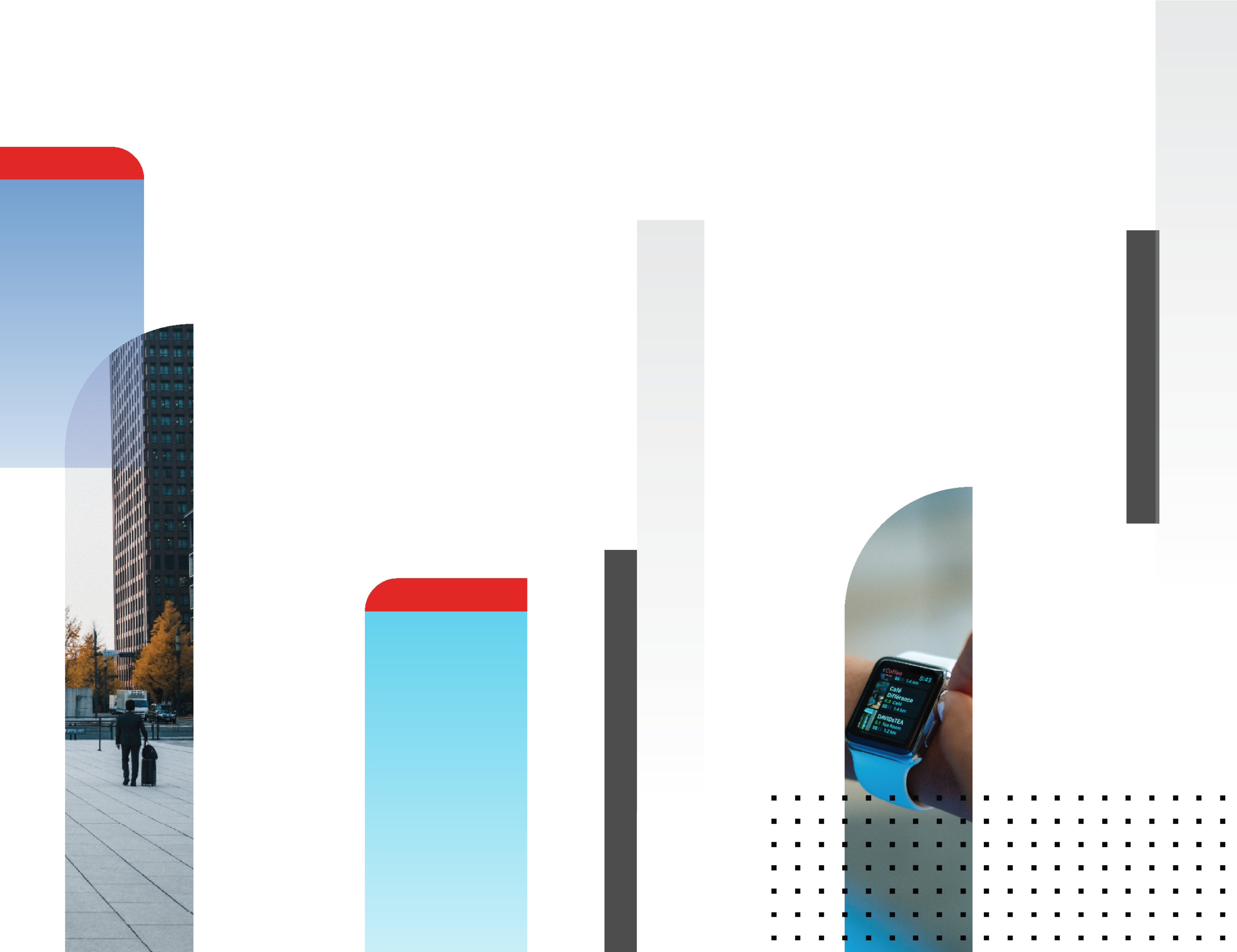
Administration Guide

AWS Firewall Rules 7.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

November 16, 2021
AWS Firewall Rules 7.0 Administration Guide
00-700-758732-20211116

TABLE OF CONTENTS

AWS network firewall partner rule groups

AWS network firewall partner rule groups are contract-based firewall signatures that Fortinet offers to augment the basic protections that AWS Network Firewall offers. With these rule groups, AWS Network Firewall customers can choose prepackaged rules based on their requirements. The following lists the rule groups on offer:

Rule groups	Type	What this rule group detects
Fortinet-ips-client-enable-rulegroup1	Intrusion prevention system (IPS)	Attempts to exploit vulnerabilities in common client applications, including desktop software.
Fortinet-ids-client-alert-rulegroup1	Intrusion detection system (IDS)	
Fortinet-ips-malware-enable-rulegroup1	IPS	Communication attempts from malware backdoors, worms, and remote access trojans, including command and control traffic.
Fortinet-ids-malware-alert-rulegroup1	IDS	
Fortinet-ips-serveros-enable-rulegroup1	IPS	Vulnerabilities targeting operating systems (OS) and common server applications, including DNS, email, and remote access.
Fortinet-ips-serveros-enable-rulegroup2		
Fortinet-ids-serveros-alert-rulegroup1	IDS	
Fortinet-ids-serveros-alert-rulegroup2		
Fortinet-ips-webclient-enable-rulegroup1	IPS	Exploits targeting vulnerabilities in web browsers, including Chrome, Firefox, Internet Explorer, Edge, and so on.
Fortinet-ids-webclient-alert-rulegroup1	IDS	
Fortinet-ips-webapp-enable-rulegroup1	IPS	Exploits targeting vulnerabilities in common web applications, including popular content management platforms such as WordPress and Joomla.
Fortinet-ids-webapp-alert-rulegroup1	IDS	
Fortinet-ips-webserver-enable-rulegroup1	IPS	Exploits targeting web server vulnerabilities, including web servers such as Apache and proxy web servers such as Squid.
Fortinet-ids-webserver-alert-rulegroup1	IDS	

The listed rule groups allow for network traffic to be examined for predetermined attack patterns. This is accomplished by matching the signatures of incoming packets to the signature available in the rule groups. There are two types of rule groups:

Type	Description
IPS	Can perform the DROP or ALERT action. If alert logging is configured, an alert is sent to the firewall logs for each matching rule. The packet is then forwarded or dropped based on the action setting in the first matched rule. Use of this rule group helps prevent the ingress of malicious traffic into the network. For information regarding stateful actions, see AWS Network Firewall - Rule Actions.
IDS	When a signature matches, sends an ALERT and forwards the packet to its intended destination. Using this rule group helps detect and log malicious activity without disrupting traffic.

You can use any combination of the listed IPS and IDS rule groups in a firewall policy, as long as it is within the firewall policy rule limit of 30000 rules. When you apply IPS and IDS rule groups from the same category, the packet is evaluated against all rules with drop and alert action settings. The packet is then handled according to the action setting of the first rule that matched the packet. For information regarding stateful actions, see AWS Network Firewall - Rule Actions.

The following presents three use cases for AWS network firewall rule groups:

Use case	Applicable rule groups
If the protected network contains endpoint devices such as desktop computers, laptops, smartphones, and tablets, you must secure the network against common client vulnerabilities that affect applications, as well as OS and web browser-based malware and vulnerabilities.	• Fortinet-ips-client-enable-rulegroup1 • Fortinet-ips-malware-enable-rulegroup1 • Fortinet-ips-webclient-enable-rulegroup1
If the protected network contains servers or hosted services including web applications, databases, email, DNS, and other services that must be secured against targeted attacks.	• Fortinet-ips-serveros-enable-rulegroup1 and rulegroup2 • Fortinet-ips-malware-enable-rulegroup1 • Fortinet-ips-webapp-enable-rulegroup1 • Fortinet-ips-webserver-enable-rulegroup1
Scenario where you must monitor resource activity without disrupting connectivity and traffic flow.	Endpoint-based rule groups: • Fortinet-ids-client-alert-rulegroup1 • Fortinet-ids-malware-alert-rulegroup1 • Fortinet-ids-webclient-alert-rulegroup1 Server-based rule groups: • Fortinet-ids-serveros-alert-rulegroup1 and rulegroup2

Use case	Applicable rule groups
	- Fortinet-ids-malware-alert-rulegroup1 - Fortinet-ids-webapp-alert-rulegroup1 - Fortinet-ids-webserver-alert-rulegroup1

The rules listed for the first and second use cases are of the IPS type, which means that when a signature match occurs, the packet is dropped. You can use these rule groups with their IDS counterparts to design a more robust firewall with logging of malicious activity. See AWS Network Firewall - Rule Actions. The third use case uses IDS rule groups.

Each rule group has a predefined capacity for the maximum number of rules in the rule group. You must consider the capacity when configuring the firewall policy, as the AWS firewall policy has a global rule limit of 30000 rules. Selecting seven rule groups currently occupies 20000 rules. The following shows the capacity for each rule group:

Rule group	Capacity (maximum number of rules)
Fortinet-ips-client-enable-rulegroup1 / Fortinet-ids-client-alert-rulegroup1	5000
Fortinet-ips-malware-enable-rulegroup1 / Fortinet-ids-malware-alert-rulegroup1	2000
Fortinet-ips-serveros-enable-rulegroup1 / Fortinet-ids-serveros-alert-rulegroup1	5000
Fortinet-ips-serveros-enable-rulegroup2 / Fortinet-ids-serveros-alert-rulegroup2	2500
Fortinet-ips-webclient-enable-rulegroup1 / Fortinet-ids-webclient-alert-rulegroup1	1500
Fortinet-ips-webapp-enable-rulegroup1 / Fortinet-ids-webapp-alert-rulegroup1	2500
Fortinet-ips-webserver-enable-rulegroup1 / Fortinet-ids-webserver-alert-rulegroup1	1500

You cannot select rule groups with capacity that adds up to more than 30000 rules in a single firewall policy.

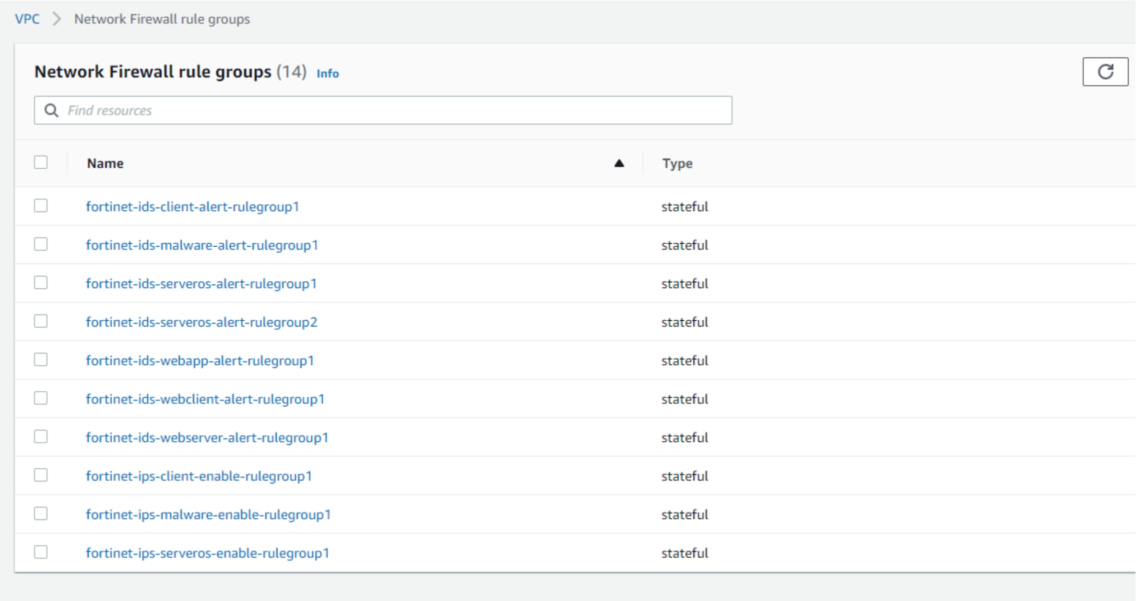
Sharing AWS firewall rules resources

To share AWS firewall rules resources:

1. After Fortinet has shared the firewall rules, in the AWS management console, go to *Resource Access Manager* > *Shared with me* > *Resource shares*.

   If you cannot see the new invitation in *Resource shares*, contact Customer Service & Support or your Fortinet representative, as they must resend the invitation.

2. Go to the AWS firewall rules resource, and click *Accept resource share*.
3. Go to *Resource Access Manager* > *Shared with me* > *Shared resources* and confirm that multiple rule groups are visible.
4. Go to *VPC Dashboard* > *Network Firewall* > *Network Firewall rule groups* and confirm that the rule groups are visible.



VPC > Network Firewall rule groups

Network Firewall rule groups (14) Info

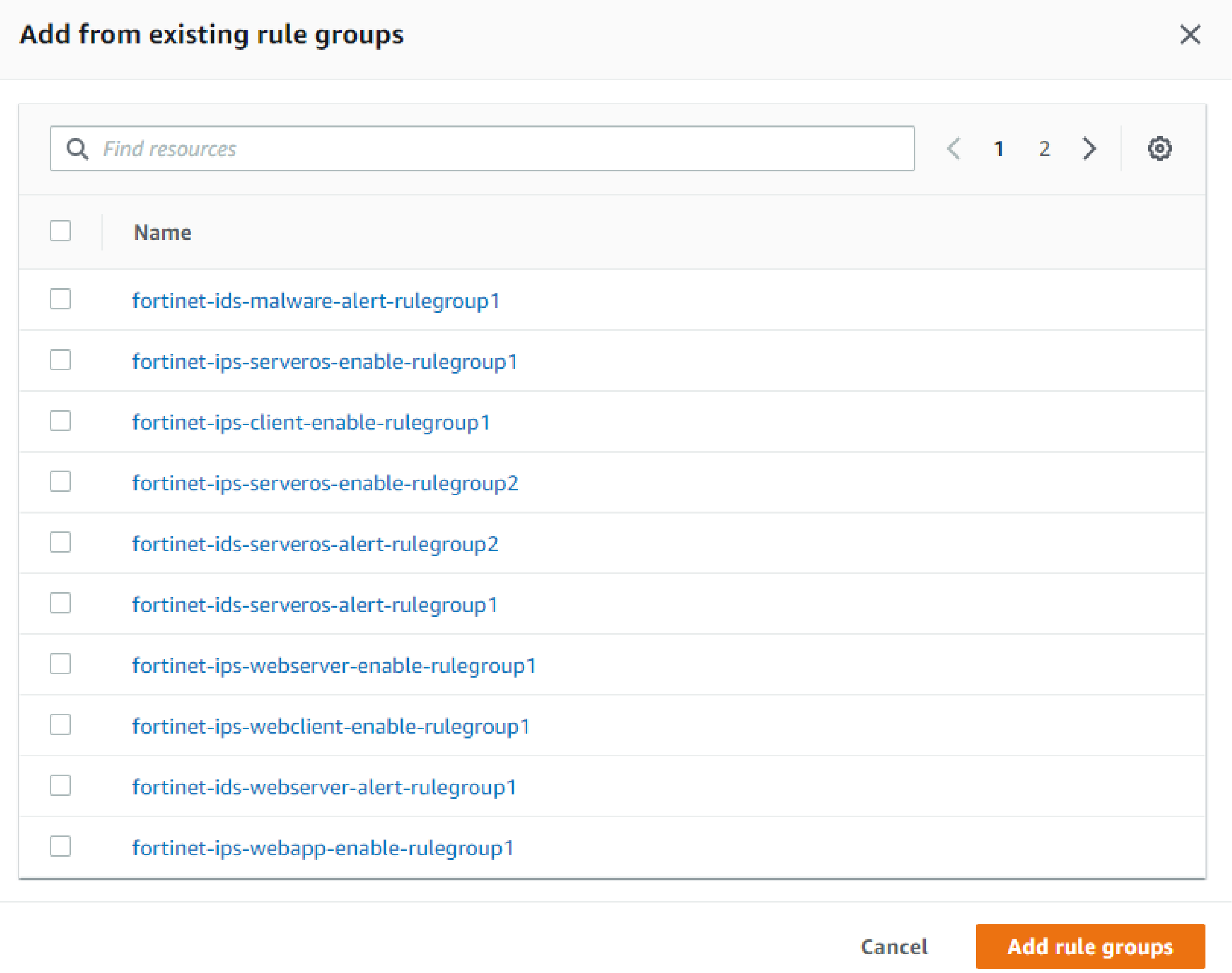
Find resources

□	Name ▲	Type
□	fortinet-ids-client-alert-rulegroup1	stateful
□	fortinet-ids-malware-alert-rulegroup1	stateful
□	fortinet-ids-serveros-alert-rulegroup1	stateful
□	fortinet-ids-serveros-alert-rulegroup2	stateful
□	fortinet-ids-webapp-alert-rulegroup1	stateful
□	fortinet-ids-webclient-alert-rulegroup1	stateful
□	fortinet-ids-webserver-alert-rulegroup1	stateful
□	fortinet-ips-client-enable-rulegroup1	stateful
□	fortinet-ips-malware-enable-rulegroup1	stateful
□	fortinet-ips-serveros-enable-rulegroup1	stateful

Attaching rule groups to a firewall policy

To attach rule groups to a firewall policy:

1. Go to *VPC Dashboard* > *Network Firewall* > *Firewalls*.
2. Create a firewall policy or use an existing policy.
3. Under *Stateless default actions* and *Stateful rule and default action*, configure the desired actions.
4. Under *Stateful Rule Groups*, select *Add Rule Groups*.
5. Select the desired rule groups, then click *Add rule groups*.



Add from existing rule groups

□	Name
□	fortinet-ids-malware-alert-rulegroup1
□	fortinet-ips-serveros-enable-rulegroup1
□	fortinet-ips-client-enable-rulegroup1
□	fortinet-ips-serveros-enable-rulegroup2
□	fortinet-ids-serveros-alert-rulegroup2
□	fortinet-ids-serveros-alert-rulegroup1
□	fortinet-ips-webserver-enable-rulegroup1
□	fortinet-ips-webclient-enable-rulegroup1
□	fortinet-ids-webserver-alert-rulegroup1
□	fortinet-ips-webapp-enable-rulegroup1

6. Select *Next*, then *Create Firewall Policy*.

Creating the firewall

Before creating the firewall, you must create a dedicated firewall subnet in the same availability zone (AZ) on the VPC where you are implementing the firewall. You then configure the VPC route tables to route traffic in and out of the VPC via the firewall endpoint located in the firewall subnet. See AWS Network Firewall VPC configuration.

You can create or a use an existing firewall. The following instructions describe creating a firewall.

To create a firewall:

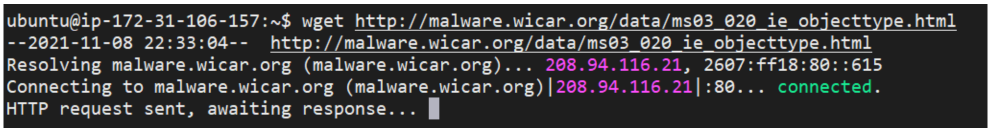
1. Go to *VPC* > *Network Firewalls* > *Firewalls*.
2. Under *Firewall subnets*, from the *Availability Zone* dropdown list, select the AZ where the firewall subnet is located.
3. From the *Subnet* dropdown list, select the firewall subnet.
4. Associate the firewall with the policy that you created.
5. Click *Create Firewall*.

Validating the rule group configuration

There are multiple logging destinations available for AWS network firewalls. This example uses CloudWatch to store and display logs. For details, see AWS Network Firewall Logging Destinations.

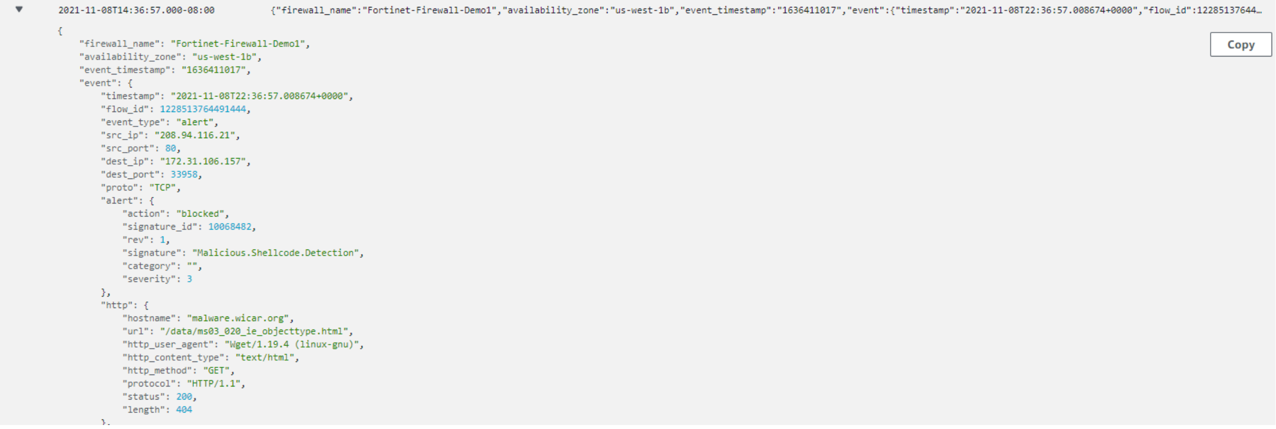
To validate the rule group configuration:

1. Create a log group:
   a. Go to *CloudWatch > Logs > Log Groups*.
   b. Click *Create log group*.
   c. Under *Tags*, in the *Key* field, enter AWSNetworkFirewallManaged.
   d. Click *Create*.
2. Configure logging for the firewall:
   a. Go to *VPC > Network Firewalls > Firewalls*.
   b. Select the firewall that contains the Fortinet rule groups.
   c. On the *Firewall Details* tab, under *Logging*, click *Edit*.
   d. Under *Log type*, select *Alert* and *Flow*.
   e. Under *Log destination for alerts*, select *CloudWatch log group*.
   f. In the *CloudWatch log group* field, select the desired group.
   g. Repeat steps e-f in *Log destination for flows*.
3. Create an instance in the protected region behind the AWS network firewall.
4. Remotely access the instance via SSH.
5. Attempt to download malware. The following shows desired output when using an intrusion prevention system rule group. The file is blocked and cannot be downloaded.



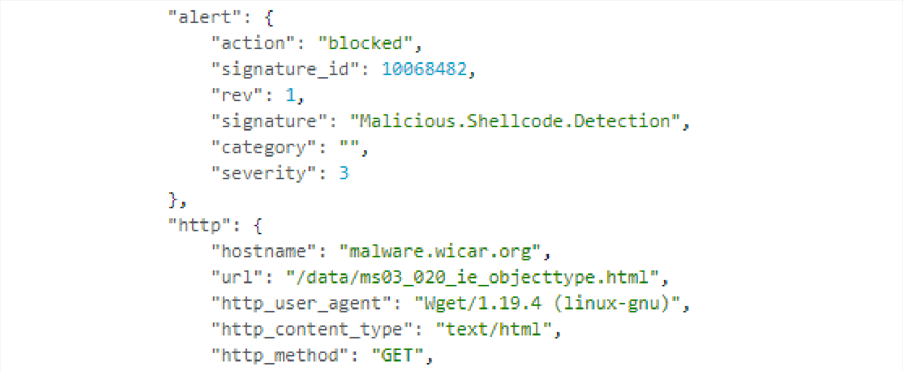
```
ubuntu@ip-172-31-106-157:~$ wget http://malware.wicar.org/data/ms03_020_ie_objecttype.html
--2021-11-08 22:33:04--  http://malware.wicar.org/data/ms03_020_ie_objecttype.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org)|208.94.116.21|:80... connected.
HTTP request sent, awaiting response...
```

6. On the AWS management console, go to *CloudWatch > Logs > Log Groups*.
7. Select the log group that you selected in step 2f.
8. Open the generated log stream to confirm that the attempted malware download was logged.



```
▼     2021-11-08T14:36:57.000-08:00        {"firewall_name":"Fortinet-Firewall-Demo1","availability_zone":"us-west-1b","event_timestamp":"1636411017","event":{"timestamp":"2021-11-08T22:36:57.008674+0000","flow_id":12285137644…
      {
          "firewall_name": "Fortinet-Firewall-Demo1",
          "availability_zone": "us-west-1b",
          "event_timestamp": "1636411017",
          "event": {
              "timestamp": "2021-11-08T22:36:57.008674+0000",
              "flow_id": 1228513764491444,
              "event_type": "alert",
              "src_ip": "208.94.116.21",
              "src_port": 80,
              "dest_ip": "172.31.106.157",
              "dest_port": 33958,
              "proto": "TCP",
              "alert": {
                  "action": "blocked",
                  "signature_id": 10068482,
                  "rev": 1,
                  "signature": "Malicious.Shellcode.Detection",
                  "category": "",
                  "severity": 3
              },
              "http": {
                  "hostname": "malware.wicar.org",
                  "url": "/data/ms03_020_ie_objecttype.html",
                  "http_user_agent": "Wget/1.19.4 (linux-gnu)",
                  "http_content_type": "text/html",
                  "http_method": "GET",
                  "protocol": "HTTP/1.1",
                  "status": 200,
                  "length": 404
              },
```

Frequently asked questions

<table>
<tr><th>Question</th><th>Answer</th></tr>
<tr><td>Are partner rule groups deployed globally or per region?</td><td>Per region. You must deploy partner rule groups in each AWS region where you have deployed applications.</td></tr>
<tr><td>Can I view the signatures/rules within the rule group itself?</td><td>No. The signatures/rules are propietary vendor information and not exposed to customers.</td></tr>
<tr><td>Can I view the name of the rule that blocked a request?</td><td>Yes. AWS network firewall logs reveal the signature ID and name. If needed, contact Fortinet Customer Service & Support for information.

<pre><code>"alert": {
    "action": "blocked",
    "signature_id": 10068482,
    "rev": 1,
    "signature": "Malicious.Shellcode.Detection",
    "category": "",
    "severity": 3
},
"http": {
    "hostname": "malware.wicar.org",
    "url": "/data/ms03_020_ie_objecttype.html",
    "http_user_agent": "Wget/1.19.4 (linux-gnu)",
    "http_content_type": "text/html",
    "http_method": "GET",
</code></pre></td></tr>
<tr><td>Why do I get access denied when I click on a rule set to view?</td><td>The permissions within the AWS Network Firewall rule groups only permits blanket read/write/execute permissions, so Fortinet cannot share any viewing of the rules without exposing the entire rule set contents.</td></tr>
<tr><td>How can I check if the rule group addresses a particular malware/CVE/vulnerability?</td><td>The latest on Fortinet's signatures and insights on ongoing threats throughout the world can be found on the FortiGuard Labs website. There is currently no mechanism to share signature information.</td></tr>
<tr><td>What regions are these rules available in?</td><td>Network Firewall Rules are currently available in the following regions.
Americas:
• us-east-1
• us-east-2
• us-west-1
• us-west-2
• ca-central-1
• sa-east-1
Europe:
• eu-central-1
• eu-west-1
• eu-west-2
• eu-west-3
• eu-south-1
• eu-north-1</td></tr>
</table>

Question	Answer
	APAC: - ap-east-1 - ap-south-1 - ap-northeast-1 - ap-northeast-2 - ap-northeast-3 - ap-southeast-1 - ap-southeast-2 Other: - af-south-1 - me-south-1
How frequently does Fortinet update these rules?	The current rules update frequency is once per week.
Does the Fortinet rule group include support?	Yes. By purchasing a Fortinet rule group, customers are entitled for support from Fortinet.
What is the process for opening a support ticket with Fortinet?	Contact Fortinet directly at awsips@fortinet.com.

Change log

Date	Change Description
2021-11-16	Initial release.

FORTINET®

www.fortinet.com