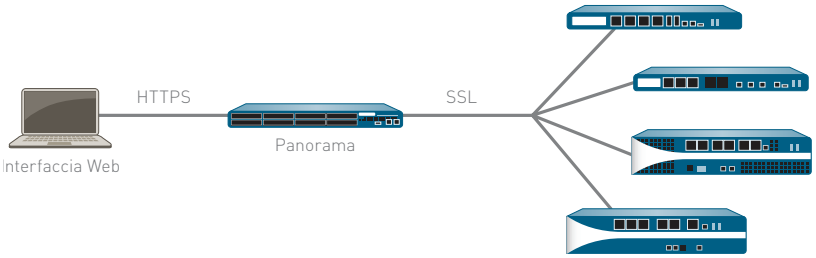
PANORAMA

Panorama consente la gestione centralizzata di policy e dispositivi attraverso una rete di firewall di nuova generazione Palo Alto Networks™.

- Grafici di riepilogo delle applicazioni presenti nella rete, i rispettivi utenti e il potenziale impatto sulla sicurezza.
- Implementazione di policy aziendali a livello centralizzato da utilizzare insieme alle policy locali per la massima flessibilità.
- Possibilità di delegare i ruoli in base a livelli appropriati di controllo amministrativo a livello di dispositivo o a livello globale con una gestione basata sui ruoli.
- Analisi, indagini e generazione di report sul traffico di rete, sugli incidenti di sicurezza e sulle modifiche amministrative a livello centralizzato.



Le grandi imprese di norma distribuiscono diversi firewall attraverso la rete e molto spesso la gestione e il controllo di un ambiente di questo tipo si trasformano in attività estremamente dispendiose a causa delle complessità e delle incoerenze che caratterizzano i singoli dispositivi. Ne consegue un aumento delle attività di amministrazione e dei costi associati.

Panorama garantisce la gestione centralizzata e la visibilità completa dei firewall di nuova generazione Palo Alto Networks. Da una posizione centralizzata, gli amministratori possono controllare tutti i dati relativi ad applicazioni, utenti e contenuti che attraversano i firewall. La conoscenza degli elementi che viaggiano nella rete, insieme alle policy di abilitazione sicura delle applicazioni, consente di massimizzare la protezione e il controllo minimizzando gli interventi amministrativi. È possibile eseguire analisi, generare report, eseguire indagini a livello centralizzato con dati aggregati nel tempo o archiviati sul firewall locale.

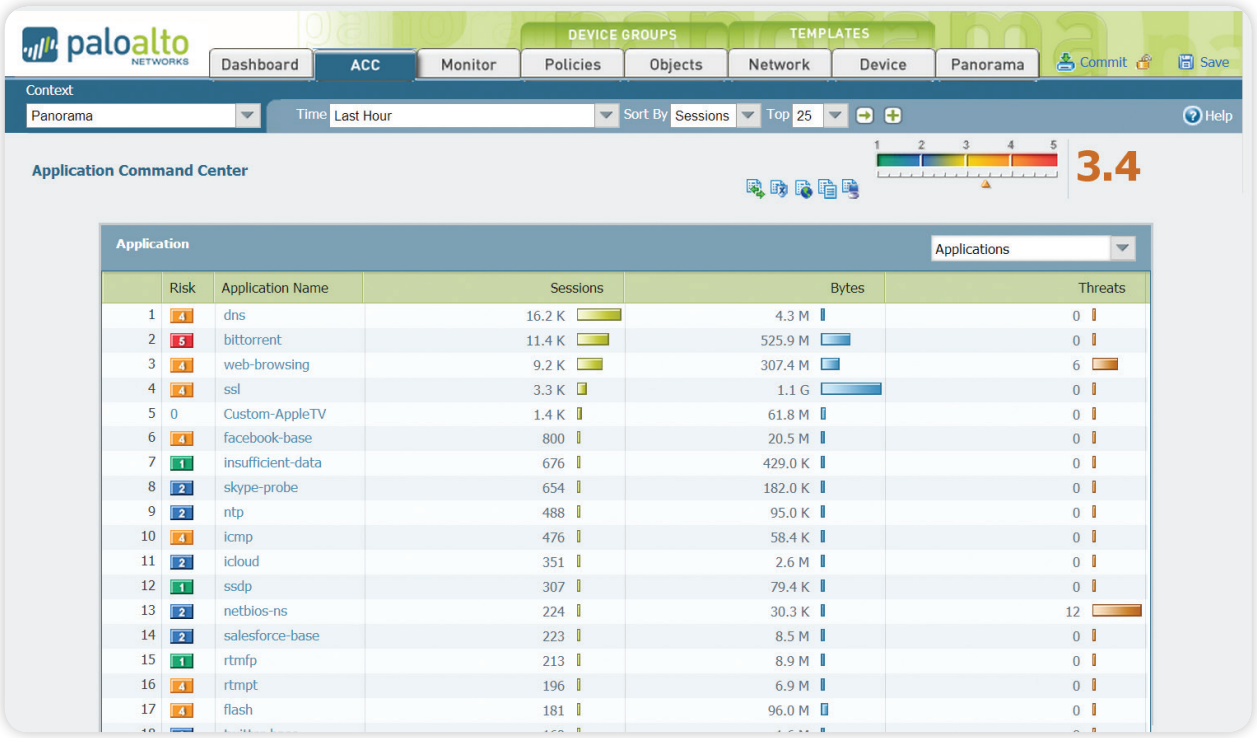
Sia Panorama sia i singoli dispositivi condividono la stessa interfaccia basata su Web riducendo al minimo la curva di apprendimento o i ritardi nell'esecuzione delle operazioni manuali. Palo Alto Networks aderisce a una filosofia di gestione che pone al centro la coerenza, garantendo un vantaggio significativo rispetto alle offerte della concorrenza.

Visibilità a livello centralizzato: ACC (Application Command Center)

Application Command and Control (ACC) di Panorama offre agli amministratori viste in formato grafico di applicazioni, URL, minacce e dati (file e schemi) che attraversano tutti i dispositivi Palo Alto Networks gestiti. ACC raccoglie in modo dinamico i dati da ciascun dispositivo garantendo agli amministratori una vista aggiornata delle applicazioni che si trovano sulla rete, degli utenti che le utilizzano e delle potenziali minacce. Gli amministratori potranno quindi analizzare le applicazioni nuove o poco conosciute con un semplice clic, visualizzandone la descrizione, le principali funzionalità, le caratteristiche e gli utenti che le stanno utilizzando.

Inoltre, dati più approfonditi rispetto alle categorie di URL e alle minacce consentono di ottenere un quadro più completo e dettagliato dell'attività di rete. La visibilità garantita da ACC permette agli amministratori di prendere decisioni informate sull'implementazione delle policy e di rispondere rapidamente alle potenziali minacce alla sicurezza.

paloalto NETWORKS
the network security company™



	Risk	Application Name	Sessions	Bytes	Threats
1	4	dns	16.2 K	4.3 M	0
2	5	bittorrent	11.4 K	525.9 M	0
3	4	web-browsing	9.2 K	307.4 M	6
4	4	ssl	3.3 K	1.1 G	0
5	0	Custom-AppleTV	1.4 K	61.8 M	0
6	4	facebook-base	800	20.5 M	0
7	1	insufficient-data	676	429.0 K	0
8	2	skype-probe	654	182.0 K	0
9	2	ntp	488	95.0 K	0
10	4	icmp	476	58.4 K	0
11	2	icloud	351	2.6 M	0
12	1	ssdp	307	79.4 K	0
13	2	netbios-ns	224	30.3 K	12
14	2	salesforce-base	223	8.5 M	0
15	1	rtmfp	213	8.9 M	0
16	4	rtmpt	196	6.9 M	0
17	4	flash	181	96.0 M	0

Application Command Center offre viste globali e locali del traffico delle applicazioni, complete di informazioni specifiche e dettagliate per avere un quadro più completo dell'attività di rete attuale.

Controllo globale delle policy: abilitazione sicura delle applicazioni

Per abilitazione sicura delle applicazioni si intende la possibilità di consentire l'accesso a determinate applicazioni in base a policy specifiche di prevenzione delle minacce e di filtraggio di file, dati e URL. Panorama facilita l'abilitazione sicura delle applicazioni attraverso l'intera rete di firewall consentendo agli amministratori di gestire le regole da una posizione centralizzata.

Le policy condivise basate su Panorama favoriscono la conformità ai requisiti interni e normativi, mentre le regole locali per i dispositivi garantiscono protezione e flessibilità. Abbinando il controllo amministrativo centralizzato e locale in base a policy e oggetti è possibile raggiungere il necessario equilibrio tra una protezione coerente e un livello di flessibilità su scala globale e locale.

Gli amministratori possono implementare policy che consentono di abilitare in modo sicuro le applicazioni o le funzioni applicative in base agli utenti, tramite l'integrazione dei servizi di directory, mentre i meccanismi di prevenzione delle minacce specifici per le applicazioni proteggono i contenuti e la rete. La possibilità di configurare una singola policy che abiliti in modo sicuro le applicazioni in base agli utenti, e non agli indirizzi IP, permette alle imprese di ridurre significativamente il numero di policy necessarie. Un ulteriore vantaggio dell'integrazione dei servizi di directory è la riduzione sostanziale del carico amministrativo associato all'integrazione, agli spostamenti e alle modifiche dell'organico che possono verificarsi quotidianamente; le policy di protezione restano infatti stabili mentre il personale può essere trasferito da un gruppo all'altro.

Monitoraggio del traffico: analisi, generazione di report e indagini

Panorama utilizza lo stesso set di potenti strumenti di monitoraggio e generazione di report disponibile a livello di gestione locale dei dispositivi e permette una visibilità più approfondita tramite una vista aggregata delle attività. Mentre gli amministratori inviano query ai registri e generano i report, Panorama estrae in modo dinamico i dati più attuali direttamente dai firewall gestiti o dai registri inoltrati a Panorama. L'accesso alle informazioni più recenti per tutti i dispositivi consente agli amministratori di affrontare gli incidenti di sicurezza e di agire in modo proattivo per proteggere le risorse aziendali.

- **Visualizzatore dei registri:** gli amministratori di Panorama hanno la possibilità di visualizzare rapidamente le attività di registro per uno o per tutti i dispositivi, utilizzando funzionalità dinamiche di filtraggio dei registri, accessibili con un semplice clic su un valore di una cella o tramite l'utility di creazione di espressioni per definire il criterio di ordinamento. È inoltre possibile salvare i risultati per query future o esportarli a scopo di ulteriore analisi.
- **Generazione di report personalizzati:** è possibile utilizzare i report predefiniti senza modificarli oppure personalizzarli o raggrupparli in un unico report in modo che rispondano a requisiti specifici.
- **Report dell'attività degli utenti:** i report dell'attività degli utenti disponibili in Panorama consentono di visualizzare le applicazioni utilizzate, le categorie di URL, i siti Web e gli URL visitati rispetto a un periodo di tempo specifico e per singoli utenti. Panorama genera i report in base a una vista aggregata dell'attività degli utenti, indipendentemente dal firewall, dall'IP o dal dispositivo utilizzato.

Architettura di gestione di Panorama

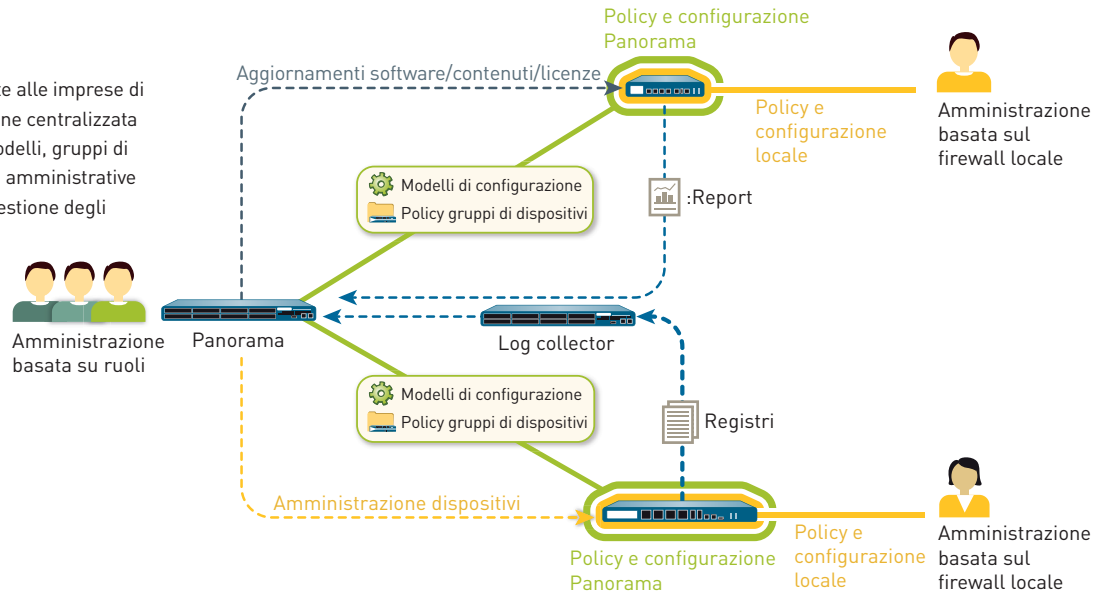
Panorama consente alle imprese di gestire i firewall Palo Alto Networks in base a un modello che garantisce il controllo a livello centrale e locale. Panorama offre una serie di strumenti per l'amministrazione centralizzata.

- **Modelli:** Panorama gestisce la configurazione comune di dispositivi e di rete tramite modelli. È possibile utilizzare i modelli per gestire la configurazione a livello centrale quindi implementare le modifiche tramite un'operazione di pushing su tutti i firewall gestiti. Questo approccio permette di evitare di implementare ripetutamente le stesse modifiche sui singoli firewall per i diversi dispositivi. Un esempio di questo tipo di utilizzo è il pushing di impostazioni comuni di server DNS e NTP per centinaia di firewall, piuttosto che apportare la stessa modifica dispositivo per dispositivo.
- **Gruppi di dispositivi:** Panorama gestisce policy e oggetti comuni tramite gruppi di dispositivi. I gruppi di dispositivi vengono utilizzati per gestire a livello centralizzato le basi di regole per vari dispositivi che condividono requisiti comuni. Ad esempio, è possibile raggruppare i dispositivi in gruppi a livello geografico (ad esempio Europa e Nord America) o a livello funzionale (ad esempio in base al perimetro o al data center). All'interno dei gruppi di dispositivi, i sistemi virtuali vengono interpretati come dispositivi singoli allo stesso livello dei firewall fisici. Questo consente di condividere una base di regole comune tra diversi sistemi virtuali su un dispositivo.

  È quindi possibile implementare policy condivise per un controllo centralizzato garantendo comunque all'amministratore del firewall l'autonomia per apportare specifiche modifiche in risposta ai requisiti locali. A livello del gruppo di dispositivi, gli amministratori hanno la facoltà di creare policy condivise definite come primo set di regole (pre-regole) e ultimo set di regole (post-regole) da valutare rispetto ai criteri di corrispondenza. Le pre-regole e le post-regole possono essere visualizzate su un firewall gestito, ma modificate solo tramite Panorama all'interno del contesto dei ruoli amministrativi definiti. Le regole per i dispositivi locali (quelle che si trovano tra le pre-regole e le post-regole) possono essere modificate sia dall'amministratore locale sia dall'amministratore di Panorama che accede da un contesto di firewall locale. Inoltre, è possibile utilizzare oggetti condivisi definiti da un amministratore di Panorama e fare in modo che le regole per i dispositivi, gestite a livello locale, facciano riferimento a questi.
- **Amministrazione basata su ruoli:** è possibile utilizzare criteri di amministrazione basata su ruoli per delegare l'accesso amministrativo a livello di funzionalità (abilitato, sola lettura, disabilitato e nascosto) a diversi membri del personale. In quest'ottica è possibile garantire a determinati amministratori l'accesso appropriato alle operazioni pertinenti alle rispettive mansioni, impostando altre operazioni come nascoste o accessibili in sola lettura. Un modo per implementare questo tipo di controllo degli accessi è quello di definire diversi ruoli per responsabilità e attività diverse nell'impresa, ad esempio amministratori di protezione e amministratori di rete. Tutte le modifiche apportate dagli amministratori vengono registrate insieme alla data e all'ora, all'amministratore, all'interfaccia di gestione utilizzata (Web UI, CLI, Panorama), al comando eseguito o all'azione intrapresa.
- **Gestione degli aggiornamenti di software, contenuti e licenze.** Con la crescita delle dimensioni delle implementazioni, molte imprese vogliono la sicurezza che gli aggiornamenti siano inviati attraverso i vari flussi in modo organizzato. Ad esempio, i team di protezione potrebbero preferire la qualificazione centralizzata degli aggiornamenti software prima della distribuzione tramite Panorama a tutti i firewall di produzione. Con Panorama è possibile operare una gestione centralizzata dei processi di aggiornamento che riguardano software, contenuti (aggiornamenti di applicazioni, firme antivirus, firme di minacce, database di filtraggio di URL eccetera) e licenze.

Tramite l'uso di modelli, gruppi di dispositivi, funzioni amministrative basate su ruoli e gestione degli aggiornamenti, le imprese possono delegare gli accessi appropriati a tutte le funzioni di gestione; strumenti di visualizzazione, creazione di policy, generazione di report e registrazione possono essere distribuiti a livello globale e locale.

Panorama consente alle imprese di bilanciare la gestione centralizzata e locale tramite modelli, gruppi di dispositivi, funzioni amministrative basate su ruoli e gestione degli aggiornamenti.



Flessibilità di implementazione

Le imprese possono scegliere di implementare Panorama come appliance hardware o come appliance virtuale.

Appliance hardware

Le imprese che preferiscono implementare Panorama su hardware dedicato ad alte prestazioni o che desiderano separare la gestione e le funzioni di registrazione di Panorama per grandi volumi di dati di registro, possono scegliere l'appliance hardware M-100 per soddisfare le loro esigenze. È possibile implementare Panorama su piattaforma M-100 nei seguenti modi.

- **Centralizzato:** in questo scenario, tutte le funzioni di gestione e registrazione di Panorama vengono consolidate in un singolo dispositivo (con opzione per l'alta disponibilità).
- **Distribuito:** se l'impresa preferisce separare le funzioni di gestione e registrazione per i vari dispositivi, questa configurazione consente di suddividere le funzioni tra manager e log collector.
  - **Manager di Panorama:** il manager di Panorama è responsabile della gestione delle operazioni associate alla configurazione di policy e dispositivi per tutti i dispositivi gestiti. Il manager non archivia i dati di registro in locale, ma li gestisce attraverso log collector separati. Analizza quindi i dati archiviati nei log collector per la generazione di report centralizzata.
  - **Log collector di Panorama:** le imprese con registri di elevato volume e requisiti di conservazione rigorosi possono scegliere di implementare i dispositivi log collector dedicati di Panorama che consentono di aggregare le informazioni di registro da più firewall gestiti.

La separazione dei ruoli di gestione e raccolta di registri consente di ottimizzare l'implementazione per soddisfare i requisiti di scalabilità, organizzativi e legati alle distanze geografiche.

Appliance virtuale

È possibile implementare Panorama come appliance virtuale su piattaforma VMware ESX(i), in modo da supportare le iniziative di virtualizzazione dell'impresa e consolidare lo spazio in rack talvolta limitato o eccessivamente costoso nel data center. Sono disponibili due metodi di implementazione per l'appliance virtuale.

- **Centralizzato:** tutte le funzioni di gestione e registrazione di Panorama vengono consolidate in un appliance virtuale (con opzione per l'alta disponibilità).
- **Distribuito:** la funzionalità di raccolta di registri distribuita di Panorama supporta la combinazione di appliance hardware e virtuale.
  - **Manager di Panorama:** l'appliance virtuale funge da manager di Panorama ed è responsabile della gestione delle operazioni associate alla configurazione di policy e dispositivi per tutti i dispositivi gestiti.
  - **Log collector di Panorama:** i log collector di Panorama consentono di ridurre il carico nelle operazioni intensive di raccolta di registri e di elaborazione ed è possibile implementarli utilizzando la piattaforma M-100. Non è possibile utilizzare l'appliance virtuale come log collector di Panorama.

Grazie alla scelta tra implementazione come piattaforma hardware o virtualizzata e la possibilità di combinare o separare le funzioni di Panorama, si ottiene massima flessibilità nella gestione di più firewall Palo Alto Networks in un ambiente di rete distribuito.

SPECIFICHE DI PANORAMA

Numero di dispositivi supportati	Fino a 1.000
Alta disponibilità	Active/Passive
Autenticazione amministratori	Database locale RADIUS

SPECIFICHE DELL'APPLIANCE DI GESTIONE M-100

I/O

- (1) 10/100/1000, (3) 10/100/1000 (per utilizzo futuro), (1) porta seriale console DB9

STORAGE (2 OPZIONI)

- M-100 con 1 TB in RAID: 2 x HDD certificati da 1 TB in RAID per 1 TB di storage RAID
- M-100 da 4 TB in RAID: 8 x HDD certificati da 1 TB in RAID per 4 TB di storage RAID

ALIMENTAZIONE/CONSUMO MASSIMO

- 500 W/500 W

BTU/ORA MASSIMI

- 1.705 BTU/ora

TENSIONE IN INGRESSO (FREQUENZA IN INGRESSO)

- da 100 a 240 VCA (da 50 a 60 Hz)

CONSUMO MASSIMO DI CORRENTE

- 10 A a 100 VCA

TEMPO MEDIO TRA I GUASTI (MTBF)

- 14,5 anni

MONTABILE IN RACK (DIMENSIONI)

- Rack standard a 1 U, da 19 poll. (1,75" H x 23" L x 17.2" P)

PESO (DISPOSITIVO AUTONOMO/COME FORNITO)

- 12,1 kg/15,9 kg

SICUREZZA

- UL, CUL, CB

EMI

- FCC Classe A, CE Classe A, VCCI Classe A

AMBIENTE

- Temperatura di esercizio: da 5° a 40° C
- Temperatura non di esercizio: da -40° a -65° C

SPECIFICHE DELL'APPLIANCE VIRTUALE

REQUISITI SERVER MINIMI

- Disco rigido da 40 GB
- RAM da 4 GB
- Quad-Core CPU (2GHz+)

SUPPORTO VMWARE

- VMware ESX 4.1 o versioni successive

BROWSER SUPPORTATI

- IE v7 o versioni successive
- Firefox v3.6 o versioni successive
- Safari v5.0 o versioni successive
- Chrome v11.0 o versioni successive

STORAGE REGISTRI

- VMware Virtual Disk: massimo 2 TB
- NFS

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