Programmgesteuerter Ansatz zur Optimierung der Remote Access VPN-Einrichtung mithilfe von Datenanalysen

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie das Remote Access VPN, das über einige der derzeit verfügbaren Programmiermodule und Open-Source-Tools eingerichtet wurde, überwacht und optimiert wird. Heutzutage werden viele Daten selbst in kleinsten Netzwerken generiert, die genutzt werden können, um nützliche Informationen zu erhalten. Durch die Anwendung von Analysen auf diese gesammelten Daten lassen sich schnellere und fundiertere Geschäftsentscheidungen treffen, die durch Fakten gestützt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- VPN für Remote-Zugriff
- Grundlegende Python-Programmierkonzepte

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen von Cisco ASA oder FTD beschränkt.

> **Hinweis**: Pandas, Streamlit, CSV und Matplotlib sind einige Python-Bibliotheken, die verwendet werden.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen von Befehls- und Python-Skripts verstehen.

Problem

Da viele Unternehmen für die meisten ihrer Mitarbeiter überall das Heimmodell "Work From Home" verwenden, ist die Anzahl der Benutzer, die ihre Arbeit über VPN erledigen, erheblich gestiegen. Dies führte zu einer plötzlichen und beträchtlichen Zunahme der Belastung der VPN-Konzentratoren, die die Administratoren dazu veranlasste, ihre VPN-Konfigurationen zu überdenken und neu zu planen. Um fundierte Entscheidungen zur Reduzierung der Belastung der ASA-Konzentratoren treffen zu können, müssen die Geräte über einen bestimmten Zeitraum eine Vielzahl von Informationen sammeln und diese Informationen einschätzen. Dies ist eine komplexe Aufgabe, die bei manueller Durchführung einen beträchtlichen Zeitaufwand erfordern würde.

Lösung

Da heute mehrere Python-Module und Open-Source-Tools für Netzwerkprogrammierung und Datenanalysen verfügbar sind, kann sich die Programmierung bei der Erfassung und Analyse von Daten, Planung und Optimierung der VPN-Konfiguration als sehr hilfreich erweisen.

Erstanalyse basierend auf VPN-Benutzern und gleichzeitigen Verbindungen

Um die Analyse zu starten, ermitteln Sie die Anzahl der Benutzer, die Verbindungen gleichzeitig hergestellt haben, und deren Auswirkungen auf die Bandbreite. Die folgenden Cisco ASA-Befehlsausgaben liefern diese Details:

- **show vpn-sessiondb anyconnect**
- **Show Conn**

Das Python-Modul **Netmiko** kann verwendet werden, um auf das Gerät zu ssh, die Befehle auszuführen und die Ausgaben zu analysieren.

```
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)
```

Sammeln Sie die Anzahl der VPN-Benutzer und -Verbindungen in regelmäßigen Abständen (alle 2 Stunden können ein guter Start sein) in einer Liste, und erhalten Sie die maximale Tageszahl für einen Tag.

```
#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 ist eine effiziente Datenbank für Datenanalyse und -manipulation, und alle geparsten Daten können als Serien- oder Datenrahmen in Pandas gespeichert werden, was die Bedienung der Daten erleichtert.

```
import pandas as pd

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

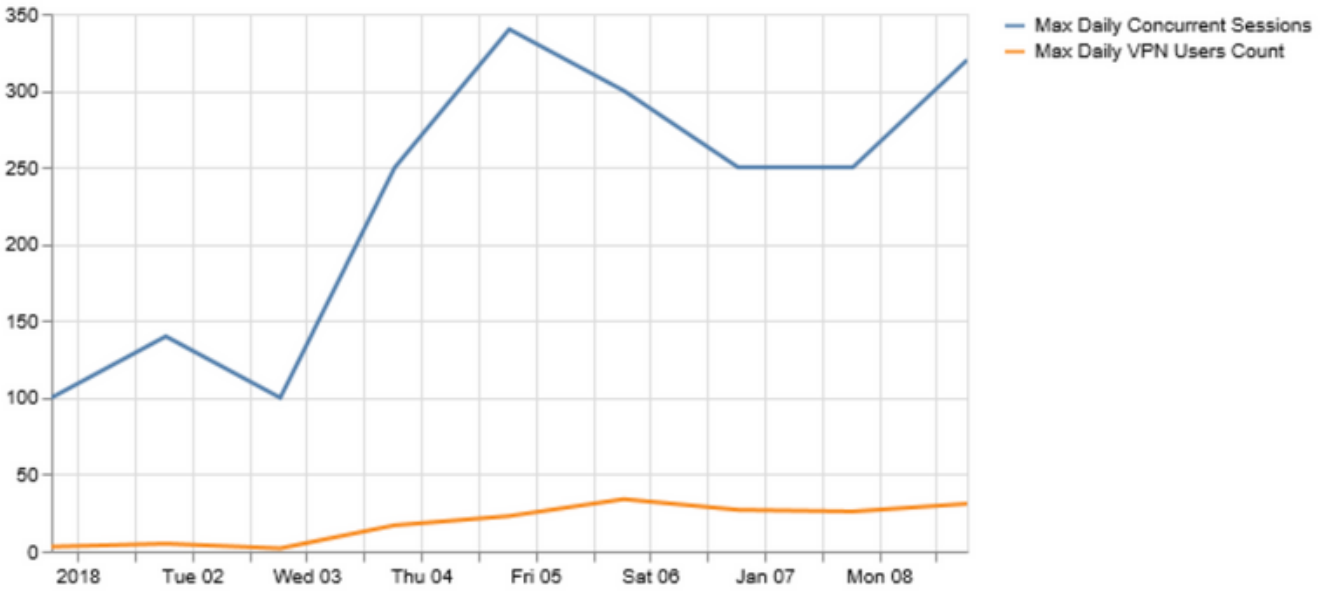
Daily Max VPN user Count - Max concurrent count

	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

Analysieren Sie die **täglichen maximalen VPN-Benutzer** und die **maximale Anzahl gleichzeitiger Verbindungen**, um die Notwendigkeit zur Optimierung der VPN-Einstellungen zu ermitteln.

Verwenden Sie die Plotfunktion in Pandas und **matplotlib** Bibliothek, wie im Bild hier gezeigt.

```
df.plot()

matplotlib.pyplot.show()
```



Wenn die Anzahl der VPN-Benutzer oder der gleichzeitigen Verbindungen der Kapazität des VPN-Headends nähert, kann dies folgende Probleme verursachen:

- Neue VPN-Benutzer werden verworfen.
- Neue Datenverbindungen über die ASA werden verworfen, und Benutzer können nicht auf die Ressourcen zugreifen.
- Hohe CPU und/oder Speicher.

Der Trend über einen bestimmten Zeitraum kann dabei helfen festzustellen, ob die Box ihren Grenzwert erreicht.

Identifizieren des Datenverkehrstrends zu internen oder externen Netzwerken

Show conn Output on Cisco ASA kann zusätzliche Details bereitstellen, z. B. ob der Datenverkehr in interne oder externe Netzwerke fließt und wie viele Daten in Byte pro Datenfluss über die Firewall übertragen werden.

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

Die Verwendung des Netadr-Python-Moduls vereinfacht die Aufteilung der ermittelten Verbindungstabelle in Datenflüsse zu externen Netzwerken und internen Netzwerken.

```
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]
```

Dies ist das Bild des internen Datenverkehrs.

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

Dies ist das Bild des externen Datenverkehrs.

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

Dadurch erhalten Sie einen Einblick in den Anteil des VPN-Datenverkehrs, der für interne Netzwerke bestimmt ist, und in den Umfang, in dem dieser Verkehr in das Internet fließt. Die Erfassung dieser Informationen über einen bestimmten Zeitraum und die Analyse des Trends können dabei helfen festzustellen, ob der VPN-Datenverkehr überwiegend extern oder intern ist.

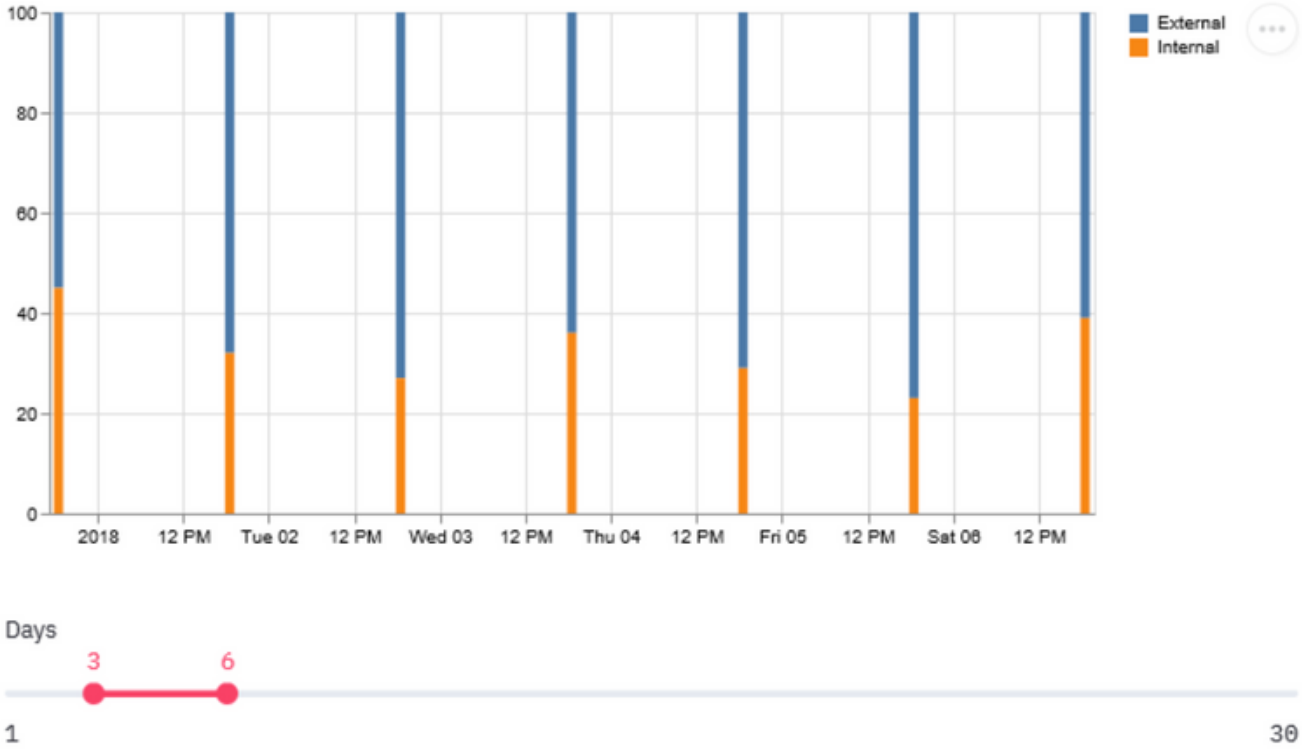
VPN Usage

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

Module wie **Streamlit** ermöglichen nicht nur die Konvertierung tabellarischer Daten in eine grafische Darstellung, sondern auch die Anpassung in Echtzeit, um die Analyse zu unterstützen. Sie kann das Zeitfenster der erfassten Daten ändern oder den überwachten Parametern zusätzliche Daten hinzufügen.

```
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)
```

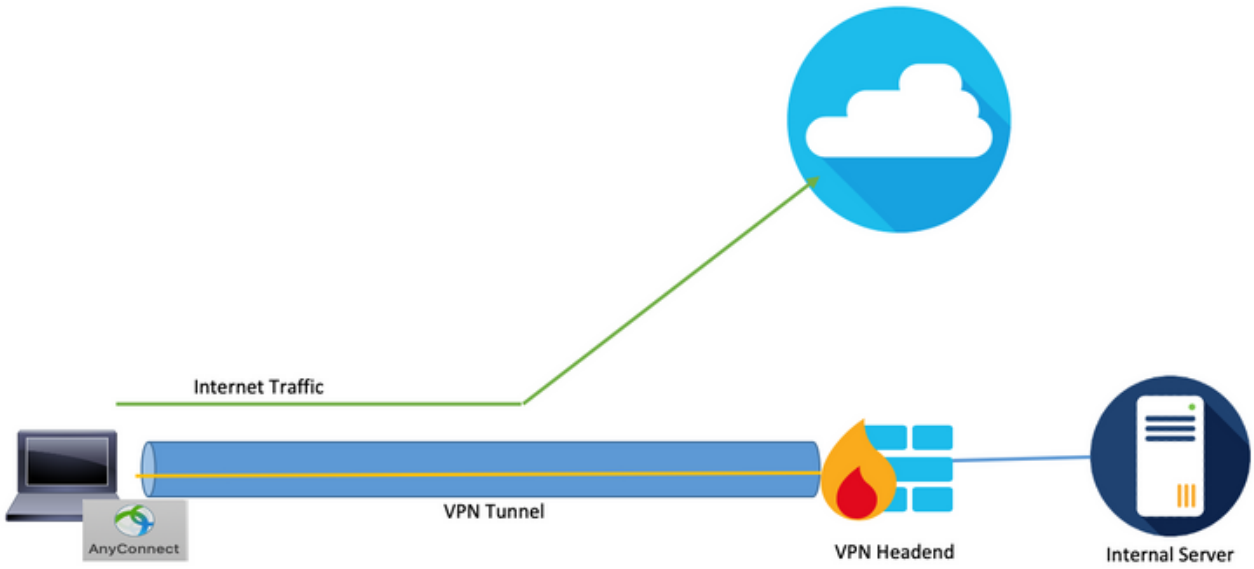


Ein Trend, der zu einem höheren internen Datenverkehr führt, könnte bedeuten, dass die meisten VPN-Benutzer auf interne Ressourcen zugreifen. Daher ist es wichtig, Upgrades für größere Geräte zu planen oder die Last für Konzepte wie den VPN-Lastenausgleich freizugeben, um diesem Problem zu begegnen und die Last zu erhöhen.

In einigen Fällen liegt die VPN-Kapazität möglicherweise noch unter dem Schwellenwert, aber eine Erhöhung der Anzahl von VPN-Benutzern kann den aktuell konfigurierten VPN-Pool ausschöpfen. In solchen Fällen sollte der VPN-IP-Pool erhöht werden.

Wenn der Trend jedoch zeigt, dass der Großteil des VPN-Datenverkehrs extern ist, können Sie Split-Tunneling verwenden.

Split-Tunneling-Funktion verwenden



Diese Funktion leitet nur einen bestimmten Datenverkehr durch den Tunnel vom Benutzersystem weiter, und der restliche Datenverkehr wird ohne VPN-Verschlüsselung an das Standard-Gateway weitergeleitet. Um die Belastung des VPN-Konzentrators zu reduzieren, konnte nur der für das interne Netzwerk bestimmte Datenverkehr über den Tunnel geleitet und der Internetdatenverkehr über den lokalen ISP des Benutzers weitergeleitet werden. Dies ist eine effektive und weit verbreitete Methode, die aber mit einigen Risiken verbunden ist.

Ein Mitarbeiter, der über ungeschützte Netzwerke auf einige Social Media-Sites zugreift, kann seinen Laptop mit Malware infizieren, die sich im gesamten Unternehmen verbreitet, da es an den am Arbeitsplatz eingerichteten Sicherheitsebenen fehlt. Sobald das kompromittierte Gerät infiziert ist, könnte es zum Drehpunkt des Internets zum vertrauenswürdigen Segment werden, wobei die Perimeterabwehr umgangen wird.

Eine Möglichkeit, das Risiko bei Nutzung dieser Funktion zu reduzieren, besteht darin, Split-Tunneling nur für Cloud-Services zu verwenden, die strenge Sicherheitskriterien erfüllen, einschließlich guter Datenhygiene und Kompatibilität mit Duo Security. Dies ist hilfreich, wenn ein Großteil des zuvor beobachteten externen Datenverkehrs für diese sicheren Cloud-Services bestimmt ist. Dies erfordert eine Analyse der Webanwendungen, auf die VPN-Benutzer zugreifen.

Die meisten Firewalls der nächsten Generation wie Cisco FirePOWER Threat Defense (FTD) enthalten Anwendungsinformationen, die mit dem Ereignis in Protokollen verknüpft sind. Das Analysieren und Reinigen dieser Protokolldaten mit Python-**CSV-Bibliotheken** und Datenbearbeitungsfunktionen für Pandas kann ein ähnliches Dataset bereitstellen, wie oben beschrieben, und es können zusätzliche Anwendungen hinzugefügt werden, auf die zugegriffen wird.

```
#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

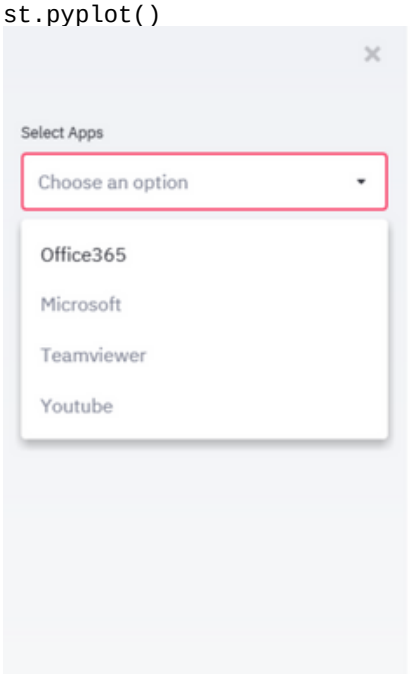
Nachdem ein Daten-Frame wie oben angegeben abgerufen wurde, können Sie den gesamten externen Datenverkehr basierend auf der Anwendung über Pandas kategorisieren.

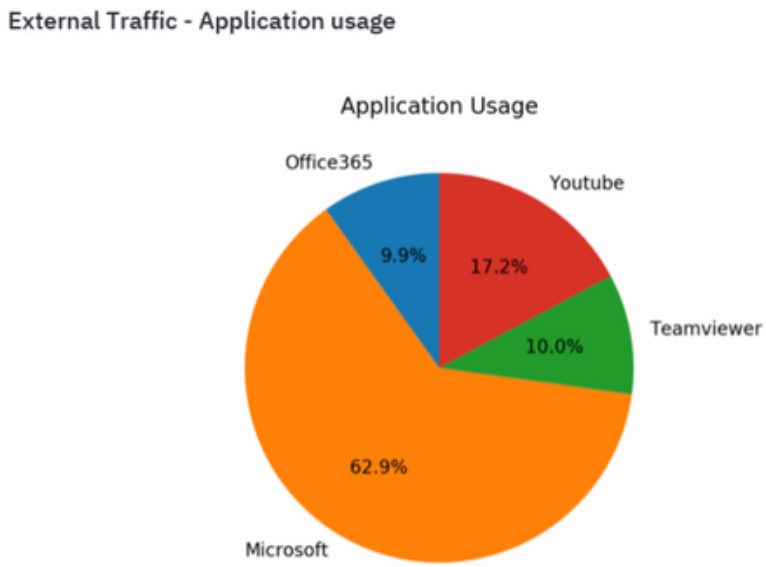
```
df2 = df.groupby('Application')

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

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

Die Verwendung von Streamlit erhält wiederum eine grafische Darstellung des Anteils jeder Anwendung am gesamten Datenverkehr. Es ermöglicht die Flexibilität, das Zeitfenster für die Einfügung von Daten zu ändern und Anwendungen auf der Benutzeroberfläche selbst zu filtern, ohne dass Änderungen am Code erforderlich sind, was die Analyse einfach und präzise macht.

```
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()
```





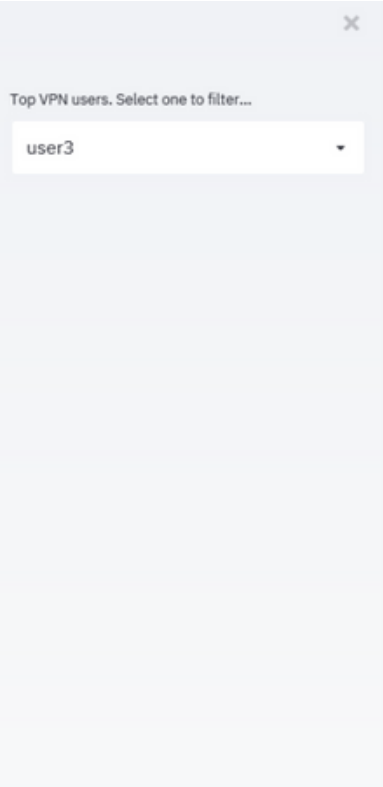
Dies kann die Identifizierung der wichtigsten Webanwendungen, die von VPN-Benutzern über einen bestimmten Zeitraum verwendet werden, vereinfachen, wenn diese Anwendungen Cloud-Services schützen sollen oder nicht.

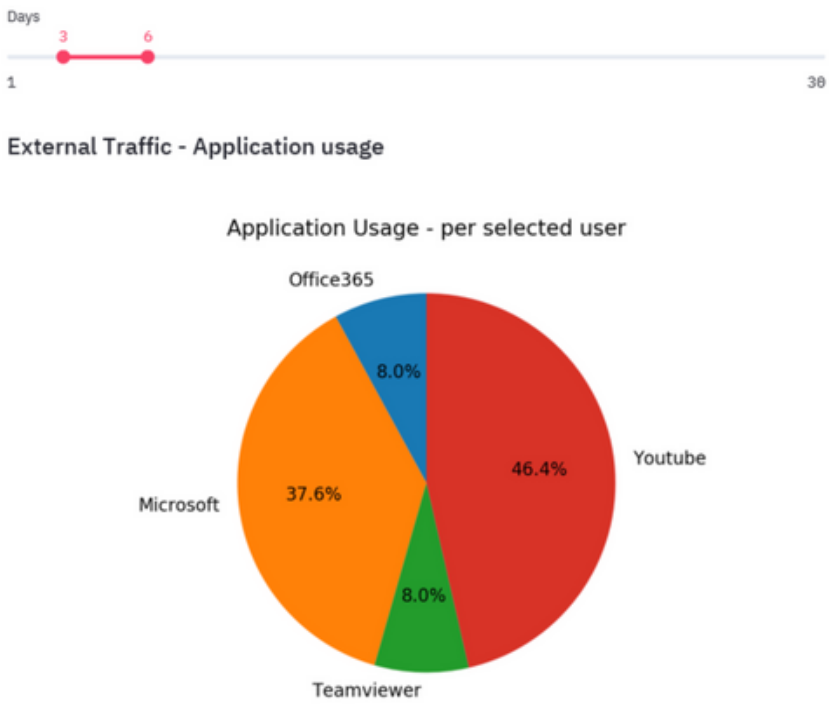
Wenn die umfangreichsten Anwendungen dazu bestimmt sind, sichere Cloud-Services zu

identifizieren, können sie mit einem Split-Tunnel verwendet werden, um die Last für einen VPN-Konzentrator zu reduzieren. Wenn es sich bei den wichtigsten Anwendungen jedoch um Services handelt, die weniger sicher sind oder ein Risiko darstellen können, ist es sicherer, diese über den VPN-Tunnel zu leiten. Der Grund hierfür ist, dass andere Netzwerksicherheitsgeräte den Datenverkehr verarbeiten können, bevor dieser weitergeleitet werden darf. Anschließend können Sie die Zugriffsrichtlinien der Firewalls nutzen, um den Zugriff auf externe Netzwerke zu beschränken.

Identitätsspezifische nicht konforme VPN-Benutzer

In einigen Fällen könnte die Zunahme mit nur wenigen Benutzern verbunden sein, die bestimmte Richtlinien nicht einhalten. Die oben verwendeten Module und Datensätze können erneut verwendet werden, um die wichtigsten VPN-Benutzer und die Webanwendungen zu identifizieren, auf die sie zugreifen. Dies kann dazu beitragen, solche Benutzer zu isolieren und ihre Auswirkungen auf die Gerätelast zu beobachten.





In Szenarien, in denen keine der Methoden geeignet ist, sollten Administratoren Sicherheitslösungen für Endgeräte wie die AMP-Lösung für Endgeräte und die Cisco Umbrella-Lösung berücksichtigen, um die Endpunkte in ungeschützten Netzwerken zu schützen.