AWS Firewall Manager

Firewall Management

API Version 2018-01-01

AWS Firewall Manager: Firewall Management

Table of Contents

Welcome

This is the *AWS Firewall Manager API Reference*. This guide is for developers who need detailed information about the AWS Firewall Manager API actions, data types, and errors. For detailed information about AWS Firewall Manager features, see the AWS Firewall Manager Developer Guide.

Some API actions require explicit resource permissions. For information, see the developer guide topic Firewall Manager required permissions for API actions.

This document was last published on October 6, 2021.

Actions

The following actions are supported:

- AssociateAdminAccount (p. 3)
- DeleteAppsList (p. 5)
- DeleteNotificationChannel (p. 7)
- DeletePolicy (p. 8)
- DeleteProtocolsList (p. 11)
- DisassociateAdminAccount (p. 13)
- GetAdminAccount (p. 14)
- GetAppsList (p. 16)
- GetComplianceDetail (p. 19)
- GetNotificationChannel (p. 22)
- GetPolicy (p. 24)
- GetProtectionStatus (p. 27)
- GetProtocolsList (p. 32)
- GetViolationDetails (p. 35)
- ListAppsLists (p. 44)
- ListComplianceStatus (p. 47)
- ListMemberAccounts (p. 50)
- ListPolicies (p. 53)
- ListProtocolsLists (p. 56)
- ListTagsForResource (p. 59)
- PutAppsList (p. 61)
- PutNotificationChannel (p. 64)
- PutPolicy (p. 66)
- PutProtocolsList (p. 70)
- TagResource (p. 73)
- UntagResource (p. 75)

AssociateAdminAccount

Sets the AWS Firewall Manager administrator account. The account must be a member of the organization in AWS Organizations whose resources you want to protect. AWS Firewall Manager sets the permissions that allow the account to administer your Firewall Manager policies.

The account that you associate with AWS Firewall Manager is called the AWS Firewall Manager administrator account.

Request Syntax

```
{
   "AdminAccount": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

AdminAccount (p. 3)

The AWS account ID to associate with AWS Firewall Manager as the AWS Firewall Manager administrator account. This must be an AWS Organizations member account. For more information about AWS Organizations, see Managing the AWS Accounts in Your Organization.

Type: String

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

Pattern: `^[0-9]+$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

DeleteAppsList

Permanently deletes an AWS Firewall Manager applications list.

Request Syntax

```
{
   "ListId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ListId (p. 5)

The ID of the applications list that you want to delete. You can retrieve this ID from `PutAppsList`, `ListAppsLists`, and `GetAppsList`.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

DeleteNotificationChannel

Deletes an AWS Firewall Manager association with the IAM role and the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager SNS logs.

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

DeletePolicy

Permanently deletes an AWS Firewall Manager policy.

Request Syntax

```
{
   "DeleteAllPolicyResources": boolean,
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

DeleteAllPolicyResources (p. 8)

If `True`, the request performs cleanup according to the policy type.

For AWS WAF and Shield Advanced policies, the cleanup does the following:

- Deletes rule groups created by AWS Firewall Manager
- Removes web ACLs from in-scope resources
- Deletes web ACLs that contain no rules or rule groups

For security group policies, the cleanup does the following for each security group in the policy:

- Disassociates the security group from in-scope resources
- Deletes the security group if it was created through Firewall Manager and if it's no longer associated with any resources through another policy

After the cleanup, in-scope resources are no longer protected by web ACLs in this policy. Protection of out-of-scope resources remains unchanged. Scope is determined by tags that you create and accounts that you associate with the policy. When creating the policy, if you specify that only resources in specific accounts or with specific tags are in scope of the policy, those accounts and resources are handled by the policy. All others are out of scope. If you don't specify tags or accounts, all resources are in scope.

Type: Boolean

Required: No

PolicyId (p. 8)

The ID of the policy that you want to delete. You can retrieve this ID from `PutPolicy` and `ListPolicies`.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

- AWS SDK for Ruby V3

DeleteProtocolsList

Permanently deletes an AWS Firewall Manager protocols list.

Request Syntax

```
{
   "ListId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ListId (p. 11)

The ID of the protocols list that you want to delete. You can retrieve this ID from `PutProtocolsList`, `ListProtocolsLists`, and `GetProtocolsLost`.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

DisassociateAdminAccount

Disassociates the account that has been set as the AWS Firewall Manager administrator account. To set a different account as the administrator account, you must submit an `AssociateAdminAccount` request.

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetAdminAccount

Returns the AWS Organizations account that is associated with AWS Firewall Manager as the AWS Firewall Manager administrator.

Response Syntax

```
{
   "AdminAccount": "string",
   "RoleStatus": "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.

AdminAccount (p. 14)

The AWS account that is set as the AWS Firewall Manager administrator.

Type: String

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

Pattern: `^[0-9]+$`

RoleStatus (p. 14)

The status of the AWS account that you set as the AWS Firewall Manager administrator.

Type: String

Valid Values: `READY | CREATING | PENDING_DELETION | DELETING | DELETED`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetAppsList

Returns information about the specified AWS Firewall Manager applications list.

Request Syntax

```
{
   "DefaultList": boolean,
   "ListId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

DefaultList (p. 16)

Specifies whether the list to retrieve is a default list owned by AWS Firewall Manager.

Type: Boolean

Required: No

ListId (p. 16)

The ID of the AWS Firewall Manager applications list that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Syntax

```
{
   "AppsList": {
      "AppsList": [
         {
            "AppName": "string",
            "Port": number,
            "Protocol": "string"
         }
      ],
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousAppsList": {
         "string" : [
            {
               "AppName": "string",
               "Port": number,
               "Protocol": "string"
            }
         ]
      }
   },
   "AppsListArn": "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.

AppsList (p. 16)

Information about the specified AWS Firewall Manager applications list.

Type: AppsListData (p. 81) object

AppsListArn (p. 16)

The Amazon Resource Name (ARN) of the applications list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetComplianceDetail

Returns detailed compliance information about the specified member account. Details include resources that are in and out of compliance with the specified policy.

- Resources are considered noncompliant for AWS WAF and Shield Advanced policies if the specified policy has not been applied to them.
- Resources are considered noncompliant for security group policies if they are in scope of the policy, they violate one or more of the policy rules, and remediation is disabled or not possible.
- Resources are considered noncompliant for AWS Network Firewall policies if a firewall is missing in the VPC, if the firewall endpoint isn't set up in an expected Availability Zone and subnet, if a subnet created by the Firewall Manager doesn't have the expected route table, and for modifications to a firewall policy that violate the Firewall Manager policy's rules.
- Resources are considered noncompliant for DNS Firewall policies if a DNS Firewall rule group is missing from the rule group associations for the VPC.

Request Syntax

```
{
   "MemberAccount": "string",
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

MemberAccount (p. 19)

The AWS account that owns the resources that you want to get the details for.

Type: String

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

Pattern: `^[0-9]+$`

Required: Yes

PolicyId (p. 19)

The ID of the policy that you want to get the details for. `PolicyId` is returned by `PutPolicy` and by `ListPolicies`.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Syntax

```
{
   "PolicyComplianceDetail": {
      "EvaluationLimitExceeded": boolean,
      "ExpiredAt": number,
      "IssueInfoMap": {
         "string" : "string"
      },
      "MemberAccount": "string",
      "PolicyId": "string",
      "PolicyOwner": "string",
      "Violators": [
         {
            "ResourceId": "string",
            "ResourceType": "string",
            "ViolationReason": "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.

PolicyComplianceDetail (p. 20)

Information about the resources and the policy that you specified in the `GetComplianceDetail` request.

Type: PolicyComplianceDetail (p. 134) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetNotificationChannel

Information about the Amazon Simple Notification Service (SNS) topic that is used to record AWS Firewall Manager SNS logs.

Response Syntax

```
{
   "SnsRoleName": "string",
   "SnsTopicArn": "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.

SnsRoleName (p. 22)

The IAM role that is used by AWS Firewall Manager to record activity to SNS.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

SnsTopicArn (p. 22)

The SNS topic that records AWS Firewall Manager activity.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetPolicy

Returns information about the specified AWS Firewall Manager policy.

Request Syntax

```
{
   "PolicyId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

PolicyId (p. 24)

The ID of the AWS Firewall Manager policy that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Syntax

```
{
   "Policy": {
      "DeleteUnusedFMManagedResources": boolean,
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceTypeList": [ "string" ],
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   },
   "PolicyArn": "string"
}
```

Response Elements

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

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

Policy (p. 24)

Information about the specified AWS Firewall Manager policy.

Type: Policy (p. 130) object

PolicyArn (p. 24)

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

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

InvalidTypeException

The value of the `Type` parameter is invalid.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

GetProtectionStatus

If you created a Shield Advanced policy, returns policy-level attack summary information in the event of a potential DDoS attack. Other policy types are currently unsupported.

Request Syntax

```
{
   "EndTime": number,
   "MaxResults": number,
   "MemberAccountId": "string",
   "NextToken": "string",
   "PolicyId": "string",
   "StartTime": number
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

EndTime (p. 27)

The end of the time period to query for the attacks. This is a `timestamp` type. The request syntax listing indicates a `number` type because the default used by AWS Firewall Manager is Unix time in seconds. However, any valid `timestamp` format is allowed.

Type: Timestamp

Required: No

MaxResults (p. 27)

Specifies the number of objects that you want AWS Firewall Manager to return for this request. If you have more objects than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of objects.

Type: Integer

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

Required: No

MemberAccountId (p. 27)

The AWS account that is in scope of the policy that you want to get the details for.

Type: String

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

Pattern: `^[0-9]+$`

Required: No

NextToken (p. 27)

If you specify a value for `MaxResults` and you have more objects than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response, which you can use to retrieve another group of objects. For the second and subsequent `GetProtectionStatus` requests, specify the value of `NextToken` from the previous response to get information about another batch of objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PolicyId (p. 27)

The ID of the policy for which you want to get the attack information.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

StartTime (p. 27)

The start of the time period to query for the attacks. This is a `timestamp` type. The request syntax listing indicates a `number` type because the default used by AWS Firewall Manager is Unix time in seconds. However, any valid `timestamp` format is allowed.

Type: Timestamp

Required: No

Response Syntax

```
{
   "AdminAccountId": "string",
   "Data": "string",
   "NextToken": "string",
   "ServiceType": "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.

AdminAccountId (p. 28)

The ID of the AWS Firewall Manager administrator account for this policy.

Type: String

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

Pattern: `^[0-9]+$`

Data (p. 28)

Details about the attack, including the following:

- Attack type
- Account ID
- ARN of the resource attacked
- Start time of the attack
- End time of the attack (ongoing attacks will not have an end time)

The details are in JSON format.

Type: String

NextToken (p. 28)

If you have more objects than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more objects, submit another `GetProtectionStatus` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

AWS SDKs provide auto-pagination that identify `NextToken` in a response and make subsequent request calls automatically on your behalf. However, this feature is not supported by `GetProtectionStatus`. You must submit subsequent requests with `NextToken` using your own processes.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

ServiceType (p. 28)

The service type that is protected by the policy. Currently, this is always `SHIELD_ADVANCED`.

Type: String

Valid Values: `WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON | SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT | NETWORK_FIREWALL | DNS_FIREWALL`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

Examples

Example response

This example illustrates one usage of GetProtectionStatus.

```
[
            {
            accountId: account1
            attackSummaries:[
            {
            attackId: attackId1
            resourceARN: resource1
            attackVector: [SYC_FLOOD, UDP_REFLECTION]
            startTime: 1234567890123
            endTime: 1234567890123
             },
             {
            attackId: attackId2
            resourceARN: resource2
            attackVector: [SYC_FLOOD]
            startTime: 1234567890123
            endTime: 1234567890123
            }
            ]
            },

            {
            accountId: account2
            attackSummaries:[
            {
            attackId: attackId3
            resourceARN: resource3
            attackVector: [SYC_FLOOD, UDP_REFLECTION]
            startTime: 1234567890123
            endTime: 1234567890123
            },
            {
            attackId: attackId4
            resourceARN: resource4
            attackVector: [SYC_FLOOD]
            startTime: 1234567890123
            endTime: 1234567890123
            }
            ]
            },
]
```

See Also

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

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

- AWS SDK for Python
- AWS SDK for Ruby V3

GetProtocolsList

Returns information about the specified AWS Firewall Manager protocols list.

Request Syntax

```
{
   "DefaultList": boolean,
   "ListId": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

DefaultList (p. 32)

Specifies whether the list to retrieve is a default list owned by AWS Firewall Manager.

Type: Boolean

Required: No

ListId (p. 32)

The ID of the AWS Firewall Manager protocols list that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Syntax

```
{
   "ProtocolsList": {
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousProtocolsList": {
         "string" : [ "string" ]
      },
      "ProtocolsList": [ "string" ]
   },
   "ProtocolsListArn": "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.

ProtocolsList (p. 32)

Information about the specified AWS Firewall Manager protocols list.

Type: ProtocolsListData (p. 142) object

ProtocolsListArn (p. 32)

The Amazon Resource Name (ARN) of the specified protocols list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetViolationDetails

Retrieves violations for a resource based on the specified AWS Firewall Manager policy and AWS account.

Request Syntax

```
{
   "MemberAccount": "string",
   "PolicyId": "string",
   "ResourceId": "string",
   "ResourceType": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

MemberAccount (p. 35)

The AWS account ID that you want the details for.

Type: String

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

Pattern: `^[0-9]+$`

Required: Yes

PolicyId (p. 35)

The ID of the AWS Firewall Manager policy that you want the details for. This currently only supports security group content audit policies.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

ResourceId (p. 35)

The ID of the resource that has violations.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ResourceType (p. 35)

The resource type. This is in the format shown in the AWS Resource Types Reference. Supported resource types are: `AWS::EC2::Instance`, `AWS::EC2::NetworkInterface`, `AWS::EC2::SecurityGroup`, `AWS::NetworkFirewall::FirewallPolicy`, and `AWS::EC2::Subnet`.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Syntax

```
{
   "ViolationDetail": {
      "MemberAccount": "string",
      "PolicyId": "string",
      "ResourceDescription": "string",
      "ResourceId": "string",
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceViolations": [
         {
            "AwsEc2InstanceViolation": {
               "AwsEc2NetworkInterfaceViolations": [
                  {
                     "ViolatingSecurityGroups": [ "string" ],
                     "ViolationTarget": "string"
                  }
               ],
               "ViolationTarget": "string"
            },
            "AwsEc2NetworkInterfaceViolation": {
               "ViolatingSecurityGroups": [ "string" ],
               "ViolationTarget": "string"
            },
            "AwsVPCSecurityGroupViolation": {
               "PartialMatches": [
                  {
                     "Reference": "string",
                     "TargetViolationReasons": [ "string" ]
                  }
               ],
               "PossibleSecurityGroupRemediationActions": [
                  {
                     "Description": "string",
                     "IsDefaultAction": boolean,
                     "RemediationActionType": "string",
                     "RemediationResult": {
                        "FromPort": number,
                        "IPV4Range": "string",
                        "IPV6Range": "string",
                        "PrefixListId": "string",
                        "Protocol": "string",
                        "ToPort": number
                     }
                  }
               ],
               "ViolationTarget": "string",
               "ViolationTargetDescription": "string"
            },
            "DnsDuplicateRuleGroupViolation": {
               "ViolationTarget": "string",
               "ViolationTargetDescription": "string"
            },
            "DnsRuleGroupLimitExceededViolation": {
               "NumberOfRuleGroupsAlreadyAssociated": number,
               "ViolationTarget": "string",
               "ViolationTargetDescription": "string"
            },
            "DnsRuleGroupPriorityConflictViolation": {
               "ConflictingPolicyId": "string",
               "ConflictingPriority": number,
               "UnavailablePriorities": [ number ],
               "ViolationTarget": "string",
               "ViolationTargetDescription": "string"
            },
            "NetworkFirewallBlackHoleRouteDetectedViolation": {
               "RouteTableId": "string",
               "ViolatingRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "ViolationTarget": "string",
               "VpcId": "string"
            },
            "NetworkFirewallInternetTrafficNotInspectedViolation": {
               "ActualFirewallSubnetRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "ActualInternetGatewayRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "CurrentFirewallSubnetRouteTable": "string",
               "CurrentInternetGatewayRouteTable": "string",
               "ExpectedFirewallEndpoint": "string",
               "ExpectedFirewallSubnetRoutes": [
                  {
                     "AllowedTargets": [ "string" ],
                     "ContributingSubnets": [ "string" ],
                     "IpV4Cidr": "string",
                     "IpV6Cidr": "string",
                     "PrefixListId": "string",
                     "RouteTableId": "string"
                  }
               ],
               "ExpectedInternetGatewayRoutes": [
                  {
                     "AllowedTargets": [ "string" ],
                     "ContributingSubnets": [ "string" ],
                     "IpV4Cidr": "string",
                     "IpV6Cidr": "string",
                     "PrefixListId": "string",
                     "RouteTableId": "string"
                  }
               ],
               "FirewallSubnetId": "string",
               "InternetGatewayId": "string",
               "IsRouteTableUsedInDifferentAZ": boolean,
               "RouteTableId": "string",
               "SubnetAvailabilityZone": "string",
               "SubnetId": "string",
               "ViolatingRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "VpcId": "string"
            },
            "NetworkFirewallInvalidRouteConfigurationViolation": {
               "ActualFirewallEndpoint": "string",
               "ActualFirewallSubnetId": "string",
               "ActualFirewallSubnetRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "ActualInternetGatewayRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "AffectedSubnets": [ "string" ],
               "CurrentFirewallSubnetRouteTable": "string",
               "CurrentInternetGatewayRouteTable": "string",
               "ExpectedFirewallEndpoint": "string",
               "ExpectedFirewallSubnetId": "string",
               "ExpectedFirewallSubnetRoutes": [
                  {
                     "AllowedTargets": [ "string" ],
                     "ContributingSubnets": [ "string" ],
                     "IpV4Cidr": "string",
                     "IpV6Cidr": "string",
                     "PrefixListId": "string",
                     "RouteTableId": "string"
                  }
               ],
               "ExpectedInternetGatewayRoutes": [
                  {
                     "AllowedTargets": [ "string" ],
                     "ContributingSubnets": [ "string" ],
                     "IpV4Cidr": "string",
                     "IpV6Cidr": "string",
                     "PrefixListId": "string",
                     "RouteTableId": "string"
                  }
               ],
               "InternetGatewayId": "string",
               "IsRouteTableUsedInDifferentAZ": boolean,
               "RouteTableId": "string",
               "ViolatingRoute": {
                  "Destination": "string",
                  "DestinationType": "string",
                  "Target": "string",
                  "TargetType": "string"
               },
               "VpcId": "string"
            },
            "NetworkFirewallMissingExpectedRoutesViolation": {
               "ExpectedRoutes": [
                  {
                     "AllowedTargets": [ "string" ],
                     "ContributingSubnets": [ "string" ],
                     "IpV4Cidr": "string",
                     "IpV6Cidr": "string",
                     "PrefixListId": "string",
                     "RouteTableId": "string"
                  }
               ],
               "ViolationTarget": "string",
               "VpcId": "string"
            },
            "NetworkFirewallMissingExpectedRTViolation": {
               "AvailabilityZone": "string",
               "CurrentRouteTable": "string",
               "ExpectedRouteTable": "string",
               "ViolationTarget": "string",
               "VPC": "string"
            },
            "NetworkFirewallMissingFirewallViolation": {
               "AvailabilityZone": "string",
               "TargetViolationReason": "string",
               "ViolationTarget": "string",
               "VPC": "string"
            },
            "NetworkFirewallMissingSubnetViolation": {
               "AvailabilityZone": "string",
               "TargetViolationReason": "string",
               "ViolationTarget": "string",
               "VPC": "string"
            },
            "NetworkFirewallPolicyModifiedViolation": {
               "CurrentPolicyDescription": {
                  "StatefulRuleGroups": [
                     {
                        "ResourceId": "string",
                        "RuleGroupName": "string"
                     }
                  ],
                  "StatelessCustomActions": [ "string" ],
                  "StatelessDefaultActions": [ "string" ],
                  "StatelessFragmentDefaultActions": [ "string" ],
                  "StatelessRuleGroups": [
                     {
                        "Priority": number,
                        "ResourceId": "string",
                        "RuleGroupName": "string"
                     }
                  ]
               },
               "ExpectedPolicyDescription": {
                  "StatefulRuleGroups": [
                     {
                        "ResourceId": "string",
                        "RuleGroupName": "string"
                     }
                  ],
                  "StatelessCustomActions": [ "string" ],
                  "StatelessDefaultActions": [ "string" ],
                  "StatelessFragmentDefaultActions": [ "string" ],
                  "StatelessRuleGroups": [
                     {
                        "Priority": number,
                        "ResourceId": "string",
                        "RuleGroupName": "string"
                     }
                  ]
               },
               "ViolationTarget": "string"
            },
            "NetworkFirewallUnexpectedFirewallRoutesViolation": {
               "FirewallEndpoint": "string",
               "FirewallSubnetId": "string",
               "RouteTableId": "string",
               "ViolatingRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "VpcId": "string"
            },
            "NetworkFirewallUnexpectedGatewayRoutesViolation": {
               "GatewayId": "string",
               "RouteTableId": "string",
               "ViolatingRoutes": [
                  {
                     "Destination": "string",
                     "DestinationType": "string",
                     "Target": "string",
                     "TargetType": "string"
                  }
               ],
               "VpcId": "string"
            },
            "PossibleRemediationActions": {
               "Actions": [
                  {
                     "Description": "string",
                     "IsDefaultAction": boolean,
                     "OrderedRemediationActions": [
                        {
                           "Order": number,
                           "RemediationAction": {
                              "Description": "string",
                              "EC2AssociateRouteTableAction": {
                                 "Description": "string",
                                 "GatewayId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "SubnetId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2CopyRouteTableAction": {
                                 "Description": "string",
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "VpcId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2CreateRouteAction": {
                                 "Description": "string",
                                 "DestinationCidrBlock": "string",
                                 "DestinationIpv6CidrBlock": "string",
                                 "DestinationPrefixListId": "string",
                                 "GatewayId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "VpcEndpointId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2CreateRouteTableAction": {
                                 "Description": "string",
                                 "VpcId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2DeleteRouteAction": {
                                 "Description": "string",
                                 "DestinationCidrBlock": "string",
                                 "DestinationIpv6CidrBlock": "string",
                                 "DestinationPrefixListId": "string",
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2ReplaceRouteAction": {
                                 "Description": "string",
                                 "DestinationCidrBlock": "string",
                                 "DestinationIpv6CidrBlock": "string",
                                 "DestinationPrefixListId": "string",
                                 "GatewayId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              },
                              "EC2ReplaceRouteTableAssociationAction": {
                                 "AssociationId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 },
                                 "Description": "string",
                                 "RouteTableId": {
                                    "Description": "string",
                                    "ResourceId": "string"
                                 }
                              }
                           }
                        }
                     ]
                  }
               ],
               "Description": "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.

ViolationDetail (p. 36)

Violation detail for a resource.

Type: ViolationDetail (p. 163) object

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

- AWS Command Line Interface

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

ListAppsLists

Returns an array of `AppsListDataSummary` objects.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

DefaultLists (p. 44)

Specifies whether the lists to retrieve are default lists owned by AWS Firewall Manager.

Type: Boolean

Required: No

MaxResults (p. 44)

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

If you don't specify this, AWS Firewall Manager returns all available objects.

Type: Integer

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

Required: Yes

NextToken (p. 44)

If you specify a value for `MaxResults` in your list request, and you have more objects than the maximum, AWS Firewall Manager returns this token in the response. For all but the first request, you provide the token returned by the prior request in the request parameters, to retrieve the next batch of objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "AppsLists": [ 
      { 
         "AppsList": [ 
            { 
               "AppName": "string",
               "Port": number,
               "Protocol": "string"
            }
         ],
         "ListArn": "string",
         "ListId": "string",
         "ListName": "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.

AppsLists (p. 44)

An array of `AppsListDataSummary` objects.

Type: Array of AppsListDataSummary (p. 83) objects

NextToken (p. 44)

If you specify a value for `MaxResults` in your list request, and you have more objects than the maximum, AWS Firewall Manager returns this token in the response. You can use this token in subsequent requests to retrieve the next batch of objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

ListComplianceStatus

Returns an array of `PolicyComplianceStatus` objects. Use `PolicyComplianceStatus` to get a summary of which member accounts are protected by the specified policy.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

MaxResults (p. 47)

Specifies the number of `PolicyComplianceStatus` objects that you want Firewall Manager to return for this request. If you have more `PolicyComplianceStatus` objects than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of `PolicyComplianceStatus` objects.

Type: Integer

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

Required: No

NextToken (p. 47)

If you specify a value for `MaxResults` and you have more `PolicyComplianceStatus` objects than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of `PolicyComplianceStatus` objects. For the second and subsequent `ListComplianceStatus` requests, specify the value of `NextToken` from the previous response to get information about another batch of `PolicyComplianceStatus` objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PolicyId (p. 47)

The ID of the AWS Firewall Manager policy that you want the details for.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "PolicyComplianceStatusList": [
      {
         "EvaluationResults": [
            {
               "ComplianceStatus": "string",
               "EvaluationLimitExceeded": boolean,
               "ViolatorCount": number
            }
         ],
         "IssueInfoMap": {
            "string" : "string"
         },
         "LastUpdated": number,
         "MemberAccount": "string",
         "PolicyId": "string",
         "PolicyName": "string",
         "PolicyOwner": "string"
      }
   ]
}
```

Response Elements

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

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

NextToken (p. 48)

If you have more `PolicyComplianceStatus` objects than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more `PolicyComplianceStatus` objects, submit another `ListComplianceStatus` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

PolicyComplianceStatusList (p. 48)

An array of `PolicyComplianceStatus` objects.

Type: Array of PolicyComplianceStatus (p. 136) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

ListMemberAccounts

Returns a `MemberAccounts` object that lists the member accounts in the administrator's AWS organization.

The `ListMemberAccounts` must be submitted by the account that is set as the AWS Firewall Manager administrator.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

MaxResults (p. 50)

Specifies the number of member account IDs that you want AWS Firewall Manager to return for this request. If you have more IDs than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of member account IDs.

Type: Integer

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

Required: No

NextToken (p. 50)

If you specify a value for `MaxResults` and you have more account IDs than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of IDs. For the second and subsequent `ListMemberAccountsRequest` requests, specify the value of `NextToken` from the previous response to get information about another batch of member account IDs.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "MemberAccounts": [ "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.

MemberAccounts (p. 50)

An array of account IDs.

Type: Array of strings

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

Pattern: `^[0-9]+$`

NextToken (p. 50)

If you have more member account IDs than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more IDs, submit another `ListMemberAccounts` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

- AWS SDK for JavaScript
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListPolicies

Returns an array of `PolicySummary` objects.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

MaxResults (p. 53)

Specifies the number of `PolicySummary` objects that you want AWS Firewall Manager to return for this request. If you have more `PolicySummary` objects than the number that you specify for `MaxResults`, the response includes a `NextToken` value that you can use to get another batch of `PolicySummary` objects.

Type: Integer

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

Required: No

NextToken (p. 53)

If you specify a value for `MaxResults` and you have more `PolicySummary` objects than the number that you specify for `MaxResults`, AWS Firewall Manager returns a `NextToken` value in the response that allows you to list another group of `PolicySummary` objects. For the second and subsequent `ListPolicies` requests, specify the value of `NextToken` from the previous response to get information about another batch of `PolicySummary` objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "PolicyList": [
      {
         "DeleteUnusedFMManagedResources": boolean,
         "PolicyArn": "string",
         "PolicyId": "string",
         "PolicyName": "string",
         "RemediationEnabled": boolean,
         "ResourceType": "string",
         "SecurityServiceType": "string"
      }
   ]
}
```

Response Elements

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

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

NextToken (p. 53)

If you have more `PolicySummary` objects than the number that you specified for `MaxResults` in the request, the response includes a `NextToken` value. To list more `PolicySummary` objects, submit another `ListPolicies` request, and specify the `NextToken` value from the response in the `NextToken` value in the next request.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

PolicyList (p. 53)

An array of `PolicySummary` objects.

Type: Array of PolicySummary (p. 138) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

ListProtocolsLists

Returns an array of `ProtocolsListDataSummary` objects.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

DefaultLists (p. 56)

Specifies whether the lists to retrieve are default lists owned by AWS Firewall Manager.

Type: Boolean

Required: No

MaxResults (p. 56)

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

If you don't specify this, AWS Firewall Manager returns all available objects.

Type: Integer

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

Required: Yes

NextToken (p. 56)

If you specify a value for `MaxResults` in your list request, and you have more objects than the maximum, AWS Firewall Manager returns this token in the response. For all but the first request, you provide the token returned by the prior request in the request parameters, to retrieve the next batch of objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "ProtocolsLists": [
      {
         "ListArn": "string",
         "ListId": "string",
         "ListName": "string",
         "ProtocolsList": [ "string" ]
      }
   ]
}
```

Response Elements

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

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

NextToken (p. 56)

If you specify a value for `MaxResults` in your list request, and you have more objects than the maximum, AWS Firewall Manager returns this token in the response. You can use this token in subsequent requests to retrieve the next batch of objects.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

ProtocolsLists (p. 56)

An array of `ProtocolsListDataSummary` objects.

Type: Array of ProtocolsListDataSummary (p. 144) objects

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

ListTagsForResource

Retrieves the list of tags for the specified AWS resource.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ResourceArn (p. 59)

The Amazon Resource Name (ARN) of the resource to return tags for. The AWS Firewall Manager resources that support tagging are policies, applications lists, and protocols lists.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Syntax

```
{
   "TagList": [
      {
         "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.

TagList (p. 59)

The tags associated with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

PutAppsList

Creates an AWS Firewall Manager applications list.

Request Syntax

```
{
   "AppsList": {
      "AppsList": [
         {
            "AppName": "string",
            "Port": number,
            "Protocol": "string"
         }
      ],
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousAppsList": {
         "string" : [
            {
               "AppName": "string",
               "Port": number,
               "Protocol": "string"
            }
         ]
      }
   },
   "TagList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

AppsList (p. 61)

The details of the AWS Firewall Manager applications list to be created.

Type: AppsListData (p. 81) object

Required: Yes

TagList (p. 61)

The tags associated with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
   "AppsList": {
      "AppsList": [
         {
            "AppName": "string",
            "Port": number,
            "Protocol": "string"
         }
      ],
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousAppsList": {
         "string" : [
            {
               "AppName": "string",
               "Port": number,
               "Protocol": "string"
            }
         ]
      }
   },
   "AppsListArn": "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.

AppsList (p. 62)

The details of the AWS Firewall Manager applications list.

Type: AppsListData (p. 81) object

AppsListArn (p. 62)

The Amazon Resource Name (ARN) of the applications list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

PutNotificationChannel

Designates the IAM role and Amazon Simple Notification Service (SNS) topic that Firewall Manager uses to record SNS logs.

To perform this action outside of the console, you must configure the SNS topic to allow the Firewall Manager role `AWSServiceRoleForFMS` to publish SNS logs. For more information, see Firewall Manager required permissions for API actions in the *AWS Firewall Manager Developer Guide*.

Request Syntax

```
{
   "SnsRoleName": "string",
   "SnsTopicArn": "string"
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

SnsRoleName (p. 64)

The Amazon Resource Name (ARN) of the IAM role that allows Amazon SNS to record AWS Firewall Manager activity.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

SnsTopicArn (p. 64)

The Amazon Resource Name (ARN) of the SNS topic that collects notifications from AWS Firewall Manager.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

PutPolicy

Creates an AWS Firewall Manager policy.

Firewall Manager provides the following types of policies:

- An AWS WAF policy (type WAFV2), which defines rule groups to run first in the corresponding AWS WAF web ACL and rule groups to run last in the web ACL.
- An AWS WAF Classic policy (type WAF), which defines a rule group.
- A Shield Advanced policy, which applies Shield Advanced protection to specified accounts and resources.
- A security group policy, which manages VPC security groups across your AWS organization.
- An AWS Network Firewall policy, which provides firewall rules to filter network traffic in specified Amazon VPCs.
- A DNS Firewall policy, which provides Amazon Route 53 Resolver DNS Firewall rules to filter DNS queries for specified VPCs.

Each policy is specific to one of the types. If you want to enforce more than one policy type across accounts, create multiple policies. You can create multiple policies for each type.

You must be subscribed to Shield Advanced to create a Shield Advanced policy. For more information about subscribing to Shield Advanced, see CreateSubscription.

Request Syntax

```
{
   "Policy": {
      "DeleteUnusedFMManagedResources": boolean,
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceTypeList": [ "string" ],
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   },
   "TagList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

Policy (p. 66)

The details of the AWS Firewall Manager policy to be created.

Type: Policy (p. 130) object

Required: Yes

TagList (p. 66)

The tags to add to the AWS resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
   "Policy": {
      "DeleteUnusedFMManagedResources": boolean,
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceTypeList": [ "string" ],
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "Type": "string"
      }
   },
   "PolicyArn": "string"
}
```

Response Elements

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

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

Policy (p. 67)

The details of the AWS Firewall Manager policy.

Type: Policy (p. 130) object

PolicyArn (p. 67)

The Amazon Resource Name (ARN) of the policy.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

InvalidTypeException

The value of the `Type` parameter is invalid.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

PutProtocolsList

Creates an AWS Firewall Manager protocols list.

Request Syntax

```
{
   "ProtocolsList": {
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousProtocolsList": {
         "string" : [ "string" ]
      },
      "ProtocolsList": [ "string" ]
   },
   "TagList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ProtocolsList (p. 70)

The details of the AWS Firewall Manager protocols list to be created.

Type: ProtocolsListData (p. 142) object

Required: Yes

TagList (p. 70)

The tags associated with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

Response Syntax

```
{
   "ProtocolsList": {
      "CreateTime": number,
      "LastUpdateTime": number,
      "ListId": "string",
      "ListName": "string",
      "ListUpdateToken": "string",
      "PreviousProtocolsList": { 
         "string" : [ "string" ]
      },
      "ProtocolsList": [ "string" ]
   },
   "ProtocolsListArn": "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.

ProtocolsList (p. 70)

The details of the AWS Firewall Manager protocols list.

Type: ProtocolsListData (p. 142) object

ProtocolsListArn (p. 70)

The Amazon Resource Name (ARN) of the protocols list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

TagResource

Adds one or more tags to an AWS resource.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ResourceArn (p. 73)

The Amazon Resource Name (ARN) of the resource to return tags for. The AWS Firewall Manager resources that support tagging are policies, applications lists, and protocols lists.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

TagList (p. 73)

The tags to add to the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

LimitExceededException

The operation exceeds a resource limit, for example, the maximum number of `policy` objects that you can create for an AWS account. For more information, see Firewall Manager Limits in the *AWS WAF Developer Guide*.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

UntagResource

Removes one or more tags from an AWS resource.

Request Syntax

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

Request Parameters

For information about the parameters that are common to all actions, see Common Parameters (p. 165).

The request accepts the following data in JSON format.

ResourceArn (p. 75)

The Amazon Resource Name (ARN) of the resource to return tags for. The AWS Firewall Manager resources that support tagging are policies, applications lists, and protocols lists.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

TagKeys (p. 75)

The keys of the tags to remove from the resource.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 200 items.

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Response Elements

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

Errors

For information about the errors that are common to all actions, see Common Errors (p. 167).

InternalErrorException

The operation failed because of a system problem, even though the request was valid. Retry your request.

HTTP Status Code: 400

InvalidInputException

The parameters of the request were invalid.

HTTP Status Code: 400

InvalidOperationException

The operation failed because there was nothing to do or the operation wasn't possible. For example, you might have submitted an `AssociateAdminAccount` request for an account ID that was already set as the AWS Firewall Manager administrator. Or you might have tried to access a Region that's disabled by default, and that you need to enable for the Firewall Manager administrator account and for AWS Organizations before you can access it.

HTTP Status Code: 400

ResourceNotFoundException

The specified resource was not found.

HTTP Status Code: 400

See Also

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

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

Data Types

The AWS Firewall Manager 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:

- PolicySummary (p. 138)
- PossibleRemediationAction (p. 140)
- PossibleRemediationActions (p. 141)
- ProtocolsListData (p. 142)
- ProtocolsListDataSummary (p. 144)
- RemediationAction (p. 146)
- RemediationActionWithOrder (p. 148)
- ResourceTag (p. 149)
- ResourceViolation (p. 150)
- Route (p. 153)
- SecurityGroupRemediationAction (p. 154)
- SecurityGroupRuleDescription (p. 155)
- SecurityServicePolicyData (p. 157)
- StatefulRuleGroup (p. 160)
- StatelessRuleGroup (p. 161)
- Tag (p. 162)
- ViolationDetail (p. 163)

ActionTarget

Describes a remediation action target.

Contents

Description

A description of the remediation action target.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

ResourceId

The ID of the remediation target.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

App

An individual AWS Firewall Manager application.

Contents

AppName

The application's name.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Port

The application's port number, for example `80`.

Type: Long

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: Yes

Protocol

The IP protocol name or number. The name can be one of `tcp`, `udp`, or `icmp`. For information on possible numbers, see Protocol Numbers.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 20.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AppsListData

An AWS Firewall Manager applications list.

Contents

AppsList

An array of applications in the AWS Firewall Manager applications list.

Type: Array of App (p. 80) objects

Required: Yes

CreateTime

The time that the AWS Firewall Manager applications list was created.

Type: Timestamp

Required: No

LastUpdateTime

The time that the AWS Firewall Manager applications list was last updated.

Type: Timestamp

Required: No

ListId

The ID of the AWS Firewall Manager applications list.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

ListName

The name of the AWS Firewall Manager applications list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ListUpdateToken

A unique identifier for each update to the list. When you update the list, the update token must match the token of the current version of the application list. You can retrieve the update token by getting the list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PreviousAppsList

A map of previous version numbers to their corresponding `App` object arrays.

Type: String to array of App (p. 80) objects map

Key Length Constraints: Minimum length of 1. Maximum length of 2.

Key Pattern: `^\d{1,2}$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AppsListDataSummary

Details of the AWS Firewall Manager applications list.

Contents

AppsList

An array of `App` objects in the AWS Firewall Manager applications list.

Type: Array of App (p. 80) objects

Required: No

ListArn

The Amazon Resource Name (ARN) of the applications list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ListId

The ID of the applications list.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

ListName

The name of the applications list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AwsEc2InstanceViolation

Violation detail for an EC2 instance resource.

Contents

AwsEc2NetworkInterfaceViolations

Violation detail for network interfaces associated with the EC2 instance.

Type: Array of AwsEc2NetworkInterfaceViolation (p. 86) objects

Required: No

ViolationTarget

The resource ID of the EC2 instance.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AwsEc2NetworkInterfaceViolation

Violation detail for network interfaces associated with an EC2 instance.

Contents

ViolatingSecurityGroups

List of security groups that violate the rules specified in the primary security group of the AWS Firewall Manager policy.

Type: Array of strings

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolationTarget

The resource ID of the network interface.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

AwsVPCSecurityGroupViolation

Violation detail for the rule violation in a security group when compared to the primary security group of the AWS Firewall Manager policy.

Contents

PartialMatches

List of rules specified in the security group of the AWS Firewall Manager policy that partially match the `ViolationTarget` rule.

Type: Array of PartialMatch (p. 129) objects

Required: No

PossibleSecurityGroupRemediationActions

Remediation options for the rule specified in the `ViolationTarget`.

Type: Array of SecurityGroupRemediationAction (p. 154) objects

Required: No

ViolationTarget

The security group rule that is being evaluated.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

ViolationTargetDescription

A description of the security group that violates the policy.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ComplianceViolator

Details of the resource that is not protected by the policy.

Contents

ResourceId

The resource ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ResourceType

The resource type. This is in the format shown in the AWS Resource Types Reference. For example: `AWS::ElasticLoadBalancingV2::LoadBalancer`, `AWS::CloudFront::Distribution`, or `AWS::NetworkFirewall::FirewallPolicy`.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolationReason

The reason that the resource is not protected by the policy.

Type: String

Valid Values: `WEB_ACL_MISSING_RULE_GROUP | RESOURCE_MISSING_WEB_ACL | RESOURCE_INCORRECT_WEB_ACL | RESOURCE_MISSING_SHIELD_PROTECTION | RESOURCE_MISSING_WEB_ACL_OR_SHIELD_PROTECTION | RESOURCE_MISSING_SECURITY_GROUP | RESOURCE_VIOLATES_AUDIT_SECURITY_GROUP | SECURITY_GROUP_UNUSED | SECURITY_GROUP_REDUNDANT | FMS_CREATED_SECURITY_GROUP_EDITED | MISSING_FIREWALL | MISSING_FIREWALL_SUBNET_IN_AZ | MISSING_EXPECTED_ROUTE_TABLE | NETWORK_FIREWALL_POLICY_MODIFIED | INTERNET_GATEWAY_MISSING_EXPECTED_ROUTE | FIREWALL_SUBNET_MISSING_EXPECTED_ROUTE | UNEXPECTED_FIREWALL_ROUTES | UNEXPECTED_TARGET_GATEWAY_ROUTES | TRAFFIC_INSPECTION_CROSSES_AZ_BOUNDARY | INVALID_ROUTE_CONFIGURATION | MISSING_TARGET_GATEWAY | INTERNET_TRAFFIC_NOT_INSPECTED | BLACK_HOLE_ROUTE_DETECTED | BLACK_HOLE_ROUTE_DETECTED_IN_FIREWALL_SUBNET | RESOURCE_MISSING_DNS_FIREWALL`

Required: No

See Also

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

- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DnsDuplicateRuleGroupViolation

A DNS Firewall rule group that Firewall Manager tried to associate with a VPC is already associated with the VPC and can't be associated again.

Contents

ViolationTarget

Information about the VPC ID.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

ViolationTargetDescription

A description of the violation that specifies the rule group and VPC.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DnsRuleGroupLimitExceededViolation

The VPC that Firewall Manager was applying a DNS Fireall policy to reached the limit for associated DNS Firewall rule groups. Firewall Manager tried to associate another rule group with the VPC and failed due to the limit.

Contents

NumberOfRuleGroupsAlreadyAssociated

The number of rule groups currently associated with the VPC.

Type: Integer

Valid Range: Minimum value of -2147483648. Maximum value of 2147483647.

Required: No

ViolationTarget

Information about the VPC ID.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

ViolationTargetDescription

A description of the violation that specifies the rule group and VPC.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

DnsRuleGroupPriorityConflictViolation

A rule group that Firewall Manager tried to associate with a VPC has the same priority as a rule group that's already associated.

Contents

ConflictingPolicyId

The ID of the Firewall Manager DNS Firewall policy that was already applied to the VPC. This policy contains the rule group that's already associated with the VPC.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

ConflictingPriority

The priority setting of the two conflicting rule groups.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 10000.

Required: No

UnavailablePriorities

The priorities of rule groups that are already associated with the VPC. To retry your operation, choose priority settings that aren't in this list for the rule groups in your new DNS Firewall policy.

Type: Array of integers

Valid Range: Minimum value of 0. Maximum value of 10000.

Required: No

ViolationTarget

Information about the VPC ID.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

ViolationTargetDescription

A description of the violation that specifies the VPC and the rule group that's already associated with it.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2AssociateRouteTableAction

The action of associating an EC2 resource, such as a subnet or internet gateway, with a route table.

Contents

Description

A description of the EC2 route table that is associated with the remediation action.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

GatewayId

The ID of the gateway to be used with the EC2 route table that is associated with the remediation action.

Type: ActionTarget (p. 79) object

Required: No

RouteTableId

The ID of the EC2 route table that is associated with the remediation action.

Type: ActionTarget (p. 79) object

Required: Yes

SubnetId

The ID of the subnet for the EC2 route table that is associated with the remediation action.

Type: ActionTarget (p. 79) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2CopyRouteTableAction

An action that copies the EC2 route table for use in remediation.

Contents

Description

A description of the copied EC2 route table that is associated with the remediation action.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

RouteTableId

The ID of the copied EC2 route table that is associated with the remediation action.

Type: ActionTarget (p. 79) object

Required: Yes

VpcId

The VPC ID of the copied EC2 route table that is associated with the remediation action.

Type: ActionTarget (p. 79) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2CreateRouteAction

Information about the CreateRoute action in Amazon EC2.

Contents

Description

A description of CreateRoute action in Amazon EC2.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

DestinationCidrBlock

Information about the IPv4 CIDR address block used for the destination match.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationIpv6CidrBlock

Information about the IPv6 CIDR block destination.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationPrefixListId

Information about the ID of a prefix list used for the destination match.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

GatewayId

Information about the ID of an internet gateway or virtual private gateway attached to your VPC.

Type: ActionTarget (p. 79) object

Required: No

RouteTableId

Information about the ID of the route table for the route.

Type: ActionTarget (p. 79) object

Required: Yes

VpcEndpointId

Information about the ID of a VPC endpoint. Supported for Gateway Load Balancer endpoints only.

Type: ActionTarget (p. 79) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2CreateRouteTableAction

Information about the CreateRouteTable action in Amazon EC2.

Contents

Description

A description of the CreateRouteTable action.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

VpcId

Information about the ID of a VPC.

Type: ActionTarget (p. 79) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2DeleteRouteAction

Information about the DeleteRoute action in Amazon EC2.

Contents

Description

A description of the DeleteRoute action.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

DestinationCidrBlock

Information about the IPv4 CIDR range for the route. The value you specify must match the CIDR for the route exactly.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationIpv6CidrBlock

Information about the IPv6 CIDR range for the route. The value you specify must match the CIDR for the route exactly.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationPrefixListId

Information about the ID of the prefix list for the route.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RouteTableId

Information about the ID of the route table.

Type: ActionTarget (p. 79) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2ReplaceRouteAction

Information about the ReplaceRoute action in Amazon EC2.

Contents

Description

A description of the ReplaceRoute action in Amazon EC2.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

DestinationCidrBlock

Information about the IPv4 CIDR address block used for the destination match. The value that you provide must match the CIDR of an existing route in the table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationIpv6CidrBlock

Information about the IPv6 CIDR address block used for the destination match. The value that you provide must match the CIDR of an existing route in the table.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

DestinationPrefixListId

Information about the ID of the prefix list for the route.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

GatewayId

Information about the ID of an internet gateway or virtual private gateway.

Type: ActionTarget (p. 79) object

Required: No

RouteTableId

Information about the ID of the route table.

Type: ActionTarget (p. 79) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EC2ReplaceRouteTableAssociationAction

Information about the ReplaceRouteTableAssociation action in Amazon EC2.

Contents

AssociationId

Information about the association ID.

Type: ActionTarget (p. 79) object

Required: Yes

Description

A description of the ReplaceRouteTableAssociation action in Amazon EC2.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

RouteTableId

Information about the ID of the new route table to associate with the subnet.

Type: ActionTarget (p. 79) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

EvaluationResult

Describes the compliance status for the account. An account is considered noncompliant if it includes resources that are not protected by the specified policy or that don't comply with the policy.

Contents

ComplianceStatus

Describes an AWS account's compliance with the AWS Firewall Manager policy.

Type: String

Valid Values: `COMPLIANT | NON_COMPLIANT`

Required: No

EvaluationLimitExceeded

Indicates that over 100 resources are noncompliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

ViolatorCount

The number of resources that are noncompliant with the specified policy. For AWS WAF and Shield Advanced policies, a resource is considered noncompliant if it is not associated with the policy. For security group policies, a resource is considered noncompliant if it doesn't comply with the rules of the policy and remediation is disabled or not possible.

Type: Long

Valid Range: Minimum value of 0.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ExpectedRoute

Information about the expected route in the route table.

Contents

AllowedTargets

Information about the allowed targets.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

ContributingSubnets

Information about the contributing subnets.

Type: Array of strings

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

IpV4Cidr

Information about the IPv4 CIDR block.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

IpV6Cidr

Information about the IPv6 CIDR block.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

PrefixListId

Information about the ID of the prefix list for the route.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

RouteTableId

Information about the route table ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallBlackHoleRouteDetectedViolation

Violation detail for an internet gateway route with an inactive state in the customer subnet route table or Network Firewall subnet route table.

Contents

RouteTableId

Information about the route table ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolatingRoutes

Information about the route or routes that are in violation.

Type: Array of Route (p. 153) objects

Required: No

ViolationTarget

The subnet that has an inactive state.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallInternetTrafficNotInspectedViolation

Violation detail for the subnet for which internet traffic that hasn't been inspected.

Contents

ActualFirewallSubnetRoutes

The actual firewall subnet routes.

Type: Array of Route (p. 153) objects

Required: No

ActualInternetGatewayRoutes

The actual internet gateway routes.

Type: Array of Route (p. 153) objects

Required: No

CurrentFirewallSubnetRouteTable

Information about the subnet route table for the current firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

CurrentInternetGatewayRouteTable

The current route table for the internet gateway.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedFirewallEndpoint

The expected endpoint for the current firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedFirewallSubnetRoutes

The firewall subnet routes that are expected.

Type: Array of ExpectedRoute (p. 105) objects

Required: No

ExpectedInternetGatewayRoutes

The internet gateway routes that are expected.

Type: Array of ExpectedRoute (p. 105) objects

Required: No

FirewallSubnetId

The firewall subnet ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

InternetGatewayId

The internet gateway ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

IsRouteTableUsedInDifferentAZ

Information about whether the route table is used in another Availability Zone.

Type: Boolean

Required: No

RouteTableId

Information about the route table ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

SubnetAvailabilityZone

The subnet Availability Zone.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

SubnetId

The subnet ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolatingRoutes

The route or routes that are in violation.

Type: Array of Route (p. 153) objects

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallInvalidRouteConfigurationViolation

Violation detail for the improperly configured subnet route. It's possible there is a missing route table route, or a configuration that causes traffic to cross an Availability Zone boundary.

Contents

ActualFirewallEndpoint

The actual firewall endpoint.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ActualFirewallSubnetId

The actual subnet ID for the firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ActualFirewallSubnetRoutes

The actual firewall subnet routes that are expected.

Type: Array of Route (p. 153) objects

Required: No

ActualInternetGatewayRoutes

The actual internet gateway routes.

Type: Array of Route (p. 153) objects

Required: No

AffectedSubnets

The subnets that are affected.

Type: Array of strings

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

CurrentFirewallSubnetRouteTable

The subnet route table for the current firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

CurrentInternetGatewayRouteTable

The route table for the current internet gateway.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedFirewallEndpoint

The firewall endpoint that's expected.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedFirewallSubnetId

The expected subnet ID for the firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedFirewallSubnetRoutes

The firewall subnet routes that are expected.

Type: Array of ExpectedRoute (p. 105) objects

Required: No

ExpectedInternetGatewayRoutes

The expected routes for the internet gateway.

Type: Array of ExpectedRoute (p. 105) objects

Required: No

InternetGatewayId

The internet gateway ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

IsRouteTableUsedInDifferentAZ

Information about whether the route table is used in another Availability Zone.

Type: Boolean

Required: No

RouteTableId

The route table ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolatingRoute

The route that's in violation.

Type: Route (p. 153) object

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallMissingExpectedRoutesViolation

Violation detail for an expected route missing in AWS Network Firewall.

Contents

ExpectedRoutes

The expected routes.

Type: Array of ExpectedRoute (p. 105) objects

Required: No

ViolationTarget

The target of the violation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallMissingExpectedRTViolation

Violation detail for AWS Network Firewall for a subnet that's not associated to the expected Firewall Manager managed route table.

Contents

AvailabilityZone

The Availability Zone of a violating subnet.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

CurrentRouteTable

The resource ID of the current route table that's associated with the subnet, if one is available.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExpectedRouteTable

The resource ID of the route table that should be associated with the subnet.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolationTarget

The ID of the AWS Network Firewall or VPC resource that's in violation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

VPC

The resource ID of the VPC associated with a violating subnet.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallMissingFirewallViolation

Violation detail for AWS Network Firewall for a subnet that doesn't have a Firewall Manager managed firewall in its VPC.

Contents

AvailabilityZone

The Availability Zone of a violating subnet.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

TargetViolationReason

The reason the resource has this violation, if one is available.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `\w+`

Required: No

ViolationTarget

The ID of the AWS Network Firewall or VPC resource that's in violation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

VPC

The resource ID of the VPC associated with a violating subnet.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallMissingSubnetViolation

Violation detail for AWS Network Firewall for an Availability Zone that's missing the expected Firewall Manager managed subnet.

Contents

AvailabilityZone

The Availability Zone of a violating subnet.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

TargetViolationReason

The reason the resource has this violation, if one is available.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `\w+`

Required: No

ViolationTarget

The ID of the AWS Network Firewall or VPC resource that's in violation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

VPC

The resource ID of the VPC associated with a violating subnet.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallPolicyDescription

The definition of the AWS Network Firewall firewall policy.

Contents

StatefulRuleGroups

The stateful rule groups that are used in the Network Firewall firewall policy.

Type: Array of StatefulRuleGroup (p. 160) objects

Required: No

StatelessCustomActions

Names of custom actions that are available for use in the stateless default actions settings.

Type: Array of strings

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

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

Required: No

StatelessDefaultActions

The actions to take on packets that don't match any of the stateless rule groups.

Type: Array of strings

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

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

Required: No

StatelessFragmentDefaultActions

The actions to take on packet fragments that don't match any of the stateless rule groups.

Type: Array of strings

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

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

Required: No

StatelessRuleGroups

The stateless rule groups that are used in the Network Firewall firewall policy.

Type: Array of StatelessRuleGroup (p. 161) objects

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallPolicyModifiedViolation

Violation detail for AWS Network Firewall for a firewall policy that has a different NetworkFirewallPolicyDescription (p. 122) than is required by the Firewall Manager policy.

Contents

CurrentPolicyDescription

The policy that's currently in use in the individual account.

Type: NetworkFirewallPolicyDescription (p. 122) object

Required: No

ExpectedPolicyDescription

The policy that should be in use in the individual account in order to be compliant.

Type: NetworkFirewallPolicyDescription (p. 122) object

Required: No

ViolationTarget

The ID of the AWS Network Firewall or VPC resource that's in violation.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallUnexpectedFirewallRoutesViolation

Violation detail for an unexpected route that's present in a route table.

Contents

FirewallEndpoint

The endpoint of the firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

FirewallSubnetId

The subnet ID for the firewall.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RouteTableId

The ID of the route table.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolatingRoutes

The routes that are in violation.

Type: Array of Route (p. 153) objects

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

NetworkFirewallUnexpectedGatewayRoutesViolation

Violation detail for an unexpected gateway route that's present in a route table.

Contents

GatewayId

Information about the gateway ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RouteTableId

Information about the route table.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ViolatingRoutes

The routes that are in violation.

Type: Array of Route (p. 153) objects

Required: No

VpcId

Information about the VPC ID.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PartialMatch

The reference rule that partially matches the `ViolationTarget` rule and violation reason.

Contents

Reference

The reference rule from the primary security group of the AWS Firewall Manager policy.

Type: String

Required: No

TargetViolationReasons

The violation reason.

Type: Array of strings

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `\w+`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Policy

An AWS Firewall Manager policy.

Contents

DeleteUnusedFMManagedResources

Indicates whether AWS Firewall Manager should automatically remove protections from resources that leave the policy scope and clean up resources that Firewall Manager is managing for accounts when those accounts leave policy scope. For example, Firewall Manager will disassociate a Firewall Manager managed web ACL from a protected customer resource when the customer resource leaves policy scope.

By default, Firewall Manager doesn't remove protections or delete Firewall Manager managed resources.

This option is not available for Shield Advanced or AWS WAF Classic policies.

Type: Boolean

Required: No

ExcludeMap

Specifies the AWS account IDs and AWS Organizations organizational units (OUs) to exclude from the policy. Specifying an OU is the equivalent of specifying all accounts in the OU and in any of its child OUs, including any child OUs and accounts that are added at a later time.

You can specify inclusions or exclusions, but not both. If you specify an `IncludeMap`, AWS Firewall Manager applies the policy to all accounts specified by the `IncludeMap`, and does not evaluate any `ExcludeMap` specifications. If you do not specify an `IncludeMap`, then Firewall Manager applies the policy to all accounts except for those specified by the `ExcludeMap`.

You can specify account IDs, OUs, or a combination:

- Specify account IDs by setting the key to `ACCOUNT`. For example, the following is a valid map: `{“ACCOUNT” : [“accountID1”, “accountID2”]}`.
- Specify OUs by setting the key to `ORG_UNIT`. For example, the following is a valid map: `{“ORG_UNIT” : [“ouid111”, “ouid112”]}`.
- Specify accounts and OUs together in a single map, separated with a comma. For example, the following is a valid map: `{“ACCOUNT” : [“accountID1”, “accountID2”], “ORG_UNIT” : [“ouid111”, “ouid112”]}`.

Type: String to array of strings map

Valid Keys: `ACCOUNT | ORG_UNIT`

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ExcludeResourceTags

If set to `True`, resources with the tags that are specified in the `ResourceTag` array are not in scope of the policy. If set to `False`, and the `ResourceTag` array is not null, only resources with the specified tags are in scope of the policy.

Type: Boolean

Required: Yes

IncludeMap

Specifies the AWS account IDs and AWS Organizations organizational units (OUs) to include in the policy. Specifying an OU is the equivalent of specifying all accounts in the OU and in any of its child OUs, including any child OUs and accounts that are added at a later time.

You can specify inclusions or exclusions, but not both. If you specify an `IncludeMap`, AWS Firewall Manager applies the policy to all accounts specified by the `IncludeMap`, and does not evaluate any `ExcludeMap` specifications. If you do not specify an `IncludeMap`, then Firewall Manager applies the policy to all accounts except for those specified by the `ExcludeMap`.

You can specify account IDs, OUs, or a combination:

- Specify account IDs by setting the key to `ACCOUNT`. For example, the following is a valid map: `{“ACCOUNT” : [“accountID1”, “accountID2”]}`.
- Specify OUs by setting the key to `ORG_UNIT`. For example, the following is a valid map: `{“ORG_UNIT” : [“ouid111”, “ouid112”]}`.
- Specify accounts and OUs together in a single map, separated with a comma. For example, the following is a valid map: `{“ACCOUNT” : [“accountID1”, “accountID2”], “ORG_UNIT” : [“ouid111”, “ouid112”]}`.

Type: String to array of strings map

Valid Keys: `ACCOUNT | ORG_UNIT`

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

PolicyName

The name of the AWS Firewall Manager policy.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

PolicyUpdateToken

A unique identifier for each update to the policy. When issuing a `PutPolicy` request, the `PolicyUpdateToken` in the request must match the `PolicyUpdateToken` of the current policy version. To get the `PolicyUpdateToken` of the current policy version, use a `GetPolicy` request.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RemediationEnabled

Indicates if the policy should be automatically applied to new resources.

Type: Boolean

Required: Yes

ResourceTags

An array of `ResourceTag` objects.

Type: Array of ResourceTag (p. 149) objects

Array Members: Minimum number of 0 items. Maximum number of 8 items.

Required: No

ResourceType

The type of resource protected by or in scope of the policy. This is in the format shown in the AWS Resource Types Reference. To apply this policy to multiple resource types, specify a resource type of `ResourceTypeList` and then specify the resource types in a `ResourceTypeList`.

For AWS WAF and Shield Advanced, example resource types include `AWS::ElasticLoadBalancingV2::LoadBalancer` and `AWS::CloudFront::Distribution`. For a security group common policy, valid values are `AWS::EC2::NetworkInterface` and `AWS::EC2::Instance`. For a security group content audit policy, valid values are `AWS::EC2::SecurityGroup`, `AWS::EC2::NetworkInterface`, and `AWS::EC2::Instance`. For a security group usage audit policy, the value is `AWS::EC2::SecurityGroup`. For an AWS Network Firewall policy or DNS Firewall policy, the value is `AWS::EC2::VPC`.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ResourceTypeList

An array of `ResourceType` objects. Use this only to specify multiple resource types. To specify a single resource type, use `ResourceType`.

Type: Array of strings

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

SecurityServicePolicyData

Details about the security service that is being used to protect the resources.

Type: SecurityServicePolicyData (p. 157) object

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyComplianceDetail

Describes the noncompliant resources in a member account for a specific AWS Firewall Manager policy. A maximum of 100 entries are displayed. If more than 100 resources are noncompliant, `EvaluationLimitExceeded` is set to `True`.

Contents

EvaluationLimitExceeded

Indicates if over 100 resources are noncompliant with the AWS Firewall Manager policy.

Type: Boolean

Required: No

ExpiredAt

A timestamp that indicates when the returned information should be considered out of date.

Type: Timestamp

Required: No

IssueInfoMap

Details about problems with dependent services, such as AWS WAF or AWS Config, and the error message received that indicates the problem with the service.

Type: String to string map

Valid Keys: `AWSCONFIG | AWSWAF | AWSSHIELD_ADVANCED | AWSVPC`

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

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=,+\-@]*)$`

Required: No

MemberAccount

The AWS account ID.

Type: String

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

Pattern: `^[0-9]+$`

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

PolicyOwner

The AWS account that created the AWS Firewall Manager policy.

Type: String

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

Pattern: `^[0-9]+$`

Required: No

Violators

An array of resources that aren't protected by the AWS WAF or Shield Advanced policy or that aren't in compliance with the security group policy.

Type: Array of ComplianceViolator (p. 88) objects

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicyComplianceStatus

Indicates whether the account is compliant with the specified policy. An account is considered noncompliant if it includes resources that are not protected by the policy, for AWS WAF and Shield Advanced policies, or that are noncompliant with the policy, for security group policies.

Contents

EvaluationResults

An array of `EvaluationResult` objects.

Type: Array of EvaluationResult (p. 104) objects

Required: No

IssueInfoMap

Details about problems with dependent services, such as AWS WAF or AWS Config, and the error message received that indicates the problem with the service.

Type: String to string map

Valid Keys: `AWSCONFIG | AWSWAF | AWSSHIELD_ADVANCED | AWSVPC`

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

Value Pattern: `^([\p{L}\p{Z}\p{N}_.:/=,+\-@]*)$`

Required: No

LastUpdated

Timestamp of the last update to the `EvaluationResult` objects.

Type: Timestamp

Required: No

MemberAccount

The member account ID.

Type: String

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

Pattern: `^[0-9]+$`

Required: No

PolicyId

The ID of the AWS Firewall Manager policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

PolicyName

The name of the AWS Firewall Manager policy.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PolicyOwner

The AWS account that created the AWS Firewall Manager policy.

Type: String

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

Pattern: `^[0-9]+$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PolicySummary

Details of the AWS Firewall Manager policy.

Contents

DeleteUnusedFMManagedResources

Indicates whether AWS Firewall Manager should automatically remove protections from resources that leave the policy scope and clean up resources that Firewall Manager is managing for accounts when those accounts leave policy scope. For example, Firewall Manager will disassociate a Firewall Manager managed web ACL from a protected customer resource when the customer resource leaves policy scope.

By default, Firewall Manager doesn't remove protections or delete Firewall Manager managed resources.

This option is not available for Shield Advanced or AWS WAF Classic policies.

Type: Boolean

Required: No

PolicyArn

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

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PolicyId

The ID of the specified policy.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

PolicyName

The name of the specified policy.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RemediationEnabled

Indicates if the policy should be automatically applied to new resources.

Type: Boolean

Required: No

ResourceType

The type of resource protected by or in scope of the policy. This is in the format shown in the AWS Resource Types Reference. For AWS WAF and Shield Advanced, examples include `AWS::ElasticLoadBalancingV2::LoadBalancer` and `AWS::CloudFront::Distribution`. For a security group common policy, valid values are `AWS::EC2::NetworkInterface` and `AWS::EC2::Instance`. For a security group content audit policy, valid values are `AWS::EC2::SecurityGroup`, `AWS::EC2::NetworkInterface`, and `AWS::EC2::Instance`. For a security group usage audit policy, the value is `AWS::EC2::SecurityGroup`. For an AWS Network Firewall policy or DNS Firewall policy, the value is `AWS::EC2::VPC`.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

SecurityServiceType

The service that the policy is using to protect the resources. This specifies the type of policy that is created, either an AWS WAF policy, a Shield Advanced policy, or a security group policy.

Type: String

Valid Values: `WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON | SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT | NETWORK_FIREWALL | DNS_FIREWALL`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PossibleRemediationAction

A list of remediation actions.

Contents

Description

A description of the list of remediation actions.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

IsDefaultAction

Information about whether an action is taken by default.

Type: Boolean

Required: No

OrderedRemediationActions

The ordered list of remediation actions.

Type: Array of RemediationActionWithOrder (p. 148) objects

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

PossibleRemediationActions

A list of possible remediation action lists. Each individual possible remediation action is a list of individual remediation actions.

Contents

Actions

Information about the actions.

Type: Array of PossibleRemediationAction (p. 140) objects

Required: No

Description

A description of the possible remediation actions list.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtocolsListData

An AWS Firewall Manager protocols list.

Contents

CreateTime

The time that the AWS Firewall Manager protocols list was created.

Type: Timestamp

Required: No

LastUpdateTime

The time that the AWS Firewall Manager protocols list was last updated.

Type: Timestamp

Required: No

ListId

The ID of the AWS Firewall Manager protocols list.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

ListName

The name of the AWS Firewall Manager protocols list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ListUpdateToken

A unique identifier for each update to the list. When you update the list, the update token must match the token of the current version of the application list. You can retrieve the update token by getting the list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

PreviousProtocolsList

A map of previous version numbers to their corresponding protocol arrays.

Type: String to array of strings map

Key Length Constraints: Minimum length of 1. Maximum length of 2.

Key Pattern: `^\d{1,2}$`

Length Constraints: Minimum length of 1. Maximum length of 20.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ProtocolsList

An array of protocols in the AWS Firewall Manager protocols list.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 20.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ProtocolsListDataSummary

Details of the AWS Firewall Manager protocols list.

Contents

ListArn

The Amazon Resource Name (ARN) of the specified protocols list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ListId

The ID of the specified protocols list.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: No

ListName

The name of the specified protocols list.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

ProtocolsList

An array of protocols in the AWS Firewall Manager protocols list.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 20.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go

- AWS SDK for Java V2
- AWS SDK for Ruby V3

RemediationAction

Information about an individual action you can take to remediate a violation.

Contents

Description

A description of a remediation action.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

EC2AssociateRouteTableAction

Information about the AssociateRouteTable action in the Amazon EC2 API.

Type: EC2AssociateRouteTableAction (p. 94) object

Required: No

EC2CopyRouteTableAction

Information about the CopyRouteTable action in the Amazon EC2 API.

Type: EC2CopyRouteTableAction (p. 95) object

Required: No

EC2CreateRouteAction

Information about the CreateRoute action in the Amazon EC2 API.

Type: EC2CreateRouteAction (p. 96) object

Required: No

EC2CreateRouteTableAction

Information about the CreateRouteTable action in the Amazon EC2 API.

Type: EC2CreateRouteTableAction (p. 98) object

Required: No

EC2DeleteRouteAction

Information about the DeleteRoute action in the Amazon EC2 API.

Type: EC2DeleteRouteAction (p. 99) object

Required: No

EC2ReplaceRouteAction

Information about the ReplaceRoute action in the Amazon EC2 API.

Type: EC2ReplaceRouteAction (p. 101) object

Required: No

EC2ReplaceRouteTableAssociationAction

Information about the ReplaceRouteTableAssociation action in the Amazon EC2 API.

Type: EC2ReplaceRouteTableAssociationAction (p. 103) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

RemediationActionWithOrder

An ordered list of actions you can take to remediate a violation.

Contents

Order

The order of the remediation actions in the list.

Type: Integer

Valid Range: Minimum value of -2147483648. Maximum value of 2147483647.

Required: No

RemediationAction

Information about an action you can take to remediate a violation.

Type: RemediationAction (p. 146) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceTag

The resource tags that AWS Firewall Manager uses to determine if a particular resource should be included or excluded from the AWS Firewall Manager policy. Tags enable you to categorize your AWS resources in different ways, for example, by purpose, owner, or environment. Each tag consists of a key and an optional value. Firewall Manager combines the tags with "AND" so that, if you add more than one tag to a policy scope, a resource must have all the specified tags to be included or excluded. For more information, see Working with Tag Editor.

Contents

Key

The resource tag key.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Value

The resource tag value.

Type: String

Length Constraints: Maximum length of 256.

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ResourceViolation

Violation detail based on resource type.

Contents

AwsEc2InstanceViolation

Violation detail for an EC2 instance.

Type: AwsEc2InstanceViolation (p. 85) object

Required: No

AwsEc2NetworkInterfaceViolation

Violation detail for a network interface.

Type: AwsEc2NetworkInterfaceViolation (p. 86) object

Required: No

AwsVPCSecurityGroupViolation

Violation detail for security groups.

Type: AwsVPCSecurityGroupViolation (p. 87) object

Required: No

DnsDuplicateRuleGroupViolation

Violation detail for a DNS Firewall policy that indicates that a rule group that Firewall Manager tried to associate with a VPC is already associated with the VPC and can't be associated again.

Type: DnsDuplicateRuleGroupViolation (p. 90) object

Required: No

DnsRuleGroupLimitExceededViolation

Violation detail for a DNS Firewall policy that indicates that the VPC reached the limit for associated DNS Firewall rule groups. Firewall Manager tried to associate another rule group with the VPC and failed.

Type: DnsRuleGroupLimitExceededViolation (p. 91) object

Required: No

DnsRuleGroupPriorityConflictViolation

Violation detail for a DNS Firewall policy that indicates that a rule group that Firewall Manager tried to associate with a VPC has the same priority as a rule group that's already associated.

Type: DnsRuleGroupPriorityConflictViolation (p. 92) object

Required: No

NetworkFirewallBlackHoleRouteDetectedViolation

Violation detail for an internet gateway route with an inactive state in the customer subnet route table or Network Firewall subnet route table.

Type: NetworkFirewallBlackHoleRouteDetectedViolation (p. 107) object

Required: No

NetworkFirewallInternetTrafficNotInspectedViolation

Violation detail for the subnet for which internet traffic hasn't been inspected.

Type: NetworkFirewallInternetTrafficNotInspectedViolation (p. 109) object

Required: No

NetworkFirewallInvalidRouteConfigurationViolation

The route configuration is invalid.

Type: NetworkFirewallInvalidRouteConfigurationViolation (p. 112) object

Required: No

NetworkFirewallMissingExpectedRoutesViolation

Expected routes are missing from AWS Network Firewall.

Type: NetworkFirewallMissingExpectedRoutesViolation (p. 115) object

Required: No

NetworkFirewallMissingExpectedRTViolation

Violation detail for an Network Firewall policy that indicates that a subnet is not associated with the expected Firewall Manager managed route table.

Type: NetworkFirewallMissingExpectedRTViolation (p. 116) object

Required: No

NetworkFirewallMissingFirewallViolation

Violation detail for an Network Firewall policy that indicates that a subnet has no Firewall Manager managed firewall in its VPC.

Type: NetworkFirewallMissingFirewallViolation (p. 118) object

Required: No

NetworkFirewallMissingSubnetViolation

Violation detail for an Network Firewall policy that indicates that an Availability Zone is missing the expected Firewall Manager managed subnet.

Type: NetworkFirewallMissingSubnetViolation (p. 120) object

Required: No

NetworkFirewallPolicyModifiedViolation

Violation detail for an Network Firewall policy that indicates that a firewall policy in an individual account has been modified in a way that makes it noncompliant. For example, the individual account owner might have deleted a rule group, changed the priority of a stateless rule group, or changed a policy default action.

Type: NetworkFirewallPolicyModifiedViolation (p. 124) object

Required: No

NetworkFirewallUnexpectedFirewallRoutesViolation

There's an unexpected firewall route.

Type: NetworkFirewallUnexpectedFirewallRoutesViolation (p. 125) object

Required: No

NetworkFirewallUnexpectedGatewayRoutesViolation

There's an unexpected gateway route.

Type: NetworkFirewallUnexpectedGatewayRoutesViolation (p. 127) object

Required: No

PossibleRemediationActions

A list of possible remediation action lists. Each individual possible remediation action is a list of individual remediation actions.

Type: PossibleRemediationActions (p. 141) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Route

Describes a route in a route table.

Contents

Destination

The destination of the route.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

DestinationType

The type of destination for the route.

Type: String

Valid Values: `IPV4 | IPV6 | PREFIX_LIST`

Required: No

Target

The route's target.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

TargetType

The type of target for the route.

Type: String

Valid Values: `GATEWAY | CARRIER_GATEWAY | INSTANCE | LOCAL_GATEWAY | NAT_GATEWAY | NETWORK_INTERFACE | VPC_ENDPOINT | VPC_PEERING_CONNECTION | EGRESS_ONLY_INTERNET_GATEWAY | TRANSIT_GATEWAY`

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SecurityGroupRemediationAction

Remediation option for the rule specified in the `ViolationTarget`.

Contents

Description

Brief description of the action that will be performed.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Pattern: `.*`

Required: No

IsDefaultAction

Indicates if the current action is the default action.

Type: Boolean

Required: No

RemediationActionType

The remediation action that will be performed.

Type: String

Valid Values: `REMOVE | MODIFY`

Required: No

RemediationResult

The final state of the rule specified in the `ViolationTarget` after it is remediated.

Type: SecurityGroupRuleDescription (p. 155) object

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SecurityGroupRuleDescription

Describes a set of permissions for a security group rule.

Contents

FromPort

The start of the port range for the TCP and UDP protocols, or an ICMP/ICMPv6 type number. A value of `-1` indicates all ICMP/ICMPv6 types.

Type: Long

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: No

IPV4Range

The IPv4 ranges for the security group rule.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

IPV6Range

The IPv6 ranges for the security group rule.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 256.

Pattern: `[a-f0-9:./]+`

Required: No

PrefixListId

The ID of the prefix list for the security group rule.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

Protocol

The IP protocol name (`tcp`, `udp`, `icmp`, `icmpv6`) or number.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

ToPort

The end of the port range for the TCP and UDP protocols, or an ICMP/ICMPv6 code. A value of `-1` indicates all ICMP/ICMPv6 codes.

Type: Long

Valid Range: Minimum value of 0. Maximum value of 65535.

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

SecurityServicePolicyData

Details about the security service that is being used to protect the resources.

Contents

ManagedServiceData

Details about the service that are specific to the service type, in JSON format. For service type `SHIELD_ADVANCED`, this is an empty string.

- Example: `DNS_FIREWALL`

  ```
  "{\"type\":\"DNS_FIREWALL\",\"preProcessRuleGroups\":[{\"ruleGroupId
  \":\"rslvr-frg-1\",\"priority\":10}],\"postProcessRuleGroups\":
  [{\"ruleGroupId\":\"rslvr-frg-2\",\"priority\":9911}]}"
  ```

  > **Note**
  > Valid values for `preProcessRuleGroups` are between 1 and 99. Valid values for `postProcessRuleGroups` are between 9901 and 10000.

- Example: `NETWORK_FIREWALL`

  ```
  "{\"type\":\"NETWORK_FIREWALL\",
  \"networkFirewallStatelessRuleGroupReferences\":
  [{\"resourceARN\":\"arn:aws:network-firewall:us-
  west-1:1234567891011:stateless-rulegroup/rulegroup2\",\"priority
  \":10}],\"networkFirewallStatelessDefaultActions\":[\"aws:pass\",
  \"custom1\"],\"networkFirewallStatelessFragmentDefaultActions\":
  [\"custom2\",\"aws:pass\"],\"networkFirewallStatelessCustomActions\":
  [{\"actionName\":\"custom1\",\"actionDefinition\":{\"publishMetricAction
  \":{\"dimensions\":[{\"value\":\"dimension1\"}]}}},{\"actionName
  \":\"custom2\",\"actionDefinition\":{\"publishMetricAction
  \":{\"dimensions\":[{\"value\":\"dimension2\"}]}}}],
  \"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
  \":\"arn:aws:network-firewall:us-west-1:1234567891011:stateful-
  rulegroup/rulegroup1\"}],\"networkFirewallOrchestrationConfig\":
  {\"singleFirewallEndpointPerVPC\":true,\"allowedIPV4CidrList\":
  [\"10.24.34.0/28\"]} }"
  ```

- Example: `WAFV2`

  ```
  "{\"type\":\"WAFV2\",\"preProcessRuleGroups\":[{\"ruleGroupArn\":null,
  \"overrideAction\":{\"type\":\"NONE\"},\"managedRuleGroupIdentifier
  \":{\"version\":null,\"vendorName\":\"AWS\",\"managedRuleGroupName
  \":\"AWSManagedRulesAmazonIpReputationList\"},\"ruleGroupType\":
  \"ManagedRuleGroup\",\"excludeRules\":[{\"name\":\"NoUserAgent_HEADER
  \"}]}],\"postProcessRuleGroups\":[],\"defaultAction\":{\"type\":\"ALLOW
  \"},\"overrideCustomerWebACLAssociation\":false,\"loggingConfiguration
  \":{\"logDestinationConfigs\":[\"arn:aws:firehose:us-
  west-2:12345678912:deliverystream/aws-waf-logs-fms-admin-destination
  \"],\"redactedFields\":[{\"redactedFieldType\":\"SingleHeader\",
  \"redactedFieldValue\":\"Cookies\"},{\"redactedFieldType\":\"Method\"}]}}"
  ```

  In the `loggingConfiguration`, you can specify one `logDestinationConfigs`, you can optionally provide up to 20 `redactedFields`, and the `RedactedFieldType` must be one of `URI`, `QUERY_STRING`, `HEADER`, or `METHOD`.

- Example: `AWS WAF Classic`

```
"{\"type\": \"WAF\", \"ruleGroups\": [{\"id\":\"12345678-1bcd-9012-
efga-0987654321ab\", \"overrideAction\" : {\"type\": \"COUNT\"}}],
\"defaultAction\": {\"type\": \"BLOCK\"}}"
```

- Example: `SECURITY_GROUPS_COMMON`

  ```
  "{\"type\":\"SECURITY_GROUPS_COMMON\",\"revertManualSecurityGroupChanges
  \":false,\"exclusiveResourceSecurityGroupManagement\":false,
  \"applyToAllEC2InstanceENIs\":false,\"securityGroups\":[{\"id\":\"
  sg-000e55995d61a06bd\"}]}"
  ```

- Example: Shared VPCs. Apply the preceding policy to resources in shared VPCs as well as to those in VPCs that the account owns

  ```
  "{\"type\":\"SECURITY_GROUPS_COMMON\",\"revertManualSecurityGroupChanges
  \":false,\"exclusiveResourceSecurityGroupManagement\":false,
  \"applyToAllEC2InstanceENIs\":false,\"includeSharedVPC\":true,
  \"securityGroups\":[{\"id\":\" sg-000e55995d61a06bd\"}]}"
  ```

- Example: `SECURITY_GROUPS_CONTENT_AUDIT`

  ```
  "{\"type\":\"SECURITY_GROUPS_CONTENT_AUDIT\",\"securityGroups\":[{\"id\":
  \"sg-000e55995d61a06bd\"}],\"securityGroupAction\":{\"type\":\"ALLOW\"}}"
  ```

  The security group action for content audit can be `ALLOW` or `DENY`. For `ALLOW`, all in-scope security group rules must be within the allowed range of the policy's security group rules. For `DENY`, all in-scope security group rules must not contain a value or a range that matches a rule value or range in the policy security group.

- Example: `SECURITY_GROUPS_USAGE_AUDIT`

  ```
  "{\"type\":\"SECURITY_GROUPS_USAGE_AUDIT\",\"deleteUnusedSecurityGroups
  \":true,\"coalesceRedundantSecurityGroups\":true}"
  ```

Type: String

Length Constraints: Minimum length of 1. Maximum length of 4096.

Pattern: `.*`

Required: No

Type

The service that the policy is using to protect the resources. This specifies the type of policy that is created, either an AWS WAF policy, a Shield Advanced policy, or a security group policy. For security group policies, Firewall Manager supports one security group for each common policy and for each content audit policy. This is an adjustable limit that you can increase by contacting AWS Support.

Type: String

Valid Values: `WAF | WAFV2 | SHIELD_ADVANCED | SECURITY_GROUPS_COMMON | SECURITY_GROUPS_CONTENT_AUDIT | SECURITY_GROUPS_USAGE_AUDIT | NETWORK_FIREWALL | DNS_FIREWALL`

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatefulRuleGroup

AWS Network Firewall stateful rule group, used in a NetworkFirewallPolicyDescription (p. 122).

Contents

ResourceId

The resource ID of the rule group.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RuleGroupName

The name of the rule group.

Type: String

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

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

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

StatelessRuleGroup

AWS Network Firewall stateless rule group, used in a NetworkFirewallPolicyDescription (p. 122).

Contents

Priority

The priority of the rule group. AWS Network Firewall evaluates the stateless rule groups in a firewall policy starting from the lowest priority setting.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 65535.

Required: No

ResourceId

The resource ID of the rule group.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: No

RuleGroupName

The name of the rule group.

Type: String

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

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

Required: No

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Tag

A collection of key:value pairs associated with an AWS resource. The key:value pair can be anything you define. Typically, the tag key represents a category (such as "environment") and the tag value represents a specific value within that category (such as "test," "development," or "production"). You can add up to 50 tags to each AWS resource.

Contents

Key

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: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

Value

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: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

ViolationDetail

Violations for a resource based on the specified AWS Firewall Manager policy and AWS account.

Contents

MemberAccount

The AWS account that the violation details were requested for.

Type: String

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

Pattern: `^[0-9]+$`

Required: Yes

PolicyId

The ID of the AWS Firewall Manager policy that the violation details were requested for.

Type: String

Length Constraints: Fixed length of 36.

Pattern: `^[a-z0-9A-Z-]{36}$`

Required: Yes

ResourceDescription

Brief description for the requested resource.

Type: String

Length Constraints: Minimum length of 0. Maximum length of 1024.

Required: No

ResourceId

The resource ID that the violation details were requested for.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ResourceTags

The `ResourceTag` objects associated with the resource.

Type: Array of Tag (p. 162) objects

Array Members: Minimum number of 0 items. Maximum number of 200 items.

Required: No

ResourceType

The resource type that the violation details were requested for.

Type: String

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

Pattern: `^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

Required: Yes

ResourceViolations

List of violations for the requested resource.

Type: Array of ResourceViolation (p. 150) objects

Required: Yes

See Also

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

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2
- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see Signature Version 4 Signing Process in the *Amazon Web Services General Reference*.

Action

The action to be performed.

Type: string

Required: Yes

Version

The API version that the request is written for, expressed in the format YYYY-MM-DD.

Type: string

Required: Yes

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Task 2: Create a String to Sign for Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Handling Dates in Signature Version 4 in the *Amazon Web Services General Reference*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS Security Token Service, go to AWS Services That Work with IAM in the *IAM User Guide*.

Condition: If you're using temporary security credentials from the AWS Security Token Service, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Task 1: Create a Canonical Request For Signature Version 4 in the *Amazon Web Services General Reference*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 400

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 400

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

InvalidAction

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 400

InvalidClientTokenId

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

InvalidParameterCombination

Parameters that must not be used together were used together.

HTTP Status Code: 400

InvalidParameterValue

An invalid or out-of-range value was supplied for the input parameter.

HTTP Status Code: 400

InvalidQueryParameter

The AWS query string is malformed or does not adhere to AWS standards.

HTTP Status Code: 400

MalformedQueryString

The query string contains a syntax error.

HTTP Status Code: 404

MissingAction

The request is missing an action or a required parameter.

HTTP Status Code: 400

MissingAuthenticationToken

The request must contain either a valid (registered) AWS access key ID or X.509 certificate.

HTTP Status Code: 403

MissingParameter

A required parameter for the specified action is not supplied.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 400

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400