تمكين ميزات الأمان باستخدام مجموعات التكوين ل SDWAN

المحتويات

المقدمة

يصف هذه المستند تكوين NGFW، وتصفية عنوان URL، و AMP، و IPS/IDs عبر مجموعات التكوين، بما في ذلك التعليمات الخاصة بالتسجيل الموحد.

المتطلبات الأساسية

تمكين قابلية التدفق وإمكانية رؤية التطبيقات

إذا كنت تستخدم مجموعات نهج لتحديد السياسات :

- حدد مجموعة النهج ثم حدد أولوية التطبيق واتفاقية مستوى الخدمة (SLA).
- تحديد إضافة جديد
- انقر على إعدادات إضافية وقم بتمكين رؤية التطبيق وإمكانية الرؤية بالتدفق

إذا كنت تستخدم السياسة القديمة

- حدد ملف تعريف وظيفة CLI الإضافية في مجموعة التكوين وأضف الأوامر التالية

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

تأكد من امتثالك لمتطلبات الميزات الأساسية كما هو موضح هنا 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
```

يركز هذا المستند على الميزات التي سيتم تمكينها باستخدام مجموعات النهج

جدار الحماية من الجيل التالي (NGFW)

لتمكين NGFW تنفيذ الخطوات المذكورة:

- حدد مجموعة النهج وانقر فوق NGFW وانقر فوق إضافة نهج NGFW
- قم بإعطائه اسم نهج وانقر فوق التالي
- حدد مجموعة التكوين لإقرانها بنهج NGFW
- قم بإضافة القواعد وانقر فوق التالي
- إنشاء نهج NGFW الخاص بك

لتمكين التسجيل، قم بتحرير سياسة NGFW ثم حدد الإعدادات الإضافية وقم بتشغيل التسجيل الموحد

تصفية URL

لتمكين تصفية URL للإصدارات قبل 20.18:

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر فوق مجموعات المصالح
- حدد تأمين ثم قم بتوسيع التوصيفات

لتمكين تصفية عنوان URL للإصدارات 20.18 والإصدارات الأحدث :

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر على كائنات وتوصيفات
- حدد توصيفات التأمين

حدد إضافة تصفية URL، أدخل التفاصيل وانقر فوق حفظ

الحماية المتقدمة من البرامج الضارة

لتمكين AMP للإصدارات قبل 20.18:

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر فوق مجموعات المصالح
- حدد تأمين ثم قم بتوسيع التوصيفات

لتمكين AMP للإصدارات 20. 18 والإصدارات الأحدث :

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر على كائنات وتوصيفات
- حدد توصيفات التأمين

حدد الحماية المتقدمة من البرامج الضارة وانقر فوق إضافة الحماية المتقدمة من البرامج الضارة

حفظ وأضف التفاصيل وانقر فوق

نظام منع التسلل (IDS) منع التسلل/اكتشاف (IPS)

لتمكين IPS/IDS للإصدارات قبل 20.18:

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر فوق مجموعات المصالح
- حدد تأمين ثم قم بتوسيع التوصيفات

لتمكين IPS/IDS للإصدارات 20. 18 والإصدارات الأحدث :

- حدد تكوين على واجهة المستخدم ثم مجموعة النهج ثم انقر على كائنات وتوصيفات
- حدد توصيفات التأمين

حدد منع التطفل وانقر فوق إضافة منع التطفل

حفظ وأضف التفاصيل وانقر فوق

إنشاء ملف تعريف فحص متقدم (AIP)

لتمكين دليل الطيران للإصدارات قبل 20.18:

- حل المصالح تاعومجم قوف رقنا مث جهنلا ةعومجم مث مدختسملا ةهجاو ىلع نيوكت ددح
- تافيصوتلا عيسوتب مق مث نيمأت ددح

لتمكين دليل الطيران للإصدارات 20. 18 والإصدارات الأحدث :

- تافيصوتو تانئاك ىلع رقنا مث جهنلا ةعومجم مث مدختسملا ةهجاو ىلع نيوكت ددح
- نيمأتلا تافيصوت ديدحت

مدقتم صحف صيصخت فلم ةفاضإ رقناو مدقتم صحف صيصخت فلم ددح

- قوف رقناو ةقباسلا تاوطخلا يف اهؤاشنإ مت يتلا AMP/IPS/URL ةيفصت ءامسأ لخدأ ظفح

جمعية دليل الطيران إلى الجمعية الوطنية للأرملة والطفل

- NGFW قوف رقناو جهنلا تاعومجم ددح مث نيوكت ددح
- اقبسم هؤاشنإ مت يذلا NGFW جهن ريرحت
- مت يذلا AIP فيرعت فلم طبرو ريرحتب مق ،اقباس اهئاشنإ مت يتلا NGFW دعاوق ظفح رقناو اقباس هئاشنإ

تسجيل الدخول

للتسجيل، قم بتمكين الميزة على الموجه عبر مجموعة التكوين باستخدام CLI (واجهة سطر الأوامر المضافة)

```
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
```

التحقق

```
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:                         0000000000000000000000000000000000000000000000000
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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).