FORTINET
Training Institute

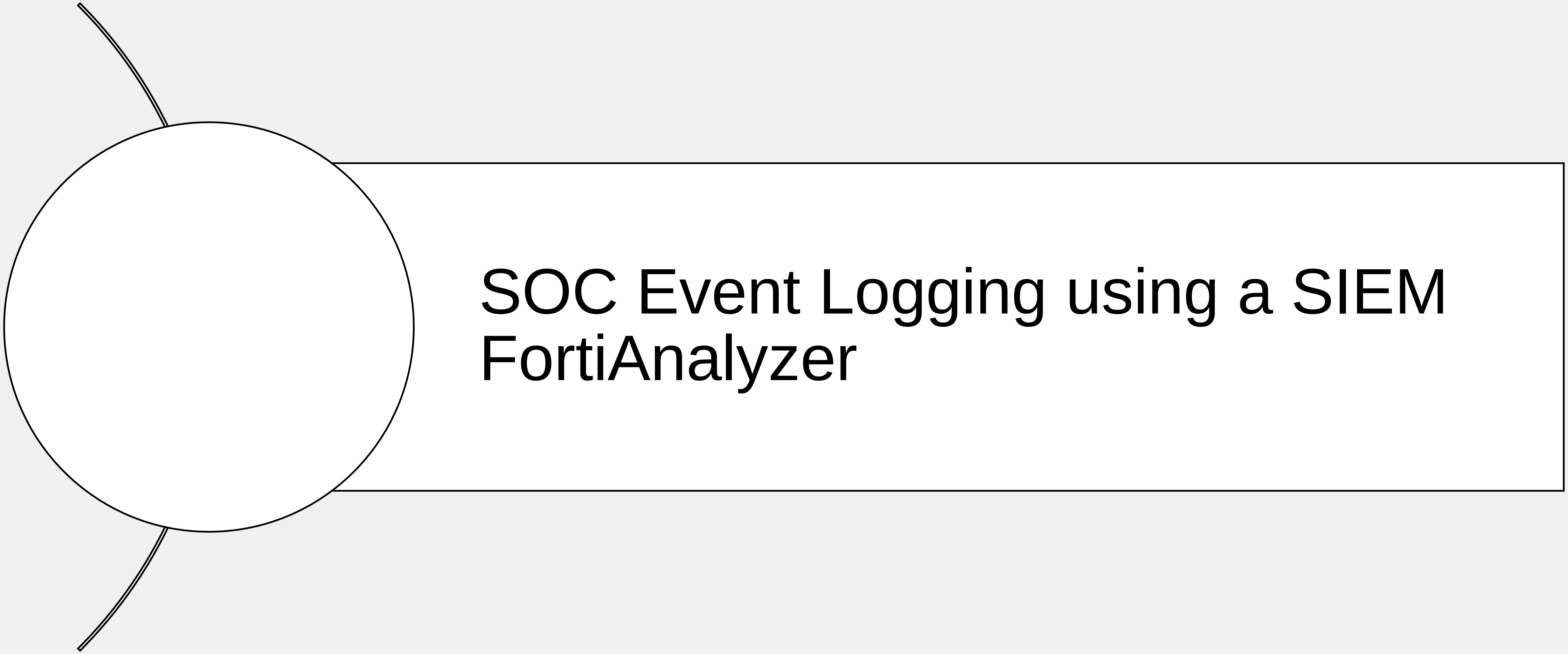
FORTINET
CERTIFIED
SOLUTION
SPECIALIST
Security
Operations

Security Operations Analyst

FortiAnalyzer Architecture

Last Modified: 21 January 2025

Lesson Overview



SOC Event Logging using a SIEM FortiAnalyzer

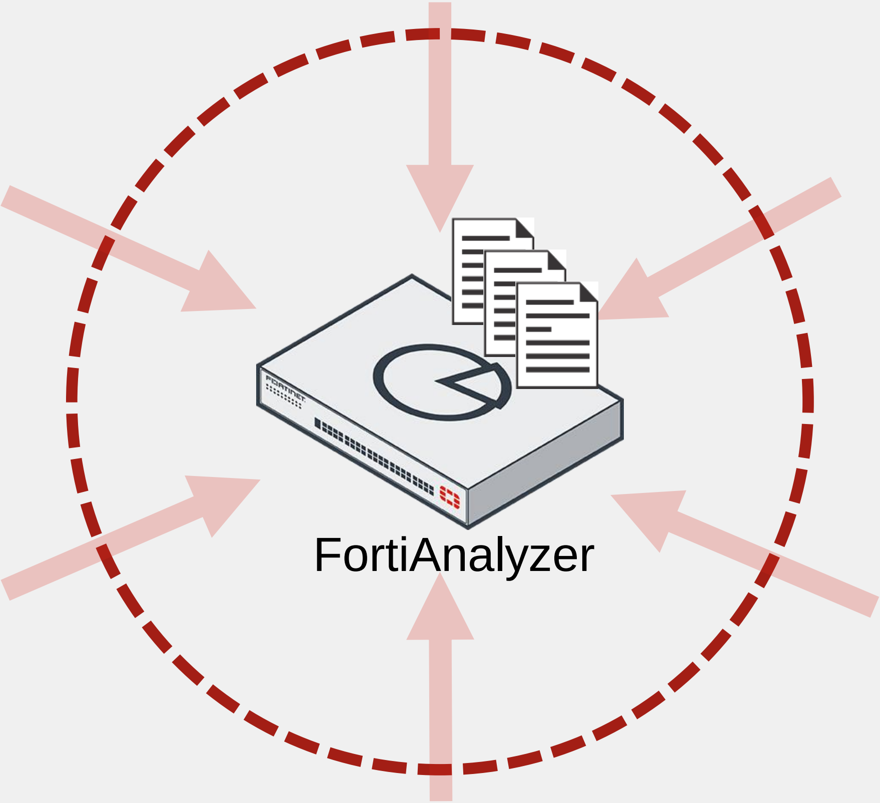
FortiAnalyzer Architecture

Objectives

- Describe the purpose of FortiAnalyzer in a SOC
- Describe administrative domains (ADOMs)

Centralized Log Repository

- FortiAnalyzer aggregates log data from one or more Fortinet devices
- Single view of security events taking place on a range of devices



Supported devices:

- FortiGate/FortiCarrier
- FortiAnalyzer
- FortiAuthenticator
- FortiCache
- FortiClient
- FortiDDoS
- FortiMail
- FortiManager
- FortiNAC
- FortiSandbox
- FortiWeb
- Syslog
- Chassis

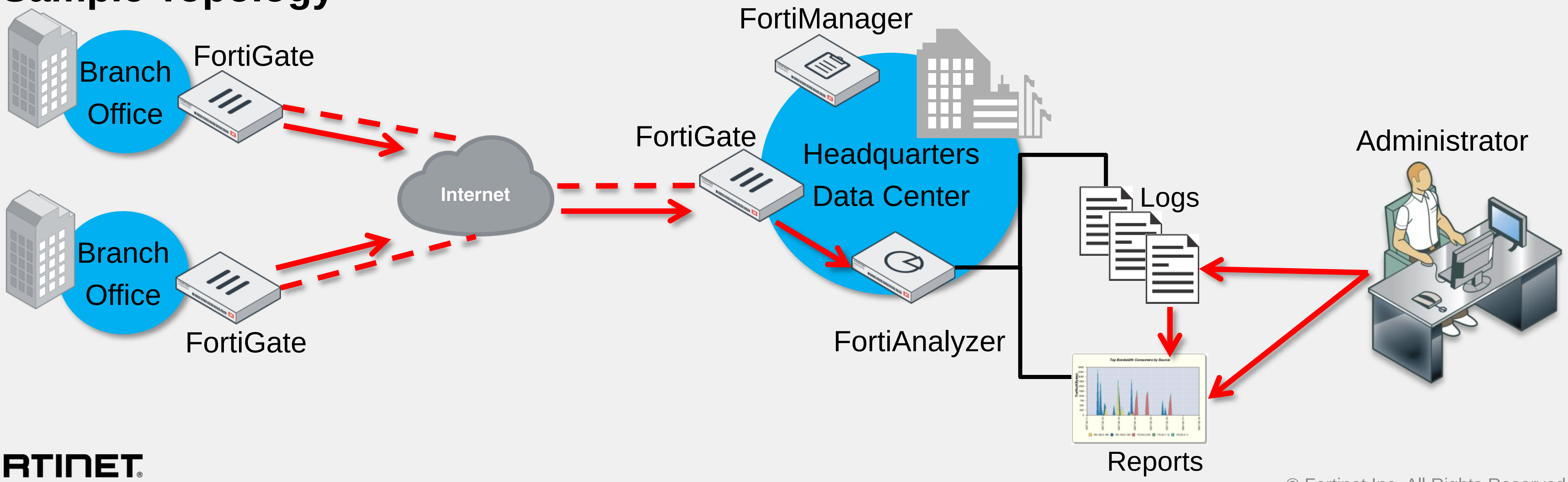
Note: The list is not exhaustive

Centralized Log Repository (Contd)

Workflow

1. Registered devices send logs to FortiAnalyzer
2. FortiAnalyzer buffers, reorganizes, and stores the logs
3. Administrators:
   - View and search the logs
   - Configure, request, and view reports (based on log data)

Sample Topology



FORTINET
Training Institute

Reports, Events, and Content Archiving

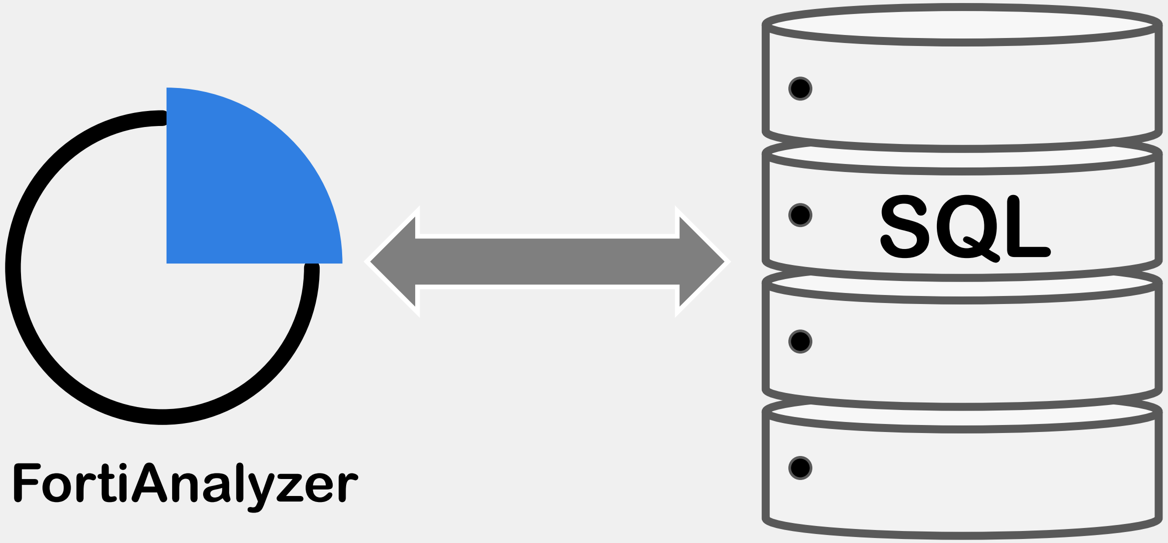
- **Reports**
  - Network-wide reporting of device events, activities, and trends
  - Archived, filtered, and mined for compliance or historical analysis purposes

- **Events**
  - Identify and react to security threats quickly when configured conditions are met
  - View events through **Event Monitor** (on the GUI), email, SNMP, or syslog
  - Events that require further investigation can be used to generate new incidents

- **Content archiving**
  - Simultaneously logs and archives full or summary copies of content transmitted over the network (email, FTP, NNTP, and web traffic)
  - Typically used to prevent sensitive information from leaving your network

Database Language Support

- FortiAnalyzer supports Structured Query Language (SQL) for logging and reporting
- FortiAnalyzer inserts log data into the SQL database for log view and report generation
- FortiAnalyzer uses a PostgreSQL database
- *Advanced reporting capabilities require some knowledge of SQL and databases*



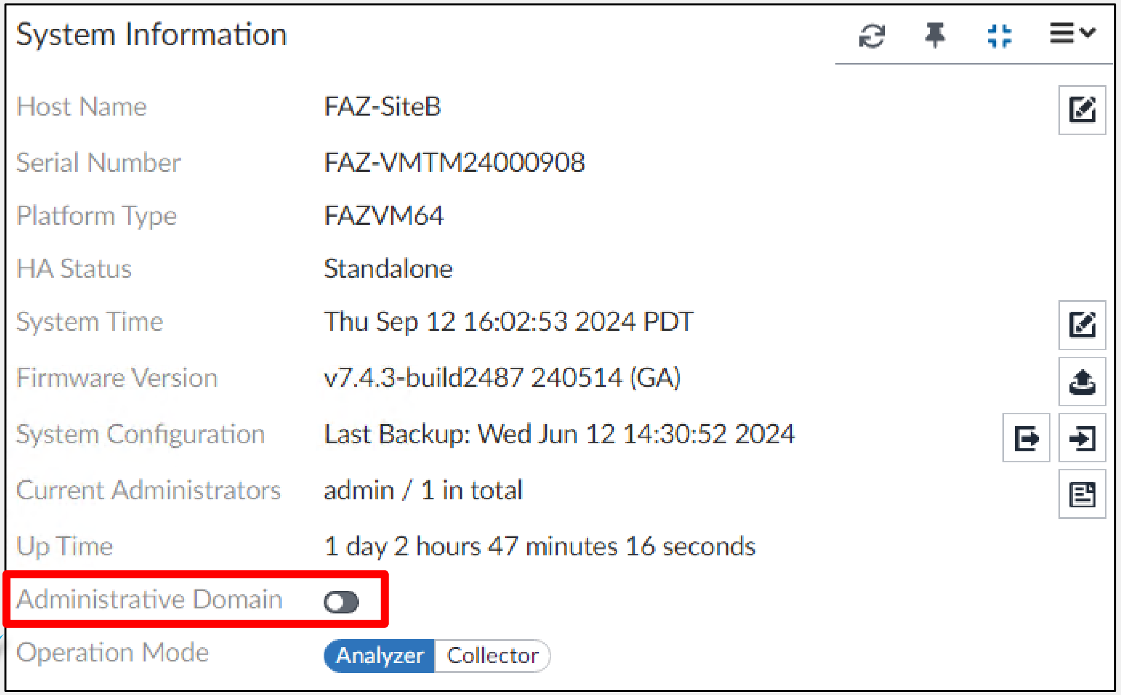
ADOMs

- ADOMs group devices for administrators to monitor and manage
  - One or more devices are assigned to ADOMs and administrators are assigned to administer one or more ADOMs

- Purpose:
  - To divide administration of devices and restrict access
    - VDOMs, a feature of FortiGate, further restrict access
  - To more efficiently manage data policies and disk space allocation
    - Set for each ADOM (not for each device)

ADOMs are not enabled by default

Dashboard > System Information

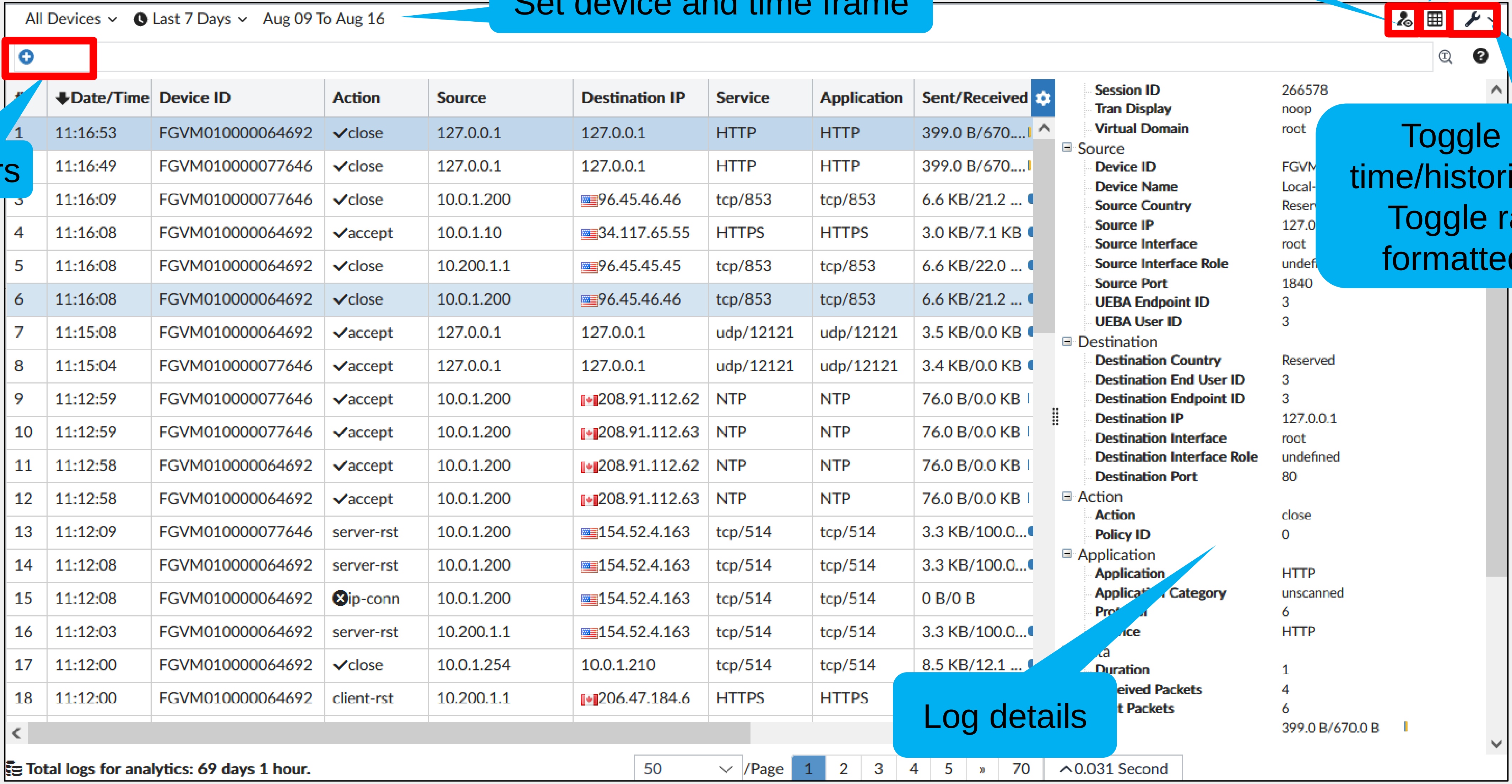


System Information

Host Name	FAZ-SiteB
Serial Number	FAZ-VMTM24000908
Platform Type	FAZVM64
HA Status	Standalone
System Time	Thu Sep 12 16:02:53 2024 PDT
Firmware Version	v7.4.3-build2487 240514 (GA)
System Configuration	Last Backup: Wed Jun 12 14:30:52 2024
Current Administrators	admin / 1 in total
Up Time	1 day 2 hours 47 minutes 16 seconds
Administrative Domain	○
Operation Mode	Analyzer Collector

```
# config system global
   set adom-status {enable | disable}
  end
```

Logging Interface Overview



Set device and time frame

Custom view

Column options

Set filters

Toggle real-time/historical logs
Toggle raw or formatted logs

Log details

#	Date/Time	Device ID	Action	Source	Destination IP	Service	Application	Sent/Received
1	11:16:53	FGVM010000064692	✓close	127.0.0.1	127.0.0.1	HTTP	HTTP	399.0 B/670....
	11:16:49	FGVM010000077646	✓close	127.0.0.1	127.0.0.1	HTTP	HTTP	399.0 B/670....
3	11:16:09	FGVM010000077646	✓close	10.0.1.200	96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 ...
4	11:16:08	FGVM010000064692	✓accept	10.0.1.10	34.117.65.55	HTTPS	HTTPS	3.0 KB/7.1 KB
5	11:16:08	FGVM010000064692	✓close	10.200.1.1	96.45.45.45	tcp/853	tcp/853	6.6 KB/22.0 ...
6	11:16:08	FGVM010000064692	✓close	10.0.1.200	96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 ...
7	11:15:08	FGVM010000064692	✓accept	127.0.0.1	127.0.0.1	udp/12121	udp/12121	3.5 KB/0.0 KB
8	11:15:04	FGVM010000077646	✓accept	127.0.0.1	127.0.0.1	udp/12121	udp/12121	3.4 KB/0.0 KB
9	11:12:59	FGVM010000077646	✓accept	10.0.1.200	208.91.112.62	NTP	NTP	76.0 B/0.0 KB
10	11:12:59	FGVM010000077646	✓accept	10.0.1.200	208.91.112.63	NTP	NTP	76.0 B/0.0 KB
11	11:12:58	FGVM010000064692	✓accept	10.0.1.200	208.91.112.62	NTP	NTP	76.0 B/0.0 KB
12	11:12:58	FGVM010000064692	✓accept	10.0.1.200	208.91.112.63	NTP	NTP	76.0 B/0.0 KB
13	11:12:09	FGVM010000077646	server-rst	10.0.1.200	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0...
14	11:12:08	FGVM010000064692	server-rst	10.0.1.200	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0...
15	11:12:08	FGVM010000064692	⊗ip-conn	10.0.1.200	154.52.4.163	tcp/514	tcp/514	0 B/0 B
16	11:12:03	FGVM010000064692	server-rst	10.200.1.1	154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0...
17	11:12:00	FGVM010000064692	✓close	10.0.1.254	10.0.1.210	tcp/514	tcp/514	8.5 KB/12.1 ...
18	11:12:00	FGVM010000064692	client-rst	10.200.1.1	206.47.184.6	HTTPS	HTTPS	

Session ID	266578
Tran Display	noop
Virtual Domain	root
⊟ Source	
Device ID	FGVM
Device Name	Local-
Source Country	Reser
Source IP	127.0
Source Interface	root
Source Interface Role	undef
Source Port	1840
UEBA Endpoint ID	3
UEBA User ID	3
⊟ Destination	
Destination Country	Reserved
Destination End User ID	3
Destination Endpoint ID	3
Destination IP	127.0.0.1
Destination Interface	root
Destination Interface Role	undefined
Destination Port	80
⊟ Action	
Action	close
Policy ID	0
⊟ Application	
Application	HTTP
Applicati Category	unscanned
Prot l	6
ice	HTTP
ta	
Duration	1
eived Packets	4
t Packets	6
	399.0 B/670.0 B

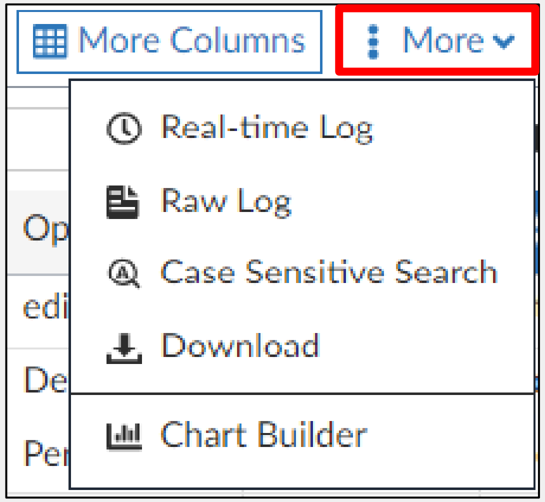
Total logs for analytics: 69 days 1 hour.

50 /Page 1 2 3 4 5 » 70 0.031 Second

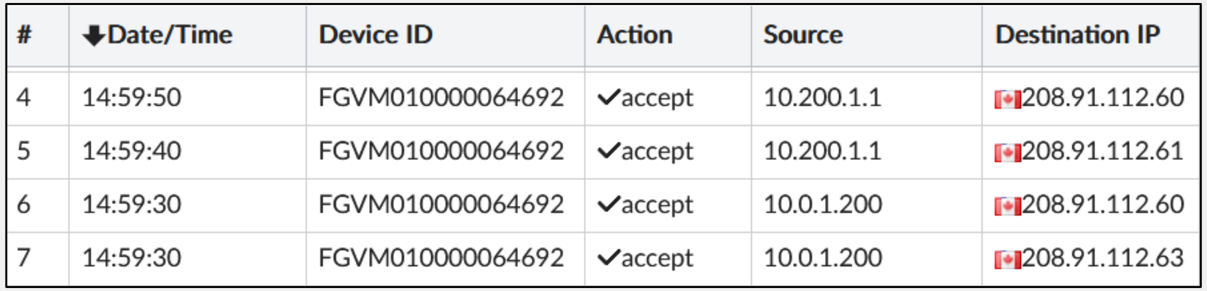
Training Institute

Tools

- Toggle between **formatted/raw** logs
  - Formatted logs are sortable and columns can be customized
  - Raw logs are more difficult to read, but can be useful in providing syntax guidance
- Toggle between **historical/real-time** logs
  - View historical logs with the option to specify a time period
  - Real-time logs are shown as they come in, but you can pause them
- Enable/disable case-sensitive search
- Download logs based on the current filters

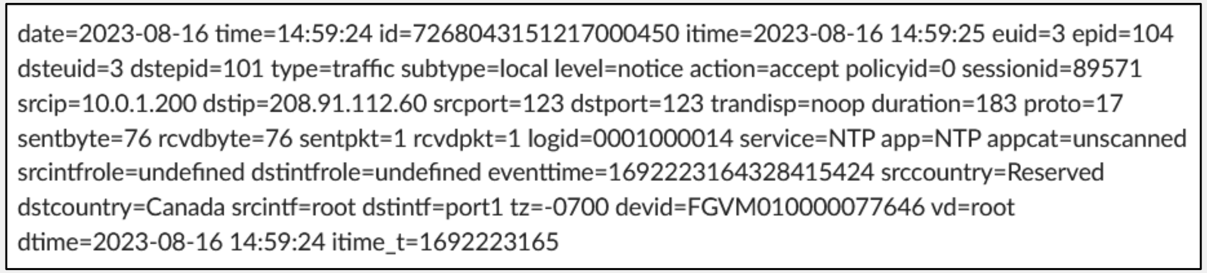


Formatted



#	Date/Time	Device ID	Action	Source	Destination IP
4	14:59:50	FGVM010000064692	✓accept	10.200.1.1	208.91.112.60
5	14:59:40	FGVM010000064692	✓accept	10.200.1.1	208.91.112.61
6	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.60
7	14:59:30	FGVM010000064692	✓accept	10.0.1.200	208.91.112.63

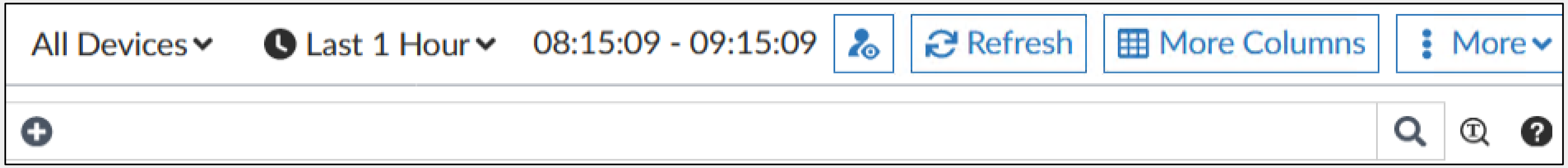
Raw



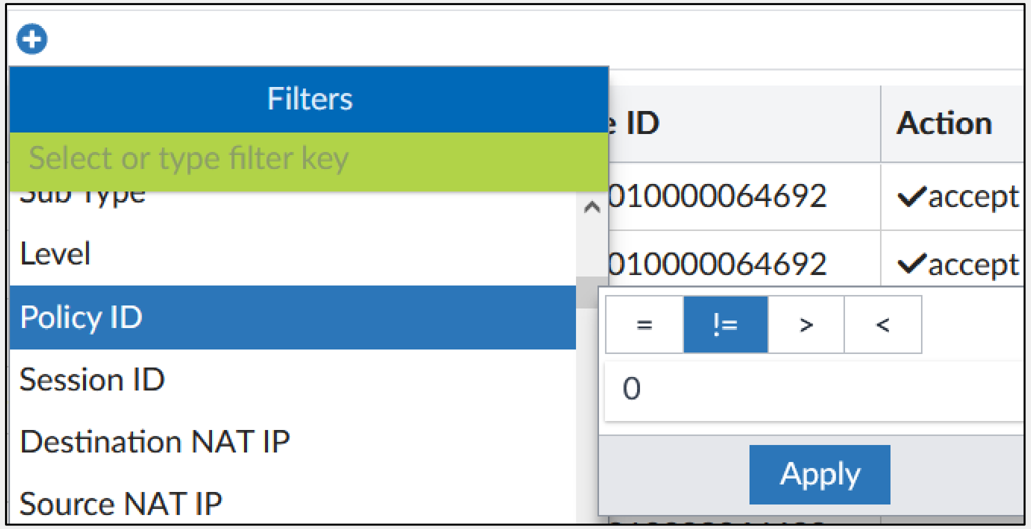
```
date=2023-08-16 time=14:59:24 id=7268043151217000450 itime=2023-08-16 14:59:25 euid=3 epid=104
dsteuid=3 dstepid=101 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=89571
srcip=10.0.1.200 dstip=208.91.112.60 srcport=123 dstport=123 trandisp=noop duration=183 proto=17
sentbyte=76 rcvdbyte=76 sentpkt=1 rcvdpkt=1 logid=0001000014 service=NTP app=NTP appcat=unscanned
srcintfrole=undefined dstintfrole=undefined eventtime=1692223164328415424 srccountry=Reserved
dstcountry=Canada srcintf=root dstintf=port1 tz=-0700 devid=FGVM010000077646 vd=root
dtime=2023-08-16 14:59:24 itime_t=1692223165
```

Search Tips

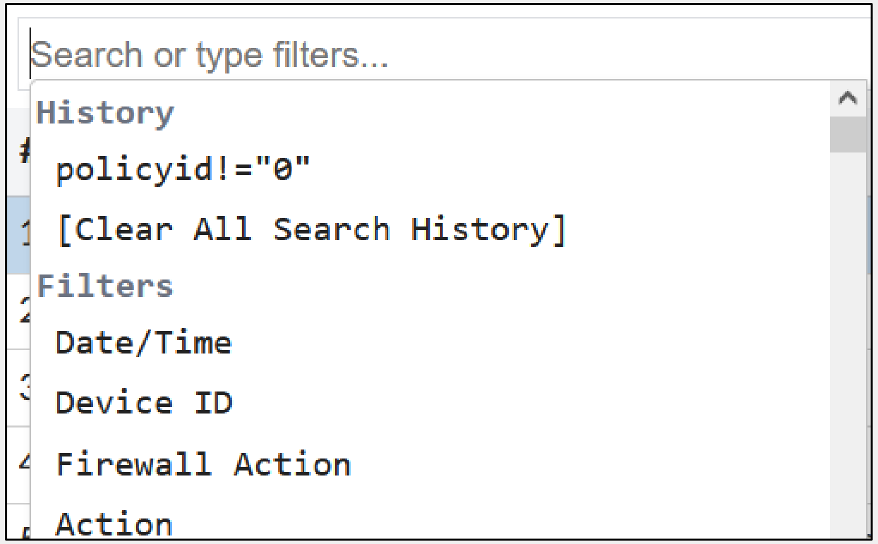
- Click on the magnifying glass to toggle between filter and text mode



- Filter mode allows you to click the filter search bar and define your search criteria using the GUI

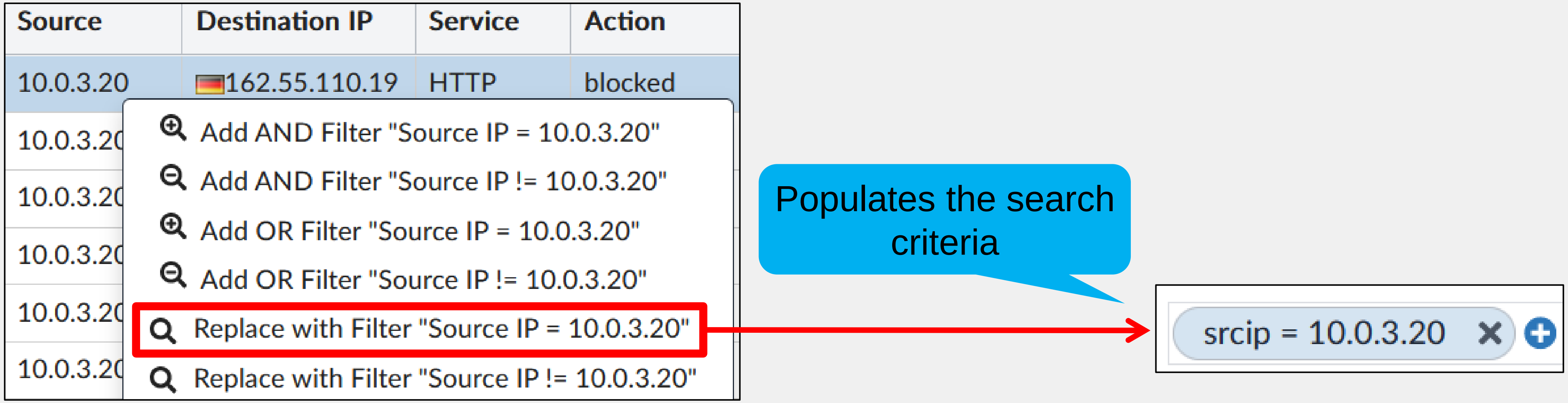


- Text mode allows you to type in your filter and conditions manually, or pick a filter from history



Search Tips (Contd)

- Right-click the desired field value to set a filter based on that data



Source	Destination IP	Service	Action
10.0.3.20	162.55.110.19	HTTP	blocked
10.0.3.20			
10.0.3.20			
10.0.3.20			
10.0.3.20			
10.0.3.20			

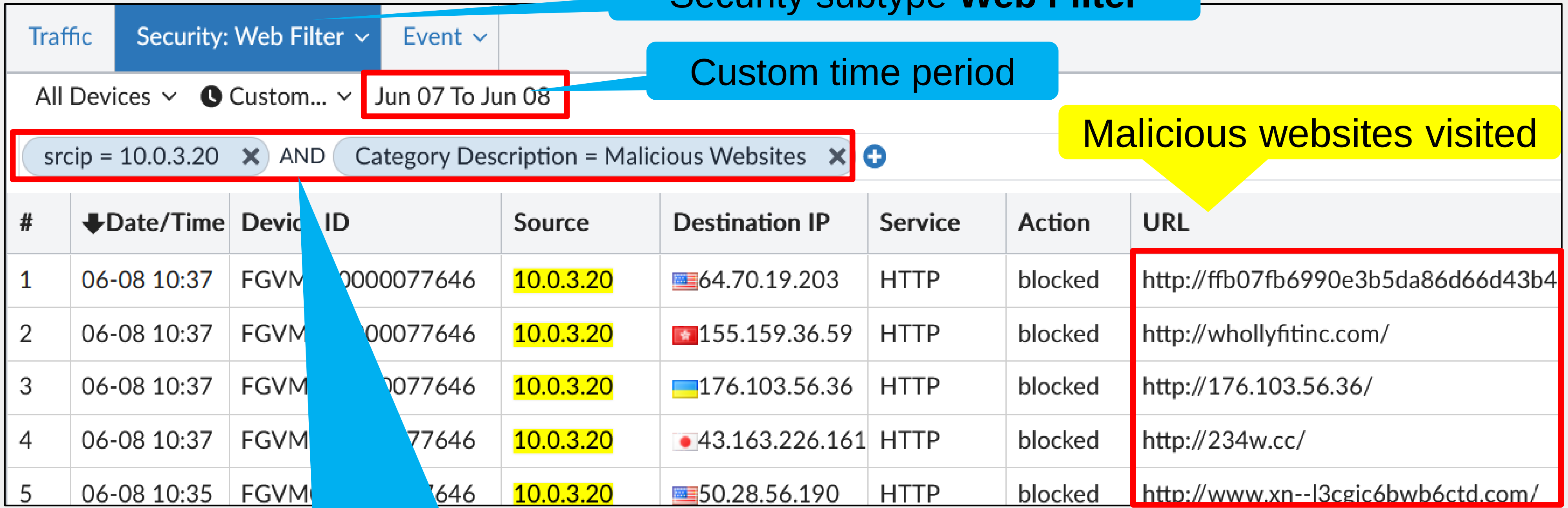
Add AND Filter "Source IP = 10.0.3.20"
Add AND Filter "Source IP != 10.0.3.20"
Add OR Filter "Source IP = 10.0.3.20"
Add OR Filter "Source IP != 10.0.3.20"
Replace with Filter "Source IP = 10.0.3.20"
Replace with Filter "Source IP != 10.0.3.20"
srcip = 10.0.3.20

Populates the search criteria

- Can include (=), or exclude (!=) the selected value from the search results
- Use the AND logic if all conditions must be true
- Use the OR logic if any of the conditions must be true
- Can also replace the current filter with your new conditions

Example of a Log Search

- You need to identify the malicious websites visited by the client with the IP address `10.0.3.20` for a specific time period



Security subtype **Web Filter**

Custom time period

Malicious websites visited

srcip = 10.0.3.20 ✕ AND Category Description = Malicious Websites ✕

#	Date/Time	Devic ID	Source	Destination IP	Service	Action	URL
1	06-08 10:37	FGVM 0000077646	10.0.3.20	64.70.19.203	HTTP	blocked	http://ffb07fb6990e3b5da86d66d43b4
2	06-08 10:37	FGVM 00077646	10.0.3.20	155.159.36.59	HTTP	blocked	http://whollyfitinc.com/
3	06-08 10:37	FGVM 0077646	10.0.3.20	176.103.56.36	HTTP	blocked	http://176.103.56.36/
4	06-08 10:37	FGVM 77646	10.0.3.20	43.163.226.161	HTTP	blocked	http://234w.cc/
5	06-08 10:35	FGVM 646	10.0.3.20	50.28.56.190	HTTP	blocked	http://www.xn--l3cgic6bwb6ctd.com/

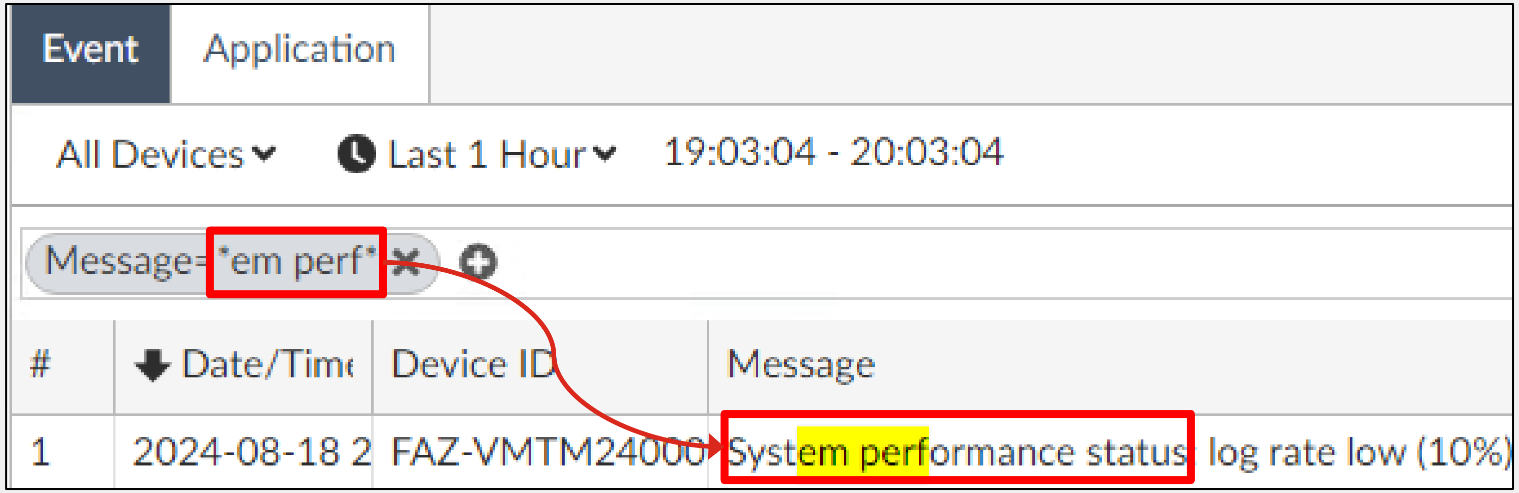
Filters are based on the client's IP as the source, and the category description

Fields used in the filter are highlighted

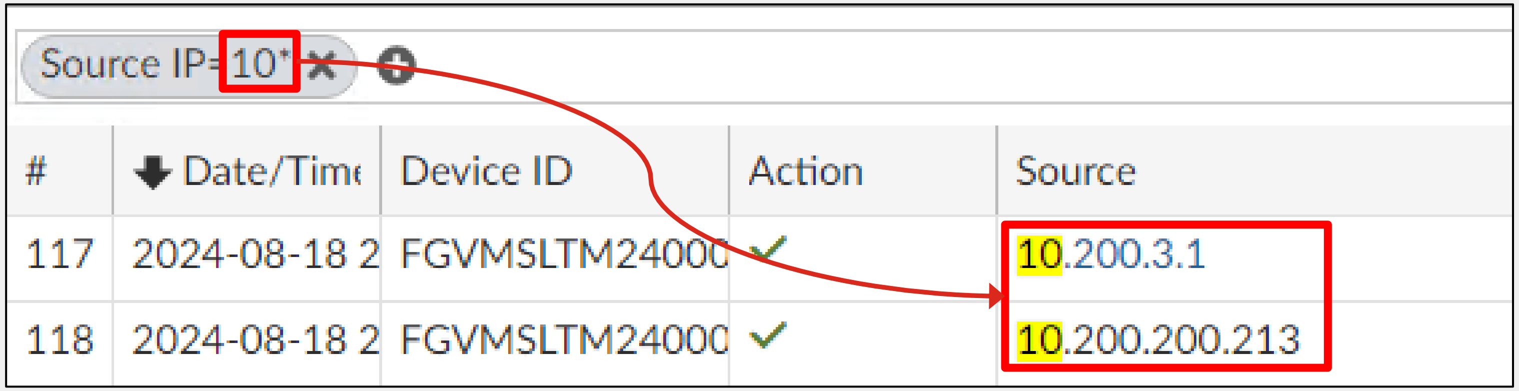
Training Institute

Example of a Log Search (Contd)

- Search also supports wildcards
  - Use * for partial matches, which matches any sequence of characters, including an empty sequence
  - For example, the string `*em perf*` will match **System performance status**



#	Date/Tim	Device ID	Message
1	2024-08-18 2	FAZ-VMTM24000	System performance status log rate low (10%)



#	Date/Tim	Device ID	Action	Source
117	2024-08-18 2	FGVMSLTM24000	✓	10.200.3.1
118	2024-08-18 2	FGVMSLTM24000	✓	10.200.200.213

Regex

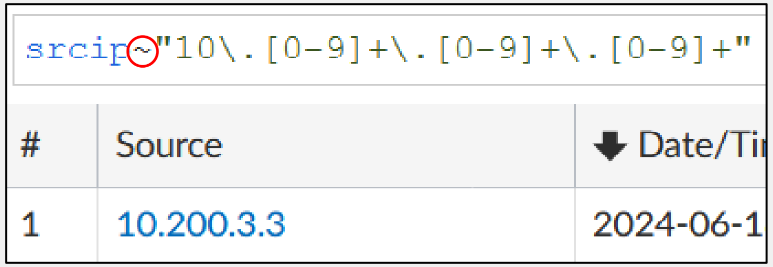
- You can use regex in FortiAnalyzer to search logs or match a generic text filter
- This table lists common regex operators:

Operator	Function	Operator	Function
~	Matches the following regex pattern	+	Matches one or more of the preceding element
!~	Does not match the following regex pattern	\	Character escape for special characters
.	Matches any character	|	Used as an OR operator
[ ]	Matches any one character from a set or range	( )	Used for grouping patterns together so that operators such as +, *, ?, | can be applied to the group
*	Matches zero or more of the preceding element	^	Anchors the pattern to the beginning of the string
?	Matches zero or one of the preceding element	$	Anchors the pattern to the end of the string

Regex (Contd)

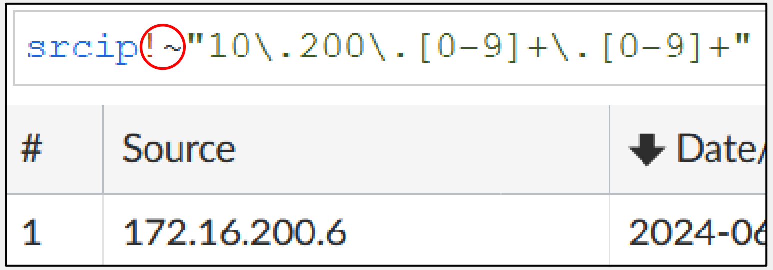
~ matches the regex pattern

!~ does not match the regex pattern (negate logic)



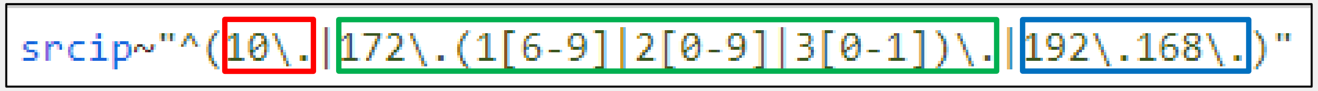
```
srcip~"10\.[0-9]+\.[0-9]+\.[0-9]+"
```

#	Source	Date/Ti
1	10.200.3.3	2024-06-1



```
srcip!~"10\.200\.[0-9]+\.[0-9]+"
```

#	Source	Date/
1	172.16.200.6	2024-06



```
srcip~"^(10\.|172\.(1[6-9]|2[0-9]|3[0-1])\.|192\.168\.)"
```

- Matches private IP address ranges with patterns *beginning* with `10.` OR `172.16-31.` OR `192.168.`

Knowledge Check

1. What does FortiAnalyzer use for log viewing and report generation?
   - ✓ A. Queries on a database
   - B. Queries of plain text files

2. What is the purpose of using ADOMs?
   - ✓ A. To divide administration of devices, restrict access, and manage data policies
   - B. To reduce resource usage on FortiAnalyzer

Review

✓Understand SOC Logging

FORTINET
Training Institute