Course › LAB GUIDE › Lab 3 - Looking for ... › Looking for events t...

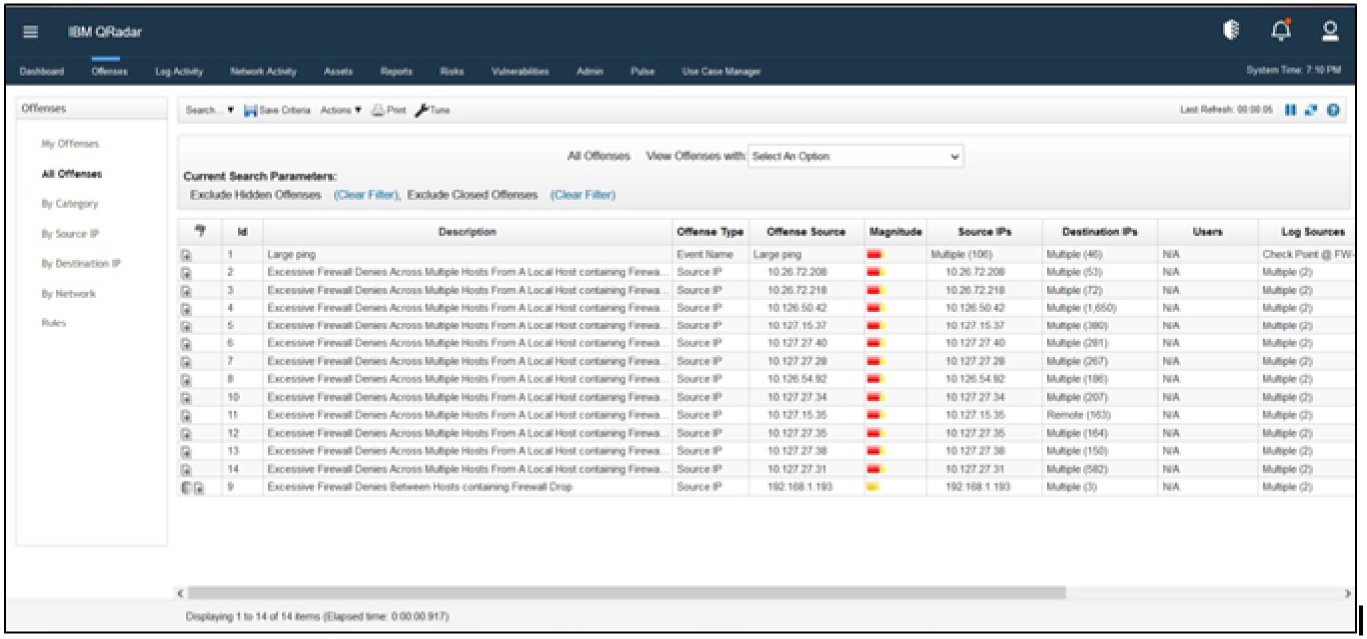
Looking for events that contribute to an offense

Looking for events that contribute to an offense

In the previous lab exercise, we learnt about Investigating an offense. In this exercise, we will further analyze and explore the events that are contributed to any offense.

Perform the below steps:

1. Login in the Qradar Interface, on Home page, Click the **Offenses** tab. The All Offenses page opens.

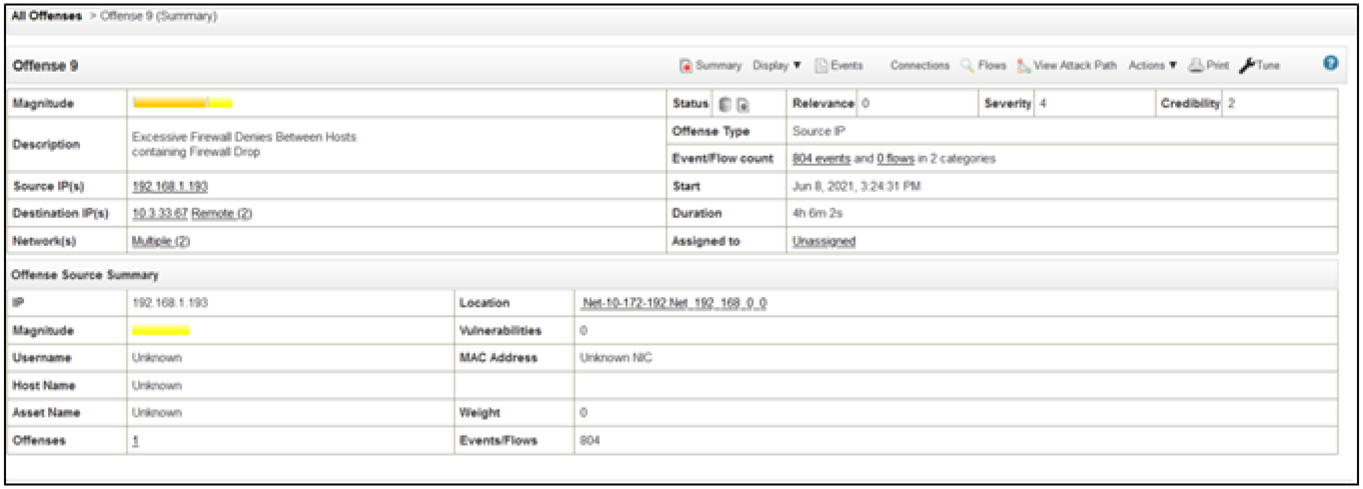


Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	1	Large ping	Event Name	Large ping	🟥	Multiple (106)	Multiple (46)	N/A	Check Point @ FW-
	2	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.208	🟥	10.26.72.208	Multiple (53)	N/A	Multiple (2)
	3	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.26.72.218	🟥	10.26.72.218	Multiple (72)	N/A	Multiple (2)
	4	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.50.42	🟥	10.126.50.42	Multiple (1,650)	N/A	Multiple (2)
	5	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.37	🟥	10.127.15.37	Multiple (380)	N/A	Multiple (2)
	6	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.40	🟥	10.127.27.40	Multiple (281)	N/A	Multiple (2)
	7	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.28	🟥	10.127.27.28	Multiple (267)	N/A	Multiple (2)
	8	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.126.54.92	🟥	10.126.54.92	Multiple (186)	N/A	Multiple (2)
	10	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.34	🟥	10.127.27.34	Multiple (207)	N/A	Multiple (2)
	11	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.15.35	🟥	10.127.15.35	Remote (163)	N/A	Multiple (2)
	12	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.35	🟥	10.127.27.35	Multiple (164)	N/A	Multiple (2)
	13	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.38	🟥	10.127.27.38	Multiple (150)	N/A	Multiple (2)
	14	Excessive Firewall Denies Across Multiple Hosts From A Local Host containing Firewa...	Source IP	10.127.27.31	🟥	10.127.27.31	Multiple (582)	N/A	Multiple (2)
	9	Excessive Firewall Denies Between Hosts containing Firewall Drop	Source IP	192.168.1.193	🟨	192.168.1.193	Multiple (3)	N/A	Multiple (2)

Displaying 1 to 14 of 14 items (Elapsed time: 0:00:00.917)

2. Find and double-click the **"Excessive Firewall Denies between Hosts containing Firewall Drop".**



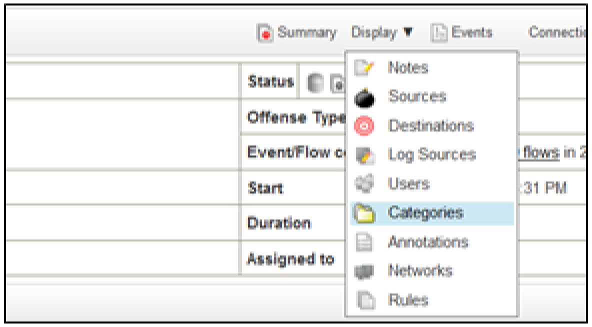
Offense 9

Magnitude	🟨	Status		Relevance	0	Severity	4	Credibility	2
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	Offense Type	Source IP				
		Event/Flow count	804 events and 0 flows in 2 categories				
Source IP(s)	192.168.1.193	Start	Jun 8, 2021, 3:24:31 PM				
Destination IP(s)	10.3.33.67 Remote (2)	Duration	4h 6m 2s				
Network(s)	Multiple (2)	Assigned to	Unassigned				

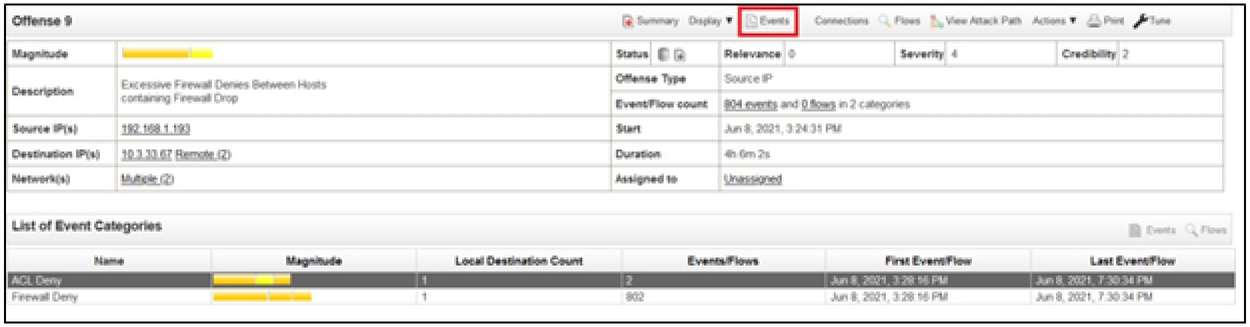
Offense Source Summary

IP	192.168.1.193	Location	Net-10-172-192.Net_192_168_0_0
Magnitude	🟨	Vulnerabilities	0
Username	Unknown	MAC Address	Unknown NIC
Host Name	Unknown		
Asset Name	Unknown	Weight	0
Offenses	1	Events/Flows	804

3. Show the low-level categories of the offense's events by selecting **Display > Categories** on the toolbar



4. To investigate the events that are associated with this offense in the low-level category, Right click the table row that shows the Event category and click **Events.**



Offense 9

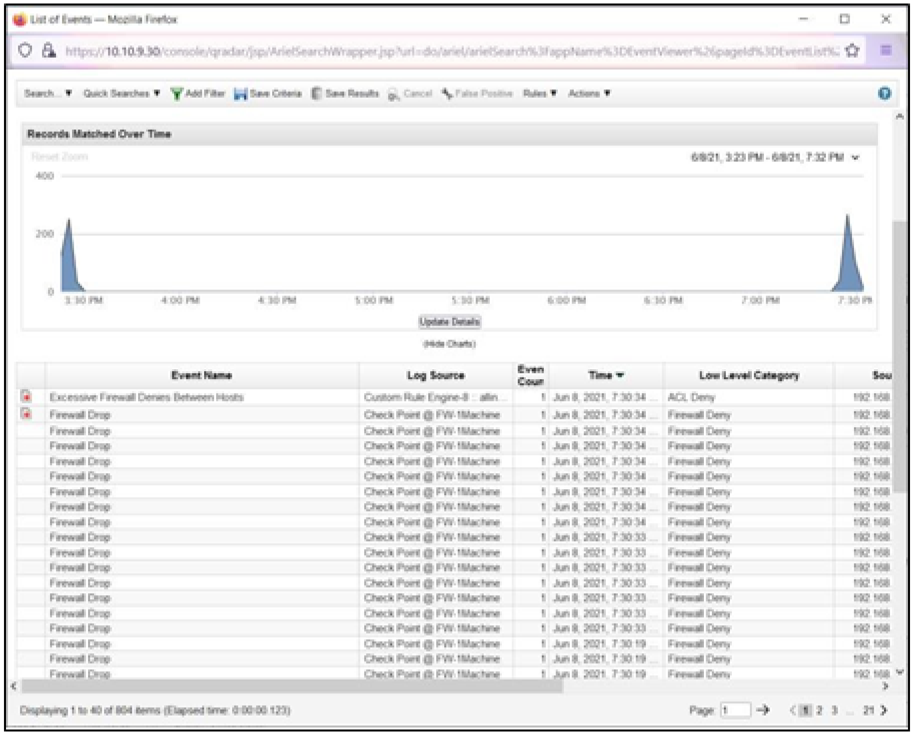
Magnitude		Status		Relevance	0	Severity 4	Credibility 2
Description	Excessive Firewall Denies Between Hosts containing Firewall Drop	Offense Type	Source IP				
		Event/Flow count	804 events and 0 flows in 2 categories				
Source IP(s)	192.168.1.193	Start	Jun 8, 2021, 3:24:31 PM				
Destination IP(s)	10.3.33.67 Remote (2)	Duration	4h 6m 2s				
Network(s)	Multiple (2)	Assigned to	Unassigned				

List of Event Categories

Name	Magnitude	Local Destination Count	Events/Flows	First Event/Flow	Last Event/Flow
ACL Deny		1	2	Jun 8, 2021, 3:28:16 PM	Jun 8, 2021, 7:30:34 PM
Firewall Deny		1	802	Jun 8, 2021, 3:28:16 PM	Jun 8, 2021, 7:30:34 PM

Note: You can select any of the event and category from the **"List of Event categories"** table.

The List of the events page opens.



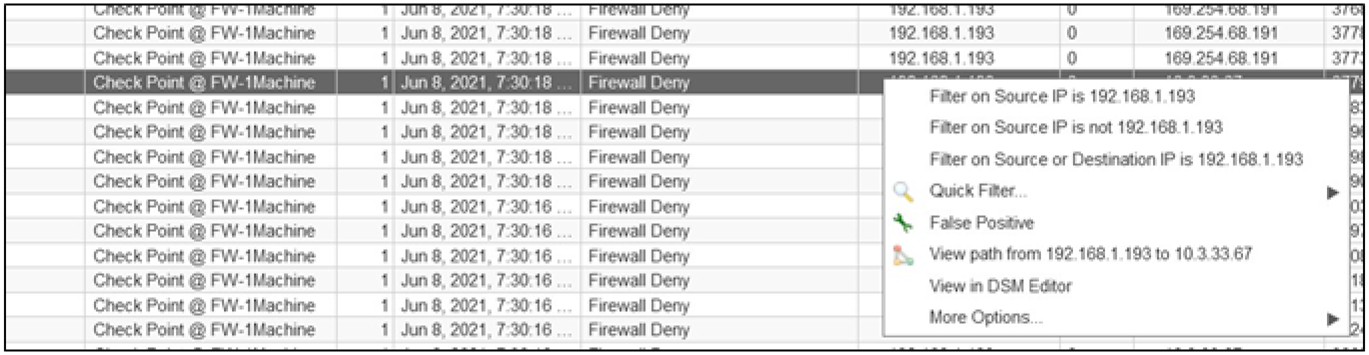
List of Events — Mozilla Firefox
https://10.10.9.30/console/qradar/jsp/ArielSearchWrapper.jsp?url=do/ariel/arielSearch%3FappName%3DEventViewer%26pageId%3DEventList%
Search... ▼
Quick Searches ▼
Add Filter
Save Criteria
Save Results
Cancel
False Positive
Rules ▼
Actions ▼
Records Matched Over Time
Reset Zoom
6/8/21, 3:23 PM - 6/8/21, 7:32 PM
400
200
0
3:30 PM
4:00 PM
4:30 PM
5:00 PM
5:30 PM
6:00 PM
6:30 PM
7:00 PM
7:30 PM
Update Details
(Hide Charts)

	Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Sou
	Excessive Firewall Denies Between Hosts	Custom Rule Engine-8 :: alin ...	1	Jun 8, 2021, 7:30:34 ...	ACL Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:34 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:33 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168
	Firewall Drop	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:19 ...	Firewall Deny	192.168

Displaying 1 to 40 of 804 items (Elapsed time: 0:00:00.123)

5. Create a filter to exclude the source IP that contributed to the offense.

- Select an event, Right-click on **<IP Address>** and select **Filter on Source IP is not <IP Address>**.



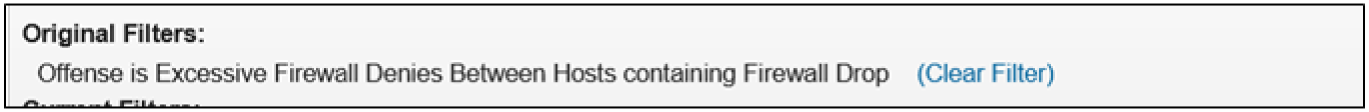
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	376
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	377
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny	192.168.1.193	0	169.254.68.191	377
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				377
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				83
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				9
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				9
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:18 ...	Firewall Deny				9
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				0
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				9
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				0
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				1
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				1
	Check Point @ FW-1Machine	1	Jun 8, 2021, 7:30:16 ...	Firewall Deny				2

Filter on Source IP is 192.168.1.193
Filter on Source IP is not 192.168.1.193
Filter on Source or Destination IP is 192.168.1.193
Quick Filter... ▶
False Positive
View path from 192.168.1.193 to 10.3.33.67
View in DSM Editor
More Options... ▶

6. What results are returned?

7. What do the results of this search indicate?

8. To look for similar other events unrelated to the particular offense, click Clear Filter for the Offense is **“Excessive Firewall Denies between Hosts containing Firewall Drop”.**



Original Filters:

Offense is Excessive Firewall Denies Between Hosts containing Firewall Drop (Clear Filter)

What results are returned? Why?

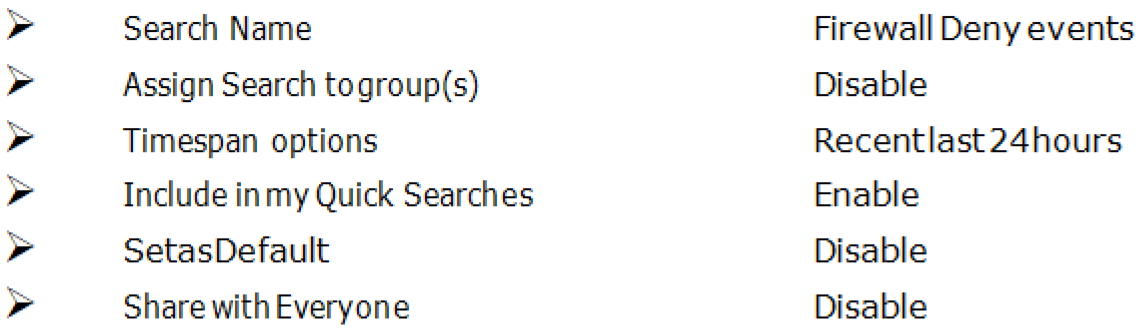
9. Select **Last 24 Hours** to view events from the last 24 hours, in the View drop-down list.

Explore other search filters and options. You can also save the filter criteria by following the below steps.

1. Save the current search criteria

    a. On the Toolbar, click **Save Criteria.**

    b. Configure the Save Criteria window as shown below



➢	Search Name	Firewall Deny events
➢	Assign Search togroup(s)	Disable
➢	Timespan options	Recentlast 24hours
➢	Include in my Quick Searches	Enable
➢	SetasDefault	Disable
➢	Share with Everyone	Disable

c. Review the Save Criteria and Click **OK.**

2. Save the current search results.

a. On the toolbar, click **Save Results.**

b. Enter the name in the name field.

c. Click **Ok.**

3. Revisit or delete your saved search results.

a. On the list of events page’s toolbar, click **Search > Manage Search Results.**

b. In the Search Results management page, select your search results and click Delete.

c. Close the Search Results Management page