# Optimierung des AnyConnect Split-Tunnels für Microsoft Office 365/WebEx

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie Sie eine ASA mit Einstellungen konfigurieren, um Datenverkehr, der an Microsoft Office 365 (Microsoft Teams) und Cisco WebEx gerichtet ist, von der VPN-Verbindung auszuschließen.

## Hintergrundinformationen

Bei der Konfiguration der Adaptive Security Appliance (ASA) sind für AnyConnect-Clients, die die Appliance unterstützen, auch Ausschlüsse von Netzwerkadressen und dynamische Ausschlüsse auf Basis von vollqualifizierten Domänennamen (FQDN) möglich.

## Split-Tunneling

Die ASA muss so konfiguriert werden, dass die angegebene Liste der IPv4- und IPv6-Ziele, die aus dem Tunnel ausgeschlossen werden sollen, ausgeschlossen wird. Leider ist die Adressliste dynamisch und kann sich ändern. Im Abschnitt "Konfiguration" finden Sie ein Python-Skript und einen Link zu einer Online-Python-Read-Eval-Print-Schleife (REPL), mit der die Liste abgerufen und eine Beispielkonfiguration generiert werden kann.

## Dynamisches Split Tunneling

Zusätzlich zur Split-Exclude-Netzwerkadressliste wurde dynamisches Split-Tunneling in AnyConnect 4.6 für Windows und Mac hinzugefügt. Beim dynamischen Split-Tunneling wird der FQDN verwendet, um zu bestimmen, ob die Verbindung über den Tunnel verlaufen kann. Das Python-Skript bestimmt außerdem die FQDNs der Endpunkte, die den benutzerdefinierten AnyConnect-Attributen hinzugefügt werden sollen.

## Konfiguration

Führen Sie dieses Skript entweder in einer Python 3 REPL oder in einer öffentlichen REPL-Umgebung wie AnyConnectO365[DynamicExclude aus.](#)

```
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#configurin
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-Servi
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 relate
#
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 Office
#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
    )
)
```

---

> **Hinweis**: Microsoft empfiehlt, Datenverkehr, der für wichtige Office 365-Dienste bestimmt ist, aus dem Bereich der VPN-Verbindung auszuschließen, indem Split-Tunneling mit den veröffentlichten IPv4- und IPv6-Adressbereichen konfiguriert wird. Um eine optimale Leistung und eine effiziente Nutzung der VPN-Kapazität zu erzielen, kann der Datenverkehr zu diesen dedizierten IP-Adressbereichen von Office 365 Exchange Online, SharePoint Online und Microsoft Teams (in der Microsoft-Dokumentation als "Kategorie optimieren" bezeichnet) direkt außerhalb des VPN-Tunnels weitergeleitet werden. Detailliertere Informationen zu dieser Empfehlung finden Sie unter Optimize Office 365 connectivity for remote users using VPN split tunneling.

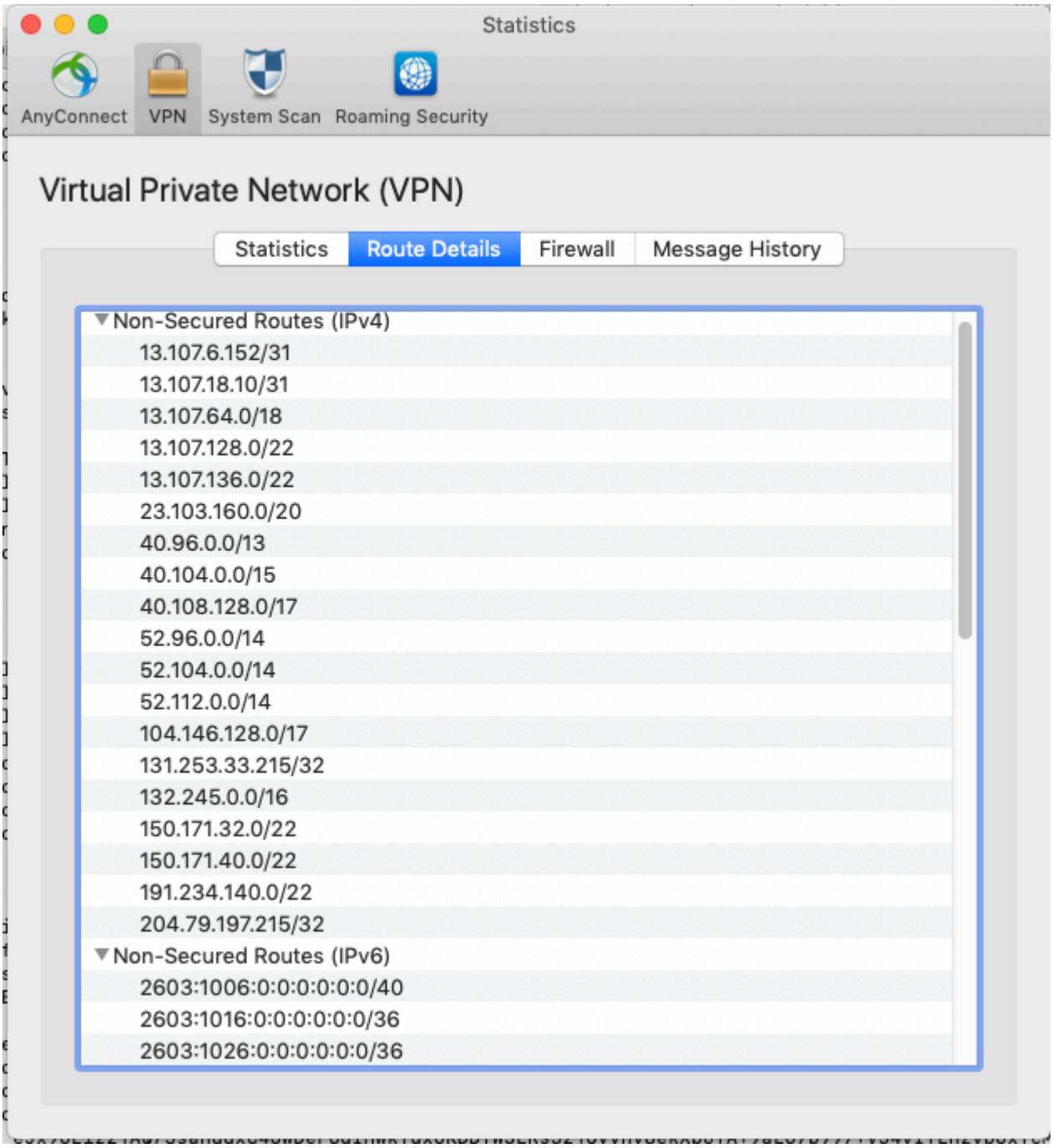
---

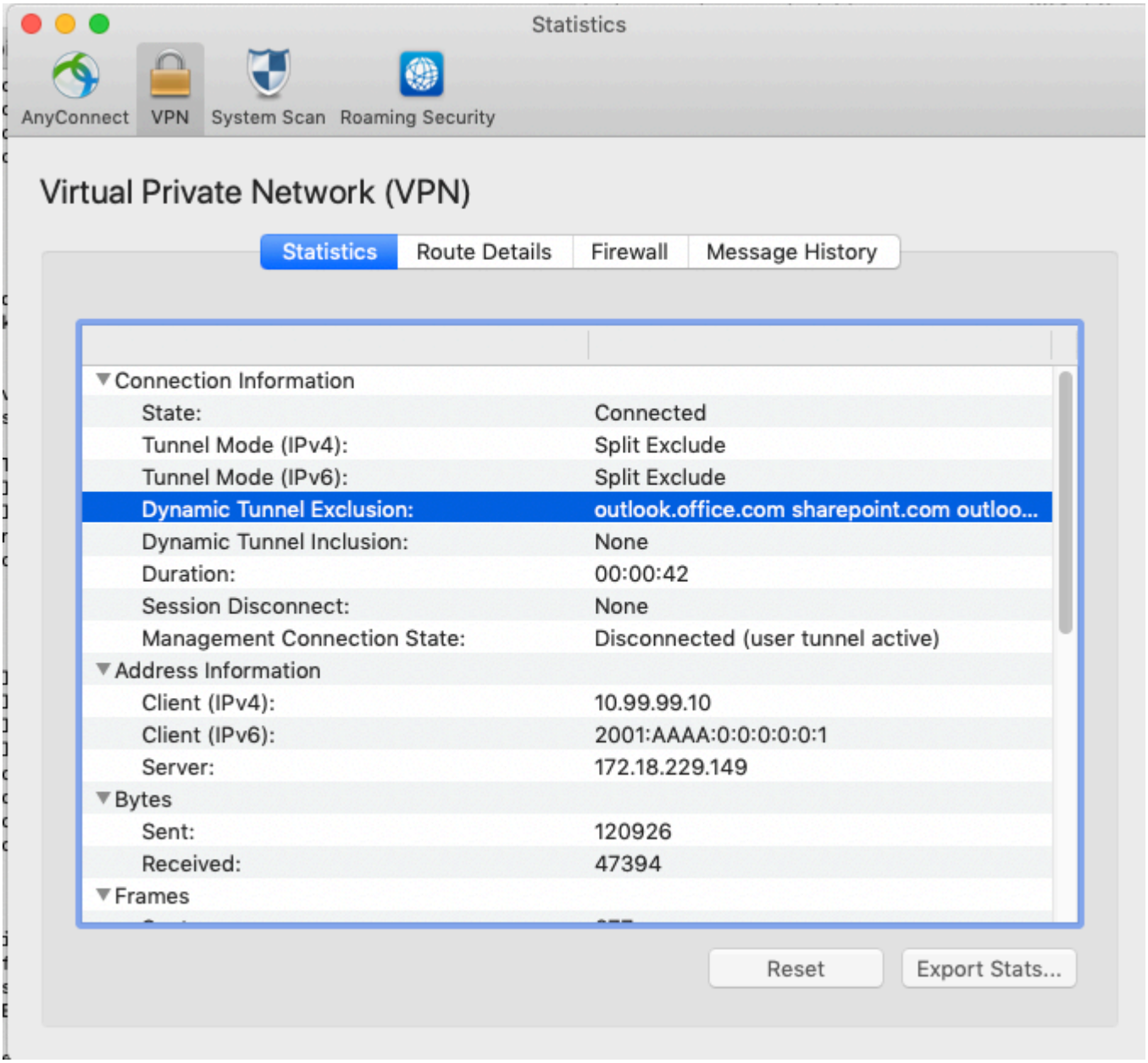
> **Hinweis**: Microsoft Teams ist seit Anfang April 2020 davon abhängig, dass der IP-Bereich 10.107.60.1/32 aus dem Tunnel ausgeschlossen werden muss. Weitere Informationen finden Sie unter Konfigurieren und Sichern des Medienverkehrs von Teams.

---

# Verifizierung

Sobald ein Benutzer verbunden ist, werden die nicht sicheren Routen mit den in der ACL bereitgestellten Adressen sowie der Ausschlussliste für dynamische Tunnel ausgefüllt.


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...

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.