paloalto
TECHDOCS

IoT Security Best Practices

July 8, 2020

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support.html

About the Documentation

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

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

©2020–2021 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 8, 2020

Table of Contents

©2021 Palo Alto Networks, Inc.

 ©2021 Palo Alto Networks, Inc.

paloalto TECHDOCS

IoT Security Best Practices

This document is a streamlined checklist of predeployment, deployment, and post-deployment best practices that you should follow when you implement IoT Security.

This guide is organized into the following sections:

Plan Your IoT Security Deployment Using Best Practices

Consider the following best practices when preparing an IoT Security deployment.

STEP 1 | Set goals for your IoT Security deployment. What will it provide as part of your network security strategy?

Examples:

- Goal 1: Gain visibility into your IoT assets through a dynamically generated IoT device inventory
- Goal 2: Protect your IoT devices and network resources from attack by reducing device vulnerabilities and by enforcing security policies

STEP 2 | Define responsibilities.

Determine who will be responsible for addressing risks that IoT Security detects, who will require access to the IoT Security portal and the level of access they'll need, and whether you'll need a team for patching device software.

STEP 3 | Foster cross-functional collaboration between your IT infrastructure and networking team and your IT security team.

These teams should work together during the design phase to determine whether the current firewall deployment is sufficient and, if not, where you'll need to add firewalls to act as network traffic sensors and as potential policy enforcers.

STEP 4 | Decide where to position firewalls.

Firewalls must see IoT device traffic and have DHCP traffic routed through them so that IoT Security can map device IP addresses to MAC addresses. Use the following list to determine where to put firewalls on your network.

- ❑ Deploy one or more firewalls where they see traffic from IoT devices. IoT Security must collect data from network traffic for analysis. For example, because most IoT devices in enterprises connect to servers, you could place firewalls where they can see traffic from IoT devices to those servers, whether they're in private data centers or the cloud. Deploying more firewalls in the MDF (main distribution frame) and IDFs (intermediate distribution frames) can further maximize coverage. You might also need to add firewalls internally to see traffic behind NAT devices. You can deploy firewalls inline to collect data and enforce policy, or deploy them as sensors (inline or in tap mode) to function only as data collectors.
- ❑ Ensure that DHCP traffic between DHCP relay agents or DHCP clients and the DHCP server flows through the firewall. Alternatively, use the firewall as a DHCP relay agent. DHCP traffic is essential for IoT Security to learn the MAC addresses of IoT devices because it uses them to track each device and learn its behavior.
- ❑ When devices are behind a NAT device, put another firewall behind the NAT device to gain visibility into those devices.

STEP 5 | Decide if you will perform a phased deployment (often necessary in a large network).

 ©2021 Palo Alto Networks, Inc.

STEP 6 | Set the level of granularity for Security policy enforcement that you want to achieve.

For example, put devices in groups sharing a specific attribute–category, profile, vendor, model, OS family, or OS version–or use a profile or category grouping. A next-generation firewall administrator can do the following:

1. Include multiple device objects in a single security policy under source or destination.
2. Create a single device object that has multiple attributes (for example, Category=Entertainment, Profile=Acme TV, and OS family=Acme OS).

 ©2021 Palo Alto Networks, Inc.

Deploy IoT Security Using Best Practices

Consider the following best practices when deploying IoT Security and then when using it.

STEP 1 | Gain insight into your IoT inventory.

1. Give new unidentified devices default network access so they can establish their normal behavior and IoT Security can identify them. Then the firewall will apply policy rules to traffic to and from those new devices based on a device ID attribute—device category, profile, vendor, model, OS family, or OS version.
2. Enable logging and log forwarding on the firewall and provision IoT Security.
   - Enable all available logging on the firewall, including Enhanced Application Logs (EALs), on the firewall. EALs are necessary to capture the data in packet payloads, which the IoT Security solution uses to identify devices.
   - Enable log forwarding so that the firewall sends collected data to Cortex Data Lake and so the IoT Security solution can access that data.
   - Provision an IoT Security cloud tenant to start analyzing data. For information about onboarding IoT Security, see the IoT Security Administrator Guide.
3. Allow approximately one week for IoT Security to gather and analyze enough traffic to establish a stable device inventory and baseline. Although IoT Security will identify most devices within hours of receiving logs from the firewall, it is normal for device identification to change during the first few days as more data is collected. Additionally, IoT Security will identify devices with more traffic faster than those that generate less traffic.
4. If the confidence level for an IoT device isn't high confidence, there could be several causes and several actions you can take.
   - The device is inactive and there isn't enough data about its network behavior to identify it with a high level of confidence. If this is the case, you can help the device to generate more network traffic.
   - If changes to the deployment or security posture of a device affected its network behavior or the collection of its behavior, restart the baseline process to give it a fresh start.
   - If the IoT device is behind a NAT device along with other devices, their traffic will appear to come from the same source and present a mix of behaviors. In this case, consider deploying a firewall to collect network data from behind the NAT device.
   - If you deploy a firewall as a sensor in tap mode, check if incoming data from the SPAN port on the switch includes both TX and RX data. If not, it's possible that asymmetric routing is not delivering traffic to the same SPAN port. Reconfigure the switch to correct this.
   - If you know the identity of the IoT device, manually enter the information in Device Details in the IoT Security portal.
   - If you don't recognize the device, you've eliminated the other possible causes above, and IoT Security still hasn't confidently identified the device, then there might not be enough samples of network behavior for this particular device profile. In this case, the

 ©2021 Palo Alto Networks, Inc.

only option is to allow additional time for IoT Security to collect data and learn about the device and similar devices in that same profile.

Device confidence scores are on the Devices page in the IoT Security portal.

STEP 2 | Identify and protect your most critical IoT devices.

1. Determine which IoT devices are mission-critical; that is, those devices that are required to sustain business continuity. For example, for healthcare companies, this could be medical equipment used to diagnose and treat patients; or for industrial environments, this could be factory-line devices such as programmable logic controllers on the factory floor.
2. Make sure the confidence level is high. This is important because IoT Security will not push IP address-to-device mappings to firewalls until they reach a high confidence level. See the suggested actions to take when a device does not achieve high confidence described in Step 1.
3. Check that the IP address-to-device mappings in the firewall are accurate by picking a few IoT devices at random and comparing their device category, profile, vendor, model, OS family, and OS version (OS name + version) in the IoT Security portal and firewall.
4. Use device profiles identified by IP address-to-device mappings as the source or destination in your Security policy rules and place them in suitable positions near the top of your rulebase so they will match. This enables you to simplify your security policy configuration by using IoT device types instead of IP address groups.

STEP 3 | Extend protection to all IoT devices.

Conduct continuous assessments of your device inventory to find devices on your network that IoT Security has not yet discovered. Investigate why these devices are missing. You might need more firewalls to capture traffic in certain sections of your network. Check whether DHCP traffic is observed from those devices and, if not, find any gaps in coverage and fill them.

STEP 4 | Implement a zero-trust policy.

Use IoT Security to implement a zero-trust policy as described in Best Practices Implementing Zero Trust with Palo Alto Networks. The following are the five steps for this implementation strategy:

1. Identify your critical protect surfaces; that is, the data, applications, assets, and services (DAAS) that you want to protect. IoT Security assists with this step by detecting and classifying all IT and IoT devices on your network.
2. Map your critical transaction flows. IoT Security helps with this by tracking network behaviors of all your devices.
3. Architect your zero-trust network. Logically organize the IoT devices into a manageable number of groups. Within each group, the devices share the same set of policy rules. The configuration construct on the firewall is a device object containing all the devices that are sharing a specific attribute–category, profile, vendor, model, or OS group. The granularity of this filter is up to each administrator but applying a Security policy rule at the device profile level should satisfy most cases.
4. Create zero-trust policy rules. IoT Security helps with this by making policy recommendations based on the observed device behaviors and activities. When implementing your Security policy rules, start with your most valuable and critical DAAS

 ©2021 Palo Alto Networks, Inc.

protect surfaces. Then move on to the next set of protect surfaces on the priority list and keep going through the list until you reach your security goals.

5. Keep your network security current. IoT Security helps with this by dynamically maintaining a device inventory of your monitored devices and their network behaviors.

STEP 5 | Enable notifications of security alerts via email, SMS, or both.

This enables IoT Security to notify you immediately so that you can respond faster.

STEP 6 | Configure the weekly generation of risk reports to discover new risks and to check on the status of those under investigation.

 ©2021 Palo Alto Networks, Inc.

Monitor Your IoT Security Deployment Using Best Practices

When maintaining your IoT Security deployment, it's helpful to view the maintenance in terms of daily, weekly, and monthly tasks.

Daily

- Check security alerts that you learn about through email or SMS notifications or by scanning the Security Alerts page in the IoT Security portal (**Alerts** > **Security Alerts**) and respond as appropriate for their severity and urgency.
- Review system alerts in the IoT Security portal (**Alerts** > **System Alerts**) and the Firewalls page (**Administration** > **Sites and Firewalls** > **Firewalls**) to check that firewalls are connected to IoT Security. If a firewall is disconnected, IoT Security stops analyzing log data and no new device detections and identifications occur. Serious events that increase risk to your devices and your network could be missed.
- Scan the Devices page for newly discovered devices and confirm that their network access is authorized. Unauthorized devices pose a threat if they did not undergo an onboarding process that provisions them to do all the following: connect to appropriate network segments, use only approved applications, and (if the devices support it) run required endpoint protection.

Weekly

- On the Firewalls page in the IoT Security portal, watch for unusually large shifts in log volume from firewalls. An unexpected spike or dip might indicate anomalous network activity or a change to the configuration or connection of a firewall.
- Track the network activity of high-value devices on the Devices page in the IoT Security portal. If a normally active device is unexpectedly inactive, check the last time it was active (you can also do this on the Devices page). Investigate further if the length of inactivity raises concern.
- Review the weekly Risk report to check for any new risks and track the status of work remediating existing risks.
- Check that the firewall regularly receives IP address-to-device mappings from IoT Security to ensure no devices are missing from policy enforcement. Use the following two CLI commands to check the connection status between the edge servers and firewall and which mappings the firewall received:

  `show iot icd statistics verdict` – Shows statistics about the IP address-to-device mappings, or verdicts, that the ICD (Identity Client Daemon) running on the edge server in front of the IoT Security cloud sent to the IoTd (IoT daemon) running on the firewall.

  `show iot ip-device-mapping all` – Shows which IP address-to-device mappings (verdicts) the firewall received.

 ©2021 Palo Alto Networks, Inc.

Monthly

- When there's a network expansion, look for new network segments. If necessary, deploy more firewalls to provide additional coverage and make sure traffic from devices in these segments reaches the firewall and is reported to Cortex™ Data Lake.
- Review user audit logs in the IoT Security portal (**Administration** > **Audit Logs**) for unusual activities, such as unexpected configuration changes.
- Use Policy Optimizer (**Policies** > **Security** > **Policy Optimizer**) in the firewall web interface to check if recommended policies added to the firewall are being used and make adjustments to policy rules as needed.

©2021 Palo Alto Networks, Inc.