Improve Productivity for Government Branch Offices

Industry

US Government

Use Case

Securely offload branch internet and sanctioned SaaS applications

Business Benefits

- Improve branch worker productivity and digital experiences with faster, seamless connectivity to critical SaaS applications, cloud resources, and the internet with a guaranteed SLA.
- Avoid costs associated with upgrading branch WAN links to the data center.
- Improve the performance of data center applications via recovered capacity on government WAN networks.

Operational Benefits

- Simplify deployment and minimize capital expenditure and disruption with a cloud-based service.
- Decrease demand on dedicated WAN connections to data centers by offloading internet-bound traffic and routing directly from the branch to Prisma Access.
- Efficiently manage the service and associated security controls, including Zero Trust architectures, from the same centralized interface as Palo Alto Networks Next-Generation Firewalls (NGFWs).

Security Benefits

- Provide the same robust security in branch offices as in the data center.
- Reduce the attack surface by scanning for threats hidden in files, web links, encrypted traffic, and more.
- Apply consistent granular security controls, including Zero Trust architectures, across branch internet connections.
- Comply with key functional guidelines, including Trusted Internet Connections (TIC) 3.0, for branch office use cases.
- Meet government needs for additional security controls with a FedRAMP Authorized service.

Business Drivers

As governments modernize their IT, they are relying more on cloud and software-as-a-service (SaaS) applications to serve citizens and accomplish their missions. Commercial cloud and SaaS applications demonstrated their versatility and scalability advantages during the COVID-19 pandemic, and adoption is accelerating. However, access to and from these applications requires even more security controls than traditional applications housed in the data center.

Business Problem

Government branch office workers provide essential services to citizens and communities, and any business disruption can have serious effects. Governments are popular targets for ransomware and other attacks from malicious actors, which makes securing traffic from internet and SaaS applications doubly important.

Traditional Approach

Traditionally, government agencies have routed all internet traffic—including from branch offices—through a low number of controlled access points in the data center, where firewalls and other appliances inspect traffic for threats and applied security policies. This hub-and-spoke model was not built for cloud and SaaS applications, however. Backhauling (or "hairpinning") this traffic from branch offices through the data center and then out to the internet introduces significant latency, particularly for federal entities whose branch offices may span the country. Delay will increase as cloud and internet traffic increase, unless network and security teams continually upgrade access connections and deploy more equipment in the data center, a costly approach.

Some agencies have investigated setting up separate firewall, intrusion prevention system (IPS), content filtering, and anti-malware appliances in branch offices for internet traffic, but this has its own set of challenges. Branch offices typically do not have local IT support, so adding more to the technology footprint can complicate ongoing operations and support as well as make it difficult to gain a consolidated view of traffic and potential threats.

Palo Alto Networks Approach

Government agencies can break out a secure, trusted connection to the internet and SaaS applications from branch offices without deploying extra hardware or adding complexity for security or networking teams. Prisma® Access is a cloud-delivered, FedRAMP Authorized security service that protects all application traffic while offering an exceptional user experience. Prisma Access consolidates many security capabilities—firewall as a service (FWaaS), cloud secure web gateway (CSWG), DNS security, content filtering, decryption, malware prevention and more—offering complete security for branch offices. With Layer 7 visibility and traffic inspection, agencies can define granular security policies that smooth access to sanctioned SaaS applications while flagging or eliminating potential threats that might disrupt operations.

Actual Customer Solution

A US government civilian agency serves citizens through several hundred offices spread across the country. Workers in these offices increasingly use SaaS apps, particularly Microsoft 365™ and Box, while also relying on applications in the data center. Regardless of the application, traffic from the hundreds of branch offices travels across broadband links to the data center, and traffic destined for the internet is inspected and ultimately forwarded.

Customer Challenge

The agency was refreshing firewalls and other security appliances in its primary and secondary data center. The security stack included firewalls, SWG, IPS appliances, and sandbox appliances from three different vendors. The agency was looking to simplify its security footprint and gain greater visibility into agency traffic. Palo Alto Networks suggested that, rather than upgrading the broadband connections and security appliances at every office, the agency could offload internet traffic directly at each branch office.

Solution Overview

After conducting market research, a competitive product review, a proof of concept and testing, and verification with numerous cybersecurity vendors, the agency chose Palo Alto Networks NGFWs for the data center, Prisma Access to offload internet traffic from branch offices, and Prisma SaaS. Prisma SaaS protects the integrity and privacy of data in SaaS environments, while Prisma Access inspects traffic to and from the internet and SaaS applications. With no new products to deploy at the branches, deployment was swift. The agency also purchased Professional Services QuickStart engagements for the NGFWs, Prisma Access, and Prisma SaaS to fast-track the implementation as well as ensure alignment with best practices and the agency environment.

Each NGFW, with a suite of security services, replaces four security point products in the data center, unifying and simplifying security policy creation and management. Panorama™ network security management, which also manages Prisma Access, enables network and security teams to configure security policies and gain visibility into all traffic from a central location.

Products Purchased

- PA-7000 and PA-5250 NGFWs in a high availability configuration, with subscriptions for Threat Prevention, WildFire® malware prevention service, URL Filtering, and DNS Security
- Prisma Access for branch offices
- Prisma SaaS cloud access security broker (CASB)
- Panorama network security management

How Prisma Access Secures Internet Offload Traffic

With Prisma Access, internet and SaaS traffic are routed directly to a broadband internet connection at the branch. Prisma Access terminates an IPsec VPN on the existing branch office router. Agencies can perform selective TLS/SSL decryption on suspicious traffic (e.g., from recently published websites) as well as develop granular security policies that include decryption, web filtering, quality of service (QoS), and limiting or blocking of unsanctioned SaaS or personal accounts for sanctioned applications.

Prisma Access scans for threats, including the latest malicious URLs and malware discovered anywhere in the world.

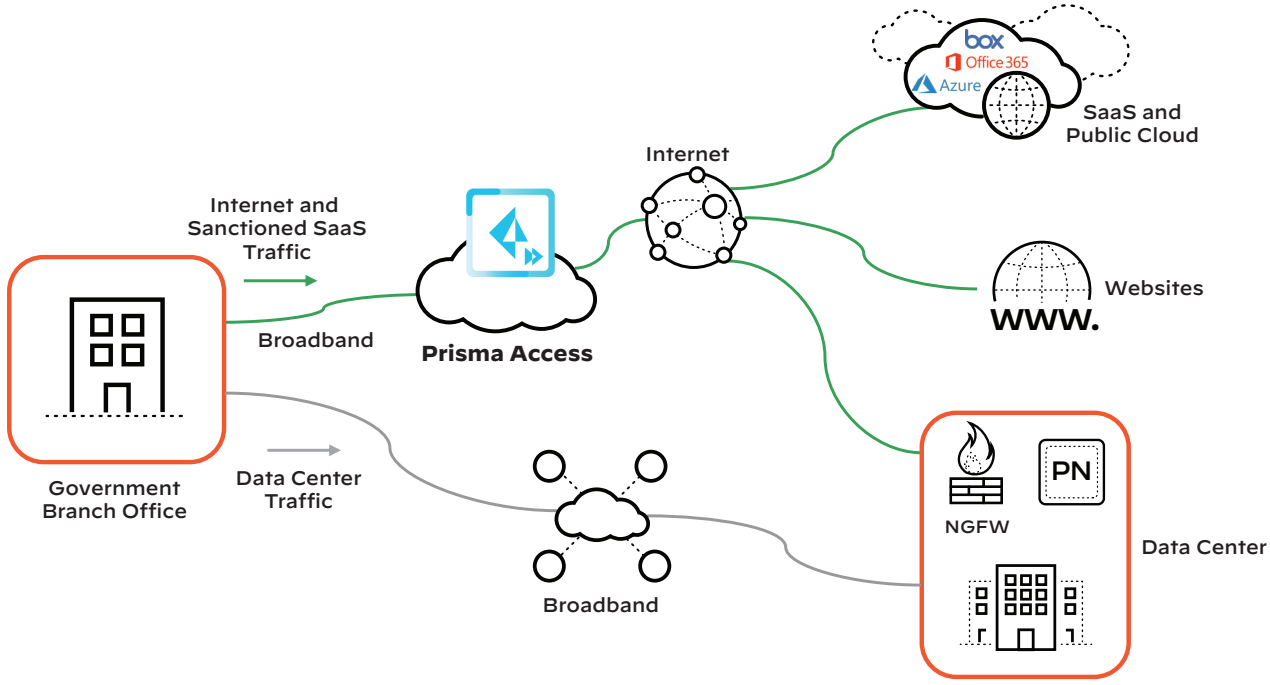

Figure 1: Secure offloading of internet and SaaS traffic from hundreds of branch offices

Taking advantage of the same security capabilities as Palo Alto Networks NGFWs, Prisma Access makes it simple to deploy consistent security policies across the data center and hundreds of branch offices.

Panorama network security management manages both NGFWs and Prisma Access. Granular administrative permissions grant networking and security teams access to the services they need in Panorama. Networking teams have control over networking, and security teams have control over security policies.

With access points across the country, Prisma Access improves latency and includes a guaranteed service-level agreement (SLA).

Benefits of Securely Offloading Internet and SaaS Traffic

Business Benefits

- Gain excellent performance and uptime connecting to internet and SaaS apps with a guaranteed SLA.
- Improve the performance of data center applications via recovered capacity on government WAN networks.

Operational Benefits

- Speed up deployment as well as minimize capital expenditure and disruption with a cloud-based service.
- Decrease the demand on private links to data centers by offloading internet-bound traffic and routing directly from the branch.
- Efficiently manage the secure offload and associated security controls from the same centralized interface as Palo Alto Networks NGFWs.

Security Benefits

- Provide the same robust security in branch offices as in the data center.
- Reduce the attack surface by scanning for threats hidden in files, web links, encrypted traffic, and more.
- Apply consistent security policies across branch internet connections.
- Comply with key functional guidelines, including TIC 3.0, for branch office use cases.
- Meet government needs for additional security controls with a FedRAMP Authorized service.

Additional Resources

Visit our US federal government page for key resources about modernizing your agency operations while measuring and managing risks.

Services to Help You

Palo Alto Networks offers a number of services to help you maximize the value of your investment and protect your business. For more information on support services, professional services, and education and training opportunities, visit our Services Overview page.

- Our global Customer Support provides timely, expert assistance to keep you up and running safely. Our support has been rated outstanding by third-party assessments. All Customer Support plans include online case management, online support resources, and license keys and upgrades. Premium and Premium Plus support options offer additional resources.
- Our Professional Services and Certified Professional Services Partners deliver the tools, best practices, and assistance you need to define an effective strategy, simplify operations, and prevent successful cyberattacks.
- Education and Training Services help you expand knowledge and skills with world-class training, certification and accreditation, and digital learning options.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com