Habilitar funciones de seguridad mediante grupos de configuración para SDWAN

Contenido

Introducción

En este documento se describe la configuración de NGFW, filtrado de URL, AMP e IPS/IDS mediante grupos de configuración, incluidas instrucciones para el registro unificado.

Prerequisites

Habilitar visibilidad del flujo y de las aplicaciones

Si utiliza grupos de directivas para definir directivas:

- Seleccione Grupo de políticas y, a continuación, Prioridad de la aplicación y SLA.
- Seleccione Add New (Agregar nuevo).
- Haga clic en Configuración adicional y active Visibilidad de la aplicación y Visibilidad del flujo

Si utiliza la política heredada

- Seleccione un perfil de complemento de Cli en el grupo de configuración y agregue estos

comandos

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

Asegúrese de cumplir los requisitos previos para las funciones que se indican aquí 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
```

Este documento se centra en las funciones que se deben habilitar mediante los grupos de políticas

Firewall de última generación (NGFW)

Para activar NGFW, siga los pasos que se indican a continuación:

- Seleccione Grupo de políticas, haga clic en NGFW y, a continuación, en Agregar política NGFW
- Asigne un nombre a la directiva y haga clic en Next (Siguiente)
- Seleccione el grupo de configuración que desea asociar a la política de NGFW.
- Agregue las reglas y haga clic en Siguiente
- Cree su política de NGFW

Para habilitar el desregistro, edite la política de NGFW, seleccione Parámetros adicionales y active el registro unificado

Filtrado de URL

Para activar el filtrado de URL para versiones anteriores a 20.18:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de políticas y haga clic en Grupos de interés
- Seleccione Seguridad y expanda Perfiles

Para habilitar el filtrado de url para las versiones 20.18 y posteriores:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de directivas y, a continuación, haga clic en Objetos y perfiles
- Seleccionar perfiles de seguridad

Seleccione agregar filtrado de URL, introduzca los detalles y haga clic en guardar

Advanced Malware Protection (AMP)

Para activar AMP para versiones anteriores a 20.18:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de políticas y haga clic en Grupos de interés
- Seleccione Seguridad y expanda Perfiles

Para habilitar AMP para las versiones 20.18 y posteriores:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de directivas y, a continuación, haga clic en Objetos y perfiles
- Seleccionar perfiles de seguridad

Seleccione Protección frente a malware avanzado y haga clic en Agregar protección frente a malware avanzado

Agregue los detalles y haga clic en Guardar

Sistema de prevención de intrusiones (IPS)/Detección de prevención de intrusiones (IDS)

Para activar IPS/IDS para versiones anteriores a 20.18:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de políticas y

haga clic en Grupos de interés
- Seleccione Seguridad y expanda Perfiles

Para activar IPS/IDS para las versiones 20.18 y posteriores:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de directivas y, a continuación, haga clic en Objetos y perfiles
- Seleccionar perfiles de seguridad

Seleccione Prevención de intrusiones y haga clic en Agregar prevención de intrusiones

Agregue los detalles y haga clic en Guardar

Crear perfil de inspección avanzado (AIP)

Para activar AIP para versiones anteriores a 20.18:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de políticas y haga clic en Grupos de interés
- Seleccione Seguridad y expanda Perfiles

Para habilitar AIP para las versiones 20.18 y posteriores:

- Seleccione Configuración en la interfaz de usuario y, a continuación, Grupo de directivas y, a continuación, haga clic en Objetos y perfiles
- Seleccionar perfiles de seguridad

Seleccione Perfil de inspección avanzado y haga clic en Agregar perfil de inspección avanzado

- Introduzca los nombres de filtrado de AMP/IPS/URL creados en los pasos anteriores y haga clic en Guardar

Asociación de AIP a NGFW

- Seleccione Configuración y, a continuación, Grupos de políticas y haga clic en NGFW
- Editar la política de NGFW creada anteriormente
- Para las reglas de NGFW creadas anteriormente, edite y asocie el perfil AIP creado anteriormente y haga clic en Guardar

Ulogging

Para la desconexión , habilite la función en el router a través del grupo de configuración mediante 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
```

Verificación

```
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
```

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).