Automation

OVERVIEW

MAY 2020

paloalto® NETWORKS

Table of Contents

Preface 1

Purpose of This Guide 3

Audience 3

Related Documentation 3

Introduction 4

Automation 5

Automation within the Platform 8

Threat Intelligence 8

Cortex 9

Automating with the Platform 11

Palo Alto Networks APIs and Features for Automation 11

Automation Tools 16

Use-Cases for Automation 20

Deployment Use-Cases 20

Configuration Use-Cases 22

Response Use-Cases 23

Assess Use-Cases 26

Summary 28

Related Resources 28

Preface

GUIDE TYPES

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

Reference architecture 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.

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 VERSION OF GUIDES

We continually update reference architecture and deployment 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

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

- Branding changes for Strata, Prisma™, and Cortex™ platforms
- Minor corrections

Comprehensive revision history for this guide

Purpose of This Guide

This guide describes how organizations can use automation along with the Palo Alto Networks Strata, Cortex, and Prisma platforms to increase the speed, consistency, quality, and reliability of the tasks they perform. This guide also covers how the platform elements natively use automation to provide a security posture that keeps pace with attackers.

AUDIENCE

This guide is written for technical readers, including system architects and design engineers, who want to explore ways they can use automation with the Palo Alto Networks platforms. It assumes the reader is familiar with the basic concepts of applications, networking, virtualization, and security, as well as a basic understanding of network, data center, and public cloud architectures.

RELATED DOCUMENTATION

The following document supports this guide:

- Prevention, Detection, and Response for Security Operations: Reference Architecture Guide—This guide provides solutions for prevention, detection, investigation, and response to help security operations prevent threats and efficiently manage alerts.

Introduction

In order to monetize their attacks, cybercriminals are evolving and attacking everywhere that data and computing live. Although attackers continue to use exploits and search out vulnerabilities, their methods are evolving with file-less attacks, through the hijacking of legitimate tools such as software update mechanisms, and through automation and automatic propagation to make their attacks more impactful. Not only are attackers evolving, but the number of attackers is also increasing. Malware toolkits, botnets for hire, and attack frameworks are contributing to an increased volume and sophistication of attacks against which organizations must defend.

Because data and computing reside in so many places, manually monitoring all of the possible attack vectors is challenging and getting harder every day. Traditional security infrastructure with dozens of disparate security products, which each monitor a specific attack vector, requires analysts to stitch together insights from many disconnected sources before acting. Analysts are missing attacks in the deluge of data. Even when analysts find attacks, in many cases it is too late.

Not only are many organizations finding it challenging to keep their security posture up-to-date in the face of these evolving attacks, they also are struggling with their evolving technology environments as they onboard increasing numbers of applications and devices. One of the primary challenges organizations face is that performing the routine tasks required to operate their security infrastructure takes so much time that there isn’t enough time left to devote to improving or updating the security infrastructure and posture. The amount of time these routine tasks take have a real impact on security. To properly provide security, as changes occur in the applications and data, the security infrastructure needs to change along with it. If it takes a significant amount of time for the security infrastructure to reflect those changes then during that period either the security posture is reduced, or the organization can’t take advantage of the changes until the security teams bring the infrastructure up-to-date.

Two trends exacerbate the amount of time these routine tasks take. The first trend is that applications and systems are increasingly more dynamic. It doesn’t take months to deploy a new application anymore. Organizations can deploy new applications in less than a day. Systems, especially those built around IaaS and PaaS environments, are also increasingly dynamic. Some cloud applications might live only for minutes. Every time an application is on-boarded or removed, or when environments change, the security infrastructure also needs to be updated. The second trend is the increasing number of systems and environments that must work together for any one application or service to function correctly. Distributed systems that allow for easier scaling have taken over for monolithic applications. Changes now have a cascade effect on the security infrastructure, as well as requiring coordination across many separate systems.

Manually keeping up with the pace of change and the number of systems involved takes more resources than most organizations have, causing a large queue of uncomplete work. Manual operations aren't going to get easier. The number of applications and systems will only increase, and few organizations can hire enough staff to handle routine tasks manually much less have time to focus on hunting threats, combatting sophisticated attacks, and other activities that add value to the organization. Hiring enough staff isn't just a problem of money. Manually operating the security infrastructure and integrating it into an organization's systems requires a wealth of experience and finding qualified candidates for open positions with the expertise required can be challenging.

Working faster isn't necessarily a solution, either, because it is critical that organizations follow best practices when designing and configuring security infrastructure. Moving faster in a manual environment often produces mistakes and often only a best-effort implementation of best practices and governance. Human error and lack of governance have a significant detrimental impact on the security posture. However, many organizations are having to choose between a security infrastructure that slightly works but is easy to operate and one that protects but is slow to change.

AUTOMATION

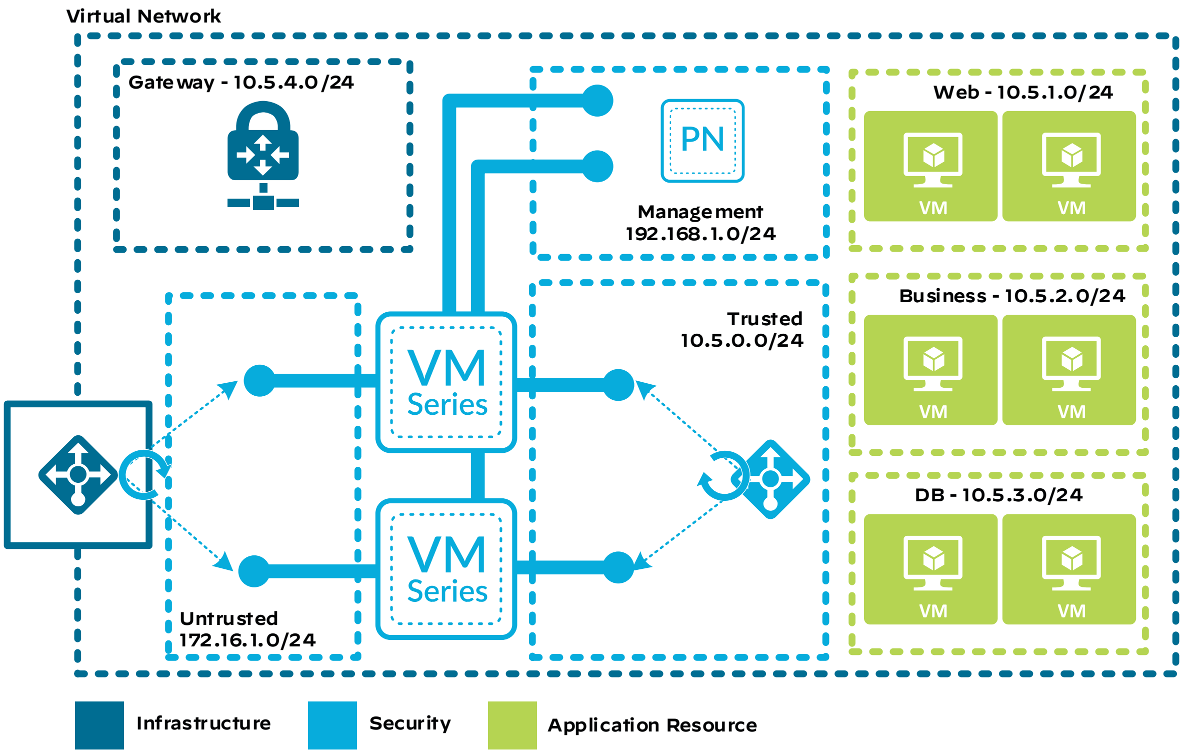
By increasing the speed, consistency, quality, and reliability of tasks, automation helps organizations deal with both evolving attackers as well as their own evolving technical environments. Automation is an extensive topic and can be used across many areas of an organization, as well as for different deployment and operational use-cases.

One method of simplifying automation is to consider the dependencies and layers of a system as separate building blocks. Common building blocks include:

- **Infrastructure**—Networking, routing, load balancers, and infrastructure security such as access control lists (ACLs).
- **Security**—Security infrastructure, firewalls, and policies integrated into the infrastructure building block as well as services that may live outside the infrastructure.
- **Application Resources**—Compute, storage, and services specific to an application and integrated into the infrastructure.
- **Application**—Application code running on and interacting with the application resources.

Although automation can live across these layers, modularizing and focusing automation tasks to specific building blocks allow the organization to leverage the automation across multiple projects and allow the automation to scale. If a single automation task worked across all the layers, it would be useful only to that specific scenario, and any future scenario would require rework. Instead of a monolithic automation action that does everything, the organization modularizes the automation tasks—modularization with a higher-level automation action that runs the tasks in order and with the scenario specific parameters brings significant leverage and reuse.

Figure 1 System layers



Not every task should be automated. The most significant benefit to an organization comes from automating tasks that are frequently executed, simple to perform, or error-prone. The dynamic nature of cloud environments drives automation requirements across all of the building blocks, while more static environments might only have automation needs in a single building block. The key to defining what should be automated is to find the tasks that bring value to the organization through efficiency.

Organizations can find value in automation without having complex automation infrastructure or processes. Automation can be implemented through techniques anywhere between simple scripts to complex continuous integration/continuous delivery (CI/CD) workflows.

Automation is often associated with DevOps philosophies and practices that aim to unify developers and operations staff by eliminating hand-off processes and functional silos. DevOps focuses on shorter development cycles, with increased deployment frequency and more reliable releases. DevOps is a cultural shift that many organizations are going through, and automation is critical to that transition. However, organizations are not required to have a DevOps culture to find value through automation. As more systems use automation natively to simplify the administrative burden and become more efficient, it is possible that for some use-cases organizations might not have to develop automation themselves but instead choose products that use built-in automation.

This guide focuses on the value and use-cases of automation in the security layer. Automation is a broad topic and there are many ways to use automation to better deal with the routine tasks performed on the security infrastructure. One way to simplify security automation is to group tasks based on when they are executed. Common groups of security tasks are:

- **Deploy**—Automation that supports the deployment of the Palo Alto Networks platform elements. Often described as “Day-1” tasks, deployment automation typically uses templates and declarative statements to define the state of the infrastructure to be deployed.
- **Configure**—Automation that configures the elements of the Palo Alto Networks platforms after their deployment to make them operational. Configuration automation not only deals with “Day-1” configuration but also supports the day-to-day or “Day-N” operation of the platform elements. “Day-N” automation performs the create, read, update, and delete operations as needed by the organization. These operations are often planned or scheduled based on business needs.
- **Respond**—Automation of configuration changes in response to specific operational or security events. These unplanned changes allow Palo Alto Networks platforms to adapt to changes in the environment and threat landscape automatically.
- **Assess—**Automation that supports the retrieval, processing, and reporting of security data. The data can be from a single source or correlated across multiple disparate systems. This automation makes no changes to the Palo Alto Networks platforms but instead leverages the security data it contains.

Automation within the Platform

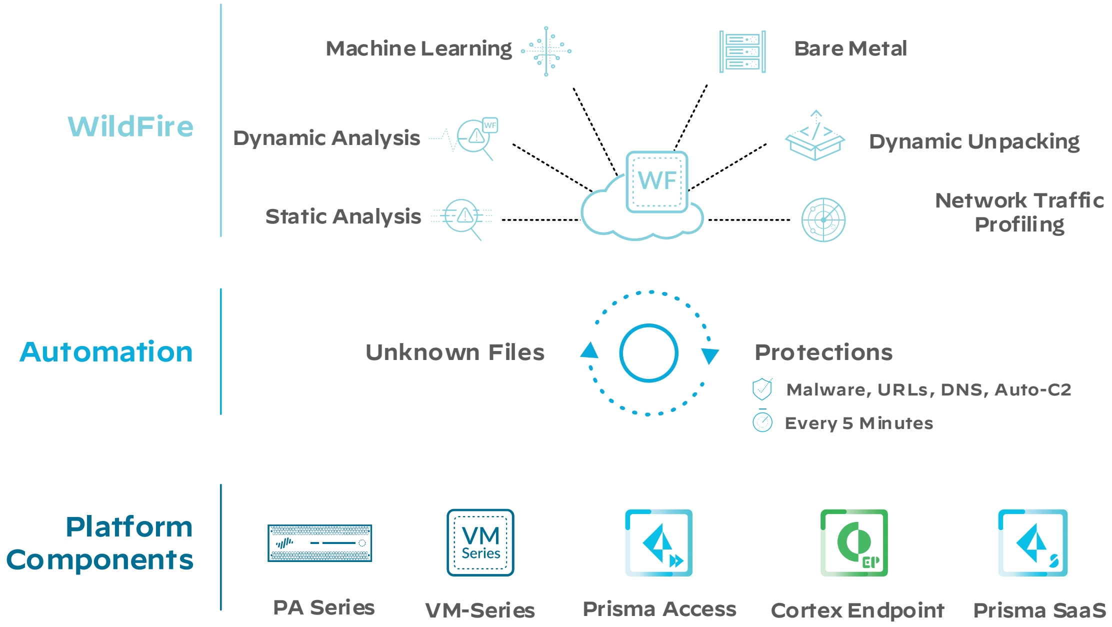
Automated protections through cloud-delivered security services allow the Palo Alto Networks Strata, Cortex, and Prisma platforms solutions to automatically deal with the deluge of data required to identify and protect against attacks. The platforms do this in two ways. First, through a global sensor network that turns unknown threats into known threats and automatically extends new protections to customer devices in minutes. Second, through a data analytics platform that allows organizations to rapidly adopt innovative new security technology and automated responses with the same scale, leverage, and agility employed by their adversaries.

THREAT INTELLIGENCE

The Palo Alto Networks platforms benefit from a community of comprehensive global threat data sharing to minimize the spread of attacks and raise the costs to attackers. No single organization will ever see all global threats, but as part of a network, they benefit from collective intelligence. The detection and sharing of a new threat in one organization triggers the automatic creation and dissemination of prevention mechanisms across the entire community. As the community grows, the wider protections propagate, limiting the spread of attacks and, consequently, their effectiveness.

As a core element of the Palo Alto Networks Threat Intelligence Cloud, WildFire® is a large distributed sensor system that identifies and prevents unknown threats, with tens of thousands of subscribers contributing to the collective immunity. When WildFire sees a new malware or exploit, WildFire automatically creates and shares a new prevention control in about 5 minutes, without human intervention.

Figure 2 Security automation with WildFire



CORTEX

Cortex simplifies security operations and improves security outcomes through its open and integrated AI-based continuous security platform. Deployed on a global, scalable public cloud platform, Cortex automatically speeds the analysis of the massive amount of security data generated by the Palo Alto Networks platform elements. Cortex leverages Cortex Data Lake, where customers securely and privately store the data. Cortex Data Lake normalizes the data, allowing apps, such as Cortex XDR, to stitch together relevant information received from across the organization to find threats and orchestrate responses automatically.

Cortex Data Lake

Cortex Data Lake is a customer-specific data store that allows apps to deliver precise, instrumented outcomes built upon high-fidelity data across the entire platform. It enables apps to deliver unique value from data collected through next-generation firewall enhanced logs, endpoint events, and SaaS security events from the components of the platform. Cortex Data Lake stores all potentially valuable raw data from which new transforms are created for consumption by another system or analytics engine. These transforms can calculate new fields or trends, correlate with other data sets, and broaden or narrow the data view to fit a specific purpose and timeframe.

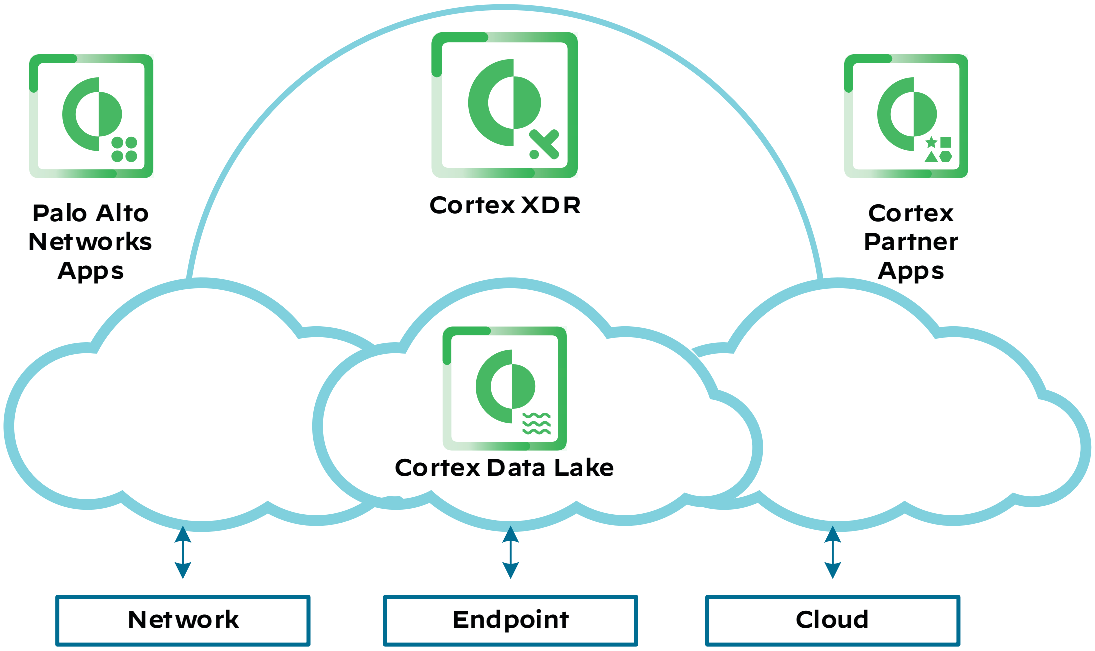
Cortex XDR—Analytics

Cortex XDR—Analytics empowers you to automatically discover malware, command and control, lateral movement, and data exfiltration. By applying machine learning to network, endpoint and cloud data, it accurately identifies targeted attacks, malicious insiders, and malware. Cortex XDR—Analytics uses behavioral analytics and machine learning to analyze information stored in Cortex Data Lake to track hundreds of attributes of behavior. Cortex XDR—Analytics uses this information to baseline activity to determine normal behavior on a network and build profiles of users and devices. Using these profiles, it generates alerts for observed abnormal behavior, allowing you to identify malicious traffic which would otherwise remain hidden or ignored.

Cortex XDR—Investigation and Response

Cortex XDR—Investigation and Response consumes and correlates data from Cortex Data Lake to reveal threat causalities and timelines and to provide visibility into your endpoint and network traffic. The Cortex XDR—Investigation and Response app triggers alerts based on indicators of compromise, including behavioral anomalies, and can send those alerts to Cortex Data Lake. Cortex XDR—Investigation and Response speeds alert triage and incident response by providing a complete picture of each attack and revealing the root cause automatically for you.

Figure 3 Cortex components



Automating with the Platform

The automation capabilities built into the elements of the Strata, Prisma, and Cortex platforms enable the automatic detection and response to evolving security threats. The platforms also provide organizations with the ability to build automation specific to the deployment, configuration, and response requirements unique to their environment.

This automation is enabled through APIs and other features built-into the platform elements. To make automation simpler, Palo Alto Networks also offers examples and integrations for industry-standard automation tools.

PALO ALTO NETWORKS APIS AND FEATURES FOR AUTOMATION

The elements of Palo Alto Networks platforms have extensive features and capabilities that can be used to support automation. Each element of the platform has a different role to play in automation, and their automation capabilities match their role.

The features and capabilities you should use when automating a task depend on the type of tasks being automated. Use the following table to determine which features and capabilities are relevant to each area.

Table 1 Platform automation features by area of automation

Feature	Deploy	Configure	Respond	Assess
FW bootstrapping	✓	—	—	—
PAN-OS® API	✓	✓	—	—
User-ID™ and dynamic address groups	—	✓	✓	—
Auto tagging	—	—	✓	—
HTTP log forwarding	—	—	✓	—
External dynamic lists w/ Cortex XSOAR	—	—	✓	—
WildFire API	—	—	✓	—
Prisma Cloud integrations	—	—	✓	—
Prisma SaaS auto-remediation and API	—	—	✓	✓
AutoFocus™ API	—	—	—	✓
Cortex XSOAR	—	—	✓	✓

PAN-OS APIs and Features

There is a rich set of capabilities that helps organizations integrate deployment, configuration, response, and assessment automation to PAN-OS devices such as the VM-Series and PA-Series firewalls, as well as Panorama™.

Bootstrapping

Bootstrapping allows you to create a repeatable process of deploying VM-Series or PA-Series firewalls through a bootstrap package. The package can contain everything required to make the firewall ready for production or just enough information to get the firewall operational and connected to Panorama. The amount of information contained in the bootstrap package often will reflect how comfortable the organization is with automation technologies. Organizations that have adopted DevOps methodologies are more likely to configure the firewalls through the bootstrap package or external automation, and organizations that have not adopted DevOps are more likely to use a centralized system like Panorama to manage the security policy. The bootstrap package contains directories for configuration, content, license, and software. On the first boot, the firewall mounts the file share and uses the information in the directories to configure and upgrade the firewall. After the firewall is out of the factory default state, it stops looking for a bootstrap package.

You can use bootstrapping for the deployment of PA-Series and VM-Series firewalls, in both private networks and in the public cloud. You can use it to deploy PA-Series firewalls to hundreds of remote branches as well as VM-Series firewalls in public cloud environments. One of the fundamental design differences between traditional and public-cloud deployments is the lifetime of resources. One method of achieving resiliency in public cloud deployments is through the quick deployment of new resources and quick destruction of failed resources. One of the requirements for achieving quick resource build-out and tear down is current and readily available configuration information for the resource to use during initial deployment. When the configuration is static, the simplest method of achieving this for VM-Series firewalls is to use bootstrapping to configure the firewall policies during firewall deployment.

After bootstrapped firewalls deploy, external automation templates can configure the firewall and keep the firewall policy up-to-date. Alternatively, firewalls can automatically pull configuration information from Panorama. VM-Series firewalls use a VM authorization key and Panorama IP address in the bootstrap package to authenticate and register to Panorama on its initial boot. You must generate the VM authorization key in Panorama before creating the bootstrap package. If you provide a device group and template in the bootstrap package's basic configuration file, Panorama assigns the firewall to the appropriate device group and template so that the relevant rulesets are applied, and you can manage the device in Panorama going forward.

APIs

The PAN-OS API allows organizations to manage VM-Series and PA-Series firewalls, as well as Panorama, through either an XML-based or representational state transfer (REST) API. The APIs allow organizations to use automation tools, applications, or scripts to manage the PAN-OS devices instead of the traditional GUI or CLI.

The PAN-OS XML API uses a tree of XML nodes to map firewall or Panorama functionality. Although the API is well documented, the firewalls and Panorama provide an API browser to allow you to explore the API interactively. The API browser lets you navigate and view the corresponding XPath and API URLs. You can also use the API browser along with the debug console to explore the underlying XML and XPath used when performing tasks in the GUI.

The PAN-OS REST API was added with the PAN-OS 9.0 release. The REST API provides access to firewall functions associated with managing objects and policies. It provides a URI scheme for representing resources and supports data formats of JSON and XML.

API access is secured through the out-of-band management interface, which provides role-based access control and requires an authentication key before granting access to the API. Use the PAN-OS XML API to automate tasks such as:

- Creating, updating, and modifying firewall and Panorama configurations.
- Executing operational mode commands, such as restart the system or validate configurations.
- Managing users through User-ID.
- Updating dynamic objects without having to modify or commit new configurations.

User-ID and Dynamic Address Groups

Because organizations define security policies based on application usage, a vital component of that policy is who should be able to use those applications. IP addresses are ineffective identifiers of the user or the role of the server with the dynamic nature of most networks. With the PAN-OS User-ID and dynamic address group features, organizations can automatically associate an IP address with a user or the role of a server in the data center. After they set these associations, organizations can define security policies that automatically adapt to changing environments.

User-ID agents derive user-to-IP mapping information from a variety of sources and inform the firewall via API calls. The User-ID agent provides out-of-the-box automation not only of user-to-IP mapping but also user-to-group mapping. When user-to-IP mapping information is stored in a source not directly supported by the agents, the User-ID XML API and Syslog listeners provide organizations a programmatic and customizable way to map users to IP addresses.

When tying IP addresses to specific users, User-ID gives only half the picture. Servers and many other devices cannot use a user to identify their security access requirements, but the roles and IP addresses of users can be just as dynamic as those of a workstation. Dynamic address groups allow organizations to create a policy that automatically adapts to device additions, moves, or deletions. They also enable the flexibility to apply a security policy to the device based on its role on the network.

A dynamic address group uses tags as a filtering criteria in order to determine its members. Tags can be defined statically or registered dynamically. The IP address and associated tags for a device can be dynamically registered on the firewall using the XML API or the VM Monitoring Agent on the firewall; each registered IP address can have multiple tags.

Because the members of a dynamic address group are automatically updated, organizations can use address groups to adapt to changes in their environment without relying on a system administrator to make policy changes and committing them.

Action-Oriented Log Forwarding

To integrate with IT infrastructure and workflows, the firewall can trigger an action or initiate a workflow on an external HTTP-based service based on log information.

- **Auto-tagging**— In response to a log event, the firewall tags the source or destination IP address in a log entry automatically and registers the IP address and tag mapping to a User-ID agent on the firewall or Panorama. Based on observed activity, auto tagging effectively allows the firewall to automatically associate IP addresses to a security policy rule through the use of dynamic address groups.
- **HTTP log forwarding**—Based on events in the firewall log, the firewall sends an HTTP-based API request directly to an external application or service to trigger an action. HTTP log forwarding works with any HTTP-based service that exposes an API and allows you to modify the URL, HTTP header, parameters, and the payload in the HTTP request to perform the integration. HTTP log forwarding allows you to automate workflows and tasks without relying on an external system to convert Syslog messages or SNMP traps to an HTTP request.

External Dynamic Lists

An *external dynamic list* (EDL) is a text file that is hosted on an external web server so that the firewall can import objects—IP addresses, URLs, domains—included in the list and enforce policy. To enforce policy on the entries included in the external dynamic list, organizations must reference the list in a supported policy rule or profile. As you modify the list, the firewall dynamically imports the list at the configured interval and enforces policy without the need to make a configuration change or a commit on the firewall. If the web server hosting the file is unreachable, the firewall will use the last successfully retrieved list for enforcing policy until the connection is restored, but only if the list is not secured with SSL.

Cortex XSOAR processes indicator feeds. You can use it to continuously retrieve indicators from external sources, process them, and produce new feeds that can be directly consumed by PA-Series and VM-Series firewalls. One use-case for Cortex XSOAR is generating feeds to be used on PAN-OS as EDLs. You can create EDLs to track the IP addresses, URLs and domains used by ransomware, known APT groups and active malware campaigns. You can also create EDLs to track the IPs and URLs used by SaaS applications, such as Microsoft Office 365.

WildFire

The WildFire API extends the malware-detection capabilities of WildFire through a RESTful XML-based API. Using the API, organizations can get file analyses from WildFire and query for details on the WildFire public cloud or the WF-500 appliance. Using the WildFire API, organizations can automate the submission of files and links to WildFire for analysis. They can also use the WildFire API through automation scripts or tools to query WildFire for verdicts, samples, and reports.

Prisma Cloud

Prisma Cloud helps organizations implement and maintain security within their public cloud environments. It provides security to public cloud environments and enable organizations to automate the management of cloud security so they can minimize the attack surface and protect their public cloud deployments.

Prisma Cloud is an API-driven cloud service that integrates well with DevOps and SecOps methodologies, as well as risk/compliance tools. The APIs enable security to be embedded into the cloud application development process without compromising agility. Prisma Cloud enables automated remediation to swiftly enforce policies as defined by the organization. Risks can be addressed promptly, and necessary changes can be made to configurations and settings without manual intervention, getting the environment back to a compliant state quickly.

Prisma SaaS

Prisma SaaS secures sanctioned software as a service applications. Without any configuration on endpoints, it provides complete visibility across all users, folders, and activity within a SaaS application, and it enables detailed analysis and analytics of application use to prevent data risk and compliance violations. Prisma SaaS is a cloud service that connects directly to sanctioned SaaS applications by using the SaaS application's API. More importantly, Prisma SaaS allows granular context-aware policy control within these SaaS applications in order to drive enforcement and quarantine users and data as soon as a violation occurs.

The auto-remediation feature in Prisma SaaS can be a valuable tool in resolving data-governance risks automatically. Use automatic remediation to address incidents across large numbers of assets that Prisma SaaS finds. You can configure automatic remediation actions including:

- **Quarantine**—If an asset poses an immediate threat to intellectual property or proprietary data, you can automatically move the compromised asset to a quarantine folder. Depending on the SaaS application, that quarantine folder can either be in the asset owner's root directory or a special admin quarantine folder that only admin users can access. When you quarantine an asset, a placeholder (tombstone) file replaces the original asset.
- **Change sharing**—You can automatically change sharing to remove public links from an asset. You have the option to remove either the direct link on the asset only or the links from parent folders that expose the asset due to inheritance. When Prisma SaaS changes sharing on an asset, it can send the asset owner a remediation digest email.
- **Notification**—Instead of automatically fixing the issue, you can send the asset owner a remediation digest email that describes what actions the owner can take to remediate the risk.

In additional to its auto-remediation capabilities, Prisma SaaS includes a public REST API that organizations can use to write API clients that integrate with Prisma SaaS and collect log events. Organizations can leverage the Prisma SaaS API to pull relevant information and correlate it with other data in order to assess security events.

AutoFocus

AutoFocus threat intelligence brings speed, consistency, and precision to threat investigation. AutoFocus gives you access to the samples and artifacts collected from WildFire malware analysis. AutoFocus combines automated analysis with human intelligence from the Palo Alto Networks Unit 42 threat research team, adding context and attribution to threats.

Although the primary interface for AutoFocus is through the web UI, the AutoFocus API provides access to most of the same information. The AutoFocus API aids in the automated retrieval of threat intelligence. This allows organizations to build custom tools that can mine log information and automatically assess for threats.

AUTOMATION TOOLS

There is a wide spectrum of tools available to facilitate automation in an enterprise today. At one end, building customized tools from scratch can provide full control and flexibility, but also requires time and developer knowledge. At the other end, purchasing an application can enable an organization to deliver specific capabilities with limited programming knowledge and tend to be more environmentally focused. In between are tools that provide varying levels of abstraction and can cater to a range of skills and requirements. The spectrum of tools includes:

- Python packages that simplify PAN-OS API access
- Custom support for configuration management and provisioning tools, such as Ansible and Terraform
- Security orchestration, automation and response (SOAR) with the Cortex XSOAR platform for coordinated incident response

These tools fall into two categories: tools built for specific environments and tools that work across environments.

Developer Automation Tools

When organizations want the most flexibility and functionality when creating automation for their environments, developer tools such as Python are ideal tools. Built-in capabilities within the language, combined with extensive libraries, provide a way to build both solutions to simple and complex problems. For organizations that prefer to build custom systems that integrate into the PAN-OS APIs, the following library packages are available:

- **Pan-Python**—Pan-python is a Python package for Palo Alto Networks' next-generation firewalls, WildFire, and AutoFocus. It provides a Python and command line interface to the PAN-OS, WildFire, and AutoFocus APIs.
- **Pandevice**—The Palo Alto Networks Device Framework (or *pandevice*) is a Python library for interacting with PAN-OS devices. Pandevice leverages pan-python but enhances it by providing easier connectivity, virtual system support, and high availability awareness, as well as the ability to find and handle specific exceptions.
- **Pango**—Pango is a Golang package for interacting with Palo Alto Networks devices (including PA-Series and VM-Series firewalls and Panorama).

Environment-Specific Automation Tools

Public cloud environments typically provide tools specific to their environments that allow organizations to define a cloud deployment based on a template, as well as monitor it after deployment. Although the templates might be written in a common file format like JSON or Python, they can only be used within the environment for which they are written. These tools are typically used to automate the deployment but not the configuration, response, or security assessment of the VM-Series and PA-Series firewalls. Example environment specific automation tools include:

- **AWS CloudFormation templates**—AWS CloudFormation Templates simplify provisioning and management on AWS. Organizations can create templates for the service or application architectures they want and have AWS CloudFormation use those templates for quick and reliable provisioning of the services or applications (called *stacks*).
- **Azure ARM templates**—ARM templates are the most efficient way to deploy repeatable and tested designs in Azure. Templates define resources and their dependencies in a JSON file. Azure does not process templates in a step-by-step order but does ensure that dependencies are complete before deploying a resource. For example, before firewall deployment, Azure ensures the existence of the required networks that separate private and public zones.
- **GCP Cloud Deployment Manager template**—This template is a separate file that is imported and used in a configuration. You can use as many templates as you want in a configuration, and Deployment Manager will recursively expand any imported templates to create your full configuration. Templates allow you to separate your configuration into different pieces that you can use and reuse across different deployments. Templates can be as generalized or specific as you need. With templates, you can also take advantage of features like template properties, environment variables, modules, and other template functionality to create dynamic configuration and template files.

Environment-Independent Automation Tools

A better option than environment-specific tools for most organizations as the choice for building out automation are environment-independent automation tools. Environment-independent automation tools are recommended because they not only provide organizations with a single tool that works across environments, but they also provide organizations with a method to configure, respond, and assess in addition to deployment. There are many industry standard automation tools available. Palo Alto Networks provides enhanced functionality for Terraform and Ansible.

Terraform

Terraform is an open-source tool that builds and deploys infrastructure without agents running on the resources. Terraform supports many public and private cloud environments. Terraform uses configuration files to describe the resources that an application requires and then determines what it needs to deploy or configure in the environment to reach the desired state. After execution, if changes are made to the configuration files, Terraform is able to determine what changed and modify only what is required in the existing environment to achieve the new state.

The Palo Alto Networks Terraform provider allows you to deploy and configure the Palo Alto Networks VM-Series and PA-Series firewalls, as well as Panorama.

Ansible

Ansible is an automation engine that enables the orchestration of complex tasks across multiple, diverse devices to facilitate end-to-end workflows. Ansible takes a declarative approach to enforce the desired state of endpoints by using a push model that does not require agents. Ansible uses YAML documents consisting of an ordered list of tasks, called *playbooks*, and identifies groupings of hosts on which to execute the tasks. Ansible provides a thin layer of abstraction to simplify command execution across a wide range of endpoints without having to learn a whole new language. Ansible is owned by Red Hat, Inc., and is offered as open source or with paid support models. You can operate Ansible using a CLI tool or an optional graphical user interface tool.

Palo Alto Networks has created a module for Ansible Galaxy that provides a custom role and the associated functions that allow access to Panorama and PAN-OS devices. You can use this module to run configuration and operational functions as tasks from Ansible playbooks. For example, you can create NAT rules or restart devices that uses PAN-OS XML API calls wrapped within the Ansible framework.

Cortex XSOAR

Cortex XSOAR is a SOAR solution that manages alerts, standardizes processes, and automates responses, giving your security teams more time to be more proactive and effective by eliminating multiple trivial manual tasks. Cortex XSOAR combats security challenges facing security operations with three main areas of focus: workflow automation, incident management, and collaboration. Cortex XSOAR helps security teams to reduce mean time to response, create consistent incident management processes, and increase team productivity.

Cortex XSOAR employs a visual playbook editor that provides a front-end for an automation engine that simplifies the implementation of security incident response workflows. There is native support for hundreds of products and thousands of actions, as well as facilities to extend for customized devices and workflows. In addition to the automation engine, the platform includes a built-in ticketing system, collaboration facilities, and automated report generation. The DBot feature provides a force multiplier for your security analysts by using machine learning to provide incident handling guidance that is derived from past analyst actions and historical information. Together, these features enable security analysts to be more productive by spending less time on routine tasks and allow them to focus their skills on the formidable challenges enterprises face today.

Use-Cases for Automation

DEPLOYMENT USE-CASES

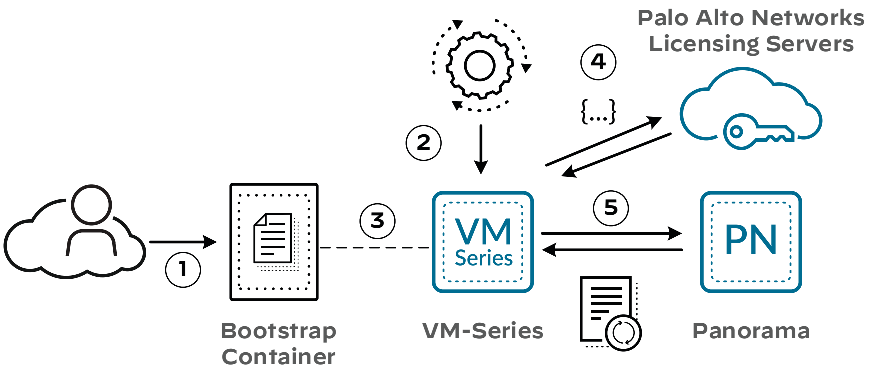
Deployment automation supports "Day 1" tasks for Palo Alto Networks platform elements such as bootstrapping and auto-scaling.

Bootstrapping VM-Series Firewalls

Whether you are deploying a VM-Series or a PA-Series next-generation firewall, bootstrapping provides a flexible, consistent, and scalable process for setting up a firewall. Bootstrapping not only speeds up the process of configuring and licensing the firewall but also makes it operational on the network. The bootstrapping process allows you to choose whether to configure the firewall with only a basic configuration so that it can connect to Panorama and obtain the complete configuration or to fully configure the firewall. Centralizing policy in Panorama is strongly recommended because it provides a central location for security administrators to define policy and ensure all firewalls have an up-to-date security posture. Keeping the firewall policy up-to-date can be challenging when you are statically configuring security policy in the bootstrap file. The bootstrapping process consists of the following:

1. The administrator creates a bootstrap container with the relevant configuration, auth code, content and software for the deployment. This needs to be done only once.
2. An automation task deploys the VM-Series firewall instance with an attached container.
3. The firewall initializes with the configuration defined in the bootstrap container and updates its software to the version defined in the bootstrap container as necessary.
4. The firewall registers the auth code defined in the container with the licensing servers, which return keys. The firewall then reboots. A single auth code can support multiple registrations.
5. After successful bootstrap, the firewall registers to Panorama. Panorama automatically pushes the appropriate security policy and objects to the firewall.

Figure 4 Firewall initialization with bootstrapping



Auto-Scale VM-Series Firewalls in a Public Cloud Environment

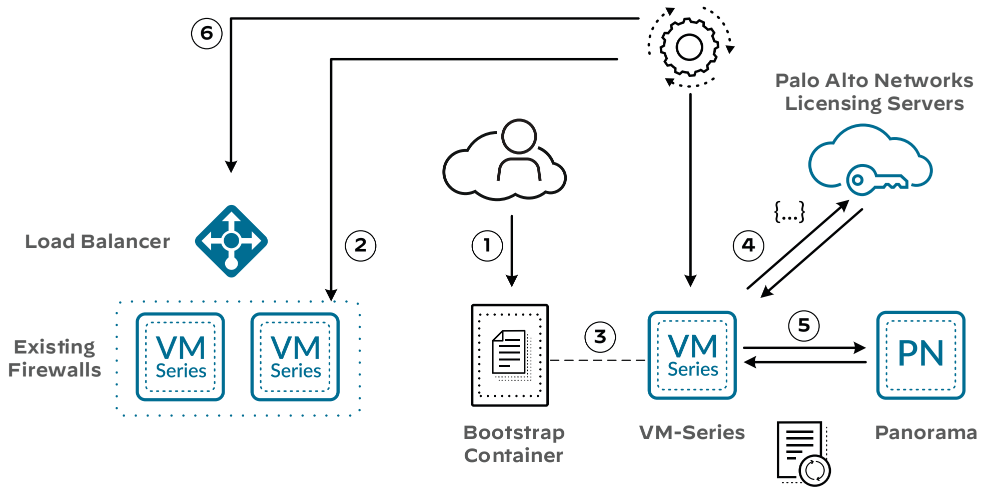
In the previous example, bootstrapping is manually executed as needed to deploy new environments and to manage scale. For environments that require an automatic deployment as scale out of the security services is required, you can combine bootstrapping with additional automation that monitors the security services and, when performance limits are reached, triggers the automatic deployment and bootstrap of a new firewall to the security layer.

Auto-scaling works differently in every environment because tools that are specific to each public cloud environment monitor and trigger the firewall deployment. Auto-scaling in AWS uses AWS services such as Lambda, Amazon CloudWatch, S3, and SNS, in addition to the APIs and bootstrapping on the firewalls. In Azure, you use AppInsights and Virtual Machine Scale Sets to monitor the environment and trigger the automatic deployment of a new firewall. You can use a number of metrics in order to trigger the auto-scale event. Examples include:

- Data Plane CPU Utilization %
- GP Gateway Utilization %
- Active Sessions
- Data Plane Packet Buffer Utilization %
- SSL Proxy Session Utilization %
- Session Utilization %

Just like in the previous example, you must create the bootstrap container before automatic scale-out. The automation monitors the appropriate metric on the existing firewalls, and after the value is higher than allowed for the right amount of time, the scale-out event triggers the same firewall deployment as in the previous example. After the firewall is deployed and has a configuration provided by Panorama, the auto-scale automation adds the new firewall to the backend pool of the load balancer, ensuring that traffic load is appropriately distributed to the new firewall.

Figure 5   Auto scale-out of VM-Series firewalls



CONFIGURATION USE-CASES

Configuration automation supports the day-to-day operation of the platforms. These use-cases focus on the create, read, update, and delete operations that are often performed manually.

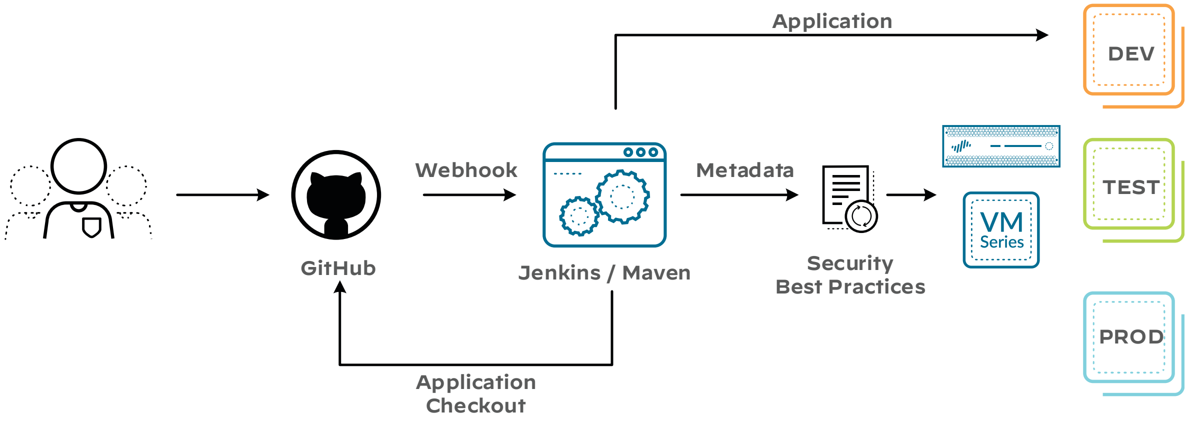
Automating Configuration Through a CI/CD Pipeline

When the speed of application deployment increases, many organizations struggle with ensuring the security team can adequately secure the application while not becoming a bottleneck in the application deployment. When the applications are dynamic, such as when an organization has adopted a CI/CD workflow, you can use automation to pull metadata that is part of the application development and use it to define a security policy for the application while providing control to the security administrators.

CI/CD workflows typically use configuration files to ensure the resources required by the application are built and available before deploying the application (for example, web servers' daemons running on specific TCP ports). Pipeline automation can take advantage of this metadata, combined with security best practices, to configure the firewall or Panorama with the security rules that use all of the capabilities of the next-generation firewall to protect the application. In this way, neither the application developer, nor the security administrators need to be involved in the deployment of the security policy for the application. Because the metadata doesn't have all the information required to build rules that properly secure the traffic—such as policy requirements around applications, malware, and vulnerability protections—the automation uses best practices and profiles built by the security team to build the appropriate policy around the metadata. This approach supports the concept of infrastructure-as-code (IaC), which treats server and network device configuration files like application source code by using version control systems and accessing devices programmatically instead of manually via the WebUI.

Modularizing the creation of the security policy provides the security administrators the ability to define the appropriate security posture for a service, such as web servers, but allows the automation pipeline the flexibility to define what IP addresses and ports on which those web servers are instantiated. Using metadata from the application development is very flexible. There are many ways that the CI/CD pipeline can use metadata to define the security policy beyond this use-case, such as defining policy based on if the application is being deployed in a development, test, or production environment.

Figure 6 CI/CD pipeline automation



RESPONSE USE-CASES

The following use-cases show automated configuration changes in response to specific operational or security events. These unplanned changes allow the firewalls to adapt to changes in the environment and threat landscape automatically.

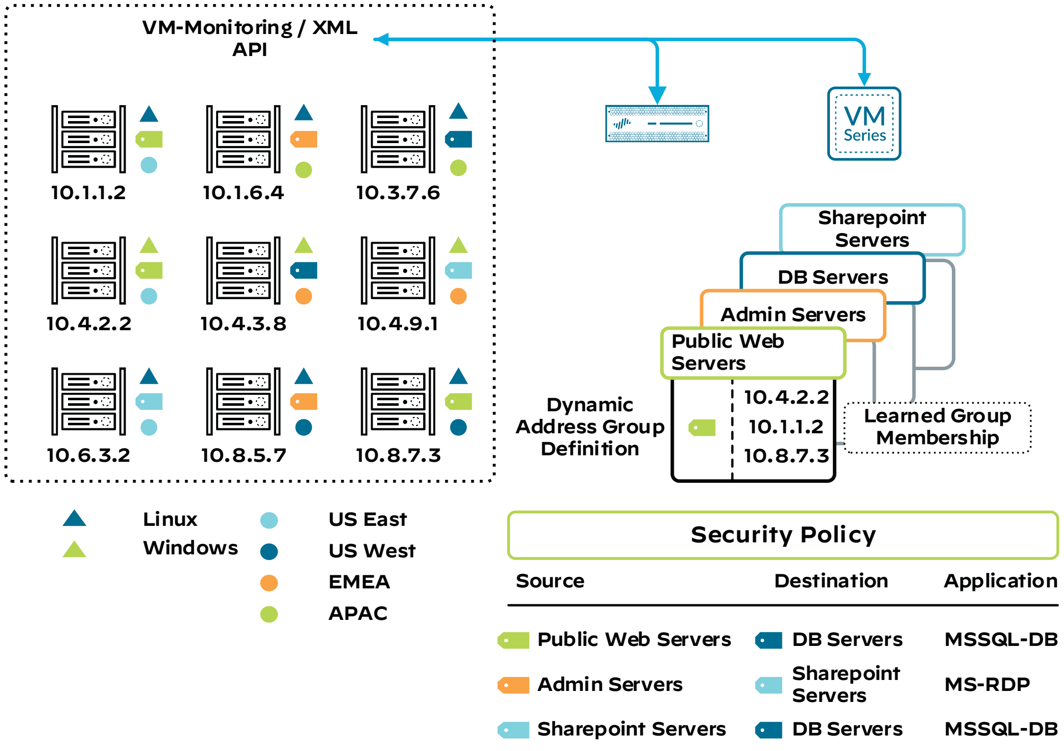
Operational Response to a Changing Environment

In virtual private data center and public cloud environments where new compute instances are created as needed for scale, the administrative overhead in managing security policy can be cumbersome. Using dynamic address groups in security policy allows for agility and prevents disruption in services or gaps in protection.

The VM-Monitoring Agent on the firewall can pull IP address and tag information from the cloud environment. Pre-defined dynamic address groups use the tag information to automatically associate IP addresses to pre-defined rules in the security policy. When there are multiple firewalls in the environment, they all can monitor the same source for IP and tag information. This provides the firewalls a dynamic but consistent view of the resources within the environment.

Dynamic address groups allow the firewall security policy to respond to a changing environment, but the applications running in the environment must be well known for the appropriate dynamic address groups and security policy rules to be created. Configuration automation can be used to provide a security policy that is automatically configured when new applications are deployed to the environment.

Figure 7 Operational response with dynamic address groups



Source	Destination	Application
Public Web Servers	DB Servers	MSSQL-DB
Admin Servers	Sharepoint Servers	MS-RDP
Sharepoint Servers	DB Servers	MSSQL-DB

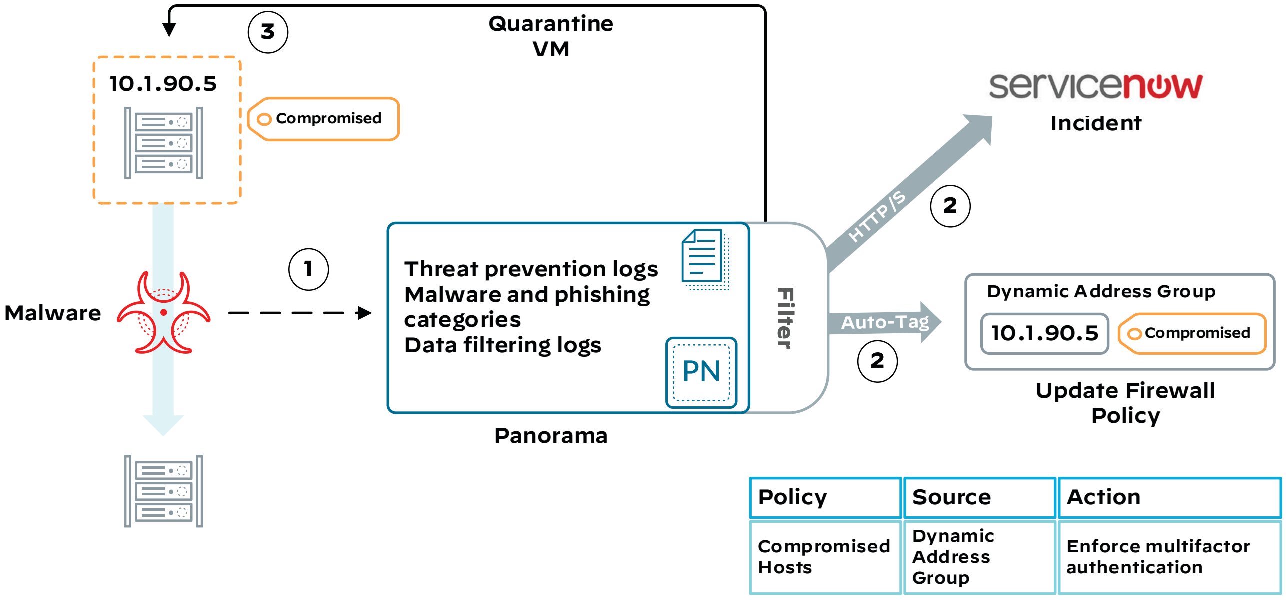
Security Response Based on Log Information

Although log information alone can be extremely valuable to a security administrator, manually sifting through the logs and responding to security events takes too long and requires too many administrative resources. Automated security actions in the firewall can respond when a previously identified scenario presents itself in the logs. For example, when Panorama sees a correlation event, it can use the source IP address from the log and use auto-tagging to attach a predefined tag, such as “Compromised.”

You can configure a dynamic address group on the firewall that is associated to the IP addresses with the “Compromised” tag. You can then create a security policy that blocks the traffic or enforces multi-factor authentication (MFA) for these endpoints that uses the dynamic address group as the source. If the user on the endpoint is malicious, MFA blocks their attempt to move laterally within the network, protecting sensitive data.

If the user continues to attempt to move laterally, Panorama can automatically use additional tags to block the IP and HTTP log forwarding to log an incident. Panorama can use the ServiceNow ticketing system HTTP API to create a ticket so that the operations team is aware of this action on the endpoint. They can then investigate the incident, remediate the endpoint if needed, and remove the associated tags the apply the enhanced security policy.

Figure 8 Automated security response



Policy	Source	Action
Compromised Hosts	Dynamic Address Group	Enforce multifactor authentication

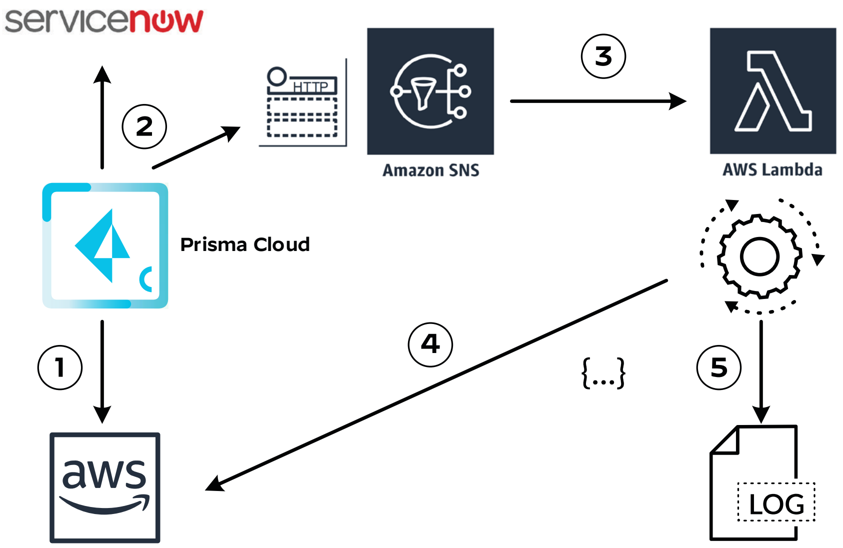
Security Response to Improper Cloud Environment Configuration

Prisma Cloud provides organizations configuration security alerting for AWS, Azure, and GCP environments and provides integrations that allow remediation to be automated. Using auto-remediation, organizations can make sure alerts are automatically remediated before they, or malicious actors, even know there's an issue. For example, reconfiguring a security group rule that allows ingress traffic from the public Internet and opening a ticket with ServiceNow for tracking minutes after it's been created.

Prisma Cloud uses the following automation process to remediate issues:

1. Using the cloud environment's API, continuously perform checks against the configured signatures and policies.
2. If the resulting analysis determines a signature did not pass, send the failed alert to an integration such as ServiceNow or AWS Simple Notification Service (SNS).
3. The AWS SNS service triggers the workflow automation and launches the AWS Lambda auto-remediation function.
4. Using the AWS API, auto-remediate and fix the offending issue.
5. Send the resulting logs to AWS CloudWatch.

Figure 9 Automation of public cloud remediation



ASSESS USE-CASES

Assessment automation retrieves, processes, and reports on security data. The data can be from a single source or correlated across multiple disparate systems. This type of automation makes no changes to the elements of Palo Alto Networks platforms but instead leverages the security data they store.

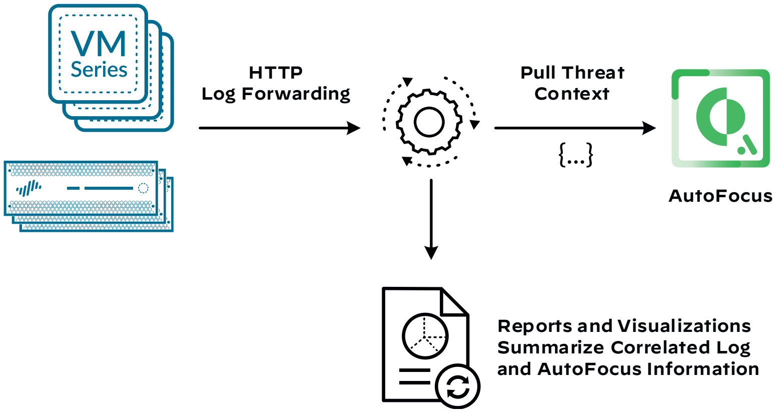
Classify and Visualize Threat and Traffic Information

Valuable information about traffic flows and threats is stored in logs, but manually sifting through the information and finding the interesting data, especially when there are a significant number of firewalls, can be time consuming and challenging. Automating the gathering and classification of the data allows organizations to explore the data in new ways. They can query data based on triggers seen in other systems, allowing organizations the ability to look back in time. They can also use automation on the data to create visualizations that allow the organizations to view, in near-real time, data about all the traffic that is passing through the firewalls.

In addition to gathering traffic and threat data from the firewalls, you can also query AutoFocus for additional context around IP addresses, domains, and URLs that the firewall observed and classified as malicious activity. AutoFocus provides context and attribution to threats based on the WildFire automated analysis, as well as additional detail from Unit 42.

Automating the process of classifying and visualizing log data from the security platform elements can help organizations generate actionable information that can be used to hunt threats in their organization.

Figure 10 Contextual automation



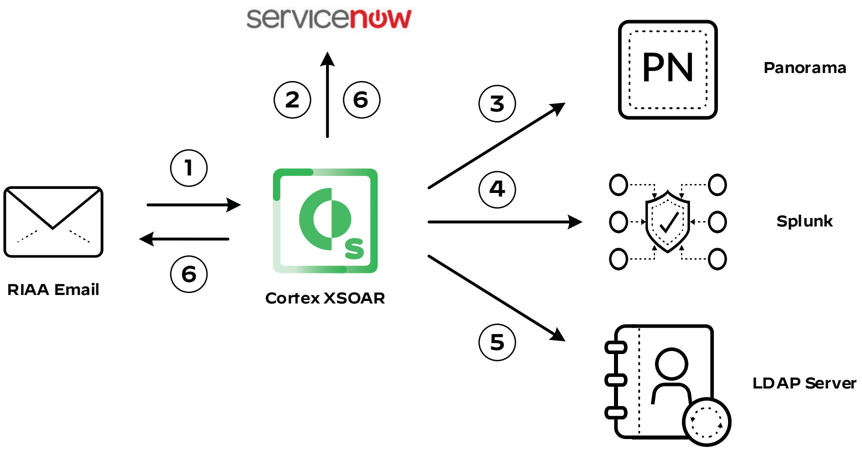
Automate a Search and Correlation Workflow

One of the responsibilities of the Recording Industry Association of America (RIAA) is to track the illegal downloading and sharing of copyrighted music. When it finds incidents of copyright infringement, such as peer-to-peer sharing of media files, RIAA sends a notice to the registered owner of the observed IP address. This type of activity is common on university campuses and IT staff at those institutions frequently receive email notices from RIAA. Traditionally, it was a manual and time-consuming process for administrators to determine the user associated with the offending IP address. Administrators had to search through and correlate logs from various systems, such as firewalls, DHCP servers, and authentication, authorization and accounting (AAA) servers. Cortex XSOAR can be used to orchestrate the automation of this workflow and free IT administrators to focus on less tedious tasks that fully utilize their extensive skills.

You can use Cortex XSOAR to automate the following steps in the search and correlation workflow:

1. RIAA sends an email to an address monitored by Cortex XSOAR (this event triggers the workflow).
2. Cortex XSOAR extracts the offending public IP address and date from the email and creates a ticket with the information.
3. Cortex XSOAR queries Panorama and obtains the private IP address that was mapped to the offending public IP on the specified date.
4. Cortex XSOAR queries Splunk to search the DHCP and AAA logs to find the username associated with the offending address on the specified date.
5. Cortex XSOAR checks the LDAP server to gather the contact details associated with the username.
6. If successful, Cortex XSOAR sends a response to RIAA with the user’s contact information, then logs the details and closes the ticket. If Cortex XSOAR is unable to obtain the user’s contact information, then it logs what it can to the ticket and sends it on for an IT administrator to investigate manually.

Figure 11 Automated search and correlation



Summary

Organizations can find significant value through automating tasks that are frequently executed, simple to perform, and error-prone. Automation is a very broad topic, but by breaking systems down into building blocks, you can build modular automation tasks that scale and are easy to reuse. Organizations that do not have automation teams can still benefit from using automated tools, features, and processes long before they get to the CI/CD stage.

Automation specific to the security layer focuses on four high-level use-cases: deployment, configuration, response, and assessment. The elements of the Palo Alto Networks platforms use built-in automation to identify malware and vulnerabilities and distribute protections to the platform elements. The elements of the platform also provide a variety of capabilities and features that allow organizations to build their own automation around tasks that they will find value in through efficiency.

The use-cases discussed in this guide are examples of how automation that leverages these capabilities and features can be used in an organization. These examples are not an all-encompassing list but instead a starting point for exploring how automation can be used.

RELATED RESOURCES

- PAN-OS Bootstrapper UI—Provides a simple web frontend for building all required files to bootstrap a Palo Alto Networks PAN-OS device. The output is an archive package, either ISO or ZIP, with all required files fully compiled from the supplied templates and input variables.
- Iron Skillet—Provides a repository of configuration templates that configure security on Palo Alto Networks next-generation firewalls in accordance with best practice recommendations. You can easily load these configuration snippets into a firewall or Panorama, minimizing configuration time and reducing errors.
- Safe Networking™—Using the Palo Alto Networks Threat Intelligence Cloud, as well as threat and traffic syslog events received from a Palo Alto Networks next-generation firewall, Safe Networking can correlate threat logs (DNS queries mainly) with malware known to be associated with the event.
- Palo Alto Networks Device Framework—Pandevice is a python library for interacting with next-generation firewalls, as well as Panorama.
- Public Cloud Integration Scripts and Templates—Templates that deploy and configure a combination of Palo Alto Networks and their respective cloud environment.
- Terraform and Ansible Introductory Lab—A hands-on lab covering the basics of interacting with PAN-OS devices using Terraform and Ansible.

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

HEADQUARTERS

Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054, USA
http://www.paloaltonetworks.com

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

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at http://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.

B-000109P-1-20a