



**SOLUTION
GUIDE**

Securing IoT Environments

Part of the “On-Premises Network Security for the Branch” and
“SASE for Securing Internet” reference architectures

NOVEMBER 2024

Table of Contents

Preface.....	3
Purpose of This Guide.....	5
Audience.....	5
Related Documentation.....	5
Introduction.....	7
Security Challenges.....	8
Essential Capabilities.....	9
Solution Overview.....	9
IoT Security Design Details.....	10
Solution Components.....	10
IoT Security Approach.....	18
Design Considerations.....	34
Design Models	39
Deploying IoT Security for On-Premises NGFW.....	45
Assumptions and Prerequisites.....	46
Onboarding IoT Security.....	46
Creating Zero Trust Security Policies.....	48
Implementing Zero Trust Security Policies.....	53
Updating Security Rules with Device-ID.....	54
Deploying IoT Security for Prisma SASE Attached Remote Sites.....	59
Assumptions and Prerequisites.....	59
Onboarding IoT Security	60
Creating Zero Trust Security Policies.....	62
Implementing Zero Trust Security Policies.....	66
Updating Security Rules with Device-ID.....	68
Working with Risk, Vulnerabilities, and Alerts.....	72
Evaluating IoT Risk.....	72
Resolving IoT Vulnerabilities.....	75
Resolving Security Alerts.....	79
Feedback.....	84

Preface

GUIDE TYPES



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

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

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

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

DOCUMENT CONVENTIONS



Notes provide additional information.



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

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

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

Bold text denotes:

- Command-line commands.

show device-group branch-offices

- User-interface elements.

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

- Navigational paths.

Navigate to **Network > Virtual Routers**.

- A value to be entered.

Enter the password **admin**.

Italic text denotes the introduction of important terminology.

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

Highlighted text denotes emphasis.

Total valid entries: 755

ABOUT PROCEDURES

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

GETTING THE LATEST VERSIONS OF GUIDES

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

<https://www.paloaltonetworks.com/referencearchitectures>

WHAT'S NEW IN THIS RELEASE

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

- Added next-generation firewall (NGFW) management by using Strata™ Cloud Manager (SCM)
- Changed the logging service from Cortex® Data Lake to Strata Logging Service
- Added policy enforcement for IoT devices at remote sites connected using Prisma® SD-WAN
- Made minor corrections to product navigation and improvements for readability

Purpose of This Guide

This guide builds on the reference architecture described in the following:

- [**Securing the Branch with On-Premises Network Security: Design Guide**](#)
- [**Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**](#)
- [**SASE for Securing Internet: Design Guide**](#)
- [**SASE for Securing Internet: Deployment Guide**](#)

This guide provides design and deployment guidance for the IoT Security solution, which allows you to discover, identify, and inventory your organization's deployed IoT devices. You can also use the solution to assess risks and enforce policies that mitigate them.

AUDIENCE

This guide is for technical readers, including solution architects and engineers, who want to deploy the Palo Alto Networks IoT Security solution, NGFWs, and Prisma Access. It assumes the reader is familiar with the basic concepts of applications, networking, virtualization, security, and high availability.

RELATED DOCUMENTATION

The following documents support this guide:

- [**Zero Trust Enterprise: Design Guide**](#)—Provides design guidance for securing users, applications, and infrastructure by using the Palo Alto Networks Zero Trust Enterprise approach to eliminate implicit trust and continuously validate every stage of a digital interaction.
- [**On-Premises Network Security: Overview**](#)—Introduces multiple solutions for providing on-premises remote-site (or branch) network security and connectivity.
- [**On-Premises Network Security and SD-WAN for the Branch: Design Guide**](#)—Provides design guidance for using Palo Alto Networks next-generation firewalls to secure and interconnect multiple remote sites. Includes descriptions of common remote-site network layouts, as well as design and deployment considerations for centralized management, advanced logging capabilities, and PAN-OS SD-WAN.
- [**Securing the Branch with On-Premises Network Security: Design Guide**](#)—Provides design guidance for using Palo Alto Networks next-generation firewalls to secure branch offices. Includes descriptions of common branch office network layouts, as well as design and deployment considerations for centralized management and advanced logging capabilities.

- **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**—Provides implementation details for using Palo Alto Networks next-generation firewalls to secure branch offices. Includes high-level tasks and step-by-step configuration details for centralized management and advanced logging capabilities.
- **SASE for Securing Internet: Design Guide**—Provides design and deployment guidance for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations.
- **SASE for Securing Internet: Deployment Guide**—Provides implementation details for using Prisma Access and Prisma SD-WAN to secure internet access for mobile users and users located at remote-site locations. Includes decision criteria for deployment scenarios, as well as step-by-step procedures to achieve an integrated design.

Introduction

Companies that successfully integrate IoT into their business models stand to reap huge benefits for their own internal processes, employees, and customers. Although some of the most striking benefits of IoT revolve around business process efficiency, productivity, and cost reduction, an increasing number of enterprises are also recognizing IoT as a valuable source of intelligence into their products.

The enterprise has adopted IoT for multiple capabilities such as security, safety, environmental controls, employee productivity, asset tracking, and more. Common types of IoT devices found in the enterprise include security cameras, printers, TVs, video conferencing equipment, digital signage, intelligent lighting, smart thermostats, smart assistants such as Amazon Alexa, and even smart coffee machines. The idea around digitizing the office with intelligent, connected devices is to create an environment that you can modify and customize based on an employee. The office can become an intelligent ecosystem that makes the work environment safer and more comfortable, an easier place to collaborate, and much more energy efficient.

IoT in healthcare, known as the *internet of medical things* (IoMT), helps with operational efficiencies, cost reduction, and improving treatments in order to better serve patients and reduce errors. IoMT use cases include hospital bed-availability tracking, medical-equipment tracking, remote-patient monitoring, pathogen detection, and hospital-facilities management. Connected medical devices provide the ability to save lives by determining when a patient needs treatment, and they provide diagnostic details of a patient's current health. IoMT devices include heart-rate monitors, connected inhalers, and ingestible sensors.

In the manufacturing industry, IoT systems and processes are called *operational technology* (OT). OT controls, maintains, and operates industrial equipment. Due to digital transformation, OT has seen a rapid increase in connected devices. In manufacturing, IoT enables operational efficiencies such as production-line monitoring, predictive maintenance of equipment, remote production-control, asset tracking, logistics management, and more. Most manufacturing organizations have IT and OT systems in different parts of their business. Historically, IT and OT did not integrate, but this has started to change because OT groups require access to IT-provided platforms, the public cloud, and SaaS. To improve the integration between OT and IT environments and to secure plant floors, we developed two reference architectures: **Securing OT Services by Using an Industrial DMZ** and **Securing OT Infrastructure with Plant Segmentation**.

Combining IoT with the retail sector allows store managers to establish connections with their customers, create direct customer engagements, and improve the process of product maintenance. IoT sensors collect important data on customers' location in the store, the products they view, and their shopping lifecycles while in the store. After the data is processed, the information provides valuable insights to help managers make informed decisions to personalize the retail experience and improve their operations. IoT-enabled machines and connected stores can be partially or fully automated to drive efficiency, sustainability, and resilience to retail operations and experiences. For example, a Target customer can use the mobile app to get product recommendations related to their location in the store while they are shopping.

From these industry examples, it is clear IoT has become a business enabler, but it also introduces new security challenges for network and security teams alike. Today, it is estimated that IoT devices account for more than 60% of all network-connected enterprise endpoints. Chief information security officers and security leaders need an IoT security posture that reliably enables IoT and protects the network from existing and unknown threats. The true value of IoT comes from the insights derived through IoT-generated data that is invaluable to business-decision makers.

SECURITY CHALLENGES

A growing number of IoT devices operate on enterprise networks every day. These devices range from building automation, flow monitors, and surveillance cameras to IP phones, point-of-sale systems, conference room technology, and medical devices. Often, organizations allow these IoT, IoMT, and OT devices to participate unchecked on the network, thereby significantly expanding an organization's attack surface. Conventional network-perimeter defenses, legacy processes and point solutions are simply not equipped to address the surge of new IoT security issues:

- **Incomplete device inventory**—Most organizations lack an understanding of both IT and IoT devices on their networks. Even with an inventory, they can't update it regularly, making it hard to analyze traffic, control access, and detect compromised devices.
- **Vulnerability assessments**—IoT devices are simple devices, but securing them becomes complicated because of the diversity of hardware, software, and communication protocols involved. Their variations are large enough that each type of device must be examined for its own behavior and characteristics. Although legacy vulnerability assessments are helpful to a degree in identifying potential weaknesses, these assessments do not solve the underlying problem.
- **Network access control**—Legacy NAC solutions and their methodologies do not scale well for the IoT environment. They lack the sophistication required to correctly identify and provide acceptable security to IoT devices in the context of today's expanding threat landscape. NAC systems are useful for enforcement only after a device with a potential issue is identified.
- **Point solutions for IoT security**—Point solutions require too much effort from security teams. The teams must implement single-purpose sensors and then integrate them with existing security systems, which creates a high learning curve for the overworked IT engineering staff.
- **IoT data profiling and traffic risks**—As the number of IoT devices grows, their network operation becomes crucial. Frequent additions and complex network placements make isolating these devices challenging and complicates VLAN segmentation. On wireless networks, IoT-specific SSIDs help, but on wired networks, managing VLANs remains difficult. Unrestricted IoT access poses risks if devices are compromised.
- **IoT device vulnerabilities and security risks**—The rapid increase in IoT devices makes their security crucial to preventing network infiltrations. Attackers are targeting unprotected IoT devices, which are easy prey due to outdated systems and lack of endpoint protection.
- **IoT operations integration into core security**—IoT devices and their systems differ greatly from traditional IT systems, and they often use unique communication protocols. Despite being critical to operations, IoT device integration into existing security frameworks is challenging for IT engineers, due to a lack of ongoing device visibility.

ESSENTIAL CAPABILITIES

To effectively address the security challenges posed by IoT devices, a comprehensive solution must provide the following capabilities:

1. Discover and collect a full inventory of all devices on your network.
2. Assess the current risks and vulnerabilities associated with the devices in the inventory.
3. Reduce risk through Zero Trust security policies, segmentation, software, and firmware updates.

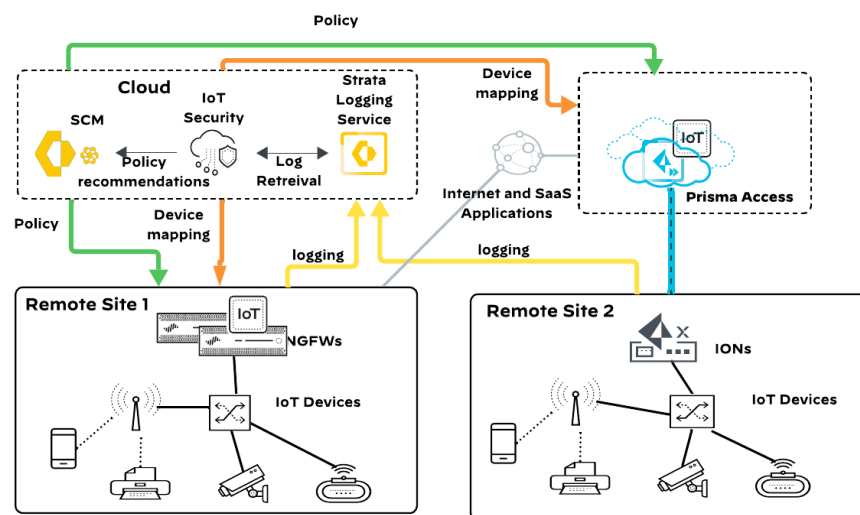
SOLUTION OVERVIEW

Palo Alto Networks offers an IoT Security solution, delivered as a cloud service, that takes a lifecycle approach to securing your IoT environment. Your existing NGFWs and ION devices perform discovery, visibility, and enforcement tasks by enabling IoT license without requiring dedicated probes.

The IoT Security solution provides complete visibility, in-depth risk analysis, and automated enforcement with the NGFW and Prisma Access. The components of the IoT solution consist of an IoT Security app residing on the Palo Alto Networks hub, data storage, and log retention, as well as an IoT Security subscription.

- The NGFWs and ION devices inspect network traffic and generate enhanced application logs, which they send to Strata Logging Service (SLS), where the IoT Security app leverages this data.
- The IoT Security app analyses the data, provides IP-address-to-device mappings, and creates recommendations for policy rules to implement.
- From SCM, you can create security policy rules, which you can then push to NGFW or Prisma Access for enforcement.

Figure 1 IoT security solution



IoT Security Design Details

The Palo Alto Networks IoT Security solution includes a cloud-delivered IoT Security subscription, which takes a life-cycle approach to securing your IoT environment. The solution provides discovery, visibility, and enforcement, with your existing Palo Alto Networks NGFWs and IONs.

As part of its integration with the NGFW, the solution uses the following mechanisms:

- **Logging**—The NGFWs and the ION devices at the remote sites send their logging information to the SLS.
- **Device dictionary**—The IoT Security app generates a device-dictionary XML file and provides it to the NGFW and Prisma Access. The file contains a list of device attributes that you use in security policy rules. The device attributes include the device vendor, model, OS version, OS family, profile, and category. When configuring a security policy rule, you have the option to select specific device attributes from the device dictionary.
- **IP address-to-device mappings**—These mappings tell the firewall a device's attributes, based on its current IP address. When traffic to or from that IP address reaches the firewall, it checks if one of its attributes matches a policy and, if so, the firewall applies the policy.
- **Policy rule recommendations**—If you create a set of policy rules in SCM, based on traffic from devices that are part of a device profile, you push them to the NGFW and Prisma Access as recommendations to use in a security policy. Policy recommendations are based on device profiles that apply to all devices that match the profile (for example, HP printers).

SOLUTION COMPONENTS

Using AI and machine learning (ML), the IoT Security solution automatically discovers and identifies all network-connected devices and constructs a data-rich, dynamically updating inventory. In addition to identifying IoT devices and traditional IT devices, the IoT Security solution provides deep visibility into network behaviors, establishing what is normal and discerning what is suspicious. When it detects a device vulnerability or anomalous behavior posing a threat, the IoT Security app notifies administrators, who can then take action to investigate and remediate the issue.

You license one subscription per NGFW, and it is available as two different packages:

- **Enterprise IoT Security Plus**—This package addresses the use case of discovering and segmenting IoT devices, managing their risk, and obtaining policy recommendations. It requires the Cortex Data Lake (IoT License) and can be deployed into PA-Series, VM-Series, and Prisma Access. An advantage of this package is that other apps can also use SLS for their logging requirements.
- **Enterprise IoT Security**—This package specifically targets the need for segmenting IoT devices. It does not offer risk management for these devices or provide policy recommendations. The package does not require the data lake (IoT DRDL License) because the IoT Security app uses its own internal logging mechanism. Additionally, this package is not compatible with Prisma Access SASE for IoT Security.

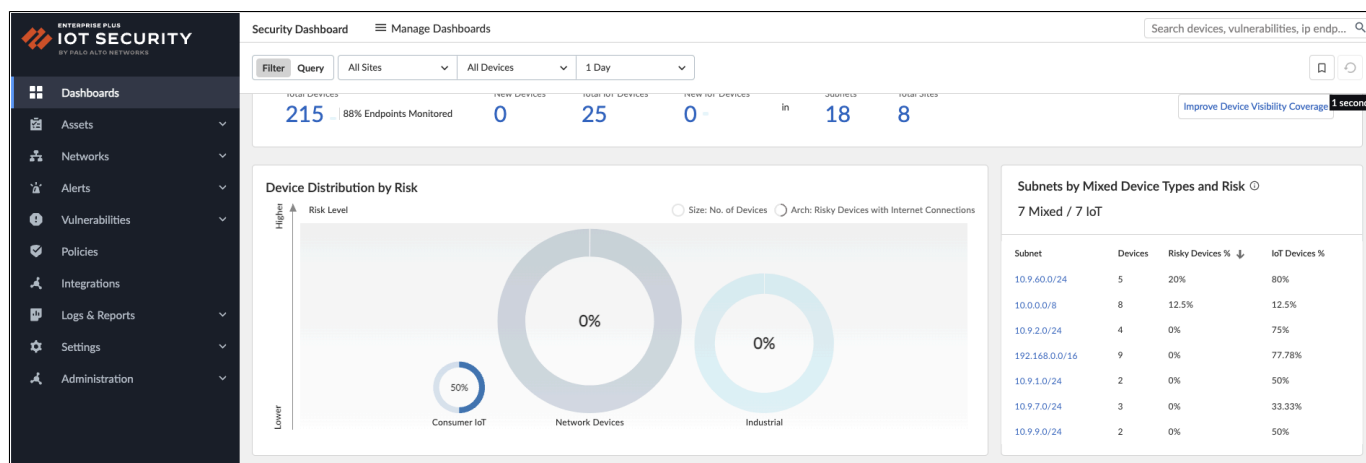
IoT Security App

The IoT Security app analyzes the network behavior of a device and classifies it within three levels or tiers. At the broadest tier, the app identifies behavioral similarities that assign a device to a category, such as security camera, even if it does not yet know the exact vendor and model. At the next tier, to assign the device to a specific profile, the app gathers more granular behavioral attributes shared by certain vendors. At the third tier, the algorithms create a model of unique behaviors for this individual security camera, such as its usage pattern.

In addition to device identification, the IoT Security app applies proprietary and supplemental ML technologies to threat detection. The app automatically detects device vulnerabilities and notifies IoT Security administrators. It also detects anomalous network behavior indicative of attack or reconnaissance and generates security alerts.

The app's navigation pane provides access to all features and functions. The items in the left navigation menu are loosely grouped into four sections. The first section is organized around visibility: Dashboard, Assets, and Networks. The next section is security related: Alerts, Vulnerabilities, and Policies. The third section is where you configure and review settings to integrate IoT Security with third-party products: Integrations. Finally, the last section is where you can check logs, reports, firewalls, and data quality, and manage administrative settings: Logs & Reports, Settings, and Administration.

Figure 2 IoT Security app



You use the left navigation menu for navigating to different pages in the IoT Security portal. When there are data filters at the top of a page, use them to control the data that appears on the page by site, device type, and relative time.

Using the dashboard, you can view a summary of all discovered devices, device types, applications, active alerts, and vulnerabilities. You can also view detailed information about each of the IoT devices deployed in your organization. The dashboard shows a full inventory of network segments and indicates all current risks with the deployed devices. It categorizes risks according to severity and the number of vulnerabilities per severity.

The dashboard view summarizes your organization's current state, including the total number of devices, device types, applications, vulnerabilities, and a risk score. You can view more information by hovering over fields or use the navigation menu to navigate to the sections about which you want further information.

Next-Generation Firewall

Palo Alto Networks ML-powered NGFWs provide a single-pass architecture, prevent known threats, proactively stop unknown threats, gain network-wide visibility (including IoT devices), and reduce errors with automatic policy recommendations.

NGFWs come in the following form factors:

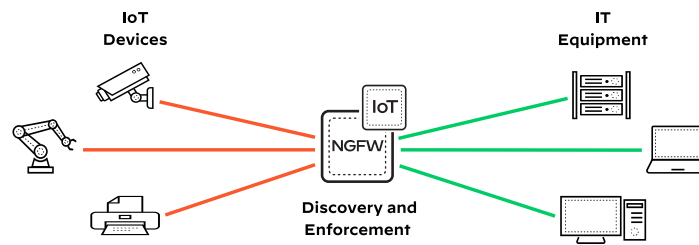
- **PA-Series**—The PA-Series firewalls are physical-appliance, ML-powered NGFWs. All PA-Series firewalls have PAN-OS® feature-parity across the range, and multiple models are available in order to meet your requirements such as size, scale, and connectivity. The models provide deployment options for the branch, campus, and data center environments.
- **VM-Series**—The VM-Series firewalls are virtualized form-factor, ML-powered NGFWs that you can deploy in a range of diverse cloud and virtualized use cases, such as public-cloud and private-cloud deployments. Multiple models are available for varying size and scale requirements, and all models have feature parity.

Palo Alto Networks enables visibility at the application, user, and device level by integrating the following features into the NGFW and Prisma Access:

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

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

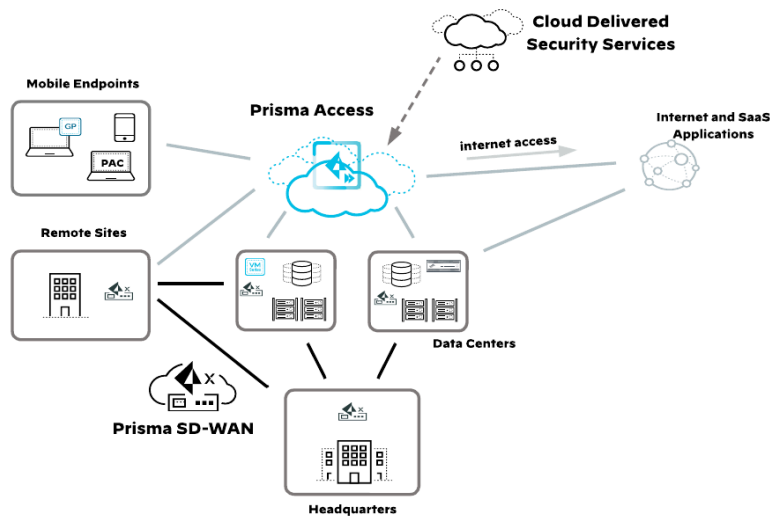
Figure 3 NGFW for device discovery and policy enforcement



Prisma Secure Access Service Edge

Secure Access Service Edge (SASE) integrates technologies to secure data and application access for users in any location. It combines data transport and security into a single, managed cloud-native solution. Palo Alto Networks' SASE solution combines all essential SASE elements into a unified platform with Prisma Access and Prisma SD-WAN. Prisma Access secures mobile users and remote sites globally, while Prisma SD-WAN provides secure WAN transport between various locations and SaaS applications. Prisma SASE 3.0 enhances security, visibility, and control for any device and application, featuring innovations such as Prisma Access Browser, AI-powered data security, and App Acceleration for seamless performance and unified management.

Figure 4 Prisma SASE



Prisma Access

Prisma Access, powered by PAN-OS, is a cloud service by Palo Alto Networks providing secure access to internet and business applications for managed and un-managed devices. Its firewall-as-a-service (FWaaS) capabilities inspect all traffic types to identify applications, threats, and content. Because Prisma Access is cloud based, it scales with demand, avoids firewall-sizing issues, and simplifies security deployment for remote networks and mobile users.

The Prisma Access infrastructure is comprised of security-processing nodes (SPNs), which are specialized virtual machines deployed globally in the locations you specify. Prisma Access automatically provisions and configures the nodes with IP addressing, routing, certificates, and DNS information.

Prisma SD-WAN

Prisma SD-WAN simplifies organization-wide network deployment by integrating next-generation, software-defined networking and cloud orchestration. It enables automatic, secure connections between sites and supports application-aware networking with built-in Layer 7 intelligence. When you use Prisma SD-WAN Instant-On Network (ION) devices, managed via a cloud portal, deployment is streamlined with zero-touch provisioning. These devices establish VPNs automatically and select optimal WAN paths based on real-time performance metrics and business policies, enhancing application performance and compliance with minimal manual configuration.

You connect remote sites to Prisma Access via Prisma SD-WAN or an industry-standard IPSec VPN-capable device. This deployment model is suitable for remote sites with one or more WAN links (or public WAN transports) and provides direct internet access through Prisma Access without the requirement to backhaul traffic to the central site.

Strata Cloud Manager

SCM provides unified management across an organizations' entire Palo Alto Networks Network Security infrastructure, including NGFWs and SASE environments, from a single, centralized user interface.

SCM consolidates a variety of tools that are designed to streamline the management of physical and virtual firewalls in order to enhance network security. These include a hierarchical folder structure for configuration and policy, actionable insights through several dashboards, and easy troubleshooting and problem resolution.

SCM offers administrators consistent policy enforcement, easy deployment of configurations, and updates to multiple firewalls and sites. SCM identifies deployed security capabilities and guides administrators to enable additional features based on the best practices in order to strengthen your security posture. SCM also enhances operational efficiency through automation and reduces complexity by unifying management tasks. Many of the available dashboards support scheduled generation of reports that show current operational states and can easily be shared with stakeholders.

Folders and Snippets

SCM includes a pre-defined folder structure where you can apply configuration settings and enforce policy globally across your entire environment, or specifically target certain devices and services within your organization. The pre-defined structure has at its root the Global folder. Settings at the Global level apply across all your network traffic.

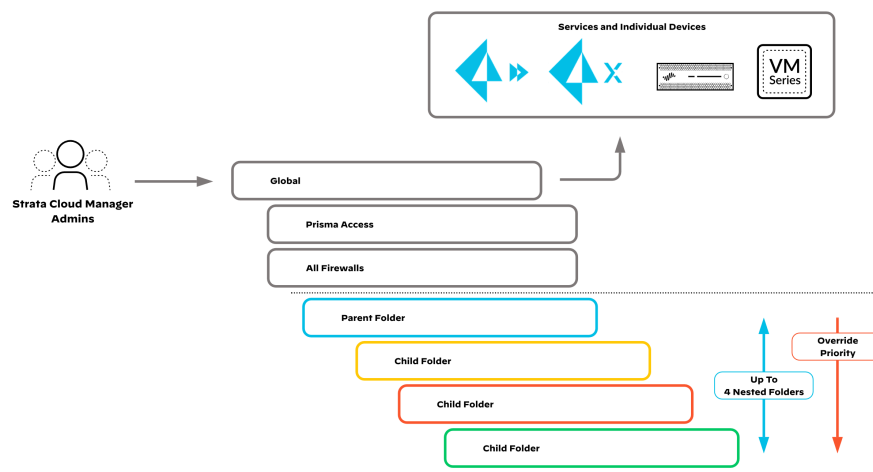
Within the Global folder are the following folders:

- **Prisma Access**—Settings at this level apply across all your Prisma Access deployment.
 - **Mobile Users Container**—Settings apply across all mobile user connection types (GlobalProtect® and Explicit Proxy) or individually to each connection type.
 - **Remote Networks**—Settings apply to remote network sites (branch offices, retail locations, etc.).
 - **Service Connections**—Settings apply to service connection sites (HQ and data centers).
- **All Firewalls**—Settings apply across all your NGFWs. You create specific folders under this level to group together NGFWs that require shared or specific configuration settings or policy enforcement.

In addition to creating configuration at the folder level, SCM provides an additional method to apply configuration to firewalls or deployments. A snippet is a configuration object, or a set of objects, that you can associate with a folder, deployment, or device. You can use snippets to standardize a common base configuration for a set of firewalls. For example, you onboard a new firewall in a CSP or a remote branch. You can associate a set of snippets that contain all the required network and policy configurations with the folder the new firewall belongs to.

In the event of conflicting values, snippet associations have a top-down priority. This means that if the first and the last associated snippets have different values for the same object, the value from the first snippet is inherited by the device or deployment. Additionally, you can override at the child folder, deployment, or device level all configurations inherited from a snippet.

Figure 5 SCM folder structure



Variables give you the flexibility to accommodate unique configuration values that are device specific or deployment specific. You use variables in your standardized configurations to accommodate device-specific or deployment-specific configuration objects. You can create variables at the folder, deployment, or firewall level. When you create a variable at a folder level, the variable is inherited by all folders nested under the folder. In the event of conflicting variables throughout the folder structure, the firewall or deployment inherits the variable value from the folder containing the nested folders. However, you can override an inherited variable at the nested folder, deployment, or firewall level.

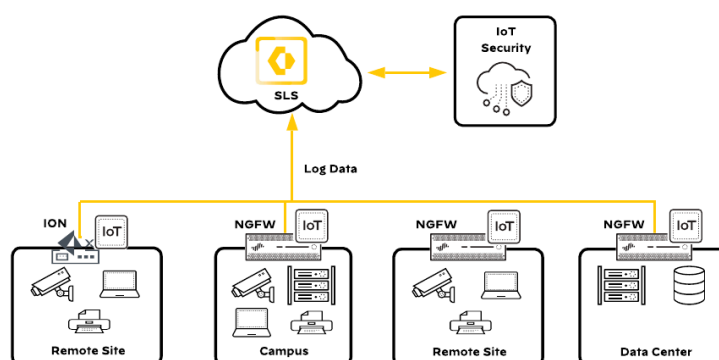
Logging

Prisma Access, NGFWs, IONs, and SCM use SLS to store their logs. SLS is a cloud-based log collector service that provides resilient storage and fast search capabilities for large amounts of logging data. The NGFWs and ION devices encrypt the logs and then send them to SLS over TLS/SSL connections. SLS enables you to scale your logging storage as your branch deployment scales, because licensing is based on storage capacity and not the number of devices sending log data.

The IoT Security solution uses a cloud-based log-forwarding process in order to direct the logs from firewalls to destinations such as the IoT Security app and SLS. Depending on the type of IoT Security subscription you purchase, the logging service either streams metadata to your IoT Security account and SLS instance or to your IoT Security account only.

If you subscribe to IoT Security Package 1, SLS stores logs from the NGFW, such as traffic, threat, and EAL logs. These logs contain metadata that the IoT Security app uses for device discovery and identification.

Figure 6 IoT Security with SLS



SLS provides centralized storage with the ability to have a single source of data from multiple environments including endpoints, devices, network, and cloud. The IoT Security and third-party apps can use centralized data. SLS forwards logs via syslog and email.

Alternatively, if you subscribe to the second option The "IoT Security, Does Not Require Data Lake", then this subscription sends data logs to a cloud-logging service that streams them directly to the IoT Security app without storing them in a data lake. It is important to note that both IoT Security and IoT Security (DRDL) subscriptions provide the same functionality in terms of IoT security and Device-ID.

If an active SLS license is in your Customer Support Portal account, all of your firewalls forward logs to the data lake, even if you activate them with IoT Security subscriptions that do not require a data lake. If you do not want to store data from individual firewalls in the data lake, in the SLS page, on the Firewalls page, toggle Store Log Data off for them. Although the data lake does not retain logs from these firewalls, the IoT Security app continues to ingest the logs and analyze their data.

Third-Party Integrations Using Cortex XSOAR

The IoT Security solution integrates with third-party systems, augmenting their inventory, network management, network security, and vulnerability detection by making them IoT aware and by gathering device and network data from other sources in order to enrich its own inventory and capabilities. The solution does this by leveraging Cortex XSOAR® technology in order to integrate with third-party systems.

The IoT Security solution uses either a cohosted, partially featured Cortex XSOAR instance that is available at no extra charge when you purchase an IoT Security Third-Party Integrations Add-On license or a full-featured, on-premises Cortex XSOAR server. There is also a third option for integrating Cortex XSOAR with the solution through the IoT Security API.

IoT Security with a Cohosted Cortex XSOAR Instance

If you want to integrate the IoT Security solution with third-party systems but do not have a Cortex XSOAR server, you can buy an IoT Security Third-Party Add-On license. After you activate the license, the solution automatically generates a cohosted XSOAR instance with the functionality necessary for supporting IoT Security integrations. When the IoT Security app communicates with third-party systems, it does so through the XSOAR instance, which connects with other systems and runs various jobs such as importing device data into the app or sending work orders for security alerts and vulnerabilities to other systems for investigation and remediation.

IoT Security with an On-Premises Cortex XSOAR Server

If you already have a full-featured Cortex XSOAR server deployed on-premises, you can use that to integrate the IoT Security solution with third-party systems without needing to buy an add-on license and use a limited cloud-hosted XSOAR module. For the Cortex XSOAR server to support IoT Security third-party integrations, you must install an IoT Security content pack and configure an integration instance on the XSOAR server. The content pack provides XSOAR with all third-party integration instance settings, playbooks, and jobs that the solution requires, and the Palo Alto Networks IoT third-party integration instance allows XSOAR to establish a permanent web socket connection with the IoT Security app.

The XSOAR server continues to provide the same functionality it did before you set it up to work with the IoT Security solution. However, the solution integrations the XSOAR server supports are limited to those in the content pack you install. The content pack has the same set of integrations that a cohosted XSOAR instance has, with one exception: you can modify the playbooks for IoT Security integrations on an XSOAR server but not on a cloud-hosted instance. To be precise, you cannot modify the playbooks directly, but you can duplicate them, modify the duplicate playbooks, and then use those on the server, which is something you cannot do in a cloud-hosted instance.

When integrating the IoT Security solution with third-party systems in a deployment that must comply with FedRAMP moderate authorization, you must use a full on-premises XSOAR server running a vendor-approved Federal Information Processing Standards (FIPS) version that complies with the FIPS 140-2 standard. This option supports the same IoT Security solution integrations as the cohosted version but is FIPS-compliant and does not require the purchase of a third-party integrations add-on license.

Cortex XSOAR Using the IoT Security API

If you have a Cortex XSOAR instance and your goal is to integrate it with the IoT Security solution—for example, to run an automation or playbook that downloads its inventory of IoT devices—see the [Palo Alto Networks IoT](#) topic. There you can learn the commands for creating a direct IoT Security-to-Cortex XSOAR integration. Note that this is different from the type of integrations in which the solution leverages XSOAR in order to work with third-party systems, as described in this guide.

IOT SECURITY APPROACH

Palo Alto Networks recommends the following phased approach to implementing IoT security:

- Discover and collect a full inventory of all devices on your network.
- Assess the current risks and vulnerabilities associated with the discovered devices.
- Employ risk reduction through Zero Trust security policies, segmentation, software, and firmware updates. You also deploy any available endpoint-security management software on the devices.

The phased approach is part of a lifecycle methodology. You need to continuously discover new devices, determine new risks, and take decisive action that reduces risk.

Visibility with ML-Based Discovery

The IoT Security solution relies on traffic data captured by the NGFWs and ION devices. In general, the more logging data that can be sent to the SLS for analysis, the higher the fidelity of IoT device visibility and verdicts. Incorrect placement of the NGFWs leads to insufficient data for device visibility and policy enforcement. Therefore, a fundamental step when implementing the IoT Security solution is to ensure that you correctly deploy the NGFWs and ION devices in your network, in order to provide the following:

- **Visibility**—So that the IoT Security app can build a full inventory of all devices, the NGFW assists the app with visibility of what devices are deployed. For device discovery, the NGFW needs to be deployed in the path of DHCP traffic between the DHCP clients and the DHCP server. The more traffic the NGFW sees, the more accurate device discovery becomes. You can manually add static IP devices, or the IoT Security app can identify them over time by using AI mapping.
- **Enforcement**—To protect your devices and other resources on the network from attacks, placement of the NGFW is also important for segmentation and applying security policies for enforcement.

Device Discovery

Compared to IT devices, IoT devices are built for a specific function. IoT devices generate unique behaviors and patterns that the IoT Security app uses when identifying and categorizing them for inventory. Using ML, the IoT Security app uses the NGFW logs' metadata in order to identify and classify devices. The app uses patented three-tier ML model combined with our patented App-ID technology and crowdsourced telemetry in order to discover devices.

During the discovery process, ML helps to determine information such as the device vendor, model numbers, operating system, firmware versions running on the device, and the applications it uses. These attributes are bound to a Device-ID that the NGFW uses in policy rules. Even after discovery, the IoT Security app continuously learns and updates the baseline, based on device behaviors.

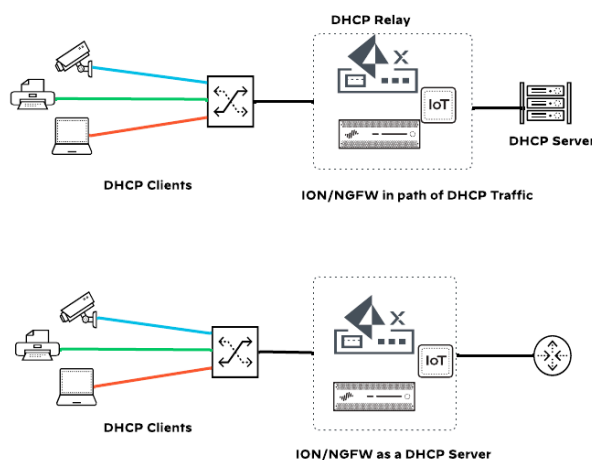
The first step in securing your IoT environment from potential exploits and vulnerabilities is to discover what types of devices are deployed. After discovery, you need a complete inventory of all devices based on their specific types and functions.

When an unknown device joins the network, NGFWs log the network traffic and send it to SLS. The logs include traffic flow, metadata, and EALs. EAL logging needs to be enabled on the firewall globally, and log forwarding must be enabled per security rule. EAL logs provide increased visibility into apps and services such as DHCP IP address assignment, which are required for device discovery.

DHCP traffic is important because it provides a way to link an IP address to a MAC address for device mapping, which is required for device classification. When it receives a DHCP unicast message, the firewall generates an EAL. This happens when the DHCP clients send a DHCP request to the DHCP server through the NGFW. The NGFW can be the DHCP server or, if your DHCP servers are centralized, perform the DHCP relay function. If the firewall is running virtual wire between the client and the DHCP server, the NGFW can also see broadcast DHCP traffic.

As shown in Figure 7, the NGFWs or ION devices either need to be in the path of DHCP traffic or be the DHCP server in a branch. DHCP session data is captured in Layer 3, Layer 2, tap, and virtual wire NGFW interface deployment modes. The NGFW configured as a DHCP server with PAN-OS 10.0 and above also generates DHCP EALs.

Figure 7 NGFW and DHCP traffic

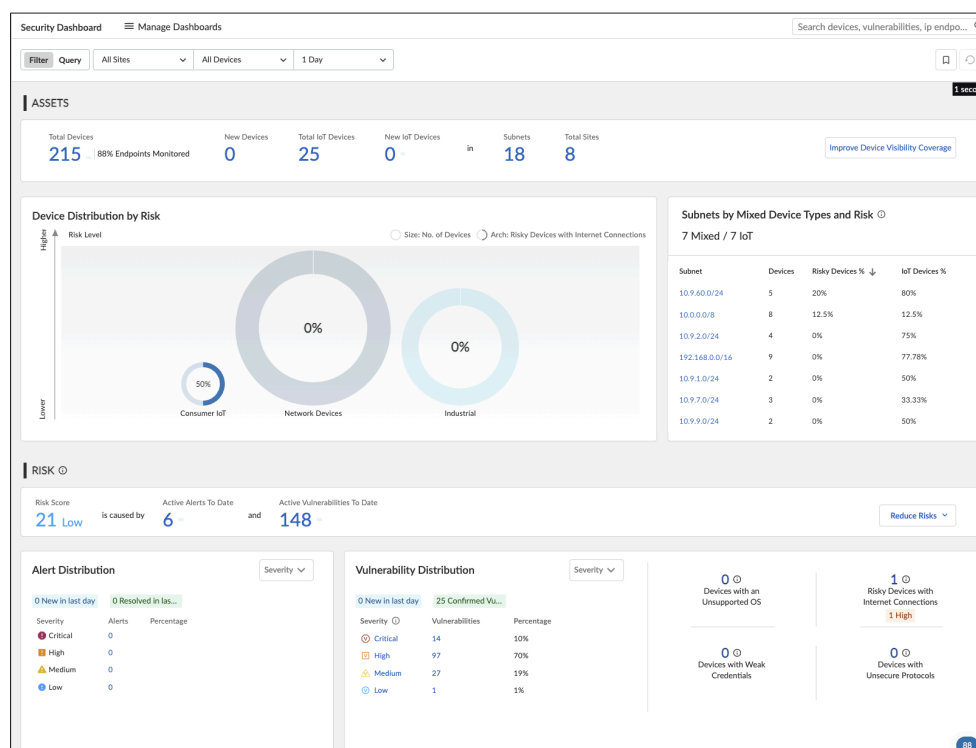


Security Dashboard

IoT Security offers specialized portals tailored for various industries, including enterprise, industrial, and medical sectors. For enterprises, two options are available: Enterprise IoT Security and Enterprise IoT Security Plus. The basic Enterprise IoT Security identifies and classifies devices but does not include advanced security features. In contrast, Enterprise IoT Security Plus not only incorporates the foundational features of Enterprise IoT Security but also offers automatic policy recommendations, security alerts, and device vulnerability assessments. Additionally, it integrates with third-party services. Similar to Enterprise IoT Security Plus, Industrial IoT Security and Medical IoT Security provide specialized capabilities designed to meet the specific needs of their respective industries. This guide primarily focuses on Enterprise IoT Security Plus.

To understand more about these themes, please see the TechDocs topic, "[Vertical-themed Portals](#)". This guide focuses on Enterprise IoT Security Plus, which enables comprehensive visibility and protection for all IoT devices within your organization, aligning with NIST guidelines.

Figure 8 Security summary of the Enterprise IoT Security Plus theme



Device Inventory

In the IoT Security app, you can view discovered devices on the dashboard in the following ways:

- The Devices tab summarizes the devices and displays all device categories. You can view each category and examine the devices, profiles, subnets, and vulnerabilities for that specific category, such as video and audio conferencing.
- Clicking Assets > Devices in the navigation pane shows the full inventory of devices. This provides more information on the devices discovered, and you can view individual devices in more detail.
- For each device, the full inventory list provides the status, risk, device name, profile, vendor, model, OS, IP address, MAC address, VLAN, and last activity. If you want to import the list into another inventory platform, you can download the full device inventory list in a CSV file. To see more details about the device, you can view each device independently. You also have the option to run a search query for a device by IP address, MAC address, device type, etc.

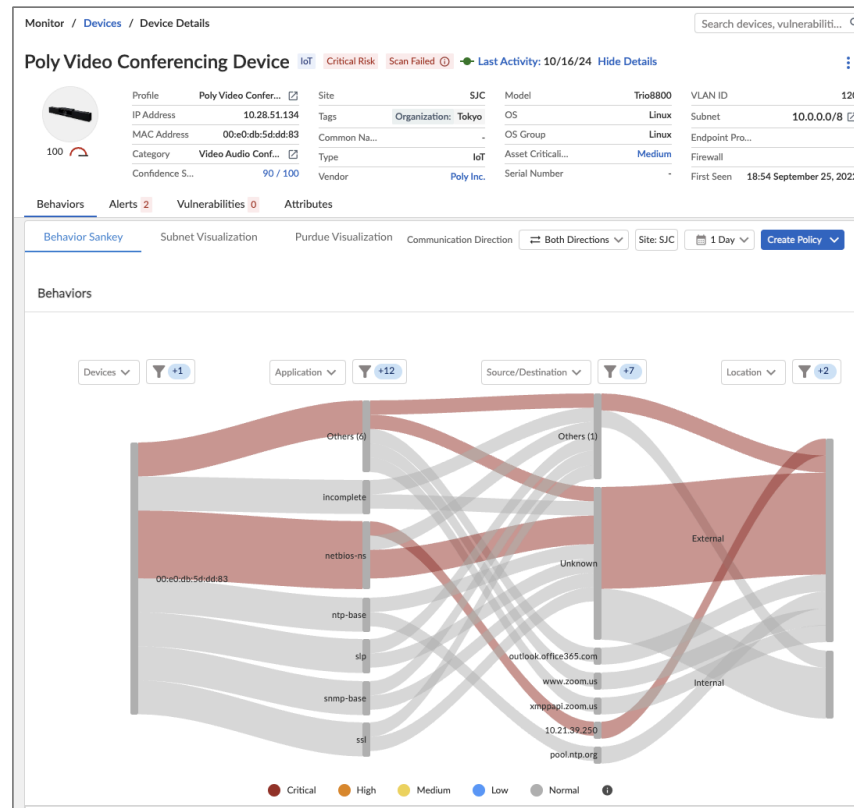
Figure 9 Inventory

Inventory (73,976)								
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>								
Status	Risk	↓	Device Name	Profile	Vendor	Model	OS	
<input type="checkbox"/>		100	Poly Video Conferencing Devi...	Poly Video...	Poly Inc.	Trio8800		
<input type="checkbox"/>		99	Zebra Label Printer	Zebra Lab...	Zebra Tec...	ZT410	Link-OS	
<input type="checkbox"/>		99	Axis Communications Networ...	Axis Com...	Axis Com...	P3265-LVE	Linux	
<input type="checkbox"/>		99	Cisco IP phone	Cisco IP P...	Cisco Syst...	CP-8861	Cisco IOS	
<input type="checkbox"/>		99	Crestron Building Automation...	Crestron B...	Crestron	TSW-730	Embedded	
<input type="checkbox"/>		96	c4:2f:90:89:90:b9	Hikvision ...	Hikvision		Linux	
<input type="checkbox"/>		96	F5 Networks Device	F5 Networ...	F5 Networ...	Device XX...		
<input type="checkbox"/>		96	BrightSign Signage Media Pla...	BrightSign...	BrightSign	XT1144	BrightSign...	

Figure 10 shows details about a Poly Video Conferencing device. These details include the following:

- Risk score
- Device identity details such as the firmware version, serial number, model, OS version, and site
- A security summary
- Additional details such as network traffic, applications, and the device's network use

Figure 10 Details about Poly Video Conferencing Device



In the Inventory pane, you can also view the various attributes Enterprise IoT Security Plus collects during the device discovery by clicking on the Columns icon (three vertical bars) on the right. All the attributes listed, regardless of whether they are selected for display, are collected during device discovery.

Figure 11 Attributes collected by the Enterprise IoT Security Plus by default

The 'Find a column' dialog box displays a list of attributes organized into five columns: Basic, Custom Attribute, Identity, Mobile, and Network. Each attribute has a checkbox next to it, indicating whether it is selected for display. The 'Basic' column includes attributes like Status, Device Name, Profile, IP Address, MAC Address, Category, Confidence Level, Confidence Score, Description, Site, Common Name, Distinguished Name, SAM Account Name, Tag, and User Defined Type. The 'Custom Attribute' column includes Zone Name, test, test2, Asset Criticality, and Purdue Level. The 'Identity' column includes Type, Vendor, OUI Vendor, Model, OS, OS Support, Infrastructure Device, OS Version, Serial Number, Department, Asset Tag, Location, AE Title, and AP Location. The 'Mobile' column includes Mobile Equipment Identity, Mobile Subscriber Identity, Mobile Subscriber ISDN, Mobile APN, Radio Access Technology, Mobile Base Station Code, Mobile Area Code, Mobile Network Code, Mobile Country Code, Mobile TAC, Network Slice, and Mobile Device. The 'Network' column includes VLAN ID, VLAN Description, VLAN ACL, Interfaces, Subnet, AD Groups, Wired - Wireless, DHCP, Network Location, Connected Switch, Switch Port, Switch IP, Switch MAC, Network Segments, Source, CMMS Source, CMMS Category, CMMS State, AD Domain, AD Username, NAC Source, NAC Profile, and NAC Authentication.

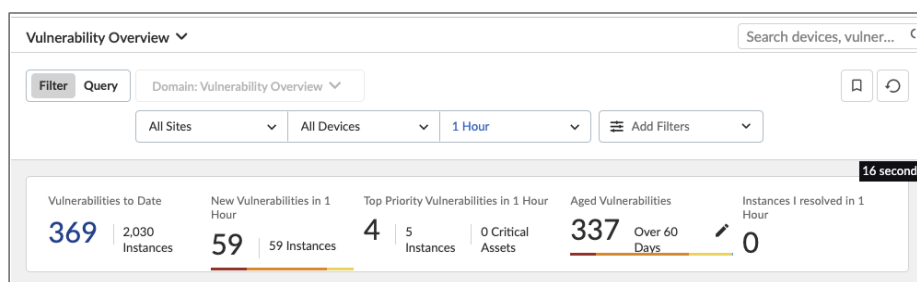
Risk Assessment

The first step in securing your network is discovering and understanding your security risks. The IoT Security app provides risk assessment of your discovered IoT devices, including their current risk level, vulnerabilities, and generated security alerts.

IoT Device Vulnerabilities

The Vulnerabilities > Vulnerability Overview page provides an overview of your network's vulnerabilities, including how many vulnerabilities there are per severity level, based on the filter configured. In the following example, the query is for the All sites and for all the Devices and the time period is one hour. These vulnerabilities are categorized as critical, high, medium, or low.

Figure 12 Vulnerability Overview



When you click on the New Vulnerabilities in 1 Hour, the All Vulnerabilities tab displays a list of vulnerabilities, sorted by the priority of vulnerability. Each vulnerability includes a link to where you can view further details, shown in Figure 13.

Figure 13 Vulnerabilities

Vulnerabilities (59)

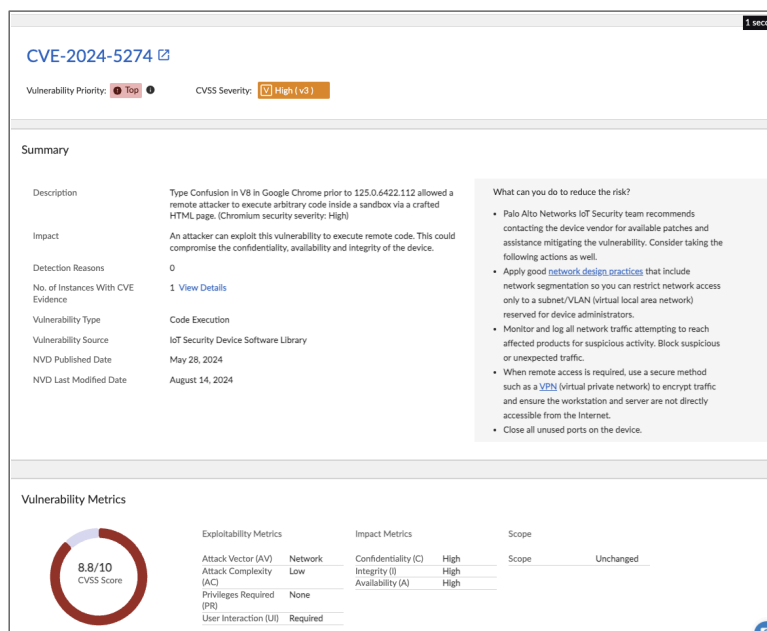
59 instances were identified for the following vulnerabilities.

Priority

Vulnera...

The Vulnerabilities Details page, shown in Figure 14 provides a description of the vulnerability and essential details about it, such as its type, what its impact is, and recommended actions for remediation. From the Vulnerabilities Details page, you can click the CVE number and obtain more details about the CVE.

Figure 14 Vulnerability details of a selected vulnerability



All instances of the vulnerability are listed in a table. You can view more details by selecting a device. Each instance has one of the following statuses, which you change as needed:

- **Detected**—Indicates a newly detected vulnerability instance. This is the default status.
- **Investigating**—Indicates that you are currently investigating this vulnerability.
- **Remediating**—Indicates that you are actively taking action to remediate this device.
- **Resolved**—Indicates that you have either resolved or chosen to ignore the issue. You must provide a reason to change a status to Resolved.

To aid anyone viewing the status of a vulnerability instance, you can add notes. You can assign an instance to a colleague by entering their username or email address. This notifies them to investigate and resolve the instance.

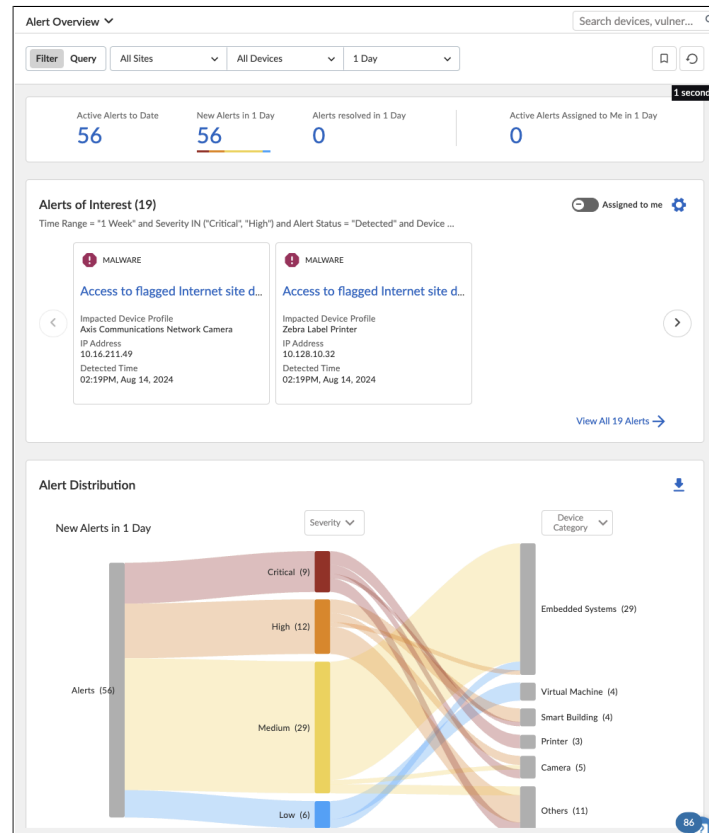
Security Alerts

The Alerts > Security Alerts page provides insight into security alerts based on device settings and network behavior. ML algorithms learn normal device behavior and detect abnormal behavior. The IoT Security app analyzes traffic patterns (including traffic flow to and from devices) and threats (obtained from logs generated by NGFWs).

Unsecured device settings, such as default usernames and passwords, trigger security alerts. Other alert triggers can include suspicious behavior (such as multiple login attempts from or to a device), multiple DNS lookup failures, and detected reconnaissance activities (such as port sweeps).

The Security Alerts page provides an alert summary that shows the number of active alerts, alert distribution per device category, and a table of alerts that you can examine in further detail. It also provides an important summary that management can use to quickly assess the current threats. By default, the page shows the status of all active alerts.

Figure 15 Security alerts



The Alerts table lists each alert, which you can click in order to see more detail. The table lists alerts by severity and shows the impacted devices, device category, location of the device, and when it was detected. You can change the sort order of each column, from ascending to descending and vice versa.

Figure 16 Alerts table





















Alerts (56)					
<input type="checkbox"/>	Severity	Alert Title	Status	Impacted Devi...	Device Catego...
<input type="checkbox"/>		Manufacturer default username and password in http login	Detected 	867186046686...	Tracking and Loc...
<input type="checkbox"/>		Manufacturer default username and password in http login	Detected 	Axis Communica...	Camera
<input type="checkbox"/>		Access to flagged Internet site detected	Detected 	Poly Video Conf...	Video Audio Con...
<input type="checkbox"/>		Access to flagged Internet site detected	Detected 	Cisco IP phone	IP Phone
<input type="checkbox"/>		Access attempt to flagged Internet sites detected	Detected 	10.21.23.22	Network Securit...
<input type="checkbox"/>		Insecure hosted telnet service	Detected 	00:1d:9c:c5:40:40	HMI Panel
<input type="checkbox"/>		Access to flagged Internet site detected	Detected 	BrightSign Signa...	Digital Signage
<input type="checkbox"/>		Microsoft Windows SMB NT Rename Buffer Overflow Vu...	Detected 	Crestron Buildin...	Smart Building
<input type="checkbox"/>		HTTP Authentication Brute Force Attempt Detected	Detected 	Axis Communica...	Camera
<input type="checkbox"/>		Anonymous netbios-ssn login attempt	Detected 	Crestron Buildin...	Smart Building

Figure 17 shows an example alert where the device accessed a flagged internet site. The alert shows when the alert was detected, severity of the alert, the client and server IP addressing, and details on the number of sessions and login count.

Figure 17 Alert details

Access to flagged Internet site detected

Severity **Critical** Status **New** Assignee **Assign** Traffic Restricted **No**

Poly Video Conferencing Device

Client

IP: 10.28.51.134
 Category: Video Audio Conference
 Site: SJC
 Confidence Level: High

146.0.32.144

Server Internet

Port: 80
 Protocol: http

Country: NL
 Web Category: Malware
 Web Reputation: 10

Alert Events

Alert Detected
 17:19, August 14, 2024

Some services and hosts at specific IP addresses are flagged by up-to-date security research as being risky or having malicious intentions. Such websites are known to mislead users into providing personal information, deceive them into downloading viruses or malware, and even download malware just because users visited the site (something known as a drive-by download). Accessing services at these IP addresses risks infection and poses a security risk to the device.

A deviation from the normal baseline was detected.

local port	59072
risky category	Malware
risky remote	146.0.32.144
host	
payload bytes	3634
received	
payload bytes transmitted	956

The alert details also include the impact section, which explains how the issue affects security of the device, network, or user. This section also provides recommendations for how to address the issue.

To obtain IoT alert information, you do not have to constantly monitor the IoT Security app. You can configure automatic notifications that are sent, through either email or text, when security alerts occur or when another user assigns an alert to you. After investigating an alert, based on its importance and urgency, you can view the recommendations for resolution and take appropriate actions to reduce the risk.

Risk Reduction

The IoT Security app can determine what mitigation options are available for securing an IoT device. Each vulnerability or alert provides suggestions for reducing the risk associated with the current state of a device.

Remediation steps might include the following:

- **Isolating the device**—If a device has been infected by malware, you need to quarantine the device from the rest of the network until you have removed the malware. If the device has a supported OS for endpoint security management, you should update to that OS.
- **Updating the device**—If a device has a vulnerability from outdated software or patches, you need to update the device.
- **Replacing credentials**—If the device is using its default username and password, you need to change these credentials.

You have two options for responding to alerts and reducing risks based on the information provided by the IoT Security app:

- Automated Zero Trust policy recommendations with Device-ID
- Network security

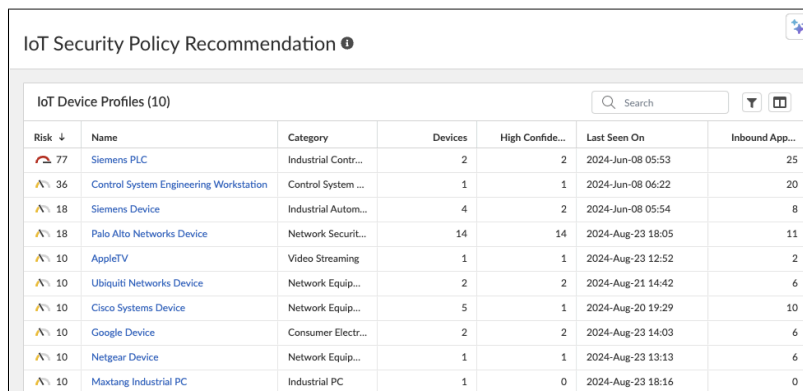
Automated Zero Trust Policy Recommendations with Device-ID

For prevention and securing your network, the NGFW applies multiple traffic-filtering capabilities through security policies. NGFWs are stateful, and all traffic passing through the firewall is matched against a session, which is then matched against a security policy rule. Policy rules use multiple match criteria in order to control network traffic, including applications, users, content, and devices. For devices, the NGFW uses Device-ID to apply security policies that restrict or allow access to and from devices.

Device-ID allows you to create policy rules that are based on a specific device, regardless of changes to its IP address or location. Device-ID allows you to gain context for how events relate to devices and write policies that are associated with those devices, instead of relying on User-ID, locations, or IP address, all of which can change over time. You can use Device-ID in security decryption, quality of service, and authentication policies.

The IoT policy recommendations page in the SCM page shows automatic policy recommendations for control of IoT device traffic based on device profiles. For example, you could have a policy recommendation to block cameras connecting to the internet or to restrict access to a specific network video recorder application.

Figure 18 Policy recommendations



The screenshot shows a web interface titled "IoT Security Policy Recommendation". Below the title is a search bar and a table titled "IoT Device Profiles (10)". The table has columns for Risk, Name, Category, Devices, High Confidence, Last Seen On, and Inbound App. The data is as follows:

Risk	Name	Category	Devices	High Confidence	Last Seen On	Inbound App...
77	Siemens PLC	Industrial Contr...	2	2	2024-Jun-08 05:53	25
36	Control System Engineering Workstation	Control System ...	1	1	2024-Jun-08 06:22	20
18	Siemens Device	Industrial Autom...	4	2	2024-Jun-08 05:54	8
18	Palo Alto Networks Device	Network Securit...	14	14	2024-Aug-23 18:05	11
10	AppleTV	Video Streaming	1	1	2024-Aug-23 12:52	2
10	Ubiquiti Networks Device	Network Equip...	2	2	2024-Aug-21 14:42	6
10	Cisco Systems Device	Network Equip...	5	1	2024-Aug-20 19:29	10
10	Google Device	Consumer Electr...	2	2	2024-Aug-23 14:03	6
10	Netgear Device	Network Equip...	1	1	2024-Aug-23 13:13	6
10	Maxtang Industrial PC	Industrial PC	1	0	2024-Aug-23 18:16	0

Network Security

Network-security solutions are particularly crucial when organizations use IoT devices that process sensitive information that must be protected both in transit and at rest. To protect against the legal and regulatory liabilities that a breach of such data would cause, organizations must ensure that sensitive data is secure. Regulations might also dictate how this data is accessed and secured, such as payment-card industry (PCI) requirements for payment transactions and Health Insurance Portability and Accountability Act (HIPAA) requirements for medical devices that deal with patient information.

For meeting these challenges, the Palo Alto Networks network-security solution combines two practices:

- **Security policy**—Security policy on the firewall restricts or allows specific access to and from your devices. Security policy also includes additional protection mechanisms, such as threat prevention and URL filtering, that you apply to policy rules.
- **Network segmentation**—IoT devices that pose significant risk are segmented into their own virtual network. This reduces the risk of compromise and prevents their compromising devices in other segments. Segmentation also enables the NGFW to apply policy to each segment based on risk posed by specific devices in the segment.

Security Policy

Security policy protects network assets from threats and disruptions and helps to optimally allocate network resources for enhancing productivity and efficiency in business processes. On a Palo Alto Networks firewall, individual security policy rules determine whether to block or allow a session. The determination is based on traffic attributes, such as the source and destination security zone, the source and destination IP address, the application, the user, and the service.

All traffic passing through the firewall is matched against a session, and each session is matched against a security policy rule. When a session matches a rule, the firewall applies the matching security policy rule to bidirectional traffic in that session (client to server and server to client). For traffic that does not match any defined rules, the default rules apply. The default rules—displayed at the bottom of the security rule base—are predefined to allow all intrazone traffic (within a zone) and deny all interzone traffic (between zones). Although these rules are part of the predefined configuration and are read-only by default, you can override them and change a limited number of settings, including the tags, action (allow or block), log settings, and security profiles.

Security policy rules are evaluated left-to-right and from top-to-bottom. A packet is matched against the first rule that meets the defined criteria, and after a match is triggered, subsequent rules are not evaluated. Therefore, the more specific rules must precede more generic ones in order to enforce the best match criteria. Traffic that matches a rule generates a log entry at the end of the session in the traffic log if you enable logging for that rule. The logging options are configurable for each rule and can, for example, be configured to log at the start of a session instead of, or in addition to, logging at the end of a session.

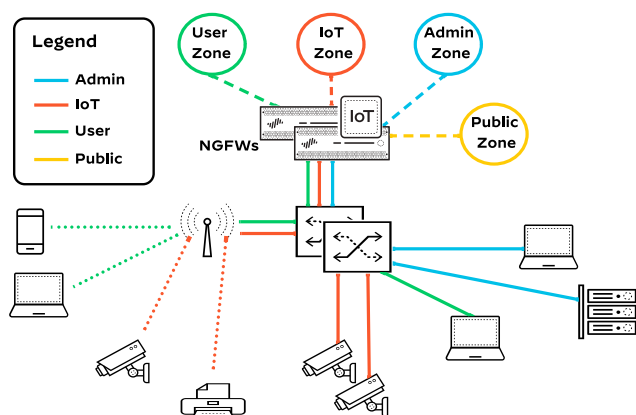
Network Segmentation

Segmentation is grouping devices on the network based on their risk to the organization. Segmentation enables the NGFW to apply policy to each group based on its devices' risk to the organization. Palo Alto Networks NGFWs offer flexible deployment modes and capabilities to segment networks. To control and log traffic, you can use security zones to group physical or logical interfaces.

IoT devices and traditional IT users are often deployed on the same network segments. You should segment IoT devices that pose significant security risk to the organization into their own network. This reduces the risk they can be compromised or that they compromise devices in other segments.

Figure 19 shows a simple network in which different devices are deployed on separate VLANs. For example, IoT devices are on a separate VLAN from the IT administrators and users. On the NGFW, the VLAN interfaces are associated with separate security zones. This allows traffic to be inspected between each zone, as well as to and from the public zone. If an IoT device is compromised on the IoT zone, malicious activity is detected and blocked at the firewall.

Figure 19 Segmenting IoT devices



When you cannot introduce segmentation into your environment, you can still achieve a level of segmentation on the NGFW by using security policy with Device-ID. Device-ID allows you to group devices and control device access to and from the network.

Common Security Threats

IoT devices pose several different kinds of threats within your organization. Three common vulnerabilities within your network are the following:

- Legacy IoT devices no longer receiving patches.
- IoT devices with access to sensitive data.
- Mission-critical IoT devices that are difficult to patch.

To determine if you face any of these threats, we recommend that you discover the IoT devices on your network. After you have discovered any IoT devices that pose a threat, you should execute a plan that mitigates the threat by patching them, removing them, or segmenting them from your critical applications and data.

Threats can be inbound and outbound. Determining the traffic flow between IoT devices is important to securing your network. This could include devices that are low risk internally but that you do not want to access the internet. As you build your security policy, identifying these types of devices, what they can access, and who can access them is important.

IoT Devices No Longer Receiving Patches

Your organization might be using legacy IoT devices that can no longer receive patches. For example, HVAC systems often have this issue. HVAC systems typically do not support any type of endpoint-protection software, so you do not have any method of securing them directly. One way to secure them is to block traffic to and from the HVAC systems, therefore segmenting them from specific users, critical applications, and data. An NGFW provides this level of control and threat prevention and secures all traffic flows to and from the devices. Because HVAC systems often leverage platforms outside the local network, you cannot simply block traffic to and from external destinations.

The NGFW provides policy rules that give you granular control, allowing only permitted users (identified with User-ID) and permitted applications (identified with App-ID) to communicate with specific devices (identified with Device-ID). Through previous device discovery based on the device attributes, Device-ID identifies the specific device type and manufacturer (example: a Honeywell HVAC system) and identifies the individual devices instead of just their IP addresses. This allows policy rules to specify which traffic flows are permitted between the specific devices and other systems with which they need to communicate, without worrying about how they are connected on the network. For example, a facilities management station is permitted to connect to smart thermostats and to manage the HVAC systems locally or remotely from the internet.

The IoT Security app provides the NGFW with dictionary files and IP-address-to-device mappings. With the information provided, you create a security policy rule that controls traffic flows to and from the device by using App-ID, User-ID, and Device-ID. Even though you cannot upgrade the device, you are still protecting the device from potential threats. And if the device should become compromised, you are also protecting the rest of the network by limiting its access.

In addition to applying security policy, you use segmentation to provide an additional layer of security. It is recommended that you isolate un-patchable devices into separate network segments. If you segment these devices and they still require communication with other devices or applications, you need to implement proper security policies. With a NGFW and strong security policy configuration, these devices are more secure as traffic moves across segments, and you monitor for suspicious activity.

IoT Devices with Access to Sensitive Data

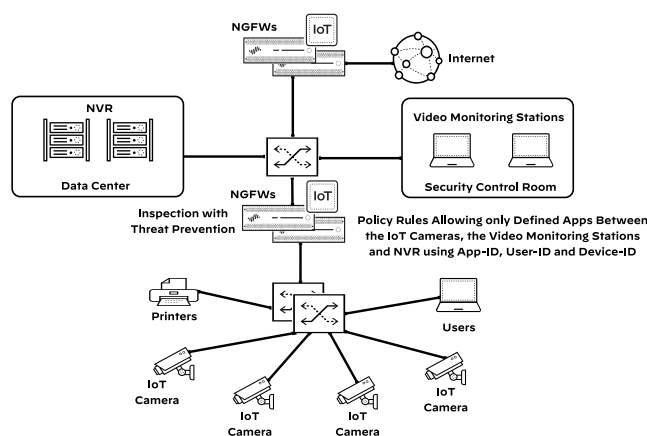
We recommend that you protect IoT devices that deal with sensitive information because any loss or exposure would provide significant risk to the business. Regulations may also dictate how this data is accessed and secured, such as PCI for payment transactions and HIPAA for medical devices that deal with patient information. Such devices can include video surveillance, payment-processing machines, and any type of medical device.

When securing IoT devices that access sensitive data, it is critical that you segment and monitor the devices and apply policy that controls traffic flow. Device-ID allows you to use security policy rules in order to control traffic between such devices. Data-loss prevention adds an additional level of security, and you can apply it as a subscription in the NGFW.

In Figure 20, IoT cameras are providing security surveillance and are streaming to video-monitoring stations. The perimeter NGFWs protect internet traffic, and inline campus NGFWs protect traffic on the LAN.

Video images are stored on network video recorder (NVR) servers. Using Device-ID, the IoT Security app identifies the devices and allows the NGFW to specify the device type in security rule policy. Additionally, User-ID and App-ID provide granular control of which users and applications can communicate with the IoT security cameras.

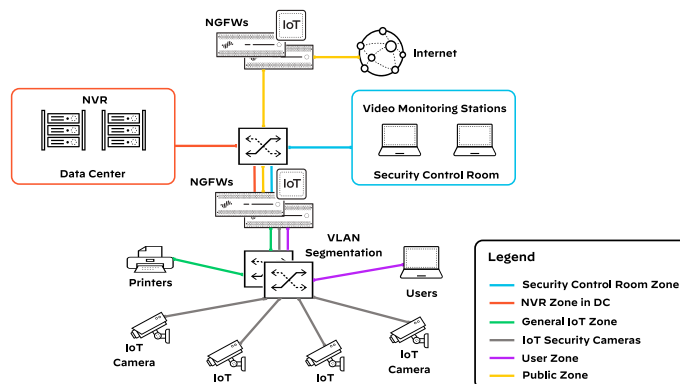
Figure 20 Securing video surveillance with security policy



Highly sensitive data should reside on dedicated resources, and you should group those resources in their own network segment. For example, cameras should be segmented into their own security zone.

Figure 21 depicts a network with IoT security cameras the security control room accesses. Images are stored on the NVR system. Segmenting the network into separate security zones protects the sensitive data from compromise by other devices that would normally exist on the same segment. This reduces the attack surface and makes it easier to apply granular security rules on the NGFW for access in and out of the zone.

Figure 21 Segmenting video surveillance with security zones



Mission-Critical IoT Devices That Are Difficult to Patch

Some continuously operating, mission-critical devices receive updates infrequently. These devices might include robotics and sensors on a factory production line, video surveillance, and medical devices. Because these devices receive infrequent updates, you need to protect them and protect your key assets from a mission-critical device that might have been compromised.

To do so, you implement granular visibility, control, and monitoring. Until you update the devices, you use policy within the segment to control data flow, and you monitor for any abnormal behavior. The NGFW provides granular control of policy rules through User-ID, App-ID, and Device-ID, which allow you control and secure the communications of IoT devices.

These devices often operate 24/7. The NGFW secures all traffic between production lines and the operations and engineering stations, denying all other sessions and inspecting the traffic for threats. Policy rules are configured with App-ID, User-ID, and Device-ID, which ensures that only permitted users and required applications are allowed between the production lines and the operations and engineering stations.

In this type of environment, you place the production lines into separate VLANs on a switch. Adding VLANs and multiple security zones provides an additional security layer, which avoids exposing the robotic devices to anything else on the local network that could affect the operations of the equipment.

Continuous IoT Threat and Behavior Analysis

The IoT Security solution enhances existing security subscriptions by providing device context, providing safe web access, and blocking DNS. For complete IoT security, you need to enable the security subscriptions on the NGFW in order to block these threats.

Multiple Palo Alto Networks threat-prevention capabilities are built into security policies in the form of *security profiles*. Security profiles are attached to security policy rules and provide capabilities such as antivirus, vulnerability protection, antispyware, URL filtering, file blocking, data filtering, and WildFire® analysis. You add these profiles to policy rules where you want to add this capability, such as those rules securing and identifying devices with Device-ID. The threat prevention capabilities are delivered as security subscriptions on the NGFW.

The security subscriptions are the following:

- **Threat Prevention**—Provides comprehensive protection against all threats, irrespective of port, protocol, and encryption. When you enable Threat Prevention on an NGFW, the NGFW scans, inspects, classifies, and blocks threats in a single pass. The Threat Prevention subscription includes antivirus, vulnerability protection, and antispware.
- **URL Filtering**—Enables you to configure the NGFW to identify and control access to websites at a per-user level and compares all web traffic against the URL-filtering database, PAN-DB, which contains millions of URLs grouped into approximately 65 categories. You can classify sites based on their content, features, and risk. The malware and phishing URL categories in PAN-DB update in real time, which means that if a first attempt to access a malware or phishing is treated as unknown, URL Filtering matches subsequent attempts against the updated URL-filtering database and prevents user access. For fast and easy access to frequently visited URLs, PAN-DB provides high-performance local caching.
- **DNS Security**—Is also another recommended Palo Alto Networks security subscription. Enable DNS Security on the NGFWs in order to protect and defend your network from advanced threats that are using DNS. The DNS Security service leverages machine learning and predictive analytics to provide real-time DNS request analysis. The analysis enables production and distribution of DNS signatures that are specifically designed to defend against malware that uses DNS for command-and-control and data exfiltration.
- **WildFire**—Is a cloud-based threat analysis service that acts as a threat-intelligence sandbox in the cloud. All unknown threats are converted to known threats, and the threat-intelligence data is fed back to the NGFWs.

Because adversaries target IoT devices, Threat Prevention, URL Filtering, DNS Security, and WildFire subscriptions are an important part of implementing the IoT Security solution that you should enable on the NGFW.

Enhanced Traditional IT Security Policies with Device-ID

Using Device-ID on your firewall or to push policy from SCM, you can get device context for events on your network, write policies based on devices, and enforce security policy. User-ID provides user-based policy, and App-ID provides app-based policy. Although Device-ID provides policy rules that are based on a device, regardless of changes to its IP address or location. By providing traceability for devices and associating network events with specific devices, Device-ID allows you to gain context for how events relate to devices and write policies that are associated with devices instead of with users, locations, or IP addresses, all of which can change over time. You can use Device-ID in security, decryption, quality of service (QoS), and authentication policies.

For Device-ID features to be available on a firewall, you must purchase an IoT Security subscription and select the firewall during the IoT Security onboarding process. To permit connections to the IoT Security app, a firewall needs a device license, and to permit connections to the logging service, it needs a logging service license. To identify and classify devices, the app uses metadata from logs, network protocols, and sessions on the firewall. This does not include private or sensitive information or data that is not relevant for device identification.

After the IoT Security app identifies and classifies the devices by using the NGFW already in your network, Device-ID can leverage this data to match devices with policy rules and provide device context for network events. Through the visibility, the firewall provides for traffic, apps, users, devices, and threats. You can trace network events back to individual devices and obtain security policy rule recommendations for securing those devices.

The IoT Security app discovers and identifies all devices on the network. After the app identifies a device as a traditional IT device, the IoT Security app stops tracking the device's traffic and behavior patterns. However, the Device-ID information is available for all devices so it can be used to enhance the traditional IT security policies of non-IoT devices.

For optimal deployment and operation of Device-ID, we recommend the following best practices:

- Deploy Device-ID on firewalls that are centrally located in your network. For example, if you have a large environment, deploy Device-ID on a firewall that is upstream from the IP address management device. If you have a small environment, deploy Device-ID on a firewall that is acting as a DHCP server or in the path of the DHCP server being used for the site.
- During initial deployment, allow Device-ID to collect metadata from your network for at least fourteen days. If devices are not active daily, the identification process may take longer.
- Write device-based policy in order of your most critical devices to least critical. Prioritize policies by the following criteria:
 - Class (secure networked devices first)
 - Critical devices (such as servers or MRI machines)
 - Environment-specific devices (such as fire alarms and badge readers)
 - Consumer-facing IoT devices (such as a smart watch or smart speaker)
- Enable Device-ID on a per-zone basis for internal zones only.

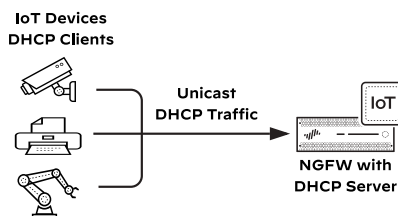
DESIGN CONSIDERATIONS

The IoT Security solution requires traffic visibility in order to maximize IoT device discovery, risk assessment, anomaly detection, and threat detection. Accurate firewall policy enforcement also relies on precise device identification and baseline of the normal traffic for each device. The following sections describe a few key design considerations.

DHCP Traffic: Key to Device Classification

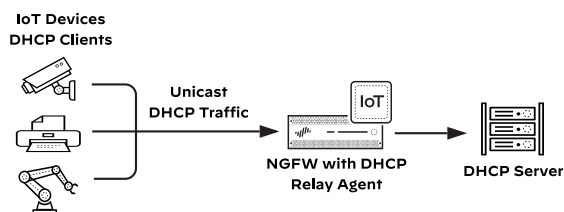
DHCP traffic is of particular importance to the IoT security solution because it provides a way to create an IP address-to-device mapping that is required for classification. However, a firewall typically generates an EAL entry only when the firewall receives a unicast DHCP message. For example, when the firewall is the DHCP server for the attached VLANs, it generates the EAL entry.

Figure 22 NGFW with internal DHCP server



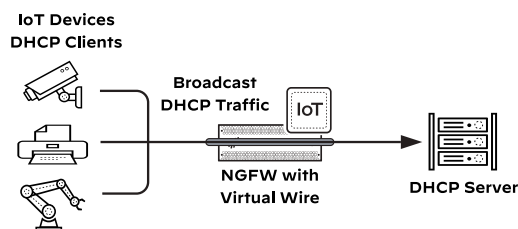
The firewall also sees unicast DHCP traffic when there is a centralized DHCP Server and either the firewall or another local device acts as a DHCP relay agent and sends the traffic through the firewall. The figure below illustrates another common use case where the firewall generates EALs for unicast DHCP traffic because it is in the traffic flow between the DHCP Relay agent and the DHCP Server.

Figure 23 NGFW with a DHCP relay agent



When the firewall sees the packet on a virtual wire interface with multicast firewalling enabled, the firewall also generates an EAL entry for broadcast DHCP traffic, as shown below.

Figure 24 NGFW with a virtual wire interface



For devices that use DHCP, their MAC addresses are the best choice as the unique identifier. The following approaches are available to acquire the IP/MAC binding.

Table 1 DHCP approaches to acquire IP/MAC binding

Approach	Perimeter FW	Campus FW
Inline - Layer 2	Yes	—
Inline - Layer 3	—	Yes
TAP - Layer 2	Yes	—
TAP - Layer 3	Yes	Yes
DHCP Relay	Yes	Yes
DHCP Server Log Ingestion	Yes	Yes
ARP Traffic	Yes	Yes
SNMP Query	Yes	Yes

Inline, TAP, and DHCP Relay Point

The inline and TAP interface approaches work similarly. When the NGFW directly sees traffic, each security policy logs the related DHCP information.

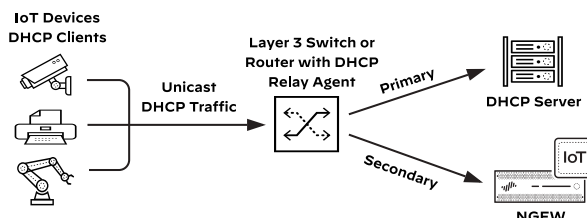
NGFWs directly processing the DHCP traffic have the following benefits:

- DHCP leases provide the IP/MAC binding in real time. It is the best way to track the IP changes for each device.
- Not only the native broadcast-base DHCP traffic within VLAN but also the DHCP-helper/DHCP server traffic can provide the data.
- It is important to see both the DHCP request and response traffic.
- DHCP options provide additional details when identifying IoT devices.

The DHCP Relay Point option is different than the DHCP Relay Agent option shown in Figure 23. In this example, an external network device like a Layer 3 switch or router has the DHCP Relay Agent, but the NGFW is not in the direct path of the DHCP server.

Instead of moving the NGFW or the DHCP server, you configure the NGFW as a secondary DHCP server. The unicast DHCP traffic is sent directly to the NGFW from the Layer 3 switch or router for logging, and the information is processed by the IoT Security app.

Figure 25 NGFW as a DHCP relay point

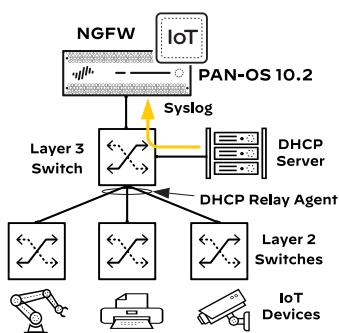
**Note**

Because the IP/MAC mapping is processed in the cloud, you can send the DHCP traffic to any NGFW in the correct physical location.

DHCP Server Log Ingestion (PAN-OS 10.2)

When a DHCP server leases IP addresses to devices, it generates a log that contains the IP and MAC addresses involved in the event. When the DHCP server is capable, the logs can be pushed to the NGFW through syslog. The NGFW is acting as a syslog server in this situation, and the logs are forwarded to the IoT Security app in order to parse and retrieve the IP/MAC binding.

Figure 26 DHCP server log ingestion



All DHCP server log formats are supported, and the IoT Security solution validates the following:

- InfoBlox
- Microsoft
- Cisco

ARP Traffic

Using address-resolution protocol (ARP) logs, the IoT Security app learns IP address-to-MAC address mappings and adds devices with static IP addresses which are not discovered through DHCP. However, by the very nature of ARP broadcasts, this works only for devices within the same Layer 2 broadcast domains as the reporting firewalls.

In this approach, the NGFW processes the Layer 2 VLAN traffic in one of two ways:

- The NGFW has a Layer 3 interface inside each VLAN and is the default gateway of the subnets.
- The Layer 2 traffic is copied and sent to the NGFW's TAP interface through SPAN.

The benefits to this approach are as follows:

- The ARP traffic is used to capture the IP/MAC address assignments for DHCP devices.
- MAC addresses of static-IP devices can also be retrieved, so there is no need to deal with manually adding static IP separately as described in later sections.

SNMP Crawling of Static IP Addresses

To retrieve device information from devices that are deployed with static IP addresses, the NGFW and the ION devices support SNMP polling. This feature is important when you want to discover devices that don't generate DHCP traffic because they have static IP addresses. When SNMP feature is enabled in any device, an SNMP engine is created in it by default. This engine is responsible for collecting and transmitting data from network devices to the network management system, processing management commands, and sending alerts for specific events. When SNMP is enabled in NGFW or the ION device, they become an SNMP management system, and they start communicating with network switches to obtain information about the devices attached to them. They begin by establishing trust with an entry switch, usually at the aggregation layer, by sending it an SNMP community string for read-only access. After connecting, the NGFW or the ION device queries the switch's ARP table for information about attached devices.

The SNMP engine in ION or NGFW learns the switch name and IP address, device MAC address and IP address, and for Cisco Catalyst switches, the name of the physical port on the switch to which a device connects. The engine also queries the entry switch for the IP addresses of neighboring switches on the network. It continues to collect device information and get lists of neighboring switches until all switches are discovered. You use multiple integration jobs to cover segments of networks that are not discoverable through CDP/LLDP neighbors.

After collecting information through SNMP, the ION device or NGFW updates the IoT security application details about existing devices and also adds newly discovered devices to its inventory.



Note

Using SNMP to collect information from network switches requires the purchase and activation of a third-party integration add-on. The basic integration plan includes a license for three integration add-ons, one of which you can use for SNMP discovery.

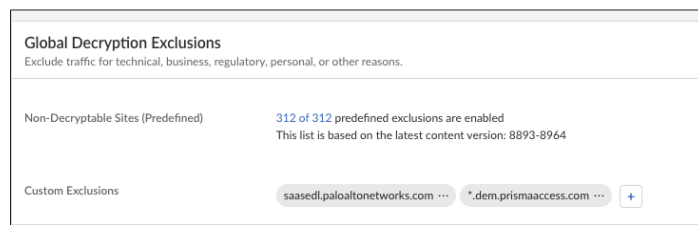
Decryption for IoT Devices

Organizations rely on encryption to secure applications and services, with over 85% of internet traffic being encrypted, which adversaries exploit to hide malicious activities. To mitigate this, based on decryption policies, Prisma Access decrypts inbound and outbound SSL/TLS connections, enforces security rules to protect against threats, and re-encrypts the traffic. It preserves the original cryptographic settings and allows specifying supported protocol versions and cipher suites in order to mitigate risks from older protocols. Additionally, it ensures the validity of certificates through Certificate Revocation List/Online Certificate Status protocol checks.

In this design, you use the SSL forward proxy default configuration to decrypt all outbound internet traffic from all IoT devices. To secure the connection, SSL uses certificates to establish trust between the client and server. Most commonly, to establish this trust, an organization uses its own public key infrastructure to generate a trusted signing certificate for Prisma Access. The endpoints must install the Prisma Access Root CA certificate into their certificate store so that the client session to Prisma Access can be established.

In case, the IoT endpoint does not support installing Prisma Access root certificate, then you should configure the application the IoT device is trying to reach as a hostname or use a wildcard domain as a custom decryption exclusion.

Figure 27 Decryption exclusions



DESIGN MODELS

You secure IoT traffic going to the Internet from remote sites deployed by using NGFW or by using Prisma SASE. You discover devices and then identify and mitigate the security risks for IoT devices belonging to either remote site. The IoT Security portal recommends the security policy for your remote sites, and by using SCM, you apply this on the NGFW or on Prisma Access. This solution works when the remote sites are deployed in either Layer 2 or Layer 3 mode. The data from either of the remote sites is logged to SLS and managed through SCM, which ensures that consistent security policy is applied to both types of remote sites.

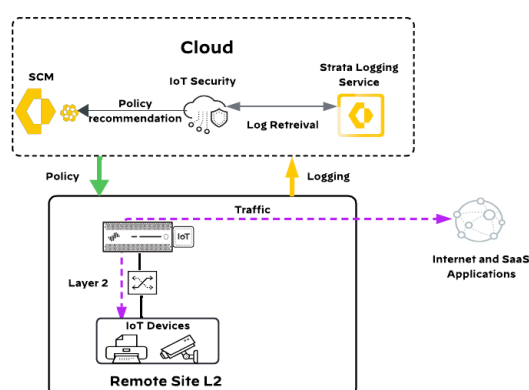
On-Premises NGFW

For the best visibility, all traffic should be collected from the access switches and sent to the perimeter NGFW. However, this is not a typical NGFW deployment model. Also, it is not practical to collect data from all access switches, even though it might be possible using port mirroring at a Layer 2 site.

At branch locations with a simple Layer 2 network, the NGFW acts as the Layer 3 device between the LAN and the WAN interfaces. For the purposes of device discovery, the firewall can be the DHCP server, or if your DHCP servers are centralized, the firewall can provide the DHCP Relay function. If you have data centers or headquarter locations, the NGFW at the head end can also apply policies by using the Device-ID information learned from the IoT Security app.

When IoT Security is enabled in a Layer 2 branch NGFW, all traffic traversing the NGFW is subject to policy-based Device-ID enforcement. This means internet traffic and application traffic to and from devices that traverse the perimeter NGFW are tracked. Specific security policies are created to automatically enforce traffic rules and allowable applications, which reduces the attack surface of IoT devices communicating on the internet and in the branch. The perimeter NGFW sees the north-south and most of the east-west traffic, so it is in the flow to provide enforcement as needed.

Figure 28 Layer 2 design model for on-premises NGFW



This Layer 2 design model has the following characteristics:

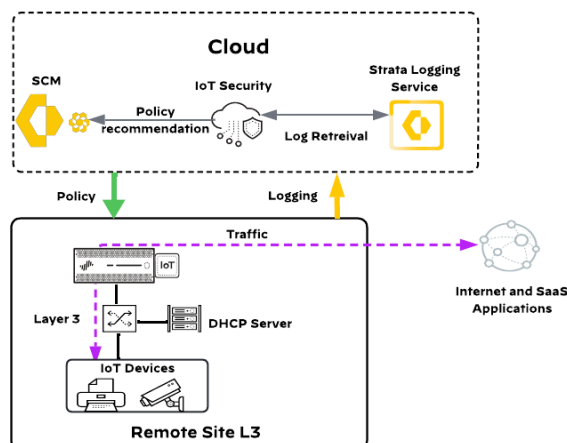
- The NGFW acts as the DHCP server, or if DHCP servers are centralized, the NGFW provides the DHCP Relay function.
- For visibility and policy enforcement, the NGFW sees north-south and most of the east-west traffic.
- Traffic traversing the NGFW is subject to policy-based Device-ID enforcement.
- Zero Trust security policies are created automatically, reducing the attack surface of IoT devices.
- The NGFW at the headend can use the Device-ID information for security policies.

The next-best location in the network to retrieve data is at the aggregation layer where Layer 2 turns to Layer 3. At this point in the network, the majority of the Layer 2 data is available, which provides a balanced solution between good visibility and ease of deployment.

At branch or campus locations with a Layer 3 network, it is recommended you use a campus NGFW at the aggregation layer boundary while allowing the perimeter NGFW to retain its original purpose of protecting the site from traffic to and from the internet. Both firewalls send their logs for analysis to the IoT Security app, and the perimeter firewall provides the north-south visibility, while the campus firewall provides east-west visibility.

The campus NGFW at the aggregation layer is required for policy enforcement of east-west traffic. The perimeter NGFW is used for north-south traffic policy enforcement. It is not possible to apply security policies to east-west traffic spanned to a TAP port. For this reason alone, it is better to start out with a second NGFW for visibility, so when the time comes to apply enforcement policies by using Device-ID, there are no additional changes required.

Figure 29 Layer 3 design model for on-premises NGFW



This Layer 3 design model has the following characteristics:

- A Layer 3 switch or router provides the DHCP relay function.
- A perimeter NGFW sees north-south traffic, for visibility and policy enforcement.
- Traffic traversing the NGFWs is subject to policy-based Device-ID enforcement.
- Zero Trust security policies are created automatically, reducing the attack surface of IoT devices.

Layer 3 deployments that have only a perimeter NGFW with north-south traffic flows are not sufficient for device visibility, let alone policy enforcement. To increase your device visibility, you use one of the following methods to allow the firewall to see east-west traffic:

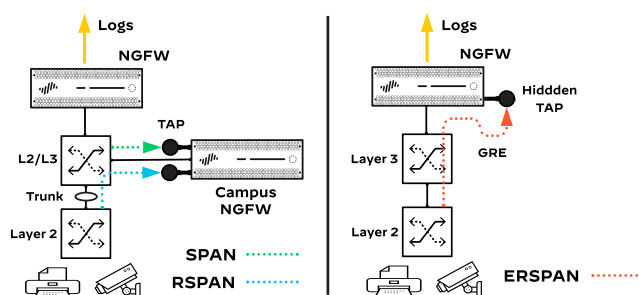
- **SPAN**—Copy local data from the switch to a TAP port. You have two options:
 - The NGFW is in the same room as the switch, and the traffic is copied locally.
 - The NGFW is in a different room or building, and the traffic is copied from the switch directly through a dedicated fiber cable.

- **RSPAN**—Copy data from a remote switch that has a Layer 2 trunk port connected to the primary switch. RSPAN traffic cannot pass through a Layer 3 boundary but can be used over trunk ports. Managing RSPAN requires patience and great care in order to avoid loops in the network.
- **ERSPAN**—Copy data through a Layer 3 GRE tunnel to a hidden TAP port on the NGFW. This method makes it easy to scale supporting multiple source switches. The GRE tunnel seamlessly passes traffic through a routed IP network. No additional cabling is required, so you can do the deployment 100% remotely.

**Note**

Spanning traffic to TAP ports increases visibility but does not assist with policy enforcement. For policy-enforcement purposes, a campus NGFW must be in line with the traffic flow.

Figure 30 Increase visibility with SPAN, RSPAN, and ERSPAN for Layer 3 sites



Prisma SASE

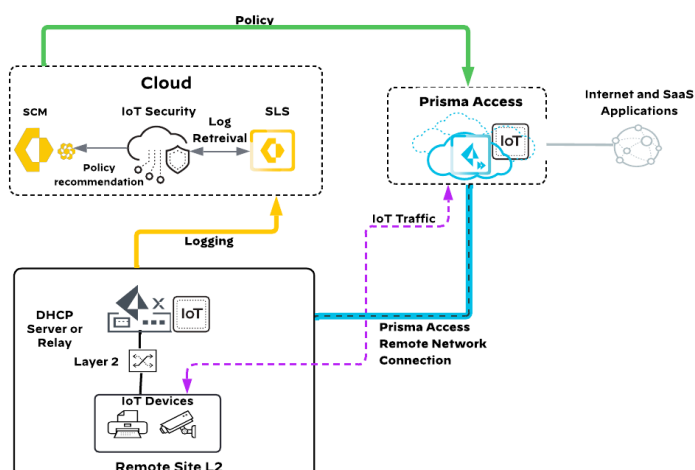
At branch locations with a simple Layer 2 network, the ION device acts as the Layer 3 device between the LAN and the WAN interfaces. For the purposes of device discovery, the ION device can be the DHCP server, or if your DHCP servers are centralized, the ION device can provide the DHCP Relay function. The ION device would send this log information to the SLS. The IoT Security portal retrieves these logs and discovers the IoT devices in the branch.

In addition, the IoT Security portal allows administrators to build Zero Trust policies recommended for the branch that can be applied to Prisma Access. When these policies are applied in Prisma Access, all the internet traffic traversing the branch is subjected to the newly created policy.

**Note**

The more detailed data provided in the logs, the better the IoT Security app can identify devices. There are always trade-offs between deployment complexity and cost, so IoT security administrators must examine both sides of the equation when making their decision.

Figure 31 Design model for Layer 2 sites using Prisma SASE

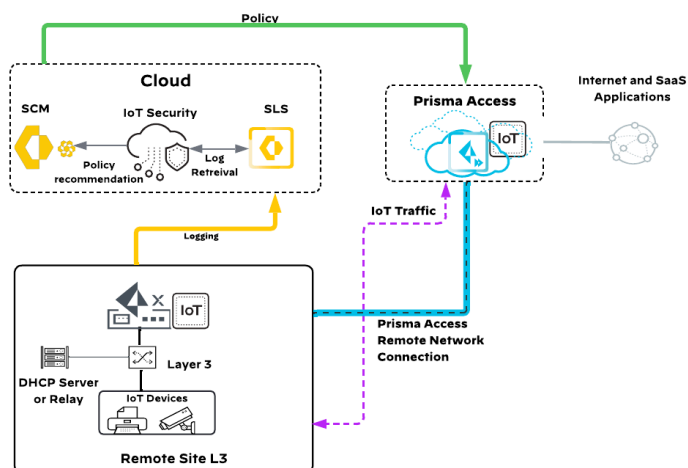


This Layer 2 design model has the following characteristics:

- The ION device acts as the DHCP server, or if DHCP servers are centralized, the ION device provides the DHCP relay function.
- For visibility and policy enforcement, Prisma Access sees north-south traffic.
- Traffic traversing Prisma Access is subject to policy-based Device-ID enforcement.
- Zero Trust security policies are created automatically, reducing the attack surface of IoT devices.

At branch or campus locations with a Layer 3 network, it is recommended that the Layer 3 switch is enabled with the DHCP relay function that sends a copy of DHCP messages to the ION device. The ION device sends this log information to the SLS. The IoT Security portal retrieves these logs and discovers the IoT devices present in the branch.

Figure 32 IoT Security design model for Layer 3 sites using Prisma SASE



Common Security Profiles

Regardless of which deployment you deploy, you should also enable security profiles to prevent known malware, vulnerabilities, and threats in traffic allowed by the security policy. Security profiles enabled in the firewall policies should include the following:

- **Antivirus and WildFire**—Inspect traffic for known antivirus signatures.
- **Anti-spyware**—Prevent infected endpoints from sending malicious traffic to command-and-control systems.
- **URL filtering**—Block command-and-control traffic and access to known-malicious websites.
- **File blocking**—Block files that are known to carry threats.
- **Vulnerability protection**—Protect against buffer overflows, illegal code execution, and other attempts to exploit system vulnerabilities.

Deploying IoT Security for On-Premises NGFW

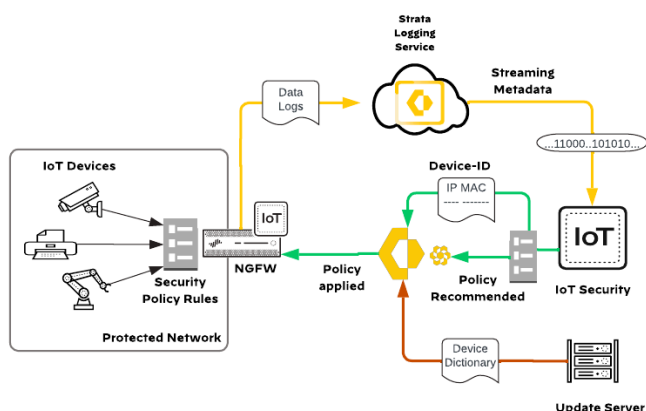
This deployment follows the Small-Site Standard Perimeter Firewall Design Model as described in the **Securing the Branch with On-Premises Network Security: Design Guide**. You should follow the procedures mentioned in this guide and ensure that the firewall is registered successfully with SCM. To understand all aspects of deploying the NGFW using the SCM, you should follow the guidance in the **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**.

Using AI and ML, the IoT Security app automatically discovers and identifies all network-connected devices and constructs a dynamically updating inventory. In addition to identifying IoT and traditional IT devices, the app provides deep visibility into network behaviors, establishing what is normal and recognizing what is suspicious on a per device basis. When it detects a device vulnerability or anomalous behavior posing a threat, the app notifies administrators, who can take action to investigate and remediate the issue.

To accomplish this, the IoT Security app works with remote sites deployed with NGFWs managed by SCM or Prisma SD-WAN remote sites also managed by SCM. In the first deployment model, where you deploy remote sites by using NGFW with IoT Security subscriptions, NGFWs collect information about network traffic and forward their logs to the logging service, which streams metadata to the IoT Security app for analysis.

- The update server provides firewalls with a regularly-updated device dictionary file of device attributes (profile, vendor, category, etc.) that security policy rules use for Device-ID.
- The app recommends security-policy rules (based on Device-ID) to firewalls managed by SCM.
- The app maps IP addresses to devices and notifies firewalls of their corresponding device attributes so that the firewalls can enforce Device-ID-based security-policy rules that reference attributes in IP-address-to-device mappings.

Figure 33 IoT Security solution for on-premises NGFW



ASSUMPTIONS AND PREREQUISITES

Palo Alto Networks NGFWs and SCM:

- Your organization has an active SCM tenant with an SLS license.
- You use SCM for centrally managing your firewall devices and configuration.
- Cloud management for NGFW is enabled on your SCM tenant.
- Firewall logging uses SLS.
- The tested PAN-OS version in this deployment guide is 11.2.3 for all devices.

Palo Alto Networks licensing:

- Your organization has sufficient licenses for the expected number of NGFWs.
- Your firewalls have been activated with AIOPS for NGFW Premium license (required for firewalls to be managed by SCM).
- If your SCM tenant includes an active SaaS Security license, your firewalls must also have been activated with a SaaS Security (SaaS Inline) license.
- IoT Security belongs to the same tenant service group (TSG) that your SCM is present.
- You have sufficient IoT Security licenses (for the current and expected number of sites for your organization) to allow the use of Device-ID and automated Zero Trust policy recommendations.

Procedures

Onboarding IoT Security

- 1.1 Activate IoT Security Subscriptions
- 1.2 Verify IoT Security Subscription for NGFW

In these procedures, you activate your IoT subscription and onboard your NGFW to the IoT Security portal.



Note

If you have an Enterprise License Agreement, the onboarding process starts either in the Customer Support Portal or in the hub.

1.1 Activate IoT Security Subscriptions

It is important that you keep the IoT Security activation email you received from Palo Alto Networks. It not only contains confidential activation-related data, but if you still have unused IoT Security licenses after completing the onboarding process, you can click the Activate button in the email again to repeat the process and activate more firewalls later.



Note

If you activate at least one IoT Security license and then lose the email, you can restart the activation process by using the Customer Support Portal. Log in to your Customer Support Portal account and select Activate Products, and then click Activate Now for the IoT Security licenses you want to onboard.

Step 1: Open your IoT Security activation email and click **Activate**. The Palo Alto Networks Customer Support Portal opens in your default web browser.

Step 2: Log in with your Customer Support Portal account credentials.

Step 3: Activate IoT Security Subscription by following the steps in the TechDocs topic [Activate IoT Security](#).



Note

When you purchase IoT Security production subscriptions, the licenses are specific to firewall models. It is not possible to use licenses created for one model with a different model. On the other hand, when evaluating IoT security, Palo Alto Networks provides temporary eval and trial licenses that you can use on any firewall model.

1.2 Verify IoT Security Subscription for NGFW

After the IoT Security subscriptions are activated, confirm that the firewalls are licensed and working properly.

Step 1: Log in to the IoT Security portal with the unique URL created during the device activation process (example: [examplesubdomain.iot.paloaltonetworks.com](#)).

Step 2: Navigate to **Administration > Firewalls**. The Firewalls page appears.

Step 3: Scroll down to the Firewalls pane. The Log Status column shows a colored cloud icon for each device.

Firewalls (15)										
<input type="checkbox"/>	Log Status	Serial N...	Hostname	Model	IoT Dev...	EAL	DHCP	Traffic	ARP	Software V...
<input type="checkbox"/>		02410101...	Ent-OT-PA-3410-1	PA-3410	9	338.5K	—	643.4K	15.7K	11.1.2-h3
<input type="checkbox"/>		02120110...	PA-440	PA-440	5	51.7K	—	26.6K	4.8K	11.2.0
<input type="checkbox"/>		03110100...	PA-450R-C1	PA-450R	9	60.9K	—	65.6K	16.6K	11.2.0
<input type="checkbox"/>		421c6632...	—	—	2	16.9K	—	—	15.1K	6.4.1-b7
<input type="checkbox"/>		00795600...	PA-VM	PA-VM	1	122.4K	—	56K	9.8K	11.1.2-h3
<input type="checkbox"/>		421c6336...	—	—	2	19.4K	8	—	19.4K	6.3.2-b5
<input type="checkbox"/>		10-00361...	—	—	2	62.5K	24	—	47.4K	6.4.1-b7
<input type="checkbox"/>		03110100...	PA-450R-C2	PA-450R	9	22K	—	45K	16.9K	11.2.0
<input type="checkbox"/>		10-00361...	—	—	1	6.6K	—	—	6.6K	6.3.1-b6

Step 4: For each NGFW, hover over the cloud icon and read its status details.

The individual NGFW devices' cloud log status can be in one of several states:

- **Red “Configuration error”**—The firewall does not have the required certificate installed and is not forwarding any logs to the logging service. In this case, do the following:
 - Set up your logging service instance.
 - Check that the Logging Service license on the firewall is active and set a service route for Palo Alto Networks Services using by either the management interface or a data interface.
- **Red “Not receiving logs”**—The firewall has the required certificate but is not yet configured to forward logs. In this case, do the following:
 - Configure the firewall to log traffic and forward the logs to the logging service.
- **Green “Receiving logs”**—The firewall is configured and deployed properly to send the logging service logs that the IoT Security app requires to function.



Note

The IoT Security app waits a full hour before determining it is not receiving one or more log types. It then displays a red “Not receiving...” status. After it starts receiving the required logs, it immediately displays the cloud status as green “Receiving logs”.

Step 5: To verify that the IoT license is installed from the NGFW, log in to the web interface of the activated firewall and navigate to **Device > Licenses**.

Step 6: In the License Management section, click **Retrieve license keys from license server**.

Step 7: After the licenses are retrieved, confirm that the IoT Security license has an expiration date beyond today's date.

IoT Security

Date Issued August 21, 2024
 Date Expires August 21, 2025
 Description 30 day evaluation, IoT

Procedures

Creating Zero Trust Security Policies

- 2.1 Discover IoT Devices
- 2.2 Creating Zero Trust Policies by Using SCM

The IoT Security app accesses the data from the logging service and uses its advanced ML algorithms and three-tier profiling system in order to analyze network behaviors and form a baseline for the device. The app then compares that baseline with the behaviors of other known devices. By doing so, the app determines the unique personality of the device and creates a profile consisting of device type, category, vendor, model, operating system, and OS family. The app automatically builds a behavioral profile for the device, including a baseline of acceptable behaviors and communication patterns with other devices.

2.1 Discover IoT Devices

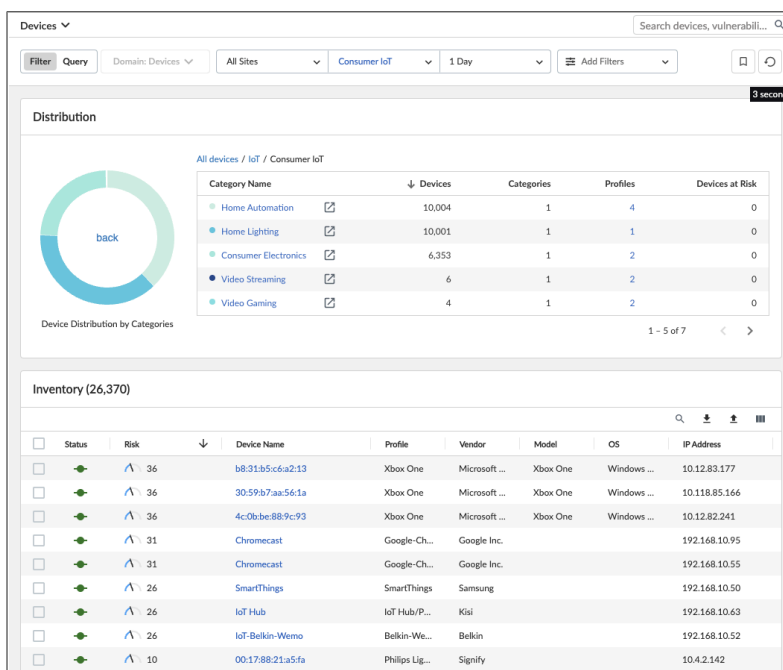
The time required to build initial device profiles depends on the following factors:

- **The number of active devices on the network**—Because it has more data to analyze, the IoT Security app can profile a device that produces a lot of traffic faster than it can profile a device that produces a little.
- **The number of the same type of devices on the network**—Because the app can aggregate knowledge learned from multiple devices simultaneously, the more devices of the same type there are, the faster the profiling works.
- **The complexity of the behavior of an individual device**—For example, the app learns the behavior of a network-connected thermostat much faster than that of a surgical robot in a hospital.

In the IoT Security portal, the devices that the app discovers and identifies appear on the Devices page.

Step 1: Log in to the IoT Security portal with the unique URL created during the device activation process (example: examplesubdomain.iot.paloaltonetworks.com).

Step 2: To review your inventory of discovered devices, navigate to **Assets > Devices** and select any category and then a particular device.



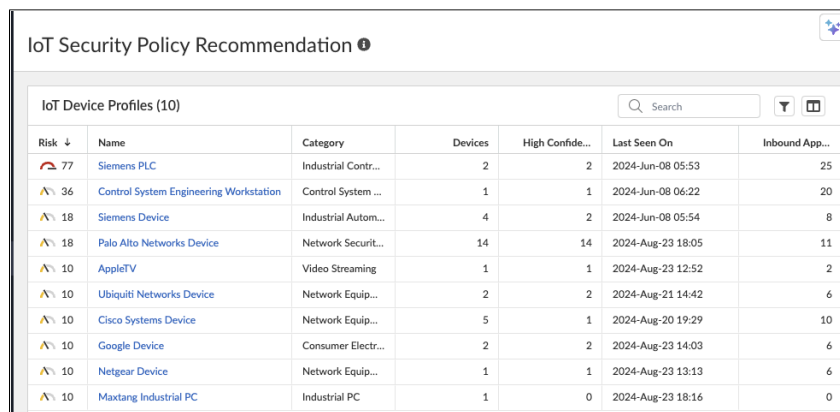
2.2 Creating Zero Trust Policies by Using SCM

As described in [Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide](#), the security policy can be applied to the Global or to specific folders. In this procedure, you apply the policies to the [Remote Site L2](#) folder.

The device profiles discovered by the IoT Security App are sent to SCM, and this section shows how to create policies by using the device profiles discovered.

Step 1: Log in to [SCM](#).

Step 2: Navigate to **Manage > Configuration > IoT Policy Recommendation**.



IoT Device Profiles (10)						
Risk ↓	Name	Category	Devices	High Confide...	Last Seen On	Inbound App...
77	Siemens PLC	Industrial Contr...	2	2	2024-Jun-08 05:53	25
36	Control System Engineering Workstation	Control System ...	1	1	2024-Jun-08 06:22	20
18	Siemens Device	Industrial Autom...	4	2	2024-Jun-08 05:54	8
18	Palo Alto Networks Device	Network Securit...	14	14	2024-Aug-23 18:05	11
10	AppleTV	Video Streaming	1	1	2024-Aug-23 12:52	2
10	Ubiquiti Networks Device	Network Equip...	2	2	2024-Aug-21 14:42	6
10	Cisco Systems Device	Network Equip...	5	1	2024-Aug-20 19:29	10
10	Google Device	Consumer Electr...	2	2	2024-Aug-23 14:03	6
10	Netgear Device	Network Equip...	1	1	2024-Aug-23 13:13	6
10	Mxtang Industrial PC	Industrial PC	1	0	2024-Aug-23 18:16	0

Step 3: Click the device profile that you want to create policies for (example: [AppleTV](#)). The device profile page shows a table of the behaviors for that profile.

Step 4: In the table, select the applications that you need policies for (example: **icloud-base**, **itunes-base**, and **apple-push-notifications**), and then click **Create Security Policy**.

IoT Policy Recommendation > AppleTV

AppleTV

AppleTV Profile Behaviors (21) Create Security Policy

	Application	App Risk	Security Policy Created	Discove...	Locally ...	App Usage	Destination Address & FQDN	Destination Profile	Last Seen
<input type="checkbox"/>	dns-base	3	No	internal	No	Common	any	PC-ChromeBook	-
<input type="checkbox"/>	dns-base	3	No	internal	No	Common	any	Asset Vulnerability Sc...	-
<input type="checkbox"/>	dhcp	2	No	internal	No	Common	any	VMware	-
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	F5 Networks Device	-
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	Nessus Vulnerability S...	-
<input type="checkbox"/>	ssl	4	No	external	No	Common	sas.pcms.apple.com	-	-
<input checked="" type="checkbox"/>	icloud-base	2	No	external	No	Common	calendars.fe2.apple-dns.ne	-	-
<input type="checkbox"/>	apple-maps	1	No	external	No	Common	ocsp2.g.aapling.com	-	-
<input type="checkbox"/>	web-browsing	4	No	external	No	Common	cl1.g.aapling.com	-	-
<input checked="" type="checkbox"/>	itunes-base	3	No	external	No	Common	su.itunes.apple.com	-	-
<input type="checkbox"/>	ntp-base	2	No	external	No	Common	time-osx.g.aapling.com	-	-
<input type="checkbox"/>	google-base	4	No	external	No	Common	googleads.g.doubleclick.ne	-	-
<input type="checkbox"/>	quic	1	No	external	No	Common	mask.apple-dns.net	-	-
<input type="checkbox"/>	ocsp	2	No	external	No	Common	192.124.249.22	-	-
<input type="checkbox"/>	apple-siri	1	No	external	No	Common	guzzoni.apple.com	-	-
<input checked="" type="checkbox"/>	apple-push-noti...	1	No	external	No	Common	us-sw-courier-4.push-appl	-	-
<input type="checkbox"/>	dns-over-https	3	No	external	No	Common	doh.opendns.com	-	-

Step 5: On the Create Security Policy dialog box, change the name of each rule in order to make it intuitive.

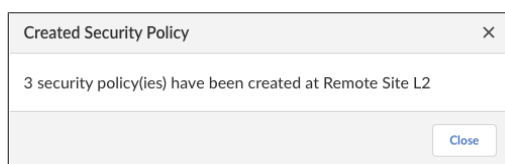
Create Security Policy

This is preview of security rules that will be created. After creating them, you can make changes from Security Policy screen.

Name	Application	Tag	SOURCE				DESTINATION		
			Zone	Add...	User	Device	Zone	Add...	Device
AppleTV - icloud	icloud-base	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	calenda...	any
AppleTV - itunes	itunes-base	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	su.itune...	any
AppleTV - apple-push-notifications	apple-push-notifications	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	us-sw-c...	any

Step 6: For Config Scope, select **Folder**, and then in the **Scope Selection** list, choose **Remote Site L2**.

Step 7: Click **Create Security Policy**, and then on the dialog box confirming that the policies were created, click **Close**.



Step 8: Navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

Step 9: In the Configuration Scope pane, choose **Remote Site L2**. At the bottom of the Security Policy Rules table are the policy rules that you created.

Security Policy Rules (20)

Search

Delete

Enable

Disable

Clone

Move

Add Rule

					SOURCE				DESTINATION			
<input type="checkbox"/>	#	Name	Action	Security Posture	Zone	Address	User	Device	Zone	Address	Device	Application
Remote Site L2 - Pre Rules (17)												
<input type="checkbox"/>	11	IT Unsanctioned AI Apps	<div><div></div>Deny</div>	<div><div></div><div></div><div></div></div>	zone-private	any	any	any	zone-public	any	any	<div><div></div>AI-Unsanctioned</div>
<input type="checkbox"/>	12	RemoteSite-to-Internet	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	zone-private zone-privile... zone-iot	any	any	any	zone-public	any	any	<div><div><div></div>google-base</div><div><div></div>ssl</div><div><div></div>web-browsing</div><div><div></div>zoom-base</div><div><div></div>zoom-meeting</div><div>more...</div></div>
<input type="checkbox"/>	13	Guest-to-Internet	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	zone-guest	any	any	any	zone-public	any	any	<div><div><div></div>dns</div><div><div></div>google-base</div><div><div></div>ssl</div><div><div></div>web-browsing</div></div>
<input type="checkbox"/>	14	Privileged-to-Private	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	zone-privile...	any	any	any	zone-private	any	any	<div><div><div></div>ms-rdp</div><div><div></div>ping</div><div><div></div>ssh</div></div>
<input type="checkbox"/>	15	Privileged-to-IOT	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	zone-privile...	any	any	any	zone-iot	any	any	<div><div><div></div>ms-rdp</div><div><div></div>ping</div><div><div></div>ssh</div></div>
<input type="checkbox"/>	16	AppleTV - icloud	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	any	any	any	<div><div></div>AppleTV</div>	\$iot_untrust	<div><div></div><div></div></div> calen...	any	<div><div></div>icloud-base</div>
<input type="checkbox"/>	17	AppleTV - itunes	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	any	any	any	<div><div></div>AppleTV</div>	\$iot_untrust	<div><div></div><div></div></div> su.itu...	any	<div><div></div>itunes-base</div>
<input type="checkbox"/>	18	AppleTV - apple-push-notificati...	<div><div></div>Allow</div>	<div><div></div><div></div><div></div></div>	any	any	any	<div><div></div>AppleTV</div>	\$iot_untrust	<div><div></div><div></div></div> us-sw...	any	<div><div></div>apple-push-notifications</div>

Step 10: On the menu bar, click **Overview**, and then under Variables, click the blue number. The Manage Variables page opens.

Step 11: Click **\$iot_trust\$**, then in the **Value** list, choose **zone-private**, and then click **Save**.

Variables | Global / All Firewalls / On-Premises Remote Sites / Remote Site L2 > Variables

Variables

Type *
Zone: Security zone used in policies and represents a logical grouping of interfaces

Name*
\$ iot_trust

Description

Value *
zone-private

* Required Field

Step 12: Click **\$iot_untrust\$**, then in the **Value** list, choose **zone-public**, and then click **Save**.

Now you can push the configuration changes to the devices in the Remote Site L2 folder.

Step 13: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 14: In the **Admin Scope** list, choose **All Admins**.

Step 15: In Description pane, enter a description.

Step 16: Select the row [Remote Site L2](#), and then click **Push**.

Procedures

Implementing Zero Trust Security Policies

3.1 Enable Device-ID on Internal Zones

In these procedures, you implement Device-ID for the internal zones and push the configuration to the folder.

3.1 Enable Device-ID on Internal Zones

You must enable Device-ID in each internal zone where you want to use Device-ID to detect devices and enforce security policy. By default, Device-ID maps all subnets in the zones where you enable it. You can modify which subnetworks Device-ID maps in the Include List and Exclude List. In this procedure, you enable Device-ID for all devices under the [Remote Site L2](#) folder.



Note

It is recommended that you enable only Device-ID for internal zones.

Step 1: Log in to [SCM](#).

Step 2: Navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Device Settings** menu, choose **Zones**.

Step 3: In the Configuration Scope pane, select [Remote Sites L2](#).

Step 4: On the Zones pane, click [zone-iot](#).

Step 5: In the **zone-iot** page, select **Enable Device Identification** check box, and then click **Save**.

Now that you have assigned values to all site-specific variables, you can push the configurations from SCM to the devices.

Step 6: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 7: In the **Admin Scope** list, choose **All Admins**.

Step 8: In Description pane, enter a description.

Step 9: Select the row **Remote Site L2**, and then click **Push**.

Procedures

Updating Security Rules with Device-ID

- 4.1 Create Device Objects
- 4.2 Update Existing Rules with Device Objects
- 4.3 Update Policy Rule Recommendations in IoT Security

These procedures are optional. If you do not want to secure traditional IT devices in your environment, skip to the "Working with Risk, Vulnerabilities, and Alerts".

Because they are not tracked the same way as IoT devices, you cannot secure traditional IT devices, such as laptops and smartphones, by using IoT Security policy rule recommendations. If you want to secure IT devices with Device-ID information, you must perform the procedures in this section.

4.1 Create Device Objects

Device objects are automatically created for IoT devices when a policy rule is imported from the IoT Security app into your NGFW. Traditional IT devices are identified in IoT Security, but there is no automatic method to create the device objects required for security policy rules.

Step 1: Log in to **SCM**.

Step 2: Navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Devices**.

Step 3: In the Configuration Scope pane, select **Remote Sites L2**.

Step 4: Click **Add Devices**. The Devices page appears.

Step 5: In the **Name** box, enter a unique name (example: **Corporate HP ZBook**).

Step 6: In the **Description** box, enter a valid description.

Step 7: In the **Category** list, choose **Personal Computer**.

Step 8: In the **Vendor** list, choose **Hewlett Packard**.

Step 9: In the **Profile** list, choose **PC-Windows**.

Step 10: In the **OS Family** list, choose **Windows**.

Step 11: In the **OS Version** list, enter **Windows 10**.

Step 12: In the **Model** list, enter **HP ZBook 15u G3**, and then click **Save**.

Devices [All Firewalls / On-Premises Remote Sites / Remote Site L2] > Devices

Devices

Name * Corporate HP ZBook

Description * Device Profile for HP laptops

Match Criteria Filter each criteria by keyword Clear Filters

Category	Personal Computer	X	▼
Vendor	Hewlett Packard	X	▼
Profile	PC-Windows	X	▼
OS Family	Windows	X	▼
OS Version	Windows 10	X	▼
Model	HP ZBook 15u G3	X	▼

* Required Field

Cancel Save

Step 13: To create additional device objects for your traditional IT devices, repeat Step 4 through Step 10.

4.2 Update Existing Rules with Device Objects

After you create the device objects, you update the source device in existing security rules.

Step 1: In SCM, navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

Step 2: In the Configuration Scope pane, choose **Remote Site L2**.

Step 3: In the Security Rules pane, click **Add Rule**, and then choose **Pre Rules**.

Step 4: In the **Name** box, enter **Google Workspace**.

Step 5: In the Source pane, next to Zones, select **Select**, and then select **zone-iot**.

Step 6: Next to Addresses, select **Any**.

Step 7: Next to Devices, select **Select**, click **Device Profiles**, and then select **Corporate HP ZBook**.

Step 8: In the Destination pane, next to Zones, select **Select**, and then select **zone-public**.

Step 9: Next to Addresses, select **Any**.

Step 10: On the Application/Service pane, next to Application, select **Any**.

Step 11: In the Actions pane, in the **Action** list, choose **Allow**.

Step 12: In the **Profile Group** list, choose **best-practice**, and then click **Save**.

Step 13: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 14: In the **Admin Scope** list, choose **All Admins**.

Step 15: In Description pane, enter a description.

Step 16: Select the row **Remote Site L2**, and then click **Push**.

As devices gain new capabilities and access different applications, the IoT Security app updates the policy rule recommendations with additional traffic or protocols the NGFW should allow. You should check the app daily and update your policy rule recommendations when the new updates are available.

4.3 Update Policy Rule Recommendations in IoT Security



To ensure that your policy rule recommendations and device objects are current or to restore policy rule recommendation mappings that might be out of sync, use this procedure.

Step 1: Log in to **SCM**.

Step 2: Navigate to **Manage > Configuration > IoT Policy Recommendation**.

Step 3: In the IOT Device Profiles table, click the profile name whose policies you want to update (example: [AppleTV](#)).

IoT Security Policy Recommendation ⓘ

IoT Device Profiles (19)  

Risk ↓	Name	Category	Devices	High Confidence ...	Last Seen On	Inbound Applicati...	Outbound Applic...
77	Siemens PLC	Industrial Controller	2	2	2024-Jun-08 05:53	25	6
69	AppleTV	Video Streaming	1	1	2024-Aug-23 12:52	2	37
36	Control System Engineer	Control System Engin...	1	1	2024-Jun-08 06:22	17	96
18	Siemens Device	Industrial Automation	4	2	2024-Jun-08 05:54	7	7
17	Palo Alto Networks De	Network Security Eq...	16	16	2024-Aug-28 20:23	9	24
11	iRobot Device	Home Automation	2	2	2024-Aug-28 19:02	4	11
11	TP-LINK Device	Network Equipment	1	1	2024-Aug-28 19:02	7	12
11	Smart Plug	Smart Plug	4	4	2024-Sep-02 15:53	3	8
11	Nest Device	Home Automation	3	3	2024-Aug-30 04:56	4	8
11	Amazon Ring Device	Home Security	1	0	2024-Aug-28 19:02	2	18
10	Amazon Device	Consumer Electronics	1	0	2024-Aug-28 20:28	4	11
10	Ubiquiti Networks Dev	Network Equipment	2	2	2024-Aug-21 14:42	6	9
10	Google Device	Consumer Electronics	7	5	2024-Aug-29 13:24	3	48

Step 4: On the device profile page, select an application that you wish to create a security policy for (example: [apple-maps](#)), and then click **Create Security Profile**.

IoT Policy Recommendation > AppleTV ⓘ




AppleTV Profile Behaviors (21) [Create Security Policy](#)

<input type="checkbox"/>	Application	App ...	Security Policy Created	Disc...	Loca...	App ...	Destination Address & FQDN	Destination Profile
<input type="checkbox"/>	dhcp	2	No	internal	No	Common	any	VMware
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	F5 Networks Device
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	Nessus Vulnerability S...
<input type="checkbox"/>	ssl	4	No	external	No	Common	sas.pcms.apple.com	-
<input type="checkbox"/>	icloud-base	2	No	external	No	Common	calendars.fe2.apple-dns.ne	-
<input checked="" type="checkbox"/>	apple-maps	1	No	external	No	Common	ocsp2.g.aapling.com	-
<input type="checkbox"/>	web-browsing	4	No	external	No	Common	cl1.g.aapling.com	-

Step 5: On the Create Security Policy dialog box, modify the default name to something that is more relevant (example: [AppleTV - maps](#)).

Create Security Policy ⓘ

This is preview of security rules that will be created. After creating them, you can make changes from Security Policy screen.

Name	Application	Tag	SOURCE		
<input type="text" value="AppleTV - maps"/>	 apple-maps	 IoT Recom...  AppleTV	Zone	Add...	User
			any	any	any

Step 6: At the bottom of the dialog box, for Config Scope, select **Folders**, and then in the **Scope Selection** list, choose [Remote Site L2](#).

Step 7: Click **Create Security Policy**, and then, on the confirmation dialog box, click **Close**.

Step 8: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 9: In the **Admin Scope** list, choose **All Admins**.

Step 10: In Description pane, enter a description.

Step 11: Select the row **Remote Site L2**, and then click **Push**.

Now that you have completed deploying IoT Security for on-premises NGFW, see the "Working with Risk, Vulnerabilities, and Alerts" section.

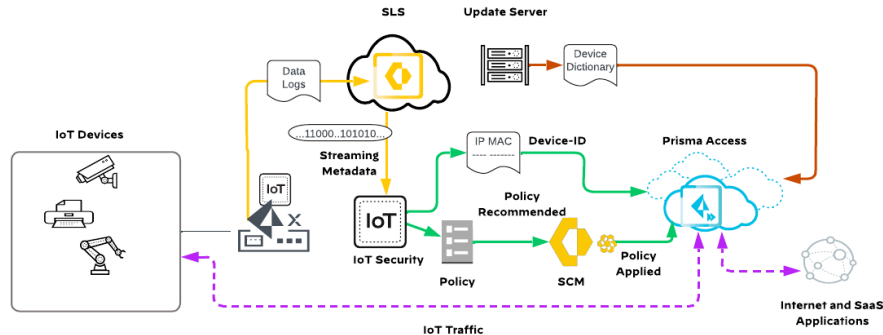
Deploying IoT Security for Prisma SASE Attached Remote Sites

This deployment follows the Prisma SASE for Securing Internet Design Model as described in the **SASE for Securing Internet: Design Guide**. You should follow the procedures mentioned in this guide and ensure that the firewall is registered successfully with SCM. To understand all aspects of deploying the NGFW using the SCM, you should follow the guidance in the **SASE for Securing Internet: Deployment Guide**.

In this deployment option, you deploy remote sites by using Prisma SD-WAN, and ION devices collect information about network traffic and forward their logs to the logging service, which streams metadata to the IoT Security app for analysis.

- The update server provides Prisma Access with a regularly updated device dictionary file of device attributes (profile, vendor, category, etc.) that security policy rules use for Device-ID.
- The app recommends security-policy rules (based on Device-ID) to Prisma Access managed by SCM.
- The app maps IP addresses to devices and notifies firewalls of their corresponding device attributes so the firewalls can enforce Device-ID-based security policy rules that reference attributes in IP-address-to-device mappings.

Figure 34 IoT Security solution for Prisma SASE



ASSUMPTIONS AND PREREQUISITES

Prisma SASE:

- Your organization has an active SCM tenant with an SLS license.
- Cloud-managed Prisma Access.
- Prisma Access logging uses SLS.
- The Prisma Access dataplane version in this deployment guide is 10.2.11-h1.

Palo Alto Networks licensing:

- If your SCM tenant includes an active SaaS Security license, your tenant must also have been activated with a SaaS Security (SaaS Inline) license.
- IoT Security belongs to the same TSG that your SCM is present.

Procedures

Onboarding IoT Security

- 5.1 Activate IoT Security Subscriptions
- 5.2 Verify IoT Subscription for Prisma Access
- 5.3 Verify Prisma Access SPN and ION Devices Are Registered to the IoT Portal

In these procedures, you activate your IoT subscription and onboard your Prisma SASE to the IoT Security portal.

5.1 Activate IoT Security Subscriptions

It is important that you keep the IoT Security activation email you received from Palo Alto Networks. It not only contains confidential activation-related data, but if you still have unused IoT Security licenses after completing the onboarding process, you can click the Activate button in the email again to repeat the process and activate more firewalls later.



Note

If you activate at least one IoT Security license and then lose the email, you can restart the activation process by using the Customer Support Portal. Log in to your Customer Support Portal account and select Activate Products, and then click Activate Now for the IoT Security licenses you want to onboard.

Step 1: Open your IoT Security activation email and click **Activate**. The Palo Alto Networks Customer Support Portal opens in your default web browser.

Step 2: Log in with your Customer Support Portal account credentials.

Step 3: Activate IoT Security Subscription by following the steps in the TechDocs topic, "[Activating IoT Subscription](#)".



Note

When you purchase IoT Security production subscriptions, the licenses are specific to firewall models. It is not possible to use licenses created for one model with a different model. On the other hand, when evaluating IoT security, Palo Alto Networks provides temporary eval and trial licenses that you can use on any firewall model.

5.2 Verify IoT Subscription for Prisma Access

Step 1: Log in to **SCM**.

Step 2: Navigate to **Settings > Tenants**.

Step 3: On the Products tab, find Prisma Access and verify that it is enabled with an IoT Security license.

Prisma Access	Complete	Mobile Users: 1000 Users Remote Network: 1000 Mbps Customer Success: N/A Autonomous DEM Mobile Users: 1 Autonomous DEM Remote Network Enterprise DLP: N/A SaaS Security: N/A AI powered ADEM: 1000 Prisma Access Browser: 1000 IoT Security: N/A	012400000005942	09/14/2024	United States - Americas
---------------	----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------	------------	--------------------------

5.3 Verify Prisma Access SPN and ION Devices Are Registered to the IoT Portal

After the IoT Security subscriptions are activated, confirm that the SPN and ION are licensed and working properly.

Step 1: Log in to the IoT Security portal with the unique URL created during the device activation process (example: examplesubdomain.iot.paloaltonetworks.com).

Step 2: Navigate to **Administration > Firewalls**. The Firewalls page appears.

Step 3: Scroll down to the Firewalls pane. The Log Status column shows a colored cloud icon for each device.

Firewalls (58)									
0 Rows selected									
<input type="checkbox"/>	Log Status	Serial Number	Hostname	Model	IoT Dev...	EAL	DHCP	Traffic	ARP
<input type="checkbox"/>		7CB045F1C266536	AUTO-CGX_RS11_01_a870	—	2	33.2K	—	41.2K	30.6K
<input type="checkbox"/>		7AA77AFFEY85D86	—	—	1	29.7K	—	—	29.7K
<input type="checkbox"/>		78EA1B487F594DF	—	—	1	30.5K	—	—	30.5K
<input type="checkbox"/>		7834850808B4BF	—	—	1	30.2K	—	—	30.2K
<input type="checkbox"/>		7CED38DE7D523F	—	—	1	30.1K	—	—	30.1K
<input type="checkbox"/>		78B5EAC7C1E946	GP cloud service	—	1	14.9K	—	66	14.8K
<input type="checkbox"/>		75095130D409E0F	—	—	1	29.7K	—	—	29.7K
<input type="checkbox"/>		73254491631B559	—	—	1	30.3K	—	—	30.3K
<input type="checkbox"/>		10-003651-7138	—	—	3	14K	2	—	209
<input type="checkbox"/>		71E5D2A5E22C099	—	—	1	30.3K	—	—	30.3K
<input type="checkbox"/>		74E674F461FFB84	GP cloud service	—	1	17K	—	410	16.3K
<input type="checkbox"/>		7536198D2AEAA18	—	—	1	30.2K	—	—	30.2K
<input type="checkbox"/>		7DF7D0D498E57C4	AUTO-CGX_D3XLQTH4P1EO_01_cc80	—	2	54.4K	—	33.7K	30.3K
<input type="checkbox"/>		7FE86C8E364DECC	AUTO-CGX_D3XLQTH4P1EO_01_56e0	—	2	31.2K	—	249	30.7K
<input type="checkbox"/>		7D5C8BE33FF7FC8	—	—	1	29.7K	—	—	29.7K



Note

To identify the device type, scroll to the right and find the Instance Type column. You can use the instance type to determine if a device is an ION device or SPN.

Step 4: For each Prisma Access SPN or ION device, hover over the cloud icon and read its status details.

The IoT security portal must show Prisma Access SPNs and the ION devices connected to the IoT Security Portal. Prisma Access and ION devices' cloud log status can be in one of several states:

- **Red “Configuration error”**—The SPN or the ION device does not have the required certificate installed and is not forwarding any logs to the logging service. In this case, do the following:
 - Set up your logging service instance.
 - Check that the Logging Service license on the SPN or ION device is active and set a service route for Palo Alto Networks Services using by either the management interface or a data interface.
- **Red “Not receiving logs”**—The SPN or ION device has the required certificate but is not yet configured to forward logs. In this case, do the following:
 - Configure the SPN or ION devices to log traffic and forward the logs to the logging service.
- **Green “Receiving logs”**—The SPN or ION device is configured and deployed properly to send the logging service logs that the IoT Security app requires in order to function.



Note

The IoT Security app waits a full hour before determining it is not receiving one or more log types. It then displays a red “Not receiving...” status. After it starts receiving the required logs, it immediately displays the cloud status as green “Receiving logs”.

Procedures

Creating Zero Trust Security Policies

- 6.1 Discover IoT Devices
- 6.2 Creating Zero Trust Policies by Using SCM

The IoT Security app accesses the data from the logging service and uses its advanced ML algorithms and three-tier profiling system in order to analyze network behaviors and form a baseline for the device. The app then compares that baseline with the behaviors of other known devices. By doing so, the app determines the unique personality of the device and creates a profile consisting of device type, category, vendor, model, operating system, and OS family. The app automatically builds a behavioral profile for the device, including a baseline of acceptable behaviors and communication patterns with other devices.

6.1 Discover IoT Devices

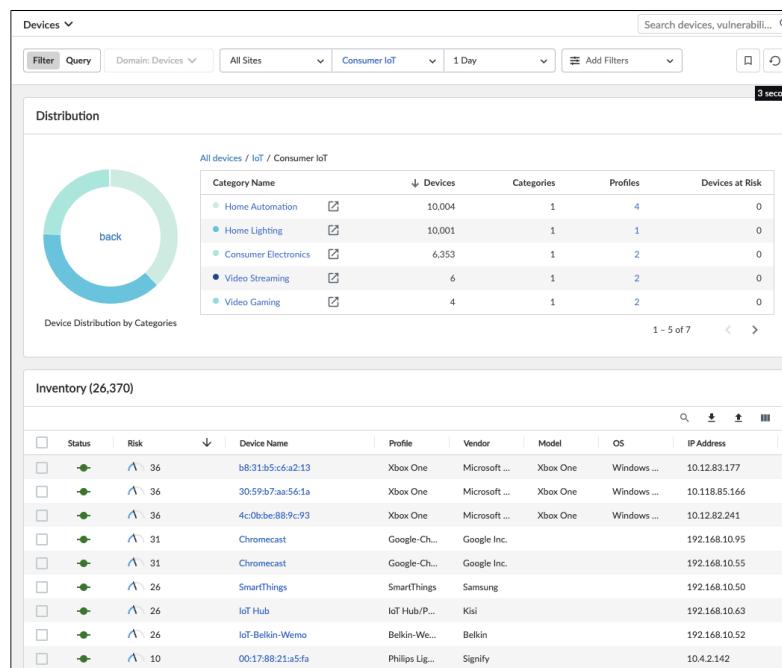
The time required to build initial device profiles depends on several factors:

- **The number of active devices on the network**—Because it has more data to analyze, the IoT Security app can profile a device that produces a lot of traffic faster than it can profile a device that produces a little.
- **The number of the same type of devices on the network**—Because the app can aggregate knowledge learned from multiple devices simultaneously, the more devices of the same type there are, the faster the profiling works.
- **The complexity of the behavior of an individual device**—For example, the app learns the behavior of a network-connected thermostat much faster than that of a surgical robot in a hospital.

In the IoT Security portal, the devices that the app discovers and identifies appear on the Devices page.

Step 1: Log in to the IoT Security portal with the unique URL created during the device activation process (example: examplesubdomain.iot.paloaltonetworks.com).

Step 2: To review your inventory of discovered devices, navigate to **Assets > Devices** and select any category and then a particular device.



6.2 Creating Zero Trust Policies by Using SCM



As described in **Securing the Branch with On-Premises Network Security and Strata Cloud Manager: Deployment Guide**, the security policy can be applied to the Global or to specific folders. In this procedure group, you will apply the policies to the **Remote Networks** folder.

The device profiles discovered by the IoT Security App are sent to SCM and this section shows how to create policies using the device profiles discovered.

Step 1: Log in to **SCM**.

Step 2: Navigate to **Manage > Configuration > IoT Policy Recommendation**.

IoT Security Policy Recommendation ⓘ


IoT Device Profiles (10)  

Risk ↓	Name	Category	Devices	High Confide...	Last Seen On	Inbound App...
77	Siemens PLC	Industrial Contr...	2	2	2024-Jun-08 05:53	25
36	Control System Engineering Workstation	Control System ...	1	1	2024-Jun-08 06:22	20
18	Siemens Device	Industrial Autom...	4	2	2024-Jun-08 05:54	8
18	Palo Alto Networks Device	Network Securit...	14	14	2024-Aug-23 18:05	11
10	AppleTV	Video Streaming	1	1	2024-Aug-23 12:52	2
10	Ubiquiti Networks Device	Network Equip...	2	2	2024-Aug-21 14:42	6
10	Cisco Systems Device	Network Equip...	5	1	2024-Aug-20 19:29	10
10	Google Device	Consumer Electr...	2	2	2024-Aug-23 14:03	6
10	Netgear Device	Network Equip...	1	1	2024-Aug-23 13:13	6
10	Maxtang Industrial PC	Industrial PC	1	0	2024-Aug-23 18:16	0

Step 3: Click the device profile that you want to create policies for (example: **AppleTV**). The device profile page shows a table of the behaviors for that profile.

Step 4: In the table, select the applications that you that you need policies for (example: **icloud-base**, **itunes-base**, and **apple-push-notifications**), and then click **Create Security Policy**.

IoT Policy Recommendation > AppleTV

AppleTV  AppleTV

AppleTV Profile Behaviors (21) [Create Security Policy](#)

<input type="checkbox"/>	Application	App Risk	Security Policy Created	Discove...	Locally ...	App Usage	Destination Address & FQDN	Destination Profile	Last Seen
<input type="checkbox"/>	dns-base	3	No	internal	No	Common	any	PC-ChromeBook	-
<input type="checkbox"/>	dns-base	3	No	internal	No	Common	any	Asset Vulnerability Sc...	-
<input type="checkbox"/>	dhcp	2	No	internal	No	Common	any	VMware	-
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	F5 Networks Device	-
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	Nessus Vulnerability S...	-
<input type="checkbox"/>	ssl	4	No	external	No	Common	sas.pcms.apple.com	-	-
<input checked="" type="checkbox"/>	icloud-base	2	No	external	No	Common	calendars.fe2.apple-dns.ne	-	-
<input type="checkbox"/>	apple-maps	1	No	external	No	Common	ocsp2.g.aapling.com	-	-
<input type="checkbox"/>	web-browsing	4	No	external	No	Common	c11.g.aapling.com	-	-
<input checked="" type="checkbox"/>	itunes-base	3	No	external	No	Common	su.itunes.apple.com	-	-
<input type="checkbox"/>	ntp-base	2	No	external	No	Common	time-osx.g.aapling.com	-	-
<input type="checkbox"/>	google-base	4	No	external	No	Common	googleads.g.doubleclick.ne	-	-
<input type="checkbox"/>	quic	1	No	external	No	Common	mask.apple-dns.net	-	-
<input type="checkbox"/>	ocsp	2	No	external	No	Common	192.124.249.22	-	-
<input type="checkbox"/>	apple-siri	1	No	external	No	Common	guzzoni.apple.com	-	-
<input checked="" type="checkbox"/>	apple-push-noti...	1	No	external	No	Common	us-sw-courier-4.push-appl	-	-
<input type="checkbox"/>	dns-over-https	3	No	external	No	Common	doh.opendns.com	-	-

Step 5: On the Create Security Policy dialog box, change the name of each rule in order to make it intuitive.

Create Security Policy

This is preview of security rules that will be created. After creating them, you can make changes from Security Policy screen.

Name	Application	Tag	SOURCE				DESTINATION		
			Zone	Add...	User	Device	Zone	Add...	Device
AppleTV - icloud	icloud-base	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	calenda...	any
AppleTV - itunes	itunes-base	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	su.itune...	any
AppleTV - apple-push-notifications	apple-push...	IoT Recom... AppleTV	any	any	any	AppleTV	\$iot_un...	us-sw-c...	any

Step 6: For Config Scope, select **Folder**, and then in the **Scope Selection** list, choose **Remote Networks**.

Step 7: Click **Create Security Policy**, and then on the dialog box confirming that the policies were created, click **Close**.

Created Security Policy

3 security policy(ies) have been created at Remote Networks

Close

Step 8: Navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

Step 9: In the Configuration Scope pane, choose **Remote Networks**. In the Security Policy Rules table, at the bottom of the Remote Networks section, the three policy rules that you created appear.

Configuration Scope: Remote Networks

Overview Security Services Network Policies Identity Services Objects Global Settings

Security Policy

Security Policy Rules (65)

Search

Delete Enable Disable Clone Move Add Rule

#	Name	Action	Security Posture	SOURCE				DESTINATION			Application	URL Cate...	Service
				Zone	Address	User	Device	Zone	Address	Device			
Prisma Access - Pre Rules (49)													
Remote Networks (8)													
50	PrismaAccess-Portal-RN	Allow	🚫 ⚡ 🛡️	any	Net-Pris...	any	any	untrust	PrismaAc...	any	palooa-to-shared-services panos-global-protect ssl	any	applicati...
51	AzureAD-SAML-RN	Allow	🚫 ⚡ 🛡️	any	Net-Pris...	any	any	untrust	any	any	ms-office365-base	any	service...
52	Allow RN EP Traffic to Prisma Acc...	Allow	🚫 ⚡ 🛡️	trust	Net-Pris...	any	any	untrust	any	any	any	any	any
53	Permit Proxy	Allow	🚫 ⚡ 🛡️	any	Net-Pris...	any	any	any	any	any	web-browsing panos-global-protect http-proxy	any	service...
54	RS113-to-DC01	Allow	🚫 ⚡ 🛡️	trust	10.130...	any	any	trust	Data Co...	any	web-browsing ssl	any	applicati...
55	AppleTV - icloud	Allow	🚫 ⚡ 🛡️	any	any	any	AppleTV	untrust	calen...	any	icloud-base	any	applicati...
56	AppleTV - itunes	Allow	🚫 ⚡ 🛡️	any	any	any	AppleTV	untrust	su.itu...	any	itunes-base	any	applicati...
57	AppleTV - apple-push-notificati...	Allow	🚫 ⚡ 🛡️	any	any	any	AppleTV	untrust	us-sw...	any	apple-push-notifications	any	applicati...

Step 10: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 11: In the **Admin Scope** list, choose **All Admins**.

Step 12: In Description pane, enter a description.

Step 13: In the Push Scope table, select **Remote Networks**, and then click **Push**. The Jobs dialog box displays the status of the push job.

Step 14: When you are ready to close the Jobs dialog box, click **Done**.

Step 15: Verify again that the new rules appear on the Security Policy Rules table.

If you notice that a rule in the Prisma Access - Pre Rules section is shadowing the rules you created, then you need to move the new rules above that rule. The next steps show you how to move these rules.

Step 16: Note the name of the rule that you are going to push these rule above. In this example, it is **All Web Browsing - All Users**.

Step 17: Select the rule you need to move (ex: **AppleTV-itunes**). On the top right corner, in the **Move** list, choose **Move to Different Location**. The Move to Different Location dialog box opens.

Selected Rules	
Name	Location
AppleTV - itunes	Remote Networks

Destination Rule Type: ☒ Folders ☐ Snippets

Destination: Remote Networks

Rule Order: Top

☒ Error out on first detected error in validation

Cancel Move

Step 18: In the Destination list, choose **Prisma Access**.

Step 19: In the **Rule Order** list, choose **Before Rule**, choose **All Web Browsing - All users**, and then click **Move**.

Procedures

Implementing Zero Trust Security Policies

7.1 Verify Device-ID Is Enabled on Prisma Access

In these procedures, you implement Device Identification from Prisma Access Set up, enable Device-ID in the ION device, and push configuration to the folder.

7.1 Verify Device-ID Is Enabled on Prisma Access

Step 1: Log in to **SCM**.

Step 2: Navigate to **Workflows > Prisma Access Setup > Prisma Access**.

Step 3: Under Infrastructure Settings, verify that Device Identification is Enabled.

Prisma Access Setup

Push Config

Infrastructure Settings

IPv6 for Internal Traffic	Disabled
Infrastructure Subnet	172.16.55.0/24
Infrastructure BGP AS	65534
Egress IP API Key	dt73sowrnc__KKseADmSfA3rH5SztKVwk9kUjINDPjxv8hP0qy2s Copy API Key Generate New API Key
Egress IP Notification URL	pa-egressip-notify.example.com
Tunnel Monitor IP Address	172.16.55.254
Captive Portal Redirect IP Address	172.16.55.254
Remote Networks DNS IP Address	172.16.55.254
Loopback IPs	172.16.55.2
ZTNA Connector IPs	Application IP Blocks: 100.64.0.0/24Connector IP Blocks: 100.64.128.0/20
Pre-prod or Lab Tenant	Disabled
Device Identification	Enabled

Step 4: Navigate to **Workflows > Prisma SD-WAN Setup > Branch Sites**.

Step 5: Verify that IoT Device Visibility is enabled in the remote site.

RS12-EastUS Branch

TAGS: prisma_name:RS12, prisma_access: 10 Snowshoe Dr, 26209, United States

Site Summary | **Configuration** | Overlay Connections

Advanced Refresh

CONNECTIVITY Physical: 2 of 2 Secure Fabric: 4 of 6 Prisma Access: 0 of 0 Standard VPN: 1 of 1	MODE Control	DOMAIN East US	PATH POLICY SET STACK MPLS+INET PathStack PERFORMANCE MANAGEMENT POLICY SET STACK Default Performance Policy Se... QOS POLICY SET STACK Default QoS Simple Stack (Sim... NAT POLICY SET STACK Default-NATPolicySetStack	SECURITY POLICY SET STACK ZBFW SecurityStack
WAN MULTICAST No profile Create Profile WAN Multicast Configurations	INTERNET CIRCUITS ISP-DSL-RS12 Change Circuits	PRIVATE WAN CIRCUITS MPLS-RS12 Change Circuits	DEVICES RS12-ION3102v (ion 3102v) Assign Device	IP PREFIXES (View) Global: 10.130.48.0/21 Change IP Prefixes
VRF Profile Global Profile Create Profile	1 DHCP Scope	IOT DEVICE VISIBILITY Enabled	IOT DISCOVERY PROFILE No profile Create Profile Configure IoT SNMP Start Nodes	BRANCH GATEWAY Disabled

Procedures

Updating Security Rules with Device-ID

- 8.1 Create Device Objects
- 8.2 Update Existing Rules with Device Objects
- 8.3 Update Policy Rule Recommendations in IoT Security

These procedures are optional. If you do not want to secure traditional IT devices in your environment, skip to the "Working with Risk, Vulnerabilities, and Alerts" section.

8.1 Create Device Objects

Step 1: Log in to **SCM**.

Step 2: Navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Objects** menu, choose **Devices**.

Step 3: In the Configuration Scope pane, select **Remote Networks**.

Step 4: Click **Add Devices**. The Devices page appears.

Step 5: In the **Name** box, enter a unique name (example: **Corporate HP ZBook**).

Step 6: In the **Description** box, enter a valid description.

Step 7: In the **Category** list, choose **Personal Computer**.

Step 8: In the **Vendor** list, choose **Hewlett Packard**.

Step 9: In the **Profile** list, choose **PC-Windows**.

Step 10: In the **OS Family** list, choose **Windows**.

Step 11: In the **OS Version** list, choose **Windows 10**.

Step 12: In the **Model** list, choose **HP ZBook 15u G3**, and then click **Save**.

Devices [All Firewalls / On-Premises Remote Sites / Remote Site L2] > Devices

Devices

Name * Corporate HP ZBook

Description * Device Profile for HP laptops

Match Criteria Filter each criteria by keyword Clear Filters

Category	Personal Computer	×	▼
Vendor	Hewlett Packard	×	▼
Profile	PC-Windows	×	▼
OS Family	Windows	×	▼
OS Version	Windows 10	×	▼
Model	HP ZBook 15u G3	×	▼

* Required Field

Cancel Save

Step 13: To create additional device objects for your traditional IT devices, repeat Step 4 through Step 12.

8.2 Update Existing Rules with Device Objects

After you create the device objects, you update the source device in existing security rules.

Step 1: In SCM, navigate to **Manage > Configuration > NGFW and Prisma Access**, and then from the **Security Services** menu, choose **Security Policy**.

Step 2: In the Configuration Scope pane, choose **Remote Networks**.

Step 3: In the Security Rules pane, click **Add Rule**.

Step 4: In the **Name** box, enter **Google Workspace**.

Step 5: In the Source pane, next to Zones, select **Select**, and then select **trust**.

Step 6: Next to Addresses, select **Any**.

Step 7: Next to Devices, select **Select**, click **Device Profiles**, and then select **Corporate HP ZBook**.

Step 8: In the Destination pane, next to Zones, select **Select**, and then select **un-trust**.

Step 9: Next to Address, select **Any**.

Step 10: On the Applications/Service pane, select **Any**.

Step 11: In the Actions pane, in the **Action** list, choose **Allow**.

Step 12: In the **Profile Group** list, choose **best-practice**, and then click **Save**.

Step 13: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 14: In the **Admin Scope** list, choose **All Admins**.

Step 15: In Description pane, enter a description.

Step 16: Select the row **Remote Networks**, and then click **Push**.

As devices gain new capabilities and access different applications, the IoT Security app updates the policy rule recommendations with additional traffic or protocols the NGFW should allow. You should check the app daily and update your policy rule recommendations when the new updates are available.

8.3 Update Policy Rule Recommendations in IoT Security

To ensure that your policy rule recommendations and device objects are current or to restore policy rule recommendation mappings that might be out of sync, use this procedure.

Step 1: Log in to **SCM**.

Step 2: Navigate to **Manage > Configuration > IoT Policy Recommendation**.

Step 3: In the IOT Device Profiles table, click the profile name whose policies you want to update (example: **AppleTV**).

IoT Security Policy Recommendation ⓘ

IoT Device Profiles (19)

Risk ↓	Name	Category	Devices	High Confidence ...	Last Seen On	Inbound Applicati...	Outbound Applic...
77	Siemens PLC	Industrial Controller	2	2	2024-Jun-08 05:53	25	6
69	AppleTV	Video Streaming	1	1	2024-Aug-23 12:52	2	37
36	Control System Engine	Control System Engin...	1	1	2024-Jun-08 06:22	17	96
18	Siemens Device	Industrial Automation	4	2	2024-Jun-08 05:54	7	7
17	Palo Alto Networks De	Network Security Eq...	16	16	2024-Aug-28 20:23	9	24
11	iRobot Device	Home Automation	2	2	2024-Aug-28 19:02	4	11
11	TP-LINK Device	Network Equipment	1	1	2024-Aug-28 19:02	7	12
11	Smart Plug	Smart Plug	4	4	2024-Sep-02 15:53	3	8
11	Nest Device	Home Automation	3	3	2024-Aug-30 04:56	4	8
11	Amazon Ring Device	Home Security	1	0	2024-Aug-28 19:02	2	18
10	Amazon Device	Consumer Electronics	1	0	2024-Aug-28 20:28	4	11
10	Ubiquiti Networks Dev	Network Equipment	2	2	2024-Aug-21 14:42	6	9
10	Google Device	Consumer Electronics	7	5	2024-Aug-29 13:24	3	48

Step 4: On the device profile page, select an application that you wish to create a security policy for (example: **apple-maps**), and then click **Create Security Profile**.

IoT Policy Recommendation > AppleTV ⓘ

AppleTV

AppleTV Profile Behaviors (21) Create Security Policy

	Application	App ...	Security Policy Created	Disc...	Loca...	App ...	Destination Address & FQDN	Destination Profile
<input type="checkbox"/>	dhcp	2	No	internal	No	Common	any	VMware
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	F5 Networks Device
<input type="checkbox"/>	ssl	4	No	internal	No	Common	any	Nessus Vulnerability S...
<input type="checkbox"/>	ssl	4	No	external	No	Common	sas.pcms.apple.com	-
<input type="checkbox"/>	icloud-base	2	No	external	No	Common	calendars.fe2.apple-dns.ne	-
<input checked="" type="checkbox"/>	apple-maps	1	No	external	No	Common	ocsp2.g.aapling.com	-
<input type="checkbox"/>	web-browsing	4	No	external	No	Common	c11.g.aapling.com	-

Step 5: On the Create Security Policy dialog box, modify the default name to something that is more relevant (example: **AppleTV - maps**).

Name	Application	Tag	SOURCE		
			Zone	Add...	User
AppleTV - maps	apple-maps	IoT Recom... AppleTV	any	any	any

Step 6: At the bottom of the dialog box, for Config Scope, select **Folders**, and then in the **Scope Selection** list, choose **Remote Networks**.

Step 7: Click **Create Security Policy**, and then, on the confirmation dialog box, click **Close**.

Step 8: In the upper right of the page, click **Push Config**, and then click **Push**.

Step 9: In the **Admin Scope** list, choose **All Admins**.

Step 10: In Description pane, enter a description.

Step 11: Select the row **Remote Networks**, and then click **Push**.

Now that you have completed deploying IoT Security with Prisma Access, see the "Working with Risk, Vulnerabilities, and Alerts" section.

Working with Risk, Vulnerabilities, and Alerts

With IoT Security deployed, you must incorporate using the IoT Security portal into your security operations. The procedures in this section provide a starting point for how to use IoT Security to evaluate your IoT risk, how to understand and resolve vulnerabilities in your devices, and how to respond and resolve alerts.

Procedures

Evaluating IoT Risk

- 9.1 Review Device Risk
- 9.2 Review Device Distribution by Risk

Assessing risk is a continuous process of discovering vulnerabilities and detecting threats. During this ongoing process, the IoT Security app measures risk and assigns a score for risk that it observes. The app scores risk at four levels of your organization, starting from individual IoT devices and expanding in scope to device profiles, sites, and finally, the entire organization. The different scores provide a simple means to check the risk posed at various points and areas of your network.

When assessing risk, the IoT Security solution uses both static and dynamic factors. Static risks form a baseline and include the following:

- Intrinsic risk factors specific to a profile such as OS, applications, roles, environment
- Trending threats that are hard to mitigate
- The usage behavior specific to a profile or a device
- All MDS2 risks (for medical equipment)

The solution adds the following dynamic risks on top of the baseline risk:

- Threats detected in real time (example: alerts)
- Behavioral risks, such as anomalies or user-practice issues, that also trigger alerts
- Vulnerabilities discovered through passive analysis and detections and through vulnerability scans using integrated third-party vulnerability scanning engines such as Qualys and Rapid7

By collecting and modeling data and analyzing vulnerabilities and threats, the IoT Security app calculates risk. The risk scores it generates consists of alerts, vulnerabilities, behavioral anomalies, and threat intelligence. When calculating the risk scores of device profiles, sites, and organizations, the app considers not only the scores of individual devices within a particular group but also the percent of risky devices in relation to all devices in the group.

9.1 Review Device Risk

The IoT Security app displays the risk score for each device on the Devices page in the Risk column. The app generates risk scores for devices daily.

Step 1: Log in to the IoT Security portal (example: examplesubdomain.iot.paloaltonetworks.com).

Step 2: Navigate to **Assets > Devices**.

Step 3: Review the device types and inventory on your network,

The Inventory section is sorted with the highest risk devices at the top. In the example shown below, Poly Video Conferencing devices have a risk score of 100.

Inventory (37,125)										
<input type="checkbox"/>	Status	Risk	Device Name	Profile	Vendor	Model	OS	IP Address	MAC Address	VLAN ID
<input type="checkbox"/>		100	Poly Video Conferencing Dev...	Poly Video...	Poly Inc.	Trio8800	Linux	10.28.51.134	00:e0:db:5d:dd:83	120
<input type="checkbox"/>		99	Crestron Building Automation...	Crestron B...	Crestron	TSW-730	Embedded	10.118.84.28	00:10:71:45:4d:a4	203
<input type="checkbox"/>		99	Cisco IP phone	Cisco IP P...	Cisco Syst...	CP-8861	Cisco IOS	10.128.242.205	58:97:1e:cc:94:ef	250
<input type="checkbox"/>		99	Zebra Label Printer	Zebra Lab...	Zebra Tec...	ZT410	Link-OS	10.128.10.32	ac:3f:a4:02:d3:20	275
<input type="checkbox"/>		99	Axis Communications Networ...	Axis Com...	Axis Com...	P3265-LVE	Linux	10.16.211.49	ac:cc:8e:bf:55:d5	120
<input type="checkbox"/>		96	c4:2f:90:89:90b9	Hikvision ...	Hikvision ...		Linux	192.168.1.17	c4:2f:90:89:90b9	
<input type="checkbox"/>		96	BrightSign Signage Media Pla...	BrightSign...	BrightSign...	XT1144	BrightSign...	10.28.51.133	90:ac:3f:24:2a:59	110
<input type="checkbox"/>		96	F5 Networks Device	F5 Networ...	F5 Networ...	Device XX...		172.16.241.4	00:94:a1:e5:42:86	2
<input type="checkbox"/>		74	8671860466867909	Worlex Tr...	Shenzhen ...		Embedded	10.194.67.178		
<input type="checkbox"/>		74	b8:27:eb:c7:e9:c9	Raspberry ...	Raspberry ...		Raspberry ...	192.168.100.103	b8:27:eb:c7:e9:c9	
<input type="checkbox"/>		74	00:1d:9c:c5:40:40	Rockwell ...	Rockwell ...			10.126.10.85	00:1d:9c:c5:40:40	91
<input type="checkbox"/>		64	b8:27:eb:9a:7d:a9	Raspberry ...	Raspberry ...		Raspberry ...	192.168.1.197	b8:27:eb:9a:7d:a9	

Step 4: To understand why this device has a high-risk score, click on the device name in the inventory section. As you scroll down, you see two severe alerts detected for this device:

- Access to a flagged Internet site detected.
- Suspicious port scanning activity.

Severity ▼
Active Alerts ▼
1 Week ▼

1 Access to flagged Internet site detected

1 Suspicious port scanning activity

Access to flagged Internet site detected

Detected
Investigating
Remediating
Resolved

Some services and hosts at specific IP addresses are flagged by up-to-date security research as being risky or having malicious intentions. Such websites are known to mislead users into providing personal information, deceive them into downloading viruses or malware, and even download malware just because users visited the site (something known as a drive-by download). Accessing services at these IP addresses risks infection and poses a security risk to the device.

Alert Type	Malware
local port	59072
risky category	Malware
risky remote host	146.0.32.144
payload bytes received	3634
payload bytes transmitted	956

Recommendation

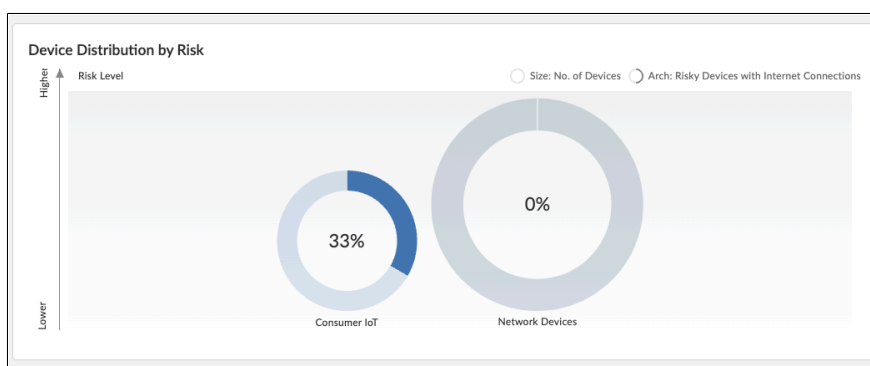
Events

Alert Detected
18:19, September 19, 2024

Step 5: As you scroll further, you will see that there are twenty-three vulnerabilities present in this device. Due to these and protocol behaviors exhibited by this device, IoT Security App has flagged this device as a high risk with a score of 100.

9.2 Review Device Distribution by Risk

Step 1: Continuing in the IoT Security portal, on the main page, you will see the window Device Distribution by Risk.



Step 2: To review the risk score for the devices, hover over the Consumer IoT circle.

Step 3: Click **Risky Devices**. A list of risky devices appears.

Inventory (3)												
0 Rows selected												
<input type="checkbox"/>	Status	Risk	Device Name	Profile	Vendor	Model	OS	IP Address	MAC Address	VLAN ID	VLAN Desc...	Last Ac
<input type="checkbox"/>		100	AppleTV	AppleTV	Apple Inc.	Apple TV	tvOS 8.4.4	10.130.80.100	6c:94:f8:e5:d3:23			08:52:
<input type="checkbox"/>		0	f4:f5:e8:68:27:e2	Google De...	Google Inc.			192.168.1.1	f4:f5:e8:68:27:e2			10:31:
<input type="checkbox"/>		0	b0:e4:d5:81:4a:aa	Google De...	Google Inc.			192.168.1.167	b0:e4:d5:81:4a:aa			10:56:

Procedures

Resolving IoT Vulnerabilities

- 10.1 Review an IoT Vulnerability
- 10.2 Resolve an IoT Vulnerability

A *vulnerability* refers to an intrinsic flaw built into the software or hardware of a device that is often well-known and can be exploited. A *risk*, on the other hand, considers environmental, configuration, behavioral, and security policy-related factors in addition to one or more underlying vulnerabilities. This distinction is important because some risks appear in the device details page but not on the Vulnerabilities page, and yet they can influence the severity level that the IoT Security app assigns to a vulnerability.

The app considers a vulnerability to be "potential" when it applies to a specific device type, model, and version number and one or more devices match the specified device type, but their model and/or version number are unknown. A vulnerability can also be considered "potential" if it applies only to devices with certain serial numbers and there are devices whose serial numbers are unknown but match the vulnerability description in all other regards.



Note

The IoT Security app detects vulnerabilities for IoT devices only. It does not provide vulnerability detection, alerts, policy recommendations, and network behavior analysis for IT devices. For IT devices, the app provides only device identification.

10.1 Review an IoT Vulnerability

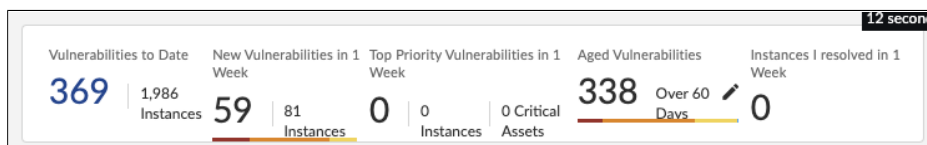
The Vulnerabilities page provides an overview of the vulnerabilities and vulnerable devices that the app detected, presenting the following information:

- The total number of confirmed and potential vulnerabilities organized by severity level
- A bar chart that shows the distribution of vulnerabilities by device profile
- A table listing vulnerabilities, each of which links to a page with further details

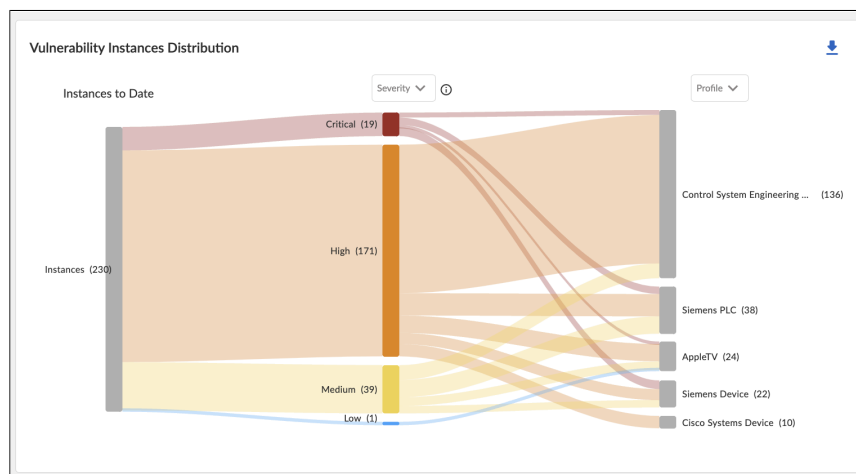
Step 1: Log in to the IoT Security portal (example: examplesubdomain.iot.paloaltonetworks.com).

Step 2: Navigate to **Vulnerabilities > Vulnerability Overview**, and then review the vulnerabilities and their distribution across the IoT device profiles on your network.

The summary of the vulnerabilities present over a time period (example one week) is shown at the top.



Step 3: To review the vulnerabilities and their distribution across the IoT device profiles on your network, scroll down.



Step 4: For additional details on the vulnerability, in the Vulnerability Instances Distribution section, click a device profile name (example: [AppleTV](#)). The All Vulnerabilities tab shows a table of vulnerability instances specific to the profile you clicked. In this example, there are 24 open vulnerabilities present in this device.

Vulnerabilities (24)

24 instances were identified for the following vulnerabilities.

Priority ↓

Vulnera...

Vulnerability Me...

S...C...E...E...A...C...P...C...C...P...Cr...

Threat & Compensating Metrics

Impact Metrics

<input type="checkbox"/>	Top	CVE-2021...	<div><div></div><div></div></div>	8.8	76%	Exploi...	No	No	No	Yes	1	0
<input type="checkbox"/>	Top	CVE-2024...	<div><div></div><div></div></div>	8.8	45%	Exploi...	No	No	No	Yes	1	0
<input type="checkbox"/>	Top	CVE-2023...	<div><div></div><div></div></div>	5.5	67%	Exploi...	No	No	No	Yes	1	0
<input type="checkbox"/>	Top	CVE-2020...	<div><div></div><div></div></div>	7.8	31%	Exploi...	No	No	No	Yes	1	0
<input type="checkbox"/>	Top	CVE-2021...	<div><div></div><div></div></div>	8.8	79%	Exploi...	No	No	Yes	Yes	1	0
<input type="checkbox"/>	Top	CVE-2024...	<div><div></div><div></div></div>	7.8	59%	Exploi...	No	No	No	Yes	1	0
<input type="checkbox"/>	Top	CVE-2022...	<div><div></div><div></div></div>	7	72%	Exploi...	No	No	No	Yes	1	0

Step 5: Click a vulnerability (example: [CVE-2021-30655](#)). The Vulnerability Details page appears.

Although a severity level in the IoT Security solution reflects a CVSS score, there is not always a direct correlation between the two. For example, a hard-coded password in a device might have a CVSS score of 10.0, but an IoT Security severity level of High rather than Critical. This can happen when there is not proof that the device can be accessed from the internet or by an unauthorized user. Although NIST assigns a CVSS score to a vulnerability generically, the solution assigns a “risk severity” level to vulnerabilities based on the specifics of each case.

Vulnerabilities / Vulnerability Details

Filter Query Entity = "vulnerability" Time Range = "All to Date" Profile = "AppleTV" x

Vulnerability = "CVE-2021-30655" x Add more filters or press "Enter" to search

Vulnerability Priority: ● Top CVSS Severity: High (v3)

Summary

Description A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 7.4.1, iOS 14.5.1 and iPadOS 14.5.1, tvOS 14.6, iOS 12.5.3, macOS Big Sur 11.3.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited..

Impact An attacker can exploit this vulnerability to execute remote code. This could compromise the confidentiality, availability and integrity of the device.

Detection Reasons 1 [View Details](#)

No. of Instances With CVE Evidence 0

Vulnerability Type Code Execution

Vulnerability Source IoT Security

NVD Published Date September 08, 2021

NVD Last Modified Date May 15, 2024

What can you do to reduce the risk?

- Palo Alto Networks IoT Security team recommends contacting the device vendor for available patches and assistance mitigating the vulnerability. Consider taking the following actions as well.
- Apply good [network design practices](#) that include network segmentation so you can restrict network access only to a subnet/VLAN (virtual local area network) reserved for device administrators.
- Monitor and log all network traffic attempting to reach affected products for suspicious activity. Block suspicious or unexpected traffic.
- When remote access is required, use a secure method such as a [VPN](#) (virtual private network) to encrypt traffic and ensure the workstation and server are not directly accessible from the Internet.
- Close all unused ports on the device.

10.2 Resolve an IoT Vulnerability

You resolve vulnerabilities through a workflow built into the IoT Security portal by either mitigating or ignoring the vulnerability. As a result, the device risk score might be lowered depending on other contributing factors such as the severity of the risk and the number and severity of other risks. Resolving a vulnerability on a device might similarly affect its profile, site, and organization risk scores, depending on how big of an impact the change makes in relation to the number and risk levels of other devices in the same group.

Step 1: To investigate a device with the selected vulnerability, in the Active Instances section at the bottom of the page, change the status to **Investigating**.

Active Instances (1) Addressed Instances (0)

Instance	Status	Confir...	IP Address	MAC Address	Site	First Detected Time
AppleTV	Detected ^	yes	10.160.88.101	6c:94:f8:e5:d3:23	OT Industrial	19:59, August 28, 2024

Change Status to

- Investigating
- Remediating
- Resolved

Items per page 25 1 - 1 of 1 rows 1 of 1 page

Step 2: After changing the status to Investigating, you will see the status of the vulnerability instance changes to Investigating.

Active Instances (1)							Addressed Instances (0)	
<input type="checkbox"/>	Instance	Status	Confir...	IP Address	MAC Address	Site	First Detected Time	
<input type="checkbox"/>	AppleTV	Investigating	yes	10.160.88.101	6c-94:f8:e5:d3:23	OT Industrial	19:59, August 28, 2024	

Step 3: After you finished resolving the issue, return to the **Vulnerability Details** tab and change the status to **Resolved**. The Change Status window appears.

Step 4: Select **Vulnerability Mitigated**, add comments, and then click **Resolve**. You return to the Active Instances on the Vulnerabilities Details page, and the resolved instance is no longer shown.

Change Status

The vulnerability instance status will change to **Resolved**

Select the reason for resolving this vulnerability instance:

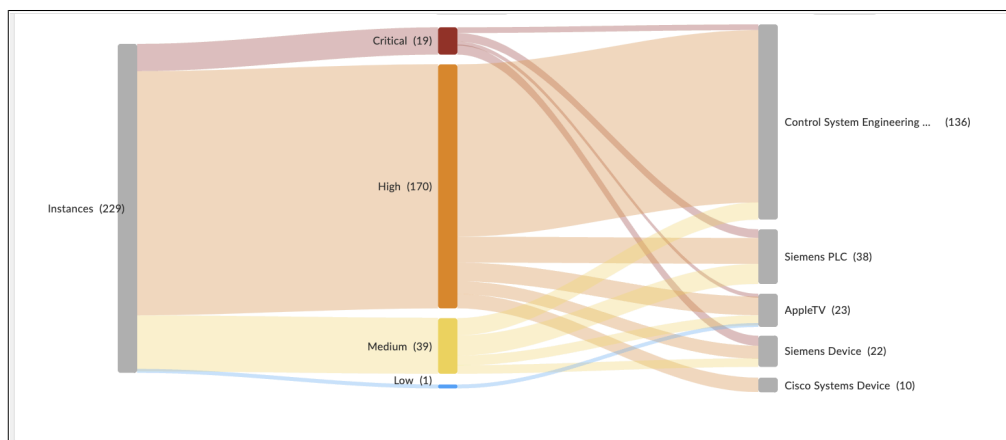
☒ **Vulnerability Mitigated**
Action was taken to mitigate the vulnerability. Select this to remove it and lower the device risk score. IoT Security will continue monitoring for this vulnerability on this device in case it reoccurs.

☐ **Vulnerability Ignored**
Select this to accept the vulnerability without taking any mitigating action. This also lowers the device risk score. IoT Security will no longer monitor for this vulnerability on this device.

Add Comments

Cancel Resolve

Step 5: To view that the vulnerability is resolved, you can go to Vulnerability Overview, scroll down to Vulnerability Instances Distribution, and hover over Apple TV, and you see the vulnerability count has reduced from 24 to 23.



Procedures

Resolving Security Alerts

- 11.1 Respond to a Security Alert
- 11.2 Resolve a Security Alert

The IoT Security app examines network traffic in real time, analyzing communications to and from every device on the network. If the app detects irregular behavior or policy-matching activity, it generates a security alert.

All security alerts are based on one of the following mechanisms:

- ML algorithms that automatically learn normal device behavior and can, therefore, detect abnormal behavior.
- Detection of specific traffic patterns without the use of ML algorithms. For example, the app generates alerts if devices connect to websites that site-reputation services have associated with malware.
- User-defined alert rules specifying activity that generates an alert when observed (blocking suspicious behavior), when not observed (allowing normal behavior), or when a device or group of devices goes offline for two hours.
- Threats on an IoT device are reported to the app in the threat log.

After you learn about a security alert, one of the first steps is to read the details and confirm that the event that triggered it occurred, possibly by checking firewall event log entries. After confirming the alert, you must quickly assess its importance and urgency, identify the type of equipment impacted, and then decide how to respond and with whom to engage. The responder might be IT security, clinical engineering, a third-party network security service provider, or perhaps the device vendor or manufacturer.



Note

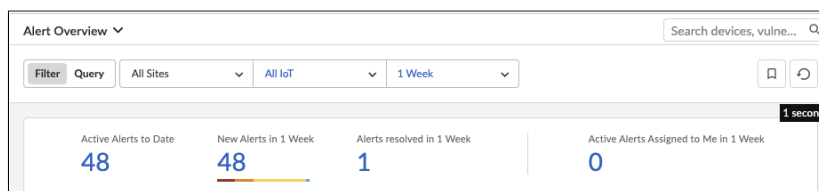
The IoT Security app generates alerts for IoT devices only. It does not provide vulnerability detection, alerts, policy recommendations, and network behavior analysis for IT devices. For IT devices, the app provides device identification only.

11.1 Respond to a Security Alert

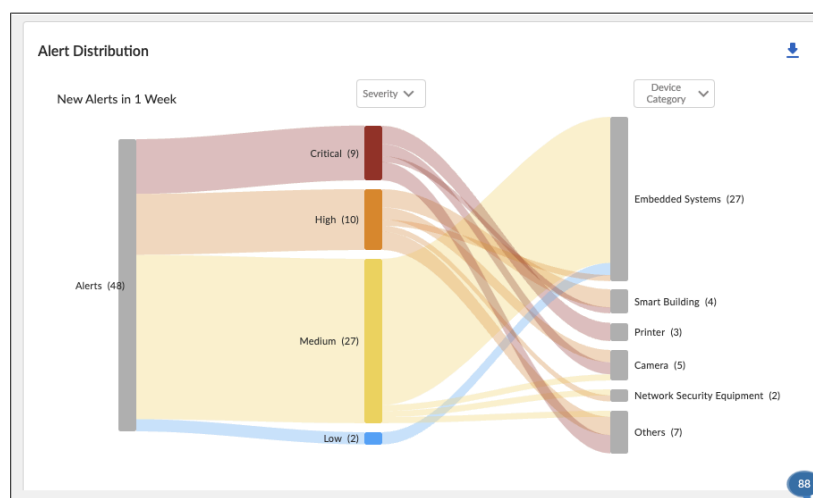
There are numerous ways to respond to a security alert. The action you take depends on the remediation requirements of the situation:

- If a device was infected by malware or a virus, unplug the device immediately. If its continued use is essential, work with IT security to quarantine it from the rest of the network. You might need to modify firewall security policies to permit only traffic absolutely required for the device to function and block everything else while you work on a resolution.
- The resolution might require a software patch, and sometimes you might have to get the equipment vendor involved to patch it. If you must continue using the equipment, enforce a strong Zero Trust policy until the patch is available.
- If an alert is generated by a security-policy violation, you can send policy recommendations to the firewall so that it only permits traffic resulting from normal device behavior.
- To assist in your analysis, the IoT Security app provides alert log files (in .csv and .log formats), which contain several days' worth of network connections involving the device that triggered an alert. You can also download the network traffic data that the app shows as a Sankey diagram and view it as an .xls spreadsheet.

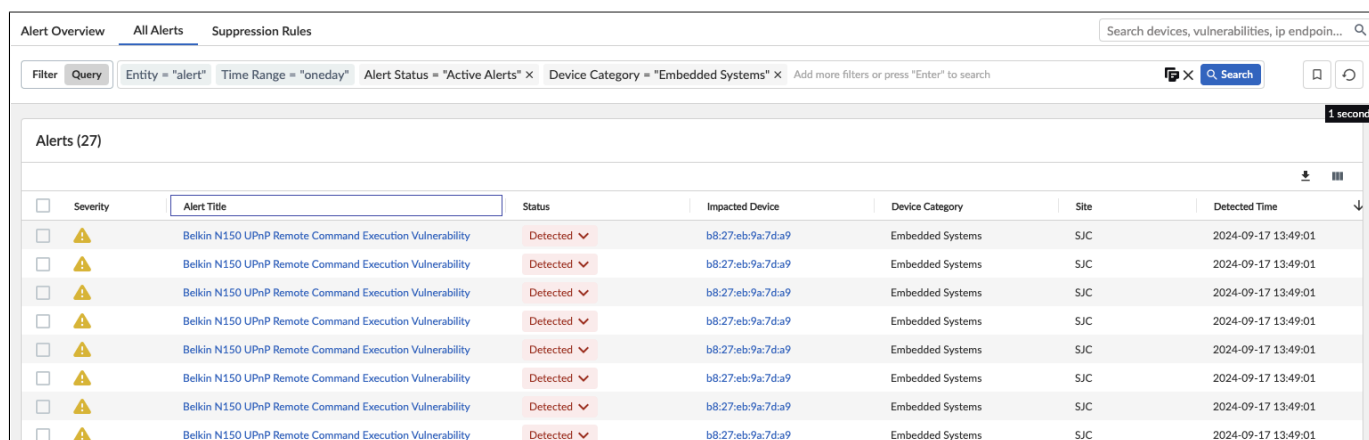
Step 1: To review the alerts and their distribution across the IoT device categories, navigate to **Alerts > Security Alerts**.



Step 2: For additional details on the alerts in a device category, in the Alert Distribution section, click a device category name (example: [Embedded Systems](#)).

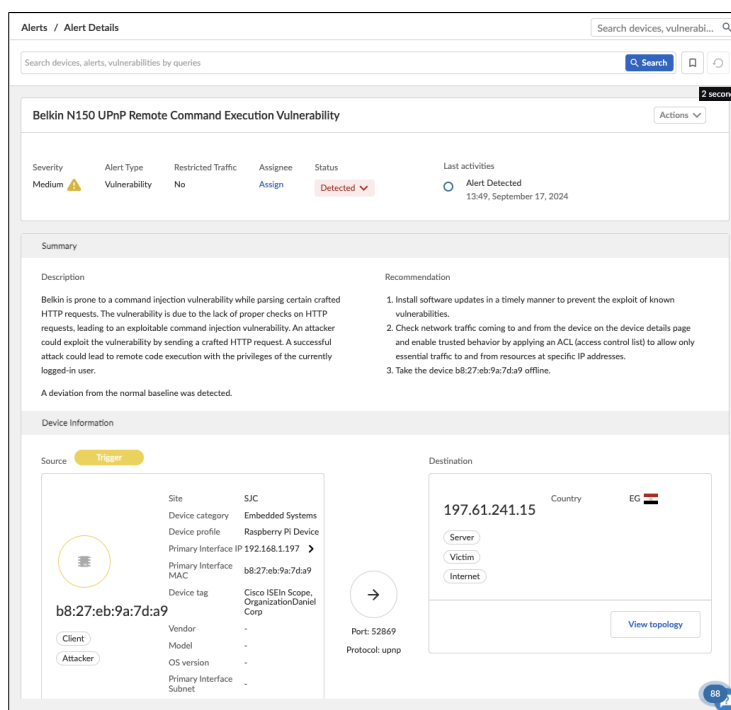


Step 3: On the All Alerts tab, select the first alert (example: [Belkin N150 UPnP Remote Command Execution Vulnerability](#)).



Severiy	Alert Title	Status	Impacted Device	Device Category	Site	Detected Time
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01
Medium	Belkin N150 UPnP Remote Command Execution Vulnerability	Detected	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01

Step 4: On the Alerts/ Alert Details page, you see the details of the alert.



Alerts / Alert Details

Search devices, alerts, vulnerabilities by queries

Belkin N150 UPnP Remote Command Execution Vulnerability

Severity: Medium **Alert Type:** Vulnerability **Restricted Traffic:** No **Assignee:** Assign **Status:** Detected **Last activities:** Alert Detected 13:49, September 17, 2024

Summary

Description

Belkin is prone to a command injection vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable command injection vulnerability. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could lead to remote code execution with the privileges of the currently logged-in user.

A deviation from the normal baseline was detected.

Recommendation

1. Install software updates in a timely manner to prevent the exploit of known vulnerabilities.
2. Check network traffic coming to and from the device on the device details page and enable trusted behavior by applying an ACL (access control list) to allow only essential traffic to and from resources at specific IP addresses.
3. Take the device b8:27:eb:9a:7d:a9 offline.

Device Information

Source **Trigger**

Site: SJC
Device category: Embedded Systems
Device profile: Raspberry Pi Device
Primary Interface IP: 192.168.1.197
Primary Interface MAC: b8:27:eb:9a:7d:a9
Device tag: Cisco ISE in Scope, Organization: Daniel Corp
Vendor: -
Model: -
OS version: -
Primary Interface Subnet: -

Destination

Country: EG
IP: 197.61.241.15
Port: 52869
Protocol: upnp

View topology

Step 5: To assign the alert, under Assignee, click **Assign**. The Assign page appears.

Step 6: In the **Assign the alert to** box, enter the email address, then in the **Comments** box, add a comment, and then click **Assign**.

11.2 Resolve a Security Alert



You resolve security alerts through a workflow built into the IoT Security portal. Essentially, you resolve them by either mitigating or ignoring the alert. As a result, the device risk score might be lowered depending on other contributing factors, such as the severity of the risk and the number and severity of other risks. Resolving an alert on a device might similarly affect its profile, site, and organization risk scores depending on how big of an impact the change makes in relation to the number and risk levels of other devices in the same group.

The status of an alert begins in the Detected state. You can leave it there or set it to a different state to reflect where it is in the remediation process.

- **Detected**—This is the state of a newly detected alert. Keep it in this state if no action has been taken to investigate, remediate, or resolve it.
- **Investigating**—Set an alert to this state after preliminary work has started and it is being verified, researched, and its impact analyzed.
- **Remediating**—Set an alert to this state while action is being taken to remediate it but has not yet completed.
- **Resolved**—An alert is resolved either by mitigating the issue or by ignoring and accepting it.

Step 1: After the assignee has resolved the alert, navigate to the **Alert > Security Alerts** page, click the **All Alerts** tab, and then change the status of the alert to **Resolved**. The Change Status window appears.

Step 2: To view resolved alerts, click the **Alert Overview** tab, and then, at the top of the page, click **Alerts resolved in 1 Day**.


Alerts (1)							
<input type="checkbox"/>	Severity	Alert Title	Status	Impacted Device	Device Category	Site	Detected Time
<input type="checkbox"/>		Belkin N150 UPnP Remote ...	Resolved 	b8:27:eb:9a:7d:a9	Embedded Systems	SJC	2024-09-17 13:49:01

Items per page: 25 1 - 1 of 1 rows

1 of 1 page


Step 3: To review the status of a resolved alert, click the alert. The Alert page appears.

The Alert Events history detailing the assignment and resolution appear on the right side of the page.


Belkin N150 UPnP Remote Command Execution Vulnerability

Severity **Medium**
Status **Resolved**
Assignee
Traffic Restricted **No**

[New Alert Detail Page](#)
Action


b8:27:eb:9a:7d:a9


Client Attacker

IP: 192.168.1.197

Category: Embedded Systems

Site:

Confidence Level: High



Port: 52869

Protocol: upnp

197.61.241.15

Server Victim Internet

Country: EG

Belkin is prone to a command injection vulnerability while parsing certain crafted HTTP requests. The vulnerability is due to the lack of proper checks on HTTP requests, leading to an exploitable command injection vulnerability. An attacker could exploit the vulnerability by sending a crafted HTTP request. A successful attack could lead to remote code execution with the privileges of the currently logged-in user.

A deviation from the normal baseline was detected.

device profile	Raspberry Pi Device
client port	57610
threat ID	56279
threat category	code-execution
threat type	vulnerability
number of occurrences	1
reference	reference
alert source	Firewall
firewall name	uk2-gcp
firewall action	Terminated the session and sent a TCP reset to both sides of the connection
firewall inbound interface	ethernet
firewall outbound interface	ethernet

Alert Events

- Alert Detected**
13:49, September 17, 2024
- test**
Issue Mitigated,
Resolved by Victor Kameyama
14:04, September 17, 2024

Feedback

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

HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA

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

©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 <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. Palo Alto Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.



You can use the [feedback form](#) to send comments about this guide.

