AWS Network Firewall

API Reference

API Version 2020-11-12

AWS Network Firewall: API Reference

Table of Contents

Welcome

This is the API Reference for AWS Network Firewall. This guide is for developers who need detailed information about the Network Firewall API actions, data types, and errors.

- The REST API requires you to handle connection details, such as calculating signatures, handling request retries, and error handling. For general information about using the AWS REST APIs, see AWS APIs.

  To access Network Firewall using the REST API endpoint: `https://network-firewall.<region>.amazonaws.com`
- Alternatively, you can use one of the AWS SDKs to access an API that's tailored to the programming language or platform that you're using. For more information, see AWS SDKs.
- For descriptions of Network Firewall features, including and step-by-step instructions on how to use them through the Network Firewall console, see the Network Firewall Developer Guide.

Network Firewall is a stateful, managed, network firewall and intrusion detection and prevention service for Amazon Virtual Private Cloud (Amazon VPC). With Network Firewall, you can filter traffic at the perimeter of your VPC. This includes filtering traffic going to and coming from an internet gateway, NAT gateway, or over VPN or AWS Direct Connect. Network Firewall uses rules that are compatible with Suricata, a free, open source intrusion detection system (IDS) engine. AWS Network Firewall supports Suricata version 5.0.2. For information about Suricata, see the Suricata website.

You can use Network Firewall to monitor and protect your VPC traffic in a number of ways. The following are just a few examples:

- Allow domains or IP addresses for known AWS service endpoints, such as Amazon S3, and block all other forms of traffic.
- Use custom lists of known bad domains to limit the types of domain names that your applications can access.
- Perform deep packet inspection on traffic entering or leaving your VPC.
- Use stateful protocol detection to filter protocols like HTTPS, regardless of the port used.

To enable Network Firewall for your VPCs, you perform steps in both Amazon VPC and in Network Firewall. For information about using Amazon VPC, see Amazon VPC User Guide.

To start using Network Firewall, do the following:

1. (Optional) If you don't already have a VPC that you want to protect, create it in Amazon VPC.
2. In Amazon VPC, in each Availability Zone where you want to have a firewall endpoint, create a subnet for the sole use of Network Firewall.
3. In Network Firewall, create stateless and stateful rule groups, to define the components of the network traffic filtering behavior that you want your firewall to have.
4. In Network Firewall, create a firewall policy that uses your rule groups and specifies additional default traffic filtering behavior.
5. In Network Firewall, create a firewall and specify your new firewall policy and VPC subnets. Network Firewall creates a firewall endpoint in each subnet that you specify, with the behavior that's defined in the firewall policy.
6. In Amazon VPC, use ingress routing enhancements to route traffic through the new firewall endpoints.

This document was last published on November 12, 2021.

Actions

The following actions are supported:

AssociateFirewallPolicy

Associates a FirewallPolicy (p. 122) to a Firewall (p. 118).

A firewall policy defines how to monitor and manage your VPC network traffic, using a collection of inspection rule groups and other settings. Each firewall requires one firewall policy association, and you can use the same firewall policy for multiple firewalls.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 4)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 4)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyArn (p. 4)

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

UpdateToken (p. 4)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 5)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 5)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

FirewallPolicyArn (p. 5)

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

UpdateToken (p. 5)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AssociateSubnets

Associates the specified subnets in the Amazon VPC to the firewall. You can specify one subnet for each of the Availability Zones that the VPC spans.

This request creates an AWS Network Firewall firewall endpoint in each of the subnets. To enable the firewall's protections, you must also modify the VPC's route tables for each subnet's Availability Zone, to redirect the traffic that's coming into and going out of the zone through the firewall endpoint.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetMappings": [
      {
         "SubnetId": "string"
      }
   ],
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 8)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 8)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetMappings (p. 8)

The IDs of the subnets that you want to associate with the firewall.

Type: Array of SubnetMapping (p. 160) objects

Required: Yes

UpdateToken (p. 8)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetMappings": [
      {
         "SubnetId": "string"
      }
   ],
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 9)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 9)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetMappings (p. 9)

The IDs of the subnets that are associated with the firewall.

Type: Array of SubnetMapping (p. 160) objects

UpdateToken (p. 9)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.

- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFirewall

Creates an AWS Network Firewall Firewall (p. 118) and accompanying FirewallStatus (p. 127) for a VPC.

The firewall defines the configuration settings for an AWS Network Firewall firewall. The settings that you can define at creation include the firewall policy, the subnets in your VPC to use for the firewall endpoints, and any tags that are attached to the firewall AWS resource.

After you create a firewall, you can provide additional settings, like the logging configuration.

To update the settings for a firewall, you use the operations that apply to the settings themselves, for example UpdateLoggingConfiguration (p. 97), AssociateSubnets (p. 8), and UpdateFirewallDeleteProtection (p. 80).

To manage a firewall's tags, use the standard AWS resource tagging operations, ListTagsForResource (p. 70), TagResource (p. 76), and UntagResource (p. 78).

To retrieve information about firewalls, use ListFirewalls (p. 64) and DescribeFirewall (p. 39).

Request Syntax

```
{
   "DeleteProtection": boolean,
   "Description": "string",
   "FirewallName": "string",
   "FirewallPolicyArn": "string",
   "FirewallPolicyChangeProtection": boolean,
   "SubnetChangeProtection": boolean,
   "SubnetMappings": [
      {
         "SubnetId": "string"
      }
   ],
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "VpcId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

DeleteProtection (p. 12)

A flag indicating whether it is possible to delete the firewall. A setting of `TRUE` indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to `TRUE`.

Type: Boolean

Required: No

Description (p. 12)

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallName (p. 12)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

FirewallPolicyArn (p. 12)

The Amazon Resource Name (ARN) of the FirewallPolicy (p. 122) that you want to use for the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FirewallPolicyChangeProtection (p. 12)

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: No

SubnetChangeProtection (p. 12)

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: No

SubnetMappings (p. 12)

The public subnets to use for your Network Firewall firewalls. Each subnet must belong to a different Availability Zone in the VPC. Network Firewall creates a firewall endpoint in each subnet.

Type: Array of SubnetMapping (p. 160) objects

Required: Yes

Tags (p. 12)

The key:value pairs to associate with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

VpcId (p. 12)

The unique identifier of the VPC where Network Firewall should create the firewall.

You can't change this setting after you create the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: Yes

Response Syntax

```
{
   "Firewall": {
      "DeleteProtection": boolean,
      "Description": "string",
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [
         {
            "SubnetId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "VpcId": "string"
   },
   "FirewallStatus": {
      "ConfigurationSyncStateSummary": "string",
      "Status": "string",
      "SyncStates": {
         "string" : {
            "Attachment": {
               "EndpointId": "string",
               "Status": "string",
               "SubnetId": "string"
            },
            "Config": {
               "string" : {
                  "SyncStatus": "string",
                  "UpdateToken": "string"
```

```
                }
            }
        }
    }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall (p. 14)

The configuration settings for the firewall. These settings include the firewall policy and the subnets in your VPC to use for the firewall endpoints.

Type: Firewall (p. 118) object

FirewallStatus (p. 14)

Detailed information about the current status of a Firewall (p. 118). You can retrieve this for a firewall by calling DescribeFirewall (p. 39) and providing the firewall name and ARN.

Type: FirewallStatus (p. 127) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateFirewallPolicy

Creates the firewall policy for the firewall according to the specifications.

An AWS Network Firewall firewall policy defines the behavior of a firewall, in a collection of stateless and stateful rule groups and other settings. You can use one firewall policy for multiple firewalls.

Request Syntax

```
{
   "Description": "string",
   "DryRun": boolean,
   "FirewallPolicy": {
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "RuleOrder": "string"
      },
      "StatefulRuleGroupReferences": [
         {
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
      "StatelessCustomActions": [
         {
            "ActionDefinition": {
               "PublishMetricAction": {
                  "Dimensions": [
                     {
                        "Value": "string"
                     }
                  ]
               }
            },
            "ActionName": "string"
         }
      ],
      "StatelessDefaultActions": [ "string" ],
      "StatelessFragmentDefaultActions": [ "string" ],
      "StatelessRuleGroupReferences": [
         {
            "Priority": number,
            "ResourceArn": "string"
         }
      ]
   },
   "FirewallPolicyName": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Description (p. 17)

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun (p. 17)

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to `TRUE`, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to `FALSE`, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to `FALSE`, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

FirewallPolicy (p. 17)

The rule groups and policy actions to use in the firewall policy.

Type: FirewallPolicy (p. 122) object

Required: Yes

FirewallPolicyName (p. 17)

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

Tags (p. 17)

The key:value pairs to associate with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Response Syntax

```
{
```

```
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
      "FirewallPolicyStatus": "string",
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse (p. 18)

The high-level properties of a firewall policy. This, along with the FirewallPolicy (p. 122), define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Type: FirewallPolicyResponse (p. 125) object

UpdateToken (p. 18)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

CreateRuleGroup

Creates the specified stateless or stateful rule group, which includes the rules for network traffic inspection, a capacity setting, and tags.

You provide your rule group specification in your request using either `RuleGroup` or `Rules`.

Request Syntax

```
{
   "Capacity": number,
   "Description": "string",
   "DryRun": boolean,
   "RuleGroup": {
      "RulesSource": {
         "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": [ "string" ],
            "TargetTypes": [ "string" ]
         },
         "RulesString": "string",
         "StatefulRules": [
            {
               "Action": "string",
               "Header": {
                  "Destination": "string",
                  "DestinationPort": "string",
                  "Direction": "string",
                  "Protocol": "string",
                  "Source": "string",
                  "SourcePort": "string"
               },
               "RuleOptions": [
                  {
                     "Keyword": "string",
                     "Settings": [ "string" ]
                  }
               ]
            }
         ],
         "StatelessRulesAndCustomActions": {
            "CustomActions": [
               {
                  "ActionDefinition": {
                     "PublishMetricAction": {
                        "Dimensions": [
                           {
                              "Value": "string"
                           }
                        ]
                     }
                  },
                  "ActionName": "string"
               }
            ],
            "StatelessRules": [
               {
                  "Priority": number,
                  "RuleDefinition": {
                     "Actions": [ "string" ],
                     "MatchAttributes": {
                        "DestinationPorts": [
                           {
```

```
                            "FromPort": number,
                            "ToPort": number
                        }
                    ],
                    "Destinations": [
                        {
                            "AddressDefinition": "string"
                        }
                    ],
                    "Protocols": [ number ],
                    "SourcePorts": [
                        {
                            "FromPort": number,
                            "ToPort": number
                        }
                    ],
                    "Sources": [
                        {
                            "AddressDefinition": "string"
                        }
                    ],
                    "TCPFlags": [
                        {
                            "Flags": [ "string" ],
                            "Masks": [ "string" ]
                        }
                    ]
                }
            }
        }
    ]
  }
},
"RuleVariables": {
  "IPSets": {
    "string" : {
      "Definition": [ "string" ]
    }
  },
  "PortSets": {
    "string" : {
      "Definition": [ "string" ]
    }
  }
},
"StatefulRuleOptions": {
  "RuleOrder": "string"
}
},
"RuleGroupName": "string",
"Rules": "string",
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Capacity (p. 21)

The maximum operating resources that this rule group can use. Rule group capacity is fixed at creation. When you update a rule group, you are limited to this capacity. When you reference a rule group from a firewall policy, Network Firewall reserves this capacity for the rule group.

You can retrieve the capacity that would be required for a rule group before you create the rule group by calling CreateRuleGroup (p. 21) with `DryRun` set to `TRUE`.

Note
You can't change or exceed this capacity when you update the rule group, so leave room for your rule group to grow.

Capacity for a stateless rule group

For a stateless rule group, the capacity required is the sum of the capacity requirements of the individual rules that you expect to have in the rule group.

To calculate the capacity requirement of a single rule, multiply the capacity requirement values of each of the rule's match settings:

- A match setting with no criteria specified has a value of 1.
- A match setting with `Any` specified has a value of 1.
- All other match settings have a value equal to the number of elements provided in the setting. For example, a protocol setting ["UDP"] and a source setting ["10.0.0.0/24"] each have a value of 1. A protocol setting ["UDP","TCP"] has a value of 2. A source setting ["10.0.0.0/24","10.0.0.1/24","10.0.0.2/24"] has a value of 3.

A rule with no criteria specified in any of its match settings has a capacity requirement of 1. A rule with protocol setting ["UDP","TCP"], source setting ["10.0.0.0/24","10.0.0.1/24","10.0.0.2/24"], and a single specification or no specification for each of the other match settings has a capacity requirement of 6.

Capacity for a stateful rule group

For a stateful rule group, the minimum capacity required is the number of individual rules that you expect to have in the rule group.

Type: Integer

Required: Yes

Description (p. 21)

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun (p. 21)

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to `TRUE`, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if

you ran it with dry run set to `FALSE`, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to `FALSE`, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

RuleGroup (p. 21)

An object that defines the rule group rules.

Note
You must provide either this rule group setting or a `Rules` setting, but not both.

Type: RuleGroup (p. 143) object

Required: No

RuleGroupName (p. 21)

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

Rules (p. 21)

A string containing stateful rule group rules specifications in Suricata flat format, with one rule per line. Use this to import your existing Suricata compatible rule groups.

Note
You must provide either this rules setting or a populated `RuleGroup` setting, but not both.

You can provide your rule group specification in Suricata flat format through this setting when you create or update your rule group. The call response returns a RuleGroup (p. 143) object that Network Firewall has populated from your string.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

Tags (p. 21)

The key:value pairs to associate with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Type (p. 21)

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: Yes

Response Syntax

```
{
   "RuleGroupResponse": {
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string"
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse (p. 25)

The high-level properties of a rule group. This, along with the RuleGroup (p. 143), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

Type: RuleGroupResponse (p. 145) object

UpdateToken (p. 25)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InsufficientCapacityException

AWS doesn't currently have enough available capacity to fulfill your request. Try your request later.

HTTP Status Code: 500

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

LimitExceededException

Unable to perform the operation because doing so would violate a limit setting.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteFirewall

Deletes the specified Firewall (p. 118) and its FirewallStatus (p. 127). This operation requires the firewall's `DeleteProtection` flag to be `FALSE`. You can't revert this operation.

You can check whether a firewall is in use by reviewing the route tables for the Availability Zones where you have firewall subnet mappings. Retrieve the subnet mappings by calling DescribeFirewall (p. 39). You define and update the route tables through Amazon VPC. As needed, update the route tables for the zones to remove the firewall endpoints. When the route tables no longer use the firewall endpoints, you can remove the firewall safely.

To delete a firewall, remove the delete protection if you need to using UpdateFirewallDeleteProtection (p. 80), then delete the firewall by calling DeleteFirewall (p. 27).

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 27)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 27)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "Firewall": {
      "DeleteProtection": boolean,
      "Description": "string",
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "SubnetChangeProtection": boolean,
      "SubnetMappings": [
         {
            "SubnetId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "VpcId": "string"
   },
   "FirewallStatus": {
      "ConfigurationSyncStateSummary": "string",
      "Status": "string",
      "SyncStates": {
         "string" : {
            "Attachment": {
               "EndpointId": "string",
               "Status": "string",
               "SubnetId": "string"
            },
            "Config": {
               "string" : {
                  "SyncStatus": "string",
                  "UpdateToken": "string"
               }
            }
         }
      }
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall (p. 28)

The firewall defines the configuration settings for an AWS Network Firewall firewall. These settings include the firewall policy, the subnets in your VPC to use for the firewall endpoints, and any tags that are attached to the firewall AWS resource.

The status of the firewall, for example whether it's ready to filter network traffic, is provided in the corresponding FirewallStatus (p. 127). You can retrieve both objects by calling DescribeFirewall (p. 39).

Type: Firewall (p. 118) object

FirewallStatus (p. 28)

Detailed information about the current status of a Firewall (p. 118). You can retrieve this for a firewall by calling DescribeFirewall (p. 39) and providing the firewall name and ARN.

Type: FirewallStatus (p. 127) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteFirewallPolicy

Deletes the specified FirewallPolicy (p. 122).

Request Syntax

```
{
   "FirewallPolicyArn": "string",
   "FirewallPolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallPolicyArn (p. 31)

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName (p. 31)

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
```

```
      "FirewallPolicyStatus": "string",
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse (p. 31)

The object containing the definition of the FirewallPolicyResponse (p. 125) that you asked to delete.

Type: FirewallPolicyResponse (p. 125) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteResourcePolicy

Deletes a resource policy that you created in a PutResourcePolicy (p. 73) request.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

ResourceArn (p. 34)

The Amazon Resource Name (ARN) of the rule group or firewall policy whose resource policy you want to delete.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidResourcePolicyException

The policy statement failed validation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteRuleGroup

Deletes the specified RuleGroup (p. 143).

Request Syntax

```
{
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

RuleGroupArn (p. 36)

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName (p. 36)

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type (p. 36)

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Note
This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "RuleGroupResponse": {
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse (p. 37)

The high-level properties of a rule group. This, along with the RuleGroup (p. 143), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

Type: RuleGroupResponse (p. 145) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

UnsupportedOperationException

The operation you requested isn't supported by Network Firewall.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFirewall

Returns the data objects for the specified firewall.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 39)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 39)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "Firewall": {
      "DeleteProtection": boolean,
      "Description": "string",
      "FirewallArn": "string",
      "FirewallId": "string",
      "FirewallName": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyChangeProtection": boolean,
      "SubnetChangeProtection": boolean,
```

```
      "SubnetMappings": [
         {
            "SubnetId": "string"
         }
      ],
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "VpcId": "string"
   },
   "FirewallStatus": {
      "ConfigurationSyncStateSummary": "string",
      "Status": "string",
      "SyncStates": {
         "string" : {
            "Attachment": {
               "EndpointId": "string",
               "Status": "string",
               "SubnetId": "string"
            },
            "Config": {
               "string" : {
                  "SyncStatus": "string",
                  "UpdateToken": "string"
               }
            }
         }
      }
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewall (p. 39)

The configuration settings for the firewall. These settings include the firewall policy and the subnets in your VPC to use for the firewall endpoints.

Type: Firewall (p. 118) object

FirewallStatus (p. 39)

Detailed information about the current status of a Firewall (p. 118). You can retrieve this for a firewall by calling DescribeFirewall (p. 39) and providing the firewall name and ARN.

Type: FirewallStatus (p. 127) object

UpdateToken (p. 39)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn’t perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3

- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeFirewallPolicy

Returns the data objects for the specified firewall policy.

Request Syntax

```
{
   "FirewallPolicyArn": "string",
   "FirewallPolicyName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallPolicyArn (p. 43)

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName (p. 43)

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "FirewallPolicy": {
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "RuleOrder": "string"
      },
      "StatefulRuleGroupReferences": [
```

```
            {
               "Priority": number,
               "ResourceArn": "string"
            }
         ],
         "StatelessCustomActions": [
            {
               "ActionDefinition": {
                  "PublishMetricAction": {
                     "Dimensions": [
                        {
                           "Value": "string"
                        }
                     ]
                  }
               },
               "ActionName": "string"
            }
         ],
         "StatelessDefaultActions": [ "string" ],
         "StatelessFragmentDefaultActions": [ "string" ],
         "StatelessRuleGroupReferences": [
            {
               "Priority": number,
               "ResourceArn": "string"
            }
         ]
      },
      "FirewallPolicyResponse": {
         "ConsumedStatefulRuleCapacity": number,
         "ConsumedStatelessRuleCapacity": number,
         "Description": "string",
         "FirewallPolicyArn": "string",
         "FirewallPolicyId": "string",
         "FirewallPolicyName": "string",
         "FirewallPolicyStatus": "string",
         "NumberOfAssociations": number,
         "Tags": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "UpdateToken": "string"
   }
```


Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicy (p. 43)

The policy for the specified firewall policy.

Type: FirewallPolicy (p. 122) object

FirewallPolicyResponse (p. 43)

The high-level properties of a firewall policy. This, along with the FirewallPolicy (p. 122), define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Type: FirewallPolicyResponse (p. 125) object

UpdateToken (p. 43)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeLoggingConfiguration

Returns the logging configuration for the specified firewall.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 47)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 47)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
```

```
            "LogType": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 47)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

LoggingConfiguration (p. 47)

Defines how AWS Network Firewall performs logging for a Firewall (p. 118).

Type: LoggingConfiguration (p. 134) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeResourcePolicy

Retrieves a resource policy that you created in a PutResourcePolicy (p. 73) request.

Request Syntax

```
{
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

ResourceArn (p. 50)

The Amazon Resource Name (ARN) of the rule group or firewall policy whose resource policy you want to retrieve.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "Policy": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Policy (p. 50)

The AWS Identity and Access Management policy for the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 395000.

Pattern: `.*\S.*`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DescribeRuleGroup

Returns the data objects for the specified rule group.

Request Syntax

```
{
   "RuleGroupArn": "string",
   "RuleGroupName": "string",
   "Type": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

RuleGroupArn (p. 52)

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName (p. 52)

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Type (p. 52)

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Note
This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

Response Syntax

```
{
   "RuleGroup": {
      "RulesSource": {
         "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": [ "string" ],
            "TargetTypes": [ "string" ]
         },
         "RulesString": "string",
         "StatefulRules": [
            {
               "Action": "string",
               "Header": {
                  "Destination": "string",
                  "DestinationPort": "string",
                  "Direction": "string",
                  "Protocol": "string",
                  "Source": "string",
                  "SourcePort": "string"
               },
               "RuleOptions": [
                  {
                     "Keyword": "string",
                     "Settings": [ "string" ]
                  }
               ]
            }
         ],
         "StatelessRulesAndCustomActions": {
            "CustomActions": [
               {
                  "ActionDefinition": {
                     "PublishMetricAction": {
                        "Dimensions": [
                           {
                              "Value": "string"
                           }
                        ]
                     }
                  },
                  "ActionName": "string"
               }
            ],
            "StatelessRules": [
               {
                  "Priority": number,
                  "RuleDefinition": {
                     "Actions": [ "string" ],
                     "MatchAttributes": {
                        "DestinationPorts": [
                           {
                              "FromPort": number,
                              "ToPort": number
                           }
                        ],
                        "Destinations": [
                           {
```

```
                            "AddressDefinition": "string"
                        }
                    ],
                    "Protocols": [ number ],
                    "SourcePorts": [
                        {
                            "FromPort": number,
                            "ToPort": number
                        }
                    ],
                    "Sources": [
                        {
                            "AddressDefinition": "string"
                        }
                    ],
                    "TCPFlags": [
                        {
                            "Flags": [ "string" ],
                            "Masks": [ "string" ]
                        }
                    ]
                }
            }
        }
    ]
  }
  },
  "RuleVariables": {
    "IPSets": {
      "string" : {
        "Definition": [ "string" ]
      }
    },
    "PortSets": {
      "string" : {
        "Definition": [ "string" ]
      }
    }
  },
  "StatefulRuleOptions": {
    "RuleOrder": "string"
  }
 },
 "RuleGroupResponse": {
  "Capacity": number,
  "ConsumedCapacity": number,
  "Description": "string",
  "NumberOfAssociations": number,
  "RuleGroupArn": "string",
  "RuleGroupId": "string",
  "RuleGroupName": "string",
  "RuleGroupStatus": "string",
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "Type": "string"
 },
 "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroup (p. 53)

The object that defines the rules in a rule group. This, along with RuleGroupResponse (p. 145), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

AWS Network Firewall uses a rule group to inspect and control network traffic. You define stateless rule groups to inspect individual packets and you define stateful rule groups to inspect packets in the context of their traffic flow.

To use a rule group, you include it by reference in an Network Firewall firewall policy, then you use the policy in a firewall. You can reference a rule group from more than one firewall policy, and you can use a firewall policy in more than one firewall.

Type: RuleGroup (p. 143) object

RuleGroupResponse (p. 53)

The high-level properties of a rule group. This, along with the RuleGroup (p. 143), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

Type: RuleGroupResponse (p. 145) object

UpdateToken (p. 53)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateSubnets

Removes the specified subnet associations from the firewall. This removes the firewall endpoints from the subnets and removes any network filtering protections that the endpoints were providing.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetIds": [ "string" ],
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 57)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 57)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetIds (p. 57)

The unique identifiers for the subnets that you want to disassociate.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^subnet-[0-9a-f]+$`

Required: Yes

UpdateToken (p. 57)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetMappings": [
      {
         "SubnetId": "string"
      }
   ],
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 58)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 58)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetMappings (p. 58)

The IDs of the subnets that are associated with the firewall.

Type: Array of SubnetMapping (p. 160) objects

UpdateToken (p. 58)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidOperationException

The operation failed because it's not valid. For example, you might have tried to delete a rule group or firewall policy that's in use.

HTTP Status Code: 400

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFirewallPolicies

Retrieves the metadata for the firewall policies that you have defined. Depending on your setting for max results and the number of firewall policies, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

MaxResults (p. 61)

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 61)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Response Syntax

```
{
   "FirewallPolicies": [
      {
         "Arn": "string",
         "Name": "string"
      }
   ],
   "NextToken": "string"
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicies (p. 61)

The metadata for the firewall policies. Depending on your setting for max results and the number of firewall policies that you have, this might not be the full list.

Type: Array of FirewallPolicyMetadata (p. 124) objects

NextToken (p. 61)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListFirewalls

Retrieves the metadata for the firewalls that you have defined. If you provide VPC identifiers in your request, this returns only the firewalls for those VPCs.

Depending on your setting for max results and the number of firewalls, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string",
   "VpcIds": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

MaxResults (p. 64)

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 64)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

VpcIds (p. 64)

The unique identifiers of the VPCs that you want Network Firewall to retrieve the firewalls for. Leave this blank to retrieve all firewalls that you have defined.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: No

Response Syntax

```
{
   "Firewalls": [
      {
         "FirewallArn": "string",
         "FirewallName": "string"
      }
   ],
   "NextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Firewalls (p. 65)

The firewall metadata objects for the VPCs that you specified. Depending on your setting for max results and the number of firewalls you have, a single call might not be the full list.

Type: Array of FirewallMetadata (p. 121) objects

NextToken (p. 65)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.

- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListRuleGroups

Retrieves the metadata for the rule groups that you have defined. Depending on your setting for max results and the number of rule groups, a single call might not return the full list.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

MaxResults (p. 67)

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 100.

Required: No

NextToken (p. 67)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "RuleGroups": [
      {
         "Arn": "string",
         "Name": "string"
      }
   ]
```

```
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 67)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

RuleGroups (p. 67)

The rule group metadata objects that you've defined. Depending on your setting for max results and the number of rule groups, this might not be the full list.

Type: Array of RuleGroupMetadata (p. 144) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListTagsForResource

Retrieves the tags associated with the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can tag the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "MaxResults": number,
   "NextToken": "string",
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

MaxResults (p. 70)

The maximum number of objects that you want Network Firewall to return for this request. If more objects are available, in the response, Network Firewall provides a `NextToken` value that you can use in a subsequent call to get the next batch of objects.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 100.

Required: No

NextToken (p. 70)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Required: No

ResourceArn (p. 70)

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

NextToken (p. 71)

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Network Firewall returns a `NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 2048.

Pattern: `[0-9A-Za-z:\/+=]+$`

Tags (p. 71)

The tags that are associated with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutResourcePolicy

Creates or updates an AWS Identity and Access Management policy for your rule group or firewall policy. Use this to share rule groups and firewall policies between accounts. This operation works in conjunction with the AWS Resource Access Manager (RAM) service to manage resource sharing for Network Firewall.

Use this operation to create or update a resource policy for your rule group or firewall policy. In the policy, you specify the accounts that you want to share the resource with and the operations that you want the accounts to be able to perform.

When you add an account in the resource policy, you then run the following Resource Access Manager (RAM) operations to access and accept the shared rule group or firewall policy.

- GetResourceShareInvitations - Returns the Amazon Resource Names (ARNs) of the resource share invitations.
- AcceptResourceShareInvitation - Accepts the share invitation for a specified resource share.

For additional information about resource sharing using RAM, see AWS Resource Access Manager User Guide.

Request Syntax

```
{
   "Policy": "string",
   "ResourceArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Policy (p. 73)

The AWS Identity and Access Management policy statement that lists the accounts that you want to share your rule group or firewall policy with and the operations that you want the accounts to be able to perform.

For a rule group resource, you can specify the following operations in the Actions section of the statement:

- network-firewall:CreateFirewallPolicy
- network-firewall:UpdateFirewallPolicy
- network-firewall:ListRuleGroups

For a firewall policy resource, you can specify the following operations in the Actions section of the statement:

- network-firewall:CreateFirewall
- network-firewall:UpdateFirewall
- network-firewall:AssociateFirewallPolicy
- network-firewall:ListFirewallPolicies

In the Resource section of the statement, you specify the ARNs for the rule groups and firewall policies that you want to share with the account that you specified in `Arn`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 395000.

Pattern: `.*\S.*`

Required: Yes

ResourceArn (p. 73)

The Amazon Resource Name (ARN) of the account that you want to share rule groups and firewall policies with.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidResourcePolicyException

The policy statement failed validation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

TagResource

Adds the specified tags to the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can tag the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

ResourceArn (p. 76)

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

Tags (p. 76)

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UntagResource

Removes the tags with the specified keys from the specified resource. Tags are key:value pairs that you can use to categorize and manage your resources, for purposes like billing. For example, you might set the tag key to "customer" and the value to the customer name or ID. You can specify one or more tags to add to each AWS resource, up to 50 tags for a resource.

You can manage tags for the AWS resources that you manage through AWS Network Firewall: firewalls, firewall policies, and rule groups.

Request Syntax

```
{
   "ResourceArn": "string",
   "TagKeys": [ "string" ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

ResourceArn (p. 78)

The Amazon Resource Name (ARN) of the resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

TagKeys (p. 78)

Type: Array of strings

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^.*$`

Required: Yes

Response Elements

If the action is successful, the service sends back an HTTP 200 response with an empty HTTP body.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallDeleteProtection

Modifies the flag, `DeleteProtection`, which indicates whether it is possible to delete the firewall. If the flag is set to `TRUE`, the firewall is protected against deletion. This setting helps protect against accidentally deleting a firewall that's in use.

Request Syntax

```
{
   "DeleteProtection": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

DeleteProtection (p. 80)

A flag indicating whether it is possible to delete the firewall. A setting of `TRUE` indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to `TRUE`.

Type: Boolean

Required: Yes

FirewallArn (p. 80)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 80)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken (p. 80)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "DeleteProtection": boolean,
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

DeleteProtection (p. 81)

Type: Boolean

FirewallArn (p. 81)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 81)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken (p. 81)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallDescription

Modifies the description for the specified firewall. Use the description to help you identify the firewall when you're working with it.

Request Syntax

```
{
   "Description": "string",
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Description (p. 84)

The new description for the firewall. If you omit this setting, Network Firewall removes the description for the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallArn (p. 84)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 84)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken (p. 84)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "Description": "string",
   "FirewallArn": "string",
   "FirewallName": "string",
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

Description (p. 85)

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

FirewallArn (p. 85)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 85)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

UpdateToken (p. 85)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateFirewallPolicy

Updates the properties of the specified firewall policy.

Request Syntax

```
{
   "Description": "string",
   "DryRun": boolean,
   "FirewallPolicy": {
      "StatefulDefaultActions": [ "string" ],
      "StatefulEngineOptions": {
         "RuleOrder": "string"
      },
      "StatefulRuleGroupReferences": [
         {
            "Priority": number,
            "ResourceArn": "string"
         }
      ],
      "StatelessCustomActions": [
         {
            "ActionDefinition": {
               "PublishMetricAction": {
                  "Dimensions": [
                     {
                        "Value": "string"
                     }
                  ]
               }
            },
            "ActionName": "string"
         }
      ],
      "StatelessDefaultActions": [ "string" ],
      "StatelessFragmentDefaultActions": [ "string" ],
      "StatelessRuleGroupReferences": [
         {
            "Priority": number,
            "ResourceArn": "string"
         }
      ]
   },
   "FirewallPolicyArn": "string",
   "FirewallPolicyName": "string",
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Description (p. 88)

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun (p. 88)

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to `TRUE`, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to `FALSE`, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to `FALSE`, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

FirewallPolicy (p. 88)

The updated firewall policy to use for the firewall.

Type: FirewallPolicy (p. 122) object

Required: Yes

FirewallPolicyArn (p. 88)

The Amazon Resource Name (ARN) of the firewall policy.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallPolicyName (p. 88)

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

UpdateToken (p. 88)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

Response Syntax

```
{
   "FirewallPolicyResponse": {
      "ConsumedStatefulRuleCapacity": number,
      "ConsumedStatelessRuleCapacity": number,
      "Description": "string",
      "FirewallPolicyArn": "string",
      "FirewallPolicyId": "string",
      "FirewallPolicyName": "string",
      "FirewallPolicyStatus": "string",
      "NumberOfAssociations": number,
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ]
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallPolicyResponse (p. 90)

The high-level properties of a firewall policy. This, along with the FirewallPolicy (p. 122), define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Type: FirewallPolicyResponse (p. 125) object

UpdateToken (p. 90)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the firewall policy. The token marks the state of the policy resource at the time of the request.

To make changes to the policy, you provide the token in your request. Network Firewall uses the token to ensure that the policy hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall policy again to get a current copy of it with current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python

- AWS SDK for Ruby V3

UpdateFirewallPolicyChangeProtection

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 93)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 93)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyChangeProtection (p. 93)

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: Yes

UpdateToken (p. 93)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "FirewallPolicyChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 94)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 94)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

FirewallPolicyChangeProtection (p. 94)

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

UpdateToken (p. 94)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateLoggingConfiguration

Sets the logging configuration for the specified firewall.

To change the logging configuration, retrieve the LoggingConfiguration (p. 134) by calling DescribeLoggingConfiguration (p. 47), then change it and provide the modified object to this update call. You must change the logging configuration one LogDestinationConfig (p. 132) at a time inside the retrieved LoggingConfiguration (p. 134) object.

You can perform only one of the following actions in any call to `UpdateLoggingConfiguration`:

- Create a new log destination object by adding a single `LogDestinationConfig` array element to `LogDestinationConfigs`.
- Delete a log destination object by removing a single `LogDestinationConfig` array element from `LogDestinationConfigs`.
- Change the `LogDestination` setting in a single `LogDestinationConfig` array element.

You can't change the `LogDestinationType` or `LogType` in a `LogDestinationConfig`. To change these settings, delete the existing `LogDestinationConfig` object and create a new one, using two separate calls to this update operation.

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
            "LogType": "string"
         }
      ]
   }
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 97)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 97)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

LoggingConfiguration (p. 97)

Defines how Network Firewall performs logging for a firewall. If you omit this setting, Network Firewall disables logging for the firewall.

Type: LoggingConfiguration (p. 134) object

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "LoggingConfiguration": {
      "LogDestinationConfigs": [
         {
            "LogDestination": {
               "string" : "string"
            },
            "LogDestinationType": "string",
            "LogType": "string"
         }
      ]
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 98)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 98)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

LoggingConfiguration (p. 98)

Defines how AWS Network Firewall performs logging for a Firewall (p. 118).

Type: LoggingConfiguration (p. 134) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

LogDestinationPermissionException

Unable to send logs to a configured logging destination.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateRuleGroup

Updates the rule settings for the specified rule group. You use a rule group by reference in one or more firewall policies. When you modify a rule group, you modify all firewall policies that use the rule group.

To update a rule group, first call DescribeRuleGroup (p. 52) to retrieve the current RuleGroup (p. 143) object, update the object as needed, and then provide the updated object to this call.

Request Syntax

```
{
   "Description": "string",
   "DryRun": boolean,
   "RuleGroup": {
      "RulesSource": {
         "RulesSourceList": {
            "GeneratedRulesType": "string",
            "Targets": [ "string" ],
            "TargetTypes": [ "string" ]
         },
         "RulesString": "string",
         "StatefulRules": [
            {
               "Action": "string",
               "Header": {
                  "Destination": "string",
                  "DestinationPort": "string",
                  "Direction": "string",
                  "Protocol": "string",
                  "Source": "string",
                  "SourcePort": "string"
               },
               "RuleOptions": [
                  {
                     "Keyword": "string",
                     "Settings": [ "string" ]
                  }
               ]
            }
         ],
         "StatelessRulesAndCustomActions": {
            "CustomActions": [
               {
                  "ActionDefinition": {
                     "PublishMetricAction": {
                        "Dimensions": [
                           {
                              "Value": "string"
                           }
                        ]
                     }
                  },
                  "ActionName": "string"
               }
            ],
            "StatelessRules": [
               {
                  "Priority": number,
                  "RuleDefinition": {
                     "Actions": [ "string" ],
                     "MatchAttributes": {
                        "DestinationPorts": [
```

```
                        {
                           "FromPort": number,
                           "ToPort": number
                        }
                     ],
                     "Destinations": [
                        {
                           "AddressDefinition": "string"
                        }
                     ],
                     "Protocols": [ number ],
                     "SourcePorts": [
                        {
                           "FromPort": number,
                           "ToPort": number
                        }
                     ],
                     "Sources": [
                        {
                           "AddressDefinition": "string"
                        }
                     ],
                     "TCPFlags": [
                        {
                           "Flags": [ "string" ],
                           "Masks": [ "string" ]
                        }
                     ]
                  }
               }
            }
         ]
      }
   },
   "RuleVariables": {
      "IPSets": {
         "string" : {
            "Definition": [ "string" ]
         }
      },
      "PortSets": {
         "string" : {
            "Definition": [ "string" ]
         }
      }
   },
   "StatefulRuleOptions": {
      "RuleOrder": "string"
   }
},
"RuleGroupArn": "string",
"RuleGroupName": "string",
"Rules": "string",
"Type": "string",
"UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

Description (p. 101)

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

DryRun (p. 101)

Indicates whether you want Network Firewall to just check the validity of the request, rather than run the request.

If set to `TRUE`, Network Firewall checks whether the request can run successfully, but doesn't actually make the requested changes. The call returns the value that the request would return if you ran it with dry run set to `FALSE`, but doesn't make additions or changes to your resources. This option allows you to make sure that you have the required permissions to run the request and that your request parameters are valid.

If set to `FALSE`, Network Firewall makes the requested changes to your resources.

Type: Boolean

Required: No

RuleGroup (p. 101)

An object that defines the rule group rules.

Note
You must provide either this rule group setting or a `Rules` setting, but not both.

Type: RuleGroup (p. 143) object

Required: No

RuleGroupArn (p. 101)

The Amazon Resource Name (ARN) of the rule group.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

RuleGroupName (p. 101)

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

Rules (p. 101)

A string containing stateful rule group rules specifications in Suricata flat format, with one rule per line. Use this to import your existing Suricata compatible rule groups.

Note
You must provide either this rules setting or a populated `RuleGroup` setting, but not both.

You can provide your rule group specification in Suricata flat format through this setting when you create or update your rule group. The call response returns a RuleGroup (p. 143) object that Network Firewall has populated from your string.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

Type (p. 101)

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Note
This setting is required for requests that do not include the `RuleGroupARN`.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

UpdateToken (p. 101)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

Response Syntax

```
{
   "RuleGroupResponse": {
      "Capacity": number,
      "ConsumedCapacity": number,
      "Description": "string",
```

```
      "NumberOfAssociations": number,
      "RuleGroupArn": "string",
      "RuleGroupId": "string",
      "RuleGroupName": "string",
      "RuleGroupStatus": "string",
      "Tags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "Type": "string"
   },
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

RuleGroupResponse (p. 104)

The high-level properties of a rule group. This, along with the RuleGroup (p. 143), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

Type: RuleGroupResponse (p. 145) object

UpdateToken (p. 104)

A token used for optimistic locking. Network Firewall returns a token to your requests that access the rule group. The token marks the state of the rule group resource at the time of the request.

To make changes to the rule group, you provide the token in your request. Network Firewall uses the token to ensure that the rule group hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the rule group again to get a current copy of it with a current token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateSubnetChangeProtection

Request Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 164).

The request accepts the following data in JSON format.

FirewallArn (p. 107)

The Amazon Resource Name (ARN) of the firewall.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName (p. 107)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

You must specify the ARN or the name, and you can specify both.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

SubnetChangeProtection (p. 107)

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: Yes

UpdateToken (p. 107)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

Response Syntax

```
{
   "FirewallArn": "string",
   "FirewallName": "string",
   "SubnetChangeProtection": boolean,
   "UpdateToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

FirewallArn (p. 108)

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

FirewallName (p. 108)

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

SubnetChangeProtection (p. 108)

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

UpdateToken (p. 108)

An optional token that you can use for optimistic locking. Network Firewall returns a token to your requests that access the firewall. The token marks the state of the firewall resource at the time of the request.

To make an unconditional change to the firewall, omit the token in your update request. Without the token, Network Firewall performs your updates regardless of whether the firewall has changed since you last retrieved it.

To make a conditional change to the firewall, provide the token in your update request. Network Firewall uses the token to ensure that the firewall hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the firewall again to get a current copy of it with a new token. Reapply your changes as needed, then try the operation again using the new token.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 166).

InternalServerError

Your request is valid, but Network Firewall couldn't perform the operation because of a system problem. Retry your request.

HTTP Status Code: 500

InvalidRequestException

The operation failed because of a problem with your request. Examples include:

- You specified an unsupported parameter name or value.
- You tried to update a property with a value that isn't among the available types.
- Your request references an ARN that is malformed, or corresponds to a resource that isn't valid in the context of the request.

HTTP Status Code: 400

InvalidTokenException

The token you provided is stale or isn't valid for the operation.

HTTP Status Code: 400

ResourceNotFoundException

Unable to locate a resource using the parameters that you provided.

HTTP Status Code: 400

ResourceOwnerCheckException

Unable to change the resource because your account doesn't own it.

HTTP Status Code: 400

ThrottlingException

Unable to process the request due to throttling limitations.

HTTP Status Code: 400

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

Data Types

The AWS Network Firewall API contains several data types that various actions use. This section describes each data type in detail.

> **Note**
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- SubnetMapping (p. 160)
- SyncState (p. 161)
- Tag (p. 162)
- TCPFlagField (p. 163)

ActionDefinition

A custom action to use in stateless rule actions settings. This is used in CustomAction (p. 116).

Contents

PublishMetricAction

Stateless inspection criteria that publishes the specified metrics to Amazon CloudWatch for the matching packet. This setting defines a CloudWatch dimension value to be published.

You can pair this custom action with any of the standard stateless rule actions. For example, you could pair this in a rule action with the standard action that forwards the packet for stateful inspection. Then, when a packet matches the rule, Network Firewall publishes metrics for the packet and forwards it.

Type: PublishMetricAction (p. 140) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Address

A single IP address specification. This is used in the MatchAttributes (p. 135) source and destination specifications.

Contents

AddressDefinition

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 255.

Pattern: `^([a-fA-F\d:\.]+($|/\d{1,3}))$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Attachment

The configuration and status for a single subnet that you've specified for use by the AWS Network Firewall firewall. This is part of the FirewallStatus (p. 127).

Contents

EndpointId

The identifier of the firewall endpoint that Network Firewall has instantiated in the subnet. You use this to identify the firewall endpoint in the VPC route tables, when you redirect the VPC traffic through the endpoint.

Type: String

Required: No

Status

The current status of the firewall endpoint in the subnet. This value reflects both the instantiation of the endpoint in the VPC subnet and the sync states that are reported in the `Config` settings. When this value is `READY`, the endpoint is available and configured properly to handle network traffic. When the endpoint isn't available for traffic, this value will reflect its state, for example `CREATING`, `DELETING`, or `FAILED`.

Type: String

Valid Values: `CREATING | DELETING | SCALING | READY`

Required: No

SubnetId

The unique identifier of the subnet that you've specified to be used for a firewall endpoint.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^subnet-[0-9a-f]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

CustomAction

An optional, non-standard action to use for stateless packet handling. You can define this in addition to the standard action that you must specify.

You define and name the custom actions that you want to be able to use, and then you reference them by name in your actions settings.

You can use custom actions in the following places:

- In a rule group's StatelessRulesAndCustomActions (p. 159) specification. The custom actions are available for use by name inside the `StatelessRulesAndCustomActions` where you define them. You can use them for your stateless rule actions to specify what to do with a packet that matches the rule's match attributes.
- In a FirewallPolicy (p. 122) specification, in `StatelessCustomActions`. The custom actions are available for use inside the policy where you define them. You can use them for the policy's default stateless actions settings to specify what to do with packets that don't match any of the policy's stateless rules.

Contents

ActionDefinition

The custom action associated with the action name.

Type: ActionDefinition (p. 113) object

Required: Yes

ActionName

The descriptive name of the custom action. You can't change the name of a custom action after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9]+$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Dimension

The value to use in an Amazon CloudWatch custom metric dimension. This is used in the `PublishMetrics` CustomAction (p. 116). A CloudWatch custom metric dimension is a name/value pair that's part of the identity of a metric.

AWS Network Firewall sets the dimension name to `CustomAction` and you provide the dimension value.

For more information about CloudWatch custom metric dimensions, see Publishing Custom Metrics in the Amazon CloudWatch User Guide.

Contents

Value

The value to use in the custom metric dimension.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-_ ]+$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Firewall

The firewall defines the configuration settings for an AWS Network Firewall firewall. These settings include the firewall policy, the subnets in your VPC to use for the firewall endpoints, and any tags that are attached to the firewall AWS resource.

The status of the firewall, for example whether it's ready to filter network traffic, is provided in the corresponding FirewallStatus (p. 127). You can retrieve both objects by calling DescribeFirewall (p. 39).

Contents

DeleteProtection

A flag indicating whether it is possible to delete the firewall. A setting of `TRUE` indicates that the firewall is protected against deletion. Use this setting to protect against accidentally deleting a firewall that is in use. When you create a firewall, the operation initializes this flag to `TRUE`.

Type: Boolean

Required: No

Description

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallId

The unique identifier for the firewall.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

The relationship of firewall to firewall policy is many to one. Each firewall requires one firewall policy association, and you can use the same firewall policy for multiple firewalls.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FirewallPolicyChangeProtection

A setting indicating whether the firewall is protected against a change to the firewall policy association. Use this setting to protect against accidentally modifying the firewall policy for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: No

SubnetChangeProtection

A setting indicating whether the firewall is protected against changes to the subnet associations. Use this setting to protect against accidentally modifying the subnet associations for a firewall that is in use. When you create a firewall, the operation initializes this setting to `TRUE`.

Type: Boolean

Required: No

SubnetMappings

The public subnets that Network Firewall is using for the firewall. Each subnet must belong to a different Availability Zone.

Type: Array of SubnetMapping (p. 160) objects

Required: Yes

Tags

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

VpcId

The unique identifier of the VPC where the firewall is in use.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^vpc-[0-9a-f]+$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallMetadata

High-level information about a firewall, returned by operations like create and describe. You can use the information provided in the metadata to retrieve and manage a firewall.

Contents

FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

FirewallName

The descriptive name of the firewall. You can't change the name of a firewall after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicy

The firewall policy defines the behavior of a firewall using a collection of stateless and stateful rule groups and other settings. You can use one firewall policy for multiple firewalls.

This, along with FirewallPolicyResponse (p. 125), define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Contents

StatefulDefaultActions

The default actions to take on a packet that doesn't match any stateful rules. The stateful default action is optional, and is only valid when using the strict rule order.

Valid values of the stateful default action:

- aws:drop_strict
- aws:drop_established
- aws:alert_strict
- aws:alert_established

For more information, see Strict evaluation order in the *AWS Network Firewall Developer Guide*.

Type: Array of strings

Required: No

StatefulEngineOptions

Additional options governing how Network Firewall handles stateful rules. The stateful rule groups that you use in your policy must have stateful rule options settings that are compatible with these settings.

Type: StatefulEngineOptions (p. 153) object

Required: No

StatefulRuleGroupReferences

References to the stateful rule groups that are used in the policy. These define the inspection criteria in stateful rules.

Type: Array of StatefulRuleGroupReference (p. 155) objects

Required: No

StatelessCustomActions

The custom action definitions that are available for use in the firewall policy's `StatelessDefaultActions` setting. You name each custom action that you define, and then you can use it by name in your default actions specifications.

Type: Array of CustomAction (p. 116) objects

Required: No

StatelessDefaultActions

The actions to take on a packet if it doesn't match any of the stateless rules in the policy. If you want non-matching packets to be forwarded for stateful inspection, specify `aws:forward_to_sfe`.

You must specify one of the standard actions: `aws:pass`, `aws:drop`, or `aws:forward_to_sfe`. In addition, you can specify custom actions that are compatible with your standard section choice.

For example, you could specify `["aws:pass"]` or you could specify `["aws:pass", "customActionName"]`. For information about compatibility, see the custom action descriptions under CustomAction (p. 116).

Type: Array of strings

Required: Yes

StatelessFragmentDefaultActions

The actions to take on a fragmented UDP packet if it doesn't match any of the stateless rules in the policy. Network Firewall only manages UDP packet fragments and silently drops packet fragments for other protocols. If you want non-matching fragmented UDP packets to be forwarded for stateful inspection, specify `aws:forward_to_sfe`.

You must specify one of the standard actions: `aws:pass`, `aws:drop`, or `aws:forward_to_sfe`. In addition, you can specify custom actions that are compatible with your standard section choice.

For example, you could specify `["aws:pass"]` or you could specify `["aws:pass", "customActionName"]`. For information about compatibility, see the custom action descriptions under CustomAction (p. 116).

Type: Array of strings

Required: Yes

StatelessRuleGroupReferences

References to the stateless rule groups that are used in the policy. These define the matching criteria in stateless rules.

Type: Array of StatelessRuleGroupReference (p. 158) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicyMetadata

High-level information about a firewall policy, returned by operations like create and describe. You can use the information provided in the metadata to retrieve and manage a firewall policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Contents

Arn

The Amazon Resource Name (ARN) of the firewall policy.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Name

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallPolicyResponse

The high-level properties of a firewall policy. This, along with the FirewallPolicy (p. 122), define the policy. You can retrieve all objects for a firewall policy by calling DescribeFirewallPolicy (p. 43).

Contents

ConsumedStatefulRuleCapacity

The number of capacity units currently consumed by the policy's stateful rules.

Type: Integer

Required: No

ConsumedStatelessRuleCapacity

The number of capacity units currently consumed by the policy's stateless rules.

Type: Integer

Required: No

Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

FirewallPolicyArn

The Amazon Resource Name (ARN) of the firewall policy.

> **Note**
> If this response is for a create request that had `DryRun` set to `TRUE`, then this ARN is a placeholder that isn't attached to a valid resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

FirewallPolicyId

The unique identifier for the firewall policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

FirewallPolicyName

The descriptive name of the firewall policy. You can't change the name of a firewall policy after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

FirewallPolicyStatus

The current status of the firewall policy. You can retrieve this for a firewall policy by calling DescribeFirewallPolicy (p. 43) and providing the firewall policy's name or ARN.

Type: String

Valid Values: `ACTIVE | DELETING`

Required: No

NumberOfAssociations

The number of firewalls that are associated with this firewall policy.

Type: Integer

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

FirewallStatus

Detailed information about the current status of a Firewall (p. 118). You can retrieve this for a firewall by calling DescribeFirewall (p. 39) and providing the firewall name and ARN.

Contents

ConfigurationSyncStateSummary

The configuration sync state for the firewall. This summarizes the sync states reported in the `Config` settings for all of the Availability Zones where you have configured the firewall.

When you create a firewall or update its configuration, for example by adding a rule group to its firewall policy, Network Firewall distributes the configuration changes to all zones where the firewall is in use. This summary indicates whether the configuration changes have been applied everywhere.

This status must be `IN_SYNC` for the firewall to be ready for use, but it doesn't indicate that the firewall is ready. The `Status` setting indicates firewall readiness.

Type: String

Valid Values: `PENDING | IN_SYNC`

Required: Yes

Status

The readiness of the configured firewall to handle network traffic across all of the Availability Zones where you've configured it. This setting is `READY` only when the `ConfigurationSyncStateSummary` value is `IN_SYNC` and the `Attachment Status` values for all of the configured subnets are `READY`.

Type: String

Valid Values: `PROVISIONING | DELETING | READY`

Required: Yes

SyncStates

The subnets that you've configured for use by the Network Firewall firewall. This contains one array element per Availability Zone where you've configured a subnet. These objects provide details of the information that is summarized in the `ConfigurationSyncStateSummary` and `Status`, broken down by zone and configuration object.

Type: String to SyncState (p. 161) object map

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Header

The basic rule criteria for AWS Network Firewall to use to inspect packet headers in stateful traffic flow inspection. Traffic flows that match the criteria are a match for the corresponding StatefulRule (p. 154).

Contents

Destination

The destination IP address or address range to inspect for, in CIDR notation. To match with any address, specify `ANY`.

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

DestinationPort

The destination port to inspect for. You can specify an individual port, for example `1994` and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

Direction

The direction of traffic flow to inspect. If set to `ANY`, the inspection matches bidirectional traffic, both from the source to the destination and from the destination to the source. If set to `FORWARD`, the inspection only matches traffic going from the source to the destination.

Type: String

Valid Values: `FORWARD | ANY`

Required: Yes

Protocol

The protocol to inspect for. To specify all, you can use `IP`, because all traffic on AWS and on the internet is IP.

Type: String

Valid Values: `IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP`

Required: Yes

Source

The source IP address or address range to inspect for, in CIDR notation. To match with any address, specify `ANY`.

Specify an IP address or a block of IP addresses in Classless Inter-Domain Routing (CIDR) notation. Network Firewall supports all address ranges for IPv4.

Examples:

- To configure Network Firewall to inspect for the IP address 192.0.2.44, specify `192.0.2.44/32`.
- To configure Network Firewall to inspect for IP addresses from 192.0.2.0 to 192.0.2.255, specify `192.0.2.0/24`.

For more information about CIDR notation, see the Wikipedia entry Classless Inter-Domain Routing.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

SourcePort

The source port to inspect for. You can specify an individual port, for example `1994` and you can specify a port range, for example `1990:1994`. To match with any port, specify `ANY`.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

IPSet

A list of IP addresses and address ranges, in CIDR notation. This is part of a RuleVariables (p. 152).

Contents

Definition

The list of IP addresses and address ranges, in CIDR notation.

Type: Array of strings

Length Constraints: Minimum length of 1.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LogDestinationConfig

Defines where AWS Network Firewall sends logs for the firewall for one log type. This is used in LoggingConfiguration (p. 134). You can send each type of log to an Amazon S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

Network Firewall generates logs for stateful rule groups. You can save alert and flow log types. The stateful rules engine records flow logs for all network traffic that it receives. It records alert logs for traffic that matches stateful rules that have the rule action set to `DROP` or `ALERT`.

Contents

LogDestination

The named location for the logs, provided in a key:value mapping that is specific to the chosen destination type.

- For an Amazon S3 bucket, provide the name of the bucket, with key `bucketName`, and optionally provide a prefix, with key `prefix`. The following example specifies an Amazon S3 bucket named `DOC-EXAMPLE-BUCKET` and the prefix `alerts`:

  ```
  "LogDestination": { "bucketName": "DOC-EXAMPLE-BUCKET", "prefix": "alerts" }
  ```

- For a CloudWatch log group, provide the name of the CloudWatch log group, with key `logGroup`. The following example specifies a log group named `alert-log-group`:

  ```
  "LogDestination": { "logGroup": "alert-log-group" }
  ```

- For a Kinesis Data Firehose delivery stream, provide the name of the delivery stream, with key `deliveryStream`. The following example specifies a delivery stream named `alert-delivery-stream`:

  ```
  "LogDestination": { "deliveryStream": "alert-delivery-stream" }
  ```

Type: String to string map

Key Length Constraints: Minimum length of 3. Maximum length of 50.

Key Pattern: `^[0-9A-Za-z.\-_@\/]+$`

Value Length Constraints: Minimum length of 1. Maximum length of 1024.

Value Pattern: `[\s\S]*$`

Required: Yes

LogDestinationType

The type of storage destination to send these logs to. You can send logs to an Amazon S3 bucket, a CloudWatch log group, or a Kinesis Data Firehose delivery stream.

Type: String

Length Constraints: Minimum length of 2. Maximum length of 30.

Pattern: `[0-9A-Za-z]+`

Valid Values: `S3 | CloudWatchLogs | KinesisDataFirehose`

Required: Yes

LogType

The type of log to send. Alert logs report traffic that matches a StatefulRule (p. 154) with an action setting that sends an alert log message. Flow logs are standard network traffic flow logs.

Type: String

Valid Values: `ALERT | FLOW`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

LoggingConfiguration

Defines how AWS Network Firewall performs logging for a Firewall (p. 118).

Contents

LogDestinationConfigs

Defines the logging destinations for the logs for a firewall. Network Firewall generates logs for stateful rule groups.

Type: Array of LogDestinationConfig (p. 132) objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

MatchAttributes

Criteria for Network Firewall to use to inspect an individual packet in stateless rule inspection. Each match attributes set can include one or more items such as IP address, CIDR range, port number, protocol, and TCP flags.

Contents

DestinationPorts

The destination ports to inspect for. If not specified, this matches with any destination port. This setting is only used for protocols 6 (TCP) and 17 (UDP).

You can specify individual ports, for example `1994` and you can specify port ranges, for example `1990:1994`.

Type: Array of PortRange (p. 138) objects

Required: No

Destinations

The destination IP addresses and address ranges to inspect for, in CIDR notation. If not specified, this matches with any destination address.

Type: Array of Address (p. 114) objects

Required: No

Protocols

The protocols to inspect for, specified using each protocol's assigned internet protocol number (IANA). If not specified, this matches with any protocol.

Type: Array of integers

Valid Range: Minimum value of 0. Maximum value of 255.

Required: No

SourcePorts

The source ports to inspect for. If not specified, this matches with any source port. This setting is only used for protocols 6 (TCP) and 17 (UDP).

You can specify individual ports, for example `1994` and you can specify port ranges, for example `1990:1994`.

Type: Array of PortRange (p. 138) objects

Required: No

Sources

The source IP addresses and address ranges to inspect for, in CIDR notation. If not specified, this matches with any source address.

Type: Array of Address (p. 114) objects

Required: No

TCPFlags

The TCP flags and masks to inspect for. If not specified, this matches with any settings. This setting is only used for protocol 6 (TCP).

Type: Array of TCPFlagField (p. 163) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PerObjectStatus

Provides configuration status for a single policy or rule group that is used for a firewall endpoint. Network Firewall provides each endpoint with the rules that are configured in the firewall policy. Each time you add a subnet or modify the associated firewall policy, Network Firewall synchronizes the rules in the endpoint, so it can properly filter network traffic. This is part of a SyncState (p. 161) for a firewall.

Contents

SyncStatus

Indicates whether this object is in sync with the version indicated in the update token.

Type: String

Valid Values: `PENDING | IN_SYNC`

Required: No

UpdateToken

The current version of the object that is either in sync or pending synchronization.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 1024.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortRange

A single port range specification. This is used for source and destination port ranges in the stateless rule MatchAttributes (p. 135), `SourcePorts`, and `DestinationPorts` settings.

Contents

FromPort

The lower limit of the port range. This must be less than or equal to the `ToPort` specification.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: Yes

ToPort

The upper limit of the port range. This must be greater than or equal to the `FromPort` specification.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PortSet

A set of port ranges for use in the rules in a rule group.

Contents

Definition

The set of port ranges.

Type: Array of strings

Length Constraints: Minimum length of 1.

Pattern: `^.*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PublishMetricAction

Stateless inspection criteria that publishes the specified metrics to Amazon CloudWatch for the matching packet. This setting defines a CloudWatch dimension value to be published.

Contents

Dimensions

Type: Array of Dimension (p. 117) objects

Array Members: Fixed number of 1 item.

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleDefinition

The inspection criteria and action for a single stateless rule. AWS Network Firewall inspects each packet for the specified matching criteria. When a packet matches the criteria, Network Firewall performs the rule's actions on the packet.

Contents

Actions

The actions to take on a packet that matches one of the stateless rule definition's match attributes. You must specify a standard action and you can add custom actions.

Note
Network Firewall only forwards a packet for stateful rule inspection if you specify `aws:forward_to_sfe` for a rule that the packet matches, or if the packet doesn't match any stateless rule and you specify `aws:forward_to_sfe` for the `StatelessDefaultActions` setting for the FirewallPolicy (p. 122).

For every rule, you must specify exactly one of the following standard actions.

- **aws:pass** - Discontinues all inspection of the packet and permits it to go to its intended destination.
- **aws:drop** - Discontinues all inspection of the packet and blocks it from going to its intended destination.
- **aws:forward_to_sfe** - Discontinues stateless inspection of the packet and forwards it to the stateful rule engine for inspection.

Additionally, you can specify a custom action. To do this, you define a custom action by name and type, then provide the name you've assigned to the action in this `Actions` setting. For information about the options, see CustomAction (p. 116).

To provide more than one action in this setting, separate the settings with a comma. For example, if you have a custom `PublishMetrics` action that you've named `MyMetricsAction`, then you could specify the standard action `aws:pass` and the custom action with `["aws:pass", "MyMetricsAction"]`.

Type: Array of strings

Required: Yes

MatchAttributes

Criteria for Network Firewall to use to inspect an individual packet in stateless rule inspection. Each match attributes set can include one or more items such as IP address, CIDR range, port number, protocol, and TCP flags.

Type: MatchAttributes (p. 135) object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroup

The object that defines the rules in a rule group. This, along with RuleGroupResponse (p. 145), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

AWS Network Firewall uses a rule group to inspect and control network traffic. You define stateless rule groups to inspect individual packets and you define stateful rule groups to inspect packets in the context of their traffic flow.

To use a rule group, you include it by reference in an Network Firewall firewall policy, then you use the policy in a firewall. You can reference a rule group from more than one firewall policy, and you can use a firewall policy in more than one firewall.

Contents

RulesSource

The stateful rules or stateless rules for the rule group.

Type: RulesSource (p. 149) object

Required: Yes

RuleVariables

Settings that are available for use in the rules in the rule group. You can only use these for stateful rule groups.

Type: RuleVariables (p. 152) object

Required: No

StatefulRuleOptions

Additional options governing how Network Firewall handles stateful rules. The policies where you use your stateful rule group must have stateful rule options settings that are compatible with these settings.

Type: StatefulRuleOptions (p. 156) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroupMetadata

High-level information about a rule group, returned by ListRuleGroups (p. 67). You can use the information provided in the metadata to retrieve and manage a rule group.

Contents

Arn

The Amazon Resource Name (ARN) of the rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: No

Name

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleGroupResponse

The high-level properties of a rule group. This, along with the RuleGroup (p. 143), define the rule group. You can retrieve all objects for a rule group by calling DescribeRuleGroup (p. 52).

Contents

Capacity

The maximum operating resources that this rule group can use. Rule group capacity is fixed at creation. When you update a rule group, you are limited to this capacity. When you reference a rule group from a firewall policy, Network Firewall reserves this capacity for the rule group.

You can retrieve the capacity that would be required for a rule group before you create the rule group by calling CreateRuleGroup (p. 21) with `DryRun` set to `TRUE`.

Type: Integer

Required: No

ConsumedCapacity

The number of capacity units currently consumed by the rule group rules.

Type: Integer

Required: No

Description

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

NumberOfAssociations

The number of firewall policies that use this rule group.

Type: Integer

Required: No

RuleGroupArn

The Amazon Resource Name (ARN) of the rule group.

> **Note**
> If this response is for a create request that had `DryRun` set to `TRUE`, then this ARN is a placeholder that isn't attached to a valid resource.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

RuleGroupId

The unique identifier for the rule group.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^([0-9a-f]{8})-([0-9a-f]{4}-){3}([0-9a-f]{12})$`

Required: Yes

RuleGroupName

The descriptive name of the rule group. You can't change the name of a rule group after you create it.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^[a-zA-Z0-9-]+$`

Required: Yes

RuleGroupStatus

Detailed information about the current status of a rule group.

Type: String

Valid Values: `ACTIVE | DELETING`

Required: No

Tags

The key:value pairs to associate with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 1 item. Maximum number of 200 items.

Required: No

Type

Indicates whether the rule group is stateless or stateful. If the rule group is stateless, it contains stateless rules. If it is stateful, it contains stateful rules.

Type: String

Valid Values: `STATELESS | STATEFUL`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleOption

Additional settings for a stateful rule. This is part of the StatefulRule (p. 154) configuration.

Contents

Keyword

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `.*`

Required: Yes

Settings

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 8192.

Pattern: `.*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RulesSource

The stateless or stateful rules definitions for use in a single rule group. Each rule group requires a single `RulesSource`. You can use an instance of this for either stateless rules or stateful rules.

Contents

RulesSourceList

Stateful inspection criteria for a domain list rule group.

Type: RulesSourceList (p. 150) object

Required: No

RulesString

Stateful inspection criteria, provided in Suricata compatible intrusion prevention system (IPS) rules. Suricata is an open-source network IPS that includes a standard rule-based language for network traffic inspection.

These rules contain the inspection criteria and the action to take for traffic that matches the criteria, so this type of rule group doesn't have a separate action setting.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 2000000.

Required: No

StatefulRules

An array of individual stateful rules inspection criteria to be used together in a stateful rule group. Use this option to specify simple Suricata rules with protocol, source and destination, ports, direction, and rule options. For information about the Suricata `Rules` format, see Rules Format.

Type: Array of StatefulRule (p. 154) objects

Required: No

StatelessRulesAndCustomActions

Stateless inspection criteria to be used in a stateless rule group.

Type: StatelessRulesAndCustomActions (p. 159) object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RulesSourceList

Stateful inspection criteria for a domain list rule group.

For HTTPS traffic, domain filtering is SNI-based. It uses the server name indicator extension of the TLS handshake.

By default, Network Firewall domain list inspection only includes traffic coming from the VPC where you deploy the firewall. To inspect traffic from IP addresses outside of the deployment VPC, you set the `HOME_NET` rule variable to include the CIDR range of the deployment VPC plus the other CIDR ranges. For more information, see RuleVariables (p. 152) in this guide and Stateful domain list rule groups in AWS Network Firewall in the *Network Firewall Developer Guide*.

Contents

GeneratedRulesType

Whether you want to allow or deny access to the domains in your target list.

Type: String

Valid Values: `ALLOWLIST | DENYLIST`

Required: Yes

Targets

The domains that you want to inspect for in your traffic flows. Valid domain specifications are the following:

- Explicit names. For example, `abc.example.com` matches only the domain `abc.example.com`.
- Names that use a domain wildcard, which you indicate with an initial `'.'`. For example, `.example.com` matches `example.com` and matches all subdomains of `example.com`, such as `abc.example.com` and `www.example.com`.

Type: Array of strings

Required: Yes

TargetTypes

The protocols you want to inspect. Specify `TLS_SNI` for `HTTPS`. Specify `HTTP_HOST` for `HTTP`. You can specify either or both.

Type: Array of strings

Valid Values: `TLS_SNI | HTTP_HOST`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RuleVariables

Settings that are available for use in the rules in the RuleGroup (p. 143) where this is defined.

Contents

IPSets

A list of IP addresses and address ranges, in CIDR notation.

Type: String to IPSet (p. 131) object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

PortSets

A list of port ranges.

Type: String to PortSet (p. 139) object map

Key Length Constraints: Minimum length of 1. Maximum length of 32.

Key Pattern: `^[A-Za-z][A-Za-z0-9_]*$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulEngineOptions

Configuration settings for the handling of the stateful rule groups in a firewall policy.

Contents

RuleOrder

Indicates how to manage the order of stateful rule evaluation for the policy. `DEFAULT_ACTION_ORDER` is the default behavior. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on certain settings. For more information, see Evaluation order for stateful rules in the *AWS Network Firewall Developer Guide*.

Type: String

Valid Values: `DEFAULT_ACTION_ORDER | STRICT_ORDER`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRule

A single Suricata rules specification, for use in a stateful rule group. Use this option to specify a simple Suricata rule with protocol, source and destination, ports, direction, and rule options. For information about the Suricata `Rules` format, see Rules Format.

Contents

Action

Defines what Network Firewall should do with the packets in a traffic flow when the flow matches the stateful rule criteria. For all actions, Network Firewall performs the specified action and discontinues stateful inspection of the traffic flow.

The actions for a stateful rule are defined as follows:

- **PASS** - Permits the packets to go to the intended destination.
- **DROP** - Blocks the packets from going to the intended destination and sends an alert log message, if alert logging is configured in the Firewall (p. 118) LoggingConfiguration (p. 134).
- **ALERT** - Permits the packets to go to the intended destination and sends an alert log message, if alert logging is configured in the Firewall (p. 118) LoggingConfiguration (p. 134).

  You can use this action to test a rule that you intend to use to drop traffic. You can enable the rule with `ALERT` action, verify in the logs that the rule is filtering as you want, then change the action to `DROP`.

Type: String

Valid Values: `PASS | DROP | ALERT`

Required: Yes

Header

The stateful inspection criteria for this rule, used to inspect traffic flows.

Type: Header (p. 129) object

Required: Yes

RuleOptions

Additional options for the rule. These are the Suricata `RuleOptions` settings.

Type: Array of RuleOption (p. 148) objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleGroupReference

Identifier for a single stateful rule group, used in a firewall policy to refer to a rule group.

Contents

Priority

An integer setting that indicates the order in which to run the stateful rule groups in a single FirewallPolicy (p. 122). This setting only applies to firewall policies that specify the `STRICT_ORDER` rule order in the stateful engine options settings.

Network Firewall evalutes each stateful rule group against a packet starting with the group that has the lowest priority setting. You must ensure that the priority settings are unique within each policy.

You can change the priority settings of your rule groups at any time. To make it easier to insert rule groups later, number them so there's a wide range in between, for example use 100, 200, and so on.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: No

ResourceArn

The Amazon Resource Name (ARN) of the stateful rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleOptions

Additional options governing how Network Firewall handles the rule group. You can only use these for stateful rule groups.

Contents

RuleOrder

Indicates how to manage the order of the rule evaluation for the rule group. `DEFAULT_ACTION_ORDER` is the default behavior. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on certain settings. For more information, see Evaluation order for stateful rules in the *AWS Network Firewall Developer Guide*.

Type: String

Valid Values: `DEFAULT_ACTION_ORDER | STRICT_ORDER`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRule

A single stateless rule. This is used in StatelessRulesAndCustomActions (p. 159).

Contents

Priority

Indicates the order in which to run this rule relative to all of the rules that are defined for a stateless rule group. Network Firewall evaluates the rules in a rule group starting with the lowest priority setting. You must ensure that the priority settings are unique for the rule group.

Each stateless rule group uses exactly one `StatelessRulesAndCustomActions` object, and each `StatelessRulesAndCustomActions` contains exactly one `StatelessRules` object. To ensure unique priority settings for your rule groups, set unique priorities for the stateless rules that you define inside any single `StatelessRules` object.

You can change the priority settings of your rules at any time. To make it easier to insert rules later, number them so there's a wide range in between, for example use 100, 200, and so on.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: Yes

RuleDefinition

Defines the stateless 5-tuple packet inspection criteria and the action to take on a packet that matches the criteria.

Type: RuleDefinition (p. 141) object

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRuleGroupReference

Identifier for a single stateless rule group, used in a firewall policy to refer to the rule group.

Contents

Priority

An integer setting that indicates the order in which to run the stateless rule groups in a single FirewallPolicy (p. 122). Network Firewall applies each stateless rule group to a packet starting with the group that has the lowest priority setting. You must ensure that the priority settings are unique within each policy.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: Yes

ResourceArn

The Amazon Resource Name (ARN) of the stateless rule group.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 256.

Pattern: `^arn:aws.*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRulesAndCustomActions

Stateless inspection criteria. Each stateless rule group uses exactly one of these data types to define its stateless rules.

Contents

CustomActions

Defines an array of individual custom action definitions that are available for use by the stateless rules in this `StatelessRulesAndCustomActions` specification. You name each custom action that you define, and then you can use it by name in your StatelessRule (p. 157) RuleDefinition (p. 141) `Actions` specification.

Type: Array of CustomAction (p. 116) objects

Required: No

StatelessRules

Defines the set of stateless rules for use in a stateless rule group.

Type: Array of StatelessRule (p. 157) objects

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SubnetMapping

The ID for a subnet that you want to associate with the firewall. This is used with CreateFirewall (p. 12) and AssociateSubnets (p. 8). AWS Network Firewall creates an instance of the associated firewall in each subnet that you specify, to filter traffic in the subnet's Availability Zone.

Contents

SubnetId

The unique identifier for the subnet.

Type: String

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SyncState

The status of the firewall endpoint and firewall policy configuration for a single VPC subnet.

For each VPC subnet that you associate with a firewall, AWS Network Firewall does the following:

- Instantiates a firewall endpoint in the subnet, ready to take traffic.
- Configures the endpoint with the current firewall policy settings, to provide the filtering behavior for the endpoint.

When you update a firewall, for example to add a subnet association or change a rule group in the firewall policy, the affected sync states reflect out-of-sync or not ready status until the changes are complete.

Contents

Attachment

The attachment status of the firewall's association with a single VPC subnet. For each configured subnet, Network Firewall creates the attachment by instantiating the firewall endpoint in the subnet so that it's ready to take traffic. This is part of the FirewallStatus (p. 127).

Type: Attachment (p. 115) object

Required: No

Config

The configuration status of the firewall endpoint in a single VPC subnet. Network Firewall provides each endpoint with the rules that are configured in the firewall policy. Each time you add a subnet or modify the associated firewall policy, Network Firewall synchronizes the rules in the endpoint, so it can properly filter network traffic. This is part of the FirewallStatus (p. 127).

Type: String to PerObjectStatus (p. 137) object map

Key Length Constraints: Minimum length of 1. Maximum length of 128.

Key Pattern: `^[a-zA-Z0-9-]+$`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A key:value pair associated with an AWS resource. The key:value pair can be anything you define. Typically, the tag key represents a category (such as "environment") and the tag value represents a specific value within that category (such as "test," "development," or "production"). You can add up to 50 tags to each AWS resource.

Contents

Key

The part of the key:value pair that defines a tag. You can use a tag key to describe a category of information, such as "customer." Tag keys are case-sensitive.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 128.

Pattern: `^.*$`

Required: Yes

Value

The part of the key:value pair that defines a tag. You can use a tag value to describe a specific value within a category, such as "companyA" or "companyB." Tag values are case-sensitive.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `^.*$`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

TCPFlagField

TCP flags and masks to inspect packets for, used in stateless rules MatchAttributes (p. 135) settings.

Contents

Flags

Used in conjunction with the `Masks` setting to define the flags that must be set and flags that must not be set in order for the packet to match. This setting can only specify values that are also specified in the `Masks` setting.

For the flags that are specified in the masks setting, the following must be true for the packet to match:

- The ones that are set in this flags setting must be set in the packet.
- The ones that are not set in this flags setting must also not be set in the packet.

Type: Array of strings

Valid Values: `FIN | SYN | RST | PSH | ACK | URG | ECE | CWR`

Required: Yes

Masks

The set of flags to consider in the inspection. To inspect all flags in the valid values list, leave this with no setting.

Type: Array of strings

Valid Values: `FIN | SYN | RST | PSH | ACK | URG | ECE | CWR`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is

not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400