

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase sans-serif font.

TECHDOCS

What's New in the NetSec Platform

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2023-2024 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 9, 2024

Table of Contents

July 2024.....	11
AI Runtime Security.....	12
Browser Support for Remote Browser Isolation.....	13
Cross-Scope Referenceability in Snippets.....	14
Disable Default HIP Profiles.....	15
Encrypted DNS for DNS Proxy and the Management Interface.....	16
Mobile Support for Remote Browser Isolation.....	17
Panorama to Strata Cloud Manager Migration.....	18
Scan support for ChatGPT Enterprise App.....	19
Support for Deleting Connector IP Blocks.....	20
Email DLP Enhancements.....	21
June 2024.....	23
Auto VPN Support for HA Devices.....	24
Cloud NGFW Policy Management Using Strata Cloud Manager.....	25
Connect to GlobalProtect App with IPSec Only.....	26
Changes to Behavior for Web Traffic Handling.....	27
Dynamic Privilege Access.....	28
Embedded Browser Framework Upgrade.....	29
End User Coaching.....	30
Enhanced HIP Remediation Process Improvements.....	31
Enhancements for Authentication Using Smart Cards-Authentication Fallback.....	32
Enhancements for Authentication Using Smart Cards-Removal of Multiple PIN Prompts.....	33
Global Find Using Config Search.....	34
Local Configuration Management Support for Firewalls.....	35
Manage and Share Common Configuration Using Snippet Sharing.....	36
Native IPv6 Compatibility.....	37
Overlapping IP Address Support.....	38
PA-410R-5G Next-Generation Firewall.....	39
Simplified License Activation and Default Tenant Creation.....	40
Strata Logging Service in Strata Cloud Manager.....	41
Third-Party CDR Integration for Remote Browser Isolation.....	42
View and Monitor App Acceleration.....	43
View and Monitor Native IPv6 Compatibility.....	44
View and Monitor Third-Party Device-IDs.....	45
ZTNA Connector Application Discovery, User-ID Across NAT, and Support for Connector IP Block Deletion.....	46

May 2024.....	47
Advanced DNS Security.....	48
Advanced Threat Prevention (ATP) Support on CN-Series Firewall.....	49
Advanced Threat Prevention: Support for Zero-day Exploit Prevention.....	50
App Acceleration Support for Additional Apps.....	51
Authorized Support Center Support View.....	52
Bulk Configuration.....	53
Business Continuity During Mergers and Acquisitions.....	54
Calgary and South Africa Central Compute Locations.....	55
CIE (SAML) Authentication using Embedded Web-view.....	56
Configuration File Compression.....	57
Dynamic DNS Registration Support for Mobile Users—GlobalProtect.....	58
Explicit Proxy Support for South Africa Central Location.....	59
Fast-Session Delete.....	60
FedRAMP Moderate.....	61
FQDNs for Remote Network and Service Connection IPSec Tunnels.....	62
GlobalProtect Portal and Gateway Support for TLSv1.3.....	63
GlobalProtect Proxy Enhancements.....	64
GlobalProtect Support for PAN-OS-11.2-DHCP-Based IP Address Assignments.....	65
GTP Support for Intelligent Security.....	66
Increased Maximum Number of Security Rules for PA-3400 Series Firewalls.....	67
IPSec Serviceability.....	68
Local Deep Learning for Advanced Threat Prevention.....	69
Monitor Bandwidth on SD-WAN Devices.....	70
NGFW Clustering of PA-7500 Series Firewalls.....	71
OOXML Support for WildFire Inline ML.....	72
PA-410R Next-Generation Firewall.....	73
PA-450R-5G Next-Generation Firewall.....	74
PAN-OS 11.0, 11.1, and 11.2 Dataplane Support.....	75
PAN-OS 11.2 Support for Panoramas That Manage Prisma Access.....	76
Post Quantum Hybrid Key Exchange VPN.....	77
Prisma Access Internal Gateway.....	78
Remote Network Tunnel Automation API.....	79
Strata Cloud Manager Connectivity Using Port 443.....	80
TLSv1.3 Support for HSM Integration with SSL Inbound Inspection.....	81
User-ID for CN-Series.....	82
User-ID Across NAT.....	83
View and Monitor Third-Party Device-ID.....	84
Virtual Systems Support on VM-Series Firewall.....	85

Intelligent Traffic Offload - Layer 3 (Dynamic Routing) Support on VM-Series Firewall.....	86
Intelligent Traffic Offload - NAT Support on VM-Series Firewall.....	87
Zero Touch Provisioning (ZTP) Onboarding Enhancements.....	88
View Preferred and Base Releases of PAN-OS Software.....	89
April 2024.....	91
Additional Private Link Types.....	92
Additional SD-WAN Hubs in VPN Cluster.....	93
Aggregate Ethernet Interface Usability Enhancement.....	94
Configuration Indicator.....	95
Device Onboarding Rules.....	96
External Gateway Integration for Prisma Access and On-Premises NGFWs.....	97
Enterprise DLP Migrator.....	98
Software Cut-through based Offload on CN-Series Firewall.....	99
Software Cut Through Support for PA-400 and PA-1400 Series Firewalls.....	100
Strata Cloud Manager: Activity Insights.....	101
Strata Cloud Manager: Command Center.....	104
Trusted IP List.....	105
View Only Administrator Role Enhancement.....	106
Web Proxy for Cloud-Managed Firewalls.....	107
March 2024.....	109
Multitenant Notifications.....	110
February 2024.....	111
Authenticate LSVPN Satellite with Serial Number and IP Address Method.....	112
Private Key Export in Certificate Management.....	113
Clone a Snippet.....	114
Security Checks.....	115
GlobalProtect Portal and Gateway.....	116
IP Optimization for Mobile Users - GlobalProtect Deployments.....	117
License Enforcement for Mobile Users (Enhancements).....	118
Multiple Virtual Routers Support on SD-WAN Hubs.....	119
Native SASE Integration with Prisma SD-WAN.....	121
New Prisma Access Cloud Management Location.....	122
Normalized Username Formats.....	123
PAN-OS Software Patch Deployment.....	124
Policy Analyzer.....	125
Saudi Arabia Compute Location.....	126
Site Template Configuration.....	127
TACACS+ Accounting.....	128

Tenant Moves and Acquisitions.....	129
Traceability and Control of Post-Quantum Cryptography in Decryption.....	130
User Session Inactivity Timeout.....	131
December 2023.....	133
FedRAMP High "In Process" Requirements and Activation.....	134
License Activation Changes.....	135
Performance Policy with Forward Error Correction (FEC).....	136
View and Monitor ZTNA Connector Access Objects.....	137
Software Cut-Through Support for PA-3400 and PA-5400 Series Firewalls.....	138
Persistent NAT for DIPP.....	139
ZTNA Connector Wildcard and FQDN Support for Applications and Additional Diagnostic Tools.....	140
November 2023.....	141
5G Cellular Interface for IPv4.....	142
Advanced WildFire Inline Cloud Analysis.....	143
API Key Certificate.....	144
App Acceleration in Prisma Access.....	145
ARM Support on VM-Series Firewall.....	146
Authentication Exemptions for Explicit Proxy.....	147
BGP MRAI Configuration Support.....	148
Cloud Managed Support for Prisma Access China.....	149
Configuration Audit Enhancements.....	150
Strata Logging Service with CN-Series Firewall.....	151
Device-ID Visibility and Policy Rule Recommendations in PAN-OS.....	152
Dynamic IPv6 Address Assignment on the Management Interface.....	153
Dynamic Routing in CN-Series HSF.....	154
Enhanced IoT Policy Recommendation Workflow for Strata Cloud Manager.....	155
Enhanced SaaS Tenants Control.....	156
Exclude All Explicit Proxy Traffic from Authentication.....	157
GlobalProtect Portal and Gateway Support for TLSv1.3.....	158
IKEv2 Certificate Authentication Support for Stronger Authentication.....	159
Improved Throughput with Lockless QoS.....	160
Increased Device Management Capacity for the Panorama Virtual Appliance.....	161
Inline Security Checks.....	162
Integrate Prisma Access with Microsoft Defender for Cloud Apps.....	163
Intelligent Security with PFCP for N6 and SGI Use Cases.....	164
IoT Security: Device Visibility and Automatic Policy Rule Recommendations.....	165
IOT Security Support for CN-Series.....	166
IP Protocol Scan Protection.....	167

IPSec VPN Monitoring.....	168
Link Aggregation Support on VM-Series.....	169
Maximum of 500 Remote Networks Per 1 Gbps IPSec Termination Node.....	170
New Platform Support for Web Proxy.....	171
New Template Variables.....	172
PA-415-5G Next-Generation Firewall.....	173
PA-450R Next-Generation Firewall.....	174
PA-455 Next-Generation Firewall.....	175
PA-5445 Next-Generation Firewall.....	176
PA-7500 Next-Generation Firewall.....	177
Policy Rulebase Management Using Tags.....	178
Post Quantum IKE VPN Support.....	179
PPPoE Client for IPv6.....	181
Public Cloud SD-WAN High Availability (HA).....	182
Remote Browser Isolation.....	185
Secure Copy Protocol (SCP) Support.....	186
Security Checks.....	187
Service Connection Identity Redistribution Management.....	188
Service Provider Backbone Integration.....	189
Session Resiliency for the VM-Series on Public Clouds.....	191
SNMP Network Discovery for IoT Security.....	192
Strata Cloud Manager: Application Name Updates.....	193
Support for Strata Logging Service Switzerland Region.....	194
TACACS+ Accounting.....	195
Throughput Enhancements for Web Proxy.....	196
TLSv1.3 Support for Administrative Access Using SSL/TLS Service Profiles.....	197
Traceability and Control of Post-Quantum Cryptography in Decryption.....	198
Traffic Replication Remote Network and Strata Cloud Manager Support.....	199
VM-Series Device Management.....	200
View and Monitor App Acceleration.....	201
View and Monitor Remote Browser Isolation.....	202
Virtual Routing Forwarding for WAN Segmentation.....	203
October 2023.....	205
Cisco Catalyst SD-WAN Integration.....	206
September 2023.....	207
Cloud IP-Tag Collection.....	208
Config Version Snapshot.....	209
Create a Custom Path Quality Profile.....	210
Delete a Snippet.....	211

Web Proxy for Cloud-Managed Firewalls.....	212
High-Bandwidth Private App Access with Colo-Connect.....	213
Integrate Prisma Access with Microsoft Defender for Cloud Apps.....	215
Introducing ADEM APIs.....	216
Log Viewer Usability Enhancements.....	217
New Predefined BGP Redistribution Profile.....	218
New Prisma Access Cloud Management Location.....	219
Refresh Pre Shared Keys for Auto VPN.....	220
Strata Logging Service Regional Support.....	221
Troubleshoot NGFW Connectivity and Policy Enforcement Anomalies.....	222
August 2023.....	223
Credential Phishing Prevention Support.....	224
Prisma Access PAC File Endpoint for Explicit Proxy.....	225
User-Based Enforcement for Explicit Proxy Kerberos Authentication.....	226
Local Zones.....	227
DLP Support for AI Applications.....	228
July 2023.....	229
June 2023.....	231
High-Bandwidth Private App Access with Colo-Connect.....	232
Traffic Replication and PCAP Support.....	234
Third-Party Device-ID in Prisma Access.....	235
New and Remapped Prisma Access Locations and Compute Locations.....	236
Transparent SafeSearch Support.....	237
Private IP Visibility and Enforcement for Explicit Proxy Traffic Originating from Remote Networks.....	238
Service Provider Backbone Integration.....	239
Cloud Management of NGFWs.....	241
Feature Adoption Dashboard.....	242
Best Practices Dashboard.....	243
Compliance Summary Dashboard.....	244
Security Posture Insights Dashboard.....	245
Advanced Threat Prevention Dashboard.....	246
Custom Dashboard.....	247
Device Health Dashboard.....	248
Incidents and Alerts.....	249
NGFW SDWAN Dashboard.....	250
Capacity Analyzer.....	251
Enhancements to CDSS Dashboard.....	252

May 2023.....	253
Conditional Connect Method for GlobalProtect.....	254
Enhanced Split Tunnel Configuration.....	255
Prisma Access Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security.....	256
Host Information Profile (HIP) Exceptions for Patch Management.....	258
Host Information Profile (HIP) Process Remediation.....	259
License Activation.....	260

July 2024

Review all the new features we've introduced across the NetSec platform in July 2024.

AI Runtime Security

Palo Alto Networks AI Runtime Security is a purpose-built firewall to discover, protect, and defend the enterprise traffic flows against all potential threats focusing on addressing AI-specific vulnerabilities such as prompt injection, and denial-of-service attacks on AI models. It combines continuous runtime threat analysis of your AI applications, models, and data sets with AI powered security to stop attackers in their tracks. The AI Runtime Security leverages real-time AI-powered security protecting your AI application ecosystem from both AI-specific and conventional network attacks.

AI Runtime Security leverages critical anomaly detection capabilities and protects AI models from manipulation to ensure the reliability and integrity of AI output data. It rejects prompt injections, malicious responses, training data poisoning, malicious URLs, command and control, embedded unsafe URLs, and lateral threat movement.

AI Runtime Security uses Palo Alto Networks Strata Cloud Manager (SCM) as the main configuration and management engine. To begin with, activate and onboard your cloud service provider account on SCM. The AI Security Profile imports security capabilities from Enterprise DLP and URL Filtering for inline detection of threats in AI application traffic.

The AI Runtime Security is powered by the following four key elements:

Discover - The AI Runtime Security discovers your enterprise AI application and all other applications. The AI Runtime Security dashboard provides complete visibility and security insights of your AI and other applications in just a few clicks. You can effortlessly gain actionable intelligence on AI traffic flows covering your applications, models, user access, and infrastructure threats.

Deploy - The AI Runtime Security deployment using Terraform templates automates the deployment procedure reducing the human error, lowering the required time for manual configuration tasks, and for protecting your enterprise AI applications. Deploy your AI Runtime Security instance downloading the Terraform templates and provide permissions to your cloud service provider account projects to analyze flow logs and DNS logs.

Detect - Identify unprotected traffic flows with potential security threats to the cloud network and detect the potential security risks based on logs and recommended actions to remediate.

Defend - Shield your organization's AI application ecosystem from AI-specific and conventional network attacks by leveraging real-time AI-powered security. Get the continuous discovery of the AI network traffic on the containers and namespaces.

To learn more about AI Runtime Security activation, onboarding, and deployment, see [AI Runtime Security](#) documentation.

Browser Support for Remote Browser Isolation

In addition to Google Chrome, Microsoft Edge, and Safari browsers, the Firefox browser is now supported for Remote Browser Isolation (RBI) on macOS and Windows desktop operating systems.

Refer to [How Remote Browser Isolation Works](#) for the combination of operating systems and browsers that your users can use for isolated browsing.

Cross-Scope Referenceability in Snippets

Enterprises need to enforce configuration objects and global settings consistently across all deployments. By referencing global settings across various scopes, such as snippets or folders, organizations can streamline operations, eliminate redundant configurations, and enhance centralized management. For example, organizations can effectively manage custom URL categories for access policy rules, threat prevention profiles, zones, addresses, and other objects representing standard network segments.

This feature allows you to reference any common configurations or objects attached to a global scope and push to NGFWs or Prisma Access deployments. These shared objects and configurations within the global scope are available to all the snippets. Snippets associated with the global scope are considered a global snippet, and the objects defined within these snippets can be [referenced](#) across any snippets in the configuration. This simplifies the process of managing configurations from a single location, updating, and enforcing global standards across all deployments.

Disable Default HIP Profiles

The default HIP objects and HIP profiles in Strata Cloud Manager have been moved from the Global-Default snippet to the HIP-Default snippet, providing greater flexibility in managing the default HIP profiles. You can choose to [disable the default HIP profiles](#) by disassociating the HIP-Default snippet from the global folder.

Encrypted DNS for DNS Proxy and the Management Interface

When your operating systems and web browsers use DNS, securing such DNS traffic with encryption helps maintain privacy and protect the traffic from man-in-the-middle attacks. When your PAN-OS firewall acts as a DNS proxy, you can enable encrypted DNS and specify that the DNS proxy will accept one or more types of DNS communication from the client: DNS-over-HTTP (DoH), DNS-over-TLS (DoT), or cleartext.

You also select the type of encrypted DNS that the DNS proxy will use with DNS servers. In the event that the DNS server rejects encrypted DNS or the DNS proxy receives no response from the primary or secondary server within a timeout period, you have the option to fall back to unencrypted DNS communications with the server.

Additionally, you can enable encrypted DNS on the firewall's management interface such that DNS requests use DoH, DoT, or optionally fall back to unencrypted DNS.

Mobile Support for Remote Browser Isolation

To help broaden the device support for your managed users, mobile support is added for Remote Browser Isolation (RBI) in addition to macOS and Windows desktop operating systems. Your managed users can now use Android, iOS, and iPadOS devices for isolated browsing.

Refer to [How Remote Browser Isolation Works](#) for the combination of operating systems and browsers that are supported for RBI.

Panorama to Strata Cloud Manager Migration

If you have an existing Prisma Access (managed by Panorama) deployment and want to switch from Panorama to cloud management, Palo Alto Networks offers an [in-product workflow](#) that lets you migrate your existing Prisma Access configuration to Strata Cloud Manager. While this migration workflow is disabled by default, you can reach out to your account teams to enable this feature and begin the migration to cloud management.

Benefits of moving to cloud management include:

- Continuous best practice assessments
- Secure default configurations
- Machine Learning (ML)-based configuration optimization
- Simplified web security workflow
- Comprehensive and actionable visualizations
- Intuitive workflows for complex tasks
- Simple and secure management APIs
- Cloud-native architecture provides scalability, resilience, and global reach
- No hardware to manage or software to maintain

Scan support for ChatGPT Enterprise App

You can connect a ChatGPT Enterprise instance to Data Security to gain visibility into the usage of ChatGPT in your enterprise. Data Asset policies can be defined to create incidents for sensitive data. [Onboard](#) your ChatGPT Enterprise app to Data Security.

Support for Deleting Connector IP Blocks

To allow more flexibility after you configure Connector IP Blocks, you can now [delete and update](#) the Connector IP Blocks. However, you can delete the Connector IP Blocks only after you delete all the ZTNA objects such as connectors, applications, wildcards, and connector-groups on the tenant.

Email DLP Enhancements

Enterprise Data Loss Prevention (E-DLP) has introduced the following enhancements to [Email DLP](#) to strengthen your security posture when inspecting outbound emails from your organization to prevent exfiltration of sensitive data.

- If you need to send an outbound email containing sensitive data, you can now forward outbound [Gmail](#) and [Microsoft Exchange](#) emails to your Proofpoint server to encrypt emails on its way to the target recipient if Enterprise DLP detects sensitive data. Encrypting outbound emails containing sensitive data prevents email messages from being read by an unintended or unauthorized individual.
- [Email DLP](#) now supports inspection of .eml files and up to five levels of nested .eml email files. Enterprise DLP can only nested .eml files, and cannot inspect any other supported file types that may contain nested files.
- ([Microsoft Exchange only](#)) You can now configure Enterprise DLP to send an email notification to the outbound email sender in an [Email DLP policy rule](#) when Enterprise DLP detects sensitive data to immediately notify email senders when their email was not sent out to their intended recipient due to data security violation. For example, this notification allows an email sender that erroneously sent an outbound email containing sensitive to modify their email and resend it.

This applies to Email DLP policy rules where the response **Action** is **Forward email for approval to end user's manager**, **Forward email for approval to admin**, or **Quarantine**.

June 2024

Review all the new features we've introduced across the NetSec platform in June 2024.

Auto VPN Support for HA Devices

(HA deployments only) In an Auto VPN with SD-WAN configuration, the Auto VPN can now generate the appropriate configuration automatically for the active and passive HA peers (both branch and hub HA pairs). It enables the HA failovers to be seamless between the HA pairs.

Cloud NGFW Policy Management Using Strata Cloud Manager

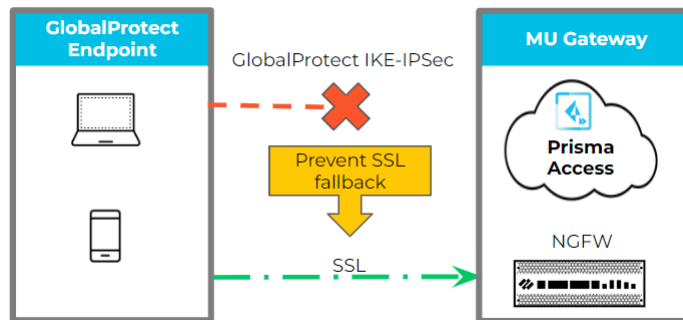
You can now link your Cloud NGFW resource with Strata Cloud Manager (SCM) for policy management. Strata Cloud Manager provides unified management for your entire network security deployment, which allows you to easily manage your Palo Alto Networks security infrastructure from a single, streamlined user interface. With this interface you gain comprehensive visibility into users, branch sites, applications, and threats across all network security enforcement points. This functionality provides actionable insights, better security, and easy troubleshooting and problem resolution.

This initial release allows you to create resources using the Cloud NGFW console, then you can register those resources with Strata Cloud Manager for centralized policy management. You'll use Strata Cloud Manager for monitoring and troubleshooting. For more information, see [Cloud Manager Policy Management for AWS](#).

Connect to GlobalProtect App with IPsec Only

To meet Federal Government compliance regulations, you can choose to prevent GlobalProtect fallback to SSL tunnel in case IPsec tunnel fails. If IPsec is not configured on the gateway, the GlobalProtect app stays disconnected.

The existing **Connect with SSL Only** feature and new **Connect with IPsec Only** features are combined under the single unified portal configuration of **Advanced Control for Tunnel Mode Behavior**. For more information, see step 5 in [Customize the GlobalProtect App](#).



Changes to Behavior for Web Traffic Handling

Embrace Web Access policies when creating new Internet Security policies or configurations, preserving existing rules in your setup. Web Security policies offer a framework for abstracting policies, enabling translation of user intent into the language understood by the enforcement node. This ensures continuity for current rules without altering user experience through default rule ordering.

This capability incrementally enhances existing [Web Security](#) workflows. Newly created Global Web Access policy rules are positioned between Web Security rules and the regular security rules, with Global Catch All policies placed on top of the intrazone default rules in post-rules.

Dynamic Privilege Access

For Enterprise IT and IT Enabled Services (ITES) companies that need to control which users have access to their customer projects, [Dynamic Privilege Access](#) provides a seamless, secure, and compartmentalized way for your users to access only those projects that they are assigned to. Employees are typically assigned to several customer projects and are provided with siloed access to these projects so that an authorized user can access only one customer project at a time.

A new predefined role called the **Project Admin** is available to allow project administrators to create and manage project definitions. Project administrators have the ability to map projects to select Prisma Access location groups, and create IP address assignments using DHCP based on the project and location group.

Embedded Browser Framework Upgrade

Starting with GlobalProtect 6.3, the embedded browser framework for SAML authentication has been upgraded to Microsoft Edge WebView2 (Windows) and WebKit (macOS). This provides a consistent experience between the embedded browser and the GlobalProtect client. WebView2 and WebKit are also compatible with FIDO2-based authentication methods.

By default, tenants using SAML authentication are configured to utilize the embedded WebView2 (Windows) or WebKit (macOS) instead of relying on the system's default browser. With this enhancement, there's no need for end users to configure a SAML landing page, eliminating the necessity to manually close the browser. This streamlines the authentication process.

In a Microsoft entra-joined environment with SSO enabled, users are not required to enter their credentials in order to authenticate to Prisma Access using GlobalProtect. This seamless experience is true whether the user is logging in to their environment for the first time or whether they have logged in before. If there is an error during the authentication, it is displayed in the embedded browser. This authentication process works across all device states.

In a non entra-joined environment with SSO enabled, users must enter their credentials during the initial login. On subsequent logins, the credentials are auto-filled as long as the SAML identity provider (IdP) session is active and has not timed out. For more information, see [CIE \(SAML\) Authentication using Embedded Web-view](#).

End User Coaching

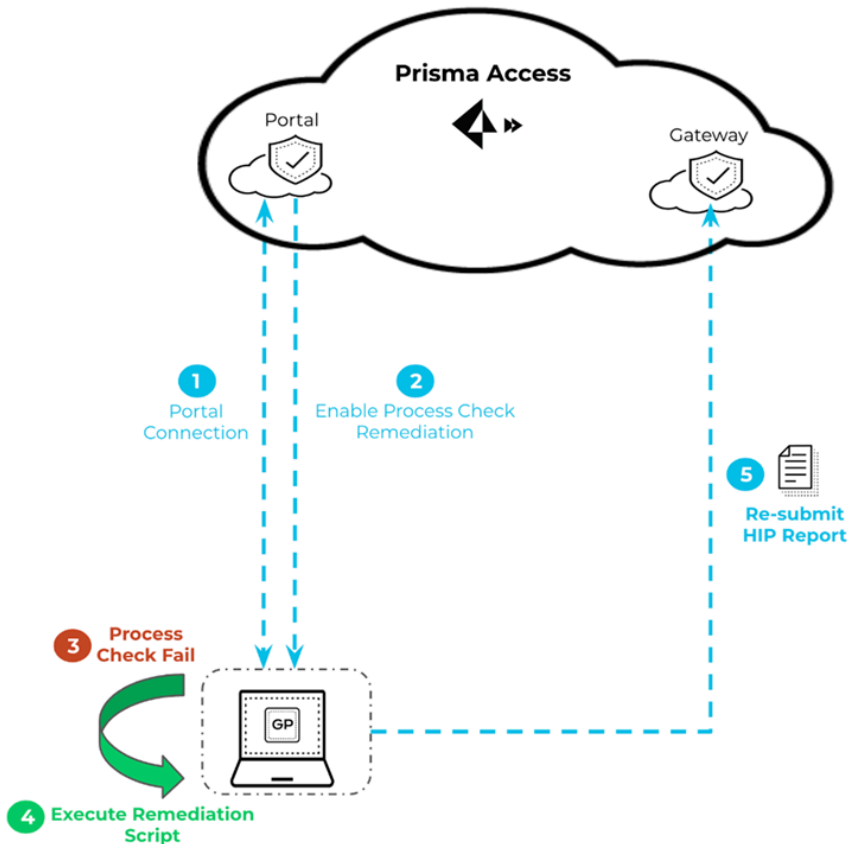
[End User Coaching](#) allows you to notify and coach end users when their actions violate a Security policy rule because it contains sensitive data that cannot leave your corporate network. Prisma Access (Managed by Strata Cloud Manager) administrators can immediately notify end users through the [Access Experience User Interface](#) (UI) when an end user uploads, downloads, or posts content that is blocked by Enterprise Data Loss Prevention (E-DLP). End user notifications are configured using the [User Coaching Notification Template](#) created on Strata Cloud Manager and are associated with a DLP rule for both **File-Based** and **Non-File Based** traffic. The notification template allows you to fully customize the message to be displayed in the notification and support variables to dynamically fill in DLP incident information based on the file name, traffic direction, application, and action. After an Enterprise DLP incident is generated, the end user who generated the incident can view the [Data Security notification](#) to view more details about current and past notifications.

Enhanced HIP Remediation Process Improvements

You can now configure the GlobalProtect app to [rerun the HIP remediation script](#) whenever the GlobalProtect endpoint fails the process check after running the configured HIP remediation process.

This feature enables the app to rerun the HIP remediation script when the process fails after the set HIP remediation timeout period to help the endpoint recover from a HIP check failure. The app reruns the remediation script after a process check failure based on the HIP Process Remediation Retry count you configure through the app settings of the GlobalProtect portal. When you enable this feature, the GlobalProtect app resubmits the HIP report only after the app reruns the HIP remediation script in case of HIP check failures.

For example, if you configure the retry count as 3 and the remediation timeout period as 5 mins in the portal configuration, then every time the endpoint fails the process check after performing the remediation process, the app runs the script three times and waits up to 5 mins before it submits the HIP report.



Enhancements for Authentication Using Smart Cards- Authentication Fallback

The smart card authentication method is enhanced to include an [authentication fallback mechanism when the smart card is not available](#) to authenticate users to the GlobalProtect app.

When you set smart card authentication for the end users to authenticate to the GlobalProtect app and when the configured smart card is not available, the user authentication will now fallback to any other username and password authentication methods that you have configured for the app.

The smart card authentication fallback will happen only if you have selected the [Allow Authentication with User Credentials OR Client Certificate](#) option while configuring the GlobalProtect gateway and portal. This option defines whether users can authenticate to the portal or gateway using credentials and/or client certificates.

Enhancements for Authentication Using Smart Cards- Removal of Multiple PIN Prompts

You can now use the [GlobalProtect app with smart card and ActivClient software without entering the smart card PIN multiple times](#) when the Connect Before Logon (CBL) connection method is configured for the GlobalProtect app.

Previously, when ActivClient software was installed on the devices and Connect Before Logon was configured for the GlobalProtect app, end users were prompted to enter the smart card PIN multiple times while trying to connect using the CBL method.

This enhancement removes the multiple smart card PIN prompts received by the end users from the Windows identity provider and ActivClient while connecting the GlobalProtect app with the smart card along with ActivClient software. The GlobalProtect app now prompts the user to enter a PIN only once and the PIN prompt is from ActivClient software.

Global Find Using Config Search

Config Search in Strata Cloud Manager enables you to search configuration objects and settings for a particular string, such as IP addresses, object name, referenced objects, duplicate objects, policy names, policy rules, policies covered for specific CVEs, rule UUID, predefined snippets, or application name.

The search results are categorized and provide links to the configuration location in the Strata Cloud Manager, allowing you to easily find all occurrences and references of the searched string.

Local Configuration Management Support for Firewalls

Eliminate the need for context switching from central management to individual firewalls for managing local configurations.

This feature enhances readability, simplifies troubleshooting, and reduces manual effort by providing visibility and control over local firewall configurations through Strata Cloud Manager. Additionally, it identifies any conflicting or overridden objects between local and pushed configurations, making it easier to troubleshoot.

Manage and Share Common Configuration Using Snippet Sharing

Manually sharing and keeping the configuration synchronized across multiple tenants is both error prone and inefficient.

This feature provides a unique and flexible way to share common configuration in a multitenant environment. You can save and manage any combination of configuration as a snippet, seamlessly sharing them across tenants under a customer account. This offers tremendous flexibility and control in managing shared configuration across tenants. This feature offers a variety of use cases such as updating configurations from lab to production environments, migrating configurations between tenants, centralizing configuration management for common use cases across tenants, and managing global configurations in a multibusiness unit setup.

Native IPv6 Compatibility

Prisma Access is extending its support for IPv6 from [private applications](#) to encompass comprehensive end-to-end IPv6 support for Mobile Users, Remote Networks, and Service Connections. One advantageous aspect of native IPv6 support is its capacity to enable Mobile Users utilizing IPv6-only endpoints to establish connections with Prisma Access via IPv6 connections using GlobalProtect. Additionally, this support facilitates accessing public SaaS applications over the internet, particularly where those destinations necessitate IPv6 connections.

IPv6 boasts a significantly larger address space compared to IPv4, thereby accommodating an almost limitless number of unique IP addresses. Through native IPv6 support, Prisma Access is engineered to be compatible with both IPv6 and dual-stack connections, facilitating the migration process from IPv4 to IPv6. This compatibility ensures backward compatibility and empowers organizations in their transition to cloud-based and IPv6-enabled networks.

Overlapping IP Address Support

Without the ability to reuse the same IP address across multiple interfaces, it can be difficult to manage large environments where the firewall resources are shared or segmented. Beginning with PAN-OS 11.1.4, [duplicate \(overlapping\) IP address support](#) allows you to use the same IPv4 or IPv6 address on multiple firewall interfaces when the interfaces belong to different logical routers. The interfaces can belong to different security zones on a single virtual system, or belong to the same zone on different virtual systems, or belong to different zones and different virtual systems.

PA-1400 Series firewalls, VM-Series firewalls, and Panorama template stacks support overlapping addresses.

Overlapping IP address support requires the Advanced Routing Engine. When you enable Advanced Routing, the option to enable Duplicate IP Address Support becomes available for you to select. The overlapping addresses can be statically configured or dynamically assigned to interfaces. All Layer 3 interfaces types (Ethernet, VLAN, tunnel, loopback, Aggregate Ethernet [AE], and AE subinterfaces) support overlapping IP addresses.

PA-410R-5G Next-Generation Firewall

The PA-410R-5G is a new ruggedized firewall appliance that is a cellular version of the PA-410R. The PA-410R-5G is designed for industrial, commercial, and government deployments. This IP65 rated hardware is suited for installation in harsh environments with extreme temperatures and high humidity levels.

The PA-410R-5G is supported on PAN-OS 11.1.4 and later versions. The firewall features four 5G multi-band antennas and two nano SIM card slots to enable connectivity using two different mobile network providers. The PA-410R-5G also has two SFP ports and four RJ-45 ports. The RJ-45 ports include two fail-open ports that can be configured to provide a pass-through connection in the event of a power failure.

The PA-410R-5G is powered by DC power and supports power redundancy. The device has a fanless design and can be installed on a wall or DIN rail. The hardware is compliant with ICS/SCADA system architecture.

Simplified License Activation and Default Tenant Creation

Products offered for free, such as AIOps Free and CIE, don't need an activation link or auth code for activation. The hub serves as the entry point for you to activate these products. Activating a product from the tenant view of the hub creates a single default tenant where the product is deployed. If you have a single Customer Support Portal account, certain fields in the activation form are prepopulated on your behalf for a simplified license activation experience.

First-time license activation for paid products is still through an email that you receive from Palo Alto Networks. The email still contains an activation link. Activating a product from the activation link creates a single default tenant where the product is deployed. If you have a single Customer Support Portal account, certain fields in the activation form are prepopulated on your behalf for a simplified license activation experience.

If you have multiple Customer Support Portal accounts, during activation you will select the Customer Support Portal account that you want to use for managing your product. If you're a managed security service provider (MSSP), during activation you will select the Customer Support Portal account that you want to use for managing your customers' products.

Get started with [License Activation, Subscription Management, Tenant Management, and Product Management](#).

Strata Logging Service in Strata Cloud Manager

You can now manage your [Strata Logging Service](#) instance with [Strata Cloud Manager](#). After you have activated and deployed Strata Logging Service, log in to Strata Cloud Manager on [hub](#) and select **Settings > Strata Logging Service** to manage your Strata Logging Service instance. Additionally, you can also continue to use the Strata Logging Service standalone app available on the hub to manage your instances. The logging data is the same in both Strata Logging Service app and Strata Cloud Manager, except for their web interface differences.

Use Strata Logging Service to:

- [Check the status](#) of a Strata Logging Service instance
- [View and onboard](#) firewalls, Cloud NGFW, Prisma Access, or Panorama appliances
- [View the allocated log storage quota](#), the available storage space, and the number of days the logs are retained based on your incoming log rate
- [Configure log storage quota](#)
- [Search, filter, and export log data](#)
- [Forward log data](#) to external servers for long-term storage, SOC, or internal audit

Third-Party CDR Integration for Remote Browser Isolation

Protect your users against zero-day threats hidden in files that they download from the internet by [integrating Remote Browser Isolation \(RBI\) with a third-party content disarm and reconstruction \(CDR\) provider](#).

When users browse the web and download various types of files to their local devices, they are exposed to zero-day threats. Even with file scanning or antivirus solutions in play, these threats could escape detection, allowing malware to be delivered to your users' managed devices and rendering them as patient-zero.

With third-party CDR integration, any files downloaded while in RBI will be disarmed and reconstructed using CDR. The CDR provider will remove the malicious content from the files and deliver the sanitized files in their original file formats to the user.

You can [integrate with Votiro](#) to utilize Votiro's CDR capabilities to process and appropriately sanitize a file before it is downloaded to the user's device from RBI, thus keeping the user protected from any potentially malicious executables embedded in the file.

View and Monitor App Acceleration

App Acceleration addresses the causes of poor app performance and acts in real-time to boost throughput while maintaining best-in-class security, improving the user experience for Prisma Access GlobalProtect and Remote Network users. You can [view and monitor App Acceleration](#) to see details about accelerated applications in your environment. In Strata Cloud Manager, select **Monitor > Applications** to view details about all accelerated applications.

View and Monitor Native IPv6 Compatibility

If you use [IPv6 networking](#) in your [Mobile Users—GlobalProtect](#) deployment, you can configure Prisma Access to use IPv6 addresses in your mobile user networking. To view information about IPv6 in your GlobalProtect deployment, go to **Insights > Users** in Strata Cloud Manager Command Center.

View and Monitor Third-Party Device-IDs

You can use the Cloud Identity Engine with Prisma Access to apply information from third-party IoT detection sources to simplify the task of identifying and closing security gaps for devices in your network. See [Configure Third-Party Device-ID in Prisma Access](#) for details about setup and configuration.

Go to **Monitor > Devices > IOT to get insights on your IoT devices**, such as the number of IoT devices connected within the last 30 minutes, all IoT devices connected during the time range selected, and details about all connected IoT devices.

ZTNA Connector Application Discovery, User-ID Across NAT, and Support for Connector IP Block Deletion

ZTNA Connector provides the following new functionalities with this release:

- **Application Discovery**—Your enterprise network can have many applications hosted in its cloud or data center environment. In many cases, the network security teams are unaware of all the applications that are hosted in the network. As a result, when you deploy a ZTNA Connector and start to add application targets in connector groups, it can be difficult to determine which applications you need to add.

Private application target discovery simplifies application hosting and discovery of applications that are hosted in AWS.

The private application target discovery service:

- Finds the Prisma Access tenant you have deployed and allows you to onboard that tenant to start the app discovery process, or lets you remove an existing tenant to remove apps that are discovered.
 - Retrieves application relevant information from one or more cloud providers accounts using Assumed Role and Work Load Identity (WLI).
 - Allows you to view the application discovery results.
 - Provides a way for other modules to query for the discovered applications.
- **User-ID Across NAT**—Mobile users access private apps using a ZTNA Connector. If your deployment uses a Next-Generation Firewall (NGFW) in the data center or headquarters location where the private apps are located, and ZTNA Connector has source NAT enabled, the NGFW can't retrieve the User-ID and Device-ID mapping. Source NAT on the service connection or ZTNA Connector prevents the mobile users' User-ID and Device-ID mapping to be distributed to the NGFW. If the NGFW can't retrieve this mapping, it can't enforce zone-based Security policy rules you have created on it based on User-ID or Device-ID mapping.

User-ID Across NAT lets your network distribute the User- or Device-ID mapping from mobile users to the NGFW, thus allowing the NGFW to enforce Security policy rules based on the User-ID mapping it has learned from the service connection or ZTNA Connector. This configuration ensures a consistent security posture across your mobile user deployment.

- **IP Connector Block Deletion**—To allow you more flexibility after configuring Connector IP Blocks, you can now delete and update the Connector IP Blocks. You can delete the Connector IP Blocks only after you delete all the ZTNA objects such as connectors, applications, wildcards, and connector-groups on the tenant.

May 2024

Review all the new features we've introduced across the NetSec platform in May 2024.

Advanced DNS Security

The [Advanced DNS Security service](#) is a new subscription offering by Palo Alto Networks that operates new domain detectors in the Advanced DNS Security cloud that inspect changes in DNS responses to detect various types of DNS hijacking in real-time. With access to Advanced DNS Security, you can detect and block DNS responses from hijacked domains and misconfigured domains. Hijacked and misconfigured domains can be introduced into your network by either directly manipulating DNS responses or by exploiting the DNS infrastructure configuration settings in order to redirect users to a malicious domain from which they initiate additional attacks. The primary difference between these two techniques is where the exploit occurs. In the case of DNS hijacking, the attackers gain the ability to resolve DNS queries to attacker-operated domains by compromising some aspect of an organization's DNS infrastructure, be it through unauthorized administrative access to a DNS provider or the DNS server itself, or an MiTM attack during the DNS resolution process. Misconfigured domains present a similar problem - the attacker seeks to incorporate their own malicious domain into an organization's DNS by taking advantage of domain configuration issues, such as outdated DNS records, which can enable attackers to take ownership of the customer's subdomain.

Advanced DNS Security can detect and categorize hijacked and misconfigured domains in real-time by operating cloud based detection engines, which provide DNS health support by analyzing DNS responses using ML-based analytics to detect malicious activity. Because these detectors are located in the cloud, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages when changes to detectors are made. Upon initial release, Advanced DNS Security supports two analysis engines: DNS Misconfiguration Domains and Hijacking Domains. Additionally, DNS responses for all DNS queries are sent to the Advanced DNS Security cloud for enhanced response analysis to more accurately categorize and return a result in a real-time exchange. Analysis models are delivered through content updates, however, enhancements to existing models are performed as a cloud-side update, requiring no updates by the user. [Advanced DNS Security is enabled and configured](#) through the Anti-Spyware (or DNS Security) profile and require active Advanced DNS Security and Advanced Threat Prevention (or Threat Prevention) licenses.

Advanced Threat Prevention (ATP) Support on CN-Series Firewall

CN-Series firewall now supports real-time [Advanced Threat Prevention \(ATP\)](#) for detecting malware and zero-day vulnerability exploits using the advanced ML engines in the cloud. The CN-Series ATP is delivered as a containerized solution for high scalability and low-latency cloud-native service.

The ATP feature is supported on PAN-OS 11.0 and later releases and all [CN-Series deployment modes](#): deploying the CN-Series firewall as a Kubernetes service, Daemonset, and a Kubernetes CNF. For the ATP feature, you need the Advanced Threat Prevention licenses and enable the **Inline Cloud Analysis**.

To enable the CN-Series ATP feature, you can use the YAML files from the Palo Alto Networks CSP for deploying the containerized firewall pods or enable the ATP feature while configuring the CN-Series deployment on the Palo Alto Customer Service Portal (CSP).

Advanced Threat Prevention: Support for Zero-day Exploit Prevention

Palo Alto Networks now operates new inline deep learning detection engines in the Advanced Threat Prevention cloud to analyze traffic for command injection and SQL injection vulnerabilities in real-time to protect users against zero-day threats. This also includes signature-based prevention for thousands of known vulnerabilities and industry-leading response times for critical and high CVEs for top vendors.

By operating cloud-based detection engines, you can access a wide array of detection mechanisms that are updated and deployed automatically without requiring the user to download update packages or operate process intensive, firewall-based analyzers which can sap resources. Inline cloud analysis operates under your Vulnerability Protection profile and supports two analysis engines upon initial release: SQL injection and Command injection. Additional analysis models are delivered through content updates, however, enhancements to existing models are performed as a cloud-side update, requiring no local update process. [Inline cloud analysis is enabled and configured using the Vulnerability Protection profile and requires an active Advanced Threat Prevention license.](#)

App Acceleration Support for Additional Apps

Enterprises today employ workers everywhere, connecting to apps that are anywhere. Hybrid workforces rely on high-performing app experiences, but slowdowns caused by cloud latency and adverse network conditions drain productivity and frustrate workers. The major causes of poor performance can consist of:

- Cloud latency experienced when apps are processing dynamic content
- Wireless connectivity issues

Both of these issues exist outside the control of the enterprise. Apps use Content Delivery Network (CDN) caching, but modern apps are powered by dynamic content that can't be cached. And consumer-grade Wi-Fi and wireless connectivity have no performance service-level agreements (SLAs) because wireless conditions like interference and signal strength are continuously changing.

App Acceleration for Prisma SASE directly addresses the causes of poor performance by accelerating dynamic content in top SaaS apps, and has added support for these apps:

- AWS S3
- Azure Storage
- Box
- Google Drive
- Microsoft OneDrive
- Salesforce
- SAP Ariba
- ServiceNow
- Slack (*file downloads*)
- Zoom (*file downloads from chat, recording downloads*)

These enhancements provide you with the following benefits:

- Up to five times the improvement over direct-to-internet app performance (measured in app response time and throughput metrics)
- Enriches AI-powered ADEM with Real User Metrics (RUM) to enhance observability into performance issues
- No code changes required

Authorized Support Center Support View

The Authorized Support Center (ASC) Support View dashboards have moved back into the Strata Multitenant Cloud Manager. The [ASC Support View](#) provides relevant tools and data to enable ASC partners to address their L1 and L2 Cloud managed SASE issues. This feature is available in **Strata Multitenant Cloud Manager > ASC Support View**.

Bulk Configuration

The Strata Multitenant Cloud Manager enables managed security service providers (MSSP) or distributed enterprise customers of Prisma Access to define and enforce global security policies in all or some of their child tenants. You would use this to create repeatable common configurations that can be applied to many tenants, while allowing for granular customization of configurations at the individual tenants for local tenant admins. [Bulk configuration](#) management is only supported for Cloud managed tenants. Panorama managed tenants are not supported as part of this feature. This feature is available in **Strata Multitenant Cloud Manager > Manage > Bulk Configuration**.

Business Continuity During Mergers and Acquisitions

If your organization has merger and acquisition (M&A) activity, you might have a need for existing gateways to either not reference an earlier brand name or reference a new brand name. With this functionality, Prisma Access ensures business continuity by updating the gateway name to the new brand name and displaying the new name in the UI, in logs, and anywhere else the gateway name is referenced.

Calgary and South Africa Central Compute Locations

Prisma Access adds two new compute locations: Canada West (Calgary) and South Africa Central. The following locations are remapped to the new compute location:

- The **South Africa Central** location is remapped to the South Africa Central compute location.
- The **Canada West** location is remapped to the Canada West (Calgary) compute location.

New deployments have the new remapping applied automatically. If you have an existing Prisma Access deployment that uses one of these locations and you want to take advantage of the remapped compute location, follow the procedure to [add a new compute location to a deployed Prisma Access location](#).

CIE (SAML) Authentication using Embedded Web-view

May 2024

- Available in PAN-OS 11.2.0 and later releases.
-

GlobalProtect now supports CIE (SAML) authentication using embedded web-view without using any pre-deployment configuration.

The enhancement also supports force authentication and enables end users to authenticate again while reconnecting to the app even when the SAML token remains valid and helps enterprises to achieve security compliance. You can now configure the GlobalProtect app to prompt the end users to reenter their credentials to authenticate whenever they reconnect the [GlobalProtect app using the Cloud Identity Engine \(CIE\) authentication method](#).

Previously, users were not prompted to re-authenticate when they tried to reconnect to the app using the CIE authentication method.

Configuration File Compression

When you push a configuration change from Strata Cloud Manager, the XML configuration file containing the existing and new configurations is pushed from Strata Cloud Manager to your NGFW (Managed by Strata Cloud Manager). Strata Cloud Manager now compresses the pushed XML configuration file exchanged by at least 15% if your NGFW (Managed by Strata Cloud Manager) is running PAN-OS 11.2. All NGFW (Managed by Strata Cloud Manager) responses, such as confirming that the XML config file was received and the commit status, queries for data, and complete and read operations from Strata Cloud Manager are also compressed and reduced by at least 15%. This helps reduce the time it takes to push configuration changes from Strata Cloud Manager and query for information from your NGFW (Managed by Strata Cloud Manager). The compression has no impact on management or data processing functionality.

Dynamic DNS Registration Support for Mobile Users— GlobalProtect

When a mobile user connects remotely to Prisma Access using GlobalProtect, the DNS and IP Address Management (IPAM) servers in your enterprise are not updated with the GlobalProtect gateway-assigned client IP address and endpoint FQDN. This results in your IT administrator and your apps not being able to identify and update remote endpoints with FQDN. With Dynamic DNS registration, Prisma Access integrates with IPAM vendors to dynamically create A and PTR records in the DNS servers with IPAM updates.

Explicit Proxy Support for South Africa Central Location

South Africa Central is added as a supported location for Prisma Access Explicit Proxy.

Fast-Session Delete

If your deployment has a requirement to delete sessions quickly, you can enable [fast session delete](#), which allows Prisma Access to reuse TCP port numbers before the TCP TIME_WAIT period expires, and can be useful for SSL decrypted sessions that may be short-lived. You can enable this functionality for Remote Networks, Service Connections, and Mobile Users – GlobalProtect; for Mobile Users–Explicit Proxy deployments, this functionality is enabled by default and cannot be changed.

FedRAMP Moderate

Fedramp requirements are security controls and well established standards for cloud solutions intended for Cloud Service Providers managing and processing the government data. Many government agencies mandate the Fedramp authorization. Palo Alto Networks products and services are Fedramp Authorized to increase security, reliability, consistency, monitoring and thereby gaining the trust and confidence of Federal agencies.

To ensure FedRAMP Moderate compliance, [Prisma SASE FedRAMP Moderate](#) adds support for additional Prisma SASE apps, add-ons, and certain features.

FQDNs for Remote Network and Service Connection IPsec Tunnels

When you onboard a Service Connection or Remote Network connection, a public IP address is assigned for the other side of the IPsec tunnel (the [Service IP Address](#)). You use these public IP addresses for your CPE in your branch site or headquarters or data center location. Keeping records of all the IP addresses you need to configure on your CPE can be time consuming.

Instead of IP addresses, Prisma Access provides you FQDNs to use for the other end of the IPsec tunnel for Service Connections and Remote Network Connections, thus facilitating CPE setup at your branch sites or headquarters or data center locations.

GlobalProtect Portal and Gateway Support for TLSv1.3

You can now [configure SSL/TLS service profiles using TLSv1.3](#) on the firewall that is hosting the GlobalProtect portal or gateway to establish TLS connectivity between GlobalProtect components. TLSv1.3 is the latest version of the TLS protocol, which provides increased network security by removing the weak ciphers supported in the earlier versions of TLS and adding more secure cipher suites. In addition, the GlobalProtect gateway and portal now support the following TLSv1.3 cipher suites:

- TLS-AES-128-GCM-SHA256
- TLS-AES-256-GCM-SHA384
- TLS-CHACHA20-POLY1305-SHA256

You can configure SSL/TLS service profiles with TLSv1.3 to provide enhanced security and a faster TLS handshake while establishing connection between GlobalProtect components. To provide the strongest security, you must set both the minimum and maximum supported version as TLSv1.3 in the SSL/TLS service profile.

GlobalProtect Proxy Enhancements

GlobalProtect Proxy now

1. supports all IPv4 TCP connections, including non-proxy-aware traffic, to better support the needs of your network beyond only proxy-aware traffic
2. supports multiple Explicit Proxy channels to different regions, enabling you to support apps and destinations that have region-specific requirements.

Additionally, Prisma Access Insights now surfaces GlobalProtect Proxy data under **Mobile Users - GlobalProtect** and includes additional metrics, such as connection method, so that you can have greater visibility into your GlobalProtect Proxy performance.

GlobalProtect Support for PAN-OS-11.2-DHCP-Based IP Address Assignments

May 2024

- Available in PAN-OS 11.2.0 and later releases.
-



Starting from PAN-OS 11.2.1, the DHCP Based IP Address Assignment feature is supported for both VM-Series virtual firewall and hardware next-generation firewall platforms.

DHCP Based IP Address Assignment feature in PAN OS 11.2.0 release is supported for VM-Series Virtual Firewalls only. The feature is not supported for hardware next-generation firewall platforms.

You can now configure a DHCP server profile on the GlobalProtect gateway to use DHCP server for managing and assigning IP addresses for the endpoints connected remotely through the GlobalProtect app. Users who are using enterprise DHCP servers can enable this feature for centralized IP management and IP address assignments. When you configure a DHCP server profile on the GlobalProtect gateway and upon successful communication between the gateway and the DHCP server, the gateway obtains DHCP IP addresses from a DHCP member server. The GlobalProtect gateway then assigns the IP addresses as the tunnel IP for the endpoints that are remotely connected through the GlobalProtect app. If the DHCP server fails to respond to the gateway within the set communication timeout and retry times period, the gateway falls back to the private Static IP pool for the allocation of IP addresses for the endpoints.

When the GlobalProtect gateway assigns the DHCP IP addresses to the endpoints, you can configure their DHCP server to create Dynamic DNS (Address and Pointer Record) records for the GlobalProtect connected users. DDNS are useful for endpoint admins to do troubleshooting on the GlobalProtect connected remote user endpoints. The IP addresses get registered to the DDNS server only when you configure IP Address Management (IPAM) on Windows server, DDNS server, or on the Infoblox server.

To configure the feature, see [DHCP Based IP Address Assignment and Management for GlobalProtect](#) section in the GlobalProtect Admin Guide

GTP Support for Intelligent Security

Intelligent Security, also known as User Equipment to IP Address Mapping or [UEIP](#), helps to correlate mobile user equipment (UE) with IP addresses for security policy enforcement. By mapping the subscriber ID and equipment ID to the IP address associated with traffic from the user equipment (UE), Intelligent Security allows you to create security policy rules for mobile network traffic and helps to ensure consistent application of the security policy rules throughout all of the devices on your network. Configuring Intelligent Security for UEIP Correlation helps you to apply subscriber and equipment identity-based security policy in an enterprise 5G network and to provide advanced threat prevention service for your enterprise 5G customers.

To enable even more deployment options when using Intelligent Security for your mobile infrastructure security policy, Intelligent Security now supports the GPRS tunneling protocol ([GTP](#)) traffic in addition to Packet Forwarding Control Protocol ([PFCP](#)) and Remote Authentication Dial-In Service ([RADIUS](#)) traffic. When you select GTP as the source for UEIP Correlation with Intelligent Security, you can also optionally apply a number of additional security measures, such as protocol validity checks, as well as gain important context through additional visibility for important information contained in GTP session logs.

By providing a simple method to secure your mobile network traffic, whether it is for perimeter security, RAN security, core security, or roaming security, Intelligent Security helps you to establish a zero trust security policy for the traffic on your 5G and 4G/LTE mobile networks.

Increased Maximum Number of Security Rules for PA-3400 Series Firewalls

(PA-3410 and PA-3420 firewalls only) The maximum number of security rules supported has increased from 2,500 to 10,000.

IPSec Serviceability

Prisma Access uses IPSec to securely connect branch offices and data centers to the service. If there is an issue with bringing up the IPSec tunnel, it can be challenging to read logs related to IKE and IPSec events in an attempt to troubleshoot the issue.

A new UI provides clear diagnostic IPSec tunnel information, including the reason for the tunnel failure, the configured and exchanged IPSec and IKE parameters, and recommended settings for IKE and IPSec crypto values for service connections and remote network connections. With the UI, you have a full picture of your IPSec tunnels. You can also trigger an IKE renegotiation for a given service connections or remote network connections.

This tunnel information reflects real-time monitoring status, along with an explanation of why any tunnels have gone down.

Local Deep Learning for Advanced Threat Prevention

Advanced Threat Prevention now supports [Local Deep Learning](#), which provides a mechanism to perform fast, local deep learning-based analysis of zero-day and other evasive threats, as a complementary feature to the [cloud-based Inline Cloud Analysis component of Advanced Threat Prevention](#). With an Advanced Threat Prevention license, known malicious traffic that matches against Palo Alto Networks published signature set are dropped (or have another user-defined action applied to them); however, certain traffic that matches the criteria for suspicious content are rerouted for analysis using the Deep Learning Analysis detection module. If further analysis is necessary, the traffic is sent to the Advanced Threat Prevention cloud for additional analysis, as well as the requisite false-positive and false-negative checks. The Deep Learning detection module is based on the proven detection modules operating in the Advanced Threat Prevention cloud, and as such, have the same zero-day and advanced threat detection capabilities. However, they also have the added advantage of processing a much higher volume of traffic, without the lag associated with cloud queries. This enables you to inspect more traffic and receive verdicts in a shorter span of time. This is especially beneficial when faced with challenging network conditions.

Updates to Local Deep Learning models are delivered through content updates. [Local Deep Learning is enabled and configured using the Anti-Spyware profile](#) and requires an active Advanced Threat Prevention license.

Monitor Bandwidth on SD-WAN Devices

Currently it's difficult for the network administrators to quickly identify the cause for an application's poor performance in an SD-WAN device. It's because there isn't enough information available to identify the issue and the available limited information (such as VPN statistics, Panorama's device health statistics, and link health statistics) are located between Panorama and firewalls. It becomes a time consuming activity for the administrators to correlate this information and locate the performance issues on an SD-WAN device.

We've introduced **bandwidth** which is a primary measure of a [link performance](#) in addition to existing **jitter**, **latency**, and **packet loss** performance measures. For a VPN cluster, you will now be able to view the bandwidth of a tunnel and a physical interface for a selected site by default. There is no configuration required from the user to view the bandwidth of a tunnel.

NGFW Clustering of PA-7500 Series Firewalls

Data centers need very high levels of network bandwidth and reliability. NGFW clustering is a way to provide redundancy to two PA-7500 Series firewalls in an NGFW cluster in the event of a link failure, card failure, or chassis failure. NGFW clustering blends the legacy HA active/active and active/passive solutions into a single high availability solution. The two cluster nodes connect over a single HSCI connection. The firewalls maintain a dual active data plane with a single active control plane. Neighboring devices see the NGFW cluster as a single Layer 2 (virtual wire) or Layer 3 device.

The NGFW cluster solution reduces failover time, increases resiliency, and supports a multichassis link aggregation group (MC-LAG). The firewalls in the NGFW cluster increase port availability, require fewer IP addresses, and rely on open standards.

OOXML Support for WildFire Inline ML

Palo Alto Networks® WildFire® now supports a new office file type analysis classification engine for [WildFire Inline ML](#): OOXML (Open Office XML). This enables you to configure your NGFW to detect and prevent malicious Office Open XML files from entering your network in real-time by applying machine learning (ML) analytics. [WildFire Inline ML](#) dynamically detects malicious files of specific types by evaluating various file details to formulate a high probability classification of a file. This protection extends to currently unknown as well as future variants of threats which match characteristics that Palo Alto Networks identifies as malicious. To take advantage of WildFire inline ML, you must have an active WildFire subscription. If you do not have WildFire Inline ML enabled on your firewall, refer to [WildFire Inline ML](#) for more information.



To access the new OOXML (Open Office XML) file analysis classification engine for [WildFire Inline ML](#), be sure to download and install the latest content release package. Applications and Threat content release 8825 and later allows NGFWs operating on supported platforms to detect and prevent malicious OOXML files from entering your network in real-time using Inline ML. For more information about the update, refer to the Applications and Threat Content Release Notes.

To download the release notes, log in to the Palo Alto Networks Support Portal, click Dynamic Updates and select the release notes listed under Apps + Threats.

PA-410R Next-Generation Firewall

The [PA-410R](#) is a new rugged firewall appliance that upgrades the PA-220R firewall. The PA-410R is designed for industrial, commercial, and government deployments. This IP65 rated hardware is suited for installation in harsh environments with extreme temperatures and high humidity levels.

The PA-410R is supported on PAN-OS 11.1.3 and later versions. The firewall features two SFP ports and four RJ-45 ports. The RJ-45 ports include two fail-open ports that can be configured to provide a pass-through connection in the event of a power or operating system failure.

The PA-410R is powered by DC power and optionally supports power redundancy. The device has a fanless design and can be installed on a wall or DIN rail. The hardware is compliant with ICS/SCADA system architecture.

PA-450R-5G Next-Generation Firewall

The [PA-450R-5G](#) is a new ruggedized firewall appliance that is a cellular version of the PA-450R. The PA-450R-5G is designed for industrial, commercial, and government deployments where cellular activity is required. The hardware is suited for installation in harsh environments with extreme temperatures and high humidity levels.

The PA-450R-5G is supported on PAN-OS 11.1 and later versions. The firewall features four 5G multi-band antennas and two nano SIM card slots to enable connectivity using two different mobile network providers. The front panel of the device also features two SFP/RJ-45 combo ports and six RJ-45 ports.

The PA-450R-5G is powered by DC power and supports power redundancy. The device has a fanless design and can be installed on a flat surface, wall, and equipment rack. The hardware is compliant with ICS/SCADA system architecture.

PAN-OS 11.0, 11.1, and 11.2 Dataplane Support

Prisma Access 5.1 Innovation supports the PAN-OS features that are available with PAN-OS 11.0, 11.1, and 11.2.

PAN-OS 11.2 Support for Panoramas That Manage Prisma Access

If you have a Panorama Managed Prisma Access deployment, you can use a Panorama running 11.2 to manage Prisma Access.

Post Quantum Hybrid Key Exchange VPN

Post Quantum Hybrid Key Exchange VPN extends your PAN-OS post-quantum VPN security by adding the ability to create post-quantum cryptographic (PQC) hybrid keys using the NIST round 3 and round 4 cryptographic suites. You can future proof your VPN encryption keys and safeguard against harvest now, decrypt later (HNDL) attacks by combining multiple key exchange mechanisms (KEM) with full crypto agility.

The hybrid key technology is based on RFC 9242 and RFC 9370, and allows you to add up to seven additional key exchange mechanisms (KEM). With each additional KEM added, the level of quantum resistance increases as the attacker needs all used KEMs to become vulnerable before the key can be broken. You can apply the hybrid key technology to both IKEv2's key exchange and IPsec's rekey key exchange to ensure all VPN key exchanges are quantum resistant.

To provide in-depth quantum defense, you can also enable both of its post quantum VPN technologies together. If both the RFC 8784 post quantum pre-shared key (released with PAN-OS 11.1) and this new PQ Hybrid Key feature are enabled, PAN-OS generates the hybrid key and then mixes in the static pre-shared key.

Prisma Access Internal Gateway

Prisma Access introduces a [native internal gateway](#) solution within the Prisma Access architecture, reducing the need to implement GlobalProtect in conjunction with an on-premises internal gateway to learn User-ID for users on an internal network. Prisma Access deployments can enable a native internal gateway natively within the Prisma Access architecture.

Use the native internal gateway to enforce user-based security policies for remote network traffic without the need to deploy an on-premises internal gateway.

Remote Network Tunnel Automation API

The Remote Network Tunnel Automation API enables you to integrate third-party SD-WAN products with Prisma Access to offer Cloud security services over your SD-WAN solution. This API is supported for Prisma Access deployments that are managed by both Panorama and Strata Cloud Manager and facilitates the onboarding of third-party SD-WAN branches to Prisma Access Remote Networks.

Strata Cloud Manager Connectivity Using Port 443

Palo Alto Networks NGFW (Managed by Strata Cloud Manager) use the [dedicated non-standard port 3978](#) to communicate with Strata Cloud Manager by default. In PAN-OS 11.2, you can instead configure NGFW (Managed by Strata Cloud Manager) [onboarding](#) to Strata Cloud Manager to use destination port 443 instead of port 3978. Ports 3978 and 443 offer the same functionality for NGFW (Managed by Strata Cloud Manager) and Strata Cloud Manager communication. However, port 443 offers some distinct advantages when managing your network configurations, reducing your network attack surface, and implementing Security policy rules and audits:

- **Ease of Configuration and Use**—Port 443 is the standard port used for HTTP traffic encrypted with SSL. Using port 443 for NGFW (Managed by Strata Cloud Manager) and Strata Cloud Manager communication greatly simplifies network configuration management for both administrators and end users.

Additionally, many corporate networks restrict incoming and outgoing traffic to a limited set of ports to minimize the network attack surface area. Port 443 is already commonly allowed on most enterprise networks without the need for additional network configurations. Using port 443 for NGFW (Managed by Strata Cloud Manager) and Strata Cloud Manager communication also improves your security posture by reducing the number of ports allowed on your network.

- **Improved Compatibility**—Port 443 is universally accepted and is the expected port for secure communications. Security tools that use port 443 are normally compatible with existing security configurations. This greatly reduces the need for custom firewall configurations and rules.

TLV1.3 Support for HSM Integration with SSL Inbound Inspection

PAN-OS now supports the [decryption of TLSv1.3 sessions](#) in SSL Inbound Inspection mode when the private keys of internal servers are stored on [Hardware Security Modules \(HSMs\)](#). The superior performance and security of TLSv1.3 combined with the protection of HSMs hardens inbound decryption. This feature is only compatible with the Thales Luna Network and Entrust nShield Connect HSMs. To activate this support, use the **set ssl inbound-inspection tls1.3-with-hsm enable yes** CLI command. This feature is disabled by default. You must [set up connectivity](#) between a supported HSM and Palo Alto Networks appliances *and* [apply a Decryption profile](#) that specifies TLSv1.3 as the minimum or maximum supported TLS version to an SSL Inbound Inspection rule first.

User-ID for CN-Series

CN-Series now qualified with support for User Identity (User-ID) in the Kubernetes as CNF mode. User-ID helps to leverage user information and provides improved visibility into application usage. User-ID also helps with policy control and reduced attack surface by providing need based user access and gives a complete picture of a security incident through logging, reporting, and forensics. For more information, see [User-ID](#).

User-ID Across NAT

Mobile users access private apps using a service connection. If your deployment uses a Next-Generation Firewall (NGFW) in the data center or headquarters location where the private apps are located, and if your service connection has source NAT enabled, the NGFW can't retrieve the User-ID and Device-ID mapping. Source NAT on the service connection prevents the mobile users' User-ID and Device-ID mapping to be distributed to the NGFW. If the NGFW can't retrieve this mapping, it can't enforce zone-based security policy rules you have created on it based on User-ID or Device-ID mapping.

User-ID Across NAT lets your network distribute the User- or Device-ID mapping from mobile users to the NGFW and then on to the headquarters or data center, thus allowing the NGFW to enforce security policy rules based on the User-ID mapping it has learned from the service connection. This configuration ensures a consistent security posture across your mobile user deployment.

View and Monitor Third-Party Device-ID

You can use the Cloud Identity Engine with Prisma Access to apply information from third-party IoT detection sources to simplify the task of identifying and closing security gaps for devices in your network. See [Configure Third-Party Device-ID in Prisma Access](#) for details about setup and configuration.

Go to **Monitor > Devices > IOT to get insights on your IoT devices**, such as the number of IoT devices connected within the last 30 minutes, all IoT devices connected during the time range selected, and details about all connected IoT devices.

Virtual Systems Support on VM-Series Firewall

The VM-Series firewall now supports virtual systems only with [flexible license](#) and with **one** virtual system by default. Virtual systems are separate, logical firewall instances within a single physical Palo Alto Networks firewall. Rather than using multiple firewalls, managed service providers and enterprises can use a single pair of firewalls (for high availability) and enable virtual systems on them. The virtual systems are easier to manage coexisting within a firewall. The additional benefits of virtual systems include improved scalability, segmented administration, and reduced capital and operational expenses. For more information, see [Benefits of Virtual Systems](#) and [Virtual System Components and Segmentation](#).

The virtual system support on the VM-Series firewall is available on PAN-OS version 11.1.3 and later. You must have a virtual system license to support multiple virtual systems on the VM-Series firewall. Purchase additional licenses based on your requirement up to a maximum number supported on a particular Tier.

Use a flexible VM-Series firewall license and Tier 3 or Tier 4 instances supporting a minimum of 16 vCPUs or more. The VM-Series firewall in Tier 3 instance supports a maximum of 25 virtual systems. The VM-Series firewall in Tier 4 instance, supports a maximum of 100 virtual systems.



The virtual system support on VM-Series firewall is introduced in PAN-OS 11.2.0, and available in PAN-OS version 11.1.3 and later on KVM platform only.

Intelligent Traffic Offload - Layer 3 (Dynamic Routing) Support on VM-Series Firewall

Intelligent Traffic Offload (ITO) is a VM-Series firewall Security subscription that, when configured with the supported [NVIDIA Bluefield](#) infrastructure compute platform, increases capacity throughput for the VM-Series firewall. In previous releases, ITO required that you deploy your VM-Series firewall in [virtual wire mode](#). This limitation prevented deployments in Layer 3 mode supporting dynamic routing.

This release removes that limitation by allowing you to deploy your VM-Series firewall with Intelligent Traffic Offload for L3 traffic supporting dynamic routing. With dynamic routing, you attain stable, high-performing, and highly available L3 routing through profile-based filtering lists and conditional route maps which can be used across logical routers. These profiles provide finer granularity to filter routes for each dynamic routing protocol and improve redistribution across multiple protocols. When combined with NAT for IPv4, you can extend security policy to protect end user devices from being exposed to outside threats.

Intelligent Traffic Offload - NAT Support on VM-Series Firewall

Intelligent Traffic Offload (ITO) is a VM-Series firewall Security subscription that, when configured with the supported [NVIDIA Bluefield](#) infrastructure compute platform, increases capacity throughput for the VM-Series firewall. In previous releases, Intelligent Traffic Offload required that you deploy your VM-Series firewall in [virtual wire mode](#). This limitation prevented deployments of VM-Series firewalls with an ITO subscription from using NAT for perimeter security.

This release removes that limitation by allowing you to deploy your VM-Series firewall with an Intelligent Traffic Offload subscription in Layer 3 mode that supports NAT for IPv4. With this functionality, your ITO subscription fully supports environments requiring robust security features that prevent end-user devices from being exposed to outside threats. NAT support extends to NAT44 and DIPP in for both deployments with Intelligent Traffic Offload (DPU-based) and software cut-through for traffic inspection.

Zero Touch Provisioning (ZTP) Onboarding Enhancements

[Zero Touch Provisioning \(ZTP\)](#) allows simplify onboarding Next-Generation firewalls to your Panorama™ management server by allowing you to minimize the manual admin intervention required to onboard the firewall and connect it to your network. PAN-OS 11.2.0 introduces additional enhancements to the ZTP onboarding experience by allowing you to activate applicable licenses and install the latest content updates when the firewall first connects to Panorama.

When you [add ZTP firewalls to Panorama](#), you can now specify the firewall authorization code required to activate the firewall license. This allows you to activate the licenses on the ZTP firewall when it connects to Panorama for the first time. Additionally, you can configure Panorama to automatically push the latest downloaded content version when the ZTP firewalls successfully connects and is onboarded to Panorama in the template stack generated through the ZTP plugin. After a successful connection to Panorama, it activates the applicable licenses associated with the auth code you added for the ZTP firewall pushes the latest predefined device group and template stack configuration, installed the latest downloaded dynamic content version.

View Preferred and Base Releases of PAN-OS Software

The Panorama web interface now displays the preferred releases and the corresponding base releases of PAN-OS software. Before you upgrade or downgrade Panorama or PAN-OS, you can view the list of preferred and base releases and choose your preferred target PAN-OS release. Preferred releases offer the latest and the most advanced features and ensure stability and performance. When there are no preferred releases available, the corresponding base version is not displayed. If necessary, you can choose to view either preferred releases or base releases.

April 2024

Review all the new features we've introduced across the NetSec platform in April 2024.

Additional Private Link Types

You can now configure [additional point-to-point private link types](#), **Private Link1**, **Private Link2**, **Private Link3**, and **Private Link4** along with the existing private link types (**MPLS**, **Satellite**, **Microwave/Radio**) for one to one connectivity while configuring the SD-WAN Interface Profile.

These private link types enable you to avail reliable providers for your remote regions to establish one to one connection with the overlay network and avoid provider outages.

Additional SD-WAN Hubs in VPN Cluster

The number of hubs to [configure in a VPN cluster](#) has been increased from 4 to 16. Only four of the 16 hubs can have the same hub priority within a VPN cluster due to ECMP.

Aggregate Ethernet Interface Usability Enhancement

Configuring an Aggregate Ethernet interface variable in snippets or folders allows you to have reusable common configuration across the entire deployment. [Aggregate Ethernet interface variable](#) reduces duplication of configuration and significantly simplifies the process of updating and maintaining common configurations.

When you add interfaces for your firewalls, you can now configure the **Aggregate Ethernet** interface variable type in addition to the existing Layer 2, Layer 3, and tap interface types.

Configuration Indicator

Get clarity on the configuration elements that are applicable for a particular scope and whether they are inherited from a common configuration scope or generated by the system.

The color-coded [configuration indicators](#) help you understand where the configurations are inherited from, and also visually distinguish the object types for easy scanning.

Device Onboarding Rules

Use a [device onboarding rule](#) to automate parts of the Palo Alto Networks NGFW onboarding to Strata Cloud Manager whether you are manually onboarding Palo Alto Networks NGFW or onboarding using Zero Touch Provisioning (ZTP). This allows you to associate the firewall with a folder and apply predefined configuration when the firewall first connects to Strata Cloud Manager. You can create multiple device onboarding rules to define different match criteria that apply to different Palo Alto Networks NGFW. Device onboarding rules are designed to simplify and greatly reduce the time spent onboarding new Palo Alto Networks NGFW at scale and ensure the correct configuration is applied to newly onboarded Palo Alto Networks NGFW.

Device onboarding rules use **Match Criteria** to define which Palo Alto Networks NGFW the rule applies to. This includes information such as the firewall **Model** and any **Labels** applied to the firewall during the onboarding process. You can define the rule **Action** to specify a **Target Folder** one or more Palo Alto Networks NGFW are added to and the **Snippet Association** define any firewall-specific snippet configurations that need to be applied. Additionally, if you use SD-WAN or Cloud Identity Engine (CIE) you can also define and apply those necessary configurations in the device onboarding rule to ensure all required connectivity and user-based visibility and policy enforcement immediately after onboarding.

External Gateway Integration for Prisma Access and On-Premises NGFWs

Enable integration between Prisma Access deployments and on-premises NGFWs deployed as external gateways.

In the Prisma Access configuration, when setting up the hybrid Prisma Access deployment with security service edge (SSE) and on-premises NGFWs, you can now configure the NGFWs as [external gateways](#) by referencing the NGFWs' GlobalProtect gateway IP addresses. This eliminates manual configuration and minimizes the risk of misconfiguration.

Enterprise DLP Migrator

Use the Enterprise Data Loss Prevention (E-DLP) [Migrator](#) to migrate your Symantec DLP policy rules and convert them into SaaS Security policy rules. This allows you to quickly transition to Palo Alto Networks Enterprise DLP without the need to manually recreate all your Security policy rules designed to prevent exfiltration of sensitive data. To migrate your existing Symantec DLP policy rules, you simply need to export them from Symantec DLP in .xml format and import them into the Enterprise DLP migration tool. The imported DLP policy rules are then evaluated to verify that they are compatible with Enterprise DLP and SaaS Security. When a Symantec DLP policy rule is successfully migrated to Enterprise DLP, a data pattern and a classic data profile with names identical to the migrated policy rule are automatically created as part of the migration to capture the traffic match criteria.

If Enterprise DLP detects an incompatible DLP policy rule traffic match criteria, you can choose to delete the incompatible match criteria from the Symantec DLP policy rule before the migration begins or choose to exclude that specific Symantec DLP policy from migration. A successfully migrated Symantec DLP policy rule is added as a **Disabled** SaaS Security Data Asset policy rule (**Manage > Configuration > SaaS Security > Data Security > Policies > Data Asset Policies**). You can then review the Data Asset policy rule, make changes if needed, and enable the policy rule.

Software Cut-through based Offload on CN-Series Firewall

You can now configure software cut-through based offload on the CN-Series firewall. With the software cut-through based Intelligent Traffic Offload (ITO) service, the CN-Series firewall eliminates the tradeoff between network performance, security, and cost. For each new flow on the network, the ITO service determines whether or not the flow can benefit from security inspection. The ITO service routes the first few packets of the flow to the firewall for inspection, which determines whether to inspect or offload the rest of the packets in the flow.

The software cut-through based offload supports the GTP-U tunnel protocol. Within a GTP-U session, after the GTPU inner session software coordinated Universal Time-through, after the GTPU inner session completes the Layer 7 inspection, the GTPU packet will follow the existing software cut-through datapath, bypass the unnecessary operations, take advantage of a FIB/MAC cache, and run to completion. In CN-Series, only the **CN-Series as a Kubernetes CNF** mode of deployment supports software cut-through based ITO.

Software Cut Through Support for PA-400 and PA-1400 Series Firewalls

The PA-400 and PA-1400 Series firewalls have significantly improved latency.

Strata Cloud Manager: Activity Insights

[Activity Insights](#) gives you an in-depth view of your network activities across Prisma Access and NGFW deployments. Activity Insights brings together visualization, monitoring, and reporting capabilities from these [dashboards](#) and provides all this data to you in a single, consolidated view.

- [Dashboards > Application Usage](#)
- [Dashboards > Network Usage](#)
- [Dashboards > User Activity](#)
- [Dashboards > Threat Insights](#)
- [Monitor > Users](#)
- [Monitor > Applications](#)

Activity Insights pairs with the new [Strata Cloud Manager Command Center](#) home page; for anomalies, security gaps, degraded user experiences, impacts on security and health of your network that the home page surfaces, you can drill down into Activity Insights and other [dashboards](#) to investigate and assess next steps.

Activity Insights

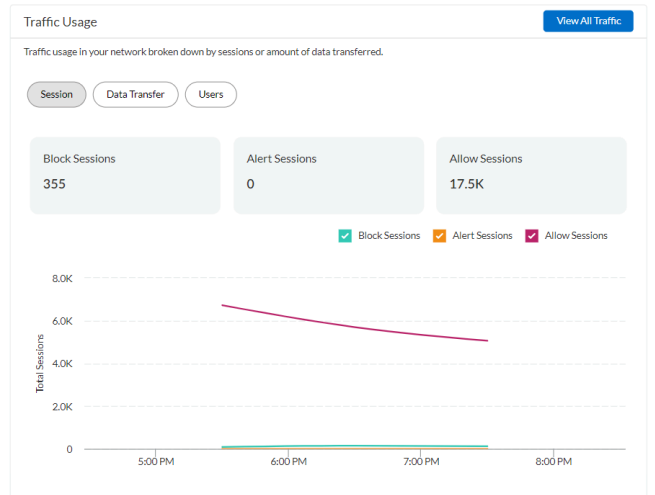
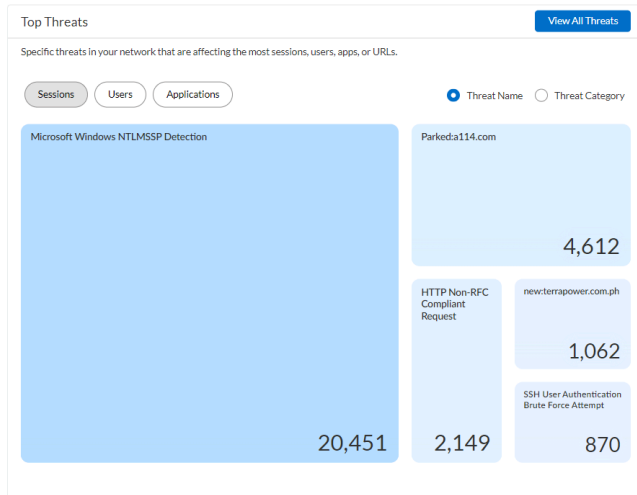
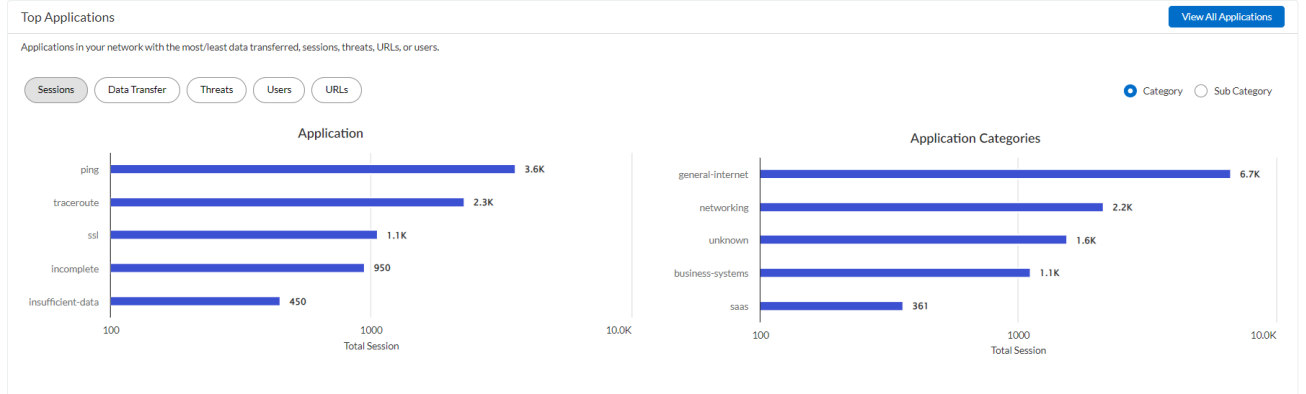
Monitor traffic usage, and view the top applications, threats, users, URLs, and rules in your network.

Search

Overview Applications SDWAN Applications Threats Users URLs Rules Regions

Time Range: Last 3 Hours X Scope Selection: All X Subtenant: cellularitaliaspa X Add Filter

Reset



Top URLs

URLs in your network with the most data transferred, threats, sessions, apps, and users.

Sessions Users Applications

#	URL	Sessions	Users	Apps
1	ocsp.paloaltonetworks.com:8080/ocsp	242	130	2
2	ch-panwhq.traps.paloaltonetworks.com/	230	92	1
3	dc-panwhq.traps.paloaltonetworks.com/	225	96	1
4	crf.paloaltonetworks.com/crf/Palo%20Alto%20Networks%20Inc%20Domain...	223	103	1

Top Rules

Rules in your network with the most data transferred, threats, sessions, apps, and users.

Sessions Data Transfer Threats Users Applications

#	Rule Name	Sessions	Data Transfer	Threats	Users	Apps	URLs
1	deny-internal-to-internet...	656	357.2 KB	0	0	0	19
2	corp-to-any-reachability	6139	964.7 KB	0	0	0	0
3	dns-outbound	604	172.9 KB	323	0	1	0
4	Lab Outbound Internet	406	1.1 MB	32	0	2	90

Activity Insights has these different tabs.

- Overview
- Applications
- SD-WAN Applications
- Threats
- Users
- URLs
- Rules

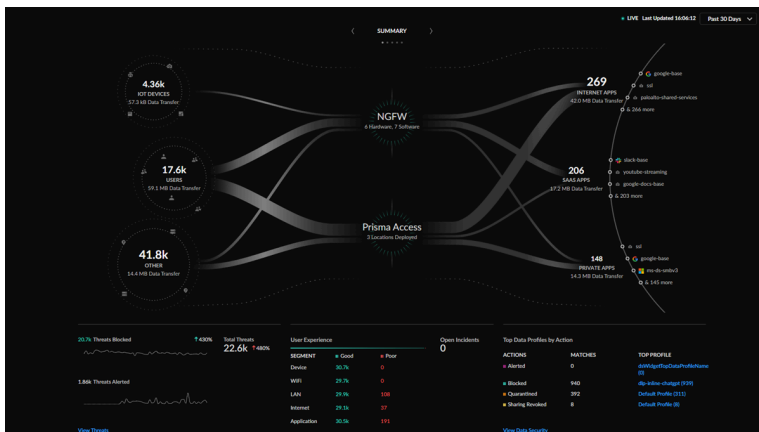
- Regions

Each of these tabs provides an unified view of network data in relation to applications, users, threats, URLs, and network usage. You can also view the performance of Prisma SD-WAN applications with details on health score over a time range, transaction statistics, and bandwidth utilization metrics. The dashboard has advanced filters on these tabs to help you focus on the security aspects that matter to your deployment.

The advanced reporting functionality enables you to [download, share, and schedule reports](#) that cover the data in the Overview tab. The report presents data separately for each filter applied in Activity Insights.

Strata Cloud Manager: Command Center

The [Strata Cloud Manager Command Center](#) is your new NetSec homepage; it is your first stop to assess the health, security, and efficiency of your network. In a single view, the command center shows you all users and IoT devices accessing the internet, SaaS applications, and private apps, and how Prisma Access, your NGFWs, and your security services are protecting them.



The command center provides you with four different views, each with its own tracked data, metrics, and actionable insights to examine and interact with:

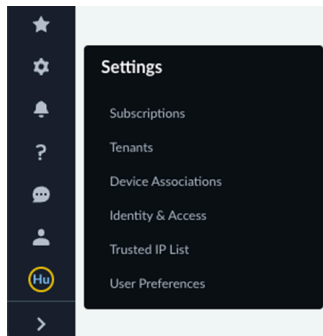
- **Summary:** A high-level look at all your network and security infrastructure. Monitor the traffic between your sources (users, IoT) and applications (private, SaaS), and see metrics onboarded security subscriptions.
- **Threats:** Dig deeper into anomalies on your network and block threats that are impacting your users. Review the traffic inspected on your network and see how threats are being detected and blocked around the clock by your Cloud-Delivered Security subscriptions.
- **Operational Health:** Review incidents of degraded user experience on your network and see root-cause analysis of the issues and remediation recommendations.
- **Data Security:** Find high-risk sensitive data and update data profiles to further secure your network. Review the sensitive data flow across your network and SaaS applications.

When the command center surfaces an issue through one of these views that you should address or investigate (an anomaly, a security gap, a degraded user experience, something that impacts the security and health of your network), it provides a path to where you can take actions to further secure your network.

For example, if you are looking at the Threats view and would like more information about Command and Control threats on your network, you can click C2 in the Blocked and Alerted Threats table and jump to [Activity Insights](#), where you can drill down and investigate details about all the Command and Control threats, such as the threat name, severity, and change the action from Alert to Drop.

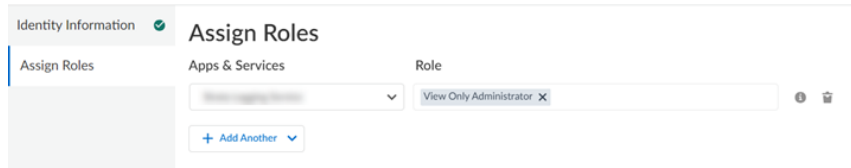
Trusted IP List

You can use the [Trusted IP List](#) to restrict access to Strata Cloud Manager by specifying IP addresses that are allowed on a per tenant basis. This feature is available in **Strata Cloud Manager** > **Settings** > **Trusted IP List**.



View Only Administrator Role Enhancement

In [Identity and Access Management](#), the **View Only Administrator** role is extended to include support for the Strata Logging Service application.



Web Proxy for Cloud-Managed Firewalls



Prisma Access has its own, separate [method of configuring explicit proxy](#). This new feature applies only to cloud-managed firewalls.

You can now [configure a web proxy on the firewalls you're managing with Strata Cloud Manager](#). That means that if you plan to use an NGFW as a proxy device to secure your network, you can now configure your proxy settings across your deployment from a simple, unified management interface.

This interface includes an in-app proxy auto-configuration (PAC) file editor so that you can edit your proxy settings and modify your PAC file all in one place whenever network changes arise.

The web proxy supports two methods for routing traffic:

- For the [explicit proxy](#) method, the request contains the destination IP address of the configured proxy and the client browser sends requests to the proxy directly. You can use one of following methods to authenticate users with the explicit proxy:
 - Kerberos, which requires a web proxy license.
 - SAML 2.0, which requires a Prisma Access license and the add-on web proxy license.
- For the [transparent proxy](#) method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules, which you can configure using Transparent Proxy Rules in Strata Cloud Manager. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).

You can push web proxy configurations to the following platforms:

- PA-1400
- PA-3400
- VM Series (with a minimum of four vCPUs)

March 2024

Review all the new features we've introduced across the NetSec platform in March 2024.

Multitenant Notifications

In a multitenant hierarchy, the notifications provide you with a consolidated view of the Strata Cloud Manager announcements and Prisma Access dataplane upgrade info that you would otherwise see in various places throughout the single tenant environment. The aggregated notifications prompt you to take necessary actions or help you to make informed decisions about all the tenants in your hierarchy.

If you're a managed security service provider (MSSP) or distributed enterprise with a multitenant hierarchy, you can [manage notification profiles](#) for all the tenants in your hierarchy. You can also configure to receive notifications via email or webhook.

February 2024

Review all the new features we've introduced across the NetSec platform in February 2024.

Authenticate LSVPN Satellite with Serial Number and IP Address Method

Beginning with PAN-OS 10.1 and later releases, we support Username/password and Satellite Cookie Authentication method for a satellite to authenticate to the portal. This method requires user intervention to get satellites authenticated by a portal that prevents automating the deployment of remote satellites and adds difficulty and complexity for the administrators to perform software upgrade and deploy new firewalls.

To remove the user intervention while onboarding a remote satellite and to enable automating the deployment of remote satellites, we introduce a new authentication method called "[Serial number and IP address Authentication](#)". You can now onboard a remote satellite using the combination of serial number and IP address in addition to the username/password and satellite cookie authentication method. This authentication method reduces the complexity by enabling you to deploy new firewalls without manual intervention.

However, Username/password and Satellite Cookie Authentication remains as a default authentication method.

Before enabling the Serial number and IP address Authentication method, configure the satellite serial number at the portal as one of the authentication verification conditions.

- Configure the satellite IP address as an "IP allow list" at the portal using the **set global-protect global-protect-portal portal <portal_name> satellite-serialnumberip-auth satellite-ip-allowlist entry <value>** command to add a satellite device IP address on the GlobalProtect portal.
- Enable the Serial number and IP address Authentication method using the **set global-protect-portal satellite-serialnumberip-auth enable** CLI command. After you enable this method, the satellite continuously attempts to authenticate with the portal for the configured retry interval (in seconds) after power-on until the portal explicitly instructs the satellite to stop.

Upon successfully configuring a satellite device allowed IP address list per portal, and configuring the satellite serial number on the GlobalProtect portal, the satellite can initiate the connection to the portal.

Private Key Export in Certificate Management

You can centrally manage the certificates you use to secure communication across your network.

You can now [export the private key](#) from Strata Cloud Manager for a self-signed certificate.

However, the export of private keys for an externally signed certificate is restricted. The supported export formats are as follows:

- **Base64 Encoded Certificate (PEM)**—This is the default format. It's the most common and has the broadest support on the internet. **Export Private Key** if you want the exported file to include the private key.
- **Encrypted Private Key and Certificate (PKCS12)**—This format is more secure than PEM but isn't as common or as broadly supported. The exported file will automatically include the private key.
- **Binary Encoded Certificate (DER)**—More operating system types support this format than the others. You can't export the private key in this format.

Clone a Snippet

Snippets are configuration objects, or groups of configuration objects, that can be associated with your folders, firewalls, and Prisma Access deployments onboarded to Strata Cloud Manager. They are used to standardize configurations, allowing you to push changes quickly to multiple areas simultaneously. Snippets can be used to manage common configurations centrally for consistent security enforcement across NGFW and Prisma Access deployments. Snippets are classified in two ways: Predefined and Custom. Predefined snippets are available to all Strata Cloud Manager users and can be used to quickly get your new firewalls and deployments up and running with best practice configurations. Custom snippets are any snippets created by administrators.

Preexisting snippets can now be cloned.

If you want to use an existing snippet as a template for a new snippet, you can easily clone it so you do not have to configure a completely new object.

Cloned snippets are not associated with any devices, folders, or deployments, allowing you to customize them freely without having to disassociate them before you begin.

Security Checks

Strata Cloud Manager leverages a set of predefined [Best Practice Checks](#) that align with industry-specific standard cybersecurity controls. These include CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology) and custom checks you create based on the specific needs of your organization. These checks evaluate configurations, identifying deviations from best practices or compliance requirements.

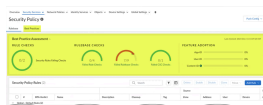
For this release, building on the features we gave you in [November](#), we have:

- Added Strata Cloud Manager Support for real-time inline check exemptions.

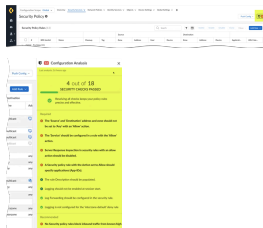
Check exemptions let you exclude checks from being applied to your deployment. There may be special cases where you want to turn off certain checks for some areas of your deployment, or when there are reasons specific checks don't make sense for you. Instead of disabling those checks, you can now restrict where checks are applied in your deployment.

- Consolidated, field-level, inline check information has been moved to an easily accessible pane on the right side of the screen.

Previously, check information was available in a banner where the checks applied and in the Best Practices tab.



Now, when checks are available for a feature, just click the (🔍) icon to see check details.




GlobalProtect Portal and Gateway

You can now use [GlobalProtect with cloud-managed NGFWs](#) to secure your mobile workforce. Enable your cloud-managed NGFWs as GlobalProtect gateways and portals, in order to provide flexible, secure remote access to users everywhere.

Whether checking email from home or updating corporate documents from an airport, the majority of today's employees work outside the physical corporate boundaries. This workforce mobility increases productivity and flexibility while simultaneously introducing significant security risks. Every time users leave the building with their laptops or smart phones, they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network. [GlobalProtect™](#) solves the security challenges introduced by roaming users by extending the network security policy that you're enforcing within the physical perimeter to all users, no matter where they are located.

IP Optimization for Mobile Users - GlobalProtect Deployments

IP Optimization is a set of architectural enhancements that reduce the overall number of IP addresses in your deployment, simplifying your allow-listing workflows while improving resiliency and enabling faster onboarding of Prisma Access tenants.

- **Simpler Public IP Address allow-listing**—Adding a Prisma Access location or experiencing a [scaling event](#) at an existing Prisma Access location could lead to new IP addresses being allocated to the mobile user security processing node (MU-SPN). It's a best practice to [retrieve the new egress and gateway IP addresses](#) that Prisma Access assigns and [add them to an allow list](#) in your network to avoid SaaS application or corporate firewall disruption. This can result in a situation where you're managing a large number of IP addresses. IP Optimization reduces the number of IP addresses you have to manage.
 - **Faster Onboarding of Prisma Access Tenants**—Without IP Optimization, you'd need to assign unique private IP addresses to each device across Prisma Access and your private networks, requiring you to allocate large IP blocks from your limited corporate routable IP address space. IP Optimization lets Prisma Access allocate addresses from shared address space by default and [NAT private application traffic](#).
-  • *IP optimization currently supports only IPv4 traffic.*
- *The [API to retrieve Prisma Access IP addresses](#) continues to work as it always has, even with IP Optimization enabled.*

License Enforcement for Mobile Users (Enhancements)

Prisma Access uses few [enforcement policies for mobile user licenses](#). Though there is no strict policing of the mobile user count, the service does track the number of unique users over the last 30 days now, which was 90 days previously, to ensure that you have purchased the proper license tier for your user base, and stricter policing of user count may be enforced if continued overages occur. This change is applicable for all types of mobile user licenses.

Multiple Virtual Routers Support on SD-WAN Hubs

With earlier SD-WAN plugin versions, you can't have SD-WAN configurations on multiple virtual routers. By default, a sdwan-default virtual router is created and it enables Panorama to automatically push the router configurations. Due to this restriction, customers faces difficulty and spends additional effort in some of the SD-WAN deployments:

User Scenario (in SD-WAN Deployments)	Single Virtual Router Configuration on SD-WAN Hub	Multiple Virtual Routers Configuration on SD-WAN Hub
Overlapping IP addresses from different branches connecting to the same hub	Customers may need to reconfigure the overlapping subnets to unique address spaces.	<p>Enable Multi-VR Support on the SD-WAN hub device.</p> <p>The traffic from different branches is directed to different virtual routers on a single hub to keep the traffic separate.</p>
Government regulations that disallow different entities to function on the same virtual router	Customers won't be able to separate routing of different entities with a single virtual router.	<p>Enable Multi-VR Support on the SD-WAN hub device to keep the traffic of different entities separate.</p> <p>Multiple virtual routers on the SD-WAN hub maps the branches to different virtual routers on the hub that provides logical separation between the branches.</p>

SD-WAN plugin now supports [multiple virtual routers on the SD-WAN hubs](#) that enable you to have overlapping IP subnet addresses on branch devices connecting to the same SD-WAN hub. Multiple virtual routers can run multiple instances of routing protocols with a neighboring router with overlapping address spaces configured on different virtual router instances. Multiple virtual router deployments provide the flexibility to maintain multiple virtual routers, which are segregated for each virtual router instance.

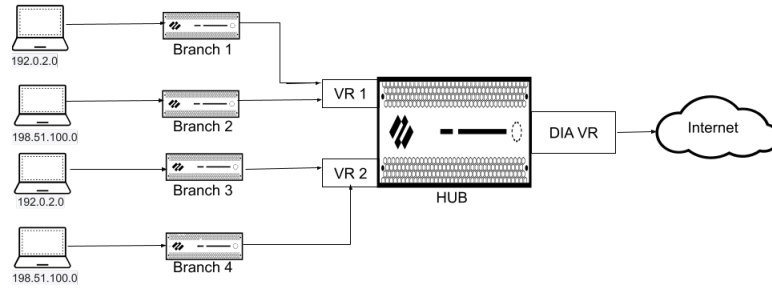
However, the number of virtual routers supported on the PAN-OS SD-WAN hub varies by platform.

Benefits:

- A hub with multiple virtual router configuration logically separates the routing for each branch office that it is connected with.
- Branches sharing the same SD-WAN hub can reuse the same IP subnet address.

The following figure illustrates an SD-WAN hub with two virtual routers. By enabling **multiple virtual routers support** on the SD-WAN hub, the four branches connecting to the same SD-WAN

hub (but different virtual routers) can have overlapping IP subnets or belong to different entities and function independently because their traffic goes to different virtual routers.



Native SASE Integration with Prisma SD-WAN

Effortlessly integrate Prisma SD-WAN with Prisma Access through a [native onboarding process](#). With previous Prisma Access versions, you needed to configure the additional component – Prisma Access for Networks (Cloud Managed) CloudBlade to onboard Prisma SD-WAN sites to Prisma Access. With the native SASE integration between Prisma SD-WAN and Prisma Access, we have further simplified the onboarding without the need to set up the CloudBlade.

Prisma Access currently supports this integration only for new Prisma SASE (Strata Cloud Manager) deployments. For Panorama Managed Prisma Access deployments, continue using CloudBlades for integration with Prisma SD-WAN.

New Prisma Access Cloud Management Location

Prisma Access Cloud Management can now be deployed in the India [region](#).

Normalized Username Formats

To better standardize usernames across your organization, all usernames in Prisma Access have been normalized.

The usernames are standardized based on the following examples.

Original Username	Normalized Username
test.User@abc.com	test.user
abc/Test.User	test.user
abc//Test.useR	test.user

This functionality does not affect security policies based on user groups and members configured using the Cloud Identity Engine.

PAN-OS Software Patch Deployment

Upgrading your Palo Alto Networks Next-Generation Firewall (NGFW), WF-500 appliance, or Panorama™ management server to a new PAN-OS release introduces new features developed to strengthen your security posture and fix known issues. This requires you to schedule downtime, and potentially introduces changes to default behaviors and additional issues that your security administrator has not yet reviewed or may not want to introduce into your production environment.

In some cases, an identified bug or Common Vulnerability and Exposure (CVE) need to be addressed immediately. PAN-OS software patch deployment allows you to download and install PAN-OS software patches to apply fixes without requiring you to schedule a prolonged maintenance you to install new PAN-OS versions. They are designed to address bugs and CVE only; no new features, functionality, or web interface changes are introduced in a PAN-OS software patch. This allows you to strengthen your security posture immediately without introducing any new known issues or changes to default behaviors that may come with installing a new PAN-OS release. A PAN-OS software patch is deployed directly from the [Palo Alto Networks Next-Generation NGFW](#) or [Panorama](#) web interface. For [Panorama managed firewalls and WF-500 appliances](#), you can install a PAN-OS software on your managed devices from the Panorama web interface.

PAN-OS software patches are cumulative. This means that more recent versions of a software patch for any given PAN-OS version include all the fixes included in the previous software patches. For example, Palo Alto Networks released the following software patches for PAN-OS 10.2.8; 10.2.8-p1.sb1, 10.2.8-p1.sb2, and 10.2.8-p1.sb3. In this case, 10.2.8-p1.sb3 includes every bug and CVE fixes introduced in 10.2.8-p1.sb1 and 10.2.8-p1.sb2.

PAN-OS software patch deployment is supported on Palo Alto Networks NGFW, WF-500 appliances, and Panorama running PAN-OS 10.2.8 or later 10.2 release. PAN-OS software patches require an outbound internet connection to download from the Palo Alto Networks Update Server. For air-gapped managed devices, Panorama must still have an outbound internet connection to download PAN-OS software patches, but an outbound internet connection isn't required to install and apply them to your managed devices.

Policy Analyzer

Updates to your Security policy rules are often time-sensitive and require you to act quickly. However, you want to ensure that any update you make to your Security policy rulebase meets your requirements and does not introduce errors or misconfigurations (such as changes that result in duplicate or conflicting rules).

Policy Analyzer in Strata Cloud Manager enables you to optimize time and resources when implementing a change request. Policy Analyzer not only analyzes and provides suggestions for possible consolidation or removal of specific rules to meet your intent but also checks for anomalies, such as Shadows, Redundancies, Generalizations, Correlations, and Consolidations in your rulebase.

See [Policy Analyzer](#) to learn more.

Saudi Arabia Compute Location

There is a new compute location, Saudi Arabia. As a result, the Saudi Arabia location has been remapped to the new Saudi Arabia compute location.

New deployments have the new remapping applied automatically. If you have an existing Prisma Access deployment that uses one of these locations and you want to take advantage of the remapped compute location, follow the procedure to [add a new compute location to a deployed Prisma Access location](#).

Site Template Configuration

The Prisma SD-WAN configuration tool offers customers a powerful solution for streamlining site deployments at scale. With our innovative [Site templates](#), now, you can effortlessly create templates, deploy sites, and provision them at scale through the Prisma SD-WAN user interface, simplifying and optimizing your network management process.

A site template is a predefined blueprint containing a list of variables that encompasses all the necessary configurations for creating fully operational sites and devices. Using this template, you can deploy multiple sites. You can use an existing template, edit an existing one or create a new template to deploy sites.

You can pre-provision sites before an ION device is available to accelerate the deployment. The device shell allows you to create elements, visualize the network, and do simple configurations. If you don't have a physical device at the time of deployment, a virtual configuration-device shell-is created associating a device to a site which can be later assigned to a device.

TACACS+ Accounting

If you use a Terminal Access Controller Access-Control System Plus (TACACS+) server for user authorization and authentication, you can now [log accounting information](#) to fully make use of the authentication, authorization, and accounting (AAA) framework that is the basis for TACACS+.

The TACACS+ Accounting feature allows you to use a TACACS+ server profile to record user behavior, such as when a user started using a specific service, the duration of use for the service, and when they stopped using the service. The TACACS+ Accounting feature helps to create logs and records of the initiation and termination of services, as well as any services in progress during the user's session, that you can then use later if needed for auditing purposes.

When you configure and enable an Accounting server profile, the TACACS+ server provides information to the firewall about the initiation, duration, and termination of services by users. The firewall also generates a log when the TACACS+ server successfully provides the accounting records to the server that you configure in the profile. If the firewall is unable to successfully send the accounting records to any of the servers in the profile, the firewall generates a critical severity alert to the system logs.

By using your existing TACACS+ server, you can now configure it to provide even more information about the use of services by users on your network, giving you even more robust visibility into user activity on your network.

Tenant Moves and Acquisitions

If you're a managed security service provider (MSSP) or distributed enterprise with a multitenant hierarchy, you can now move a tenant that is part of your tenant hierarchy to a different location. You can do this by [moving an internal tenant](#). Any tenant is considered an internal tenant if it's within your tenant hierarchy, and you have superuser access to the source and target tenants. It's possible to move tenants within the same top-most, root-level, parent tenant or intermediate tenants of your hierarchy. You would move an internal tenant primarily in the case of testing, demonstrations, reorgs, correcting mistakes, and more.

If you're a managed security service provider (MSSP) or distributed enterprise with a multitenant hierarchy, you can also acquire and manage tenants that are not part of your current tenant hierarchy. You can do this by [acquiring an external tenant](#). Any tenant is considered an external tenant if it isn't within your current tenant hierarchy. You can only acquire a top-most, root-level, parent tenant through an external tenant acquisition. You would acquire an external tenant primarily in the case of corporate acquisitions or mergers or reorgs.

Traceability and Control of Post-Quantum Cryptography in Decryption

Today, [post-quantum cryptography \(PQC\)](#) algorithms and hybrid PQC algorithms (classical and PQC algorithms combined) are accessible through open-source libraries and integrated into web browsers and other technologies. Traffic encrypted by PQC or hybrid PQC algorithms cannot be decrypted yet, making these algorithms vulnerable to misuse. To address these concerns, Palo Alto Networks firewalls now [detect, block, and log the use of PQC and hybrid PQC algorithms](#) in TLSv1.3 sessions. Successful detection, blocking, and logging of PQC and hybrid PQC algorithms depends on your SSL Decryption policy rules.

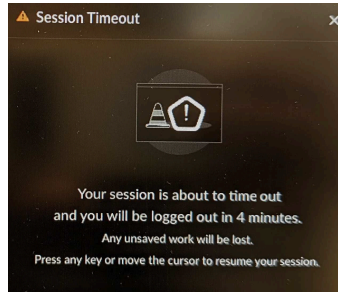
If SSL traffic matches an SSL Forward Proxy or SSL Inbound Inspection Decryption policy rule, the firewall prevents negotiation with PQC, hybrid PQC, and other unsupported algorithms. Specifically, the firewall removes these algorithms from the ClientHello, forcing the client to negotiate with classical algorithms. (For a list of supported cipher suites, see [PAN-OS 11.1 Decryption Cipher Suites](#).) This enables continuous decryption and threat identification through deep packet inspection. If the client strictly negotiates PQC or hybrid PQC algorithms, the firewall drops the session. In the Decryption log for the dropped session, the error message states that the "client only supports post-quantum algorithms." To see details of successful or unsuccessful TLS handshakes in the Decryption logs, enable both options in your Decryption policy rules.

If SSL traffic matches a "no-decrypt" Decryption policy rule or doesn't match any Decryption policy rules, the firewall allows negotiation with PQC or hybrid PQC algorithms. However, details of sessions that negotiate these algorithms are available in Decryption logs only when session traffic matches a "no-decrypt" Decryption policy rule.

Additionally, new threat signatures offer additional visibility into the use of PQC and hybrid PQC algorithms in your network. These signatures monitor ServerHello responses and trigger alerts for SSL sessions that successfully negotiate with the most commonly known PQC and hybrid PQC algorithms. A Threat Prevention license is required to receive alerts.

User Session Inactivity Timeout

The Strata Cloud Manager user session inactivity timeout occurs after 30 minutes of inactivity. Five minutes prior to the timeout, you get a notification that the session is about to time out unless you press a key or move your cursor. If you don't do anything, the notification will count down the time until approximately five seconds remain.



If you still don't press a key or move your cursor, you'll lose any unsaved work and you'll need to log in again. The inactivity timeout applies to all tenants managed in the Strata Cloud Manager.



You were logged out due to inactivity.
You were idle for more than 30 minutes so we logged you out for your safety.
Please sign in again.
[Sign In](#)

December 2023

Review all the new features we've introduced across the NetSec platform in December 2023.

FedRAMP High "In Process" Requirements and Activation

The Federal Risk and Authorization Management Program (FedRAMP) is a United States government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for government users. Palo Alto Networks has demonstrated FedRAMP compliance.

To ensure FedRAMP High "In Process" compliance, [Prisma SASE FedRAMP High In Process](#) introduces support for additional Prisma SASE apps, add-ons, and certain features.

License Activation Changes

The following changes are available in license activation.

- **Prisma SD-WAN:** Now all stand-alone Prisma SD-WAN sales orders come with an activation email regardless if the subscription is brand new or for an existing tenant. You'll see this when you [activate a license for Prisma SD-WAN](#).
- **Prisma SD-WAN:** Now you can choose a different Customer Support Account than you chose during first-time activation. You'll see this during [return visit license activation](#) for Prisma SD-WAN.
- **Software NGFW Credits:** Now you can [activate a Software NGFW Credits License using Strata Cloud Manager \(AIOps for NGFW Premium\)](#) for Panorama Managed VM-Series.

After you receive an email from Palo Alto Networks identifying the new product license you're activating, including all your add-ons and capacities, use the activation link to begin the activation process. You can activate and manage all your available licenses, device associations, tenants, and identity and access from [Common Services](#). As existing app instances transition to [tenants and tenant service groups](#) you can also use Common Services to manage those as well. After activation or transition, you can find Common Services in the [tenant view of the hub](#) or in a [variety of ways](#).

Performance Policy with Forward Error Correction (FEC)

Measuring application performance and delivering app SLAs is a core component of Prisma SD-WAN. [Performance Policy](#) builds upon the existing App SLA configuration to deliver a policy framework for the measurement, enforcement, and alerting for application SLAs.

Performance Policy utilizes link quality metrics such as Latency, Loss, and Jitter as well as application performance metrics such as Application RTT and Init failure % as SLA metrics. If the SLA metrics are violated, the system takes action to ensure that the SLA is enforced including moving flows to a compliant path (if available) and invoking line conditioning such as Forward Error Correction (FEC) to ensure the SLA is met. Optionally, an incident can be generated for critical applications when an SLA is violated. Although default policies work well for most environments, policies can be granularly tuned per application, path type, DC group, and circuit category to align to the performance needs of the business.

View and Monitor ZTNA Connector Access Objects

View and monitor private apps that were added through ZTNA Connector access objects by viewing data such as the number of apps added by FQDNs, IP subnets, and wildcards, each access object's connectivity status, and the Connector Groups and Connectors associated with each access object.

The private apps in the data centers connect to Prisma Access through your Connector virtual machines (VMs). You can add apps based on these access objects—FQDNs, FQDN wildcards, or IP subnets.

- **FQDNs**—Prisma Access resolves the FQDNs of the applications you onboard to ZTNA Connector to the IP addresses in the Application IP address block.
- **Wildcards**—For wildcard-based apps, create an FQDN-based connector group, then specify the wildcard to use (for example, *.example.com) for the app target. When users access sites that match the wildcard, those apps are automatically onboarded for access from ZTNA Connector for your mobile users and remote network users.
- **IP Subnets**—Create an IP subnet-based Connector group, and then enter the IP subnet to use for the app target.

Software Cut-Through Support for PA-3400 and PA-5400 Series Firewalls

The PA-3400 Series and PA-5400 Series (excepting the PA-5450) firewalls have significantly improved latency.

Persistent NAT for DIPP

Some applications, such as VOIP and video, use DIPP source NAT and may require STUN. DIPP NAT uses symmetric NAT, which may have compatibility issues with STUN. To alleviate those issues, persistent NAT for DIPP provides additional support for connectivity with such applications. When you enable persistent NAT for DIPP, the binding of a private source IP address and port to a specific public (translated) source IP address and port persists for subsequent sessions that arrive having that same original source IP address and port.

ZTNA Connector Wildcard and FQDN Support for Applications and Additional Diagnostic Tools

ZTNA Connector offers the following enhancements:

- **Applications Based on Wildcards and IP Subnets**—In addition to setting up applications based on FQDNs, you can set up applications based on FQDN wildcards and IP subnets.
 - For wildcard-based apps, you create an FQDN-based connector group, then specify the wildcard to use (for example, *.example.com) for the app target.

When users access sites that match the wildcard, those apps are automatically onboarded for access from ZTNA Connector for your mobile users and remote network users. For example, given a wildcard of *.example.com, when users access the app at app1.example.com, ZTNA Connector automatically allows that app to be accessed for mobile users and users at remote network sites.
 - For IP subnet-based apps, you create an IP subnet-based Connector group, then enter the IP subnet to use for the app target.
- **Additional Diagnostic Tools**—In addition to the existing [ZTNA Connector diagnostic tools](#), more diagnostic tools are available to help you troubleshoot ZTNA Connector issues:
 - **Dump Overview**—Allows you to collect a dump of the ZTNA Connector's status.
 - **Packet Captures**—Allows you to capture packets from the ZTNA Connector internal, external, or tunnel interface.
 - **Tech Support**—Allows you to generate and download a tech support file.
- **FQDN DNS Resolution to Multiple IP Addresses**—If an application FQDN resolves to multiple private IP addresses, the ZTNA connector performs an application probe to determine the status of all resolved IP addresses and load balances the FQDN access to multiple resolved IP addresses that have an application status of Up.

November 2023

Review all the new features we've introduced across the NetSec platform in November 2023.

5G Cellular Interface for IPv4

If you have a PA-415-5G firewall, you can now [configure](#) a 5G interface for IPv4 cellular traffic. The PA-415-5G is similar to the PA-415 except that it contains an integrated 5G module to support 4G/5G capability and configuration of an interface for IPv4 cellular traffic.

The 5G cellular interface enables configuration of a primary internet connection as well as configuration of a secondary connection for redundancy in case the primary connection is not available. This type of interface supports data connectivity over the 5G mobile network; if the 5G network is unavailable, the firewall automatically switches to a 4G or 3G network, depending on availability.

To enable the 5G cellular interface, configure an Access Point Name (APN) profile. The APN profile specifies which network or networks the device can access and whether the device receives a dynamic or static IP address.

You can configure a primary and secondary SIM card if it is available. If you have a secondary SIM card, you can configure the firewall to switch from one SIM card to another if one SIM card becomes unavailable. For security, enable a PIN code for the SIM card to prevent misuse. If you cannot remember the PIN code, you must obtain a Personal Unblock Key (PUK) for the SIM card to unlock it for use.

For monitoring purposes, you can enable the Dashboard widgets to view more information about the status of the 5G network.

Advanced WildFire Inline Cloud Analysis

Palo Alto Networks Advanced WildFire now operates a series of cloud-based ML detection engines that provide inline analysis of PE (portable executable) files traversing your network to detect and prevent advanced malware in real-time. [Advanced WildFire Inline Cloud Analysis](#) prevents files from being downloaded and potentially spreading through your network while it performs real-time analysis of the target sample. As with other malicious content that WildFire detects, threats detected by Advanced WildFire Inline Cloud Analysis also generate a signature that is then disseminated to customers through an update package, providing a future defense for all Palo Alto Networks customers.

This real-time defense is facilitated by new cloud-based engines that enable the detection of never-before-seen malware (e.g., a Palo Alto Networks zero-day - malware previously unseen in the wild or by Palo Alto Networks) and block it from entering your network environment. Advanced WildFire Inline Cloud Analysis utilizes a lightweight forwarding mechanism on the firewall to minimize performance impact, while the process-intensive operations take place in the cloud. The cloud-based ML models are updated seamlessly, to address the ever-changing threat landscape without requiring content updates or feature release support.

Advanced WildFire Inline Cloud Analysis is enabled and configured through the WildFire Analysis profile and requires an active Advanced WildFire license.

API Key Certificate

With PAN-OS and Panorama, the option to [encrypt the API key](#) using a self-signed certificate is now available, ensuring enhanced security when you retrieve your API key. This feature utilizes the PAN-OS device certificate management function to encrypt the API key for added protection.

See use cases for [Keys and Certificates](#) on PAN-OS for more information on how to manage certificates using PAN-OS and Panorama.

This feature introduces a new field under **Device > Setup > Management > Authentication settings** that enables you to select an **API Key Certificate** to encrypt your API key. To use this feature, simply generate an RSA Certificate above 3,027 bits and select the created certificate as the API key certificate under the **Authentication Settings** option.

The existing workflow to generate the API key will still be the same, but now all existing API keys will be invalid when you add or change an API key certificate.

App Acceleration in Prisma Access

When your users access apps, they can experience poor app performance due to decreased throughput. This condition can be caused by degraded wireless connectivity, network congestion, and other factors. These networking issues can adversely affect the employee experience and can reduce their productivity.

App Acceleration directly addresses the causes of poor app performance and acts in real-time to boost throughput while maintaining best-in-class security, dramatically improving the user experience for Prisma Access GlobalProtect and Remote Network users.

Without requiring any changes to your applications, App Acceleration securely builds an understanding of:

- **Device capability**—The type of client endpoint
- **Network capability**—The type of network
- **App Context**— The type of app being used

Using its understanding of network, device, and application context, App Acceleration maximizes throughput and adjusts in real-time to account for changing network conditions.

When compared to direct internet access, App Acceleration offers a marked throughput improvement for TCP traffic when connecting through Prisma Access.

You can view these improvements using Autonomous DEM (ADEM), which provides you with metrics such as throughput per application and the data and apps that were accelerated. Using this information, you can pinpoint how App Acceleration improved the app experience for your users.

ARM Support on VM-Series Firewall

VM-Series firewall now supports ARM based instances on [AWS Graviton 2](#) (ARM compute) instances for public clouds and [KVM](#) hypervisor for private clouds. All features that were available in x86 environments are now extended to ARM based instances including Hypervisor support, DPDK and other acceleration methods that provide better performance, while reducing the operational (OPEX) costs, power consumption, and footprints.

ARM architecture support is currently available on VM-Flex licensing models on AWS BYOL or KVM as Software NGFW credits on the following types of ARM instances:

Name	Types
AWS C6gn	8xLarge, 12xlarge, 16xlarge
AWS R6g	xlarge, 2xlarge, 4xlarge, 8xLarge, 12xlarge, and 16xlarge
AWS M6g	large, xlarge, 2xlarge, 4xlarge, 8xlarge, and 16xlarge
KVM	v8 systems such as Ampere Altra AC-106422002

Drivers	Types
KVM	i40e and mlx5
AWS	ena

ARM also supports the following capabilities:

- AWS automation templates such as Cloud formation and terraform templates
- AWS Gateway Load Balancer (GWLB)
- 64vCPU profiles
- Simple and full boot-strapping on AWS
- All security subscriptions currently supported in x86 based systems
- All features on KVM hypervisor currently supported on X86 based systems
- Telemetry data similar to what is currently supported on X86 based systems

Authentication Exemptions for Explicit Proxy

If you use the explicit proxy configuration for your web proxy, you can now [configure exemptions](#) for traffic from specific sources, destinations, or both. IoT devices, such as printers, cannot respond to an authentication request from the proxy or support a certificate or PAC file for authentication. You can configure up to three authentication exemptions for devices using the explicit proxy.

BGP MRAI Configuration Support

BGP routing offers a timer you can use to tailor BGP routing convergence in your network called the *Minimum Route Advertisement Interval* (MRAI).

MRAI acts to rate-limit updates on a per-destination basis, and the BGP routers wait for at least the configured MRAI time before sending an advertisement for the same prefix. A smaller number gives you faster convergence time but creates more advertisements in your network. A larger number decreases the number of advertisements that can be sent, but can also make routing convergence slower. You decide the number to put in your network for the best balance between faster routing convergence and fewer advertisements.

You can configure an MRAI range of between 1 and 600 seconds, with a default value of 30 seconds.

Cloud Managed Support for Prisma Access China

[Prisma Access deployments in China](#) provide you with the following enhanced functionalities:

- To provide you with greater management flexibility, Cloud Managed Prisma Access is added, allowing you to use either [Cloud Managed](#) or [Panorama Managed Prisma Access](#) to manage your deployment in China.

Cloud Managed Prisma Access includes the ability to manage your Prisma Access deployment using [Strata Cloud Manager](#). With Strata Cloud Manager, you can easily manage and monitor your network security infrastructure from a single, streamlined user interface. The new platform gives you:

- Best practice recommendations and workflows to strengthen security posture and eliminate risk.
- A common alerting framework that identifies network disruptions, so you can maintain optimal health and performance.
- Enhanced user experience, with contextual and interactive use-case driven dashboards and license-aware data enrichment.

Using cloud management, you can quickly onboard branches and mobile users through task-driven workflows that allow you to set up and test your environment in minutes. Cloud management with Strata Cloud Manager simplifies the onboarding process by providing predefined internet access and decryption policy rules based on best practices. You can quickly set up IPsec tunnels using defaults suitable for the most common IPsec-capable devices and turn on SSL decryption for recommended URL categories.

- Cloud managed deployments provide you access to the [Prisma SASE Multitenant Portal](#), allowing you to access [Common Services](#) for multiple tenants such as [subscription and tenant management](#) and [identity and access management](#).

Configuration Audit Enhancements

You can perform a [configuration audit](#) to see the configuration changes made between two selected configuration versions. This allows your administrators to assess and document impact of configuration changes, trace back changes in case of an outage, and perform regular audits in order to adhere to security compliance standards. Enhancements to configuration audits now allow you to not only view the entire XML differences between the two selected config versions, but also provides you per-object granular view of the change data.

The **XML Diff** displays the XML file differences between any two selected config versions. The **Change Summary** provides a granular details about each of the configuration objects that added, deleted, or modified between the older selected config version and the newest selected config version. The type granular details are:

- **Object Name**—Name of impacted configuration object.
- **Object Type**—Type of configuration object impacted.
- **Modified Time**—Date and time configuration object change occurred.
- **Location**—Device group, template, or template stack where the configuration change occurred.
- **Location Type**—The configuration container type where the change occurred.
- **Modified By**—Administrator that modified the configuration object.
- **Operation**—The type of operation performed on the configuration object.

Strata Logging Service with CN-Series Firewall

Strata Logging Service enables AI-based innovations for cybersecurity with the industry's only approach to normalizing and stitching together your enterprise's data. For more information, see [About Strata Logging Service](#) and [Deploy Strata Logging Service with Panorama](#). Strata Logging Service can now collect log data from [CN-Series next-generation firewall](#). When you purchase a Strata Logging Service license, all firewalls registered to your support account receive a Strata Logging Service. You will also receive a magic link that you will need to use to activate your Strata Logging Service instance.

To get started with CN-Series firewall Strata Logging Service, you must ensure that you [Install the Kubernetes Plugin and Set up Panorama for your CN-Series Firewall](#). You must provide the device certificate to the CN-MGMT pod for Strata Logging Service connectivity. It is important to register your CN-MGMT pod with a CSP account to ensure that CN-MGMT pod is reflected in your Strata Logging Service instance. Add the valid PIN-ID and PIN-value to `pan-cn-mgmt-secret.yaml` file to successfully install the device certificate. The CN-Series firewall requires a device certificate that authorizes secure access to Strata Logging Service. For more information see [Install a Device Certificate on the CN-Series Firewall](#).

After you [deploy your CN-Series firewall](#), verify that your CN-MGMT pod is visible on your CSP account, under **Registered Devices**. For more information see, [Register the Firewall](#). You must ensure that you [configure your CN-Series firewall with Panorama](#) and [Create a CN-Series Deployment Profile](#) on your CSP account and use the auth code to push licenses from Panorama to your CN-Series firewall.

Device-ID Visibility and Policy Rule Recommendations in PAN-OS

When next-generation firewalls subscribe to IoT Security services, they send the IoT Security instance that's in the same tenant service group (TSG) Traffic logs for analysis. IoT Security uses AI and machine learning to automatically discover and identify network-connected devices and then construct a data-rich, dynamically updating inventory. From PAN-OS 11.1, administrators can see this inventory directly in the PAN-OS web interface without having to open the IoT Security portal, which is the only place this information appears when IoT Security is integrated with firewalls running earlier PAN-OS releases. For further Device-ID visibility, the PAN-OS 11.1 web interface also shows a summary of the 10 most common device categories, profiles, and operating systems on the network learned from IoT Security.

In addition to identifying devices, IoT Security analyzes network behaviors to determine a baseline of normal, acceptable behaviors. It then generates policy rule recommendations that would allow devices to continue their normal network behaviors while denying behaviors that deviate from the norm. PAN-OS administrators can view these recommendations in the PAN-OS 11.1 web interface, select the ones they want their firewalls to apply, and import them into the Security policy rulebase. When using a PAN-OS release prior to PAN-OS 11.1, it was necessary to create policy rule sets in the IoT Security portal and activate them before they appeared in the PAN-OS interface. To simplify the workflow, these steps have been eliminated in PAN-OS 11.1.

From PAN-OS 11.1, you can see and manage the device inventory and top 10 common device categories, profiles, and operating systems in the PAN-OS interface. You also no longer need to create and activate policy rule sets in IoT Security. As a result, IoT device visibility is more convenient and policy rule creation is simplified.

Dynamic IPv6 Address Assignment on the Management Interface

The management (MGT) interface on the NGFW now supports dynamic IPv6 address assignment. Configuring the MGT interface for dynamic IPv6 address assignment (rather than a static address) makes it easier to insert and manage the firewall in an IPv6 network.

When you configure the MGT interface, you'll notice new IPv4 and IPv6 tabs to separate the configurations.

You have two types of addressing to choose from: stateful or stateless. On the network segment, you control the router where you set flags to indicate that the MGT interface will be one of the following:

- A stateful DHCPv6 client, which receives its IPv6 address with prefix length and other configuration information from a DHCPv6 server.
- An IPv6 stateless address autoconfiguration (SLAAC) client, which autogenerates its IPv6 address. A stateless IPv6 address avoids a DHCPv6 server having to store dynamic state information about clients; such avoidance is helpful in environments with a large number of endpoints.

The firewall uses Neighbor Discovery Protocol (NDP) to send a Router Solicitation to all routers on the link. The flags in the Router Advertisement (RA) that the sole router (or preferred router) on the link sends to the firewall control whether the firewall will use SLAAC or stateful DHCPv6 to get a dynamic address for the MGT interface.

However, the current situation is that when the Autonomous (A) flag is set in the RA message, the firewall chooses both a DHCPv6 address and a SLAAC address. Ideally, the firewall should choose only the SLAAC address and shouldn't send a DHCPv6 Solicit message. As a result of this known issue, if there is a DHCPv6 server on the segment and it can assign an IPv6 address, the firewall prefers DHCPv6 address assignment over SLAAC.

You specify either a static IPv6 default gateway address or request a dynamic IPv6 default gateway address, which the firewall learns from the RA that the router sends. Even if you configure the MGT interface with a static IPv6 address, you now have this same choice for configuring the default gateway.

Therefore, you have four possible options for configuring the MGT interface and its default gateway:

- Static IPv6 address and static IPv6 default gateway address
- Static IPv6 address and dynamic IPv6 default gateway address
- Dynamic IPv6 address and static IPv6 default gateway address
- Dynamic IPv6 address and dynamic IPv6 default gateway address

Configuring the MGT interface as a DHCPv6 client involves requesting a Non-Temporary or Temporary Address, deciding on the Rapid Commit option, and specifying the DHCPv6 Unique ID type.

Dynamic Routing in CN-Series HSF

CN-Series Hyperscale Security Fabric (HSF) introduces [dynamic routing](#) through BGP and BGP over BFD protocols. Using Dynamic routing, you can attain stable, high-performing, and highly available layer 3 routing through profile-based filtering lists and conditional route maps, which can be used across logical routers. These profiles provide finer granularity to filter routes for each dynamic routing protocol and improve route redistribution across multiple protocols.

BGP looks for the available paths that data could travel and picks the best route, based on IP prefixes that are available within autonomous systems. The Bidirectional Forwarding Detection (BFD) provides fast forwarding path failure detection times for BGP routing protocols between CN-GW pods and the external router.

Enhanced IoT Policy Recommendation Workflow for Strata Cloud Manager

Rapid IoT adoption is creating new attack vectors and implementing policy recommendations to apply least privilege Zero Trust policies to secure your organization's devices is key. If you use Strata Cloud Manager to configure Prisma Access, you can use [enhanced IoT policy recommendation workflows](#) to accomplish these goals and keep your devices and users secure.

Enhanced SaaS Tenants Control

Prisma Access allows you to granularly manage and apply distinct policies for specific tenants for an extended list of SaaS applications (for example, Github or Bitbucket). The complete list of apps is documented at <https://docs.paloaltonetworks.com/saas-security/saas-security-admin/saas-security-inline/remediate-risks-saas-security-inline/manage-saas-security-inline-policy/create-saas-policy-rule-recommendations>

This functionality allows you to enforce use cases where you might need to allow all actions (for example, uploads and downloads) for a corporate Github account, but block uploads for a partner instance of the same Github SaaS application.

Exclude All Explicit Proxy Traffic from Authentication

If you do not require authentication for your explicit proxy traffic, you can [exclude all explicit proxy traffic](#) from authentication. If you enable this option, the firewall or Panorama does not authenticate any explicit proxy traffic and does not create any logs for authentication events.

GlobalProtect Portal and Gateway Support for TLSv1.3

You can now [configure SSL/TLS service profiles using TLSv1.3](#) on the firewall that is hosting the GlobalProtect portal or gateway to establish TLS connectivity between GlobalProtect components. TLSv1.3 is the latest version of the TLS protocol, which provides increased network security by removing the weak ciphers supported in the earlier versions of TLS and adding more secure cipher suites. In addition, the GlobalProtect gateway and portal now support the following TLSv1.3 cipher suites:

- TLS-AES-128-GCM-SHA256
- TLS-AES-256-GCM-SHA384
- TLS-CHACHA20-POLY1305-SHA256

You can configure SSL/TLS service profiles with TLSv1.3 to provide enhanced security and a faster TLS handshake while establishing connection between GlobalProtect components. To provide the strongest security, you must set both the minimum and maximum supported version as TLSv1.3 in the SSL/TLS service profile.

IKEv2 Certificate Authentication Support for Stronger Authentication

The SD-WAN plugin now supports the certificate authentication type in addition to the default pre-shared key type for user environments that have strong security requirements. We support the [IKEv2 certificate authentication type](#) on all SD-WAN supported hardware and software devices.

You can configure certificate-based authentication for the following topologies, provided that you have configured all SD-WAN devices in the topology with the same (or certificate) authentication type:

- VPN clusters (hub-and-spoke and mesh)
- PAN-OS firewalls connecting to Prisma Access compute nodes

[Generate certificates](#) for the SD-WAN device using your own certificate authority (CA). Add and deploy the generated certificates in bulk across your SD-WAN cluster and autogenerate the SD-WAN overlay using the certificate-based authentication.

Improved Throughput with Lockless QoS

The Palo Alto Networks QoS implementation now supports a new QoS mode called [lockless QoS](#) for PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, PA-5440, and PA-5445 firewalls. For firewalls with higher bandwidth QoS requirements, the lockless QoS dedicates CPU cores to the QoS function that improves QoS performance, resulting in improved throughput and latency.

Increased Device Management Capacity for the Panorama Virtual Appliance

To ease the operational burden of managing the configuration of your [large-scale firewall deployments](#), the Panorama virtual appliance now supports management of up to 5,000 Palo Alto Networks Next-Generation Firewalls (NGFW) with a Panorama virtual appliance in Management Only mode. To use a single Panorama virtual appliance to manage up to 5,000 Next-Generation firewalls you must [install the Panorama virtual appliance](#) in a supported private or public hypervisor with the [minimum virtual resources](#) required to support large-scale device management.

Inline Security Checks

Strata Cloud Manager lets you validate your configuration against predefined [Best Practices](#) and custom checks you create based on the needs of your organization. As you make changes to your service routes, connection settings, allowed services, and administrative access settings for the management and auxiliary interfaces for your firewalls, Strata Cloud Manager gives you assessment results inline so you can take immediate corrective action when necessary. This eliminates problems that misalignments with best practices can introduce, such as conflicts and security gaps.

Inline checks let you:

- Gauge the effectiveness of, assess the impact of, and validate changes you make to your configuration using inline assessment results.
- Prioritize and perform remediations based on the recommendations from the inline assessment.

Integrate Prisma Access with Microsoft Defender for Cloud Apps

[Integrate Prisma Access with Microsoft Defender for Cloud Apps](#) to sync unsanctioned applications and block them inline using Prisma Access automatically.

After you integrate Microsoft Defender for Cloud Apps with Prisma Access, Prisma Access creates a block security policy for URLs that are blocked in Microsoft Defender for Cloud Apps. You can view the list of unsanctioned applications after configuring the integration settings. The Prisma Access-Microsoft Defender for Cloud Apps integration enables you to gain visibility and to discover all cloud applications and shadow IT applications being used as well as provide closed loop remediation for unsanctioned applications.

Intelligent Security with PFCP for N6 and SGI Use Cases

As enterprises migrate their networks to 5G, this transition provides the potential for vulnerability to some of the security risks associated with 5G. As an unprecedented number of devices connect to enterprise and government networks, this increases the potential for attacks and other threats.

Intelligent Security (also known as User Equipment to IP address Correlation, or UEIP) helps correlate user equipment (UE) information with IP addresses by mapping the subscriber ID and equipment ID to the IP address associated with traffic from the UE. This helps to ensure consistent policy rule enforcement in your mobile network Security policy. Intelligent Security with PFCP for N6 and SGI deployments now provides enforcement for Security policy rules that are based on:

- the 5G subscriber ID
- the 5G equipment ID
- the 5G network slice ID for a 5G or hybrid (5G and 4G) LTE network

Administrators now have multiple deployment options for correlating IP addresses and user equipment, including on perimeter interfaces (such as N6 for 5G and SGI for a 4G or LTE network).

To support the new deployment options, enable the [User Plane with GTP-U encapsulation](#) option if you're using the N1 or S1U interface or disable the option for SGI, N6, or RADIUS deployments. In addition, support for UE-to-IP mapping is now available for the PA-7000b and PA-5450 platforms.

This enables network administrators to extend Zero Trust policy rules for their 5G and 4G networks by consistently verifying all subscribers, equipment, applications, and data based on content and subscriber activity.

IoT Security: Device Visibility and Automatic Policy Rule Recommendations

Strata Cloud Manager integrates with [IoT Security](#) to provide visibility into the devices on your network and automated policy rule recommendations for policy enforcement on next-generation firewalls and Prisma Access. By having IoT Security functionality in Strata Cloud Manager, IoT device visibility and policy rule recommendations become available in the same platform you're using to manage firewalls and interact with other network security products.

When your firewalls or Prisma Access is subscribed to IoT Security, you can use the following IoT Security features from the Strata Cloud Manager web interface:

- **IoT Security Dashboard:** In Strata Cloud Manager, there is an [IoT Security dashboard](#) with information about the devices on the network, their device profiles and operating systems, and how they are distributed by device type across subnets. For advanced IoT Security products (Enterprise IoT Security Plus, Industrial IoT Security, or Medical IoT Security), the IoT Security dashboard additionally displays the total number of active alerts to date and vulnerabilities to date.
- **Assets Inventory:** See a dynamically maintained [inventory](#) of the devices on your network with numerous attributes for each one such as its IP and MAC addresses; profile, vendor, model, and OS; and (for advanced IoT Security products) its device-level risk score.
- **Security Policy Rule Recommendations:** IoT Security provides Strata Cloud Manager with automatically generated [Security policy rule recommendations](#) organized by device profile. There is one recommendation per application per profile. Choose a profile, select the rule recommendations you want to use, and then the next-generation firewalls or Prisma Access sites where you want to enforce them.

IOT Security Support for CN-Series

For Palo Alto Networks next-generation CN-Series firewall, the IoT Security solution uses machine learning (ML) to provide visibility of discovered IoT devices based on the meta-data in the logs it receives from the firewall. IoT Security also identifies vulnerabilities and assess risk in devices based on their network traffic behaviors and dynamically updated threat feeds.

You can use the policy rule recommendations that IoT Security generates as a reference when manually adding rules to your CN-Series firewall. IoT Security always generates Security policy rule recommendations regardless of the PAN-OS version.



*When using **IoT Security Subscription**, which stores data in Strata Logging Service, you need one Strata Logging Service license per account and must ensure that [Strata Logging Service configuration for your CN-Series firewall](#) is complete.*

For more information, see [IoT Security Prerequisites](#).

IP Protocol Scan Protection

Palo Alto Networks now offers [reconnaissance protection](#) for IP protocol scans. IP protocol scans cycle through IP protocol numbers to determine the IP protocols and services supported by target machines. Malicious actors use this scanning technique to identify and exploit open and insecure protocols. This feature enables your firewall to detect and block, allow, or alert on these scans. For example, you can configure the firewall to drop subsequent packets from a host exhibiting behavior consistent with IP protocol scans.

You can configure protection against IP protocol scans in the Reconnaissance Protection settings of a Zone Protection profile. The firewall identifies IP protocol scans based on the specified number of scan events that occurs within a specified interval. If necessary, you can exclude the IP addresses of trusted internal groups performing vulnerability testing from reconnaissance protection. Details of each detected scan are available in the Threat logs.

IPSec VPN Monitoring

You can now [view the status of the IPSec VPN tunnels](#) to know whether or not valid IKE and IPSec SAs have been established, and whether the tunnel interface is up and available for passing traffic.

Because the tunnel interface is a logical interface, it can't indicate a physical link status. Therefore, you must use IPSec tunnel monitoring so that the tunnel interface can verify connectivity to an IP address and determine if the path is still usable. If the IP address is unreachable, the firewall will either wait for the tunnel to recover or failover. When a failover occurs, the existing tunnel is torn down, and routing changes are triggered to set up a new tunnel and redirect traffic.

With the IPSec VPN tunnel monitoring feature, you can view the tunnel status:

- VPN cluster tunnel status
- IPSec tunnel status
- IKE gateway status
- VPN tunnel status

View the overall status of all the IPSec tunnels, IPSec tunnel status per device, and detailed status of each IPSec tunnel.

Link Aggregation Support on VM-Series

VM-Series firewalls add support for link aggregation for ESXi and KVM environments. This feature supports multiple connections that combine into a single logical bonding device with a unique name that is associated with a network device (either physical or virtual) as secondary devices. The bonded device possesses a unique MAC address that is shared among all secondary devices.

Important things to consider:

- An Aggregate Ethernet interface uses the MAC address from the base and not from the hypervisor. This takes effect after rebooting newly deployed and licensed VM-Series firewalls.
- An unlicensed Panorama VM uses an erroneous Aggregate Ethernet MAC address, while the licensed VM receives a proper MAC address. If the Panorama VM deploys initially without a license, the Aggregate Ethernet interface receives this erroneous MAC address. Once you procure the license, reboot the VM to retrieve the new base MAC address from the license key file.

To configure link aggregation, enable PAN-OS to change VM MAC addresses. To do this, configure MAC address changes: **Accept**.



Link aggregation of HA interfaces isn't supported in public cloud environments, like AWS, Azure or GCP.

Learn how to configure link aggregation support on the VM-Series for [ESXi](#) and [KVM](#).

Maximum of 500 Remote Networks Per 1 Gbps IPSec Termination Node

If your [IPSec termination node](#) that you use for [remote network onboarding](#) is configured to support 1 Gbps of bandwidth, the maximum number of remote networks those IPSec termination nodes can support is increasing from 400 to 500. You must allocate a minimum of 501 Mbps for the compute locations associated with the IPSec termination nodes to have it support up to 1 Gbps of bandwidth.



Deployments using remote networks to onboard Prisma SD-WANs cannot take advantage of this enhancement.

New Platform Support for Web Proxy

The [web proxy](#) feature is now supported on the PA-5400 series, which includes the PA-5410, PA-5420, PA-5430 PA-5440 and PA-5445 platforms.

New Template Variables

[Template and template stack variables](#) enable you to more easily reuse templates or template stacks by allowing you to replace template configuration objects with a template variable with a value specific to one or more devices. This allows you to reduce the total number of template and template stacks you need to manage while allowing you to keep any device-specific configuration values. You can now use template and template stack variables to replace hostname, IPv4 subnet, IPv6 subnet, and Pre Shared Keys in your managed firewall configurations.

- **Hostname**—Label or human readable name assigned to a device connected to the network.
- **IPv4 Subnet**—Subnet for IPv4 IP addresses. For example, 255.255.254.0.
- **IPv6 Subnet**—Subnet for IPv6 IP addresses. For example, 201:db8:3:4:6:7:8:f.
- **Pre Shared Key**—Security key for authentication when configuring a VPN tunnel. Up to 255 ASCII or non-ASCII keys are supported.

PA-415-5G Next-Generation Firewall

The [PA-415-5G](#) adds a 5G-capable appliance to the PA-400 Series firewall lineup for PAN-OS 11.1 and later versions. The 5G interface can provide primary or backup WAN connectivity, making it an optimal solution for deployments in enterprise, retail, and commercial branch locations.

The PA-415-5G features an integrated 5G module to provide cellular connectivity, four 5G SDMA antennas, and eight RJ-45 ports. There is also one SFP/RJ-45 combo port that can be used for management and data processing, making a total of nine data ports. Four of the eight RJ-45 ports can be configured as power over ethernet (PoE) interfaces to transfer up to 91W of power to a connected device.

The PA-415-5G is powered by an AC power adapter and optionally supports power redundancy. The device can be installed on a flat surface or equipment rack.

PA-450R Next-Generation Firewall

The [PA-450R](#) is a new rugged firewall appliance that upgrades the PA-220R firewall. The PA-450R is designed for industrial, commercial, and government deployments. The hardware is suited for installation in harsh environments with extreme temperatures and high humidity levels.

The PA-450R is supported on PAN-OS 11.1 and later versions. The firewall features two SFP/RJ-45 combo ports and six RJ-45 ports. The RJ-45 ports include two fail-open ports that can be configured to provide a pass-through connection in the event of a power failure.

The PA-450R is powered by DC power and optionally supports power redundancy. The device has a fanless design and can be installed on a flat surface, wall, and equipment rack. The hardware is compliant with ICS/SCADA system architecture.

PA-455 Next-Generation Firewall

The [PA-455](#) adds a new mid-range appliance to the PA-400 Series firewall lineup for PAN-OS 11.1 and later versions. This firewall is designed for deployments in enterprise, retail, and commercial branch locations.

The PA-455 features two SFP/RJ-45 combo ports and six RJ-45 ports. Both combo ports can be used for passing traffic on the network or on the WAN.

The PA-455 is powered by an AC power adapter and optionally supports power redundancy. The device can be installed on a flat surface or equipment rack.

PA-5445 Next-Generation Firewall

The [PA-5445](#) adds the highest performance fixed form-factor model to the Palo Alto Networks® Next-Generation Firewall lineup. This firewall, supported on PAN-OS 11.1 and later versions, features hardware resources dedicated to networking, security, signature matching, and management. The PA-5445 is ideal for deployments in enterprise data centers, headquarters, and regional offices.

The PA-5445 has the highest App-ID speed (93Gbps), L7 threat inspection rate (70Gbps), and session count (48M) in a fixed form-factor firewall.

The PA-5445 features eight RJ-45 ports, twelve SFP+ ports, four SFP28 ports, and four form-factor pluggable QSFP28 ports that support breakout mode. The firewall also features dedicated HSCI and HA1 ports for high availability control.

The PA-5445 can be powered by AC or DC power supplies and optionally supports power redundancy. The hardware takes up 2RU of rack space and should be mounted in a 19" equipment rack.

PA-7500 Next-Generation Firewall

The [PA-7500](#) is a new modular chassis that upgrades the PA-7000 Series firewall. The high-performance PA-7500 is intended for deployments where scalability and high speed connectivity are needed, such as high-end enterprise and service providers.

The PA-7500 is supported on PAN-OS 11.1 and later versions. The firewall features the following interface cards:

- Management Processing Card (MPC) – provides the firewall with a management interface that includes dual 400Gbps (QSFP-DD) HSCI ports, dual 100Gb/s (zQSFP) ports for logging and dual SFP28 (25GE/10GE/1GE) ports for external management connectivity.
- Network Processing Card (NPC) – provides network connectivity through eight QSFP-DD interfaces and twelve SFP-DD interfaces. The QSFP-DD ports are capable of 400Gbps speed and also support QSFP28 (100Gbps) and QSFP+ (40Gbps) optics. These optics can make use of breakout mode to provide four 25Gbps ports or four 10Gbps ports. The SFP-DD ports are capable of 100Gbps operation and support SFP28, SFP+, and SFP optics.
- Data Processing Card (DPC) – provides increased processing power and capacity to the firewall.
- Switch Fabric Card (SFC) – provides data plane connectivity to the other interface cards as well as redundant switching fabric.

The PA-7500 can be powered by AC or DC power supplies and supports power redundancy. The chassis occupies 14RU of rack space and must be installed in an appropriate 19” equipment rack.

Policy Rulebase Management Using Tags

Tags allow you to identify the purpose or function of a policy rule and help you better organize your policy rulebase. After you apply tags to the policy rules in your policy rulebase, you can use the [Tag Browser](#) to visually group and manage your policy rulebase based on the tags you assigned to your policy rules. When viewing your policy rulebase using tags, you can perform operational procedures such as adding, deleting, or moving policy rules with the applied tagging more easily. Additionally, you can filter your policy rulebase using tags to apply one or more tag search filters to the policy rulebase to narrow down the list of policy rules displayed. Viewing your policy rulebase using tags maintains the rule evaluation order.

Policy rulebase management using tags is supported for across all policy rulebases. For firewalls managed by a Panorama management server, you can create and assign tags to policy rules from Panorama. Both Panorama, managed firewalls, and standalone firewalls running PAN-OS 10.2.5 or later 10.2 or PAN-OS 11.0.3 or later release support policy rulebase base management using tags.

Post Quantum IKE VPN Support

Post-quantum VPNs resist attacks based on quantum computing and post-quantum cryptography (PQC). Palo Alto Networks post-quantum VPN support enables you to configure quantum-resistant IKEv2 VPNs and is based on the [RFC 8784](#) standard to maximize interoperability with other vendors' equipment and with future standards. Multiple government agencies around the world, including the NSA and NIAP, recommend implementing RFC 8784 to improve quantum resistance. Implementing RFC 8784 is the simplest way to create quantum-resistant VPNs because you don't need to upgrade crypto elements.

Addressing the quantum threat immediately is critical to defend against [Harvest Now, Decrypt Later](#) attacks that target long-lived data because the development of cryptographically relevant quantum computers (CRQCs) will vastly reduce the amount of time required to break classical encryption.

Configuring quantum-resistant VPNs can prevent attackers from recording critical encrypted key material and thus prevent them from decrypting the data even if they steal it. If you have long-lived data, start planning now for the threat posed by quantum computers and quantum cryptography and for your network's transition to a post-quantum world. The first step is to make your VPN connections quantum-resistant.

RFC 8784 provides a transition from today's classical cryptography to PQC. Quantum-resistant VPNs based on RFC 8784 enable using post-quantum pre-shared keys (PPKs) that are not transmitted with the data, so harvesting attacks fail because they don't capture the key material that they need to decrypt the data later. A PPK is a complex, strong hexadecimal string that you statically program into the IKE peers at the ends of the VPN tunnel.

Adding a static PPK that's delivered out-of-band to the classical Diffie-Hellman (DH) key prevents [Shor's algorithm](#) from cracking the key because the key is no longer based on prime numbers. RFC 8784 enables using long, strong PPKs that meet the NIST Category 5 security level.

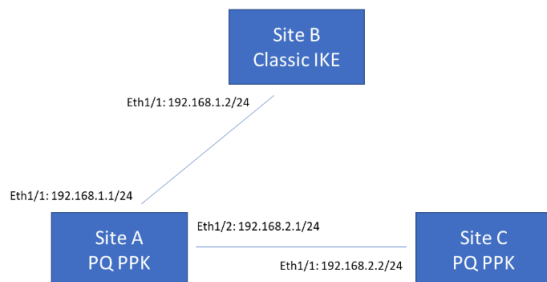
In addition, RFC 8784 provides the backward compatibility to fall back to classical cryptography if a peer can't support RFC 8784, so the implementation doesn't risk refusing legitimate connections. Palo Alto Networks implementation of RFC 8784 provides flexibility and quantum resistance for your IKEv2 VPNs:

- You can add up to ten post-quantum (PQ) PPKs to each IKEv2 VPN. Each PQ PPK is associated with a PPK KeyID, which uniquely identifies the PPK, so you can configure up to ten PPK + KeyID pairs. You can configure PPKs yourself or use a built-in tool to generate strong PPK strings. Configuring multiple active PPKs enables the firewall that initiates the IKEv2 peering to randomly select one of the active PPKs to use with the peer.
- You can configure PPK strings from 16-64 bytes (32-128 characters) in length. For best security, use PPK strings that are at least 32 bytes (64 characters) in length.
- You can set the **Negotiation Mode** to control the ciphers used to establish the connection:
 - **Mandatory**—Require that the responding peer use RFC 8784 and abort the connection if it only uses classical cryptography.
 - **Preferred**—Allow the initiating device to fall back to classical cryptography if the peer doesn't support RFC 8784.
- You can activate and deactivate individual PQ PPKs, so if a PQ PPK is lost or exposed, you can disable it and remove it from the negotiation pool.

In addition to implementing RFC 8784 now:

- Migrate to tougher cipher suites. Follow [RFC 6379](#) for Suite B Cryptographic Suites for IPsec, upgrade ciphers to Suite-B GCM-256, and avoid using weaker AES-128-bit algorithms.
- Upgrade to larger hash sizes such as SHA-384 or SHA-512. Don't use MD5 or SHA-1.
- Upgrade your CA to larger RSA key sizes. Use 4096-bit RSA key sizes and migrate VPN certificate authentication to new certificates.

The following example topology shows three VPN termination sites. Sites A and C support post-quantum VPNs based on RFC 8784. Site B supports only classical VPNs. Site A must be able to communicate with both Site B and Site C.



Site A uses both Mandatory and Preferred negotiation modes. When Site A communicates with Site B, which only supports classical cryptography, Site A falls back to classical negotiation. When Site A communicates with Site C, Site A uses a PQ PPK because Site C supports using PQ PPKs.

PPPoE Client for IPv6

The firewall supports an Ethernet Layer 3 interface or subinterface acting as a [Point-to-Point Protocol over Ethernet \(PPPoE\) IPv6 client](#) to reach an ISP that provides IPv6 internet services. In PPPoE mode, the interface or subinterface can obtain an IPv6 address dynamically using DHCPv6 either in stateful or stateless mode. In stateful mode, the PPPoE interface acquires all connection parameters dynamically from the DHCPv6 server. In stateless mode, the IPv6 address of the PPPoE interface is obtained using stateless address autoconfiguration (SLAAC), but the other parameters (DNS and prefix delegation) are obtained through DHCPv6. Stateful and stateless DHCPv6 reduce provisioning effort and errors, and simplify address management.

Only Ethernet Layer 3 interfaces and subinterfaces support an IPv6 PPPoE client (tunnel, AE, VLAN, and loopback interfaces don't support an IPv6 PPPoE client). A Layer 3 interface and its subinterface can't act as a PPPoEv6 client at the same time.



A limitation is that the interface configured with PPPoEv6 can't acquire a DNS server address or DNS prefix from Router Advertisement (RA-DNS). You'll have to rely on DHCPv6 to obtain the DNS information or configure those parameters manually.

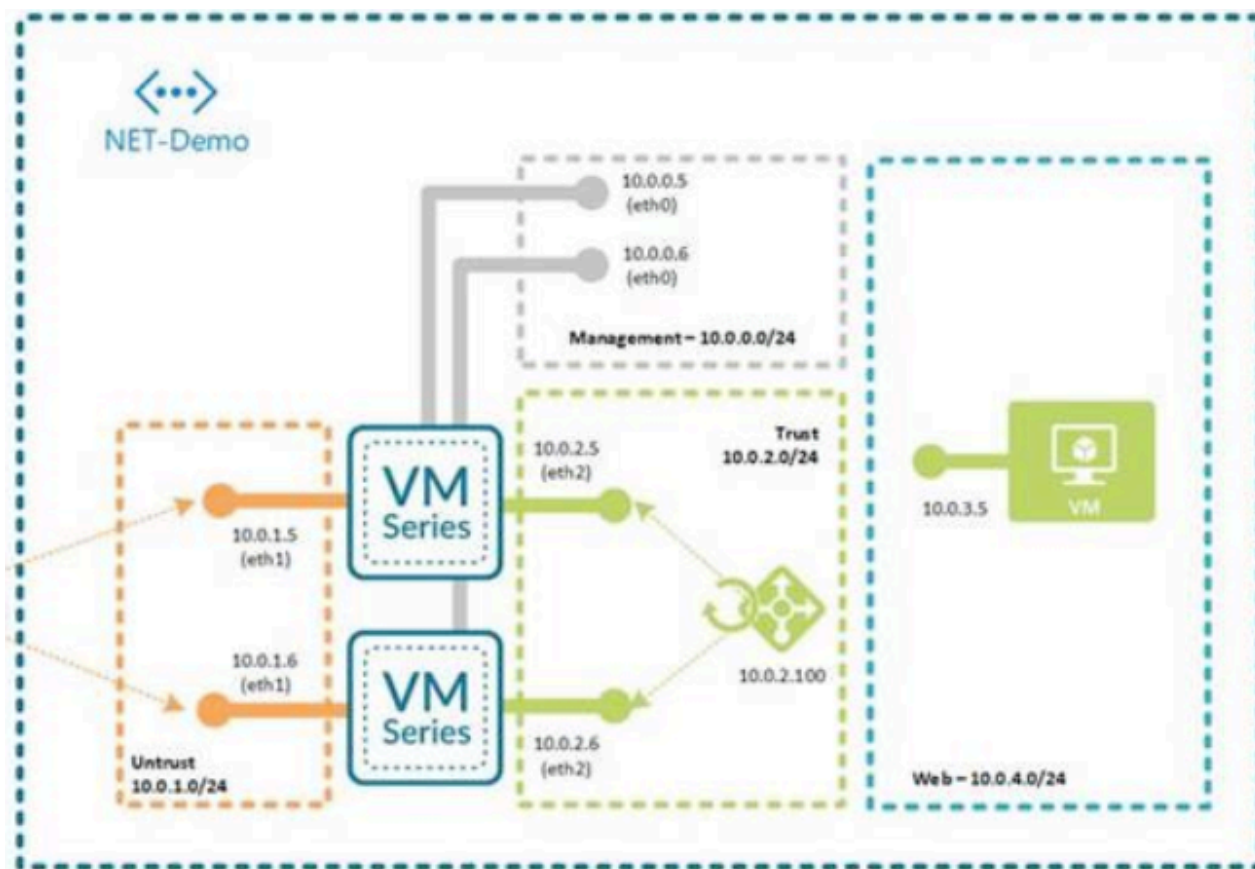


Once configured for PPPoE, an interface can't be assigned a static IP address.

Public Cloud SD-WAN High Availability (HA)

You can now reduce complexity and increase resiliency by adding high availability to your SD-WAN for next-generation firewall public cloud deployments. Configure up to [four IP addresses per SD-WAN](#) interface, allowing you to deploy SD-WAN on public clouds to achieve failover in high availability active/passive configurations. Minimize the downtime and ensure session survivability using the active/passive HA failover in public cloud SD-WAN environments.

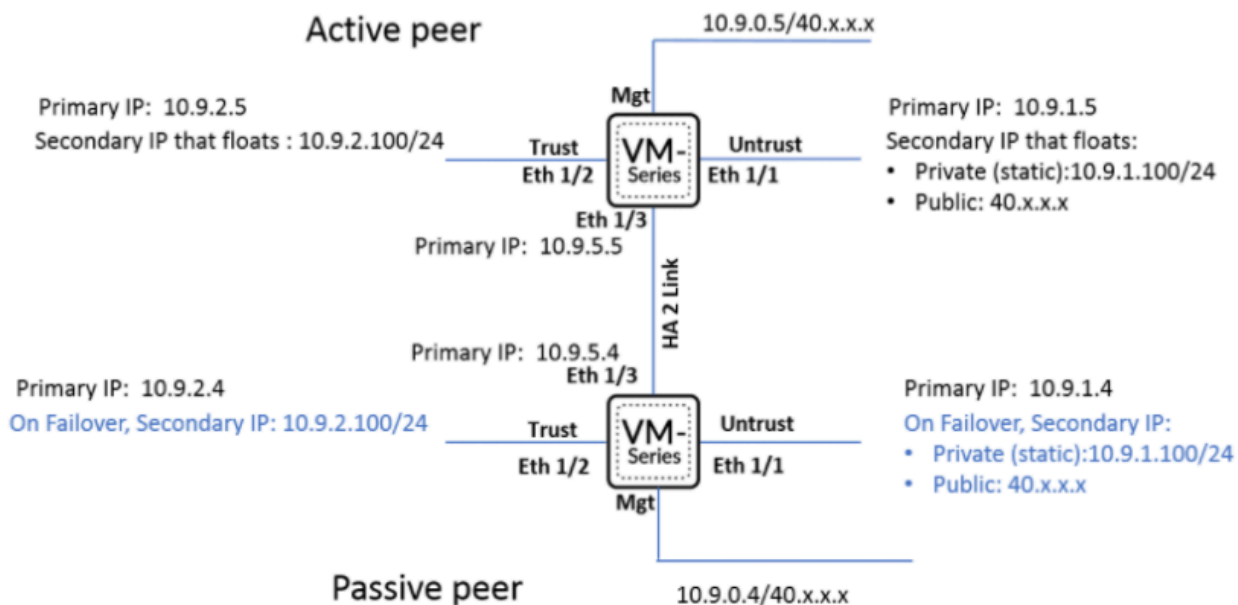
Currently, you can avail this feature on deployments using VM-Series in Azure and AWS public cloud HA environments by configuring a second floating IP address on the SD-WAN interfaces. The floating IP on the SD-WAN interface of the external zone must match with that of the internal zone. In the illustration, observe that 10.0.2.100 is the common floating IP between the external and internal zones during a HA failover.



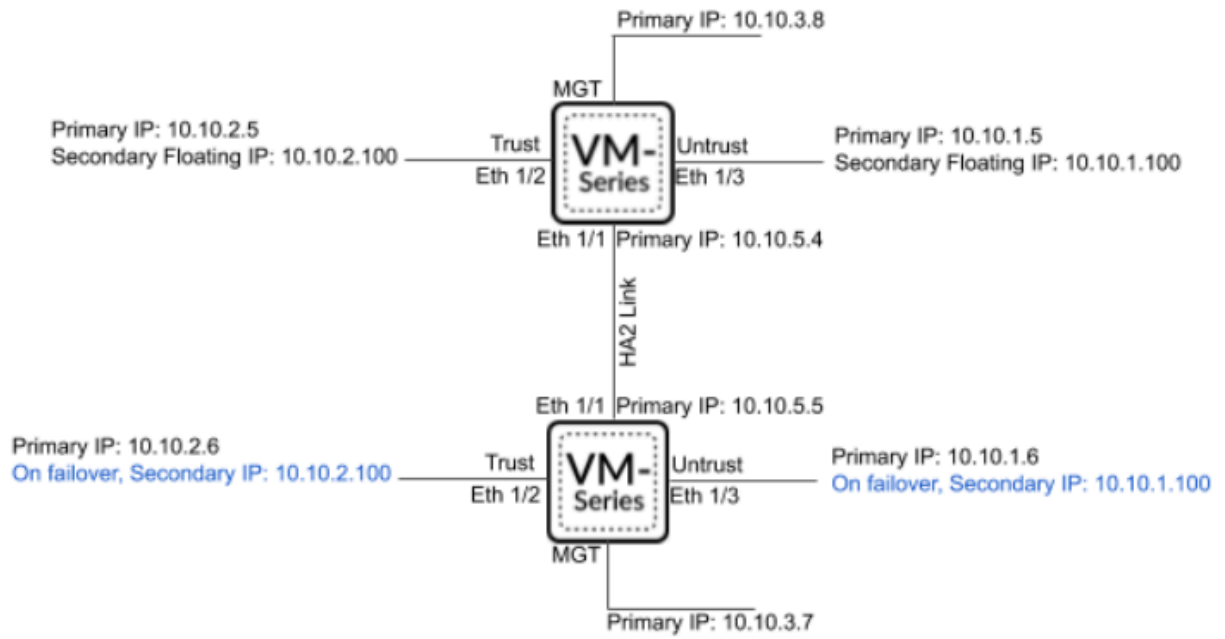


This feature is supported on PAN-OS 11.1.0 and above and on IPv4 addresses only.

The following illustration is an example of [VM-Series deployment in Azure HA A/P](#) topology and shows how the secondary floating IP address is from the same subnet and applied to both trust and untrust zones of the SD-WAN interface.



In AWS instances, you can [configure HA A/P failover](#) using multiple ways, one of which is using a second IP address that acts as the floating IP.

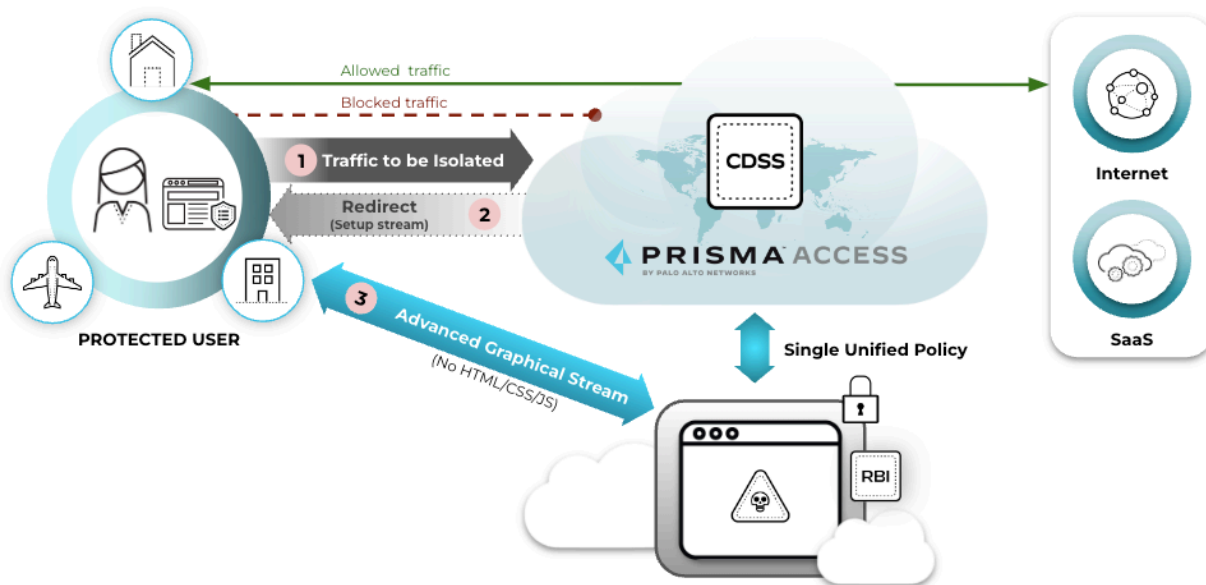


Remote Browser Isolation

Browser and web-based attacks are continuously evolving, resulting in security challenges for many enterprises. Web browsers, being a major entry point for malware to penetrate networks, pose a significant security risk to enterprises, prompting the increasing need to protect networks and devices from zero day attacks. Highly regulated industries, such as government and financial institutions, also require browser traffic isolation as a mandatory compliance requirement.

While most enterprises want to block 100% of attacks by using network security and endpoint security methods, such a goal might not be realistic. Most attacks start with the compromise of an endpoint that connects to malicious or compromised sites or by opening malicious content from those sites. An attacker only needs one miss to take over an endpoint and compromise the network. When this happens, the consequences of that compromise and the impact to your organization can be damaging.

Remote Browser Isolation (RBI) creates a no-code execution isolation environment for a user's local browser, so that no website code and files are executed on their local browser. Unlike other isolation solutions, RBI uses next-generation isolation technologies to deliver near-native experiences for users accessing websites without compromising on security.



RBI is a service that isolates and transfers all browsing activity away from the user's managed devices and corporate networks to an outside entity such as Prisma Access, which secures and isolates potentially malicious code and content within their platform. Natively integrated with Prisma Access, RBI allows you to apply isolation profiles easily to existing security policies. Isolation profiles can restrict many user controls such as copy and paste actions, keyboard inputs, and sharing options like file uploading, downloading, and printing files to keep sensitive data and information secure. 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.

Secure Copy Protocol (SCP) Support

In air-gapped deployments where your devices have no outbound internet connection, you can [enable Secure Copy Protocol \(SCP\)](#) to upload supported file types to an air-gapped device. To perform an SCP upload, you must enable SCP upload functionality for each specific Superuser administrator you want to allow to perform an SCP upload, and isn't a global device configuration. Once SCP uploads are enabled for a Superuser admin, you can use this admin to write scripts and automation for supported file uploads directly to your air-gapped device using the CLI rather than the web interface.

SCP upload are supported from devices running a Microsoft Windows, macOS, or any Linux operating system. SCP upload must be performed from your device command line. SCP applications like WinSCP and FileZilla are not supported. A system log is generated when you successfully SCP a file to your device or if an SCP upload fails for any reason.

You can SCP the following files to your device:


- **PAN-OS Software Versions—/scp/software/**
- **PAN-OS Software Patches—/scp/patch/**
- **Application & Threats Content Updates—/scp/content/**
- **WildFire Content Updates—/scp/wildfire/**
- **Antivirus Content Updates—/scp/anti-virus/**
- **PAN-OS Plugin Versions—/scp/plugin/**
- **XML Configuration Files—/scp/config/**
- **License Key Files—/scp/license/**

Security Checks

Stata Cloud Manager leverages a set of predefined [Best Practice Checks](#) that align with industry-specific standard cybersecurity controls, such as CIS (Center for Internet Security) and NIST (National Institute of Standards and Technology) and custom checks you create based on the specific needs of your organization. These checks evaluate configurations, identifying deviations from best practices or compliance requirements. Previously, we collectively called these **Compliance Checks**.

For this release, we've rolled **Compliance Checks** into **Security Posture Settings**. [Security Posture Settings](#) brings together the functionality of both the AIOps and Cloud Manager security check settings pages.

Security Checks also now let you:

- Create custom checks by cloning select existing checks, making check customization even easier.
 - Exclude checks from being applied to your deployment. In special cases where you want to turn off certain checks for some areas of your deployment or there are reasons specific checks don't make sense for you, instead of disabling them, now you can restrict where checks are applied in your deployment.
-  • The new **Check Exception** feature replaces the "Enable/Disable" functionality of the old settings page.
- *Cloud Manager Support for real-time inline check exemptions isn't available in this release, but we're working hard to bring it to you soon.*
 - Raise an **Alert** (default) for a failed check, or **Block** a configuration with failing checks from being pushed out to your deployment.
 - Get field-level, inline checks during policy creation and device setup that show you where your configuration does not align with best practice or custom checks, inline, so you can take immediate action.

Service Connection Identity Redistribution Management

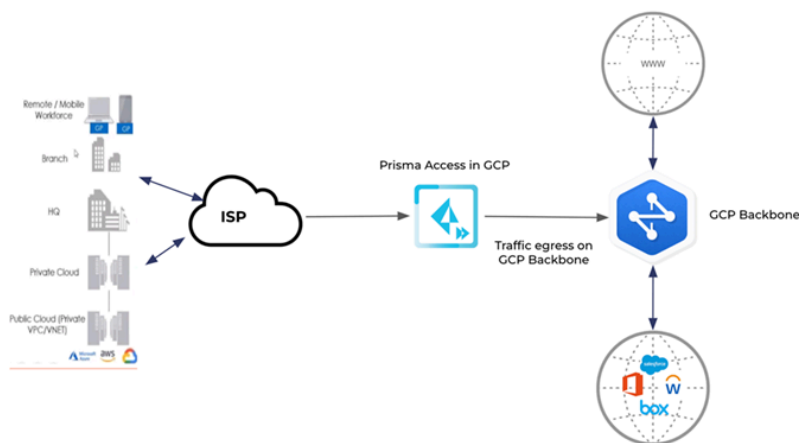
Sometimes, granular controls are needed for user-ID redistribution in particularly large scale Prisma Access deployments. Service Connection Identity Redistribution Management lets you select specific service connections for [identity redistribution](#).

By default, all of your service connections, in order of proximity, are used for identity redistribution. However, you may not know which specific service connections are being used for identity redistribution at a given moment. And, depending on the number of service connections you have and the number of User-ID agents you've configured, this method for identity redistribution can test the limits of your system resources. To solve this, we now give you the option to decide which service connections you want to use for identity redistribution.

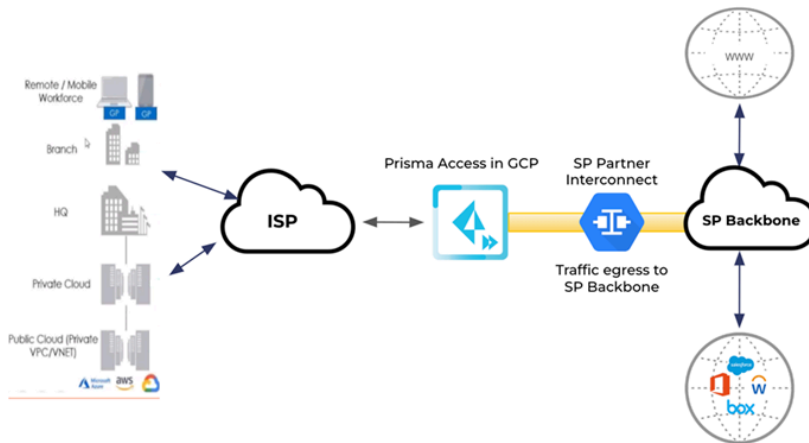
Service Provider Backbone Integration

Integrate Prisma Access with a [service provider \(SP\) backbone](#), which allows you (the SP) to assign specific region and egress internet capabilities to your tenants, providing more granular control over the Prisma Access egress traffic. Without the SP Backbone feature, Prisma Access egress traffic uses public cloud providers for network backbone instead.

The following diagram represents Prisma Access egress traffic without SP Backbone integration.



The following diagram represents Prisma Access egress traffic with SP Backbone integration.



Service Provider Backbone Integration was introduced with Prisma Access 4.1.

From Prisma Access version 5.0, you can allow [inbound flows to other remote networks](#) over the Service Provider (SP) backbone when you configure the non-inbound access remote network.



SP interconnect supports only the following:

- *Mobile users, service connections, and remote networks*
- *GCP Regions*
- *New Prisma Access deployments*
- *Explicit proxy egress traffic*

From March 2024, you can [configure](#), [view](#), and [monitor](#) Service Provider IP address pools to leverage your own IP addresses for Prisma Access egress traffic instead of the egress through public cloud providers.

Session Resiliency for the VM-Series on Public Clouds

Session resiliency allows the VM-Series firewall deployed in a cluster on [AWS](#) or [GCP](#) to maintain session continuity during a failure event. The AWS Gateway Load Balancer (GWLB) and GCP Network Load Balancer (NLB) can detect and deregister unhealthy VM-Series firewalls deployed in a horizontally scalable cluster behind. With session resiliency enabled, the GWLB and NLB can rehash existing traffic sessions flowing toward an unhealthy VM-Series and redirect the traffic to a healthy VM-Series firewall.

To maintain sessions failing over to healthy VM-Series firewalls, you must deploy a Redis cache accessible to your VM-Series firewalls—ElastiCache for Redis for AWS and Memorystore for Redis for GCP. The Redis cache maintains session information. When your load balancer detects an unhealthy VM-Series firewall, the load balancer rebalances traffic to a healthy VM-Series firewall. The healthy VM-Series firewall accesses the Redis cache for session information and continues to inspect and forward the existing traffic.



Traffic inspection of the rehashed traffic flows is Layer 4 only. The VM-Series firewall inspects traffic in new sessions up to Layer 7.

Enable session resiliency on the VM-Series firewall by passing the configuration as part of a bootstrapping `init-cfg.txt` file or in the user data field using the following new parameters.

```
op-command-modes=mgmt-interface-swap
plugin-op-commands=set-sess-ress:True
redis-endpoint=<redis-IP-address:port>
redis-auth=<redis-auth-code>
redis-certificate=
```



Session resiliency can't be enabled on existing VM-Series firewall instances; only on newly deployed instances.

SNMP Network Discovery for IoT Security

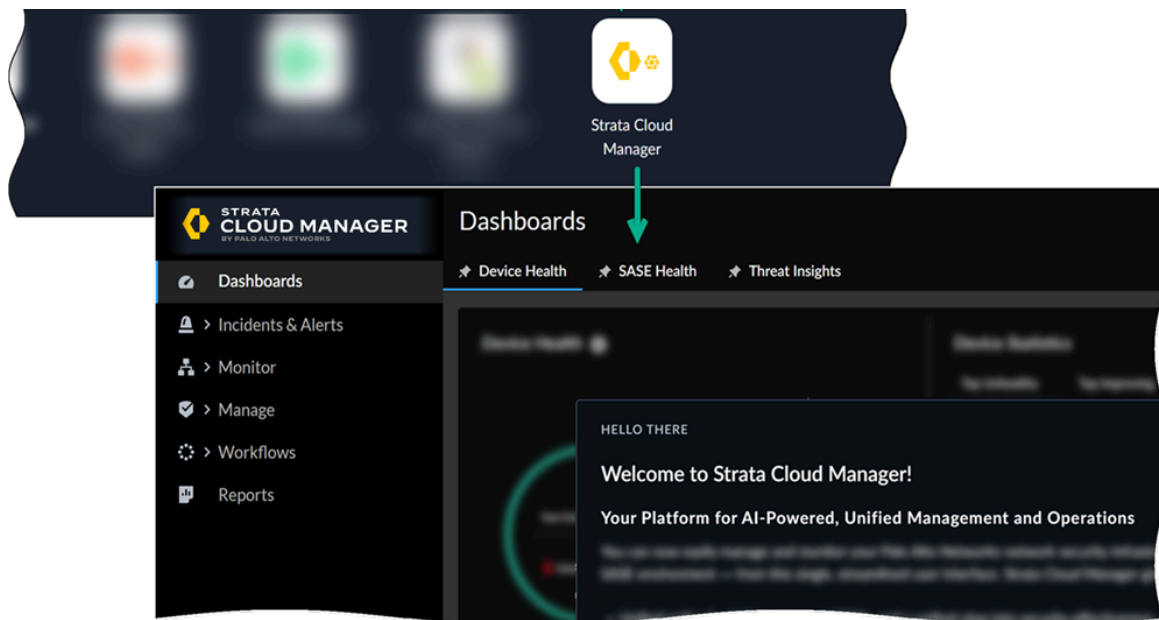
To identify devices on the network, IoT Security requires network traffic metadata for analysis. Palo Alto Networks firewalls extract and log this metadata when they apply Security policy rules that have logging enabled. The firewalls send the logs to the logging service. The logging service then streams the metadata to IoT Security, which uses AI and machine learning to automatically discover and identify network-connected devices, dynamically construct an asset inventory, detect device vulnerabilities, and determine a baseline of acceptable network behaviors that IoT Security recommends next-generation firewalls allow in Device-ID policy rules.

However, depending on where the firewalls are placed, they might not have visibility into all network traffic, resulting in device discovery gaps and lower efficacy in identifying devices, monitoring behaviors, and enforcing Device-ID rules. When firewalls don't receive traffic from all devices, they can still gather IP address-to-MAC address bindings and additional network data by using SNMP to query switches and other forwarding devices throughout the network.

When using SNMP to query network switches, firewalls first develop a network topography by requesting the Link Layer Discovery Protocol (LLDP) neighbors and Cisco Discovery Protocol (CDP) neighbors of one switch (the entry point switch) and then repeating the request with neighboring switches and child switches one by one throughout the network. After obtaining a list of switches throughout the network, or within a limited area of the network, the firewalls next query each one for its ARP table as well as other information. The ARP table contains the IP address-to-MAC address binding information for the devices connected through the switch to the network. Other device details for which firewalls query include the physical interfaces or ports on the switch to which devices connect, their VLANs and subnets, and DHCP and DNS server IP addresses. After the firewalls receive this information, they create logs and send them through the logging service to IoT Security for analysis. By using SNMP to collect more data from switches and forwarding devices in parts of the network that firewalls don't have visibility into, you enable IoT Security to form a greater view of the devices on the network and expand its services to even more devices.

Strata Cloud Manager: Application Name Updates

The application tile names on the hub for Prisma Access, Prisma SD-WAN, and AIOps for NGFW (the premium app only) are now changed to **Strata Cloud Manager**. With this update, the application URL has also changed to stratacloudmanager.paloaltonetworks.com, and you'll also now see the **Strata Cloud Manager** logo on the left navigation pane.



Moving forward, continue using the Strata Cloud Manager app to manage and monitor your deployments.

- → [Get started with Strata Cloud Manager](#)
- → [More on these changes](#)

Support for Strata Logging Service Switzerland Region

Prisma Access supports the Switzerland [Strata Logging Service region](#).

TACACS+ Accounting

If you use a Terminal Access Controller Access-Control System Plus (TACACS+) server for user authorization and authentication, you can now [log accounting information](#) to fully make use of the authentication, authorization, and accounting (AAA) framework that is the basis for TACACS+.

The TACACS+ Accounting feature allows you to use a TACACS+ server profile to record user behavior, such as when a user started using a specific service, the duration of use for the service, and when they stopped using the service. The TACACS+ Accounting feature helps to create logs and records of the initiation and termination of services, as well as any services in progress during the user's session, that you can then use later if needed for auditing purposes.

When you configure and enable an Accounting server profile, the TACACS+ server provides information to the firewall about the initiation, duration, and termination of services by users. The firewall also generates a log when the TACACS+ server successfully provides the accounting records to the server that you configure in the profile. If the firewall is unable to successfully send the accounting records to any of the servers in the profile, the firewall generates a critical severity alert to the system logs.

By using your existing TACACS+ server, you can now configure it to provide even more information about the use of services by users on your network, giving you even more robust visibility into user activity on your network.

Throughput Enhancements for Web Proxy

The throughput for both the explicit and transparent components of the [web proxy](#) has been significantly improved, resulting in better performance at scale.

TLSv1.3 Support for Administrative Access Using SSL/TLS Service Profiles

You can now configure TLSv1.3 in [SSL/TLS service profiles](#) to secure administrative access to management interfaces. TLSv1.3 delivers several performance and security enhancements, including shorter SSL/TLS handshakes and more secure cipher suites. In an SSL/TLS service profile, you can select TLSv1.3 as the minimum or maximum supported protocol version for connections to the management interface. Selecting TLSv1.3 automatically enables the following TLSv1.3 cipher suites:

- TLS-AES-128-GCM-SHA256
- TLS-AES-256-GCM-SHA384
- TLS-CHACHA20-POLY1305-SHA256



TLS-CHACHA20-POLY1305-SHA256 is not supported in FIPS-CC mode.

However, you can deselect any key exchange algorithms, encryption algorithms, or authentication algorithms as needed. In addition to offering TLSv1.3 support, SSL/TLS service profiles now enable customization of the key exchange algorithms, encryption algorithms, and authentication algorithms supported.

Traceability and Control of Post-Quantum Cryptography in Decryption

Today, [post-quantum cryptography \(PQC\)](#) algorithms and hybrid PQC algorithms (classical and PQC algorithms combined) are accessible through open-source libraries and integrated into web browsers and other technologies. Traffic encrypted by PQC or hybrid PQC algorithms cannot be decrypted yet, making these algorithms vulnerable to misuse. To address these concerns, Palo Alto Networks firewalls now [detect, block, and log the use of PQC and hybrid PQC algorithms](#) in TLSv1.3 sessions. Successful detection, blocking, and logging of PQC and hybrid PQC algorithms depends on your SSL Decryption policy rules.

If SSL traffic matches an SSL Forward Proxy or SSL Inbound Inspection Decryption policy rule, the firewall prevents negotiation with PQC, hybrid PQC, and other unsupported algorithms. Specifically, the firewall removes these algorithms from the ClientHello, forcing the client to negotiate with classical algorithms. (For a list of supported cipher suites, see [PAN-OS 11.1 Decryption Cipher Suites](#).) This enables continuous decryption and threat identification through deep packet inspection. If the client strictly negotiates PQC or hybrid PQC algorithms, the firewall drops the session. In the Decryption log for the dropped session, the error message states that the "client only supports post-quantum algorithms." To see details of successful or unsuccessful TLS handshakes in the Decryption logs, enable both options in your Decryption policy rules.

If SSL traffic matches a "no-decrypt" Decryption policy rule or doesn't match any Decryption policy rules, the firewall allows negotiation with PQC or hybrid PQC algorithms. However, details of sessions that negotiate these algorithms are available in Decryption logs only when session traffic matches a "no-decrypt" Decryption policy rule.

Additionally, new threat signatures offer additional visibility into the use of PQC and hybrid PQC algorithms in your network. These signatures monitor ServerHello responses and trigger alerts for SSL sessions that successfully negotiate with the most commonly known PQC and hybrid PQC algorithms. A Threat Prevention license is required to receive alerts.

Traffic Replication Remote Network and Strata Cloud Manager Support

In addition to providing a copy of the traffic generated by mobile users, [traffic replication](#) support for Remote Networks provides a similar function for the traffic generated by the branches. This support allows you to have complete visibility for all use cases, along with consistency in the way the traffic is being captured. The copy of the remote networks traffic is shared from the same storage buckets as the mobile users traffic, so existing customers do not have to modify the current deployments. This option is fully configurable and you have the ability to decide if for a certain location you need Traffic Replication enabled for mobile users, remote networks, or both.

Traffic Replication configuration support is added for [Cloud Managed Prisma Access](#) and [Strata Cloud Manager](#).

VM-Series Device Management

This release adds support for a bootstrapping process that allows you to configure newly deployed firewalls without manually configuring them prior to deployment. Previously, a firewall image was created for your cloud environments that required you to manually include information such as DNS entries and IP addresses in the `init.cfg` file.

This new process associates the firewall with a Panorama management host to automate the onboarding and configuration of your software firewall. With this functionality, the bootstrapping process:

- Automatically instantiates, onboards, and configures the firewall instance without prior knowledge of the firewall serial number.
- Automatically onboards the Strata Cloud Manager tenant, from which the tenant receives the initial configuration and becomes fully operational without manual intervention.

Create the bootstrap package with the following fields:

- **panorama-server**. Use this field to specify cloud management for your Panorama host. This field initiates a TLS connection to the Strata Cloud Manager service edge. For example, `panorama-server=cloud`. Values other than `cloud` are interpreted as a Panorama Internet Protocol or FQDN, and will initiate a Panorama management connection. A value defined for `panorama-server-2` is ignored when `panorama-server=cloud`.
- **dgname**. This field is used to define the Cloud Management folder in which the firewall is mapped.
- **vm-series-auto-registration-pin-id**. Include the VM-Series registration PIN ID. This automates the process of instantiating the firewall instance by establishing the connection to the Strata Cloud Manager service edge.
- **vm-series-auto-registration-pin-value**. Include the VM-Series registration PIN VALUE to automate the process of instantiating the firewall instance by establishing the connection to the Strata Cloud Manager service edge.



The PIN ID and PIN VALUE fields are used to request a Therman certificate. This certificate is used to authenticate the device and build a secure connection to the cloud service, such as Strata Cloud Manager.

View and Monitor App Acceleration

When your users access apps, they can experience poor app performance due to decreased throughput. This condition can be caused by degraded wireless connectivity, network congestion, and other factors. These networking issues can adversely affect the employee experience and can reduce their productivity. App Acceleration addresses the causes of poor app performance and acts in real-time to boost throughput while maintaining best-in-class security, dramatically improving the user experience for Prisma Access GlobalProtect and Remote Network users.

You can [view and monitor App Acceleration](#) to see details about accelerated applications in your environment. In Strata Cloud Manager, select **Insights > Applications** to view details about all accelerated applications.

View and Monitor Remote Browser Isolation

Remote Browser Isolation (RBI) creates a no-code execution isolation environment for a user's local browser, so that no website code and files are executed on their local browser. Unlike other isolation solutions, RBI uses next-generation isolation technologies to deliver near-native experiences for users accessing websites without compromising on security. [View and monitor RBI](#) to get comprehensive visibility across your network traffic and for RBI. Gain visibility into your RBI deployment by viewing metrics such as the number of active RBI users, trends, connectivity status, RBI location status, traffic measurements, and license consumption.

Virtual Routing Forwarding for WAN Segmentation

Prisma SD-WAN supports Virtual Routing and Forwarding (VRFs) for WAN segmentation of application traffic. Network segmentation will help achieve isolation of application traffic for the same customer between different business units or customers who share the same WAN infrastructure by carrying the segment identifier over the WAN overlay.

WAN Segments are first defined in global VRF profiles. These VRF profiles are then bound to sites. After that, interfaces are configured with the appropriate VRF. When traffic enters the interface, it only considers destinations with the same VRF locally or across the fabric. If the traffic is destined to go across the fabric, it gets automatically encapsulated with a unique identifier specific to that VRF. Once the traffic reaches the remote ION, it can egress onto the VRF that is appropriately configured.

October 2023

Review all the new features we've introduced across the NetSec platform in October 2023.

Cisco Catalyst SD-WAN Integration

Previously, to secure Cisco Catalyst SD-WAN, formerly known as Viptela SD-WAN, you should create remote networks and IPsec tunnels manually. Now, you can onboard a remote network using IPsec tunnels between Cisco Catalyst SD-WAN and Prisma Access automatically. Contact your Palo Alto Networks Account representative to enable this functionality. After you enable this functionality, configure the settings to establish the connection between Prisma Access and Cisco Catalyst SD-WAN. View the discovered sites that are eligible for the integration, and enable them accordingly. This creates remote networks and establishes IPsec tunnels. Ensure to follow all the requirements and prerequisites before you enable this functionality. See [Integrate Prisma Access with Cisco Catalyst SD-WAN](#) for more information.

September 2023

Review all the new features we've introduced across the NetSec platform in September 2023.

Cloud IP-Tag Collection

Enforcing your security policy consistently across all the firewalls in your network relies on those firewalls having the most up-to-date identity information from your sources, such as cloud-based identity management systems. With the array of management systems and large numbers of users and devices, it can often be time-consuming and difficult to correlate identity information with its originating sources and ensure that it was provided to all necessary devices.

You can now use Strata Cloud Manager with the Cloud Identity Engine to manage IP address-to-tag (also known as IP-tag) mappings and simplify your security policy by creating tag-based rules. When you [configure a cloud connection](#) in the Cloud Identity Engine to your cloud-based identity management system (either Azure or AWS), you can use the Cloud Identity Engine to collect IP-tag mappings.

You can see all of your IP-tag mappings, as well as their associated sources, in the Cloud Identity Manager. Using filters to highlight the most relevant information, you can quickly identify issues with your security policy, such as a source that is currently unavailable. You can then use the Strata Cloud Manager to create tag-based security policy using [dynamic address groups](#) and distribute it to the firewalls in your network to ensure they have the latest information needed to consistently enforce security policy. You can also share the IP-tag mappings with other firewalls in your network by using [User Context segments](#) in the Cloud Identity Engine.

By leveraging the capabilities of Strata Cloud Manager with the identity information that the Cloud Identity Engine provides, you can more easily create and manage your security policy using tags.

Config Version Snapshot

Manage configuration pushes for your cloud managed NGFWs alongside your Prisma Access deployments with [Config Version Snapshots](#).

Evaluate configuration pushes, compare your candidate configuration to previously pushed configurations, and rollback recent changes in the event of any unintended consequences of a recent push.

Load previous configurations to use as candidates for your configuration push and make further changes to expand the scope of the original configuration. Restore previous configurations to immediately rollback the changes of a recent configuration push.

Review the devices or deployments impacted or targeted by your configuration pushes for the full scope of the changes.

Create a Custom Path Quality Profile

Create a custom path quality profile on Strata Cloud Manager for firewalls leveraging [SD-WAN](#). A path quality profile allows you to define unique network quality requirements for business-critical and latency-sensitive applications, application filters, application groups, services, service objects and service group objects that have requirements based on latency, jitter, and packet loss percentage. Applications and services can share a path Quality profile. Specify the maximum threshold for each parameter, above which the firewall considers the path deteriorated enough to select a better path.

The firewall treats the latency, jitter, and packet loss thresholds as OR conditions, meaning if any one of the thresholds is exceeded, the firewall selects the new best (preferred) path. Any path that has latency, jitter, and packet loss less than or equal to all three thresholds is considered qualified and the firewall selected the path based on the associated [Traffic Distribution profile](#).

Add Path Quality Profile

The screenshot shows a configuration form for a custom path quality profile. The form is organized into sections for Name, Latency, Jitter, and Packet Loss. Each section contains a threshold value, a unit, a range, and a sensitivity selection.

Parameter	Threshold	Unit	Range	Sensitivity
Name *	custom-path-quality-profile			
Latency	100	ms	[10 - 3000]	Low (), Medium (x), High ()
Jitter	100	ms	[10 - 2000]	Low (), Medium (x), High ()
Packet Loss	1	%	[1 - 100]	Low (), Medium (x), High ()

Delete a Snippet

Snippets are configuration objects, or groups of configuration objects, that can be associated with your folders, firewalls, and Prisma Access deployments. They are used to standardize configurations, allowing you to push changes quickly to all areas. Snippets are classified in two ways: Predefined and Custom. Predefined snippets are available to all Strata Cloud Manager users and can be used to quickly get your new firewalls and deployments up and running with best practice configurations. Custom snippets are any snippets created by administrators.

Delete custom [snippets](#) that are no longer associated with any deployments, firewalls, or folders to keep your configuration scope organized.

Unused snippets can be deleted straight from the configuration scope view.

Deleting custom snippets is supported. Predefined snippets available in Strata Cloud Manager can't be deleted.

Web Proxy for Cloud-Managed Firewalls



Prisma Access has its own, separate [method of configuring explicit proxy](#). This new feature applies only to cloud-managed firewalls.

You can now [configure a web proxy on the firewalls you're managing with Strata Cloud Manager](#). That means that if you plan to use an NGFW as a proxy device to secure your network, you can now configure your proxy settings across your deployment from a simple, unified management interface.

This interface includes an in-app proxy auto-configuration (PAC) file editor so that you can edit your proxy settings and modify your PAC file all in one place whenever network changes arise.

The web proxy supports two methods for routing traffic:

- For the [explicit proxy](#) method, the request contains the destination IP address of the configured proxy and the client browser sends requests to the proxy directly. You can use one of following methods to authenticate users with the explicit proxy:
 - Kerberos, which requires a web proxy license.
 - SAML 2.0, which requires a Prisma Access license and the add-on web proxy license.
- For the [transparent proxy](#) method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules, which you can configure using Transparent Proxy Rules in Strata Cloud Manager. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).

You can push web proxy configurations to the following platforms:

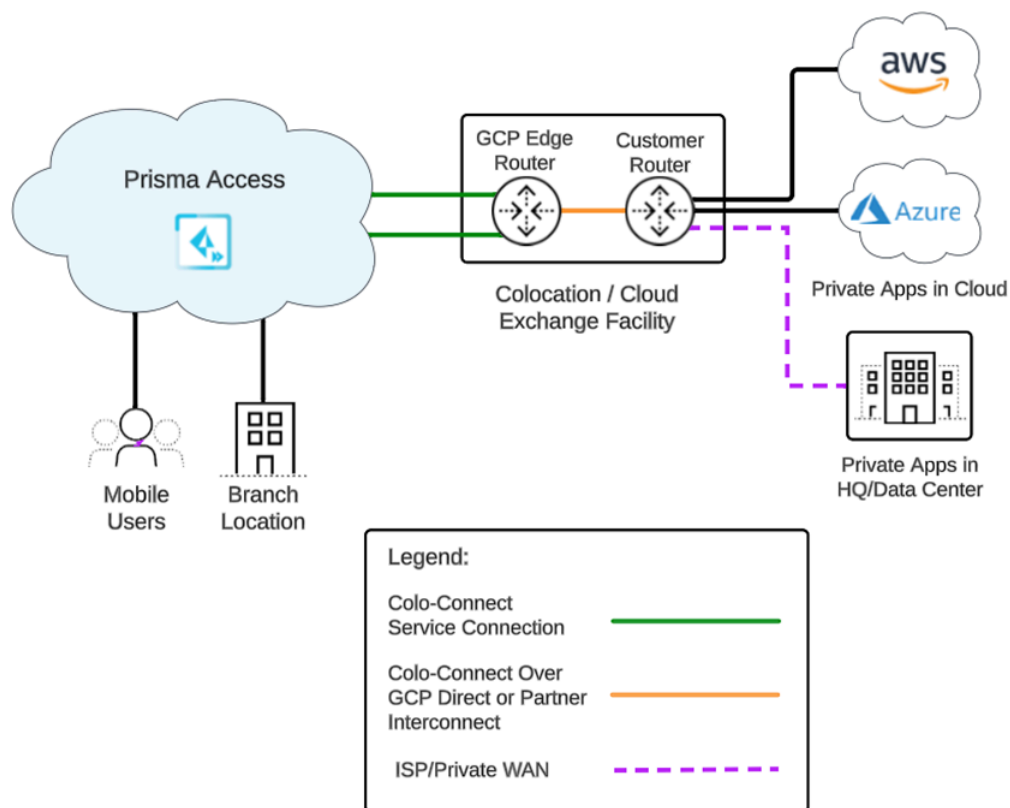
- PA-1400
- PA-3400
- VM Series (with a minimum of four vCPUs)

High-Bandwidth Private App Access with Colo-Connect

Does your organization require high-bandwidth (more than 10 Gbps) access between its network infrastructure and Prisma Access at multiple locations as part of your hybrid multicloud strategy? Perhaps you've thought about aggregating multiple service connections to achieve high bandwidth, but you're concerned about scalability. If so, [Colo-Connect](#) has you covered.

Today, large enterprises are building Colo-based performance hubs to reach private applications in hybrid, multicloud architectures because of the high-bandwidth and low-latency requirements. Typically, these hubs include interconnects to one or more cloud providers and connections to the on-premises data centers over a private or leased WAN. Performance hubs can route traffic between the public cloud and on-premises infrastructure at high speed, and are resilient because of the underlying interconnect infrastructure.

Colo-Connect builds on the Colo-based performance hub concept, offering high-bandwidth (10-20 Gbps) low-latency connections, seamless Layer 2/3 connectivity to Prisma Access from existing performance hubs. The following figure shows Prisma Access being onboarded in a GCP instance using service connections and cloud interconnects. This setup limits exposure to the internet and allows the use of private connections for private application connectivity.



Colo-Connect allows you to use Prisma Access to secure private apps using a cloud interconnect that can provide high-bandwidth service connections using the following capabilities:

- High bandwidth (up to 20-Gbps) throughput per region for private application access
- Support for [Dedicated and Partner interconnects](#) using Google Cloud Platform (GCP)
- Support for multiple VLAN attachments (up to 20) per interconnect link

- Redundant connectivity support per region

Integrate Prisma Access with Microsoft Defender for Cloud Apps

[Integrate Prisma Access with Microsoft Defender for Cloud Apps](#) to sync unsanctioned applications and block them inline using Prisma Access automatically.

After you integrate Microsoft Defender for Cloud Apps with Prisma Access, Prisma Access creates a block security policy for URLs that are blocked in Microsoft Defender for Cloud Apps. You can view the list of unsanctioned applications after configuring the integration settings. The Prisma Access-Microsoft Defender for Cloud Apps integration enables you to gain visibility and to discover all cloud applications and shadow IT applications being used as well as provide closed loop remediation for unsanctioned applications.

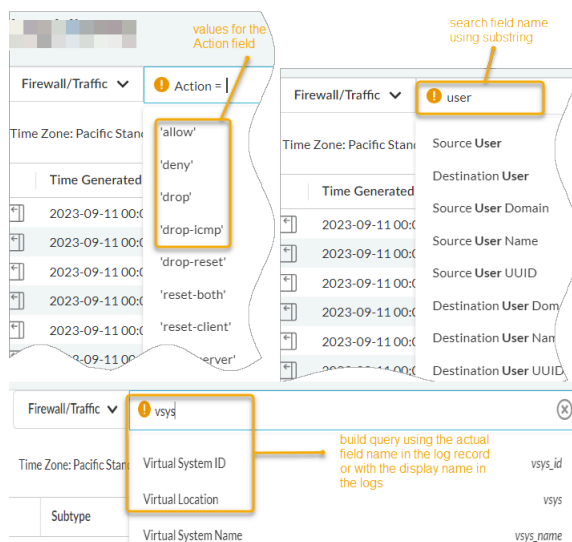
Introducing ADEM APIs

The ADEM APIs provide access to ADEM data for real-time and historical monitoring of user, applications, and sites across your deployment. Each API is illustrated with an example highlighting the lines in the API Response code that correspond to the area in the UI where the data appears. There is an FAQ section in the guide that provides details on the usage of parameters.

Log Viewer Usability Enhancements

You can now use enhanced filtering and viewing capabilities to search and view relevant logs easily. The enhancements include:

- Search in the query builder shows autosuggestions most relevant to the search string.
- Search in the query builder shows autosuggestions most relevant to the search string.
- The query builder suggests all the supported values for the field to build the query.
- Search field names using substrings (for example, search with the string 'user' returns suggestions such as source_user, destination_user).
- Search for a field based on the display name in the log table and not just the actual field name in the log record. You can create a query using both field names.
- Press Shift + Enter to start a new line in the query builder, and press Enter to submit a query.



New Predefined BGP Redistribution Profile

Auto VPN (Manage > Configuration > NGFW and Prisma Access > Global Settings > Auto VPN) allows you to configure secure connectivity between Strata Cloud Manager and your managed firewalls using **SD-WAN**. The routing protocol used by Auto VPN is the Border Gateway Protocol (BGP) Redistribution profile and determines the network reachability based on IP prefixes available within autonomous systems (AS). Firewalls added to a VPN cluster are now automatically assigned the predefined All - Connected - Routes BGP Redistribution profile by default. The All - Connected - Routes BGP Redistribution broadcasts all connected routes to the VPN peers in the cluster. Additionally, this BGP Redistribution profile not only provides the tunnel and route peering configuration required for connectivity, but also completes route advertisements to allow for branch to branch communication.

Add VPN Clusters

General

Name:
Alphanumeric string that can contain hyphen

SD-WAN: Enable

Hub devices | Branch devices

Hub devices (2) Search Delete

<input type="checkbox"/>	Prio...	Device Name	Site Name	Router	BGP Redistribution Profile	DIA VPN	Link Tag	Interfaces
<input type="checkbox"/>	1	Thiyagu_h1_169_172	Thiyagu_h1_169_172	HUB1_Snippt_LR	All-Connected-Routes	<input type="checkbox"/> Disabled		Interface1: \$eth2 Interface2: \$eth3 [Private]
<input type="checkbox"/>	1	Thiyagu_hub2_169_96	Thiyagu_hub2_169_96	HUB2-LR	All-Connected-Routes	<input type="checkbox"/> Disabled		Interface1: \$eth8 Interface2: \$eth9 [Private]

New Prisma Access Cloud Management Location

Prisma Access Cloud Management can now be deployed in the Japan [region](#).

Refresh Pre Shared Keys for Auto VPN

Auto VPN allows you to configure secure connectivity between Strata Cloud Manager and your managed firewalls using **SD-WAN**. Peers in the VPN cluster use a pre-shared key to mutually authenticate each other. Strata Cloud Manager now allows you to refresh the pre shared keys used for authenticating VPN tunnels for existing VPN clusters (**Manage > Configuration > NGFW and Prisma Access > Global Settings > Auto VPN**).

Config Push to refresh the Pre-Shared Key ×

Refreshing the Pre-shared key will generate a new security association (SA) for every SD-WAN firewall in the VPN cluster. This may cause a service disruption. If you are OK, check the acknowledgment service disruption, then click the Push button.

Acknowledge the possible service disruption

VPN Cluster thiyagu-sdwan1

Targets (4) Search

Target	Parent Location
Thiyagu_S1_168_162	All > Firewall > Thiyagu SDWAN > Spoke1
Thiyagu_S2_168_126	All > Firewall > Thiyagu SDWAN > Spoke2
Thiyagu_h1_169_172	All > Firewall > Thiyagu SDWAN > HUB1
Thiyagu_hub2_169_96	All > Firewall > Thiyagu SDWAN > HUB2

Cancel Push

Strata Logging Service Regional Support

You can now send Prisma Access Cloud Management logs to Strata Logging Service instances in the following regions:

- Israel
- Indonesia
- Qatar
- Taiwan

Troubleshoot NGFW Connectivity and Policy Enforcement Anomalies

Troubleshoot these networking and identity features—track down and resolve connectivity issues or policy enforcement anomalies:

- [NAT](#)
- [DNS Proxy](#)
- [User Groups](#)
- [Dynamic Address Groups](#)
- [Dynamic User Groups](#)
- [User ID](#)

Network Troubleshooting for NAT and DNS Proxy

Troubleshoot your NGFWs from Strata Cloud Manager without having to move between various firewall interfaces. If you experience connectivity issues after deploying and configuring your NGFWs, you can get an aggregate view of your routing and tunnel states, and drill down to specifics to find anomalies and problematic configurations.

Identity and Policy Troubleshooting

Troubleshoot your identity-based policy rules and dynamically defined endpoints. Check the status of specific NGFWs and expose possible mismatches between how you expect a policy to work and its actual enforcement behavior.

August 2023

Review all the new features we've introduced across the NetSec platform in August 2023.

Credential Phishing Prevention Support

You can [configure credential phishing prevention](#) to restrict the websites user can submit corporate credentials to and prevent successful phishing attacks. This task involves selecting the [credential detection method](#) that the firewall uses and specifying the actions the firewall takes when it detects corporate credential submissions to allowed URL categories. The firewall enforces the following actions: alert, allow, block, or continue. The continue option results in the display of an anti-phishing response page that warns users against supplying their credentials to certain websites and requires them to click "continue" before they proceed to the requested website.

Each credential detection method requires a different User-ID™ configuration and varies in detection ability. For example, the [domain credential filter method](#) requires installation of the Windows User-ID agent and User-ID credential service add-on on a read-only domain controller (RODC). These tools enable the firewall to detect valid corporate username and password pairs and verify that the IP address associated with a login attempt matches an IP address-to-username mapping. The other methods focus on username detection.

Prisma Access PAC File Endpoint for Explicit Proxy

Palo Alto Networks will begin rolling out a new endpoint for the Proxy Auto-Configuration (PAC) file used for Explicit Proxy to make it easier for you to enable access to PAC files. This new endpoint is hosted by Palo Alto Networks instead of the current AWS S3 endpoint. When you modify the PAC file after September 1, 2023, you will see the **PAC File URL** with the updated endpoint.

No immediate action is required if you are using PAC file directly, as you can continue to use the current AWS S3-based PAC File URL until Mar 31, 2024. We suggest migrating to use the PAC file URL with updated endpoint before March 31, 2024 at your convenience.

If you are using [GlobalProtect in proxy Mode](#) or [tunnel and proxy mode](#) and you don't allow your devices to access all domains under [prismaaccess.com](#) (for example, because of a third-party VPN split tunnel or firewall rule), please allow your devices to access the PAC file endpoint ([store.swg.prismaaccess.com](#)) to avoid interruptions. Alternatively, you can override the PAC File URL in the Global Protect App Settings to use the S3-based PAC file URL until you are able to make changes to allow access to the new endpoint. Please migrate to new endpoint before March 31, 2024.

Please refer to [the PAC file guidelines](#) for additional information, including IP addresses that you need to allow on your endpoints so that they can reach the PAC file at the new URL.

After the PAC file updates, if you want to refer to the previous URL, you can replace the FQDN of the new URL with the previous one. The exact FQDN that you use depends on whether you have changed your PAC file after Prisma Access 4.1. For example:

New URL	Previous URL
<a href="https://store.swg.prismaaccess.com/pac/<tenant-id>/<uuid>.pac">https://store.swg.prismaaccess.com/pac/<tenant-id>/<uuid>.pac	https://pac-files-us-west-2-prod.s3.us-west-2.amazonaws.com/<tenant-id>/<uuid>.pac OR https://pac-files-prod.s3.us-west-2.amazonaws.com/<tenant-id>/<uuid>.pac

<tenant-id> and <uuid> remain the same across URLs.

User-Based Enforcement for Explicit Proxy Kerberos Authentication

You can now implement user identity-based visibility and control using security policies for undecrypted HTTPS traffic when a user or system [authenticates using Kerberos](#). In addition, administrators no longer need to configure Trusted Source Addresses when configuring Kerberos authentication for undecrypted HTTPS traffic. This ensures consistent user visibility and policy enforcement for all HTTP(S) traffic even in cases when client IP addresses change, such as if your branch employs dynamic egress IP addresses.

Formerly, you could authenticate decrypted and undecrypted traffic, but could only enforce user-based controls for decrypted HTTPS traffic. With this new feature, all HTTP-based traffic (undecrypted HTTPS, decrypted HTTPS, and HTTP traffic) can authenticate and undergo user-based controls.

Additionally, to allow undecrypted HTTPS traffic, users or systems had to come from static IP addresses configured as Trusted Source Addresses. With this feature, that is no longer necessary, which simplifies initial configuration and supports the use case in which your branch locations have dynamic IP addresses.

Local Zones

Local zones place compute, storage, database, and other services close to large population and industry centers. These locations have their own compute locations.

Keep in mind the following guidelines when deploying local zones:

- Local zone locations do not use Palo Alto Networks registered IP addresses.
- 1 Gbps support for remote networks is not supported.
- Remote network and service connection node redundancy across availability zones is not available if you deploy them in the same local zone, as both nodes are provisioned in a single zone.
- These local zones do not use Palo Alto Networks registered IPs. If you have problems accessing URLs, [report the website issue](#) using <https://reportasite.gpcloudservice.com/> or reach out to Palo Alto Networks support.

DLP Support for AI Applications

ChatGPT is the fastest growing consumer application in history, with 100 million monthly active users just two months after launch. Many organizations may be surprised to learn that their employees are already using AI-based tools to streamline their daily workflows, potentially putting sensitive company data at risk. Software developers can upload proprietary code to help find and fix bugs, while corporate communications teams can ask for help in crafting sensitive press releases.

To safeguard against the growing risk of sensitive data leakage to AI apps and APIs, we are excited to announce a new set of capabilities to secure ChatGPT and other AI apps as part of our Next-Generation CASB solution that includes: Comprehensive app usage visibility for complete monitoring of all SaaS usage activity, including employee use of new and emerging generative AI apps that can put data at risk. Granular SaaS application controls that safely enable employee access to business-critical applications, while limiting or blocking access to high risk apps—including generative AI apps—that have no legitimate business purpose.

While AI apps can significantly boost productivity and creative output, they also pose a serious data security risk to modern enterprises. Enterprise Data Loss Prevention (E-DLP) provides advanced data security that provides ML-based data classification and data loss prevention to detect and stop company secrets, personally identifiable information (PII), and other sensitive data from being leaked to generative AI apps by well-intentioned employees.

[Use Enterprise DLP to safeguard against GPT language model data leakages](#) today.

July 2023

Review all the new features we've introduced across the NetSec platform in July 2023.

June 2023

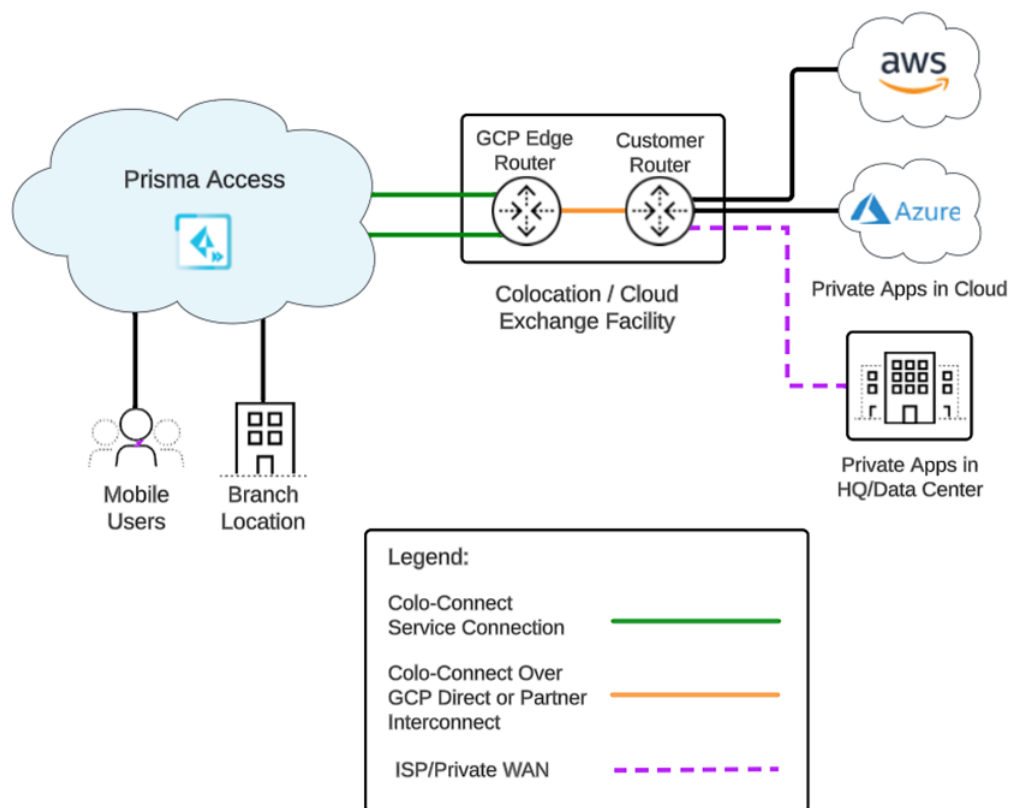
Review all the new features we've introduced across the NetSec platform in June 2023.

High-Bandwidth Private App Access with Colo-Connect

Does your organization require high-bandwidth (more than 10 Gbps) access between its network infrastructure and Prisma Access at multiple locations as part of your hybrid multicloud strategy? Perhaps you've thought about aggregating multiple service connections to achieve high bandwidth, but you're concerned about scalability. If so, [Colo-Connect](#) has you covered.

Today, large enterprises are building Colo-based performance hubs to reach private applications in hybrid, multicloud architectures because of the high-bandwidth and low-latency requirements. Typically, these hubs include interconnects to one or more cloud providers and connections to the on-premises data centers over a private or leased WAN. Performance hubs can route traffic between the public cloud and on-premises infrastructure at high speed, and are resilient because of the underlying interconnect infrastructure.

Colo-Connect builds on the Colo-based performance hub concept, offering high-bandwidth (10-20 Gbps) low-latency connections, seamless Layer 2/3 connectivity to Prisma Access from existing performance hubs. The following figure shows Prisma Access being onboarded in a GCP instance using service connections and cloud interconnects. This setup limits exposure to the internet and allows the use of private connections for private application connectivity.



Colo-Connect allows you to use Prisma Access to secure private apps using a cloud interconnect that can provide high-bandwidth service connections using the following capabilities:

- High bandwidth (up to 20-Gbps) throughput per region for private application access
- Support for [Dedicated and Partner interconnects](#) using Google Cloud Platform (GCP)
- Support for multiple VLAN attachments (up to 20) per interconnect link

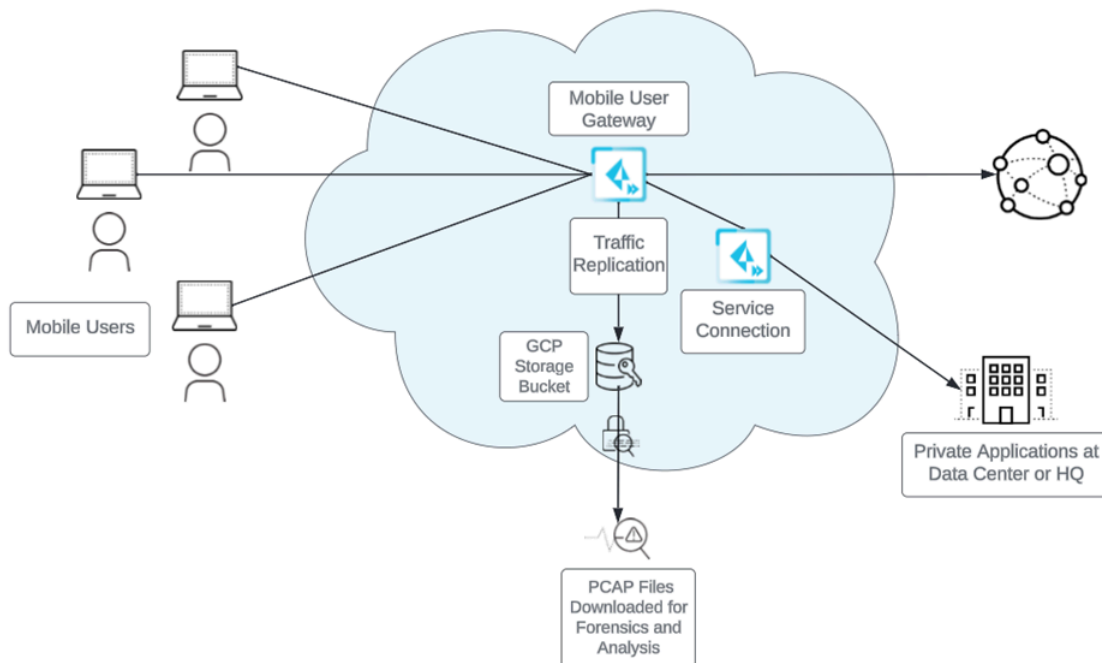
- Redundant connectivity support per region

Traffic Replication and PCAP Support

Prisma Access secures your traffic in real time based on traffic inspection, threat analysis, and security policies. While you can view Prisma Access logs to view security events, your organization might have a requirement to [save packet capture \(PCAP\) files for forensic and analytical purposes](#), for example:

- You need to examine your traffic using industry-specific or privately-developed monitoring and threat tools in your organization and those tools require PCAPs for additional content inspection, threat monitoring, and troubleshooting.
- After an intrusion attempt or the detection of a new zero-day threat, you need to preserve and collect PCAPs for forensic analysis both before and after the attempt. After you analyze the PCAPs and determine the root cause of the intrusion event, you could then create a new policy or implement a new security posture.
- Your organization needs to download and archive PCAPs for a specific period of time and retrieve as needed for legal or compliance requirements.
- Your organization requires PCAPs for network-level troubleshooting (for example, your networking team requires data at a packet level to debug application performance or other network issues).

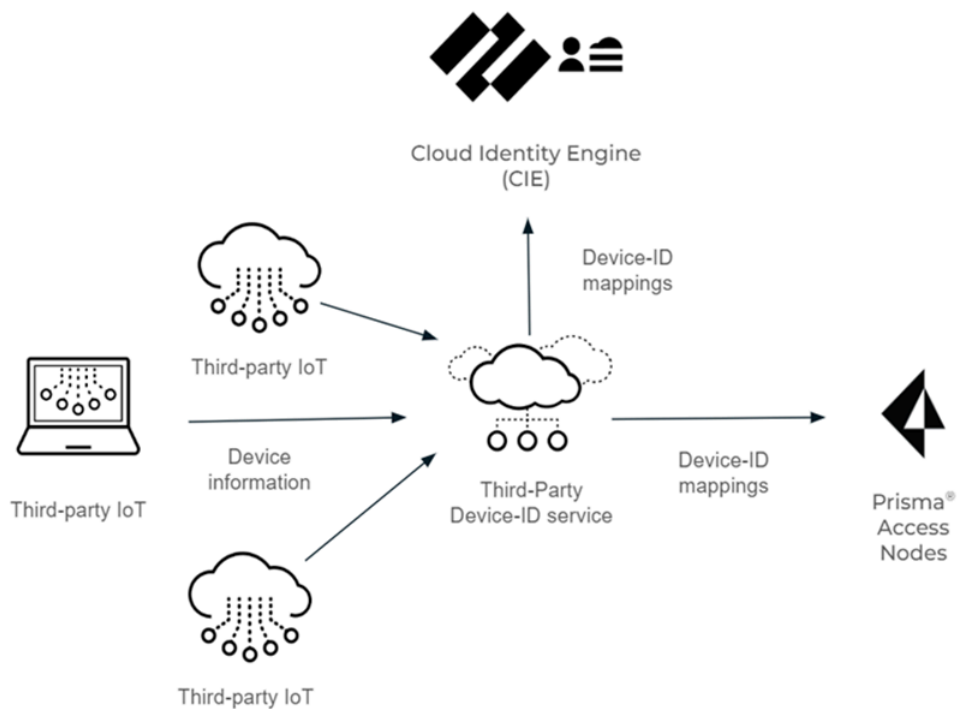
To accomplish these objectives, you can enable traffic replication which uses the Prisma Access cloud to replicate traffic and encrypt PCAP files using your organization's encryption certificates. To store the PCAP files, you create a [GCP service account](#), which Prisma Access uses as the storage location of the PCAP files.



Third-Party Device-ID in Prisma Access

You can use the Cloud Identity Engine along with Prisma Access to apply information from third-party IoT detection sources to simplify the task of identifying and closing security gaps for devices in your network. After you set up Third-Party Device-ID in the Cloud Identity Engine using an API, you can set up a device object and a security policy rule in Prisma Access to obtain and use information from third-party IoT visibility solutions through the Cloud Identity Engine for device visibility and control.

In the following figure, the Third-Party Device-ID service receives the device information from the third-party IoT solutions, which it then transmits as IP address-to-device mappings to the Cloud Identity Engine and the Prisma Access Security Processing Nodes (SPNs).



New and Remapped Prisma Access Locations and Compute Locations

The following [location](#) and [compute location](#) changes are made:

- **New Compute Locations**—The following new compute locations are added, and the following locations are moved to these compute locations:
 - **Europe North (Stockholm)**—The new Sweden location is added to this compute location.
 - **Middle-East Central (UAE)**—The United Arab Emirates location is moved to this location.
 - **Middle-East Central (Qatar)**—The new Qatar location is added to this compute location.
- **New Prisma Access Locations**—The following new Prisma Access locations are added:
 - Sweden
 - Kazakhstan
 - Qatar
 - Senegal
- **Remapped Prisma Access Locations**—To better optimize performance of Prisma Access, the following locations have been remapped to the following compute locations:
 - **Ecuador**—Remapped from the US Central compute location to the US Southeast compute location
 - **Jordan**—Remapped from the Europe Central compute location to the Europe South compute location

New deployments have the new remapping applied automatically. If you have an existing Prisma Access deployment that uses one of these locations and you want to take advantage of the remapped compute location, follow the procedure to [add a new compute location to a deployed Prisma Access location](#).

Transparent SafeSearch Support

Prisma Access allows you to resolve search engine queries from mobile users and users at remote networks to the engine's SafeSearch portal by performing an FQDN-to-IP mapping. This functionality can be useful if you have guest internet services at your organization and you want your guests to safely use search engines, preventing them from searching for potentially inappropriate or offensive material that could be against company policy.

Private IP Visibility and Enforcement for Explicit Proxy Traffic Originating from Remote Networks

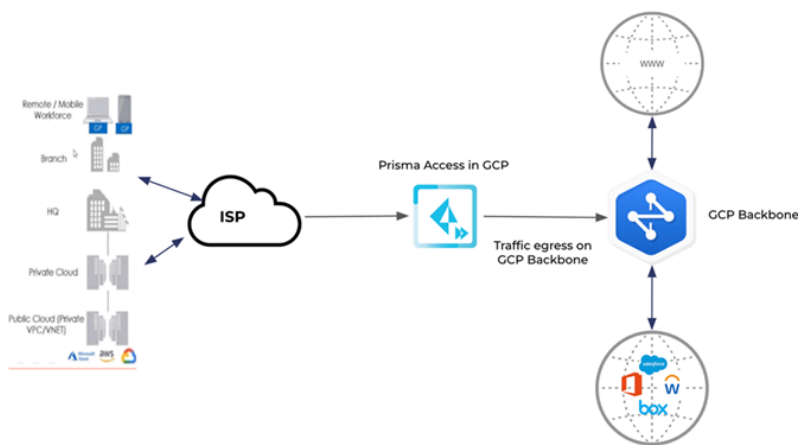
You can now leverage the private IP addresses of the systems in your branch locations that are forwarding traffic to Explicit Proxy [using Proxy mode](#). You can use the private IP address to skip authentication of headless systems that can't authenticate, set up security policies, and get visibility of the traffic on Prisma Access Explicit Proxy.

You can enable this functionality when you secure users and devices at a branch with a [site-to-site IPSec tunnel](#) using Remote Network and Explicit Proxy Secure Processing Nodes (SPNs).

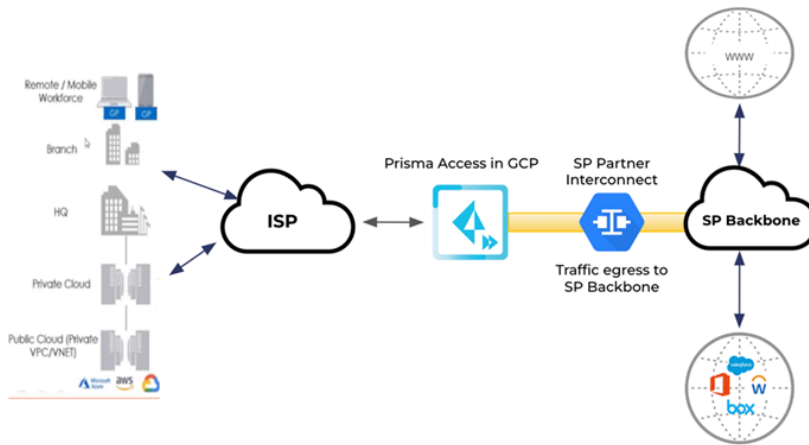
Service Provider Backbone Integration

Integrate Prisma Access with a [service provider \(SP\) backbone](#), which allows you (the SP) to assign specific region and egress internet capabilities to your tenants, providing more granular control over the Prisma Access egress traffic. Without the SP Backbone feature, Prisma Access egress traffic uses public cloud providers for network backbone instead.

The following diagram represents Prisma Access egress traffic without SP Backbone integration.



The following diagram represents Prisma Access egress traffic with SP Backbone integration.



Service Provider Backbone Integration was introduced with Prisma Access 4.1.

From Prisma Access version 5.0, you can allow [inbound flows to other remote networks](#) over the Service Provider (SP) backbone when you configure the non-inbound access remote network.



SP interconnect supports only the following:

- *Mobile users, service connections, and remote networks*
- *GCP Regions*
- *New Prisma Access deployments*
- *Explicit proxy egress traffic*

From March 2024, you can [configure](#), [view](#), and [monitor](#) Service Provider IP address pools to leverage your own IP addresses for Prisma Access egress traffic instead of the egress through public cloud providers.

Cloud Management of NGFWs

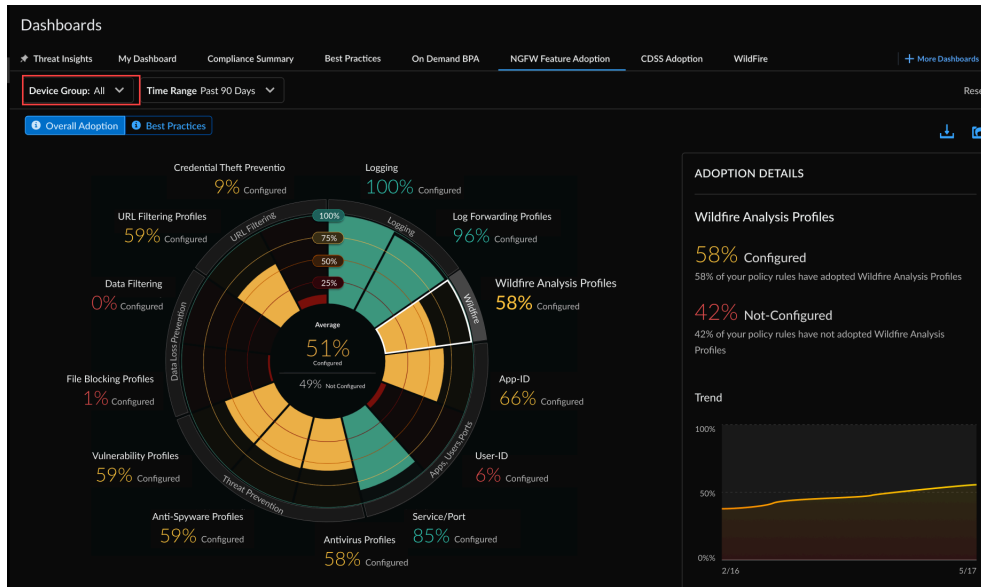
Manage your Palo Alto Networks Next-Generation firewalls from Strata Cloud Manager. [Cloud Management of NGFW](#) is a cloud-delivered and AI-powered security solution to manage Palo Alto Networks' advanced ML-powered firewalls alongside your Prisma Access deployments.

Cloud Management of NGFWs is done from a single streamlined user interface and leverages Palo Alto Networks best-in-class cloud-delivered security services. To manage your Next-Gen firewalls from Strata Cloud Manager, you must enable AIOps for NGFW Premium which also draws on PAN-OS device telemetry data to give you an overview of the health and security of your cloud managed NGFWs. For logging, Strata Logging Service provides a secure, resilient, and fault tolerant centralized log storage and aggregation.

Feature Adoption Dashboard

Monitor **Feature Adoption** and stay abreast of which security features you're using in your deployment and potential gaps in coverage. This release introduces the following new features:

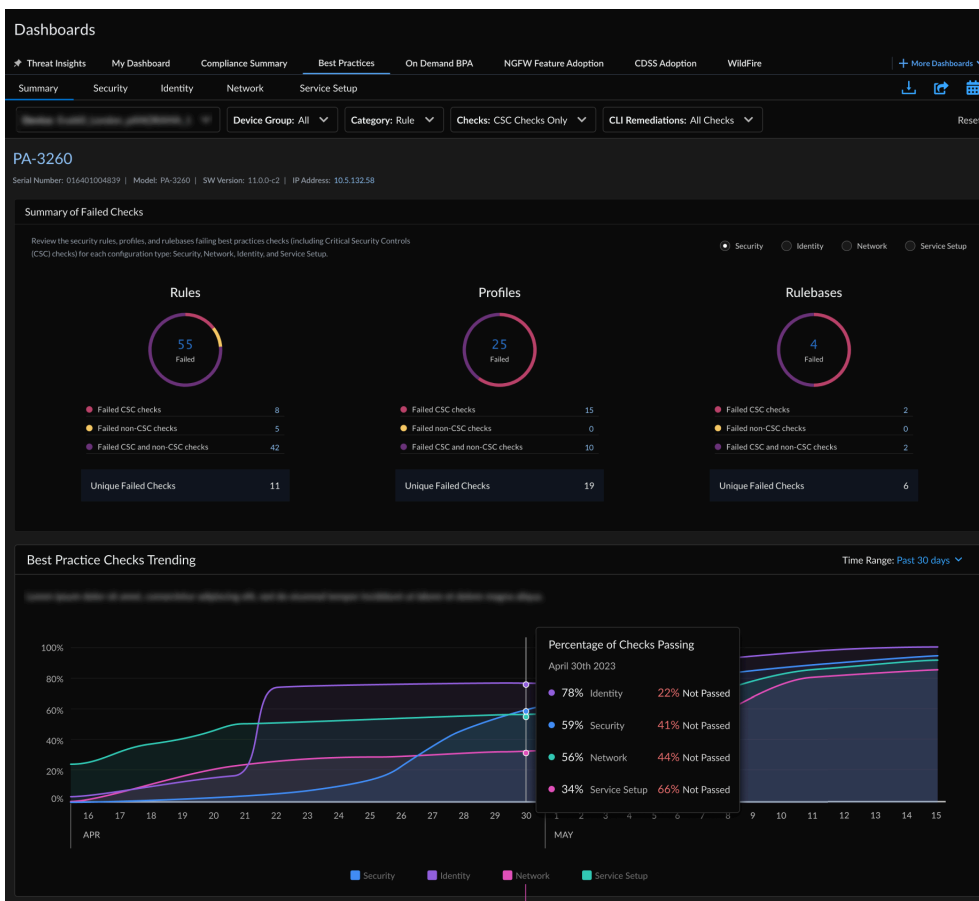
- TSF upload-generated CLI remediations (PAN-OS 9.1 and above TSFs)
- Historical adoption trend charts
- Per-device views of adoption (including for Panorama-managed devices)
- Ability to export adoption data as .csv file



Best Practices Dashboard

Check the [Best Practices dashboard](#) for daily best practices reports, and their mapping to Center for Internet Security's Critical Security Controls (CSC) checks, to help you identify areas where you can make changes to improve your best practices compliance. Share the best practice report as a PDF and schedule it to be regularly delivered to your inbox. This release introduces the following new features:

- Ability to export BPA reports in .csv format for use in third-party applications such as Microsoft Excel
- Ability to download CLI remediations in .txt format. CLI remediations are generated using TSF data you upload when generating an [On-Demand BPA report](#). (PAN-OS 9.1 and above TSFs)
- Ability to view historical trend charts for BPA checks



Compliance Summary Dashboard

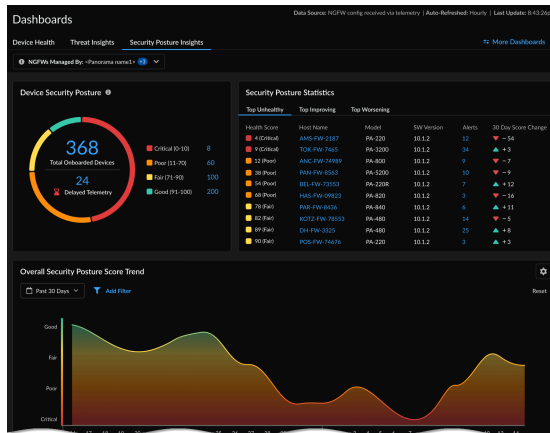
Check the [Compliance](#) dashboard to view a history of changes to the security checks made up to 12 months in the past, grouped together by Center for Internet Security (CIS) and National Institute of Standards and Technology (NIST) frameworks.



Security Posture Insights Dashboard

Get visibility into the security status and trend of your deployment based on the security postures of the onboarded NGFWs with [Security Posture Insights](#). Use this dashboard to:

- Know the trend of issues that impact the security posture of your deployment.
- Understand the security improvements that you have made in your deployment by looking at the historical security score data.
- Narrow down devices where there is an opportunity to improve the security posture and prioritize the issues to resolve them.



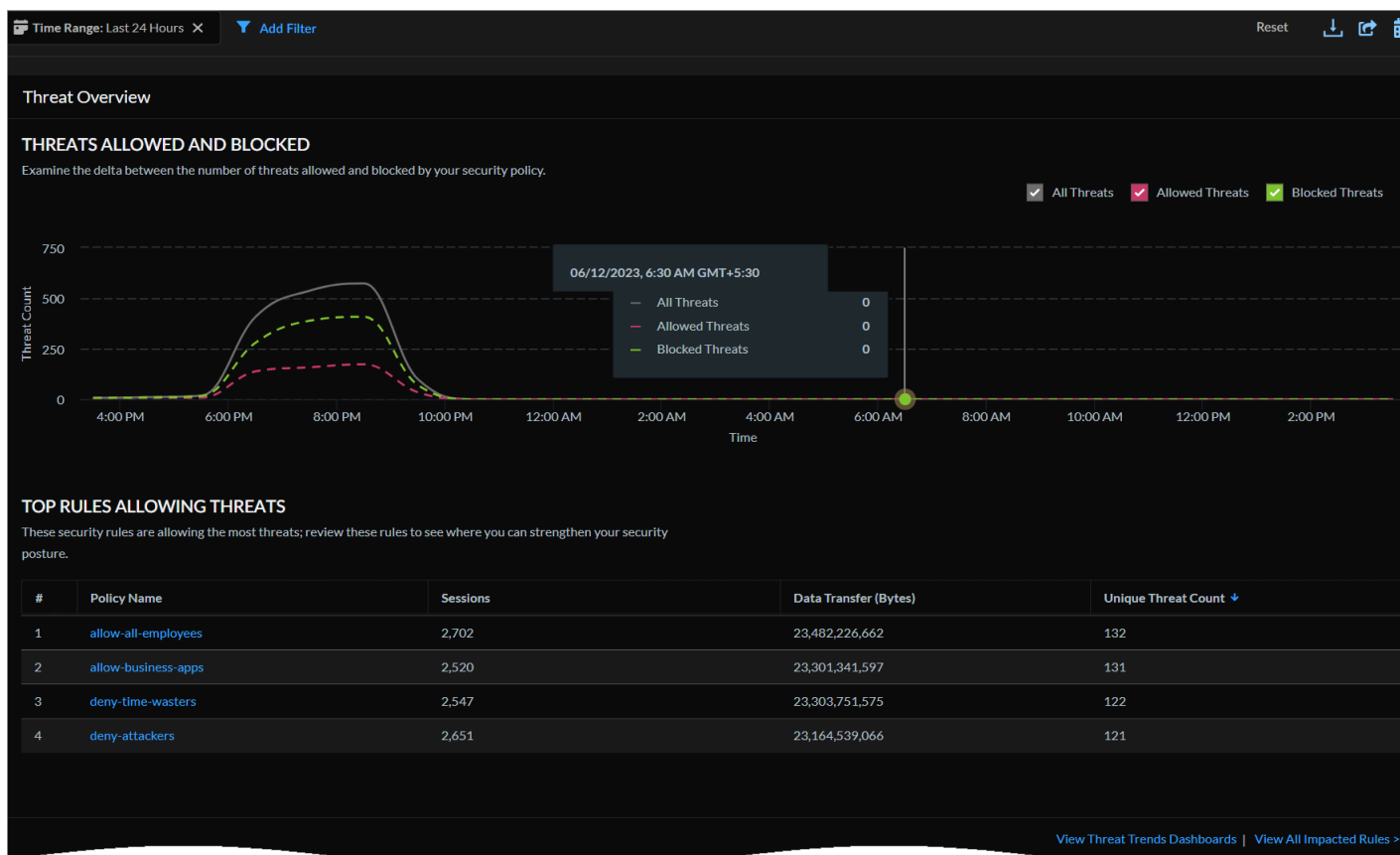
Advanced Threat Prevention Dashboard

The [Advanced Threat Prevention dashboard](#) gives insight into unknown malware, command and control (C2), and vulnerability exploit attempts in your network. The dashboard gives visibility into the real-time threat detection data by [inline cloud analysis](#) along with threats detected based on the [threat signatures](#) generated from malicious traffic data collected from various Palo Alto Networks services.

This dashboard provides:

- a time line view of threats allowed and blocked, list of source IPs and users responsible for generating command and control (C2) traffic, and hosts targeted by cloud-detected exploits.
- contextual links to [Log Viewer](#) to get context around the threat.
- [IOC search](#) result to learn about the usage patterns related to host generating traffic and host targeted by vulnerability exploits.
- cloud report and packet capture from the logs to get additional context and use Palo Alto Networks threat analytics data and threat intelligence to improve your incident response processes.

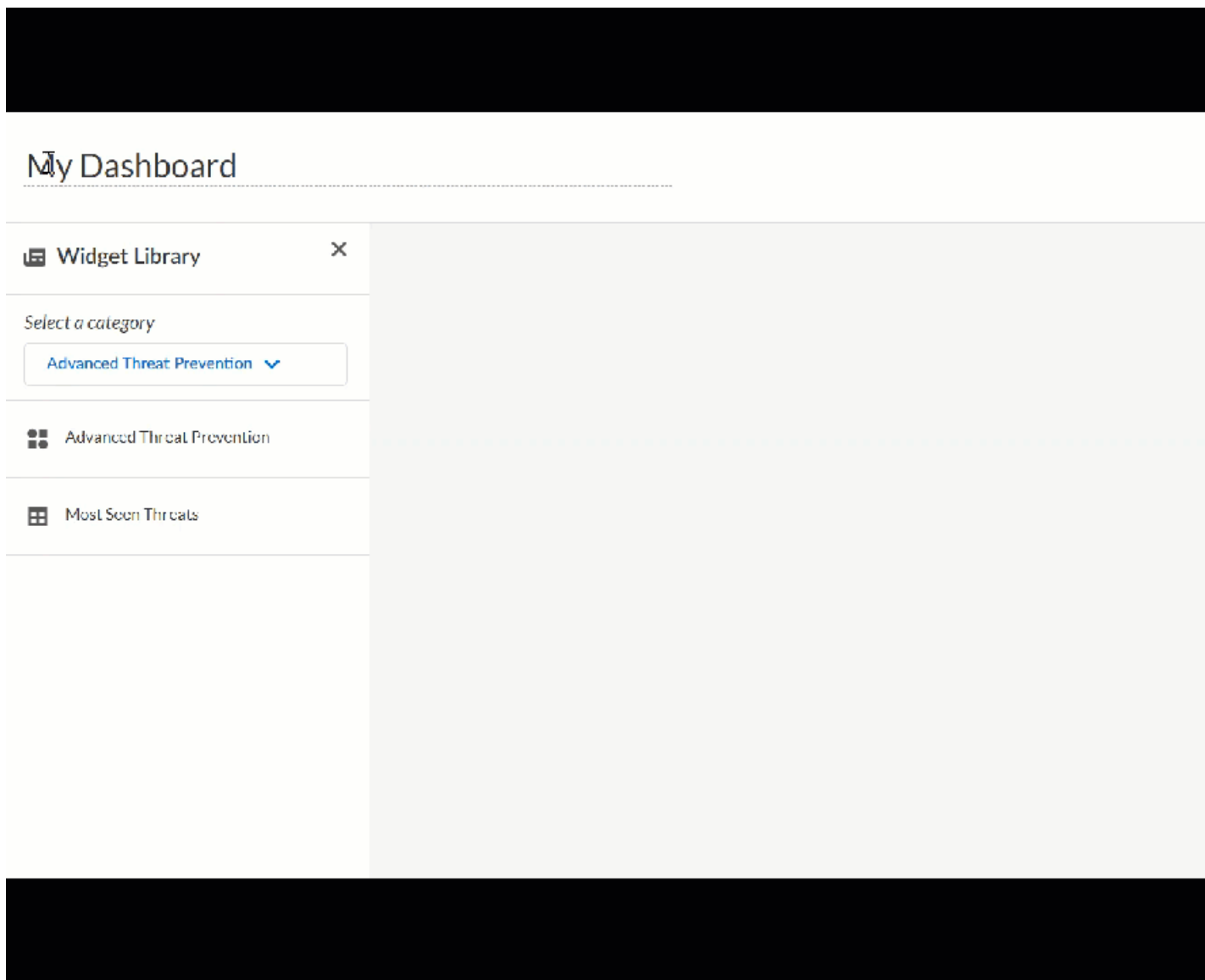
The dashboard helps to understand the security effectiveness of the Advanced [Threat Prevention service](#). Use the data along with the analysis data from your other Palo Alto Networks security services to prevent security infringement on your network infrastructure.



Custom Dashboard

Apart from the default dashboards, you can now build a [custom dashboard](#) based on your network and security visibility requirements. You can use various types of customizable widgets from the [widget library](#) to create the dashboard. The widgets available to you depend on the services [supported with your licenses](#). You can add up to 10 widgets in a custom dashboard and create 10 custom dashboards per user. The custom dashboard can be customized at any time. These are some of the customizations available in the custom dashboard:

- Customize dashboard settings such as layout, dashboard name, and descriptions
- Edit widget title, description, and show or hide filters
- Filter and sort data
- Look at the **Sample Data** view to know how your widget looks in the dashboard



Device Health Dashboard

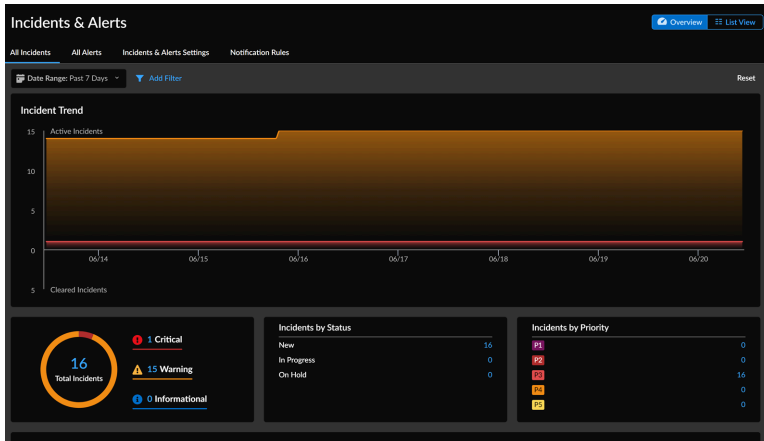
The [Device health dashboard](#) shows you the cumulative health status and performance of your onboarded NGFW devices. The device health is determined by the severity of the health score (0-100) and its corresponding health grade (good, fair, poor, critical). The health score is calculated based on the priority, quantity, type, and status of the open alerts.

This dashboard helps you:

- Understand the deployment improvements that you have made over a period by looking at the historical health score data.
- Narrow down devices that require attention in your deployment and prioritize the issues to resolve them.
- Review the device statistics and [fix the critical alerts](#) on the device to improve the health score and deployment health.

Incidents and Alerts

The **Incidents & Alerts** feature helps monitor the health of your devices and prevent disruptive incidents. It generates incidents and alerts based on detected issues with your firewall deployment. With this feature, you get a singular broad view of your **incidents and alerts across NGFWs**. Additionally, you can manage notifications by viewing and adding rules.



NGFW SDWAN Dashboard

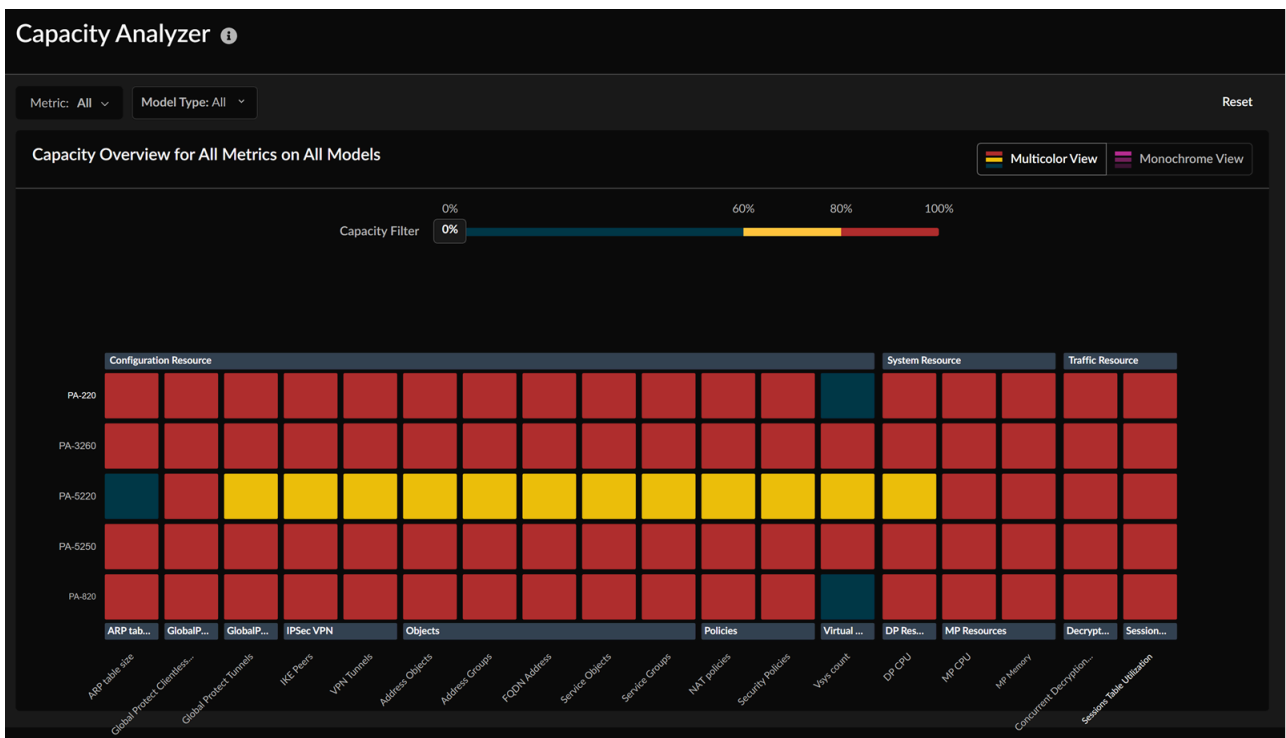
The [NGFW SD-WAN dashboard](#) provides performance metrics for cloud-managed firewalls with SD-WAN, allowing visibility into application and link performance. It helps troubleshoot issues across VPN clusters, isolates problems to affected sites, applications, and links, and generates actionable alerts for poor links and applications. These alerts are based on data-driven thresholds and offer insights into trends with machine learning-powered detection and forecasting.



Capacity Analyzer

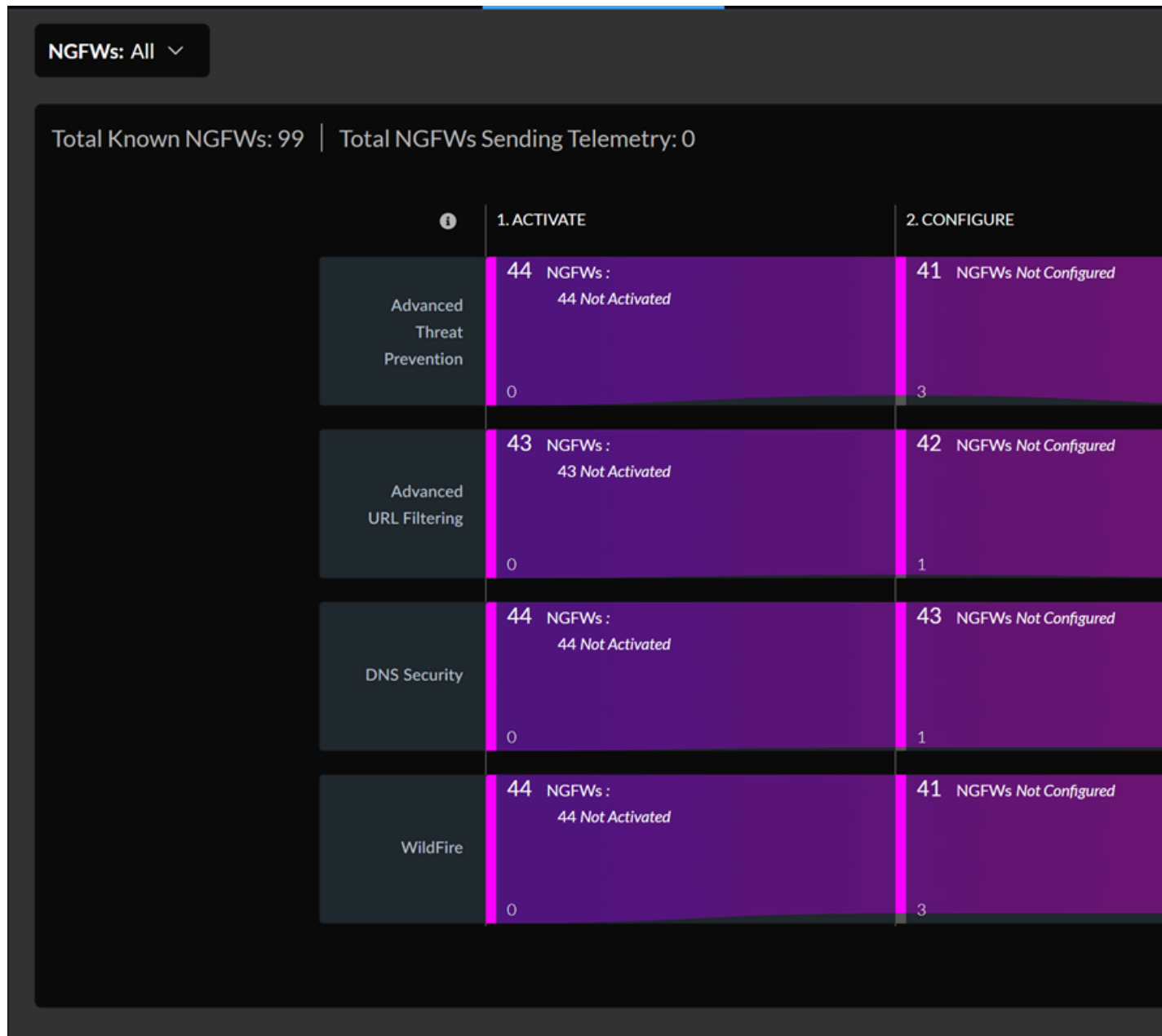
Sometimes, you can encounter a predicament where particular features on your Next-Generation Firewalls (NGFW) approach their capacity thresholds, resulting in diminished system performance and operational disruptions. Dealing with capacity-related issues can be time-consuming, and unfortunately, these issues tend to come to light only after the limits are breached.

The **Capacity Analyzer** feature allows monitoring of device resource capacity by tracking metrics usage based on model types. This feature includes a heatmap visualization to display resource consumption rates and locations for each metric. It also enables planning for upgrading to higher capacity firewalls based on specific needs. This proactive approach ensures that you know about potential capacity constraints, allowing you to take preemptive action to safeguard your business operations.



Enhancements to CDSS Dashboard

In order to enhance the security of your enterprise by identifying and addressing potential security vulnerabilities, AIOps for NGFW offers a streamlined workflow that enables you to monitor the implementation of CDSS features using the [CDSS dashboard](#). This allows you to easily track the progress of CDSS feature activation, configuration, and adherence to best practices. Moreover, you have the option to override recommendations at the firewall level, saving time by avoiding the need to override them for each role-pair individually.



May 2023

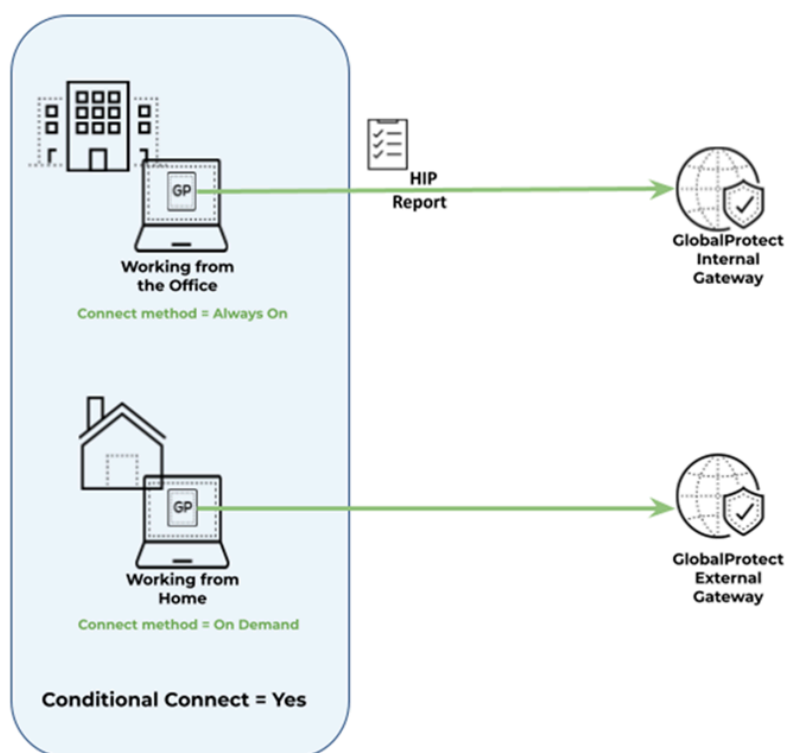
Review all the new features we've introduced across the NetSec platform in May 2023.

Conditional Connect Method for GlobalProtect

To improve the user experience with GlobalProtect, you can now [use the Conditional Connect setting](#) to have GlobalProtect dynamically change the connect method based on whether the user is on the internal network or working from a remote location. This is useful in environments where you require your users to connect to GlobalProtect at all times when in the office (Always On mode), but don't require them to connect to GlobalProtect when they are away from the office except when they need access to your private apps.

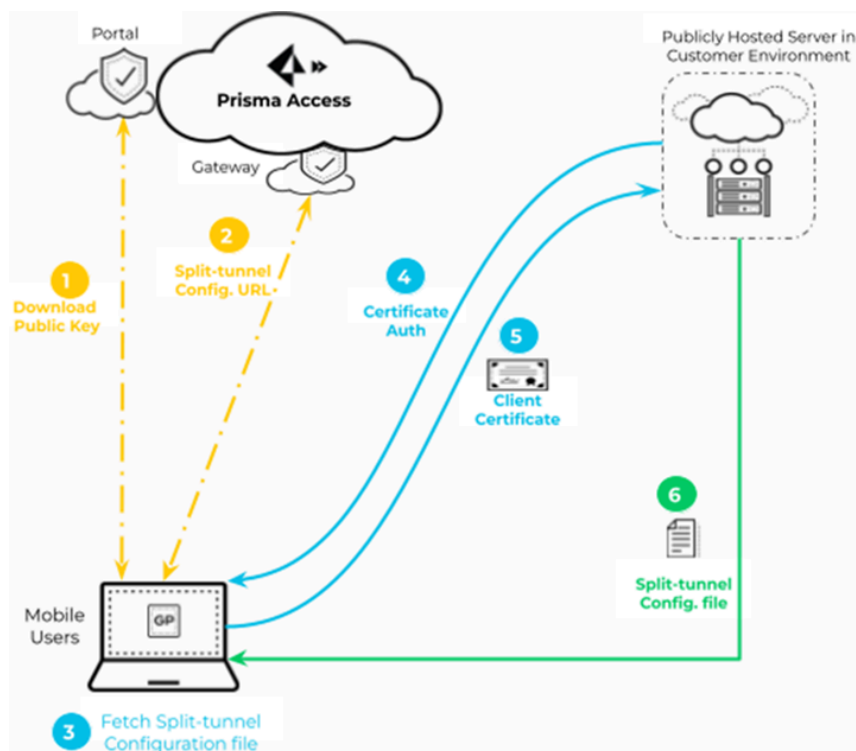
With Conditional Connect, GlobalProtect uses internal host detection (IHD) to determine whether the user is on the internal network and then sets the connect method accordingly.

To configure this feature, you must deploy the **conditional-connect** setting to the endpoint transparently to the [Windows Registry or macOS plist](#). For the feature to work, you must also enable internal host detection and configure the endpoints to use the On-demand connect method.



Enhanced Split Tunnel Configuration

With [Enhanced Split Tunnel](#) you can manage the list domains, access routes, and applications that you want to include or exclude from the GlobalProtect tunnel using a split-tunnel configuration file that you host locally in your environment. This allows you to modify your split-tunnel settings without having to modify the configuration on the GlobalProtect gateway. In addition, this feature increases the number of included and excluded split-tunnel access routes and domains that you can define from 200 to 1,000. To use this capability, create the XML file and host it on a web server that your GlobalProtect endpoints can reach. To secure the XML file, you must sign it and then enable mutual TLS on the server hosting the split-tunnel configuration file. You can push the public key certificate from the portal configuration to the endpoint. The endpoint needs the certificate to authenticate to the web server.



Prisma Access Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security

Prisma Access now supports explicit proxy connectivity for GlobalProtect 6.2. This protects users with always-on internet security while providing on-demand access to private apps through a third-party VPN, GlobalProtect with Prisma Access, or an on-premises NGFW. This capability enables you to:

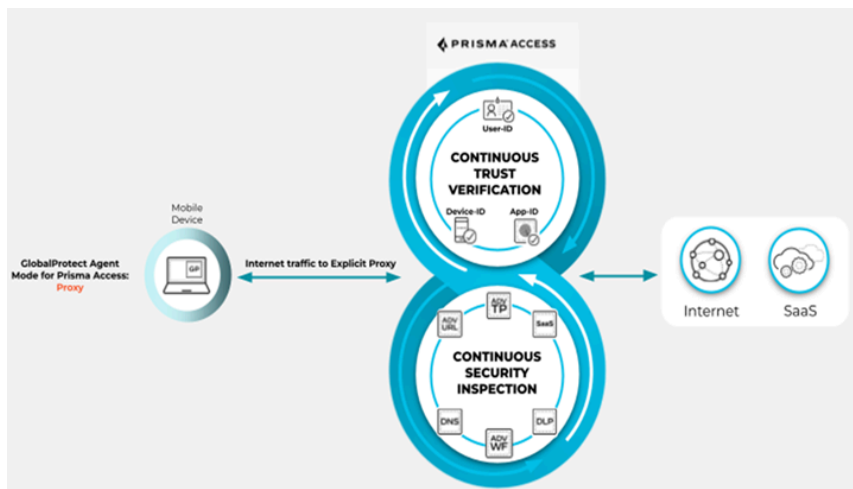
- Easily replace 3rd-party proxy solutions
- Seamlessly coexist with 3rd-party VPN agents
- Secure internet traffic using browser-based and non-browser-based apps
- Simplify proxy deployments and enforce User-ID-based policy against all traffic

In addition to [Tunnel mode](#), GlobalProtect Explicit Proxy supports two connectivity methods:

- Proxy Mode
- Tunnel and Proxy Mode

Proxy Mode

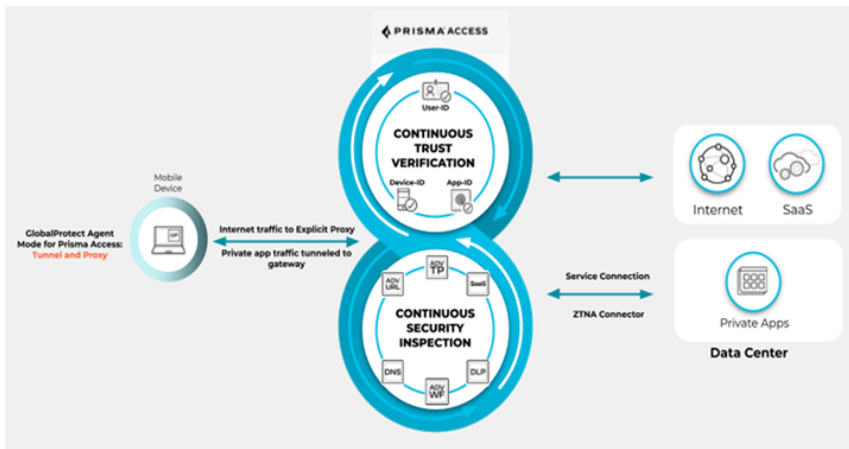
This connection method enables you to use a 3rd-party VPN agent while still using Prisma Access as a [secure web gateway](#) for consistent and superior internet and SaaS security.



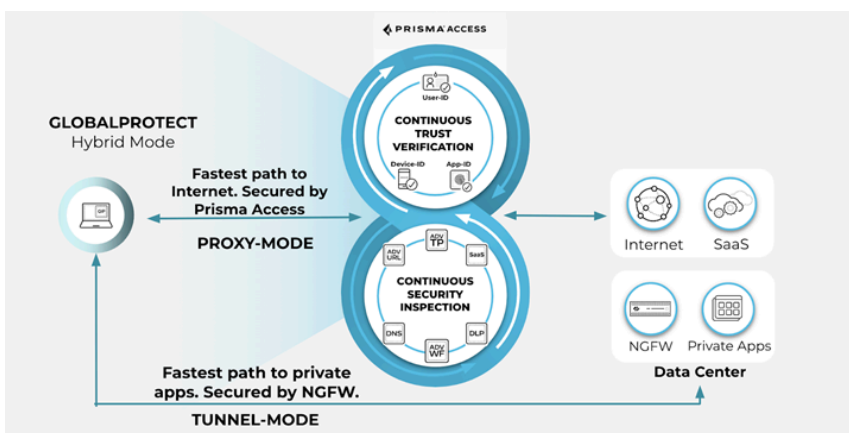
Tunnel and Proxy mode

This mode enables you to secure access to the internet and SaaS applications through proxy mode and to secure access to private apps through tunnel mode. Whether or not the GlobalProtect tunnel for private app access is enabled, access to the internet remains secure through the proxy.

Users can access private apps through Prisma Access:



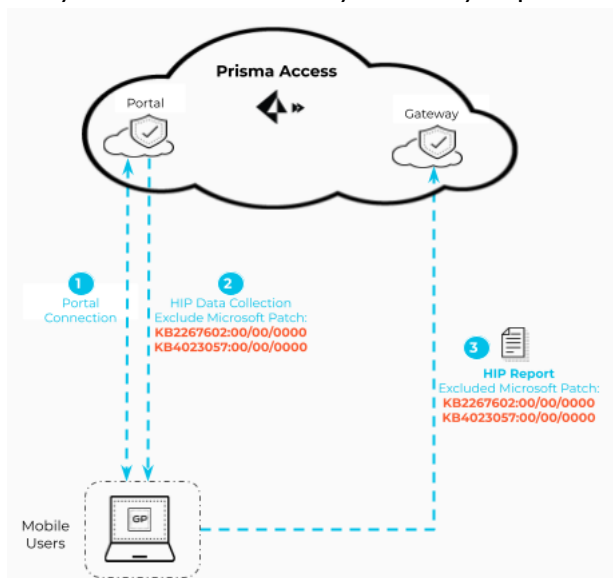
Or through an on-premises firewall:



If you don't require support for explicit proxy or 3rd-party VPNs from the GlobalProtect app, you can continue to deploy GlobalProtect in Tunnel Mode and use the [split tunnel functionality](#) to define what traffic you want to secure with Prisma Access, and which traffic can bypass the tunnel.

Host Information Profile (HIP) Exceptions for Patch Management

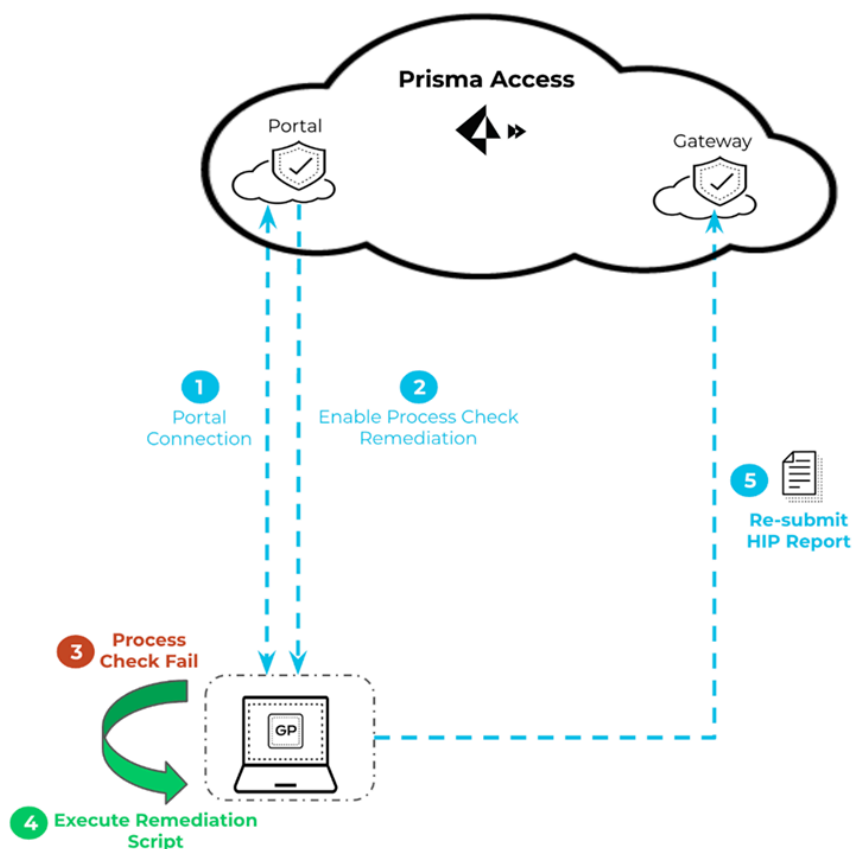
You can now configure the GlobalProtect app to exempt specific security patches from being reported as missing from the endpoint HIP report to prevent the endpoint from failing the HIP check in cases where patch updates happen frequently (for example some companies update their patches multiple times a day with threat updates). When you [enable this feature](#), you can specify specific patches to exclude from the HIP report and the duration for which you want to exclude them. For certain patches, you might want to exclude them from the HIP report permanently if you don't require them in your environment. For other patches, such as those that get updated frequently by the vendor, you might just want to exclude for a day or less to ensure that end users aren't getting blocked from accessing the resources they need whenever a patch update happens, but you also want to verify that they're patching their devices regularly.



Host Information Profile (HIP) Process Remediation

You can now enable a HIP remediation script whenever a GlobalProtect endpoint fails one or more process checks to help the endpoint recover from a HIP check failures. For example, you can create a script that will run on the endpoint whenever the HIP check—such as a process check or a registry or plist check—fails. After the endpoint runs the remediation script, the GlobalProtect app resubmits the HIP report. Remediating the issue causing the HIP check failure in real time enables your users access to the resources they need without having to wait until the next hourly HIP check.

To use this feature, you must create a remediation script and deploy it to your endpoints using your Mobile Device Management (MDM) software. You then [enable the new HIP Remediation Process Timeout setting](#) to indicate the amount of time you want to give the remediation process to complete. After the remediation timeout elapses, the GlobalProtect app resubmits the HIP report.



License Activation

After you receive an email from Palo Alto Networks identifying the new product license you're activating, including all your add-ons and capacities, use the activation link to begin the activation process. You can activate and manage all your available licenses, device associations, tenants, and identity and access from [Common Services](#). As existing app instances transition to [tenants and tenant service groups](#) you can also use Common Services to manage those as well. After activation or transition, you can find Common Services in the [tenant view of the hub](#) or in a [variety of ways](#).