

WILDFIRE



EDU-210 Version A
PAN-OS® 9.0

DETECT UNKNOWN THREATS

- WildFire® concepts
- Configuring and managing WildFire
- WildFire reporting

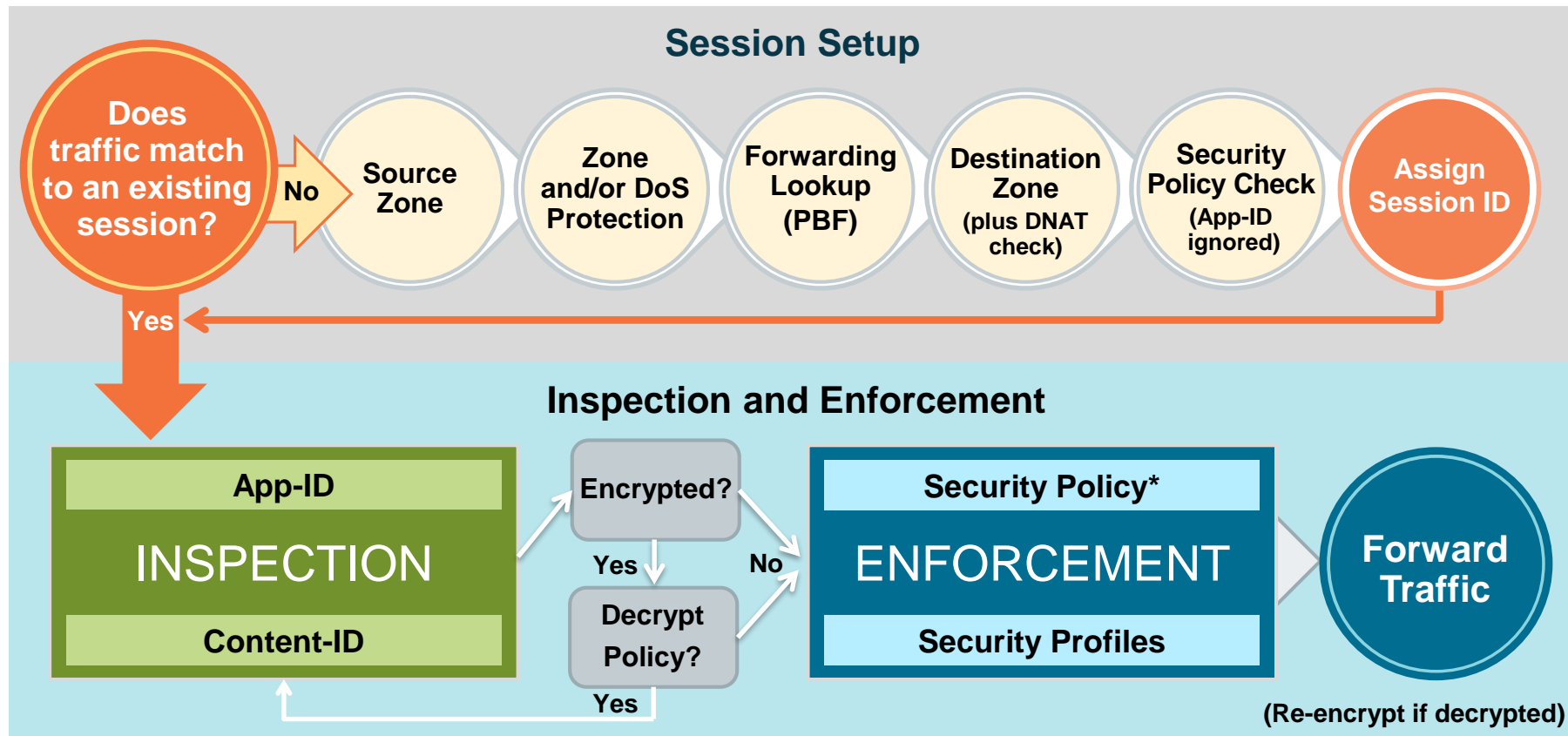
Agenda



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

- Describe how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure Session Information Settings to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses

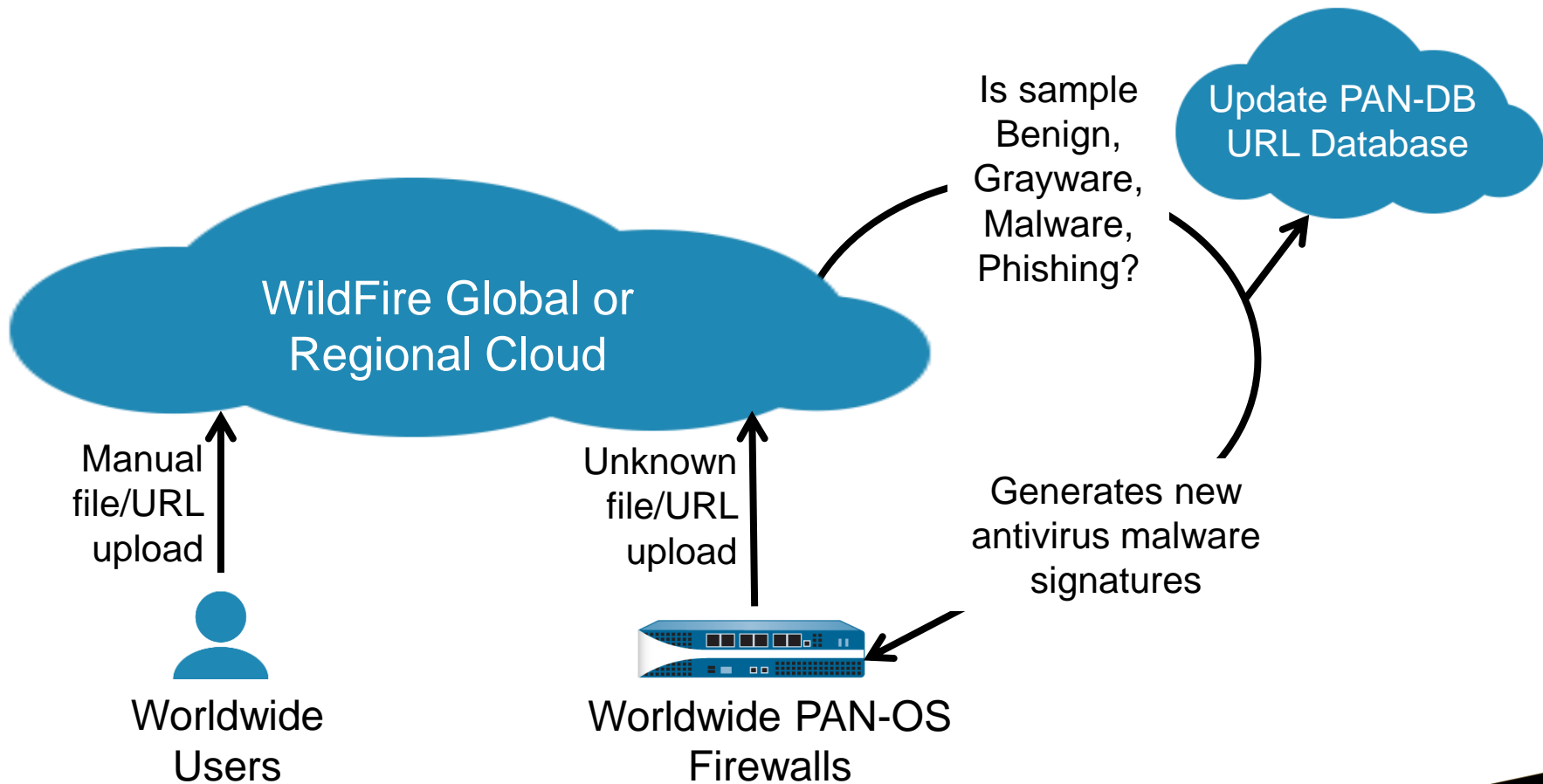


WildFire concepts

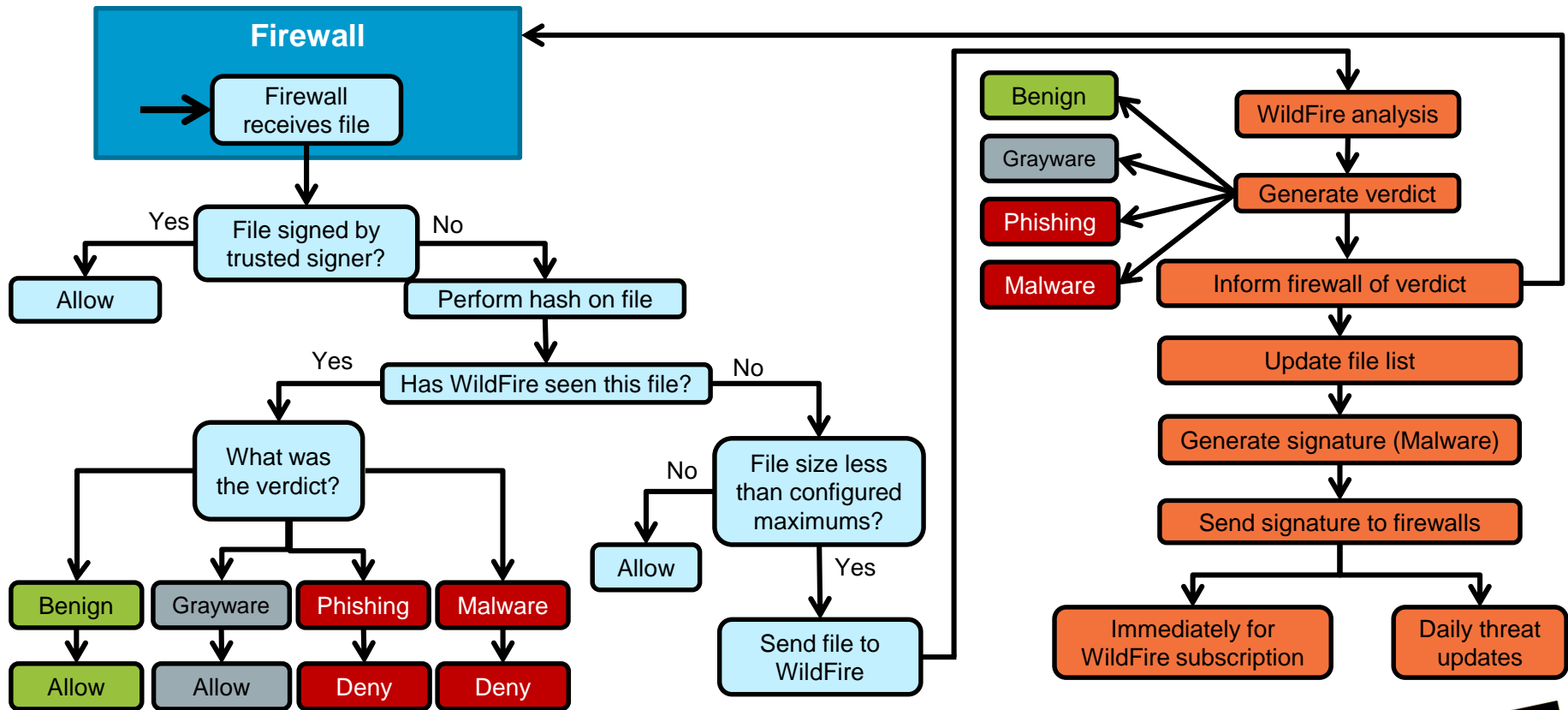
Configuring and managing WildFire

WildFire reporting

WildFire Threat Intelligence Cloud



WildFire Operation Overview

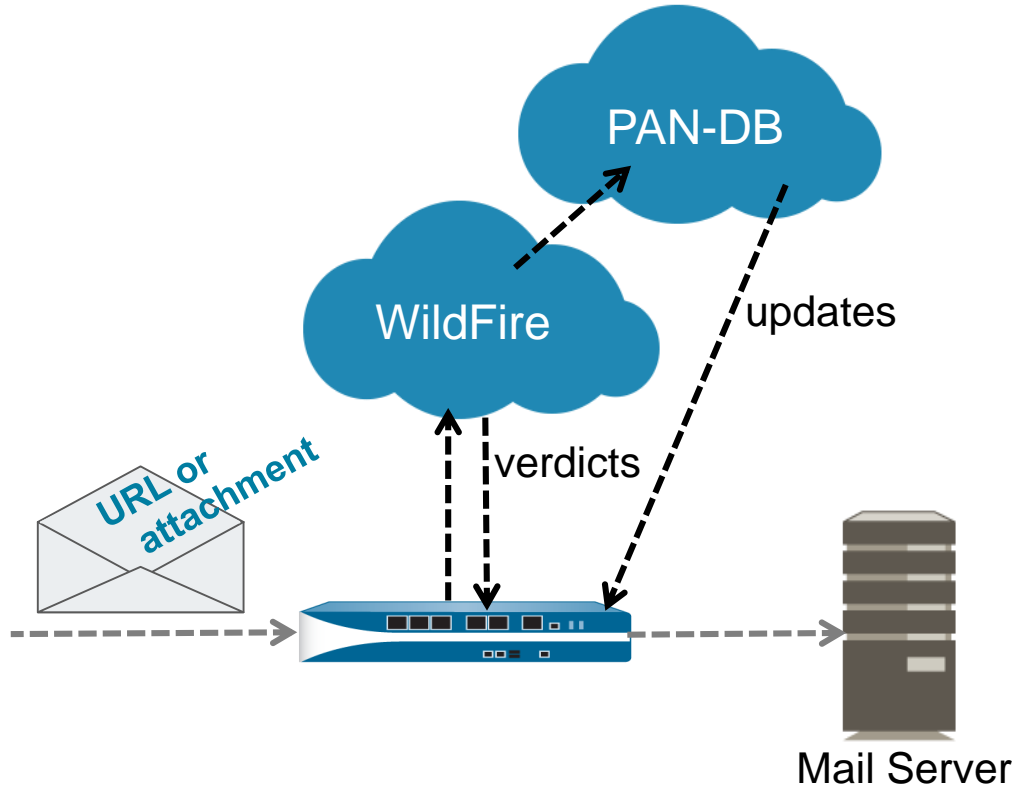


WildFire Verdict Descriptions

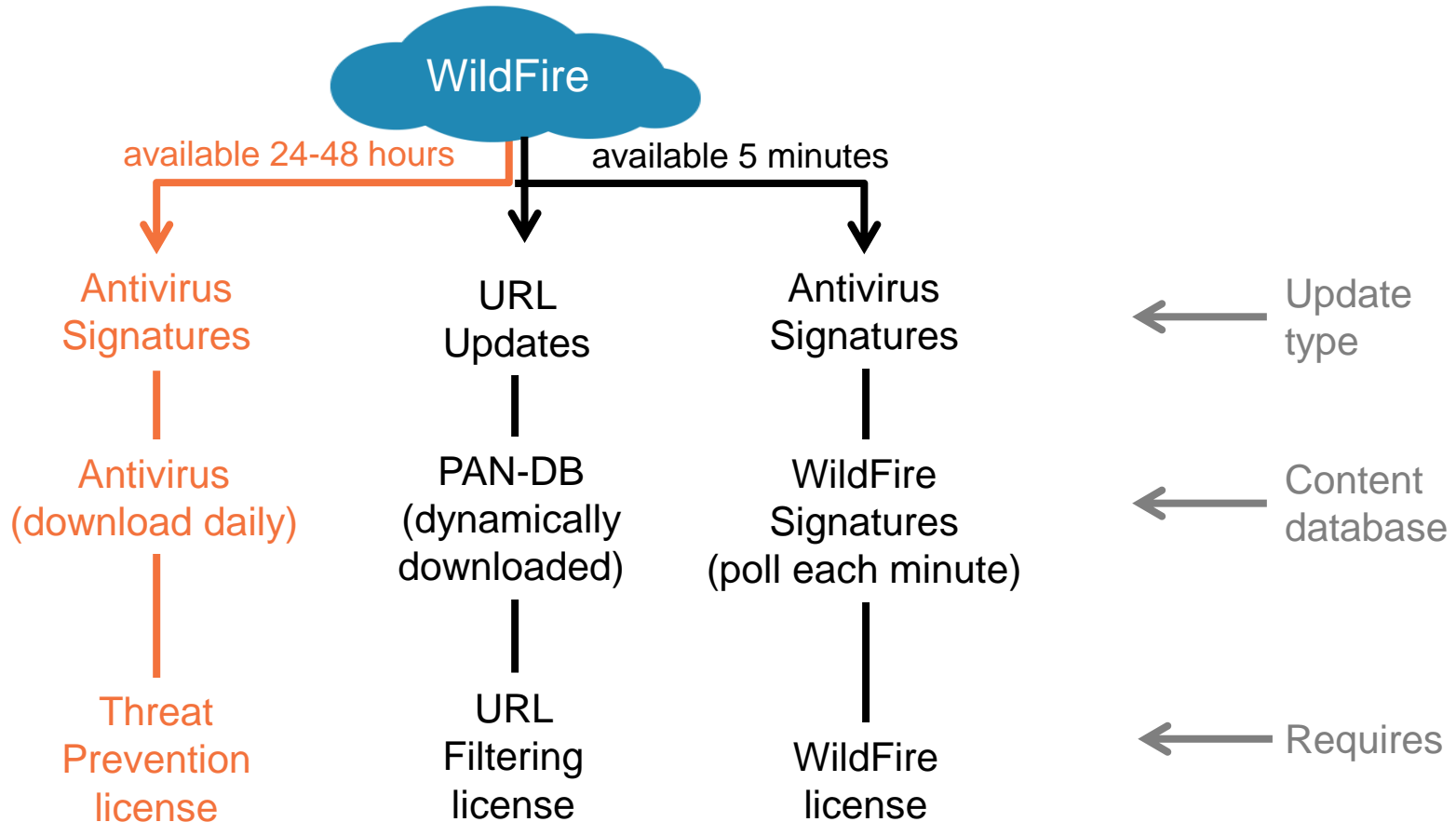
Verdict	Description
Benign	<ul style="list-style-type: none">▪ Safe and does not exhibit malicious behavior
Grayware	<ul style="list-style-type: none">▪ No security threat but might display obtrusive behavior▪ Examples include adware, spyware, and browser helper objects (BHOs)
Malware	<ul style="list-style-type: 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">▪ Based on properties and behaviors the website displays

WildFire Protects Email

- Email with attachments or URL links 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:

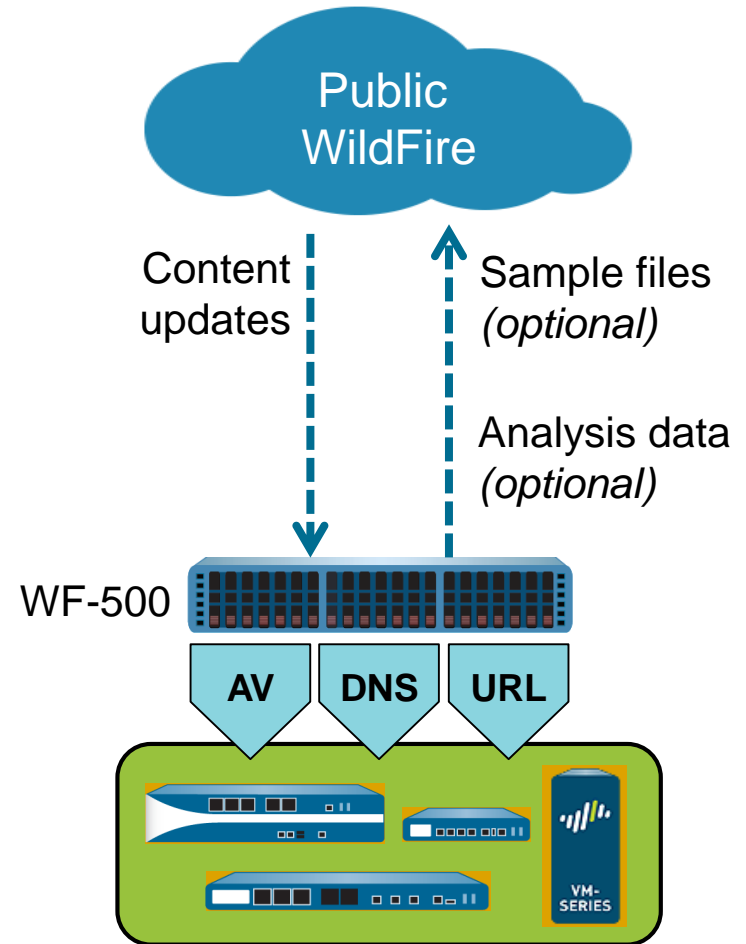
- Windows XP, 7 and 10 analysis
- Windows PE file analysis:
 - EXE, DLL, FON, SCR, others
- Antivirus signatures delivered via daily dynamic content updates (requires Threat Prevention license)
- Automatic file submission

WildFire licensed service:

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

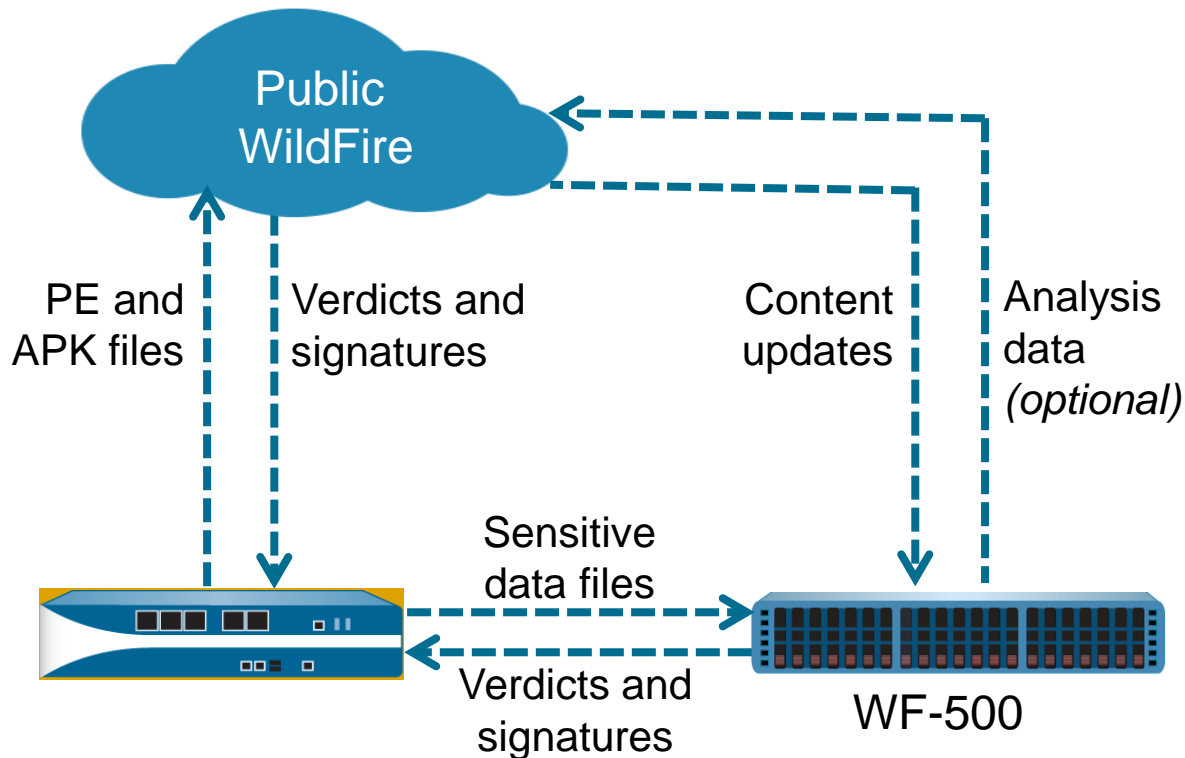
WildFire Private Cloud

- 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



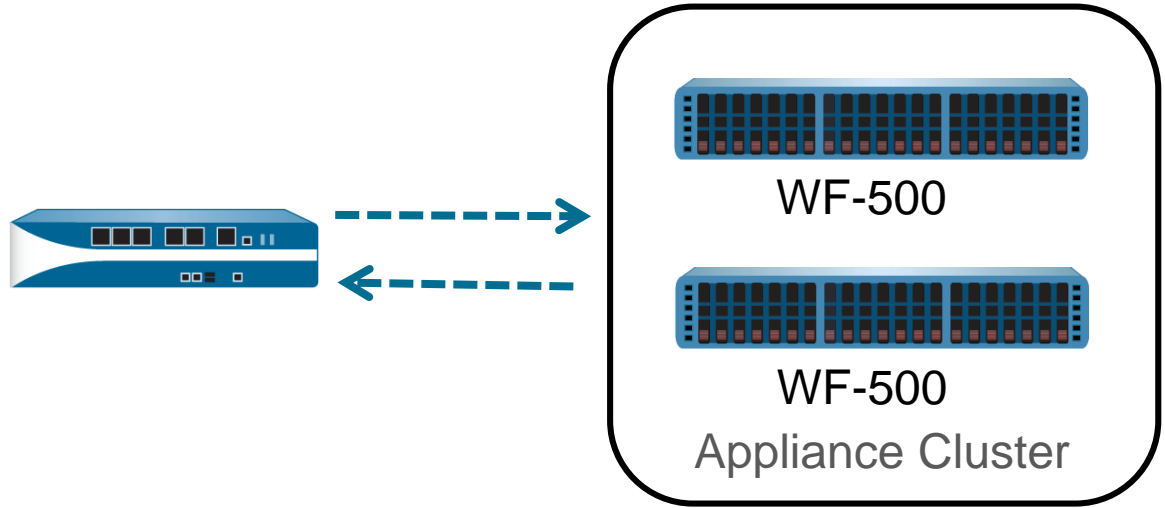
Hybrid Cloud Example

- 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

Configuring and managing WildFire

WildFire reporting

Configuring 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

Public and private hybrid solution configured

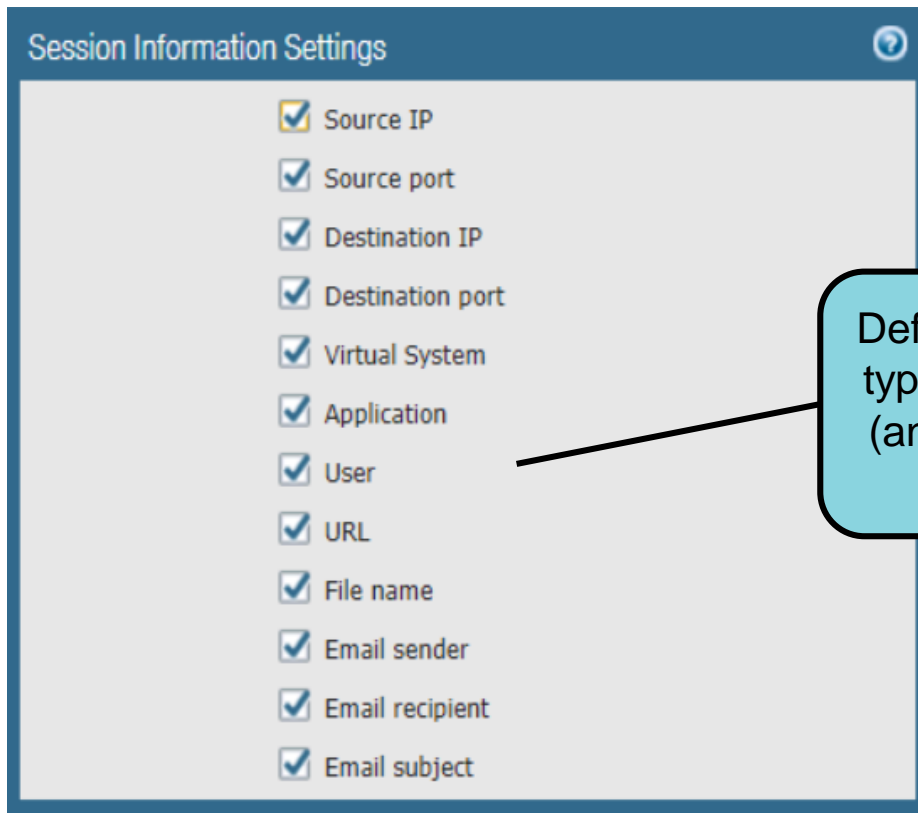
Files that exceed size are not forwarded to WildFire.

Benign and grayware files appear in WildFire Submissions log.

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

Submission Settings

Device > Setup > WildFire



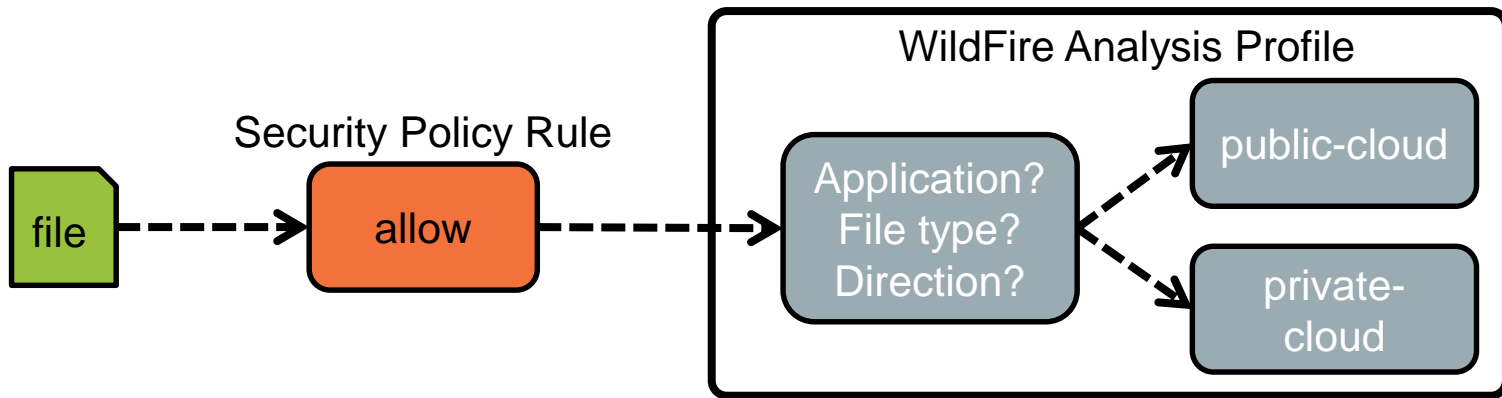
The screenshot shows a configuration window titled "Session Information Settings" with a help icon in the top right corner. Inside the window, there is a list of session information types, each with a checked checkbox. A line from a callout box points to the "User" checkbox.

Session Information Type	Selected
Source IP	Yes
Source port	Yes
Destination IP	Yes
Destination port	Yes
Virtual System	Yes
Application	Yes
User	Yes
URL	Yes
File name	Yes
Email sender	Yes
Email recipient	Yes
Email subject	Yes

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

WildFire Analysis Profile

- Profile implements additional security checks on files in allowed traffic.



WildFire Analysis Profile (Cont.)

Objects > Security Profiles > WildFire Analysis

<input type="checkbox"/>	Name	Location	Rule Name	Applications	File Types	Direction	Analysis
<input type="checkbox"/>	default	Predefined	default	any	any	both	public-cloud
<div>+ Add - Delete 🔄 Clone</div>							

Out-of-the-box profile

Default rule sends all unknown files allowed by the Security policy rule to the WildFire public cloud.

- To create customized profiles:
 - Clone the default read-only profile and edit the clone, or
 - Add a new profile

Creating a WildFire Analysis Profile

Objects > Security Profiles > WildFire Analysis > Add

WildFire Analysis Profile

Name

send-for-WildFire-analysis

Description

4 items

<input type="checkbox"/>	Name	Applications	File Types	Direction	Analysis
<input type="checkbox"/>	apk files	any	apk	both	public-cloud
<input type="checkbox"/>	safe for public	any	flash jar pe	both	public-cloud
<input type="checkbox"/>	check mail	any	email-link	both	public-cloud
<input type="checkbox"/>	not safe for public	any	ms-office	both	private-cloud

+ Add

- Delete

Attaching WildFire Analysis Profiles to Security Rules

Policies > Security > Add

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

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: My Strict Profiles

- Assign WildFire Analysis Profile to security rule
- Add WildFire Analysis Profile to Group Profile and add group to security 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 into the daily Antivirus content package.

Device > Dynamic Updates

▼ WildFire Last checked: 2019/02/26 00:08:02 UTC

Schedule: **Every minute (Download and Install)**

326382-329057	panupv2-all-wildfire-326382-329057	PAN OS 7.1 And Later	Full	8 MB	2019/02/26 00:07:07 UTC	✓ previously		Revert	Release Notes	✕
326383-329058	panupv2-all-wildfire-326383-329058	PAN OS 7.1	Full	8 MB	2019/02/26 00:12:06	✓	✓		Release Notes	✕

WildFire Update Schedule

Recurrence: Every Minute

Action: download-and-install

Cancel

None
download-only
download-and-install

Every Minute
Every 15 Minutes
Every 30 Minutes
Every Hour
None

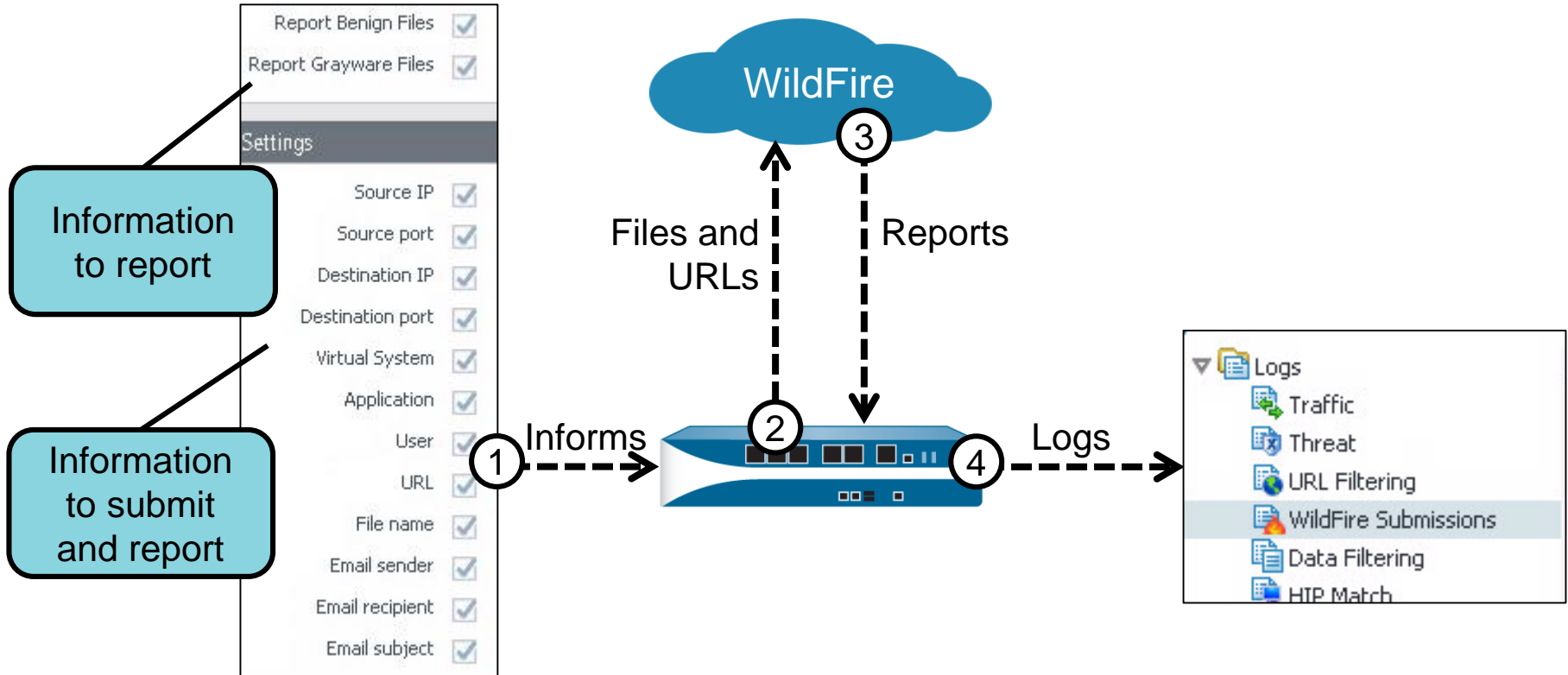


WildFire concepts

Configuring and managing WildFire

WildFire reporting

WildFire Reporting



Verifying Submissions and Viewing Reports




```
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:
- `debug wildfire upload-log show`
- View returned report information

Monitor > Logs > WildFire Submissions

	Receive Time	File Name	Source Zone	Destination Zone	Source address	Destination address	Desti... Port	Application	Rule	Verdict	Action
	02/22 01:31:47	fix832922.ms	danger	danger	10.12.1.101	194.58.100.59	80	web-browsing	danger-simulated-traffic	malicious	block
	02/22 01:31:47	89yg7g87byi	danger	danger	10.5.3.101	72.52.179.2	80	web-browsing	danger-simulated-traffic	malicious	block
	02/22 01:31:47	locky.exe	danger	danger	10.10.10.10	192.168.1.121	25	smtp	danger-simulated-traffic	malicious	allow

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	
SHA-256	885393f832f0eb5c97e470419e0858e858f7b00545f66668c33a9846788b1d18
SHA1	b415dd29d07ea57be1da428e431fc9732058c061
MD5	0a5fac5e7053f0b849e207e9dd532192
File Size	793600 bytes
First Seen Timestamp	2016-12-01 21:44:28 UTC
Verdict	malware
Sample File	Download File

Download a PDF version of the report

Download a copy of the file

PCAP	Receive Time ▲	Type	Application	Action	Rule	UUID	Byt...	Severity	Categ...	URL Categ... List	Verdict	URL	File Name
	2019/02/22 01:31:47	wildfire	web-browsing	block	danger-simula... traffic	b6668...		informatio...			malicious		fix832...

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	f05e65feb12ea9d76962477a10280121d6c476555da730e51f a2ef10ad47929b
MD5	1af3782eae55eaf7fe65ed424419ac7
Verdict	malware

Additional Information

Suggested verdict: **Grayware**

Your email address: **Grayware**

Future correspondence 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 request to Palo Alto Networks:
 - From web interface or WildFire portal
- From web interface:
 - Select Monitor > Logs > WildFire Submissions.
 - Find entry and click its detailed view icon.
 - Click WildFire Analysis Report tab.
 - Click Select Incorrect Verdict link.
 - Suggest new verdict.

WildFire Portal

<https://wildfire.paloaltonetworks.com>

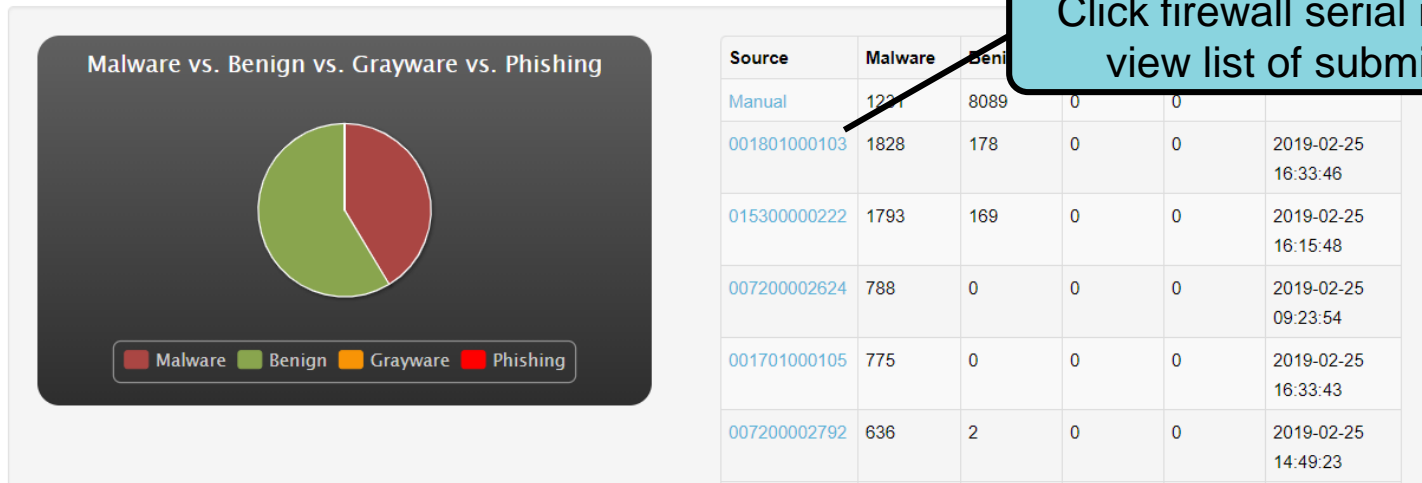


WILDFIRE



DASHBOARD

PREVIOUS 1 HOUR



Click firewall serial number to view list of submissions.



WildFire Dashboard Reports

The screenshot displays the Palo Alto Networks WildFire dashboard. The top navigation bar includes the Palo Alto Networks logo and the word 'WILDFIRE' in green. The main header shows 'Dashboard' and 'Reports' tabs. The 'Reports' tab is active, showing a search bar and a table of reports. The table has columns for 'Received Time', 'Status', and 'File Name'. A report for 'AxwNRxSaB.EXE' is highlighted, and a modal window displays its details.

WILDFIRE ANALYSIS REPORT

FILE INFORMATION

File Type	PE
File Signer	
SHA-256	c85c8c02236802f8447262d7d0a7023d3536cfe461a97b473885bcd00feba51d
MD5	76237a5f124445a052ad56e592b3acef
File Size	14848 bytes
First Seen Timestamp	2011-08-14 19:22:24 PST
Sample File	Download File
Verdict	Malware (Updated on 2015-10-15)

SESSION INFORMATION

File Source	10.154.228.79:21465
-------------	---------------------




Verdict

Benign
Benign
Pending
Benign
Benign
Pending
Pending
Malware

Report Incorrect Verdict: WildFire Portal

REPORTS

Source Any

	Received Time	Source	File / URL
	2019-02-25 16:35:38	Manual	
	2019-02-25 16:35:37	Manual	
	2019-02-25 16:35:37	Manual	wfc7348313562913238292scan

REPORT INCORRECT VERDICT

SAMPLE INFORMATION

SHA-256	f45cc1ea843737517778a839c0fa5536f68d5067305908440778500495aec189
MD5	d1b15d00f39cb9f166219ad11152c72c
Verdict	Benign

ADDITIONAL INFORMATION

Suggested verdict: Malware

Email:

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

Please include any comments that may help us understand the issue:

Cancel Submit

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 how a firewall works with the WildFire Threat Intelligence Cloud
- Describe how WildFire analysis is used to update URL categories listed in the PAN-DB URL Filtering database
- Configure Session Information Settings to specify which type of session information will be sent to WildFire
- Define a WildFire Analysis Profile
- Configure both the types of information submitted to WildFire and the amount of information that is returned to the firewall in the report

Questions?



WildFire Lab (Pages 163-169 in the Lab Guide)

- Load a firewall lab configuration
- Create and test a WildFire Analysis Profile

PROTECTION. DELIVERED.



This page intentionally left blank