

BLOCK UNKNOWN THREATS



*IF I AM PUTTING MYSELF OUT THERE
AND TAKING SOME OF THESE RISKS,
THEN I WANT TO DO IT PROPERLY*

- WildFire® concepts
- Configure and manage WildFire
- WildFire reporting

Learning Objectives

After you complete this module, you should be able to:

- Describe WildFire purposes and operation
- Describe WildFire license and deployment choices
- Configure and update WildFire
- View WildFire reports and logs





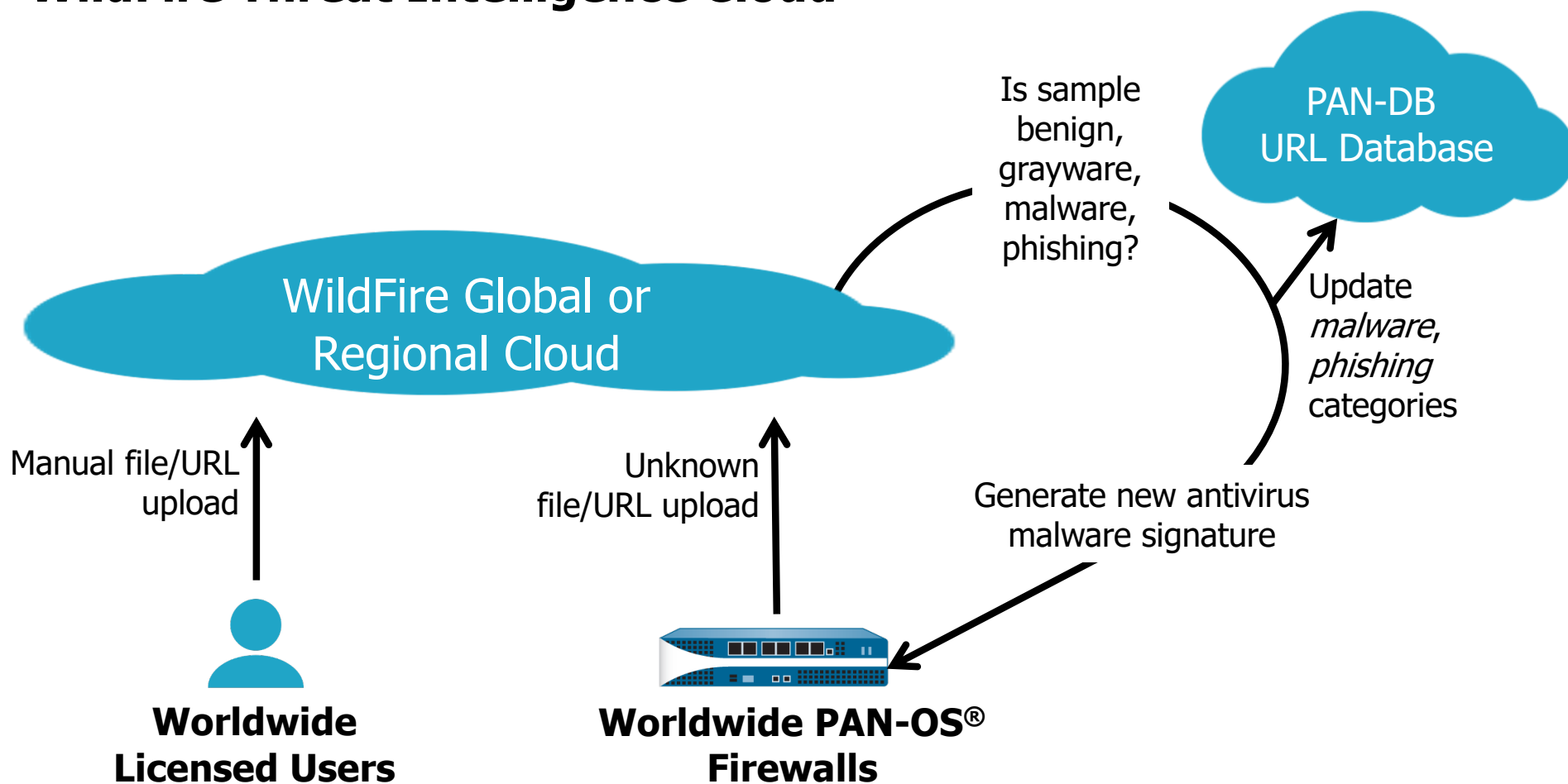
WildFire concepts

Configure and manage WildFire

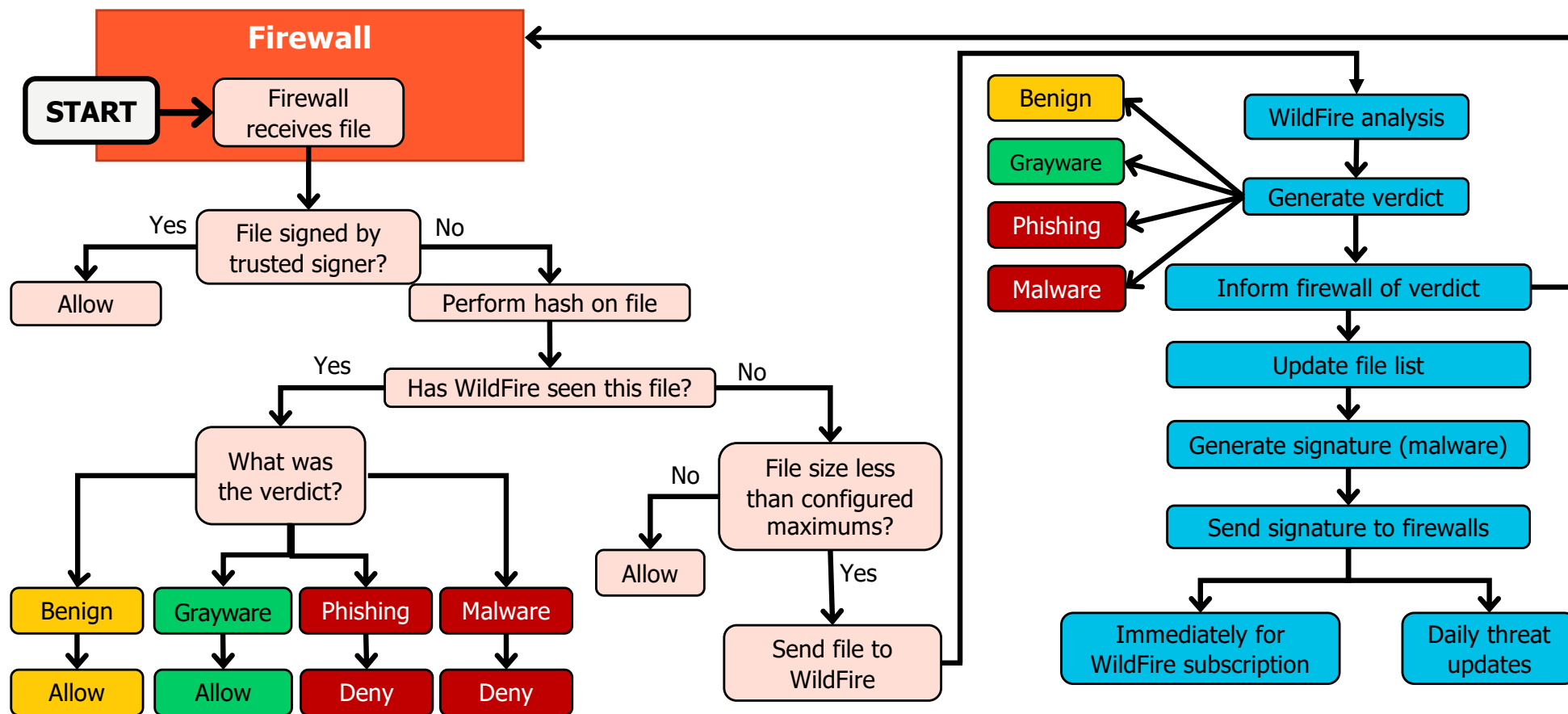
WildFire reporting



WildFire Threat Intelligence Cloud



WildFire Operation Overview

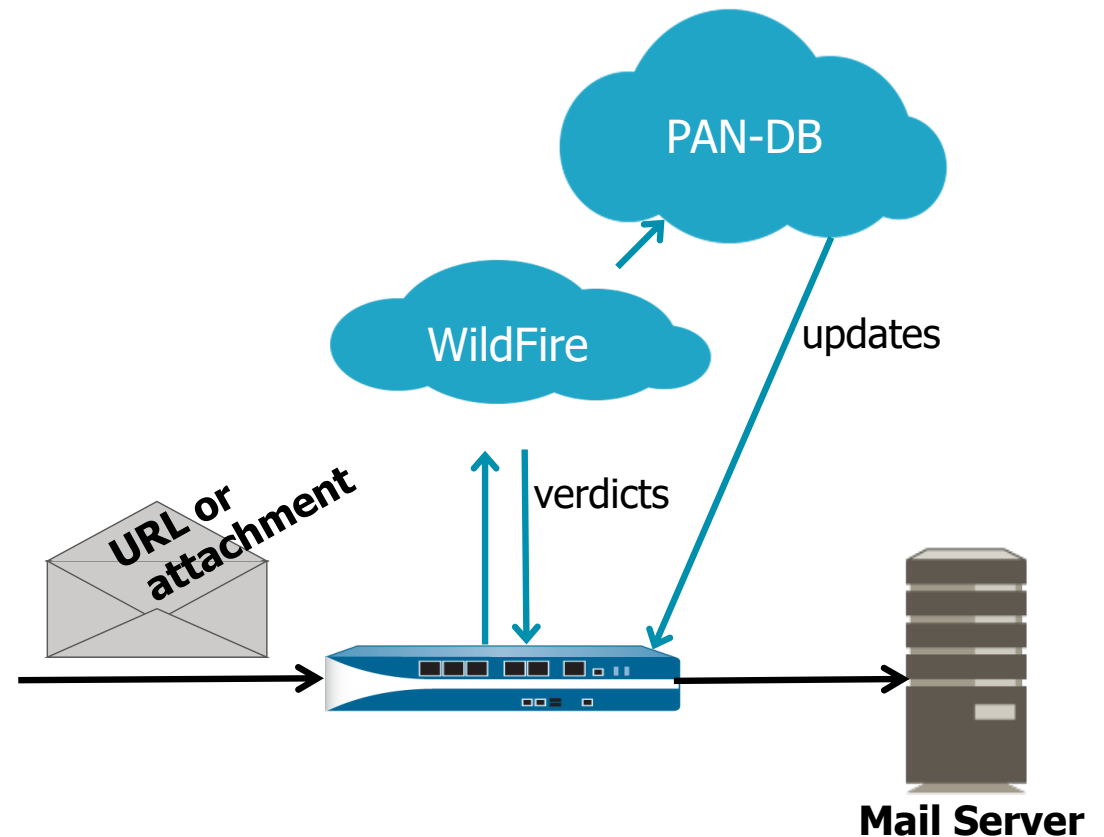


WildFire Verdict Descriptions

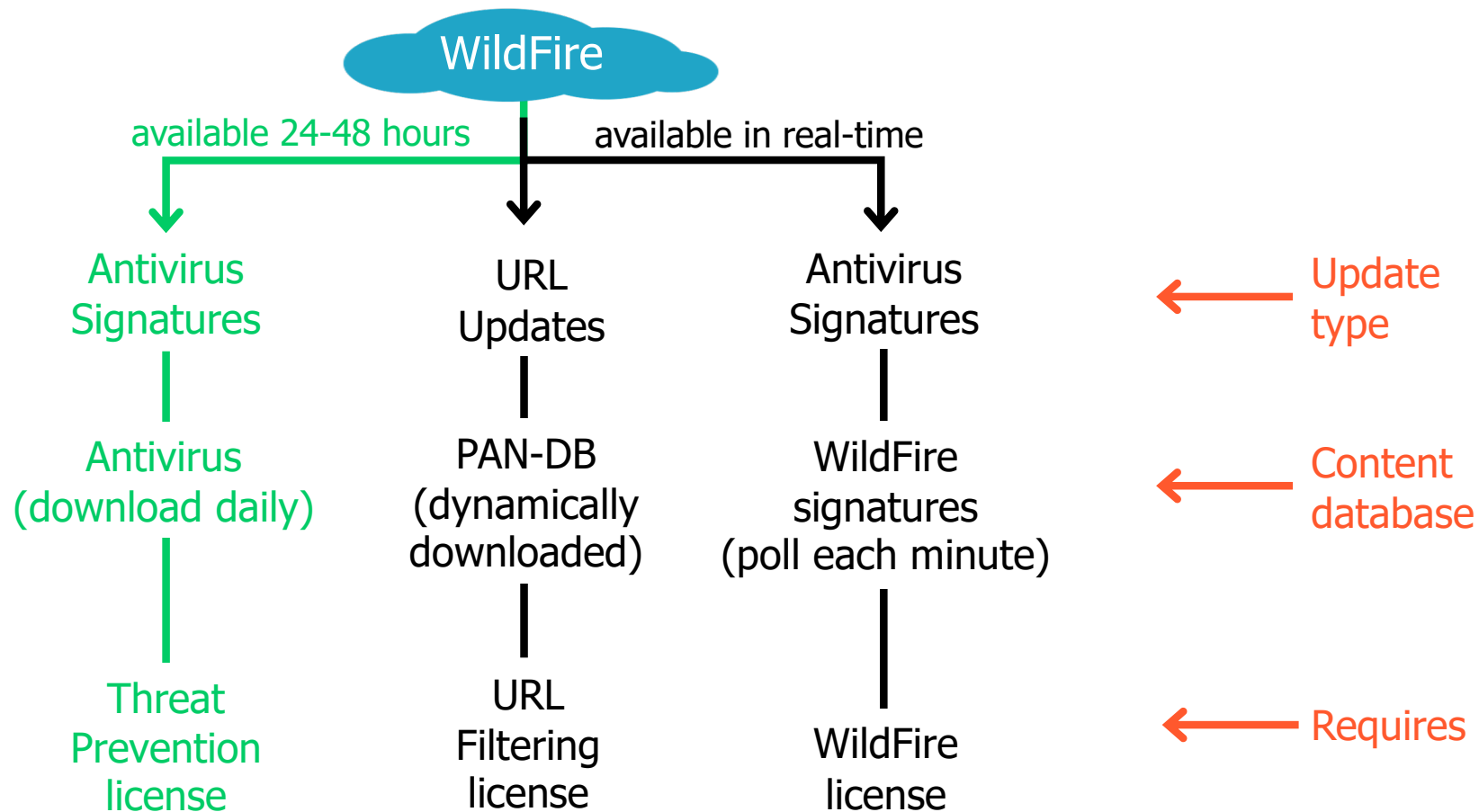
Verdict	Description
Benign	<ul style="list-style-type: none">• Safe and does not exhibit malicious behavior.
Grayware	<ul style="list-style-type: none">• No security threat but might display obtrusive behavior.• Examples include adware, spyware, and browser helper objects (BHOs).
Malware	<ul style="list-style-type: none">• Malicious in nature and intent and can pose a security threat.• Examples include viruses, worms, trojans, remote access tools (RATs), rootkits, and botnets.
Phishing	<ul style="list-style-type: none">• An attempt to trick users into revealing their login information.• Based on properties and behaviors the website displays.

WildFire Protects Email

- Email with attachments or URL links is sent to WildFire for analysis.
- If an attachment or link is malicious, WildFire can:
 - Create and download new antivirus signatures to the firewall
 - Update the PAN-DB database with malicious URLs
- The firewall uses new information to protect the network.



Content Packages and WildFire Updates



Standard and Licensed Functionality

Standard subscription service:

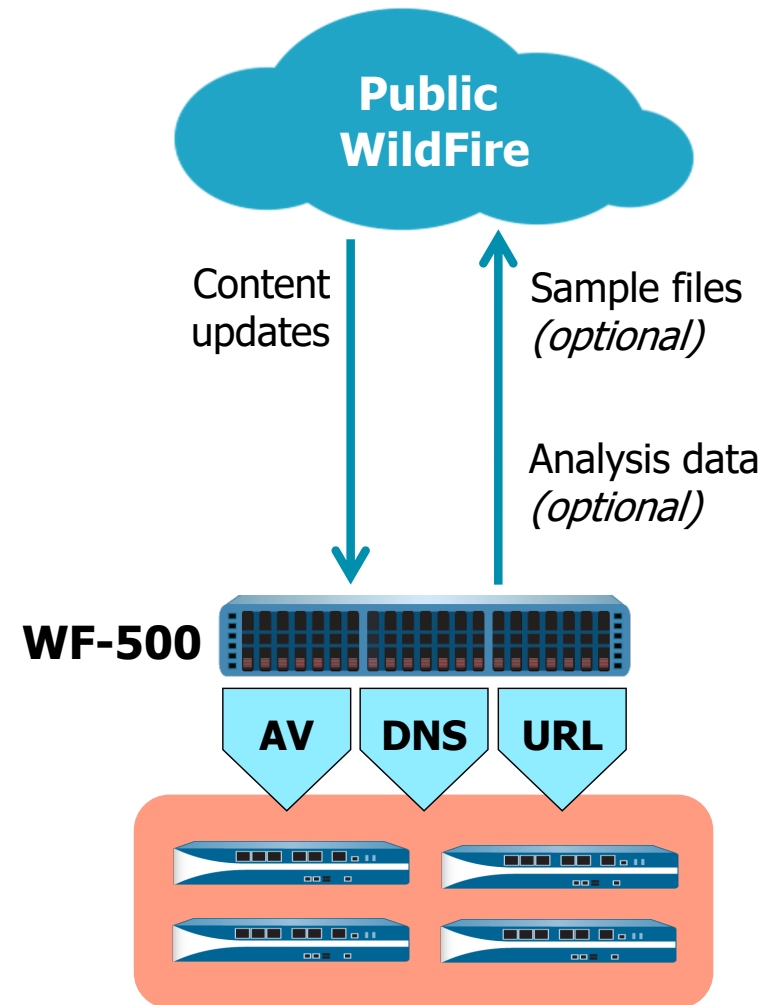
- Analysis available in Windows XP, 7, 10, macOS, Android, Linux, and bare metal
- Windows PE file analysis:
 - EXE, DLL, FON, SCR, others
- Antivirus signatures delivered via daily dynamic content updates (requires Threat Prevention license)
- Automatic file submission

WildFire licensed service:

- Standard subscription features
- Additional file type analysis:
 - Microsoft Office, PDF, JAR, CLASS, SWF, SWC, RAR, 7-Zip, Linux ELF, APK, Mach-O, DMG, PKG, JS, VBS, PS1
- WildFire signature updates every 5 minutes
- Manual file submission via API
- WildFire private cloud appliance:
 - WF-500

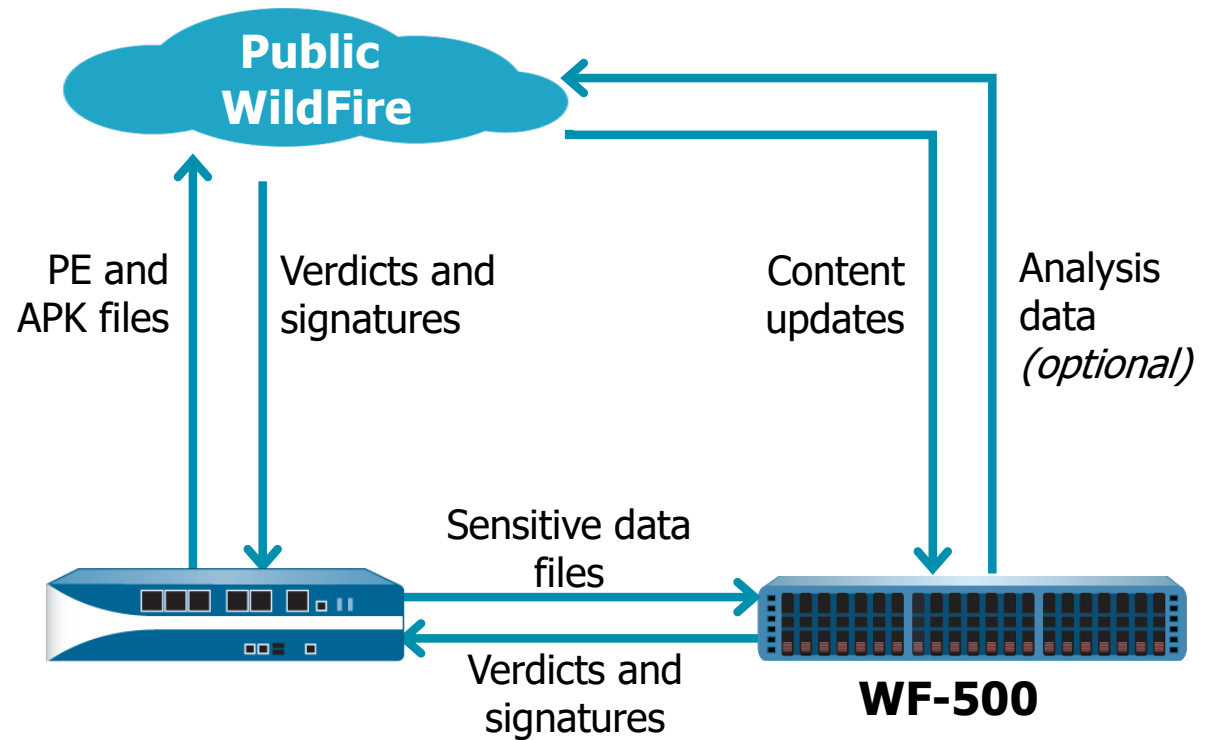
WildFire Private Cloud

- WF-500 appliance:
 - Only Windows XP and 7 virtual environments
- Locally analyzes unknown files, and files or URLs found in email:
 - Files never leave your network.
 - No APK files.
- Locally generates antivirus signatures and categorizes URLs
- Signatures updated every 5 minutes
- Supports the WildFire XML API
- Does not support the Phishing verdict



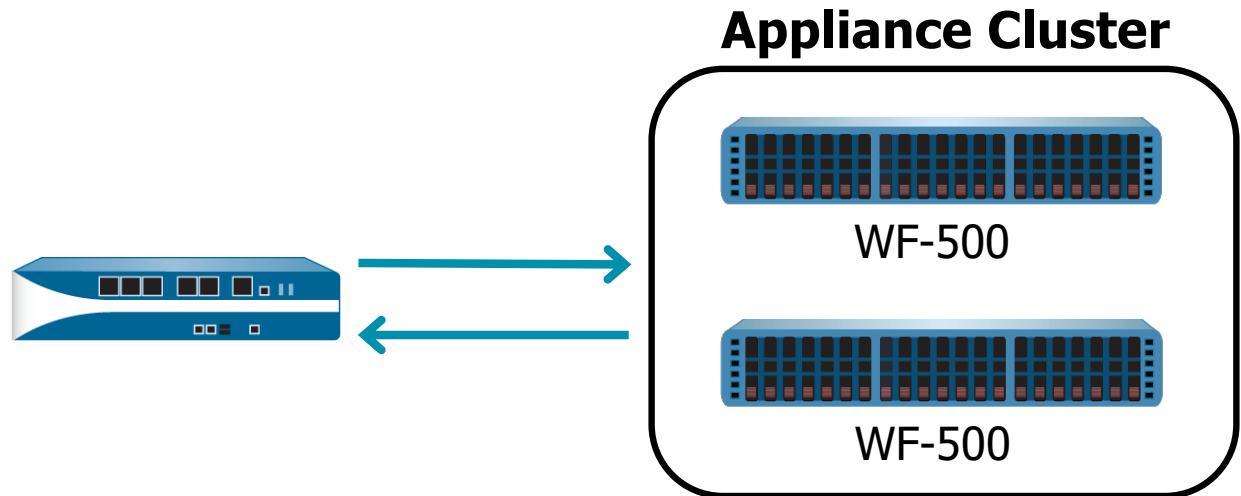
Hybrid Cloud Example

- Combines public and private cloud
- PE and APK files to public cloud?
- Sensitive data files to private cloud?



WildFire Appliance Cluster

- Combines multiple WildFire appliances for fault tolerance
- Useful when the WildFire public cloud cannot be used
- Can group up to 20 appliances



WildFire concepts



Configure and manage WildFire

WildFire reporting



Configure WildFire Settings

Device > Setup > WildFire

General Settings

WildFire Public Cloud

WildFire Private Cloud

☐ Use Proxy Settings for Private Cloud

File Size Limits

FILE TYPE	SIZE LIMIT
pe (MB)	16 (default)
apk (MB)	10 (default)
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
jar (MB)	5 (default)
flash (MB)	5 (default)
MacOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

☒ Report Benign Files

☒ Report Grayware Files

Configure connection to WildFire cloud(s).

Files that exceed size are not forwarded to WildFire.

Benign and grayware files appear in the WildFire Submissions log.

Note: Decrypted content is not forwarded to WildFire by default.

Submission Settings

Device > Setup > WildFire

Session Information Settings

☒ Source IP

☒ Source port

☒ Destination IP

☒ Destination port

☒ Virtual System

☒ Application

☒ User

☒ URL

☒ File name

☒ Email sender

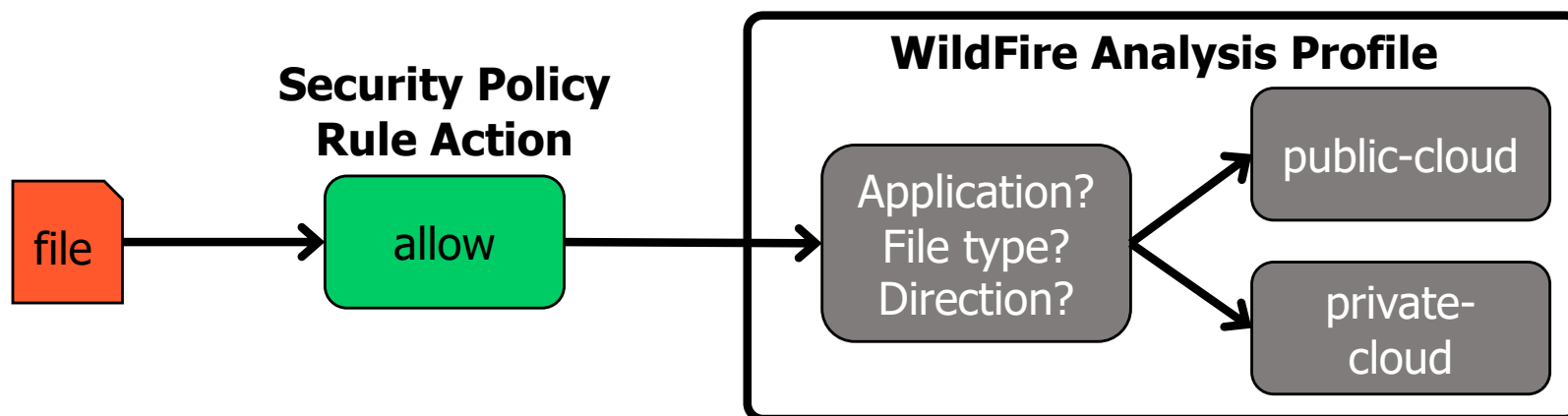
☒ Email recipient

☒ Email subject

Define session information types reported to WildFire (and therefore available in WildFire Submissions log).

WildFire Analysis Profile

Profile implements additional security checks on files in allowed traffic.



Best Practice WildFire Security Profiles

Objects > Security Profiles > WildFire Analysis > Add

<input type="checkbox"/>	NAME	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
<input type="checkbox"/>	default	default	any	any	both	public-cloud
<input type="checkbox"/>	Outbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Inbound-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Internal-WF	Forward-All	any	any	both	public-cloud
<input type="checkbox"/>	Alert-Only-WF	Forward-All	any	any	both	public-cloud

- Start with alert-only profile to determine which files to forward to analyze for unknown threats.
- Recommended profile settings are illustrated here.
- You can start with alert-only-wf to gather log information:
 - Later update to use outbound-wf, inbound-wf, and internal-wf profiles
- Recommend to set **File Types** to **any**:
 - Automatically includes any new file types added to WildFire

Attach WildFire Analysis Profiles to Security Rules

Policies > Security > Add

Security Policy Rule

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

Action Setting

Action: **Allow**

☐ Send ICMP Unreachable

Profile Setting

Profile Type: **Profiles**

Antivirus: **None**

Vulnerability Protection: **None**

Anti-Spyware: **None**

URL Filtering: **None**

File Blocking: **None**

Data Filtering: **None**

WildFire Analysis: **Public-Cloud-Profile**

Log Setting

☐ Log at Session Start

☒ Log at Session End

Profile Setting

Profile Type: **Group**

Group Profile: **Corp-Strict-Profiles**

☐ Disable Server Response Inspection

- Add WildFire Analysis Profile to Security policy rule, or
- Add WildFire Analysis Profile to Group Profile and add group to Security policy rule.

WildFire Update Schedule

- Schedule poll period for WildFire antivirus signature updates:
 - Requires a WildFire license
 - Without a license, WildFire antivirus signatures still are added to the daily Antivirus content package.

Device > Dynamic Updates

WildFire Update Schedule

Recurrence: Every Minute

Action: download-and-install

☐ Synchronize content with HA peer after download/install

Buttons: Delete Schedule, OK, Cancel

Dropdown menu options: None (Manual), Real-time, Every Minute, Every 15 Minutes, Every 30 Minutes, Every Hour

Device ID	Device Name	Version	Update Type	Size	Last Update	Status	Release Notes
467063-470000	panupv3-all-wildfire-467063-470000	PAN OS 10.0 And Later	Full	8 MB	2020/06/29 15:07:15 UTC	✓ previously	Release Notes
467667-470604	panupv3-all-w-470604					✓	Release Notes
473787-476724	panupv3-all-w-476724					✓	Release Notes

Configure Real-Time WildFire Analysis

Objects > Security Profiles > AntiVirus

Antivirus Profile

Name: WildFire-Real-Time-Analysis
Description: WildFire Inline Machine Learning Real-Time Analysis Profile

Action: Signature Exceptions: **WildFire Inline ML**

Classification engines define each file type to apply to a policy.

Define policy action for each classification engine.

Available Models

MODEL	DESCRIPTION	ACTION SETTING
Windows Executables	Machine Learning engine to dynamically identify malicious PE files	disable (for all protocols)
PowerShell Script 1	Machine Learning engine to dynamically detect malicious PowerShell scripts with known length	disable (for all protocols)
PowerShell Script 2	Machine Learning engine to dynamically detect malicious PowerShell scripts without known	disable (for all protocols)

enable (inherit per-protocol actions)
alert-only (override more strict actions to alert)
disable (for all protocols)

File Exceptions

PARTIAL HASH	FILENAME
--------------	----------

(Optionally) Add file exceptions to exclude specific files.

WildFire concepts

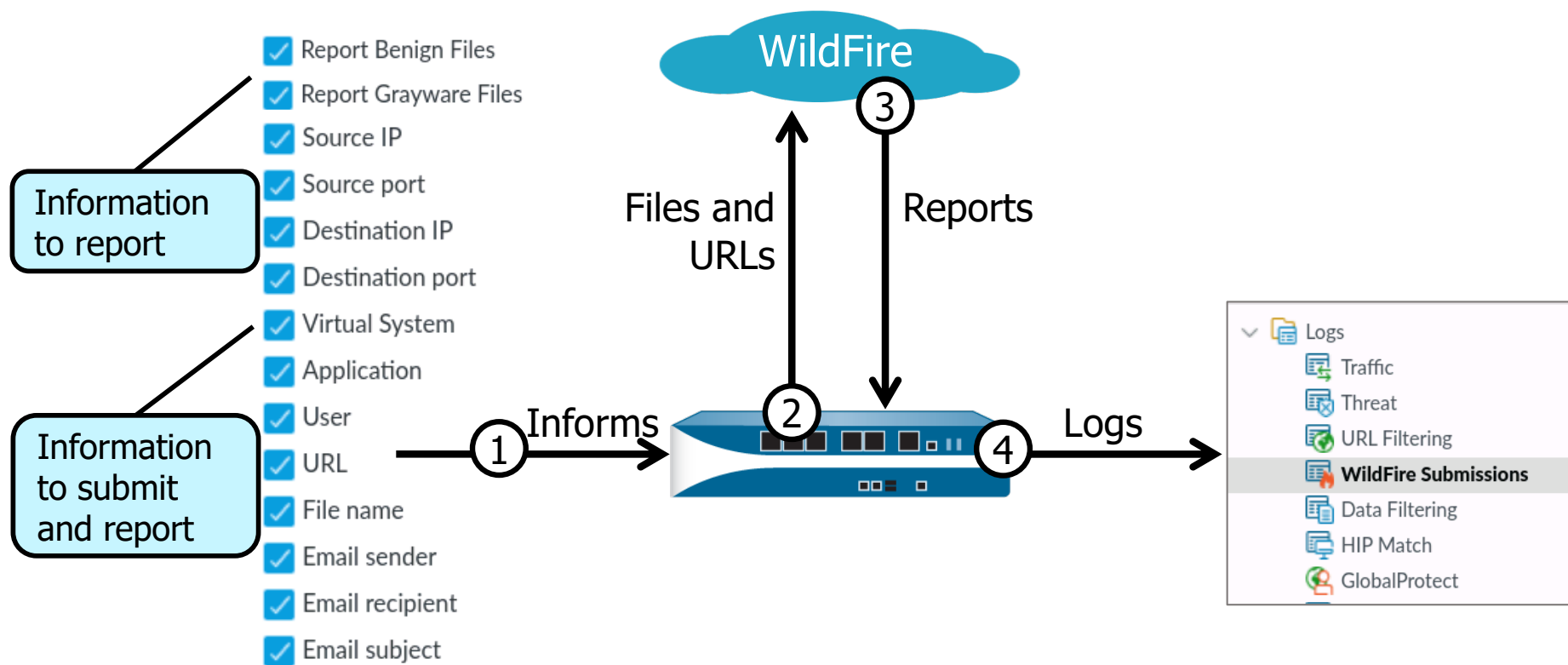
Configure and manage WildFire



WildFire reporting



WildFire Reporting



Verify Submissions and View Reports

> debug wildfire upload-log show

```
admin@firewall-a> debug wildfire upload-log show

Upload Log disk log rotation size: 2.000 MB.
Public Cloud upload logs:

log: 0, filename: wildfire-test-pe-file.exe
processed 6393 seconds ago, action: upload success
vsys_id: 1, session_id: 196, transaction_id: 3
file_len: 55296, flag: 0x801c, file type: pe
threat id: 52020, user_id: 0, app_id: 109
from 192.168.1.20/50731 to 52.20.176.145/80
SHA256: d6fbefe577a5336641f184ef4a3136889fed8fd0a37741165f01cd202549b637
```

CLI command to verify
successful file upload



View returned report
information.

Monitor > Logs > WildFire Submissions

	RECEIVE TIME	FILE NAME	SOURCE ZONE	SOURCE ADDRESS	APPLICATION	RULE	VERDICT	SEVERITY
	07/10 17:04:24	wildfire-test-pe-file.exe	Users_Net	192.168.1.20	web-browsing	Users_to_Internet	malicious	high

WildFire Analysis Verdict Example

Monitor > Logs > WildFire Submissions

Detailed Log View

Log Info | **WildFire Analysis Report**

WildFire Analysis Summary [Download PDF](#)

File Information

File Type: PE

File Signer: cc5ab063c9b9b05e830caed59b52097a43f66030572b13bb8a2bc55c7631d629

SHA-256: 1ee8da7a08a348288ad198e7cd2e8209af4997b3

MD5: a386b3ec09124906c0303f9d3f3ef4c1

File Size: 55296 bytes

First Seen Timestamp: 2020-07-22 17:22:11 UTC

Verdict: malware

Sample File: [Download File](#)

Download a PDF version of the report.

Download a copy of the file.

PCAP	RECEIVE TIME	TYPE	APPLICA...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATE...	URL CATE...	VERDICT	URL	FILE NAME
	2020/07/22 17:22:40	end	web-browsing	allow	Users_...	542e5...	62...		any				
	2020/07/22 18:53:40	wildfire	web-browsing	allow	Users_...	542e5...		high			malicious		wildfir...

Close

Report Incorrect Verdict: Web Interface

Report Incorrect Verdict

Are you sure you want to report this file as having been incorrectly categorized as malware?

This session will be flagged for further analysis by Palo Alto Networks. When analysis is complete, you will be emailed with the results of the analysis and if necessary, the verdict in this report will be updated.

Sample Information

SHA-256	cc5ab063c9b9b05e830caed59b52097a43f66030572b13bb8a
MD5	a386b3ec09124906c0303f9d3f3ef4c1
Verdict	malware

Additional Information

Suggested verdict:

Your email address:

Future correspondence related to this report will be sent to this email address.



Please include any comments that may help us understand this issue more quickly.

OK Cancel

- You can submit verdict change requests to Palo Alto Networks:
 - From web interface or WildFire portal
- From web interface:
 1. Select **Monitor > Logs > WildFire Submissions**.
 2. Find entry and click its detailed view icon.
 3. Click **WildFire Analysis Report** tab.
 4. Click **Select Incorrect Verdict** link.
 5. Suggest new verdict.

WildFire Portal

<https://wildfire.paloaltonetworks.com>




[Dashboard](#) [Reports](#) [Upload Sample](#) [Settings](#) [Account](#)

DASHBOARD

PREVIOUS 1 HOUR

Malware vs. Benign vs. Grayware vs. Phishing



■ Malware ■ Benign ■ Grayware ■ Phishing

Click the firewall serial number to view list of submissions.

Source	Malware	Benign	Grayware	Phishing	Registered
Manual	1410	129241	31	0	
015300000222	2735	261	0	0	2020-04-04 12:12:03
001801000103	2189	202	0	0	2020-04-08 13:30:09
001701000105	678	0	0	0	2020-04-08 13:30:07
007200009245	11	0	0	0	2020-04-08 13:27:35
007200004200	11	0	0	0	2020-04-08 13:27:35

WildFire Dashboard Reports

The screenshot displays the Palo Alto Networks WildFire dashboard. A modal window titled "WILDFIRE ANALYSIS REPORT" is open, showing file information for a sample. The modal includes a "Download as PDF" button and a "Download File" link. A table on the right lists the verdicts for multiple samples, with the last one marked as "Malware". An arrow points from the "Sample File" link in the modal to the "Download File" button in the table below.

WILDFIRE ANALYSIS REPORT

FILE INFORMATION

File Type	Microsoft Excel 97 - 2003 Document
File Signer	
SHA-256	498794651cf72ed4a28d876a54b58cbe15012157bb322b97fcdca9c13f23f5bf
MD5	18eb18be381cef5405f4cc189e32dd8c
File Size	13824 bytes
First Seen Timestamp	2014-09-08 10:32:38 PDT
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

Timestamp	Action	File Name
2020-04-08 13:37:43	Manual	
2020-04-08 13:37:43	Manual	
2020-04-08 13:37:43	Manual	
2020-04-08 13:37:43	Manual	YISfmTfeG7OT.XLS

Verdict

Benign
Pending
Benign
Benign
Pending
Benign
Benign
Benign
Benign
Malware

Report Incorrect Verdict: WildFire Portal

REPORTS

Source Any

	Received Time	Source	File / URL
	2020-03-30 14:56:10	Manual	mega_feb2020 FB-651.pdf
	2020-03-30 14:56:10	Manual	
	2020-03-30 14:56:10	Manual	

REPORT INCORRECT VERDICT

Are you sure you want to report this file as being incorrectly categorized as **benign**?

This sample will be flagged for further analysis by Palo Alto Networks. If you chose to give us your email address, you will receive an email with the results of the analysis review. If the verdict is found to be incorrect, it will be updated to the correct verdict in all previous and future WildFire logs featuring this sample.

SAMPLE INFORMATION

SHA-256	458f0825f25b10f4fefa6255ea473f3ca8416cc0a10da73326d84077f29293f8
MD5	4bf9885dff08be26c5a7aa73a005a26d
Verdict	Benign

ADDITIONAL INFORMATION

Suggested verdict: Malware

Email:

Future correspondence related to this incorrect verdict report will be sent to the email address

REPORT TO PALO ALTO NETWORKS

This sample was determined to be benign. If you believe this verdict is incorrect, please [report an incorrect verdict](#). This action will send sample to Palo Alto Networks for further analysis.

Module Summary

Now that you have completed this module, you should be able to:

- Describe WildFire purposes and operation
- Describe WildFire license and deployment choices
- Configure and update WildFire
- View WildFire reports and logs



Questions



Lab 15: Blocking Unknown Malware with WildFire

- Create a WildFire Analysis Profile
- Apply a WildFire Profile to Security Rules
- Test the WildFire Analysis Profile
- Examine WildFire Analysis Details



**Protecting our
digital way
of life.**