Introduzione ai Next-Generation Firewall

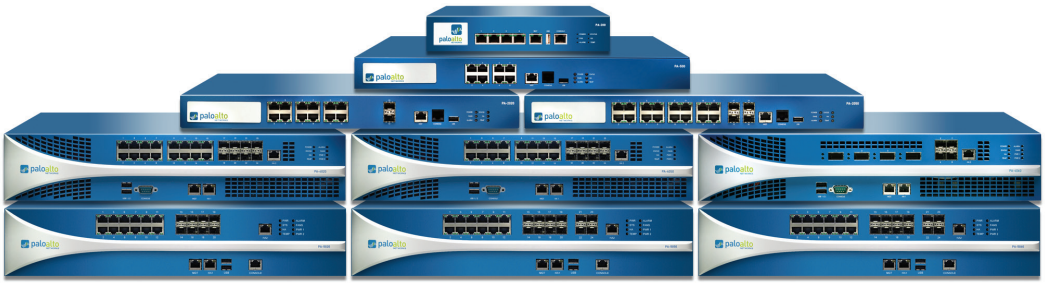
I recenti continui cambiamenti nel comportamento e nei pattern di utilizzo delle applicazioni hanno costantemente eroso la protezione offerta dai firewall tradizionali. Gli utenti accedono a qualsiasi applicazione, ovunque si trovino e tutte le volte che il proprio lavoro lo richiede. Molte di queste applicazioni utilizzano porte non standard, porte dinamiche oppure la cifratura per semplificare l'accesso degli utenti e bypassare il firewall. I cybercriminali traggono il massimo vantaggio da questo uso senza restrizioni per diffondere un nuovo tipo di malware moderno altamente mirato. La conseguenza è che il firewall tradizionale si basa su porte e protocolli non è più in grado di identificare e controllare le applicazioni e le minacce che attraversano la rete.

I tentativi di riottenere il controllo sull'uso delle applicazioni e di proteggere le risorse digitali per tutti gli utenti hanno prodotto policy di sicurezza duplicate locali e remote implementate tramite una serie di firewall-helper stand-alone o male integrati all'interno dei firewall stessi. Approcci di questo tipo generano incoerenza nei criteri e non risolvono il problema legato alla visibilità e al controllo a causa di una classificazione imprecisa o incompleta del traffico, di una gestione poco efficiente e a molteplici processi di scansione che inducono latenza. Il ripristino di visibilità e controllo richiede un approccio totalmente nuovo all'abilitazione sicura delle applicazioni che viene offerta solo da un firewall di nuova generazione.

Requisiti chiave dei Next-Generation Firewall:

- Identificare le applicazioni, non le porte. Identificare la natura dell'applicazione, indipendentemente dal protocollo, dal tipo di cifratura oppure da tattiche evasive e utilizzare l'identità come elemento di base di tutti i criteri di sicurezza.
- Identificare gli utenti, non gli indirizzi IP. Utilizzare le informazioni sugli utenti e sui gruppi provenienti dalle directory aziendali per acquisire visibilità, creare criteri, generare report ed eseguire indagini forensi, indipendentemente dalla posizione geografica dell'utente.
- Bloccare le minacce in tempo reale. Garantire protezione assoluta in tutte le fasi di un attacco, compresi applicazioni pericolose, vulnerabilità, malware, URL ad alto rischio e una vasta gamma di file e contenuti dannosi.
- Semplificare la gestione dei criteri. Abilitare le applicazioni in modo sicuro mediante strumenti grafici intuitivi e un editor di criteri unificato.
- Creare un perimetro logico. Proteggere tutti gli utenti, inclusi i viaggiatori e i pendolari, con una protezione uniforme in grado di estendersi dal perimetro fisico al perimetro logico.
- Fornite throughput multi-gigabit. Combinare hardware e software realizzati ad hoc per permettere performance multi-gigabit e bassa latenza con tutti i servizi abilitati.

I firewall di nuova generazione realizzati da Palo Alto Networks permettono di acquisire una visibilità senza precedenti e assumere il controllo di applicazioni, utenti e contenuti, utilizzando tecnologie di identificazione esclusive: App-ID™, User-ID e Content-ID. Queste tecnologie di identificazione, presenti in ogni firewall di Palo Alto Networks, consentono alle aziende di abilitare l'uso delle applicazioni in modo sicuro, riducendo al contempo e in modo significativo il total cost of ownership (TCO) tramite il consolidamento dei dispositivi.

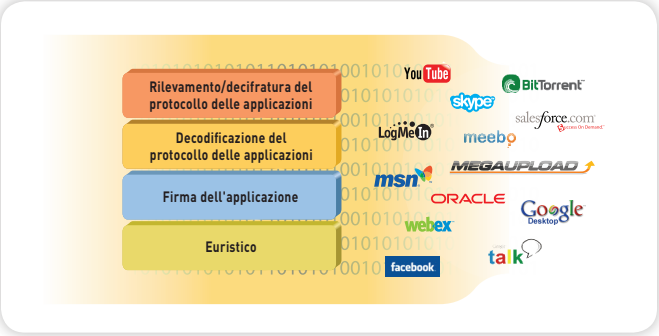


paloalto NETWORKS
the network security company™

App-ID: classificazione di tutte le applicazioni, di tutte le porte, in ogni momento

Una classificazione accurata del traffico è il nucleo centrale di qualsiasi firewall ed essenziale per la scelta del criterio di sicurezza più appropriato. I firewall tradizionali classificano il traffico in base alla porta e al protocollo, un meccanismo che, fino a un certo punto, si è rivelato soddisfacente per la protezione della rete. Oggi, le applicazioni sono in grado di evitare agevolmente un firewall basato sulle porte, saltando da una porta all'altra, utilizzando cifratura SSL e SSH, introducendosi furtivamente attraverso la porta 80 oppure usando porte non standard. App-ID risolve i limiti di visibilità della classificazione del traffico che affliggono i firewall tradizionali applicando molteplici meccanismi di classificazione al flusso di traffico non appena viene rilevato dal firewall, in modo da determinare l'esatta identità delle applicazioni che attraversano la rete.

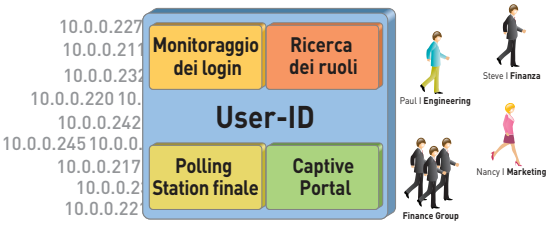
A differenza delle offerte di add-on che si basano esclusivamente sulle firme di stile IPS, implementate dopo la classificazione basata sulle porte, ogni App-ID utilizza automaticamente fino a quattro diversi meccanismi di classificazione per identificare l'applicazione. App-ID monitora continuamente lo stato dell'applicazione, riclassificando il traffico e identificando le diverse funzioni utilizzate. Il criterio di sicurezza stabilisce come gestire l'applicazione: blocco, autorizzazione o abilitazione in sicurezza (scansione e blocco di minacce incorporate, ispezione di trasferimenti file e pattern di dati non autorizzati oppure modellazione utilizzando QoS).



User-ID: abilitazione delle applicazioni in base a utenti e gruppi

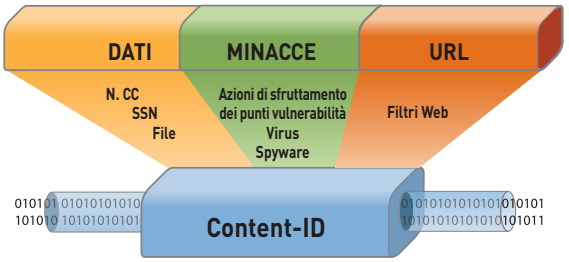
I criteri di sicurezza vengono generalmente applicati in base agli indirizzi IP, ma la natura sempre più dinamica di utenti e ambienti informatici ha dimostrato inefficace l'uso dei solo indirizzi IP come meccanismo di monitoraggio e controllo dell'attività degli utenti. User-ID consente alle organizzazioni di ampliare i criteri di abilitazione delle applicazioni basati su gruppi o utenti per tutti gli utenti di Microsoft Windows, Apple Mac OS X, Apple iOS e Linux.

Le informazioni sugli utenti possono essere raccolte da directory aziendali (Microsoft Active Directory, eDirectory e Open LDAP) e servizi terminal (Citrix e Microsoft Terminal Services) mentre l'integrazione con Microsoft Exchange, il Captive Portal e un'API XML consentono alle aziende di estendere i criteri agli utenti Apple Mac OS X, Apple iOS e UNIX che generalmente si trovano al di fuori del dominio.



Content-ID: protezione del traffico autorizzato

La maggior parte delle applicazioni odierne offre vantaggi significativi ma viene anche utilizzata per distribuire malware e minacce di nuova generazione. Content-ID, associato ad App-ID, offre agli amministratori una soluzione su due fronti per la protezione delle risorse di rete. Dopo aver utilizzato App-ID per identificare e bloccare applicazioni indesiderate, gli amministratori possono abilitare le applicazioni in modo sicuro bloccando lo sfruttamento dei punti di vulnerabilità, malware, virus, botnet moderni e altro malware ed evitandone la distribuzione in rete, indipendentemente da porte, protocolli o tecniche di evasione. Tra i molteplici elementi di controllo offerti da Content-ID è presente un database completo di URL per controllare la navigazione sul Web e le funzioni di filtraggio dei dati.



Abilitazione sicura delle applicazioni

La perfetta integrazione di App-ID, User-ID e Content-ID consente alle organizzazioni di stabilire dei criteri coerenti di abilitazione delle applicazioni, in molti casi, fino al livello funzionale, che vanno oltre i livelli di negazione o autorizzazione di base dell'accesso. Con GlobalProtect™, gli stessi criteri volti a proteggere gli utenti che lavorano in sede possono essere estesi a tutti gli utenti, indipendentemente dalla posizione geografica, creando quindi un perimetro logico per gli utenti esterni alla rete.

I criteri di abilitazione sicura iniziano con l'identità dell'applicazione che viene quindi mappata all'utente associato tramite User-ID, mentre Content-ID esegue la scansione del contenuto del traffico per ricercare minacce, file, pattern di dati e attività Web. Questi risultati vengono visualizzati in Application Command Center (ACC) dove l'amministratore è in grado di conoscere in tempo reale quello che accade nella rete. Successivamente, nell'editor dei criteri, le informazioni visualizzate in ACC relative alle applicazioni, agli utenti e al contenuto possono essere trasformate in criteri di sicurezza appropriati che bloccano le applicazioni non desiderate, mentre autorizzano e abilitano le altre in modo protetto. Infine, è possibile eseguire di nuovo qualsiasi analisi dettagliata, report o indagine forense sulla base di applicazioni, utenti e contenuto.

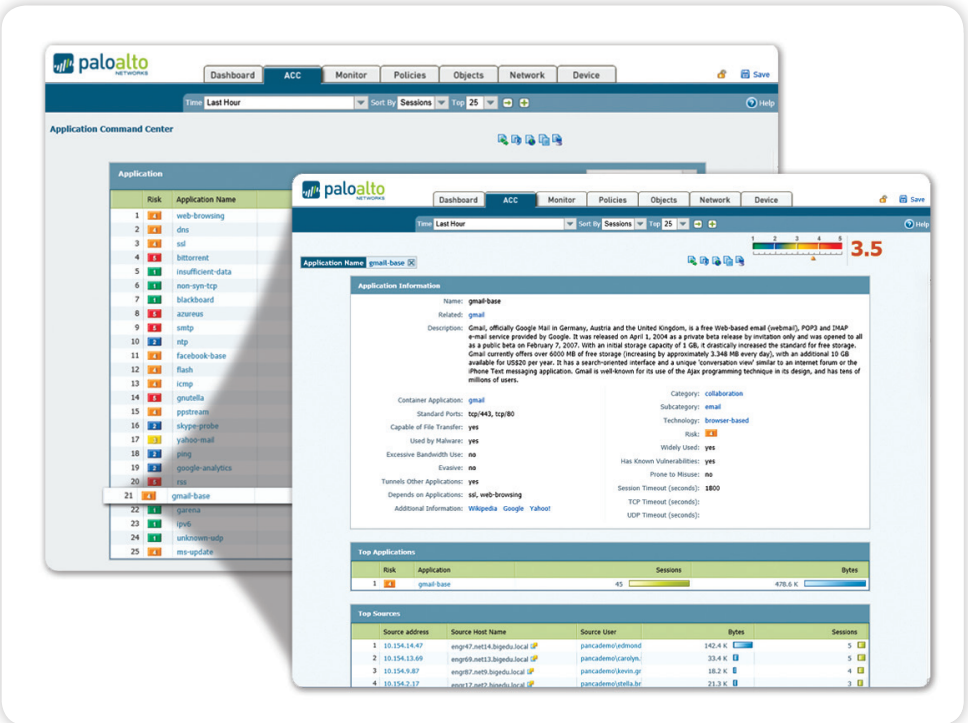
ACC (Application Command Center): la conoscenza è potere

ACC (Application Command Center) riepiloga graficamente il database log per evidenziare le applicazioni che attraversano la rete, gli utenti che le utilizzano e il potenziale impatto sulla sicurezza. ACC viene aggiornato dinamicamente, utilizzando la classificazione continua del traffico eseguita da App-ID. Se un'applicazione passa da una porta all'altra o si comporta in modo diverso, App-ID continua a vedere il traffico, visualizzando i risultati in ACC. Applicazioni nuove o sconosciute visualizzate in ACC possono essere rapidamente esaminate con un singolo clic che mostra una descrizione dell'applicazione, le relative funzioni chiave, le caratteristiche funzionali e gli utenti che la utilizzano. Una maggiore visibilità nelle categorie di URL, minacce e dati fornisce una panoramica completa e dettagliata dell'attività di rete. Grazie ad ACC un amministratore può acquisire rapidamente ulteriori informazioni sul traffico di rete e tradurre tali dati in un criterio di sicurezza più informato.

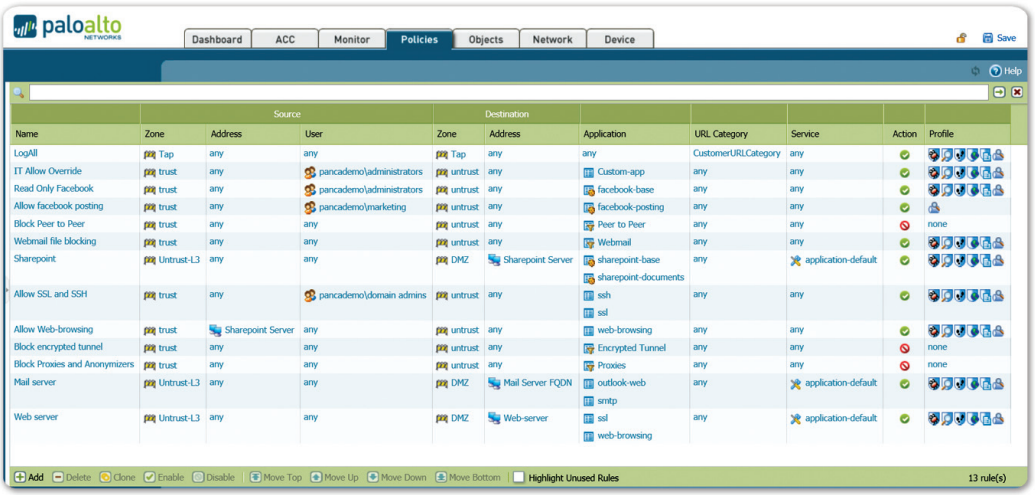
Policy Editor: trasformare la conoscenza in policy di abilitazione protetta

Le informazioni sul tipo di applicazioni che attraversano la rete, sugli utenti che le utilizzano e sul potenziale rischio per la sicurezza consente agli amministratori di distribuire rapidamente criteri di abilitazione basati su applicazioni, funzioni delle applicazioni e porte in modo sistematico e controllato. Le policy possono essere aperte (permetti), moderatamente aperte (autorizza determinate applicazioni e funzioni, quindi applica controlli sul contenuto, shaing, scheduling e così via), o chiuse (blocca). Ecco alcuni esempi:

- Proteggere un database Oracle limitando l'accesso ai gruppi finanziari, forzando il flusso di traffico attraverso le porte standard e ispezionandolo per ricercare eventuali punti di vulnerabilità dell'applicazione.
- Consentire al gruppo IT l'uso esclusivo di un set remoto di applicazioni di gestione (ad esempio, SSH, RDP, Telnet) attraverso le porte standard.
- Definire e applicare un criterio aziendale che consenta e ispezioni l'uso di determinate webmail e applicazioni di Instant Messaging ma bloccando l'uso delle rispettive funzioni di trasferimento file.
- Consentire l'uso esclusivo di Microsoft SharePoint Administration al team di amministrazione e autorizzare tutti gli altri utenti ad accedere a Microsoft SharePoint Documents.



Visibilità dell'applicazione
Visualizzazione dell'attività dell'applicazione in un formato chiaro e di facile lettura. Aggiunta e rimozione dei filtri per acquisire ulteriori informazioni sull'applicazione, sulle relative funzioni e sugli utenti che la utilizzano.



Editor dei criteri unificato
Un aspetto familiare consente la rapida creazione e l'immediata distribuzione dei criteri che controllano applicazioni, utenti e contenuti.

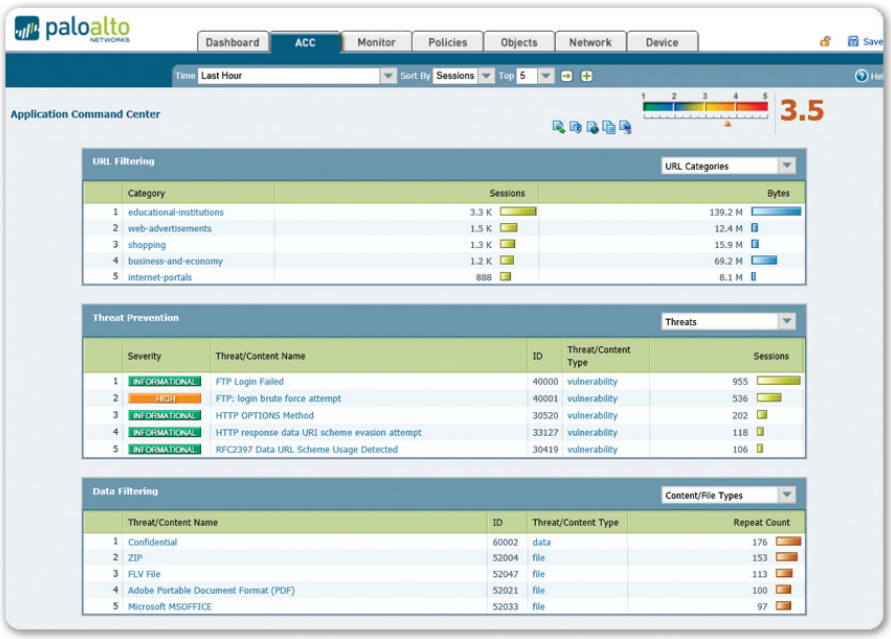
- Distribuire criteri di abilitazione del Web che autorizzano e analizzano il traffico diretto ai siti Web di interesse commerciale, bloccando invece l'accesso a siti evidentemente non correlati al lavoro, e sorvegliano l'accesso ad altri siti tramite pagine di blocco personalizzate.
- Implementare criteri QoS per autorizzare l'uso di siti Web e applicazioni multimediali che richiedono un grande consumo di larghezza di banda, ma limitano l'impatto sulle applicazioni VoIP.
- Decifrare il traffico SSL verso i siti di social network e webmail ed eseguire una scansione per rilevare malware e vulnerabilità.
- Consentire il download di file eseguibili da siti Web non classificati solo dopo la conferma da parte dell'utente per bloccare download di tipo drive-by tramite vulnerabilità di tipo "zero-day".
- Rifiutare tutto il traffico proveniente da determinati paesi o bloccare le applicazioni indesiderate quali condivisione file P2P, programmi circumventor e proxy esterni.

La perfetta integrazione del controllo delle applicazioni basata su utenti e gruppi, unita alla possibilità di sottoporre a scansione il traffico autorizzato per rilevare un'ampia gamma di minacce, permette alle organizzazioni di ridurre drasticamente il numero di modifiche delle policy dovute ai dipendenti che ogni giorno aumentano, si spostano o cambiano settore all'interno dell'azienda.

Editor dei criteri: protezione delle applicazioni abilitate

Abilitare le applicazioni in modo sicuro significa consentire di accedervi, applicando misure mirate di prevenzione delle minacce e criteri specifici di blocco file, dati o filtraggio degli URL. Tutti gli elementi inclusi in Content-ID possono essere applicati in base all'applicazione in uso.

- **Sistema IPS (Intrusion Prevention System):** la protezione dei punti di vulnerabilità integra un ricco set di funzioni IPS (Intrusion Prevention System) per bloccare lo sfruttamento dei punti di vulnerabilità a livello di rete e applicazione, i buffer overflow, gli attacchi DoS e le scansioni delle porte.
- **Antivirus per la rete:** la protezione antivirus basata sui flussi blocca milioni di varianti malware, inclusi i virus dei file in formato PDF e il malware nascosto all'interno di file compressi o nel traffico Web (HTTP/HTTPS compressi). La decifratura SSL basata sui criteri consente alle organizzazioni di proteggersi dal malware che si sposta nelle applicazioni cifrate SSL.
- **Filtri URL:** un database di filtri URL personalizzabili e completamente integrati consente agli amministratori di applicare criteri di browsing Web granulari a complemento dei criteri di visibilità e controllo dell'applicazione, tutelando al contempo l'azienda da una gamma completa di rischi di natura legale, normativa e produttiva.
- **Filtri di file e dati:** le funzioni di filtro dati consentono agli amministratori di implementare criteri che ridurranno i rischi associati ai trasferimenti di file e dati. I trasferimenti e i download di un file possono essere controllati analizzando il file, non soltanto verificandone l'estensione, per stabilire il file deve essere autorizzato. I file eseguibili, in genere presenti nei download di tipo drive-by, possono essere bloccati, proteggendo la rete dalla propagazione di malware invisibile. Infine, le funzioni di filtro dati possono rilevare e controllare il flusso di pattern di dati riservati (numeri di carte di credito e di previdenza sociale).



Visibilità sul contenuto e sulle minacce
Visualizzazione di URL, minacce e attività di trasferimento file e dati in un formato chiaro e di facile lettura. Aggiunta e rimozione di filtri per acquisire ulteriori informazioni sui singoli elementi.

Rilevamento e prevenzione dei malware moderni

I malware si sono evoluti in applicazioni di rete espandibili che forniscono agli autori di attacchi informatici un accesso e un controllo senza precedenti all'interno della rete presa di mira. Con l'aumento della potenza dei malware moderni, è fondamentale che le aziende riescano a rilevare immediatamente queste minacce, addirittura prima che dispongano di una firma. La nuova generazione di firewall di Palo Alto Networks fornisce alle organizzazioni un approccio eterogeneo basato sull'analisi diretta dei file eseguibili e del traffico di rete per proteggere le reti ancora prima che siano disponibili le firme.

- **WildFire™:** grazie a un approccio basato sul cloud, WildFire rileva i file eseguibili dannosi non rilevati dagli anti-virus o IPS osservandone il comportamento in un ambiente virtualizzato sicuro. WildFire cerca azioni dannose nei file eseguibili di Microsoft Windows, ad esempio modifiche di valori del registry o di file del sistema operativo, disattivazione di meccanismi di sicurezza o inserimento di porzioni di codice in processi in esecuzione. Questa analisi diretta consente di identificare in modo rapido e preciso i malware anche nel caso in cui non siano disponibili meccanismi di protezione. I risultati dell'analisi sono immediatamente inviati all'amministratore perchè possa rispondere in maniera tempestiva alla minaccia, e una signature viene automaticamente generata ed inclusa nel prossimo update per proteggere tutti i clienti.
- **Behavioral Botnet Detection:** App-ID classifica tutto il traffico a livello di applicazione, evidenziando in tal modo il traffico sconosciuto sulla rete, che spesso indica la presenza di malware o di altre minacce. Il behavioral report sulle botnet consente di analizzare il comportamento della rete, ed è in grado d indicare la presenza di un'infezione di botnet, ad esempio, la visita ripetuta a siti di malware, l'uso di DNS dinamico, IRC e altri comportamenti potenzialmente sospetti. I risultati visualizzano l'elenco di host potenzialmente infetti che possono essere esaminati come membri possibili di una botnet.

Monitoraggio del traffico: analisi, report e indagini forensi

Le procedure ottimali per garantire la sicurezza impongono agli amministratori di scegliere tra un approccio proattivo, che implica formazione continua e capacità di adattamento per proteggere le risorse aziendali, e un approccio reattivo, che prevede invece investigazioni, analisi e report sugli incidenti legati alla sicurezza. ACC e l'editor dei criteri possono essere utilizzati per applicare in modo proattivo i criteri di abilitazione delle applicazioni, mentre un nutrito set di strumenti di monitoraggio e report fornisce alle organizzazioni i mezzi necessari per analizzare e creare report sui flussi di applicazioni, utenti e contenuti gestiti tramite il firewall di nuova generazione di Palo Alto Networks.

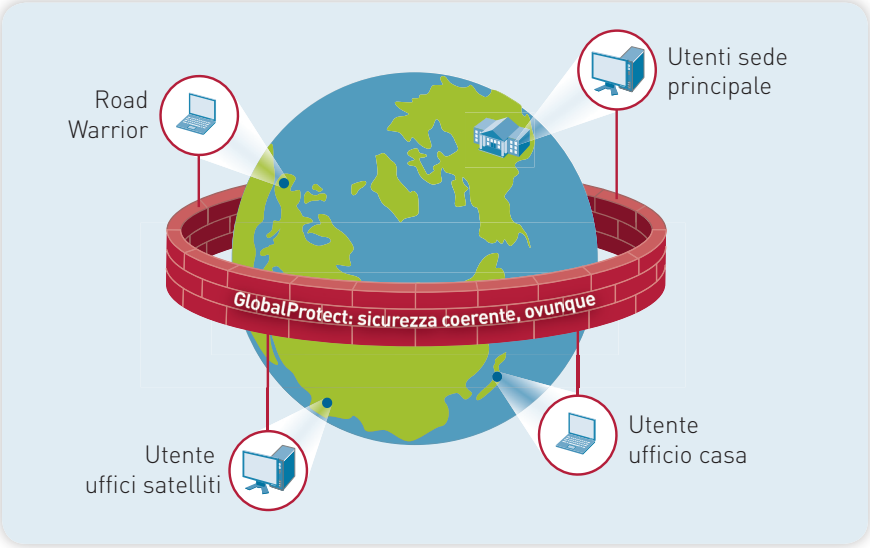
- **App-Scope:** App-scope, integrando la visualizzazione in tempo reale di applicazioni e contenuto fornita da ACC, offre una vista dinamica e personalizzabile dall'utente dell'applicazione, del traffico e dell'attività dannosa nel tempo.
- **Report:** è possibile utilizzare i report predefiniti senza 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.
- **Log:** i filtri di log in tempo reale facilitano una rapida indagine forense in ogni 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 per ulteriori analisi.
- **Strumento di rintracciabilità delle sessioni:** consente di accelerare l'indagine forense o l'analisi degli incidenti mediante una vista centralizzata e correlata in tutti i log relativi a traffico, minacce, URL e applicazioni relative a una singola sessione.

GlobalProtect: sicurezza coerente, ovunque

Le applicazioni non sono gli unici elementi che impongono dei cambiamenti all'azienda. Gli utenti finali si aspettano sempre più di potersi connettere e di poter lavorare ovunque si trovino con qualsiasi dispositivo di loro scelta. Di conseguenza, i team di IT devono estendere la sicurezza a questi dispositivi e andare oltre il perimetro fisico e tradizionale dell'azienda GlobalProtect accetta questa sfida ed estende criteri di sicurezza coerenti a tutti gli utenti, indipendentemente dalla loro posizione geografica e dal dispositivo che utilizzano.

Innanzitutto, GlobalProtect garantisce una connettività protetta a tutti gli utenti grazie a una VPN trasparente che supporta una vasta gamma di dispositivi, tra cui Microsoft Windows, Apple Mac OS X e Apple iOS. Dopo la connessione, il traffico viene classificato in base al firewall, i criteri di abilitazione vengono applicati, il traffico viene sottoposto a scansione per rilevare eventuali minacce e gli utenti sono protetti.

Inoltre, GlobalProtect esegue ulteriori controlli in base allo stato del dispositivo dell'utente finale. Ad esempio, a un utente può essere negato l'accesso a determinate applicazioni o aree riservate della rete se il dispositivo dispone di un antivirus obsoleto o non ha attivato la cifratura del disco. Ciò permette all'IT di abilitare un uso protetto delle applicazioni attraverso una vasta gamma di tipi di dispositivi degli utenti finali, pur conservando un approccio coerente di nuova generazione alla sicurezza.



GlobalProtect
Applicazione di criteri coerenti di abilitazione sicura delle applicazioni per tutti gli utenti, indipendentemente dalla posizione geografica.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054 USA

Telefono: +1.408.573.4000
Vendite: +1.866.320.4788
Assistenza: +1.866.898.9087

www.paloaltonetworks.com