Acercamiento programático para optimizar el VPN de acceso remoto puesto con el Analytics de los datos

Contenido

Introducción

Este documento describe cómo monitorear y optimizar el VPN de acceso remoto configurado con algunas de los módulos y de las herramientas de origen abierto de programación disponibles hoy. Muchos datos se generan hoy en incluso el más pequeño de las redes que se pueden aprovechar para obtener la información útil. Aplicando el analytics en esto las ayudas recogidas de los datos hacen más rápidamente, decisiones comerciales más informadas, sostenidas por los hechos.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- VPN de acceso remoto
- Conceptos de programación básicos de Python

Componentes Utilizados

Este documento no se restringe a Cisco específico ASA o a las versiones de software y hardware FTD.

> Nota: Las pandas, Streamlit, el CSV, y Matplotlib son algunas bibliotecas de Python se utilizan que.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está viva, asegúrese de que usted entienda el impacto potencial de los scripts del comando any y del pitón.

Problema

Con muchas compañías adoptando el trabajo del modelo casero para una mayoría de sus empleados por todas partes, el número de usuarios que confiaban en el VPN para realizar sus trabajos ha aumentado considerablemente. Esto ha llevado a un aumento súbito y considerable de la carga en los concentradores VPN que llevaban a los administradores a repensar y a replanificar sus configuraciones de VPN. Tomar las decisiones informadas para reducir la carga en los concentradores ASA requiere la recogida de una amplia variedad de información de los dispositivos durante un período de tiempo y evaluar esa información, que es una tarea compleja y requeriría una cantidad de tiempo considerable si está hecha manualmente.

Solución

Con el hoy disponible de varios de Python módulos y de las herramientas de origen abierto para la programabilidad de la red y analytics de los datos, la programación puede demostrar ser muy útil en la colección y la análisis de datos, las hojas de operación (planning), y optimización de la configuración de VPN.

Análisis inicial basada en los usuarios de VPN y las conexiones concurrentes

Para comenzar el análisis para obtener el número de conexión de los usuarios, de conexiones concurrentes establecidas, y de su impacto en el ancho de banda. Las salidas de comando siguientes de Cisco ASA proporcionarán estos detalles:

- muestre el anyconnect de VPN-sessiondb
- show conn

El módulo Netmiko de Python se puede utilizar al ssh al dispositivo, funciona con los comandos, y analiza las salidas.

```
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)
```

Recoja la cuenta del usuario de VPN y las conexiones cuentan a intervalos regulares (cada 2 horas pueden ser un buen comienzo) en una lista y obtienen la cuenta diaria del máximo por un día.

```
#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])
```

Las pandas son una análisis de datos eficiente y la biblioteca de la manipulación y todos los datos analizados se pueden salvar como una serie o marco de datos en las pandas que hacen las operaciones en los datos fáciles.

```
import pandas as pd

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

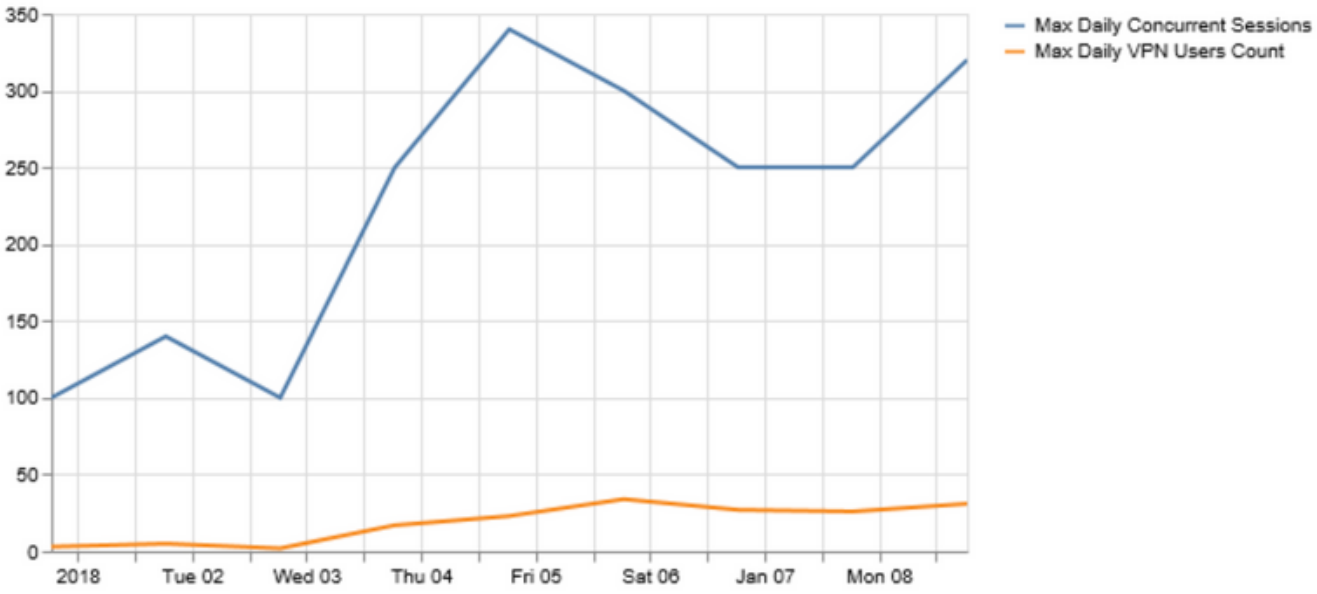
Daily Max VPN user Count - Max concurrent count

	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

Analice los **usuarios de VPN máximos diarios** y las **conexiones concurrentes máximas** que pueden ayudar a determinar la necesidad de optimizar las configuraciones VPN.

Utilice la función del diagrama en las pandas y la biblioteca del **matplotlib**, tal y como se muestra en de la imagen aquí.

```
df.plot()

matplotlib.pyplot.show()
```



Si el número de usuarios de VPN o las conexiones concurrentes está consiguiendo más cercano a la capacidad de la cabecera VPN, después puede causar estos problemas:

- Nuevos usuarios de VPN que son caídos.
- Nuevas conexiones de datos a través del ASA que es caído y de los usuarios no capaces de acceder los recursos.
- CPU elevada y/o memoria.

La tendencia durante un período de tiempo la ayuda de la poder determina si el rectángulo está alcanzando su umbral.

Identifique la tendencia del tráfico está hacia la red interna o las redes externas

La salida del **show conn** en Cisco ASA puede proporcionar los detalles adicionales por ejemplo si el tráfico está a interno o las redes externas y cuántos datos en los bytes por el flujo se pasan con el Firewall.

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

El uso del módulo del pitón de **Netaddr** hace fácil partir la tabla de conexiones obtenida en los flujos a las redes externas y a las redes internas.

```
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]
```

Ésta es la imagen del tráfico interno.

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

Ésta es la imagen del tráfico externo.

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

De tal modo, proporcionando a una penetración en qué porcentaje del tráfico VPN se destina a las redes internas y cuánto de él está saliendo a Internet. La colección de esta información durante un período de tiempo y del análisis de su tendencia puede ayudar a determinar si el tráfico VPN es predominante externo o interno.

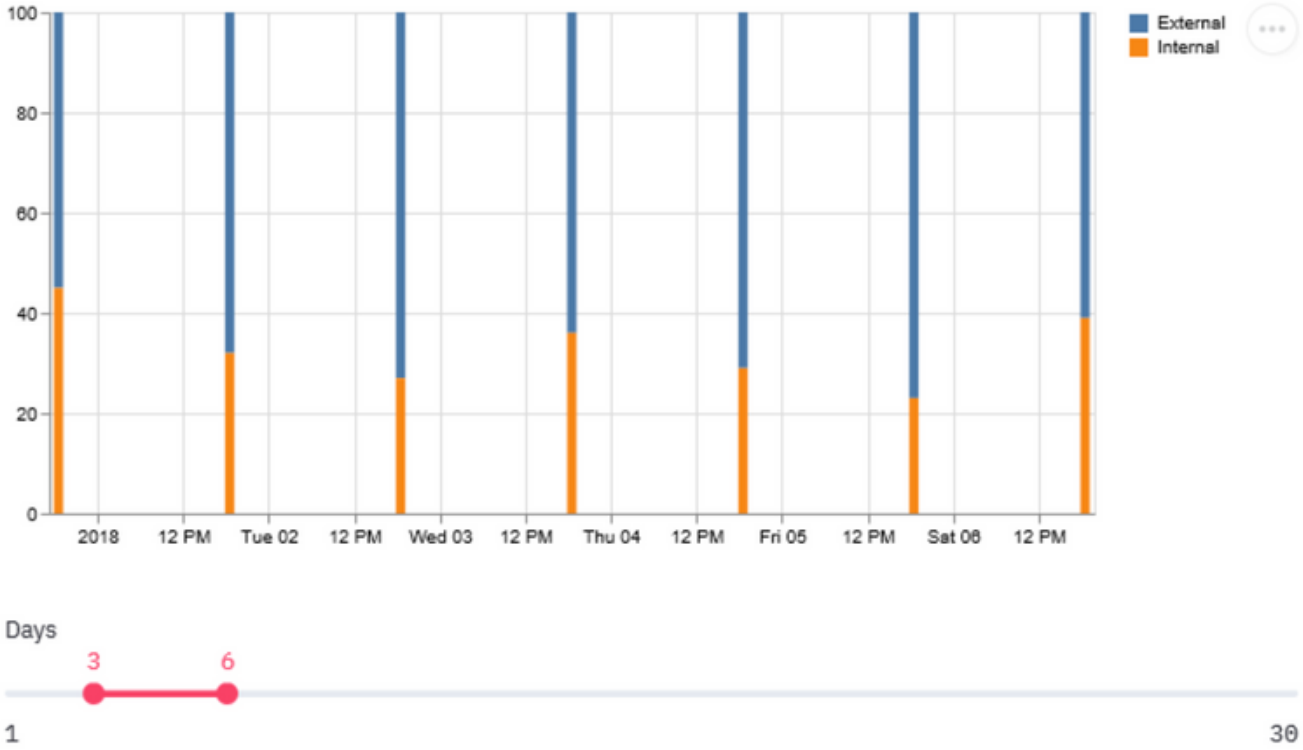
VPN Usage

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

Los módulos como **Streamlit** hacen le posibles no apenas al convertido los datos tabulares en una representación gráfica pero también aplican las modificaciones a él en el tiempo real para ayudar al análisis. Puede modificar la ventana de fecha y hora de los datos recogidos o agregar los datos adicionales a los parámetros que son monitoreados.

```
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)
```

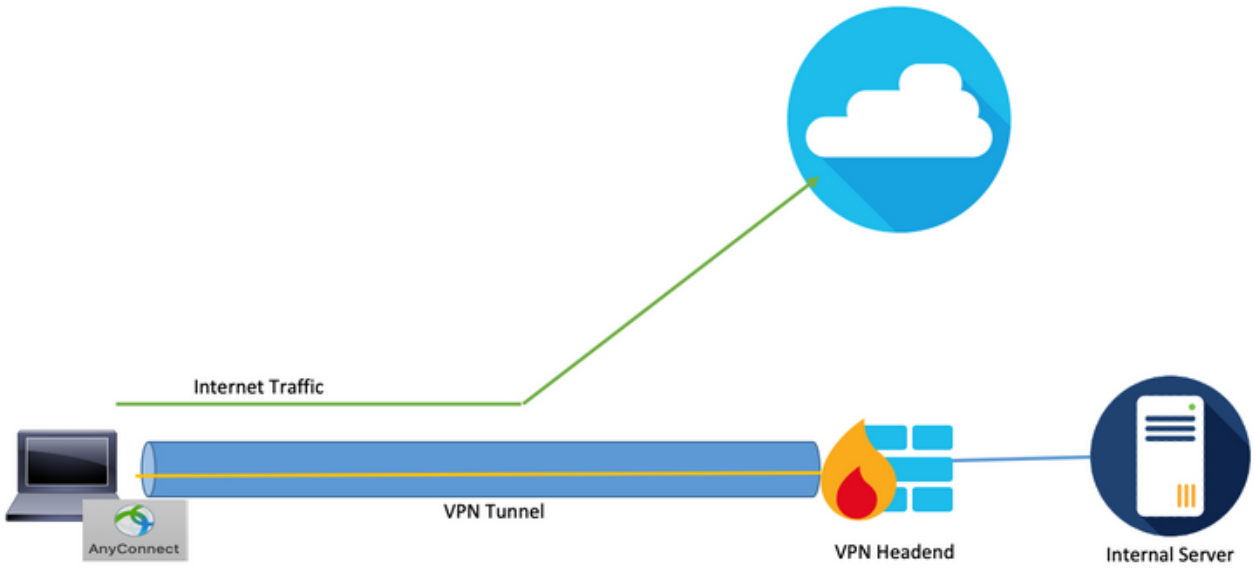


Una tendencia que se inclina hacia un tráfico interno más alto podría significar a esa mayoría de los recursos internos del acceso de usuarios de VPN. Por lo tanto, para abastecer a esto, aumento en la carga, es importante planear las actualizaciones a cuadros más grandes o compartir la carga con los conceptos como el balanceo de carga VPN.

En algunos casos, la capacidad VPN pudo todavía estar bajo umbral pero un aumento en el número de usuarios de VPN puede agotar el pool configurado corriente VPN. En estos casos, aumente la agrupación IP VPN.

Sin embargo, si la tendencia muestra que la mayoría del tráfico VPN es externa, después usted puede utilizar el Túnel dividido.

Utilice la característica del Túnel dividido



Es una característica que adelante solamente un conjunto específico de tráfico con el túnel del sistema de usuario y el resto del tráfico se remite al default gateway sin el cifrado VPN. Por lo tanto, para reducir la carga en el concentrador VPN, solamente el tráfico destinado a la red interna se podría rutear a través del túnel, y el tráfico de Internet se podría remitir con el ISP local del usuario. Esto es un método eficaz y adoptado extensamente pero tiene algunos riesgos asociados a él.

Un acceso del empleado algunos sitios de los media del social sobre las redes no protegidas para una rotura rápida puede infectar su laptop con el malware que se separa a través de la compañía debido a una falta de las capas de la Seguridad de la defensa-en-profundidad que se configuran en el lugar de trabajo. Una vez que estuvo infectado, el dispositivo comprometido podía convertirse en una punta de pivote de Internet en el segmento de confianza, con desvió las defensas de perímetro.

Una manera de reducir el riesgo mientras que utilizar esta característica sería utilizar el Túnel dividido solamente para los servicios de la nube que pasan los criterios rigurosos de la Seguridad, incluyendo la buenas higiene de los datos y compatibilidad con la Seguridad del dúo. La adopción de esto ayudará si una buena cantidad del tráfico externo observado anterior, es destinada para estos servicios seguros de la nube. Esto saca a colación la necesidad de analizar las aplicaciones de Web que son accedidas por los usuarios de VPN.

La mayor parte de los Firewall de la última generación como la defensa de la amenaza de Cisco FirePOWER (FTD) contienen la Información de la aplicación asociada al evento en los registros. El análisis y la limpieza de estos datos de registro con las **bibliotecas del csv del** pitón y las características de la manipulación de datos de las pandas pueden proveer de un grupo de datos similar como arriba una adición de las aplicaciones que son accedidas asociadas a ella.

```
#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

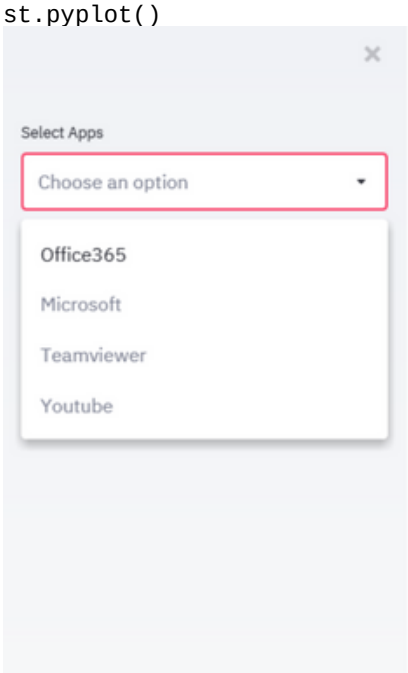
Una vez que un marco de datos como arriba se obtiene, usted puede categorizar el tráfico externo total basado en la aplicación a través de las pandas.

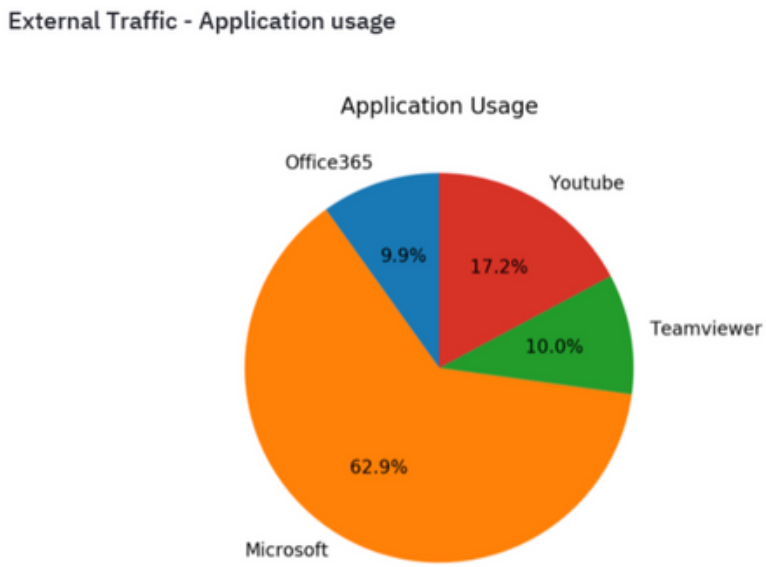
```
df2 = df.groupby('Application')

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

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

El uso de Streamlit obtiene otra vez una representación gráfica de la parte de cada aplicación en el tráfico total. Permite la flexibilidad para cambiar la ventana de fecha y hora para que los datos sean incluidos así como filtrar hacia fuera las aplicaciones en la interfaz de usuario sí mismo sin la necesidad de ningunos cambia en el código, que hace el análisis fácil y exacto.

```
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()
```





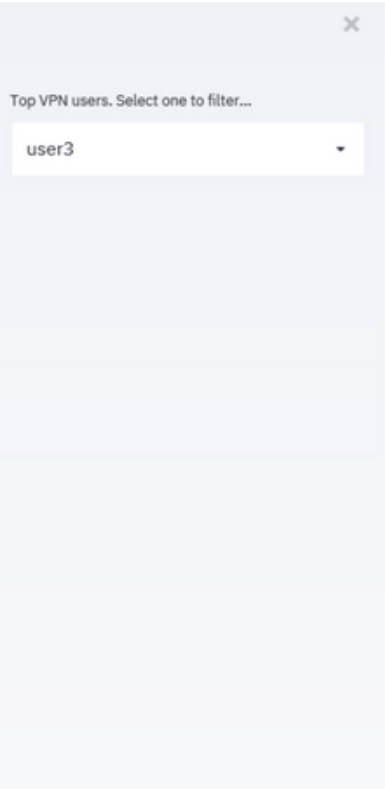
Esto puede simplificar el proceso de la identificación de las aplicaciones de Web superiores que son utilizadas por los usuarios de VPN durante un período de tiempo y si estas aplicaciones son asegurar los servicios de la nube o no.

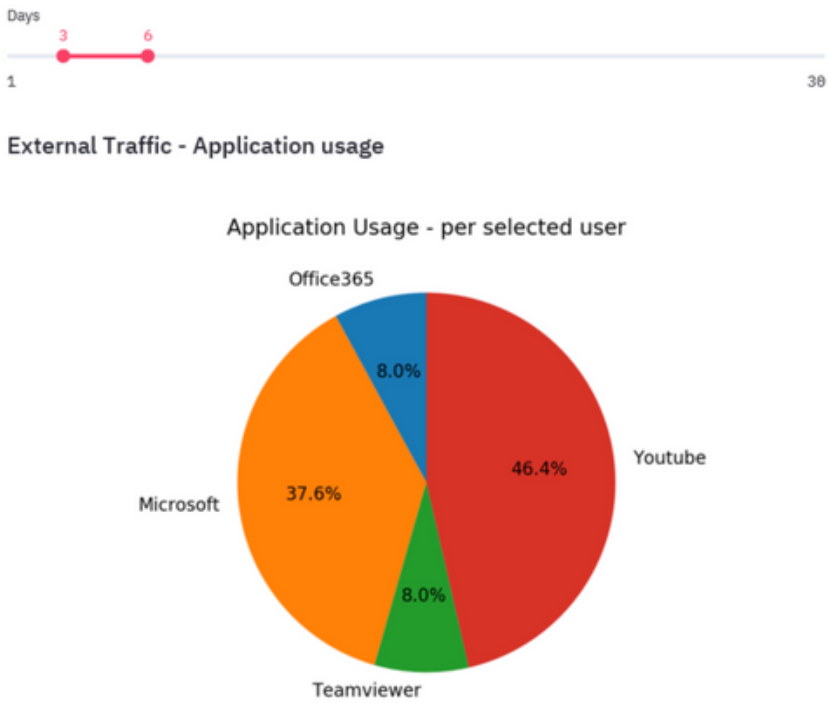
Si las aplicaciones más voluminosas se destinan para identificar los servicios seguros de la nube,

pueden ser utilizadas con un túnel dividido, así reducen la carga en un concentrador VPN. Sin embargo, si las aplicaciones superiores están a los servicios que son menos seguros o pueden plantear un riesgo, es más seguro pasarlos a través del túnel VPN. Razón que es que otros dispositivos de seguridad de la red pueden procesar el tráfico antes de que permitan que tal tráfico pase. Usted puede entonces utilizar las políticas de acceso en los Firewall para limitar el acceso a las redes externas.

Usuarios de VPN no obedientes individuales de la identidad

En algunos casos, la oleada se podría asociar solamente a algunos usuarios con ellos que no cumplen con ciertas directivas. Los módulos y los grupos de datos usados arriba se pueden utilizar otra vez para identificar los usuarios de VPN superiores y las aplicaciones de Web que acceden. Esto puede ayudar en el aislamiento de tales usuarios y observar su efecto sobre la carga del dispositivo.





En los escenarios, donde ningunos de los métodos cabidos, los admins deben mirar las soluciones de la Seguridad de terminales tales como AMP para que la solución de los puntos finales y la solución del paraguas de Cisco protejan los puntos finales en las redes no protegidas.