Ottimizza AnyConnect Split Tunnel per Microsoft Office 365/Webex

Sommario

Introduzione

In questo documento viene descritto come configurare un'ASA con impostazioni che escludano il traffico destinato a Microsoft Office 365 (Microsoft Teams) e Cisco Webex dalla connessione VPN.

Premesse

La configurazione di ASA (Adaptive Security Appliance) include anche le esclusioni degli indirizzi di rete e delle esclusioni dinamiche basate sul nome di dominio completo (FQDN) per i client AnyConnect che la supportano.

Tunneling ripartito

È necessario configurare l'ASA in modo da escludere l'elenco specificato di destinazioni IPv4 e IPv6 da escludere dal tunnel. L'elenco degli indirizzi è dinamico e potrebbe potenzialmente cambiare. Vedere la sezione Configurazione per uno script python e un collegamento a un ciclo di lettura-valutazione-stampa (REPL) python in linea che può essere utilizzato per recuperare l'elenco e generare una configurazione di esempio.

Tunneling ripartito dinamico

Oltre all'elenco degli indirizzi di rete esclusi dalla divisione, il tunneling con divisione dinamica è stato aggiunto in AnyConnect 4.6 per Windows e Mac. Il tunneling con split dinamico utilizza l'FQDN per determinare se la connessione può passare attraverso il tunnel. Lo script python determina anche i nomi FQDN degli endpoint da aggiungere agli attributi AnyConnect personalizzati.

Configurazione

Eseguire questo script in un REPL Python 3 o in un ambiente REPL pubblico, ad esempio [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",
        "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"
)
```

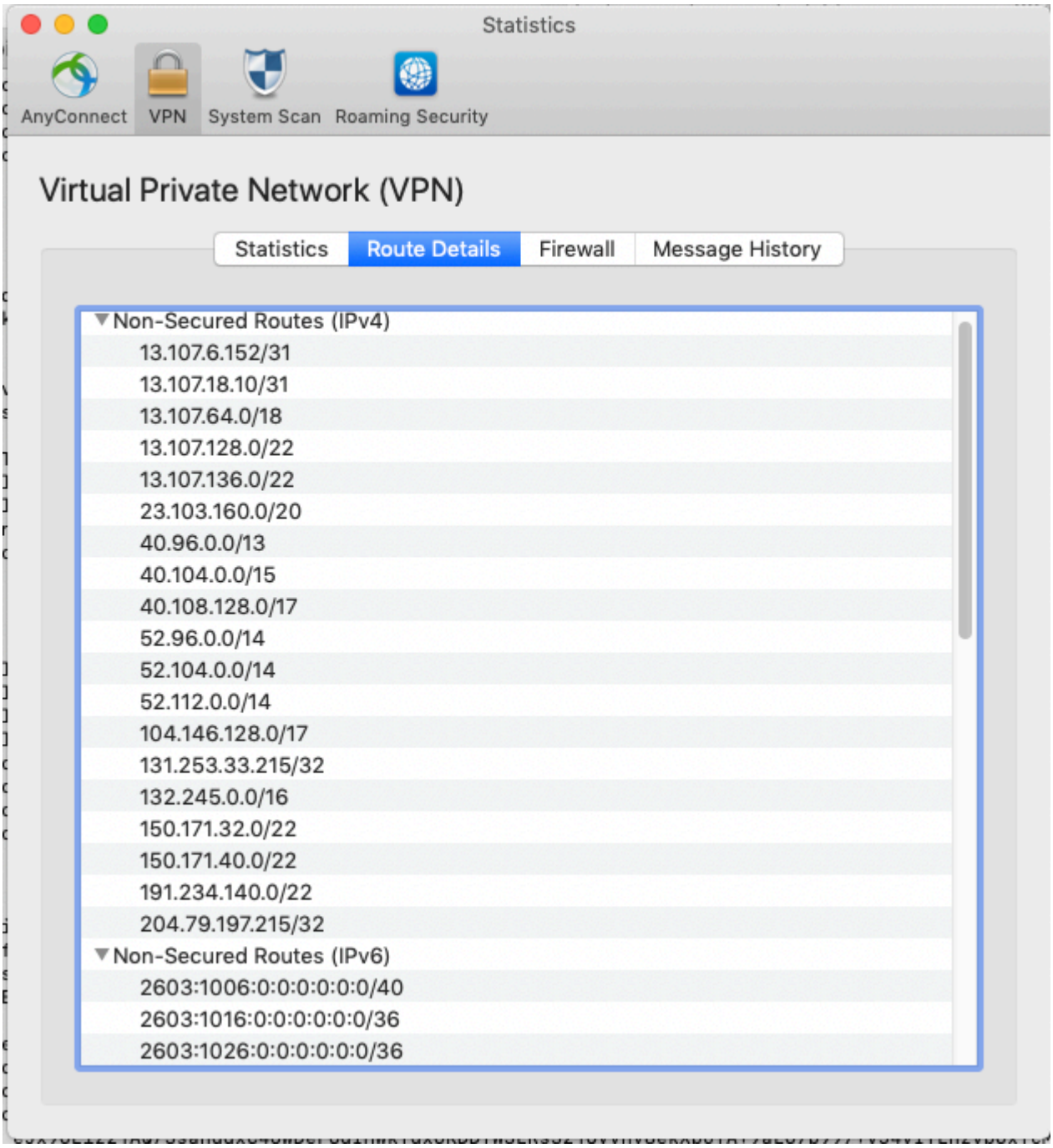
```
print("SKIP.  Per Microsoft as of April 2020 they advise not to dynamically split fqdn related to Office
#print(
#    """
#webvpn
#  anyconnect-custom-attr dynamic-split-exclude-domains description dynamic-split-exclude-domains
#
#anyconnect-custom-data dynamic-split-exclude-domains saas {}
#""".format(
#        ",".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
    )
)
```

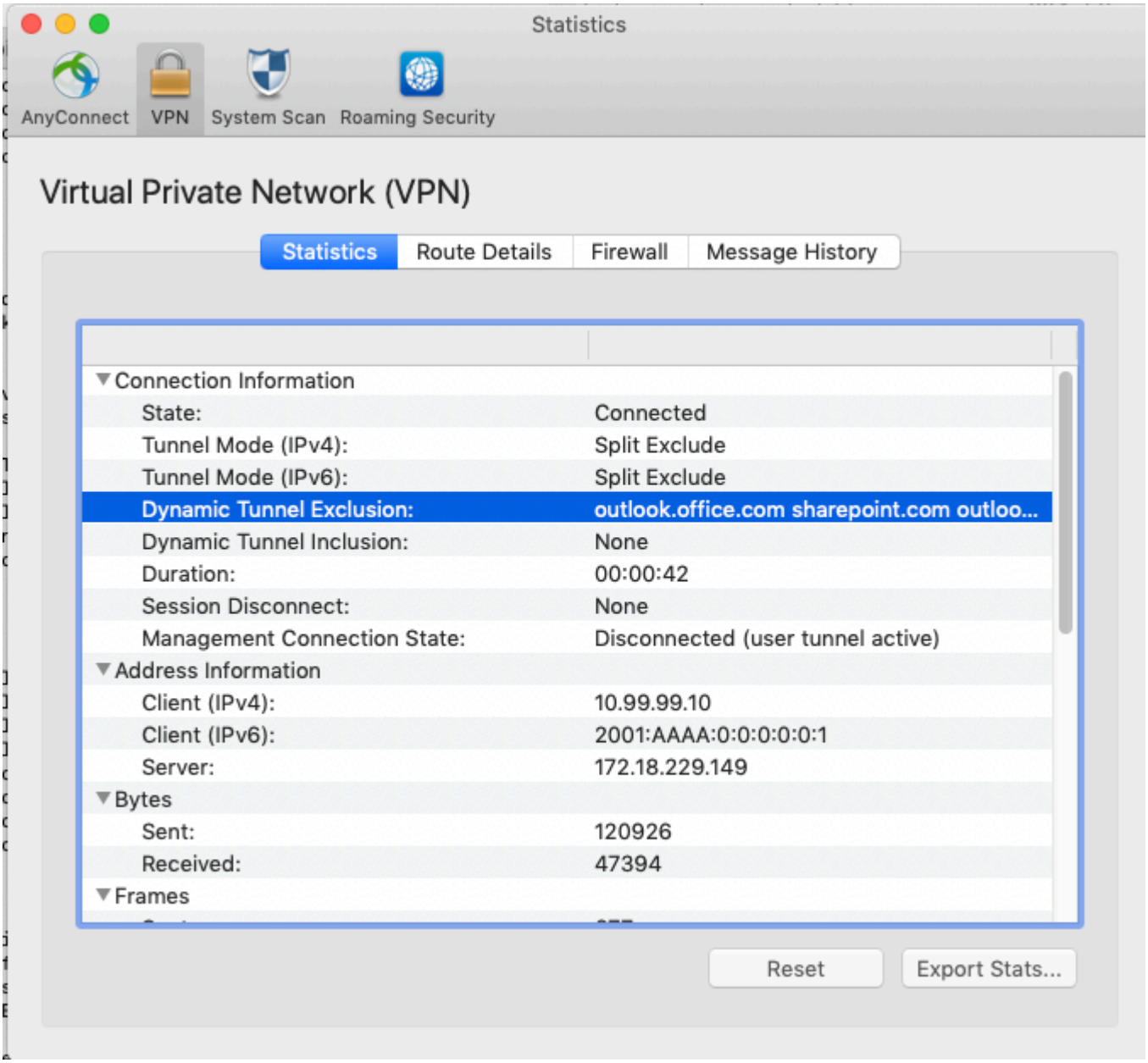
> **Nota**: Microsoft consiglia di escludere il traffico destinato ai servizi chiave di Office 365 dall'ambito della connessione VPN configurando il tunneling suddiviso utilizzando gli intervalli di indirizzi IPv4 e IPv6 pubblicati. Per ottenere prestazioni ottimali e un utilizzo più efficiente della capacità VPN, il traffico verso questi intervalli di indirizzi IP dedicati associati a Office 365 Exchange Online, SharePoint Online e ai team Microsoft (indicati come categoria Ottimizza nella documentazione Microsoft) può essere indirizzato direttamente, all'esterno del tunnel VPN. Per ulteriori informazioni su questa raccomandazione, fare riferimento a Ottimizzazione della connettività di Office 365 per gli utenti remoti che utilizzano il tunneling ripartito della VPN.

> **Nota**: all'inizio di aprile 2020, Microsoft Teams dipende dal fatto che l'intervallo IP 10.107.60.1/32 deve essere escluso dal tunnel. Per ulteriori informazioni, vedere Configurazione e protezione del traffico multimediale dei team.

Verifica

Dopo aver connesso un utente, vengono visualizzati i percorsi non protetti con gli indirizzi forniti nell'ACL e nell'elenco di esclusione del tunnel dinamico.


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...

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).