Activer les fonctions de sécurité en utilisant des groupes de configuration pour SDWAN

Table des matières

Introduction

Ce document décrit la configuration du pare-feu de nouvelle génération, du filtrage des URL, d'AMP et d'IPS/IDS via des groupes de configuration, y compris les instructions de journalisation unifiée.

Conditions préalables

Permettre une visibilité sur les flux et les applications

Si vous utilisez des groupes de stratégies pour définir des stratégies :

- Sélectionnez Groupe de stratégies, puis Priorité de l'application et SLA.
- Sélectionnez Add New (ajouter nouveau)
- Cliquez sur Paramètres supplémentaires et activez la visibilité sur les applications et sur les flux

Si vous utilisez la stratégie héritée

- Sélectionnez un profil de module complémentaire Cli dans le groupe de configuration et ajoutez ces commandes

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

Assurez-vous de respecter les conditions requises pour les fonctionnalités, comme indiqué ici 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
```

Ce document se concentre sur les fonctionnalités à activer à l'aide des groupes de stratégies

Pare-feu nouvelle génération (NGFW)

Pour activer le pare-feu de nouvelle génération, procédez comme suit :

- Sélectionnez Groupe de stratégies, cliquez sur NGFW, puis sur Ajouter une stratégie NGFW
- Donnez-lui un nom de stratégie et cliquez sur Suivant
- Sélectionnez le groupe de configuration à associer à la stratégie de pare-feu de nouvelle génération
- Ajoutez les règles et cliquez sur Suivant
- Créez votre stratégie NGFW

Pour activer la consignation, modifiez la stratégie du pare-feu de nouvelle génération, puis sélectionnez Paramètres supplémentaires et activez la consignation unifiée

Filtrage des URL

Pour activer le filtrage des URL pour les versions antérieures à 20.18 :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Groupes d'intérêt
- Sélectionnez Sécurité, puis développez Profils

Pour activer le filtrage des URL pour les versions 20.18 et ultérieures :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Objets et profils
- Sélectionner des profils de sécurité

Sélectionnez Ajouter un filtrage d'URL, entrez les détails et cliquez sur Enregistrer

Protection avancée contre les programmes malveillants (AMP)

Pour activer AMP pour les versions antérieures à la version 20.18 :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Groupes d'intérêt
- Sélectionnez Sécurité, puis développez Profils

Pour activer AMP pour les versions 20.18 et ultérieures :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Objets et profils
- Sélectionner des profils de sécurité

Sélectionnez Advanced Malware Protection et cliquez sur Add Advanced Malware Protection

Ajoutez les détails et cliquez sur Enregistrer

Système de prévention des intrusions (IPS)/Détection de prévention des intrusions (IDS)

Pour activer IPS/IDS pour les versions antérieures à 20.18 :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Groupes d'intérêt

- Sélectionnez Sécurité, puis développez Profils

Pour activer IPS/IDS pour les versions 20.18 et ultérieures :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Objets et profils
- Sélectionner des profils de sécurité

Sélectionnez Prévention des intrusions et cliquez sur Ajouter une prévention des intrusions

Ajoutez les détails et cliquez sur Enregistrer

Créer un profil d'inspection avancé (AIP)

Pour activer AIP pour les versions antérieures à 20.18 :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Groupes d'intérêt
- Sélectionnez Sécurité, puis développez Profils

Pour activer AIP pour les versions 20.18 et ultérieures :

- Sélectionnez Configuration sur l'interface utilisateur, puis Groupe de stratégies, puis cliquez sur Objets et profils
- Sélectionner des profils de sécurité

Sélectionnez Profil d'inspection avancé et cliquez sur Ajouter un profil d'inspection avancé

- Saisissez les noms de filtrage AMP/IPS/Url créés lors des étapes précédentes, puis cliquez sur Enregistrer

Association de AIP à NGFW

- Sélectionnez Configuration, puis Groupes de stratégies et cliquez sur NGFW
- Modifier la stratégie de pare-feu de nouvelle génération créée précédemment
- Pour les règles de pare-feu de nouvelle génération créées précédemment, modifiez et associez le profil AIP créé précédemment, puis cliquez sur Enregistrer

Ulogging

Pour la journalisation, activez la fonctionnalité sur le routeur via le groupe de configuration à l'aide de l'option 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
```

Vérification

```
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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.