Abordagem programática para otimizar a configuração da VPN de acesso remoto por meio da análise de dados

Contents

Introduction

Este documento descreve como monitorar e otimizar a configuração da VPN de acesso remoto por meio de alguns módulos de programação e ferramentas de código aberto disponíveis atualmente. Muitos dados são gerados hoje mesmo nas menores redes que podem ser aproveitadas para obter informações úteis. A aplicação de análises nesses dados coletados ajuda a tomar decisões comerciais mais rápidas e mais informadas, com o respaldo de fatos.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- VPN de acesso remoto
- Conceitos básicos de programação Python

Componentes Utilizados

Este documento não está restrito a versões específicas de software e hardware do Cisco ASA ou FTD.

> **Note**: Pandas, Streamlit, CSV e Matplotlib são algumas bibliotecas Python usadas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a sua rede

estiver ativa, certifique-se de que você entende o impacto potencial de qualquer comando e scripts python.

Problema

Com muitas empresas adotando o modelo Work From Home para a maioria de seus funcionários em todo o mundo, o número de usuários que dependem de VPN para realizar seus trabalhos aumentou consideravelmente. Isso levou a um aumento repentino e considerável da carga nos concentradores VPN, levando os administradores a repensar e replanejar suas configurações de VPN. Tomar decisões conscientes para reduzir a carga nos concentradores ASA exige coletar uma ampla variedade de informações dos dispositivos durante um período de tempo e avaliar essas informações, que é uma tarefa complexa e exigiria um tempo considerável se fossem feitas manualmente.

Solução

Com vários módulos Python e ferramentas de código aberto disponíveis atualmente para análise de dados e programabilidade de rede, a programação pode ser muito útil na coleta e análise de dados, planejamento e otimização da configuração da VPN.

Análise inicial baseada em usuários VPN e conexões simultâneas

Para iniciar a análise, obtenha o número de usuários conectados, conexões simultâneas estabelecidas e seu impacto na largura de banda. As seguintes saídas de comandos do Cisco ASA fornecerão estes detalhes:

- **show vpn-sessiondb anyconnect**
- **show conn**

O módulo Python **Netmiko** pode ser usado para ssh para o dispositivo, executar os comandos e analisar as saídas.

```
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)
```

Colete a contagem de usuários e conexões VPN em intervalos regulares (a cada 2 horas pode ser um bom começo) em uma lista e obtenha a contagem máxima diária para um dia.

```
#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 é uma biblioteca eficiente de análise e manipulação de dados e todos os dados analisados podem ser armazenados como uma série ou quadro de dados em pandas, facilitando as operações sobre os dados.

```
import pandas as pd

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

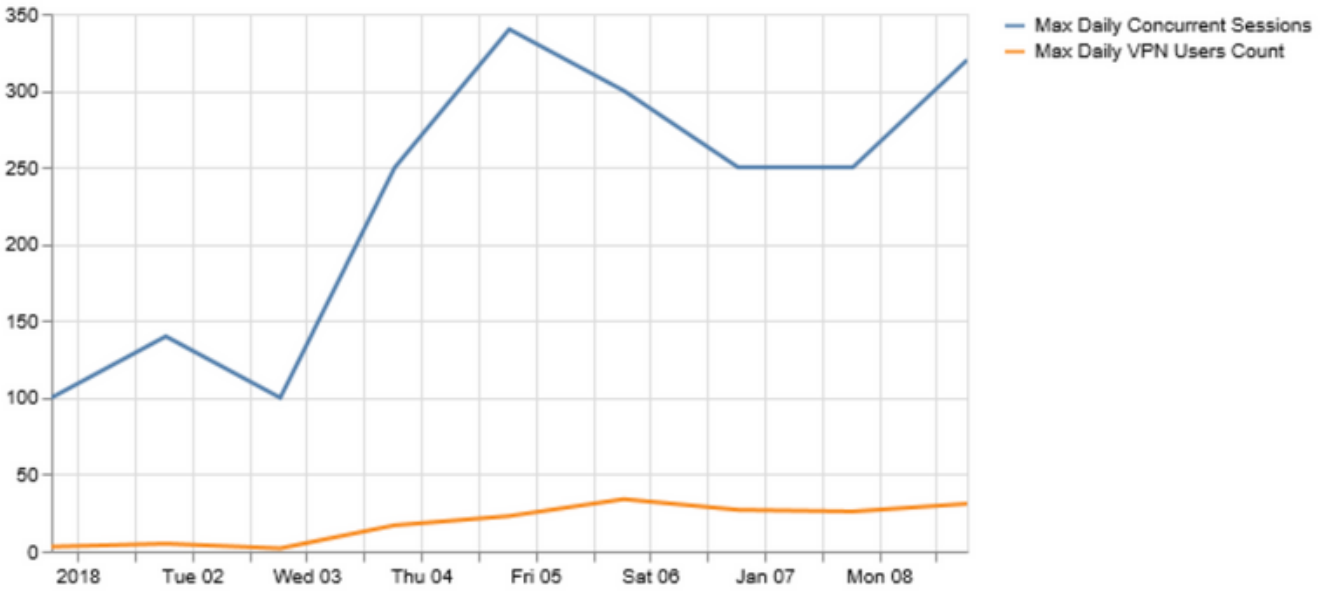
Daily Max VPN user Count - Max concurrent count

	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

Analise o **máximo diário de usuários de VPN** e o **máximo de conexões simultâneas** que podem ajudar a determinar a necessidade de otimizar as configurações de VPN.

Use a função de gráfico em pandas e na biblioteca **matplotlib**, como mostrado na imagem aqui.

```
df.plot()

matplotlib.pyplot.show()
```



Se o número de usuários de VPN ou conexões simultâneas estiver se aproximando da capacidade do headend de VPN, isso pode causar estes problemas:

- Novos usuários de VPN sendo descartados.
- Novas conexões de dados por meio do ASA estão sendo descartadas e os usuários não podem acessar os recursos.
- Alta CPU e/ou memória.

A tendência ao longo de um período de tempo pode ajudar a determinar se a caixa está atingindo seu limite.

Identificar a tendência do tráfego em direção à rede interna ou às redes externas

A saída **show conn** no Cisco ASA pode fornecer detalhes adicionais, como se o tráfego é para redes internas ou externas e a quantidade de dados em bytes por fluxo é passada pelo 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

O uso do módulo python **Netaddr** facilita a divisão da tabela de conexão obtida em fluxos para

redes externas e para 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]
```

Esta é a imagem do tráfego 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

Esta é a imagem do tráfego 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

Dessa forma, fornecer uma visão sobre qual porcentagem do tráfego VPN é destinado às redes internas e quanto dele está saindo para a Internet. A coleta dessas informações durante um período de tempo e a análise de sua tendência podem ajudar a determinar se o tráfego VPN é predominantemente externo ou interno.

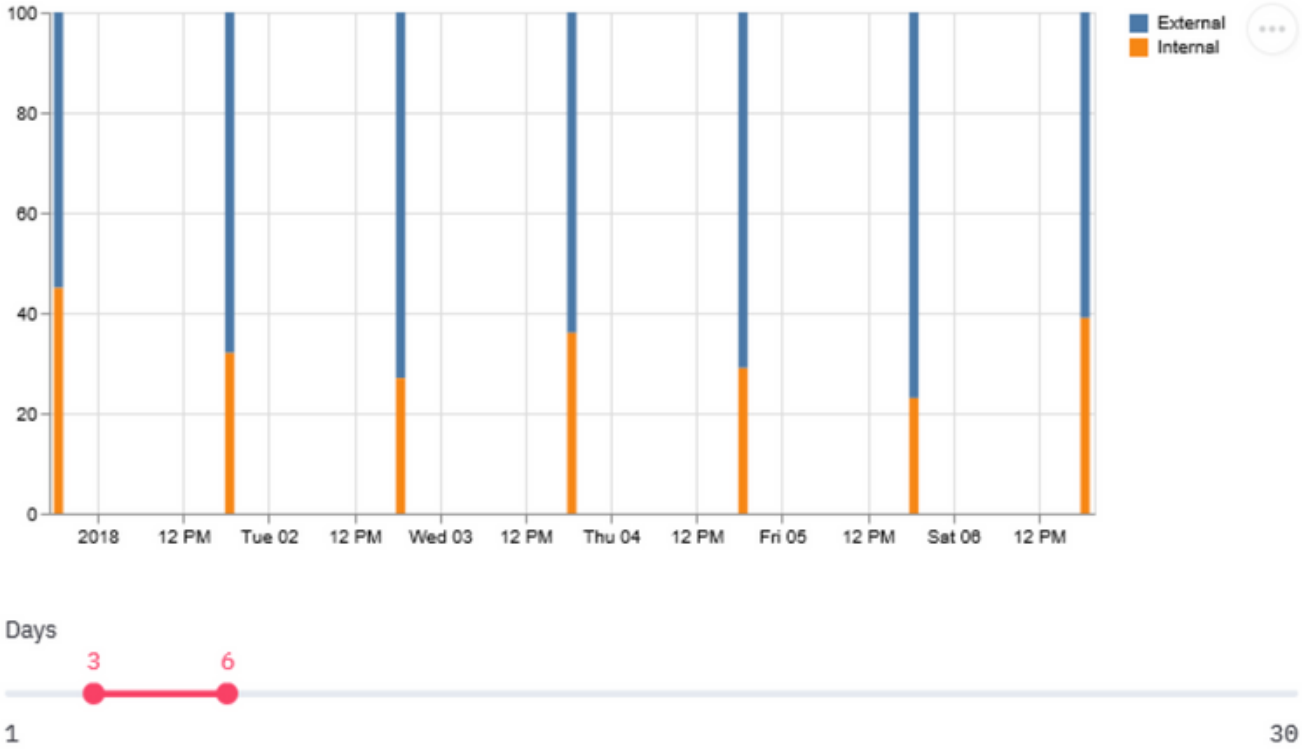
VPN Usage

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

Módulos como o **Streamlit** possibilitam não apenas converter os dados em tabela em uma representação gráfica, mas também aplicar modificações a eles em tempo real para auxiliar a análise. Ele pode modificar a janela de tempo dos dados coletados ou adicionar dados adicionais aos parâmetros que estão sendo monitorados.

```
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)
```

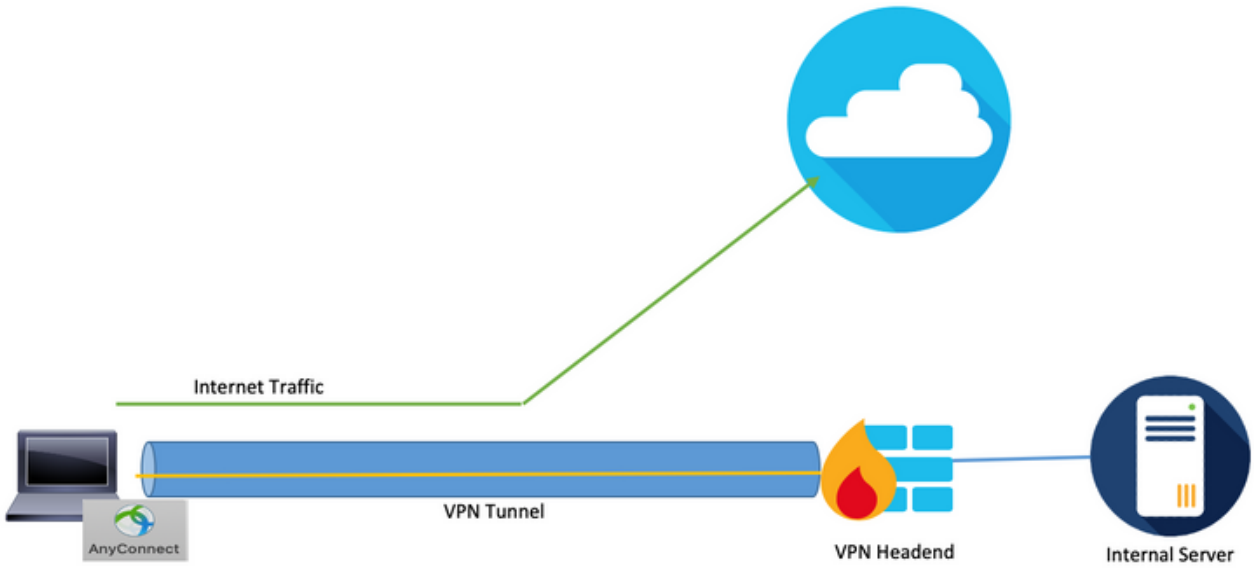


Uma tendência que se inclina para um maior tráfego interno pode significar que a maioria dos usuários de VPN acessa recursos internos. Portanto, para atender a isso, aumentar a carga, é importante planejar atualizações para caixas maiores ou compartilhar a carga com conceitos como balanceamento de carga de VPN.

Em alguns casos, a capacidade de VPN pode ainda estar abaixo do limite, mas um aumento no número de usuários de VPN pode esgotar o pool de VPN configurado atualmente. Nesses casos, aumente o VPN IP Pool.

No entanto, se a tendência mostrar que a maioria do tráfego de VPN é externo, você poderá usar o tunelamento dividido.

Utilize o recurso de tunelamento dividido



Éum recurso que encaminha apenas um conjunto específico de tráfego através do túnel do sistema do usuário e o restante do tráfego é encaminhado para o gateway padrão sem criptografia de VPN. Assim, para reduzir a carga no VPN Concentrator, somente o tráfego destinado à rede interna poderia ser roteado pelo túnel e o tráfego da Internet poderia ser encaminhado através do ISP local do usuário. Trata-se de um método eficaz e amplamente adotado, mas que comporta alguns riscos.

Um funcionário acessa alguns sites de mídia social em redes desprotegidas para uma rápida interrupção pode infectar seu laptop com malware que se espalha pela empresa devido à falta das camadas de segurança de defesa profundas que estão configuradas no local de trabalho. Depois de infectado, o dispositivo comprometido pode se tornar um ponto central da Internet para o segmento confiável, com defesas de perímetro ignoradas.

Uma maneira de reduzir o risco ao utilizar esse recurso seria usar o tunelamento dividido somente para serviços em nuvem que passem por critérios rigorosos de segurança, incluindo boa higiene de dados e compatibilidade com a segurança Duo. Adotar isso ajudará se uma boa parte do tráfego externo observado anteriormente for destinada a esses serviços de nuvem seguros. Isso aumenta a necessidade de analisar os aplicativos da Web que estão sendo acessados por usuários de VPN.

A maioria dos firewalls de próxima geração, como o Cisco Firepower Threat Defense (FTD), contém informações de aplicativos associadas ao evento em logs. A análise e limpeza destes dados de registro com **bibliotecas csv** python e funcionalidades de manipulação de dados pandas podem fornecer um conjunto de dados semelhante ao acima com uma adição dos aplicativos que estão a ser acessados mapeados para ele.

```
#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

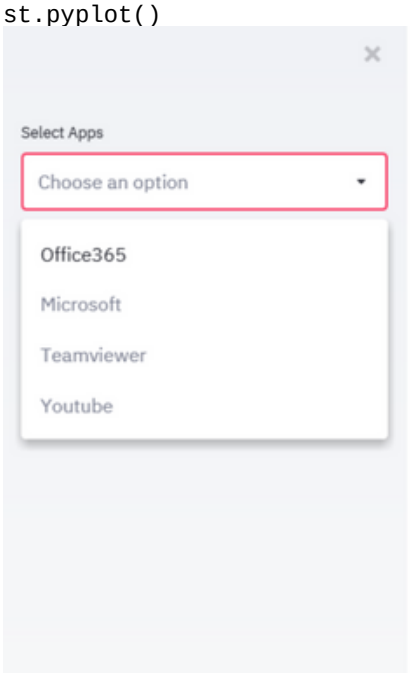
Depois que um quadro de dados como acima é obtido, você pode categorizar o tráfego externo total com base no aplicativo por meio de pandas.

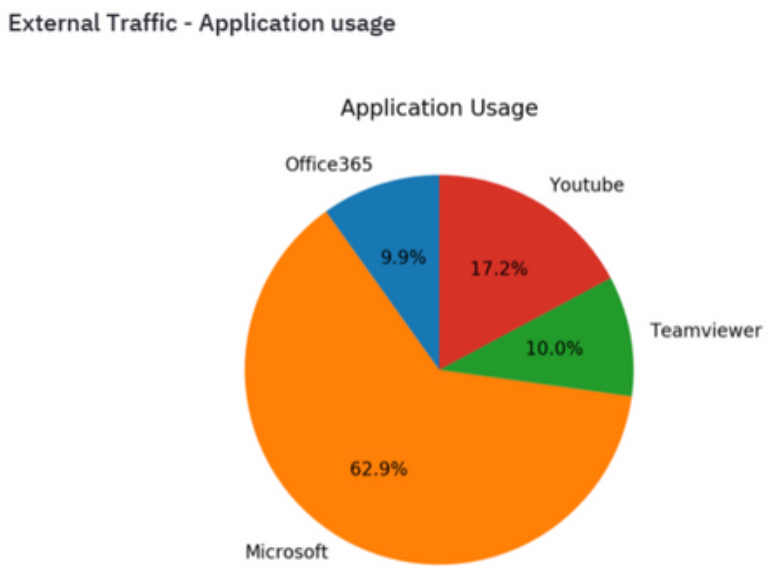
```
df2 = df.groupby('Application')

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

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

O uso do Streamlit obtém novamente uma representação gráfica do compartilhamento de cada aplicativo no tráfego total. Ele permite a flexibilidade de alterar a janela de tempo para que os dados sejam incluídos, bem como filtrar aplicativos na própria interface do usuário sem a necessidade de qualquer alteração no código, o que torna a análise fácil e precisa.

```
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()
```





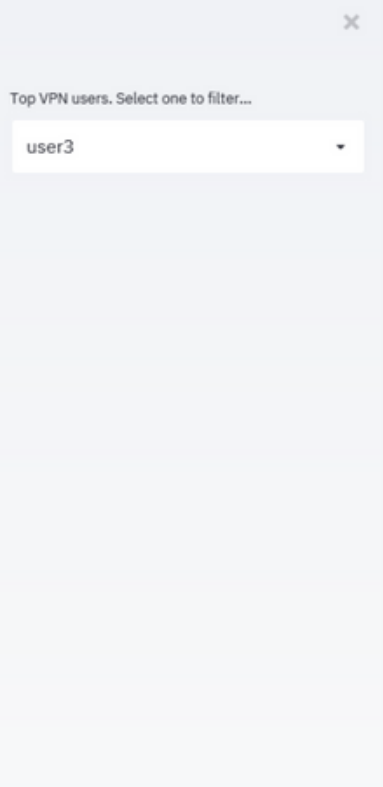
Isso pode simplificar o processo de identificação dos principais aplicativos da Web que estão sendo usados por usuários de VPN ao longo do tempo e se esses aplicativos devem proteger ou não os serviços de nuvem.

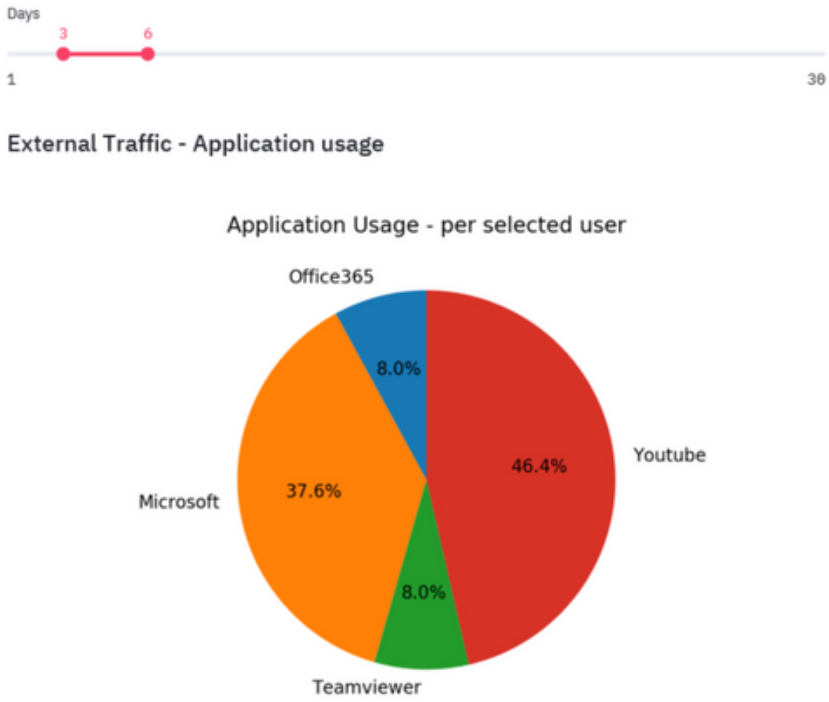
Se os aplicativos mais volumosos forem destinados a identificar serviços de nuvem seguros, eles

poderão ser usados com um túnel dividido, reduzindo assim a carga em um concentrador VPN. No entanto, se os principais aplicativos são para serviços menos seguros ou podem representar um risco, é mais seguro passá-los pelo túnel VPN. O motivo é que outros dispositivos de segurança de rede podem processar o tráfego antes de permitir a passagem desse tráfego. Você pode utilizar políticas de acesso nos firewalls para limitar o acesso a redes externas.

Identidade de usuários VPN não compatíveis

Em alguns casos, o aumento pode estar associado a apenas alguns usuários que não estão em conformidade com certas políticas. Os módulos e conjuntos de dados usados acima podem ser usados novamente para identificar os principais usuários de VPN e os aplicativos da Web que eles acessam. Isso pode ajudar no isolamento desses usuários e observar seu efeito na carga do dispositivo.





Nos cenários em que nenhum dos métodos se encaixa, os administradores devem considerar soluções de segurança de endpoints como a solução AMP para endpoints e a solução Cisco Umbrella para proteger os endpoints em redes desprotegidas.