Microsoft Office 365/Webex용 AnyConnect 스플릿 터널 최적화

목차

[소개](#)

[배경 정보](#)

[스플릿 터널링](#)

[동적 스플릿 터널링](#)

[설정](#)

[확인](#)

소개

이 문서에서는 VPN 연결에서 Microsoft Office 365(Microsoft Teams) 및 Cisco Webex로 향하는 트래픽을 제외하기 위한 설정으로 ASA를 구성하는 방법에 대해 설명합니다.

배경 정보

ASA(Adaptive Security Appliance)를 구성하면 이를 지원하는 AnyConnect 클라이언트에 대한 네트워크 주소 제외 및 동적 FQDN(정규화된 도메인 이름) 기반 제외도 통합됩니다.

스플릿 터널링

터널에서 제외할 IPv4 및 IPv6 대상의 지정된 목록을 제외하도록 ASA를 구성해야 합니다. 안타깝게도 주소 목록은 동적이며 잠재적으로 변경될 수 있습니다. Python 스크립트에 대한 구성 섹션 및 목록을 검색하고 샘플 구성을 생성하는 데 사용할 수 있는 온라인 REPL(python read-eval-print loop)에 대한 링크를 참조하십시오.

동적 스플릿 터널링

Windows 및 Mac용 AnyConnect 4.6에는 스플릿 제외 네트워크 주소 목록 외에 동적 스플릿 터널링이 추가되었습니다. 동적 스플릿 터널링은 FQDN을 사용하여 연결이 터널을 통과할 수 있는지 여부를 결정합니다. 또한 python 스크립트는 맞춤형 AnyConnect 특성에 추가할 엔드포인트의 FQDN을 결정합니다.

설정

이 스크립트를 Python 3 REPL에서 실행하거나 AnyConnectO365DynamicExclude와 같은 공용 REPL 환경에서 [실행합니다](#)

```
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",
        "192.0.2.1",
        "192.0.2.1",
        "10.224.0.0",
        "10.240.0.0",
        "10.248.0.0",
        "10.252.0.0",
        "10.254.0.0",
        "10.255.0.0",
        "10.255.128.0",
        "10.255.192.0",
        "10.255.224.0",
        "10.255.240.0",
        "10.255.248.0",
        "10.255.252.0",
        "10.255.254.0",
        "10.255.255.0",
        "10.255.255.128",
        "10.255.255.192",
        "10.255.255.224",
        "10.255.255.240",
        "10.255.255.248",
        "10.255.255.252",
        "10.255.255.254",
        "10.255.255.255",
        "10.255.255.255",
        "10.255.255.255",
        "10.255.255.255",
        "10.255.255.240",
        "10.255.255.248",
        "10.255.255.252",
        "10.255.255.254",
        "10.255.255.255",
    )
    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#configuri
print_acl_lines(
  acl_name=acl_name,
  ips=["10.107.60.1/32"],
  section_comment="v4 address for Microsoft Teams"
)
# Cisco Webex - Per https://help.webex.com/en-us/WBX000028782/Network-Requirements-for-Webex-Teams-Serv
webex_ips = [
    "10.68.96.1/19",
    "10.114.160.1/20",
    "10.163.32.1/19",
    "192.0.2.1/18",
    "192.0.2.2/19",
    "198.51.100.1/20",
    "203.0.113.1/19",
    "203.0.113.254/19",
    "203.0.113.2/19",
    "172.29.192.1/19",
    "203.0.113.1/20",
    "10.26.176.1/20",
    "10.109.192.1/18",
    "10.26.160.1/19",
]
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 relat
#
```

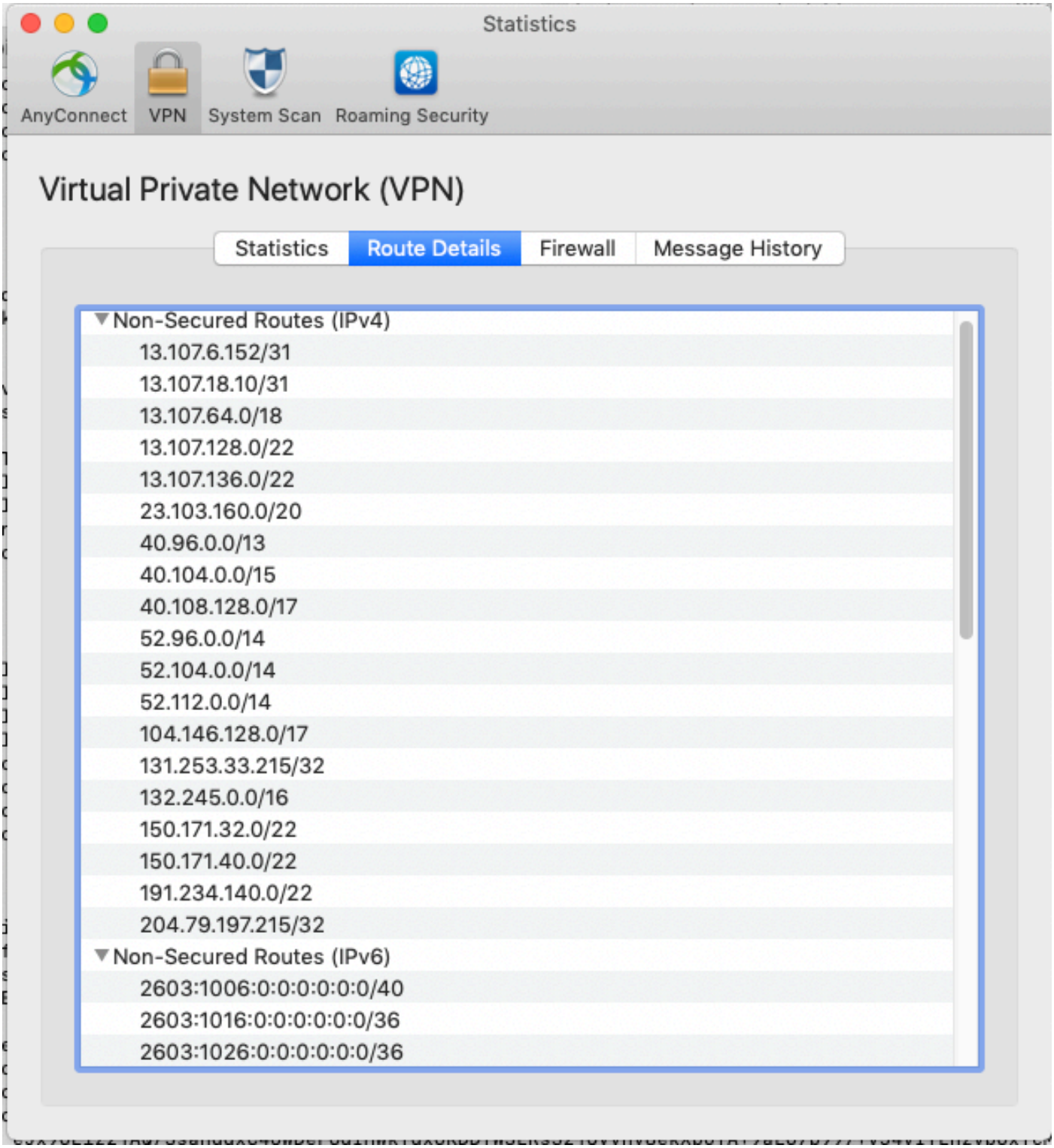
```
print(
    "\n\n##### Step 2: Create an Anyconnect custom attribute for dynamic split excludes\n"
)
print("SKIP.  Per Microsoft as of April 2020 they advise not to dynamically split fqdn related to Offic
#print(
#    """
#webvpn
#  anyconnect-custom-attr dynamic-split-exclude-domains description 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
    )
)
```

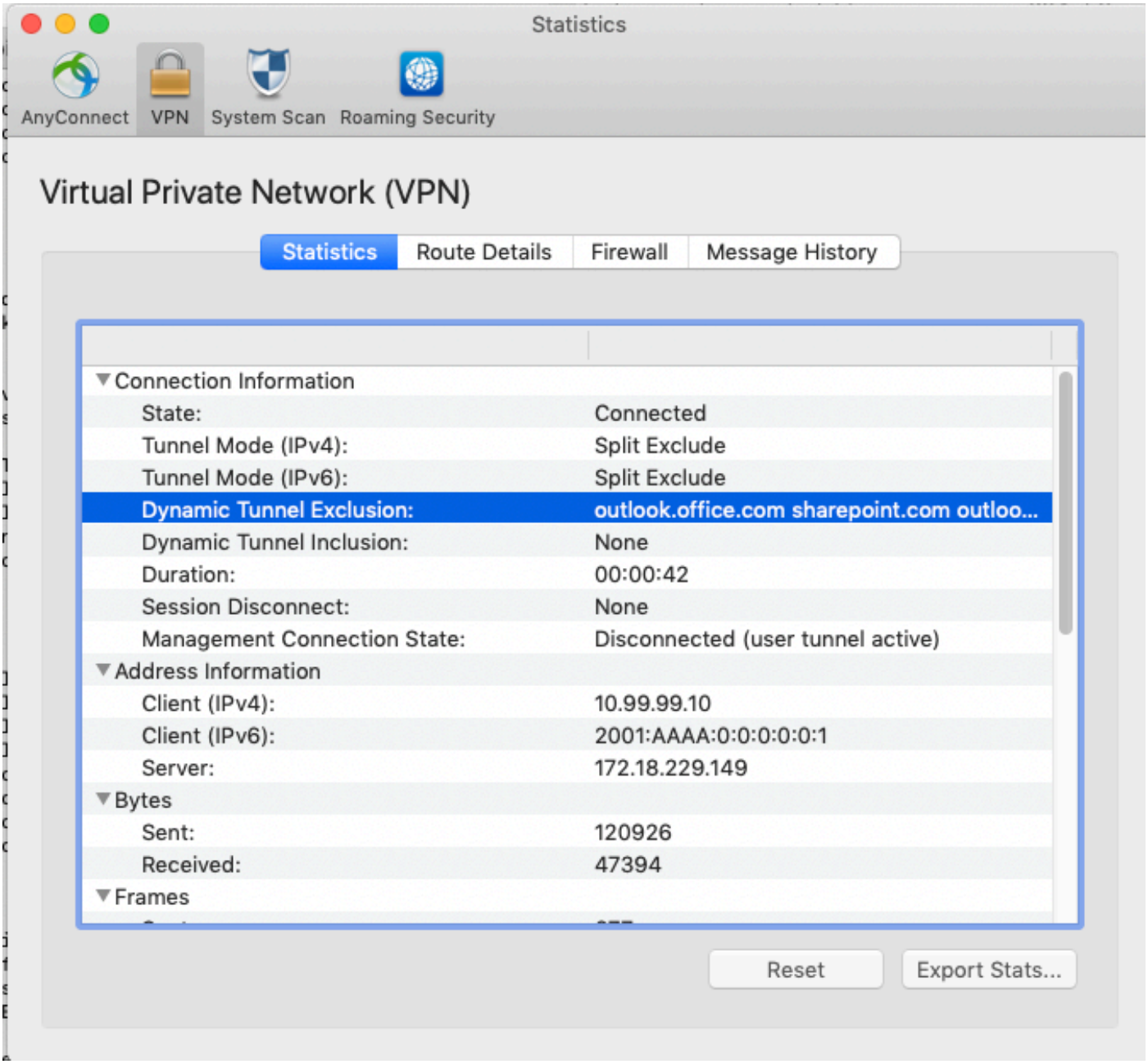
참고: Microsoft는 게시된 IPv4 및 IPv6 주소 범위를 사용하여 스플릿 터널링을 구성하여 주요 Office 365 서비스로 향하는 트래픽을 VPN 연결 범위에서 제외할 것을 권장합니다. 최상의 성능과 VPN 용량의 효율적인 사용을 위해 Office 365 Exchange Online, SharePoint Online 및 Microsoft Teams와 연결된 이러한 전용 IP 주소 범위에 대한 트래픽(Microsoft 설명서의 최적화 범주라고 함)은 VPN 터널 외부에서 직접 라우팅될 수 있습니다. 이 권장 사항에 대한 자세한 내용은 VPN 스플릿 터널링을 사용하는 원격 사용자를 위한 Office 365 연결 최적화를 참조하십시오.

참고: 2020년 4월 초부터 Microsoft Teams는 IP 범위 10.107.60.1/32을 터널에서 제외해야 한다는 종속 관계가 있습니다. 자세한 내용은 팀 미디어 트래픽 구성 및 보안을 참조하십시오.

확인

사용자가 연결되면 비보안 경로가 ACL에 제공된 주소 및 동적 터널 제외 목록으로 채워집니다.


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...

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.