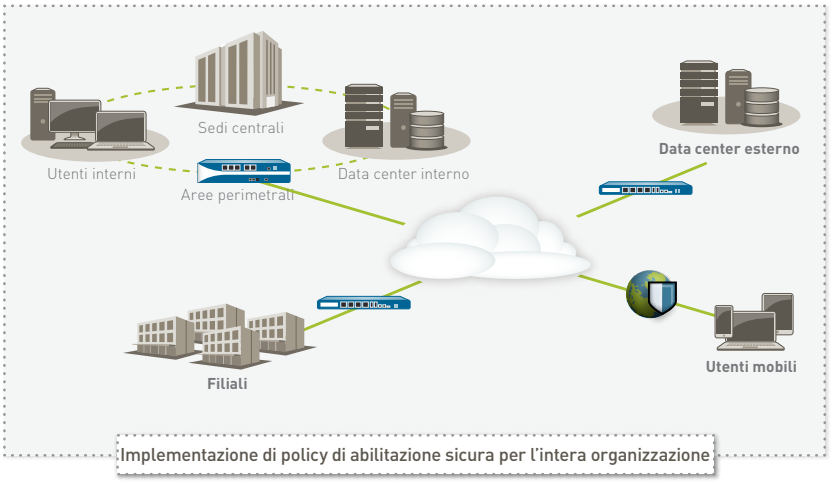
Importanti congiunture e mutamenti nel panorama delle applicazioni e delle minacce nel comportamento degli utenti e nelle infrastrutture di rete hanno costantemente eroso il muro di protezione fino a qualche tempo fa eretto dai tradizionali firewall basati sul controllo delle porte. Gli utenti accedono ad applicazioni di ogni tipo utilizzando una gamma ampissima di tipologie di dispositivi e molto spesso lo fanno semplicemente per lavorare. Nel frattempo, le iniziative di espansione del data center, di virtualizzazione, legate alla mobilità e al cloud costringono a ripensare a come abilitare l'accesso alle applicazioni proteggendo al contempo la rete.

Le tradizionali risposte a questa sfida includono il tentativo di bloccare tutto il traffico applicativo in base a un elenco costantemente aggiornato di tecnologie specifiche oltre al firewall. Restrizioni di questa portata possono tuttavia limitare il business oppure consentire l'ingresso di tutto il traffico applicativo, condizione ugualmente inaccettabile se si considera l'aumento costante dei rischi per il business e per la protezione. Il nocciolo duro del problema è che il firewall tradizionale, basato sul controllo delle porte, seppur dotato di funzionalità aggiuntive di blocco delle applicazioni, non rappresenta un'alternativa praticabile a entrambi gli approcci. Per raggiungere il punto di equilibrio tra blocco totale e accettazione totale del traffico, occorre abilitare le applicazioni in modo sicuro, utilizzando come criteri per la policy di protezione elementi pertinenti al business, quali identità delle applicazioni, utenti che le utilizzano e tipologie di contenuti.

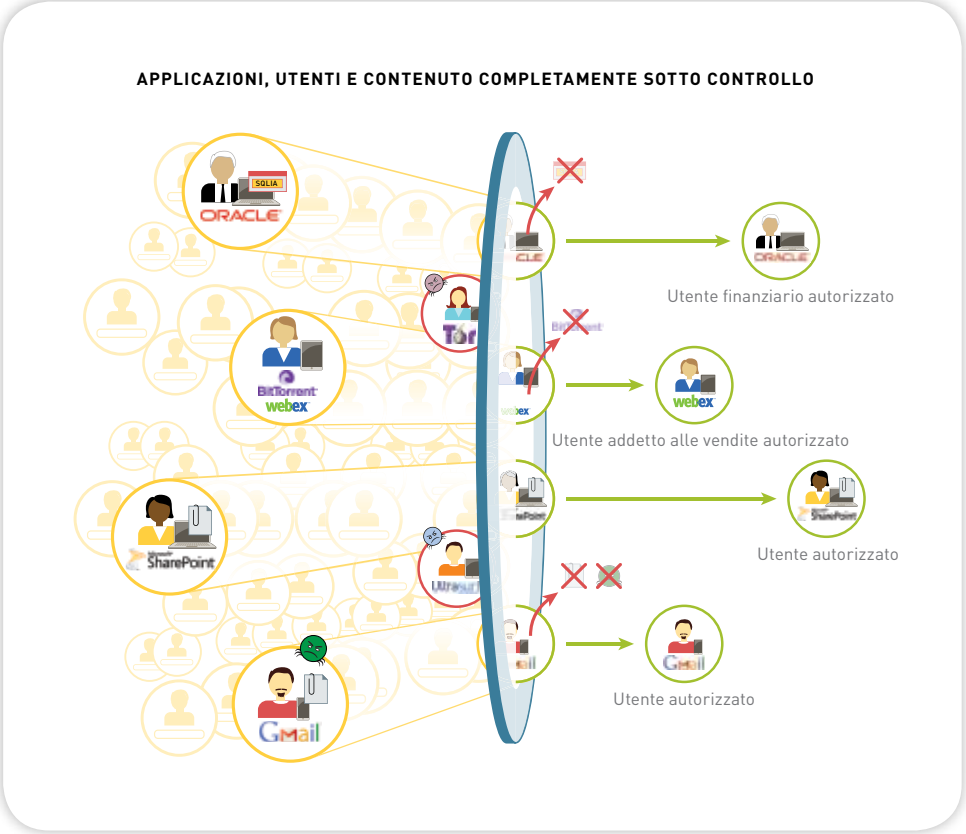
Requisiti fondamentali di abilitazione sicura

- **Identificare le applicazioni, non le porte.** Classificare il traffico, non appena raggiunge il firewall, al fine di determinare l'identità dell'applicazione, indipendentemente da protocollo, crittografia o tattica di evasione. Utilizzare quindi tale identità come base per tutte le policy di protezione.
- **Collegare l'utilizzo dell'applicazione all'identità dell'utente, non all'indirizzo IP, indipendentemente da posizione e dispositivo.** Utilizzare le informazioni su utenti e gruppi raccolte dalle directory aziendali e da altri repository di utenti per implementare policy di abilitazione coerenti per tutti gli utenti aziendali, indipendentemente da posizione e dispositivo.
- **Affrontare tutte le minacce: conosciute e sconosciute.** Prevenire la vulnerabilità a exploit, malware, spyware e URL dannosi conosciuti analizzandone al contempo il traffico, garantendo una protezione automatica contro malware altamente mirati e precedentemente sconosciuti.
- **Semplificare la gestione delle policy.** Abilitare le applicazioni in modo sicuro e ridurre gli interventi amministrativi con l'ausilio di strumenti grafici semplici da utilizzare, un editor unificato delle policy, modelli e gruppi di dispositivi.

Le policy di abilitazione sicura delle applicazioni consentono di migliorare il posizionamento della barriera di protezione, indipendentemente dal punto di implementazione. Per quanto riguarda l'area perimetrale della rete, è possibile ridurre l'impatto delle minacce bloccando una vasta gamma di applicazioni indesiderate e analizzando quelle consentite al fine di rilevare eventuali minacce, conosciute o sconosciute. All'interno del data center, sia esso basato su infrastruttura tradizionale o virtualizzata, l'abilitazione delle applicazioni si traduce nella garanzia di utilizzo delle sole applicazioni del data center e solo da parte di utenti autorizzati, proteggendo i contenuti dalle minacce e affrontando le problematiche per la protezione introdotte dalla natura dinamica delle infrastrutture virtuali. È quindi possibile proteggere filiali e utenti remoti attraverso lo stesso set di policy di abilitazione implementato nella sede centrale, con la massima coerenza.



paloalto NETWORKS
the network security company™



Abilitazione delle applicazioni per potenziare il business

L'abilitazione sicura delle applicazioni grazie ai firewall di nuova generazione Palo Alto Networks consente di affrontare i rischi di business e di protezione associati al costante aumento del numero di applicazioni che attraversano la rete. Abilitando le applicazioni per utenti o gruppi di utenti, locali, mobili e remoti e proteggendo il traffico dalle minacce conosciute e sconosciute, è possibile migliorare il posizionamento della barriera di protezione favorendo al contempo la crescita del business.

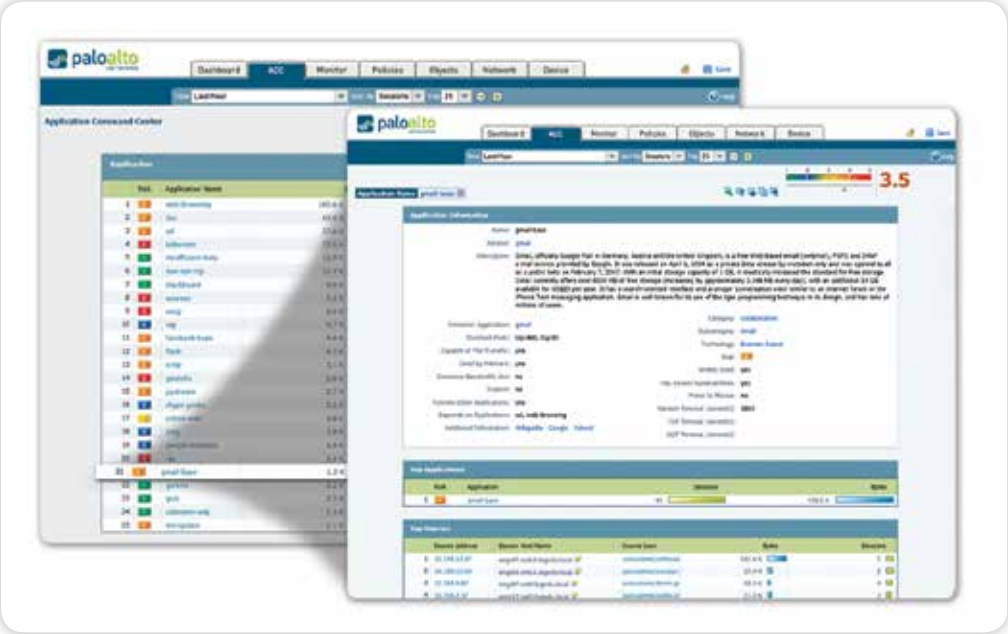
- **Classificazione delle applicazioni attraverso tutte le porte, in qualsiasi momento.** La classificazione precisa del traffico è il nucleo centrale di qualsiasi firewall; i risultati di tale classificazione costituiscono la base della policy di protezione. Al giorno d'oggi, le applicazioni sono facilmente in grado di eludere i controlli dei firewall basati sulle porte: saltano da una porta all'altra, utilizzano crittografia SSL ed SSH, si introducono furtivamente attraverso la porta 80 oppure si servono di porte non standard. App-ID consente di affrontare i limiti di visibilità della classificazione del traffico che compromettono i risultati ottenuti dai firewall tradizionali e lo fa applicando più meccanismi di classificazione ai flussi di traffico non appena questi raggiungono il firewall, determinando l'identità esatta dell'applicazione che attraversa la rete, indipendentemente da porta, crittografia (SSL o SSH) o tecnica di evasione impiegata. Individuare le applicazioni esatte che attraversano la rete, non solo la porta e il protocollo, diventa quindi il fondamento su cui basare tutte le decisioni relative alla policy di protezione. Le applicazioni non identificate, di norma una piccola percentuale di traffico ma pur sempre con un elevato potenziale di rischio, vengono automaticamente categorizzate per una gestione sistematica che può includere il controllo e la verifica della policy, la raccolta e l'analisi delle informazioni sulle minacce, la creazione di un App-ID personalizzato o l'acquisizione di pacchetti per lo sviluppo di App-ID Palo Alto Networks.

- **Integrazione di utenti e dispositivi, non solo di indirizzi IP nelle policy.** La creazione e la gestione di policy di protezione basate sulle applicazioni e sull'identità degli utenti, indipendentemente dal dispositivo o dalla posizione, rappresenta un mezzo più efficace di proteggere la rete rispetto all'affidarsi unicamente al controllo delle porte e degli indirizzi IP. L'integrazione con una vasta gamma di repository di utenti aziendali garantisce la verifica delle identità degli utenti Microsoft Windows, Mac OS X, Linux, Android o iOS che accedono alle applicazioni. Gli utenti in viaggio o che lavorano da posizioni remote vengono protetti con le medesime policy, coerentemente implementate nella rete locale o aziendale. La visibilità combinata e il controllo sull'attività applicativa degli utenti consente di abilitare in modo sicuro l'utilizzo di Oracle, BitTorrent, Gmail o qualsiasi altra applicazione che attraversa la rete, indipendentemente dalla posizione e dalle modalità con cui gli utenti vi accedono.

- **Prevenzione dalle minacce: conosciute e sconosciute.** Per proteggere la rete moderna, occorre affrontare tutta una serie di exploit, malware e spyware conosciuti insieme a minacce mirate completamente sconosciute. Questo processo parte dalla riduzione della superficie di rete vulnerabile agli attacchi, consentendo determinate applicazioni e bloccando tutte le altre attraverso criteri impliciti, con una strategia di blocco totale di tutte le applicazioni non previste, oppure tramite policy esplicite. La prevenzione coordinata delle minacce potrà quindi essere applicata a tutto il traffico consentito, bloccando i siti di malware conosciuti, gli exploit, i virus, gli spyware e le query DNS dannose che attaccano le aree vulnerabili con una singola operazione. I malware personalizzati o altrimenti sconosciuti vengono attivamente analizzati e identificati attraverso l'esecuzione dei file sconosciuti e l'osservazione diretta di oltre 100 comportamenti dannosi in un ambiente sandbox virtualizzato. Nel momento in cui vengono rilevati nuovi malware, viene generata e inviata una firma per il file infetto e il traffico correlato. Tutte le analisi preventive delle minacce utilizzano il contesto completo dell'applicazione e del protocollo, garantendo il rilevamento costante di tutte le minacce anche di quelle che tentano di eludere i controlli di protezione celandosi in tunnel, contenuti compressi o viaggiando su porte non standard.

Flessibilità di implementazione e di gestione

La funzionalità di abilitazione sicura delle applicazioni è disponibile sia su piattaforma hardware costruita ad hoc sia in un fattore di forma virtualizzato. Se si distribuiscono più firewall Palo Alto Networks, in fattori di forma hardware o virtualizzati, è possibile utilizzare Panorama, una piattaforma di gestione centralizzata opzionale che consente di ottenere maggiore visibilità sui pattern di traffico, di implementare le policy, di generare report e di ottenere aggiornamenti dei contenuti da una posizione centrale.



Visibilità delle applicazioni: viste dell'attività delle applicazioni in formato chiaro e intuitivo. Aggiunta e rimozione di filtri per acquisire ulteriori informazioni sulle applicazioni, sulle relative funzioni e sugli utenti che le utilizzano.

Abilitazione sicura delle applicazioni: un approccio end-to-end

L'abilitazione sicura delle applicazioni richiede un approccio completo per proteggere la rete e favorire la crescita del business. Tale approccio parte da una conoscenza approfondita delle applicazioni che viaggiano attraverso la rete, degli utenti che le utilizzano, indipendentemente da piattaforma e posizione, dei contenuti, se presenti, che le applicazioni trasportano. Grazie a una conoscenza più completa dell'attività di rete, è possibile creare policy di protezione più mirate e basate sugli elementi di applicazioni, utenti e contenuti pertinenti all'attività dell'impresa. La posizione dell'utente, la piattaforma utilizzata e il punto di implementazione della policy, perimetrale o in data center tradizionale o virtualizzato, in filiali o presso utenti remoti, sono fattori con un impatto bassissimo o nullo sulla metodologia di creazione della policy. È infatti possibile abilitare qualsiasi applicazione, qualsiasi utente e qualsiasi contenuto.

Conoscenza completa significa policy di protezione più rigorose

Le best practice di protezione impongono una conoscenza più esaustiva dell'attività della rete, fattore fondamentale per implementare policy di protezione più rigorose. Ad esempio, conoscere esattamente quali applicazioni attraversano la rete, piuttosto che il più ampio set di traffico basato sulle porte, consente agli amministratori di consentire esattamente le applicazioni che servono all'impresa e di bloccare quelle indesiderate. La disponibilità di informazioni accurate sull'identità degli utenti, e non solo sugli indirizzi IP, permette di aggiungere ulteriori criteri che consentono di assegnare le policy in modo più specifico.

- L'utilizzo di un set potente di strumenti di visualizzazione grafica, permette agli amministratori di avere un quadro più completo delle attività applicative, del potenziale impatto sulla protezione e di prendere decisioni più informate sulla creazione e l'implementazione delle policy. Le applicazioni vengono classificate costantemente e nel momento in cui il loro stato si modifica, i grafici di riepilogo vengono aggiornati in modo dinamico per mostrare le informazioni tramite un'interfaccia basata su Web estremamente semplice da utilizzare.
- È quindi possibile analizzare applicazioni nuove o poco note in modo rapido con un semplice clic per visualizzarne la descrizione, le caratteristiche comportamentali e gli utenti che le utilizzano.
- Una maggiore visibilità delle categorie di URL, minacce e dati fornisce una panoramica completa e dettagliata dell'attività di rete.
- Le applicazioni sconosciute, di norma una piccola percentuale su ogni rete, ma pur sempre con un elevato potenziale di rischio, vengono categorizzate a scopo di analisi per determinare se siano applicazioni interne, ovvero applicazioni commerciali non ancora identificate, o minacce.

Abilitazione delle applicazioni e riduzione dei rischi

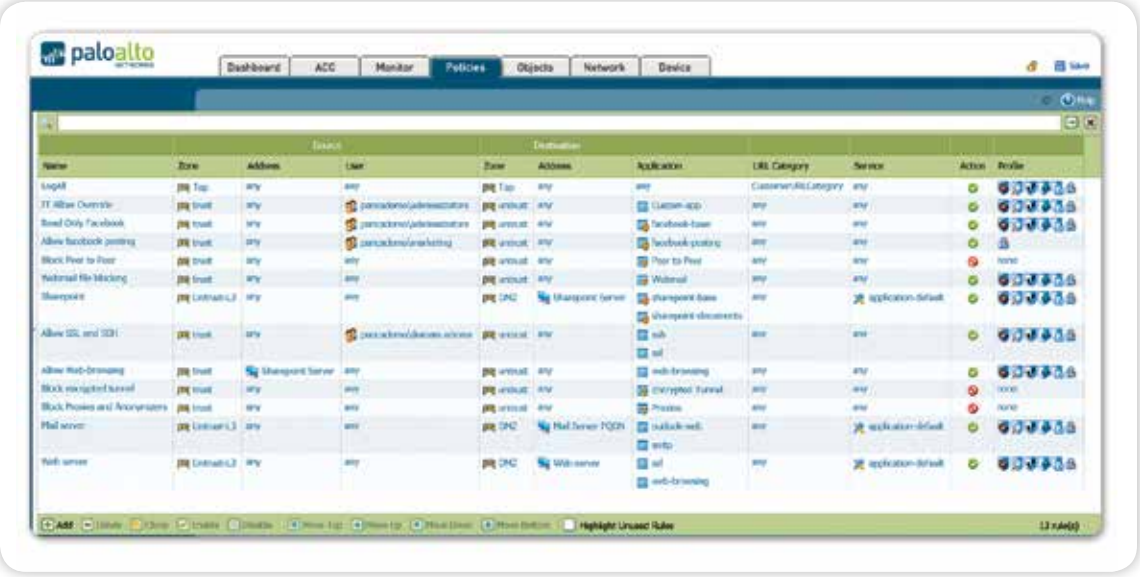
L'abilitazione sicura delle applicazioni si serve di criteri decisionali relativi alle policy che includono le relazioni funzionali applicazione/applicazione, utenti/gruppi e contenuti quale mezzo per raggiungere il punto di equilibrio tra il blocco totale delle applicazioni con impatto negativo sulla crescita del business e l'alternativa a elevato rischio di consentire tutte le applicazioni.

A livello perimetrale, che include filiali, utenti mobili e remoti, le policy di abilitazione si concentrano sull'identificazione di tutto il traffico e sull'accettazione selettiva del traffico sulla base dell'identità degli utenti; successivamente eseguono la scansione del traffico al fine di rilevare minacce. Alcuni esempi di policy:

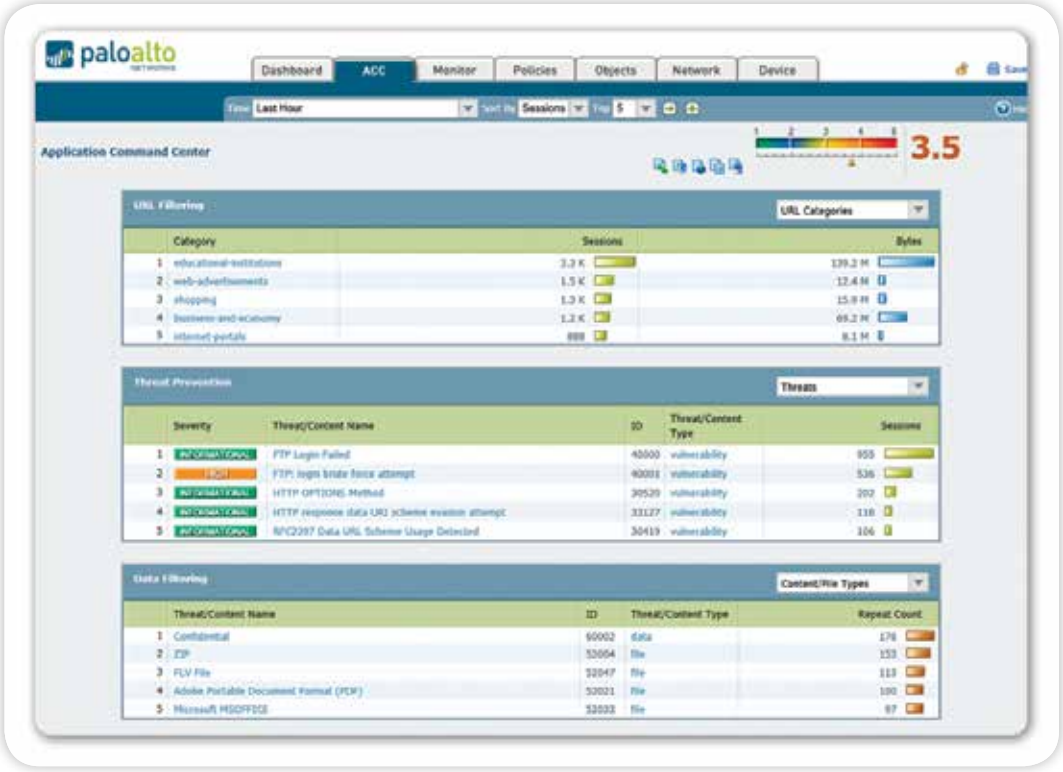
- Limitazione dell'utilizzo della posta su Web e della messaggistica istantanea a una selezione di poche varianti, decrittografia delle applicazioni che utilizzano SSL, analisi del traffico finalizzata al rilevamento di exploit e caricamento di file sconosciuti su WildFire per l'analisi e lo sviluppo di firme.
- Accettazione di applicazioni multimediali e siti Web di streaming ma applicando funzionalità QoS e di prevenzione di malware per limitare l'impatto sulle applicazioni VoIP e proteggere la rete.
- Controllo dell'utilizzo di Facebook consentendo agli utenti di "navigare", bloccando tutti i giochi e i plug-in social di Facebook e consentendo la pubblicazione di post su Facebook solo a scopo di marketing. Scansione di tutto il traffico Facebook al fine di rilevare malware ed exploit.
- Controllo della navigazione in rete consentendo e analizzando il traffico di siti Web correlati all'attività aziendale, bloccando l'accesso a siti Web che esulano ovviamente dall'attività e pilotando l'accesso a siti discutibili attraverso la personalizzazione degli elenchi di pagine bloccate.
- Implementazione di una protezione coerente attraverso la distribuzione trasparente delle stesse policy a tutti gli utenti, locali, mobili o remoti tramite GlobalProtect.
- Utilizzo di una strategia di blocco totale di tutto il traffico non previsto o di blocco esplicito delle applicazioni indesiderate quali P2P, programmi circumventor o del traffico proveniente da Paesi specifici al fine di ridurre il traffico applicativo che introduce rischi per il business e per la protezione.

All'interno del data center, tradizionale, virtualizzato o ibrido, gli esempi di abilitazione si concentrano sulla conferma delle applicazioni, la ricerca di applicazioni non autorizzate e la protezione dei dati.

- Isolamento del repository dei numeri di carte di credito basato su Oracle in una zona di protezione dedicata, controllo degli accessi a gruppi finanziari, confinamento imposto del traffico attraverso le porte standard, analisi del traffico alla ricerca di vulnerabilità applicative.
- Abilitazione del solo gruppo IT per l'accesso al data center utilizzando un set fisso di applicazioni di gestione remota (ad esempio, SSH, RDP, Telnet) attraverso le porte standard.
- Utilizzo di Microsoft SharePoint Administration consentito solo al team di amministrazione e accesso ai documenti Microsoft SharePoint consentito a tutti gli utenti.



Editor unificato delle policy: un aspetto familiare consente la rapida creazione e l'immediata implementazione di policy che controllano applicazioni, utenti e contenuti.



Visibilità sui contenuti e sulle minacce: vista di URL, minacce e attività di trasferimento di file e dati in un formato chiaro e intuitivo. Aggiunta e rimozione di filtri per acquisire ulteriori informazioni sui singoli elementi.

Protezione delle applicazioni abilitate

Per abilitazione sicura delle applicazioni si intende la capacità di consentire l'accesso a determinate applicazioni, di applicare policy specifiche e di bloccare exploit, malware e spyware conosciuti o sconosciuti, di controllare il trasferimento di dati e file e l'attività di navigazione sul Web. Le comuni tattiche di evasione delle minacce, ad esempio il passaggio furtivo attraverso le porte e il tunneling, vengono affrontate grazie all'esecuzione di policy di prevenzione delle minacce basate sul contesto delle applicazioni e dei protocolli generato dai decodificatori App-ID. Al contrario, le soluzioni UTM utilizzano un approccio alla prevenzione delle minacce basato su silos in cui tutte le funzioni, firewall, firewall, IPS, AV e filtraggio URL, eseguono una scansione indipendente del traffico, ovvero senza condividere il contesto. Tale caratteristica rende queste soluzioni più vulnerabili ai meccanismi di evasione.

- **Blocco delle minacce conosciute: anti-virus/anti-spyware IPS e di rete.** Un formato uniforme per le firme e un motore di scansione basato sui flussi consente di proteggere la rete da una vasta gamma di minacce. Le funzionalità IPS (Intrusion Prevention System, sistema di prevenzione delle intrusioni) bloccano gli exploit che attaccano le aree vulnerabili della rete e a livello applicativo, i buffer overflow, gli attacchi DoS e le scansioni delle porte. La protezione basata su anti-virus/Anti-spyware blocca milioni di varianti di malware, nonché ogni tipo di traffico ACC e generato da malware, virus nascosti in file PDF e malware celati in file compressi o nel traffico Web (HTTP/HTTPS compressi). La decrittografia SSL basata su policy per qualsiasi applicazione o porta protegge contro i malware che viaggiano in applicazioni crittografate tramite SSL.
- **Blocco di malware mirati e sconosciuti: Wildfire™.** I malware mirati o sconosciuti vengono identificati e analizzati da WildFire, che esegue direttamente e osserva i file sconosciuti in un ambiente sandbox virtualizzato e basato su cloud. WildFire esegue il monitoraggio di oltre 100 comportamenti dannosi e i risultati vengono inviati immediatamente all'amministratore sotto forma di avviso. Un abbonamento facoltativo a WildFire offre funzionalità di protezione, registrazione e generazione di report avanzate. L'abbonamento offre protezione entro un'ora e nel momento in cui vengono rilevati nuovi malware in qualsiasi punto del mondo, la loro diffusione viene bloccata prima che possa avere un impatto sull'ambiente. Inoltre, tramite l'abbonamento, si ottiene l'accesso alle funzionalità integrate di registrazione e generazione di report di WildFire e la possibilità di utilizzare un'API per l'inoltro di campioni al cloud WildFire a scopo di analisi.

- **Identificazione di host infetti da bot App-ID classifica tutte le applicazioni, attraverso tutte le porte includendo il traffico sconosciuto che spesso espone la rete ad anomalie o minacce.** Il report comportamentale per la botnet mette in correlazione traffico sconosciuto, query URL e DNS sospetti e una vasta gamma di comportamenti di rete inusuali per individuare i dispositivi potenzialmente infetti da malware. I risultati vengono mostrati sotto forma di elenco di potenziali host infetti, che è possibile analizzare ulteriormente quali probabili membri di una botnet.
- **Limitazione di trasferimenti non autorizzati di file e dati.** Le funzionalità di filtraggio dei dati consentono agli amministratori di implementare policy per ridurre i rischi associati ai trasferimenti non autorizzati di file e dati. I trasferimenti di file possono essere controllati attraverso un'analisi approfondita del contenuto dei file (e non della semplice estensione), al fine di stabilire se consentire o meno l'operazione di trasferimento. I file eseguibili, di norma presenti nei download non intenzionali, vengono bloccati per una protezione della rete dalla propagazione di malware invisibili. Infine, le funzionalità di filtraggio dei dati consentono di rilevare e controllare il flusso di pattern di dati riservati (numero di carte di credito, numeri di documenti di identità e pattern personalizzati).
- **Controllo della navigazione sul Web.** Un motore di filtraggio degli URL personalizzabile e completamente integrato consente agli amministratori di implementare policy granulari per il controllo della navigazione sul Web. Tale funzionalità completa la capacità di visibilità delle applicazioni e dell'applicazione di policy di controllo, proteggendo al contempo l'impresa da una vasta gamma di rischi legali, normativi e legati alla produttività. Inoltre le categorie di URL possono essere integrate nelle policy al fine di fornire un'ulteriore granularità nel controllo della decrittografia SSL, nella gestione del QoS e per altre basi di regole.

Gestione e analisi continua

Le best practice di protezione impongono agli amministratori l'obbligo di individuare il giusto punto di equilibrio tra una gestione proattiva del firewall, indipendentemente dal numero di dispositivi coinvolti, e la reattività nell'indagine, nell'analisi e nella generazione di report sugli incidenti di sicurezza.

- **Gestione:** ciascuna piattaforma Palo Alto Networks può essere gestita singolarmente attraverso un'interfaccia a riga di comando (CLI) o tramite un'interfaccia Web avanzata. Per le implementazioni su larga scala, Panorama può essere distribuito con licenza e implementato come soluzione di gestione centralizzata che consente di bilanciare il controllo globale e centralizzato con l'esigenza di flessibilità nell'applicazione delle policy a livello locale grazie a funzionalità quali l'utilizzo di modelli e di policy condivise. Il supporto aggiuntivo per gli strumenti basati su standard quali SNMP e REST API consente l'integrazione con gli strumenti di gestione di terze parti. L'aspetto dell'interfaccia di gestione è identico indipendentemente dal formato utilizzato (Web o Panorama) inoltre il passaggio da un formato all'altro non necessità di alcuna curva di apprendimento. Gli amministratori potranno utilizzare una qualsiasi delle interfacce supportate per apportare modifiche in qualsiasi momento senza doversi preoccupare di problemi legati alla sincronizzazione. L'amministrazione basata su ruoli è supportata da tutte le interfacce di gestione e garantisce funzionalità di assegnazione dei ruoli a persone specifiche.
- **Generazione di report:** è possibile utilizzare i report predefiniti senza modificarli oppure personalizzarli o raggrupparli in un unico report in modo che rispondano a requisiti specifici. Tutti i report possono essere esportati in formato CSV o PDF ed eseguiti e inviati tramite e-mail in base a una determinata pianificazione.
- **Registrazione:** il filtraggio dei log in tempo reale garantisce funzionalità di analisi dettagliate per ciascuna sessione che attraversa la rete. I risultati di tali filtri possono essere esportati in un file CSV o inviati a un server syslog per l'archiviazione offline o a scopo di ulteriore analisi.

Piattaforma virtualizzata o hardware costruita ad hoc

Palo Alto Networks offre una linea completa di piattaforme hardware costruite ad hoc da PA-200, progettate per uffici remoti a PA-5060, progettate per data center ad alta velocità. L'architettura della piattaforma si basa su un motore software a singola operazione e utilizza un'elaborazione basata sulle funzionalità per rete, protezione, prevenzione da minacce e gestione per garantire prestazioni prevedibili. La stessa funzionalità firewall fornita nelle piattaforme hardware è disponibile anche con il firewall virtuale Serie VM che permette di proteggere gli ambienti di elaborazione virtualizzati e basati su cloud utilizzando le stesse policy applicate ai firewall perimetrali o degli uffici remoti.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com