

# Amazon Network Firewall



# Amazon Network Firewall: API Reference

# Table of Contents

<b>Welcome .....</b>	<b>1</b>
<b>Actions .....</b>	<b>3</b>
AssociateFirewallPolicy .....	5
Request Syntax .....	5
Request Parameters .....	5
Response Syntax .....	7
Response Elements .....	7
Errors .....	8
See Also .....	9
AssociateSubnets .....	11
Request Syntax .....	11
Request Parameters .....	11
Response Syntax .....	13
Response Elements .....	13
Errors .....	14
See Also .....	15
CreateFirewall .....	17
Request Syntax .....	17
Request Parameters .....	18
Response Syntax .....	20
Response Elements .....	22
Errors .....	22
See Also .....	23
CreateFirewallPolicy .....	24
Request Syntax .....	24
Request Parameters .....	25
Response Syntax .....	27
Response Elements .....	27
Errors .....	28
See Also .....	29
CreateRuleGroup .....	30
Request Syntax .....	30
Request Parameters .....	33
Response Syntax .....	37

---

Response Elements .....	38
Errors .....	38
See Also .....	39
CreateTLSInspectionConfiguration .....	41
Request Syntax .....	41
Request Parameters .....	42
Response Syntax .....	44
Response Elements .....	45
Errors .....	46
See Also .....	47
DeleteFirewall .....	48
Request Syntax .....	48
Request Parameters .....	48
Response Syntax .....	49
Response Elements .....	50
Errors .....	51
See Also .....	52
DeleteFirewallPolicy .....	53
Request Syntax .....	53
Request Parameters .....	53
Response Syntax .....	54
Response Elements .....	54
Errors .....	55
See Also .....	56
DeleteResourcePolicy .....	57
Request Syntax .....	57
Request Parameters .....	57
Response Elements .....	57
Errors .....	57
See Also .....	58
DeleteRuleGroup .....	60
Request Syntax .....	60
Request Parameters .....	60
Response Syntax .....	61
Response Elements .....	62
Errors .....	62

---

See Also .....	63
DeleteTLSInspectionConfiguration .....	65
Request Syntax .....	65
Request Parameters .....	65
Response Syntax .....	66
Response Elements .....	66
Errors .....	67
See Also .....	68
DescribeFirewall .....	69
Request Syntax .....	69
Request Parameters .....	69
Response Syntax .....	70
Response Elements .....	71
Errors .....	72
See Also .....	73
DescribeFirewallPolicy .....	74
Request Syntax .....	74
Request Parameters .....	74
Response Syntax .....	75
Response Elements .....	76
Errors .....	77
See Also .....	78
DescribeLoggingConfiguration .....	79
Request Syntax .....	79
Request Parameters .....	79
Response Syntax .....	80
Response Elements .....	80
Errors .....	80
See Also .....	81
DescribeResourcePolicy .....	83
Request Syntax .....	83
Request Parameters .....	83
Response Syntax .....	83
Response Elements .....	83
Errors .....	84
See Also .....	85

DescribeRuleGroup .....	86
Request Syntax .....	86
Request Parameters .....	86
Response Syntax .....	87
Response Elements .....	91
Errors .....	92
See Also .....	92
DescribeRuleGroupMetadata .....	94
Request Syntax .....	94
Request Parameters .....	94
Response Syntax .....	95
Response Elements .....	95
Errors .....	97
See Also .....	98
DescribeTLSInspectionConfiguration .....	99
Request Syntax .....	99
Request Parameters .....	99
Response Syntax .....	100
Response Elements .....	101
Errors .....	103
See Also .....	103
DisassociateSubnets .....	105
Request Syntax .....	105
Request Parameters .....	105
Response Syntax .....	106
Response Elements .....	107
Errors .....	108
See Also .....	109
ListFirewallPolicies .....	110
Request Syntax .....	110
Request Parameters .....	110
Response Syntax .....	111
Response Elements .....	111
Errors .....	112
See Also .....	112
ListFirewalls .....	114

Request Syntax .....	114
Request Parameters .....	114
Response Syntax .....	115
Response Elements .....	115
Errors .....	116
See Also .....	117
ListRuleGroups .....	118
Request Syntax .....	118
Request Parameters .....	118
Response Syntax .....	119
Response Elements .....	120
Errors .....	120
See Also .....	121
ListTagsForResource .....	122
Request Syntax .....	122
Request Parameters .....	122
Response Syntax .....	123
Response Elements .....	123
Errors .....	124
See Also .....	125
ListTLSInspectionConfigurations .....	126
Request Syntax .....	126
Request Parameters .....	126
Response Syntax .....	127
Response Elements .....	127
Errors .....	128
See Also .....	128
PutResourcePolicy .....	130
Request Syntax .....	130
Request Parameters .....	130
Response Elements .....	131
Errors .....	131
See Also .....	132
TagResource .....	134
Request Syntax .....	134
Request Parameters .....	134

Response Elements .....	135
Errors .....	135
See Also .....	136
UntagResource .....	137
Request Syntax .....	137
Request Parameters .....	137
Response Elements .....	138
Errors .....	138
See Also .....	139
UpdateFirewallDeleteProtection .....	140
Request Syntax .....	140
Request Parameters .....	140
Response Syntax .....	141
Response Elements .....	142
Errors .....	143
See Also .....	144
UpdateFirewallDescription .....	145
Request Syntax .....	145
Request Parameters .....	145
Response Syntax .....	146
Response Elements .....	147
Errors .....	148
See Also .....	149
UpdateFirewallEncryptionConfiguration .....	150
Request Syntax .....	150
Request Parameters .....	150
Response Syntax .....	151
Response Elements .....	152
Errors .....	153
See Also .....	154
UpdateFirewallPolicy .....	156
Request Syntax .....	156
Request Parameters .....	157
Response Syntax .....	159
Response Elements .....	160
Errors .....	161



---

See Also .....	162
UpdateFirewallPolicyChangeProtection .....	163
Request Syntax .....	163
Request Parameters .....	163
Response Syntax .....	164
Response Elements .....	165
Errors .....	166
See Also .....	167
UpdateLoggingConfiguration .....	168
Request Syntax .....	168
Request Parameters .....	169
Response Syntax .....	170
Response Elements .....	170
Errors .....	171
See Also .....	172
UpdateRuleGroup .....	173
Request Syntax .....	173
Request Parameters .....	176
Response Syntax .....	179
Response Elements .....	180
Errors .....	181
See Also .....	182
UpdateSubnetChangeProtection .....	183
Request Syntax .....	183
Request Parameters .....	183
Response Syntax .....	184
Response Elements .....	185
Errors .....	186
See Also .....	187
UpdateTLSInspectionConfiguration .....	188
Request Syntax .....	188
Request Parameters .....	189
Response Syntax .....	191
Response Elements .....	192
Errors .....	193
See Also .....	194

<b>Data Types</b> .....	<b>195</b>
ActionDefinition .....	198
Contents .....	198
See Also .....	198
Address .....	199
Contents .....	199
See Also .....	199
AnalysisResult .....	201
Contents .....	201
See Also .....	202
Attachment .....	203
Contents .....	203
See Also .....	204
CapacityUsageSummary .....	205
Contents .....	205
See Also .....	205
CheckCertificateRevocationStatusActions .....	206
Contents .....	206
See Also .....	207
CIDRSummary .....	208
Contents .....	208
See Also .....	208
CustomAction .....	210
Contents .....	210
See Also .....	211
Dimension .....	212
Contents .....	212
See Also .....	212
EncryptionConfiguration .....	213
Contents .....	213
See Also .....	213
Firewall .....	215
Contents .....	215
See Also .....	218
FirewallMetadata .....	219
Contents .....	219

---

See Also .....	219
FirewallPolicy .....	220
Contents .....	220
See Also .....	222
FirewallPolicyMetadata .....	224
Contents .....	224
See Also .....	224
FirewallPolicyResponse .....	226
Contents .....	226
See Also .....	228
FirewallStatus .....	229
Contents .....	229
See Also .....	230
Header .....	231
Contents .....	231
See Also .....	233
IPSet .....	235
Contents .....	235
See Also .....	235
IPSetMetadata .....	236
Contents .....	236
See Also .....	236
IPSetReference .....	237
Contents .....	237
See Also .....	237
LogDestinationConfig .....	238
Contents .....	238
See Also .....	239
LoggingConfiguration .....	240
Contents .....	240
See Also .....	240
MatchAttributes .....	241
Contents .....	241
See Also .....	242
PerObjectStatus .....	243
Contents .....	243

---

See Also .....	243
PolicyVariables .....	245
Contents .....	245
See Also .....	245
PortRange .....	246
Contents .....	246
See Also .....	246
PortSet .....	247
Contents .....	247
See Also .....	247
PublishMetricAction .....	248
Contents .....	248
See Also .....	248
ReferenceSets .....	249
Contents .....	249
See Also .....	249
RuleDefinition .....	250
Contents .....	250
See Also .....	251
RuleGroup .....	252
Contents .....	252
See Also .....	253
RuleGroupMetadata .....	254
Contents .....	254
See Also .....	254
RuleGroupResponse .....	255
Contents .....	255
See Also .....	258
RuleOption .....	260
Contents .....	260
See Also .....	260
RulesSource .....	262
Contents .....	262
See Also .....	263
RulesSourceList .....	264
Contents .....	264

---

See Also .....	265
RuleVariables .....	266
Contents .....	266
See Also .....	266
ServerCertificate .....	267
Contents .....	267
See Also .....	267
ServerCertificateConfiguration .....	268
Contents .....	268
See Also .....	269
ServerCertificateScope .....	270
Contents .....	270
See Also .....	271
SourceMetadata .....	272
Contents .....	272
See Also .....	272
StatefulEngineOptions .....	274
Contents .....	274
See Also .....	275
StatefulRule .....	276
Contents .....	276
See Also .....	277
StatefulRuleGroupOverride .....	278
Contents .....	278
See Also .....	278
StatefulRuleGroupReference .....	279
Contents .....	279
See Also .....	280
StatefulRuleOptions .....	281
Contents .....	281
See Also .....	281
StatelessRule .....	282
Contents .....	282
See Also .....	282
StatelessRuleGroupReference .....	284
Contents .....	284

---

See Also .....	284
StatelessRulesAndCustomActions .....	285
Contents .....	285
See Also .....	285
SubnetMapping .....	286
Contents .....	286
See Also .....	286
SyncState .....	287
Contents .....	287
See Also .....	288
Tag .....	289
Contents .....	289
See Also .....	289
TCPFlagField .....	291
Contents .....	291
See Also .....	291
TlsCertificateData .....	293
Contents .....	293
See Also .....	294
TLSInspectionConfiguration .....	295
Contents .....	295
See Also .....	295
TLSInspectionConfigurationMetadata .....	296
Contents .....	296
See Also .....	296
TLSInspectionConfigurationResponse .....	298
Contents .....	298
See Also .....	300
<b>Common Parameters .....</b>	<b>301</b>
<b>Common Errors .....</b>	<b>304</b>

# Welcome

This is the API Reference for Amazon 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 Amazon REST APIs, see [Amazon APIs](#).

To access Network Firewall using the REST API endpoint: `https://network-firewall.<region>.amazonaws.com`

- Alternatively, you can use one of the Amazon SDKs to access an API that's tailored to the programming language or platform that you're using. For more information, see [Amazon 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 Amazon Direct Connect. Network Firewall uses rules that are compatible with Suricata, a free, open source network analysis and threat detection engine. Amazon Network Firewall supports Suricata version 6.0.9. 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 Amazon 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 May 31, 2024.



# Actions

The following actions are supported:

- [AssociateFirewallPolicy](#)
- [AssociateSubnets](#)
- [CreateFirewall](#)
- [CreateFirewallPolicy](#)
- [CreateRuleGroup](#)
- [CreateTLSInspectionConfiguration](#)
- [DeleteFirewall](#)
- [DeleteFirewallPolicy](#)
- [DeleteResourcePolicy](#)
- [DeleteRuleGroup](#)
- [DeleteTLSInspectionConfiguration](#)
- [DescribeFirewall](#)
- [DescribeFirewallPolicy](#)
- [DescribeLoggingConfiguration](#)
- [DescribeResourcePolicy](#)
- [DescribeRuleGroup](#)
- [DescribeRuleGroupMetadata](#)
- [DescribeTLSInspectionConfiguration](#)
- [DisassociateSubnets](#)
- [ListFirewallPolicies](#)
- [ListFirewalls](#)
- [ListRuleGroups](#)
- [ListTagsForResource](#)
- [ListTLSInspectionConfigurations](#)
- [PutResourcePolicy](#)
- [TagResource](#)
- [UntagResource](#)

- [UpdateFirewallDeleteProtection](#)
- [UpdateFirewallDescription](#)
- [UpdateFirewallEncryptionConfiguration](#)
- [UpdateFirewallPolicy](#)
- [UpdateFirewallPolicyChangeProtection](#)
- [UpdateLoggingConfiguration](#)
- [UpdateRuleGroup](#)
- [UpdateSubnetChangeProtection](#)
- [UpdateTLSInspectionConfiguration](#)

# AssociateFirewallPolicy

Associates a [FirewallPolicy](#) to a [Firewall](#).

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](#).

The request accepts the following data in JSON format.

### [FirewallArn](#)

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](#)

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

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

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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### FirewallPolicyArn

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

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](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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 Amazon 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": [
    {
      "IPAddressType": "string",
      "SubnetId": "string"
    }
  ],
  "UpdateToken": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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

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

Type: Array of [SubnetMapping](#) objects

Required: Yes

### UpdateToken

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": [
    {
      "IPAddressType": "string",
      "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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

## SubnetMappings

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

Type: Array of [SubnetMapping](#) objects

## UpdateToken

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](#).

### **InsufficientCapacityException**

Amazon 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)

- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# CreateFirewall

Creates an Amazon Network Firewall [Firewall](#) and accompanying [FirewallStatus](#) for a VPC.

The firewall defines the configuration settings for an Amazon 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 Amazon 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](#), [AssociateSubnets](#), and [UpdateFirewallDeleteProtection](#).

To manage a firewall's tags, use the standard Amazon resource tagging operations, [ListTagsForResource](#), [TagResource](#), and [UntagResource](#).

To retrieve information about firewalls, use [ListFirewalls](#) and [DescribeFirewall](#).

## Request Syntax

```
{
  "DeleteProtection": boolean,
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [
    {
      "IPAddressType": "string",
      "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](#).

The request accepts the following data in JSON format.

### 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

### EncryptionConfiguration

A complex type that contains settings for encryption of your firewall resources.

Type: [EncryptionConfiguration](#) object

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: Yes

### FirewallPolicyArn

The Amazon Resource Name (ARN) of the [FirewallPolicy](#) 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

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 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](#) objects

Required: Yes

## Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) objects

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

Required: No

## VpcId

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",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallArn": "string",
    "FirewallId": "string",
    "FirewallName": "string",
    "FirewallPolicyArn": "string",
    "FirewallPolicyChangeProtection": boolean,
    "SubnetChangeProtection": boolean,
    "SubnetMappings": [
      {
        "IPAddressType": "string",
        "SubnetId": "string"
      }
    ]
  }
}
```

```

    ],
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "VpcId": "string"
  },
  "FirewallStatus": {
    "CapacityUsageSummary": {
      "CIDRs": {
        "AvailableCIDRCount": number,
        "IPSetReferences": {
          "string" : {
            "ResolvedCIDRCount": number
          }
        },
        "UtilizedCIDRCount": number
      }
    },
    "ConfigurationSyncStateSummary": "string",
    "Status": "string",
    "SyncStates": {
      "string" : {
        "Attachment": {
          "EndpointId": "string",
          "Status": "string",
          "StatusMessage": "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](#)

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](#) object

### [FirewallStatus](#)

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

Type: [FirewallStatus](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **InsufficientCapacityException**

Amazon 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# CreateFirewallPolicy

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

An Amazon 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,
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "FirewallPolicy": {
    "PolicyVariables": {
      "RuleVariables": {
        "string" : {
          "Definition": [ "string" ]
        }
      }
    }
  },
  "StatefulDefaultActions": [ "string" ],
  "StatefulEngineOptions": {
    "RuleOrder": "string",
    "StreamExceptionPolicy": "string"
  },
  "StatefulRuleGroupReferences": [
    {
      "Override": {
        "Action": "string"
      },
      "Priority": number,
      "ResourceArn": "string"
    }
  ],
  "StatelessCustomActions": [
    {
      "ActionDefinition": {
        "PublishMetricAction": {
```

```

        "Dimensions": [
            {
                "Value": "string"
            }
        ]
    },
    "ActionName": "string"
}
],
"StatelessDefaultActions": [ "string" ],
"StatelessFragmentDefaultActions": [ "string" ],
"StatelessRuleGroupReferences": [
    {
        "Priority": number,
        "ResourceArn": "string"
    }
],
"TLSInspectionConfigurationArn": "string"
},
"FirewallPolicyName": "string",
"Tags": [
    {
        "Key": "string",
        "Value": "string"
    }
]
}

```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^\.*$`

Required: No

### DryRun

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

### EncryptionConfiguration

A complex type that contains settings for encryption of your firewall policy resources.

Type: [EncryptionConfiguration](#) object

Required: No

### FirewallPolicy

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

Type: [FirewallPolicy](#) object

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

## Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) objects

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

Required: No

## Response Syntax

```
{
  "FirewallPolicyResponse": {
    "ConsumedStatefulRuleCapacity": number,
    "ConsumedStatelessRuleCapacity": number,
    "Description": "string",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallPolicyArn": "string",
    "FirewallPolicyId": "string",
    "FirewallPolicyName": "string",
    "FirewallPolicyStatus": "string",
    "LastModifiedTime": number,
    "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

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

Type: [FirewallPolicyResponse](#) object

## UpdateToken

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](#).

### **InsufficientCapacityException**

Amazon 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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

```
{
  "AnalyzeRuleGroup": boolean,
  "Capacity": number,
  "Description": "string",
  "DryRun": boolean,
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "RuleGroup": {
    "ReferenceSets": {
      "IPSetReferences": {
        "string" : {
          "ReferenceArn": "string"
        }
      }
    }
  },
  "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",
"SourceMetadata": {
    "SourceArn": "string",
    "SourceUpdateToken": "string"
},
"Tags": [

```

```
{
  "Key": "string",
  "Value": "string"
},
"Type": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [AnalyzeRuleGroup](#)

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis and then creates the rule group for you. To run the stateless rule group analyzer without creating the rule group, set `DryRun` to TRUE.

Type: Boolean

Required: No

### [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](#) 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

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

### DryRun

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

### EncryptionConfiguration

A complex type that contains settings for encryption of your rule group resources.

Type: [EncryptionConfiguration](#) object

Required: No

### RuleGroup

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](#) object

Required: No

### 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

## Rules

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](#) object that Network Firewall has populated from your string.

Type: String

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

Required: No

## SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to keep track of updates made to the originating rule group.

Type: [SourceMetadata](#) object

Required: No

## Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) 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: Yes

## Response Syntax

```
{
  "RuleGroupResponse": {
    "AnalysisResults": [
      {
        "AnalysisDetail": "string",
        "IdentifiedRuleIds": [ "string" ],
        "IdentifiedType": "string"
      }
    ],
    "Capacity": number,
    "ConsumedCapacity": number,
    "Description": "string",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "LastModifiedTime": number,
    "NumberOfAssociations": number,
    "RuleGroupArn": "string",
    "RuleGroupId": "string",
    "RuleGroupName": "string",
    "RuleGroupStatus": "string",
    "SnsTopic": "string",
    "SourceMetadata": {
      "SourceArn": "string",
      "SourceUpdateToken": "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

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

Type: [RuleGroupResponse](#) object

### UpdateToken

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](#).

### **InsufficientCapacityException**

Amazon 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)

- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# CreateTLSInspectionConfiguration

Creates an Amazon Network Firewall TLS inspection configuration. Network Firewall uses TLS inspection configurations to decrypt your firewall's inbound and outbound SSL/TLS traffic. After decryption, Network Firewall inspects the traffic according to your firewall policy's stateful rules, and then re-encrypts it before sending it to its destination. You can enable inspection of your firewall's inbound traffic, outbound traffic, or both. To use TLS inspection with your firewall, you must first import or provision certificates using ACM, create a TLS inspection configuration, add that configuration to a new firewall policy, and then associate that policy with your firewall.

To update the settings for a TLS inspection configuration, use [UpdateTLSInspectionConfiguration](#).

To manage a TLS inspection configuration's tags, use the standard Amazon resource tagging operations, [ListTagsForResource](#), [TagResource](#), and [UntagResource](#).

To retrieve information about TLS inspection configurations, use [ListTLSInspectionConfigurations](#) and [DescribeTLSInspectionConfiguration](#).

For more information about TLS inspection configurations, see [Inspecting SSL/TLS traffic with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

## Request Syntax

```
{
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "TLSInspectionConfiguration": {
    "ServerCertificateConfigurations": [
      {
        "CertificateAuthorityArn": "string",
        "CheckCertificateRevocationStatus": {
          "RevokedStatusAction": "string",
```

```
    "UnknownStatusAction": "string"
  },
  "Scopes": [
    {
      "DestinationPorts": [
        {
          "FromPort": number,
          "ToPort": number
        }
      ],
      "Destinations": [
        {
          "AddressDefinition": "string"
        }
      ],
      "Protocols": [ number ],
      "SourcePorts": [
        {
          "FromPort": number,
          "ToPort": number
        }
      ],
      "Sources": [
        {
          "AddressDefinition": "string"
        }
      ]
    }
  ],
  "ServerCertificates": [
    {
      "ResourceArn": "string"
    }
  ]
},
"TLSInspectionConfigurationName": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).



The request accepts the following data in JSON format.

### Description

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

### EncryptionConfiguration

A complex type that contains optional Amazon Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an Amazon owned key that Amazon owns and manages for you. You can use either the Amazon owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see [Encryption at rest with Amazon Key Management Service](#) in the *Network Firewall Developer Guide*.

Type: [EncryptionConfiguration](#) object

Required: No

### Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) objects

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

Required: No

### TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with [TLSInspectionConfigurationResponse](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Amazon Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see [Inspecting SSL/TLS traffic with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

Type: [TLSInspectionConfiguration](#) object

Required: Yes

### [TLSInspectionConfigurationName](#)

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

Type: String

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

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

Required: Yes

## Response Syntax

```
{
  "TLSInspectionConfigurationResponse": {
    "CertificateAuthority": {
      "CertificateArn": "string",
      "CertificateSerial": "string",
      "Status": "string",
      "StatusMessage": "string"
    },
    "Certificates": [
      {
        "CertificateArn": "string",
        "CertificateSerial": "string",
        "Status": "string",
        "StatusMessage": "string"
      }
    ]
  },
}
```

```
"Description": "string",
"EncryptionConfiguration": {
  "KeyId": "string",
  "Type": "string"
},
"LastModifiedTime": number,
"NumberOfAssociations": number,
"Tags": [
  {
    "Key": "string",
    "Value": "string"
  }
],
"TLSInspectionConfigurationArn": "string",
"TLSInspectionConfigurationId": "string",
"TLSInspectionConfigurationName": "string",
"TLSInspectionConfigurationStatus": "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.

### TLSTLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the [TLSTLSInspectionConfiguration](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSTLSInspectionConfiguration](#).

Type: [TLSTLSInspectionConfigurationResponse](#) object

### UpdateToken

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

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration

hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration 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](#).

### **InsufficientCapacityException**

Amazon 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DeleteFirewall

Deletes the specified [Firewall](#) and its [FirewallStatus](#). 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](#). 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](#), then delete the firewall by calling [DeleteFirewall](#).

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [FirewallArn](#)

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

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",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallArn": "string",
    "FirewallId": "string",
    "FirewallName": "string",
    "FirewallPolicyArn": "string",
    "FirewallPolicyChangeProtection": boolean,
    "SubnetChangeProtection": boolean,
    "SubnetMappings": [
      {
        "IPAddressType": "string",
        "SubnetId": "string"
      }
    ],
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ]
  },
}
```

```

    "VpcId": "string"
  },
  "FirewallStatus": {
    "CapacityUsageSummary": {
      "CIDRs": {
        "AvailableCIDRCount": number,
        "IPSetReferences": {
          "string" : {
            "ResolvedCIDRCount": number
          }
        },
        "UtilizedCIDRCount": number
      }
    },
    "ConfigurationSyncStateSummary": "string",
    "Status": "string",
    "SyncStates": {
      "string" : {
        "Attachment": {
          "EndpointId": "string",
          "Status": "string",
          "StatusMessage": "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](#)

The firewall defines the configuration settings for an Amazon 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 Amazon resource.

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

Type: [Firewall](#) object

## [FirewallStatus](#)

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

Type: [FirewallStatus](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DeleteFirewallPolicy

Deletes the specified [FirewallPolicy](#).

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [FirewallPolicyArn](#)

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](#)

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",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallPolicyArn": "string",
    "FirewallPolicyId": "string",
    "FirewallPolicyName": "string",
    "FirewallPolicyStatus": "string",
    "LastModifiedTime": number,
    "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](#)

The object containing the definition of the [FirewallPolicyResponse](#) that you asked to delete.

Type: [FirewallPolicyResponse](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DeleteResourcePolicy

Deletes a resource policy that you created in a [PutResourcePolicy](#) request.

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [ResourceArn](#)

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)



- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DeleteRuleGroup

Deletes the specified [RuleGroup](#).

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [RuleGroupArn](#)

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](#)

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

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": {
    "AnalysisResults": [
      {
        "AnalysisDetail": "string",
        "IdentifiedRuleIds": [ "string" ],
        "IdentifiedType": "string"
      }
    ],
    "Capacity": number,
    "ConsumedCapacity": number,
    "Description": "string",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "LastModifiedTime": number,
    "NumberOfAssociations": number,
    "RuleGroupArn": "string",
    "RuleGroupId": "string",
    "RuleGroupName": "string",
    "RuleGroupStatus": "string",
```

```
    "SnsTopic": "string",
    "SourceMetadata": {
      "SourceArn": "string",
      "SourceUpdateToken": "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

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

Type: [RuleGroupResponse](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)

- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DeleteTLSInspectionConfiguration

Deletes the specified [TLSInspectionConfiguration](#).

## Request Syntax

```
{
  "TLSInspectionConfigurationArn": "string",
  "TLSInspectionConfigurationName": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [TLSInspectionConfigurationArn](#)

The Amazon Resource Name (ARN) of the TLS inspection configuration.

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

### [TLSInspectionConfigurationName](#)

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration 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

```
{
  "TLSInspectionConfigurationResponse": {
    "CertificateAuthority": {
      "CertificateArn": "string",
      "CertificateSerial": "string",
      "Status": "string",
      "StatusMessage": "string"
    },
    "Certificates": [
      {
        "CertificateArn": "string",
        "CertificateSerial": "string",
        "Status": "string",
        "StatusMessage": "string"
      }
    ],
    "Description": "string",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "LastModifiedTime": number,
    "NumberOfAssociations": number,
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "TLSInspectionConfigurationArn": "string",
    "TLSInspectionConfigurationId": "string",
    "TLSInspectionConfigurationName": "string",
    "TLSInspectionConfigurationStatus": "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.



## [TLSInspectionConfigurationResponse](#)

The high-level properties of a TLS inspection configuration. This, along with the [TLSInspectionConfiguration](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Type: [TLSInspectionConfigurationResponse](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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

## See Also

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

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallArn": "string",
    "FirewallId": "string",
    "FirewallName": "string",
    "FirewallPolicyArn": "string",
    "FirewallPolicyChangeProtection": boolean,
    "SubnetChangeProtection": boolean,
    "SubnetMappings": [
      {
        "IPAddressType": "string",
        "SubnetId": "string"
      }
    ],
    "Tags": [
      {
        "Key": "string",
        "Value": "string"
      }
    ],
    "VpcId": "string"
  },
  "FirewallStatus": {
    "CapacityUsageSummary": {
      "CIDRs": {
        "AvailableCIDRCount": number,
        "IPSetReferences": {
          "string": {
            "ResolvedCIDRCount": number
          }
        }
      }
    }
  },
}
```

```

        "UtilizedCIDRCount": number
    }
},
"ConfigurationSyncStateSummary": "string",
"Status": "string",
"SyncStates": {
    "string" : {
        "Attachment": {
            "EndpointId": "string",
            "Status": "string",
            "StatusMessage": "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

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](#) object

### FirewallStatus

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

Type: [FirewallStatus](#) object

## UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### [FirewallPolicyArn](#)

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](#)

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": {
    "PolicyVariables": {
      "RuleVariables": {
        "string": {
          "Definition": [ "string" ]
        }
      }
    },
    "StatefulDefaultActions": [ "string" ],
    "StatefulEngineOptions": {
      "RuleOrder": "string",
      "StreamExceptionPolicy": "string"
    },
    "StatefulRuleGroupReferences": [
      {
        "Override": {
          "Action": "string"
        },
        "Priority": number,
        "ResourceArn": "string"
      }
    ],
    "StatelessCustomActions": [
      {
        "ActionDefinition": {
          "PublishMetricAction": {
            "Dimensions": [
              {
                "Value": "string"
              }
            ]
          }
        },
        "ActionName": "string"
      }
    ]
  },
  ],
```

```

    "StatelessDefaultActions": [ "string" ],
    "StatelessFragmentDefaultActions": [ "string" ],
    "StatelessRuleGroupReferences": [
      {
        "Priority": number,
        "ResourceArn": "string"
      }
    ],
    "TLSInspectionConfigurationArn": "string"
  },
  "FirewallPolicyResponse": {
    "ConsumedStatefulRuleCapacity": number,
    "ConsumedStatelessRuleCapacity": number,
    "Description": "string",
    "EncryptionConfiguration": {
      "KeyId": "string",
      "Type": "string"
    },
    "FirewallPolicyArn": "string",
    "FirewallPolicyId": "string",
    "FirewallPolicyName": "string",
    "FirewallPolicyStatus": "string",
    "LastModifiedTime": number,
    "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

The policy for the specified firewall policy.

Type: [FirewallPolicy](#) object

## [FirewallPolicyResponse](#)

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

Type: [FirewallPolicyResponse](#) object

## [UpdateToken](#)

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](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### LoggingConfiguration

Defines how Amazon Network Firewall performs logging for a [Firewall](#).

Type: [LoggingConfiguration](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

## 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)

- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)



# DescribeResourcePolicy

Retrieves a resource policy that you created in a [PutResourcePolicy](#) request.

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [ResourceArn](#)

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

The IAM 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](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DescribeRuleGroup

Returns the data objects for the specified rule group.

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [AnalyzeRuleGroup](#)

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis.

Type: Boolean

Required: No

### [RuleGroupArn](#)

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

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

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": {
    "ReferenceSets": {
      "IPSetReferences": {
        "string": {
          "ReferenceArn": "string"
        }
      }
    },
    "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": {
    "AnalysisResults": [
        {
            "AnalysisDetail": "string",
            "IdentifiedRuleIds": [ "string" ],
            "IdentifiedType": "string"
        }
    ],
    "Capacity": number,
    "ConsumedCapacity": number,
    "Description": "string",
    "EncryptionConfiguration": {
        "KeyId": "string",
        "Type": "string"
    },
    "LastModifiedTime": number,
    "NumberOfAssociations": number,
    "RuleGroupArn": "string",
    "RuleGroupId": "string",
    "RuleGroupName": "string",
    "RuleGroupStatus": "string",
    "SnsTopic": "string",
    "SourceMetadata": {
        "SourceArn": "string",
        "SourceUpdateToken": "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](#)

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

Amazon 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](#) object

### [RuleGroupResponse](#)

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

Type: [RuleGroupResponse](#) object

### [UpdateToken](#)

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# DescribeRuleGroupMetadata

High-level information about a rule group, returned by operations like `create` and `describe`. You can use the information provided in the metadata to retrieve and manage a rule group. You can retrieve all objects for a rule group by calling [DescribeRuleGroup](#).

## Request Syntax

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

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [RuleGroupArn](#)

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 256.

Pattern: `^arn:aws.*`

Required: No

### [RuleGroupName](#)

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

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

```
{
  "Capacity": number,
  "Description": "string",
  "LastModifiedTime": number,
  "RuleGroupArn": "string",
  "RuleGroupName": "string",
  "StatefulRuleOptions": {
    "RuleOrder": "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.

### 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](#) with `DryRun` set to `TRUE`.

Type: Integer

### Description

Returns the metadata objects for the specified rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

### LastModifiedTime

The last time that the rule group was changed.

Type: Timestamp

### RuleGroupArn

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 256.

Pattern: `^arn:aws.*`

### RuleGroupName

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-]+$`

## StatefulRuleOptions

Additional options governing how Network Firewall handles the rule group. You can only use these for stateful rule groups.

Type: [StatefulRuleOptions](#) object

## 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.

### Note

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

Type: String

Valid Values: STATELESS | STATEFUL

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)



# DescribeTLSInspectionConfiguration

Returns the data objects for the specified TLS inspection configuration.

## Request Syntax

```
{  
  "TLSInspectionConfigurationArn": "string",  
  "TLSInspectionConfigurationName": "string"  
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

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

### TLSInspectionConfigurationName

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration 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

```
{
  "TLSInspectionConfiguration": {
    "ServerCertificateConfigurations": [
      {
        "CertificateAuthorityArn": "string",
        "CheckCertificateRevocationStatus": {
          "RevokedStatusAction": "string",
          "UnknownStatusAction": "string"
        },
        "Scopes": [
          {
            "DestinationPorts": [
              {
                "FromPort": number,
                "ToPort": number
              }
            ],
            "Destinations": [
              {
                "AddressDefinition": "string"
              }
            ],
            "Protocols": [ number ],
            "SourcePorts": [
              {
                "FromPort": number,
                "ToPort": number
              }
            ],
            "Sources": [
              {
                "AddressDefinition": "string"
              }
            ]
          }
        ],
        "ServerCertificates": [
          {
            "ResourceArn": "string"
          }
        ]
      }
    ]
  }
}
```

```

    }
  ]
},
"TLSInspectionConfigurationResponse": {
  "CertificateAuthority": {
    "CertificateArn": "string",
    "CertificateSerial": "string",
    "Status": "string",
    "StatusMessage": "string"
  },
  "Certificates": [
    {
      "CertificateArn": "string",
      "CertificateSerial": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ],
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "LastModifiedTime": number,
  "NumberOfAssociations": number,
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "TLSInspectionConfigurationArn": "string",
  "TLSInspectionConfigurationId": "string",
  "TLSInspectionConfigurationName": "string",
  "TLSInspectionConfigurationStatus": "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.

## [TLSInspectionConfiguration](#)

The object that defines a TLS inspection configuration. This, along with [TLSInspectionConfigurationResponse](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Amazon Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see [Inspecting SSL/TLS traffic with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

Type: [TLSInspectionConfiguration](#) object

## [TLSInspectionConfigurationResponse](#)

The high-level properties of a TLS inspection configuration. This, along with the [TLSInspectionConfiguration](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Type: [TLSInspectionConfigurationResponse](#) object

## [UpdateToken](#)

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

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration 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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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

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

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": [  
  {  
    "IPAddressType": "string",  
    "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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### SubnetMappings

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

Type: Array of [SubnetMapping](#) objects

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### [MaxResults](#)

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](#)

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 4096.

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](#)

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](#) objects

### [NextToken](#)

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 4096.

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)

- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### [MaxResults](#)

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](#)

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 4096.

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

Required: No

## [VpcIds](#)

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](#)

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](#) objects

### [NextToken](#)

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 4096.

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

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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

```
{
  "ManagedType": "string",
  "MaxResults": number,
  "NextToken": "string",
  "Scope": "string",
  "Type": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### ManagedType

Indicates the general category of the Amazon managed rule group.

Type: String

Valid Values: AWS\_MANAGED\_THREAT\_SIGNATURES | AWS\_MANAGED\_DOMAIN\_LISTS

Required: No

### MaxResults

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

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 4096.

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

Required: No

## Scope

The scope of the request. The default setting of `ACCOUNT` or a setting of `NULL` returns all of the rule groups in your account. A setting of `MANAGED` returns all available managed rule groups.

Type: String

Valid Values: `MANAGED` | `ACCOUNT`

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

## 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

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 4096.

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

### RuleGroups

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](#) objects

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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 Amazon resource, up to 50 tags for a resource.

You can tag the Amazon resources that you manage through Amazon 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](#).

The request accepts the following data in JSON format.

### MaxResults

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

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 4096.

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

Required: No

### ResourceArn

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

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 4096.

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

## Tags

The tags that are associated with the resource.

Type: Array of [Tag](#) 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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# ListTLSInspectionConfigurations

Retrieves the metadata for the TLS inspection configurations that you have defined. Depending on your setting for max results and the number of TLS inspection configurations, 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](#).

The request accepts the following data in JSON format.

### MaxResults

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

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 4096.

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

Required: No

## Response Syntax

```
{
  "NextToken": "string",
  "TLSInspectionConfigurations": [
    {
      "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

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 4096.

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

### TLSInspectionConfigurations

The TLS inspection configuration metadata objects that you've defined. Depending on your setting for max results and the number of TLS inspection configurations, this might not be the full list.

Type: Array of [TLSInspectionConfigurationMetadata](#) objects

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)

- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# PutResourcePolicy

Creates or updates an IAM 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 Amazon 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 [Amazon 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](#).

The request accepts the following data in JSON format.

### Policy

The IAM 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: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

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](#).

## 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)

- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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 Amazon resource, up to 50 tags for a resource.

You can tag the Amazon resources that you manage through Amazon 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](#).

The request accepts the following data in JSON format.

### ResourceArn

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

Type: Array of [Tag](#) 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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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 Amazon resource, up to 50 tags for a resource.

You can manage tags for the Amazon resources that you manage through Amazon 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](#).

The request accepts the following data in JSON format.

### [ResourceArn](#)

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](#)

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### 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: Yes

### FirewallArn

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

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

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

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

### FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### Description

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

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

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

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

A description of the firewall.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

### FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# UpdateFirewallEncryptionConfiguration

A complex type that contains settings for encryption of your firewall resources.

## Request Syntax

```
{
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "FirewallArn": "string",
  "FirewallName": "string",
  "UpdateToken": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### EncryptionConfiguration

A complex type that contains optional Amazon Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an Amazon owned key that Amazon owns and manages for you. You can use either the Amazon owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see [Encryption at rest with Amazon Key Management Service](#) in the *Network Firewall Developer Guide*.

Type: [EncryptionConfiguration](#) object

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

### 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

### UpdateToken

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

```
{
```

```
"EncryptionConfiguration": {
  "KeyId": "string",
  "Type": "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.

### EncryptionConfiguration

A complex type that contains optional Amazon Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an Amazon owned key that Amazon owns and manages for you. You can use either the Amazon owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see [Encryption at rest with Amazon Key Management Service](#) in the *Network Firewall Developer Guide*.

Type: [EncryptionConfiguration](#) object

### FirewallArn

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

## UpdateToken

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](#).

### **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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)



- [Amazon SDK for Ruby V3](#)

# UpdateFirewallPolicy

Updates the properties of the specified firewall policy.

## Request Syntax

```
{
  "Description": "string",
  "DryRun": boolean,
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "FirewallPolicy": {
    "PolicyVariables": {
      "RuleVariables": {
        "string" : {
          "Definition": [ "string" ]
        }
      }
    }
  },
  "StatefulDefaultActions": [ "string" ],
  "StatefulEngineOptions": {
    "RuleOrder": "string",
    "StreamExceptionPolicy": "string"
  },
  "StatefulRuleGroupReferences": [
    {
      "Override": {
        "Action": "string"
      },
      "Priority": number,
      "ResourceArn": "string"
    }
  ],
  "StatelessCustomActions": [
    {
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [
            {
              "Value": "string"
            }
          ]
        }
      }
    }
  ]
}
```

```
        ]
      }
    },
    "ActionName": "string"
  }
],
"StatelessDefaultActions": [ "string" ],
"StatelessFragmentDefaultActions": [ "string" ],
"StatelessRuleGroupReferences": [
  {
    "Priority": number,
    "ResourceArn": "string"
  }
],
"TLSInspectionConfigurationArn": "string"
},
"FirewallPolicyArn": "string",
"FirewallPolicyName": "string",
"UpdateToken": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### Description

A description of the firewall policy.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

### DryRun

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

### EncryptionConfiguration

A complex type that contains settings for encryption of your firewall policy resources.

Type: [EncryptionConfiguration](#) object

Required: No

### FirewallPolicy

The updated firewall policy to use for the firewall. You can't add or remove a [TLSInspectionConfiguration](#) after you create a firewall policy. However, you can replace an existing TLS inspection configuration with another [TLSInspectionConfiguration](#).

Type: [FirewallPolicy](#) object

Required: Yes

### FirewallPolicyArn

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

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

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",
    "EncryptionConfiguration": {
```

```
    "KeyId": "string",
    "Type": "string"
  },
  "FirewallPolicyArn": "string",
  "FirewallPolicyId": "string",
  "FirewallPolicyName": "string",
  "FirewallPolicyStatus": "string",
  "LastModifiedTime": number,
  "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

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

Type: [FirewallPolicyResponse](#) object

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)



# UpdateFirewallPolicyChangeProtection

Modifies the flag, `ChangeProtection`, which indicates whether it is possible to change the firewall. If the flag is set to `TRUE`, the firewall is protected from changes. This setting helps protect against accidentally changing a firewall that's in use.

## 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](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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

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

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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### 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

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# UpdateLoggingConfiguration

Sets the logging configuration for the specified firewall.

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

The request accepts the following data in JSON format.

### [FirewallArn](#)

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](#)

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](#)

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

Type: [LoggingConfiguration](#) 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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`



## LoggingConfiguration

Defines how Amazon Network Firewall performs logging for a [Firewall](#).

Type: [LoggingConfiguration](#) object

## Errors

For information about the errors that are common to all actions, see [Common Errors](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#) to retrieve the current [RuleGroup](#) object, update the object as needed, and then provide the updated object to this call.

## Request Syntax

```
{
  "AnalyzeRuleGroup": boolean,
  "Description": "string",
  "DryRun": boolean,
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "RuleGroup": {
    "ReferenceSets": {
      "IPSetReferences": {
        "string": {
          "ReferenceArn": "string"
        }
      }
    }
  },
  "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",
"SourceMetadata": {
    "SourceArn": "string",

```

```
    "SourceUpdateToken": "string"  
  },  
  "Type": "string",  
  "UpdateToken": "string"  
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### [AnalyzeRuleGroup](#)

Indicates whether you want Network Firewall to analyze the stateless rules in the rule group for rule behavior such as asymmetric routing. If set to TRUE, Network Firewall runs the analysis and then updates the rule group for you. To run the stateless rule group analyzer without updating the rule group, set `DryRun` to TRUE.

Type: Boolean

Required: No

### [Description](#)

A description of the rule group.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^\.*$`

Required: No

### [DryRun](#)

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

### EncryptionConfiguration

A complex type that contains settings for encryption of your rule group resources.

Type: [EncryptionConfiguration](#) object

Required: No

### RuleGroup

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](#) object

Required: No

### RuleGroupArn

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

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

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](#) object that Network Firewall has populated from your string.

Type: String

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

Required: No

## SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to keep track of updates made to the originating rule group.

Type: [SourceMetadata](#) object



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.

### Note

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

Type: String

Valid Values: STATELESS | STATEFUL

Required: No

## UpdateToken

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": {
  "AnalysisResults": [
    {
      "AnalysisDetail": "string",
      "IdentifiedRuleIds": [ "string" ],
      "IdentifiedType": "string"
    }
  ],
  "Capacity": number,
  "ConsumedCapacity": number,
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "LastModifiedTime": number,
  "NumberOfAssociations": number,
  "RuleGroupArn": "string",
  "RuleGroupId": "string",
  "RuleGroupName": "string",
  "RuleGroupStatus": "string",
  "SnsTopic": "string",
  "SourceMetadata": {
    "SourceArn": "string",
    "SourceUpdateToken": "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

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

Type: [RuleGroupResponse](#) object

## UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon 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](#).

The request accepts the following data in JSON format.

### FirewallArn

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

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

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

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

The Amazon Resource Name (ARN) of the firewall.

Type: String

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

Pattern: `^arn:aws.*`

### 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-]+$`

### 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

### UpdateToken

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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)

# UpdateTLSInspectionConfiguration

Updates the TLS inspection configuration settings for the specified TLS inspection configuration. You use a TLS inspection configuration by referencing it in one or more firewall policies. When you modify a TLS inspection configuration, you modify all firewall policies that use the TLS inspection configuration.

To update a TLS inspection configuration, first call [DescribeTLSInspectionConfiguration](#) to retrieve the current [TLSInspectionConfiguration](#) object, update the object as needed, and then provide the updated object to this call.

## Request Syntax

```
{
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "TLSInspectionConfiguration": {
    "ServerCertificateConfigurations": [
      {
        "CertificateAuthorityArn": "string",
        "CheckCertificateRevocationStatus": {
          "RevokedStatusAction": "string",
          "UnknownStatusAction": "string"
        },
        "Scopes": [
          {
            "DestinationPorts": [
              {
                "FromPort": number,
                "ToPort": number
              }
            ],
            "Destinations": [
              {
                "AddressDefinition": "string"
              }
            ],
            "Protocols": [ number ],
            "SourcePorts": [
```

```
    {
      "FromPort": number,
      "ToPort": number
    }
  ],
  "Sources": [
    {
      "AddressDefinition": "string"
    }
  ]
},
"ServerCertificates": [
  {
    "ResourceArn": "string"
  }
]
}
]
},
"TLSInspectionConfigurationArn": "string",
"TLSInspectionConfigurationName": "string",
"UpdateToken": "string"
}
```

## Request Parameters

For information about the parameters that are common to all actions, see [Common Parameters](#).

The request accepts the following data in JSON format.

### Description

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern:  $\wedge . * \$$

Required: No

## EncryptionConfiguration

A complex type that contains the Amazon KMS encryption configuration settings for your TLS inspection configuration.

Type: [EncryptionConfiguration](#) object

Required: No

## TLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with [TLSInspectionConfigurationResponse](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Amazon Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see [Inspecting SSL/TLS traffic with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

Type: [TLSInspectionConfiguration](#) object

Required: Yes

## TLSInspectionConfigurationArn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## TLSInspectionConfigurationName

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

Type: String

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

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

Required: No

## UpdateToken

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

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration 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

```
{
  "TLSInspectionConfigurationResponse": {
    "CertificateAuthority": {
      "CertificateArn": "string",
      "CertificateSerial": "string",
```

```

    "Status": "string",
    "StatusMessage": "string"
  },
  "Certificates": [
    {
      "CertificateArn": "string",
      "CertificateSerial": "string",
      "Status": "string",
      "StatusMessage": "string"
    }
  ],
  "Description": "string",
  "EncryptionConfiguration": {
    "KeyId": "string",
    "Type": "string"
  },
  "LastModifiedTime": number,
  "NumberOfAssociations": number,
  "Tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "TLSInspectionConfigurationArn": "string",
  "TLSInspectionConfigurationId": "string",
  "TLSInspectionConfigurationName": "string",
  "TLSInspectionConfigurationStatus": "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.

### [TLSInspectionConfigurationResponse](#)

The high-level properties of a TLS inspection configuration. This, along with the [TLSInspectionConfiguration](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#).

Type: [TLSTransactionConfigurationResponse](#) object

## UpdateToken

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

To make changes to the TLS inspection configuration, you provide the token in your request. Network Firewall uses the token to ensure that the TLS inspection configuration hasn't changed since you last retrieved it. If it has changed, the operation fails with an `InvalidTokenException`. If this happens, retrieve the TLS inspection configuration 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](#).

### 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 Amazon SDKs, see the following:

- [Amazon Command Line Interface](#)
- [Amazon SDK for .NET](#)
- [Amazon SDK for C++](#)
- [Amazon SDK for Go v2](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for JavaScript V3](#)
- [Amazon SDK for PHP V3](#)
- [Amazon SDK for Python](#)
- [Amazon SDK for Ruby V3](#)



# Data Types

The Amazon 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:

- [ActionDefinition](#)
- [Address](#)
- [AnalysisResult](#)
- [Attachment](#)
- [CapacityUsageSummary](#)
- [CheckCertificateRevocationStatusActions](#)
- [CIDRSummary](#)
- [CustomAction](#)
- [Dimension](#)
- [EncryptionConfiguration](#)
- [Firewall](#)
- [FirewallMetadata](#)
- [FirewallPolicy](#)
- [FirewallPolicyMetadata](#)
- [FirewallPolicyResponse](#)
- [FirewallStatus](#)
- [Header](#)
- [IPSet](#)
- [IPSetMetadata](#)
- [IPSetReference](#)

- [LogDestinationConfig](#)
- [LoggingConfiguration](#)
- [MatchAttributes](#)
- [PerObjectStatus](#)
- [PolicyVariables](#)
- [PortRange](#)
- [PortSet](#)
- [PublishMetricAction](#)
- [ReferenceSets](#)
- [RuleDefinition](#)
- [RuleGroup](#)
- [RuleGroupMetadata](#)
- [RuleGroupResponse](#)
- [RuleOption](#)
- [RulesSource](#)
- [RulesSourceList](#)
- [RuleVariables](#)
- [ServerCertificate](#)
- [ServerCertificateConfiguration](#)
- [ServerCertificateScope](#)
- [SourceMetadata](#)
- [StatefulEngineOptions](#)
- [StatefulRule](#)
- [StatefulRuleGroupOverride](#)
- [StatefulRuleGroupReference](#)
- [StatefulRuleOptions](#)
- [StatelessRule](#)
- [StatelessRuleGroupReference](#)
- [StatelessRulesAndCustomActions](#)
- [SubnetMapping](#)

- [SyncState](#)
- [Tag](#)
- [TCPFlagField](#)
- [TlsCertificateData](#)
- [TLSInspectionConfiguration](#)
- [TLSInspectionConfigurationMetadata](#)
- [TLSInspectionConfigurationResponse](#)

# ActionDefinition

A custom action to use in stateless rule actions settings. This is used in [CustomAction](#).

## 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](#) object

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# Address

A single IP address specification. This is used in the [MatchAttributes](#) 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 and IPv6.

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`.
- To configure Network Firewall to inspect for the IP address `1111:0000:0000:0000:0000:0000:0000:0111`, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from `1111:0000:0000:0000:0000:0000:0000:0000` to `1111:0000:0000:0000:ffff:ffff:ffff:ffff`, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# AnalysisResult

The analysis result for Network Firewall's stateless rule group analyzer. Every time you call [CreateRuleGroup](#), [UpdateRuleGroup](#), or [DescribeRuleGroup](#) on a stateless rule group, Network Firewall analyzes the stateless rule groups in your account and identifies the rules that might adversely effect your firewall's functionality. For example, if Network Firewall detects a rule that's routing traffic asymmetrically, which impacts the service's ability to properly process traffic, the service includes the rule in a list of analysis results.

## Contents

### AnalysisDetail

Provides analysis details for the identified rule.

Type: String

Required: No

### IdentifiedRuleIds

The priority number of the stateless rules identified in the analysis.

Type: Array of strings

Required: No

### IdentifiedType

The types of rule configurations that Network Firewall analyzes your rule groups for. Network Firewall analyzes stateless rule groups for the following types of rule configurations:

- STATELESS\_RULE\_FORWARDING\_ASYMMETRICALLY

**Cause:** One or more stateless rules with the action `pass` or `forward` are forwarding traffic asymmetrically. Specifically, the rule's set of source IP addresses or their associated port numbers, don't match the set of destination IP addresses or their associated port numbers.

**To mitigate:** Make sure that there's an existing return path. For example, if the rule allows traffic from source `10.1.0.0/24` to destination `20.1.0.0/24`, you should allow return traffic from source `20.1.0.0/24` to destination `10.1.0.0/24`.

- STATELESS\_RULE\_CONTAINS\_TCP\_FLAGS

**Cause:** At least one stateless rule with the action `pass` or `forward` contains TCP flags that are inconsistent in the forward and return directions.

**To mitigate:** Prevent asymmetric routing issues caused by TCP flags by following these actions:

- Remove unnecessary TCP flag inspections from the rules.
- If you need to inspect TCP flags, check that the rules correctly account for changes in TCP flags throughout the TCP connection cycle, for example SYN and ACK flags used in a 3-way TCP handshake.

Type: String

Valid Values: `STATELESS_RULE_FORWARDING_ASYMMETRICALLY` | `STATELESS_RULE_CONTAINS_TCP_FLAGS`

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# Attachment

The configuration and status for a single subnet that you've specified for use by the Amazon Network Firewall firewall. This is part of the [FirewallStatus](#).

## 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` or `DELETING`.

Type: String

Valid Values: `CREATING` | `DELETING` | `FAILED` | `ERROR` | `SCALING` | `READY`

Required: No

### StatusMessage

If Network Firewall fails to create or delete the firewall endpoint in the subnet, it populates this with the reason for the error or failure and how to resolve it. A `FAILED` status indicates a non-recoverable state, and a `ERROR` status indicates an issue that you can fix. Depending on the error, it can take as many as 15 minutes to populate this field. For more information about the causes for failure or errors and solutions available for this field, see [Troubleshooting firewall endpoint failures](#) in the *Network Firewall Developer Guide*.

Type: String

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# CapacityUsageSummary

The capacity usage summary of the resources used by the [ReferenceSets](#) in a firewall.

## Contents

### CIDRs

Describes the capacity usage of the CIDR blocks used by the IP set references in a firewall.

Type: [CIDRSummary](#) object

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# CheckCertificateRevocationStatusActions

Defines the actions to take on the SSL/TLS connection if the certificate presented by the server in the connection has a revoked or unknown status.

## Contents

### RevokedStatusAction

Configures how Network Firewall processes traffic when it determines that the certificate presented by the server in the SSL/TLS connection has a revoked status.

- **PASS** - Allow the connection to continue, and pass subsequent packets to the stateful engine for inspection.
- **DROP** - Network Firewall closes the connection and drops subsequent packets for that connection.
- **REJECT** - Network Firewall sends a TCP reject packet back to your client. The service closes the connection and drops subsequent packets for that connection. REJECT is available only for TCP traffic.

Type: String

Valid Values: PASS | DROP | REJECT

Required: No

### UnknownStatusAction

Configures how Network Firewall processes traffic when it determines that the certificate presented by the server in the SSL/TLS connection has an unknown status, or a status that cannot be determined for any other reason, including when the service is unable to connect to the OCSP and CRL endpoints for the certificate.

- **PASS** - Allow the connection to continue, and pass subsequent packets to the stateful engine for inspection.
- **DROP** - Network Firewall closes the connection and drops subsequent packets for that connection.
- **REJECT** - Network Firewall sends a TCP reject packet back to your client. The service closes the connection and drops subsequent packets for that connection. REJECT is available only for TCP traffic.

Type: String

Valid Values: PASS | DROP | REJECT

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# CIDRSummary

Summarizes the CIDR blocks used by the IP set references in a firewall. Network Firewall calculates the number of CIDRs by taking an aggregated count of all CIDRs used by the IP sets you are referencing.

## Contents

### AvailableCIDRCount

The number of CIDR blocks available for use by the IP set references in a firewall.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

### IPSetReferences

The list of the IP set references used by a firewall.

Type: String to [IPSetMetadata](#) object map

Required: No

### UtilizedCIDRCount

The number of CIDR blocks used by the IP set references in a firewall.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

## See Also

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

- [Amazon SDK for C++](#)

- [Amazon SDK for Java V2](#)
- [Amazon 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](#) 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](#) 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](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# Dimension

The value to use in an Amazon CloudWatch custom metric dimension. This is used in the `PublishMetrics` [CustomAction](#). A CloudWatch custom metric dimension is a name/value pair that's part of the identity of a metric.

Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# EncryptionConfiguration

A complex type that contains optional Amazon Key Management Service (KMS) encryption settings for your Network Firewall resources. Your data is encrypted by default with an Amazon owned key that Amazon owns and manages for you. You can use either the Amazon owned key, or provide your own customer managed key. To learn more about KMS encryption of your Network Firewall resources, see [Encryption at rest with Amazon Key Management Service](#) in the *Network Firewall Developer Guide*.

## Contents

### Type

The type of Amazon KMS key to use for encryption of your Network Firewall resources.

Type: String

Valid Values: CUSTOMER\_KMS | AWS\_OWNED\_KMS\_KEY

Required: Yes

### KeyId

The ID of the Amazon Key Management Service (KMS) customer managed key. You can use any of the key identifiers that KMS supports, unless you're using a key that's managed by another account. If you're using a key managed by another account, then specify the key ARN. For more information, see [Key ID](#) in the *Amazon KMS Developer Guide*.

Type: String

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

Pattern: `.*\S.*`

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# Firewall

The firewall defines the configuration settings for an Amazon 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 Amazon resource.

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

## Contents

### 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

### 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

### 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](#) objects

Required: Yes

### 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

### 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

### EncryptionConfiguration

A complex type that contains the Amazon KMS encryption configuration settings for your firewall.

Type: [EncryptionConfiguration](#) object

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

## 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

## 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

## Tags

Type: Array of [Tag](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#), define the policy. You can retrieve all objects for a firewall policy by calling [DescribeFirewallPolicy](#).

## Contents

### 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](#).

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](#).

Type: Array of strings

Required: Yes

### **PolicyVariables**

Contains variables that you can use to override default Suricata settings in your firewall policy.

Type: [PolicyVariables](#) object

Required: No

### **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 *Amazon 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](#) 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](#) 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](#) objects

Required: No

### **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](#) objects

Required: No

### **TLSInspectionConfigurationArn**

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## **See Also**

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#).

## 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# FirewallPolicyResponse

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

## Contents

### 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

### **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

### **EncryptionConfiguration**

A complex type that contains the Amazon KMS encryption configuration settings for your firewall policy.

Type: [EncryptionConfiguration](#) object

Required: No

### **FirewallPolicyStatus**

The current status of the firewall policy. You can retrieve this for a firewall policy by calling [DescribeFirewallPolicy](#) and providing the firewall policy's name or ARN.

Type: String

Valid Values: ACTIVE | DELETING | ERROR

Required: No

### **LastModifiedTime**

The last time that the firewall policy was changed.

Type: Timestamp

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](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# FirewallStatus

Detailed information about the current status of a [Firewall](#). You can retrieve this for a firewall by calling [DescribeFirewall](#) 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 | CAPACITY\_CONSTRAINED

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

### CapacityUsageSummary

Describes the capacity usage of the resources contained in a firewall's reference sets. Network Firewall calculates the capacity usage by taking an aggregated count of all of the resources used by all of the reference sets in a firewall.

Type: [CapacityUsageSummary](#) object

Required: No

## 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](#) object map

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# Header

The basic rule criteria for Amazon 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](#).

## 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 and IPv6.

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`.
- To configure Network Firewall to inspect for the IP address `1111:0000:0000:0000:0000:0000:0000:0111`, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from `1111:0000:0000:0000:0000:0000:0000:0000` to `1111:0000:0000:0000:ffff:ffff:ffff:ffff`, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

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 Amazon 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 and IPv6.

**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`.
- To configure Network Firewall to inspect for the IP address `1111:0000:0000:0000:0000:0000:0000:0111`, specify `1111:0000:0000:0000:0000:0000:0000:0111/128`.
- To configure Network Firewall to inspect for IP addresses from `1111:0000:0000:0000:0000:0000:0000:0000` to `1111:0000:0000:0000:ffff:ffff:ffff:ffff`, specify `1111:0000:0000:0000:0000:0000:0000:0000/64`.

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# IPSet

A list of IP addresses and address ranges, in CIDR notation. This is part of a [RuleVariables](#).

## 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# IPSetMetadata

General information about the IP set.

## Contents

### ResolvedCIDRCount

Describes the total number of CIDR blocks currently in use by the IP set references in a firewall. To determine how many CIDR blocks are available for you to use in a firewall, you can call `AvailableCIDRCount`.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 1000000.

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# IPSetReference

Configures one or more IP set references for a Suricata-compatible rule group. This is used in [CreateRuleGroup](#) or [UpdateRuleGroup](#). An IP set reference is a rule variable that references resources that you create and manage in another Amazon service, such as an Amazon VPC prefix list. Network Firewall IP set references enable you to dynamically update the contents of your rules. When you create, update, or delete the resource you are referencing in your rule, Network Firewall automatically updates the rule's content with the changes. For more information about IP set references in Network Firewall, see [Using IP set references](#) in the *Network Firewall Developer Guide*.

Network Firewall currently supports [Amazon VPC prefix lists](#) and [resource groups](#) in IP set references.

## Contents

### ReferenceArn

The Amazon Resource Name (ARN) of the resource that you are referencing in your rule group.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# LogDestinationConfig

Defines where Amazon Network Firewall sends logs for the firewall for one log type. This is used in [LoggingConfiguration](#). You can send each type of log to an Amazon S3 bucket, a CloudWatch log group, or a 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 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 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](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# LoggingConfiguration

Defines how Amazon Network Firewall performs logging for a [Firewall](#).

## Contents

### LogDestinationConfigs

Defines the logging destinations for the logs for a firewall. Network Firewall generates logs for stateful rule groups.

Type: Array of [LogDestinationConfig](#) objects

Required: Yes

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#) 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](#) 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](#) 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](#) 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](#) objects

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#) 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 | CAPACITY\_CONSTRAINED

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# PolicyVariables

Contains variables that you can use to override default Suricata settings in your firewall policy.

## Contents

### RuleVariables

The IPv4 or IPv6 addresses in CIDR notation to use for the Suricata HOME\_NET variable. If your firewall uses an inspection VPC, you might want to override the HOME\_NET variable with the CIDRs of your home networks. If you don't override HOME\_NET with your own CIDRs, Network Firewall by default uses the CIDR of your inspection VPC.

Type: String to [IPSet](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# PortRange

A single port range specification. This is used for source and destination port ranges in the stateless rule [MatchAttributes](#), [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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# ReferenceSets

Contains a set of IP set references.

## Contents

### IPSetReferences

The list of IP set references.

Type: String to [IPSetReference](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleDefinition

The inspection criteria and action for a single stateless rule. Amazon 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](#).

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](#).

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](#) object

Required: Yes

## **See Also**

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleGroup

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

Amazon 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](#) object

Required: Yes

### ReferenceSets

The list of a rule group's reference sets.

Type: [ReferenceSets](#) object

Required: No

### 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](#) 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. Some limitations apply; for more information, see [Strict evaluation order](#) in the *Amazon Network Firewall Developer Guide*.

Type: [StatefulRuleOptions](#) object

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleGroupMetadata

High-level information about a rule group, returned by [ListRuleGroups](#). 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleGroupResponse

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

## Contents

### 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

## AnalysisResults

The list of analysis results for `AnalyzeRuleGroup`. If you set `AnalyzeRuleGroup` to `TRUE` in [CreateRuleGroup](#), [UpdateRuleGroup](#), or [DescribeRuleGroup](#), Network Firewall analyzes the rule group and identifies the rules that might adversely effect your firewall's functionality. For example, if Network Firewall detects a rule that's routing traffic asymmetrically, which impacts the service's ability to properly process traffic, the service includes the rule in the list of analysis results.

Type: Array of [AnalysisResult](#) objects

Required: No

## 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](#) 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

### **EncryptionConfiguration**

A complex type that contains the Amazon KMS encryption configuration settings for your rule group.

Type: [EncryptionConfiguration](#) object

Required: No

### **LastModifiedTime**

The last time that the rule group was changed.

Type: Timestamp

Required: No

### **NumberOfAssociations**

The number of firewall policies that use this rule group.

Type: Integer

Required: No

### **RuleGroupStatus**

Detailed information about the current status of a rule group.

Type: String

Valid Values: ACTIVE | DELETING | ERROR

Required: No

### **SnsTopic**

The Amazon resource name (ARN) of the Amazon Simple Notification Service SNS topic that's used to record changes to the managed rule group. You can subscribe to the SNS topic to receive notifications when the managed rule group is modified, such as for new versions and for version expiration. For more information, see the [Amazon Simple Notification Service Developer Guide](#).

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## SourceMetadata

A complex type that contains metadata about the rule group that your own rule group is copied from. You can use the metadata to track the version updates made to the originating rule group.

Type: [SourceMetadata](#) object

Required: No

## Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) 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 Amazon SDKs, see the following:



- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleOption

Additional settings for a stateful rule. This is part of the [StatefulRule](#) configuration.

## Contents

### Keyword

The keyword for the Suricata compatible rule option. You must include a `sid` (signature ID), and can optionally include other keywords. For information about Suricata compatible keywords, see [Rule options](#) in the Suricata documentation.

Type: String

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

Pattern: `.*`

Required: Yes

### Settings

The settings of the Suricata compatible rule option. Rule options have zero or more setting values, and the number of possible and required settings depends on the Keyword. For more information about the settings for specific options, see [Rule options](#).

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)

- [Amazon 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](#) object

Required: No

### RulesString

Stateful inspection criteria, provided in Suricata compatible rules. Suricata is an open-source threat detection framework 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.

#### Note

You can't use the `priority` keyword if the `RuleOrder` option in [StatefulRuleOptions](#) is set to `STRICT_ORDER`.

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](#) objects

Required: No

### **StatelessRulesAndCustomActions**

Stateless inspection criteria to be used in a stateless rule group.

Type: [StatelessRulesAndCustomActions](#) object

Required: No

## **See Also**

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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](#) in this guide and [Stateful domain list rule groups in Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# RuleVariables

Settings that are available for use in the rules in the [RuleGroup](#) where this is defined.

## Contents

### IPSets

A list of IP addresses and address ranges, in CIDR notation.

Type: String to [IPSet](#) 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](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# ServerCertificate

Any Amazon Certificate Manager (ACM) Secure Sockets Layer/Transport Layer Security (SSL/TLS) server certificate that's associated with a [ServerCertificateConfiguration](#). Used in a [TLSInspectionConfiguration](#) for inspection of inbound traffic to your firewall. You must request or import a SSL/TLS certificate into ACM for each domain Network Firewall needs to decrypt and inspect. Amazon Network Firewall uses the SSL/TLS certificates to decrypt specified inbound SSL/TLS traffic going to your firewall. For information about working with certificates in Amazon Certificate Manager, see [Request a public certificate](#) or [Importing certificates](#) in the *Amazon Certificate Manager User Guide*.

## Contents

### ResourceArn

The Amazon Resource Name (ARN) of the Amazon Certificate Manager SSL/TLS server certificate that's used for inbound SSL/TLS inspection.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# ServerCertificateConfiguration

Configures the Amazon Certificate Manager certificates and scope that Network Firewall uses to decrypt and re-encrypt traffic using a [TLSInspectionConfiguration](#). You can configure `ServerCertificates` for inbound SSL/TLS inspection, a `CertificateAuthorityArn` for outbound SSL/TLS inspection, or both. For information about working with certificates for TLS inspection, see [Using SSL/TLS server certificates with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

## Note

If a server certificate that's associated with your [TLSInspectionConfiguration](#) is revoked, deleted, or expired it can result in client-side TLS errors.

## Contents

### CertificateAuthorityArn

The Amazon Resource Name (ARN) of the imported certificate authority (CA) certificate within Amazon Certificate Manager (ACM) to use for outbound SSL/TLS inspection.

The following limitations apply:

- You can use CA certificates that you imported into ACM, but you can't generate CA certificates with ACM.
- You can't use certificates issued by Amazon Private Certificate Authority.

For more information about configuring certificates for outbound inspection, see [Using SSL/TLS certificates with certificates with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

For information about working with certificates in ACM, see [Importing certificates](#) in the *Amazon Certificate Manager User Guide*.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

## CheckCertificateRevocationStatus

When enabled, Network Firewall checks if the server certificate presented by the server in the SSL/TLS connection has a revoked or unknown status. If the certificate has an unknown or revoked status, you must specify the actions that Network Firewall takes on outbound traffic. To check the certificate revocation status, you must also specify a `CertificateAuthorityArn` in [ServerCertificateConfiguration](#).

Type: [CheckCertificateRevocationStatusActions](#) object

Required: No

## Scopes

A list of scopes.

Type: Array of [ServerCertificateScope](#) objects

Required: No

## ServerCertificates

The list of server certificates to use for inbound SSL/TLS inspection.

Type: Array of [ServerCertificate](#) objects

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# ServerCertificateScope

Settings that define the Secure Sockets Layer/Transport Layer Security (SSL/TLS) traffic that Network Firewall should decrypt for inspection by the stateful rule engine.

## Contents

### DestinationPorts

The destination ports to decrypt for inspection, in Transmission Control Protocol (TCP) format. If not specified, this matches with any destination port.

You can specify individual ports, for example 1994, and you can specify port ranges, such as 1990:1994.

Type: Array of [PortRange](#) objects

Required: No

### Destinations

The destination IP addresses and address ranges to decrypt for inspection, in CIDR notation. If not specified, this matches with any destination address.

Type: Array of [Address](#) objects

Required: No

### Protocols

The protocols to decrypt for inspection, specified using each protocol's assigned internet protocol number (IANA). Network Firewall currently supports only TCP.

Type: Array of integers

Valid Range: Minimum value of 0. Maximum value of 255.

Required: No

### SourcePorts

The source ports to decrypt for inspection, in Transmission Control Protocol (TCP) format. If not specified, this matches with any source port.

You can specify individual ports, for example 1994, and you can specify port ranges, such as 1990:1994.

Type: Array of [PortRange](#) objects

Required: No

## Sources

The source IP addresses and address ranges to decrypt for inspection, in CIDR notation. If not specified, this matches with any source address.

Type: Array of [Address](#) objects

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# SourceMetadata

High-level information about the managed rule group that your own rule group is copied from. You can use the the metadata to track version updates made to the originating rule group. You can retrieve all objects for a rule group by calling [DescribeRuleGroup](#).

## Contents

### SourceArn

The Amazon Resource Name (ARN) of the rule group that your own rule group is copied from.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

### SourceUpdateToken

The update token of the Amazon managed rule group that your own rule group is copied from. To determine the update token for the managed rule group, call [DescribeRuleGroup](#).

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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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. `STRICT_ORDER` is the default and recommended option. With `STRICT_ORDER`, provide your rules in the order that you want them to be evaluated. You can then choose one or more default actions for packets that don't match any rules. Choose `STRICT_ORDER` to have the stateful rules engine determine the evaluation order of your rules. The default action for this rule order is `PASS`, followed by `DROP`, `REJECT`, and `ALERT` actions. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on your settings. For more information, see [Evaluation order for stateful rules](#) in the *Amazon Network Firewall Developer Guide*.

Type: String

Valid Values: `DEFAULT_ACTION_ORDER` | `STRICT_ORDER`

Required: No

### StreamExceptionPolicy

Configures how Network Firewall processes traffic when a network connection breaks midstream. Network connections can break due to disruptions in external networks or within the firewall itself.

- `DROP` - Network Firewall fails closed and drops all subsequent traffic going to the firewall. This is the default behavior.
- `CONTINUE` - Network Firewall continues to apply rules to the subsequent traffic without context from traffic before the break. This impacts the behavior of rules that depend on this context. For example, if you have a stateful rule to drop http traffic, Network Firewall won't match the traffic for this rule because the service won't have the context from session initialization defining the application layer protocol as HTTP. However, this behavior is rule dependent—a TCP-layer rule using a `flow:stateless` rule would still match, as would the `aws:drop_strict` default action.



- **REJECT** - Network Firewall fails closed and drops all subsequent traffic going to the firewall. Network Firewall also sends a TCP reject packet back to your client so that the client can immediately establish a new session. Network Firewall will have context about the new session and will apply rules to the subsequent traffic.

Type: String

Valid Values: DROP | CONTINUE | REJECT

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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 LoggingConfiguration](#).
- **ALERT** - Sends an alert log message, if alert logging is configured in the [Firewall LoggingConfiguration](#).

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 | REJECT

Required: Yes

### Header

The stateful inspection criteria for this rule, used to inspect traffic flows.

Type: [Header](#) object

Required: Yes

### RuleOptions

Additional options for the rule. These are the Suricata RuleOptions settings.

Type: Array of [RuleOption](#) objects

Required: Yes

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# StatefulRuleGroupOverride

The setting that allows the policy owner to change the behavior of the rule group within a policy.

## Contents

### Action

The action that changes the rule group from DROP to ALERT. This only applies to managed rule groups.

Type: String

Valid Values: DROP\_TO\_ALERT

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# StatefulRuleGroupReference

Identifier for a single stateful rule group, used in a firewall policy to refer to a rule group.

## Contents

### 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

### Override

The action that allows the policy owner to override the behavior of the rule group within a policy.

Type: [StatefulRuleGroupOverride](#) object

Required: No

### Priority

An integer setting that indicates the order in which to run the stateful rule groups in a single [FirewallPolicy](#). This setting only applies to firewall policies that specify the STRICT\_ORDER rule order in the stateful engine options settings.

Network Firewall evaluates 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

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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 *Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# StatelessRule

A single stateless rule. This is used in [StatelessRulesAndCustomActions](#).

## 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](#) object

Required: Yes

## See Also

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

- [Amazon SDK for C++](#)



- [Amazon SDK for Java V2](#)
- [Amazon 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](#). 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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

### StatelessRules

Defines the set of stateless rules for use in a stateless rule group.

Type: Array of [StatelessRule](#) objects

Required: Yes

### 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 RuleDefinition](#) Actions specification.

Type: Array of [CustomAction](#) objects

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# SubnetMapping

The ID for a subnet that you want to associate with the firewall. This is used with [CreateFirewall](#) and [AssociateSubnets](#). Amazon 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

### IPAddressType

The subnet's IP address type. You can't change the IP address type after you create the subnet.

Type: String

Valid Values: DUALSTACK | IPV4 | IPV6

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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, Amazon 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](#).

Type: [Attachment](#) 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](#).

Type: String to [PerObjectStatus](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# Tag

A key:value pair associated with an Amazon 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 Amazon 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)

- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# TCPFlagField

TCP flags and masks to inspect packets for, used in stateless rules [MatchAttributes](#) 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)

- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# TlsCertificateData

Contains metadata about an Amazon Certificate Manager certificate.

## Contents

### CertificateArn

The Amazon Resource Name (ARN) of the certificate.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

### CertificateSerial

The serial number of the certificate.

Type: String

Required: No

### Status

The status of the certificate.

Type: String

Required: No

### StatusMessage

Contains details about the certificate status, including information about certificate errors.

Type: String

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

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

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# TLSTLSInspectionConfiguration

The object that defines a TLS inspection configuration. This, along with [TLSTLSInspectionConfigurationResponse](#), define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling [DescribeTLSTLSInspectionConfiguration](#).

Amazon Network Firewall uses a TLS inspection configuration to decrypt traffic. Network Firewall re-encrypts the traffic before sending it to its destination.

To use a TLS inspection configuration, you add it to a new Network Firewall firewall policy, then you apply the firewall policy to a firewall. Network Firewall acts as a proxy service to decrypt and inspect the traffic traveling through your firewalls. You can reference a TLS inspection configuration from more than one firewall policy, and you can use a firewall policy in more than one firewall. For more information about using TLS inspection configurations, see [Inspecting SSL/TLS traffic with TLS inspection configurations](#) in the *Amazon Network Firewall Developer Guide*.

## Contents

### ServerCertificateConfigurations

Lists the server certificate configurations that are associated with the TLS configuration.

Type: Array of [ServerCertificateConfiguration](#) objects

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)

# TLSInspectionConfigurationMetadata

High-level information about a TLS inspection configuration, returned by `ListTLSInspectionConfigurations`. You can use the information provided in the metadata to retrieve and manage a TLS configuration.

## Contents

### Arn

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

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

Pattern: `^arn:aws.*`

Required: No

### Name

The descriptive name of the TLS inspection configuration. You can't change the name of a TLS inspection configuration 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 Amazon SDKs, see the following:

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon SDK for Ruby V3](#)



# TLSInspectionConfigurationResponse

The high-level properties of a TLS inspection configuration. This, along with the `TLSInspectionConfiguration`, define the TLS inspection configuration. You can retrieve all objects for a TLS inspection configuration by calling `DescribeTLSInspectionConfiguration`.

## Contents

### `TLSInspectionConfigurationArn`

The Amazon Resource Name (ARN) of the TLS inspection configuration.

Type: String

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

Pattern: `^arn:aws.*`

Required: Yes

### `TLSInspectionConfigurationId`

A unique identifier for the TLS inspection configuration. This ID is returned in the responses to create and list commands. You provide it to operations such as update and delete.

Type: String

Length Constraints: Fixed length of 36.

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

Required: Yes

### `TLSInspectionConfigurationName`

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

Type: String

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

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



Required: Yes

### **CertificateAuthority**

Contains metadata about an Amazon Certificate Manager certificate.

Type: [TlsCertificateData](#) object

Required: No

### **Certificates**

A list of the certificates associated with the TLS inspection configuration.

Type: Array of [TlsCertificateData](#) objects

Required: No

### **Description**

A description of the TLS inspection configuration.

Type: String

Length Constraints: Maximum length of 512.

Pattern: `^.*$`

Required: No

### **EncryptionConfiguration**

A complex type that contains the Amazon KMS encryption configuration settings for your TLS inspection configuration.

Type: [EncryptionConfiguration](#) object

Required: No

### **LastModifiedTime**

The last time that the TLS inspection configuration was changed.

Type: Timestamp

Required: No

## NumberOfAssociations

The number of firewall policies that use this TLS inspection configuration.

Type: Integer

Required: No

## Tags

The key:value pairs to associate with the resource.

Type: Array of [Tag](#) objects

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

Required: No

## TLSInspectionConfigurationStatus

Detailed information about the current status of a [TLSInspectionConfiguration](#). You can retrieve this for a TLS inspection configuration by calling [DescribeTLSInspectionConfiguration](#) and providing the TLS inspection configuration name and ARN.

Type: String

Valid Values: ACTIVE | DELETING | ERROR

Required: No

## See Also

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

- [Amazon SDK for C++](#)
- [Amazon SDK for Java V2](#)
- [Amazon 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 [Signing Amazon API requests](#) in the *IAM User Guide*.

## 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 [Create a signed Amazon API request](#) in the *IAM User Guide*.

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 [Elements of an Amazon API request signature](#) in the *IAM User Guide*.

Type: string

Required: Conditional

### **X-Amz-Security-Token**

The temporary security token that was obtained through a call to Amazon Security Token Service (Amazon STS). For a list of services that support temporary security credentials from Amazon STS, see [Amazon Web Services that work with IAM](#) in the *IAM User Guide*.

Condition: If you're using temporary security credentials from Amazon STS, 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 [Create a signed Amazon API request](#) in the *IAM User Guide*.

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 Amazon 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 Amazon 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 Amazon access key ID provided does not exist in our records.

HTTP Status Code: 403

## **NotAuthorized**

You do not have permission to perform this action.

HTTP Status Code: 400

## **OptInRequired**

The Amazon 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 Amazon service.

HTTP Status Code: 400