

The Practical Guide to Migrating Security to a SASE Model

Written by Alex Ciobanu

Table of Contents

Chapter 1 – SASE: A Paradigm Shift in Networking and Security

- Introduction
- What Is SASE?
- Why Is SASE Needed to Transform Security?
- SASE Use Cases with Prisma Access

Chapter 2 – Architecting SASE Deployments with Prisma Access

- Securing Mobile Users
- Securing Remote Networks

Chapter 3 – Migration Best Practices

- Ensure Successful Deployment of Prisma Access

Chapter 4 – Migrating From Legacy Firewall and VPN Solutions to Prisma Access

- Beginning Your Migration
- Migrating from Check Point Devices to Prisma Access
- Migrating from Cisco ASA devices to Prisma Access
- Migrating From Legacy VPN Solutions to Prisma Access

Chapter 5 – Transitioning Wide Area Networks to a SASE Model

- Overcome the Shortfalls of Legacy WANs
- Prisma Access Integration with SD-WAN
- Prisma Access Integration with Prisma SD-WAN
- SD-WAN with Prisma Access Direct Internet Access
- SD-WAN with Regional Hub-and-Spoke Architecture and Prisma Access

Chapter 1

SASE: A Paradigm Shift in Networking and Security

Introduction

As organizations embrace the cloud and mobility, the way networking and security are delivered must change. Digital transformation and work-from-anywhere requirements are fueling massive cloud usage in the enterprise, and with more users and apps now outside the enterprise, the old architectural model of backhauling traffic to the data center no longer makes sense. Cloud-based web security offerings have emerged as a potential solution, but they only solve part of the problem. Likewise, many modern secure access solutions fail to adequately enable the work-from-anywhere experience enterprises demand because of several critical limitations:

- They cannot provide access and security for all apps, increasing the risk of data breach.
- They do not provide complete, proven enterprise-grade security, exposing organizations to advanced threats.
- They provide inconsistent access levels and performance for remote workers, frustrating users and increasing the support burden for IT.

It's time for a new approach.

[Secure access service edge \(SASE\)](#) is an emerging architectural approach designed to help organizations solve these problems by converging networking and security services in the cloud. This guide is ideal for network and security professionals as an introduction to the benefits of SASE and how you can migrate your network security architecture to a SASE model using Prisma® Access by Palo Alto Networks.

What Is SASE?

SASE converges software-defined wide area networking (SD-WAN) and security services—such as firewall as a service (FWaaS), secure web gateway (SWG), cloud access security broker (CASB), and Zero Trust network access (ZTNA)—into a single cloud-delivered service. SASE solves the challenge of delivering consistent secure access no matter where users, applications, or devices are located.

Palo Alto Networks has revolutionized the way organizations transform their networking and security infrastructure with the industry's most complete SASE architecture. [Prisma Access](#) is a cloud-delivered security platform that provides the security organizations need for protecting all traffic, all applications, and all users. [Prisma SD-WAN](#) is a cloud-delivered networking platform that uses machine learning and automation to simplify WAN connectivity and to provide an exceptional user experience. By deeply integrating Prisma Access with Prisma SD-WAN, Palo Alto Networks enables organizations to secure remote workforces at scale. Together, Prisma Access and Prisma SD-WAN offer the industry's most comprehensive SASE solution.

Why Is SASE Needed to Transform Security?

Legacy network security technologies are not designed to effectively protect remote workforces against modern security threats. Moreover, traditional firewalls and web proxies are unable to consistently inspect and control all traffic across a globally distributed enterprise.

Legacy architectures also create challenges when it comes to protecting branch offices and retail locations, as these architectures were not designed to adapt to the cloud. Every independent entity in the network requires a new architecture, a new set of policies to deploy, and new interfaces to configure. This creates an administrative burden that introduces cost, complexity, and gaps in an organization's security posture.

SASE is a platform-based approach that can solve multiple use cases according to your organization's needs. These needs may start with urgent challenges around employee remote access, secure branch direct internet access, or improving web security. Prisma Access provides a modular platform that allows you to start with whatever use case is most critical to your organization, and then solve additional use cases as opportunities arise.

SASE Use Cases with Prisma Access

Prisma Access provides service-based protection for both networks and users (see figure 1).

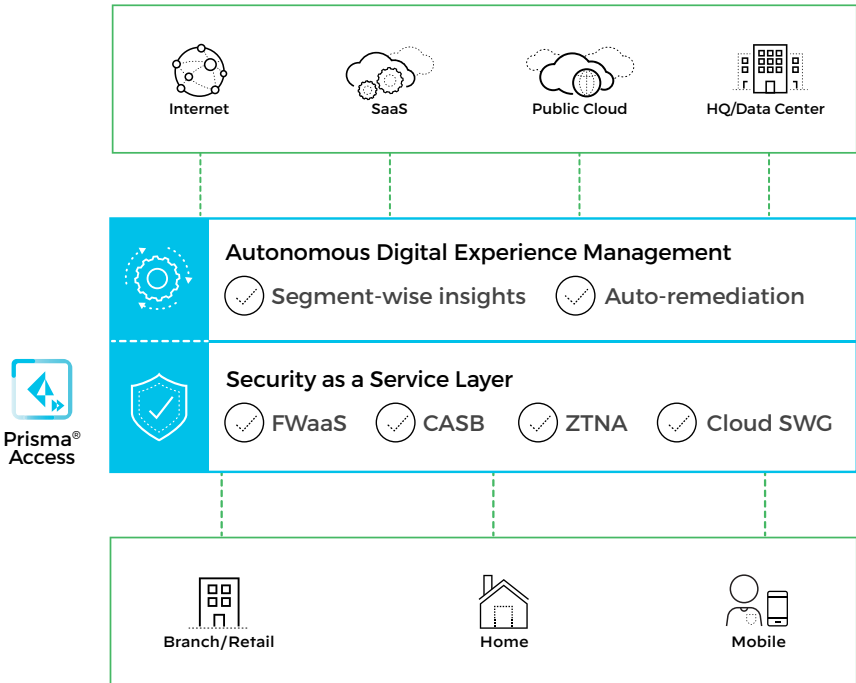


Figure 1: Prisma Access high-level architecture

Prisma Access for mobile users provides comprehensive cloud-delivered security to safely connect all users to all the applications they need, no matter from where the users are accessing them. Supporting both managed and unmanaged devices, Prisma Access ensures consistent security and seamless access to corporate resources—whether they are located in the cloud, delivered from a data center, or both—while providing an optimized user experience. Taking a ZTNA approach, Prisma Access provides access to applications and services based on defined access control policies, including post-connection monitoring of threats and signs of data loss or compromised credentials.

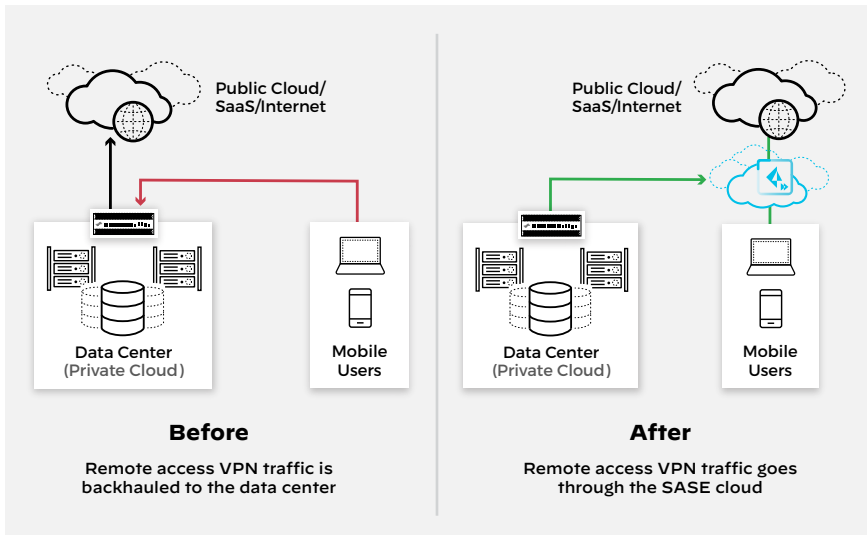


Figure 2: Mobile user security use case

Prisma Access for remote networks provides consistent connectivity and security to branch offices and remote sites. It helps organizations streamline their deployment and management of global security policies and enforcement, leveraging the cloud for rapid time-to-value. Organizations can avoid the complexity and administrative costs normally associated with managing WAN connectivity and security at a large scale.

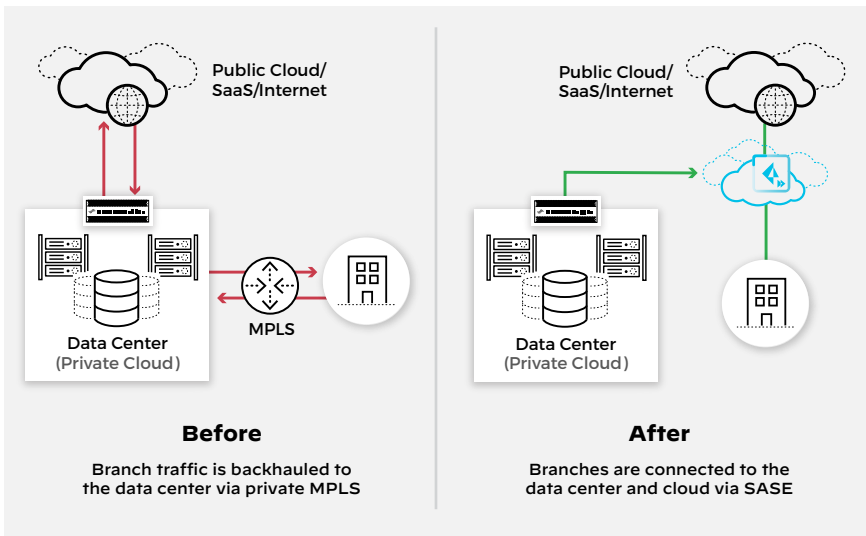


Figure 3: Remote network security use case

More Resources

Learn more on our [Prisma Access Website](#).

Chapter 2

Architecting SASE Deployments with Prisma Access

Securing Mobile Users

The growth of remote work means that secure, high-performance remote access to applications is more important than ever before. Additionally, applications need protection from improper access, threats, and malicious users.

The challenges of traditional approaches to remote access, such as traditional virtual private networks (VPNs), include not only scale and capacity, but also the lack of inline security. Prisma Access eliminates these challenges as a globally distributed, cloud-delivered service with built-in high availability, auto-scaling, and inline security inspection.

With Prisma Access, users have secure and uninterrupted access to all applications in the cloud, on the internet, or in your data center, no matter where they are located. Users anywhere in the world connect to the most optimal cloud gateway available, and consistent security is enforced, even in locations where you do not have local network presence.

Prisma Access uses a ZTNA approach to ensure users are only granted access to the applications they need, based on policy. Additionally, inline traffic inspection is applied to prevent threats and data loss, ensuring your applications and data stay safe from unauthorized access or potential malicious activity.

By leveraging the ZTNA capabilities of Prisma Access, your applications will also be shielded from public exposure on the internet by directing users through the cloud platform. Once users are authenticated via User-ID™ technology, they are allowed to access your applications based on Layer 7 policies using App-ID™

technology and the role or type of the device, regardless of location. Post-connection inspection will also be applied to scan for threats as well as monitor for data loss and potential credential theft.

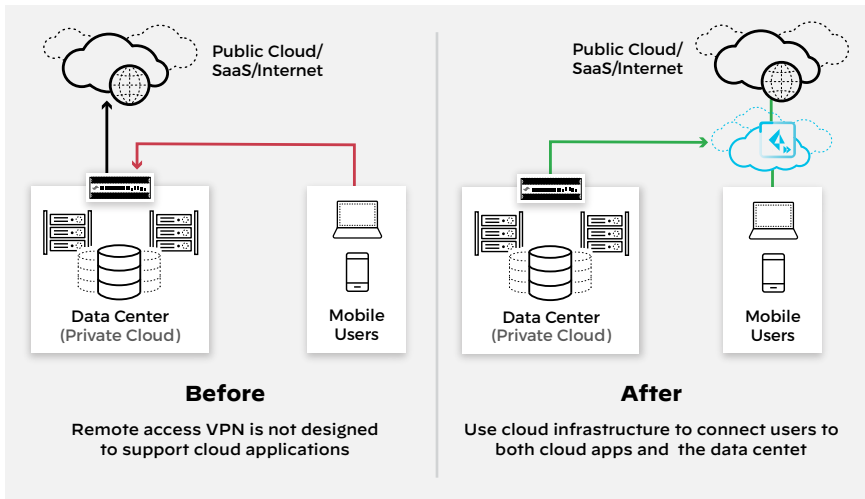


Figure 4: Cloud infrastructure for consistent security

A user’s smartphone, tablet, or laptop can connect to Prisma Access using one of the following methods:

- **GlobalProtect agent**—endpoint agent that automatically establishes a secure tunnel to Prisma Access by using the best available gateway. The GlobalProtect agent also allows for user and device information profiling as part of ZTNA.
- **Clientless**—secure remote access from SSL-enabled web browsers for devices that cannot have an agent installed on them. This is a useful option when you need to enable partner or contractor access, or safely enable unmanaged devices in bring-your-own-device (BYOD) arrangements.
- **PAC files**—a connection method that uses an explicit proxy approach while still maintaining the best-in-class security Prisma Access provides.

Securing Remote Networks

Traditionally, organizations either relied on VPN or multiprotocol label switching (MPLS) to provide a secure, private connection for their networks to access data, applications, and the internet.

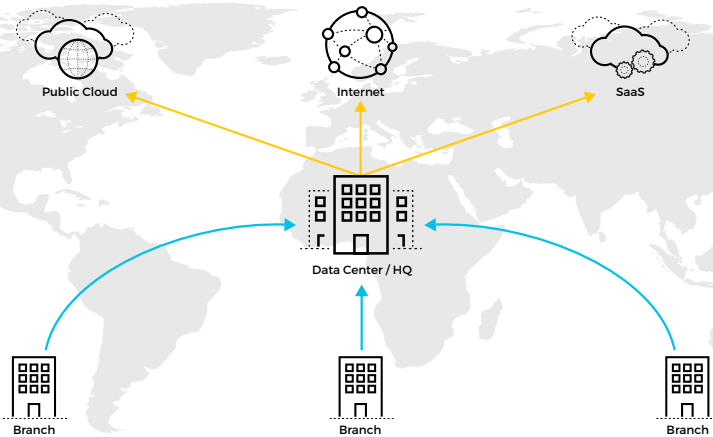


Figure 5: Traditional approach to WAN

This architectural approach, as illustrated in figure 5, introduces several challenges, including:

- Traffic to and from branches is backhauled to the data center/HQ for security, increasing latency
- MPLS circuits are expensive and complex to maintain
- Inter-branch communication is not secured

Prisma Access provides direct, secure access to cloud, software as a service (SaaS), and web resources from anywhere in the world by onboarding your remote locations via IPsec tunnels or SD-WAN. Each tunnel connects to one of the cloud security enforcement nodes. Prisma Access also securely connects your locations to your data center/headquarters. Accessing these resources is done over a separate IPsec tunnel, called a service connection, between the Prisma Access cloud and your data center.

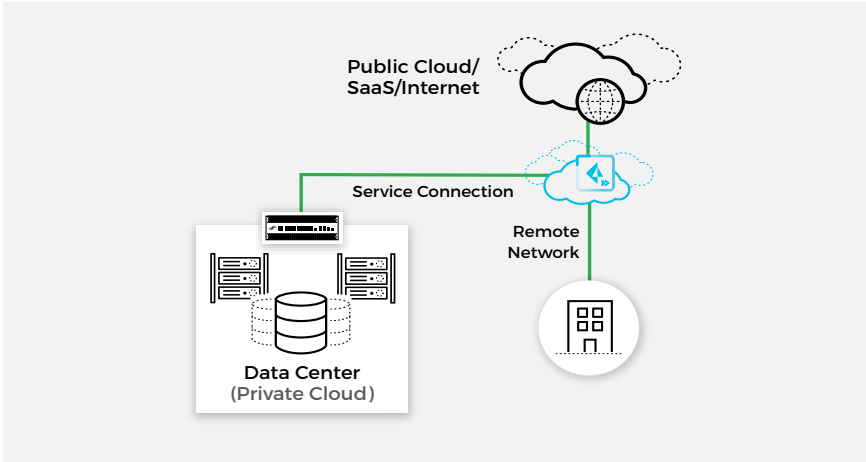


Figure 6: Secure cloud access from anywhere

Figure 6 shows how remote networks connect to Prisma Access. From a routing perspective, both static routing and Border Gateway Protocol (BGP) are supported. Figure 7 shows a configuration using static routes, which Prisma Access redistributes to other resources and users across the network and users across the network can reach the remote location.

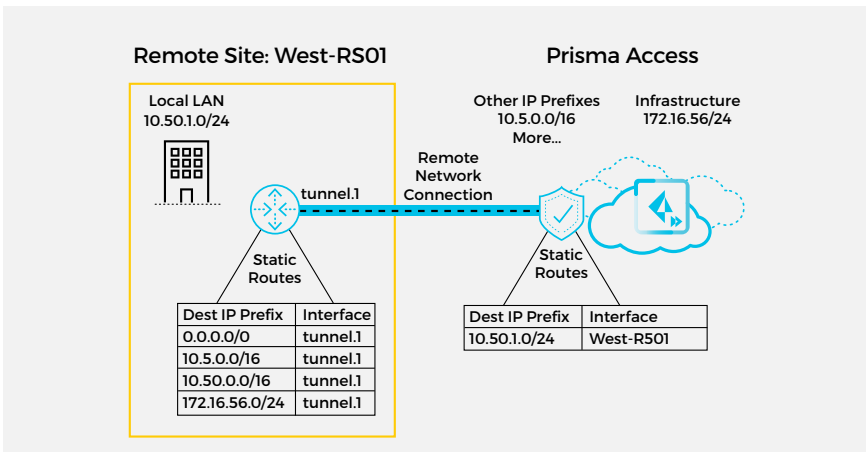


Figure 7: Remote network connection to Prisma Access

Organizations utilizing Prisma Access to secure mobile users and remote networks can benefit from:

- **Consistent security and advanced threat protection:** Your policies are applied to all traffic, wherever your users are located.
- **Data loss prevention (DLP):** Comprehensive data protection keeps your sensitive data safe by categorizing it and protecting it while in motion across remote users and locations.
- **DNS Security:** Advanced analytics and machine learning protect you against threats that attempt to exploit the Domain Name System (DNS).
- **URL filtering:** Your acceptable use policies are enforced, and access to malicious domains is filtered.

More Resources

Take a look at our [Prisma Access Reference Architectures](#)

Chapter 3

Migration Best Practices

Ensure Successful Deployment of Prisma Access

Applying the best practice features described in this chapter will provide visibility of your traffic, continuous scanning of potential malicious activity, URL filtering, and worldwide geographical coverage for your users. All features can be enabled in Prisma Access from day one.

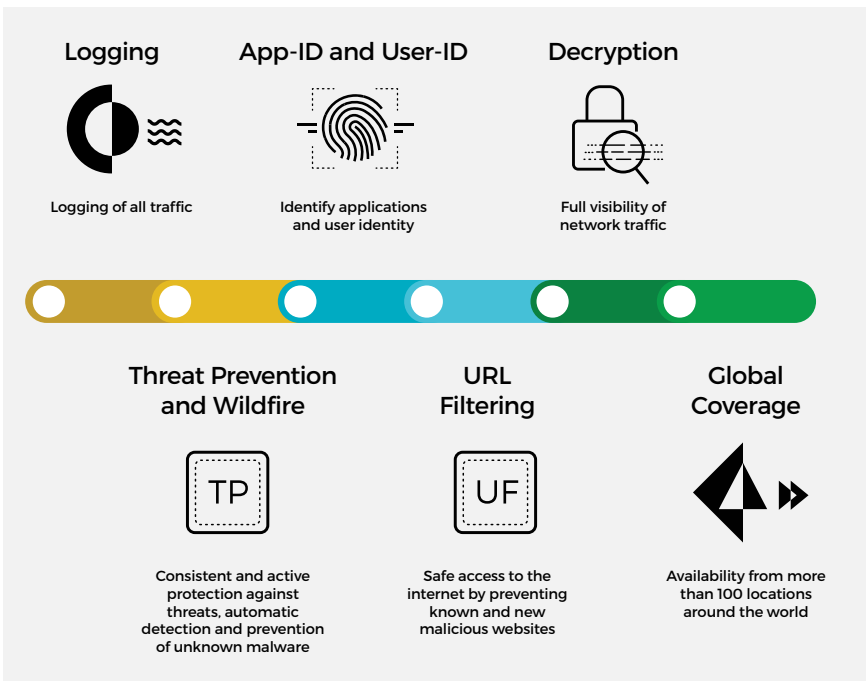


Figure 8: Migration best practices

1. Enable Logging on All Security Policies

Prisma Access uses [Cortex® Data Lake](#) to collect, integrate, and transform security log data. We highly recommend enabling logging on all security policies, whether they're migrated or newly configured. This will provide visibility over all traffic in your network. You can easily enable logging by configuring a Log Forwarding Profile and assigning it to the security policies.

If you are required to send Prisma Access logs to another location (e.g., a security information and event management [SIEM] system), you can use a [log forwarding app](#) to forward logs from Cortex Data Lake.

If you are migrating rules from legacy security solutions (as we will detail in Chapter 4), you can use the [Expedition](#) tool to create and automatically assign the profile to the rules during migration. This applies only for Prisma Access deployments managed by [Panorama™](#) network security management.

2. Configure and Enable Threat Prevention and Wildfire

Our [Threat Prevention](#) service goes beyond a typical intrusion prevention system (IPS) by inspecting all traffic for threats, regardless of port, protocol, or application. [WildFire®](#) malware prevention service provides cloud-based threat analysis for zero-day exploits and unknown malware. Threat Prevention and WildFire should be enabled on security rules from day one. If full enforcement cannot be achieved initially, we strongly recommend enabling Threat Prevention and WildFire in Alert Mode and moving to full enforcement after a certain period of time. By combining Threat Prevention and WildFire, you will give your users consistent and active protection against known and unknown threats.

3. Configure and Enable URL Filtering

[URL Filtering](#) provides safe web access for your users based on site category, features, and safety. The cloud-based service uses a combination of static analysis and machine learning to identify as well as automatically block malicious sites and phishing pages. You can also prevent credential phishing theft by tightly controlling the types of sites on which users can enter their corporate credentials. You can enforce your security policies based on URL categories.

4. Enable Application and User Identification

Prisma Access makes use of the Palo Alto Networks [App-ID](#) engine to identify applications traversing your network, irrespective of port, protocol, evasive tactic, or encryption (SSL/TLS or SSH). We strongly recommend either migrating your legacy security rules to App-ID or creating new security rules with App-ID enabled. Along with applications, you should also configure [User-ID](#) to identify the users in your network and determine who can access certain applications.

5. Create and Deploy a Decryption Strategy

[Decryption](#) plays an important role in maintaining full control and visibility on your network, and Prisma Access supports complete decryption of all traffic. You should put in place, and deploy, a decryption strategy to identify all applications, prevent malicious encrypted content from entering your network, and stop sensitive content from leaving your network concealed as encrypted traffic.

Start decrypting traffic by setting up the certificates Prisma Access requires to act as a trusted third-party to a session. For everything else, we've built in best practice decryption settings, including the option to set exclusions, such as for sensitive content or sites that are known to break when decrypted.

6. Configure Globally Available Locations for Your Remote Workers

Prisma Access leverages public cloud infrastructure to provide massive scale and global coverage for enterprises. To accommodate a remote workforce with a worldwide geographical presence, you can enable more than 100 Prisma Access locations for your users to connect to. This provides better performance and security for your remote workers along with superior communication to your data center applications, public clouds, SaaS applications, and the internet. Figure 9 shows the Prisma Access points of presence (PoPs) on each continent.

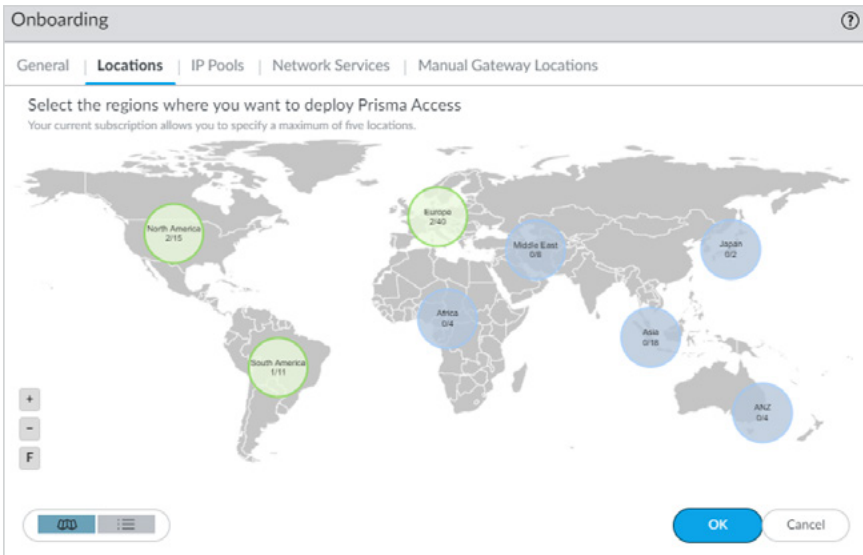


Figure 9: More than 100 service access points across 76 countries

Migrating to a SASE model requires thorough planning and some architectural changes, so the sooner you start, the better. In the next chapter, we will walk through the recommended approach to migrate from legacy architectures and products to a Prisma Access deployment, focusing on both networking and security considerations.

Chapter 4

Migrating From Legacy Firewall and VPN Solutions to Prisma Access

Beginning Your Migration

Palo Alto Networks provides two ways to deploy and manage Prisma Access:

- [Panorama Managed](#): If you already use [Panorama](#) to manage your Palo Alto Networks NGFWs, you can deploy Prisma Access with Panorama management to leverage your existing policies.
- [Cloud Managed](#)—If you don't have Panorama or you just want a simplified onboarding and management experience for Prisma Access, use the [Prisma Access app](#) on the Palo Alto Networks hub to quickly and easily enable internet access for your Prisma Access users, and then extend connectivity into your HQ, data center, and branch networks.

The following migration guides will be based on Prisma Access managed by Panorama.

When migrating from legacy firewall solutions to Prisma Access, there are few things to account for related to configuration migration. On regular zone-based firewalls, each zone is associated with an interface. Prisma Access simplifies zone assignment by creating Trust, Untrust, and Clientless VPN zones automatically. The user must only create zone mappings to achieve consistent security policy enforcement:

- **The Trust zone** contains all trusted IP addresses, service connections, and mobile users within the corporate network (e.g., mobile user IP pools, infrastructure, data center and remote network subnets).

- **The Untrust zone** contains all interfaces that are facing the internet. By default, any IP address or mobile user that is not trusted is inherently untrusted.
- **The Clientless VPN zone** is used for secure remote access (e.g., contractor access to applications).

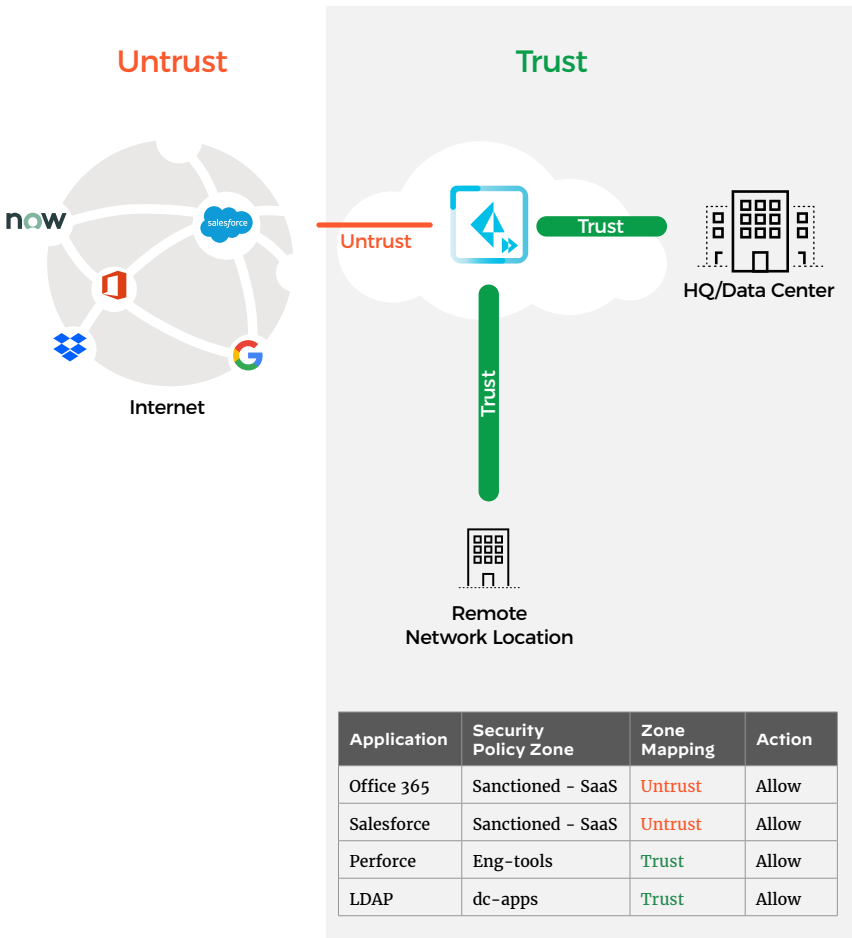


Figure 10: Automatically created zones in Prisma Access

The transformation levels outlined in figure 11 provide a seamless and safe transition to Prisma Access by minimizing migration risks and delineating a gradual adoption path for advanced features, like those mentioned in Chapter 3.

Transformation Level 1

Visibility

Into unencrypted traffic

- Layer 3/4 policy migration
- Decryption strategy created
- User-ID deployed
- Threat Prevention, URL Filtering, and WildFire enabled in alert mode

Transformation Level 2

Control

Of all traffic by reducing attack surface

- Layer 7 policy adoption
- Block unsanctioned applications
- Decryption strategy deployed
- Threat Prevention, URL Filtering, and WildFire enabled in Block mode

Transformation Level 3

Enforcement

of advanced security policy

- Policy evolution and enhancement
- Application and user segmentation
- Last-mile threat analysis/tuning/recategorization/blocking
- Decryption strategy optimized

Figure 11: Transformation levels

Migrating from Check Point Devices to Prisma Access

This section focuses on the Layer 3 and 4 policy migration considerations, including migration of objects from Check Point products. Prisma Access has many unique and dynamic settings that must be configured independently, but if you wish to migrate any of your existing policies and objects, you can use the following approach. Palo Alto Networks offers a migration tool called [Expedition](#) that you can use to migrate Check Point configurations to Prisma Access. Figure 12 shows a high-level flow for migrating your configuration using Expedition.

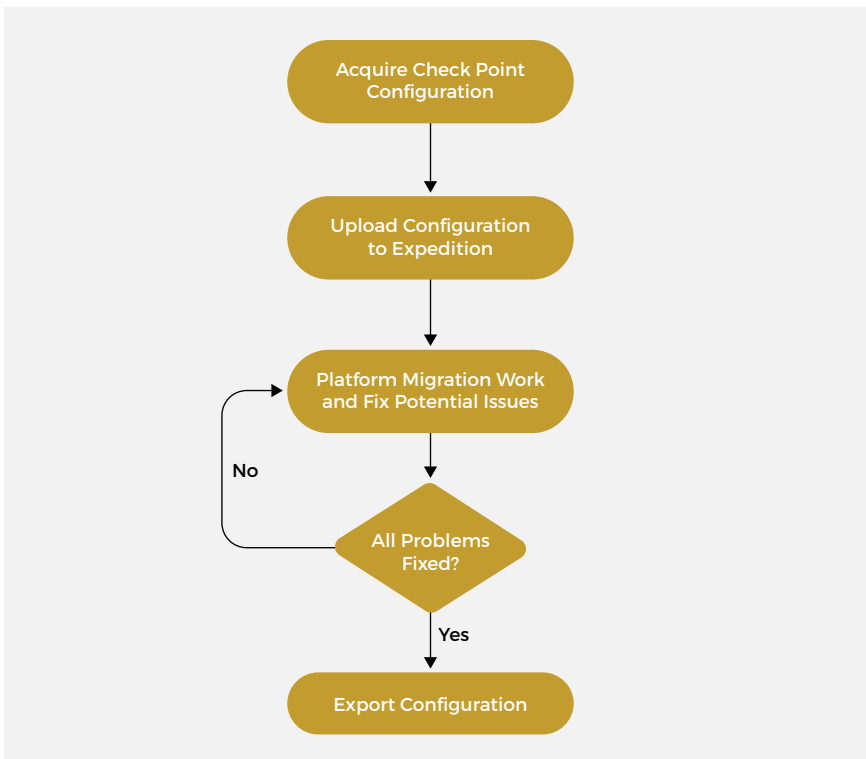


Figure 12: High-level approach for migrating with Expedition

We can split the flow into three major steps.

Step 1: Acquire Check Point Configuration and Upload It to Expedition

The required files depend on the version of Check Point software version:

- For versions lower than R80:
 - Objects_5_0.C
 - Policy.W
 - Rulebases_5_0.fws
 - Routes.txt
- For versions higher than or equal to R80, please refer to the instructions on the Expedition Web-UI for the “Version R80.x or Higher” option.

Step 2: Perform Migration Work and Fix Potential Issues

The first recommended action is to check the migration logs. This will notify you if any problems are found during the conversion process, or if any part of the configuration has been automatically fixed. Figure 13 shows some logs related to Destination NAT. These logs are only informative, with no action required from the administrator.






MIGRATION LOGS			
Level	Datetime	Message	Action
Task: Correcting Destination based on DNAT			
		Security Rule[69] covers the DNAT Rule(s)[9].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[10].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[11].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[12].	No Action required
		Security Rule[69] covers the DNAT Rule(s)[13].	No Action required

Figure 13: Logs related to Destination NAT

Cleaning unused objects comprises another recommended set of steps to perform during the migration work. The following unused objects can be removed from the configuration:

- Address
- Address Groups
- Service
- Service Groups
- Tags

We strongly suggest checking and fixing the following potential-ly misconfigured migration problems:

- Duplicate name objects
- Invalid services (e.g., “ping” identified as a service and not application)

From a networking perspective, Prisma Access does not require any of the following Check Point configurations:

- **Zones:** When exporting network zones from Expedition, all zones will be named “Zone1,” “Zone2,” “Zone3,” etc. This will be reflected automatically in the security policies. It is, however, recommended that you change the zone names. The security rules will be adjusted automatically. In the Expedition screenshot in figure 14, you can see an example of interfaces being migrated from Check Point, with the newly created and corresponding zones.
- **Virtual Router:** Prisma Access automatically takes care of all the interface configuration, internal routing, and NAT. There is no need to migrate any of the routing tables (static or dynamic entries). Static or dynamic routing configuration on Prisma Access toward data center or remote networks will be manually configured.

INTERFACES						
<input type="checkbox"/>	Name	Type	IP Address ↓	Virtual Router	Tag	Zone
Media: ethernet						
<input type="checkbox"/>	eth0	layer3	149.111.142.0/27	chkpt-vr-vsyz1	Untagged	Zone4
<input type="checkbox"/>	eth5.132	layer3	10.188.2.252/27	chkpt-vr-vsyz1	132	Zone2
<input type="checkbox"/>	eth5.32	layer3	10.188.14.33/27	chkpt-vr-vsyz1	32	Zone5
<input type="checkbox"/>	eth4	layer3	10.188.14.1/27	chkpt-vr-vsyz1	Untagged	Zone6

Figure 14: Interfaces being migrated from Check Point

Step 3: Upload the Configuration into Panorama

There are multiple ways to upload the newly prepared configuration into Panorama, but we recommend one of the following approaches:

- Direct API calls from Expedition to Panorama
- The use of “load partial” commands on the CLI
 - Offers the granularity of selecting and uploading only certain parts of the final XML configuration file into Panorama

Figure 15 shows an example of using the “load partial” command to upload to Panorama (we have chosen the “Mobile_User_Device_Group” Device Group) only individual and necessary parts from the migrated Check Point configuration. In this case, we have named the exported Expedition configuration file “cp.xml,” and we have only imported it into Panorama.

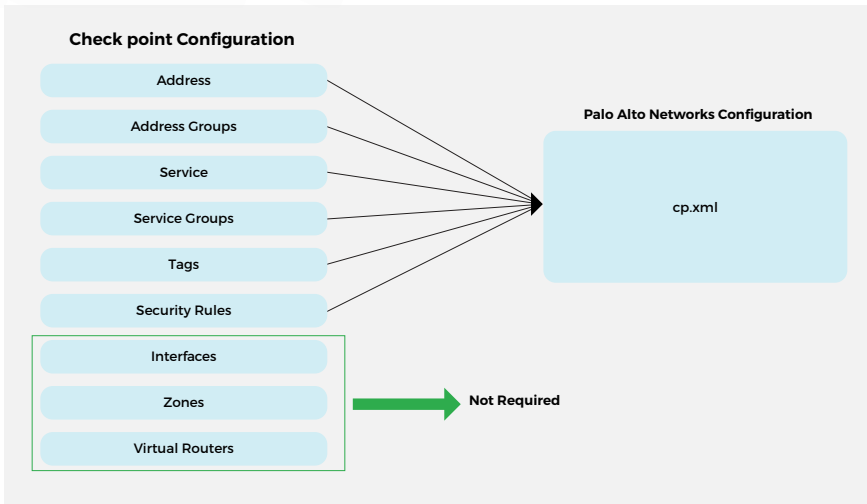


Figure 15: Only required config parts are added into the final file

Address:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address to-xpath /config/devices/entry[@name='localhost.local-
domain']/device-group/entry[@name='Mobile_User_Device_Group']/
address mode merge from cp.xml
```

Address-Group:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
address-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/address-group mode merge from cp.xml
```

Service:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service to-xpath /config/devices/entry[@name='localhost.local-
domain']/device-group/entry[@name='Mobile_User_Device_Group']/
service mode merge from cp.xml
```

Service-Group:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/service-group mode merge from cp.xml
```

Tags:

```
Admin@Pan# load config partial from-xpath /config/devic-
es/entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/tag to-xpath /config/devices/entry[@name='lo-
calhost.localdomain']/device-group/entry[@name='Mobile_User_
Device_Group']/tag mode merge from cp.xml
```

Security Rules:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
rulebase/security/rules to-xpath /config/devices/entry[@
name='localhost.localdomain']/device-group/entry[@name='Mobile_
User_Device_Group']/post-rulebase/security/rules from cp.xml
```

We have chosen to upload the security policies as “post-rules.” The security zones will not be imported, but they will be present in the policies in the new configuration. Since we only had seven zones migrated in this particular configuration, the only thing left is to manually create the zones under the “Mobile_User_Template” template settings and perform the zone mapping on the Prisma Access plugin configuration. By default, all new zones will be mapped to the Untrust zone.

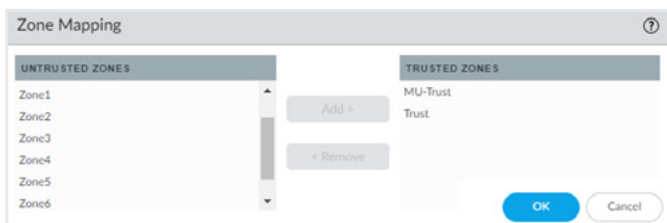


Figure 16: New zones mapped to Untrust by default

Migrating from Cisco ASA devices to Prisma Access

Migrating Cisco ASA configuration is a straightforward process. Cisco ASA makes use of Access Control Lists (ACLs) to allow or deny traffic. By using [Expedition](#), these ACLs can be easily migrated into Palo Alto Networks format along with their corresponding zones. This migration can follow the same flow we previously used for Check Point.

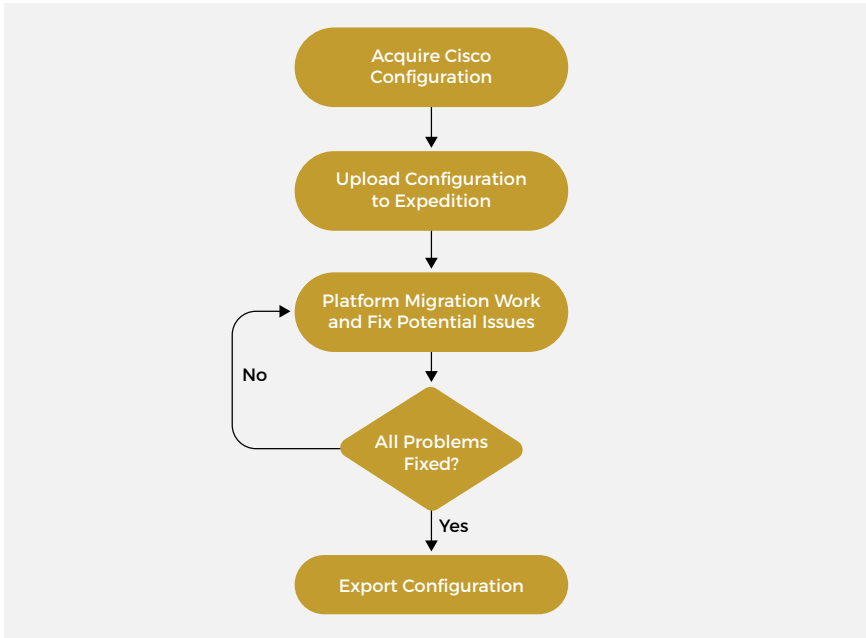


Figure 17: High-level approach for migrating with Expedition

Step 1: Acquire Cisco ASA Configuration and Upload It to Expedition

Usually, Cisco ASA configuration is retrieved by executing the command “show running” on the appliance.

Step 2: Perform Migration Work and Fix Potential Issues

From a regular configuration, we will obtain the corresponding Palo Alto Networks zones from the interface configuration. An example of interface configuration in Expedition might look like this:

```
interface GigabitEthernet0/3.1
  description DMZ-1
  vlan 74
  nameif dmz-1
  security-level 50
  ip address 10.4.0.254 255.255.0.0 standby 10.4.0.253
```

From the above Expedition output, we will extract and adopt the security rules in the required zone “dmz-1”. Figure 18 shows what the output in Expedition will look like.

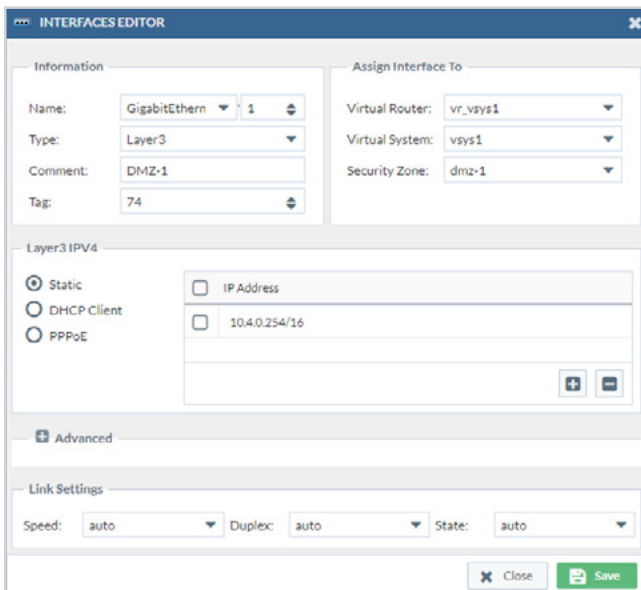


Figure 18: Output in Expedition

From a networking perspective, Prisma Access does not require the following Cisco ASA configurations:

- **Network and virtual router settings:** Prisma Access automatically takes care of all the interfaces configuration, internal routing, and NAT. There is no need to migrate any of the routing tables (static or dynamic entries) or interface configuration. Static or dynamic routing configuration on Prisma Access toward data center or remote networks will be manually configured.

As previously mentioned, if there are unused objects in the imported configuration, they can be removed. Fixing some of the invalid objects is recommended. The most common are:

- Duplicate name objects
- Invalid services

Step 3: Upload the Configuration into Panorama

Once the configuration work has been performed, to load particular objects/policies from the configuration, the “load partial” command can be used.

There are multiple ways to upload the newly prepared configuration into Panorama, but we recommend one of the following approaches:

- Direct API calls from Expedition to Panorama
- The use of “load partial” commands on the CLI.
 - Offers the granularity of selecting and uploading only certain parts of the final XML configuration file into Panorama

Figure 19 shows an example of using the “load partial” command to upload to Panorama (we have chosen the “Mobile_User_Device_Group” Device Group) only individual and necessary parts from the migrated Cisco configuration. In this case, we have named the exported Expedition configuration file “cp.xml,” and we have only imported it into Panorama.

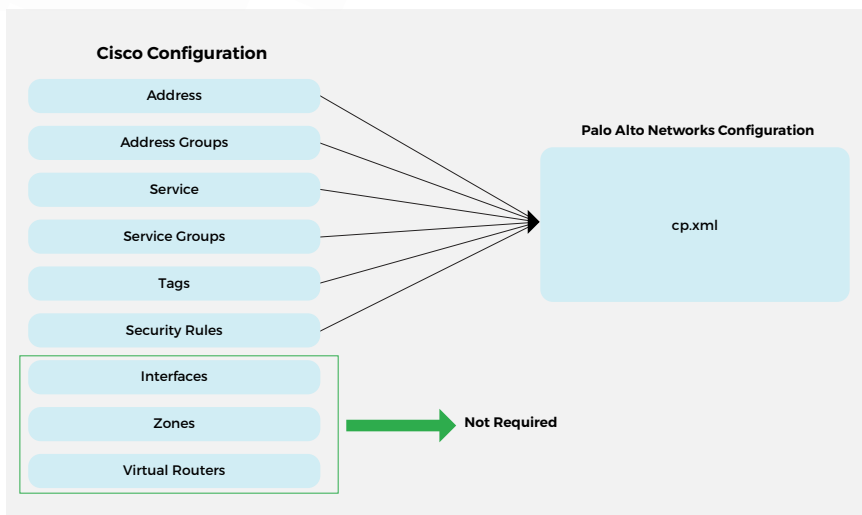


Figure 19: Only required config parts are added into the final file

Address:

```
Admin@Pan# load config partial from-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address to-xpath /config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='Mobile_User_Device_Group']/address mode merge from cp.xml
```

Address-Group:

```
Admin@Pan# load config partial from-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/address-group to-xpath /config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='Mobile_User_Device_Group']/address-group mode merge from cp.xml
```

Service:

```
Admin@Pan# load config partial from-xpath /config/devices/entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/service to-xpath /config/devices/entry[@name='localhost.localdomain']/device-group/entry[@name='Mobile_User_Device_Group']/service mode merge from cp.xml
```

Service-Group:

```
Admin@Pan# load config partial from-xpath /config/devices/
entry[@name='localhost.localdomain']/vsys/entry[@name='vsys1']/
service-group to-xpath /config/devices/entry[@name='localhost.
localdomain']/device-group/entry[@name='Mobile_User_Device_
Group']/service-group mode merge from cp.xml
```

Tags:

```
Admin@Pan# load config partial from-xpath /config/devic-
es/entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/tag to-xpath /config/devices/entry[@name='lo-
calhost.localdomain']/device-group/entry[@name='Mobile_User_
Device_Group']/tag mode merge from cp.xml
```

Security Rules:

```
Admin@Pan# load config partial from-xpath /config/devic-
es/entry[@name='localhost.localdomain']/vsys/entry[@
name='vsys1']/rulebase/security/rules to-xpath /config/devic-
es/entry[@name='localhost.localdomain']/device-group/entry[@
name='Mobile_User_Device_Group']/post-rulebase/security/rules
from cp.xml
```

We have chosen to upload the security policies as “post-rules.” The security zones will not be imported, but they will be present in the policies in the new configuration. Since we only had seven zones migrated in this particular configuration, the only thing left is to manually create the zones under the “Mobile_User_Template” template settings and perform the zone mapping on the Prisma Access plugin configuration. By default, all new zones will be mapped to the Untrust zone.

Migrating From Legacy VPN Solutions to Prisma Access

Mobile users can connect to Prisma Access using the GlobalProtect agent, Clientless VPN, or PAC files from any geographical location.

From a migration perspective, most migrations from alternative VPN solutions will be manual, as vendors have a totally different approach to architecting their VPN solutions, and most of the configurations are not compatible with each other.

However, if you are migrating from proxy-based solutions, Prisma Access enables you to create policies that inspect traffic based on all protocols, including UDP, and not just HTTP or HTTPS. This means you don't need separate solutions for non-web-based traffic—everything can be handled by Prisma Access. Moreover, when moving away from proxy-based solutions, you can still make use of URL categories in your policies, as mentioned in Chapter 3. Any proxy bypass settings can be replaced with a more optimized split tunneling setting based on applications, process names, or routes while using the GlobalProtect agent.

Once you have decided on the method through which your users will connect to Prisma Access, you can start building your policies, if you do not already use any of the migrated ones we addressed earlier. All policies should be created based on ZTNA principles. This approach will provide full content inspection to identify the users in your network and the applications they are accessing, in addition to enabling post-connection monitoring to scan for threats as well as monitor for data loss and potential credential theft.

As mentioned in Chapter 3, user identity—as opposed to just IP address—is an integral component of Prisma Access. We highly recommend using User-ID to identify users and their corresponding groups in your network and leveraging this information to build Layer 7 policies.

With Prisma Access, multiple policy types can be configured:

- Security policies allow you to enforce rules and take action at the application level, as mentioned in Chapter 3, and can be as general or specific as needed. These policies are compared against incoming traffic in sequence. Because the first rule that matches the traffic is applied, the more specific rules must precede the more general ones.
- QoS policies can be configured to prioritize business-critical traffic or traffic that requires low latency, such as VoIP or video conferencing. You can also reserve a minimum amount of bandwidth for business-critical applications. Differentiated Services Code Point (DSCP) markings are honored by default as set by your organization's on-premises device.
- Decryption policies can be configured to inspect traffic to provide visibility into threats and control protocols, validate certificates, and handle failures. Malicious content will be prevented from entering your network, and sensitive content will be prevented from leaving your network concealed as encrypted traffic. As mentioned in Chapter 3, it is a best practice to use decryption policies in your network.
- Application Override policies allow you to override normal App-ID for specific traffic, if necessary. In some cases, you might have a custom application with specific signatures. For such an application, if there is no signature available, you can use Application Override for easier identification and reporting.
- Authentication policies enable you to authenticate end users before they can access services or applications. Whenever a user requests a service or application (e.g., by visiting a web page), the firewall evaluates Authentication policy. Based on the matching Authentication policy rule, the firewall then prompts the user to authenticate using one or more methods, such as login and password, voice, SMS, push, or one-time password (OTP) authentication.

Best practices policy rules are also available for most policy types to help you to get started quickly and securely if you are using Prisma Access in Cloud Management mode.

More Resources

See our technical documentation to learn more about [Panorama Managed](#) or [Cloud Managed](#) Prisma Access.

Chapter 5

Transitioning Wide Area Networks to a SASE Model

Overcome the Shortfalls of Legacy WANs

WAN technologies are used to interconnect networks at headquarters, data centers, and remote locations for an organization. MPLS and the public internet have become the most common option for providing WAN connectivity. Service providers use MPLS to deliver WAN services by performing segmentation and isolation between customers on the same shared infrastructure.

Headquarters, data centers, and branch locations use customer edge (CE) devices to connect to provider edge (PE) devices in the MPLS network. Whereas PE devices are shared across multiple customers, each CE device is dedicated to a single customer. From a routing perspective, static routes and BGP are commonly used.

The implementation in figure 20 shows the following architectural considerations:

- Each branch location is deployed in a different geographical location using the MPLS links to connect to the data center and the internet.
- The internet is accessible only via the data center. Any direct internet connection would not have any security applied to it.(e.g., mobile user IP pools, infrastructure, data center and remote network subnets).

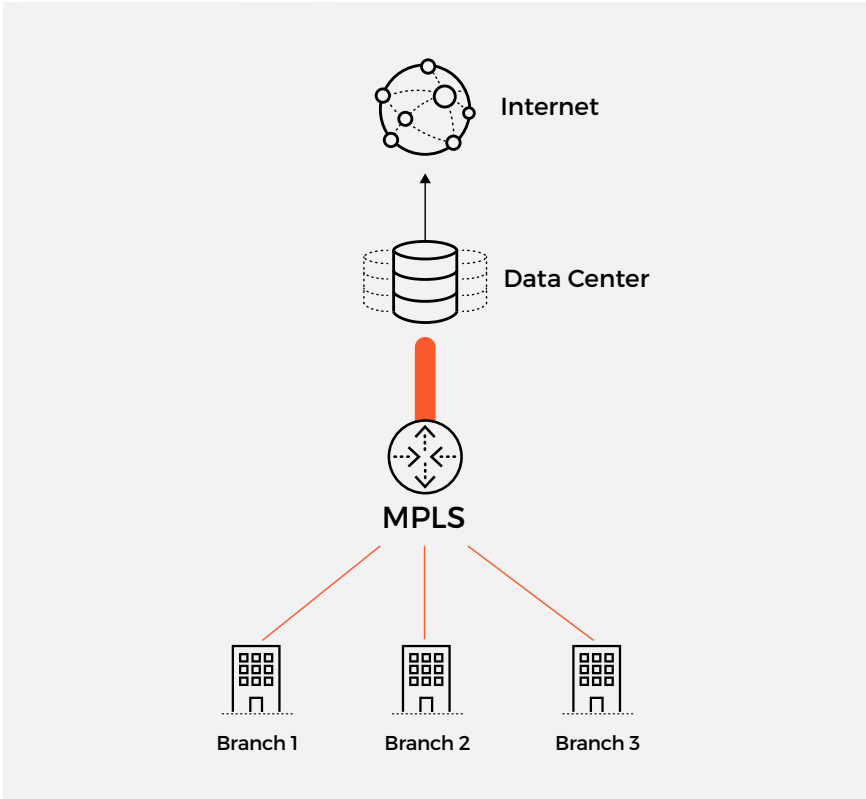


Figure 20: A simple example of a MPLS implementation

This clearly highlights a few architectural problems:

- Increased latency due to the backhauling of internet access
- Inconsistency in applying security for remote branches
- Lack of security inspection between branches

With Prisma Access, you can move to a SASE model that essentially provides a cloud-delivered network backbone from more than 100 locations in 76 countries. As such, you can fully migrate your legacy WAN and security services to a cloud native architecture.

The following changes will occur from an architectural perspective:

- Each branch will connect to Prisma Access through one of the 100+ PoPs available worldwide. Multiple PoPs can be used for resilience.
- A dedicated service connection will provide access to the data center so each branch and mobile user can have secured access to resources.
- A local breakout internet connection will be available for remote branches and mobile users. Security will be applied directly from the cloud.
- All remote networks and mobile users will have consistent security policies applied.
- All the features will be provided as a service, including scaling for performance, maintaining high availability of the resources, applying necessary updates, and more.

Prisma Access Integration with SD-WAN

SD-WAN technologies simplify the management and operations of a WAN connection and add intelligence to routing and path decisions. While adopting SD-WAN deployments, most organizations require direct internet access due to the cloud location of their SaaS applications.

SD-WAN solutions provide many benefits to organizations, such as cost savings, reducing complexity, and increasing the optimization of deployments, but they need to be properly secured. Prisma Access integrates with all SD-WAN vendors, but this guide focuses on the deeper integration provided with Prisma SD-WAN.

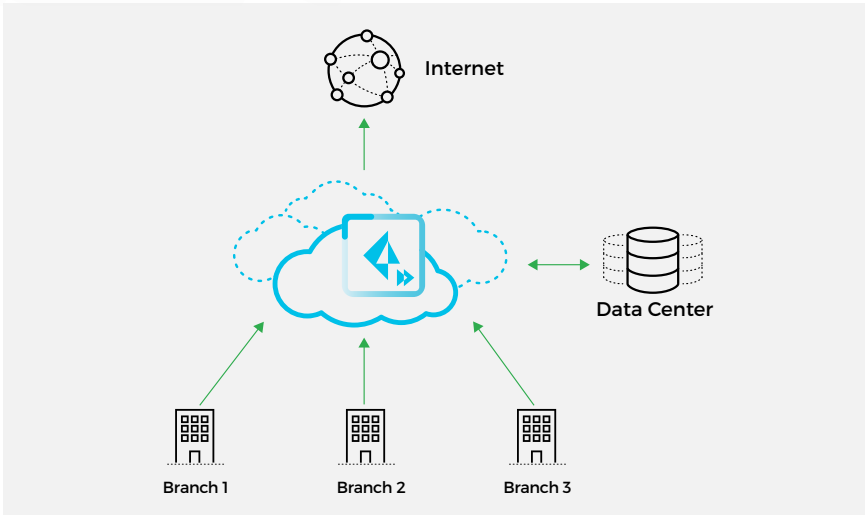


Figure 21: Example of a more efficient WAN architecture with Prisma Access

[Prisma SD-WAN](#), formerly CloudGenix SD-WAN, is a next-generation solution that helps you transform your branch office and retail locations, reduce WAN total cost of ownership, simplify management, and gain visibility into network traffic. Prisma SD-WAN fully integrates with Prisma Access to provide cloud-delivered security for branch and retail locations.

The Prisma SD-WAN [CloudBlades for Prisma Access](#) enables you to automate the deployment of remote networks with security policy automatically applied. This option requires that you deploy either an on-premises Docker container or a public cloud container to facilitate the communication between the CloudBlade for Prisma Access and Panorama.

The following sections provide guidance on how to integrate Prisma SD-WAN with Prisma Access based on two architectural scenarios:

1. SD-WAN with Prisma Access direct internet access
2. SD-WAN with regional hub/spoke architecture and Prisma Access

SD-WAN with Prisma Access Direct Internet Access

With this option, you can connect your remote site to Prisma Access by using an IPsec tunnel from the SD-WAN appliance. This tunnel can be used to transport all internet traffic to Prisma Access. Data center application traffic will travel directly to the application’s destination by using the SD-WAN fabric.

In this example (see figure 22), Prisma Access has one remote network deployed to connect to an Amsterdam office. This location connects to the Prisma SD-WAN appliance using the closest geographic PoP.

Figure 23 shows how you can configure a Prisma Access remote network in Panorama to connect to the Prisma SD-WAN appliance located in the Amsterdam office. We have used the Netherlands Central PoP and allocated a bandwidth of 50 Mbps. Static routes or BGP, or both, can be configured.

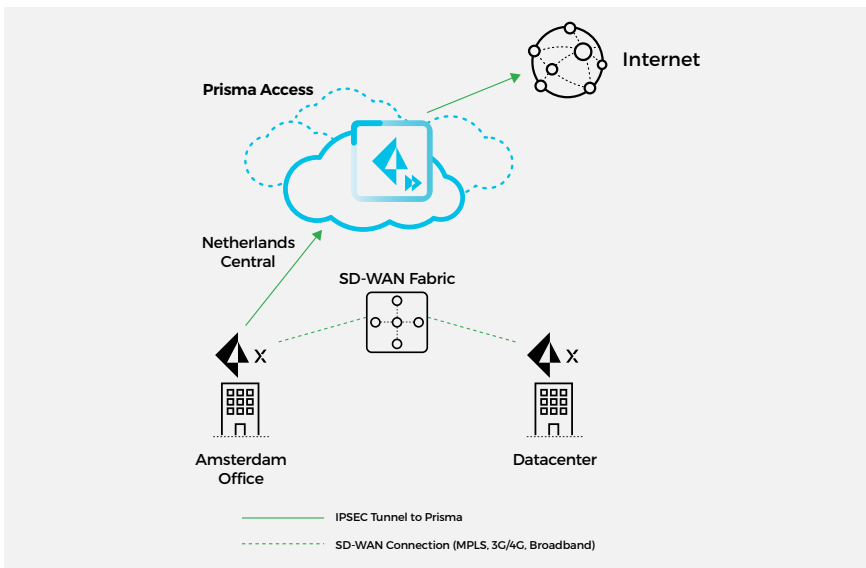
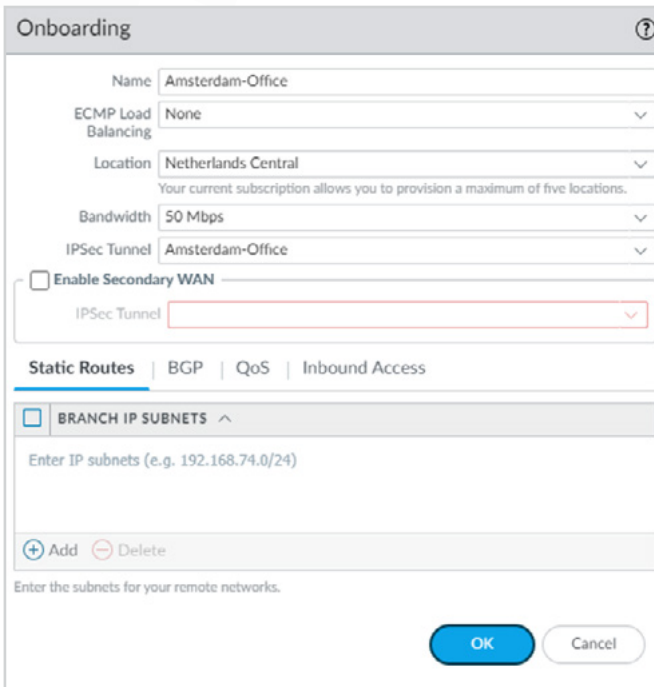


Figure 22: Prisma Access integration with Prisma SD-WAN



Onboarding ⓘ

Name:

ECMP Load Balancing:

Location:
Your current subscription allows you to provision a maximum of five locations.

Bandwidth:

IPsec Tunnel:

Enable Secondary WAN
IPsec Tunnel:

Static Routes | BGP | QoS | Inbound Access

BRANCH IP SUBNETS ^

Enter IP subnets (e.g. 192.168.74.0/24)

Enter the subnets for your remote networks.

Figure 23: Prisma Access with one remote network deployed

SD-WAN with Regional Hub-and-Spoke Architecture and Prisma Access

In this use case, not all branch offices will have a direct connection to Prisma Access. A regional data center can aggregate network traffic from smaller sites in a particular region. An example for this type of deployment would be when regional branches have a lower bandwidth connection to the internet.

In figure 24, the two data centers each have an IPsec tunnel to a separate Prisma Access location: one for US East and one for US West. The SD-WAN edge devices at each site will use traffic forwarding policies to determine the traffic to send to Prisma Access for security inspection.

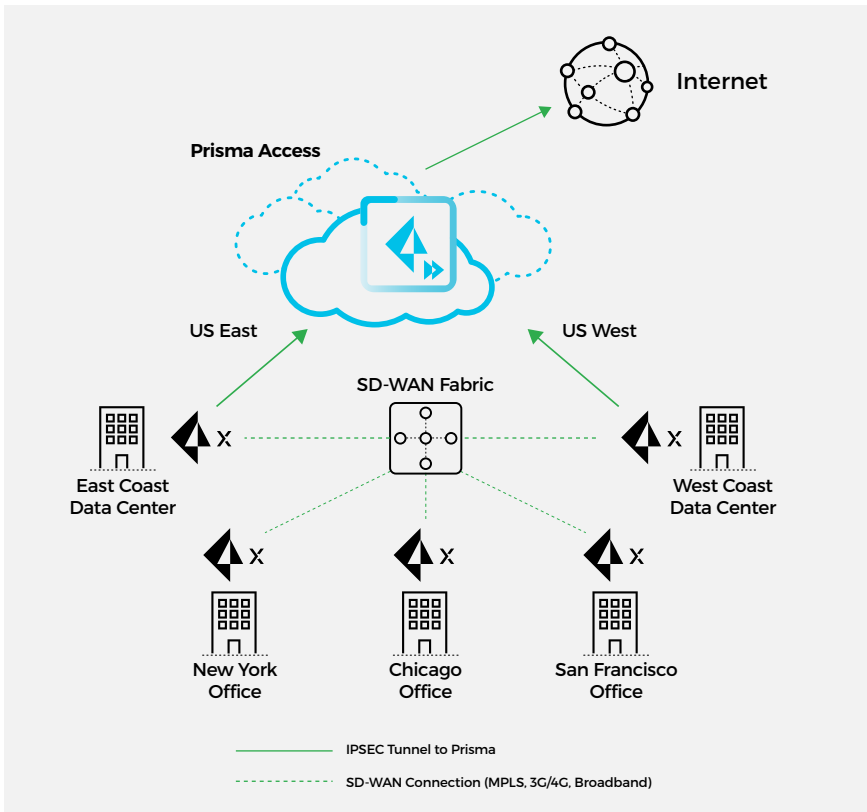


Figure 24: Regional hub-and-spoke SD-WAN integration with Prisma Access

More Resources

Learn more on our [Prisma SD-WAN website](#).

You can also take a look at our [Prisma SD-WAN with Prisma Access Deployment Guide](#).



Special thanks to:

Jason Georgi

Matt De Vincentis

Shannon Bonfiglio

Tudor Andreescu

Don Meyer

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before.

For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Prisma, and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.





paloalto[®]
NETWORKS



PRISMA[®]
BY PALO ALTO NETWORKS