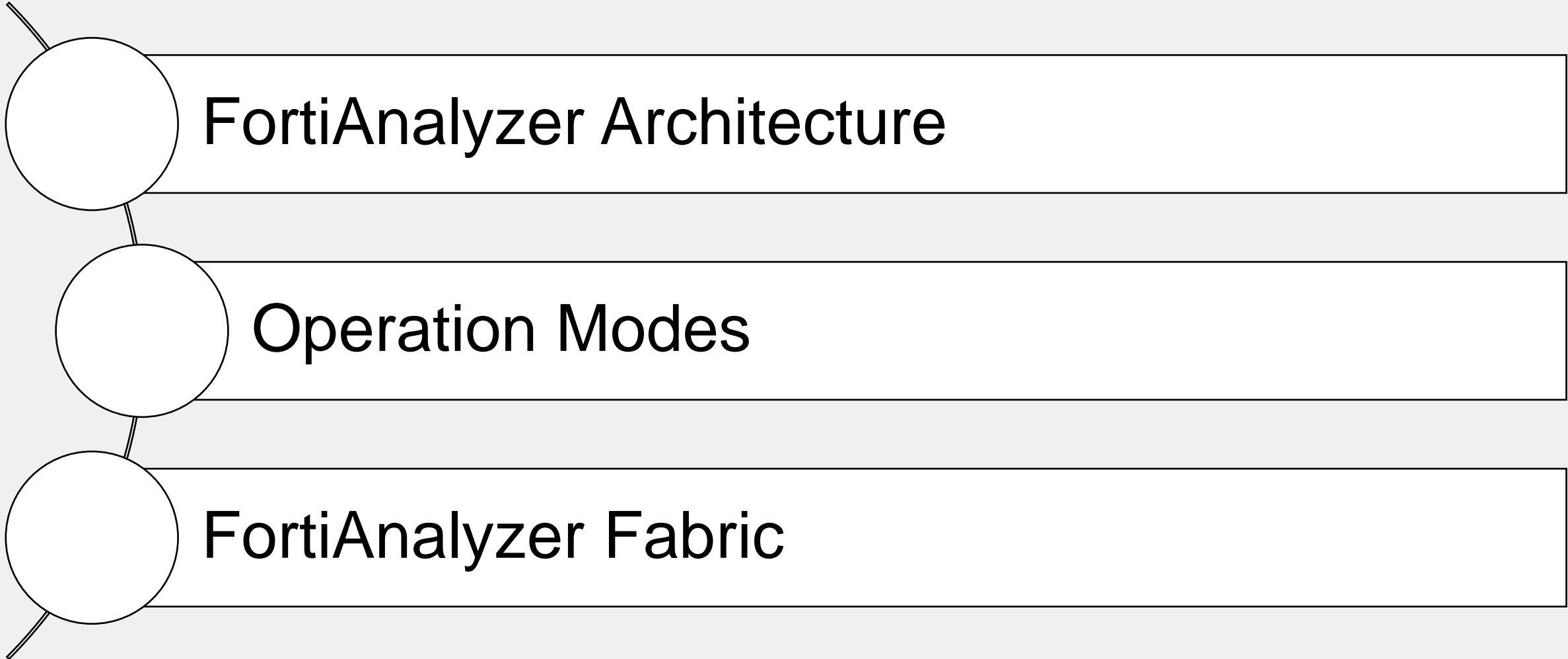



Security Operations Analyst

FortiAnalyzer Architecture

Lesson Overview





FortiAnalyzer Architecture

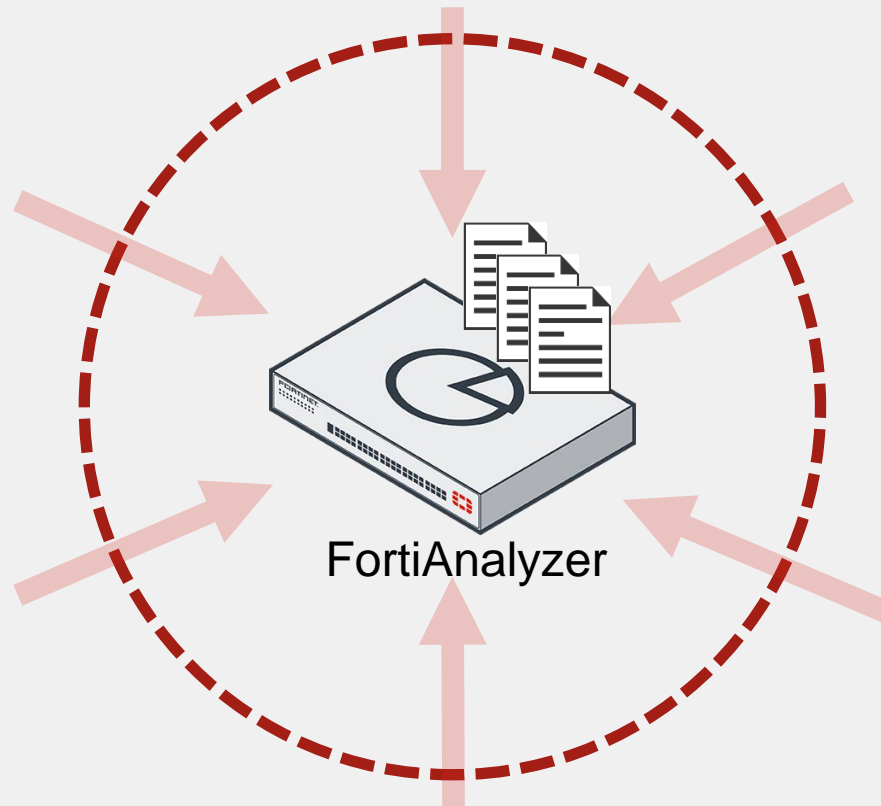


Objectives

- 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

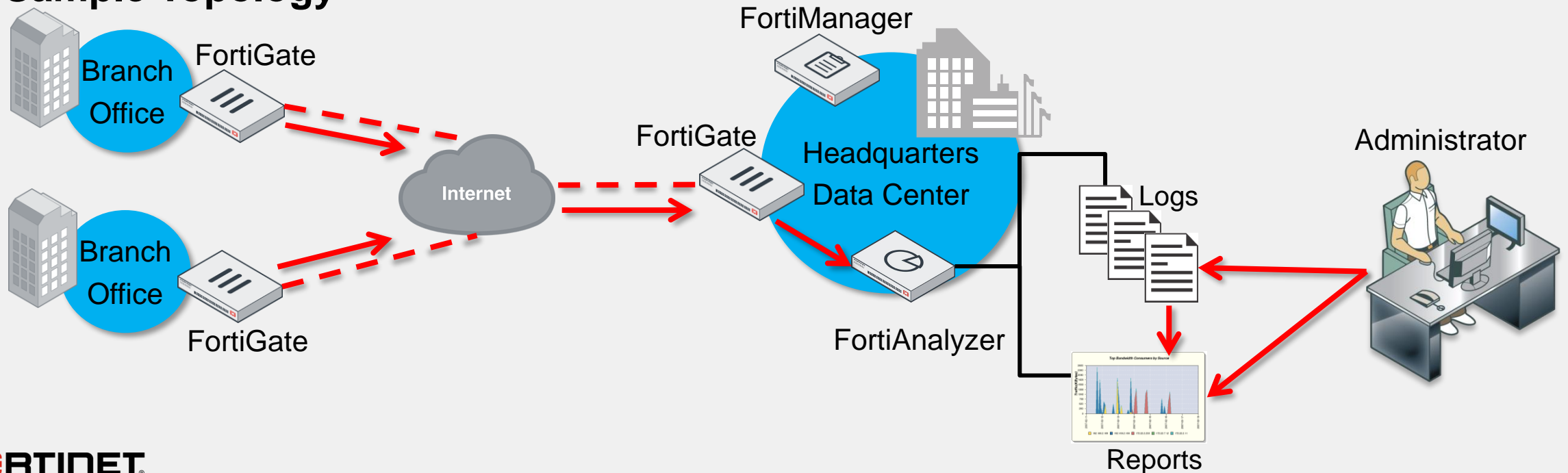
Note: The list is not exhaustive

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



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**

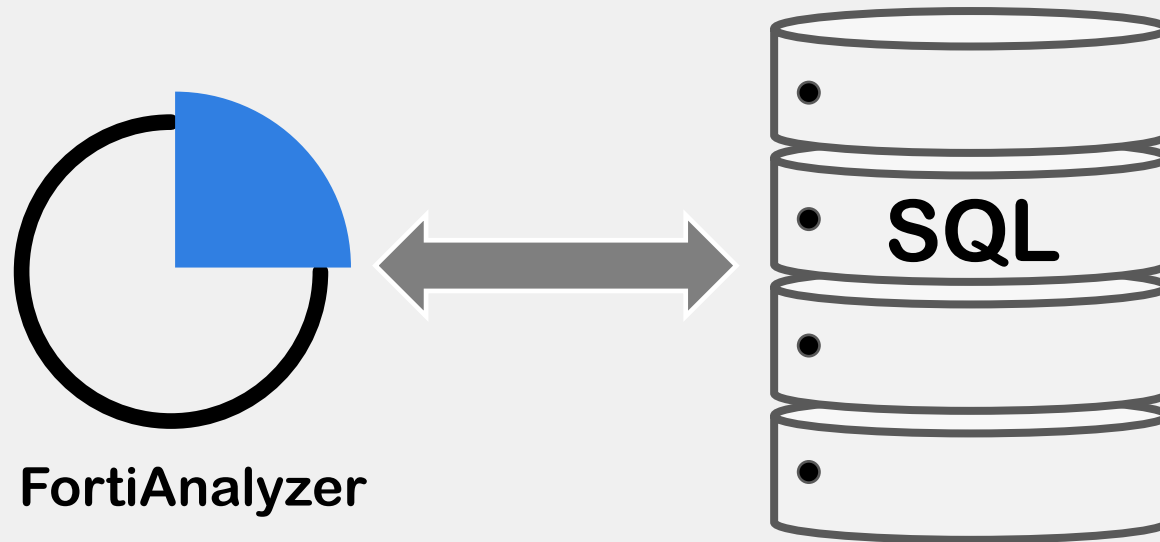
- Identify and react to security threats quickly when configured conditions are met
- View events through **Event Monitor** (on the GUI), email, SNMP, or syslog
- Events that require further investigation can be used to generate new incidents

- **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	<input type="checkbox"/>	
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

All Devices ▾ Last 7 Days ▾ Aug 09 To Aug 16

+

🔍 ?

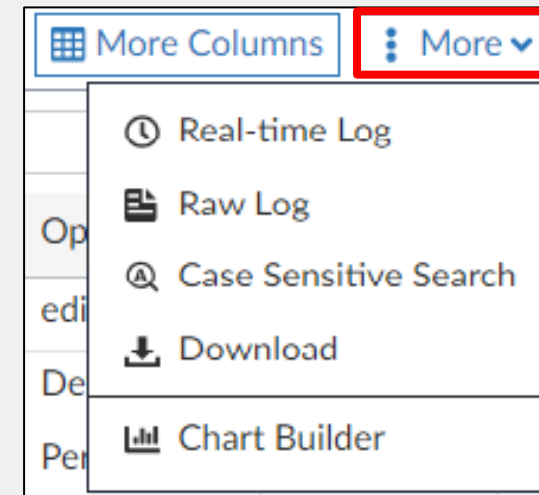
👤 📄 ⚙️

#	↓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/670.0 B	<div>Session ID 266578</div> <div>Tran Display noop</div> <div>Virtual Domain root</div> <div>Source</div> <div>Device ID FGVM010000064692</div> <div>Device Name Local-...</div> <div>Source Country Reser...</div> <div>Source IP 127.0.0.1</div> <div>Source Interface root</div> <div>Source Interface Role undefi...</div> <div>Source Port 1840</div> <div>UEBA Endpoint ID 3</div> <div>UEBA User ID 3</div> <div>Destination</div> <div>Destination Country Reserved</div> <div>Destination End User ID 3</div> <div>Destination Endpoint ID 3</div> <div>Destination IP 127.0.0.1</div> <div>Destination Interface root</div> <div>Destination Interface Role undefined</div> <div>Destination Port 80</div> <div>Action</div> <div>Action close</div> <div>Policy ID 0</div> <div>Application</div> <div>Application HTTP</div> <div>Application Category unscanned</div> <div>Protocol 6</div> <div>Service HTTP</div> <div>Duration 1</div> <div>Received Packets 4</div> <div>Transmitted Packets 6</div> <div>399.0 B/670.0 B</div>
2	11:16:49	FGVM010000077646	✓close	127.0.0.1	127.0.0.1	HTTP	HTTP	399.0 B/670.0 B	
3	11:16:09	FGVM010000077646	✓close	10.0.1.200	🇺🇸96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 KB	
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 KB	
6	11:16:08	FGVM010000064692	✓close	10.0.1.200	🇺🇸96.45.46.46	tcp/853	tcp/853	6.6 KB/21.2 KB	
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 KB	
14	11:12:08	FGVM010000064692	server-rst	10.0.1.200	🇺🇸154.52.4.163	tcp/514	tcp/514	3.3 KB/100.0 KB	
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 KB	
17	11:12:00	FGVM010000064692	✓close	10.0.1.254	10.0.1.210	tcp/514	tcp/514	8.5 KB/12.1 KB	
18	11:12:00	FGVM010000064692	client-rst	10.200.1.1	🇨🇦206.47.184.6	HTTPS	HTTPS		

⏪ Total logs for analytics: 69 days 1 hour. 50 /Page 1 2 3 4 5 » 70 ⏩ 0.031 Second

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

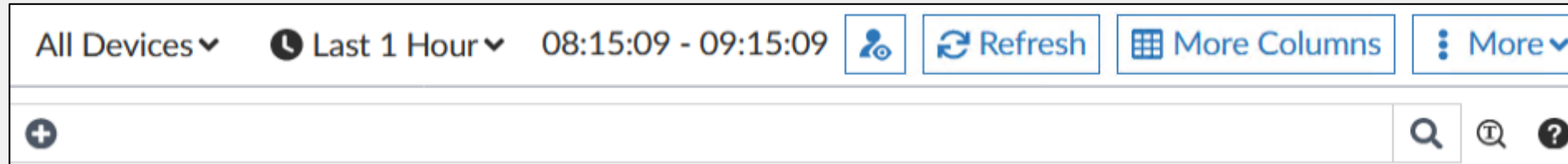
#	↓Date/Time	Device ID	Action	Source	Destination IP
4	14:59:50	FGVM010000064692	✓accept	10.200.1.1	🇨🇦208.91.112.60
5	14:59:40	FGVM010000064692	✓accept	10.200.1.1	🇨🇦208.91.112.61
6	14:59:30	FGVM010000064692	✓accept	10.0.1.200	🇨🇦208.91.112.60
7	14:59:30	FGVM010000064692	✓accept	10.0.1.200	🇨🇦208.91.112.63

Raw

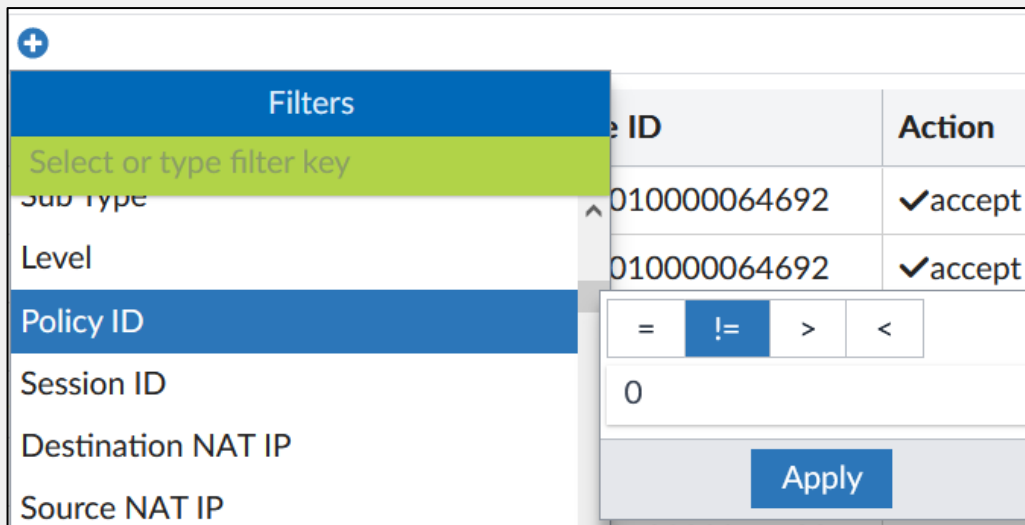
```
date=2023-08-16 time=14:59:24 id=7268043151217000450 itime=2023-08-16 14:59:25 euid=3 epid=104
dsteuid=3 dstepid=101 type=traffic subtype=local level=notice action=accept policyid=0 sessionid=89571
srcip=10.0.1.200 dstip=208.91.112.60 srcport=123 dstport=123 trandisp=noop duration=183 proto=17
sentbyte=76 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

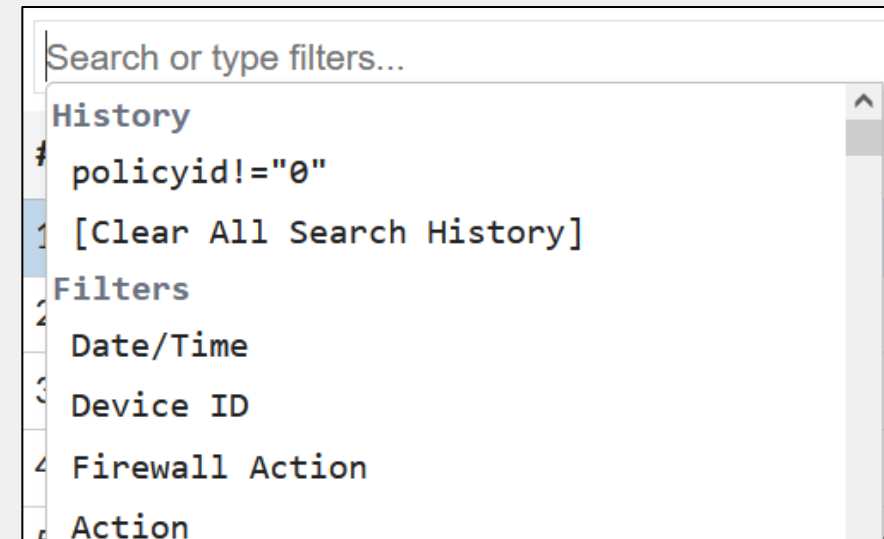
- Click on the magnifying glass to toggle between filter and text mode



- 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			
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"

Populates the search criteria

srcip = 10.0.3.20  

- 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

The screenshot shows the Fortinet log search interface. At the top, there are tabs for 'Traffic', 'Security: Web Filter', and 'Event'. Below these, there are filters for 'All Devices', 'Custom...', and a time period 'Jun 07 To Jun 08'. A search bar contains the query 'srcip = 10.0.3.20 AND Category Description = Malicious Websites'. The results table has columns: '#', 'Date/Time', 'Device ID', 'Source', 'Destination IP', 'Service', 'Action', and 'URL'. The 'Source' column is highlighted in yellow for all rows, showing '10.0.3.20'. The 'URL' column is highlighted in red for all rows, showing various blocked URLs. Annotations include: 'Security subtype Web Filter' pointing to the 'Security: Web Filter' tab; 'Custom time period' pointing to the 'Jun 07 To Jun 08' filter; 'Malicious websites visited' pointing to the 'URL' column; 'Filters are based on the client's IP as the source, and the category description' pointing to the search bar; and 'Fields used in the filter are highlighted' pointing to the highlighted 'Source' and 'URL' columns.

#	↓Date/Time	Device ID	Source	Destination IP	Service	Action	URL
1	06-08 10:37	FGVM0000077646	10.0.3.20	64.70.19.203	HTTP	blocked	http://ffb07fb6990e3b5da86d66d43b4
2	06-08 10:37	FGVM000077646	10.0.3.20	155.159.36.59	HTTP	blocked	http://whollyfitinc.com/
3	06-08 10:37	FGVM000077646	10.0.3.20	176.103.56.36	HTTP	blocked	http://176.103.56.36/
4	06-08 10:37	FGVM000077646	10.0.3.20	43.163.226.161	HTTP	blocked	http://234w.cc/
5	06-08 10:35	FGVM000077646	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

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**

Event

Application

All Devices

Last 1 Hour

19:03:04 - 20:03:04

Message=

em perf

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

Source IP=

10*

#	Date/Time	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\.|172\.(1[6-9]|2[0-9]|3[0-1])\.|192\.168\.)"
```

srcip~"10\.[0-9]+\.[0-9]+\.[0-9]+"		
#	Source	↓ Date/Time
1	10.200.3.3	2024-06-1

srcip!~"10\.200\.[0-9]+\.[0-9]+"		
#	Source	↓ Date/Time
1	172.16.200.6	2024-06

- 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

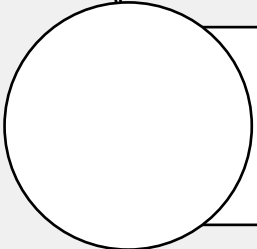
2. What is the purpose of using ADOMs?

- ✓ A. To divide administration of devices, restrict access, and manage data policies
- B. To reduce resource usage on FortiAnalyzer

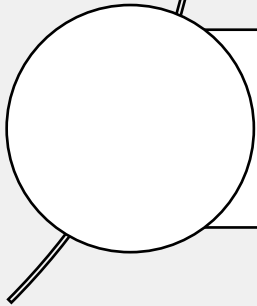
Lesson Progress



FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric



Operation Modes

Objectives

- Describe FortiAnalyzer operation modes
- Configure FortiAnalyzer collectors
- Configure FortiAnalyzer analyzers

FortiAnalyzer Operation Modes—Analyzer

Dashboard > System Information

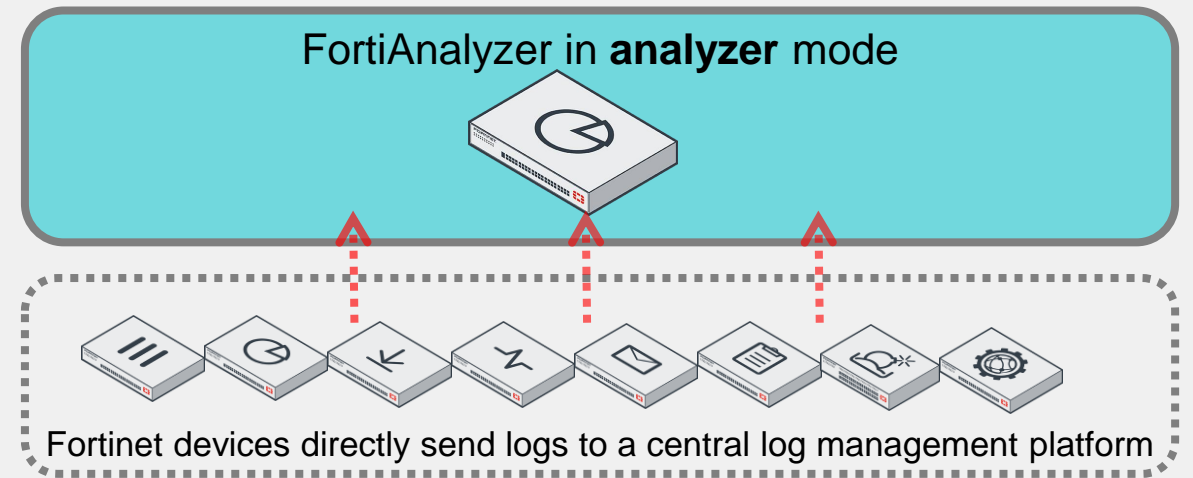
Operation Mode

Analyzer

Collector

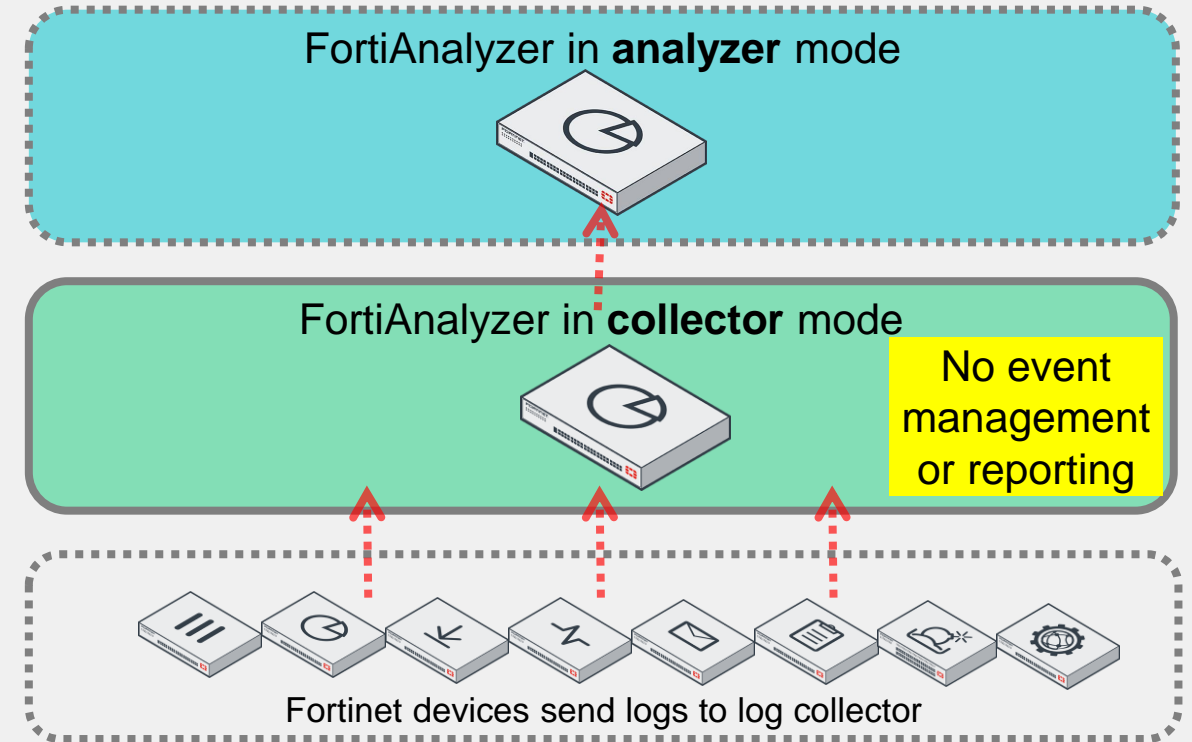
Analyzer is the default operation mode

- Central log aggregator for one or more logging devices, or FortiAnalyzer in collector mode
 - Can still forward logs to another FortiAnalyzer (or syslog/CEF server)

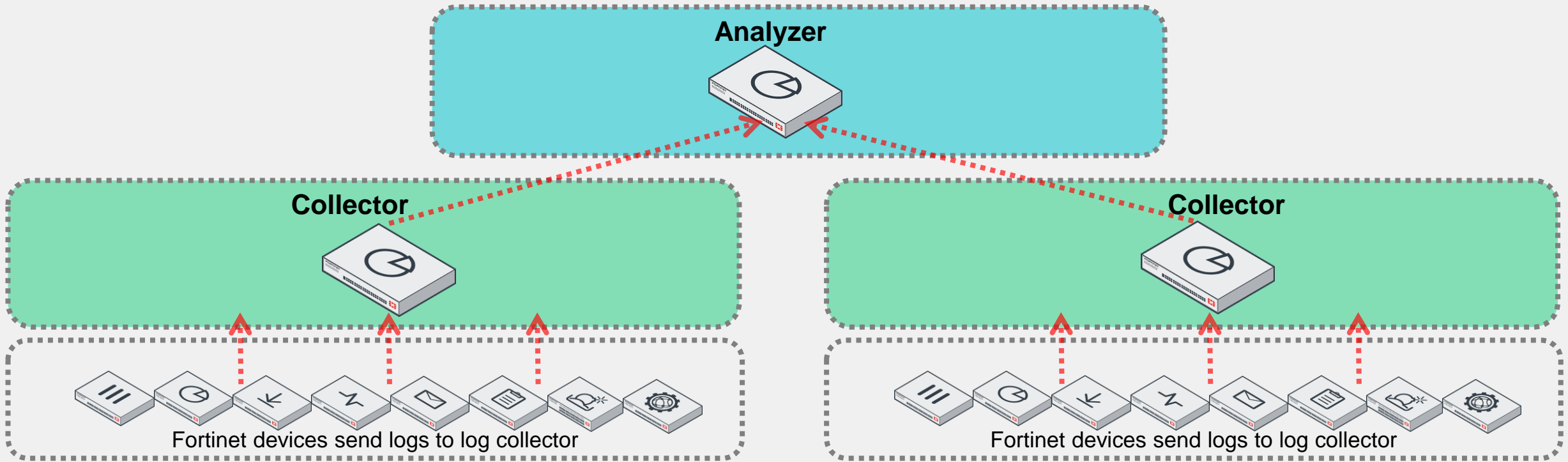


FortiAnalyzer Operation Modes—Collector

- Collects logs from multiple devices and forwards them to FortiAnalyzer in analyzer mode
 - Can aggregate logs to another FortiAnalyzer
 - Can *only* forward to syslog/CEF server in real-time forwarding mode
- Not used for analytics—archiving only



Analyzer—Collector Collaboration



- Increase FortiAnalyzer performance by using both modes
- Offload the log-receiving task to the collector
- Analyzer focuses on data analysis and reporting
- Collector can help with slow or unreliable links by storing logs and forwarding them later
- On the collector, you should allocate most of the disk space to archive logs

Collector Configuration

- Enable collector operation mode
- Modify the data policy to focus on archiving
 - Set to 0 days for analytics
 - Set archive retention based on your organizational requirements
- Modify the disk utilization quota to focus on archiving
 - Allocate most disk space for archive log use
 - Set the analytics:archive ratio to 5%:95%

Dashboard > System Information

Operation Mode

Analyzer

Collector

System Setting > ADOMs

Data Policy

Keep Logs for Analytics

0

Days

Keep Logs for Archive

365

Days

Allocated 13000 MB Maximum Available: 29.4 GB

Analytics: Archive 5% 95% ☒ Modify

Alert and Delete When Usage Reaches

90%

Note: You need to set the allocated disk quota to meet your requirements

Collector Configuration (Contd)

- Enable log forwarding on the collector
- Configure the required settings, including name, remote server type, server FQDN/IP, and other parameters
- Configure additional filters to forward matching logs, define fields to exclude, and mask sensitive fields

System Setting > Advanced > Log Forwarding

Name	FAZ-MSSP
Status	<input checked="" type="checkbox"/>
Remote Server Type	FortiAnalyzer
Server FQDN/IP	10.0.1.236
Compression	<input checked="" type="checkbox"/>
Reliable Connection	<input checked="" type="checkbox"/>
Peer Certificate CN	
Sending Frequency	Real-time Every 1 Minute Every 5 Minutes
Log Forwarding Filters	
Device Filters	Select Device
Log Filters	<input type="checkbox"/>
Enable Exclusions	<input type="checkbox"/>
Enable Masking	<input type="checkbox"/>

Analyzer Configuration

- Modify the data policy to focus on analytics
 - Set the analytics retention based on your organizational requirements
 - Set to 0 days for archive
- Modify the disk utilization quota to focus on analytics
 - Set the analytics:archive ratio to 95%:5%

System Setting > ADOMs

Data Policy		
Keep Logs for Analytics	<input type="text" value="60"/>	<input type="text" value="Days"/>
Keep Logs for Archive	<input type="text" value="0"/>	<input type="text" value="Days"/>

Note: Analytics logs take up significantly more space than archive logs, so adjust your settings appropriately

Disk Utilization			
Allocated	<input type="text" value="13000"/>	<input type="text" value="MB"/>	Maximum Available: 30.4 GB
Analytics: Archive	<input type="text" value="95%"/>	<input type="text" value="5%"/>	<input checked="" type="checkbox"/> Modify
Alert and Delete When Usage Reaches	<input type="text" value="90%"/>		

Knowledge Check

1. Which FortiAnalyzer operation mode do you use for analytics?

- ✓ A. Analyzer
- B. Collector

2. Which type of logs consume more disk space?

- ✓ A. Analytics
- B. Archive

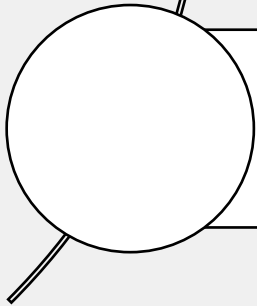
Lesson Progress



FortiAnalyzer Architecture



Operation Modes





FortiAnalyzer Fabric



FortiAnalyzer Fabric

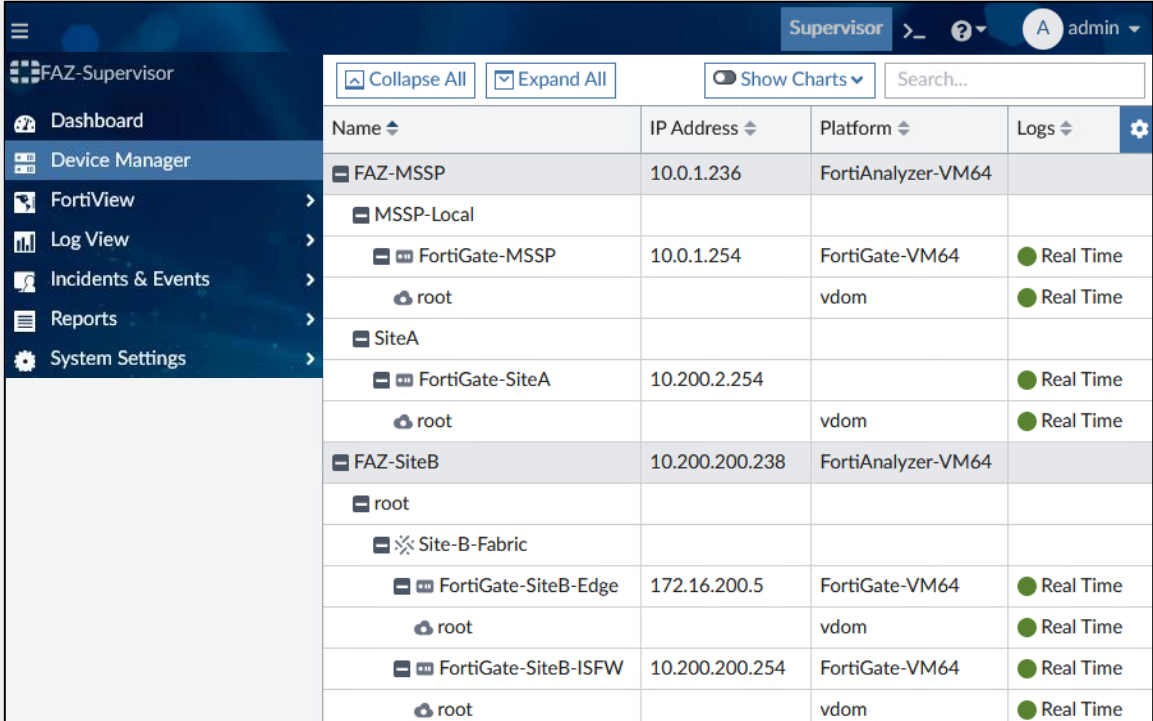


Objectives

- Describe the FortiAnalyzer Fabric
 - Design FortiAnalyzer Fabric topologies
 - Configure the FortiAnalyzer Fabric supervisor and members
 - Manage Fabric groups
- 
- 
- 

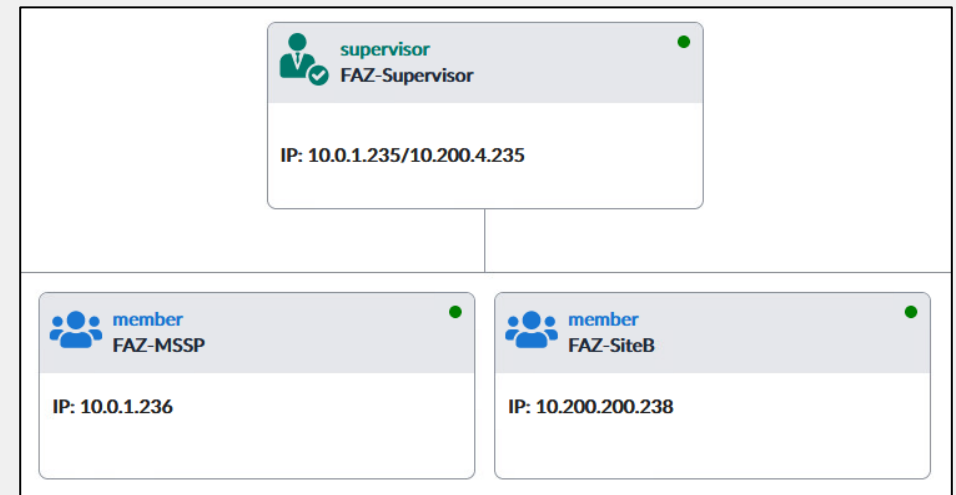
FortiAnalyzer Fabric

- Enables centralized viewing of devices, incidents, and events across multiple FortiAnalyzer devices
- Ideal for environments with multiple FortiAnalyzer devices and high log volume
- Two operation modes:
 - Supervisor—one per fabric; acts as the root
 - Member—sends information to the supervisor
- The supervisor includes these modules:
 - Device Manager
 - FortiView
 - Log View
 - Incidents & Events
 - Reports

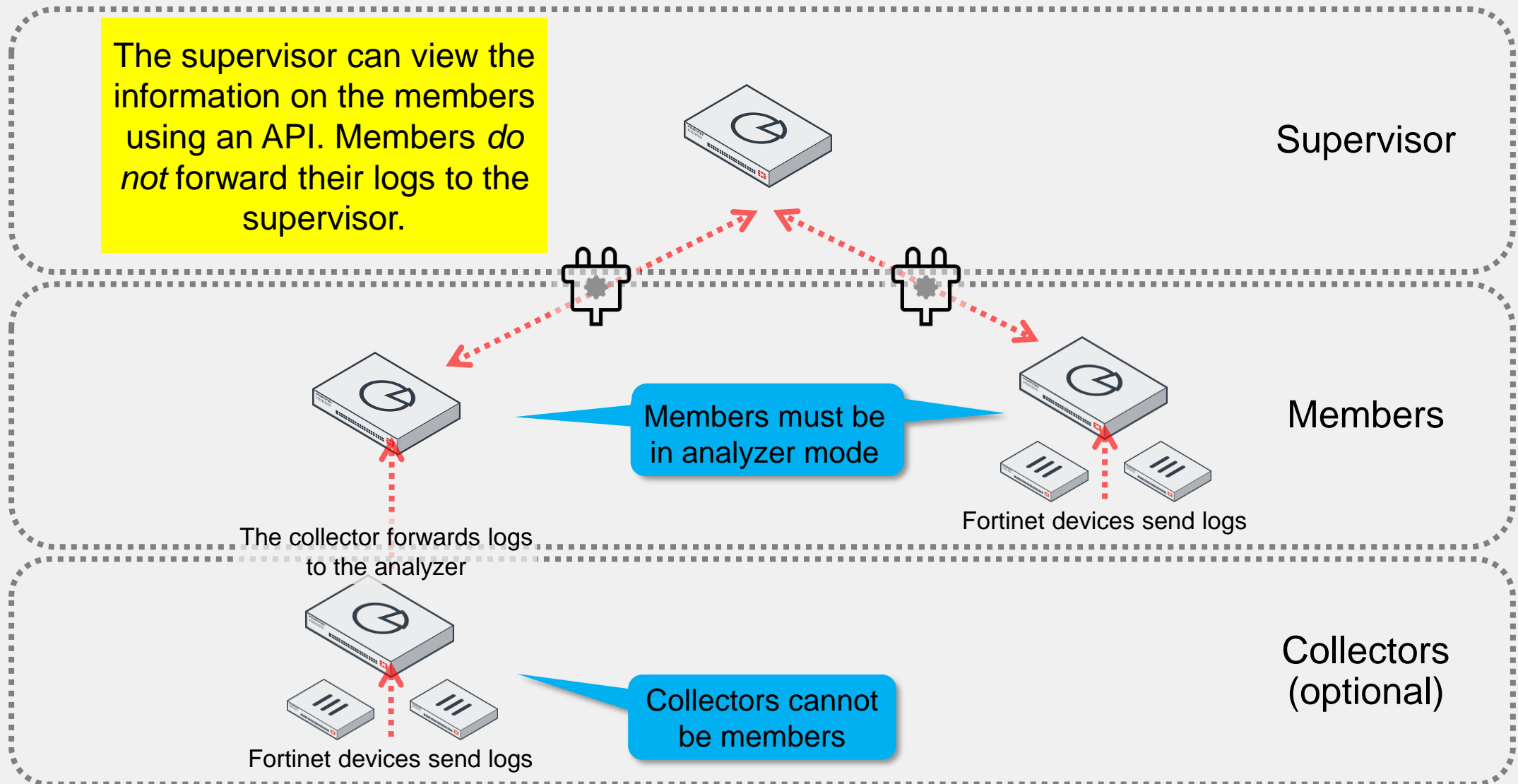


The screenshot shows the FortiAnalyzer Supervisor web interface. The left sidebar contains navigation options: Dashboard, Device Manager (selected), FortiView, Log View, Incidents & Events, Reports, and System Settings. The main panel displays a table of devices under the 'FAZ-Supervisor' header. The table has columns for Name, IP Address, Platform, and Logs. It lists various devices including FAZ-MSSP, MSSP-Local, FortiGate-MSSP, root, SiteA, FortiGate-SiteA, root, FAZ-SiteB, root, Site-B-Fabric, FortiGate-SiteB-Edge, root, FortiGate-SiteB-ISFW, and root. Each device entry includes its IP address, platform (e.g., FortiAnalyzer-VM64, FortiGate-VM64), and a 'Real Time' status indicator.

Name	IP Address	Platform	Logs
FAZ-MSSP	10.0.1.236	FortiAnalyzer-VM64	
MSSP-Local			
FortiGate-MSSP	10.0.1.254	FortiGate-VM64	Real Time
root		vdom	Real Time
SiteA			
FortiGate-SiteA	10.200.2.254		Real Time
root		vdom	Real Time
FAZ-SiteB	10.200.200.238	FortiAnalyzer-VM64	
root			
Site-B-Fabric			
FortiGate-SiteB-Edge	172.16.200.5	FortiGate-VM64	Real Time
root		vdom	Real Time
FortiGate-SiteB-ISFW	10.200.200.254	FortiGate-VM64	Real Time
root		vdom	Real Time



Sample FortiAnalyzer Fabric Topology



Configure the FortiAnalyzer Supervisor

- Configure the supervisor using the GUI:
- Alternatively, on the CLI:
- (CLI only) Enable `soc-fabric` on the interface

System Settings > Fabric Management

Status	<input checked="" type="checkbox"/>
Role	Supervisor Member
Cluster Name	MSSP-Fabric
Session Port	6443
Secure Connection	<input checked="" type="checkbox"/>

```
# config system soc-fabric
  set status enable
  set name "MSSP-Fabric"
  set supervisor <IP/DNS Name>
```

```
# config system interface
  edit <port #>
    set allowaccess soc-fabric <add other protocols you need>
  end
```

Do not forget to add other administrative access protocols, such HTTPS and SSH, as required. Existing settings will be overwritten.

Configure the FortiAnalyzer Member

- Configure the member using the GUI:
- Alternatively, on the CLI:
- (CLI only) Enable `soc-fabric` on the interface

System Settings > Fabric Management

Status	<input checked="" type="checkbox"/>
Role	<div>Supervisor Member</div>
Cluster Name	MSSP-Fabric
IP	10.0.1.235
Session Port	6443
Secure Connection	<input checked="" type="checkbox"/>

```
# config system soc-fabric
  set status enable
  set name "MSSP-Fabric"
  set supervisor <IP/DNS Name>
```

```
# config system interface
  edit <port #>
    set allowaccess soc-fabric <add other protocols you need>
  end
```

Do not forget to add other administrative access protocols, such HTTPS and SSH, as required. Existing settings will be overwritten.

Fabric Groups

- To filter information to specific FortiAnalyzer fabric members or ADOMs, you can create Fabric groups

System Settings > Fabric Groups

Create Fabric Group

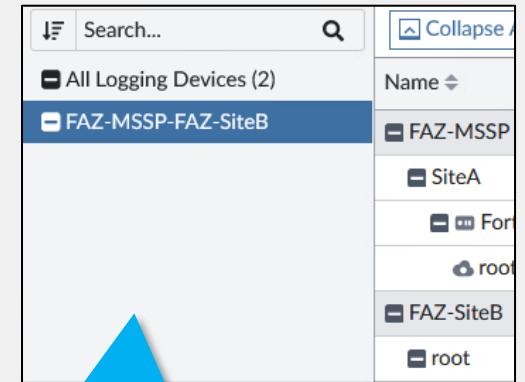
Group Name	FAZ-MSSP-FAZ-SiteB
Description	Includes ADOMs MSSP-Local and SiteA on FAZ-MSSP. Also includes all ADOMs on FAZ-SiteB

Add Member

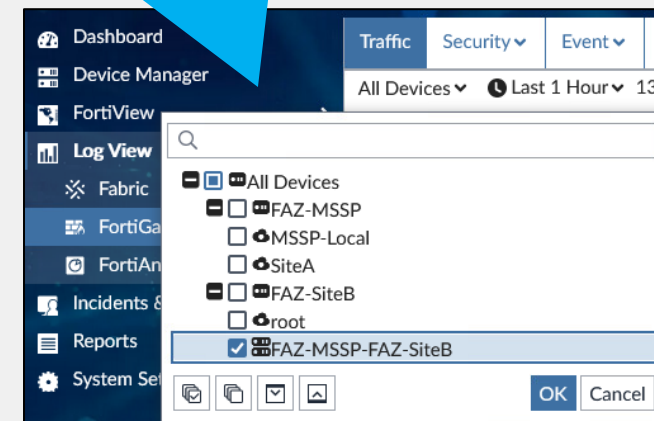
Search

- ☐ FortiSandbox
- ☐ FortiWeb
- ☐ MSSP-Local
- ☒ SiteA
- ☐ root
- ☒ FAZ-SiteB
- ☒ FortiAnalyzer
- ☒ FortiAuthenticator

FortiAnalyzer Fabric		Fabric Groups	Fabric Connectors
+ Create New		Edit	Delete
Device Name	IP Address	Platform	
FAZ-MSSP-FAZ-SiteB 2			
FAZ-MSSP 1	10.0.1.236	FortiAnalyzer-VM64	
SiteA			
FAZ-SiteB 2	10.200.200.238	FortiAnalyzer-VM64	
root			
FortiAnalyzer			
FortiAuthenticator			



The fabric group can be used to filter devices



Knowledge Check

1. Which FortiAnalyzer operation mode must you configure Fabric members in?

- ✓ A. Analyzer
- B. Collector

2. Which statement about the Fabric supervisor is true?

- A. All logging devices are registered to the Fabric supervisor.
- ✓ B. Logging devices cannot be registered to the Fabric supervisor.

Lesson Progress



Introduction to FortiAnalyzer Architecture



Operation Modes



FortiAnalyzer Fabric

Review

- ✓ Manage administrative domains
- ✓ Describe FortiAnalyzer operation modes
- ✓ Configure FortiAnalyzer collectors and analyzers
- ✓ Design and deploy FortiAnalyzer Fabric deployments
- ✓ Manage Fabric groups