Managing firewall rules

Scenario: As a security network tools engineer, you sometimes need to make sure that firewall rules are set correctly. You can do this at the firewall interface, but if a rule affects an application you may need to check which rules, if any, are involved with certain applications. This is especially true if the network operations center (NOC) has received tickets for applications that exhibit network timeout behavior. As part of your ongoing security policy audits, you want to identify rarely used rules and decide if the rare usage is an indicator of compromise. You can use Splunk software to ensure that you have rules properly configured to allow or block traffic as needed. You can also identify commonly or uncommonly used rules to optimize your firewall.

Prerequisites

To succeed in implementing this use case, you need the following dependencies, resources, and information.

- People: Security tools engineer
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Firewall data

How to use Splunk software for this use case

You can run many searches with Splunk software to manage firewall rules. Depending on what information you have available, you might find it useful to identify some or all of the following:

- Blocked traffic to host
- Blocked traffic from host
- Rarely used firewall rules

Results

Security policy audits commonly impact success with this use case. In addition, measuring impact and benefit is critical to assessing the value of IT operations. The following are example metrics that can be useful to monitor when implementing this use case:

- Number of firewall rule related incidents over time
- Number of applications or users impacted by errors with rules
- Productivity time lost due to firewall rule related errors

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.
Additional resources

This use case is also included in the IT Essentials Learn app, which provides more information about how to implement the use case successfully in your IT maturity journey. In addition, these Splunk resources might help you understand and implement this use case:

- Conf talk: [From endpoint to firewall - Building effective threat perimeters with Cisco and Splunk](#)