



Microsoft Sentinel with SonicWall Firewall Integration Guide

This document describes how SonicWall firewall integrates with Microsoft Sentinel. Combining these two tools can significantly enhance your security operations.

Understanding the [Microsoft Sentinel](#) and [SonicWall Firewall](#):

- **Microsoft Sentinel** is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Microsoft Sentinel solutions provide a consolidated way to acquire Microsoft Sentinel content like data connectors, workbooks, analytics, and automations in user's workspace with a single deployment step.
- **SonicWall next-generation firewalls (NGFW)** provide the security, control, and visibility you need to maintain an effective cybersecurity posture. With solutions designed for networks of all sizes, SonicWall's award-winning hardware and advanced technology are built into each firewall to give you the edge on evolving threats.

Topics:

- [Functionality](#)
- [Configuration](#)
- [Microsoft Sentinel Content Type](#)
- [SonicWall Support](#)

Functionality

The integration of SonicWall next-gen Firewalls with Microsoft Sentinel provides the capability to ingest SonicWall access logs (in syslog format) into Microsoft Sentinel. These integration capabilities enable our partners and customers to forward the firewall logs to Microsoft Sentinel, parse the logs and create custom workflows, and automate the responses.

Data Sources for Microsoft Sentinel in SonicWall firewall integration with Azure Sentinel:

- Microsoft Sentinel comes with several connectors for Microsoft solutions, including Microsoft Threat Protection, Microsoft 365 sources (such as Office 365, Azure AD, and Azure ATP), and more.
- Microsoft Sentinel uses standard syslog as the data source (Common Event Format or CEF) for non-Microsoft solutions like SonicWall.

- To ingest SonicAlert access logs into Azure Sentinel, we will set up a syslog forwarder on a Linux machine (which can be a VM on Azure or a physical machine on-premises).

Configuration

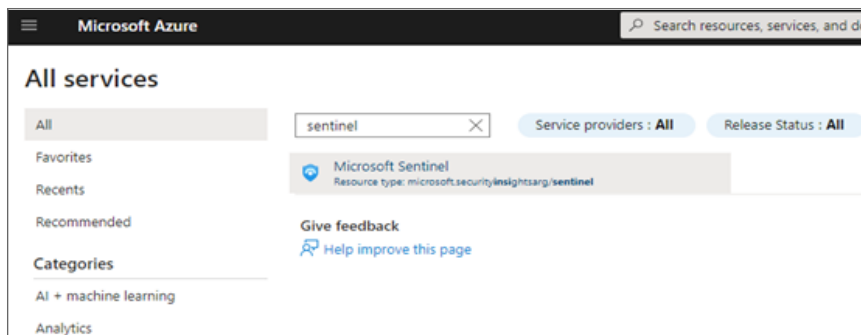
Follow the below steps to configure Microsoft Sentinel with SonicWall firewall:

1. [Deploying a Microsoft Sentinel Workspace](#)
2. [Installing the SonicWall Solution for Microsoft Sentinel](#)
3. [Installing the Operations Management Suite \(OMS\) or Log Analytics Agent](#)
4. [Configuring a Syslog Server on SonicWall Device](#)
5. [Validating the Data that Reaches Workspace](#)

Deploying a Microsoft Sentinel Workspace

To deploy a Microsoft Sentinel workspace:

1. Create a new resource using **deploy a custom template** that builds the resources needed for Microsoft Sentinel.
2. Select **QuickStart** mode template and create or select resource group.
Let deployment to be completed.
3. Do one of the following:
 - Navigate to the resource group.
 - Click the **Log Analytics** workspace resource.
4. Navigate to the Microsoft Sentinel service on **Azure Home** page.
If Microsoft Sentinel service is not presented on the home page, click **More services**.

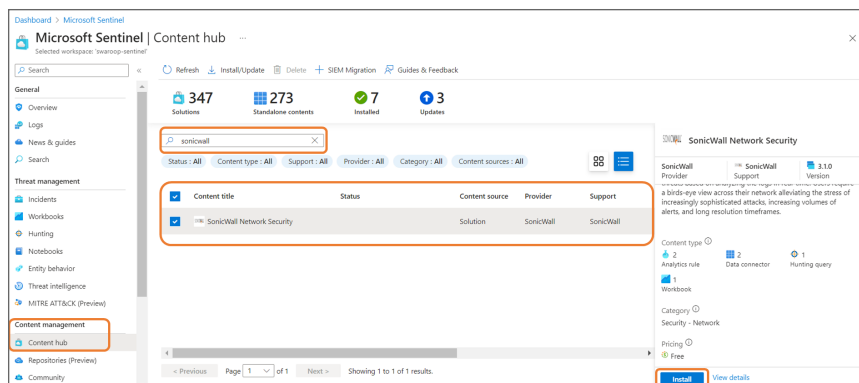


5. Click the Sentinel instance within the resource group you created.

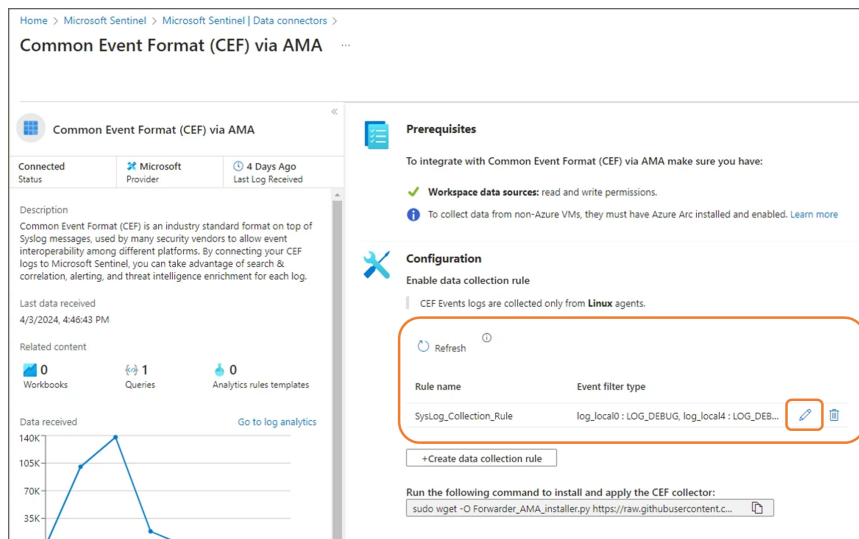
Installing the SonicWall Solution for Microsoft Sentinel

To install the SonicWall solution for Microsoft Sentinel:

1. Click the Sentinel instance within the resource group you created.
2. Install the SonicWall solution from the Content hub:
 - a. Navigate to **Content management > Content hub**.
 - b. Search for SonicWall.
 - c. Select the **SonicWall Network Security** Solution and click **Install**.



3. Configure the Common Event Format (CEF) via AMA data connector's data collection rule to set the event filter types (Syslog facilities) to collect.



4. Edit the data collection rule or create one if necessary. On the **Collect** tab of the rule's configuration, configure the following:

- LOG_LOCAL* (0-7) to LOG_DEBUG
- LOG_SYSLOG to LOG_DEBUG
- LOG_USER to LOG_DEBUG

Installing the Operations Management Suite (OMS) or Log Analytics Agent

The Operations Management Suite (OMS)/Log Analytics Agent provides a Syslog relay.

- ① **NOTE:** Make sure that this agent is installed on a host within the network and configure SonicOS to send ArcSight-formatted Syslog data to the agent. The Agent establishes a secure connection with Azure, so the log data is not sent to the cloud in plaintext.
- ① **NOTE:** Before installing one, review the requirements for the agent ([Supported operating systems](#)). Some versions of Linux have additional requirements with regard to Python that you should be aware of.

To install the Operations Management Suite (OMS) or Log Analytics Agent:

1. On the Microsoft Sentinel page, navigate to **Data Connectors** under **Configuration**.
 2. Search for **SonicWall** and Choose **[Deprecated] SonicWall Firewall via Legacy Agent** and follow the instructions to set up the forwarder agent on your machine.
 - ① **NOTE:** You can also run scripts to download the installer and execute it. They also include the workspace ID and primary key that the agent needs to connect to the workspace.
 3. Note down the IP address of the machine.
 - ① **NOTE:** This IP address is needed for SonicWall configuration.
- ① **IMPORTANT:** Log analytics agent will be retired on August 31, 2024, so make sure you migrate to Azure Monitor Agent (AMA). For more information, refer to [migration instructions](#).

Here are some other reference articles if you want to learn more about the Arc Agent and Azure Monitor Agent:

- Install the Arc Agent/Azure Connected Machine Agent
 - [Connected Machine agent prerequisites - Azure Arc](#)
 - [Overview of the Azure Connected Machine agent - Azure Arc](#)
- Install the Azure Monitor Agent extension
 - [Azure Monitor Agent overview - Azure Monitor](#)
 - [Manage Azure Monitor Agent - Azure Monitor](#)
- Install the Azure Monitor Agent (AMA) forwarder.
 - [Tutorial: Forward Syslog data to Microsoft Sentinel and Azure Monitor by using Azure Monitor Agent](#)

- Configure a Data Collection Rule (DCR)
 - [Tools for migrating to Azure Monitor Agent from legacy agents - Azure Monitor](#)
 - [Collect Syslog events with Azure Monitor Agent - Azure Monitor](#)
 - [Tutorial: Forward Syslog data to Microsoft Sentinel and Azure Monitor by using Azure Monitor Agent](#)

Configuring a Syslog Server on SonicWall Device

To configure a syslog server:

1. Configure a syslog server on your SonicWall device using syslog format as ArcSight (CEF).
2. Specify the IP address or Name of your Linux VM as the syslog server, and Syslog Facility should be **Local use 4**.



NOTE:

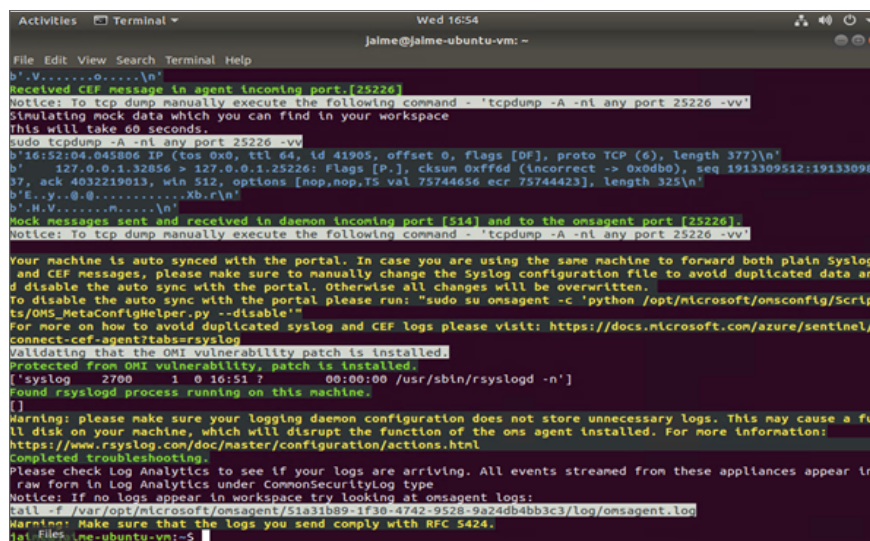
- The Syslog data is sent to the OMS Agent on UDP/514.
- For more information, refer to [Knowledge Base Article](#).

Validating the Data that Reaches Workspace

Once configured, you'll receive SonicOS-generated CEF messages in the Sentinel Workspace.

Validate that the OMS Agent is receiving CEF messages and can connect to Azure. If the validation initially fails, try again. The validation checks the connection to the workspace as well as a stream of CEF from a source. The firewall needs to be actively generating Syslog CEF messages for the validation to pass.

Log Analytics Agent



```
File Edit View Search Terminal Help
jaime@jaime-ubuntu-vm: ~
b'.V.....o.....\n'
Received CEF message in agent incoming port:[25226]
Notice: To tcp dump manually execute the following command - 'tcpdump -A -ni any port 25226 -vv'
Simulating mock data which you can find in your workspace
this will take 60 seconds.
sudo tcpdump -A -ni any port 25226 -vv
b'16:52:04.045806 IP (tos 0x0, ttl 64, id 41905, offset 0, flags [DF], proto TCP (6), length 377)\n'
b' 127.0.0.1.32856 > 127.0.0.1.25226: Flags [P.], cksum 0xffff (incorrect -> 0x0db0), seq 1913309512:1913309512, win 0, len 0, options [nop,nop,TS val 75744656, ecr 75744423], length 325\n'
b'E.y...0.0.....Xb.r\n'
b'.H.V.....f.....\n'
Mock messages sent and received in daemon incoming port [514] and to the omsagent port [25226]:
Notice: To tcp dump manually execute the following command - 'tcpdump -A -ni any port 25226 -vv'

Your machine is auto synced with the portal. In case you are using the same machine to forward both plain Syslog
and CEF messages, please make sure to manually change the Syslog configuration file to avoid duplicated data and
disable the auto sync with the portal. Otherwise all changes will be overwritten.
To disable the auto sync with the portal please run: "sudo su omsagent -c 'python /opt/microsoft/omsconfig/scripts/OHMS_MetaConfigHelper.py --disable'"
For more on how to avoid duplicated syslog and CEF logs please visit: https://docs.microsoft.com/azure/sentinel/connect-cef-agent#troubleshooting
Validating that the OMI vulnerability patch is installed.
Protected from OMI vulnerability, patch is installed.
['syslog 2700 1 0 16:51 7 00:00:00 /usr/sbin/rsyslogd -n']
Found rsyslogd process running on this machine.
[]
Warning: please make sure your logging daemon configuration does not store unnecessary logs. This may cause a full disk on your machine, which will disrupt the function of the oms agent installed. For more information:
https://www.rsyslog.com/doc/master/configuration/actions.html
Completed troubleshooting.
Please check Log Analytics to see if your logs are arriving. All events streamed from these appliances appear in raw form in Log Analytics under CommonSecurityLog type
Notice: If no logs appear in workspace try looking at omsagent logs:
tail -f /var/opt/microsoft/omsagent/51a31b89-1f30-4742-9528-9a24db4bb3c3/log/omsagent.log
Warning: Make sure that the logs you send comply with RFC 5424.
jaime@jaime-ubuntu-vm:~$
```

NOTE:

- Troubleshoot your CEF or Syslog data connector according to <https://learn.microsoft.com/en-us/azure/sentinel/troubleshooting-cef-syslog?tabs=cef>.
- `sudo wget -O cef_troubleshoot.py, https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/CEF/cef\_troubleshoot.py (python cef_troubleshoot.py [WorkspaceID]).`

Azure Monitor Agent

```
james@jame-mundm-mn-2 sudo apt -O Sentinel_AMA_troubleshoot.py https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Sentinel_AMA_troubleshoot.py&sudo python3 Sentinel_AMA_troubleshoot.py --cef
--2024-04-04 13:28:47-- https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/DataConnectors/Syslog/Sentinel_AMA_troubleshoot.py
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 49903 (49K) [text/plain]
Saving to: 'Sentinel_AMA_troubleshoot.py'

Sentinel_AMA_troubleshoot.py      100%[=====] 49.73K  --.-KB/s  in 0.009s

2024-04-04 13:28:47 (5.39 MB/s) - 'Sentinel_AMA_troubleshoot.py' saved [49903/49903]

The scenario chosen is: CEF

Starting to run the validation script for the cef scenario
Please validate you are sending messages to the agent machine

----- Starting validation tests for AMA -----
verify_ama_agent_service_is_running-----> Success
Detected AMA running version- 1.39.6
Detected ABC installed on the machine: arcmapagent version 1.39.02628.1411
verify_ama_agent_is_running-----> Success

----- Starting validation tests for data collection rules -----
verify_dcr_exists-----> Success
verify_dcr_content_has_stream-----> Success
verify_dcr_has_valid_content-----> Success
check_multi_homing-----> Success

----- Starting validation tests for the Syslog daemon -----
verify_syslog_daemon_listening-----> Success
verify_syslog_daemon_forwarding_configuration--> Success

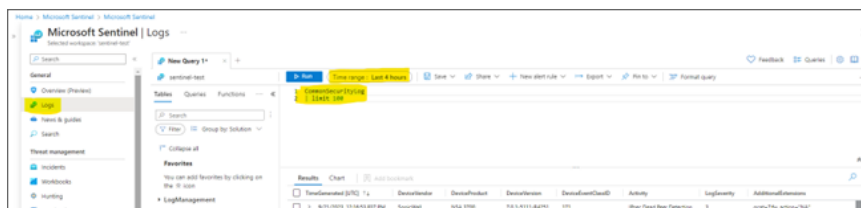
----- Starting validation tests for the operating system -----
verify_selinux_state-----> Success
verify_iptables_policy_permissive-----> Success
verify_iptables_rules_permissive_514-----> Success
verify_iptables_rules_permissive_28330-----> Success
verify_free_disk_space-----> Success

----- Starting validation tests for capturing incoming events -----
Attempting to capture events using tcpdump. This could take up to 10 seconds.
listen_to_incoming_events-----> Success
Found CEF in stream. Please verify CEF events arrived at your workspace
All tests passed successfully
This script generated an output file located here - /tmp/troubleshooter_output_file.log
Please review it if you would like to get more information on failed tests.

If you would like to open a support case please run this script with the 'collect' feature flag in order to collect additional system data for troubleshooting.'python Sentinel_AMA_troubleshoot.py [STREAM OPTION] collect'
james@jame-mundm-mn-2
```

To validate data on Microsoft Sentinel workspace:

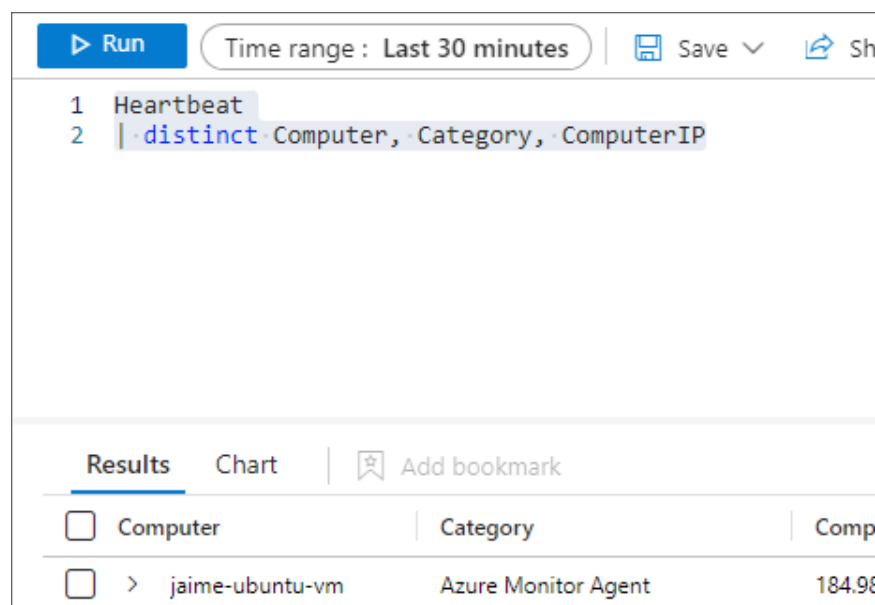
1. On the Microsoft Sentinel workspace, navigate to the **General > Logs** link.
2. Set a short time range that covers a period where data should have been ingested. It can take several minutes to begin seeing data in Log Analytics. Wait for more time if you do not see data right away.
3. Enter a basic query to confirm data is arriving at Sentinel and click **Run**.



To get AMA Heartbeat Logs:

Use **Heartbeat** query with a short time range (last 30 minutes):

- Heartbeat
- | distinct Computer, Category, ComputerIP



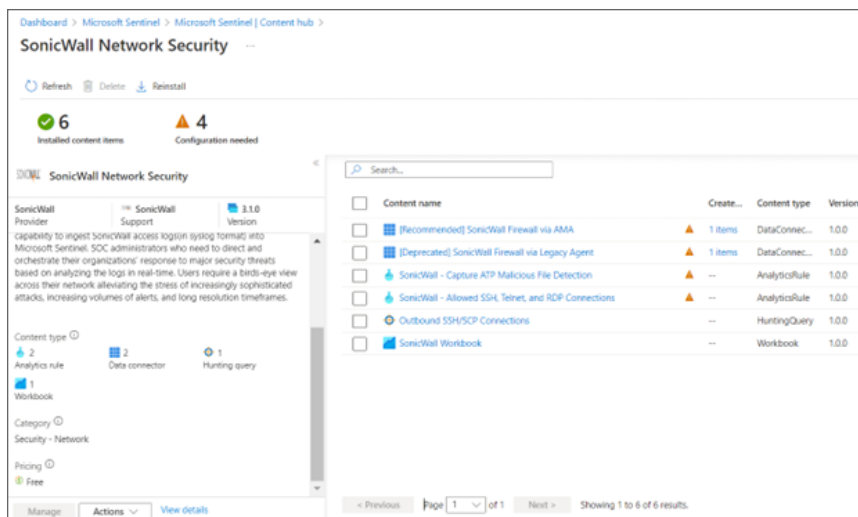
① | **NOTE:** This only applies to AMA, not the OMS/Log Analytics Agent.

Microsoft Sentinel Content Type

The SonicWall Data connector includes a Workbook containing a variety of queries for various security services as well as other traffic and security insights.

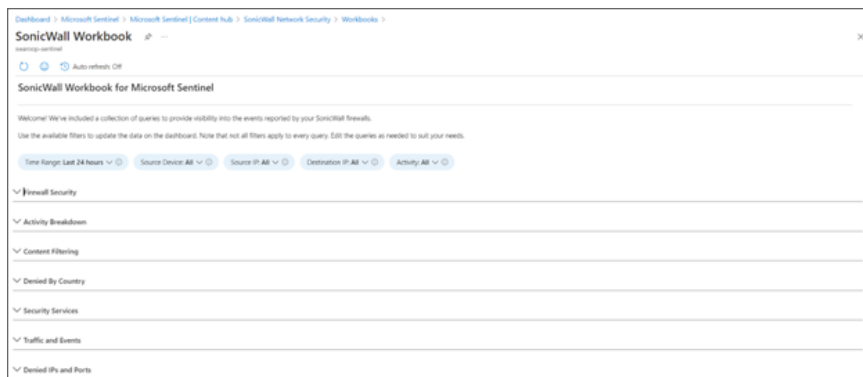
To navigate to Microsoft Sentinel content types:

1. Navigate to the **Content management > Content hub** link.
2. Click the installed **SonicWall Network Security** Solution to view the content types:
 - [Workbook](#)
 - [Analytics Rules](#)
 - [Hunting Query](#)

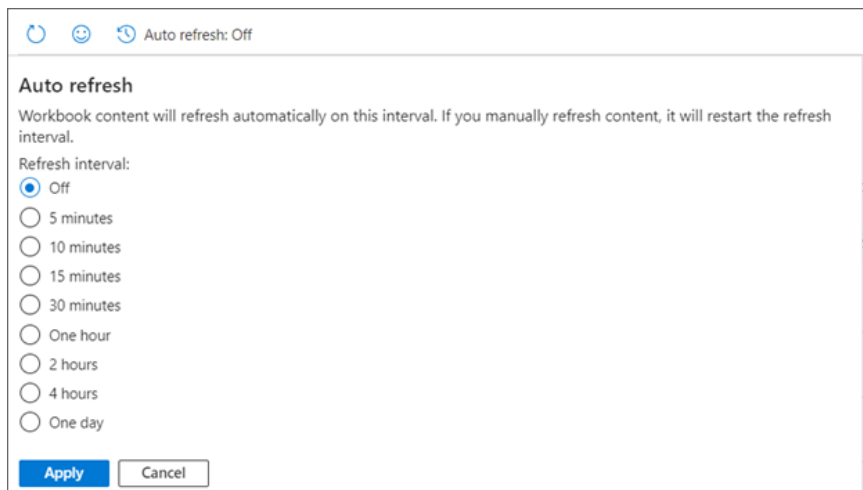


Workbook

SonicWall Workbook contains the collection of queries to provide visibility into the events reported by the SonicWall firewalls.



You can also select the Auto refresh time for the queries.



Analytics Rules

Topics:

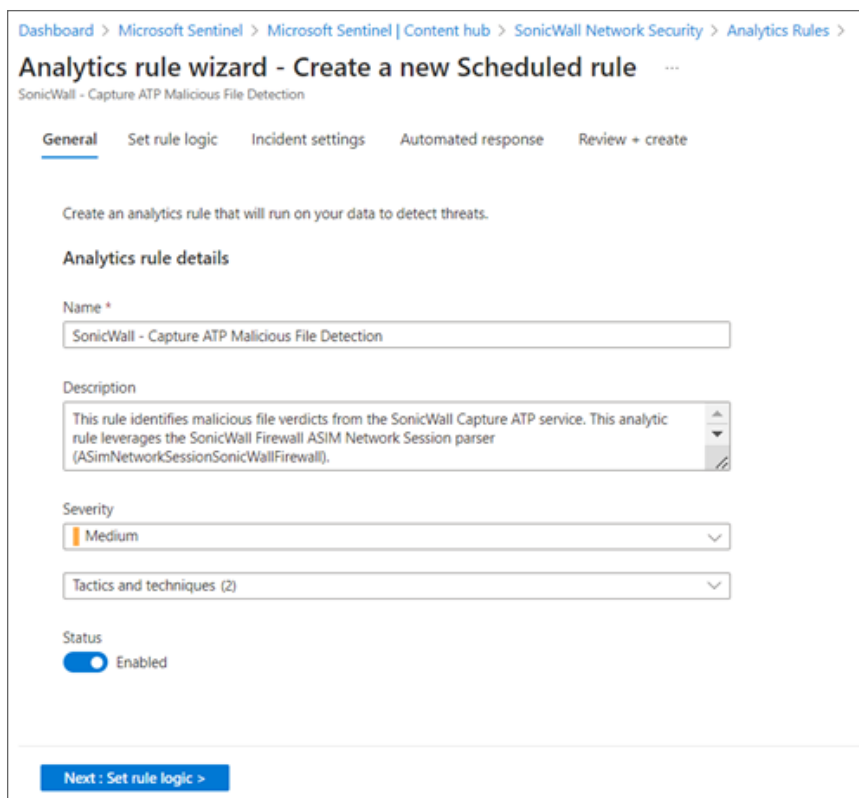
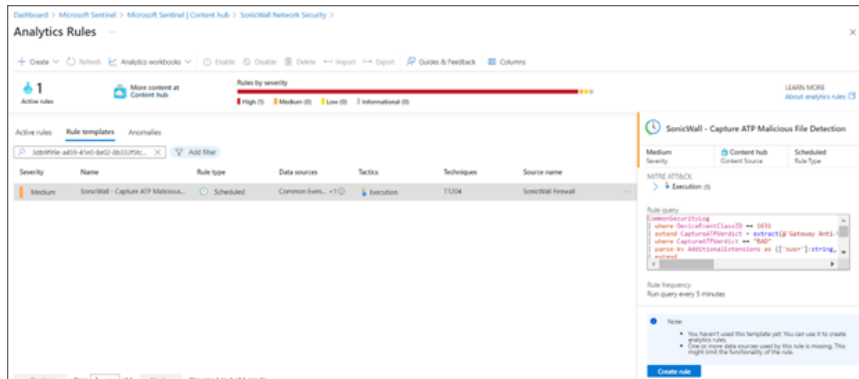
- [SonicWall - Capture ATP Malicious File Detection](#)
- [SonicWall - Allowed SSH, Telnet, and RDP Connections](#)

SonicWall - Capture ATP Malicious File Detection

SonicWall- Capture ATP Malicious File Detection identifies malicious file verdicts from the SonicWall Capture ATP service. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

To set rules logic:

1. Click the Analytics rule to create the rule and set the rules logic.



2. Navigate to **Incident Settings**, select the **Automated** response.

3. Review the settings and click **Save** to schedule the rule.

The screenshot shows the 'Analytics rule wizard - Create a new Scheduled rule' interface in Microsoft Sentinel. The 'Review & create' tab is active, displaying the following details:

- Name:** SonicWall - Capture ATP Malicious File Detection
- Description:** This rule identifies malicious file verdicts from the SonicWall Capture ATP service. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).
Ref: <https://www.sonicwall.com/products/capture-advanced-threat-protection/>
Ref: <https://www.sonicwall.com/support/knowledge-base/how-to-view-threat-reports-capture-atp/170505384713913/>
- MITRE ATTACK:** Execution (x)
- Severity:** Medium
- Status:** Enabled
- Analytics rule settings:**
 - Rule query:** CommonSecurityLog | where DeviceEventClassID == 1631 | extend CaptureATPVerdict = extract@Gateway Anti-Virus Status (7%), -1, Message | where CaptureATPVerdict == "BAD" | parse-av-AdditionalExtensions as [EventID:string, ThreatID:string with [delimeter=":"], Av_Verdict:string] | extend NetworkProtocol = tostring@Protocol contains "-" and Protocol contains "7" | topper@Time_start@ "-" : Protocol@, topper@Time_end@ "-" : Protocol@, NetworkApplicationProtocol = tostring@upper@Time_start@ "-" : Protocol@ | project TimeGenerated, DeviceModel = DeviceProduct, SerialNumber = Computer, SrcIPAddr = SourceIP, SrcUsername = coalesce@Source, SourceUsername, NetworkProtocol, NetworkApplicationProtocol, RequestURL, File = url_decode@incoming@RequestURL, /2-/3, Hash = fileid, Verdict = CaptureATPVerdict
 - Rule frequency:** Run query every 5 minutes
 - Rule period:** Last 5 minutes data
 - Rule start time:** Automatic

Buttons at the bottom: Previous, Save.

SonicWall - Allowed SSH, Telnet, and RDP Connections

SonicWall - Allowed SSH, Telnet, and RDP Connections identifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

To set rules logic:

1. Click the Analytics rule to create the rule and set the rules logic.

Dashboard > Microsoft Sentinel > Microsoft Sentinel | Content hub > SonicWall Network Security > Analytics Rules >

Analytics rule wizard - Create a new Scheduled rule

SonicWall - Allowed SSH, Telnet, and RDP Connections

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *

SonicWall - Allowed SSH, Telnet, and RDP Connections

Description

This rule identifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

Severity

Medium

Tactics and techniques (24)

Status

Enabled

Next: Set rule logic >

Dashboard > Microsoft Sentinel > Microsoft Sentinel | Content hub > SonicWall Network Security > Analytics Rules >

Analytics rule wizard - Create a new Scheduled rule

SonicWall - Allowed SSH, Telnet, and RDP Connections

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name *

SonicWall - Allowed SSH, Telnet, and RDP Connections

Description

This rule identifies allowed inbound SSH, Telnet, and RDP connections. This analytic rule leverages the SonicWall Firewall ASIM Network Session parser (ASimNetworkSessionSonicWallFirewall).

Severity

Medium

Tactics and techniques (24)

Status

Enabled

Next: Set rule logic >

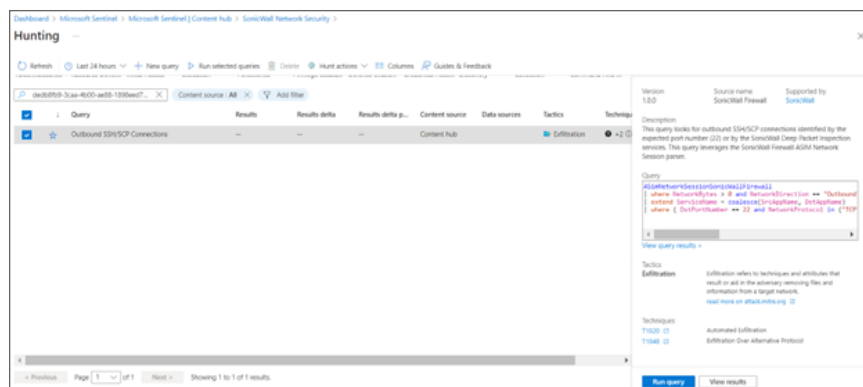
2. Navigate to **Incident Settings**, select the **Automated** response.
3. Review the settings and click **Save** to schedule the rule.

Hunting Query

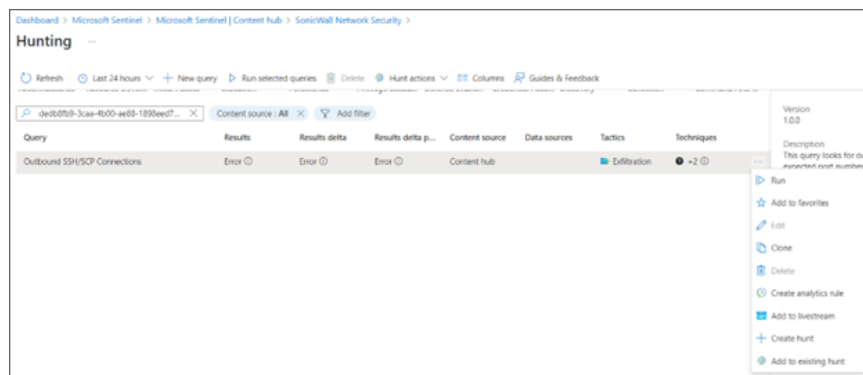
Outbound SSH/SCP Connections query looks for outbound SSH/SCP connections identified by the expected port number (22) or by the SonicWall Deep Packet Inspection services. This query leverages the SonicWall Firewall ASIM Network Session parser.

To run query:

1. Run the query in one of following ways:
 - Select the Threat hunting query and click **Run** query.



- Scroll right and click on three dots the end and run the query.
- ① | **NOTE:** You can also create your own hunting query using this.



For more information about setup instructions, refer to the [SonicWall Firewall-Sentinel Integration KB Article](#). Here is the [data connector instructions Article](#).

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The [Support Portal](#) provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The [Support Portal](#) enables you to:

- View [Knowledge Base](#) articles and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Microsoft Sentinel Integration Guide

Updated - April 2024

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.