Aktivieren von Sicherheitsfunktionen mithilfe von Konfigurationsgruppen für SDWAN

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration von NGFW, URL-Filterung, AMP und IPS/IDS über Konfigurationsgruppen beschrieben, einschließlich Anweisungen für eine einheitliche Protokollierung.

Voraussetzungen

Transparenter Datenfluss und Anwendungstransparenz

Wenn Sie Policys mithilfe von Policygruppen definieren:

- Wählen Sie die Richtliniengruppe und anschließend Anwendungspriorität und SLA aus.
- Wählen Sie Neu hinzufügen aus
- Klicken Sie auf Zusätzliche Einstellungen, um Anwendungstransparenz und Flow-Transparenz zu aktivieren.

Wenn Sie die alte Richtlinie verwenden,

- Wählen Sie in der Konfigurationsgruppe ein CLI-Add-on-Profil aus, und fügen Sie diese

Befehle hinzu.

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

Stellen Sie sicher, dass Sie die Voraussetzungen für die hier aufgeführten Funktionen erfüllen: 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
```

In diesem Dokument werden die Funktionen erläutert, die mithilfe von Richtliniengruppen aktiviert werden sollen.

Next-Generation Firewall (NGFW)

So aktivieren Sie die NGFW:

- Wählen Sie die Richtliniengruppe und klicken Sie auf NGFW und dann auf NGFW-Richtlinie hinzufügen
- Geben Sie ihm einen Richtliniennamen, und klicken Sie auf Weiter
- Wählen Sie die Konfigurationsgruppe aus, die der NGFW-Richtlinie zugeordnet werden soll.
- Fügen Sie die Regeln hinzu, und klicken Sie auf Weiter
- NGFW-Richtlinie erstellen

Um das Protokollieren zu aktivieren, bearbeiten Sie die NGFW-Richtlinie, wählen Sie dann "Additional Settings" (Zusätzliche Einstellungen) aus, und aktivieren Sie die einheitliche Protokollierung.

URL-Filterung

So aktivieren Sie die URL-Filterung für Versionen vor 20.18:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Interessengruppen.
- Wählen Sie Sicherheit aus, und erweitern Sie dann Profile.

So aktivieren Sie die URL-Filterung für Version 20.18 und höher:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Objekte und Profile
- Sicherheitsprofile auswählen

Wählen Sie URL-Filterung hinzufügen, geben Sie die Details ein, und klicken Sie auf Speichern

Advanced Malware Protection (AMP)

So aktivieren Sie AMP für Versionen vor 20.18:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Interessengruppen.
- Wählen Sie Sicherheit aus, und erweitern Sie dann Profile.

So aktivieren Sie AMP für die Versionen 20.18 und höher:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Objekte und Profile
- Sicherheitsprofile auswählen

Wählen Sie Advanced Malware Protection aus, und klicken Sie auf Advanced Malware Protection hinzufügen

Fügen Sie die Details hinzu, und klicken Sie auf Speichern.

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

So aktivieren Sie IPS/IDS für Versionen vor 20.18:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe

aus, und klicken Sie dann auf Interessengruppen.
- Wählen Sie Sicherheit aus, und erweitern Sie dann Profile.

So aktivieren Sie IPS/IDS für Version 20.18 und höher:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Objekte und Profile
- Sicherheitsprofile auswählen

Wählen Sie Intrusion Prevention aus, und klicken Sie auf Intrusion Prevention hinzufügen

Fügen Sie die Details hinzu, und klicken Sie auf Speichern.

Erweitertes Inspektionsprofil (AIP) erstellen

So aktivieren Sie AIP für Versionen vor dem 20.18:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Interessengruppen.
- Wählen Sie Sicherheit aus, und erweitern Sie dann Profile.

So aktivieren Sie AIP für Version 20.18 und höher:

- Wählen Sie Konfiguration auf der Benutzeroberfläche und anschließend Richtliniengruppe aus, und klicken Sie dann auf Objekte und Profile
- Sicherheitsprofile auswählen

Wählen Sie Advanced Inspection Profile aus, und klicken Sie auf Add Advanced Inspection Profile

- Geben Sie die Namen der AMP-/IPS-/URL-Filterung ein, die Sie mit den vorherigen Schritten erstellt haben, und klicken Sie auf Speichern.

Association of AIP to NGFW

- Wählen Sie Konfiguration und anschließend Richtliniengruppen und klicken Sie auf NGFW
- Zuvor erstellte NGFW-Richtlinie bearbeiten
- Bearbeiten und ordnen Sie für zuvor erstellte NGFW-Regeln das zuvor erstellte AIP-Profil zu, und klicken Sie auf "Speichern".

Ulogging

Aktivieren Sie zum Protokollieren die Funktion auf dem Router über die Konfigurationsgruppe, indem Sie "cli add on" verwenden.

```
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
```

Verifizierung

```
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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.