Enable Security Features Using Configuration Groups for SDWAN

Contents

Introduction

This document describes configuring NGFW, URL filtering, AMP, and IPS/IDS via configuration groups, including instructions for unified logging.

Prerequisites

Enable flow-visibily and app-visibility

If you are using Policy groups to define policies :

- Select Policy group and then select Application priority and SLA.
- Select Add new
- Click Additional settings and enable Application visibility and Flow visibility

If you are using the legacy policy

- Select a Cli Add-on Profile in Configuration Group and add these commands

```
policy
app-visibility
flow-visibility
```

Ensure that you comply with the prerequisites for the features as given here https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/security/ios-xe-17/security-book-xe/url-filtering.html

```
Note: If you are using the legacy policy along with Configuration groups :

Select Configuration and Click Security
Click Custom Options and select Policies/Profiles and then access these features to enable
```

This document focuses on the features to be enabled using Policy groups

Next Gen Firewall (NGFW)

To enable NGFW perform the steps as mentioned:

- Select Policy group and click NGFW and click Add NGFW Policy
- Give it a Policy Name and click Next
- Select Configuration group to associate with the NGFW Policy
- Add the rules and click Next
- Create your NGFW Policy

To enable ulogging ,Edit the NGFW Policy and then Select Additional Settings and turn on Unified Logging

URL Filtering

To enable URL filtering for releases before 20.18:

- Select Configuration on UI and then Policy group and then click Groups of Interest
- Select Security and then expand Profiles

To enable url filtering for releases 20.18 and later :

- Select Configuration on UI and then Policy group and then click Objects and Profiles
- Select Security Profiles

Select add url filtering,enter the details and click save

Advanced Malware Protection(AMP)

To enable AMP for releases before 20.18:

- Select Configuration on UI and then Policy group and then click Groups of Interest
- Select Security and then expand Profiles

To enable AMP for releases 20.18 and later :

- Select Configuration on UI and then Policy group and then click Objects and Profiles
- Select Security Profiles

Select Advanced Malware Protection and click Add Advanced Malware Protection

Add the details and click save

Intrusion Prevention System(IPS)/Intrusion Prevention Detection(IDS)

To enable IPS/IDS for releases before 20.18:

- Select Configuration on UI and then Policy group and then click Groups of Interest
- Select Security and then expand Profiles

To enable IPS/IDS for releases 20.18 and later :

- Select Configuration on UI and then Policy group and then click Objects and Profiles
- Select Security Profiles

Select Intrusion Prevention and click Add Intrusion Prevention

Add the details and click save

Create Advanced Inspection Profile(AIP)

To enable AIP for releases before 20.18:

- Select Configuration on UI and then Policy group and then click Groups of Interest
- Select Security and then expand Profiles

To enable AIP for releases 20.18 and later :

- Select Configuration on UI and then Policy group and then click Objects and Profiles
- Select Security Profiles

Select Advanced Inspection Profile and click Add Advanced Inspection Profile

- Enter the AMP/IPS/Url filtering names created in the earlier steps and click save

Association of AIP to NGFW

- Select Configuration and then select Policy groups and click NGFW
- Edit the NGFW policy created earlier
- For the NGFW rules created earlier ,edit and associate the AIP profile created earlier and click save

Ulogging

For ulogging ,enable the feature on the router via configuration group using cli add on

```
policy
ip visibility features
ulogging enable

parameter-map type inspect-global
log dropped-packets
log flow-export fnf
log flow
!
utd engine standard unified-policy
utd global
flow-logging all
```

Verification

```
show  flow monitor sdwan-flow-monitor cache

IPV4 SOURCE ADDRESS:                        10.100.10.75
IPV4 DESTINATION ADDRESS:                   10.10.10.25
TRNS SOURCE PORT:                           53
TRNS DESTINATION PORT:                      34796
IP VPN ID:                                  10
IP PROTOCOL:                                17
tcp flags:                                  0x00
interface input:                            Gi2
interface output:                           Gi3
flow cts source group tag:                  0
flow cts destination group tag:             0
counter bytes long:                         125
```

```
counter packets long:                              1
timestamp abs first:                               14:59:47.613
timestamp abs last:                                14:59:47.613
flow end reason:                                   Not determined
connection initiator:                              Reverse initiator
interface overlay session id input:                10
interface overlay session id output:               0
connection connection id long:                     0x000000000050D9CC
drop cause id:                                     0
counter bytes drop long:                           0
sdwan sla not met :                                0
sdwan preferred color not met :                    0
sdwan queue id :                                   2
counter packets drop long:                         0
ulogging fw zp id:                                 4
ulogging fw zone id array:                         3 3
ulogging fw class id:                              12544961
ulogging fw policy id:                             5559936
ulogging fw proto id:                              25
ulogging fw action:                                2
ulogging fw drop reason id:                        0
ulogging fw source ipv4 address translated:        0.0.0.0
ulogging fw destination ipv4 address translated:   0.0.0.0
ulogging fw source port translated:                0
ulogging fw destination port translated:           0
ulogging utd ips pri:                              1
ulogging utd ips sid:                              57756
ulogging utd ips gid:                              1
ulogging utd ips cid:                              21
ulogging utd urlf url hash:                        00000000000000000000000000000000
ulogging utd urlf url category:                    0
ulogging utd urlf url reputation:                  0
ulogging utd urlf application name:
ulogging utd amp dispos:                           0
ulogging utd amp filename hash:                    00000000000000000000000000000000
ulogging utd amp file type:                        0
ulogging utd amp file hash:                        0000000000000000000000000000000000000000000000000000000000000000
ulogging utd amp malname hash:                     00000000000000000000000000000000
ulogging utd drop reason id:                       0
ulogging sdvt drop reason id:                      0
ulogging utd ips policy id:                        1
ulogging utd ips action id:                        1
ulogging utd urlf policy id:                       N/A
ulogging utd urlf action id:                       N/A
ulogging utd amp policy id:                        N/A
ulogging utd amp action id:                        N/A
ulogging utd urlf reason id:                       0
ulogging ulogging flow direction:                  Reverse initiator
ulogging fw user name:
ulogging fw source ipv6 address translated:        ::
ulogging fw destination ipv6 address translated:   ::
ip dscp:                                           0x00
application name:                                  port dns
```