

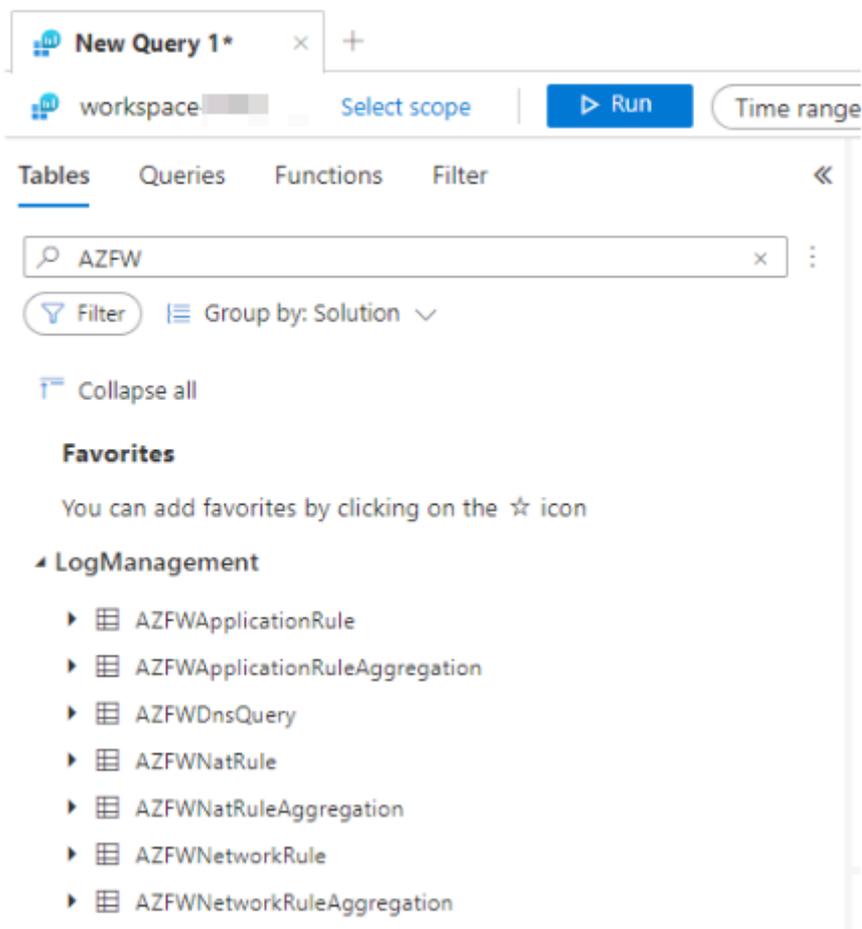
Query Azure Firewall Logs

Azure Firewall Logs can be stored in an Azure Log Analytics Workspace. This workspace then contains all status logs along with permitted and denied connections. So, to find out if a connection is wrongly blocked or to make a specific firewall request, we can use these logs to give us insights.

Find log tables

First of all you have to select the scope on which you want to search for the logs. You can choose the Log Analytics scope with "Select scope".

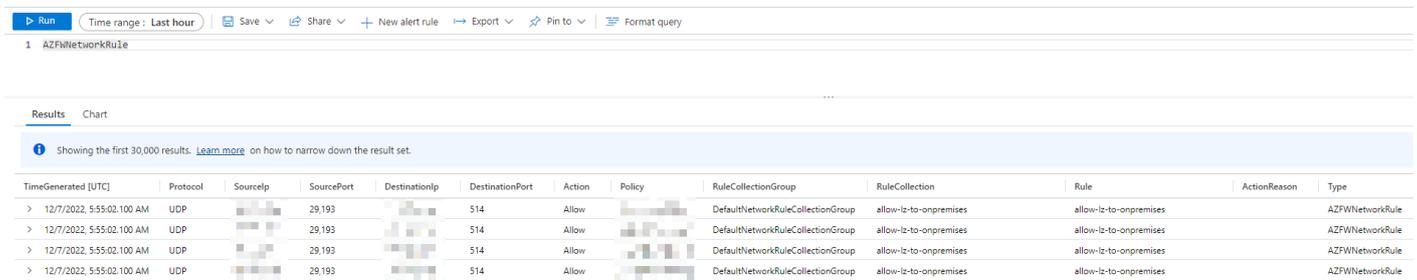
Azure Firewalls save logs to different tables. To find all the different log table you can search in the tables pane for "AZFW". These Tables contain the corresponding log data.



Azure Firewall rule logs are stored within the "AZFWNetworkRule" table.

View whole table content

To view the whole table content you can write the name of the table into the KQL (Kusto Query Language) section. In this case "AZFWNetworkRule" is enough to see all the permitted and denied connections.



The screenshot shows the Azure portal's KQL query interface. At the top, there's a toolbar with options like 'Run', 'Time range: Last hour', 'Save', 'Share', 'New alert rule', 'Export', 'Pin to', and 'Format query'. Below the toolbar, the query '1 AZFWNetworkRule' is entered. The results section shows a table with the following columns: TimeGenerated [UTC], Protocol, SourceIp, SourcePort, DestinationIp, DestinationPort, Action, Policy, RuleCollectionGroup, RuleCollection, Rule, ActionReason, and Type. The table displays four rows of data, all with an 'Allow' action and 'allow-iz-to-onpremises' rule.

TimeGenerated [UTC]	Protocol	SourceIp	SourcePort	DestinationIp	DestinationPort	Action	Policy	RuleCollectionGroup	RuleCollection	Rule	ActionReason	Type
> 12/7/2022, 5:55:02.100 AM	UDP	[REDACTED]	29,193	[REDACTED]	514	Allow	[REDACTED]	DefaultNetworkRuleCollectionGroup	allow-iz-to-onpremises	allow-iz-to-onpremises		AZFWNetworkRule
> 12/7/2022, 5:55:02.100 AM	UDP	[REDACTED]	29,193	[REDACTED]	514	Allow	[REDACTED]	DefaultNetworkRuleCollectionGroup	allow-iz-to-onpremises	allow-iz-to-onpremises		AZFWNetworkRule
> 12/7/2022, 5:55:02.100 AM	UDP	[REDACTED]	29,193	[REDACTED]	514	Allow	[REDACTED]	DefaultNetworkRuleCollectionGroup	allow-iz-to-onpremises	allow-iz-to-onpremises		AZFWNetworkRule
> 12/7/2022, 5:55:02.100 AM	UDP	[REDACTED]	29,193	[REDACTED]	514	Allow	[REDACTED]	DefaultNetworkRuleCollectionGroup	allow-iz-to-onpremises	allow-iz-to-onpremises		AZFWNetworkRule

Filter logs after IP address

Most of the time we want to filter for specific addresses. These Firewall logs can be queried with the powerful KQL language. This language helps to explore data and discover patterns, identify anomalies and outliers, create statistical modeling, and more. The query uses schema entities that are organized in a hierarchy similar to SQL's: databases, tables, and columns.

Filter for source IPs

```
AZFWNetworkRule  
| where SourceIp == "<yoursourceipaddress>"
```

Filter for destination IPs

```
AZFWNetworkRule  
| where DestinationIp == "<yourdestinationipaddress>"
```

Revision #4

Created 6 December 2022 14:02:23 by Luca Noah Caprez

Updated 9 December 2022 14:26:02 by Luca Noah Caprez