Prisma Access Privacy

The purpose of this document is to provide customers of Palo Alto Networks with information needed to assess the impact of this service on their overall privacy posture by detailing how personal information may be captured, processed, and stored by and within the service.

Product Summary

Prisma™ Access provides network security for off-premises mobile users and branch offices. Prisma Access uses cloud-based security infrastructure as an alternative to installing or managing firewalls around the world and eliminates the need to backhaul cloud traffic to a central firewall.

Prisma Access interacts with several Palo Alto Networks products:

- Panorama™ network security management provides centralized administration for Prisma Access.
- The hub provides a web-based administrative framework, as an alternative to using Panorama. The Prisma Access app on the hub interacts with Prisma Access.
- Prisma™ SaaS provides cloud access security broker (CASB) management of software-as-a-service (SaaS) applications. Prisma Access integrates with Prisma SaaS to provide Security Assertion Markup Language (SAML) proxy support.
- Cortex™ Data Lake provides cloud-based storage of the logs Prisma Access generates.
- Integration with the enterprise Data Loss Prevention (DLP) service provides visibility and policy control over sensitive and regulated data while in transit.
- PAN-DB, Threat Prevention, and WildFire® malware prevention service are included with Prisma Access to protect against known and unknown threats.
- AutoFocus™ contextual threat intelligence service is optionally available for accelerated analysis of threat activity.

Prisma Access for remote networks protects branch offices and retail locations. Traffic from remote networks routes to Prisma Access, which inspects the traffic and enforces security policies before routing it out to the internet, cloud applications, headquarters, or a private data center.

Similarly, Prisma Access for mobile users provides security infrastructure to off-premises users around the world. Laptops and mobile devices with the GlobalProtect™ app automatically connect to Prisma Access via an IPsec/SSL tunnel for network security. Laptops and mobile devices that do not have the GlobalProtect app can manually connect to Prisma Access via a web browser to the Clientless VPN.

Prisma Access for Clean Pipe allows service providers to offer Prisma Access to tenants via cloud-based peering. Prisma Access for Clean Pipe will inspect traffic and enforce security policies for tenant traffic accessing the internet and cloud applications.

Prisma Access Insights is a network and mobile user monitoring application that identifies and remediates network connectivity issues in real time. Prisma Access Insights leverages advanced end user-level monitoring and role-based access rights to provide a seamless, latency-free network experience tailored to a user's specific network demands and work responsibilities. Prisma Access Insights solves the challenges of optimizing network-wide connectivity with advanced visibility, proactive assistance, capacity planning, and auto-remediation services across managed and unmanaged devices.

Information Processed by Prisma Access

Categories of information processed by Prisma Access include:

- **Configuration, security policies, and operational data**: Prisma Access will receive, store, and process operational data, configuration, and policies established by the customer through the Panorama interface or Prisma Access app on the hub. Policies may include information about the host state, users, and the applications as well as content that users or user groups are allowed to access. Operational data may include user information required for improved troubleshooting and visibility.
- **Network traffic**: Prisma Access processes network traffic, which includes source/destination IP addresses, port numbers, and packet content, among other information. In the event of a support request, the customer controls permissions for packet capture. SSL/SSH decryption enables inspection of encrypted network traffic. The customer establishes and manages decryption policies to enforce security policies, control access to applications, and stop malicious content.
- **User identification**: When enabled, Prisma Access employs User-ID™ technology on remote networks and mobile users to provide the customer's organization with user and user group identification by, for instance, retrieving it from Active Directory® to map security policies to network activities. Group information may be retained by the cloud service as long as the customer's subscription is active.
- **Malicious file content**: Prisma Access inspects and analyzes file content in unencrypted network traffic to detect and prevent known and unknown threats. The customer can establish security policies to control file transfer, inspect data, and block files with malicious content or that violate policy. If the customer is using WildFire, when Prisma Access encounters an unknown file, it will forward the file to WildFire for further analysis. This option is controlled by the customer's security policies.
- **Sensitive file content**: Prisma Access with DLP service inspects file content in motion to detect and protect sensitive data defined by data patterns and data profiles, based on corporate policy. It helps monitor sensitive file uploads to web applications and protects them from leakage. DLP on Prisma Access enables organizations to enforce data security standards and prevent the loss of sensitive data across mobile users and remote networks.
- **URLs**: URLs users interact with are inspected, blocked, and logged in accordance with the customer's security policies. This enables enforcement of policies to control acceptable use and stop access to harmful or blocked content.

Through Prisma Access Insights, customers' administrators will have access to 30 days worth of data concerning:

- Service and network health, including Prisma Access, Prisma Access locations, and customer deployment (RN, GW, SC).
- Customer network configuration-/setup-related information, including tunnel details and status, remote network health, bandwidth consumption, regions of deployment, number of security processing nodes, types of nodes, etc.
- Usage metrics, including license consumption, bandwidth consumption, mobile user connections (IP and location), behavior, and trends.
- Alerts, including all aforementioned metrics and combinations of metrics. Administrators will also see alerts when a tunnel or node goes down, or when issues are resolved.

Purpose of Information Processed by Prisma Access

The primary purpose of processing information through Prisma Access is to stop cyberattacks by:

- Inspecting traffic that goes through the firewall and generating logs.
- Blocking known threats.
- Monitoring and preventing transfers of sensitive data based on policy.
- Authenticating users that connect to a network either from a mobile device or from a branch office that does not operate its own firewall.
- Sending unknown files to the WildFire cloud for further inspection and analysis.
- Transferring logs to Cortex Data Lake for storage and analysis.

How Prisma Access Addresses EU Data Protection

Processing personal data to ensure network and information security—for instance, through Prisma Access or another part of the Palo Alto Networks product portfolio—is broadly recognized as a "legitimate interest" and specifically called out as such in the EU General Data Protection Regulation:

(49) The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned.

This could, for example, include preventing unauthorized access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.[1]

[1] GDPR, recital 49; see also Article 29 Working Party Opinion 06/2014 on the notion of legitimate interest of the data controller, WP217, adopted 9 April 2014, p. 24–25.

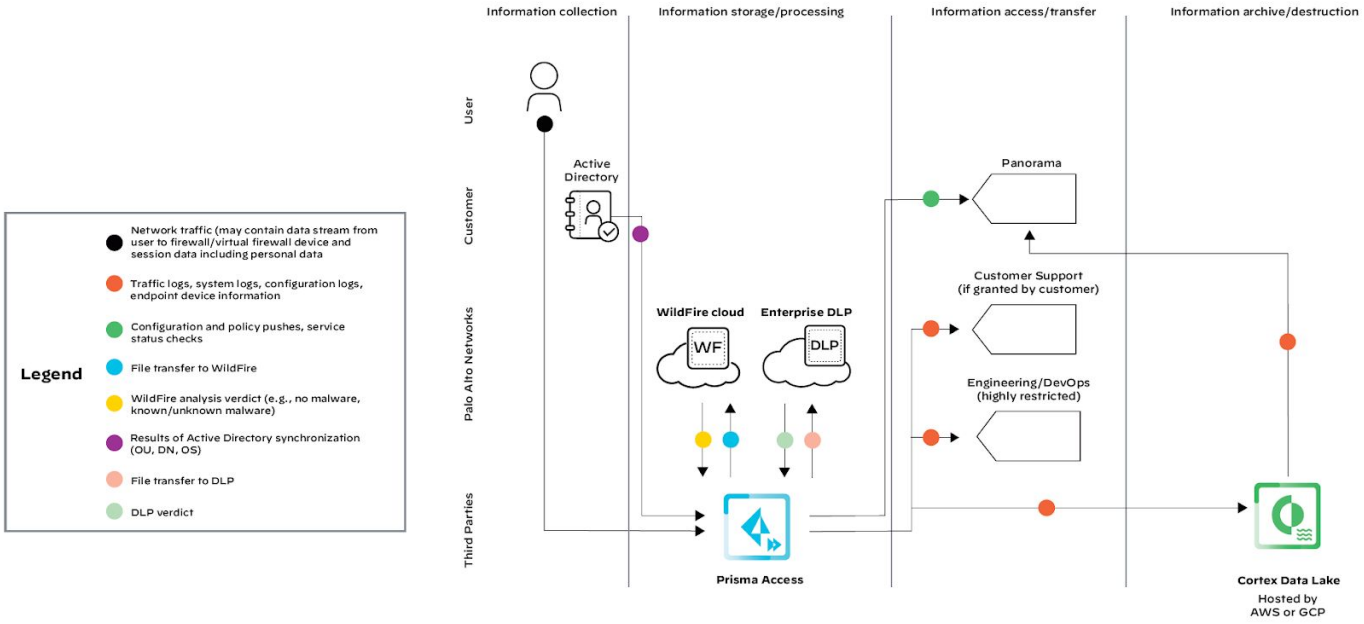

Figure 1: Prisma Access data flow

Where a service provider, such as Palo Alto Networks, processes personal data to ensure network and information security, this is a legitimate interest of the service provider and its customers, providing a basis for the processing of personal data by Palo Alto Networks under EU data protection laws.

This legitimate interest generally also provides a basis for customers storing personal data in the cloud or monitoring network traffic for security events, in accordance with privacy or regulatory requirements. In such an event, customers can use their privacy options, described herein, when configuring firewall or Panorama administration accounts, to limit data processing or access.

In the event of a need to share logs or information with Palo Alto Networks offices in other regions, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission[2] or other legal instruments, provided for in EU data protection law.

What Palo Alto Networks Does to Comply with Data Protection Rules

Palo Alto Networks is committed to protecting personal data processed by Prisma Access. We will not access the content of the information in a way that would allow the service to acquire meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats or investigating suspicious behavior indicative of attack.

Any logs stored on or processed by Palo Alto Networks systems are secured with state-of-the-art technologies, and Palo Alto Networks operates rigorous technical and organizational security controls.

[2] "Data protection," European Commission, accessed August 1, 2019, https://ec.europa.eu/info/law/law-topic/data-protection_en.

Subprocessors

Security compute locations may be hosted in Amazon Web Services (AWS®) or Google Cloud Platform (GCP®). Prisma Access is hosted in AWS and GCP public cloud data centers.

Customers' Privacy Options

Whereas Prisma Access for remote networks leverages cloud locations that are in proximity to the branch office, Prisma Access for mobile users can rely on cloud locations deployed worldwide so that customers can benefit from network security everywhere, with minimal latency. When onboarding, customers can choose a deployment region that is associated with a security compute location for processing traffic.

Furthermore, when configuring the service, customers can determine what information gets logged and sent to Cortex Data Lake.

Customers can control access to the data processed by Prisma Access by applying the business need-to-know rule through Panorama.

The logs on the firewall may be accessed by Palo Alto Networks support teams to investigate a support case initiated by a customer.

Retention

Logs from Prisma Access are temporarily stored in the cloud service before being transferred to Cortex Data Lake. See the Cortex Data Lake Privacy datasheet for details on the controls and processes related to retention of logs. Data consumed by Prisma Access Insights is retained for 30 days.

Access and Disclosure

Access by the Customer

Customers access information related to Prisma Access through the Panorama interface or the Prisma Access app on the hub. The customer's system administrator controls access to Panorama by granting appropriate privileges to authorized users. To use the Prisma Access app on the hub, the customer's system administrator must have an account on the Palo Alto Networks Customer Support Portal with an app administrator role.

Access by Palo Alto Networks

Data processing by Prisma Access is mostly automated, and access by Palo Alto Networks occurs when required to troubleshoot a customer support inquiry or address issues related to the service. All access privileges are managed by Palo Alto Networks Customer Support and Engineering leadership and audited for privilege access violations.

Prisma Access will be able to collect contact information to enable us to directly reach out to our customers, if required, for service-related matters. The contact information is optional for customers

to share, it is stored in conformance with our privacy policies and customers can choose to delete the contact information they shared at any time.

Prisma Access Locations

Prisma Access offers a local experience in more than 100 locations worldwide. Each location is mapped to a security compute location based on optimized performance and latency. This means that, unless otherwise modified by a system administrator, the traffic in certain countries will be directed to a defined compute location.

Table 1 shows the list of Prisma Access Locations and the corresponding compute country. System administrators can deselect countries in the configuration menu if they do not want to use the associated compute location indicated in the list. Please review the Prisma Access Administrator's Guide (Panorama Managed) or the Prisma Access Administrator's Guide (Cloud Managed) for more information.

Table 1: Prisma Access Mapping to Prisma Access Compute, WildFire, and DLP Locations

Prisma Access Locations: Local Connection Locations	Prisma Access Compute Country Physical Location of Security Compute		WildFire Location	DLP Location
	1.7 Deployments	Deployments after November 2020		
Australia East Australia South Australia Southeast New Zealand Papua New Guinea	Australia	Australia	Singapore	Singapore
Bahrain	Bahrain	Bahrain	Netherlands	Germany
Belgium	Belgium	Belgium	Netherlands	Germany
Argentina Bolivia Brazil Central Brazil East Brazil South Chile Ecuador Paraguay Peru Venezuela	Brazil	Brazil	United States	United States
Colombia	Brazil	United States	United States	United States
Canada Central Canada East	Canada	Canada	United States	United States
Belarus Finland Lithuania Norway Russia Central Russia Northwest Sweden	Finland	Finland	Netherlands	Germany
France North	France	France	Netherlands	Germany

Table 1: Prisma Access Mapping to Prisma Access Compute, WildFire, and DLP Locations (continued)				
Prisma Access Locations: Local Connection Locations	**Prisma Access Compute Country Physical Location of Security Compute**		**WildFire Location**	**DLP Location**
	1.7 Deployments	**Deployments after November 2020**		
Andorra Austria Bulgaria Croatia Czech Republic Egypt Germany Central Germany North Germany South Greece Hungary Israel Italy Jordan Kenya Kuwait Liechtenstein Luxembourg Moldova Monaco Nigeria Poland Portugal Romania Saudi Arabia Slovakia Slovenia South Africa Central Spain Central Spain East Turkey Ukraine United Arab Emirates Uzbekistan	Germany	Germany	Netherlands	Germany
South Africa West	Germany	South Africa	Netherlands	Germany
Switzerland	Switzerland	Switzerland	Netherlands	Germany
Hong Kong	Hong Kong	Hong Kong	Japan	Singapore
Bangladesh India North India South India West Pakistan South Pakistan West	India	India	Singapore	Singapore
Ireland	Ireland	Ireland	Netherlands	Germany
Japan Central Japan South	Japan	Japan	Japan	Singapore
Denmark Netherlands Central Netherlands South	Netherlands	Netherlands	Netherlands	Germany

Table 1: Prisma Access Mapping to Prisma Access Compute, WildFire, and DLP Locations (continued)				
Prisma Access Locations: Local Connection Locations	Prisma Access Compute Country Physical Location of Security Compute		WildFire Location	DLP Location
	1.7 Deployments	Deployments after November 2020		
Cambodia Indonesia Malaysia Myanmar Philippines Singapore Thailand Vietnam	Singapore	Singapore	Singapore	Singapore
South Korea	South Korea	South Korea	Japan	Singapore
Taiwan	Taiwan	Taiwan	Japan	Singapore
France South United Kingdom	United Kingdom	United Kingdom	Netherlands	Germany
Canada West Costa Rica Mexico Central Mexico West Panama US Central US East US Northeast US Northwest US South US Southeast US Southwest US West	United States	United States	United States	United States

Security

We deploy dedicated infrastructure for each customer. No instance serves multiple customers. Any data stored on or processed by Palo Alto Networks systems is secured with state-of-the-art technologies, and we operate rigorous technical and organizational security controls. Palo Alto Networks has achieved SOC 2 Type II Plus certification for Prisma Access to demonstrate its strong security policies and internal controls. For more information, visit paloaltonetworks.com/legal-notices/trust-center/soc2.

Resources

- Cortex Data Lake resource page: paloaltonetworks.com/cortex/cortex-data-lake
- Prisma Access resource page: paloaltonetworks.com/prisma/access
- WildFire resource page: paloaltonetworks.com/products/secure-the-network/wildfire
- DLP resource page: paloaltonetworks.com/enterprise-data-loss-prevention

About This Datasheet

The information provided with this paper that concerns technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.