
digitalscepter
FALCO
Automating Palo Alto Networks
Best Practices

# About Digital Scepter

- Security focused network integrator
- Palo Alto Networks experts since 2007
- Specialized in complex deployments
- Work with hundreds of districts, COEs, counties and more

# What We'll Cover

- Falco as a solution
- World-class support
- EDL Service
- Beyond the reports

# Pain Points for the managing firewalls

- Thousands of options and features
- Configuration drift
- Managing multiple firewalls adds complexity
- Requires dedicated firewall engineer
- Lack of institutional knowledge
- Existing tools fall short

# What is Falco?

- A tool to detect configuration issues
- A managed service to assist with fixing them

FALCO

FALCO

# Sample Falco Report

Falco Plus

Summary | Policies | Objects | Network | Device

Device: PA5250-1

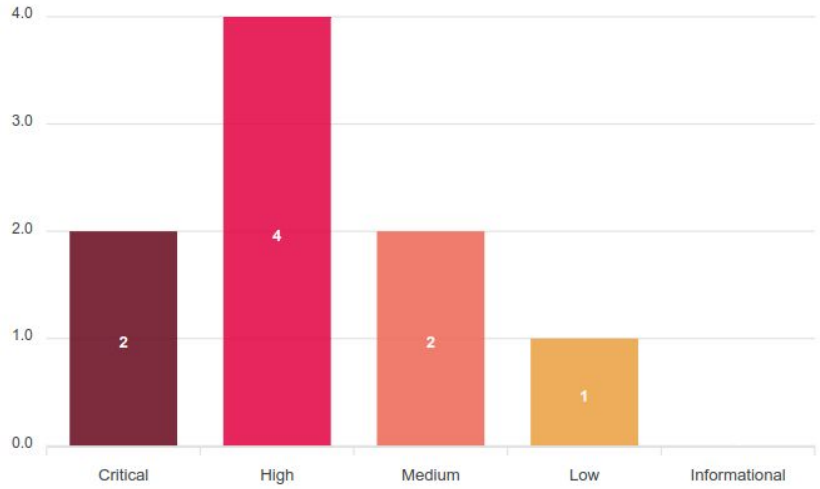
80% passed
1 Devices Audited

1/1 devices
Recommended Releases

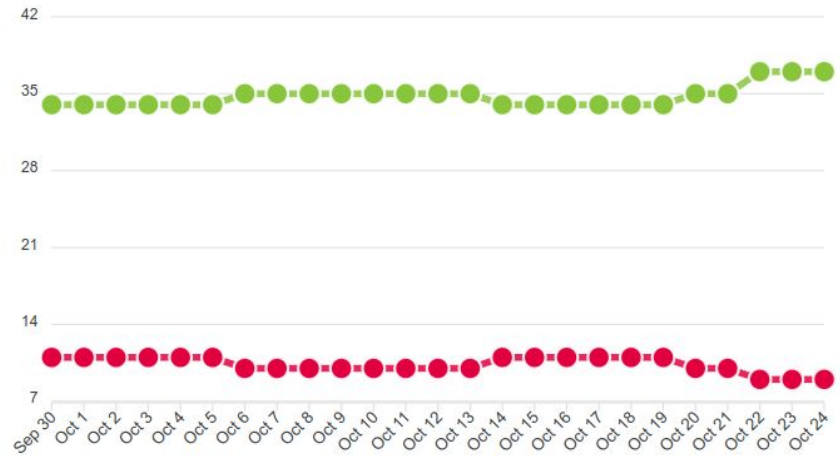
No Vulnerabilities
No Known Vulnerabilties Found

Support Licenses
All Devices Have Valid Support Licenses

## Failed Check Severity




## Report History



# How does Falco address these issues?

# Issue: Configuration Drift

- Loss of structure
- Partial config
- Large config makes reasoning difficult
- “I don’t know how it works but it does, so don’t touch it”
- Security concerns
- New features

# Solution: Automatic Configuration Monitoring

- Constant config audits
- Regression notifications
- Detailed explanations
- Remediation suggestions
- Progress tracking

FALCO

# Sample Falco Report

Falco Plus

Summary | Policies | Objects | Network | Device

Device: PA5250-1

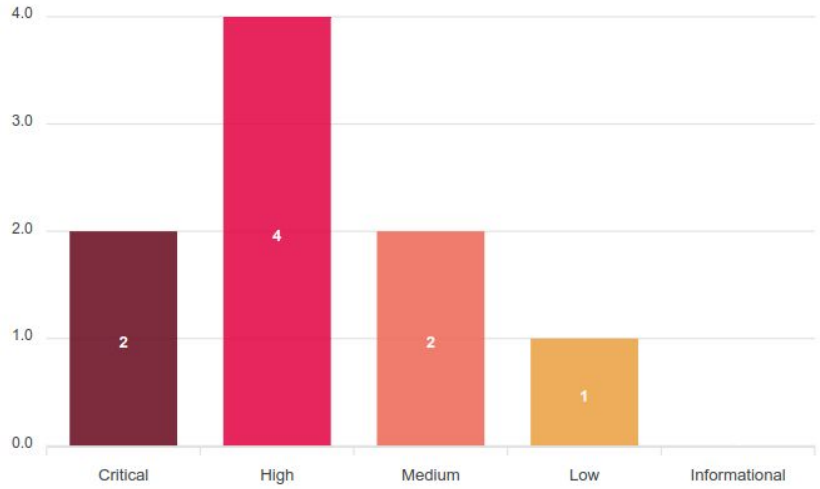
80% passed
1 Devices Audited

1/1 devices
Recommended Releases

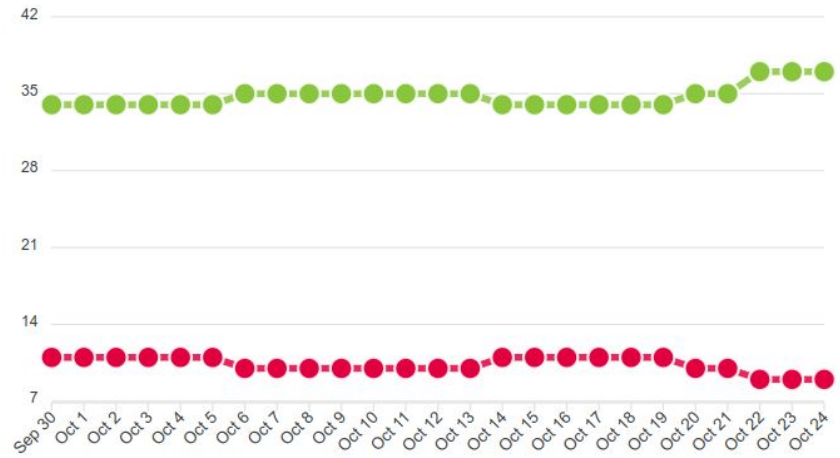
No Vulnerabilities
No Known Vulnerabilties Found

Support Licenses
All Devices Have Valid Support Licenses

## Failed Check Severity




## Report History



HIGH

## Security Rules That Allow SSH Without Log At Session Start

**Pass Rate** 60%

**Result**

Not all rules that allow SSH traffic are set to log at session start

**Description**

By default all security policies will create log entries when matching sessions end. This means that long running sessions may not be noticed since there will be no log messages until the session has ended, which may be days or weeks later. We recommend that all rules that allow SSH traffic have log at session start enabled.

**Remediation Steps**

Go to `Policies → Security` and edit the affected rules. On the `Actions` tab check log at session start.

| Rule | Action | Apps | Log at Session Start | Result |
|---|---|---|---|---|
| Example Rule #1 | Allow | panorama, ssh, ssl | ✗ | ✗ |
| Example Rule #2 | Allow | ssh, ssl | ✗ | ✗ |
| Example Rule #3 | Allow | ssh, ssl, web-browsing | ✗ | ✗ |

HIGH

## Secure Management SSH Service Profiles

**Pass Rate** 16%

**Result**

A suitable SSH management service profile was not found in use on this device.

**Description**

By default devices accept SSH supports all ciphers, key exchange algorithms, and message authentication codes, which can leave management SSH connections vulnerable to downgrade or brute force attacks. By configuring a management SSH Service Profile these attacks can be effectively mitigated. These profiles were added PAN-OS 10.0.

**Remediation Steps**

Create a suitable SSH management service profile under `Device → Certification Management → SSH Service Profile` and enable it under `Device → Setup → Management`. Here are the acceptable crypto settings, make sure that at least one of these is enable in each respective section:
Ciphers: aes256-gcm, aes128-gcm, aes256-ctr, aes192-ctr, aes128-ctr
MACs: hmac-sha2-512, hmac-sha2-256
KEX: ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256
Commit the changes, then restart the SSH service from the CLI using `set ssh service-restart mgmt` to start using the new profile.

**Documentation**

Configure an SSH Service Profile (10.0)
Mozilla OpenSSH Configuration Guidelines

HIGH

## Advanced URL Filtering Inline Machine Learning Models In Use

**Pass Rate** 14%

**Result**

Not all URL Filtering profiles have inline ML models enabled.

**Description**

Starting in PAN-OS 10.0 firewalls with an active Advanced URL Filtering license can enable in-line machine learning models that can categorize unknown URLs in real-time. In order to make full use of the Advanced URL Filtering license we recommend that both local and cloud inline categorization be enabled for all URL filtering profiles.

**Remediation Steps**

Go to `Objects → Security Profiles → URL Filtering` and enable the local and cloud inline categorization for each profile.

**Documentation**

Configure URL Filtering Inline ML (PAN-OS 10.1)

| URL Filtering Profile | Local Inline Categorization | Cloud Inline Categorization | Result |
|---|---|---|---|
| sample-profile | ✓ | ✗ | ✗ |

FALCO

**Regression Detected for Digital Scepter**

Generated 2022/11/18 03:42 PM

A recent audit of your devices detected a configuration regression. Here's the checks that failed:

# Device: prdpra01

## Expired Licenses

Critical

**Description:**

When a license expires the device loses the ability to retrieve updates for the content the license provided. The device will continue to function, but with an increasingly outdated content database as time goes on.

**Result:**

There are expired licenses

**Remediation:**

Contact DigitalScepter to renew the license and then click on `Retrieve license keys from license server` in `Device → Licenses → License Management` to retrieve the new licenses.

For licenses that don't need to be renewed, you can delete them from the CLI with the command: `delete license key`. You can use tab completion to find the file name.

For more information, open the attached interactive report with your browser.

# Keeping up with Vulnerabilities

# Palo Alto Networks Security Advisories

Search

Filter Clear

**version**

version

**severity**

- [ ] CRITICAL
- [ ] HIGH
- [ ] MEDIUM
- [ ] LOW
- [ ] NONE

**product**

- [ ] AutoFocus 3
- [ ] Bridgecrew 4
- [ ] Bridgecrew Checkov 2
- [ ] Cloud NGFW 5

26 - 50 of 223 < > Newest

| CVSS | Summary | Versions | Affected | Unaffected | Published | Updated |
|---|---|---|---|---|---|---|
| 7.5 N | CVE-2021-3053 PAN-OS: Exceptional Condition Denial-of-Service (DoS) | PAN-OS 10.1 | none | 10.1.* | 2021-09-08 | 2021-09-13 |
| | | PAN-OS 10.0 | < 10.0.5 | >= 10.0.5 | | |
| | | PAN-OS 9.1 | < 9.1.9 | >= 9.1.9 | | |
| | | PAN-OS 9.0 | < 9.0.14 | >= 9.0.14 | | |
| | | PAN-OS 8.1 | < 8.1.20 | >= 8.1.20 | | |
| 7.2 | CVE-2021-3054 PAN-OS: Unsigned Code Execution During Plugin Installation Race Condition Vulnerability | PAN-OS 10.1 | < 10.1.2 | >= 10.1.2 | 2021-09-08 | 2021-09-12 |
| | | PAN-OS 10.0 | < 10.0.7 | >= 10.0.7 | | |
| | | PAN-OS 9.1 | < 9.1.11 | >= 9.1.11 | | |
| | | PAN-OS 9.0 | < 9.0.14 | >= 9.0.14 | | |
| | | PAN-OS 8.1 | < 8.1.20 | >= 8.1.20 | | |
| 6.5 | CVE-2021-3055 PAN-OS: XML External Entity (XXE) Reference Vulnerability in the PAN-OS Web Interface | PAN-OS 10.1 | none | 10.1.* | 2021-09-08 | 2021-09-12 |
| | | PAN-OS 10.0 | < 10.0.6 | >= 10.0.6 | | |
| | | PAN-OS 9.1 | < 9.1.10 | >= 9.1.10 | | |
| | | PAN-OS 9.0 | < 9.0.14 | >= 9.0.14 | | |
| | | PAN-OS 8.1 | < 8.1.20 | >= 8.1.20 | | |
| 8.8 | CVE-2021-3050 PAN-OS: OS Command Injection Vulnerability in Web Interface | PAN-OS 10.1 | >= 10.1.0 | >= 10.1.2 | 2021-08-11 | 2021-08-11 |
| | | PAN-OS 10.0 | >= 10.0.0 | | | |
| | | PAN-OS 9.1 | >= 9.1.4 | | | |

https://security.paloaltonetworks.com

# Tracking vulnerabilities is just Another Check


## PAN-OS Vulnerabilities

Pass Rate 20%

**Result**
There are potential vulnerabilities that affect this device.

**Description**
This check uses the list of security notices published by Palo Alto Networks and cross-references it with the versions of your devices. Please note that this check shows potential vulnerabilities and it may have false positives or false negatives. This is a result of vulnerability data being automatically fetched from Palo Altos vuln database combined with the limited context provided in the database.

**Remediation Steps**
Typically in order to remediate the vulnerability, you will need to upgrade the device to a newer OS release. Some vulnerabilities will not have a fix available yet. For more information, see the link next to each vulnerability.

| CVE-ID | CVSS | TITLE | SEVERITY | DATE ISSUED | LINK |
|---|---|---|---|---|---|
| CVE-2022-0778 | 7.5 | Impact of the OpenSSL Infinite Loop Vulnerability CVE-2022-0778 | High | 2022-03-30 | link |
| CVE-2022-0028 | 8.6 | PAN-OS: Reflected Amplification Denial-of-Service (DoS) Vulnerability in URL Filtering | High | 2022-08-10 | link |

# Issue: Allowing Cloud Services is Hard

- Modern services are complex
- Vendors err on the insecure side
- You can’t trust DNS
- Managing IP lists is difficult
- Everything is dynamic now

# Example: Zoom

3.7.35.0/25
3.21.137.128/25
3.22.11.0/24
3.23.93.0/24
3.25.41.128/25
3.25.42.0/25
3.25.49.0/24
3.80.20.128/25
3.96.19.0/24
3.101.32.128/25
3.101.52.0/25
3.104.34.128/25
3.120.121.0/25
3.127.194.128/25
3.208.72.0/25
3.211.241.0/25
3.235.69.0/25
3.235.71.128/25
3.235.72.128/25
3.235.73.0/25
3.235.82.0/23
3.235.96.0/23
4.34.125.128/25
4.35.64.128/25
8.5.128.0/23
13.52.6.128/25
13.52.146.0/25
15.220.80.0/24
15.220.81.0/25
18.157.88.0/24
18.205.93.128/25
18.254.23.128/25
18.254.61.0/25
20.203.158.80/28
20.203.190.192/26
50.239.202.0/23
50.239.204.0/24
52.61.100.128/25
52.84.151.0/24
52.202.62.192/26
52.215.168.0/25
64.125.62.0/24
64.211.144.0/24
64.224.32.0/19
65.39.152.0/24
69.174.57.0/24
69.174.108.0/22
99.79.20.0/25
101.36.167.0/24
101.36.170.0/23
103.122.166.0/23
111.33.115.0/25
111.33.181.0/25
115.110.154.192/26
115.114.56.192/26
115.114.115.0/26
115.114.131.0/26
120.29.148.0/24
129.151.1.128/27
129.151.1.192/27
129.151.2.0/27
129.151.3.160/27
129.151.7.96/27
129.151.11.64/27
129.151.11.128/27
129.151.12.0/27
129.151.13.64/27
129.151.15.224/27
129.151.16.0/27
129.151.31.224/27
129.151.40.0/25
129.151.40.160/27
129.151.40.192/27
129.151.41.0/25
129.151.41.192/26
129.159.2.32/27
129.159.2.192/27
129.159.3.0/24
129.159.4.0/23
129.159.6.0/27
129.159.6.96/27
129.159.6.128/26
129.159.6.192/27
129.159.160.0/26
129.159.160.64/27
129.159.163.0/26
129.159.163.160/27
129.159.208.0/21
129.159.216.0/26
129.159.216.64/27
129.159.216.128/26
130.61.164.0/22
132.226.176.0/25
132.226.176.128/26
132.226.177.96/27
132.226.177.128/25
132.226.178.0/27
132.226.178.128/27
132.226.178.224/27
132.226.179.0/27
132.226.179.64/27
132.226.180.128/27
132.226.183.160/27
132.226.185.192/27
134.224.0.0/16
140.238.128.0/24
140.238.232.0/22
144.195.0.0/16
147.124.96.0/19
149.137.0.0/17
150.230.224.0/25
150.230.224.128/26
150.230.224.224/27
152.67.20.0/24
152.67.118.0/24
152.67.168.0/22
152.67.180.0/24
152.67.184.32/27
152.67.240.0/21
152.70.0.0/25
152.70.0.128/26
152.70.0.224/27
152.70.1.0/25
152.70.1.128/26
152.70.1.192/27

# External Dynamic Lists

Name: Sample EDL

**Create List** | List Entries And Exceptions

Type: IP List

Description:

Source: http://

**Server Authentication**

Certificate Profile: None

Check for updates: Every five minutes

Test Source URL | OK | Cancel

digitalscepter

# EDL Index

Search:

| List Name | Source | Entries | Bytes | Last Change | Tags |
|---|---|---|---|---|---|
| AzureServices-AzureCloud | AzureServices | 7000 | 115496 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AWS-IPv4 | AWS | 7362 | 93668 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AWS-AMAZON | AWS | 4680 | 73858 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| Zoom-CDN | Zoom | 3513 | 50544 | 11/17/2022 6:17:50 PM | voice meeting cdn |
| AzureServices-AzureMonitor | AzureServices | 1597 | 31538 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AzureServices-AppService | AzureServices | 1250 | 22270 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AWS-IPv6 | AWS | 1887 | 22261 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AzureServices-Sql | AzureServices | 1133 | 20717 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AzureServices-LogicApps | AzureServices | 1084 | 19484 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |
| AzureServices-CognitiveServicesManagement | AzureServices | 1099 | 19264 | 11/17/2022 6:18:02 PM | infrastructure public-cloud |

# You've Just Found a Misconfiguration, Now What?

- All checks include remediation steps
- Difficulty varies by check
- Issues require cross-functional fixes
- PAN TAC is break-fix only

# Tiers & Features

## Lite

*Our introductory tier available for free to all current CITE members.*

- Automated PAN Config Audits
- Panorama Support
- PAN-OS Vulnerability Scanning

Most Popular

## Standard

*All the reporting features, plus a support entitlement to fix any discovered issues.*

**Everything in the Lite tier plus:**

- Email Notifications for Config Regressions
- Per-VSYS Reporting
- 2 Tickets/Month Entitlement*
- Hourly Config Backups
- Scheduled Report Setup

## Enterprise

*A custom solution tailored to fit your needs. Our white-glove service.*

**Everything in the Standard tier plus:**

- Access to 160+ pre-built lists using our EDL Service
- Critical System Log Monitoring
- SSL Decryption Setup
- Customized Digital Scepter involvement with your team

* Open up to two tickets per month with Digital Scepter's support engineers (see terms and conditions). Can be used for remote threat support, PAN-OS upgrades, configuration assistance, support questions, User-ID, environment reviews, change reviews and more. Tickets are limited to four hours per ticket.

# Setup Process

# How to get your report

- Reach out to set up an appointment
- Simple connection via the API
- Uses a read-only account
- Takes less than 30 minutes

# What to expect in your first report?

- Expect to pass ~50%
- Checks show pass-rate
- Low hanging fruit
- 80-20 rule


Everything You Can Do
Everything You
Should Be Doing
Best
Practices


Q&A

# Thanks for Attending

sales@digitalscepter.com
(888) 299-3718

digitalscepter