Windows PowerShell Get-Help on Cmdlet 'New-AzFirewallPolicyIntrusionDetectionBypassTraffic'

PS:\>Get-HELP New-AzFirewallPolicyIntrusionDetectionBypassTraffic -Full

WARNING: The names of some imported commands from the module 'Microsoft.Azure.PowerShell.Cmdlets.Network' include unapproved verbs that might make them less discoverable.

To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

NAME

New-AzFirewallPolicyIntrusionDetectionBypassTraffic

SYNOPSIS

Creates a new Azure Firewall Policy Intrusion Detection Bypass Traffic Setting

SYNTAX

New-AzFirewallPolicyIntrusionDetectionBypassTraffic [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]

[-Description <System.String>] [-DestinationAddress <System.String[]>] [-DestinationIpGroup <System.String[]>] -DestinationPort <System.String[]> -Name

<System.String> -Protocol {TCP | UDP | ICMP | ANY} [-SourceAddress <System.String[]>] [-SourceIpGroup <System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallPolicyIntrusionDetectionBypassTraffic cmdlet creates an Azure Firewall Policy Intrusion Detection Bypass Traffic Object.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-Description <System.String>

Bypass setting description.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-DestinationAddress <System.String[]>

List of destination IP addresses or ranges.

Required? false
Position? named
Default value None
Accept pipeline input? False
Accept wildcard characters? false

-DestinationIpGroup <System.String[]>

List of destination IpGroups.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationPort <System.String[]>

List of destination ports or ranges.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Bypass setting name.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Protocol <System.String>

Bypass setting protocol.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourceAddress <System.String[]>

List of source IP addresses or ranges.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourceIpGroup <System.String[]>

List of source IpGroups.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

None

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetectionBypassTrafficSetting

NOTES

Example 1: Create bypass traffic with specific port and source address

```
$bypass = New-AzFirewallPolicyIntrusionDetectionBypassTraffic -Name "bypass-setting" -Protocol "TCP"
-DestinationPort "80" -SourceAddress "10.0.0.0"
-DestinationAddress "*"
New-AzFirewallPolicyIntrusionDetection -Mode "Deny" -BypassTraffic $bypass
```

This example creates intrusion detection with bypass traffic setting

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/az.network/new-azfirewallpolicyintrusiondetectionbypasstraffic