Powershell скрипт за генериране на VPN връзки в Windows

Александър Ташков, Синформа ЕООД

Powershell скрипт за генериране на VPN връзки в Windows

- VPN връзки в Windows
  - Новини за дефиниране
  - Under the Hood
  - Изграждане и прекъсване на VPN връзки
- Скрипт за генериране
  - Възможности
  - Параметри
  - Демо
- Следващи стъпки

Начини за създаване на VPN връзки в Windows

- През „класическия“ потребителски интерфейс
- През „новия“ потребителски интерфейс
- С команди на Powershell

Класически потребителски интерфейс

- Могат да бъдат дефинирани почти всички необходими параметри

- Не могат да бъдат зададени име и парола за VPN връзката
- Не могат да бъдат премахнати връзките на някои мрежови драйвери
- Не могат да бъдат дефинирани мрежи, достъпни през VPN връзката
- При Windows 10 – достъпът до него е усложнен

Нов потребителски интерфейс

- По-лесен достъп до него, отколкото до „класическия“
- Могат да бъдат зададени име и парола

- Силно ограничен набор от параметри, които могат да бъдат дефинирани

Команди на Powershell

- Могат да бъдат дефинирани почти всички необходими параметри
- Могат да бъдат дефинирани мрежи, достъпни през VPN връзката
- Дефинирането може да бъде опростено чрез създаване на скрипт
- Интересна опция – дефиниране на алтернативни сървъри за VPN връзката

- Не могат да бъдат премахнати връзките на мрежови драйвери
- Не могат да бъдат зададени име и парола за VPN връзката
- Изисква писане на ръка, ако не е подготвен скрипт
- Не работи под Windows 7 (и по-стари версии)

Къде се съхранява информацията за VPN връзките

- За **текущия** потребител:

  %APPDATA%\Microsoft\Network\Connections\Pbk\rasphone.pbk

  т.е.

  %SystemDrive%\Users\%UserName%\AppData\Roaming\Microsoft\Network\Connections\Pbk\rasphone.pbk

- За **всички** потребители

  %ALLUSERSPROFILE%\Microsoft\Network\Connections\Pbk\rasphone.pbk

  т.е.

  %PROGRAMDATA%\Microsoft\Network\Connections\Pbk\rasphone.pbk

Структура на rasphone.pbk

- Стандартен Windows INI файл
- Съдържа 1 или повече **RRAS phonebook section**
- Всяка RRAS phonebook section дефинира точно една връзка
  - Име
  - Параметри

```
[VPNTestL2TP]
Encoding=1
PBVersion=5
Type=2
AutoLogon=0
UseRasCredentials=1
LowDateTime=-868875312
HighDateTime=30830696
DialParamsUID=515978921
Guid=170F66A98E10BB439D889AE5F3CAA9BE
VpnStrategy=3
ExcludedProtocols=8
LcpExtensions=1
DataEncryption=256
SwCompression=0
NegotiateMultilinkAlways=0
SkipDoubleDialDialog=0
DialMode=0
OverridePref=15
RedialAttempts=3
RedialSeconds=60
IdleDisconnectSeconds=0
RedialOnLinkFailure=1
CallbackMode=0
CustomDialDll=
```

Интересни параметри в rasphone.pbk

- **Encoding**

  0 – ASCII
  1 – Unicode

- **PBVersion**

  Up to Windows 7/ Server 2008 R2 – **1**
  Windows 8.1 / Server 2012 R2 – **4**
  Windows 10 / Server 2016-2019 – **5**

- **Type**

  1 – Dial-up connection
  2 – VPN connection
  5 – Broadband connection

Интересни параметри в rasphone.pbk

- **VpnStrategy**

  1 – PPTP
  3 – L2TP
  5 – SSTP
  0, **2** – опитват се различни VPN тунели

- **PreferredPort** / **Port**

  COM[X]
  VPN1-0 – SSTP
  VPN3-0 – L2TP

- **PreferredDevice** / **Device**

  WAN Miniport (SSTP)
  WAN Miniport (L2TP)

Интересни параметри в rasphone.pbk

- **PhoneNumber**
  NumServers
  ServerListServerName
  ServerListFriendlyName

Дефинират 1 или няколко сървъра, към които се изгражда връзката

Интересни параметри в rasphone.pbk

1 сървър

```
PhoneNumber=ServerAddress
NumServers=0
ServerListServerName
ServerListFriendlyName
```

Интересни параметри в rasphone.pbk

3 сървъра

```
PhoneNumber=Server1
NumServers=3
ServerListServerName=server1.com
ServerListServerName=server2.com
ServerListServerName=server3.com
ServerListFriendlyName=Server1
ServerListFriendlyName=Server2
ServerListFriendlyName=Server3
```

Дефиниране на връзка с няколко сървра

1. Дефиниране на VPN сървърни адреси

```
PS C:\> $Server1 = New-VpnServerAddress -ServerAddress server1.com -FriendlyName Server1
```

Дефиниране на връзка с няколко сървра

2. Дефиниране на масив с адреси

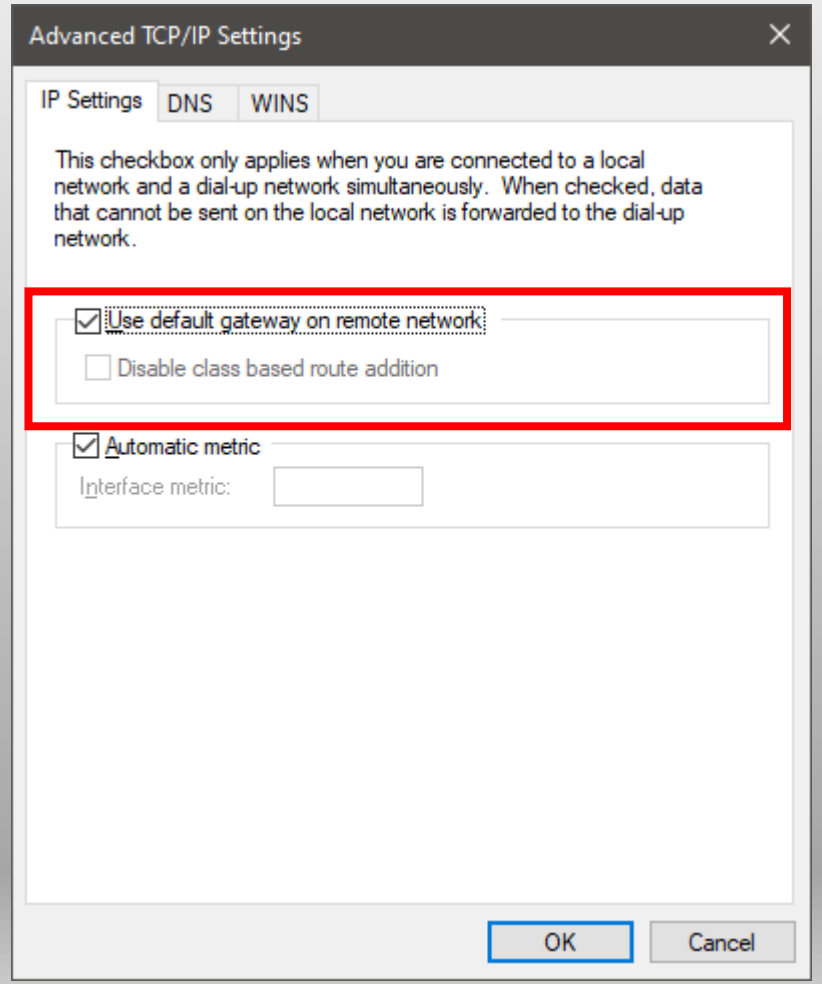
```
PS C:\> $Server1 = New-VpnServerAddress -ServerAddress server1.com -FriendlyName Server1
PS C:\> $Server2 = New-VpnServerAddress -ServerAddress server2.com -FriendlyName Server2
PS C:\> $Server3 = New-VpnServerAddress -ServerAddress server3.com -FriendlyName Server3
PS C:\> $Servers = @($Server1, $Server2, $Server3)
```

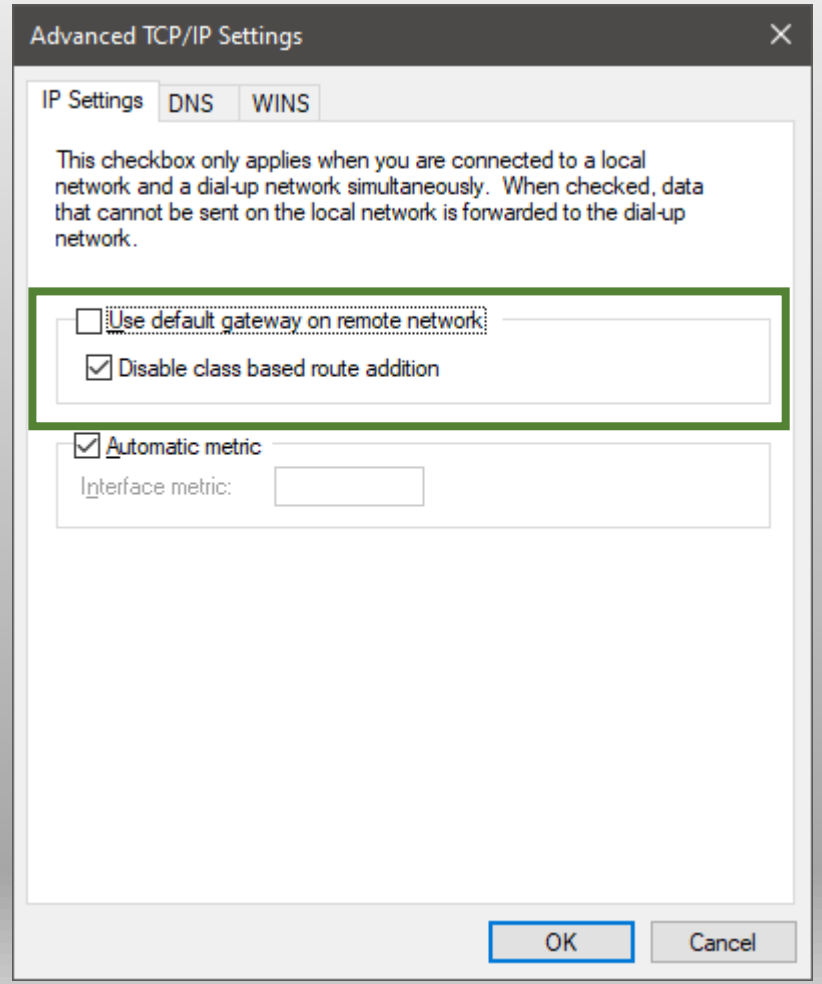
Дефиниране на връзка с няколко сървра

3. Използване на масива при дефинирането на VPN връзка

```
PS C:\> $Server1 = New-VpnServerAddress -ServerAddress server1.com -FriendlyName Server1
PS C:\> $Server2 = New-VpnServerAddress -ServerAddress server2.com -FriendlyName Server2
PS C:\> $Server3 = New-VpnServerAddress -ServerAddress server3.com -FriendlyName Server3
PS C:\> $Servers = @($Server1, $Server2, $Server3)
PS C:\> Add-VpnConnection -Name MultipleServersTest -ServerAddress Server1 -TunnelType L2tp -ServerList $Servers
```

Рутиране през VPN връзка





Рутиране през VPN връзка

Добавяне на маршрут

`route.exe` ↔ **`Add-VPNConnectionRoute`**

Изисква административни привилегии

Остава постоянно в рутинг-таблицата

НЕ изисква административни привилегии

Добавя се при изграждане на връзката и се премахва след прекъсването ѝ

Рутиране през VPN връзка

Параметри в rasphone.pbk

- **`RouteVersion`** **`1`**
- **`NumRoutes`** Брой дефинирани маршрути
- **`Routes`** Кодиран текст,
  72 шестнадесетични символа / маршрут
  до 128 символа в 1 **`Routes`** запис

Изграждане и прекъсване на VPN връзка

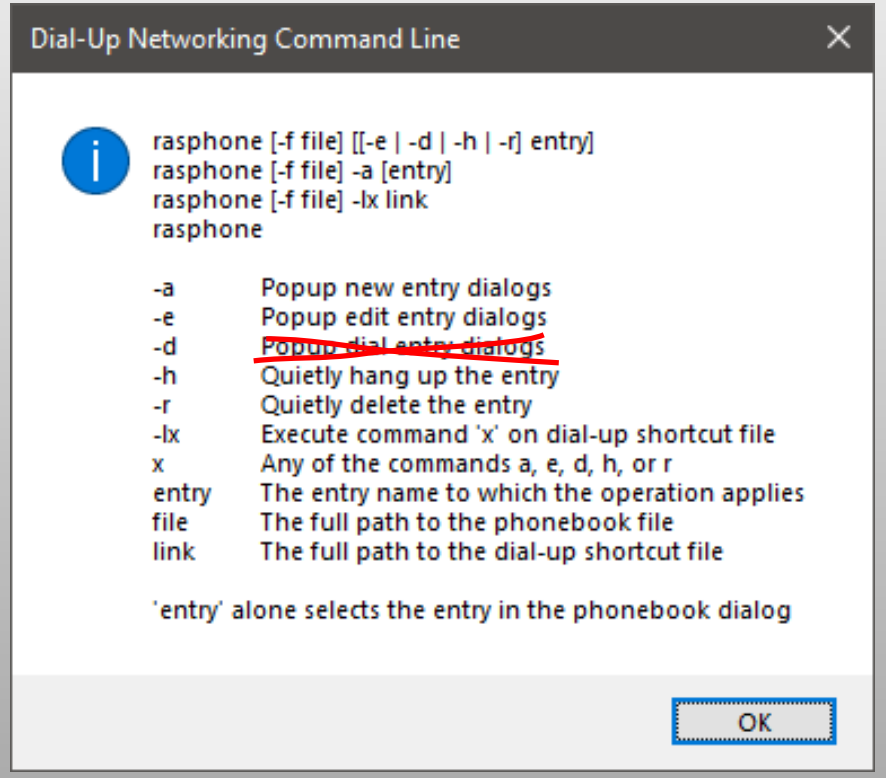
- През потребителския интерфейс
- **`rasdial.exe`** ⟵ Win32 RasDial API
- **`rasphone.exe`** ⟵ Win32 RasPhoneDlg API
- няма Powershell команда за изграждане/прекъсване на VPN връзка

`rasdial.exe` ↔ `rasphone.exe`

- Конзолно приложение
- Win32 RasDial API
- Изградените връзки не се отразяват в UI на Windows
- Параметри:
  `UserName` / **`Password`**
- ----

- Графично приложение
- Win32 RasPhonebook API
- Изградените връзки се отразяват в UI на Windows
- ----
- Кеширане на UN / Pwd

rasphone.exe



-d dials the connection

Дали ще се изобрази диалогов прозорец за въвеждане на име и парола се определя от параметъра **PreviewUserPw** в раздела за връзката във **phonebook.pbk**

Скрипт за създаване на VPN връзки

New-VPNConnection

Изисквания

- Да генерира връзки за вградения в Windows VPN клиент
- Да позволява въвеждането на всички съществени параметри при дефинирането на VPN връзки
- Да използва само вградена в Windows функционалност
- Да няма компилиран код

Функционалност

- Дефиниране на **L2TP/IPsek PSK** и на **SSTP** VPN
- Използва **split tunneling**; достъпните през VPN мрежи трябва да бъдат изрично зададени
- Възможност за инсталиране на необходимия за SSTP сертификат (пита за акаунт с административни привилегии)

Функционалност

- Възможност за задаване на потребителско име и парола
- Ако са зададени име и парола, се прави опит за изграждане на връзката; при успешно изграждане името и паролата се кешират автоматично от Windows
- Изключва се показването на диалогов прозорец за име и парола при изграждане на VPN връзката

Функционалност

- Възможност за дефиниране на VPN за текущия потребител или за всички потребители (необходимо е **стартиране** с административни привилегии)
- По подразбиране изключва свързването на IPv6, File and Printer Sharing for MS Networks, Client for MS Networks и Network Monitor Driver (ако е инсталиран MS Network Monitor); възможност за включване на желаните компоненти
- Стандартна помощна информация в Powershell стил

Параметри

- Задължителни:
  - **ConnectionName**
  - **TunnelType**
  - **ServerAddress**
  - **NetworksBehindVPN**
  - **PSK** – само за L2TP/IPSec
- По избор:
  - **IsAllUsersConnection**
  - **RootCertificateFQFN**
  - **UserName**
  - **Password**
  - **BindMSServer**
  - **BindMSClient**
  - **BindIPv6**
  - **BindNetMon**

Проверки на параметрите

- **`ServerAddress`**
  - валиден IPv4 адрес
  - валидно DNS име
- **`NetworksBehindVPN`**
  - валиден CIDR адрес (на мрежа/хост)
  - FQFN на файл с CIDR адреси на мрежи/хостове – по един на ред
- **`IsAllUsersConnection`**
  - проверка за наличие на административни привилегии

Демо

Следващи стъпки

- Генериране на връзки в самостоятелни файлове и структура от линкове за изграждане/прекъсване на връзките
- Възможност за дефиниране на повече от един VPN сървър
- Добавяне на IKEv2 VPN със сертификат
- Добавяне на L2TP/IPSec VPN със сертификат

Благодаря за вниманието!