

Subscriptions You Can Use With the Firewall

The following Palo Alto Networks subscriptions unlock certain firewall features or enable the firewall to leverage a Palo Alto Networks cloud-delivered service (or both). Here you can read more about each service or feature that requires a subscription to work with the firewall. To enable a subscription, you must first [Activate Subscription Licenses](#); once active, most subscription services can use [Dynamic Content Updates](#) to provide new and updated functionality to the firewall.

| Subscriptions You Can Use With the Firewall | |
|---|---|
| Strata Cloud Manager | <p>Manage your Palo Alto Networks Next-Generation Firewalls (NGFW) from Strata Cloud Manager. This cloud-delivered, AI-powered security solution allows seamless management of your advanced ML-powered NGFWs, alongside Prisma Access deployments, through a single, streamlined user interface. Strata Cloud Manager has two licensing tiers: Strata Cloud Manager Essentials and Strata Cloud Manager Pro. This unified structure streamlines the deployment of network security offerings, including AIOps for NGFW, Autonomous Digital Experience Management (ADEM), cloud management functionality, and Strata Logging Service.</p> <ul style="list-style-type: none">Get Started with Strata Cloud ManagerStrata Cloud Manager LicenseCloud Management for NGFWs |
| IoT Security | <p>The IoT Security solution works with next-generation firewalls to dynamically discover and maintain a real-time inventory of the IoT devices on your network. Through AI and machine-learning algorithms, the IoT Security solution achieves a high level of accuracy, even classifying IoT device types encountered for the first time. And because it's dynamic, your IoT device inventory is always up to date. IoT Security also provides the automatic generation of policy recommendations to control IoT device traffic, as well as the automatic creation of IoT device attributes for use in firewall policies.</p> <ul style="list-style-type: none">Get Started with IoT Security. |
| SD-WAN | <p>Provides intelligent and dynamic path selection on top of the industry-leading security that PAN-OS software already delivers. Managed by Panorama, the SD-WAN implementation includes:</p> <ul style="list-style-type: none">Centralized configuration managementAutomatic VPN topology creationTraffic distributionMonitoring and troubleshooting <ul style="list-style-type: none">Get Started with |
| Threat Prevention | <p>Threat Prevention provides:</p> <ul style="list-style-type: none">Antivirus, anti-spyware (command-and-control), and vulnerability protection.Built-in external dynamic lists that you can use to secure your network against malicious hosts.Ability to identify infected hosts that try to connect to malicious domains. <ul style="list-style-type: none">Get Started with Threat Prevention |
| Advanced Threat Prevention | <p>In addition to all of the features included with Threat Prevention, the Advanced Threat Prevention subscription provides an inline cloud-based threat detection and prevention engine, leveraging deep learning models trained on high fidelity threat intelligence gathered by Palo Alto Networks, to defend your network from evasive and unknown command-and-control (C2) threats by inspecting all network traffic.</p> <ul style="list-style-type: none">Get Started with Advanced Threat Prevention |
| DNS Security | <p>Provides enhanced DNS sinkholing capabilities by querying DNS Security, an extensible cloud-based service capable of generating DNS signatures using advanced predictive analytics and machine learning. This service provides full access to the continuously expanding DNS-based threat intelligence produced by Palo Alto Networks.</p> <p>To set up DNS Security, you must first purchase and install a Threat Prevention license.</p> <ul style="list-style-type: none">Get Started with DNS Security |
| URL Filtering | <p>Provides the ability to not only control web-access, but how users interact with online content based on dynamic URL categories. You can also prevent credential theft by controlling the sites to which users can submit their corporate credentials.</p> <p>To set up URL Filtering, you must purchase and install a subscription for the supported URL filtering database, PAN-DB. With PAN-DB, you can set up access to the PAN-DB public cloud or to the PAN-DB private cloud.</p> <div><div></div><div>URL Filtering is no longer available as a standalone subscription. All URL Filtering features are included with the Advanced URL Filtering subscription.</div></div> <ul style="list-style-type: none">Get Started with URL Filtering |
| Advanced URL Filtering | <p>Advanced URL Filtering uses a cloud-based ML-powered web security engine to perform ML-based inspection of web traffic in real-time. This reduces reliance on URL databases and out-of-band web crawling to detect and prevent advanced, file-less web-based attacks including targeted phishing, web-delivered malware and exploits, command-and-control, social engineering, and other types of web attacks.</p> <ul style="list-style-type: none">Get Started with Advanced URL Filtering |
| WildFire | <p>Although basic WildFire® support is included as part of the Threat Prevention license, the WildFire subscription service provides enhanced services for organizations that require immediate coverage for threats, frequent WildFire signature updates, advanced file type forwarding (APK, PDF, Microsoft Office, and Java Applet), as well as the ability to upload files using the WildFire API. A WildFire subscription is also required if your firewalls will be forwarding files to an on-premise WF-500 appliance.</p> <ul style="list-style-type: none">Get Started with WildFire |
| Advanced WildFire | <p>Advanced WildFire is a subscription offering that provides access to Intelligent Run-time Memory Analysis: a cloud-based advanced analysis engine that complements static and dynamic analysis, to detect and prevent evasive malware threats. By leveraging a cloud-based detection infrastructure, Intelligent Run-time Memory Analysis detection engines operate a wide array of detection mechanisms to target these highly-evasive malware.</p> <ul style="list-style-type: none">Get Started with Advanced WildFire |
| AutoFocus | <p>Provides a graphical analysis of firewall traffic logs and identifies potential risks to your network using threat intelligence from the AutoFocus portal. With an active license, you can also open an AutoFocus search based on logs recorded on the firewall.</p> <ul style="list-style-type: none">Get Started with AutoFocus |
| Cortex Data Lake | <p>Provides cloud-based, centralized log storage and aggregation. The Cortex Data Lake is required or highly-recommended to support several other cloud-delivered services, including Cortex XDR, IoT Security, and Prisma Access, and Traps management service.</p> <ul style="list-style-type: none">Get Started with Cortex Data Lake |
| GlobalProtect Gateway | <p>Provides mobility solutions and/or large-scale VPN capabilities. By default, you can deploy GlobalProtect portals and gateways (without HIP checks) without a license. If you want to use advanced GlobalProtect features (HIP checks and related content updates, the GlobalProtect Mobile App, IPv6 connections, or a GlobalProtect Clientless VPN) you will need a GlobalProtect Gateway license for each gateway.</p> <ul style="list-style-type: none">Get Started with GlobalProtect |
| Virtual Systems | <p>This is a perpetual license, and is required to enable support for multiple virtual systems on PA-3200 Series firewalls. In addition, you must purchase a Virtual Systems license if you want to increase the number of virtual systems beyond the base number provided by default on PA-400 Series, PA-3400 Series, PA-5200 Series, PA-5400 Series, and PA-7000 Series firewalls (the base number varies by platform). The PA-220, PA-800 Series, and VM-Series firewalls do not support virtual systems.</p> <ul style="list-style-type: none">Get Started with Virtual Systems |
| Enterprise Data Loss Prevention (DLP) | <p>Provides cloud-based protection against unauthorized access, misuse, extraction, and sharing of sensitive information. Enterprise DLP provides a single engine for accurate detection and consistent policy enforcement for sensitive data at rest and in motion using machine learning-based data classification, hundreds of data patterns using regular expressions or keywords, and data profiles using Boolean logic to scan for collective types of data.</p> <ul style="list-style-type: none">Get Started with Enterprise DLP |
| SaaS Security Inline | <p>The SaaS Security solution works with Cortex Data Lake to discover all of the SaaS applications in use on your network. SaaS Security Inline can discover thousands of Shadow IT applications and their users and usage details. SaaS Security Inline also enforces SaaS policy rule recommendations seamlessly across your existing Palo Alto Networks firewalls. App-ID Cloud Engine (ACE) also requires SaaS Security Inline.</p> <ul style="list-style-type: none">Get Started with SaaS Security Inline |