نهج برمجي لتحسين إعداد VPN للوصول عن بعد من خلال تحليلات البيانات

المحتويات

المقدمة

يوضح هذا المستند كيفية مراقبة إعداد شبكة VPN للوصول عن بعد وتحسينها من خلال بعض وحدات البرمجة والأدوات مفتوحة المصدر المتوفرة اليوم. يتولد الكثير من البيانات اليوم حتى في أصغر الشبكات التي يمكن تسخيرها للحصول على معلومات مفيدة. يساعد تطبيق التحليلات على هذه البيانات المجمعة في إتخاذ قرارات عمل أسرع وأكثر إستنارة، مدعوما بالحقائق.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- شبكة VPN للوصول عن بعد
- مفاهيم برمجة بايثون الأساسية

المكونات المستخدمة

ال يقيد هذا وثيقة إلى خاص cisco ASA أو FTD برمجية وجهاز صيغة.

> **ملاحظة**: البانداس، وسترينغيو، CSV، و Matplotlib هي عدد قليل من مكتبات Python التي يتم إستخدامها.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أوامر أو برامج نصية خاصة بالإيثون.

المشكلة

مع تبني العديد من الشركات نموذج العمل من المنزل (Work From Home) لغالبية موظفيها في جميع أنحاء العالم، فقد زاد عدد المستخدمين الذين يعتمدون على الشبكات الخاصة الظاهرية (VPN) لتنفيذ أعمالهم بشكل كبير. وقد أدى ذلك إلى زيادة مفاجئة وكبيرة في الحمل على مركزات الشبكات الخاصة الظاهرية (VPN) مما دفع المسؤولين إلى إعادة التفكير في حوالات الشبكات الخاصة الظاهرية (VPN) الخاصة بهم وإعادة تخطيطها. ويتطلب إتخاذ قرارات مستنيرة لتقليل الحمل على مركزات ASA جمع مجموعة واسعة من المعلومات من الأجهزة على مدى فترة من الزمن وتقييم تلك المعلومات، وهي مهمة معقدة وتتطلب قدرا كبيرا من الوقت إذا تم القيام بها يدويا.

الحل

من خلال إستخدام العديد من وحدات Python والأدوات مفتوحة المصدر المتوفرة اليوم لقابلية الشبكات للبرمجة وتحليلات البيانات، يمكن أن تكون البرمجة مفيدة للغاية في جمع البيانات وتحليلها والتخطيط لإعداد الشبكة الخاصة الظاهرية (VPN) وتحسينه.

التحليل الأولي استنادا إلى مستخدمي VPN والاتصالات المتزامنة

لبدء التحليل، يمكن الحصول على عدد المستخدمين المتصلين، والاتصالات المتزامنة التي تم إنشاؤها، وتأثيرها على النطاق الترددي. ستوفر مخرجات أمر Cisco ASA التالية التفاصيل التالية:

- show vpn-sessionDB AnyConnect
- عرض المخرج

يمكن إستخدام وحدة Python النمطية **NetMiko** لبروتوكول SSH إلى الجهاز، وتشغيل الأوامر، وتحليل المخرجات.

```
cisco_asa_device = {

        "host": host,

        "username": username,

        "password": password,

        "secret": secret,

        "device_type": "cisco_asa",

    }

    net_conn = ConnectHandler(**cisco_asa_device)

    command = "show vpn-sessiondb anyconnect"

    command_output = net_conn.send_command(command)
```

قم بجمع عدد مستخدمي شبكة VPN وعدد الاتصالات على فواصل زمنية منتظمة (يمكن أن تكون كل ساعتين بداية جيدة) في قائمة واحصل على الحد الأقصى للعدد اليومي ليوم واحد.

```
#list1 is the list of user counts collected in a day
#list2 is the list of connection counts in a day
list1.sort()
max_vpn_user = list1[-1]

list2.sort()
max_conn = list2[-1]

df1.append([max_vpn_user,max_conn])
```

PANDAS هي مكتبة فعالة لتحليل البيانات ومعالجتها ويمكن تخزين جميع البيانات التي تم تحليلها كسلسلة أو إطار بيانات في البانداز مما يسهل عمليات البيانات.

```
import pandas as pd

df = pd.DataFrame(df1, columns=['Max Daily VPN Users Count','Max Daily Concurrent
Connections'],index=<date range>)
```

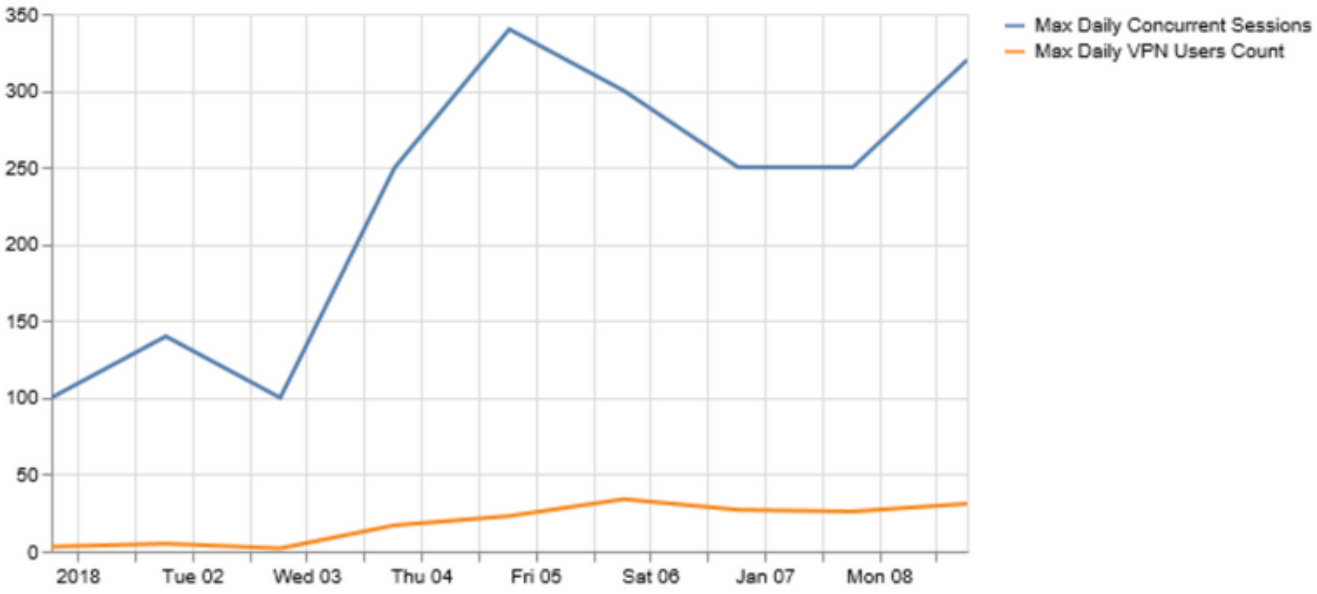
Daily Max VPN user Count - Max concurrent count

	Max Daily VPN Users Count	Max Daily Concurrent Sessions
Jan 1, 2018	3	100
Jan 2, 2018	5	140
Jan 3, 2018	2	100
Jan 4, 2018	17	250
Jan 5, 2018	23	340
Jan 6, 2018	34	300
Jan 7, 2018	27	250
Jan 8, 2018	26	250
Jan 9, 2018	31	320

تحليل **الحد الأقصى اليومي لمستخدمي الشبكة الخاصة الظاهرية (VPN)** و**الحد الأقصى للاتصالات المتزامنة** التي يمكن أن تساعد في تحديد الحاجة إلى تحسين إعدادات الشبكة الخاصة الظاهرية (VPN).

أستخدم دالة الرسم البياني في مكتبة **البانداز** Matplotlib، كما هو موضح في الصورة هنا.

```
df.plot()

matplotlib.pyplot.show()
```



إذا كان عدد مستخدمي VPN أو الاتصالات المتزامنة يقترب من سعة وحدة الاستقبال والبث الخاصة بالشبكة الخاصة الظاهرية (VPN)، فقد يتسبب ذلك في حدوث هذه المشاكل:

- مستخدمو شبكة VPN الجدد يتم إسقاطهم.
- يتم إسقاط اتصالات البيانات الجديدة من خلال ASA والا يمكن للمستخدمين الوصول إلى الموارد.
- وحدة معالجة مركزية (CPU) و/أو ذاكرة فائقة.

يمكن أن يساعد الإتجاه على مدى فترة من الزمن في تحديد ما إذا كان المربع يصل إلى الحد.

تحديد إتجاه حركة المرور باتجاه الشبكة الداخلية أو الشبكات الخارجية

يمكن أن يوفر **عرض** إخراج **المحتوى** على Cisco ASA تفاصيل إضافية مثل ما إذا كانت حركة المرور إلى الشبكات الداخلية أو الخارجية ومدى تمرير البيانات بالبايت لكل تدفق من خلال جدار الحماية.

Soure IP	Destination IP	Service	Bytes
10.10.1.1	10.30.2.2	tcp/445	1234
10.10.1.2	40.5.2.3	tcp/443	2341
10.10.1.4	42.4.2.33	tcp/80	5432
10.10.2.3	52.3.2.34	tcp/443	1223
10.10.6.5	10.30.22.2	tcp/80	212
10.10.3.2	10.30.2.3	udp/389	1212
10.10.3.4	32.3.22.2	tcp/443	2123

يسهل إستخدام وحدة **NetAddr** python تقسيم جدول الاتصال الذي تم الحصول عليه إلى

تدفقات إلى الشبكات الخارجية وإلى الشبكات الداخلية.

```
for f in df['Responder IP']:
   private.append(IPAddress(f).is_private())

df['private'] = private

df_ext = df[df['private'] == False]

df_int = df[df[‘private’] == True]
```

هذه هي صورة حركة المرور الداخلية.

Soure IP	Destination	Service	Bytes
10.10.1.1	10.30.2.2	tcp/445	1234
10.10.6.5	10.30.22.2	tcp/80	212
10.10.3.2	10.30.2.3	udp/389	1212

هذه هي صورة حركة المرور الخارجية.

Soure IP	Destination	Service	Bytes
10.10.1.2	40.5.2.3	tcp/443	2341
10.10.1.4	42.4.2.33	tcp/80	5432
10.10.2.3	52.3.2.34	tcp/443	1223
10.10.3.4	32.3.22.2	tcp/443	2123

ومن ثم، يساعد هذا على توفير رؤية متعمقة حول النسبة المئوية لحركة مرور الشبكات الخاصة الظاهرية (VPN) الموجهة إلى الشبكات الداخلية وكميتها التي يتم إرسالها إلى الإنترنت. ويمكن أن يساعد جمع هذه المعلومات على مدى فترة من الوقت وتحليل إتجاها في تحديد ما إذا كانت حركة مرور شبكة VPN معظمها خارجية أو داخلية.

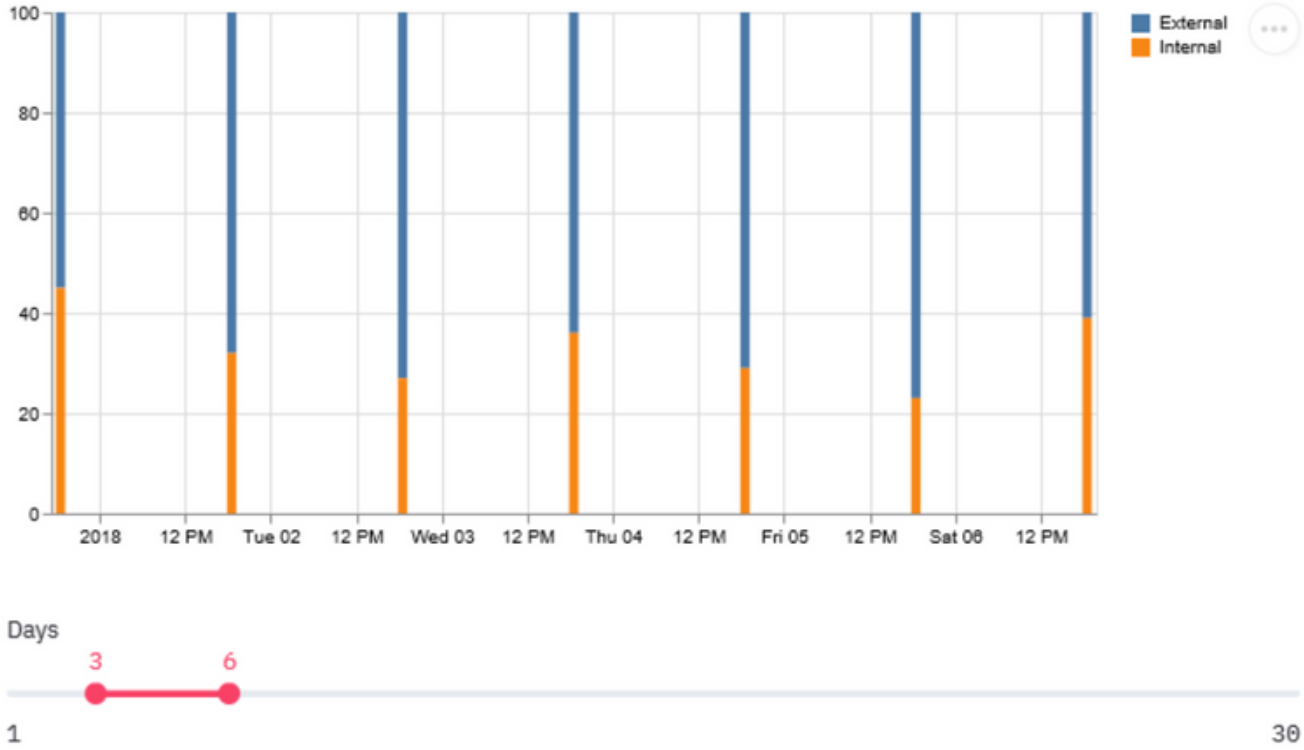
VPN Usage

Traffic Segregation - Internal and External

	External	Internal
Jan 1, 2018	55	45
Jan 2, 2018	68	32
Jan 3, 2018	73	27
Jan 4, 2018	64	36
Jan 5, 2018	71	29
Jan 6, 2018	77	23
Jan 7, 2018	61	39

تتيح وحدات مثل StreamLit ليس فقط تحويل البيانات الجدولية إلى تمثيل رسومي بل أيضا تطبيق التعديلات عليها في الوقت الحقيقي للمساعدة في التحليل. يمكنه تعديل الإطار الزمني للبيانات المجمعة أو إضافة بيانات إضافية إلى المعلمات التي يتم مراقبتها.

```
import streamlit

#traffic_ptg being a 2D array containing the data collected as in the table above

d = st.slider('Days',1,30,(1,7))

idx = pd.date_range('2018-01-01', periods=7, freq='D')

df = pd.DataFrame(d<subset of the list traffic_ptg based on slider
value>,columns=['External','Internal'],index=idx)

st.bar_chart(df)
```

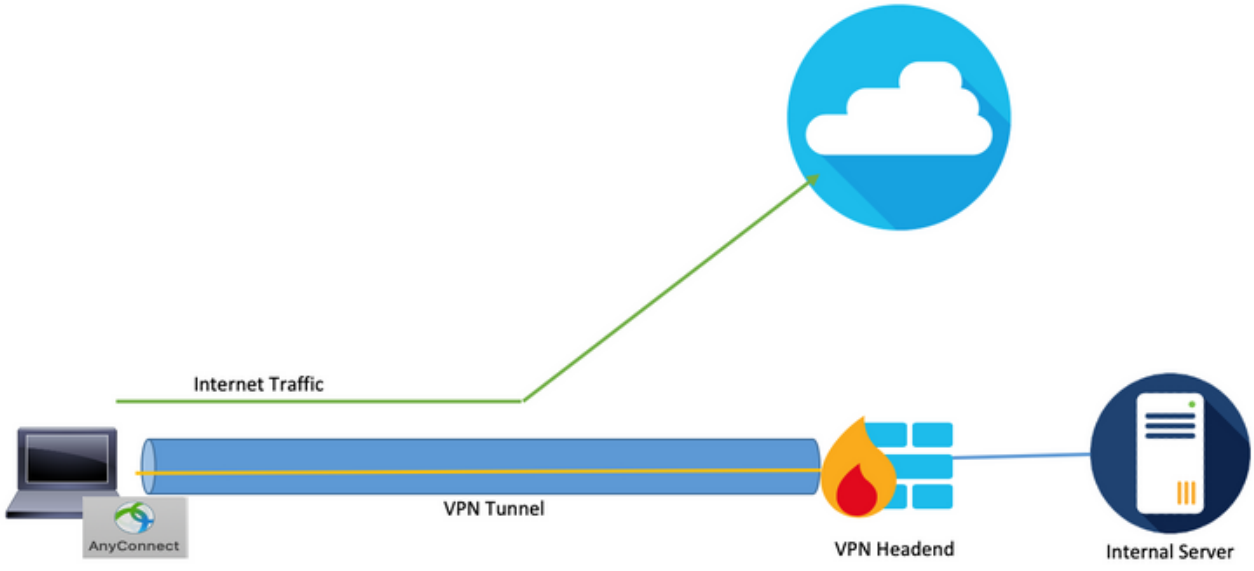


وقد يعني الإتجاه الذي يميل إلى زيادة حركة المرور الداخلية أن غالبية مستخدمي شبكة VPN يمكنهم الوصول إلى الموارد الداخلية. وبالتالي، لتلبية هذه المشكلة، زيادة الحمل، من المهم تخطيط الترقيات إلى مربعات أكبر أو مشاركة الحمل مع مفاهيم مثل موازنة حمل الشبكة الخاصة الظاهرية (VPN).

في بعض الحالات، قد تكون سعة الشبكة الخاصة الظاهرية (VPN) ال تزال تحت الحد غير أن زيادة في عدد مستخدمي الشبكة الخاصة الظاهرية (VPN) يمكن أن تستنفد تجمع الشبكات الخاصة الظاهرية (VPN) الحالي الذي تم تكوينه. في مثل هذه الحالات، قم بزيادة تجمع IP لشبكة VPN.

مهما، إن يبدي الإتجاه أن الغالبية من ال VPN حركة مرور خارجي، بعد ذلك أنت يستطيع استعملت انقسام tunneling.

الاستفادة من ميزة تقسيم الاتصال النفقي



هو سمة أن يرسل فقط مجموعة خاص حركة مرور خلال النفق من المستعمل نظام وبقيت الحركة مرور أرسلت إلى التقصير مدخل دون VPN تشفير. وبالتالي، لتقليل الحمل على مركز الشبكة الخاصة الظاهرية (VPN)، يمكن توجيه حركة المرور الموجهة إلى الشبكة الداخلية فقط من خلال النفق، ويمكن إعادة توجيه حركة مرور الإنترنت من خلال مزود خدمة الإنترنت (ISP) المحلي الخاص بالمستخدم. وهذه طريقة فعالة ومعتمدة على نطاق واسع ولكنها تنطوي على بعض المخاطر.

يمكن أن يصيب الموظف الذي يدخل بعض مواقع الوسائط الاجتماعية عبر الشبكات غير المحمية للحصول على كسر سريع جهاز الكمبيوتر المحمول الخاص به ببرامج ضارة تنتشر في أنحاء الشركة بسبب عدم وجود طبقات حماية معمقة مهيأة في مكان العمل. وبمجرد إصابتها، يمكن أن تصبح الجهاز الذي تم اكتشافه نقطة محورية من الإنترنت إلى الجزء الموثوق به، مع تجاوز الدفاعات المحيطة.

تتمثل إحدى الطرق للحد من المخاطر أثناء إستخدام هذه الميزة في إستخدام إنشاء قنوات منفصلة فقط للخدمات السحابية التي تجتاز معايير الأمان الصارمة، بما في ذلك النظافة الجيدة للبيانات والتوافق مع ميزة الأمان Duo. سيؤدي اعتماد هذا الإجراء إلى المساعدة في حالة توجيه قدر كبير من حركة المرور الخارجية التي تمت ملاحظتها مسبقا، للحصول على خدمات الشبكات الآمنة هذه. وهذا من شأنه أن يبرز الحاجة إلى تحليل تطبيقات الويب التي يمكن لمستخدمي الشبكات الخاصة الظاهرية (VPN) الوصول إليها.

تحتوي معظم جدران الحماية من الجيل التالي مثل Cisco Firepower Threat Defense (FTD) على معلومات تطبيق مقترنة بالحدث في السجلات. يمكن أن توفر عملية تحليل بيانات السجل هذه وظيفتها باستخدام **مكتبات** Python **csv** وميزات معالجة بيانات Pandas مجموعة بيانات مماثلة كما هو موضح أعلاه مع إضافة التطبيقات التي يتم الوصول إليها والتي تم تعيينها.

```
#connections.csv contains the connection events from ASA and events_with_app.csv contains connection events with Application details fromFTD

df1 = pd.read_csv('connections.csv') df2 = pd.read_csv('events_with_app.csv') df_merged = pd.merge(df1,df2,on=['Source IP','Destination IP','Service'])
```

Soure IP	Destination IP	Service	Bytes	Application
10.10.1.1	10.30.2.2	tcp/445	1234	
10.10.1.2	40.5.2.3	tcp/443	2341	Microsoft
10.10.1.4	42.4.2.33	tcp/80	5432	Microsoft
10.10.2.3	52.3.2.34	tcp/443	1223	Office365
10.10.6.5	10.30.22.2	tcp/80	212	
10.10.3.2	10.30.2.3	udp/389	1212	
10.10.3.4	32.3.22.2	tcp/443	2123	Youtube

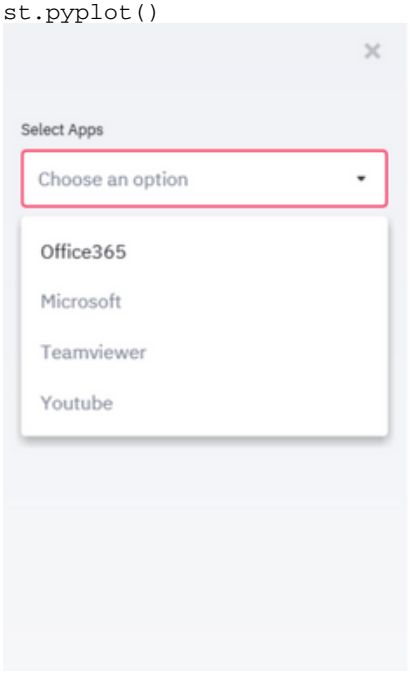
بمجرد الحصول على إطار بيانات كما هو موضح أعلاه، يمكنك تصنيف حركة المرور الخارجية الإجمالية بناء على التطبيق عبر الباندا.

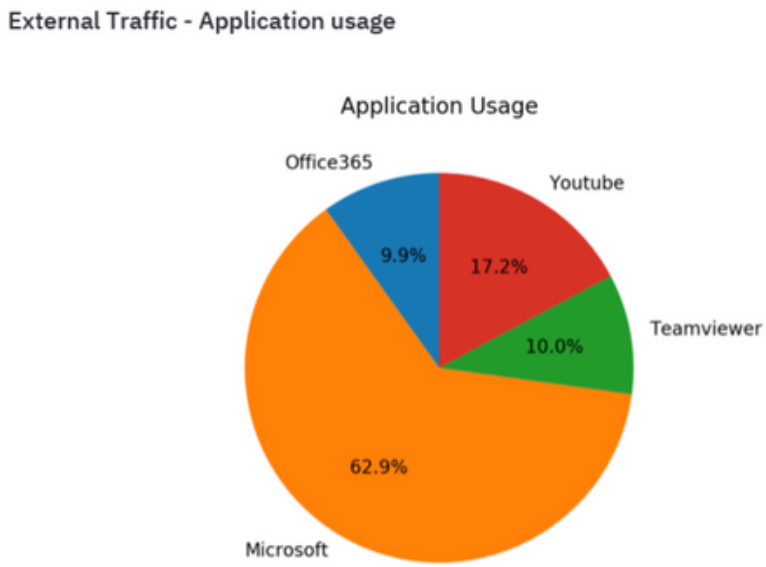
```
df2 = df.groupby('Application')

df3 = df2['Bytes'].sum()
```

```
Application
Microsoft      7773
Office365      1223
Teamviewer     1234
Youtube        2123
Name: Bytes, dtype: int64
```

مرة أخرى، يحصل إستخدام StreamLight على تمثيل رسومي لنسبة كل تطبيق في حركة المرور الإجمالية. فهي تتيح المرونة لتغيير الإطار الزمني لتضمين البيانات وكذلك تصفية التطبيقات على واجهة المستخدم نفسها دون الحاجة إلى أي تغييرات في التعليمات البرمجية، مما يجعل التحليل سهلا ودقيقا.

```
import matplotlib.pyplot as plt

apps = ['Office365', 'Microsoft', 'Teamviewer', 'Youtube']
app_select = st.sidebar.multiselect('Select Apps',activities)

# app_bytes - list containing the applications and bytes

plt.pie(app_bytes, labels=apps)
plt.title('Application Usage')

st.pyplot()
```





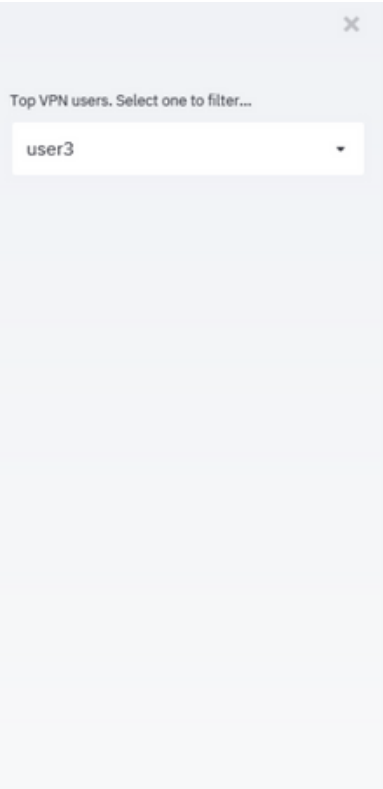
ويمكن أن يؤدي ذلك إلى تبسيط عملية تعريف تطبيقات الويب العليا التي يستخدمها مستخدمو شبكات VPN على مدى فترة من الوقت وإذا كانت هذه التطبيقات مخصصة لتأمين خدمات الشبكات أم ال.

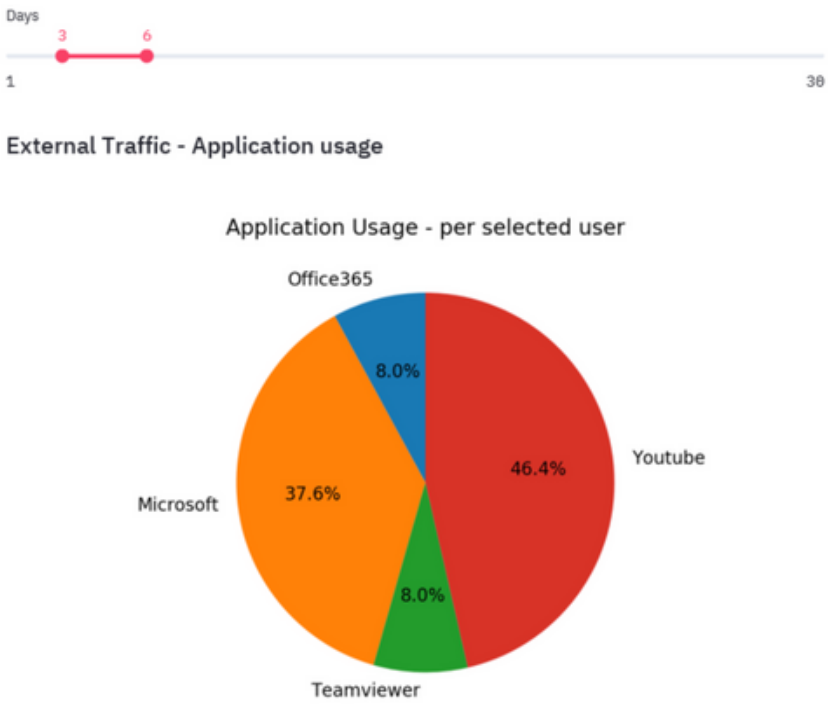
إذا كان الهدف من التطبيقات كثيرة الحجم وه تحديد خدمات الشبكة الآمنة، فيمكن

إستخدامها مع نفق منفصل، وبالتالي تقليل الحمل على مركز الشبكة الخاصة الظاهرية (VPN). ومع ذلك، إذا كانت التطبيقات العليا عبارة عن خدمات أقل أمانا أو قد تشكل خطرا، فهذا يعني أنه أكثر أمانا لتمريرها عبر نفق الشبكة الخاصة الظاهرية (VPN). السبب هو أن أجهزة أمان الشبكة الأخرى يمكن أن تعالج حركة المرور قبل أن تسمح لحركة المرور هذه بالمرور. يمكنك بعد ذلك إستخدام سياسات الوصول على جدران الحماية للحد من الوصول إلى الشبكات الخارجية.

مستخدمو شبكة VPN الفرديون غير المتوافقين مع الهوية

وفي بعض الحالات، يمكن ربط الزيادة المفاجئة بعدد قليل من المستخدمين فقط الذين لا يمتثلون لسياسات معينة. يمكن إستخدام الوحدات النمطية ومجموعات البيانات المستخدمة أعلاه مرة أخرى لتحديد مستخدمي شبكات VPN العليا وتطبيقات الويب التي يمكنهم الوصول إليها. يمكن أن يساعد ذلك في عزل هؤلاء المستخدمين ويلاحظ تأثيرهم على حمل الجهاز.





في السيناريوهات، حيث لا توجد أي من الطرق المناسبة، يجب أن ينظر المسؤولون إلى حلول أمان نقاط النهاية مثل AMP لحل نقاط النهاية وحل Cisco Umbrella لحماية نقاط النهاية في الشبكات غير المحمية.

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).