Optimice el túnel dividido de AnyConnect para Microsoft Office 365 y el WebEx de Cisco

Contenido

[Introducción](#)
[Tunelización dividida](#)
[Túnel dividido dinámico](#)
[Configuración](#)
[Verificación](#)

Introducción

Este documento describe cómo configurar un dispositivo de seguridad adaptante (ASA) con las configuraciones para excluir el tráfico destinado Microsoft Office a 365 (incluye a los equipos de Microsoft) y al WebEx de Cisco de una conexión VPN. Incorpora las exclusiones de la dirección de red y (nombre de dominio completo (FQDN) basado) las exclusiones dinámicas para los clientes de AnyConnect que lo utilizan.

Tunelización dividida

El ASA necesita ser configurado “excluye” la lista especificada de destinos IPv4 y del IPv6 que se excluirán del túnel. Desafortunadamente la lista de direccionamientos es dinámica y podría potencialmente cambiar. Vea que la sección de configuración para un script del pitón y un link a un pitón en línea leído – eval – imprimen el loop (REPL) que se puede utilizar para extraer la lista y para generar una configuración de muestra.

Túnel dividido dinámico

Además de la fractura excluya la lista de dirección de red, el Túnel dividido dinámico fue agregado en AnyConnect 4.6 para Windows y el mac. El Túnel dividido dinámico utiliza el FQDN para determinar independientemente de si la conexión debe pasar el túnel. El script del pitón también determina los FQDN de las puntos finales para agregar a los atributos de encargo de AnyConnect.

Configuración

Ejecute este script en Python 3 REPL o ejecútelo en un entorno del público REPL tal como https://repl.it/@ministryofjay/AnyConnectO365DynamicExclude.

```
import urllib.request
import uuid
import json
import re
```

```
def print_acl_lines(acl_name, ips, section_comment):
    slash_to_mask = (
        "0.0.0.0",
        "128.0.0.0",
        "192.0.0.0",
        "224.0.0.0",
        "240.0.0.0",
        "248.0.0.0",
        "252.0.0.0",
        "254.0.0.0",
        "255.0.0.0",
        "255.128.0.0",
        "255.192.0.0",
        "255.224.0.0",
        "255.240.0.0",
        "255.248.0.0",
        "255.252.0.0",
        "255.254.0.0",
        "255.255.0.0",
        "255.255.128.0",
        "255.255.192.0",
        "255.255.224.0",
        "255.255.240.0",
        "255.255.248.0",
        "255.255.252.0",
        "255.255.254.0",
        "255.255.255.0",
        "255.255.255.128",
        "255.255.255.192",
        "255.255.255.224",
        "255.255.255.240",
        "255.255.255.248",
        "255.255.255.252",
        "255.255.255.254",
        "255.255.255.255",
    )
    print(
        "access-list {acl_name} remark {comment}".format(
            acl_name=acl_name, comment=section_comment
        )
    )
    for ip in sorted(ips):
        if ":" in ip:
            # IPv6 address
            print(
                "access-list {acl_name} extended permit ip {ip} any6".format(
                    acl_name=acl_name, ip=ip
                )
            )
        else:
            # IPv4 address.  Convert to a mask
            addr, slash = ip.split("/")
            slash_mask = slash_to_mask[int(slash)]
            print(
                "access-list {acl_name} extended permit ip {addr} {mask} any4".format(
                    acl_name=acl_name, addr=addr, mask=slash_mask
                )
            )


# Fetch the current endpoints for O365
http_res = urllib.request.urlopen(
    url="https://endpoints.office.com/endpoints/worldwide?clientrequestid={}".format(
```

```
        uuid.uuid4()
    )
)
res = json.loads(http_res.read())
o365_ips = set()
o365_fqdns = set()
for service in res:
    if service["category"] == "Optimize":
        for ip in service.get("ips", []):
            o365_ips.add(ip)
        for fqdn in service.get("urls", []):
            o365_fqdns.add(fqdn)

# Generate an acl for split excluding For instance
print("##### Step 1: Create an access-list to include the split-exclude networks\n")
acl_name = "ExcludeSass"
# O365 networks
print_acl_lines(
    acl_name=acl_name,
    ips=o365_ips,
    section_comment="v4 and v6 networks for Microsoft Office 365",
)
# Microsoft Teams
# https://docs.microsoft.com/en-us/office365/enterprise/office-365-vpn-implement-split-
tunnel#configuring-and-securing-teams-media-traffic
print_acl_lines(
  acl_name=acl_name,
  ips=["13.107.60.1/32"],
  section_comment="v4 address for Microsoft Teams"
)
# Cisco Webex - Per https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-
Teams-Services
webex_ips = [
    "64.68.96.0/19",
    "66.114.160.0/20",
    "66.163.32.0/19",
    "170.133.128.0/18",
    "173.39.224.0/19",
    "173.243.0.0/20",
    "207.182.160.0/19",
    "209.197.192.0/19",
    "216.151.128.0/19",
    "114.29.192.0/19",
    "210.4.192.0/20",
    "69.26.176.0/20",
    "62.109.192.0/18",
    "69.26.160.0/19",
]
print_acl_lines(
    acl_name=acl_name,
    ips=webex_ips,
    section_comment="IPv4 and IPv6 destinations for Cisco Webex",
)

# Edited. April 1st 2020
# Per advice from Microsoft they do NOT advise using dynamic split tunneling for their
properties related to Office 365
#
print(
    "\n\n##### Step 2: Create an Anyconnect custom attribute for dynamic split excludes\n"
)
print("SKIP.  Per Microsoft as of April 2020 they advise not to dynamically split fqdn related
to Office365")
#print(
```

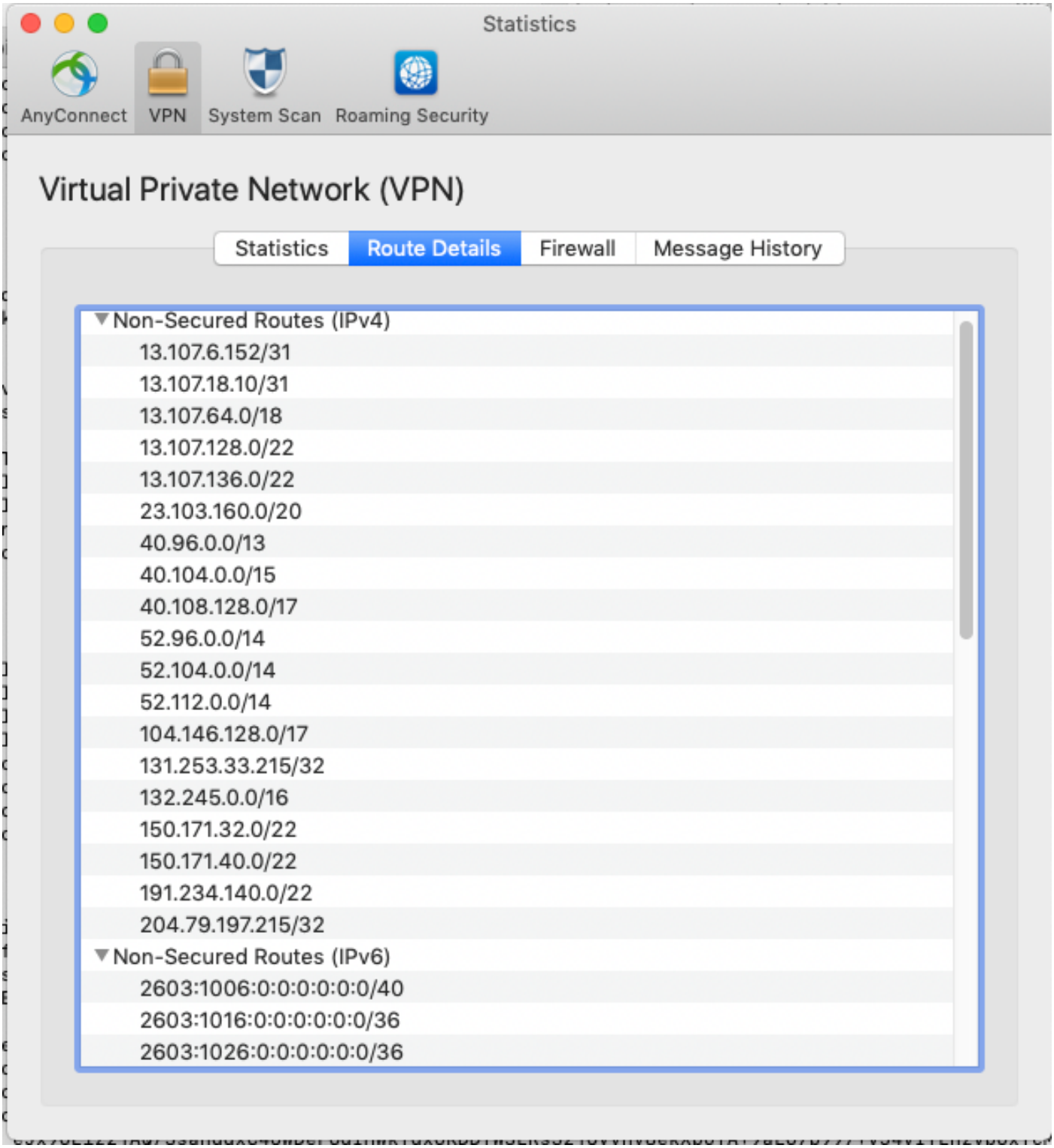
```
#    """
#webvpn
#  anyconnect-custom-attr dynamic-split-exclude-domains description dynamic-split-exclude-
domains
#
#anyconnect-custom-data dynamic-split-exclude-domains saas {}
#""".format(
#        ",".join([re.sub(r"^\*\.", "", f) for f in o365_fqdns])
#    )
#)
#
print("\n##### Step 3: Configure the split exclude in the group-policy\n")
print(
    """
group-policy GP1 attributes
 split-tunnel-policy excludespecified
 ipv6-split-tunnel-policy excludespecified
 split-tunnel-network-list value {acl_name}
""".format(
        acl_name=acl_name
    )
)
```

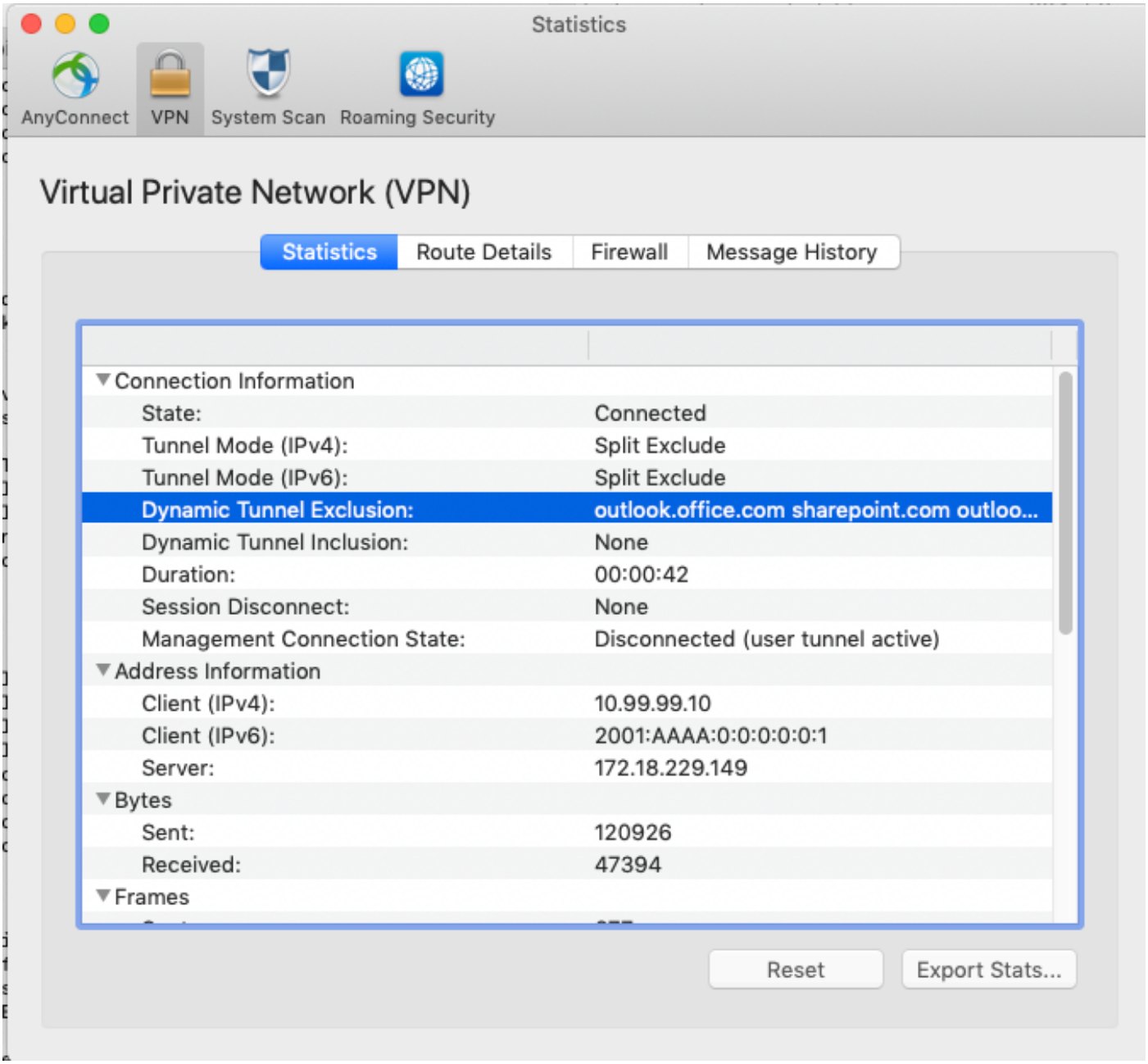
> Nota: Microsoft recomienda excluir el tráfico destinado para cerrar los servicios de la oficina 365 del alcance de la conexión VPN configurando el Túnel dividido usando los rangos de direccionamiento publicado IPv4 y del IPv6. Para el mejor funcionamiento y el uso más eficiente de la capacidad VPN, el tráfico a éstos los rangos de dirección IP dedicados asociados al Online del intercambio de la oficina 365, al Online de SharePoint, y a los equipos de Microsoft (referidos como optimizan categoría en la documentación de Microsoft) se debe encaminar directamente, fuera del túnel VPN. Refiérase optimizan la Conectividad de la oficina 365 para los usuarios remotos que usan la tunelización dividida VPN para información más detallada sobre esta recomendación.

> Nota: A principios de abril 2020, los equipos de Microsoft tiene una dependencia que el intervalo de direcciones IP 13.107.60.1/32 se debe excluir del túnel. Vea configurar y la sujeción del tráfico de los media de los equipos para más información.

Verificación

Una vez que un usuario está conectado deben ver las “rutas No-aseguradas” pobladas con los direccionamientos proporcionados en el ACL así como “la lista de la exclusión del túnel dinámico”.


Statistics
AnyConnect
VPN
System Scan
Roaming Security
Virtual Private Network (VPN)
Statistics
Route Details
Firewall
Message History
Non-Secured Routes (IPv4)
13.107.6.152/31
13.107.18.10/31
13.107.64.0/18
13.107.128.0/22
13.107.136.0/22
23.103.160.0/20
40.96.0.0/13
40.104.0.0/15
40.108.128.0/17
52.96.0.0/14
52.104.0.0/14
52.112.0.0/14
104.146.128.0/17
131.253.33.215/32
132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
Non-Secured Routes (IPv6)
2603:1006:0:0:0:0:0:0/40
2603:1016:0:0:0:0:0:0/36
2603:1026:0:0:0:0:0:0/36


Statistics
AnyConnect
VPN
System Scan
Roaming Security
Virtual Private Network (VPN)
Statistics
Route Details
Firewall
Message History
Connection Information
State: Connected
Tunnel Mode (IPv4): Split Exclude
Tunnel Mode (IPv6): Split Exclude
Dynamic Tunnel Exclusion: outlook.office.com sharepoint.com outloo...
Dynamic Tunnel Inclusion: None
Duration: 00:00:42
Session Disconnect: None
Management Connection State: Disconnected (user tunnel active)
Address Information
Client (IPv4): 10.99.99.10
Client (IPv6): 2001:AAAA:0:0:0:0:0:1
Server: 172.18.229.149
Bytes
Sent: 120926
Received: 47394
Frames
Reset
Export Stats...