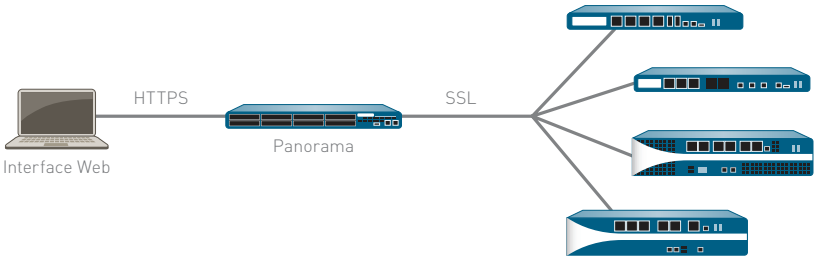
PANORAMA

Panorama permet une gestion centralisée des stratégies et des dispositifs sur un réseau de pare-feu nouvelle génération Palo Alto Networks.

- Visualisez un résumé graphique des applications et des utilisateurs présents sur le réseau et de leur impact potentiel sur la sécurité.
- Déployez des stratégies d'entreprise centralisées pouvant être utilisées conjointement à des stratégies locales pour une flexibilité maximale.
- Attribuez des niveaux de contrôle administratif appropriés localement ou globalement grâce à la gestion basée sur les rôles.
- Analysez et examinez de manière centralisée le trafic réseau, les incidents de sécurité et les modifications administratives, puis générez des rapports.



Les grandes entreprises ont pour habitude de déployer un grand nombre de pare-feu sur leur réseau, rendant par la même la gestion de ces pare-feu particulièrement contraignante en raison des spécificités de chaque dispositif. Il en résulte un alourdissement des procédures administratives et une augmentation des coûts.

Panorama permet une gestion centralisée des pare-feu nouvelle génération de Palo Alto Networks. Depuis un emplacement central, les administrateurs peuvent accéder aux informations des applications, des utilisateurs et du contenu qui transitent par les pare-feu. Cette connaissance des éléments du réseau associée aux stratégies d'utilisation sécurisée des applications garantissent une protection et un contrôle optimums tout en réduisant les contraintes administratives. Les administrateurs peuvent analyser de manière centralisée les données agrégées ou celles stockées dans les pare-feu locaux et générer des rapports.

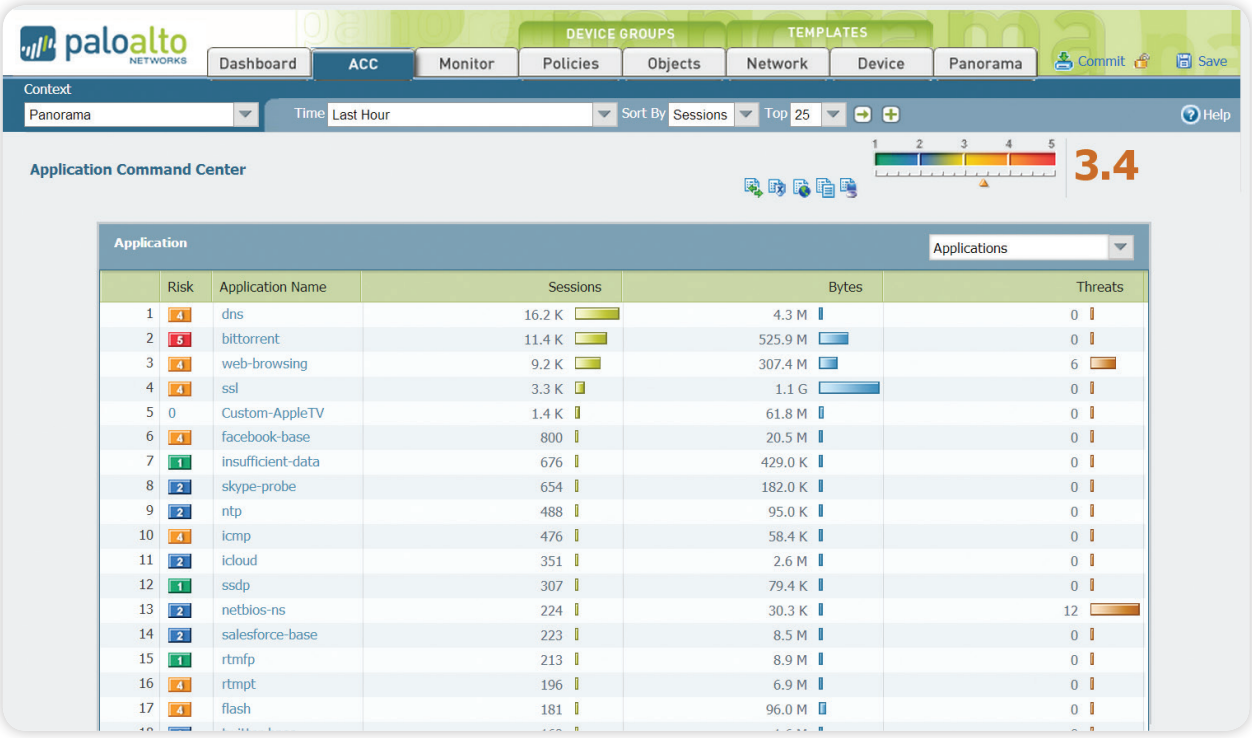
Panorama et les différents équipements partagent la même interface Web, réduisant ainsi le temps de prise en main de l'outil. Palo Alto Networks adopte une philosophie de gestion axée sur la cohérence, ce qui est un avantage important face à la concurrence.

Visibilité centrale : Centre de contrôle des applications ACC (Application Command Center)

L'utilisation de l'ACC dans Panorama offre aux administrateurs une visibilité des applications, URL, menaces et données (fichiers et modèles) qui transitent par les différents boîtiers Palo Alto Networks gérés. L'ACC collecte de manière dynamique les données des différents boîtiers afin de fournir aux administrateurs une vue actualisée des applications présentes sur le réseau, des utilisateurs qui s'en servent et des menaces de sécurité potentielles. D'un simple clic, les administrateurs peuvent obtenir une description des applications nouvelles ou inconnues, de leurs principales fonctionnalités, de leurs caractéristiques comportementales, et découvrir qui les utilise.

Des données complémentaires sur les catégories d'URL et les menaces fournissent une vision complète et globale de l'activité du réseau. La visibilité offerte par l'ACC permet aux administrateurs de prendre les décisions stratégiques appropriées et de réagir rapidement aux menaces de sécurité.

paloalto NETWORKS
the network security company™



L'ACC offre une vue consolidée globale et locale du trafic par application, avec des fonctionnalités d'exploration permettant d'en savoir plus sur l'activité en cours.

Contrôle stratégique global : utilisation sécurisée des applications

L'utilisation sécurisée des applications consiste à autoriser l'accès à des applications spécifiques en appliquant des politiques de prévention des menaces et de filtrage des fichiers, données ou URL. Panorama facilite l'utilisation sécurisée des applications sur l'ensemble du réseau de pare-feu en permettant aux administrateurs de gérer les règles depuis un emplacement central.

Les stratégies de partage basées sur Panorama favorisent le respect des exigences internes ou réglementaires tandis que les règles des dispositifs locaux confèrent une certaine souplesse d'administration. La combinaison d'un contrôle administratif central et local sur les politiques et les objets permet d'atteindre un équilibre entre la cohérence de la sécurité au niveau global et le maintien de la flexibilité au niveau local.

L'intégration aux services d'annuaires permet aux administrateurs de déployer des politiques d'utilisation sécurisée des applications en fonction des utilisateurs tandis que des stratégies de prévention des menaces spécifiques aux applications protègent les contenus et le réseau. La possibilité de définir une stratégie unique qui active de manière sécurisée les applications en fonction des utilisateurs, et non des adresses IP, permet aux entreprises de réduire considérablement le nombre de politiques requises. Un autre avantage de l'intégration de services d'annuaires est la réduction spectaculaire des frais administratifs liés aux ajouts, déplacements et changements d'employés susceptibles de se produire quotidiennement : les stratégies de sécurité ne changent pas lorsque les employés sont transférés d'un groupe à un autre.

Surveillance du trafic : analyse, création de rapports et investigation

Panorama utilise le même jeu d'outils puissants de surveillance et de génération de rapports que celui disponible pour la gestion des boîtiers au niveau local et accroît la visibilité en offrant une vue agrégée des activités. Lorsque les administrateurs soumettent des requêtes de journal de log et génèrent des rapports, Panorama extrait de manière dynamique les données les plus récentes directement des pare-feu gérés ou des journaux qui lui sont transmis. L'accès aux informations les plus récentes sur tous les boîtiers permet aux administrateurs de régler les incidents de sécurité et de prendre des mesures proactives pour protéger les actifs de l'entreprise.

- **Visualiseur de journaux :** Les administrateurs de Panorama peuvent facilement visualiser les activités consignées dans les journaux d'un ou plusieurs boîtiers grâce aux fonctions de filtrage dynamique des journaux : il leur suffit pour cela de définir les critères de tri en cliquant sur la valeur d'une cellule ou en utilisant l'éditeur de requêtes. Les résultats peuvent être enregistrés pour exécuter de futures requêtes ou être exportés en vue d'une analyse plus approfondie.
- **Génération de rapports personnalisés :** Des rapports prédéfinis au format pdf peuvent être générés, personnalisés ou consolidés dans un rapport composite afin de répondre à des exigences particulières.
- **Rapports sur l'activité des utilisateurs :** Panorama fournit un rapport sur l'activité des utilisateurs répertoriant les applications utilisées, les catégories d'URL et les sites Web visités, ainsi que toutes les URL visitées sur une période donnée. Panorama génère ces rapports en utilisant une vue agrégée de l'activité des utilisateurs, indépendamment du type de pare-feu, de l'adresse IP ou du dispositif.

Architecture de gestion de Panorama

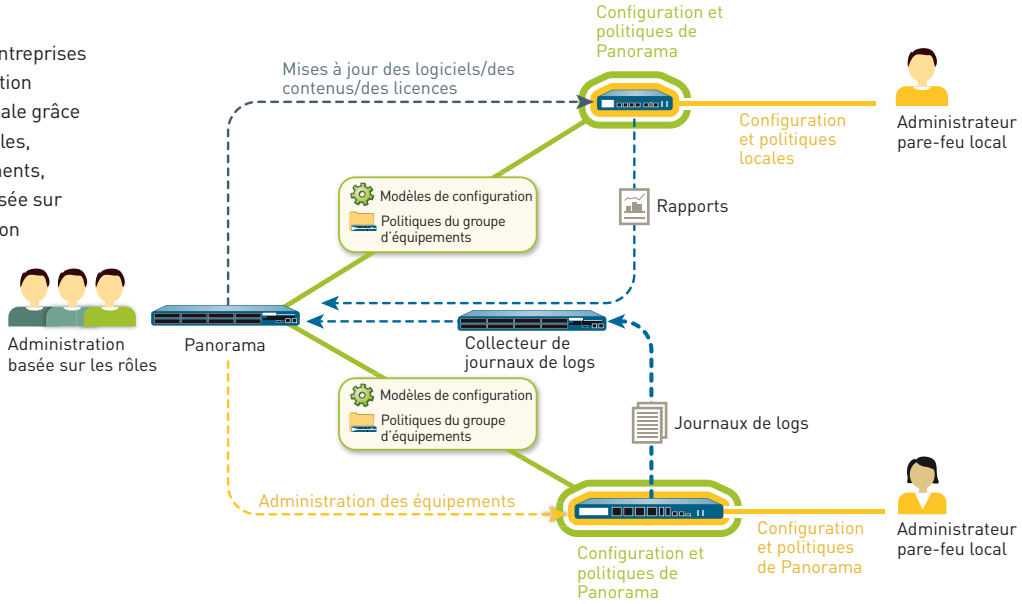
Panorama permet aux entreprises de gérer leurs pare-feu Palo Alto Networks à l'aide d'un modèle offrant à la fois une supervision globale et un contrôle local. Panorama fournit des outils de gestion centralisée tels que :

- **Modèles :** Panorama gère la configuration courante du réseau et des boîtiers au moyen de modèles. Ceux-ci peuvent être utilisés pour gérer la configuration de manière centralisée, puis pour répercuter les changements sur tous les pare-feu gérés. Cette approche permet d' effectuer la même modification sur l'ensemble des pare-feu d'un parc. Un exemple de ce type d'utilisation consiste à répercuter des paramètres de serveur DNS et NTP communs sur des centaines de pare-feu, plutôt que d'effectuer la même modification individuellement sur chaque boîtier.
- **Groupes d'équipements :** Panorama gère les politiques de sécurité et les objets courants via des groupes d'équipements. L'utilisation de ces groupes permet de gérer de manière centralisée les éléments de base des règles d'un grand nombre d'équipements ayant des exigences communes. Les équipements peuvent par exemple être regroupés par zone géographique (ex. : Europe et Amérique du Nord) ou fonctionnalité (ex. : périmètre ou data center). Au sein des groupes d'équipements, les systèmes virtuels sont traités en tant qu'équipements individuels, au même niveau que les pare-feu physiques. Ceci permet le partage d'éléments de base de règles communs entre plusieurs systèmes virtuels d'un même équipement.

  Les entreprises peuvent partager des politiques permettant un contrôle centralisé des pare-feu tout en donnant aux administrateurs la possibilité d'effectuer des ajustements spécifiques pour répondre aux contraintes locales. Au niveau des groupes d'équipements, les administrateurs peuvent créer des politiques partagées définies comme premier ensemble de règles (pré-règles) et dernier ensemble de règles (post-règles) à évaluer par rapport aux critères. Les pré- et post-règles peuvent être visualisées sur un pare-feu géré, mais sont modifiables uniquement dans le contexte des rôles administratifs définis dans Panorama. Les règles locales des équipements (qui se situent sur le boîtier local entre les pré- et post-règles) peuvent être modifiées par l'administrateur local ou par un administrateur Panorama intervenant dans le contexte du pare-feu local. En outre, une entreprise peut utiliser des objets partagés définis par un administrateur Panorama et auxquels les règles des équipements gérés localement peuvent faire référence.
- **Gestion basée sur les rôles :** Les entreprises peuvent utiliser la gestion basée sur les rôles pour attribuer l'accès administratif des fonctionnalités (activée, en lecture seule ou désactivée et non visible) aux différents membres du personnel. Il est possible d'accorder à certains administrateurs un accès correspondant aux tâches qu'ils doivent effectuer, tout en maintenant les autres accès masqués ou en lecture seule. Un exemple d'utilisation de ce type de contrôle d'accès consiste à créer des rôles distincts pour le personnel responsable de différentes tâches au sein de l'entreprise (ex. : administrateurs de la sécurité et administrateurs du réseau). Toutes les modifications réalisées par un administrateur sont consignées en mentionnant l'heure, l'administrateur, l'interface de gestion (interface Web, CLI, Panorama), la commande exécutée ou l'action effectuée.
- **Gestion des mises à jour des logiciels, du contenu et des licences :** A mesure que les déploiements prennent de l'ampleur, les entreprises veulent s'assurer que les mises à jour sont transmises de manière rationnelle aux boîtiers situés en aval. Par exemple, les équipes chargées de la sécurité peuvent vouloir valider une mise à jour logicielle à un niveau global avant de la diffuser simultanément à tous les pare-feu via Panorama. Panorama permet la gestion centralisée des mises à jour des logiciels, des contenus (mises à jour d'applications, signatures antivirales, signatures de menaces, base d'URL, etc.) et des licences.

L'utilisation de modèles, de groupes d'équipements, d'une gestion basée sur les rôles et d'une centralisation des mises à jour permet aux entreprises d'accorder un accès approprié aux outils de visualisation et aux fonctions de gestion, de création de stratégies, de génération de rapports et de journaux de logs, tant au niveau local que global.

Panorama offre aux entreprises un équilibre entre gestion centrale et gestion locale grâce à l'utilisation de modèles, de groupes d'équipements, de l'administration basée sur les rôles et de la gestion des mises à jour.



Flexibilité des déploiements

Les entreprises peuvent déployer Panorama soit sur du matériel dédié (plateforme M100) soit sur une machine virtuelle (VMWare ESXi).

Solution matérielle

Les entreprises qui choisissent de déployer Panorama sur un matériel dédié performant ou qui souhaitent séparer les fonctions de gestion et de journal de log de Panorama pour les volumes importants de données peuvent acquérir notre plateforme dédiée : M-100. Le déploiement de Panorama sur M-100 peut s'effectuer de différentes manières :

- **Déploiement centralisé :** Dans ce scénario, l'ensemble des fonctions de journalisation et de gestion de Panorama sont regroupées sur un même équipement (avec option de haute disponibilité).
- **Déploiement distribué :** Une entreprise peut choisir de séparer les fonctions de journal de log des fonctions de gestion et les répartir entre plusieurs matériels. Dans cette configuration, les différentes fonctions sont réparties entre gestionnaires et collecteurs de journaux de logs.
  - **Gestionnaire Panorama :** Le gestionnaire Panorama est chargé de l'exécution des tâches associées à la configuration des politiques et des équipements sur l'ensemble des boitiers gérés. Il ne stocke pas les données de journalisation localement, mais utilise des collecteurs de journaux de logs séparés pour la gestion des données consignées. Le gestionnaire analyse les données stockées dans les collecteurs de journaux de logs pour la création centralisée de rapports.
  - **Collecteur de logs Panorama :** Les entreprises ayant d'importants volumes de données à consigner et des exigences de stockage élevées peuvent déployer des collecteurs de logs Panorama dédiés qui recueilleront les informations de journalisation auprès des différents pare-feu gérés.

La séparation de la gestion et de la collecte des données permet aux entreprises d'optimiser les déploiements afin de satisfaire aux exigences organisationnelles, géographiques ou d'évolutivité.

Solution virtuelle

Panorama peut être déployé en tant que solution virtuelle sur VMware ESX(i) afin de prendre en charge les initiatives de virtualisation des entreprises et de renforcer l'espace rack parfois limité ou coûteux au sein d'un data center. Le déploiement de la solution virtuelle peut s'effectuer de deux manières :

- **Déploiement centralisé : L'ensemble des fonctions de log et de gestion Panorama sont regroupées sur une solution virtuelle unique (avec option de haute disponibilité).**
- **Déploiement distribué :** La fonction de collecte des données distribuées de Panorama prend en charge une solution hybride matérielle et virtuelle.
  - **Gestionnaire Panorama :** La solution virtuelle peut agir en tant que gestionnaire Panorama et est chargée d'exécuter les tâches associées à la configuration des politiques et des équipements sur l'ensemble des boîtiers gérés.
  - **Collecteurs de logs Panorama :** Ces collecteurs ont pour mission de réduire l'intensité des tâches de collecte et de traitement des données. Ils peuvent être déployés via la solution M-100. La solution virtuelle ne peut pas être utilisée comme collecteur de logs Panorama.

Le fait de pouvoir choisir entre une plateforme matérielle et une plateforme virtuelle et de combiner ou de séparer les fonctions Panorama offre aux entreprises une flexibilité maximale pour la gestion des pare-feu Palo Alto Networks au sein d'un environnement réseau distribué.
Caractéristiques techniques de Panorama

CARACTÉRISTIQUES TECHNIQUES DE PANORAMA

Nombre de boîtiers pris en charge	Jusqu'à 1 000
Haute disponibilité	Actif/Passif
Authentification des administrateurs	Base de données locale
	RADIUS

CARACTÉRISTIQUES TECHNIQUES DES SOLUTIONS DE GESTION M-100

ENTRÉE/SORTIE

- (1) 10/100/1000, (3) 10/100/1000 (pour utilisation future), (1) port série console DB9

STOCKAGE (2 OPTIONS)

- RAID M-100 1To : Disque dur certifié RAID 1To x 2 pour 1To de stockage RAID
- RAID M-100 4To : Disque dur certifié RAID 1To x 8 pour 4To de stockage RAID

ALIMENTATION / CONSOMMATION ÉLECTRIQUE MAX.

- 500W/500W

BTU/H MAX.

- 1 705 BTU/h

TENSION D'ENTRÉE (FRÉQUENCE D'ENTRÉE)

- 100-240VCA (50-60Hz)

CONSOMMATION DE COURANT MAX.

- 10A@100VCA

TEMPS MOYEN ENTRE DEFAILLANCES (MTBF)

14 ANS

INSTALLABLE EN RACK (DIMENSIONS)

- 1U, rack standard 19" (4,45 cm H x 58,42 cm P x 43,69 cm L)

POIDS (PÉRIPHÉRIQUE SEUL / EMBALLAGE)

- 12 kg/15 kg

SÉCURITÉ

- UL, CUL, CB

EMI (POTENTIEL D'INTERFÉRENCE ÉLECTROMAGNÉTIQUE)

- FCC classe A, CE classe A, VCCI classe A

ENVIRONNEMENT

- Température de fonctionnement : 40 à 104 °F, 5 à 40 °C
- Température de non fonctionnement : -40 à 149 °F, -40 à 65 °C

CARACTÉRISTIQUES TECHNIQUES DES SOLUTIONS VIRTUELLES

CONFIGURATION MINIMALE REQUISE POUR LE SERVEUR

- Disque dur 40 Go
- RAM 4 Go
- Quad-Core CPU (2GHz+)

VERSIONS DE VMWARE PRISES EN CHARGE

- VMware ESX 4.1 ou versions ultérieures

NAVIGATEURS PRIS EN CHARGE

- IE v7 ou versions ultérieures
- Firefox v3.6 ou versions ultérieures
- Safari v5.0 ou versions ultérieures
- Chrome v11.0 ou versions ultérieures

STOCKAGE DES LOGS

- Disque virtuel VMware : 2 To maximum
- 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