Firewall Management

AWS Firewall Manager

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 Service roles for Firewall Manager.

This document was last published on April 29, 2026.

Actions

The following actions are supported:

- AssociateAdminAccount
- AssociateThirdPartyFirewall
- BatchAssociateResource
- BatchDisassociateResource
- DeleteAppsList
- DeleteNotificationChannel
- DeletePolicy
- DeleteProtocolsList
- DeleteResourceSet
- DisassociateAdminAccount
- DisassociateThirdPartyFirewall
- GetAdminAccount
- GetAdminScope
- GetAppsList
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- GetProtectionStatus
- GetProtocolsList
- GetResourceSet
- GetThirdPartyFirewallAssociationStatus
- GetViolationDetails
- ListAdminAccountsForOrganization
- ListAdminsManagingAccount
- ListAppsLists
- ListComplianceStatus
- ListDiscoveredResources

- ListMemberAccounts
- ListPolicies
- ListProtocolsLists
- ListResourceSetResources
- ListResourceSets
- ListTagsForResource
- ListThirdPartyFirewallFirewallPolicies
- PutAdminAccount
- PutAppsList
- PutNotificationChannel
- PutPolicy
- PutProtocolsList
- PutResourceSet
- TagResource
- UntagResource

AssociateAdminAccount

Sets a AWS Firewall Manager default administrator account. The Firewall Manager default administrator account can manage third-party firewalls and has full administrative scope that allows administration of all policy types, accounts, organizational units, and Regions. This account must be a member account of the organization in AWS Organizations whose resources you want to protect.

For information about working with Firewall Manager administrator accounts, see Managing Firewall Manager administrators in the *Firewall Manager Developer Guide*.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

AdminAccount

The AWS account ID to associate with AWS Firewall Manager as the AWS Firewall Manager default administrator account. This account must be a member account of the organization in AWS Organizations whose resources you want to protect. 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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

AssociateThirdPartyFirewall

Sets the Firewall Manager policy administrator as a tenant administrator of a third-party firewall service. A tenant is an instance of the third-party firewall service that's associated with your AWS customer account.

Request Syntax

```
{
   "ThirdPartyFirewall": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ThirdPartyFirewall

The name of the third-party firewall vendor.

Type: String

Valid Values: `PALO_ALTO_NETWORKS_CLOUD_NGFW | FORTIGATE_CLOUD_NATIVE_FIREWALL`

Required: Yes

Response Syntax

```
{
   "ThirdPartyFirewallStatus": "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.

ThirdPartyFirewallStatus

The current status for setting a Firewall Manager policy administrator's account as an administrator of the third-party firewall tenant.

- `ONBOARDING` - The Firewall Manager policy administrator is being designated as a tenant administrator.
- `ONBOARD_COMPLETE` - The Firewall Manager policy administrator is designated as a tenant administrator.
- `OFFBOARDING` - The Firewall Manager policy administrator is being removed as a tenant administrator.
- `OFFBOARD_COMPLETE` - The Firewall Manager policy administrator has been removed as a tenant administrator.
- `NOT_EXIST` - The Firewall Manager policy administrator doesn't exist as a tenant administrator.

Type: String

Valid Values: `ONBOARDING | ONBOARD_COMPLETE | OFFBOARDING | OFFBOARD_COMPLETE | NOT_EXIST`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

BatchAssociateResource

Associate resources to a Firewall Manager resource set.

Request Syntax

```
{
   "Items": [ "string" ],
   "ResourceSetIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Items

The uniform resource identifiers (URIs) of resources that should be associated to the resource set. The URIs must be Amazon Resource Names (ARNs).

Type: Array of strings

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

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

Required: Yes

ResourceSetIdentifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "FailedItems": [
      {
         "Reason": "string",
         "URI": "string"
      }
   ],
   "ResourceSetIdentifier": "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.

FailedItems

The resources that failed to associate to the resource set.

Type: Array of FailedItem objects

ResourceSetIdentifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

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

BatchDisassociateResource

Disassociates resources from a Firewall Manager resource set.

Request Syntax

```
{
   "Items": [ "string" ],
   "ResourceSetIdentifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Items

The uniform resource identifiers (URI) of resources that should be disassociated from the resource set. The URIs must be Amazon Resource Names (ARNs).

Type: Array of strings

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

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

Required: Yes

ResourceSetIdentifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "FailedItems": [
      {
         "Reason": "string",
         "URI": "string"
      }
   ],
   "ResourceSetIdentifier": "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.

FailedItems

The resources that failed to disassociate from the resource set.

Type: Array of FailedItem objects

ResourceSetIdentifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

ListId

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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 Error Types.

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 V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

DeleteAllPolicyResources

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

For AWS WAF and Shield Advanced policies, the cleanup performs these actions:

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

> **Note**
>
> For AWS WAF and Shield Advanced policies, Firewall Manager removes Firewall Manager generated web ACLs that are not associated with any resources, even if `DeleteAllPolicyResources` is set to `False`.

For security group policies, the cleanup performs these actions for each security group in the policy:

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

> **Note**
>
> For security group common policies, Firewall Manager removes all Firewall Manager generated security groups that aren't associated with any other resources through another policy, even if `DeleteAllPolicyResources` is set to `False`.

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

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 Error Types.

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 V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

ListId

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DeleteResourceSet

Deletes the specified ResourceSet.

Request Syntax

```
{
   "Identifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Identifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

Length Constraints: Fixed length of 22.

Pattern: ^[a-z0-9A-Z]{22}$

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateAdminAccount

Disassociates an AWS Firewall Manager administrator account. To set a different account as an Firewall Manager administrator, submit a PutAdminAccount request. To set an account as a default administrator account, you must submit an AssociateAdminAccount request.

Disassociation of the default administrator account follows the first in, last out principle. If you are the default administrator, all Firewall Manager administrators within the organization must first disassociate their accounts before you can disassociate your account.

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

DisassociateThirdPartyFirewall

Disassociates a Firewall Manager policy administrator from a third-party firewall tenant. When you call `DisassociateThirdPartyFirewall`, the third-party firewall vendor deletes all of the firewalls that are associated with the account.

Request Syntax

```
{
   "ThirdPartyFirewall": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ThirdPartyFirewall

The name of the third-party firewall vendor.

Type: String

Valid Values: `PALO_ALTO_NETWORKS_CLOUD_NGFW | FORTIGATE_CLOUD_NATIVE_FIREWALL`

Required: Yes

Response Syntax

```
{
   "ThirdPartyFirewallStatus": "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.

ThirdPartyFirewallStatus

The current status for the disassociation of a Firewall Manager administrators account with a third-party firewall.

Type: String

Valid Values: `ONBOARDING | ONBOARD_COMPLETE | OFFBOARDING | OFFBOARD_COMPLETE | NOT_EXIST`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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 default 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

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

Type: String

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

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

RoleStatus

The status of the account that you set as the AWS Firewall Manager default 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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetAdminScope

Returns information about the specified account's administrative scope. The administrative scope defines the resources that an Firewall Manager administrator can manage.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

AdminAccount

The administrator account 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

Response Syntax

```
{
   "AdminScope": {
      "AccountScope": {
         "Accounts": [ "string" ],
         "AllAccountsEnabled": boolean,
         "ExcludeSpecifiedAccounts": boolean
      },
      "OrganizationalUnitScope": {
```

```
         "AllOrganizationalUnitsEnabled": boolean,
         "ExcludeSpecifiedOrganizationalUnits": boolean,
         "OrganizationalUnits": [ "string" ]
      },
      "PolicyTypeScope": {
         "AllPolicyTypesEnabled": boolean,
         "PolicyTypes": [ "string" ]
      },
      "RegionScope": {
         "AllRegionsEnabled": boolean,
         "Regions": [ "string" ]
      }
   },
   "Status": "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.

AdminScope

Contains details about the administrative scope of the requested account.

Type: AdminScope object

Status

The current status of the request to onboard a member account as an Firewall Manager administrator.

- `ONBOARDING` - The account is onboarding to Firewall Manager as an administrator.
- `ONBOARDING_COMPLETE` - Firewall Manager The account is onboarded to Firewall Manager as an administrator, and can perform actions on the resources defined in their AdminScope.
- `OFFBOARDING` - The account is being removed as an Firewall Manager administrator.
- `OFFBOARDING_COMPLETE` - The account has been removed as an Firewall Manager administrator.

Type: String

Valid Values: `ONBOARDING | ONBOARDING_COMPLETE | OFFBOARDING | OFFBOARDING_COMPLETE`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

DefaultList

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

Type: Boolean

Required: No

ListId

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

Information about the specified AWS Firewall Manager applications list.

Type: AppsListData object

AppsListArn

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2

- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The reasons for resources being considered compliant depend on the Firewall Manager policy type.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MemberAccount

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

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": [
         {
            "Metadata": {
               "string" : "string"
            },
            "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

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

Type: PolicyComplianceDetail object

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- 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

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

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

PolicyId

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" ]
      },
      "PolicyDescription": "string",
      "PolicyId": "string",
```

```
      "PolicyName": "string",
      "PolicyStatus": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceSetIds": [ "string" ],
      "ResourceTagLogicalOperator": "string",
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceTypeList": [ "string" ],
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "PolicyOption": {
            "NetworkAclCommonPolicy": {
               "NetworkAclEntrySet": {
                  "FirstEntries": [
                     {
                        "CidrBlock": "string",
                        "Egress": boolean,
                        "IcmpTypeCode": {
                           "Code": number,
                           "Type": number
                        },
                        "Ipv6CidrBlock": "string",
                        "PortRange": {
                           "From": number,
                           "To": number
                        },
                        "Protocol": "string",
                        "RuleAction": "string"
                     }
                  ],
                  "ForceRemediateForFirstEntries": boolean,
                  "ForceRemediateForLastEntries": boolean,
                  "LastEntries": [
                     {
                        "CidrBlock": "string",
                        "Egress": boolean,
                        "IcmpTypeCode": {
                           "Code": number,
```

```
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  }
               ]
            }
         },
         "NetworkFirewallPolicy": {
            "FirewallDeploymentModel": "string"
         },
         "ThirdPartyFirewallPolicy": {
            "FirewallDeploymentModel": "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

Information about the specified AWS Firewall Manager policy.

Type: Policy object

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}_.:/=+\-@]*)$`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

EndTime

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

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

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

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

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

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

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

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

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

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 | THIRD_PARTY_FIREWALL | IMPORT_NETWORK_FIREWALL | NETWORK_ACL_COMMON`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

DefaultList

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

Type: Boolean

Required: No

ListId

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

Information about the specified AWS Firewall Manager protocols list.

Type: ProtocolsListData object

ProtocolsListArn

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetResourceSet

Gets information about a specific resource set.

Request Syntax

```
{
   "Identifier": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Identifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

Length Constraints: Fixed length of 22.

Pattern: ^[a-z0-9A-Z]{22}$

Required: Yes

Response Syntax

```
{
   "ResourceSet": {
      "Description": "string",
      "Id": "string",
      "LastUpdateTime": number,
      "Name": "string",
      "ResourceSetStatus": "string",
      "ResourceTypeList": [ "string" ],
      "UpdateToken": "string"
   },
   "ResourceSetArn": "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.

ResourceSet

Information about the specified resource set.

Type: ResourceSet object

ResourceSetArn

The Amazon Resource Name (ARN) of the resource set.

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

GetThirdPartyFirewallAssociationStatus

The onboarding status of a Firewall Manager admin account to third-party firewall vendor tenant.

Request Syntax

```
{
   "ThirdPartyFirewall": "string"
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ThirdPartyFirewall

The name of the third-party firewall vendor.

Type: String

Valid Values: `PALO_ALTO_NETWORKS_CLOUD_NGFW | FORTIGATE_CLOUD_NATIVE_FIREWALL`

Required: Yes

Response Syntax

```
{
   "MarketplaceOnboardingStatus": "string",
   "ThirdPartyFirewallStatus": "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.

MarketplaceOnboardingStatus

The status for subscribing to the third-party firewall vendor in the AWS Marketplace.

- `NO_SUBSCRIPTION` - The Firewall Manager policy administrator isn't subscribed to the third-party firewall service in the AWS Marketplace.
- `NOT_COMPLETE` - The Firewall Manager policy administrator is in the process of subscribing to the third-party firewall service in the AWS Marketplace, but doesn't yet have an active subscription.
- `COMPLETE` - The Firewall Manager policy administrator has an active subscription to the third-party firewall service in the AWS Marketplace.

Type: String

Valid Values: `NO_SUBSCRIPTION | NOT_COMPLETE | COMPLETE`

ThirdPartyFirewallStatus

The current status for setting a Firewall Manager policy administrators account as an administrator of the third-party firewall tenant.

- `ONBOARDING` - The Firewall Manager policy administrator is being designated as a tenant administrator.
- `ONBOARD_COMPLETE` - The Firewall Manager policy administrator is designated as a tenant administrator.
- `OFFBOARDING` - The Firewall Manager policy administrator is being removed as a tenant administrator.
- `OFFBOARD_COMPLETE` - The Firewall Manager policy administrator has been removed as a tenant administrator.
- `NOT_EXIST` - The Firewall Manager policy administrator doesn't exist as a tenant administrator.

Type: String

Valid Values: `ONBOARDING | ONBOARD_COMPLETE | OFFBOARDING | OFFBOARD_COMPLETE | NOT_EXIST`

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- 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.

The request accepts the following data in JSON format.

MemberAccount

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

The ID of the AWS Firewall Manager policy that you want the details for. You can get violation details for the following policy types:

- AWS WAF
- DNS Firewall
- Imported Network Firewall
- Network Firewall
- Security group content audit

- Network ACL
- Third-party firewall

Type: String

Length Constraints: Fixed length of 36.

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

Required: Yes

ResourceId

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

The resource type. This is in the format shown in the AWS Resource Types Reference. Supported resource types are: `AWS::WAFv2::WebACL`, `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"
         },
         "FirewallSubnetIsOutOfScopeViolation": {
            "FirewallSubnetId": "string",
            "SubnetAvailabilityZone": "string",
            "SubnetAvailabilityZoneId": "string",
            "VpcEndpointId": "string",
            "VpcId": "string"
         },
         "FirewallSubnetMissingVPCEndpointViolation": {
            "FirewallSubnetId": "string",
            "SubnetAvailabilityZone": "string",
            "SubnetAvailabilityZoneId": "string",
            "VpcId": "string"
         },
         "InvalidNetworkAclEntriesViolation": {
            "CurrentAssociatedNetworkAcl": "string",
            "EntryViolations": [
               {
                  "ActualEvaluationOrder": "string",
                  "EntriesWithConflicts": [
                     {
                        "EntryDetail": {
                           "CidrBlock": "string",
                           "Egress": boolean,
                           "IcmpTypeCode": {
```

```
                        "Code": number,
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  },
                  "EntryRuleNumber": number,
                  "EntryType": "string"
               }
            ],
            "EntryAtExpectedEvaluationOrder": {
               "EntryDetail": {
                  "CidrBlock": "string",
                  "Egress": boolean,
                  "IcmpTypeCode": {
                     "Code": number,
                     "Type": number
                  },
                  "Ipv6CidrBlock": "string",
                  "PortRange": {
                     "From": number,
                     "To": number
                  },
                  "Protocol": "string",
                  "RuleAction": "string"
               },
               "EntryRuleNumber": number,
               "EntryType": "string"
            },
            "EntryViolationReasons": [ "string" ],
            "ExpectedEntry": {
               "EntryDetail": {
                  "CidrBlock": "string",
                  "Egress": boolean,
                  "IcmpTypeCode": {
                     "Code": number,
                     "Type": number
                  },
                  "Ipv6CidrBlock": "string",
```

```
                        "PortRange": {
                           "From": number,
                           "To": number
                        },
                        "Protocol": "string",
                        "RuleAction": "string"
                     },
                     "EntryRuleNumber": number,
                     "EntryType": "string"
                  },
                  "ExpectedEvaluationOrder": "string"
               }
            ],
            "Subnet": "string",
            "SubnetAvailabilityZone": "string",
            "Vpc": "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": {
```

```
            "StatefulDefaultActions": [ "string" ],
            "StatefulEngineOptions": {
               "RuleOrder": "string",
               "StreamExceptionPolicy": "string"
            },
            "StatefulRuleGroups": [
               {
                  "Override": {
                     "Action": "string"
                  },
                  "Priority": number,
                  "ResourceId": "string",
                  "RuleGroupName": "string"
               }
            ],
            "StatelessCustomActions": [ "string" ],
            "StatelessDefaultActions": [ "string" ],
            "StatelessFragmentDefaultActions": [ "string" ],
            "StatelessRuleGroups": [
               {
                  "Priority": number,
                  "ResourceId": "string",
                  "RuleGroupName": "string"
               }
            ]
         },
         "ExpectedPolicyDescription": {
            "StatefulDefaultActions": [ "string" ],
            "StatefulEngineOptions": {
               "RuleOrder": "string",
               "StreamExceptionPolicy": "string"
            },
            "StatefulRuleGroups": [
               {
                  "Override": {
                     "Action": "string"
                  },
                  "Priority": number,
                  "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": {
      "CreateNetworkAclAction": {
         "Description": "string",
         "FMSCanRemediate": boolean,
         "Vpc": {
            "Description": "string",
            "ResourceId": "string"
         }
      },
      "CreateNetworkAclEntriesAction": {
         "Description": "string",
         "FMSCanRemediate": boolean,
         "NetworkAclEntriesToBeCreated": [
            {
               "EntryDetail": {
                  "CidrBlock": "string",
                  "Egress": boolean,
                  "IcmpTypeCode": {
                     "Code": number,
                     "Type": number
                  },
                  "Ipv6CidrBlock": "string",
                  "PortRange": {
                     "From": number,
                     "To": number
                  },
                  "Protocol": "string",
                  "RuleAction": "string"
               },
               "EntryRuleNumber": number,
               "EntryType": "string"
            }
         ],
         "NetworkAclId": {
            "Description": "string",
            "ResourceId": "string"
         }
      },
      "DeleteNetworkAclEntriesAction": {
         "Description": "string",
         "FMSCanRemediate": boolean,
         "NetworkAclEntriesToBeDeleted": [
```

```
                        {
                           "EntryDetail": {
                              "CidrBlock": "string",
                              "Egress": boolean,
                              "IcmpTypeCode": {
                                 "Code": number,
                                 "Type": number
                              },
                              "Ipv6CidrBlock": "string",
                              "PortRange": {
                                 "From": number,
                                 "To": number
                              },
                              "Protocol": "string",
                              "RuleAction": "string"
                           },
                           "EntryRuleNumber": number,
                           "EntryType": "string"
                        }
                     ],
                     "NetworkAclId": {
                        "Description": "string",
                        "ResourceId": "string"
                     }
                  },
                  "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"
                        }
                     },
                     "FMSPolicyUpdateFirewallCreationConfigAction": {
                        "Description": "string",
                        "FirewallCreationConfig": "string"
                     },
                     "ReplaceNetworkAclAssociationAction": {
                        "AssociationId": {
                           "Description": "string",
                           "ResourceId": "string"
                        },
                        "Description": "string",
                        "FMSCanRemediate": boolean,
                        "NetworkAclId": {
                           "Description": "string",
                           "ResourceId": "string"
                        }
                     }
                  }
               }
            ]
         }
```

```
            ],
            "Description": "string"
         },
         "RouteHasOutOfScopeEndpointViolation": {
            "CurrentFirewallSubnetRouteTable": "string",
            "CurrentInternetGatewayRouteTable": "string",
            "FirewallSubnetId": "string",
            "FirewallSubnetRoutes": [
               {
                  "Destination": "string",
                  "DestinationType": "string",
                  "Target": "string",
                  "TargetType": "string"
               }
            ],
            "InternetGatewayId": "string",
            "InternetGatewayRoutes": [
               {
                  "Destination": "string",
                  "DestinationType": "string",
                  "Target": "string",
                  "TargetType": "string"
               }
            ],
            "RouteTableId": "string",
            "SubnetAvailabilityZone": "string",
            "SubnetAvailabilityZoneId": "string",
            "SubnetId": "string",
            "ViolatingRoutes": [
               {
                  "Destination": "string",
                  "DestinationType": "string",
                  "Target": "string",
                  "TargetType": "string"
               }
            ],
            "VpcId": "string"
         },
         "ThirdPartyFirewallMissingExpectedRouteTableViolation": {
            "AvailabilityZone": "string",
            "CurrentRouteTable": "string",
            "ExpectedRouteTable": "string",
            "ViolationTarget": "string",
            "VPC": "string"
```

```
            },
            "ThirdPartyFirewallMissingFirewallViolation": {
               "AvailabilityZone": "string",
               "TargetViolationReason": "string",
               "ViolationTarget": "string",
               "VPC": "string"
            },
            "ThirdPartyFirewallMissingSubnetViolation": {
               "AvailabilityZone": "string",
               "TargetViolationReason": "string",
               "ViolationTarget": "string",
               "VPC": "string"
            },
            "WebACLHasIncompatibleConfigurationViolation": {
               "Description": "string",
               "WebACLArn": "string"
            },
            "WebACLHasOutOfScopeResourcesViolation": {
               "OutOfScopeResourceList": [ "string" ],
               "WebACLArn": "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

Violation detail for a resource.

Type: ViolationDetail object

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAdminAccountsForOrganization

Returns a `AdminAccounts` object that lists the Firewall Manager administrators within the organization that are onboarded to Firewall Manager by AssociateAdminAccount.

This operation can be called only from the organization's management account.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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

Type: Integer

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

Required: No

NextToken

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

Type: String

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

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

Required: No

Response Syntax

```
{
   "AdminAccounts": [
      {
         "AdminAccount": "string",
         "DefaultAdmin": boolean,
         "Status": "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.

AdminAccounts

A list of Firewall Manager administrator accounts within the organization that were onboarded as administrators by AssociateAdminAccount or PutAdminAccount.

Type: Array of AdminAccountSummary objects

NextToken

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

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4

- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListAdminsManagingAccount

Lists the accounts that are managing the specified AWS Organizations member account. This is useful for any member account so that they can view the accounts who are managing their account. This operation only returns the managing administrators that have the requested account within their AdminScope.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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

Type: Integer

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

Required: No

NextToken

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

Type: String

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

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

Required: No

Response Syntax

```
{
   "AdminAccounts": [ "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.

AdminAccounts

The list of accounts who manage member accounts within their AdminScope.

Type: Array of strings

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

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

NextToken

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

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

DefaultLists

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

Type: Boolean

Required: No

MaxResults

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

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

An array of `AppsListDataSummary` objects.

Type: Array of AppsListDataSummary objects

NextToken

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

MaxResults

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

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

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

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

An array of `PolicyComplianceStatus` objects.

Type: Array of PolicyComplianceStatus objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListDiscoveredResources

Returns an array of resources in the organization's accounts that are available to be associated with a resource set.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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

Type: Integer

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

Required: No

MemberAccountIds

The AWS account IDs to discover resources in. Only one account is supported per request. The account must be a member of your organization.

Type: Array of strings

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

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

Required: Yes

NextToken

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

Type: String

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

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

Required: No

ResourceType

The type of resources to discover.

Type: String

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

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

Required: Yes

Response Syntax

```
{
   "Items": [
      {
         "AccountId": "string",
         "Name": "string",
         "Type": "string",
         "URI": "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.

Items

Details of the resources that were discovered.

Type: Array of DiscoveredResource objects

NextToken

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

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

Either an Firewall Manager administrator or the organization's management account can make this request.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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

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

An array of account IDs.

Type: Array of strings

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

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

NextToken

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

MaxResults

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

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",
         "PolicyStatus": "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

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

An array of `PolicySummary` objects.

Type: Array of PolicySummary objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

DefaultLists

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

Type: Boolean

Required: No

MaxResults

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

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

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

An array of `ProtocolsListDataSummary` objects.

Type: Array of ProtocolsListDataSummary objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++

- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListResourceSetResources

Returns an array of resources that are currently associated to a resource set.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

Identifier

A unique identifier for the resource set, used in a request to refer to the resource set.

Type: String

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

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

Required: Yes

MaxResults

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

Type: Integer

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

Required: No

NextToken

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

Type: String

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

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

Required: No

Response Syntax

```
{
   "Items": [
      {
         "AccountId": "string",
         "URI": "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.

Items

An array of the associated resources' uniform resource identifiers (URI).

Type: Array of Resource objects

NextToken

When you request a list of objects with a `MaxResults` setting, if the number of objects that are still available for retrieval exceeds the maximum you requested, Firewall Manager returns a

`NextToken` value in the response. To retrieve the next batch of objects, use the token returned from the prior request in your next request.

Type: String

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

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

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListResourceSets

Returns an array of `ResourceSetSummary` objects.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

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

Type: Integer

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

Required: No

NextToken

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

Type: String

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

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

Required: No

Response Syntax

```
{
   "NextToken": "string",
   "ResourceSets": [
      {
         "Description": "string",
         "Id": "string",
         "LastUpdateTime": number,
         "Name": "string",
         "ResourceSetStatus": "string"
      }
   ]
}
```

Response Elements

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

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

NextToken

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

Type: String

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

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

ResourceSets

An array of `ResourceSetSummary` objects.

Type: Array of ResourceSetSummary objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

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

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- 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.

The request accepts the following data in JSON format.

ResourceArn

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

The tags associated with the resource.

Type: Array of Tag 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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListThirdPartyFirewallFirewallPolicies

Retrieves a list of all of the third-party firewall policies that are associated with the third-party firewall administrator's account.

Request Syntax

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

Request Parameters

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

The request accepts the following data in JSON format.

MaxResults

The maximum number of third-party firewall policies that you want Firewall Manager to return. If the specified third-party firewall vendor is associated with more than `MaxResults` firewall policies, the response includes a `NextToken` element. `NextToken` contains an encrypted token that identifies the first third-party firewall policies that Firewall Manager will return if you submit another request.

Type: Integer

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

Required: Yes

NextToken

If the previous response included a `NextToken` element, the specified third-party firewall vendor is associated with more third-party firewall policies. To get more third-party firewall policies, submit another `ListThirdPartyFirewallFirewallPoliciesRequest` request.

For the value of `NextToken`, specify the value of `NextToken` from the previous response. If the previous response didn't include a `NextToken` element, there are no more third-party firewall policies to get.

Type: String

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

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

Required: No

ThirdPartyFirewall

The name of the third-party firewall vendor.

Type: String

Valid Values: `PALO_ALTO_NETWORKS_CLOUD_NGFW | FORTIGATE_CLOUD_NATIVE_FIREWALL`

Required: Yes

Response Syntax

```
{
   "NextToken": "string",
   "ThirdPartyFirewallFirewallPolicies": [
      {
         "FirewallPolicyId": "string",
         "FirewallPolicyName": "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

The value that you will use for `NextToken` in the next `ListThirdPartyFirewallFirewallPolicies` request.

Type: String

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

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

ThirdPartyFirewallFirewallPolicies

A list that contains one `ThirdPartyFirewallFirewallPolicies` element for each third-party firewall policies that the specified third-party firewall vendor is associated with. Each `ThirdPartyFirewallFirewallPolicies` element contains the firewall policy name and ID.

Type: Array of ThirdPartyFirewallFirewallPolicy objects

Errors

For information about the errors that are common to all actions, see Common Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutAdminAccount

Creates or updates an Firewall Manager administrator account. The account must be a member of the organization that was onboarded to Firewall Manager by AssociateAdminAccount. Only the organization's management account can create an Firewall Manager administrator account. When you create an Firewall Manager administrator account, the service checks to see if the account is already a delegated administrator within AWS Organizations. If the account isn't a delegated administrator, Firewall Manager calls Organizations to delegate the account within Organizations. For more information about administrator accounts within Organizations, see Managing the AWS Accounts in Your Organization.

Request Syntax

```
{
   "AdminAccount": "string",
   "AdminScope": {
      "AccountScope": {
         "Accounts": [ "string" ],
         "AllAccountsEnabled": boolean,
         "ExcludeSpecifiedAccounts": boolean
      },
      "OrganizationalUnitScope": {
         "AllOrganizationalUnitsEnabled": boolean,
         "ExcludeSpecifiedOrganizationalUnits": boolean,
         "OrganizationalUnits": [ "string" ]
      },
      "PolicyTypeScope": {
         "AllPolicyTypesEnabled": boolean,
         "PolicyTypes": [ "string" ]
      },
      "RegionScope": {
         "AllRegionsEnabled": boolean,
         "Regions": [ "string" ]
      }
   }
}
```

Request Parameters

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

The request accepts the following data in JSON format.

AdminAccount

The AWS account ID to add as an Firewall Manager administrator account. The account must be a member of the organization that was onboarded to Firewall Manager by AssociateAdminAccount. 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

AdminScope

Configures the resources that the specified Firewall Manager administrator can manage. As a best practice, set the administrative scope according to the principles of least privilege. Only grant the administrator the specific resources or permissions that they need to perform the duties of their role.

Type: AdminScope object

Required: No

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 Error Types.

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

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

AppsList

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

Type: AppsListData object

Required: Yes

TagList

The tags associated with the resource.

Type: Array of Tag 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

The details of the AWS Firewall Manager applications list.

Type: AppsListData object

AppsListArn

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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 first configure the SNS topic's access policy to allow the `SnsRoleName` to publish SNS logs. If the `SnsRoleName` provided is a role other than the `AWSServiceRoleForFMS` service-linked role, this role must have a trust relationship configured to allow the Firewall Manager service principal `fms.amazonaws.com` to assume this role. For information about configuring an SNS access policy, see Service roles for Firewall Manager 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.

The request accepts the following data in JSON format.

SnsRoleName

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

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutPolicy

Creates an AWS Firewall Manager policy.

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

If you add a new account to an organization that you created with AWS Organizations, Firewall Manager automatically applies the policy to the resources in that account that are within scope of the policy.

Firewall Manager provides the following types of policies:

- **AWS WAF policy** - This policy applies AWS WAF web ACL protections to specified accounts and resources.
- **Shield Advanced policy** - This policy applies Shield Advanced protection to specified accounts and resources.
- **Security Groups policy** - This type of policy gives you control over security groups that are in use throughout your organization in AWS Organizations and lets you enforce a baseline set of rules across your organization.
- **Network ACL policy** - This type of policy gives you control over the network ACLs that are in use throughout your organization in AWS Organizations and lets you enforce a baseline set of first and last network ACL rules across your organization.
- **Network Firewall policy** - This policy applies Network Firewall protection to your organization's VPCs.
- **DNS Firewall policy** - This policy applies Amazon Route 53 Resolver DNS Firewall protections to your organization's VPCs.
- **Third-party firewall policy** - This policy applies third-party firewall protections. Third-party firewalls are available by subscription through the AWS Marketplace console at AWS Marketplace.
  - **Palo Alto Networks Cloud NGFW policy** - This policy applies Palo Alto Networks Cloud Next Generation Firewall (NGFW) protections and Palo Alto Networks Cloud NGFW rulestacks to your organization's VPCs.
  - **Fortigate CNF policy** - This policy applies Fortigate Cloud Native Firewall (CNF) protections. Fortigate CNF is a cloud-centered solution that blocks Zero-Day threats and secures cloud

infrastructures with industry-leading advanced threat prevention, smart web application firewalls (WAF), and API protection.

Request Syntax

```
{
   "Policy": {
      "DeleteUnusedFMManagedResources": boolean,
      "ExcludeMap": {
         "string" : [ "string" ]
      },
      "ExcludeResourceTags": boolean,
      "IncludeMap": {
         "string" : [ "string" ]
      },
      "PolicyDescription": "string",
      "PolicyId": "string",
      "PolicyName": "string",
      "PolicyStatus": "string",
      "PolicyUpdateToken": "string",
      "RemediationEnabled": boolean,
      "ResourceSetIds": [ "string" ],
      "ResourceTagLogicalOperator": "string",
      "ResourceTags": [
         {
            "Key": "string",
            "Value": "string"
         }
      ],
      "ResourceType": "string",
      "ResourceTypeList": [ "string" ],
      "SecurityServicePolicyData": {
         "ManagedServiceData": "string",
         "PolicyOption": {
            "NetworkAclCommonPolicy": {
               "NetworkAclEntrySet": {
                  "FirstEntries": [
                     {
                        "CidrBlock": "string",
                        "Egress": boolean,
                        "IcmpTypeCode": {
                           "Code": number,
```

```
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  }
               ],
               "ForceRemediateForFirstEntries": boolean,
               "ForceRemediateForLastEntries": boolean,
               "LastEntries": [
                  {
                     "CidrBlock": "string",
                     "Egress": boolean,
                     "IcmpTypeCode": {
                        "Code": number,
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  }
               ]
            }
         },
         "NetworkFirewallPolicy": {
            "FirewallDeploymentModel": "string"
         },
         "ThirdPartyFirewallPolicy": {
            "FirewallDeploymentModel": "string"
         }
      },
      "Type": "string"
   }
},
"TagList": [
   {
```

```
            "Key": "string",
            "Value": "string"
        }
    ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

Policy

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

Type: Policy object

Required: Yes

TagList

The tags to add to the AWS resource.

Type: Array of Tag 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" ]
      },
      "PolicyDescription": "string",
      "PolicyId": "string",
```

```
   "PolicyName": "string",
   "PolicyStatus": "string",
   "PolicyUpdateToken": "string",
   "RemediationEnabled": boolean,
   "ResourceSetIds": [ "string" ],
   "ResourceTagLogicalOperator": "string",
   "ResourceTags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "ResourceType": "string",
   "ResourceTypeList": [ "string" ],
   "SecurityServicePolicyData": {
      "ManagedServiceData": "string",
      "PolicyOption": {
         "NetworkAclCommonPolicy": {
            "NetworkAclEntrySet": {
               "FirstEntries": [
                  {
                     "CidrBlock": "string",
                     "Egress": boolean,
                     "IcmpTypeCode": {
                        "Code": number,
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  }
               ],
               "ForceRemediateForFirstEntries": boolean,
               "ForceRemediateForLastEntries": boolean,
               "LastEntries": [
                  {
                     "CidrBlock": "string",
                     "Egress": boolean,
                     "IcmpTypeCode": {
                        "Code": number,
```

```
                        "Type": number
                     },
                     "Ipv6CidrBlock": "string",
                     "PortRange": {
                        "From": number,
                        "To": number
                     },
                     "Protocol": "string",
                     "RuleAction": "string"
                  }
               ]
            }
         },
         "NetworkFirewallPolicy": {
            "FirewallDeploymentModel": "string"
         },
         "ThirdPartyFirewallPolicy": {
            "FirewallDeploymentModel": "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

The details of the AWS Firewall Manager policy.

Type: Policy object

PolicyArn

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

ProtocolsList

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

Type: ProtocolsListData object

Required: Yes

TagList

The tags associated with the resource.

Type: Array of Tag 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

The details of the AWS Firewall Manager protocols list.

Type: ProtocolsListData object

ProtocolsListArn

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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

PutResourceSet

Creates the resource set.

An AWS Firewall Manager resource set defines the resources to import into an Firewall Manager policy from another AWS service.

Request Syntax

```
{
   "ResourceSet": {
      "Description": "string",
      "Id": "string",
      "LastUpdateTime": number,
      "Name": "string",
      "ResourceSetStatus": "string",
      "ResourceTypeList": [ "string" ],
      "UpdateToken": "string"
   },
   "TagList": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

Request Parameters

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

The request accepts the following data in JSON format.

ResourceSet

Details about the resource set to be created or updated.>

Type: ResourceSet object

Required: Yes

TagList

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

Type: Array of Tag objects

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

Required: No

Response Syntax

```
{
   "ResourceSet": {
      "Description": "string",
      "Id": "string",
      "LastUpdateTime": number,
      "Name": "string",
      "ResourceSetStatus": "string",
      "ResourceTypeList": [ "string" ],
      "UpdateToken": "string"
   },
   "ResourceSetArn": "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.

ResourceSet

Details about the resource set.

Type: ResourceSet object

ResourceSetArn

The Amazon Resource Name (ARN) of the resource set.

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 Error Types.

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

See Also

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

- AWS Command Line Interface V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

ResourceArn

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

The tags to add to the resource.

Type: Array of Tag 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 Error Types.

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 V2
- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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.

The request accepts the following data in JSON format.

ResourceArn

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

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 Error Types.

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 V2

- AWS SDK for .NET V4
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- 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:

- AccountScope
- ActionTarget
- AdminAccountSummary
- AdminScope
- App
- AppsListData
- AppsListDataSummary
- AwsEc2InstanceViolation
- AwsEc2NetworkInterfaceViolation
- AwsVPCSecurityGroupViolation
- ComplianceViolator
- CreateNetworkAclAction
- CreateNetworkAclEntriesAction
- DeleteNetworkAclEntriesAction
- DiscoveredResource
- DnsDuplicateRuleGroupViolation
- DnsRuleGroupLimitExceededViolation
- DnsRuleGroupPriorityConflictViolation
- EC2AssociateRouteTableAction
- EC2CopyRouteTableAction

- EC2CreateRouteAction
- EC2CreateRouteTableAction
- EC2DeleteRouteAction
- EC2ReplaceRouteAction
- EC2ReplaceRouteTableAssociationAction
- EntryDescription
- EntryViolation
- EvaluationResult
- ExpectedRoute
- FailedItem
- FirewallSubnetIsOutOfScopeViolation
- FirewallSubnetMissingVPCEndpointViolation
- FMSPolicyUpdateFirewallCreationConfigAction
- InvalidNetworkAclEntriesViolation
- NetworkAclCommonPolicy
- NetworkAclEntry
- NetworkAclEntrySet
- NetworkAclIcmpTypeCode
- NetworkAclPortRange
- NetworkFirewallBlackHoleRouteDetectedViolation
- NetworkFirewallInternetTrafficNotInspectedViolation
- NetworkFirewallInvalidRouteConfigurationViolation
- NetworkFirewallMissingExpectedRoutesViolation
- NetworkFirewallMissingExpectedRTViolation
- NetworkFirewallMissingFirewallViolation
- NetworkFirewallMissingSubnetViolation
- NetworkFirewallPolicy
- NetworkFirewallPolicyDescription
- NetworkFirewallPolicyModifiedViolation
- NetworkFirewallStatefulRuleGroupOverride

- NetworkFirewallUnexpectedFirewallRoutesViolation
- NetworkFirewallUnexpectedGatewayRoutesViolation
- OrganizationalUnitScope
- PartialMatch
- Policy
- PolicyComplianceDetail
- PolicyComplianceStatus
- PolicyOption
- PolicySummary
- PolicyTypeScope
- PossibleRemediationAction
- PossibleRemediationActions
- ProtocolsListData
- ProtocolsListDataSummary
- RegionScope
- RemediationAction
- RemediationActionWithOrder
- ReplaceNetworkAclAssociationAction
- Resource
- ResourceSet
- ResourceSetSummary
- ResourceTag
- ResourceViolation
- Route
- RouteHasOutOfScopeEndpointViolation
- SecurityGroupRemediationAction
- SecurityGroupRuleDescription
- SecurityServicePolicyData
- StatefulEngineOptions
- StatefulRuleGroup

- StatelessRuleGroup
- Tag
- ThirdPartyFirewallFirewallPolicy
- ThirdPartyFirewallMissingExpectedRouteTableViolation
- ThirdPartyFirewallMissingFirewallViolation
- ThirdPartyFirewallMissingSubnetViolation
- ThirdPartyFirewallPolicy
- ViolationDetail
- WebACLHasIncompatibleConfigurationViolation
- WebACLHasOutOfScopeResourcesViolation

AccountScope

Configures the accounts within the administrator's AWS Organizations organization that the specified Firewall Manager administrator can apply policies to.

Contents

Accounts

The list of accounts within the organization that the specified Firewall Manager administrator either can or cannot apply policies to, based on the value of `ExcludeSpecifiedAccounts`. If `ExcludeSpecifiedAccounts` is set to `true`, then the Firewall Manager administrator can apply policies to all members of the organization except for the accounts in this list. If `ExcludeSpecifiedAccounts` is set to `false`, then the Firewall Manager administrator can only apply policies to the accounts in this list.

Type: Array of strings

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

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

Required: No

AllAccountsEnabled

A boolean value that indicates if the administrator can apply policies to all accounts within an organization. If true, the administrator can apply policies to all accounts within the organization. You can either enable management of all accounts through this operation, or you can specify a list of accounts to manage in `AccountScope$Accounts`. You cannot specify both.

Type: Boolean

Required: No

ExcludeSpecifiedAccounts

A boolean value that excludes the accounts in `AccountScope$Accounts` from the administrator's scope. If true, the Firewall Manager administrator can apply policies to all members of the organization except for the accounts listed in `AccountScope$Accounts`. You can either specify a list of accounts to exclude by `AccountScope$Accounts`, or you can enable

management of all accounts by `AccountScope$AllAccountsEnabled`. You cannot specify both.

Type: Boolean

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 Java V2
- AWS SDK for Ruby V3

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 Java V2
- AWS SDK for Ruby V3

AdminAccountSummary

Contains high level information about the Firewall Manager administrator account.

Contents

AdminAccount

The AWS account ID of the Firewall Manager administrator's account.

Type: String

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

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

Required: No

DefaultAdmin

A boolean value that indicates if the administrator is the default administrator. If true, then this is the default administrator account. The default administrator can manage third-party firewalls and has full administrative scope. There is only one default administrator account per organization. For information about Firewall Manager default administrator accounts, see Managing Firewall Manager administrators in the *Firewall Manager Developer Guide*.

Type: Boolean

Required: No

Status

The current status of the request to onboard a member account as an Firewall Manager administrator.

- `ONBOARDING` - The account is onboarding to Firewall Manager as an administrator.
- `ONBOARDING_COMPLETE` - Firewall Manager The account is onboarded to Firewall Manager as an administrator, and can perform actions on the resources defined in their AdminScope.
- `OFFBOARDING` - The account is being removed as an Firewall Manager administrator.
- `OFFBOARDING_COMPLETE` - The account has been removed as an Firewall Manager administrator.

Type: String

Valid Values: `ONBOARDING | ONBOARDING_COMPLETE | OFFBOARDING | OFFBOARDING_COMPLETE`

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 Java V2
- AWS SDK for Ruby V3

AdminScope

Defines the resources that the Firewall Manager administrator can manage. For more information about administrative scope, see Managing Firewall Manager administrators in the *Firewall Manager Developer Guide*.

Contents

AccountScope

Defines the accounts that the specified Firewall Manager administrator can apply policies to.

Type: AccountScope object

Required: No

OrganizationalUnitScope

Defines the AWS Organizations organizational units that the specified Firewall Manager administrator can apply policies to. For more information about OUs in Organizations, see Managing organizational units (OUs) in the *Organizations User Guide*.

Type: OrganizationalUnitScope object

Required: No

PolicyTypeScope

Defines the Firewall Manager policy types that the specified Firewall Manager administrator can create and manage.

Type: PolicyTypeScope object

Required: No

RegionScope

Defines the AWS Regions that the specified Firewall Manager administrator can perform actions in.

Type: RegionScope 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 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 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 objects

Required: Yes

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

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

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 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 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 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 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 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 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 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 objects

Required: No

PossibleSecurityGroupRemediationActions

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

Type: Array of SecurityGroupRemediationAction 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 Java V2
- AWS SDK for Ruby V3

ComplianceViolator

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

Contents

Metadata

Metadata about the resource that doesn't comply with the policy scope.

Type: String to string map

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

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

Required: No

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 | FIREWALL_SUBNET_IS_OUT_OF_SCOPE | 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 | ROUTE_HAS_OUT_OF_SCOPE_ENDPOINT | FIREWALL_SUBNET_MISSING_VPCE_ENDPOINT | INVALID_NETWORK_ACL_ENTRY | WEB_ACL_CONFIGURATION_OR_SCOPE_OF_USE`

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 Java V2
- AWS SDK for Ruby V3

CreateNetworkAclAction

Information about the `CreateNetworkAcl` action in Amazon EC2. This is a remediation option in `RemediationAction`.

Contents

Description

Brief description of this remediation action.

Type: String

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

Required: No

FMSCanRemediate

Indicates whether it is possible for Firewall Manager to perform this remediation action. A false value indicates that auto remediation is disabled or Firewall Manager is unable to perform the action due to a conflict of some kind.

Type: Boolean

Required: No

Vpc

The VPC that's associated with the remediation action.

Type: ActionTarget 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 Java V2

- AWS SDK for Ruby V3

CreateNetworkAclEntriesAction

Information about the `CreateNetworkAclEntries` action in Amazon EC2. This is a remediation option in `RemediationAction`.

Contents

Description

Brief description of this remediation action.

Type: String

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

Required: No

FMSCanRemediate

Indicates whether it is possible for Firewall Manager to perform this remediation action. A false value indicates that auto remediation is disabled or Firewall Manager is unable to perform the action due to a conflict of some kind.

Type: Boolean

Required: No

NetworkAclEntriesToBeCreated

Lists the entries that the remediation action would create.

Type: Array of EntryDescription objects

Required: No

NetworkAclId

The network ACL that's associated with the remediation action.

Type: ActionTarget 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 Java V2
- AWS SDK for Ruby V3

DeleteNetworkAclEntriesAction

Information about the `DeleteNetworkAclEntries` action in Amazon EC2. This is a remediation option in `RemediationAction`.

Contents

Description

Brief description of this remediation action.

Type: String

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

Required: No

FMSCanRemediate

Indicates whether it is possible for Firewall Manager to perform this remediation action. A false value indicates that auto remediation is disabled or Firewall Manager is unable to perform the action due to a conflict of some kind.

Type: Boolean

Required: No

NetworkAclEntriesToBeDeleted

Lists the entries that the remediation action would delete.

Type: Array of EntryDescription objects

Required: No

NetworkAclId

The network ACL that's associated with the remediation action.

Type: ActionTarget 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 Java V2
- AWS SDK for Ruby V3

DiscoveredResource

A resource in the organization that's available to be associated with a Firewall Manager resource set.

Contents

AccountId

The AWS account ID associated with the discovered resource.

Type: String

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

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

Required: No

Name

The name of the discovered resource.

Type: String

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

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

Required: No

Type

The type of the discovered resource.

Type: String

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

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

Required: No

URI

The universal resource identifier (URI) of the discovered resource.

Type: String

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

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 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 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 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 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

RouteTableId

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

Type: ActionTarget object

Required: Yes

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 object

Required: No

SubnetId

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

Type: ActionTarget 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 Java V2
- AWS SDK for Ruby V3

EC2CopyRouteTableAction

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

Contents

RouteTableId

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

Type: ActionTarget object

Required: Yes

VpcId

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

Type: ActionTarget object

Required: Yes

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

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 Java V2
- AWS SDK for Ruby V3

EC2CreateRouteAction

Information about the CreateRoute action in Amazon EC2.

Contents

RouteTableId

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

Type: ActionTarget object

Required: Yes

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 object

Required: No

VpcEndpointId

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

Type: ActionTarget 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 Java V2
- AWS SDK for Ruby V3

EC2CreateRouteTableAction

Information about the CreateRouteTable action in Amazon EC2.

Contents

VpcId

Information about the ID of a VPC.

Type: ActionTarget object

Required: Yes

Description

A description of the CreateRouteTable action.

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 Java V2
- AWS SDK for Ruby V3

EC2DeleteRouteAction

Information about the DeleteRoute action in Amazon EC2.

Contents

RouteTableId

Information about the ID of the route table.

Type: ActionTarget object

Required: Yes

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

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 Java V2
- AWS SDK for Ruby V3

EC2ReplaceRouteAction

Information about the ReplaceRoute action in Amazon EC2.

Contents

RouteTableId

Information about the ID of the route table.

Type: ActionTarget object

Required: Yes

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 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 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 object

Required: Yes

RouteTableId

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

Type: ActionTarget 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

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 Java V2
- AWS SDK for Ruby V3

EntryDescription

Describes a single rule in a network ACL.

Contents

EntryDetail

Describes a rule in a network ACL.

Each network ACL has a set of numbered ingress rules and a separate set of numbered egress rules. When determining whether a packet should be allowed in or out of a subnet associated with the network ACL, AWS processes the entries in the network ACL according to the rule numbers, in ascending order.

When you manage an individual network ACL, you explicitly specify the rule numbers. When you specify the network ACL rules in a Firewall Manager policy, you provide the rules to run first, in the order that you want them to run, and the rules to run last, in the order that you want them to run. Firewall Manager assigns the rule numbers for you when you save the network ACL policy specification.

Type: NetworkAclEntry object

Required: No

EntryRuleNumber

The rule number for the entry. ACL entries are processed in ascending order by rule number. In a Firewall Manager network ACL policy, Firewall Manager assigns rule numbers.

Type: Integer

Valid Range: Minimum value of 0. Maximum value of 2147483647.

Required: No

EntryType

Specifies whether the entry is managed by Firewall Manager or by a user, and, for Firewall Manager-managed entries, specifies whether the entry is among those that run first in the network ACL or those that run last.

Type: String

Valid Values: `FMS_MANAGED_FIRST_ENTRY | FMS_MANAGED_LAST_ENTRY | CUSTOM_ENTRY`

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 Java V2
- AWS SDK for Ruby V3

EntryViolation

Detailed information about an entry violation in a network ACL. The violation is against the network ACL specification inside the Firewall Manager network ACL policy. This data object is part of `InvalidNetworkAclEntriesViolation`.

Contents

ActualEvaluationOrder

The evaluation location within the ordered list of entries where the `ExpectedEntry` is currently located.

Type: String

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

Required: No

EntriesWithConflicts

The list of entries that are in conflict with `ExpectedEntry`.

Type: Array of EntryDescription objects

Required: No

EntryAtExpectedEvaluationOrder

The entry that's currently in the `ExpectedEvaluationOrder` location, in place of the expected entry.

Type: EntryDescription object

Required: No

EntryViolationReasons

Descriptions of the violations that Firewall Manager found for these entries.

Type: Array of strings

Valid Values: `MISSING_EXPECTED_ENTRY | INCORRECT_ENTRY_ORDER | ENTRY_CONFLICT`

Required: No

ExpectedEntry

The Firewall Manager-managed network ACL entry that is involved in the entry violation.

Type: EntryDescription object

Required: No

ExpectedEvaluationOrder

The evaluation location within the ordered list of entries where the `ExpectedEntry` should be, according to the network ACL policy specifications.

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 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 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 Java V2
- AWS SDK for Ruby V3

FailedItem

Details of a resource that failed when trying to update it's association to a resource set.

Contents

Reason

The reason the resource's association could not be updated.

Type: String

Valid Values: `NOT_VALID_ARN | NOT_VALID_PARTITION | NOT_VALID_REGION | NOT_VALID_SERVICE | NOT_VALID_RESOURCE_TYPE | NOT_VALID_ACCOUNT_ID`

Required: No

URI

The univeral resource indicator (URI) of the resource that failed.

Type: String

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

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 Java V2
- AWS SDK for Ruby V3

FirewallSubnetIsOutOfScopeViolation

Contains details about the firewall subnet that violates the policy scope.

Contents

FirewallSubnetId

The ID of the firewall subnet that violates the policy scope.

Type: String

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

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

Required: No

SubnetAvailabilityZone

The Availability Zone of the firewall subnet that violates the policy scope.

Type: String

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

Required: No

SubnetAvailabilityZoneId

The Availability Zone ID of the firewall subnet that violates the policy scope.

Type: String

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

Required: No

VpcEndpointId

The VPC endpoint ID of the firewall subnet that violates the policy scope.

Type: String

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

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

Required: No

VpcId

The VPC ID of the firewall subnet that violates the policy scope.

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 Java V2
- AWS SDK for Ruby V3

FirewallSubnetMissingVPCEndpointViolation

The violation details for a firewall subnet's VPC endpoint that's deleted or missing.

Contents

FirewallSubnetId

The ID of the firewall that this VPC endpoint is associated with.

Type: String

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

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

Required: No

SubnetAvailabilityZone

The name of the Availability Zone of the deleted VPC subnet.

Type: String

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

Required: No

SubnetAvailabilityZoneId

The ID of the Availability Zone of the deleted VPC subnet.

Type: String

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

Required: No

VpcId

The resource ID of the VPC associated with the deleted VPC 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 Java V2
- AWS SDK for Ruby V3

FMSPolicyUpdateFirewallCreationConfigAction

Contains information about the actions that you can take to remediate scope violations caused by your policy's `FirewallCreationConfig`. `FirewallCreationConfig` is an optional configuration that you can use to choose which Availability Zones Firewall Manager creates Network Firewall endpoints in.

Contents

Description

Describes the remedial action.

Type: String

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

Required: No

FirewallCreationConfig

A `FirewallCreationConfig` that you can copy into your current policy's SecurityServiceData in order to remedy scope violations.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 30000.

Pattern: `^((?!\\[nr]).)+`

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 Java V2
- AWS SDK for Ruby V3

InvalidNetworkAclEntriesViolation

Violation detail for the entries in a network ACL resource.

Contents

CurrentAssociatedNetworkAcl

The network ACL containing the entry violations.

Type: String

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

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

Required: No

EntryViolations

Detailed information about the entry violations in the network ACL.

Type: Array of EntryViolation objects

Required: No

Subnet

The subnet that's associated with the network ACL.

Type: String

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

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

Required: No

SubnetAvailabilityZone

The Availability Zone where the network ACL is in use.

Type: String

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

Required: No

Vpc

The VPC where the violation was found.

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 Java V2
- AWS SDK for Ruby V3

NetworkAclCommonPolicy

Defines a Firewall Manager network ACL policy. This is used in the `PolicyOption` of a `SecurityServicePolicyData` for a `Policy`, when the `SecurityServicePolicyData` type is set to `NETWORK_ACL_COMMON`.

For information about network ACLs, see Control traffic to subnets using network ACLs in the *Amazon Virtual Private Cloud User Guide*.

Contents

NetworkAclEntrySet

The definition of the first and last rules for the network ACL policy.

Type: NetworkAclEntrySet 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 Java V2
- AWS SDK for Ruby V3

NetworkAclEntry

Describes a rule in a network ACL.

Each network ACL has a set of numbered ingress rules and a separate set of numbered egress rules. When determining whether a packet should be allowed in or out of a subnet associated with the network ACL, AWS processes the entries in the network ACL according to the rule numbers, in ascending order.

When you manage an individual network ACL, you explicitly specify the rule numbers. When you specify the network ACL rules in a Firewall Manager policy, you provide the rules to run first, in the order that you want them to run, and the rules to run last, in the order that you want them to run. Firewall Manager assigns the rule numbers for you when you save the network ACL policy specification.

Contents

Egress

Indicates whether the rule is an egress, or outbound, rule (applied to traffic leaving the subnet). If it's not an egress rule, then it's an ingress, or inbound, rule.

Type: Boolean

Required: Yes

Protocol

The protocol number. A value of "-1" means all protocols.

Type: String

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

Required: Yes

RuleAction

Indicates whether to allow or deny the traffic that matches the rule.

Type: String

Valid Values: `allow | deny`

Required: Yes

CidrBlock

The IPv4 network range to allow or deny, in CIDR notation.

Type: String

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

Required: No

IcmpTypeCode

ICMP protocol: The ICMP type and code.

Type: NetworkAclIcmpTypeCode object

Required: No

Ipv6CidrBlock

The IPv6 network range to allow or deny, in CIDR notation.

Type: String

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

Required: No

PortRange

TCP or UDP protocols: The range of ports the rule applies to.

Type: NetworkAclPortRange 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 Java V2

- AWS SDK for Ruby V3

NetworkAclEntrySet

The configuration of the first and last rules for the network ACL policy, and the remediation settings for each.

Contents

ForceRemediateForFirstEntries

Applies only when remediation is enabled for the policy as a whole. Firewall Manager uses this setting when it finds policy violations that involve conflicts between the custom entries and the policy entries.

If forced remediation is disabled, Firewall Manager marks the network ACL as noncompliant and does not try to remediate. For more information about the remediation behavior, see Remediation for managed network ACLs in the *AWS Firewall Manager Developer Guide*.

Type: Boolean

Required: Yes

ForceRemediateForLastEntries

Applies only when remediation is enabled for the policy as a whole. Firewall Manager uses this setting when it finds policy violations that involve conflicts between the custom entries and the policy entries.

If forced remediation is disabled, Firewall Manager marks the network ACL as noncompliant and does not try to remediate. For more information about the remediation behavior, see Remediation for managed network ACLs in the *AWS Firewall Manager Developer Guide*.

Type: Boolean

Required: Yes

FirstEntries

The rules that you want to run first in the Firewall Manager managed network ACLs.

> **Note**
>
> Provide these in the order in which you want them to run. Firewall Manager will assign the specific rule numbers for you, in the network ACLs that it creates.

You must specify at least one first entry or one last entry in any network ACL policy.

Type: Array of NetworkAclEntry objects

Required: No

LastEntries

The rules that you want to run last in the Firewall Manager managed network ACLs.

> **Note**
>
> Provide these in the order in which you want them to run. Firewall Manager will assign the specific rule numbers for you, in the network ACLs that it creates.

You must specify at least one first entry or one last entry in any network ACL policy.

Type: Array of NetworkAclEntry 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 Java V2
- AWS SDK for Ruby V3

NetworkAclIcmpTypeCode

ICMP protocol: The ICMP type and code.

Contents

Code

ICMP code.

Type: Integer

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

Required: No

Type

ICMP type.

Type: Integer

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

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 Java V2
- AWS SDK for Ruby V3

NetworkAclPortRange

TCP or UDP protocols: The range of ports the rule applies to.

Contents

From

The beginning port number of the range.

Type: Integer

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

Required: No

To

The ending port number of the range.

Type: Integer

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 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 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 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 objects

Required: No

ActualInternetGatewayRoutes

The actual internet gateway routes.

Type: Array of Route 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 objects

Required: No

ExpectedInternetGatewayRoutes

The internet gateway routes that are expected.

Type: Array of ExpectedRoute 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 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 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 objects

Required: No

ActualInternetGatewayRoutes

The actual internet gateway routes.

Type: Array of Route 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 objects

Required: No

ExpectedInternetGatewayRoutes

The expected routes for the internet gateway.

Type: Array of ExpectedRoute 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 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 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 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 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 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 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 Java V2
- AWS SDK for Ruby V3

NetworkFirewallPolicy

Configures the firewall policy deployment model of AWS Network Firewall. For information about Network Firewall deployment models, see AWS Network Firewall example architectures with routing in the *Network Firewall Developer Guide*.

Contents

FirewallDeploymentModel

Defines the deployment model to use for the firewall policy. To use a distributed model, set PolicyOption to `NULL`.

Type: String

Valid Values: `CENTRALIZED | DISTRIBUTED`

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 Java V2
- AWS SDK for Ruby V3

NetworkFirewallPolicyDescription

The definition of the AWS Network Firewall firewall policy.

Contents

StatefulDefaultActions

The default actions to take on a packet that doesn't match any stateful rules. The stateful default action is optional, and is only valid when using the strict rule order.

Valid values of the stateful default action:

- aws:drop_strict
- aws:drop_established
- aws:alert_strict
- aws:alert_established

Type: Array of strings

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

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

Required: No

StatefulEngineOptions

Additional options governing how Network Firewall handles stateful rules. The stateful rule groups that you use in your policy must have stateful rule options settings that are compatible with these settings.

Type: StatefulEngineOptions object

Required: No

StatefulRuleGroups

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

Type: Array of StatefulRuleGroup 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 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 Java V2
- AWS SDK for Ruby V3

NetworkFirewallPolicyModifiedViolation

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

Contents

CurrentPolicyDescription

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

Type: NetworkFirewallPolicyDescription object

Required: No

ExpectedPolicyDescription

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

Type: NetworkFirewallPolicyDescription 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 Java V2

- AWS SDK for Ruby V3

NetworkFirewallStatefulRuleGroupOverride

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

Contents

Action

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

Type: String

Valid Values: `DROP_TO_ALERT`

Required: No

See Also

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

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

OrganizationalUnitScope

Defines the Organizations organizational units (OUs) that the specified Firewall Manager administrator can apply policies to. For more information about OUs in Organizations, see Managing organizational units (OUs) in the *Organizations User Guide*.

Contents

AllOrganizationalUnitsEnabled

A boolean value that indicates if the administrator can apply policies to all OUs within an organization. If true, the administrator can manage all OUs within the organization. You can either enable management of all OUs through this operation, or you can specify OUs to manage in `OrganizationalUnitScope$OrganizationalUnits`. You cannot specify both.

Type: Boolean

Required: No

ExcludeSpecifiedOrganizationalUnits

A boolean value that excludes the OUs in `OrganizationalUnitScope $OrganizationalUnits` from the administrator's scope. If true, the Firewall Manager administrator can apply policies to all OUs in the organization except for the OUs listed in `OrganizationalUnitScope$OrganizationalUnits`. You can either specify a list of OUs to exclude by `OrganizationalUnitScope$OrganizationalUnits`, or you can enable management of all OUs by `OrganizationalUnitScope $AllOrganizationalUnitsEnabled`. You cannot specify both.

Type: Boolean

Required: No

OrganizationalUnits

The list of OUs within the organization that the specified Firewall Manager administrator either can or cannot apply policies to, based on the value of `OrganizationalUnitScope $ExcludeSpecifiedOrganizationalUnits`. If `OrganizationalUnitScope $ExcludeSpecifiedOrganizationalUnits` is set to `true`, then the Firewall Manager administrator can apply policies to all OUs in the organization except for the OUs in this list. If

`OrganizationalUnitScope$ExcludeSpecifiedOrganizationalUnits` is set to `false`, then the Firewall Manager administrator can only apply policies to the OUs in this list.

Type: Array of strings

Length Constraints: Minimum length of 16. Maximum length of 68.

Pattern: `^ou-[0-9a-z]{4,32}-[a-z0-9]{8,32}$`

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 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 Java V2
- AWS SDK for Ruby V3

Policy

An AWS Firewall Manager policy.

Contents

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

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

RemediationEnabled

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

Type: Boolean

Required: Yes

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`.

The following are valid resource types for each Firewall Manager policy type:

- AWS WAF Classic - `AWS::ApiGateway::Stage`, `AWS::CloudFront::Distribution`, and `AWS::ElasticLoadBalancingV2::LoadBalancer`.
- AWS WAF - `AWS::ApiGateway::Stage`, `AWS::ElasticLoadBalancingV2::LoadBalancer`, and `AWS::CloudFront::Distribution`.
- Shield Advanced - `AWS::ElasticLoadBalancingV2::LoadBalancer`, `AWS::ElasticLoadBalancing::LoadBalancer`, `AWS::EC2::EIP`, and `AWS::CloudFront::Distribution`.
- Network ACL - `AWS::EC2::Subnet`.
- Security group usage audit - `AWS::EC2::SecurityGroup`.
- Security group content audit - `AWS::EC2::SecurityGroup`, `AWS::EC2::NetworkInterface`, and `AWS::EC2::Instance`.
- DNS Firewall, AWS Network Firewall, and third-party firewall - `AWS::EC2::VPC`.

Type: String

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

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

Required: Yes

SecurityServicePolicyData

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

Type: SecurityServicePolicyData object

Required: Yes

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

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

PolicyDescription

Your description of the AWS Firewall Manager policy.

Type: String

Length Constraints: Maximum length of 256.

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

PolicyStatus

Indicates whether the policy is in or out of an admin's policy or Region scope.

- ACTIVE - The administrator can manage and delete the policy.
- OUT_OF_ADMIN_SCOPE - The administrator can view the policy, but they can't edit or delete the policy. Existing policy protections stay in place. Any new resources that come into scope of the policy won't be protected.

Type: String

Valid Values: ACTIVE | OUT_OF_ADMIN_SCOPE

Required: No

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

ResourceSetIds

The unique identifiers of the resource sets used by the policy.

Type: Array of strings

Length Constraints: Fixed length of 22.

Pattern: ^[a-z0-9A-Z]{22}$

Required: No

ResourceTagLogicalOperator

Specifies whether to combine multiple resource tags with AND, so that a resource must have all tags to be included or excluded, or OR, so that a resource must have at least one tag.

Default: `AND`

Type: String

Valid Values: `AND | OR`

Required: No

ResourceTags

An array of `ResourceTag` objects.

Type: Array of ResourceTag objects

Array Members: Minimum number of 0 items. Maximum number of 50 items.

Required: No

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

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 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 4096.

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 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 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 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 4096.

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 Java V2
- AWS SDK for Ruby V3

PolicyOption

Contains the settings to configure a network ACL policy, a AWS Network Firewall firewall policy deployment model, or a third-party firewall policy.

Contents

NetworkAclCommonPolicy

Defines a Firewall Manager network ACL policy.

Type: NetworkAclCommonPolicy object

Required: No

NetworkFirewallPolicy

Defines the deployment model to use for the firewall policy.

Type: NetworkFirewallPolicy object

Required: No

ThirdPartyFirewallPolicy

Defines the policy options for a third-party firewall policy.

Type: ThirdPartyFirewallPolicy 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 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

PolicyStatus

Indicates whether the policy is in or out of an admin's policy or Region scope.

- `ACTIVE` - The administrator can manage and delete the policy.
- `OUT_OF_ADMIN_SCOPE` - The administrator can view the policy, but they can't edit or delete the policy. Existing policy protections stay in place. Any new resources that come into scope of the policy won't be protected.

Type: String

Valid Values: `ACTIVE | OUT_OF_ADMIN_SCOPE`

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.

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 | THIRD_PARTY_FIREWALL | IMPORT_NETWORK_FIREWALL | NETWORK_ACL_COMMON`

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 Java V2
- AWS SDK for Ruby V3

PolicyTypeScope

Defines the policy types that the specified Firewall Manager administrator can manage.

Contents

AllPolicyTypesEnabled

Allows the specified Firewall Manager administrator to manage all Firewall Manager policy types, except for third-party policy types. Third-party policy types can only be managed by the Firewall Manager default administrator.

Type: Boolean

Required: No

PolicyTypes

The list of policy types that the specified Firewall Manager administrator can manage.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 32 items.

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

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 Java V2
- AWS SDK for Ruby V3

PossibleRemediationAction

A list of remediation actions.

Contents

OrderedRemediationActions

The ordered list of remediation actions.

Type: Array of RemediationActionWithOrder objects

Required: Yes

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

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 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 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 Java V2
- AWS SDK for Ruby V3

ProtocolsListData

An AWS Firewall Manager protocols list.

Contents

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

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

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

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

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 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 Java V2
- AWS SDK for Ruby V3

RegionScope

Defines the AWS Regions that the specified Firewall Manager administrator can manage.

Contents

AllRegionsEnabled

Allows the specified Firewall Manager administrator to manage all AWS Regions.

Type: Boolean

Required: No

Regions

The AWS Regions that the specified Firewall Manager administrator can perform actions in.

Type: Array of strings

Array Members: Minimum number of 0 items. Maximum number of 64 items.

Length Constraints: Minimum length of 6. Maximum length of 32.

Pattern: `^(af|ap|ca|eu|il|me|mx|sa|us|cn|us-gov)-\w+-\d+$`

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 Java V2
- AWS SDK for Ruby V3

RemediationAction

Information about an individual action you can take to remediate a violation.

Contents

CreateNetworkAclAction

Information about the `CreateNetworkAcl` action in Amazon EC2.

Type: CreateNetworkAclAction object

Required: No

CreateNetworkAclEntriesAction

Information about the `CreateNetworkAclEntries` action in Amazon EC2.

Type: CreateNetworkAclEntriesAction object

Required: No

DeleteNetworkAclEntriesAction

Information about the `DeleteNetworkAclEntries` action in Amazon EC2.

Type: DeleteNetworkAclEntriesAction object

Required: No

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 object

Required: No

EC2CopyRouteTableAction

Information about the CopyRouteTable action in the Amazon EC2 API.

Type: EC2CopyRouteTableAction object

Required: No

EC2CreateRouteAction

Information about the CreateRoute action in the Amazon EC2 API.

Type: EC2CreateRouteAction object

Required: No

EC2CreateRouteTableAction

Information about the CreateRouteTable action in the Amazon EC2 API.

Type: EC2CreateRouteTableAction object

Required: No

EC2DeleteRouteAction

Information about the DeleteRoute action in the Amazon EC2 API.

Type: EC2DeleteRouteAction object

Required: No

EC2ReplaceRouteAction

Information about the ReplaceRoute action in the Amazon EC2 API.

Type: EC2ReplaceRouteAction object

Required: No

EC2ReplaceRouteTableAssociationAction

Information about the ReplaceRouteTableAssociation action in the Amazon EC2 API.

Type: EC2ReplaceRouteTableAssociationAction object

Required: No

FMSPolicyUpdateFirewallCreationConfigAction

The remedial action to take when updating a firewall configuration.

Type: FMSPolicyUpdateFirewallCreationConfigAction object

Required: No

ReplaceNetworkAclAssociationAction

Information about the `ReplaceNetworkAclAssociation` action in Amazon EC2.

Type: ReplaceNetworkAclAssociationAction 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 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 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 Java V2
- AWS SDK for Ruby V3

ReplaceNetworkAclAssociationAction

Information about the `ReplaceNetworkAclAssociation` action in Amazon EC2. This is a remediation option in `RemediationAction`.

Contents

AssociationId

Describes a remediation action target.

Type: ActionTarget object

Required: No

Description

Brief description of this remediation action.

Type: String

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

Required: No

FMSCanRemediate

Indicates whether it is possible for Firewall Manager to perform this remediation action. A false value indicates that auto remediation is disabled or Firewall Manager is unable to perform the action due to a conflict of some kind.

Type: Boolean

Required: No

NetworkAclId

The network ACL that's associated with the remediation action.

Type: ActionTarget 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 Java V2
- AWS SDK for Ruby V3

Resource

Details of a resource that is associated to an Firewall Manager resource set.

Contents

URI

The resource's universal resource indicator (URI).

Type: String

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

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

Required: Yes

AccountId

The AWS account ID that the associated resource belongs to.

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 Java V2
- AWS SDK for Ruby V3

ResourceSet

A set of resources to include in a policy.

Contents

Name

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

Type: String

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

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

Required: Yes

ResourceTypeList

Determines the resources that can be associated to the resource set. Depending on your setting for max results and the number of resource sets, a single call might not return the full list.

Type: Array of strings

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

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

Required: Yes

Description

A description of the resource set.

Type: String

Length Constraints: Maximum length of 256.

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

Required: No

Id

A unique identifier for the resource set. This ID is returned in the responses to create and list commands. You provide it to operations like update and delete.

Type: String

Length Constraints: Fixed length of 22.

Pattern: `^[a-z0-9A-Z]{22}$`

Required: No

LastUpdateTime

The last time that the resource set was changed.

Type: Timestamp

Required: No

ResourceSetStatus

Indicates whether the resource set is in or out of an admin's Region scope.

- `ACTIVE` - The administrator can manage and delete the resource set.
- `OUT_OF_ADMIN_SCOPE` - The administrator can view the resource set, but they can't edit or delete the resource set. Existing protections stay in place. Any new resource that come into scope of the resource set won't be protected.

Type: String

Valid Values: `ACTIVE | OUT_OF_ADMIN_SCOPE`

Required: No

UpdateToken

An optional token that you can use for optimistic locking. Firewall Manager returns a token to your requests that access the resource set. The token marks the state of the resource set resource at the time of the request. Update tokens are not allowed when creating a resource set. After creation, each subsequent update call to the resource set requires the update token.

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

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

Type: String

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

Pattern: `^([\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 Java V2
- AWS SDK for Ruby V3

ResourceSetSummary

Summarizes the resource sets used in a policy.

Contents

Description

A description of the resource set.

Type: String

Length Constraints: Maximum length of 256.

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

Required: No

Id

A unique identifier for the resource set. This ID is returned in the responses to create and list commands. You provide it to operations like update and delete.

Type: String

Length Constraints: Fixed length of 22.

Pattern: `^[a-z0-9A-Z]{22}$`

Required: No

LastUpdateTime

The last time that the resource set was changed.

Type: Timestamp

Required: No

Name

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

Type: String

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

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

Required: No

ResourceSetStatus

Indicates whether the resource set is in or out of an admin's Region scope.

- `ACTIVE` - The administrator can manage and delete the resource set.
- `OUT_OF_ADMIN_SCOPE` - The administrator can view the resource set, but they can't edit or delete the resource set. Existing protections stay in place. Any new resource that come into scope of the resource set won't be protected.

Type: String

Valid Values: `ACTIVE | OUT_OF_ADMIN_SCOPE`

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 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. If you add more than one tag to a policy, you can specify whether to combine them using the logical AND operator or the logical OR operator. For more information, see Working with Tag Editor.

Every resource tag must have a string value, either a non-empty string or an empty string. If you don't provide a value for a resource tag, Firewall Manager saves the value as an empty string: "". When Firewall Manager compares tags, it only matches two tags if they have the same key and the same value. A tag with an empty string value only matches with tags that also have an empty string value.

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. To specify an empty string value, either don't provide this or specify it as "".

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 Java V2
- AWS SDK for Ruby V3

ResourceViolation

Violation detail based on resource type.

Contents

AwsEc2InstanceViolation

Violation detail for an EC2 instance.

Type: AwsEc2InstanceViolation object

Required: No

AwsEc2NetworkInterfaceViolation

Violation detail for a network interface.

Type: AwsEc2NetworkInterfaceViolation object

Required: No

AwsVPCSecurityGroupViolation

Violation detail for security groups.

Type: AwsVPCSecurityGroupViolation 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 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 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 object

Required: No

FirewallSubnetIsOutOfScopeViolation

Contains details about the firewall subnet that violates the policy scope.

Type: FirewallSubnetIsOutOfScopeViolation object

Required: No

FirewallSubnetMissingVPCEndpointViolation

The violation details for a third-party firewall's VPC endpoint subnet that was deleted.

Type: FirewallSubnetMissingVPCEndpointViolation object

Required: No

InvalidNetworkAclEntriesViolation

Violation detail for the entries in a network ACL resource.

Type: InvalidNetworkAclEntriesViolation 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 object

Required: No

NetworkFirewallInternetTrafficNotInspectedViolation

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

Type: NetworkFirewallInternetTrafficNotInspectedViolation object

Required: No

NetworkFirewallInvalidRouteConfigurationViolation

The route configuration is invalid.

Type: NetworkFirewallInvalidRouteConfigurationViolation object

Required: No

NetworkFirewallMissingExpectedRoutesViolation

Expected routes are missing from AWS Network Firewall.

Type: NetworkFirewallMissingExpectedRoutesViolation 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 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 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 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 object

Required: No

NetworkFirewallUnexpectedFirewallRoutesViolation

There's an unexpected firewall route.

Type: NetworkFirewallUnexpectedFirewallRoutesViolation object

Required: No

NetworkFirewallUnexpectedGatewayRoutesViolation

There's an unexpected gateway route.

Type: NetworkFirewallUnexpectedGatewayRoutesViolation 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 object

Required: No

RouteHasOutOfScopeEndpointViolation

Contains details about the route endpoint that violates the policy scope.

Type: RouteHasOutOfScopeEndpointViolation object

Required: No

ThirdPartyFirewallMissingExpectedRouteTableViolation

The violation details for a third-party firewall that has the Firewall Manager managed route table that was associated with the third-party firewall has been deleted.

Type: ThirdPartyFirewallMissingExpectedRouteTableViolation object

Required: No

ThirdPartyFirewallMissingFirewallViolation

The violation details for a third-party firewall that's been deleted.

Type: ThirdPartyFirewallMissingFirewallViolation object

Required: No

ThirdPartyFirewallMissingSubnetViolation

The violation details for a third-party firewall's subnet that's been deleted.

Type: ThirdPartyFirewallMissingSubnetViolation object

Required: No

WebACLHasIncompatibleConfigurationViolation

The violation details for a web ACL whose configuration is incompatible with the Firewall Manager policy.

Type: WebACLHasIncompatibleConfigurationViolation object

Required: No

WebACLHasOutOfScopeResourcesViolation

The violation details for a web ACL that's associated with at least one resource that's out of scope of the Firewall Manager policy.

Type: WebACLHasOutOfScopeResourcesViolation 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 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 Java V2
- AWS SDK for Ruby V3

RouteHasOutOfScopeEndpointViolation

Contains details about the route endpoint that violates the policy scope.

Contents

CurrentFirewallSubnetRouteTable

The route table associated with the current firewall subnet.

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 associated with the Internet Gateway.

Type: String

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

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

Required: No

FirewallSubnetId

The ID of the firewall subnet.

Type: String

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

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

Required: No

FirewallSubnetRoutes

The list of firewall subnet routes.

Type: Array of Route objects

Required: No

InternetGatewayId

The ID of the Internet Gateway.

Type: String

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

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

Required: No

InternetGatewayRoutes

The routes in the route table associated with the Internet Gateway.

Type: Array of Route objects

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

SubnetAvailabilityZone

The subnet's Availability Zone.

Type: String

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

Required: No

SubnetAvailabilityZoneId

The ID of the subnet's Availability Zone.

Type: String

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

Required: No

SubnetId

The ID of the subnet associated with the route that violates the policy scope.

Type: String

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

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

Required: No

ViolatingRoutes

The list of routes that violate the route table.

Type: Array of Route objects

Required: No

VpcId

The VPC ID of the route that violates the policy scope.

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 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 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 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 Java V2
- AWS SDK for Ruby V3

SecurityServicePolicyData

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

Contents

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 | THIRD_PARTY_FIREWALL | IMPORT_NETWORK_FIREWALL | NETWORK_ACL_COMMON`

Required: Yes

ManagedServiceData

Details about the service that are specific to the service type, in JSON format.

- 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: `IMPORT_NETWORK_FIREWALL`

```
"{\"type\":\"IMPORT_NETWORK_FIREWALL\",\"awsNetworkFirewallConfig\":
{\"networkFirewallStatelessRuleGroupReferences\":[{\"resourceARN\":
```

```
\"arn:aws:network-firewall:us-west-2:000000000000:stateless-rulegroup
\/rg1\",\"priority\":1}],\"networkFirewallStatelessDefaultActions
\":[\"aws:drop\"],\"networkFirewallStatelessFragmentDefaultActions
\":[\"aws:pass\"],\"networkFirewallStatelessCustomActions\":[],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN\":
\"arn:aws:network-firewall:us-west-2:aws-managed:stateful-rulegroup
\/ThreatSignaturesEmergingEventsStrictOrder\",\"priority\":8}],
\"networkFirewallStatefulEngineOptions\":{\"ruleOrder\":\"STRICT_ORDER
\"},\"networkFirewallStatefulDefaultActions\":[\"aws:drop_strict\"]}}"

"{\"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` - Centralized deployment model

```
"{\"type\":\"NETWORK_FIREWALL\",\"awsNetworkFirewallConfig
\":{\"networkFirewallStatelessRuleGroupReferences
\":[{\"resourceARN\":\"arn:aws:network-firewall:us-
east-1:123456789011:stateless-rulegroup/test\",\"priority\":1}],
\"networkFirewallStatelessDefaultActions\":[\"aws:forward_to_sfe\",
\"customActionName\"],\"networkFirewallStatelessFragmentDefaultActions
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessCustomActions\":[{\"actionName\":
\"customActionName\",\"actionDefinition\":{\"publishMetricAction
\":{\"dimensions\":[{\"value\":\"metricdimensionvalue\"}]}}}],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
\":\"arn:aws:network-firewall:us-east-1:123456789011:stateful-
rulegroup/test\"}],\"networkFirewallLoggingConfiguration
\":{\"logDestinationConfigs\":[{\"logDestinationType\":
\"S3\",\"logType\":\"ALERT\",\"logDestination\":{\"bucketName
\":\"s3-bucket-name\"}},{\"logDestinationType\":\"S3\",
```

```
\"logType\":\"FLOW\",\"logDestination\":{\"bucketName\":
\"s3-bucket-name\"}}],\"overrideExistingConfig\":true}},
\"firewallDeploymentModel\":{\"centralizedFirewallDeploymentModel
\":{\"centralizedFirewallOrchestrationConfig\":{\"inspectionVpcIds
\":[{\"resourceId\":\"vpc-1234\",\"accountId\":\"123456789011\"}],
\"firewallCreationConfig\":{\"endpointLocation\":
{\"availabilityZoneConfigList\":[{\"availabilityZoneId\":null,
\"availabilityZoneName\":\"us-east-1a\",\"allowedIPV4CidrList\":
[\"10.0.0.0/28\"]}]}},\"allowedIPV4CidrList\":[]}}}"
```

To use the centralized deployment model, you must set PolicyOption to CENTRALIZED.

- Example: NETWORK_FIREWALL - Distributed deployment model with automatic Availability Zone configuration

```
"{\"type\":\"NETWORK_FIREWALL\",
\"networkFirewallStatelessRuleGroupReferences\":[{\"resourceARN\":
\"arn:aws:network-firewall:us-east-1:123456789011:stateless-rulegroup/
test\",\"priority\":1}],\"networkFirewallStatelessDefaultActions
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessFragmentDefaultActions
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessCustomActions\":[{\"actionName\":
\"customActionName\",\"actionDefinition\":{\"publishMetricAction
\":{\"dimensions\":[{\"value\":\"metricdimensionvalue\"}]}}}],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
\":\"arn:aws:network-firewall:us-east-1:123456789011:stateful-
rulegroup/test\"}],\"networkFirewallOrchestrationConfig\":
{\"singleFirewallEndpointPerVPC\":false,\"allowedIPV4CidrList\":
[\"10.0.0.0/28\",\"192.168.0.0/28\"],\"routeManagementAction\":\"OFF
\"},\"networkFirewallLoggingConfiguration\":{\"logDestinationConfigs
\":[{\"logDestinationType\":\"S3\",\"logType\":\"ALERT\",
\"logDestination\":{\"bucketName\":\"s3-bucket-name\"}},
{\"logDestinationType\":\"S3\",\"logType\":\"FLOW\",\"logDestination
\":{\"bucketName\":\"s3-bucket-name\"}}],\"overrideExistingConfig
\":true}}"
```

With automatic Availbility Zone configuration, Firewall Manager chooses which Availability Zones to create the endpoints in. To use the distributed deployment model, you must set PolicyOption to NULL.

- Example: NETWORK_FIREWALL - Distributed deployment model with automatic Availability Zone configuration and route management

```
"{\"type\":\"NETWORK_FIREWALL\",
\"networkFirewallStatelessRuleGroupReferences\":[{\"resourceARN\":
\"arn:aws:network-firewall:us-east-1:123456789011:stateless-rulegroup/
test\",\"priority\":1}],\"networkFirewallStatelessDefaultActions
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessFragmentDefaultActions
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessCustomActions\":[{\"actionName\":
\"customActionName\",\"actionDefinition\":{\"publishMetricAction
\":{\"dimensions\":[{\"value\":\"metricdimensionvalue\"}]}}}],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
\":\"arn:aws:network-firewall:us-east-1:123456789011:stateful-
rulegroup/test\"}],\"networkFirewallOrchestrationConfig\":
{\"singleFirewallEndpointPerVPC\":false,\"allowedIPV4CidrList\":
[\"10.0.0.0/28\",\"192.168.0.0/28\"],\"routeManagementAction\":
\"MONITOR\",\"routeManagementTargetTypes\":[\"InternetGateway\"]},
\"networkFirewallLoggingConfiguration\":{\"logDestinationConfigs\":
[{\"logDestinationType\":\"S3\",\"logType\":\"ALERT\",\"logDestination
\":{\"bucketName\":\"s3-bucket-name\"}},{\"logDestinationType\":
\"S3\",\"logType\": \"FLOW\",\"logDestination\":{\"bucketName\":\"s3-
bucket-name\"}}],\"overrideExistingConfig\":true}}"
```

To use the distributed deployment model, you must set PolicyOption to NULL.

- Example: NETWORK_FIREWALL - Distributed deployment model with custom Availability Zone configuration

```
"{\"type\":\"NETWORK_FIREWALL\",
\"networkFirewallStatelessRuleGroupReferences\":[{\"resourceARN\":
\"arn:aws:network-firewall:us-east-1:123456789011:stateless-rulegroup/
test\",\"priority\":1}],\"networkFirewallStatelessDefaultActions
```

```
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessFragmentDefaultActions\":
[\"aws:forward_to_sfe\",\"fragmentcustomactionname\"],
\"networkFirewallStatelessCustomActions\":[{\"actionName\":
\"customActionName\", \"actionDefinition\":{\"publishMetricAction
\":{\"dimensions\":[{\"value\":\"metricdimensionvalue
\"}]}}},{\"actionName\":\"fragmentcustomactionname\",
\"actionDefinition\":{\"publishMetricAction\":{\"dimensions
\":[{\"value\":\"fragmentmetricdimensionvalue\"}]}}}],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
\":\"arn:aws:network-firewall:us-east-1:123456789011:stateful-
rulegroup/test\"}],\"networkFirewallOrchestrationConfig
\":{\"firewallCreationConfig\":{ \"endpointLocation\":
{\"availabilityZoneConfigList\":[{\"availabilityZoneName\":
\"us-east-1a\",\"allowedIPV4CidrList\":[\"10.0.0.0/28\"]},
{\"availabilityZoneName\":\"us-east-1b\",\"allowedIPV4CidrList\":
[ \"10.0.0.0/28\"]}]} },\"singleFirewallEndpointPerVPC\":false,
\"allowedIPV4CidrList\":null,\"routeManagementAction\":\"OFF\",
\"networkFirewallLoggingConfiguration\":{\"logDestinationConfigs\":
[{\"logDestinationType\":\"S3\",\"logType\":\"ALERT\",\"logDestination
\":{\"bucketName\":\"s3-bucket-name\"}},{\"logDestinationType\":
\"S3\",\"logType\":\"FLOW\",\"logDestination\":{\"bucketName\":\"s3-
bucket-name\"}}],\"overrideExistingConfig\":boolean}}"
```

With custom Availability Zone configuration, you define which specific Availability Zones to create endpoints in by configuring `firewallCreationConfig`. To configure the Availability Zones in `firewallCreationConfig`, specify either the `availabilityZoneName` or `availabilityZoneId` parameter, not both parameters.

To use the distributed deployment model, you must set PolicyOption to `NULL`.

- Example: `NETWORK_FIREWALL` - Distributed deployment model with custom Availability Zone configuration and route management

```
"{\"type\":\"NETWORK_FIREWALL\",
\"networkFirewallStatelessRuleGroupReferences\":[{\"resourceARN\":
\"arn:aws:network-firewall:us-east-1:123456789011:stateless-rulegroup/
test\",\"priority\":1}],\"networkFirewallStatelessDefaultActions
```

```
\":[\"aws:forward_to_sfe\",\"customActionName\"],
\"networkFirewallStatelessFragmentDefaultActions\":
[\"aws:forward_to_sfe\",\"fragmentcustomactionname\"],
\"networkFirewallStatelessCustomActions\":[{\"actionName\":
\"customActionName\",\"actionDefinition\":{\"publishMetricAction
\":{\"dimensions\":[{\"value\":\"metricdimensionvalue
\"}]}}},{\"actionName\":\"fragmentcustomactionname\",
\"actionDefinition\":{\"publishMetricAction\":{\"dimensions
\":[{\"value\":\"fragmentmetricdimensionvalue\"}]}}}],
\"networkFirewallStatefulRuleGroupReferences\":[{\"resourceARN
\":\"arn:aws:network-firewall:us-east-1:123456789011:stateful-
rulegroup/test\"}],\"networkFirewallOrchestrationConfig
\":{\"firewallCreationConfig\":{\"endpointLocation\":
{\"availabilityZoneConfigList\":[{\"availabilityZoneName\":
\"us-east-1a\",\"allowedIPV4CidrList\":[\"10.0.0.0/28\"]},
{\"availabilityZoneName\":\"us-east-1b\",\"allowedIPV4CidrList
\":[\"10.0.0.0/28\"]}]}},\"singleFirewallEndpointPerVPC\":false,
\"allowedIPV4CidrList\":null,\"routeManagementAction\":\"MONITOR
\",\"routeManagementTargetTypes\":[\"InternetGateway\"],
\"routeManagementConfig\":{\"allowCrossAZTrafficIfNoEndpoint\":true}},
\"networkFirewallLoggingConfiguration\":{\"logDestinationConfigs\":
[{\"logDestinationType\":\"S3\",\"logType\":\"ALERT\",\"logDestination
\":{\"bucketName\":\"s3-bucket-name\"}},{\"logDestinationType\":
\"S3\",\"logType\":\"FLOW\",\"logDestination\":{\"bucketName\":\"s3-
bucket-name\"}}],\"overrideExistingConfig\":boolean}}"
```

To use the distributed deployment model, you must set PolicyOption to NULL.

- Example: SECURITY_GROUPS_COMMON

```
"{\"type\":\"SECURITY_GROUPS_COMMON\",\"securityGroups\":[{\"id
\":\"sg-03b1f67d69ed00197\"}],\"revertManualSecurityGroupChanges
\":true,\"exclusiveResourceSecurityGroupManagement\":true,
\"applyToAllEC2InstanceENIs\":false,\"includeSharedVPC\":true,
\"enableSecurityGroupReferencesDistribution\":true}"
```

- Example: SECURITY_GROUPS_COMMON - Security group tag distribution

```
""{\"type\":\"SECURITY_GROUPS_COMMON\",\"securityGroups\":[{\"id
\":\"sg-000e55995d61a06bd\"}],\"revertManualSecurityGroupChanges
\":true,\"exclusiveResourceSecurityGroupManagement\":false,
\"applyToAllEC2InstanceENIs\":false,\"includeSharedVPC\":false,
\"enableTagDistribution\":true}""
```

Firewall Manager automatically distributes tags from the primary group to the security groups created by this policy. To use security group tag distribution, you must also set `revertManualSecurityGroupChanges` to `true`, otherwise Firewall Manager won't be able to create the policy. When you enable `revertManualSecurityGroupChanges`, Firewall Manager identifies and reports when the security groups created by this policy become non-compliant.

Firewall Manager won't distribute system tags added by AWS services into the replica security groups. System tags begin with the `aws:` prefix.

- 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\",\"preManagedOptions\":
[{\"denyProtocolAllValue\":true},{\"auditSgDirection\":{\"type\":
\"ALL\"}}],\"securityGroups\":[{\"id\":\"sg-049b2393a25468971\"}],
\"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,\"optionalDelayForUnusedInMinutes\":60}"
```

- Example: SHIELD_ADVANCED with web ACL management

  ```
  "{\"type\":\"SHIELD_ADVANCED\",\"optimizeUnassociatedWebACL\":true}"
  ```

  If you set optimizeUnassociatedWebACL to true, Firewall Manager creates web ACLs in accounts within the policy scope if the web ACLs will be used by at least one resource. Firewall Manager creates web ACLs in the accounts within policy scope only if the web ACLs will be used by at least one resource. If at any time an account comes into policy scope, Firewall Manager automatically creates a web ACL in the account if at least one resource will use the web ACL.

  Upon enablement, Firewall Manager performs a one-time cleanup of unused web ACLs in your account. The cleanup process can take several hours. If a resource leaves policy scope after Firewall Manager creates a web ACL, Firewall Manager doesn't disassociate the resource from the web ACL. If you want Firewall Manager to clean up the web ACL, you must first manually disassociate the resources from the web ACL, and then enable the manage unused web ACLs option in your policy.

  If you set optimizeUnassociatedWebACL to false, and Firewall Manager automatically creates an empty web ACL in each account that's within policy scope.

- Specification for SHIELD_ADVANCED for Amazon CloudFront distributions and ALB

  ```
  "{\"type\":\"SHIELD_ADVANCED\",\"automaticResponseConfiguration
  \": {\"automaticResponseStatus\":\"ENABLED|IGNORED|
  DISABLED\", \"automaticResponseAction\":\"BLOCK|COUNT
  \"}, \"overrideCustomerWebaclClassic\":true|false,
  \"optimizeUnassociatedWebACL\":true|false}"
  ```

  For example: `"{\"type\":\"SHIELD_ADVANCED\",
  \"automaticResponseConfiguration\": {\"automaticResponseStatus\":
  \"ENABLED\", \"automaticResponseAction\":\"COUNT\"}}"`

  The default value for automaticResponseStatus is IGNORED. The value for automaticResponseAction is only required when automaticResponseStatus is set to ENABLED. The default value for overrideCustomerWebaclClassic is false.

For other resource types that you can protect with a Shield Advanced policy, this ManagedServiceData configuration is an empty string.

- Example: THIRD_PARTY_FIREWALL

  Replace THIRD_PARTY_FIREWALL_NAME with the name of the third-party firewall.

  ```
  "{ "type":"THIRD_PARTY_FIREWALL",
  "thirdPartyFirewall":"THIRD_PARTY_FIREWALL_NAME",
  "thirdPartyFirewallConfig":{ "thirdPartyFirewallPolicyList":
  ["global-1"] }, "firewallDeploymentModel":
  { "distributedFirewallDeploymentModel":
  { "distributedFirewallOrchestrationConfig":{ "firewallCreationConfig":
  { "endpointLocation":{ "availabilityZoneConfigList":
  [ { "availabilityZoneName":"${AvailabilityZone}" } ] } },
  "allowedIPV4CidrList":[ ] } } } }"
  ```

- Example: WAFV2 - Account takeover prevention, Bot Control managed rule groups, optimize unassociated web ACL, and rule action override

  ```
  "{\"type\":\"WAFV2\",\"preProcessRuleGroups\":[{\"ruleGroupType
  \":\"ManagedRuleGroup\",\"overrideAction\":{\"type\":\"NONE
  \"},\"sampledRequestsEnabled\":true,\"excludeRules\":[],
  \"managedRuleGroupIdentifier\":{\"managedRuleGroupName\":
  \"AWSManagedRulesAntiDDoSRuleSet\",\"vendorName\":\"AWS\",
  \"versionEnabled\":null,\"version\":null,\"managedRuleGroupConfigs
  \":[{\"awsmanagedRulesAntiDDoSRuleSet\":{\"clientSideActionConfig
  \":{\"challenge\":{\"usageOfAction\":\"ENABLED\",\"sensitivity
  \":\"HIGH\",\"exemptUriRegularExpressions\":[\"\\\\/api\\\\/|\
  \\\.(acc|avi|css|gif|ico|jpe?g|js|json|mp[34]|ogg|otf|pdf|png|
  tiff?|ttf|webm|webp|woff2?|xml)$\"]}},\"sensitivityToBlock\":
  \"LOW\"}}]}},{\"ruleGroupArn\":null,\"overrideAction\":{\"type\":
  \"NONE\"},\"managedRuleGroupIdentifier\":{\"versionEnabled\":null,
  \"version\":null,\"vendorName\":\"AWS\",\"managedRuleGroupName
  \":\"AWSManagedRulesATPRuleSet\",\"managedRuleGroupConfigs\":
  [{\"awsmanagedRulesATPRuleSet\":{\"loginPath\":\"/loginpath\",
  \"requestInspection\":{\"payloadType\":\"FORM_ENCODED|JSON\",
  \"usernameField\":{\"identifier\":\"/form/username\"},\"passwordField
  ```

```
\":{\"identifier\":\"/form/password\"}}}}]},\"ruleGroupType\":
\"ManagedRuleGroup\",\"excludeRules\":[],\"sampledRequestsEnabled
\":true},{\"ruleGroupArn\":null,\"overrideAction\":{\"type\":
\"NONE\"},\"managedRuleGroupIdentifier\":{\"versionEnabled\":null,
\"version\":null,\"vendorName\":\"AWS\",\"managedRuleGroupName
\":\"AWSManagedRulesBotControlRuleSet\",\"managedRuleGroupConfigs
\":[{\"awsmanagedRulesBotControlRuleSet\":{\"inspectionLevel
\":\"TARGETED|COMMON\"}}]},\"ruleGroupType\":\"ManagedRuleGroup
\",\"excludeRules\":[],\"sampledRequestsEnabled\":true,
\"ruleActionOverrides\":[{\"name\":\"Rule1\",\"actionToUse\":
{\"allow|block|count|captcha|challenge\":{}}},{\"name\":\"Rule2\",
\"actionToUse\":{\"allow|block|count|captcha|challenge\":{}}}]},
\"postProcessRuleGroups\":[],\"defaultAction\":{\"type\":\"ALLOW
\"},\"customRequestHandling\":null,\"customResponse\":null,
\"overrideCustomerWebACLAssociation\":false,\"loggingConfiguration
\":null,\"sampledRequestsEnabledForDefaultActions\":true,
\"optimizeUnassociatedWebACL\":true}"
```

- Anti-DDoS - For information about `AWSManagedRulesAntiDDoSRuleSet` managed rule groups, see AWSManagedRulesAntiDDoSRuleSet in the *AWS WAF API Reference*.

  > **Note**
  >
  > In most cases, we recommend that you give `AWSManagedRulesAntiDDoSRuleSet` priority above other rule groups. Rule groups you create with IPSets in them should be prioritized above the `AWSManagedRulesAntiDDoSRuleSet`. In the console, the `AWSManagedRulesAntiDDoSRuleSet` is set to the highest priority by default, but you can adjust the priority when adding rule groups.

- Bot Control - For information about `AWSManagedRulesBotControlRuleSet` managed rule groups, see AWSManagedRulesBotControlRuleSet in the *AWS WAF API Reference*.
- Fraud Control account takeover prevention (ATP) - For information about the properties available for `AWSManagedRulesATPRuleSet` managed rule groups, see AWSManagedRulesATPRuleSet in the *AWS WAF API Reference*.
- Optimize unassociated web ACL - If you set `optimizeUnassociatedWebACL` to `true`, Firewall Manager creates web ACLs in accounts within the policy scope if the web ACLs will be used by at least one resource. Firewall Manager creates web ACLs in the accounts within

policy scope only if the web ACLs will be used by at least one resource. If at any time an account comes into policy scope, Firewall Manager automatically creates a web ACL in the account if at least one resource will use the web ACL.

Upon enablement, Firewall Manager performs a one-time cleanup of unused web ACLs in your account. The cleanup process can take several hours. If a resource leaves policy scope after Firewall Manager creates a web ACL, Firewall Manager disassociates the resource from the web ACL, but won't clean up the unused web ACL. Firewall Manager only cleans up unused web ACLs when you first enable management of unused web ACLs in a policy.

If you set `optimizeUnassociatedWebACL` to `false` Firewall Manager doesn't manage unused web ACLs, and Firewall Manager automatically creates an empty web ACL in each account that's within policy scope.

- Rule action overrides - Firewall Manager supports rule action overrides only for managed rule groups. To configure a `RuleActionOverrides` add the `Name` of the rule to override, and `ActionToUse`, which is the new action to use for the rule. For information about using rule action override, see RuleActionOverride in the *AWS WAF API Reference*.

- Example: `WAFV2` - `CAPTCHA` and `Challenge` configs

```
"{\"type\":\"WAFV2\",\"preProcessRuleGroups\":[{\"ruleGroupArn
\":null,\"overrideAction\":{\"type\":\"NONE\"},
\"managedRuleGroupIdentifier\":{\"versionEnabled\":null,
\"version\":null,\"vendorName\":\"AWS\",\"managedRuleGroupName
\":\"AWSManagedRulesAdminProtectionRuleSet\"},\"ruleGroupType\":
\"ManagedRuleGroup\",\"excludeRules\":[],\"sampledRequestsEnabled
\":true}],\"postProcessRuleGroups\":[],\"defaultAction\":{\"type\":
\"ALLOW\"},\"customRequestHandling\":null,\"customResponse\":null,
\"overrideCustomerWebACLAssociation\":false,\"loggingConfiguration
\":null,\"sampledRequestsEnabledForDefaultActions\":true,
\"captchaConfig\":{\"immunityTimeProperty\":{\"immunityTime\":500}},
\"challengeConfig\":{\"immunityTimeProperty\":{\"immunityTime\":800}},
\"tokenDomains\":[\"google.com\",\"amazon.com\"],\"associationConfig
\":{\"requestBody\":{\"CLOUDFRONT\":{\"defaultSizeInspectionLimit\":
\"KB_16\"}}}}"
```

  - `CAPTCHA` and `Challenge` configs - If you update the policy's values for `associationConfig`, `captchaConfig`, `challengeConfig`, or `tokenDomains`, Firewall Manager will overwrite your local web ACLs to contain the new value(s). However, if you

don't update the policy's `associationConfig`, `captchaConfig`, `challengeConfig`, or `tokenDomains` values, the values in your local web ACLs will remain unchanged. For information about association configs, see AssociationConfig. For information about CAPTCHA and Challenge configs, see CaptchaConfig and ChallengeConfig in the *AWS WAF API Reference*.

- `defaultSizeInspectionLimit` - Specifies the maximum size of the web request body component that an associated Amazon CloudFront distribution should send to AWS WAF for inspection. For more information, see DefaultSizeInspectionLimit in the *AWS WAF API Reference*.

- Example: `WAFV2` - AWS Firewall Manager support for AWS WAF managed rule group versioning

```
"{\"preProcessRuleGroups\":[{\"ruleGroupType\":\"ManagedRuleGroup
\",\"overrideAction\":{\"type\":\"NONE\"},\"sampledRequestsEnabled
\":true,\"managedRuleGroupIdentifier\":{\"managedRuleGroupName\":
\"AWSManagedRulesAdminProtectionRuleSet\",\"vendorName\":\"AWS\",
\"managedRuleGroupConfigs\":null}}],\"postProcessRuleGroups\":
[],\"defaultAction\":{\"type\":\"ALLOW\"},\"customRequestHandling
\":null,\"tokenDomains\":null,\"customResponse\":null,
\"type\":\"WAFV2\",\"overrideCustomerWebACLAssociation
\":false,\"sampledRequestsEnabledForDefaultActions\":true,
\"optimizeUnassociatedWebACL\":true,\"webACLSource\":
\"RETROFIT_EXISTING\"}"
```

  To use a specific version of a AWS WAF managed rule group in your Firewall Manager policy, you must set `versionEnabled` to `true`, and set `version` to the version you'd like to use. If you don't set `versionEnabled` to `true`, or if you omit `versionEnabled`, then Firewall Manager uses the default version of the AWS WAF managed rule group.

- Example: `WAFV2` - Logging configurations

```
"{\"type\":\"WAFV2\",\"preProcessRuleGroups\":[{\"ruleGroupArn\":null,
\"overrideAction\":{\"type\":\"NONE\"},\"managedRuleGroupIdentifier
\": {\"versionEnabled\":null,\"version\":null,\"vendorName\":\"AWS
\", \"managedRuleGroupName\":\"AWSManagedRulesAdminProtectionRuleSet
\"} ,\"ruleGroupType\":\"ManagedRuleGroup\",\"excludeRules\":[],
\"sampledRequestsEnabled\":true}],\"postProcessRuleGroups\":[],
\"defaultAction\":{\"type\":\"ALLOW\"},\"customRequestHandling
```

```
\" :null,\"customResponse\":null,\"overrideCustomerWebACLAssociation
\" :false,\"loggingConfiguration\":{\"logDestinationConfigs\":
[\"arn:aws:s3:::aws-waf-logs-example-bucket\"] ,\"redactedFields
\":[],\"loggingFilterConfigs\":{\"defaultBehavior\":\"KEEP\",
\"filters\":[{\"behavior\":\"KEEP\",\"requirement\":\"MEETS_ALL\",
\"conditions\":[{\"actionCondition\":\"CAPTCHA\"},{\"actionCondition
\": \"CHALLENGE\"}, {\"actionCondition\":\"EXCLUDED_AS_COUNT\"}]}]}},
\"sampledRequestsEnabledForDefaultActions\":true}"
```

Firewall Manager supports Amazon Kinesis Data Firehose and Amazon S3 as the `logDestinationConfigs` in your `loggingConfiguration`. For information about AWS WAF logging configurations, see LoggingConfiguration in the *AWS WAF API Reference*

In the `loggingConfiguration`, you can specify one `logDestinationConfigs`. Optionally provide as many as 20 `redactedFields`. The `RedactedFieldType` must be one of `URI`, `QUERY_STRING`, `HEADER`, or `METHOD`.

- Example: `AWS WAF Classic`

```
"{\"ruleGroups\":[{\"id\":\"78cb36c0-1b5e-4d7d-82b2-
cf48d3ad9659\",\"overrideAction\":{\"type\":\"NONE\"}}],
\"overrideCustomerWebACLAssociation\":true,\"defaultAction\":{\"type
\":\"ALLOW\"},\"type\":\"WAF\"}"
```

Type: String

Length Constraints: Minimum length of 1. Maximum length of 30000.

Pattern: `^((?!\\[nr]).)+`

Required: No

PolicyOption

Contains the settings to configure a network ACL policy, a AWS Network Firewall firewall policy deployment model, or a third-party firewall policy.

Type: PolicyOption 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 Java V2
- AWS SDK for Ruby V3

StatefulEngineOptions

Configuration settings for the handling of the stateful rule groups in a Network Firewall firewall policy.

Contents

RuleOrder

Indicates how to manage the order of stateful rule evaluation for the policy. Stateful rules are provided to the rule engine as Suricata compatible strings, and Suricata evaluates them based on certain settings. For more information, see Evaluation order for stateful rules in the *AWS Network Firewall Developer Guide*.

Default: `DEFAULT_ACTION_ORDER`

Type: String

Valid Values: `STRICT_ORDER | DEFAULT_ACTION_ORDER`

Required: No

StreamExceptionPolicy

Indicates how Network Firewall should handle traffic when a network connection breaks midstream.

- `DROP` - Fail closed and drop all subsequent traffic going to the firewall.
- `CONTINUE` - Continue to apply rules to subsequent traffic without context from traffic before the break. This impacts the behavior of rules that depend on context. For example, with a stateful rule that drops HTTP traffic, Network Firewall won't match subsequent traffic because the it won't have the context from session initialization, which defines the application layer protocol as HTTP. However, a TCP-layer rule using a `flow:stateless` rule would still match, and so would the `aws:drop_strict` default action.
- `REJECT` - Fail closed and drop all subsequent traffic going to the firewall. With this option, Network Firewall also sends a TCP reject packet back to the client so the client can immediately establish a new session. With the new session, Network Firewall will have context and will apply rules appropriately.

  For applications that are reliant on long-lived TCP connections that trigger Gateway Load Balancer idle timeouts, this is the recommended setting.

- `FMS_IGNORE` - Firewall Manager doesn't monitor or modify the Network Firewall stream exception policy settings.

For more information, see Stream exception policy in your firewall policy in the *AWS Network Firewall Developer Guide*.

Default: `FMS_IGNORE`

Type: String

Valid Values: `DROP | CONTINUE | REJECT | FMS_IGNORE`

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 Java V2
- AWS SDK for Ruby V3

StatefulRuleGroup

AWS Network Firewall stateful rule group, used in a NetworkFirewallPolicyDescription.

Contents

Override

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

Type: NetworkFirewallStatefulRuleGroupOverride object

Required: No

Priority

An integer setting that indicates the order in which to run the stateful rule groups in a single Network Firewall firewall policy. This setting only applies to firewall policies that specify the `STRICT_ORDER` rule order in the stateful engine options settings.

Network Firewall evalutes each stateful rule group against a packet starting with the group that has the lowest priority setting. You must ensure that the priority settings are unique within each policy. For information about

You can change the priority settings of your rule groups at any time. To make it easier to insert rule groups later, number them so there's a wide range in between, for example use 100, 200, and so on.

Type: Integer

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 Java V2
- AWS SDK for Ruby V3

StatelessRuleGroup

AWS Network Firewall stateless rule group, used in a NetworkFirewallPolicyDescription.

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 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 Java V2
- AWS SDK for Ruby V3

ThirdPartyFirewallFirewallPolicy

Configures the third-party firewall's firewall policy.

Contents

FirewallPolicyId

The ID of the specified firewall policy.

Type: String

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

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

Required: No

FirewallPolicyName

The name of the specified firewall policy.

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 Java V2
- AWS SDK for Ruby V3

ThirdPartyFirewallMissingExpectedRouteTableViolation

The violation details for a third-party firewall that's not associated with an AWS Firewall Manager managed route table.

Contents

AvailabilityZone

The Availability Zone of the firewall subnet that's causing the violation.

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 third-party firewall or VPC resource that's causing the 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 fireawll subnet that's causing the violation.

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 Java V2
- AWS SDK for Ruby V3

ThirdPartyFirewallMissingFirewallViolation

The violation details about a third-party firewall's subnet that doesn't have a Firewall Manager managed firewall in its VPC.

Contents

AvailabilityZone

The Availability Zone of the third-party firewall that's causing the violation.

Type: String

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

Required: No

TargetViolationReason

The reason the resource is causing this violation, if a reason is available.

Type: String

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

Pattern: `\w+`

Required: No

ViolationTarget

The ID of the third-party firewall that's causing the 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 third-party firewall.

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 Java V2
- AWS SDK for Ruby V3

ThirdPartyFirewallMissingSubnetViolation

The violation details for a third-party firewall for an Availability Zone that's missing the Firewall Manager managed subnet.

Contents

AvailabilityZone

The Availability Zone of a subnet that's causing the violation.

Type: String

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

Required: No

TargetViolationReason

The reason the resource is causing the violation, if a reason is available.

Type: String

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

Pattern: `\w+`

Required: No

ViolationTarget

The ID of the third-party firewall or VPC resource that's causing the 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 subnet that's causing the violation.

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 Java V2
- AWS SDK for Ruby V3

ThirdPartyFirewallPolicy

Configures the deployment model for the third-party firewall.

Contents

FirewallDeploymentModel

Defines the deployment model to use for the third-party firewall policy.

Type: String

Valid Values: `CENTRALIZED | DISTRIBUTED`

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 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

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

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 objects

Required: Yes

ResourceDescription

Brief description for the requested resource.

Type: String

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

Required: No

ResourceTags

The `ResourceTag` objects associated with the resource.

Type: Array of Tag objects

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

Required: No

See Also

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

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

WebACLHasIncompatibleConfigurationViolation

The violation details for a web ACL whose configuration is incompatible with the Firewall Manager policy.

Contents

Description

Information about the problems that Firewall Manager encountered with the web ACL configuration.

Type: String

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

Required: No

WebACLArn

The Amazon Resource Name (ARN) of the web ACL.

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 Java V2
- AWS SDK for Ruby V3

WebACLHasOutOfScopeResourcesViolation

The violation details for a web ACL that's associated with at least one resource that's out of scope of the Firewall Manager policy.

Contents

OutOfScopeResourceList

An array of Amazon Resource Name (ARN) for the resources that are out of scope of the policy and are associated with the web ACL.

Type: Array of strings

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

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

Required: No

WebACLArn

The Amazon Resource Name (ARN) of the web ACL.

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 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 Signing AWS API requests in the *IAM User Guide*.

X-Amz-Algorithm

The hash algorithm that you used to create the request signature.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Valid Values: `AWS4-HMAC-SHA256`

Required: Conditional

X-Amz-Credential

The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: `20120325T120000Z`.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see Elements of an AWS API request signature in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

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

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Error Types

This section lists common error types that this AWS service may return. Not all services return all error types listed here. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You don't have permission to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request has expired. Request a new security token and try again.

HTTP Status Code: 403

IncompleteSignature

The request signature doesn't conform to AWS standards. Verify that you're using valid AWS credentials and that your request is properly formatted. If you're using an SDK, ensure it's up to date.

HTTP Status Code: 403

InternalFailure

The request can't be processed right now because of an internal server issue. Try again later. If the problem persists, contact AWS Support.

HTTP Status Code: 500

MalformedHttpRequestException

The request body can't be processed. This typically happens when the request body can't be decompressed using the specified content encoding algorithm. Verify that the content encoding header matches the compression format used.

HTTP Status Code: 400

NotAuthorized

You don't have permissions to perform this action. Verify that your IAM policy includes the required permissions.

HTTP Status Code: 401

OptInRequired

Your AWS account needs a subscription for this service. Verify that you've enabled the service in your account.

HTTP Status Code: 403

RequestAbortedException

The request was aborted before a response could be returned. This typically happens when the client closes the connection.

HTTP Status Code: 400

RequestEntityTooLargeException

The request entity is too large. Reduce the size of the request body and try again.

HTTP Status Code: 413

RequestTimeoutException

The request timed out. The server didn't receive the complete request within the expected time frame. Try again.

HTTP Status Code: 408

ServiceUnavailable

The service is temporarily unavailable. Try again later.

HTTP Status Code: 503

ThrottlingException

Your request rate is too high. The AWS SDKs automatically retry requests that receive this exception. Reduce the frequency of requests.

HTTP Status Code: 400

UnknownOperationException

The action or operation isn't recognized. Verify that the action name is spelled correctly and that it's supported by the API version you're using.

HTTP Status Code: 404

UnrecognizedClientException

The X.509 certificate or AWS access key ID you provided doesn't exist in our records. Verify that you're using valid credentials and that they haven't expired.

HTTP Status Code: 403

ValidationError

The input doesn't meet the required format or constraints. Check that all required parameters are included and that values are valid.

HTTP Status Code: 400