Optimize Anyconnect Split Tunnel for Office365

Contents

How to optimize Anyconnect for Office365 connections:

This document will walk through how to configure an ASA with settings to exclude traffic destined to O365 from a VPN connection. It incorporates both network address exclusions and dynamic (FQDN based) exclusions for Anyconnect clients that support it.

Split Tunneling

The ASA will need to be configured to "exclude" the specified list of IPv4 and IPv6 destinations to be excluded. Unfortunately the list of addresses is dynamic and could potentially change. Below is included a python script and a link to an online python read–eval–print loop (REPL) that can be used to retrieve the list and generate a sample configuration.

Dynamic Split Tunneling

In addition to the split exclude network address list dynamic split tunneling was added in AnyConnect 4.6 for Windows and Mac. Dynamic Split tunneling uses the FQDN to determine whether or not the connection should go over the tunnel. The script below also determines the fqdns of the endpoints to add to the custom AnyConnect Attributes.

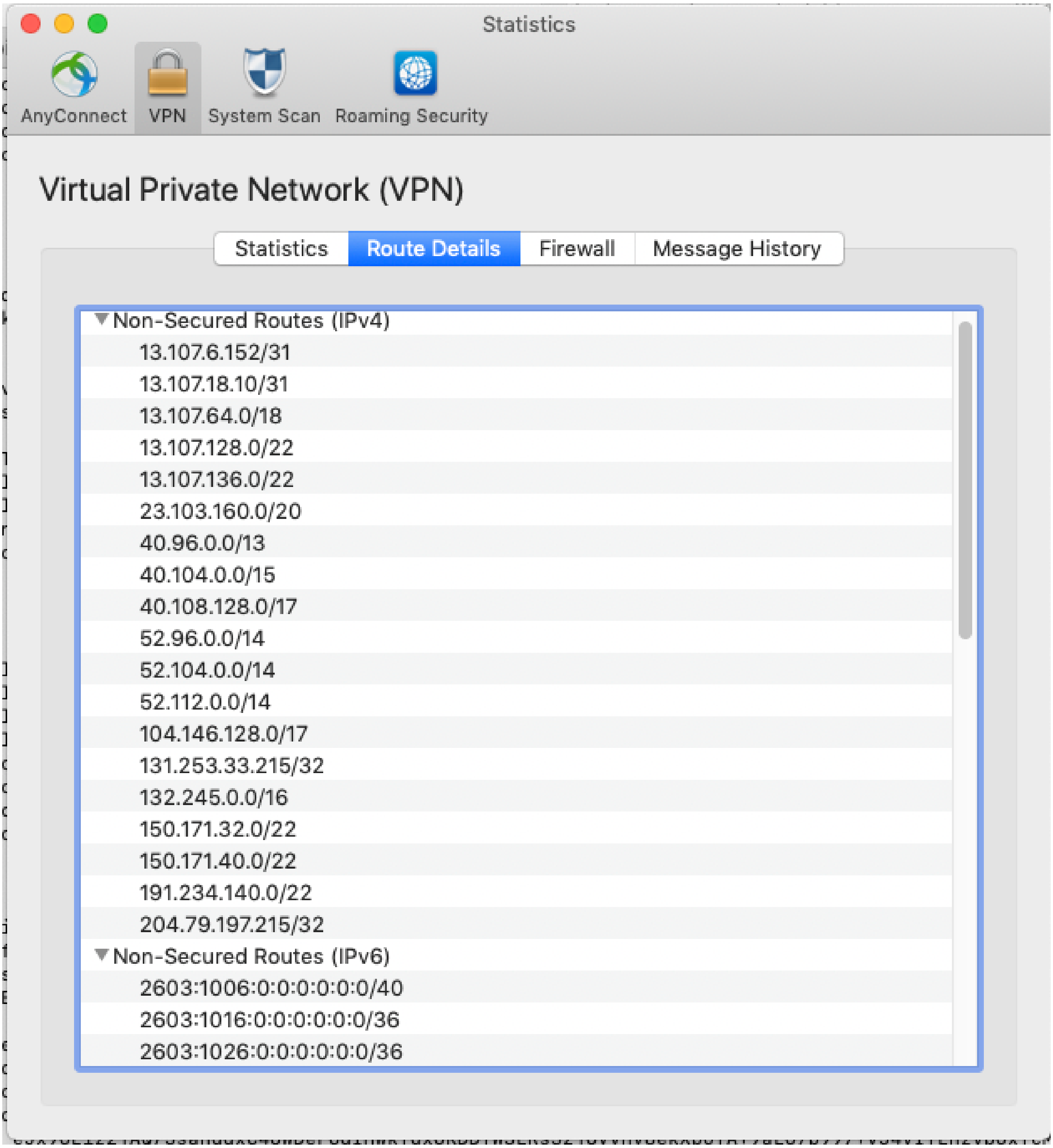
Configuration

Either run the following script in a python3 REPL or run it in a public Repl environment like (For instance https://repl.it/@ministryofjay/AnyConnectO365DynamicExclude)

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

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",
)


# 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())
ips = set()
fqdns = set()
for service in res:
    if service["category"] == "Optimize":
        for ip in service.get("ips", []):
            ips.add(ip)
        for fqdn in service.get("urls", []):
            fqdns.add(fqdn)

# Generate an acl for split excluding For instance
# access-list ExcludeO365 extended permit ip x.x.0.0 255.255.0.0 any4
# access-list ExcludeO365 extended permit ip 2603:10a6:600::/40 any6

print("##### Step 1: Create an access-list to include the split-exclude networks\n")
for ip in sorted(ips):
    if ":" in ip:
        # IPv6 address
        print("access-list ExcludeO365 extended permit ip {} any6".format(ip))
    else:
        # IPv4 address.  Convert to a mask
        addr, slash = ip.split("/")
        slash_mask = slash_to_mask[int(slash)]
        print(
            "access-list ExcludeO365 extended permit ip {addr} {mask} any4".format(
                addr=addr, mask=slash_mask
            )
        )

print(
    "\n\n##### Step 2: Create an Anyconnect custom attribute for dynamic split excludes\n"
)
print(
    """
webvpn
  anyconnect-custom-attr dynamic-split-exclude-domains description dynamic-split-exclude-
domains"

anyconnect-custom-data dynamic-split-exclude-domains o365 {}
""".format(
        ",".join([re.sub(r"^\*\.", "", f) for f in 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 Exclude0365
 anyconnect-custom dynamic-split-exclude-domains value o365
"""
)
```

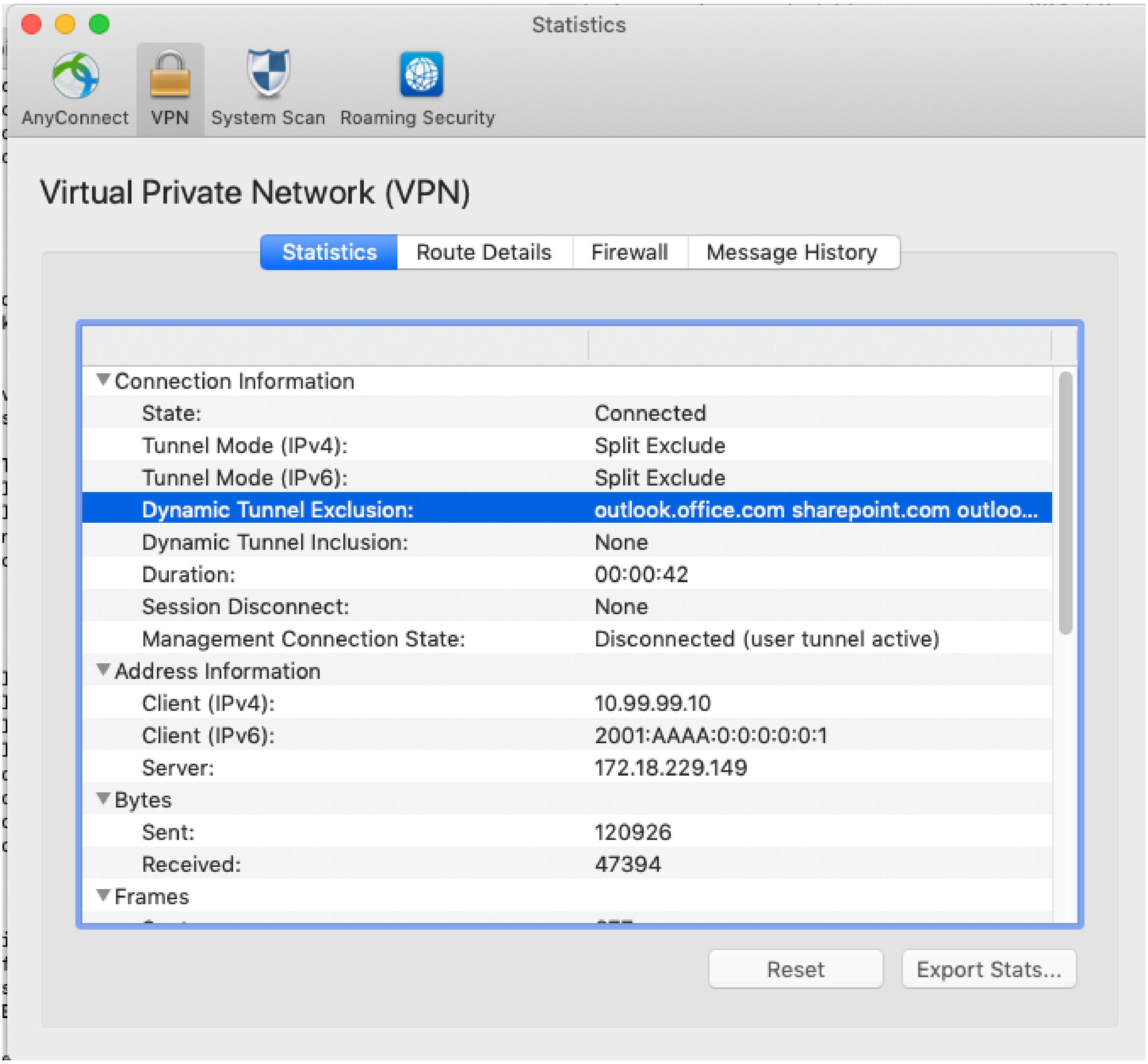
Verfication

Once a user is connected they should see the "Non-Secured Routes" populated with the addresses provided in the ACL as well as the "Dynamic Tunnel Exclusion" list.



Virtual Private Network (VPN)

```
▼ 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
```



Virtual Private Network (VPN)

▼ 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	