SASE

OVERVIEW

SASE

JUNE 2024

Table of Contents

Preface

GUIDE TYPES

Overview guides provide high-level introductions to technologies or concepts.

Design guides provide an architectural overview for using Palo Alto Networks® technologies to provide visibility, control, and protection to applications built in a specific environment. These guides are required reading prior to using their companion deployment guides.

Deployment guides provide decision criteria for deployment scenarios, as well as procedures for combining Palo Alto Networks technologies with third-party technologies in an integrated design.

Solution guides provide add-on solutions for post-deployment use cases.

DOCUMENT CONVENTIONS

Notes provide additional information.

Cautions warn about possible data loss, hardware damage, or compromise of security.

Blue text indicates a configuration variable for which you need to substitute the correct value for your environment.

In the **IP** box, enter 10.5.0.4/24, and then click **OK**.

Bold text denotes:

- Command-line commands.

  # show device-group branch-offices

- User-interface elements.

  In the **Interface Type** list, choose **Layer 3**.

- Navigational paths.

  Navigate to **Network > Virtual Routers**.

- A value to be entered.

  Enter the password **admin**.

Italic text denotes the introduction of important terminology.

An *external dynamic* list is a file hosted on an external web server so that the firewall can import objects.

Highlighted text denotes emphasis.

Total valid entries: 755

ABOUT PROCEDURES

These guides sometimes describe other companies' products. Although steps and screen-shots were up-to-date at the time of publication, those companies might have since changed their user interface, processes, or requirements.

GETTING THE LATEST VERSIONS OF GUIDES

We continually update reference architecture guides. You can access the latest version of this and all guides at this location:

https://www.paloaltonetworks.com/referencearchitectures

WHAT'S NEW IN THIS RELEASE

Since the last version of this guide, Palo Alto Networks made the following changes:

- Added information for Prisma® SASE 3.0
- Updated naming of Cortex® Data Lake to Strata™ Logging Service
- Changed phrasing, terminology, and diagrams for technical accuracy

Purpose of This Guide

This guide describes the Secure Access Service Edge (SASE) set of technologies and introduces the Palo Alto Networks SASE solution.

This guide:

- Provides an overview of the capabilities of a SASE solution.
- Describes the products in the Palo Alto Networks portfolio that you can use to build a SASE solution for your organization.
- Provides guidance on where to obtain more information about implementing a SASE solution.
- Is recommended for using the SASE series of reference-architecture design and deployment guides and can provide guidance regarding which set of guides you would want to follow up with first.

AUDIENCE

This guide is for technical readers, including system architects, security engineers, and security support staff, IT engineers, and design engineers, who are considering migrating to a SASE solution for their mobile users and remote sites (or *branches*).

RELATED DOCUMENTATION

The following documents support this guide:

- **SASE for Securing Internet: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations.
- **SASE for Securing Internet: Deployment Guide**—Provides implementation details for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations. Includes decision criteria for deployment scenarios, as well as step-by-step procedures to achieve an integrated design.
- **SASE for Securing Private Applications: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure access to private applications for mobile users and users located at remote-site locations.
- **SASE for Securing Private Applications: Deployment Guide**—Provides implementation details for using Prisma Access and Prisma SD-WAN to secure access to private applications for mobile users and users located at remote-site locations. Includes decision criteria for deployment scenarios, as well as step-by-step procedures for programming features to achieve an integrated design.
- **SASE Secure Internet Policy Design: Solution Guide**—Provides policy design and deployment guidance for securing internet services by using the Prisma Access cloud-delivered security platform.

- **Identity-Based and Posture-Based Security for SASE: Solution Guide**—Provides design and deployment guidance for obtaining and applying identity-based and posture-based policies in Palo Alto Networks SASE platform.
- **Securing Internet Access by Using Explicit Proxy: Solution Guide**—Provides design and deployment guidance for securing internet access by using Palo Alto Networks Prisma Access explicit proxy solution.
- **AI-Powered Autonomous Digital Experience Management: Solution Guide**—Provides design, deployment, and operational guidance for integrating ADEM and AI-Powered ADEM with the Palo Alto Networks Prisma SASE solution.
- **Securing Private Application Access with ZTNA Connector: Solution Guide**—Provides design and deployment guidance for securing private application access by using Palo Alto Networks Prisma Access and ZTNA Connector.

Introduction

Organizations are undergoing a digital transformation in order to accelerate business processes, develop products faster, and maximize profits while delivering quality products and services to their customers. *Digital transformation* is the process of integrating of digital technologies into all areas of a business, from application development and deployment to everyday business functions, such as human resources and customer management.

As more parts of an organization transitioned to digital processes, and before the widespread adoption of cloud computing, the data center increasingly became the center of the organization. The challenge was to securely connect remote sites and mobile users to the data center. Dedicated wide-area networks and VPN tunnels connected remote sites and mobile users to the single source of an organization's digital assets—the data center—while perimeter security products protected against breaches and malware.

The rapid adoption of cloud computing in recent years has upended this centralized model. The scalability and cost-effectiveness of public cloud services and SaaS applications has caused organizations to move some or even all their digital assets out of the on-premises data center and into the cloud. The network perimeter has become less defined, and the traditional data center has become just one of many sources of business-critical applications and data.

Compared to traditional remote-site traffic patterns, where data flowed from a remote site to a data center, modern remote-site traffic patterns have data moving in different directions and to and from various destinations, such as corporate data centers, public clouds, and SaaS providers. Traditional security systems for legacy networks don’t scale to meet the new network traffic patterns, and these systems don't provide the agility and flexibility needed to connect to new and emerging services.

Mobile users likewise experience the effects of the decentralization of data and applications. Traditionally, mobile users would use a VPN tunnel to access the organization's sensitive assets in the on-premises data center. If they required access outside of the corporate network, their sessions routed through the organization's centralized security. However, with more and more data and applications moving outside of the data center, mobile-user traffic to destinations outside of the corporate network has increased dramatically, straining the organization's resources. As many organizations found out during the pandemic of 2020, when workers were required to work from home, the traditional solution does not scale quickly or easily.

Organizations need a solution for remote sites and mobile users that is scalable, resilient, and responsive. It needs to be able to scale quickly, even during usage surges, without compromising the user experience, and it needs to allow users to access corporate assets securely from anywhere, whether from a remote site or an airport, no matter where those digital assets reside.

SASE is such a solution.

THE SASE SOLUTION

SASE is the convergence of WAN edge/software-defined WAN (SD-WAN) networking as a service and cloud-based network security services. A SASE solution integrates these services seamlessly and provides secure access to applications and data no matter where they reside or from where it is being accessed. Furthermore, it provides that security and access along the

path from the user to the application or data without unnecessary redirects, such as through a centralized data center. This reduces latency and improves the user experience. Security is improved because users no longer "turn off the VPN" to get the performance they want from their applications.

Figure 1 shows the main components of a SASE solution.

Figure 1 The SASE solution

In general, the key components of a SASE solution include:

- **Cloud secure web gateway (SWG)**—Provides URL filtering, SSL decryption, application control, and threat detection and prevention for user web sessions.
- **Firewall as a service (FWaaS)**—Provides a cloud-native, next generation firewall that provides advanced Layer 7 inspection, access control, threat detection and prevention, and other security services.
- **Cloud-access security broker (CASB)**—Monitors the use of sanctioned and unsanctioned SaaS applications; provides malware and threat detection in SaaS applications; and, as part of a data loss prevention (DLP) solution, provides sensitive data visibility and control in order to detect improperly-stored data in SaaS file repositories.
- **SD-WAN**—Provides an overlay network decoupled from the underlying hardware, providing flexible, secure traffic between sites.
- **DNS security**—Provides protection against DNS-based threats, such as DNS tunneling, DNS rebinding, and so on.
- **Network sandbox**—Enables unknown files to be opened in a sandbox environment and scanned for malware or other threats.
- **Remote browser isolation (RBI)**—Enables websites to be rendered in a sandbox environment to detect and remove malware and threats before they reach the endpoint.
- **Support for managed and unmanaged devices**—Ensures support for the rapidly-increasing number of personal devices and contractor or temporary worker devices accessing an organization's digital assets, regardless of whether these devices have specific agents or security services on them.

Ideally, a SASE solution integrates these capabilities into as few products or services as possible, from as few vendors as possible. This creates a solution that operates as close to line rate as possible and is easier to manage. Daisy-chaining products from multiple vendors to create a SASE solution not only introduces latency that degrades the end-user experience but also creates organizational challenges in training staff to manage multiple, disparate products and correlating the information discovered by those products.

Zero Trust Network Access 2.0

In legacy VPNs, after you authenticate and connect to the network, you have access to all resources in the network. There are several deficiencies with this approach. Organizations should authorize access to only the resources that users absolutely require in order to complete their tasks. Similarly, the organization initially authorizing users' access to a resource should not imply that they can continue to access the resource when conditions, such as your security posture, change. Finally, an organization should monitor authorized access to protect information and applications from improper use. The Zero Trust security model remedies these deficiencies.

The Palo Alto Networks SASE solution provides the means to enable a ZTNA 2.0-compliant network. ZTNA 2.0 builds upon the tenets of a Zero Trust by including the following capabilities:

- **Least-privileged access**—Granting users the minimum access they require in order to perform their tasks. You achieve this by identifying applications at Layer 7, enabling precise access control at the app and sub-app levels, independent of network constructs like IP and port numbers.
- **Continuous trust verification**—After access to an app is granted, trust is continually assessed based on changes in device posture, user behavior, and app behavior.
- **Continuous security inspection**—Providing deep and ongoing inspection of all traffic, even for allowed connections, to prevent all threats including zero-day threats.
- **Protection of all data**—Providing consistent control of data across all apps used in the enterprise, including private apps and SaaS, with a single DLP policy.
- **Security for all apps**—Safeguarding all applications used across the enterprise, including modern cloud-native apps, legacy private apps, and SaaS apps. This includes apps that use dynamic ports and apps that leverage server-initiated connections.

SASE vs On-Premises Solutions

Palo Alto Networks has two solutions for securing access to distributed applications and data:

- Cloud-delivered network security (the SASE solution)
- On-premises network security (using next-generation firewalls at the edge)

Both options provide security for remote sites and mobile users, and both offer the same level of connectivity and security services. Although this guide focuses on the cloud-delivered network security solution, SASE, this document would be incomplete without mentioning the on-premises network security solution as a comparison.

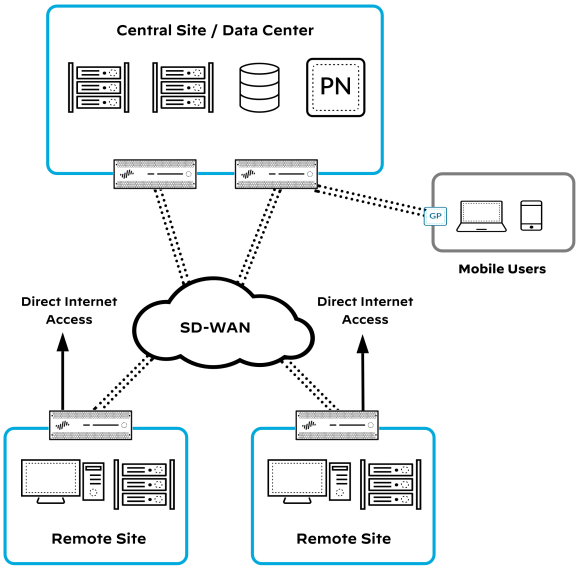
For some customers, a cloud-based solution may not be an option. The reasons may include:

- Using the next-generation firewall to provide segmentation at remote sites.
- Regulatory or compliance issues, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA) and payment card industry (PCI) data security standards, that may restrict the use of cloud services or drive the need for segmentation and DLP services at the remote-site edge.
- An existing investment in next-generation firewalls in their remote site and central locations.

The on-premises network security solution can use an edge next-generation firewall to provide the SD-WAN capabilities. Application-aware policy determines how the local LAN traffic should flow and whether outbound traffic is sent to the WAN or directly to the internet. The local firewall performs the Layer 7 traffic inspection and access control, threat prevention, and security services for users accessing internet-based applications and data.

The on-premises device is also the delivery method for the Palo Alto Networks cloud-delivered security subscriptions, such as DLP, WildFire® threat prevention, and SaaS Security.

Figure 2 On-premises SD-WAN and mobile-user access



Access for mobile users is provided by VPN tunnels from a client on the endpoint, terminated at the central site or sometimes a regional VPN access point.

The on-premises solution provides the security of controlling the infrastructure but at the expense of having to purchase, maintain, and manage the equipment at each site.

The Palo Alto Networks Approach

One of the challenges of deploying a SASE solution is integrating the various components into a coherent architecture. There are many vendors that may be strong in one or two aspects of SASE, such as CASB and SWG, but lack in other areas, such as FWaaS and SD-WAN. Organizations struggle with integrating solutions from various vendors and then training and maintaining the staff to manage the multiple point products.

However, Palo Alto Networks delivers the most comprehensive, integrated SASE solution in the security and networking industries—Prisma SASE—which includes the following main components:

- Prisma Access
- Prisma SD-WAN

PRISMA ACCESS

Prisma Access is a complete next-generation firewall delivered as a cloud-native service. It provides secure access to internet and business applications for both mobile users and remote sites, whether those applications are hosted in a corporate data center or a public cloud.

Prisma Access provides SWG access to users via either the GlobalProtect® app or clientless VPN service, providing support for managed device and unmanaged or guest devices. Remote sites can direct traffic destined for the internet to Prisma Access, providing secure, direct internet access from the remote sites without the requirement to backhaul traffic to a central site.

Zero Trust is a security model designed specifically to protect the security of sensitive data and critical applications. Palo Alto Networks Zero Trust Enterprise is a strategic, platform-based approach to security organized into three pillars: Zero Trust for users, Zero Trust for applications, and Zero Trust for infrastructure. Prisma Access enforces a Zero Trust for users access model with a combination of the following services:

- Integration with identity access management methods like security assertion markup language (SAML) allows strong authentication when validating users.
- GlobalProtect supplies device information and User-ID™ when users connect.
- Security policies combine App-ID™, User-ID, and threat prevention to enforce least-privileged access and scan application content for malicious activity.
- Inline DLP scanning and enforcement secure sensitive data flowing through the network.

Prisma Access extends support for the Zero Trust for infrastructure pillar with the IoT add-on, which provides additional inspection to identify headless devices in order to build least-privileged access policies for remote sites connected to Prisma Access.

The Prisma Access FWaaS capabilities inspect all traffic—not just HTTPS and HTTP. This enables Prisma Access to uniquely identify each application, user, and device accessing your services, enabling you to identify threats and create granular Zero Trust policies that control access to your most sensitive data and applications.

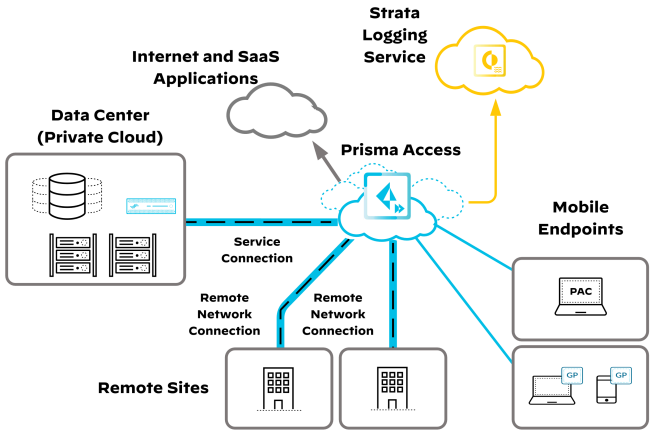
The visibility provided by Prisma Access also enables additional security services, such as the following:

- Threat prevention
- URL filtering
- Network sandboxing with WildFire
- DLP
- DNS Security
- SaaS application usage visibility and data security
- Integration with remote browser isolation services

Prisma Access' single-pass architecture provides these services. The single-pass architecture minimizes performance degradation by performing multiple operations only once on a packet, enabling Prisma Access to process your traffic at line-rate speeds. For more detail about these services, see the "Securing the Service Edge" section."

Security and operational data are sent to Strata Logging Service (formerly *Cortex Data Lake*) for operational information, anomaly detection, and forensics. SaaS Security uses the data Prisma Access sends to Strata Logging Service (SLS) to provide reporting on which SaaS applications users are accessing and how frequently.

Figure 3 Prisma Access

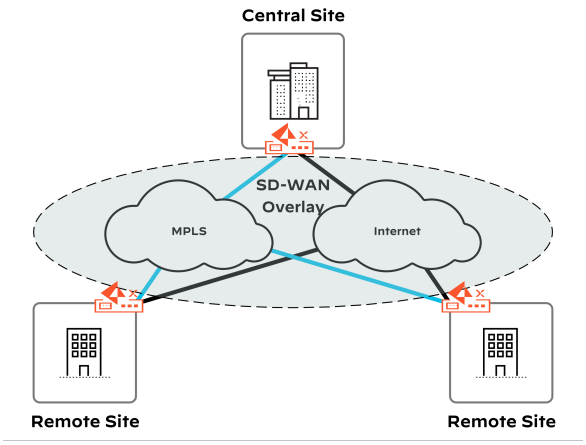


PRISMA SD-WAN

To enable simplified deployment across your organization, Prisma SD-WAN provides next-generation, software-defined, wide-area networking combined with cloud-orchestration. At the core of the system, Prisma SD-WAN uses built-in Layer 7 intelligence, providing application-aware networking, traffic steering, and security policies. It also allows for complete visibility into the application health across all locations and collects granular application-driven analytics, which you can use for monitoring and troubleshooting.

You enable the SD-WAN service by using Prisma SD-WAN Instant-On Network (ION) devices. Available in both hardware and virtual (software) forms, ION devices allow you to enforce policies based on business intent, enable dynamic path selection, and provide visibility into performance and availability for applications and networks. You can easily deploy your ION devices by using their zero-touch provisioning capabilities, reducing the burden of manual provisioning and the time it takes to onboard new sites.

Figure 4 Prisma SD-WAN



BENEFITS OF THE PALO ALTO NETWORKS SASE SOLUTION

There are many benefits to using the Palo Alto Networks SASE solution, including the following:

- **Cloud-native, cloud-based delivery**—Over 100 points of presence worldwide reduces latency, enhancing the user experience, and includes support of in-country or in-region resources and regulatory requirements.
- **Scalability**—Quickly and easily onboard users without overloading your existing infrastructure or needing to acquire and deploy additional resources. Bring new sites online quickly with the Prisma SD-WAN ION device.
- **Line-rate security**—Prisma Access's single-pass architecture provides a suite of security services without adding the latency that you would have when daisy-chaining security products.
- **Single vendor management**—The components of Palo Alto Networks SASE solution work together seamlessly, managed from a common portal. There is no need to figure out how to piece together various products from multiple vendors using multiple APIs and orchestration applications.
- **ZTNA 2.0 capabilities**—Using ZTNA 2.0, you can eliminate the deficiencies of legacy VPNs and overcome the limitations of early zero trust implementations.

Prisma SASE 3.0

Employees increasingly demand the freedom to be productive from anywhere, using any device, and accessing any application. Homes, coffee shops, and mobile phones have become seamless extensions of the corporate network. Many organizations also need to support contractors or third parties on their network. To enable this, companies have turned to multiple secure access tools, all with different policies, network sensors and management panes in place. This creates challenges in ensuring policy consistency and achieving a unified view of your network security.

As organizations look ahead, the limitations of a patchwork SASE approach become increasingly clear. These existing SASE solutions may have initially sufficed, but the compromises inherent in disconnected solutions will hinder your future growth in the following ways:

- **Security Gaps**—Contractors, third-party collaborators, and BYOD devices introduce unique security risks that your current solutions might not fully cover.
- **Inadequate Data Protection**—Limited data-classification capabilities can leave you vulnerable to potentially damaging data breaches.
- **Inconsistent Application Performance**—Legacy SASE models may impact user productivity because these models struggle to deliver the seamless user experience that modern dynamic applications demand.

The ideal solution is to adopt a complete, fully integrated SASE solution to provide security, visibility, and control from any device to any application.

Prisma SASE 3.0 provides security, visibility, and control from any device to any application. Through the use of innovations such as Prisma Access Browser, AI-powered data security, and App Acceleration, Prisma SASE 3.0 offers a fully integrated SASE solution with unified management and uncompromised application performance for both managed and unmanaged devices.

Securing the Service Edge

Prisma SASE provides more than a cloud-based firewall as a service and software-defined wide-area networking. To provide a complete solution for securing the service edge, Prisma SASE integrates many of the Palo Alto Networks security services through Prisma Access.

REDUCING RISK WITH VISIBILITY AND CONTROL

Adversaries can masquerade as legitimate traffic by hiding their malicious activities in everyday applications and tools, posing a sophisticated and stealthy threat. As an organization, you need to have full visibility and control of your traffic, including users, applications, and devices. You can't protect what you can't see, so network-wide visibility is important.

Decryption

Organizations secure most of their applications and services with encryption, and over 85% of their internet traffic is encrypted. This has become an opportunity for adversaries who are taking advantage of encryption in order to hide their malicious activities in encrypted sessions and evade detection. To provide inline protection, you need to decrypt traffic to have visibility so that you can detect threats, such as malware, that hide in encrypted sessions.

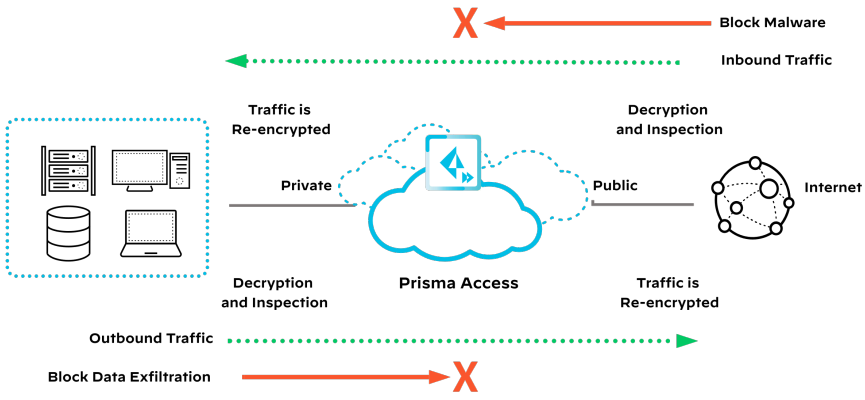
Malware can be hosted anywhere, not just within known risky applications, so it is important that you inspect all allowed traffic to detect malware. Because malware can be disguised in encrypted traffic, it is important to be able to decrypt traffic inline at all network perimeters and across traffic flows. For example, unsuspecting users can easily download malware from websites. Decryption capabilities allow you to enforce policies on encrypted traffic so that the firewall can prevent malicious, encrypted content from entering the network and prevent sensitive, encrypted data from leaving your network.

Prisma Access supports session decryption, which is applied as part of the single-pass architecture through a decryption policy on selected traffic that you define. After Prisma Access decrypts the traffic specified in your decryption policy, it enforces the security policy, providing protection against known and unknown threats while enabling users to access their data and applications. Prisma Access then re-encrypts the traffic before the traffic exits the system.

You can apply decryption policies to traffic flow inbound, outbound, or both. You can define sensitive traffic types, such as HIPAA data, as exempt from decryption policies. Prisma Access also decrypts TLS version 1.3 traffic, which future-proofs your network security investment as you start to adopt the new TLS standard.

Figure 5 shows a scenario with a private internal network and a public external network. Based on configured policy, Prisma Access decrypts traffic inbound from external networks in order to determine if there is malicious content to block. To ensure that no malicious activity, such as data exfiltration through an encrypted channel, is present in the outgoing traffic, Prisma Access also decrypts traffic coming from the internal network going to the internet. Prisma Access then re-encrypts traffic when the traffic leaves.

Figure 5 Decryption with Prisma Access



Applications, Users, and Devices

Applications reside in multiple locations, such as the campus, data center, public cloud, and SaaS providers. To determine their potential risks to their business, data, and resources, you must determine which applications are sanctioned or unsanctioned. Adversaries like to leverage common applications in order to hide their activity within the network and leverage compromised or stolen credentials in order to invoke malicious activity and steal data.

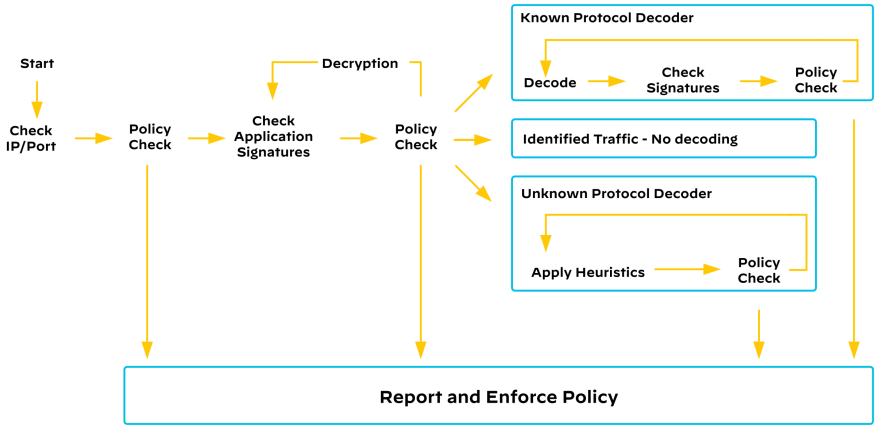
To reduce risk and protect themselves against threats, organizations need to have full visibility into the applications used on the network, including which users and devices are accessing them. This provides a baseline of normal activity and allows you to detect abnormal activity.

To have visibility and control of the applications' use requires the ability to identify and classify applications, irrespective of the port, protocol, encryption, or potential evasive technique. It is critical that you can identify which device or user is accessing an application, identify the source of file transfers, and identify devices and users that may be transmitting a threat. This visibility allows you to strengthen your security policies and reduce your incident response time. Palo Alto Networks enables this visibility at the application, user, and device level by providing the following features integrated into Prisma Access:

- **App-ID**—App-ID uses multiple identification techniques in order to determine the exact identity of applications traveling through your network, including those that try to evade detection by disguising themselves as legitimate traffic, by hopping ports, or by using encryption. To match based on actual applications rather than port numbers, App-ID is used in combination with security policies.
- **User-ID**—User-ID enables you to leverage user information stored in a wide range of repositories, such as LDAP and user authentication, via security assertion markup language. User-based policy controls can include application information, including its category and subcategory, its underlying technology, and its application characteristics. You can define policy rules in outbound or inbound directions in order to safely enable applications based on users or groups of users.
- **Device-ID**—Device-ID enables you to use device information in your security policies, rather than an IP address. You can identify devices by their attributes, such as a device type (for example, a printer), model, software version, or vendor.

App-ID, User-ID, and Device-ID are important features for an effective security infrastructure because they provide Prisma Access with visibility, policy control, and logging and reporting capabilities.

Figure 6 App-ID policy enforcement



IoT Security

IoT devices are on the increase because many organizations are deploying IoT devices into their environments in order to increase productivity, help with digital transformation, and provide operational efficiency. IoT devices can vary from simple printers and security cameras to advanced robotic and medical devices. Unfortunately, IoT devices bring a new challenge to securing your organization. Often, IT departments do not have complete visibility of the IoT devices on the network. IoT devices often run outdated or unpatched operating systems. And IoT devices are often deployed without changing the default user ID and password.

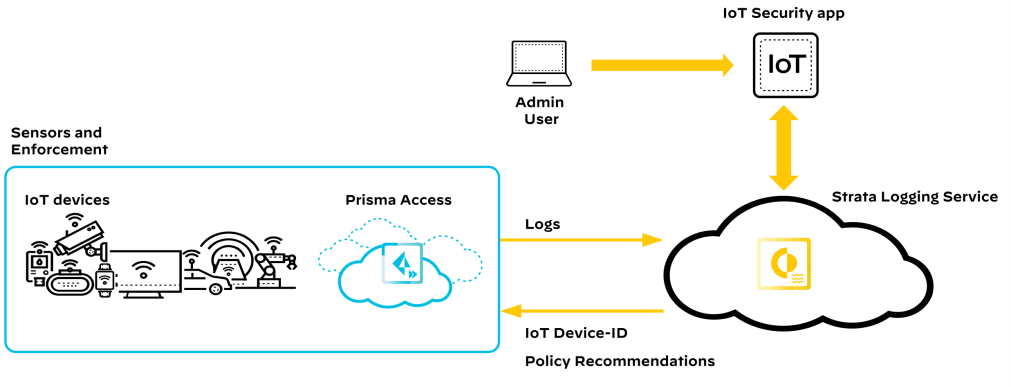
Palo Alto Networks offers a cloud-delivered, subscription IoT security solution, which is available on Prisma Access for networks. The IoT Security subscription provides discovery of all devices and provides visibility and security risk-reduction actions based on detailed information received from all discovered devices. You achieve discovery, visibility, and enforcement with Prisma Access, as opposed to other solutions that require you to buy separate probes in the network.

IoT introduces a concept of policy enforcement by using Device-ID. Similar to the use of App-ID and User-ID, you can use Device-ID to define policy based on the attributes of the device, regardless of any changes to the IP address or physical location.

Prisma Access security-processing nodes are an important part of IoT security because they behave as sensors and generate enhanced application logs. The security processing nodes send the logs to SLS, where the IoT Security app leverages this data. The IoT Security app analyzes the data, maps IP addresses to devices, and recommends policy rules. You can create security policy rules from the IoT Security app and import them to Prisma Access for enforcement.

> **Note**
>
> For accurate and complete device identification, Prisma Access needs to observe DHCP broadcast and unicast traffic. The IoT Security app automatically detects new devices from this traffic.

Figure 7 IoT Security solution



CONNECTING AND SECURING SITES

You have a number of choices when you want to connect and secure multiple locations. Your choices depend on your network's architecture and connectivity requirements. This section describes a remote-site interconnection solution that uses Prisma SD-WAN. This section also describes secure direct internet access solutions for all sites and offers flexibility in how you deploy a cloud-delivered firewall option that uses Prisma Access and Prisma SD-WAN.

When you connect a remote site to your organization's network, you can use the connection for the following purposes:

- You can secure access to private applications.
- You can secure access from the remote site to the internet.

You can also choose to secure access for both purposes concurrently.

When you host the private applications in a central site or data center, you can use a private WAN or SD-WAN in order to provide access to the applications. How you provide secure access to private applications does not depend on the method you choose for providing secure access to the internet. In some cases, you might not need to provide any internet access for remote-site users. However, in most cases, your remote-site users and devices require some basic level of internet access.

Alternatively, depending on your organization's requirements, users at remote sites might need to access only SaaS applications and there are no private applications hosted in private data centers. If this is the case, then the organization might not require any private WAN or SD-WAN to connect remote sites to central sites. You would only need to provide secure access from the remote site to the internet.

Prisma Access

To provide the same firewall services that an on-premises NGFW can deliver, Prisma Access uses a cloud-based infrastructure. This allows your organization to avoid the challenges of sizing firewalls and allocating compute resources for a multi-site deployment, minimizing coverage gaps or inconsistencies associated with your distributed organization. The elasticity of the cloud scales as demand shifts and traffic patterns change. The cloud service operationalizes next-generation security deployment to remote sites and mobile users by leveraging a cloud-based security infrastructure managed by Palo Alto Networks. The security processing nodes deployed within the service natively inspect all traffic in order to identify applications, threats, and content. Prisma Access provides visibility into the use of SaaS applications and the ability to control which SaaS applications are available to your users.

Prisma Access for networks provides security services and threat prevention for all your sites, safely enabling commonly used applications and web access. You connect remote sites to Prisma Access via an industry-standard, IPSec, VPN-capable device. Globally, Prisma Access offers over 100 sites to which you can connect, making web pages localized in-country and reducing the latency of going to cloud-hosted applications.

Prisma Access is ideally suited for any site with one or multiple internet links, provides direct internet access, and directly connects enterprise remote sites. Prisma Access provides direct internet access without the requirement to backhaul traffic to a central site. Functionally, there is no need to compromise on remote-site security, because Prisma Access provides the same security, visibility, and control as provided by the Palo Alto Networks next-generation firewalls at the central site.

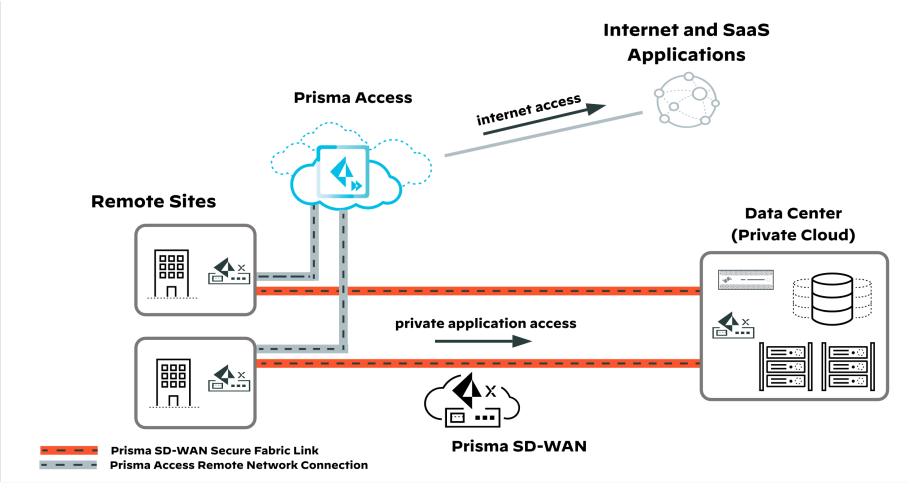
Prisma SD-WAN

Prisma Access with Prisma SD-WAN provides cloud-delivered, consistent security to all your sites, giving you full visibility and control of all your applications. The solution consists of a Prisma SD-WAN ION device deployed at a site managed from Strata Cloud Manager.

Prisma SD-WAN creates a secure fabric and service links over multiple types of WAN services and connections, including MPLS, direct internet, long-term evolution, and Prisma Access. This allows you to control and optimize all your WAN links. Internal user-traffic is protected by using IPSec tunnels over the public networks, ensuring data privacy through strong encryption. The ION devices automatically choose the best WAN path for your applications based on business policy and real-time analysis of the application performance metrics and WAN links.

Because Prisma SD-WAN is Layer 7 application–aware, it can use application-based policies to make packet forwarding decisions. These policies take precedence over the forwarding information in the routing tables. Prisma SD-WAN's application awareness also lets you prioritize specific applications and application types in times of high network utilization. Application-aware QoS enables you to keep your critical applications available and responsive during surges in network traffic.

Figure 8 Prisma Access with Prisma SD-WAN



CONNECTING AND SECURING MOBILE USERS

When you want to connect and secure your mobile users, you have a number of choices. Your choices depend on your network's architecture and connectivity requirements. This section describes a remote-access solution that uses Prisma Access.

When you connect a mobile user to your organization's network, you can use the connection for the following purposes:

- You can secure access to private applications.
- You can secure access from the mobile user to the internet.

You can also choose to secure access for both purposes concurrently.

When you host the private applications in a central site or data center, you can use Prisma Access in order to provide access to the applications. How you provide secure access to private applications does not depend on the method you choose for providing secure access to the internet. In some cases, you might not need to provide any internet access for remote-site users, However, in most cases, your mobile users require some basic level of internet access.

Alternatively, depending on your organization's requirements, mobile users might need to access only SaaS applications and there are no private applications hosted in private data centers. If this is the case, then the organization might not require any access to central sites. You would only need to provide secure access to the internet.

Prisma Access provides a cloud-delivered, scalable, and secure remote-access solution for all your mobile users. It provides consistent application visibility and control for all users, regardless of their location. The Prisma Access backbone interconnects a global network of more than 100 secure access locations. This allows users to connect to websites within their own country for localized content. The Prisma Access backbone uses VPN technology to keep your enterprise traffic secure and separated from other organizations' traffic.

There are three connection methods for securing mobile-user access with Prisma Access:

- The GlobalProtect app on managed endpoints
- Prisma Access explicit proxy via a proxy auto-configuration (PAC) file managed by your organization
- Prisma Access Clientless VPN for unmanaged endpoints to access secured applications via the Prisma Access gateway

Securing Access with GlobalProtect

The GlobalProtect app connects to a Prisma Access cloud-based portal, where the app authenticates and obtains configuration information and a list of Prisma Access gateway locations. The GlobalProtect app then chooses the best Prisma Access node to connect to in order to access internet or on-premises applications. In addition to HTTP and HTTPS, the GlobalProtect app and Prisma Access provides secure connectivity to applications across all ports and protocols.

Also, if required, the GlobalProtect app inventories the endpoint configuration and builds a host information profile (HIP) that it shares with Prisma Access. You can use this information to build HIP-based policies based on several attributes, including the following:

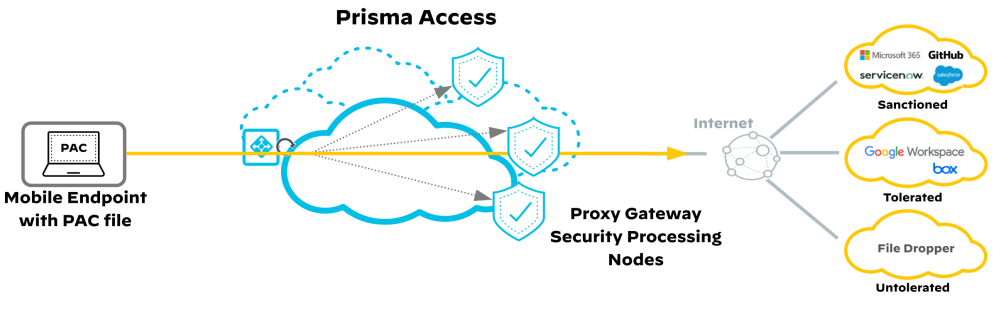
- The operating system and application-patch level.
- The version and state of the host anti-malware or firewall.
- Customized host conditions (examples: registry entries, running software)

Based on the endpoint operating system, Prisma Access can provide differentiated authentication profiles and methods, which Prisma Access determines through the information pushed from the GlobalProtect app. For example, Windows endpoints can use an LDAP authentication method, while Android endpoints use SAML. The GlobalProtect app runs on Windows, macOS, Linux, iOS, Android, and Chrome. For unmanaged personal, partner, and contractor endpoints on which you can't install a client, the Prisma Access clientless VPN provides secure access from SSL-enabled web browsers without installing the GlobalProtect app.

Explicit Proxy

In addition to using the GlobalProtect connection method, you can also use the explicit-proxy connection method to connect to Prisma Access in order to provide a secure web gateway for mobile users who have managed devices accessing the internet and SaaS services. If you have already been using an on-premises explicit proxy to secure internet-bound traffic, the Prisma Access explicit-proxy method provides an easy migration option. To migrate away from an existing on-premises proxy service, you configure the user's operating system or browser to point to the new Prisma Access explicit-proxy URL. The ability to limit the changes to a browser reconfiguration allows organizations to easily migrate to a cloud-based SWG.

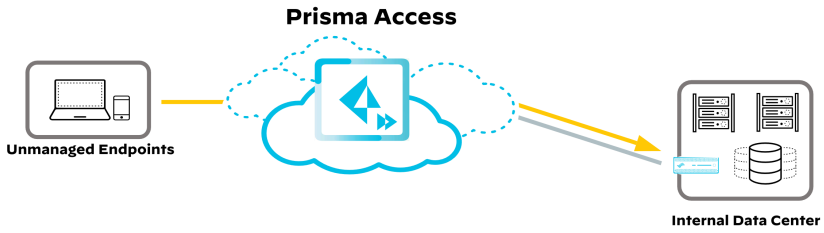
Figure 9 Prisma Access explicit proxy



Clientless VPN

For unmanaged personal, partner, and contractor endpoints on which you can't install a client, the GlobalProtect clientless VPN provides secure access to on-premises applications from SSL-enabled web browsers without installing the GlobalProtect app. Clientless VPN proxies access for the web applications that you make available to them.

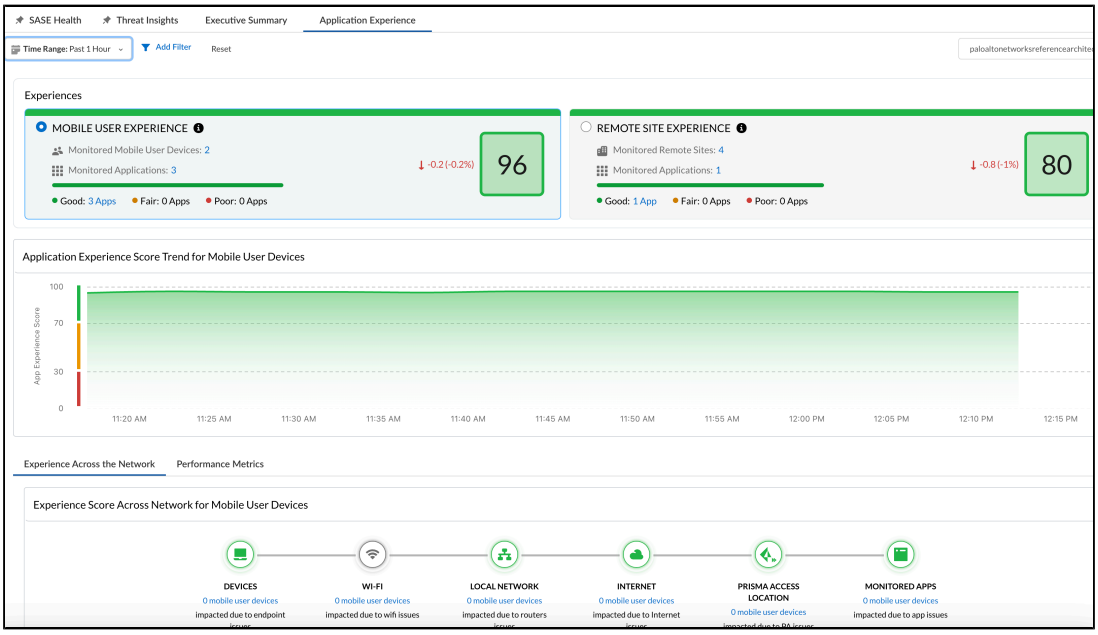
Figure 10 Clientless VPN



Monitoring the User Experience

Autonomous Digital Experience Management (ADEM) is a service that provides native, end-to-end visibility and insights for all users and remote site locations in your SASE environment. ADEM delivers visibility with segment-wise insights across the entire service delivery path, including intelligence gathered from endpoint devices, synthetic tests, and real user traffic. ADEM also monitors application and endpoint performance at remote site locations and natively integrates with Prisma SD-WAN for comprehensive overlay and underlay remote-network performance visibility on all configured WAN paths.

Figure 11 ADEM application experience



The ADEM functionality is natively integrated into the GlobalProtect app for mobile-user experience monitoring, and into the Prisma SD-WAN ION device operating system for remote network monitoring. With ADEM, you do not need to deploy any additional appliances or software in order to monitor your user's application experience.

AI-Powered ADEM is an integration of AIOps with ADEM. It combines artificial intelligence and machine -learning capabilities in order to automatically identify patterns, detect anomalies, perform event correlation, and generate alerts. These capabilities allow customers deep visibility into the IT infrastructure and help automate complex IT and NOC functions, increase productivity, and reduce mean-time-to-resolution. To proactively remediate issues that can cause service interruption, IT teams can now leverage AI-based problem detection and predictive analytics.

AI-Powered ADEM uses ADEM as a foundation, and it enriches the data collected by ADEM by using AI/ML models built by Palo Alto Networks. You don’t need to configure anything for this capability. After activation, it is enabled by default. For this capability to function, you need only to configure ADEM and activate the AIOps license.

BLOCKING INTERNET AND DNS THREATS

Organizations use multiple websites for everyday productivity. Adversaries can compromise these sites with multiple security threats that can harm your organization. A compromised website can deliver threats through injection flaws, security misconfigurations, or *cross-site scripting*, where an adversary uses scripts delivered in a user's web browser to deliver malicious code or hijack the user's session.

Common threats include phishing, exploit kit delivery, malware, credential theft, data theft, command-and-control (C2) attacks, and ransomware. Adversaries often execute these types of threats from malicious and compromised websites, often unknown to the website owners. Adversaries leverage multiple tools and techniques, including automation, to generate thousands of malicious URLs daily and exploit DNS to deliver malware and exfiltrate data.

It's important to verify which users are accessing which websites and, at the same time, protect their users from exposure to threats. Palo Alto Networks offers a comprehensive solution to provide safe web access by restricting access to known harmful sites and securing user sessions that are accessing web content.

URL Filtering to Secure Web Access

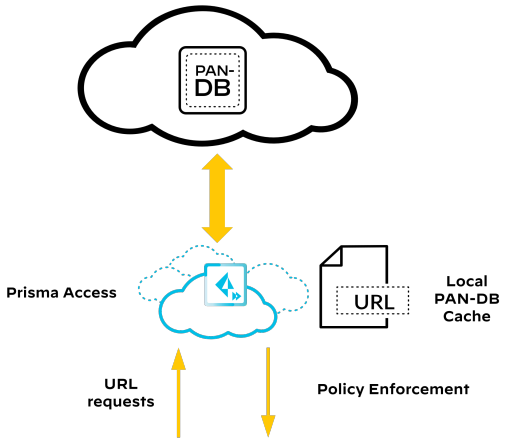
URL Filtering complements User-ID, Device-ID, and App-ID by enabling you to configure Prisma Access to identify and control access to websites at a per-user level. You can use the URL category as a match criterion in policies, which permits exception-based behavior and granular policy enforcement. For example, you can deny access to malware and hacking sites for all users but allow access for users who belong to the IT security group. This protects your organization from websites hosting malware and phishing pages while allowing access only for those users who might need it. Palo Alto Networks offers a URL Filtering subscription that provides granular control, credential theft protection, user-based policies, and selective SSL decryption.

When you enable URL Filtering, it compares all web traffic against the URL-filtering database, PAN-DB, which contains millions of URLs grouped into approximately 65 categories. You can classify sites based on their content, features, and risk. The malware and phishing URL categories in PAN-DB update in real time, which means that if a first attempt to access a malware or phishing is treated as unknown, URL Filtering matches subsequent attempts against the updated URL-filtering database and prevents user access. For fast and easy access to frequently visited URLs, PAN-DB provides high-performance local caching.

The security processing nodes in Prisma Access use a seed database as a cache for URLs from PAN-DB. If Prisma Access does not find a URL in the cache, it contacts PAN-DB to lookup the URL. Security policies use URL Filtering profiles in order to either allow or deny access to a URL based on a category. Other options including asking the user if they want to proceed to the site and logging the traffic.

Dynamically analyzing and detecting malicious content by using machine learning prevents malicious variants of JavaScript exploits and phishing from entering your network. ML examines multiple web page details through a series of ML models. The ML model looks at patterns, decoder fields, and file details to determine a probability, classification, and verdict. ML then sends malicious URLs to PAN-DB for additional analysis.

Figure 12 URL Filtering comparing web traffic against the URL-filtering database, PAN-DB



By preventing users from going to phishing sites, URL Filtering can protect users in real time against attempts to steal user credentials. URL Filtering can prevent users from submitting corporate credentials to untrusted sites but allow them to use their credentials on sanctioned corporate sites. Even if someone steals a user's credentials, multi-factor authentication (MFA) can prevent the abuse of those credentials. Prisma Access supports multi-factor authentication and integrates with multiple MFA vendors through APIs. MFA on Prisma Access works in conjunction with an authentication portal, which challenges the user to input an additional authentication factor beyond their standard credentials.

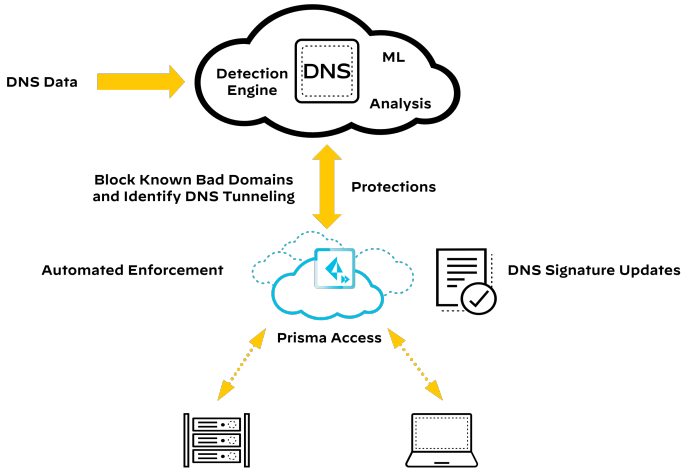
Securing DNS

DNS is required for domain-name-to IP-address mapping translation, which is common when users are accessing external resources, such as websites. At the same time, DNS is a massive and frequently overlooked attack surface. Adversaries can compromise DNS and use it for malicious activity in order to steal data or establish connections with C2 servers.

Adversaries can use DNS tunneling in order to encode data of non-DNS based programs with DNS queries and DNS responses, which the adversaries can often use as a channel to exfiltrate data. Palo Alto Networks DNS tunneling detection can detect a tunnel-based attack and block it with security policies, avoiding data theft.

Static lists of malicious DNS entries and manual responses don’t scale. The DNS Security service from Palo Alto Networks is a subscription-based service that is designed to protect and defend your network from advanced threats that are using DNS. The DNS Security service leverages machine learning and predictive analytics to provide real-time DNS request analysis. The analysis enables production and distribution of DNS signatures that are specifically designed to defend against malware that uses DNS for command-and-control and data exfiltration.

Figure 13 Securing DNS with the DNS Security service



The DNS Security service allows Prisma Access to sinkhole internal DNS requests, which allows the Prisma Access security processing node to forge a response to a DNS query for a known malicious domain or URL and then causes the malicious domain name to resolve to a definable, fake IP address given to the client. If the client attempts to access the fake IP address, a security rule blocks traffic to this IP address and logs the information.

The DNS Security service also uses techniques such as domain-generation algorithm (DGA) detection and DNS-tunneling detection. Because malicious domains are frequently autogenerated by machines, a DGA analysis determines whether it was a person or machine that likely generated a domain. By reverse-engineering and analyzing other frequently used techniques, the DNS Security service can identify and block previously unknown DGA-based threats in real time.

Securing Web Access with Remote Browser Isolation

With the rise of web-based applications, the web browser has become one of the biggest attack vectors against endpoints. Threats can hide in a website's code or malicious sites accessed through legitimate, approved sites, such as ransomware accessed by a seemingly legitimate advertisement on a benign site.

Prisma Access decrypts traffic and can detect both known and unknown threats in files and can use Advanced URL filtering to provide site and site-category allow and deny lists. However, with the proliferation of new web sites and applications every day, it can be difficult to manage uncategorized or unidentified sites. Simply blocking them can create user frustration or operational overhead because your security team must evaluate each unknown requested site to determine if they are a threat or should be allowed.

To alleviate the threat of unknown sites and the operational overhead of managing access to those sites, Prisma Access has a native RBI.

Policies in Prisma Access send requests for specific sites, such as unknown or uncategorized sites, or even specific categories of sites, to the service. There, the sites are rendered in a remote container, away from the endpoint and corporate network, and examined for threats and vulnerabilities. Any malicious content is rendered in the remote container, and only safe content is allowed through to the end user.

Natively integrated with Prisma Access, RBI allows you to easily apply isolation profiles to your existing security policies. To keep sensitive data and information secure, isolation profiles can restrict browser controls such as copy-and-paste actions, keyboard inputs, and sharing options such as uploading, downloading, and printing files. All traffic in isolation undergoes analysis and threat prevention provided by Cloud-Delivered Security Services (CDSS) such as Advanced Threat Prevention, Advanced WildFire, Advanced URL Filtering, DNS Security, and SaaS Security.

With User-ID, you can create policies to protect high-risk users who are often specifically targeted, such as your company executives, from attacks by sending all their web-application and cloud-application traffic to the RBI service.

DETECTING THREATS AND ENFORCING POLICY

With all these advanced threats facing your organization, you need a comprehensive solution that protects your network against malicious attacks, blocking each step of the cyberattack lifecycle. Palo Alto Networks stops malicious activity by using multiple features and functions, but this section focuses on two key features: Threat Prevention and WildFire.

Threat Prevention

Threat Prevention is a subscription for Prisma Access that provides comprehensive protection against all threats, irrespective of port, protocol, and encryption. When Threat Prevention is licensed and enabled on Prisma Access, the Prisma Access security processing nodes scan, inspect, classify, and block threats in a single pass.

The Threat Prevention subscription contains security profiles, which Prisma Access uses in order to prevent threats from compromising your network. You use *security policy rules* to allow or deny traffic, and you use *security profiles* to scan the allowed traffic for threats. When traffic matches the allow rule defined in the security policy, the security profiles attached to that rule provide additional content scanning capabilities. Default profiles are available, or you can create your own custom profiles.

The Threat Prevention subscription uses the following default security profile groups:

- **Antivirus profiles**—Prisma Access uses a stream-based malware prevention engine to protect against downloads of common malware types, such as viruses, worms, trojans, and spyware. These profiles scan for a wide variety of malware in executables. You can use application exceptions to avoid false positives. These profiles provide protection against malware concealed in common file types, such as Microsoft Office documents and PDFs.
- **Anti-spyware profiles**—You can use anti-spyware profiles to block spyware on compromised hosts reaching out to external C2 servers. You can apply anti-spyware profiles to inspect all zone traffic, and you can apply various levels of protection between zones. Compromised hosts try to access malicious sites. In order to prevent access to these sites, you can enable DNS sinkholing within the anti-spyware profile, which enables the Prisma Access to respond to DNS queries for known malicious domains. The Prisma Access security processing node makes the DNS query resolve to an IP address you specify, which helps to identify the infected hosts attempting to reach the DNS sinkhole address.
- **Vulnerability protection profiles**—At the network and application layers, these profiles detect and block exploit attempts and evasive techniques, including port scans, buffer overflows, remote code execution, protocol fragmentation, and obfuscation. The profiles stop attempts based on threats that have patterns related to exploits' attacks on system vulnerabilities.

The Threat Prevention subscription bundles the antivirus, anti-spyware, and vulnerability protection profiles into one license. In addition to the Threat Prevention subscription, in order to avoid threats, you can leverage the following additional default profile groups in the URL Filtering and WildFire services:

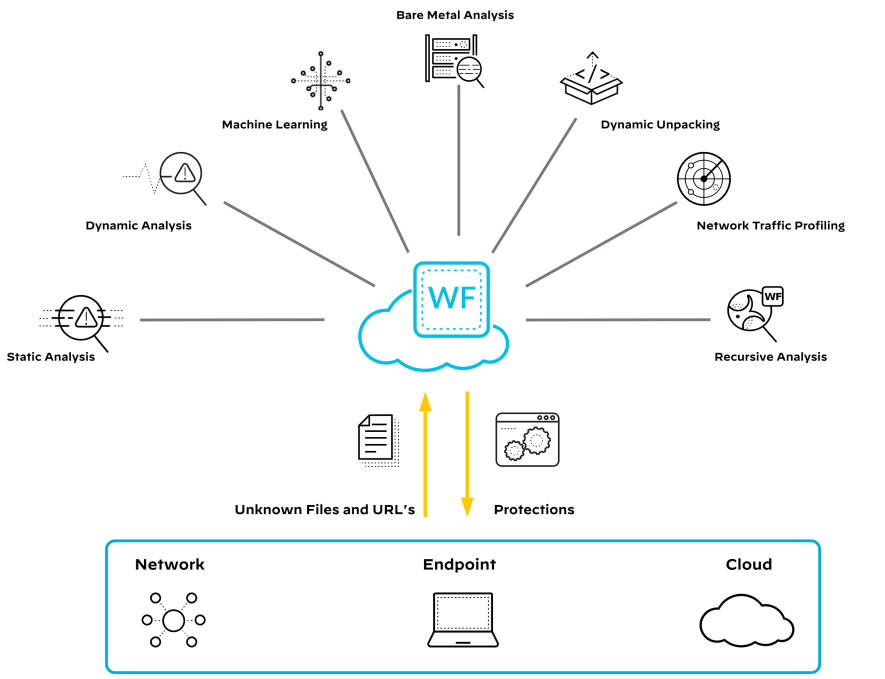
- **Data-filtering profiles**—With data-filtering profiles, you can define data patterns for which you want to filter, such as credit card information, social security numbers, HIPAA data, and many more. Within the profile, you can define whether you want to block, alter, or log the activity. You can use a default data-filtering profile or customize your own. With a data filtering profile, you can avoid data theft by blocking the specific types of data (based on data patterns) that are not permitted to leave your environment.
- **File-blocking profiles**—These profiles allow you to identify specific file types that you want to block or monitor. For most traffic, including traffic on your internal network, you want to block files that are known to carry threats or that have no real use case for upload or download. Based on the specific matching file types and applications, file-blocking profiles block prohibited, malicious, and suspect files in order to protect end users from downloading or uploading known malware executables.
- **DoS-protection profiles**—DoS attacks cause disruption to a targeted server or services. DoS-protection profiles allow you to control the number of sessions between interfaces and zones in order to avoid an internal session attack from a compromised host within the network. DoS-protection profiles protect the network and resources from a *flood attack*, where an adversary attempts to overwhelm network resources by sending too many packets or by using many hosts to establish multiple sessions. The profile supports settings for SYN, UDP, and ICMP floods.
- **Zone-protection profiles**—These profiles increase network security and prevent lateral movement activities. Within a zone-protection profile, you have the ability to configure reconnaissance protection. Zone-protection profiles have configurable settings for flood attack protection, reconnaissance protection, packet-based attack protection, and protocol protection. Enabling lateral movement reconnaissance protection allows you to configure settings for TCP and UDP port scans as well as host sweeps. The settings include response actions based on configured time intervals.
- **URL Filtering profiles**—Covered previously, these profiles enable you to configure Prisma Access to use URL categories in order to control access to websites and protect your organization from websites hosting malware and phishing pages.
- **WildFire analysis profiles**—These profiles forward unknown files or email links to WildFire for analysis. You can specify forwarding based on the application, file type, and traffic direction.

WildFire

Palo Alto Networks offers a security service, *WildFire*, which is a threat intelligence cloud and virtual sandbox that provides machine-learning analytics capabilities in order to prevent known and unknown threats. When a Prisma Access security processing node receives a file or URL, it determines whether WildFire has seen it before and what the verdict was. If the file or URL is unknown, Prisma Access forwards it to WildFire for analysis. WildFire determines whether it is benign, grayware, malware, or a phishing threat and then provides a verdict immediately for WildFire subscribers. WildFire provides content signatures for prevention. A single signature protects against millions of polymorphic variants of a single malware.

In addition to protecting you from malicious and exploitive files and links, WildFire looks deeply into malicious outbound communication, disrupting C2 activity with anti-C2 signatures and DNS-based callback signatures. WildFire also feeds this information into URL Filtering with PAN-DB, which automatically blocks newly discovered malicious URLs. This correlation of threat data and automated protections is key to identifying and blocking ongoing intrusion attempts and future attacks on your organization, without requiring policy updates and configuration commits.

Figure 14 WildFire multiple-threat analysis techniques



WildFire provides multiple techniques to uncover and prevent new threats, techniques such as dynamic analysis, machine learning, static analysis, bare-metal analysis, and a custom-built hypervisor. The multiple techniques detect threats that would normally evade single-technique sandbox environments.

To uncover hidden threats in the files and URLs that WildFire examines, WildFire identifies hundreds of potentially malicious behaviors, including the following:

- **Changes made to host**—WildFire monitors all processes for modifications to the host, including file and registry activity, code injection, memory heap-spraying (exploits), mutexes, Windows service activity, the addition of auto-run programs, and other potentially suspicious activities.
- **Suspicious network traffic**—WildFire performs analysis of all network activity produced by the suspicious file, such as creating backdoors, downloading next-stage malware, visiting low-reputation domains, performing network reconnaissance, and more.
- **Anti-analysis detection**—WildFire monitors techniques used by advanced malware that is designed to avoid virtual machine–based analysis, such as debugger detection, hypervisor detection, code injection into trusted processes, disabling of host-based security features, and more.

Leveraging innovations in machine learning, artificial intelligence, and big-data analytics is the only way to stay ahead of a fast-moving adversary. However, all such analytics solutions depend on massive amounts of data from many sources in order to identify new threats and exploit techniques and to generate and share threat intelligence. These threat-intelligence capabilities are strengthened when information is combined across a large base of contributors. Sharing data acquired from multiple organizations to identify malicious behavior and their sources benefits the entire community. This sharing model enables rapid response across a broad base in order to prevent successful cyberattacks.

SECURING DATA

Organizations are increasingly relying on cloud-based solutions for storing sensitive data. Data stored in SaaS applications is subject to additional risks than data stored in a traditional, on-premises data center. These risks include files with confidential or sensitive data, such as health, financial, or other personally identifiable information stored in a public folder or with incorrect sharing settings, and files with malware uploaded and rapidly shared throughout the organization.

To address these risks, the Palo Alto Networks SASE solution uses next-generation CASB, which provides SaaS application visibility and control, data protection and governance, and threat prevention. The two elements of next-generation CASB are SaaS Security, which consists of SaaS Security Inline and SaaS Security API, and Enterprise DLP.

Securing Data Stored in SaaS Applications

SaaS Security contains a growing database of SaaS applications, currently with over 15,000 entries, with associated risk scores for each application. These risk scores enable you to monitor and evaluate the risks associated with unsanctioned yet tolerated SaaS applications and to control access to unsanctioned applications.

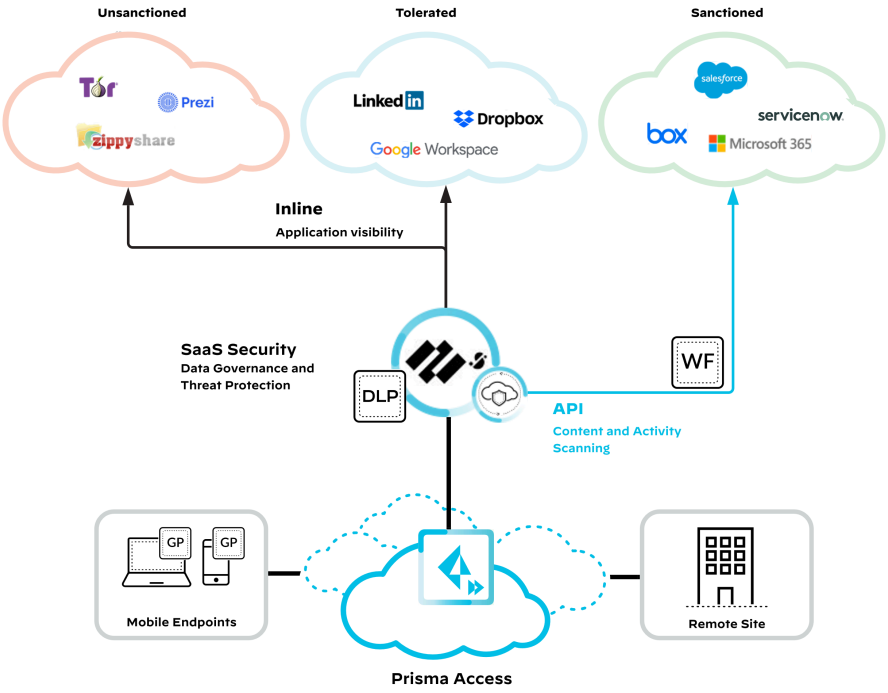
SaaS Security can help you to create Zero Trust policies that do the following:

- Monitor and control employee use of SaaS applications.
- Protect the transfer of credentials and sensitive data to sanctioned and unsanctioned apps, keeping corporate and employee data safe.
- Monitor data in the SaaS applications for compliance to storage standards for sensitive data, such as PII, PCI, and other compliance standards
- Block ever-evolving threats, ensuring that prevention is consistent and minimizing risk of data and time loss.

To secure the data in your sanctioned SaaS applications and data moving to and from SaaS applications, SaaS Security has the following two components:

- **SaaS Security API**—Provides threat protection, data exfiltration, and sensitive data loss prevention for information stored in your sanctioned SaaS applications
- **SaaS Security Inline**—Provides visibility into the SaaS applications your users access, whether the applications are sanctioned or not, enabling you to create policies to control that access.

Figure 15 SaaS Security



SaaS Security API

After your data leaves your network and is stored in a SaaS application, Prisma Access can't see access and changes to the data. Palo Alto Networks SaaS Security provides visibility and control for data stored in SaaS applications. Visibility and control even extend to data and activities that originate on personal devices and collaborators who aren't part of your organization, enabling Zero Trust policies to extend into your SaaS environments.

SaaS Security API provides security for data-at-rest in your sanctioned applications. When you first connect a sanctioned SaaS application to SaaS Security, the application's API allows SaaS Security to discover and retroactively inspect all files and data (called *assets* in SaaS Security) managed by the application. SaaS Security inspects and analyzes all assets and identifies exposures, external collaborators, risky user behavior, and sensitive documents, as well as identifying the potential risks associated with each asset. The service also performs deep content inspection and protects both historical assets and new assets from malware, data exposure, and data exfiltration in near real-time. SaaS Security leverages Palo Alto Networks Enterprise DLP to categorize sensitive and regulated data and the WildFire malware analysis engine to identify and protect against all file-based threats.

As SaaS Security identifies incidents, you can assess them and define automated actions to remediate the incidents or alert users and administrators to the risks. For ongoing incident assessment and protection, in addition to the initial inspection of historical assets, SaaS Security continuously monitors the SaaS application and applies the policy to new or modified assets.

SaaS Security Inline

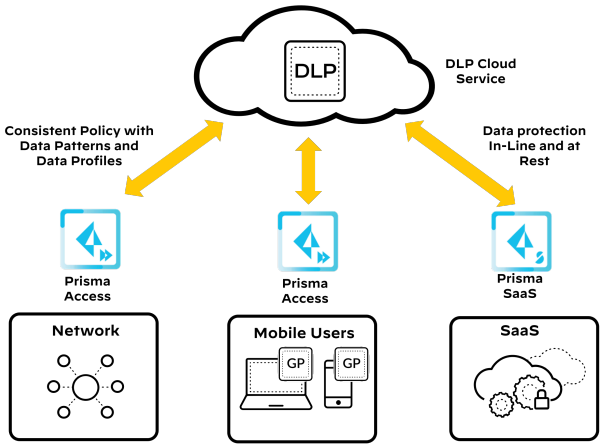
SaaS Security Inline provides security for data-in-motion. SaaS Security Inline works in conjunction with Prisma Access to monitor access to SaaS applications and evaluate the data being sent or retrieved. The SaaS Security Inline service uses cloud-based machine learning in order to discover SaaS applications The service also provides advanced analytics and reporting, so that your organization has the insight into the data-security risks of sanctioned and unsanctioned SaaS application use, or *shadow IT*, on your network. You can monitor the use of unsanctioned applications and create policies to block them altogether, or you can limit access to tolerated unsanctioned applications to specific users or groups. SaaS Security Inline provides complete control of SaaS application use from your corporate network and managed devices that traverse Prisma Access. To provide a consistent management experience, it integrates with your existing security.

Using both API-based and inline services, the Palo Alto Networks SaaS Security portfolio of services provides visibility and control of your SaaS applications. Without your reconfiguring your network, adding probes, or configuring endpoints, SaaS Security provides complete CASB services with visibility across all users accessing a SaaS application.

Data Classification with Enterprise DLP

The Palo Alto Networks Enterprise DLP service is a cloud-based subscription service that uses advanced analytics and machine learning to discover, monitor, and protect your sensitive data.

Figure 16 Enterprise DLP service



The DLP cloud service provides detection and response through data policies. Detection rules find and classify sensitive information based on data patterns. Response rules are actions that mitigate the risk of data loss, such as blocking an action for example.

The DLP cloud service uses pre-defined patterns, as well as DLP profiles, to provide a much more granular data matching option than just using search patterns. Today, over 380 patterns and 17 data profiles are available, including profiles for GDPR, CCPA, PII, and many other requirements.

The predefined data patterns match on keywords and strings. You also can create your own custom data patterns and file-property data patterns. You can create custom data patterns with regular expressions and keywords. For looking at metadata and other file attributes, you can create file-property data patterns to match on a name-value pair.

Data profiles are a combination of multiple patterns. To narrow down what you want to find, the profiles use machine learning and document properties to reduce false positives and be more specific. Data profiles use Boolean operations on matches, allowing you to match different confidence levels and patterns. For example, you could match on patterns A and C and not pattern B.

Next Steps

This guide provided a brief overview of SASE and the Palo Alto Networks implementation of an end-to-end, next generation SASE solution. It introduced SASE and the products and capabilities of the Palo Alto Networks portfolio that support deploying a SASE solution for your remote sites and mobile users.

For a more in-depth discussion of how you can leverage Palo Alto Networks to develop a SASE solution for your organization, see the "Related Documentation" section, particularly the following guides:

- **SASE for Securing Internet: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations.
- **SASE for Securing Private Applications: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure access to private applications for mobile users and users located at remote-site locations.

Feedback

You can use the **feedback form** to send comments about this guide.

HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
https://www.paloaltonetworks.com

Phone: +1 (408) 753-4000
Sales: +1 (866) 320-4788
Fax: +1 (408) 753-4001
info@paloaltonetworks.com

You can use the **feedback form** to send comments about this guide.

P-213P-24062024