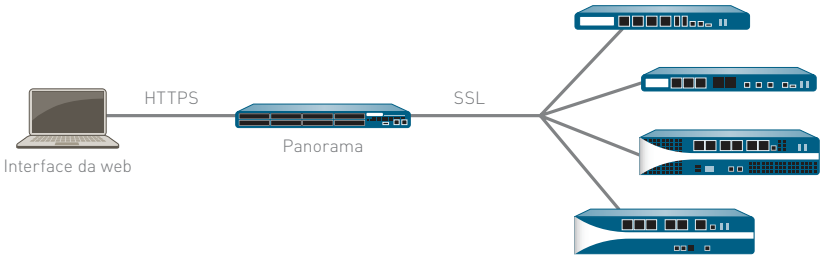
PANORAMA

O Panorama fornece gerenciamento centralizado de políticas e dispositivos em uma rede de firewalls de próxima geração da Palo Alto Networks.

- Exiba um resumo gráfico dos aplicativos na rede, os respectivos usuários e o impacto potencial na segurança.
- Implante centralmente políticas corporativas para serem usadas junto com políticas locais para obter flexibilidade máxima.
- Delegue níveis apropriados de controle administrativo no nível do dispositivo, ou globalmente com o gerenciamento baseado em funções.
- Analise, investigue e faça relatórios do tráfego de rede, incidentes de segurança e modificações administrativas de forma centralizada.



As grandes organizações normalmente têm muitos firewalls implantados por toda a rede e, muito frequentemente, o processo de gerenciá-los e controlá-los é difícil, devido às complexidades e inconsistências entre dispositivos individuais. O resultado é o aumento nos esforços administrativos e custos associados.

O Panorama fornece gerenciamento centralizado e visibilidade dos firewalls de próxima geração da Palo Alto Networks. A partir de uma central, os administradores podem ter uma visão dos aplicativos, usuários e conteúdo que passa pelos firewalls. Saber o que está na rede, junto com política de permissão segura de aplicativo, maximiza a proteção e controle, minimizando, ao mesmo tempo, o esforço administrativo. Os administradores podem executar análises e relatórios de forma centralizada, com dados agregados ao longo do tempo ou em dados armazenados no firewall local.

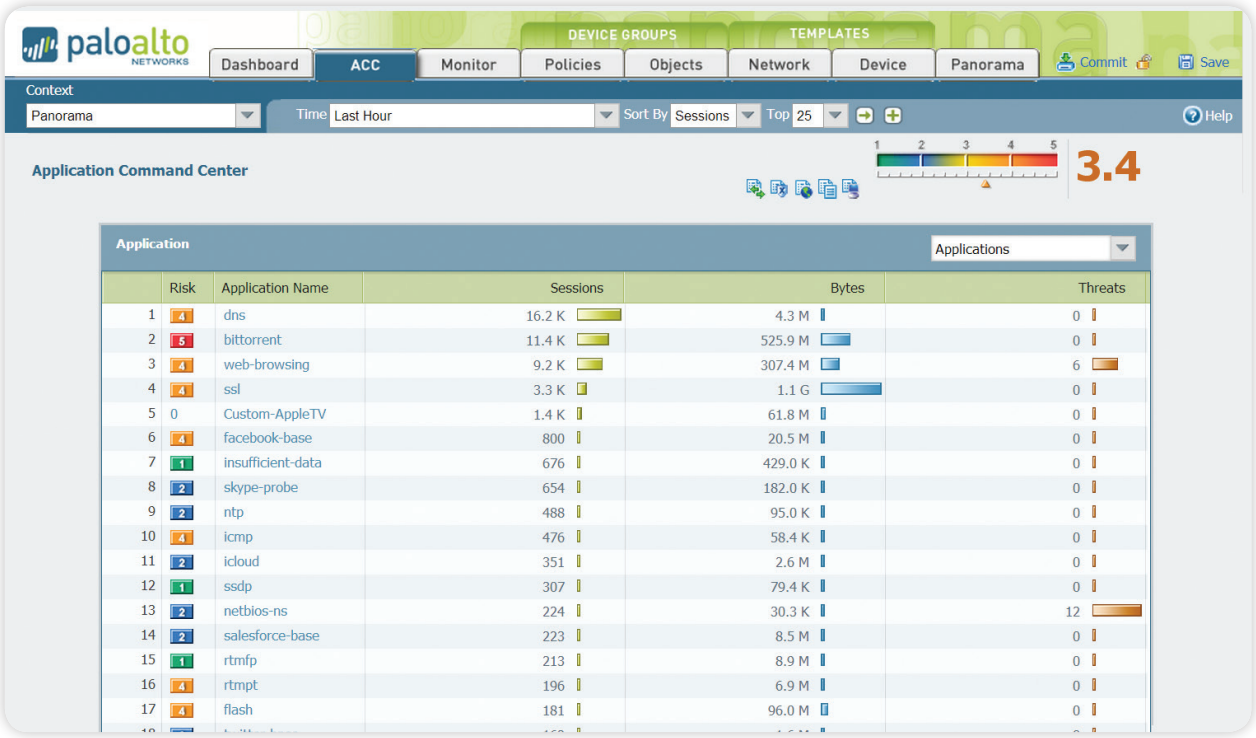
Tanto o Panorama como os dispositivos individuais compartilham a mesma aparência e experiência baseada em web, minimizando qualquer curva de aprendizado ou atraso na execução da tarefa à disposição; A Palo Alto Networks segue uma filosofia de gerenciamento que enfatiza a consistência, fornecendo uma vantagem significativa sobre as ofertas dos concorrentes.

Visibilidade central: Application Command Center

Usar o Application Command and Control (ACC) do Panorama fornece ao administrador uma exibição gráfica do aplicativo, URL, ameaça e dados (arquivos e padrões) que passam por todos os dispositivos da Palo Alto Networks sob seu gerenciamento. O ACC busca dinamicamente dados de cada dispositivo para garantir que os administradores tenham uma exibição atualizada dos aplicativos na rede, quem os utiliza e as ameaças potenciais que eles podem representar. Os administradores podem investigar aplicativos novos ou desconhecidos com um único clique, exibindo uma descrição do aplicativo, seus recursos principais, suas características comportamentais e quem os utiliza.

Dados adicionais em categorias de URL e ameaças fornecem uma boa imagem da atividade de rede. A visibilidade a partir do ACC permite que os administradores tomem decisões de política bem informadas e respondam rapidamente a ameaças potenciais de segurança.

paloalto NETWORKS
the network security company™



Legenda: O Application Command Center fornece exibições global e local do tráfego de aplicativos, completas com detalhes para saber mais sobre a atividade atual.

Controle de política global: permitindo aplicativos com segurança

Permitir aplicativos com segurança significa permitir acesso a aplicativos específicos com prevenção contra ameaças específicas e políticas de filtragem de arquivos, dados ou URL aplicadas. O Panorama facilita a permissão de aplicativos com segurança em toda a rede de firewalls, permitindo que os administradores gerenciem regras a partir de uma central.

As políticas compartilhadas baseadas no Panorama ajudam a garantir a conformidade com exigências internas ou regulatórias, enquanto as regras do dispositivo local mantêm a segurança e flexibilidade. Combinar controle administrativo centralizado e local sobre políticas e objetos pode ajudar a obter um equilíbrio entre segurança consistente em um nível global e flexibilidade no nível local.

Os administradores podem implantar políticas que permitam aplicativos ou funções de aplicativo com segurança baseadas em usuários, através da integração com serviços de diretório, enquanto a prevenção de ameaças específicas ao aplicativo protege o conteúdo e a rede. A capacidade de definir uma única política que permite aplicativos com segurança baseada no usuário (e não em endereço IP) permite que as organizações reduzam drasticamente o número de políticas necessárias. Um benefício adicional da integração com serviços de diretório é uma redução drástica nas despesas administrativas associadas com os acréscimos, mudanças e alterações de funcionários que ocorrem diariamente - as políticas de segurança permanecem estáveis enquanto os funcionários são movidos de um grupo para outro.

Monitoramento de tráfego: análise e relatórios

O Panorama utiliza o mesmo conjunto de ferramentas de monitoramento e relatórios disponívedisponíveisl no nível de gerenciamento do dispositivo local e acrescenta visibilidade fornecendo uma exibição agregada das atividades. À medida que os administradores executam consultas de log e geram relatórios, o Panorama envia dinâamicamente os dados mais atuais diretamente dos firewalls sob gerenciamento ou de logs encaminhados ao Panorama. O acesso às informações mais recentes em todos os dispositivos permite que os administradores tratem os incidentes com segurança, além de tomar uma posição proativa para proteger os ativos corporativos.

- **Visualizador de log:** Em um dispositivo individual ou em todos os dispositivos, os administradores do Panorama podem exibir rapidamente atividades de log usando filtragem de log dinâmica clicando em um valor de célula e/ou usando o construtor de expressões para definir os critérios de ordenação. Os resultados podem ser salvos para consultar futuras ou exportados para mais análises.
- **Relatórios personalizados:** Os relatórios predefinidos podem ser usados como são, personalizados ou agrupados como um único relatório para se ajustarem a exigências específicas.
- **Relatórios de atividade do usuário:** No Panorama, um relatório de atividade do usuário exibe os aplicativos usados, categorias de URL visitados, web sites visitados, e todos os URLs visitados ao longo de um tempo especificado para usuários individuais. O Panorama cria os relatórios usando uma exibição agregada da atividade do usuário, sem importar qual firewall o protege, ou qual IP ou dispositivo ele está usando.

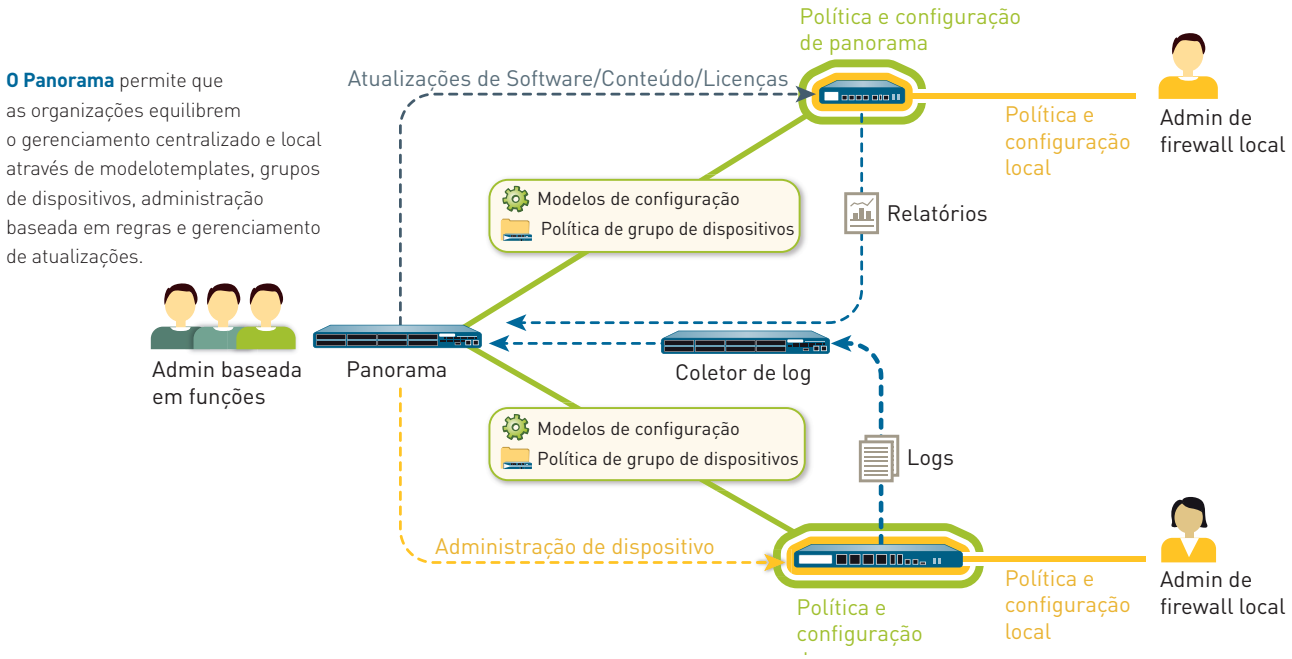
Arquitetura de gerenciamento do Panorama

O Panorama permite que as organizações gerenciem seus firewalls da Palo Alto Networks usando um template que fornece tanto vigilância central quanto controle local. O Panorama fornece várias ferramentas para administração centralizada:

- **Templates:** O Panorama gerencia a configuração comum de dispositivos e rede através de templates. Os templates podem ser usados para gerenciar configurações de maneira centralizada e depois enviar as alterações para todos os firewalls gerenciados. Esta abordagem evita ter que fazer as mesmas alterações de firewall repetidamente em muitos dispositivos. Um exemplo desse uso é enviar configurações comuns de servidor DNS e NTP para centenas de firewalls, em vez de realizar a mesma alteração em cada dispositivo.
- **Grupos de dispositivos:** O Panorama gerencia política e objetos comuns em grupos de dispositivos. Os grupos de dispositivos são usados para gerenciar de forma centralizada as bases de regras de muitos dispositivos com requisitos comuns. Como exemplo, os dispositivos podem ser agrupados geograficamente (ex., Europa a América do Norte) ou funcionalmente (ex., perímetro ou datacenter). Dentro dos grupos de dispositivos, os sistemas virtuais são tratados como dispositivos individuais, no mesmo nível dos firewalls físicos. Isso permite compartilhar uma base de regras comuns nos diferentes sistemas virtuais em um dispositivo.

  As organizações podem usar políticas compartilhadas para controle central, fornecendo ainda ao administrador de firewall a autonomia para fazer ajustes específicos para exigências locais. No nível do grupo de dispositivos, os administradores podem criar políticas compartilhadas que são definidas como o primeiro conjunto de regras (pré-regras) e o último conjunto de regras (pós-regras) a serem avaliadas em comparação com critérios de correspondência. As pré-regras e pós-regras podem ser exibidas em um firewall gerenciado, mas podem ser editadas apenas no Panorama dentro do contexto das funções administrativas definidas. As regras do dispositivo local (aquelas entre as pré- e pós-regras) podem ser editadas tanto pelo administrador local quanto por um administrador do Panorama, que foi mudado para um contexto de firewall local. Além disso, uma organização pode usar objetos compartilhados definidos por um administrador do Panorama, que podem ser referenciados por regras de dispositivo localmente gerenciadas.
- **Administração baseada em funções:** As organizações podem usar a administração baseada em funções para delegar acesso administrativo no nível de recursos (ativado, somente leitura ou desativado e oculto da exibição) para diferentes membros da equipe. Administradores específicos podem receber acesso apropriado às tarefas que são pertinentes ao seu trabalho, e ao mesmo tempo ter outros acessos ocultos ou somente para leitura. Um exemplo de como este tipo de controle de acesso pode ser usado é para definir funções diferentes para equipes responsáveis por diferentes tarefas na empresa, como administradores de segurança em comparação com administradores de rede. Todas as alterações feitas por um administrador são registradas, mostrando a hora de ocorrência, o administrador, a interface de gerenciamento usada (Web UI, CLI, Panorama), o comando ou ação realizada.
- **Gerenciamento de atualização de software, conteúdo e licença:** Conforme uma implantação aumenta de tamanho, muitas organizações querem ter certeza de que as atualizações são enviadas para os aparelhos abaixo na hierarquia de maneira organizada. Por exemplo, as equipes de segurança podem preferir qualificar de forma centralizada uma atualização de software antes que ela seja fornecida através do Panorama para todos os firewalls de produção simultaneamente. Usando o Panorama, o processo de atualização de software, conteúdo (atualizações de aplicativo, assinaturas de antivírus, assinaturas de ameaça, banco de dados de filtragem de URL, etc.) e licenças pode ser gerenciado de forma centralizada.

Usando templates, grupos de dispositivos, administração baseada em regras e gerenciamento de atualizações, as organizações podem delegar acesso apropriado a todas as funções de gerenciamento; ferramentas de virtualização, criação de políticas, relatórios e registros, tanto em um nível global quanto local.



Flexibilidade de implantação

As organizações podem implantar o Panorama tanto como dispositivo de hardware quanto dispositivo virtual.

Dispositivo de hardware

As organizações que preferem implantar o Panorama em um hardware dedicado de alto desempenho, ou que gostariam de separar o gerenciamento do Panorama e as funções de registro de grandes volumes de dados de log, podem usar o hardware M-100 para atender às suas necessidades. O Panorama executado no M-100 pode ser implantado das seguintes maneiras:

- **Centralizado:** Neste caso, todo o gerenciamento do Panorama e funções de registro são consolidados em um único dispositivo (com a opção de alta disponibilidade).
- **Distribuído:** Uma organização pode preferir separar o gerenciamento e funções de registro em vários dispositivos. Nesta configuração, as funções são divididas entre gerentes e coletores de log.
  - **Gerente do Panorama:** O gerente do Panorama é responsável por lidar com tarefas associadas com a configuração de políticas e dispositivos em todos os dispositivos gerenciados. O gerente não armazena dados de log localmente, mas usa coletores de log separados para manipular os dados de log. O gerente analisa os dados armazenados nos coletores de log para a criação centralizada de relatórios.
  - **Coletor de log do Panorama:** As organizações com alto volume de log e exigências de retenção podem implantar dispositivos coletores de log dedicados do Panorama que agregarão informações de log de vários firewalls gerenciados.

A separação do gerenciamento e coleta de logs permite que as organizações otimizem sua implantação para atender requisitos organizacionais, geográficos ou de dimensionamento.

Dispositivo virtual

O Panorama pode ser implantado como um dispositivo virtual no VMware ESX(i), permitindo que as organizações apoiem suas iniciativas de virtualização e consolidem o espaço do rack que às vezes é limitado ou caro em um data center. O dispositivo virtual pode ser implantado de duas maneiras:

- **Centralizado:** Todo o gerenciamento do Panorama e a criação de logs são consolidados em um único dispositivo virtual (com a opção de alta disponibilidade).
- **Distribuído:** A coleção de logs distribuídos suporta uma combinação de dispositivos de hardware e virtuais.
  - **Gerente do Panorama:** O dispositivo virtual pode servir como um gerente do Panorama, e é responsável por lidar com tarefas associadas com configuração de políticas e dispositivos em todos os dispositivos gerenciados.
  - **Coletor de log do Panorama:** Os coletores de log do Panorama são responsáveis por descarregar tarefas intensivas de coleta e processamento de logs, e podem ser implantados usando o M-100. O dispositivo virtual não pode ser usado como um coletor de log do Panorama.

Fornecer uma opção de plataforma em hardware ou virtualizada, assim como a opção de combinar ou separar as funções do Panorama, fornece às organizações uma flexibilidade máxima para gerenciar vários firewalls da Palo Alto Networks firewalls em um ambiente distribuído de rede.

ESPECIFICAÇÕES DO PANORAMA

Número de dispositivos suportados	Até 1.000
Alta disponibilidade	Ativo/Passivo
Autenticação do administrador	Banco de dados local
	RADIUS

ESPECIFICAÇÕES DO DISPOSITIVO DE GERENCIAMENTO M-100

E/S

- (1) 10/100/1000, (3) 10/100/1000 (para uso futuro), (1) porta serial de console DB9

ARMAZENAMENTO (2 OPÇÕES)

- M-100 1TB RAID: 2 x HDD certificado RAID de 1TB para 1TB de armazenamento RAID
- M-100 4TB RAID: 8 x HDD certificado RAID de 1TB para 4TB de armazenamento RAID

FONTE DE ALIMENTAÇÃO/CONSUMO DE ENERGIA MÁXIMO

- 500W/500W

BTU/H MÁXIMO

- 1.705 BTU/h

TENSÃO DE ENTRADA (FREQUÊNCIA DE ENTRADA)

- 100-240 VCA (50-60Hz)

CONSUMO MÁXIMO DE CORRENTE

- 10A@100VCA

TEMPO MÉDIO ENTRE FALHAS (MTBF)

- 14,5 anos

MONTADO EM RACK (DIMENSÕES)

- 1U, rack padrão de 19" (1,75"A x 23"P x 17,2"L)

PESO (DISPOSITIVO AUTÔNOMO/NO ENVIO)

- 26,7lbs/35lbs

SEGURANÇA

- UL, CUL, CB

EMI

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

AMBIENTE

- Temperatura operacional: 40 a 104 F, 5 a 40 C
- Temperatura não operacional: -40 a 149 F, -40 a 65 C

ESPECIFICAÇÕES DO DISPOSITIVO VIRTUAL

REQUISITOS MÍNIMOS DE SERVIDOR

- 40 GB de disco rígido
- 4 GB RAM
- Quad-Core CPU (2GHz+)

SUPORTE DE VMWARE

- VMware ESX 4.1 ou superior

SUPORTE DE NAVEGADOR

- IE v7 ou superior
- Firefox v3.6 ou superior
- Safari v5.0 ou superiorr
- Chrome v11.0 ou superior

ARMAZENAMENTO DE LOG

- Disco virtual VMware: 2TB no máximo
- NFS

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com