AWS re:Start

LAB

Malware Protection

WEEK 4

aws re/start

Overview

Malware, short for malicious software, refers to any intrusive software developed by cybercriminals to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan horses, spyware, adware, and ransomware.

Firewalls are like physical security walls situated between an organization's internal network and any external public networks such as the internet. The firewall protects an internal network from access by unauthorized users on an external network.

Users need access to the internet for business reasons, but they can inadvertently download malware, which can impact network and data security.

Malware threats can be present, and organizations can use various techniques and services to mitigate these threats. This lab focuses on countermeasure techniques using a firewall.

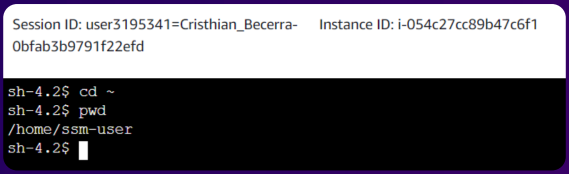
In this scenario, a company has hired you as a new security engineer, and the company has tasked you with hardening the company’s security perimeter. There have been reports of users accidentally downloading malware after accessing specific websites. The IT team has provided you with the URLs of the sites hosting the malware. It is your job to find a solution to mitigate access to these malicious actor files.

Task 1

Confirm Reachability

Log into the test instance

Log into the TestInstance EC2 server via AWS Systems Manager Session Manager.

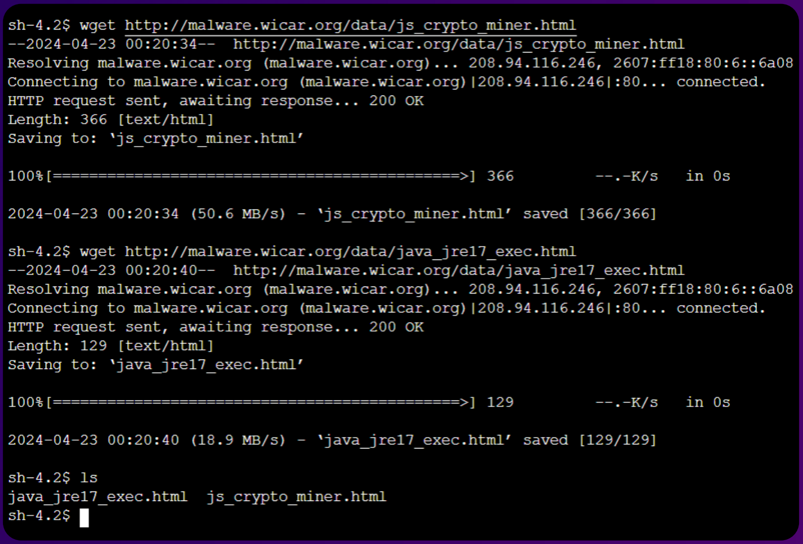


Session ID: user3195341=Cristhian_Becerra-0bfab3b9791f22efd   Instance ID: i-054c27cc89b47c6f1

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ █
```

Download the malware files

Download the test malware files inside the protected lab environment. The URL hosting the malware files is accessible through the current network firewall.



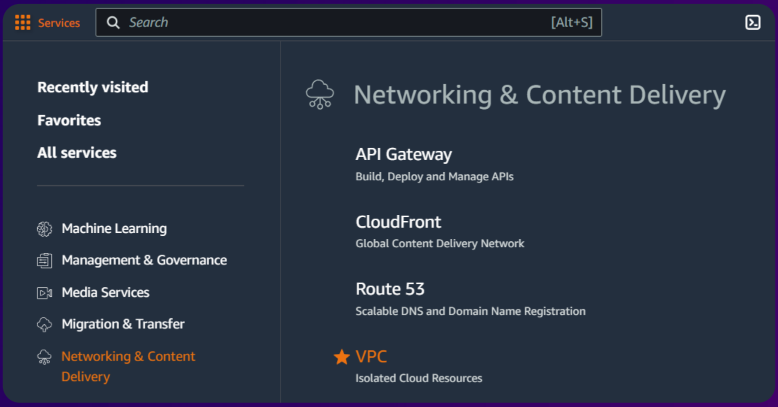
```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2024-04-23 00:20:34--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: ‘js_crypto_miner.html’

100%[============================================>] 366         --.-K/s   in 0s

2024-04-23 00:20:34 (50.6 MB/s) - ‘js_crypto_miner.html’ saved [366/366]

sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-04-23 00:20:40--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: ‘java_jre17_exec.html’

100%[============================================>] 129         --.-K/s   in 0s

2024-04-23 00:20:40 (18.9 MB/s) - ‘java_jre17_exec.html’ saved [129/129]

sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$ █
```

Task 2

Inspect the network firewall

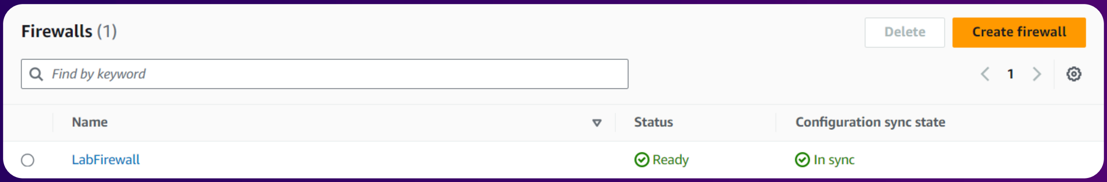
Step 1: Access the VPC management console

Open the AWS Management Console, and select VPC.



Step 2: Review VPC Network Firewalls

Navigate to the **Firewalls** section. The LabFirewall is listed.



	Name	Status	Configuration sync state
○	LabFirewall	✓ Ready	✓ In sync

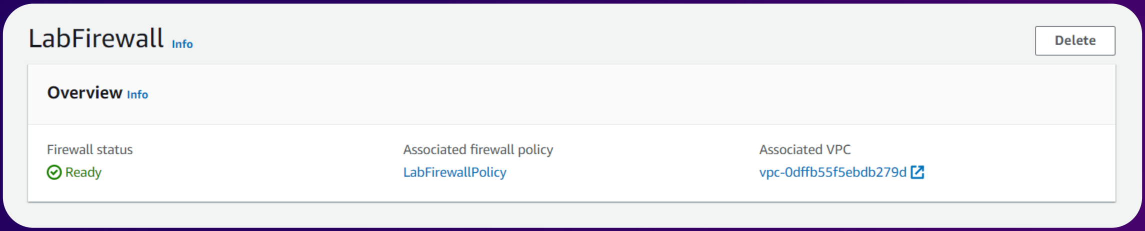
aws re/start

Task 2

Inspect the network firewall

Step 3: Review firewall policy

Select the LabFirewall and review its associated firewall policy LabFirewallPolicy.



LabFirewall Info

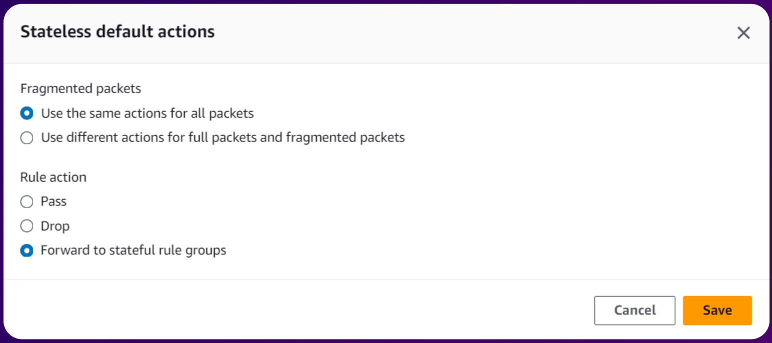
Delete

Overview Info

Firewall status	Associated firewall policy	Associated VPC
✓ Ready	LabFirewallPolicy	vpc-0dffb55f5ebdb279d

Step 4: Stateless default actions

In the **Stateless default actions** section from LabFirewallPolicy, configure the following options.



Stateless default actions

Fragmented packets

● Use the same actions for all packets

○ Use different actions for full packets and fragmented packets

Rule action

○ Pass

○ Drop

● Forward to stateful rule groups

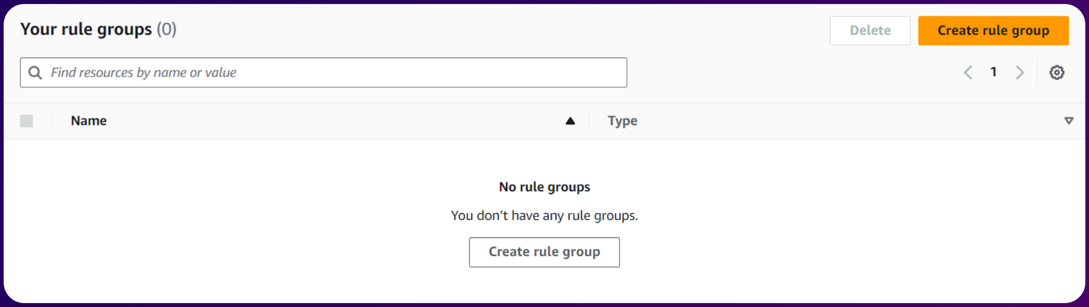
Cancel Save

Task 3

Create a firewall rule group

Step 1: Create rule group

Navigate to the **Network Firewall rule groups** section and select Create rule group.



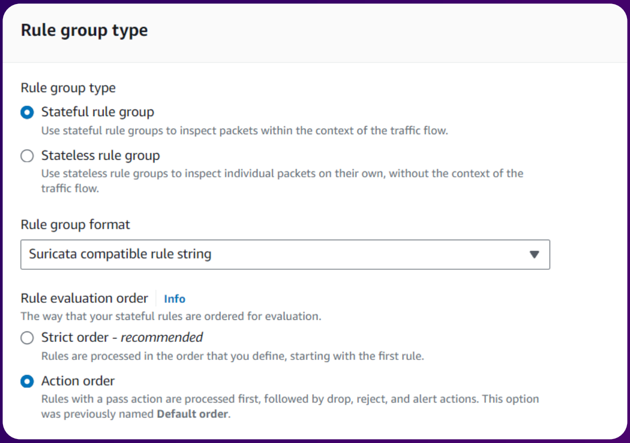
Your rule groups (0)

No rule groups

You don't have any rule groups.

Step 2: Rule group type

In the **Rule group type** section, configure the following options.



Rule group type

Rule group type

● Stateful rule group
Use stateful rule groups to inspect packets within the context of the traffic flow.

○ Stateless rule group
Use stateless rule groups to inspect individual packets on their own, without the context of the traffic flow.

Rule group format

Suricata compatible rule string ▼

Rule evaluation order Info
The way that your stateful rules are ordered for evaluation.

○ Strict order - *recommended*
Rules are processed in the order that you define, starting with the first rule.

● Action order
Rules with a pass action are processed first, followed by drop, reject, and alert actions. This option was previously named **Default order**.

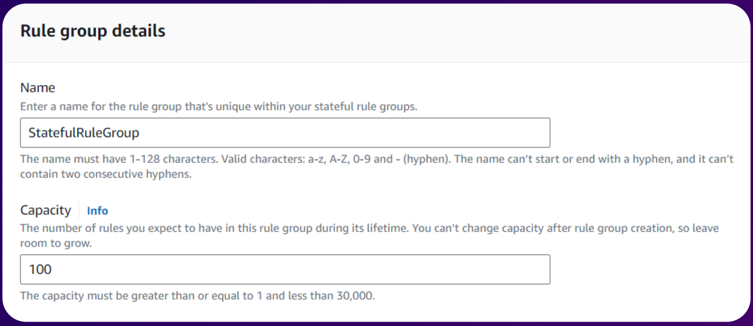
aws re/start

Task 3

Create a firewall rule group

Step 3: Rule group details

In the **Rule group details** section, configure the following options.



Rule group details

Name

Enter a name for the rule group that's unique within your stateful rule groups.

StatefulRuleGroup

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

Capacity Info

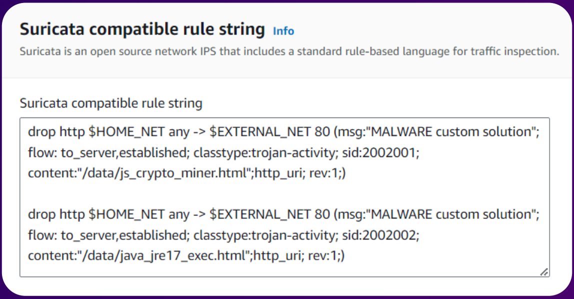
The number of rules you expect to have in this rule group during its lifetime. You can't change capacity after rule group creation, so leave room to grow.

100

The capacity must be greater than or equal to 1 and less than 30,000.

Step 4: Suricata compatible rule string

In the **Suricata compatible rule string** section, enter the following code into the text box. The two Suricata rules will block traffic that matches the malicious URLs.



Suricata compatible rule string Info

Suricata is an open source network IPS that includes a standard rule-based language for traffic inspection.

Suricata compatible rule string

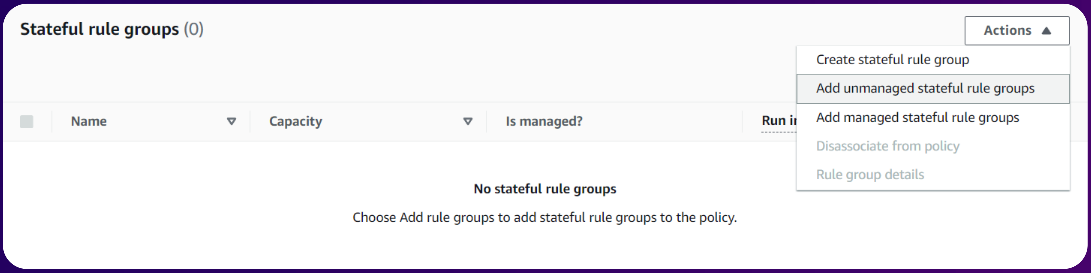
```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution";
flow: to_server,established; classtype:trojan-activity; sid:2002001;
content:"/data/js_crypto_miner.html";http_uri; rev:1;)

drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution";
flow: to_server,established; classtype:trojan-activity; sid:2002002;
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

Task 4

Attach a rule group to the network firewall

Add unmanaged stateful rule group

In the **Stateful rule groups** section from LabFirewall select Add unmanaged stateful rule groups.



Stateful rule groups (0)

Name	Capacity	Is managed?	Run i

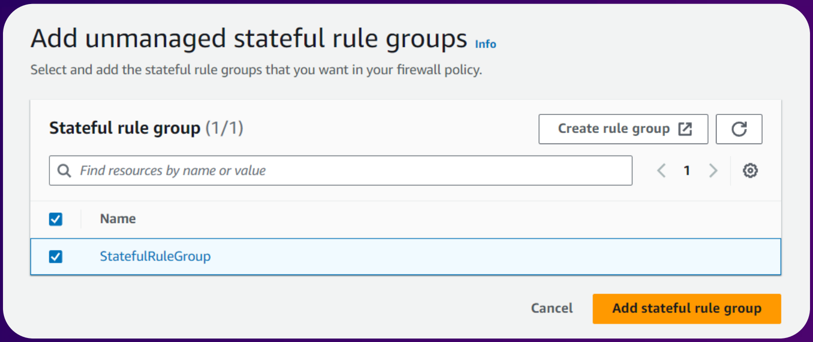
No stateful rule groups

Choose Add rule groups to add stateful rule groups to the policy.

Actions ▲
Create stateful rule group
Add unmanaged stateful rule groups
Add managed stateful rule groups
Disassociate from policy
Rule group details

Add stateful rule group

Add the existing stateful rule group StatefulRuleGroup to the firewall policy.



Add unmanaged stateful rule groups Info

Select and add the stateful rule groups that you want in your firewall policy.

Stateful rule group (1/1)

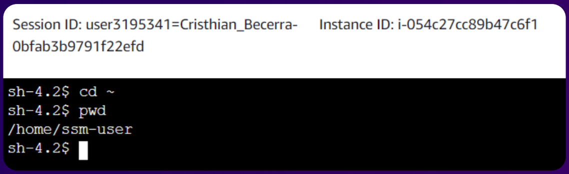
☑	Name
☑	StatefulRuleGroup

Task 5

Validate the solution

Log into the test instance

Log again into the TestInstance EC2 server via AWS Systems Manager Session Manager.

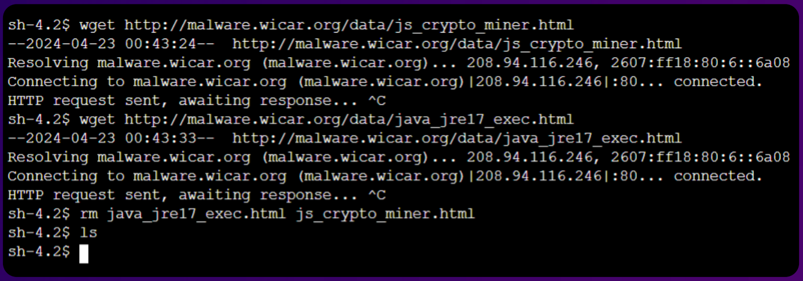


Session ID: user3195341=Cristhian_Becerra-0bfab3b9791f22efd   Instance ID: i-054c27cc89b47c6f1

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ 
```

Test the network firewall

Attempt to access the malicious files. The output confirms that the malware sites and files are no longer accessible and have been successfully blocked by the network firewall. Then, remove the test malware files from the protected lab environment.



```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2024-04-23 00:43:24--  http://malware.wicar.org/data/js_crypto_miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... ^C
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2024-04-23 00:43:33--  http://malware.wicar.org/data/java_jre17_exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.246, 2607:ff18:80:6::6a08
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.246|:80... connected.
HTTP request sent, awaiting response... ^C
sh-4.2$ rm java_jre17_exec.html js_crypto_miner.html
sh-4.2$ ls
sh-4.2$ 
```

Conclusions

VPC Network Firewalls

VPC Network Firewalls provide essential protection by filtering inbound and outbound traffic based on predefined rules, enhancing network security in AWS environments.

Protected enviroments

Protected environments, such as sandboxes, serve as isolated testing environments to safely analyze and evaluate malware behavior without risking the production environment.

The wget command

The wget command is a powerful tool used to retrieve files from remote servers, including malware samples for analysis and testing in a controlled environment.

Stateless default actions

Stateless default actions in firewall policies define how traffic is handled without maintaining session state, allowing for efficient packet filtering and security enforcement.

Stateful rule groups

Stateful rule groups in network firewalls maintain context-aware state information to make decisions about allowing or blocking traffic, offering more advanced security capabilities for threat prevention and detection.

aws re/start

Cristhian Becerra

cristhian-becerra-espinoza

+51 951 634 354

cristhianbecerra99@gmail.com

Lima, Peru