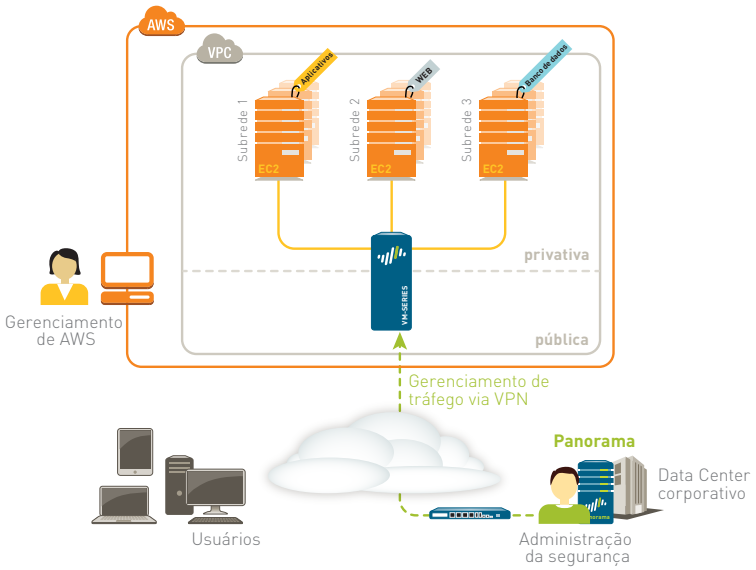
VM-Series para Amazon Web Services

Principais Recursos de Segurança:

Os firewalls VM-Series da Palo Alto Networks® dão a sua empresa a flexibilidade de manter serviços de firewall de última geração nas instâncias de VPC (Virtual Private Cloud, Nuvem Virtual Privada) dentro de Amazon Web Services (AWS).

- Identifique e controle o fluxo de tráfego dentro e para a sua VPC, limite o acesso aos aplicativos de acordo com o usuário e bloqueie ameaças conhecidas e desconhecidas.
- Automatize as atualizações das políticas de segurança e fique em dia com as mudanças na sua VPC.
- Isole e segmente dados e aplicativos críticos aplicando princípios ZeroTrust (não confiar nunca, verificar sempre).



Amazon Web Services (AWS) oferece mundialmente uma ampla variedade de serviços de computação, aplicativos, armazenamento e implementação que permitem expandir as suas iniciativas de computação em nuvem de forma rápida e eficiente, criando uma VPC (Virtual Private Cloud, Nuvem Virtual Privada) dentro da AWS. Quando se pensa em migrar dados e aplicativos críticos, não se pode esquecer a segurança.

Mais especificamente, quais recursos de segurança você precisa para proteger sua VPC? Esses recursos conseguem acompanhar as mudanças nas cargas de trabalho virtuais implementadas nas suas instâncias de EC2 (Elastic Cloud Compute)? O VMSeries para AWS atende esses importantes desafios com o mesmo firewall de última geração e avançados recursos de prevenção de ameaças disponíveis nos nossos equipamentos físicos, além de um conjunto nativo de recursos de automação que atualizam dinamicamente as suas políticas de segurança de acordo com as mudanças nas instâncias EC2.

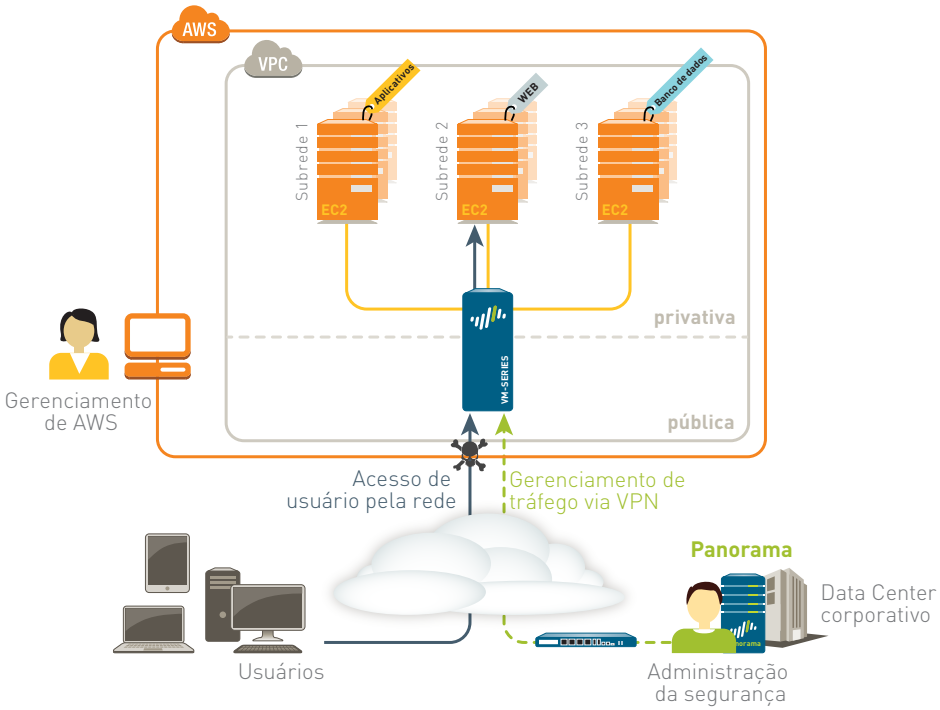
O VMSeries for AWS analisa todo tráfego rapidamente para determinar a identidade do aplicativo, do conteúdo desse aplicativo e quem é o usuário. O aplicativo, conteúdo e identidade do usuário são então usados como componentes da sua política de segurança, permitindo a você isolar seus aplicativos críticos e protegê-los contra ameaças - conhecidas e desconhecidas.

Para garantir que a segurança acompanhe as mudanças na sua VPC, os recursos nativos de automação como o monitoramento de máquina virtual eos grupos de endereço dinâmico permitem que você monitore proativamente qualquer mudança nas suas instâncias EC2, alimentando automaticamente esse contexto direto na política e eliminando, assim, o hiato entre o momento em que uma mudança é feita na infraestrutura virtualizada e o momento em que esta é incorporada à política de segurança do firewall.

paloalto networks

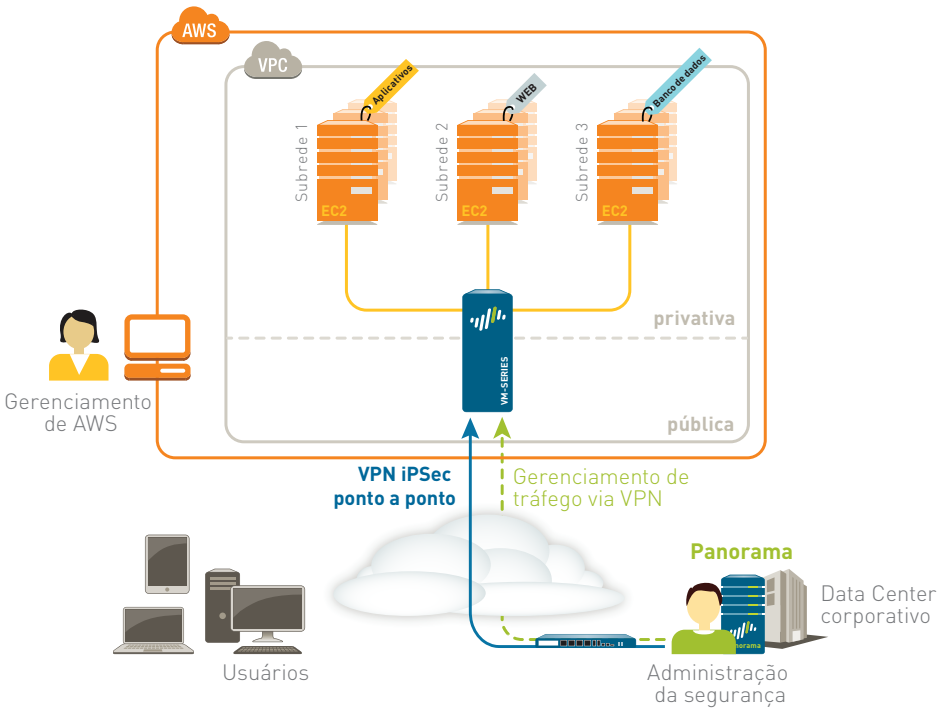
CASO DE USO DE VM-SERIES FOR AWS: GATEWAY NO PERÍMETRO

Criar uma VPC não é muito diferente de criar uma nova rede física completa com um firewall novo no perímetro. Nesse caso de uso, a VMSeries pode ser implementada como firewall de gateway, protegendo a sua VPC baseada em aplicativo, independente de porta, inspecionando o tráfego em busca de ameaças conhecidas e desconhecidas e controlando o acesso com base na identidade do usuário. À medida que são adicionadas ou alteradas novas cargas de trabalho EC2, o monitoramento de máquinas virtuais e os grupos de endereço dinâmico permitem que as suas políticas de segurança acompanhem as respectivas mudanças do ambiente EC2.



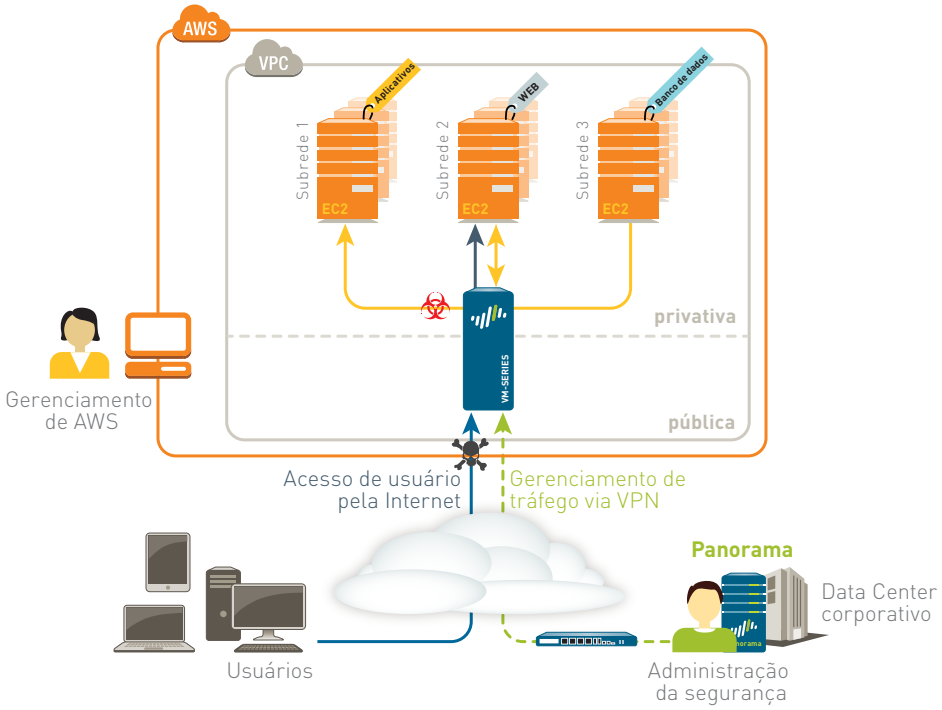
CASO DE USO DE VM-SERIES FOR AWS: VPN IPSEC PARA A REDE CORPORATIVA

Sua VPC é uma extensão do seu ambiente corporativo de computação, facilitando e agilizando a escalabilidade e minimizando as despesas de capital e operacionais. Nesse caso, o VMSeries oferece exatamente os mesmos recursos disponíveis em nossos equipamentos físicos, entre eles VPN IPSec ponto a ponto baseada em padrões. O VMSeries pode ser configurado para estabelecer uma conexãoVPN IPSec, com acesso controlado de acordo com o aplicativo, conteúdo e identidade do usuário. Na realidade, você consegue estender as mesmas políticas que controlam a sua rede corporativa para a sua VPC. Aqui também os recursos de automação que coletam as mudanças dinâmicas e contextuais podem ser alimentados em firewalls virtualizados e físicos, permitindo então que a política acompanhe quaisquer alterações no ambiente dos aplicativos.



CASO DE USO DE VM-SERIES FOR AWS: SEGURANÇA ENTRE MÁQUINAS VIRTUAIS

As recentes ameaças de maior destaque mostraram que os criminosos do mundo virtual são capazes de se esconder à vista de todos tão logo consigam driblar os controles no perímetro e, a partir de então, se expandir para toda a rede. Em uma rede física você consegue proteger seus aplicativos e dados segmentando a rede pela aplicação dos princípios ZeroTrust de nunca confiar, sempre verificar. Na sua VPC, você pode usar o VMSeries para implementaros mesmos princípios ZeroTrust para controlar o tráfego entre as subredes IP baseadas em aplicativos e usuários e, ao mesmo tempo, inspecionar as ameaças virtuais. Nesse cenário, os recursos de automação monitoram as mudanças nas suas instâncias de EC2, alimentando esse contexto em políticas para manter a segurança atualizada de forma dinâmica.



RESUMO

O VMSeries for AWS permite proteger sua VPC usando nosso firewall de última geração e avançados serviços de prevenção de ameaças. O fluxo de tráfego para dentro e entre a sua implementação de AWS é identificado e protegido de acordo com a identidade do aplicativo e inspecionado em busca de ameaças virtuais conhecidas e desconhecidas. Os recursos de automação do VMSeries ajudam a garantir que assuas políticas de segurança possam acompanhar quaisquer mudanças contextuais em uma máquina virtual da sua VPC. Já o Panorama permite gerenciar centralizadamente toda a implementação de appliances físicos e virtualizados da Palo Alto Networks.

paloalto networks
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com