使用配置組為SDWAN啟用安全功能

目錄

簡介

本文檔介紹通過配置組配置NGFW、URL過濾、AMP和IPS/IDS，包括統一日誌記錄的說明。

必要條件

實現流可視性和應用可視性

如果使用策略組定義策略：

- 選擇策略組，然後選擇應用程式優先順序和SLA。
- 選擇Add new
- 點選其他設定並啟用應用可視性和流可視性

如果您使用的是舊策略

- 在配置組中選擇一個Cli附加配置檔案，然後新增以下命令

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

確保您符合此處所給功能的先決條件
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
```

本文檔重點介紹使用策略組啟用的功能

新世代防火牆(NGFW)

要啟用NGFW，請執行以下步驟：

- 選擇Policy group（策略組），然後點選NGFW，然後點選Add NGFW Policy（新增NGFW策略）
- 為其指定策略名稱，然後按一下「下一步」
- 選擇要與NGFW策略關聯的配置組
- 新增規則，然後按一下「下一步」
- 建立NGFW策略

要啟用日誌記錄，請編輯NGFW策略，然後選擇其他設定並開啟統一日誌記錄

URL篩選

為20.18之前的版本啟用URL過濾：

- 選擇UI上的Configuration，然後選擇Policy group，然後按一下Groups of Interest
- 選擇安全，然後展開配置檔案

要為版本20.18及更高版本啟用url過濾：

- 選擇UI上的Configuration，然後選擇Policy組，然後按一下Objects and Profiles
- 選擇安全配置檔案

選擇「新增url過濾」，輸入詳細資訊並按一下「儲存」

進階惡意軟體防護 (AMP)

為20.18之前的版本啟用AMP:

- 選擇UI上的Configuration，然後選擇Policy group，然後按一下Groups of Interest
- 選擇安全，然後展開配置檔案

為版本20.18及更高版本啟用AMP :

- 選擇UI上的Configuration，然後選擇Policy組，然後按一下Objects and Profiles
- 選擇安全配置檔案

選擇Advanced Malware Protection，然後點選Add Advanced Malware Protection

新增詳細資訊並按一下「儲存」

入侵防禦系統(IPS)/入侵防禦檢測(IDS)

要為20.18之前的版本啟用IPS/IDS，請執行以下操作：

- 選擇UI上的Configuration，然後選擇Policy group，然後按一下Groups of Interest
- 選擇安全，然後展開配置檔案

要為版本20.18及更高版本啟用IPS/IDS，請執行以下操作：

- 選擇UI上的Configuration，然後選擇Policy組，然後按一下Objects and Profiles
- 選擇安全配置檔案

選擇Intrusion Prevention並按一下Add Intrusion Prevention

新增詳細資訊並按一下「儲存」

建立高級檢查配置檔案(AIP)

要為20.18之前的版本啟用AIP，請執行以下操作：

- 選擇UI上的Configuration，然後選擇Policy group，然後按一下Groups of Interest
- 選擇安全，然後展開配置檔案

要為版本20.18及更高版本啟用AIP，請執行以下操作：

- 選擇UI上的Configuration，然後選擇Policy組，然後按一下Objects and Profiles
- 選擇安全配置檔案

選擇Advanced Inspection Profile，然後按一下Add Advanced Inspection Profile

- 輸入在前面的步驟中建立的AMP/IPS/Url過濾名稱，然後點選儲存

AIP與NGFW的關聯

- 選擇Configuration（配置），然後選擇Policy groups（策略組），然後按一下NGFW
- 編輯之前建立的NGFW策略
- 對於先前建立的NGFW規則，請編輯並關聯先前建立的AIP配置檔案，然後按一下「儲存」

Ulogging

要執行日誌記錄，請使用cli add on通過配置組在路由器上啟用該功能

```
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
```

驗證

```
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
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。