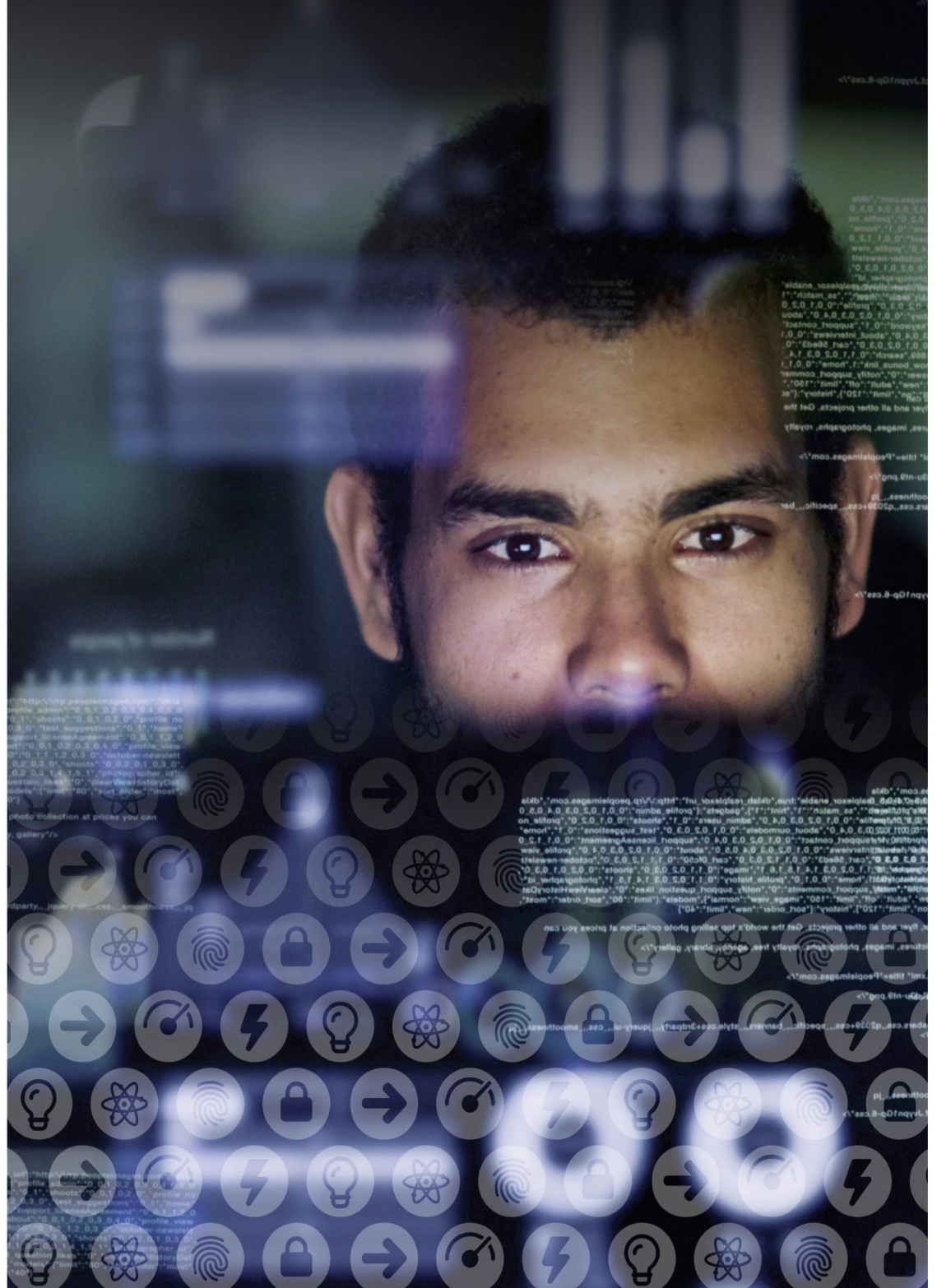




Config Guide

Optimizing Office 365 traffic on Remote Access through VPNs when using BIG-IP APM

F5 Networks, Inc.





The main objective of this document is to guide you on the Network Access configuration to split tunneling and dynamic exclusion of Office 365 URLs and IPs when using BIG-IP APM.

Over the past several weeks we have seen organizations adapt quickly, and as it relates to APM, implement split tunneling configurations to specifically allow Office 365 traffic to egress a client's local interface instead of the corporate network via the VPN tunnel. Microsoft publishes their Office 365 endpoints (URLs & IPs) via an API but occasionally they make changes and keeping on top of those changes can be an administrative nightmare.

To make the ongoing maintenance of the Network Access Lists / split tunneling configuration as seamless as possible, I've adapted a Python script we commonly use for SSL Orchestrator deployments to fetch Office 365 endpoints and update one or more Network Access Lists. Used in conjunction with iCall, this script will periodically check for and apply updates to your Network Access List(s) without any administrative intervention, allowing you to focus on other mission critical tasks.

Microsoft has provided us with a statement concerning their recommendations for Office 365 and split tunneling:

"Microsoft recommends excluding traffic destined to key Office 365 services from the scope of VPN connection by configuring split tunneling using published IPv4 and IPv6 address ranges. For best performance and most efficient use of VPN capacity, traffic to these dedicated IP address ranges associated with Office 365 Exchange Online, SharePoint Online and Microsoft Teams (referred to as Optimize category in Microsoft documentation) should be routed directly, outside of the VPN tunnel. Please refer to Microsoft guidance for more detailed information about this recommendation."



In the first step you need to create the Network Access profile. For this one, you can use the f5 wizard.

- Open the **Wizards > Device Wizards** page, and with **Network Access Setup Wizard for Remote Access** selected click **Next**.

The screenshot shows the F5 Network Manager interface. The top status bar indicates 'ONLINE (ACTIVE)' and 'Standalone'. The left sidebar contains navigation links: Main, Help, About, Statistics, iApps, Wizards (selected), Device Wizards (sub-selected), DNS, and SSL Orchestrator. The main content area is titled 'Wizards >> Device Wizards' and shows a 'Wizard List' with three options: 'Access Policy Manager Configuration', 'Network Access Setup Wizard for Remote Access' (selected with a blue radio button), 'Portal Access Setup Wizard', and 'Web Application Access Management for Local Traffic Virtual Servers'. Below the list, the 'Description' section shows the selected wizard's description: 'Configure a network access VPN connection for remote access. Creates an access policy and local traffic vir'. A 'Next...' button is visible at the bottom.

- On the **Basic Properties** page:
 - In the **Policy Name** box, type **vpn_profile_office365**.
 - Leave the **Default Language** set to **en**.
 - Leave the **Full Webtop** option cleared.
 - **Clear** the **Client Side Checks or Enable Antivirus Check in Access Policy** checkbox, and then click **Next**.

The screenshot shows the 'Basic Properties' configuration page. It includes a description of the 'Policy Name' field, the 'Default Language' dropdown (set to 'en'), the 'Full Webtop' checkbox (unchecked), the 'Caption' field (set to 'vpn_profile_office365'), and the 'Client Side Checks' checkbox (unchecked). Below this is the 'Default Gateway Configuration' section with an 'IPv6 Gateway Address' field. At the bottom are 'Cancel' and 'Next' buttons.

- On the **Select Authentication** page, you have two options: **Create New** and **Use Existing**

Create New: You will create a new AD/LDAP/RADIUS config.

Use Existing: You already have created this config before.

For this config guide we will create a new config.

Select Authentication

Please select the type of authentication you would like to configure for your access policy server.

If you would like to test a basic access policy without authentication, you are not authenticating and add an authentication action.

Authentication Options

☒ Create New
☐ Use Existing

☐ RADIUS
☐ LDAP
☒ Active Directory
☐ SecurID
☐ HTTP
☐ OCSP Responder
☐ CRLDP
☐ TACACS+
☐ No Authentication

Select Authentication

Use the following information for the AAA Server, and then click **Next**.

Domain Name: domain

Server Connection: Direct

Domain Controller: IP Address

Admin Name: username

Admin Password (and Verify): password

Configure AAA Server

Configure the authentication details for the selected authentication type. For configuration details on each option, see the documentation.

Domain Name

f5demo.com

Server Connection

☐ Use Pool
☒ Direct

Domain Controller

10.1.20.251

Admin Name

service_account

Admin Password

Verify Admin Password

Group Cache Lifetime

30

Days

Password Security Object Cache Lifetime

30

Days

Password Security Object Cache Lifetime

30

Days

Kerberos Preauthentication Encryption Type

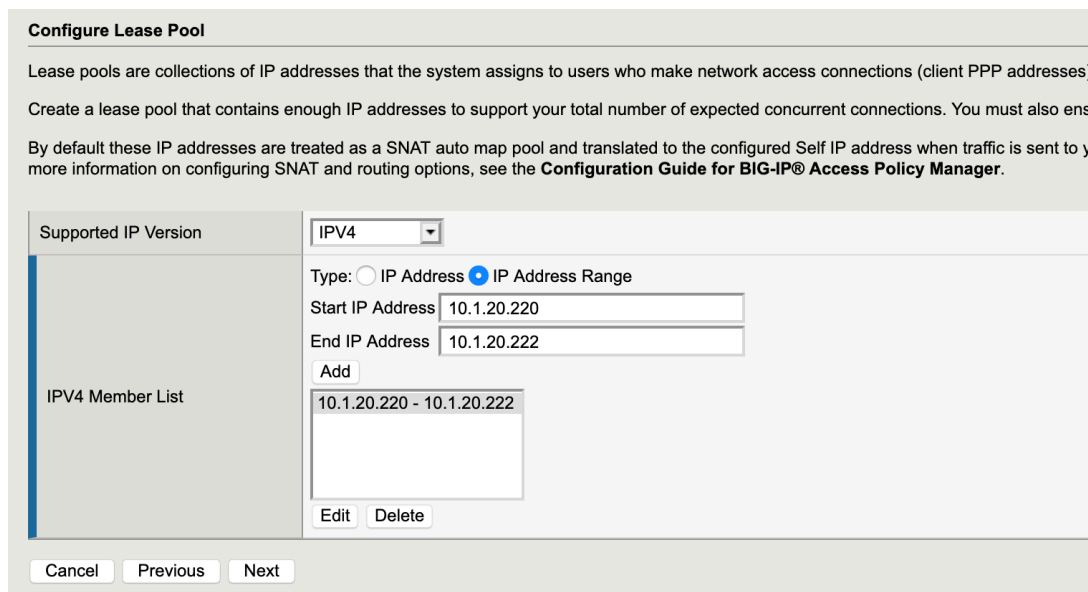
None

APM Split Tunneling for Office 365 – LATAM

Page 4

- On the **Configure Lease Pool** page, you need to add the address range which will be used by an user. Follow an example:

Lease pools are collections of IP addresses that the system assigns to users who make network access connections (client PPP addresses). A lease pool IP address is assigned to each client when the network access connection is established.



- On the **Configure Network Access** page, you will configure the **Split Tunneling**. **On this step we won't add any IP or Host from Microsoft...it will be done later.**

- On the **Client Settings**:

- In the **Traffic Options** box, select **Use split tunneling for traffic**.
- In the **IPv4 LAN Address Space**: Provides a list of addresses or address/mask pairs describing the target LAN.

When using split tunneling, only the traffic to these addresses and network segments goes through the tunnel configured for Network Access.

- IP Address: 0.0.0.0

- Mask: 0.0.0.0

Then click **Add**

PS: With this config, we are sending all traffic through the tunnel...the config for O365 comes later.

- In the **DNS Address Space**:

- DNS: *

Then click **Add**

PS: On the DNS setting, we type “*” to use the internal DNS Server and avoid an unnecessary traffic through the tunnel: If you do not specify a DNS address space, or *, DNS does not work over split tunnels on Windows, macOS, Linux, or iOS. To pass all DNS requests to the internal DNS server, specify *.

- Leave all the other option cleared and then click **Next**.

Configure Network Access

Configure the network access resource. For a basic network access connection, use the default values. For more information, see the documentation.

The lease pool you defined previously is assigned to this network access resource.

Compression

No Compression

Client Settings

Traffic Options

☐ Force all traffic through tunnel
☒ Use split tunneling for traffic

IPV4 LAN Address Space

IP Address

0.0.0.0

Mask

0.0.0.0

Add

0.0.0.0/0.0.0.0

Edit Delete

DNS Address Space

DNS

*

Add

*

Edit Delete

Allow Local Subnet

☐ Enable

Client Side Security

☐ Prohibit routing table changes during Network Access connection

DTLS

☐

Cancel

Previous

Next

- On the **Configure DNS Hosts for Network Access** page, you will set the **DNS** config which will be used by the user device. For this config guide, we are using the Google DNS, the click **Next**.

Configure DNS Hosts for Network Access

Specify DNS name servers, WINS servers, and a DNS default domain suffix. These servers and settings are assigned to end user client internal network resources.

These settings may be different than the BIG-IP system settings configured under **System : Configuration : Device : DNS**. For more information, see the [DNS Configuration Guide](#).

IPv4 Primary Name Server	<input type="text" value="8.8.8.8"/>
IPv4 Secondary Name Server	<input type="text"/>
Primary WINS Server	<input type="text"/>
Secondary WINS Server	<input type="text"/>
DNS Default Domain Suffix	<input type="text" value="localdomain"/>
Static Hosts	<div> Host Name <input type="text"/> IP Address <input type="text"/> </div> <div>Add</div> <div><input type="text"/></div> <div>Edit Delete</div>

Cancel Previous Next

- On the **Virtual Server (HTTPS connection)** page, you will specify an IP Address for the **Virtual Server** which will receive the SSL VPN connection from the user device.

Virtual Server IP Address: IP Address

Then click **Next**.

Virtual Server (HTTPS connection)

Specify an IP address to create a local traffic virtual server that is correctly configured for network access. Your end users connect to the virtual server IP address and are redirected to the destination address.

Check the option **Create Redirect Virtual Server (HTTP to HTTPS)** to create a local traffic virtual server that automatically redirects HTTP traffic to HTTPS.

For information on installing a valid SSL server certificate and using this destination address behind a firewall, please see the [SSL Configuration Guide](#).

Virtual Server IP Address	<input type="text" value="10.1.10.193"/>
Redirect Server	<input checked="" type="checkbox"/> Create Redirect Virtual Server (HTTP to HTTPS)

Cancel Previous Next



- On the **Review Configuration** page, you will review all the config made and then click **Next**.

Review Configuration

Please check your configuration below. To change a setting, use the **Previous** button to go back to the page you want to edit.

Click **Next** to complete the configuration and apply the settings.

Click **Cancel** to quit the wizard without making any changes.

General Properties

Policy Name	vpn_profile_office365
Default Language	en
Enable Antivirus Check in Access Policy	Disabled
Full Webtop	Disabled

Authentication

Type	Active Directory
Domain Controller	10.1.20.251
Domain Name	f5demo.com
Admin Name	service_account
Admin Password	*****
accesscontrol.aaaservers.padataEncType	0

Network Access

Compression	No Compression
Traffic Options	Use split tunneling for traffic
IPV4 LAN Address Space	0.0.0.0/0.0.0.0
DNS Address Space	*
Allow Local Subnet	Disabled
Prohibit routing table changes during Network Access connection	Disabled
DTLS	Disabled
Assigned IPV4 Lease Pool	vpn_profile_office365_ip
IPV4 Primary Name Server	8.8.8.8

On the next page, just click **Finished**.

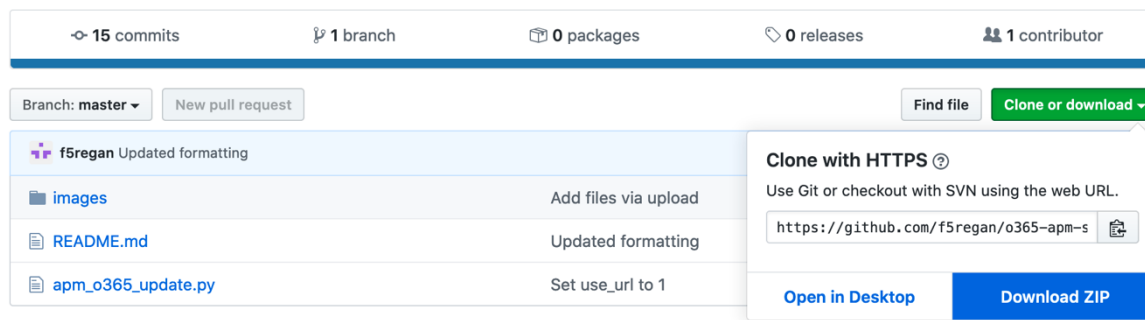


In the next step you need download the Office 365 script, which will fetch all URLs and IPs (IPv4 and IPv6) from Microsoft:

Script: `apm_o365_update.py`

URL: <https://github.com/f5regan/o365-apm-split-tunnel>

A Python script that fetches O365 URLs and IPs from Microsoft and dynamically updates Network Access List "Exclude" properties



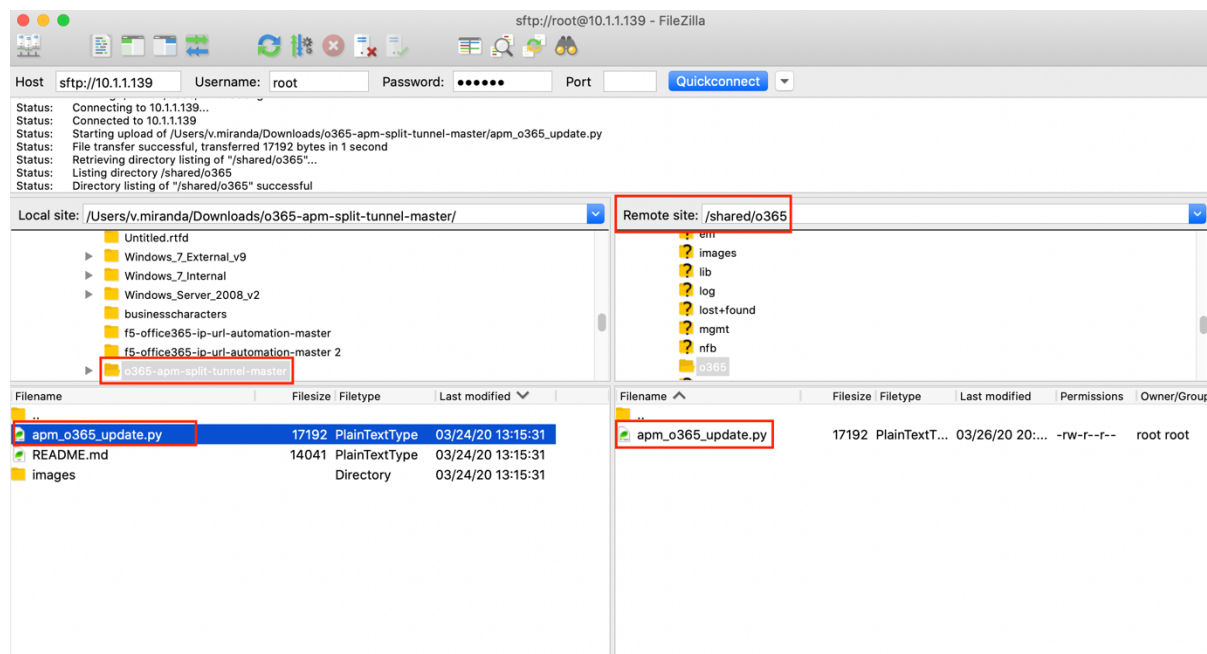
Once the download is completed, unzip the file. Now we need import this file to BIG-IP, but first let's create the Office 365 directory.

Connect through SSH on the BIG-IP;

PS: If you are using TMSH, go to bash with this command: `run util bash`

Create the Office 365 directory: `mkdir /shared/o365`

Now let's import the `apm_o365_update.py` file to the BIG-IP. On this config guide, we are using FileZilla, but feel free to use other software you want.



Now that we have the file imported, let's edit the script file to insert the Network Access profile created before.

- Connect through SSH on the BIG-IP;
- PS: If you are using TMSH, go to bash with this command: **run util bash**
- Navigate to the Office 365 directory: **cd /shared/o365**
- Open the script file with your preferred editor...for this config guide we are using **VIM**:

```
[root@f5demo:TimeLimitedModules::Active:Standalone] o365 # vim apm_o365_update.py
```

In the next step we will type the **access_profile** and **na_lists** into the script and then save...with **VIM: ESC → :wq! → Enter**.

You can find those information following these steps bellow:

Navigate to: Access → Profiles/Policies → Access Profiles (Per-Session Policies)

access_profile: **vpn_profile_office365**

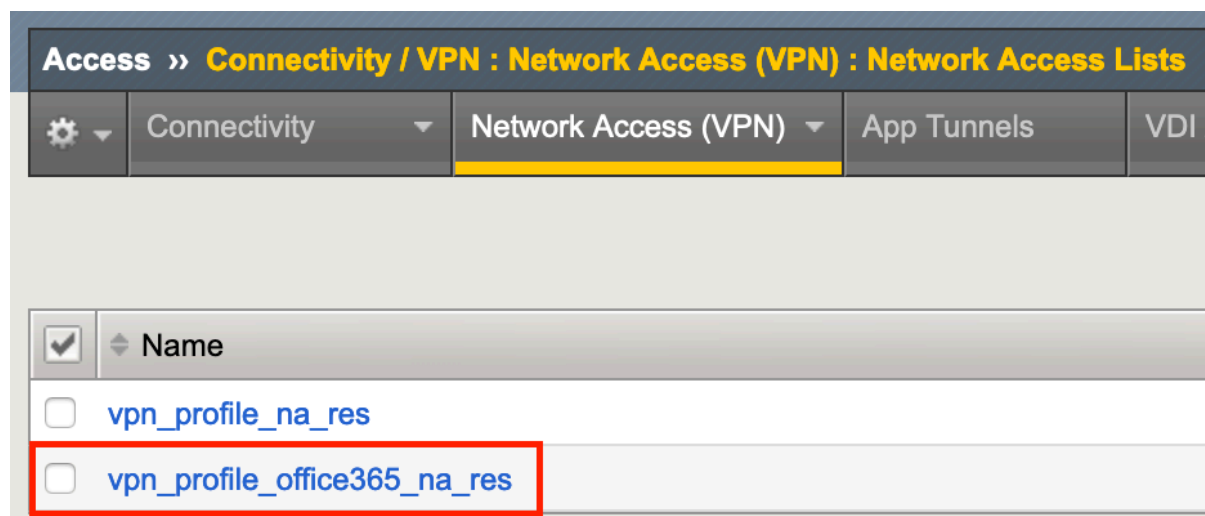
The screenshot shows the F5 BIG-IP configuration interface. The top navigation bar indicates the current location: **Access » Profiles / Policies : Access Profiles (Per-Session Policies)**. Below this, there are tabs for **Access Profiles**, **Per-Request Policies**, **Policy Sync**, and **Customization**. A search bar is present with the text "Search".

<input checked="" type="checkbox"/>	Status	Access Profile Name	Application	Profile Type
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>		vpn_profile_office365		All

At the bottom of the table, there are buttons for **Delete...** and **Apply**.

Navigate to: Access → Connectivity/VPN → Network Access (VPN)

na_lists: vpn_profile_office365_na_res



Now the script should look like this:

```
#-----
# User Options - Configure as desired
#-----

# Access Profile Name(s) - ex. SINGLE ["AP1"]
access_profiles = ["vpn_profile_office365"]

# Network Access List Name(s) - ex. SINGLE ["N
na_lists = ["vpn_profile_office365_na_res"]
```

PS: If you have a HA pair, you need repeat the procedure of import the script and edit the file...it's pretty easy.

This step is **ONLY** if you have a HA pair. In the script file, you need to type the "device_group_name" and change the ha_config from 0 to 1.

```
# BIG-IP HA Configuration
device_group_name = "device-group1"
ha_config = 1
```

Once you have finished all those steps, now it's time to execute our script:

- Connect through SSH on the BIG-IP;
- PS: If you are using TMSH, go to bash with this command: **run util bash**
- Command: **python /shared/o365/apm_o365_update.py**

To check if our script was executed with success, take a look at the log file:

Command: **cat /var/log/o365_update**

```
2020-03-26 22:14:13 This BIG-IP is standalone or HA ACTIVE. Initiating O365 update.
2020-03-26 22:14:13 Created GUID file /shared/o365/guid.txt because it did not exist.
2020-03-26 22:14:13 Generated a new GUID, and saved it to /shared/o365/guid.txt.
2020-03-26 22:14:13 Valid previous VERSION was not found. Wrote dummy value in /shared/o365/o365_version.txt.
2020-03-26 22:14:17 Number of unique ENDPOINTS to import...
2020-03-26 22:14:17 URL: 200
2020-03-26 22:14:17 IPv4 host/net: 79
2020-03-26 22:14:18 Completed O365 URL/IP address update process.
```

You can also check into the Network Access profile.

Navigate to: Access → Connectivity/VPN → Network Access (VPN) → Network Settings

Scroll down until you see the **IPv4 Exclude Address Space**. On this field you will gonna find a list of IP Address recommended by Microsoft from the category “Optimize” by default. This category is what you need to start the main optimization of Office 365 traffic, but if you want to add all categories, the script needs to be update.

IPv4 Exclude Address Space	IP Address	<input type="text"/>
	Mask	<input type="text"/>
	Add	
	104.146.128.0/255.255.128.0 13.107.128.0/255.255.252.0 13.107.136.0/255.255.252.0 13.107.18.10/255.255.255.254 13.107.6.152/255.255.255.254	
	Edit	Delete

OPTIONAL

Updating the script to get all categories:

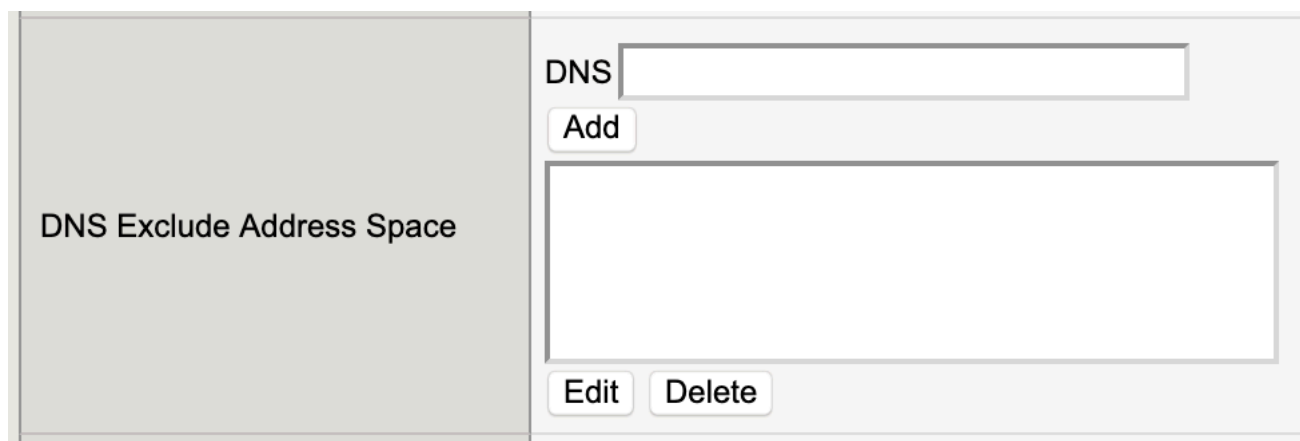
```
# O365 Categories to download & update
o365_categories = 0 # 0=Optimize only, 1= Optimize & Allow, 2 = Optimize, Allow, and Default
```

0 = Optimize only (DEFAULT);

1 = Optimize & Allow;

2 = Optimize, Allow and Default;

Regarding the DNS Exclude Address Space



We didn't add any URL by default following what Microsoft has recommended, but you still have this option to get all URLs by enabling it into the script.

OPTIONAL

Updating the script to get the URLs of Office 365:

```
# 0365 Record types to download & update
use_url = 0           # DNS/URL exclusions: 0=do not use, 1=use
use_ipv4 = 1          # IPv4 exclusions: 0=do not use, 1=use
use_ipv6 = 0          # IPv6 exclusions: 0=do not use, 1=use
```

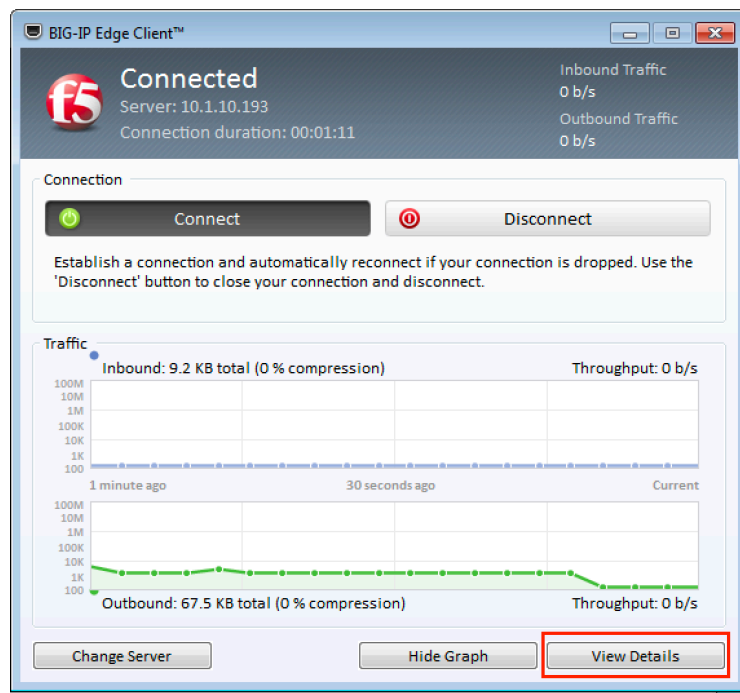
0 = do not use (DEFAULT);

1 = use;

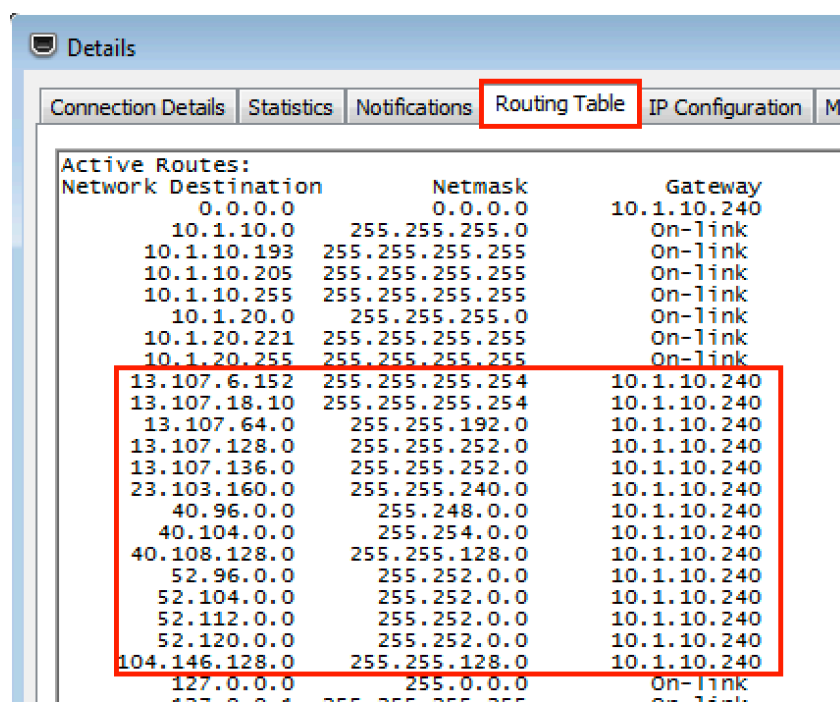
How do I know if my new config is working?

The answer is: just check the Routing Table on your VPN client.

First, open your VPN client and click on “View Details”



Now let's check the Routing Table:



If you want to keep your base of URLs and IPs updated, you can create an **iCall**. This script executes the `apm_o365_update.py` script when it is called by an iCall handler, which we will create in the next step. Ensure the correct path to the script is referenced, in case defaults were not used.

- Connect through SSH on the BIG-IP;
- PS: If you are using TMSH, go to bash with this command: **run util bash**
- Command: **tmsh create sys icall script o365_update_script definition { catch { exec python /shared/o365/apm_o365_update.py } }**

Now we need to create an **iCall handler**. This handler will run at the configured interval and will execute the iCall script, which in turn executes the `apm_o365_update.py` Python script. A few examples of periodic handlers are given, choose (and adapt) the one that suits your needs best.

Example: Run once every 60 minutes (3600 seconds), starting now:

- Command: **tmsh create sys icall handler periodic o365_update_handler script o365_update_script interval 3600**

Example: Run once every 24 hours (86400 seconds), starting on March 24, 2020 at 03:00:

- Command: **tmsh create sys icall handler periodic o365_update_handler script o365_update_script interval 86400 first-occurrence 2020-03-24:03:00:00**

Once you have finished, don't forget to save the config:

- Command: **tmsh save sys config**

WE MAKE APPS  FASTER.
SMARTER.
SAFER.

F5 Networks, Inc. | f5.com



US Headquarters: 401 Elliott Ave W, Seattle, WA 98119 | 888-882-4447 // Americas: info@f5.com // Asia-Pacific: apacinfo@f5.com // Europe/Middle East/Africa: emeainfo@f5.com // Japan: f5j-info@f5.com
©2017 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. These training materials and documentation are F5 Confidential Information and are subject to the F5 Networks Reseller Agreement. You may not share these training materials and documentation with any third party without the express written permission of F5.