通過資料分析最佳化遠端訪問VPN設定的程式設計方法

目錄

簡介

本文檔介紹如何監控和最佳化通過當前可用的某些程式設計模組和開源工具設定的遠端訪問VPN。如今，即使是最小的網路也會生成大量資料，這些網路也可以被用來獲取有用的資訊。對收集到的資料進行分析有助於根據事實做出更快、更明智的業務決策。

必要條件

需求

思科建議您瞭解以下主題：

- 遠端存取VPN
- 基本Python程式設計概念

採用元件

本檔案所述內容不限於特定的Cisco ASA或FTD軟體和硬體版本。

> **附註**：Pandas、Streamlit、CSV和Matplotlib是使用的一些Python庫。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您已瞭解任何指令和python指令可能造成的影響。

問題

隨著許多公司對其大部分員工採用在家工作模式，依賴VPN執行工作的使用者數量顯著增加。這導

致VPN集中器上的負載突然大幅增加，導致管理員重新思考和重新規劃其VPN設定。要做出明智的決策來減少ASA集中器的負載，需要在一段時間內從裝置收集大量資訊並評估該資訊，這是一項複雜的任務，如果手動完成則需要相當長的時間。

解決方案

由於目前有幾個Python模組和開源工具可用於網路可程式設計性和資料分析，程式設計可以證明在收集和分析資料、規劃和最佳化VPN設定方面非常有用。

基於VPN使用者和併發連線的初步分析

要開始分析，需要獲得連線的使用者數量、建立的併發連線及其對頻寬的影響。以下Cisco ASA命令輸出將提供以下詳細資訊：

- show vpn-sessiondb anyconnect
- show conn

Python模組**Netmiko**可用於ssh到裝置、運行命令並分析輸出。

```
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)
```

在清單中定期收集VPN使用者計數和連線計數（每2小時可以作為一個好的開始），獲取一天的最大日計數。

```
#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])
```

熊貓是一種高效的資料分析和操作庫，所有解析後的資料可以作為一個系列或資料框架儲存在熊貓體內，使得對資料的操作更加容易。

```
import pandas as pd
```

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

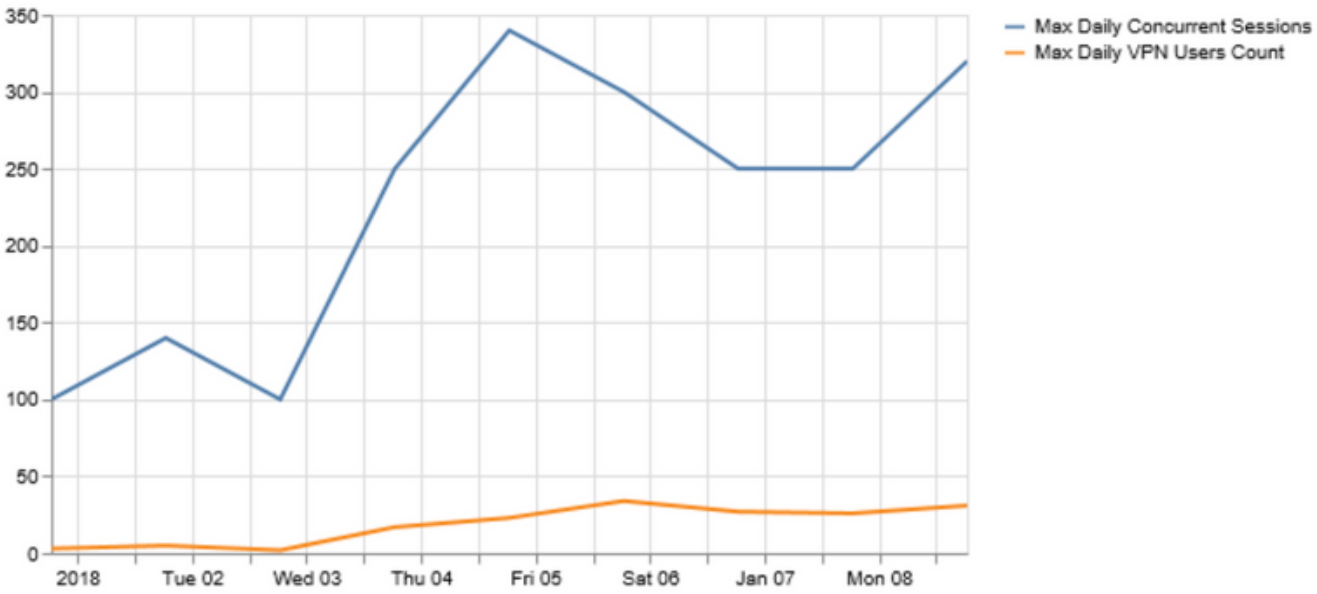
Daily Max VPN user Count - Max concurrent count

	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

分析每**天最大VPN使用者**數和**最大併發連線**數，以確定最佳化VPN設定的需要。

使用pandas和**matplotlib**庫中的plot函式，如下圖所示。

```
df.plot()

matplotlib.pyplot.show()
```



如果VPN使用者或併發連線的數量接近VPN頭端的容量，則可能導致以下問題：

- 正在丟棄的新VPN使用者。
- 通過ASA的新資料連線被丟棄，使用者無法訪問資源。
- 高CPU和/或記憶體。

一段時間內的趨勢有助於確定包裝盒是否達到其閾值。

確定流向內部網路或外部網路的流量趨勢

Show conn output on Cisco ASA可以提供額外的詳細資訊，例如流量是流向內部網路還是外部網路，以及每個流通過防火牆的資料量（以位元組為單位）。

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

使用**Netaddr** python模組可以輕鬆地將獲得的連線表拆分為到外部網路和內部網路的流。

```
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]
```

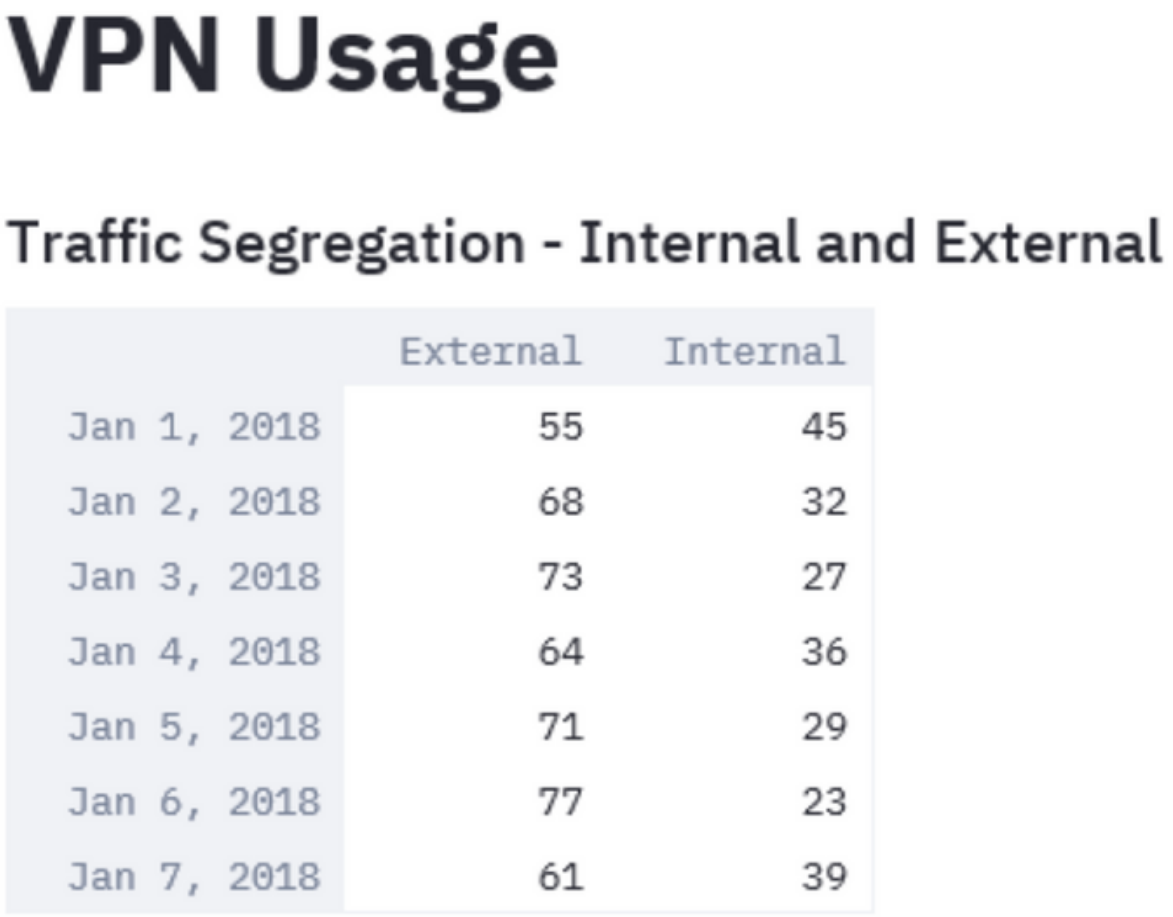
這是內部流量的影象。

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

這是外部流量的影象。

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

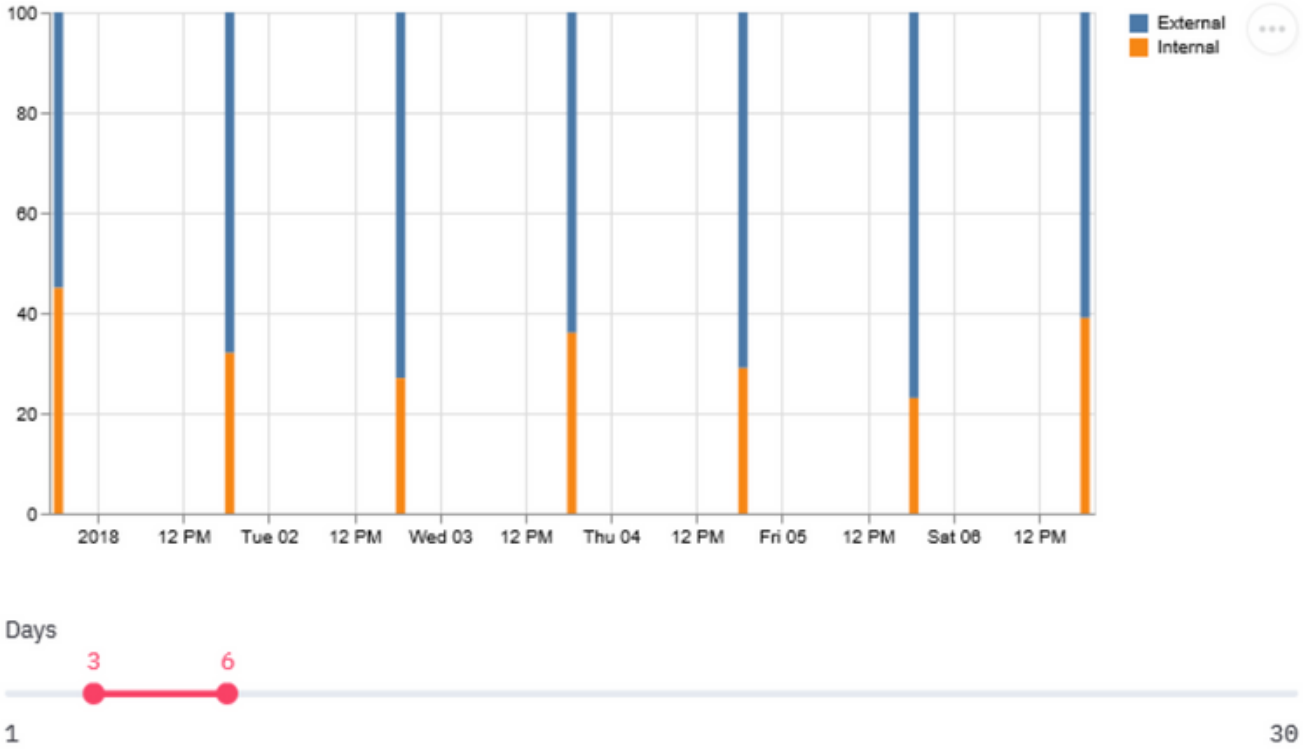
因此，您可以深入瞭解VPN流量中流向內部網路的百分比，以及有多少流量流向網際網路。在一段時間內收集此資訊並分析其趨勢有助於確定VPN流量主要是外部流量還是內部流量。



	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

Streamlit等模組不僅可以將表格資料轉換為圖形表示，還可以即時對表格資料應用修改以幫助分析。它可以修改所收集的資料的時間視窗或者向正被監視的引數新增其他資料。

```
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)
```

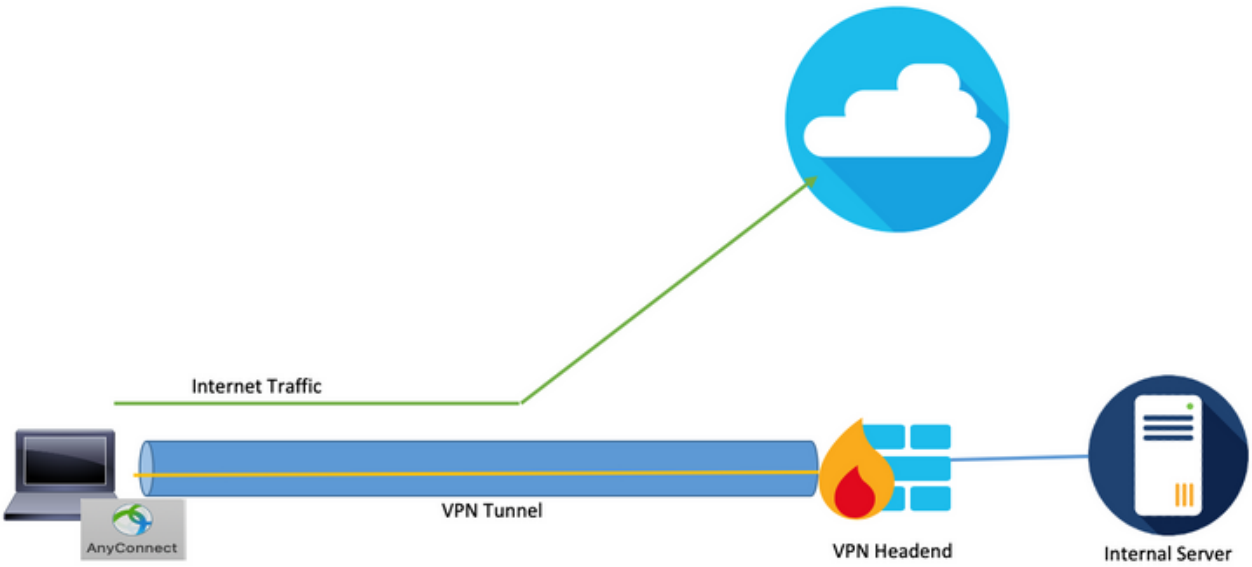


傾向於增加內部流量的趨勢可能意味著大多數VPN使用者訪問內部資源。因此，為了滿足這一需求，增加負載，計畫升級到更大的裝置或使用VPN負載平衡等概念共用負載非常重要。

在某些情況下，VPN容量可能仍然低於閾值，但增加VPN使用者數可能會耗盡當前配置的VPN池。在這種情況下，請增加VPN IP池。

但是，如果趨勢顯示大多數VPN流量是外部流量，則可以使用分割隧道。

利用分割通道功能



這是一種功能，它只從使用者系統通過隧道轉發特定流量集，其餘流量則轉發到預設網關，不進行VPN加密。因此，為了降低VPN集中器上的負載，只有發往內部網路的流量可以通過隧道路由，而網際網路流量可以通過使用者的本地ISP轉發。這是一種行之有效的方法、被廣泛採用、但存在一定的風險。

員工可通過未受保護的網路快速訪問某些社群媒體站點，從而感染其筆記型電腦上的惡意軟體。由於缺少工作場所設定的深度防禦安全層，該惡意軟體會擴散到整個公司。一旦被感染，受感染的裝置可能會成為從網際網路進入受信任網段的樞紐，從而繞過邊界防禦。

在使用此功能時降低風險的一種方法是，只對通過嚴格安全標準的雲服務使用拆分隧道，包括良好的資料安全以及與Duo Security的相容性。如果先前觀測到的大量外部流量都流向這些安全雲服務，則採用這一方法會有所幫助。這就需要分析VPN使用者正在訪問的Web應用程式。

大多數下一代防火牆(如Cisco Firepower威脅防禦(FTD))都包含與日誌中的事件相關的應用資訊。使用python **csv**庫和pandas資料操作功能解析和清除此日誌資料可以提供類似的資料集，並新增要被訪問到的對映到該資料的應用程式。

```
#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

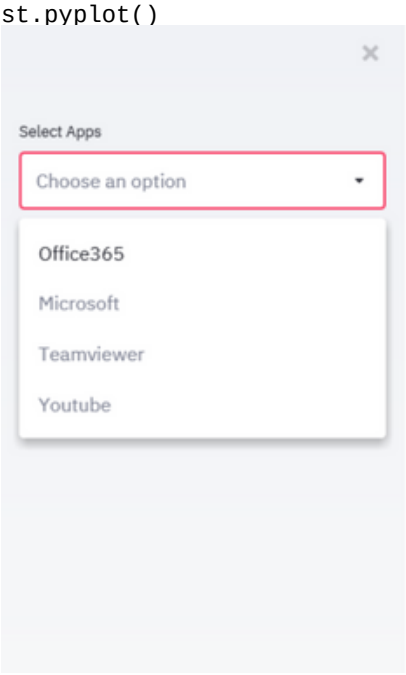
一旦獲得上述資料幀，您就可以根據應用程式通過Panda對外部總流量進行分類。

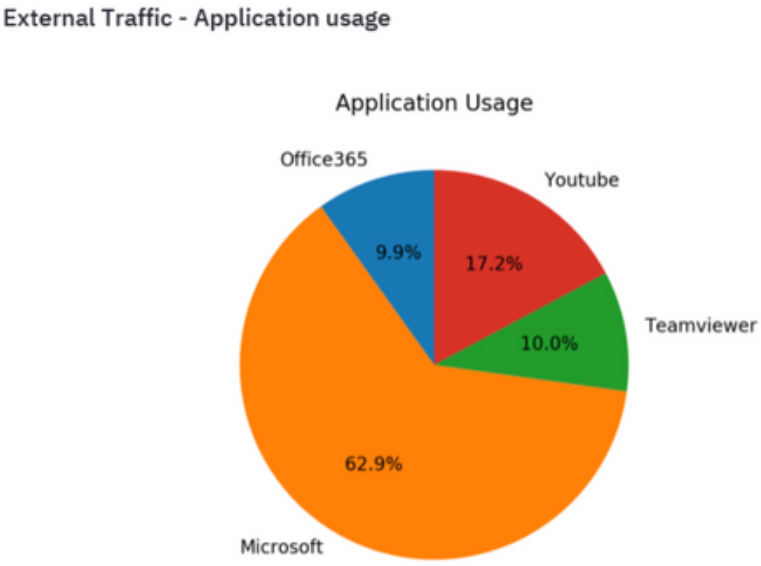
```
df2 = df.groupby('Application')

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

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

再次使用Streamlit可以獲得每個應用佔總流量的份額的圖形表示。它允許靈活地更改要包含的資料的時間視窗，並過濾掉使用者介面上的應用程式而無需對代碼進行任何更改，這使得分析簡單而準確。

```
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()
```



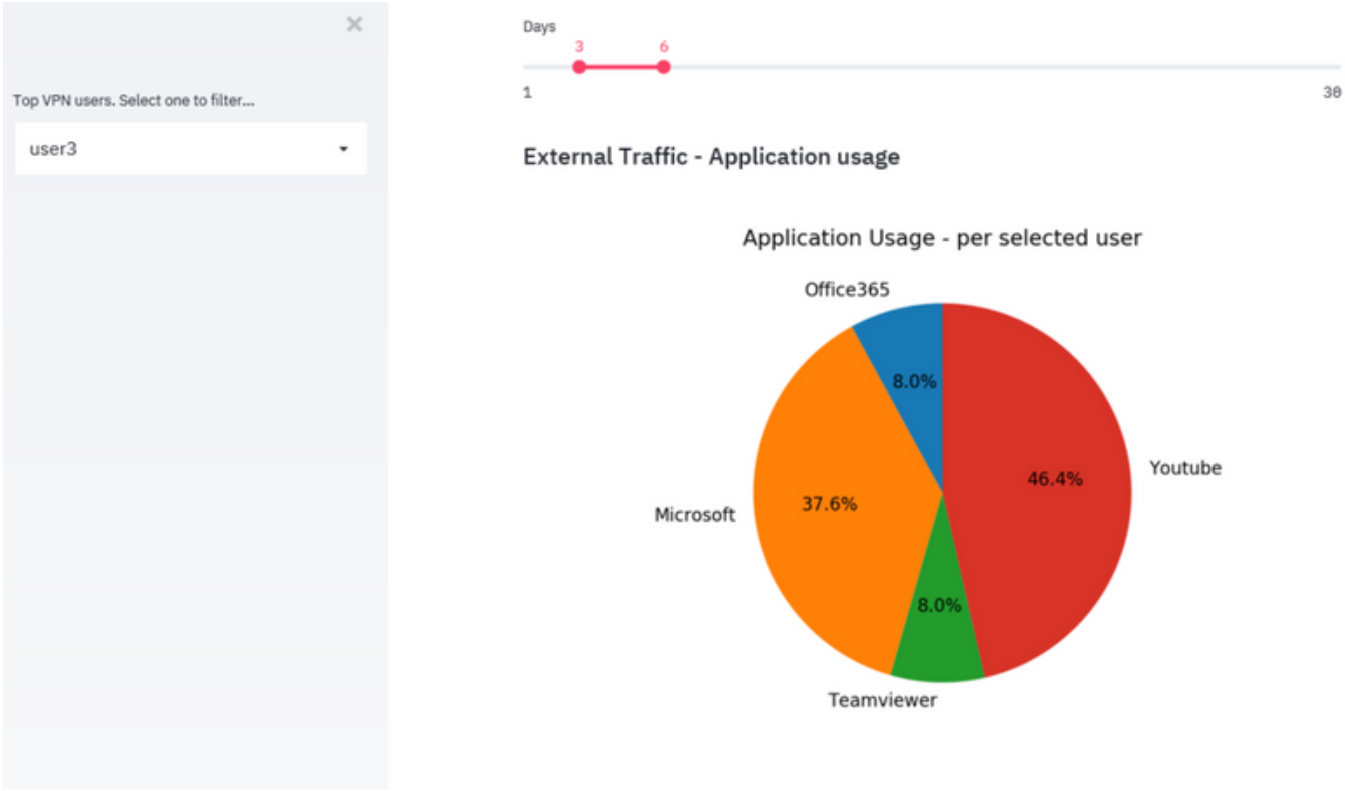


這可以簡化VPN使用者在一段時間內使用的頂級Web應用的識別過程，以及這些應用是否用於保護雲服務。

如果大量應用的目標是要識別安全的雲服務，則它們可與拆分隧道一起使用，從而降低VPN集中器的負載。但是，如果排名靠前的應用程式用於安全性較低或可能帶來風險的服務，則通過VPN隧道傳輸這些應用程式更加安全。原因是，其他網路安全裝置可以在允許此類流量通過之前處理流量。然後，您可以利用防火牆上的訪問策略來限制對外部網路的訪問。

標識單個不符合VPN的使用者

在某些情況下，激增可能只與少數不符合某些策略的使用者有關。以上使用的模組和資料集可以再次用於識別頂級VPN使用者及其訪問的Web應用程式。這有助於隔離此類使用者，並觀察其對裝置負載的影響。



如果任何方法都不適用，管理員應檢視終端安全解決方案（如面向終端的AMP解決方案和思科Umbrella解決方案），以保護未受保護網路中的終端。