Microsoft Office 365/Webex用のAnyConnectスプリットトンネルの最適化

内容

はじめに

このドキュメントでは、Microsoft Office 365(Microsoft Teams)およびCisco Webex宛てのトラフィックをを除外する設定でASAを設定する方法について説明します。

背景説明

適応型セキュリティアプライアンス(ASA)を設定すると、ネットワークアドレスの除外と、ASAをサポートするAnyConnectクライアントのダイナミック完全修飾ドメイン名(FQDN)ベースの除外も組み込まれます。

スプリット トンネリング

ASAは、指定されたIPv4およびIPv6の宛先リストをトンネルから除外するように設定する必要があります。残念ながら、アドレスのリストは動的であり、変更される可能性があります。Pythonスクリプトの設定セクションと、リストを取得してサンプル設定を生成するために使用できるオンラインのpython read-eval-print loop (REPL)へのリンクを参照してください。

ダイナミックスプリットトンネリング

スプリット除外ネットワークアドレスのリストに加えて、AnyConnect 4.6 for Windows and Macでダイナミックスプリットトンネリングが追加されました。ダイナミックスプリットトンネリングでは、接続がトンネルを通過できるかどうかを判断するためにFQDNが使用されます。Pythonスクリプトは、カスタムAnyConnect属性に追加するエンドポイントのFQDNも決定します。

コンフィギュレーション

このスクリプトは、Python 3 REPLまたはAnyConnectO365DynamicExcludeなどのパブリック

REPL環境で実行してください

```
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",
)
```

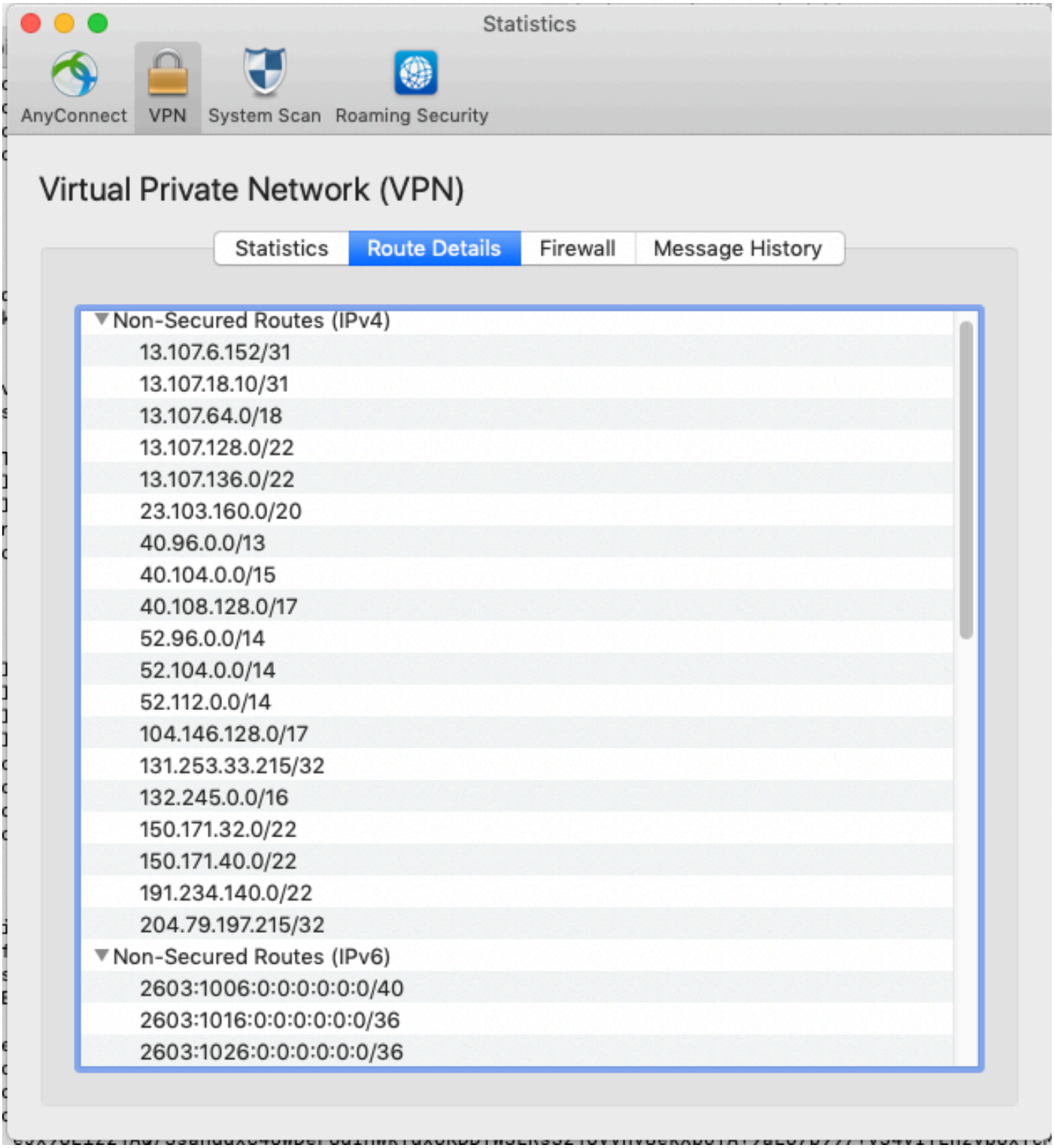
```
# Edited. April 1st 2020
# Per advice from Microsoft they do NOT advise using dynamic split tunneling for their properties relat
#
print(
    "\n\n##### Step 2: Create an Anyconnect custom attribute for dynamic split excludes\n"
)
print("SKIP.  Per Microsoft as of April 2020 they advise not to dynamically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

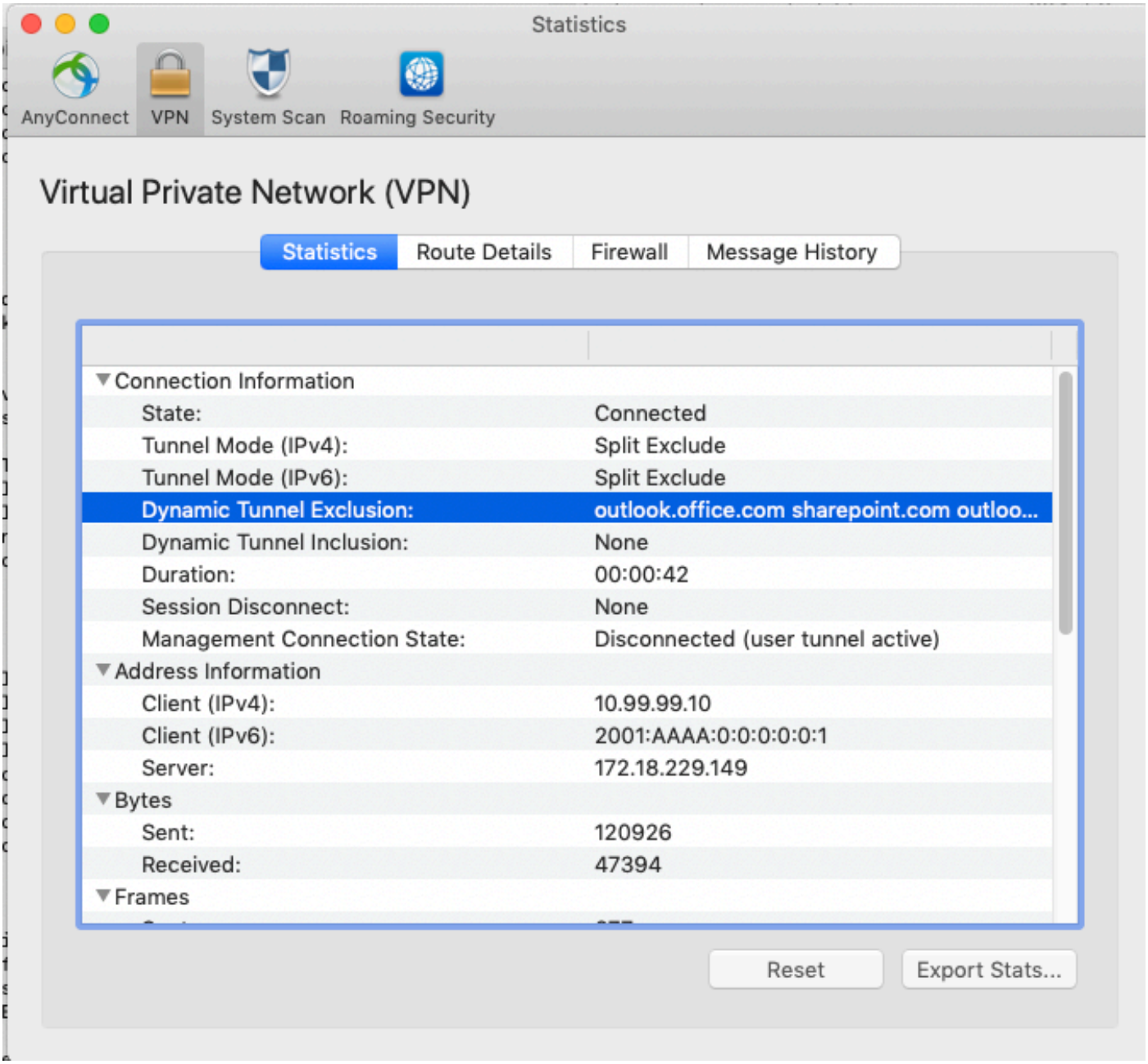
注:Microsoftでは、公開されているIPv4およびIPv6アドレス範囲を使用してスプリットトンネリングを設定することにより、主要なOffice 365サービス宛てのトラフィックをVPN接続の範囲から除外することを推奨しています。VPN容量を最大限に活用し、最高のパフォーマンスを実現するために、Office 365 Exchange Online、SharePoint Online、およびMicrosoft Teamsに関連付けられたこれらの専用IPアドレス範囲（Microsoftドキュメントでは Optimizeカテゴリと呼びます）へのトラフィックを、VPNトンネルの外部に直接ルーティングできます。この推奨事項の詳細については、「VPNスプリットトンネリングを使用したリモートユーザー向けのOffice 365接続の最適化」を参照してください。

注:2020年4月上旬の時点で、Microsoft Teamsには、IP範囲10.107.60.1/32をトンネルから除外する必要があるという依存関係があります。詳細については、「チームのメディアトラフィックの設定と保護」を参照してください。

検証

ユーザが接続されると、ACLで指定されたアドレスが入力された非セキュアルートと、ダイナミックトンネル除外リストが表示されます。


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...

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。