digitalscepter

You Bought an NGFW—Now Use It:
Practical Security Patterns for Palo Alto Networks Firewalls

COLEMAN NUGENT - SYSTEMS ENGINEER
FEBRUARY 2026

About Digital Scepter

- Security focused network integrator
- Palo Alto Networks experts since 2007
- Specialized in Palo Alto Networks deployments
- Working with over 100 districts, COEs, cities and counties

digitalscepter

What We'll Cover: Four Main Patterns

- Write readable policies
- Let identity and device context drive policy enforcement
- Decrypt if possible
- Leverage the NGFW features you already have

Common Gaps in K-12

- Access is based on network location, not role
- Networks are flat or segmented only for infrastructure reasons
- Teams are wearing multiple hats, with no dedicated FW engineer
- Working configurations aren’t revisited periodically
- Visibility limited to North-South traffic only
- Minimal firewall feature utilization
- Very limited decryption rollout
- Configurations are fragile and hard to modify

How these gaps translate into real risk

- Attacks can come from any part of the network
- ACLs based on source IP make access control a network team responsibility
- Not every network segment is the same risk-wise
- Unused or legacy configuration further taxes your team
- All your external services use encryption, so do the attackers
- Your firewall config needs to keep up with new workflows

Making Policies Readable

Making Policy Readable: Why do it?

- Preventing “config drift” might be the hardest part of network security
- Security suffers once a rulebase can no longer be understood by one person
- Well structured rulebases are easier to understand and extend
- The structure of a firewall rulebase directly affects its behaviour

Making Policy Readable: What to Focus On?

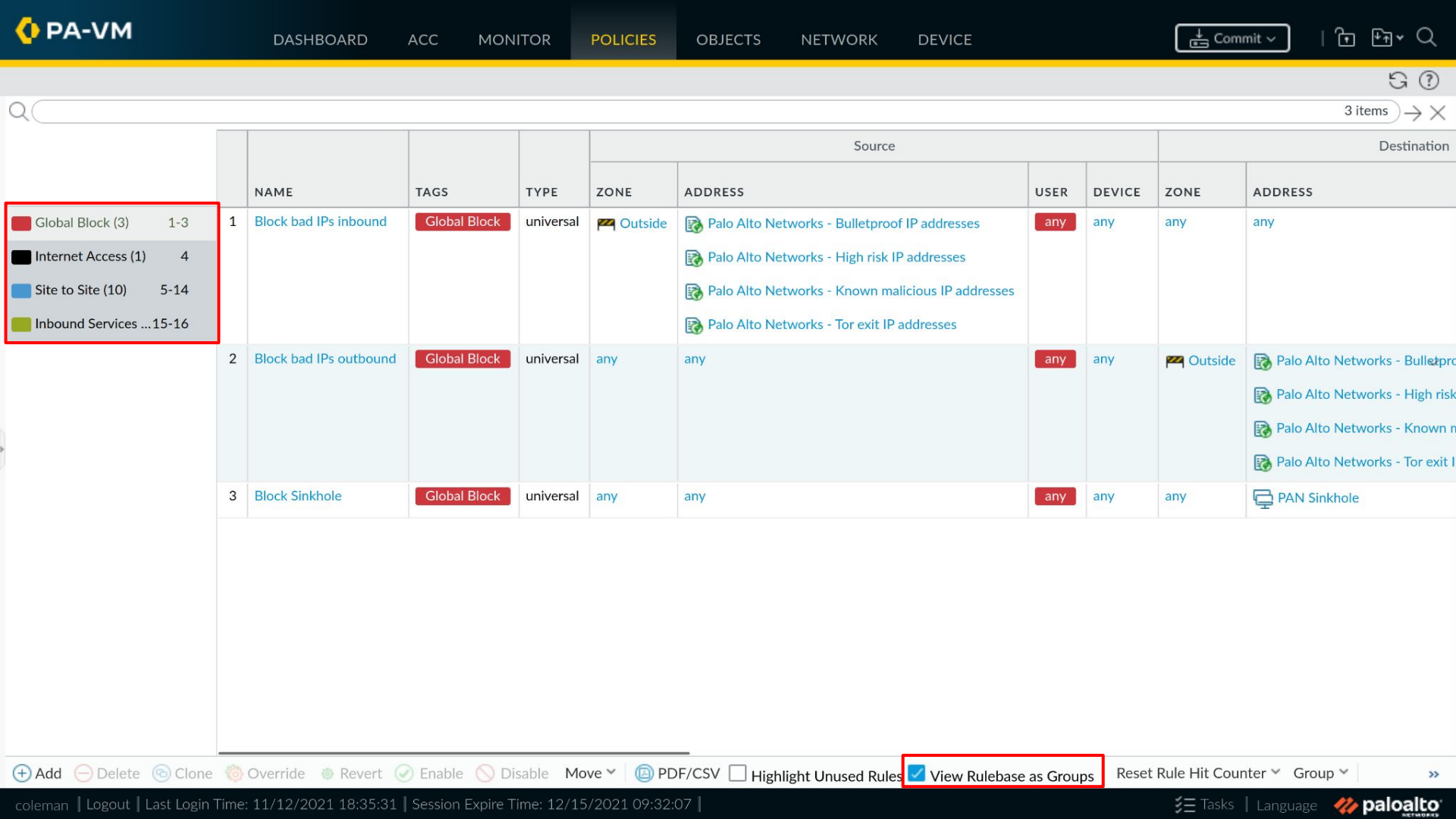
- Setup your network and zones to work with you
- Consistent naming conventions and good descriptions
- Turn common themes into explicit patterns
- Don’t repeat yourself
- Leverage User-ID to simplify rules
- Group similar rules into “sub-rulebases” and use *Group Rulebase by Tags*

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

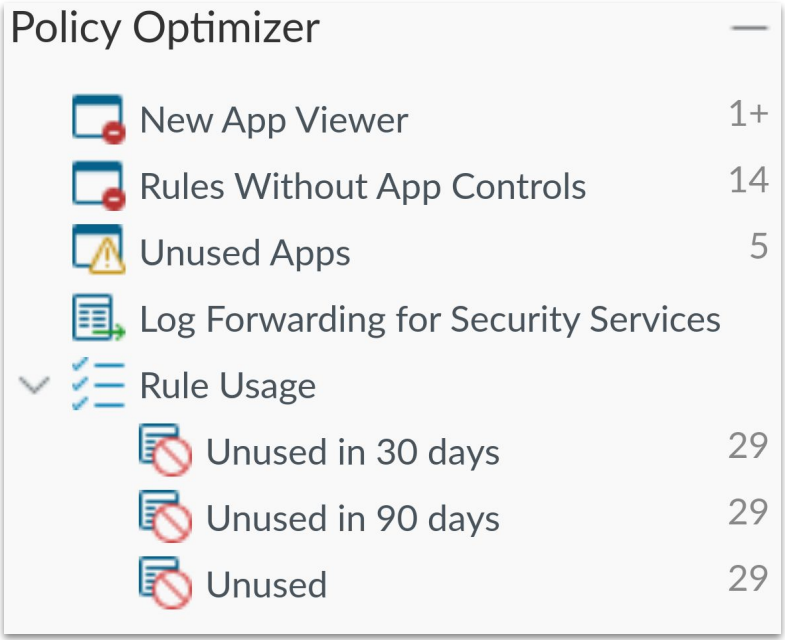
Name	Block Sinkhole
Rule Type	universal (default)
Description	
Tags	Global Block
Group Rules By Tag	Global Block
Audit Comment	

Audit Comment Archive


PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
Commit
3 items
Global Block (3) 1-3
Internet Access (1) 4
Site to Site (10) 5-14
Inbound Services ... 15-16
NAME
TAGS
TYPE
Source
ZONE
ADDRESS
USER
DEVICE
Destination
ZONE
ADDRESS
1 Block bad IPs inbound Global Block universal Outside Palo Alto Networks - Bulletproof IP addresses Palo Alto Networks - High risk IP addresses Palo Alto Networks - Known malicious IP addresses Palo Alto Networks - Tor exit IP addresses any any any any
2 Block bad IPs outbound Global Block universal any any any any Outside Palo Alto Networks - Bulletpro Palo Alto Networks - High risk Palo Alto Networks - Known n Palo Alto Networks - Tor exit I
3 Block Sinkhole Global Block universal any any any any any PAN Sinkhole
Add
Delete
Clone
Override
Revert
Enable
Disable
Move
PDF/CSV
Highlight Unused Rules
View Rulebase as Groups
Reset Rule Hit Counter
Group
coleman | Logout | Last Login Time: 11/12/2021 18:35:31 | Session Expire Time: 12/15/2021 09:32:07 |
Tasks
Language
paloalto

Leveraging the Policy Optimizer

- Located in the bottom left corner of the Policies Tab
- Available for most policy types, not just Security Policies
- Allow you to quickly adjust policies to match actual usage



Applications & Usage - Allow VPN to Internet

Timeframe: Anytime

Apps on Rule

- [x] Any
- [ ] APPLICATIONS

Browse | Add | Delete

Apps Seen 171

171 items

APPLICATIONS	SUBCATEGORY	RISK	FIRST SEEN	LAST SEEN	TRAFFIC (30 DAYS)
ssl	encrypted-tunnel	4	2024-04-22	2026-02-20	31.1G
ms-update	software-update	4	2024-04-22	2026-02-20	6.0G
gmail-base	email	1	2024-04-22	2026-02-20	5.9G
quic-base	infrastructure	1	2024-09-17	2026-02-20	2.6G
twitter-base	social-networking	1	2024-04-23	2026-02-01	973.6M
google-base	internet-utility	4	2024-04-22	2026-02-20	440.9M
web-browsing	internet-utility	4	2024-04-22	2026-02-20	406.5M
crowdstrike	management	2	2024-04-22	2026-02-20	343.5M

Create Cloned Rule | Add to This Rule | Add to Existing Rule | Match Usage

The last new app was discovered **11 days ago.**

Segmentation: What do we mean?

- Process of dividing the network into different zones for security or administrative purposes
- Can be done at multiple levels: physical, VLAN, subnet, VRF, etc.
- PAN takes a more agnostic approach: **zones**

INTERFACE	IP ADDRESS	TAG	SECURITY ZONE	FEATURES
Aggregate Group				
ae1	none	Untagged	none	
ae1.2	10.1.2.1/24	2	management	
ae1.130	10.1.130.1/24	130	domain	
ae1.131	10.1.131.1/24	131	application	
ae1.133	10.1.133.1/24	133	dmz	
ae1.134	10.1.134.1/24	134	test	
ae1.175	10.1.175.1/24	175	dev	
ae1.254	199.255.27.68/28	254	outside	
ae1.911	10.252.1.1/29	911	inside	
ae1.912	10.252.1.9/30	912	sdwan	
ae1.1500	10.1.150.1/29	1500	accounting	
ae1.1640	10.1.64.1/29	1640	database	
ae1.1641	10.1.64.9/29	1641	database	
ae1.1642	10.1.64.17/29	1642	terminal	
ae1.1643	10.1.64.25/29	1643	docker	
ae1.1644	10.1.64.33/29	1644	devops	
ae1.1645	10.1.64.41/29	1645	rapid7	
ae1.1646	10.1.64.49/29	1646	demolition	
ae1.1647	10.1.64.57/29	1647	iblox	
ae1.1648	10.1.64.65/29	1648	cisco-lab	

Segmentation: How to draw the line?

- Goal is to group network resources to make protecting them easier
- Functional roles tend to work better than network location
- Each zone should be as specific as possible without causing too much overhead
- Talking through your major traffic flows at a high level is a good place to start

INTERFACE	IP ADDRESS	TAG	SECURITY ZONE	FEATURES
Aggregate Group				
ae1	none	Untagged	none	
ae1.2	10.1.2.1/24	2	management	
ae1.130	10.1.130.1/24	130	domain	
ae1.131	10.1.131.1/24	131	application	
ae1.133	10.1.133.1/24	133	dmz	
ae1.134	10.1.134.1/24	134	test	
ae1.175	10.1.175.1/24	175	dev	
ae1.254	199.255.27.68/28	254	outside	
ae1.911	10.252.1.1/29	911	inside	
ae1.912	10.252.1.9/30	912	sdwan	
ae1.1500	10.1.150.1/29	1500	accounting	
ae1.1640	10.1.64.1/29	1640	database	
ae1.1641	10.1.64.9/29	1641	database	
ae1.1642	10.1.64.17/29	1642	terminal	
ae1.1643	10.1.64.25/29	1643	docker	
ae1.1644	10.1.64.33/29	1644	devops	
ae1.1645	10.1.64.41/29	1645	rapid7	
ae1.1646	10.1.64.49/29	1646	demolition	
ae1.1647	10.1.64.57/29	1647	iblox	
ae1.1648	10.1.64.65/29	1648	cisco-lab	

Policy Best Practices

- Good policies should read like English
- Leverage App-ID, User-ID, HIP profiles and specific zones
- Every allow rule should have a Security Profile Group
- Use the Policy Optimizer
- Make use of inline ML
- Use dynamic objects (EDLs, address groups, app filters, etc.)
- Remove unused rules

Leveraging Identity & Device Context

Leveraging User-ID: Background

- UID information is a list of IP → User mappings
- Can be used for policies, QoS, Decryption, PBF, etc.
- Multiple IPs can point to the same user
- All entries have a timeout
- New mappings overwrite existing mappings

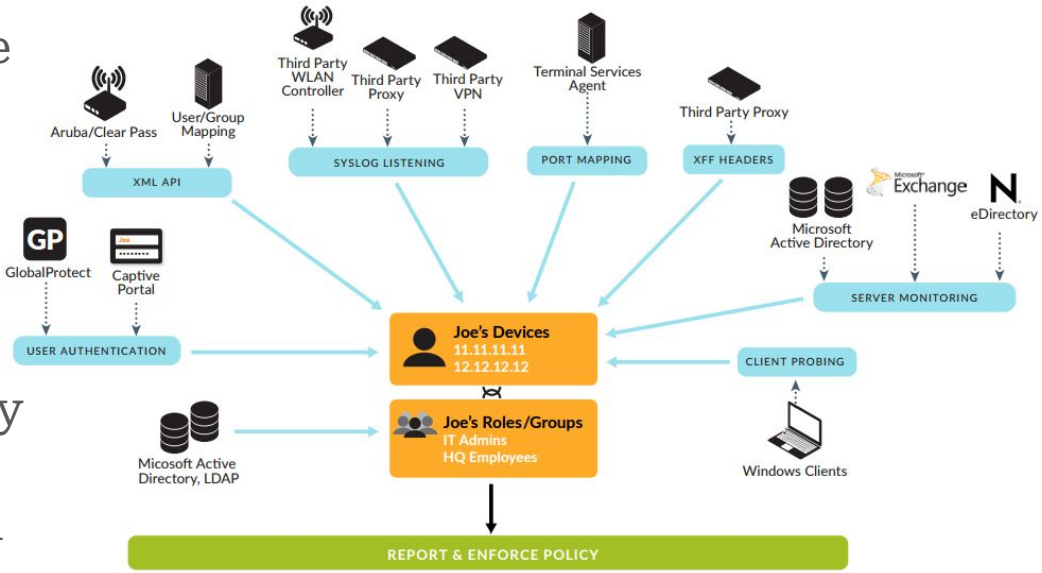
IP	User	Timeout
192.168.0.1	ds\coleman	2700
10.0.0.1	ds\zach	256
172.16.0.1	ds\jon	65535

Leveraging User-ID: Why do it?

- Role Based Access Control > Network Based Access Control
- Write network location agnostic rules
- Tightly couples security policies to directory information
- Moves access control burden off network team
- Enhance logs with usernames

Getting Reliable User-ID Mappings

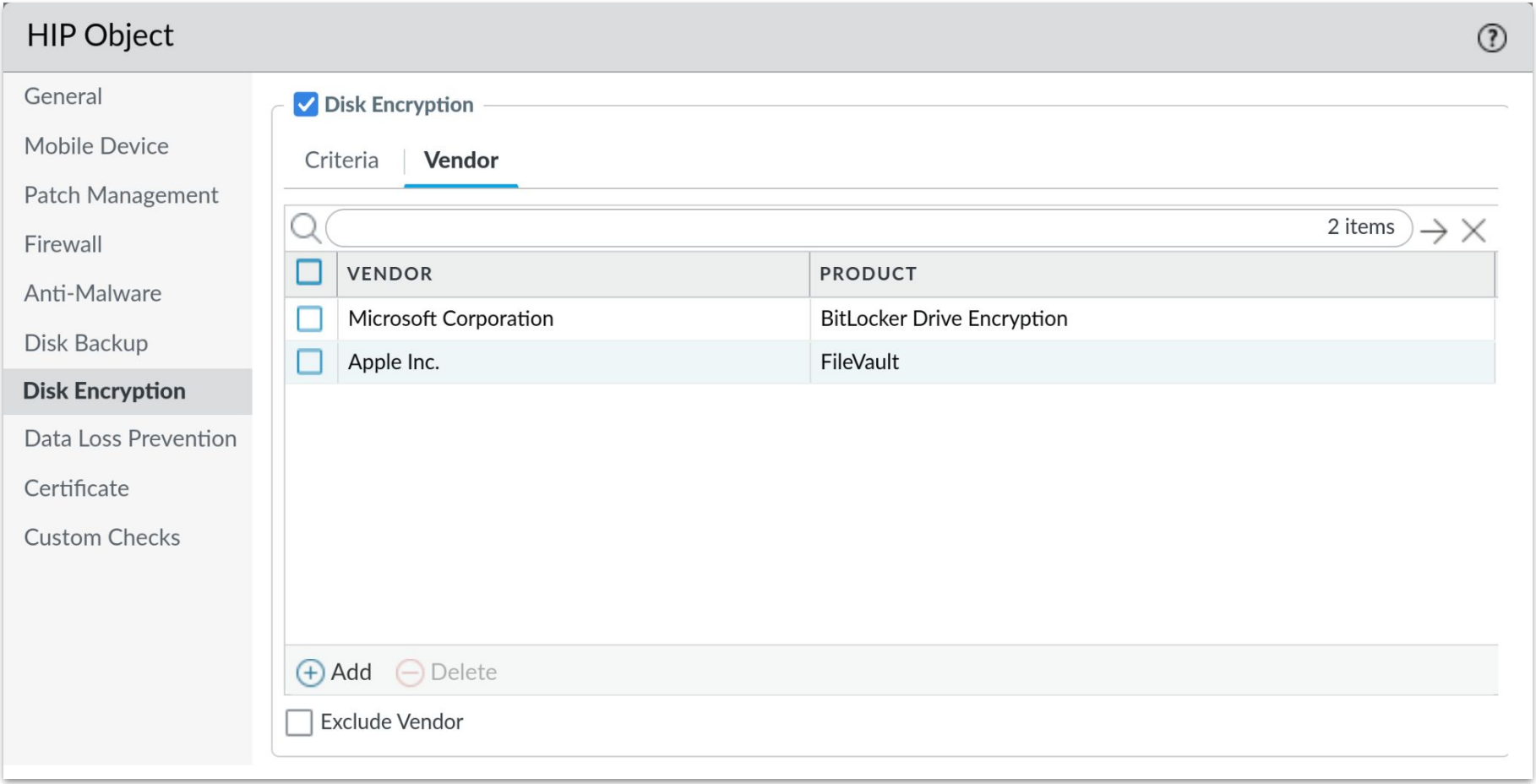
- Use as many sources as possible
  - GlobalProtect VPN
  - AD Domain Controllers
  - Wireless Controllers
  - Captive Portal
  - Syslog
  - XML API
  - Other 3rd party integrations
- Design your sources to be highly available
- Ensure that all firewalls have all mappings

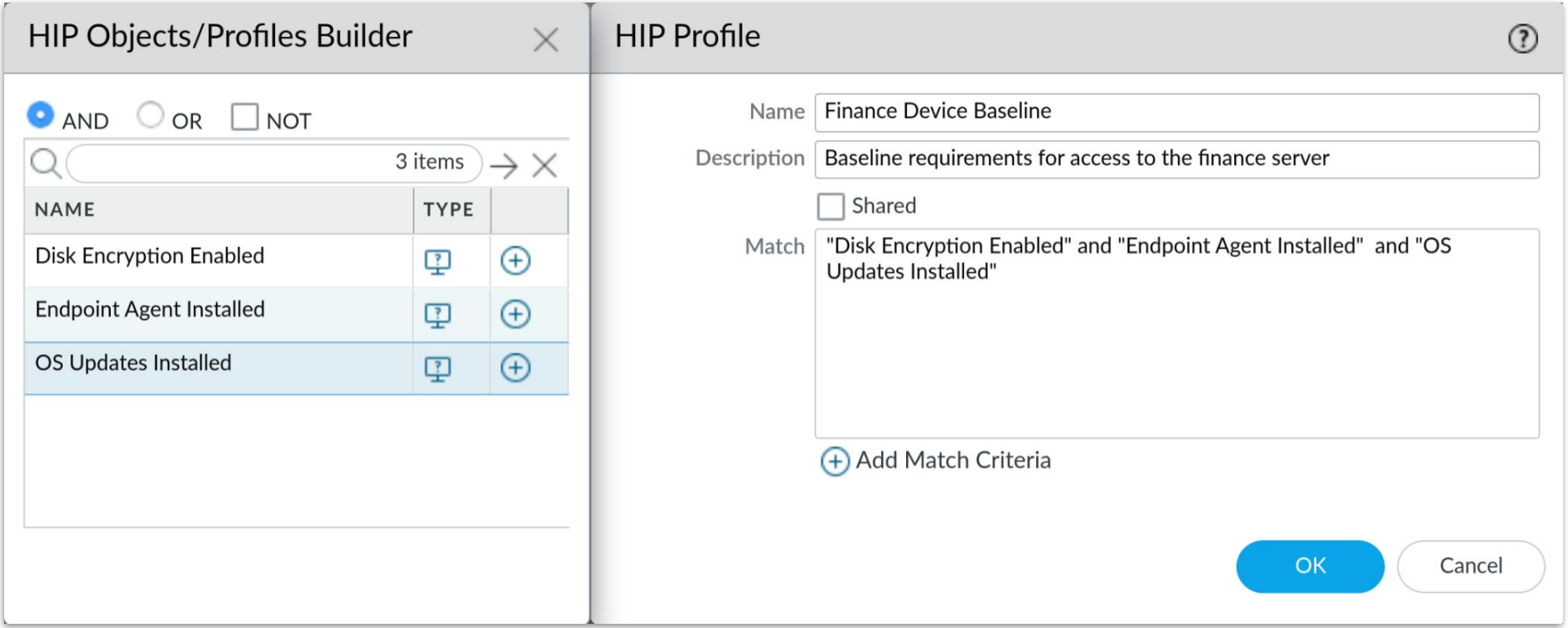


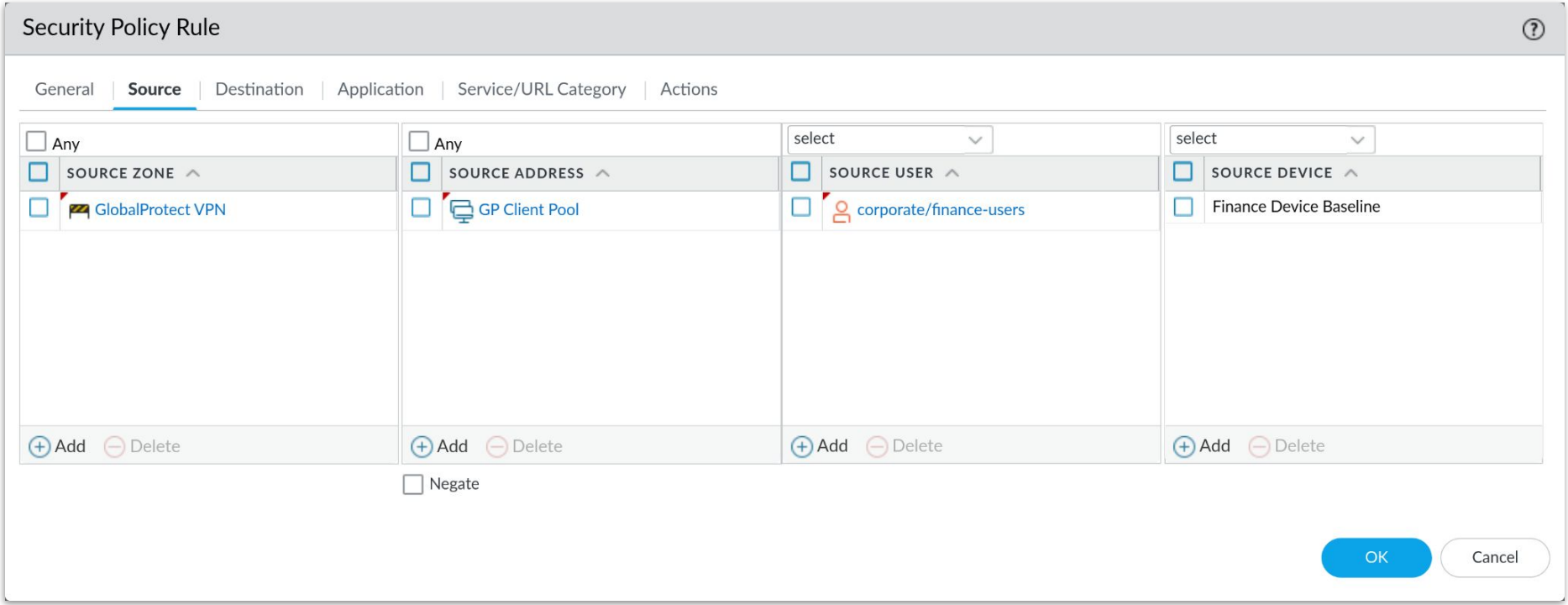
digitalscepter

HIP Checks: Overview

- HIP: Host Information Profile
- HIP data is gathered by the GlobalProtect client
- Provides additional match criteria for rules
- HIP Objects specify match conditions for HIP data
- HIP Objects can be combined into HIP Profiles
- HIP requires the GlobalProtect license







Regaining Visibility with Decrypt

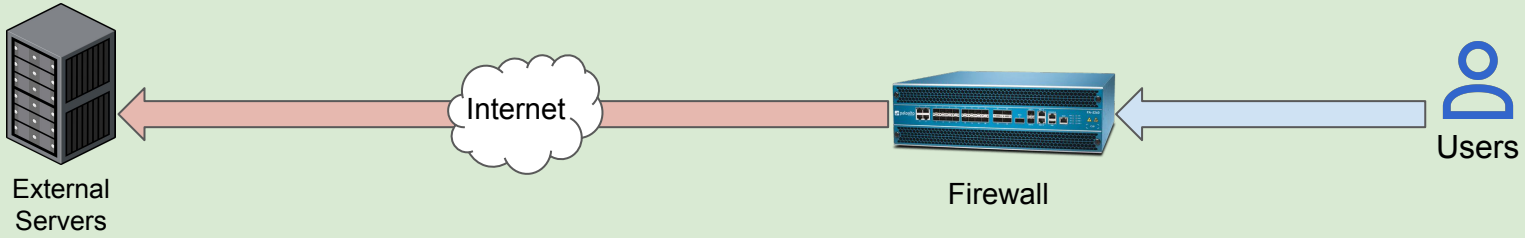
What the firewall sees *without* decryption

What the firewall sees *with* decryption

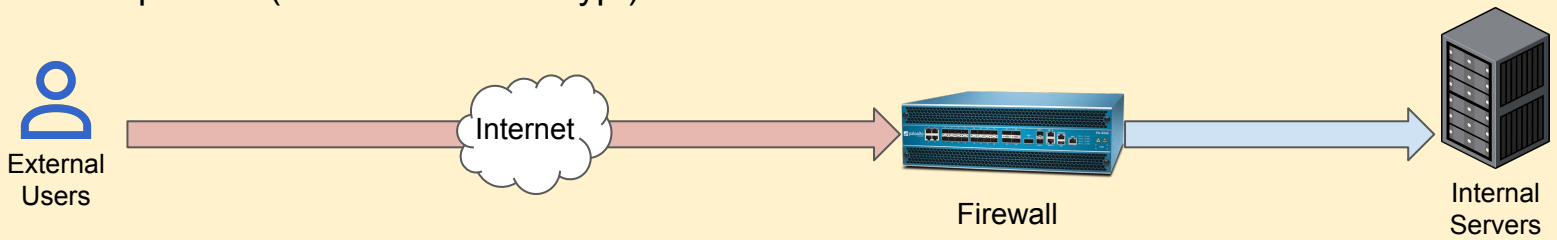
GET /classes/details?id=CS101; DROP TABLE STUDENTS HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:146.0) Gecko/20100101 Firefox/146.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
HTTP/1.1 200 OK
Content-Encoding: gzip
Accept-Ranges: bytes
Age: 460608
Cache-Control: max-age=604800
Content-Type: text/html; charset=UTF-8
Date: Mon, 21 Jan 2026 23:54:11 GMT

TLS Decryption: Overview

Forward Proxy (what most people mean when they say decrypt)



Inbound Inspection (aka. inbound decrypt)

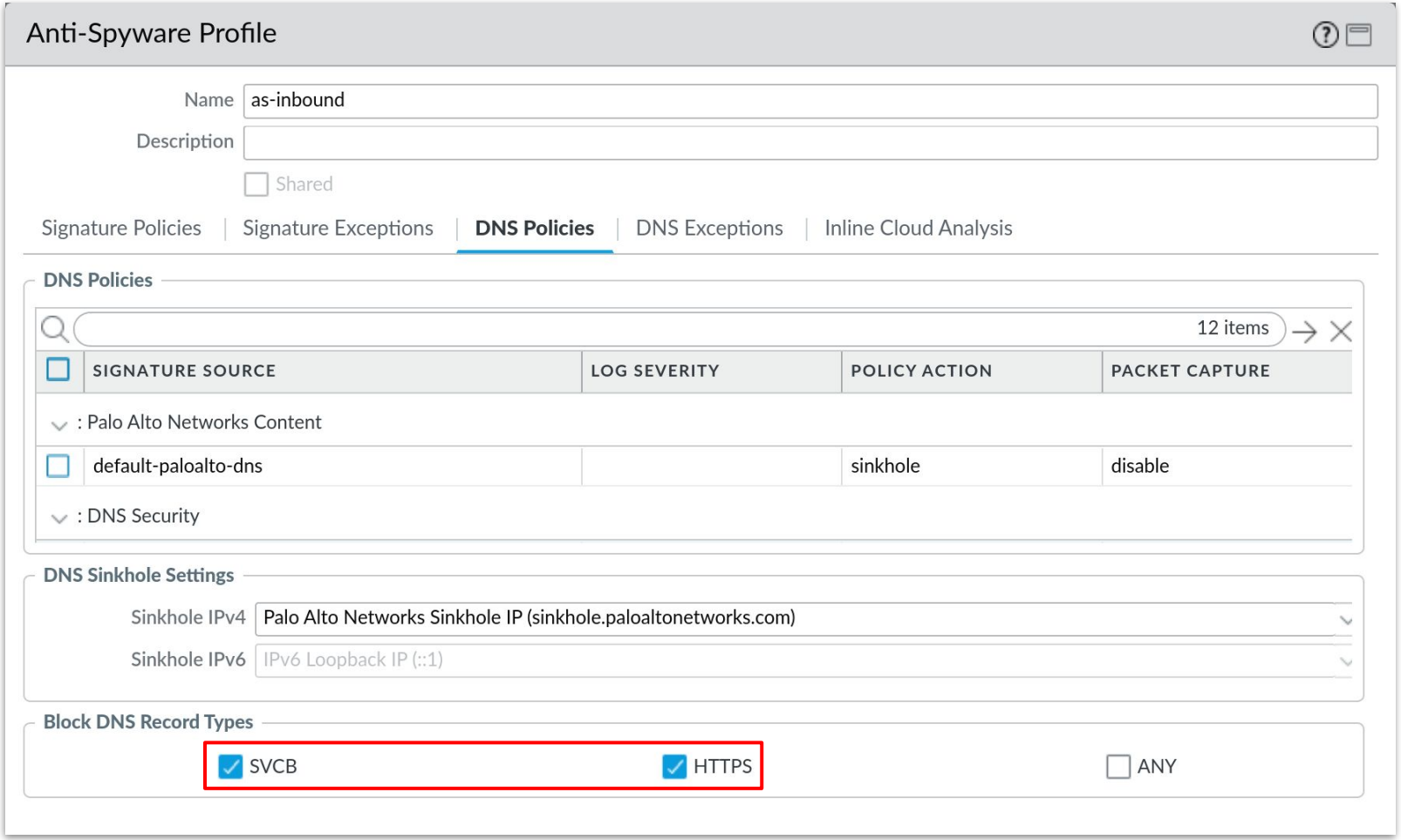


DoH, DoT, DoQ, QUIC, ECH, oh my!

- **These protocols affect our ability to filter DNS and HTTP traffic**
- DoH: DNS over HTTPS
- DoT: DNS over TLS
- DoQ: DNS over QUIC
- QUIC: Google's secure alternative to TCP, built on UDP
  - Allows for 0-RTT session resumption with preexisting ephemeral keys
- ECH: Encrypted Client Hello
  - Allows clients to encrypt the entire ClientHello message
  - Client must securely retrieve server's ECH public keys over DNS first

Dealing with DoH, DoT, DoQ, QUIC, & ECH

- Disable in managed browsers
- Enforce that your users use your DNS servers
- You can decrypt DoH in PAN-OS >= 11.0
- Block all other outbound DNS on the firewall
- Block QUIC on the firewall (with exceptions for performance)
- Block the DNS requirements for ECH
  - Filter SVCB and HTTPS DNS record types on your DNS servers
  - Can block these record types on FW, but may cause latency



Credential Theft Detection

- Firewalls can inspect traffic looking for valid credentials in data streams
- Enables the firewall to block phishing attacks even if the user is fooled
- Utilizes a bloom filter so neither creds nor hashes are known to the firewall
- Requirements
  - Decryption
  - User-ID entry for the user
  - User-ID agent running on Server 2016 RODC with password replication enabled
- Configurable per-URL category on the URL Filtering Profile
- Can be configured to look for just usernames

URL Filtering Profile

Name: ds_standard

Description:

Shared

Disable override

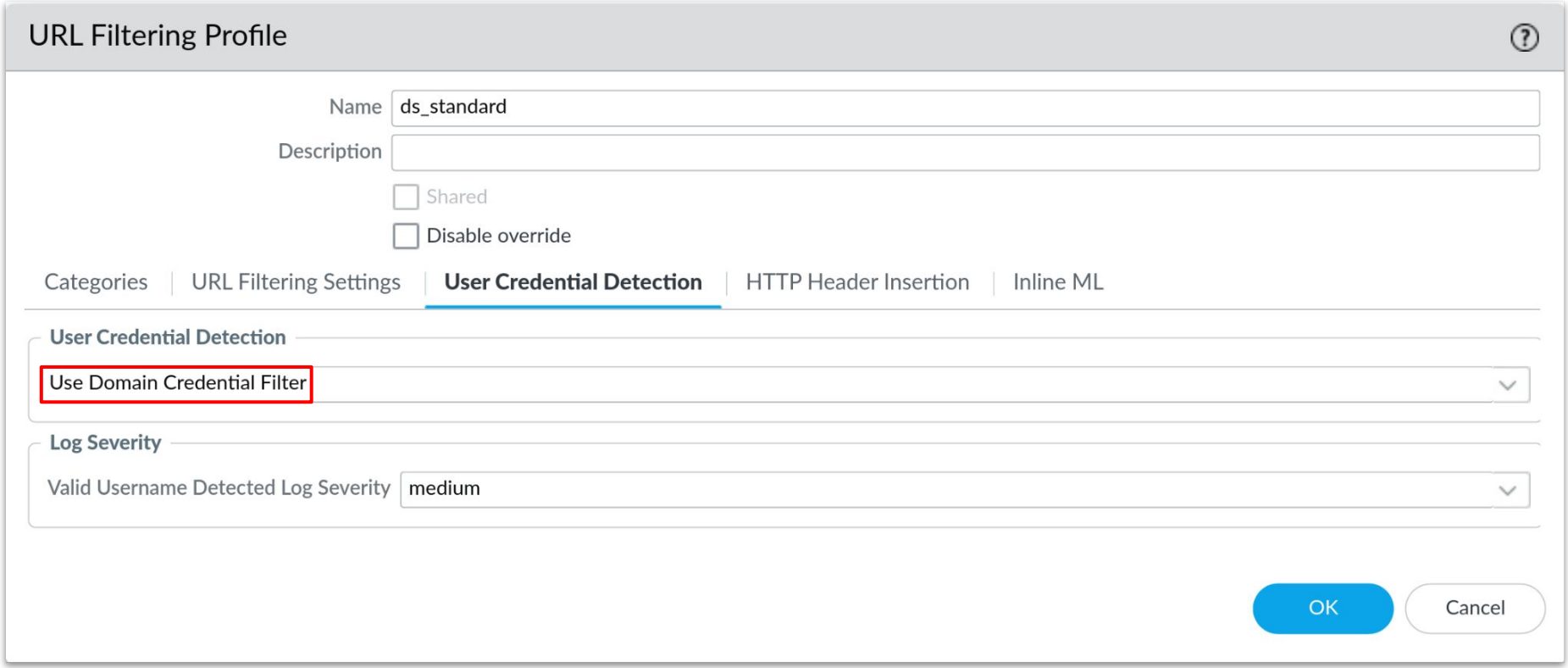
Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

dynamic — 88 items

CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
adult	block	block
alcohol-and-tobacco	alert	block
auctions	alert	block
business-and-economy	alert	block
command-and-control	block	block
computer-and-internet-info	alert	block
content-delivery-networks	alert	block
copyright-infringement	block	block

* indicates a custom URL category, + indicates external dynamic list

Check URL Category



Suspected Credential Phishing Detected

Username and/or password submission to the page you are trying to access has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: ds\cnugent

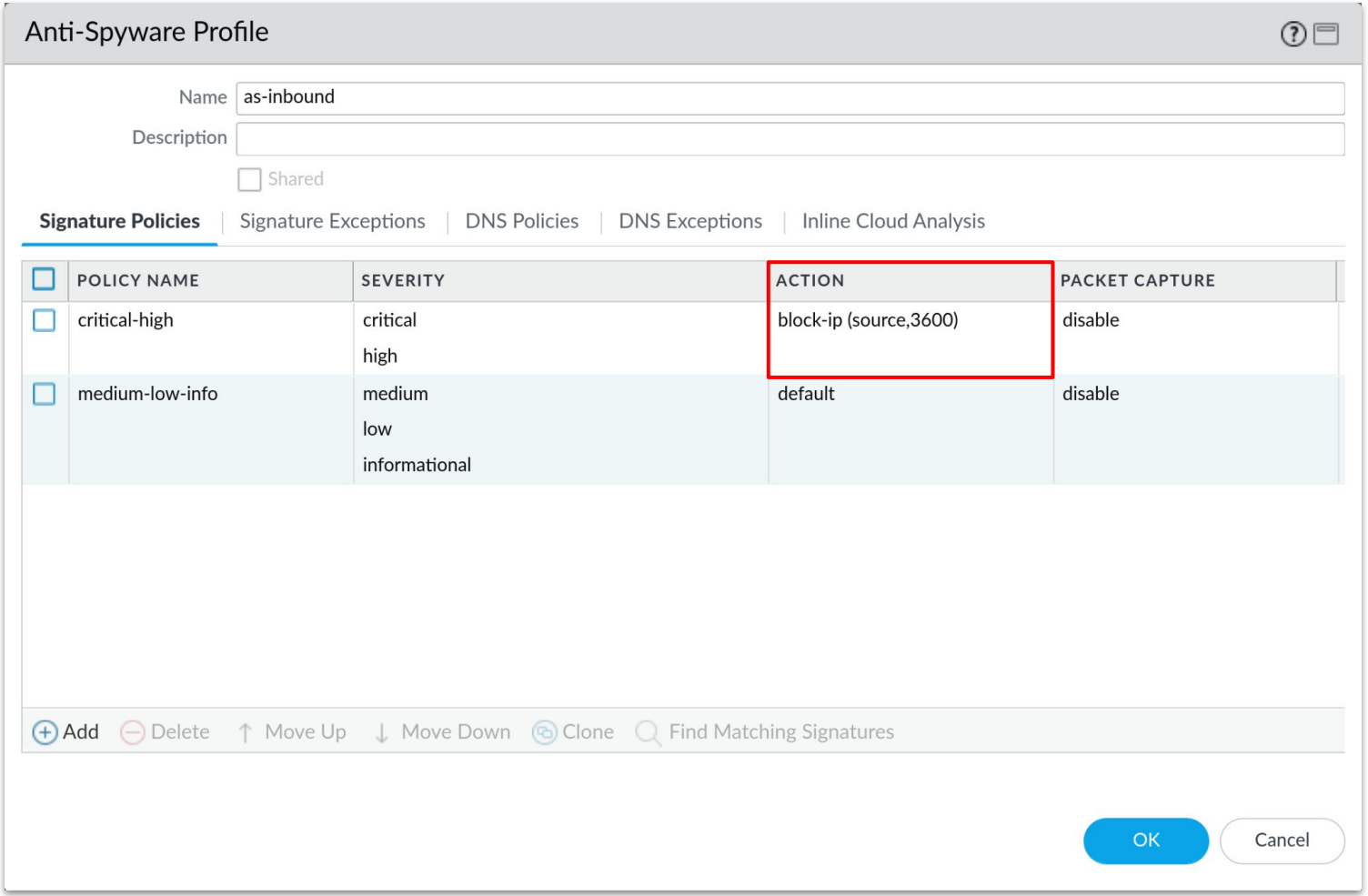
URL:
slowshinysilvermelody.neverssl.com/online?username=admin%26password=nicetry

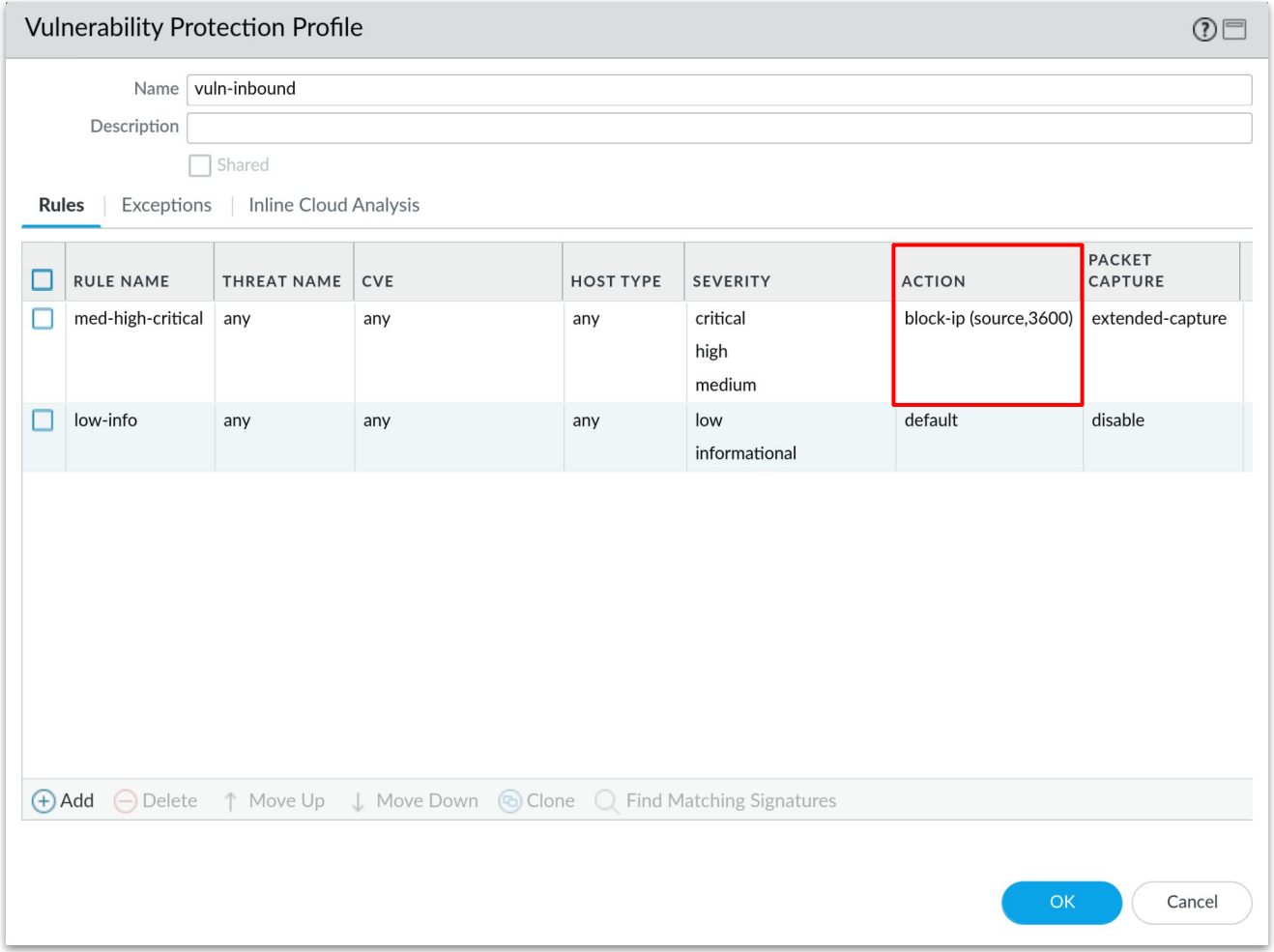
Category: computer-and-internet-info

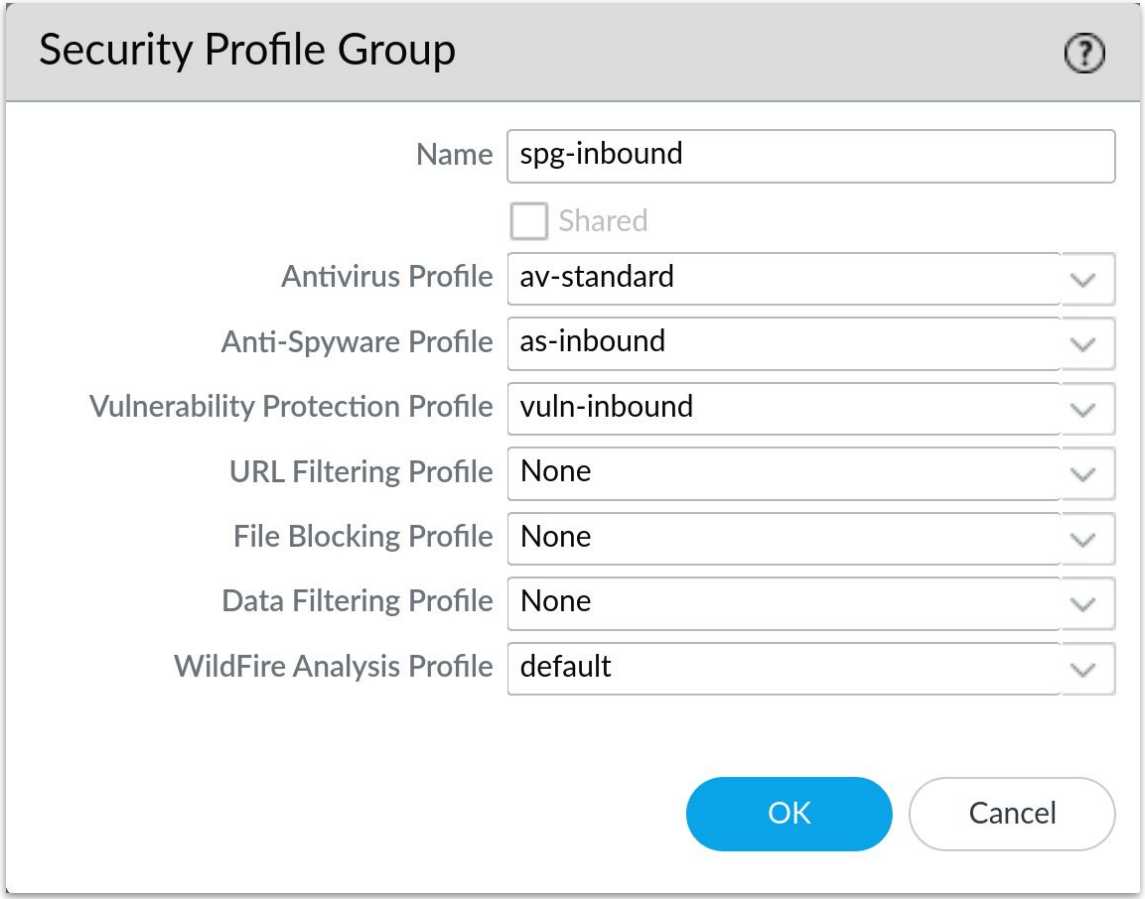
Leveraging the NGFW You Already Have

Treat Inbound Traffic Differently

- Most threats are coming from the outside of your network
- Your infrastructure is a higher-value target than your users
- While your outbound workflows are dynamic, your inbound workflows are mostly static and easier to secure
- The firewall can remember attackers

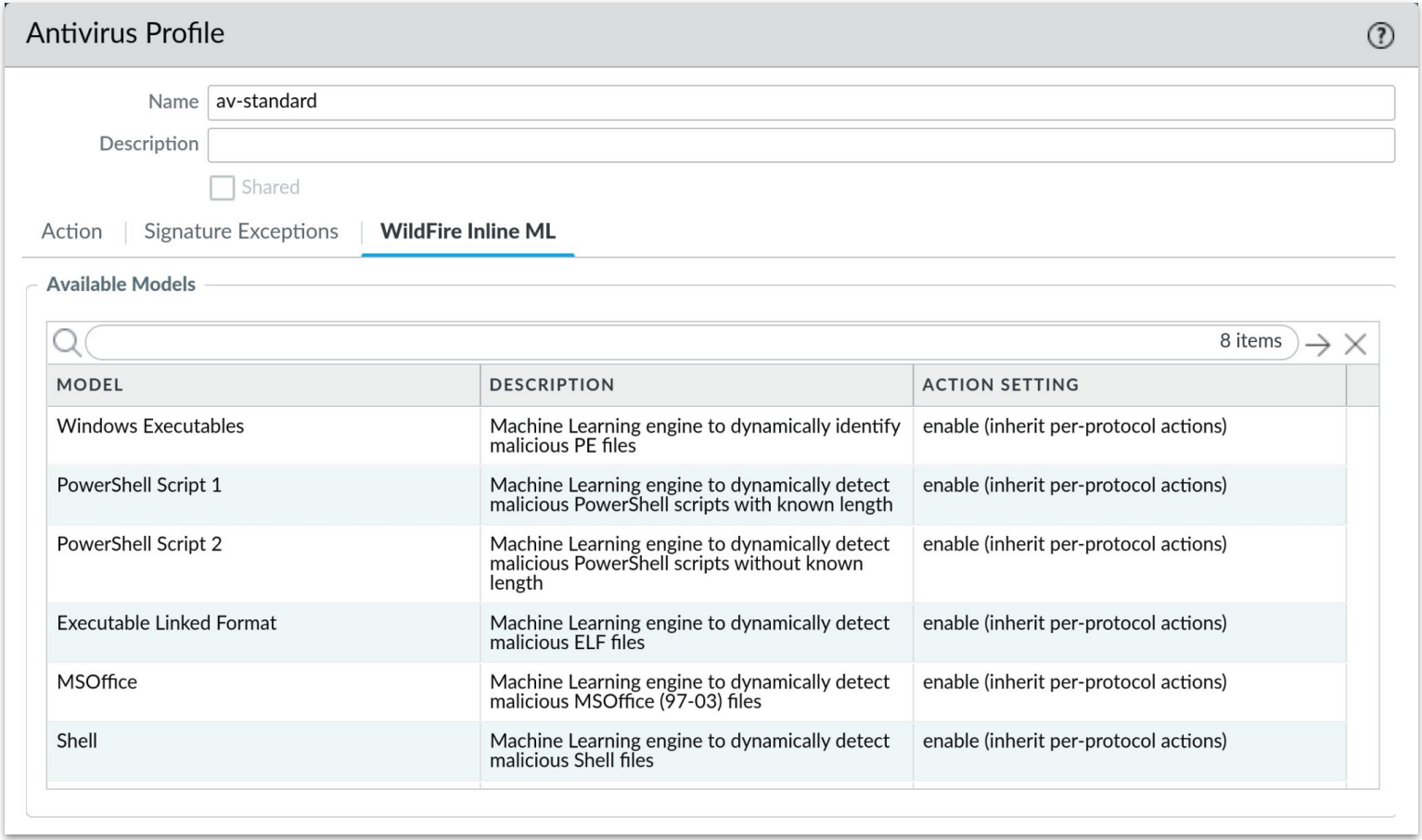


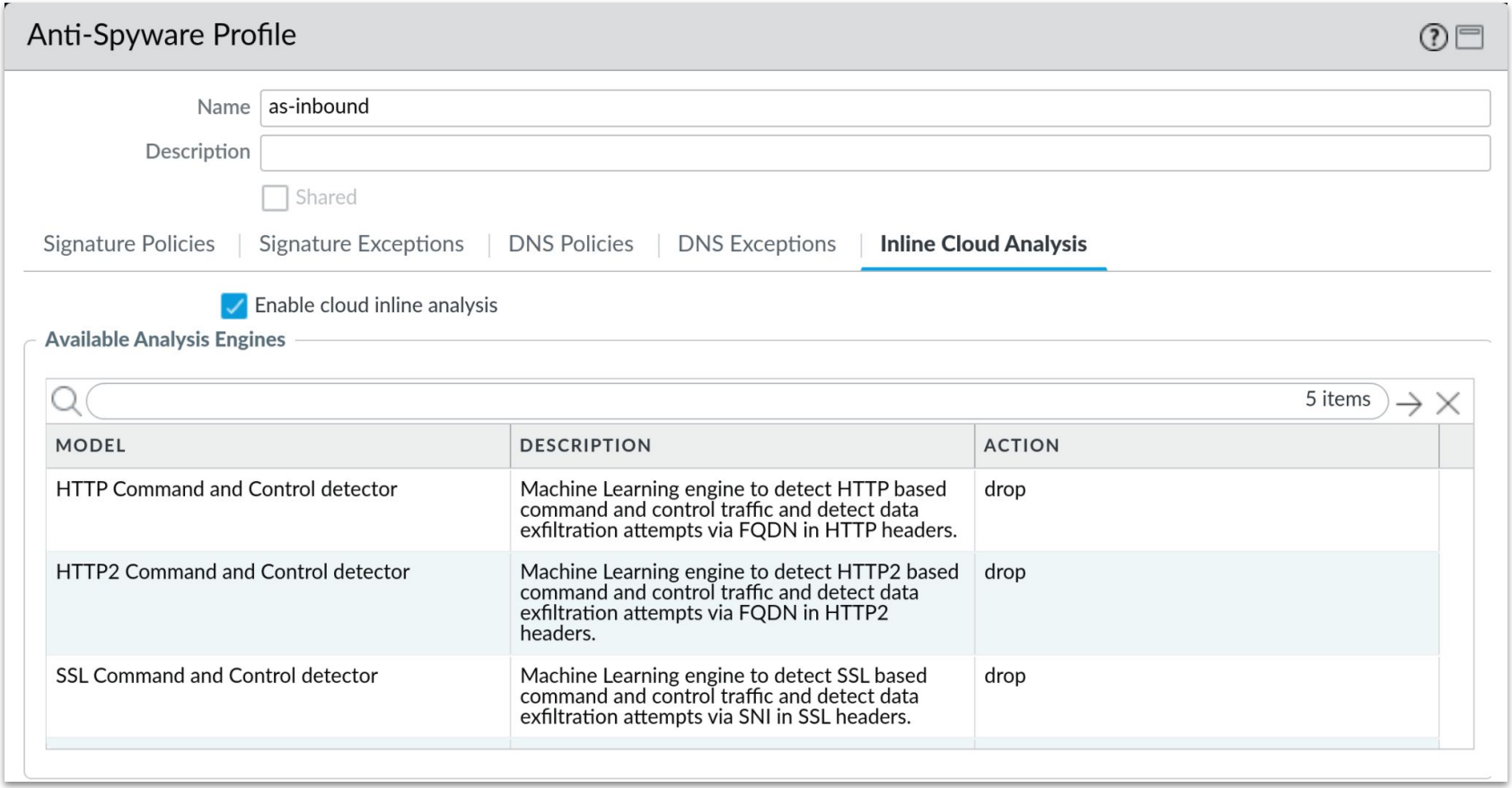




Use the new ML Features

- Anti-Virus: WildFire Inline ML
  - Runs certain file types through ML models to detect threats
  - Requires PAN-OS >= 10.0.0 and the WildFire license
- Anti-Spyware: Inline Cloud Analysis
  - Inspects certain protocols using cloud ML to detect threats
  - Requires PAN-OS >= 10.2.0 and the Advanced Threat Protection license
- Vulnerability Protection: Inline Cloud Analysis
  - Inspects certain protocols using cloud ML to detect threats
  - Requires PAN-OS >= 11.0 and the Advanced Threat Protection license
- URL Filtering: Inline Categorization
  - Local and cloud based ML models to detect threats in web traffic
  - Requires PAN-OS >= 10.2 and the Advanced URL Filtering license
- WildFire Analysis: Inline Cloud Analysis
  - Forwards suspicious files to cloud based ML models to detect threats
  - Requires PAN-OS >= 11.1 and the Advanced WildFire license





Vulnerability Protection Profile

Name: vuln-inbound

Description:

Shared

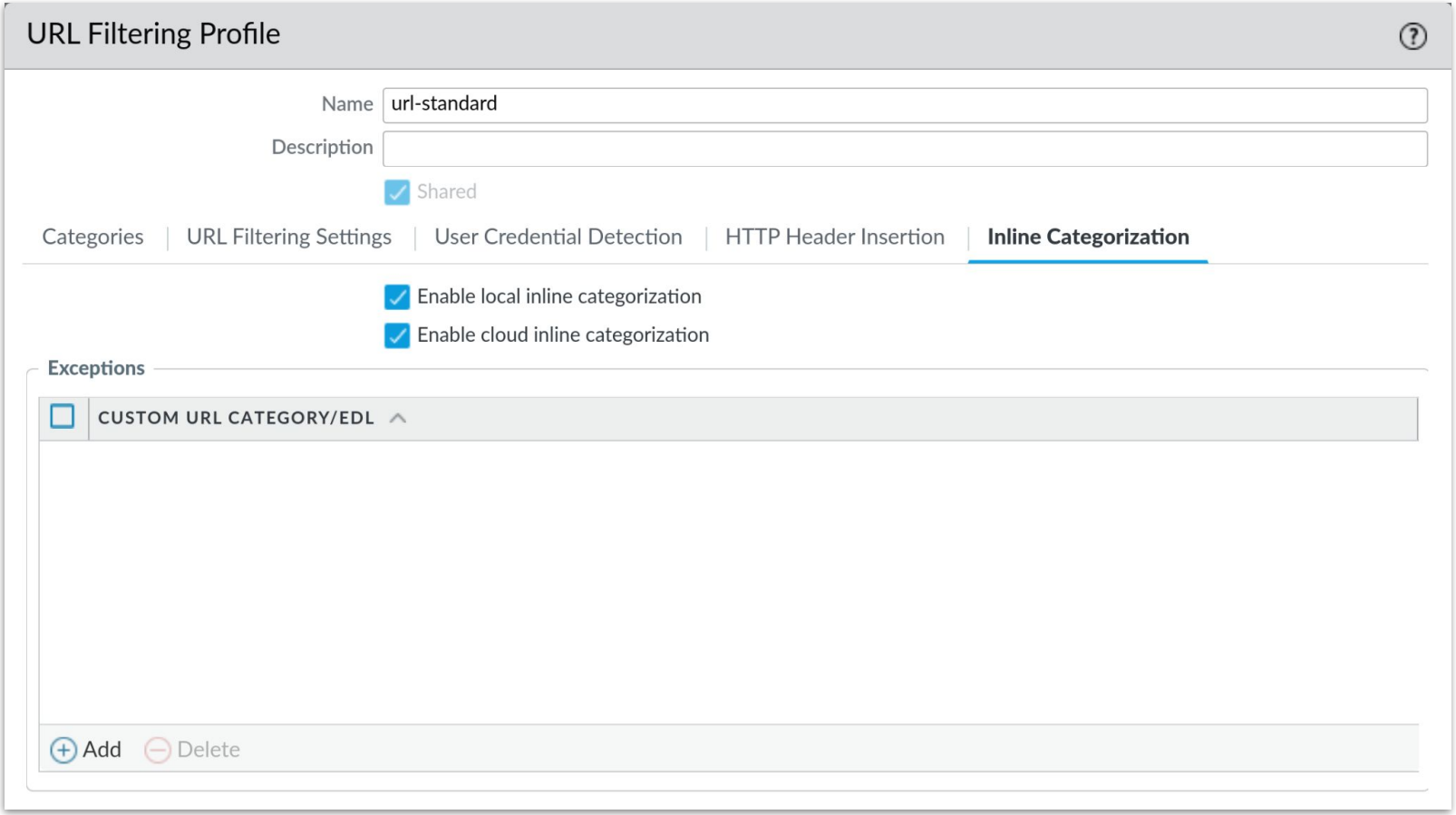
Rules | Exceptions | **Inline Cloud Analysis**

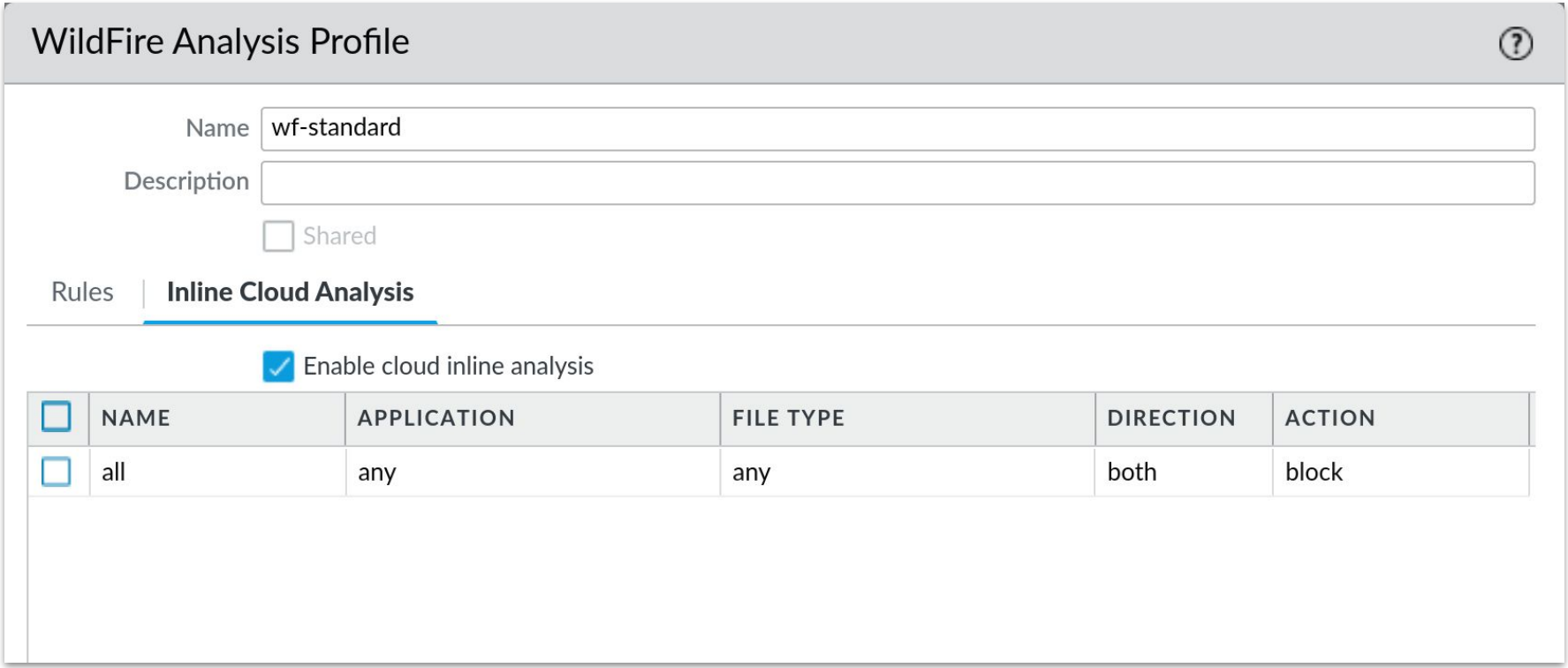
Enable cloud inline analysis

Available Analysis Engines

2 items

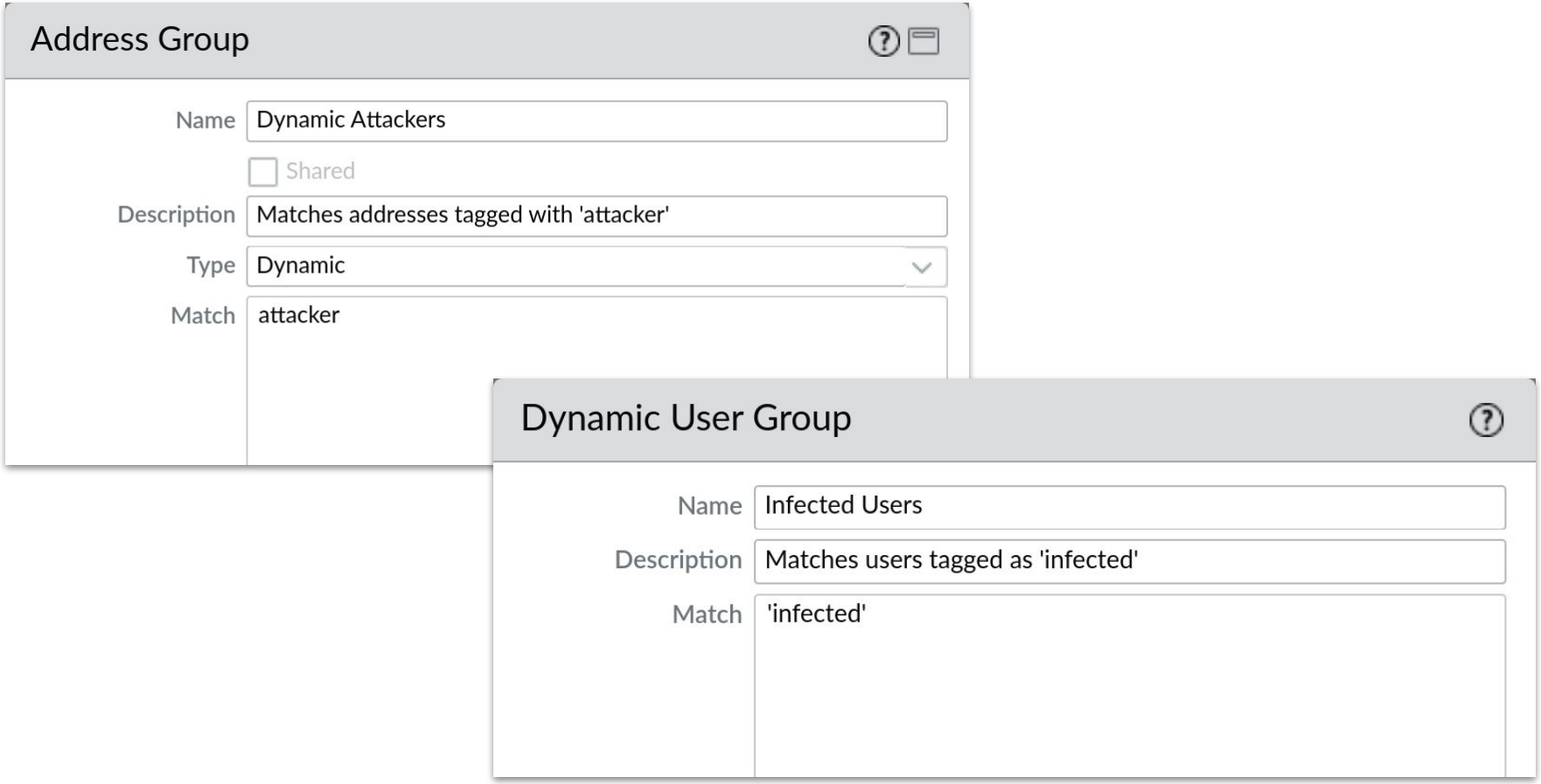
MODEL	DESCRIPTION	ACTION
SQL Injection	Detects a common hacking technique where an attacker inserts SQL queries into an applications' request	reset-both
Command Injection	Detects a common hacking technique that allows an attacker to execute arbitrary operating system	reset-both





Use Dynamic Objects, Dynamic Tagging & EDLs

- Dynamic objects can include members by tags
  - Address Groups set to type ‘Dynamic’
  - Dynamic User Groups
  - Address Objects with a matching tag behave like members of the group
- Dynamic tagging of IPs/Users with Log Forwarding Profiles
  - Log Forwarding Profiles attached to rules can trigger on certain traffic
  - Traffic that triggers these profiles can tag the source/dest IP or the user
  - These tags then match existing Dynamic Address/User groups
- External Dynamic Lists
  - Firewall fetches a file from a web server at regular intervals
  - Can be a list of IPs, domains, or URLs
  - Great for automation, or delegating filtering to non-network teams



Log Forwarding Profile

Name: tagging-example

Shared

Description:

1 item

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
critical threat sources	threat	(severity eq critical)		**Tagging** • tag critical attackers

Add Delete Clone

OK Cancel

Log Forwarding Profile Match List

Name: critical threat sources

Description:

Log Type: threat

Filter: (severity eq critical)

Forward Method

Panorama

SNMP	EMAIL
Add Delete	Add Delete

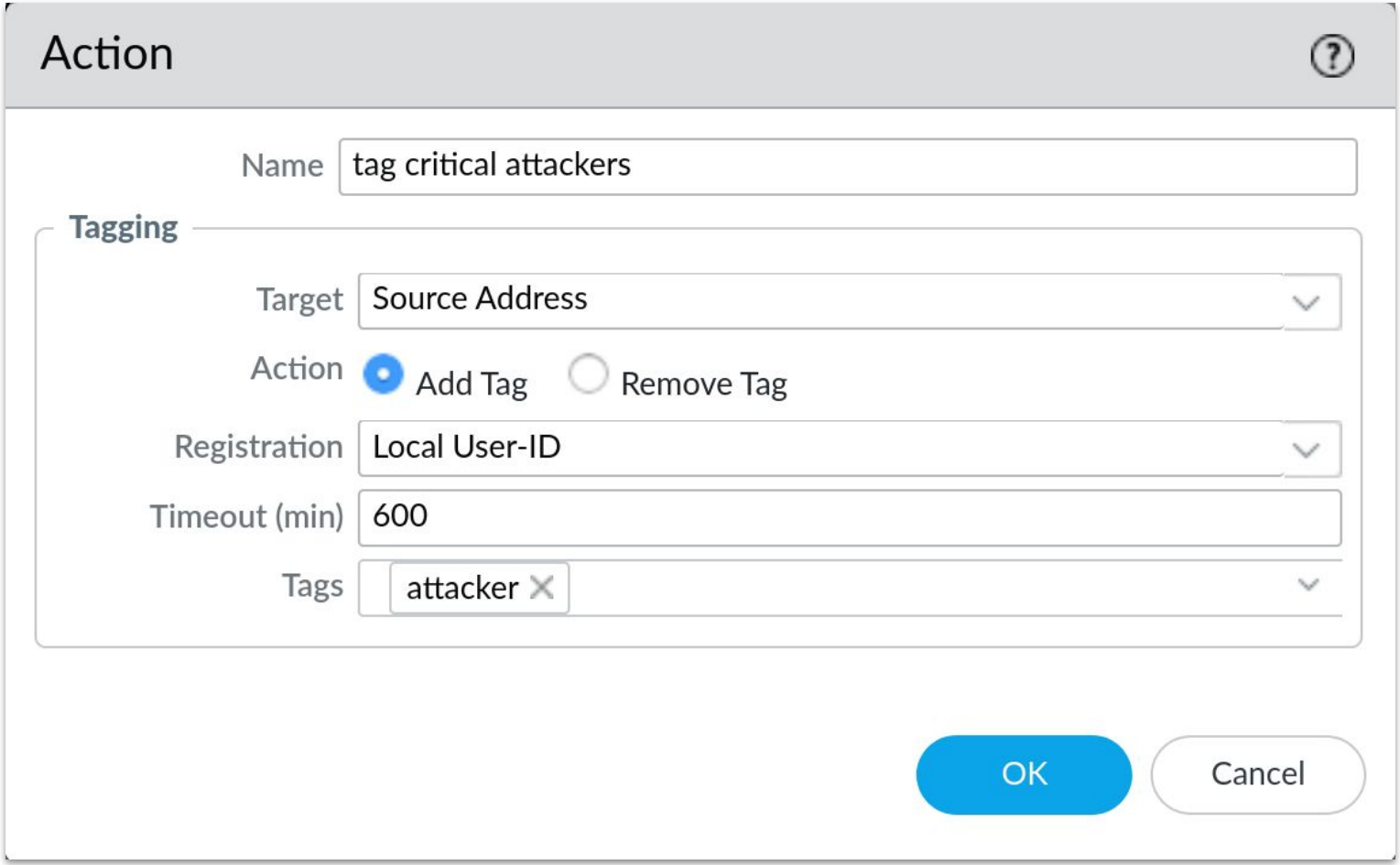
SYSLOG	HTTP
Add Delete	Add Delete

Built-in Actions

Quarantine

NAME	TYPE
tag critical attackers	tagging

Add Delete



Four Things You Can Do Now

1. Review your rulebase, tag unclear rules and disable unused rules
2. Get at least one User-ID source configured
3. Enable inbound decrypt for at least one external service
4. Configure aggressive inbound security profiles and enable inline ML engines

Bonus: How to stay on top of your config automatically

FALCO

Summary | Remediation New | Policies | Objects | Network | Device

Lorem Unified School District

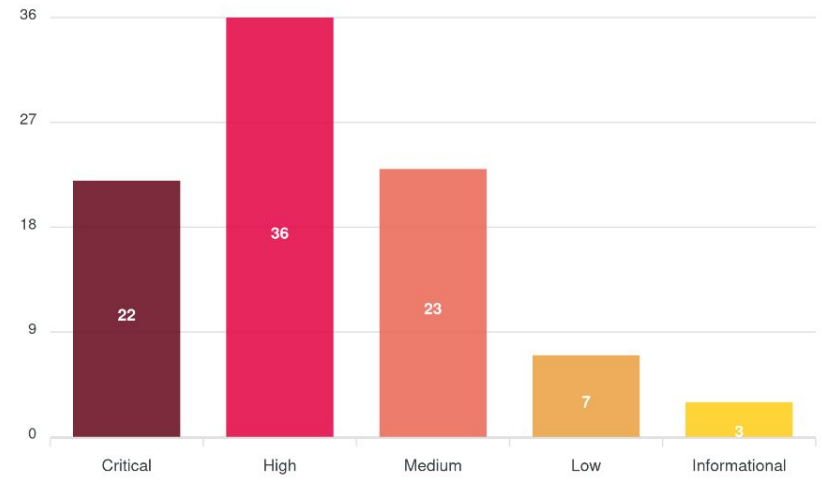
Falco Enterprise

73% passed
6 Devices Audited

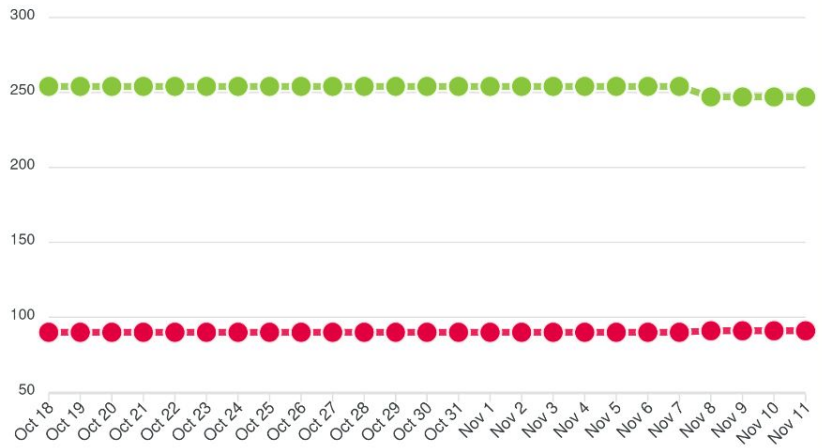
4 Vulnerable Devices
Known Vulnerabilties Found

5 Devices
Without Valid Support License

Failed Check Severity



Report History



What is Falco?

FALCO

The Software

- Continuous config audits
- Weekly summary reports
- Regression notifications
- Detailed explanations
- Remediation suggestions
- Progress tracking

The Service

- Designed to resolve issues surfaced by the report
- Direct access to experienced engineers
- Ticket entitlement for fixes or improvements
- Fast resolution

HIGH

Security Rules That Allow SSH Without Log At Session Start

Global Pass Rate	54%
Company Pass Rate	40%

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

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
Allow SCP to labmon01	Allow	ssh	✗	✗
Allow SCP to labwinfra01	Allow	ssh	✗	✗
Allow term to pan management-app	Allow	ssh, ssl	✗	✗
Allow TS Engineers to Web	Allow	ssh	✗	✗

Regression Detected

Digital Scepter team,

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

Device: devlpra01

Expired Certificates

Critical

Description:

Expired certificates should be immediately replaced with valid certs or removed if they are no longer needed.

Result:

There are expired certificates

Remediation:

Go to `Device → Certificates → Device Certificates` on a firewall, or `Panorama → Certificate Management → Certificates` and replace or remove the expired certs. To replace a cert without affecting operations, import the replacement cert with the exact same name, then commit.

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

If you need support, reply to this email to open a ticket.

How to get your free Falco report

- Lite tier free for everyone
- Reach out to set up an appointment
- Takes less than 30 minutes

Looking for a quick self-guided review of your firewall health? Grab a Falco Scorecard to see how you stand.

Stop by Booth #21 if you have more questions