Затыкаем рот Windows 10

Windows 10 очень любит Интернет. Обновления, синхронизации, телеметрия и ещё куча разной другой очень нужной ЕЙ информации постоянно гуляет через наши сетевые соединения. В «стандартном» сценарии использования, когда Windows 10 управляет домашним или рабочим компьютером, это, в общем-то, терпимо, хотя и не очень приятно.

Однако жизнь сложная штука и не ограничивается только стандартными вариантами. Существуют ситуации, когда подобная сетевая активность операционной системы (ОС) нежелательна и даже вредна. За примерами далеко ходить не надо. Попробуйте подключить к Интернету давно не используемый резервный компьютер, собранный на старом железе. Пока софт на нём не обновится, использовать его будет практически невозможно, всё будет дико тормозить и еле шевелиться. А если вам в этот момент нужно срочно что-то сделать?

Для того чтобы подобного не происходило, необходимо «заткнуть рот Windows», то есть сделать так, чтобы она самостоятельно перестала «стучаться» в Интернет, устанавливать обновления и заниматься прочими непотребствами. Вот именно этим мы с вами и займёмся.

Если бы операционная система (ОС) разрабатывалась для удовлетворения нужд потребителей, то эту статью писать бы не пришлось. В ОС были бы стандартные механизмы настройки, с помощью которых можно было бы отключить весь ненужный функционал, но, к сожалению, это не так.

Проблема в том, что компьютер, управляемый Windows 10, нам не принадлежит. ОС содержит неудаляемые приложения, она может самостоятельно отменять действия пользователя, удалять или инсталлировать программы, а также делать

другие вещи, идущие вразрез с мнением пользователя, будь он даже администратор системы.

Интеграция с облачными сервисами в Windows 10 реализована так жёстко, что безболезненно отключить её просто невозможно. При любой попытке деактивации хотя бы части этого функционала в ОС обязательно что-нибудь да сломается. Поэтому дальнейший материал, так сказать, для профессионального использования. Не рекомендуется применять его на ваших компьютерах без предварительного тестирования и отладки.

Знай своего врага в лицо

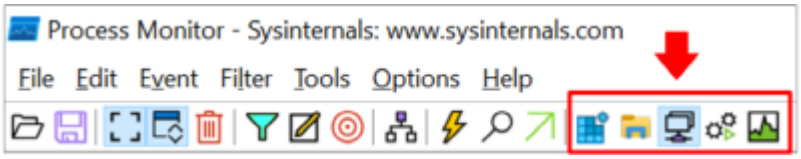
Первым шагом в нашей войне с «паразитной» сетевой активностью ОС будет исследование этой самой активности. Для этого мы соберём простейший лабораторный стенд, состоящий из двух виртуальных машин (ВМ).

Здесь Windows 10 будет выходить в Интернет через промежуточный Linux-шлюз, который будет оказывать ей услуги NAT и DNS-сервера.

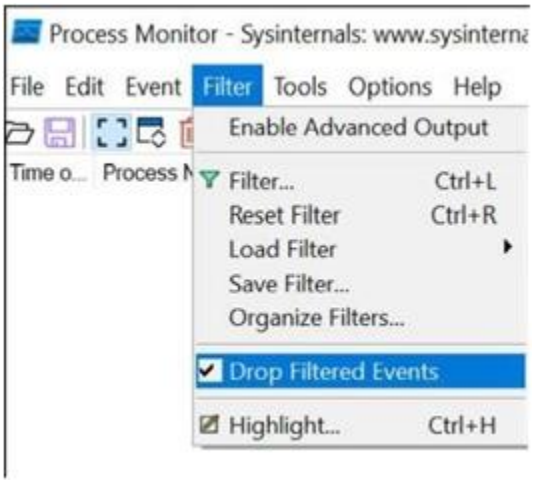
Исследовать «паразитный» сетевой трафик будем как на Linux-шлюзе, так и на самой Windows 10. На шлюзе это будем делать с помощью сниффера tcpdump и логов DNS-сервера, а на Windows 10 мы воспользуемся утилитой Process Monitor из пакета Sysinternals.

Настройку Linux-шлюза опустим из-за банальности, а про Process Monitor скажем пару слов. Для наших целей сделаем следующие шаги:

1. Отключим захват всех событий, кроме тех, что связаны с сетью. Для этого главный тулбар настроим следующим образом:

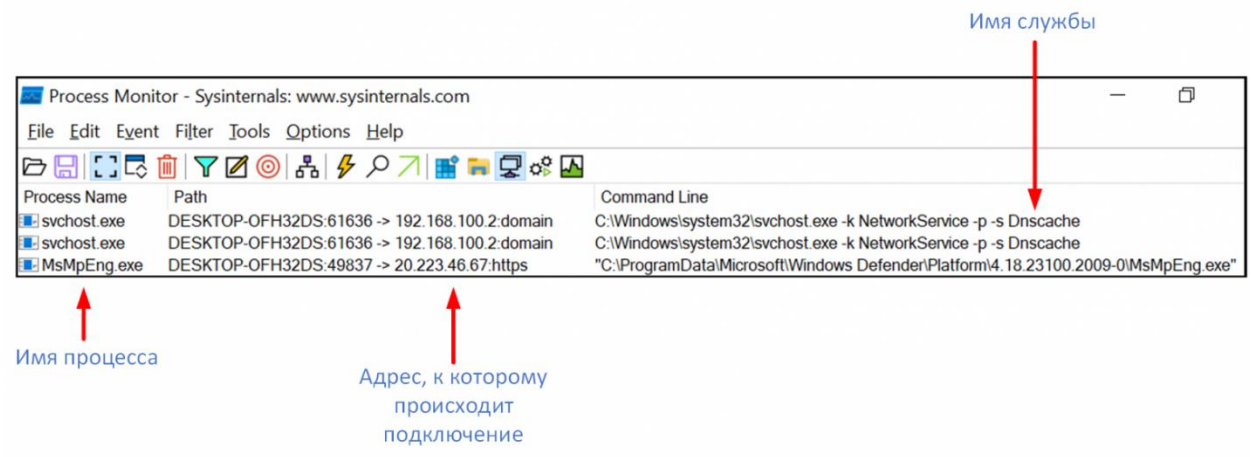


2. Настроим сброс отфильтрованных событий, чтобы не было переполнения памяти.
   Для этого в Menu > Filter и активируем опцию «Drop filtered events».



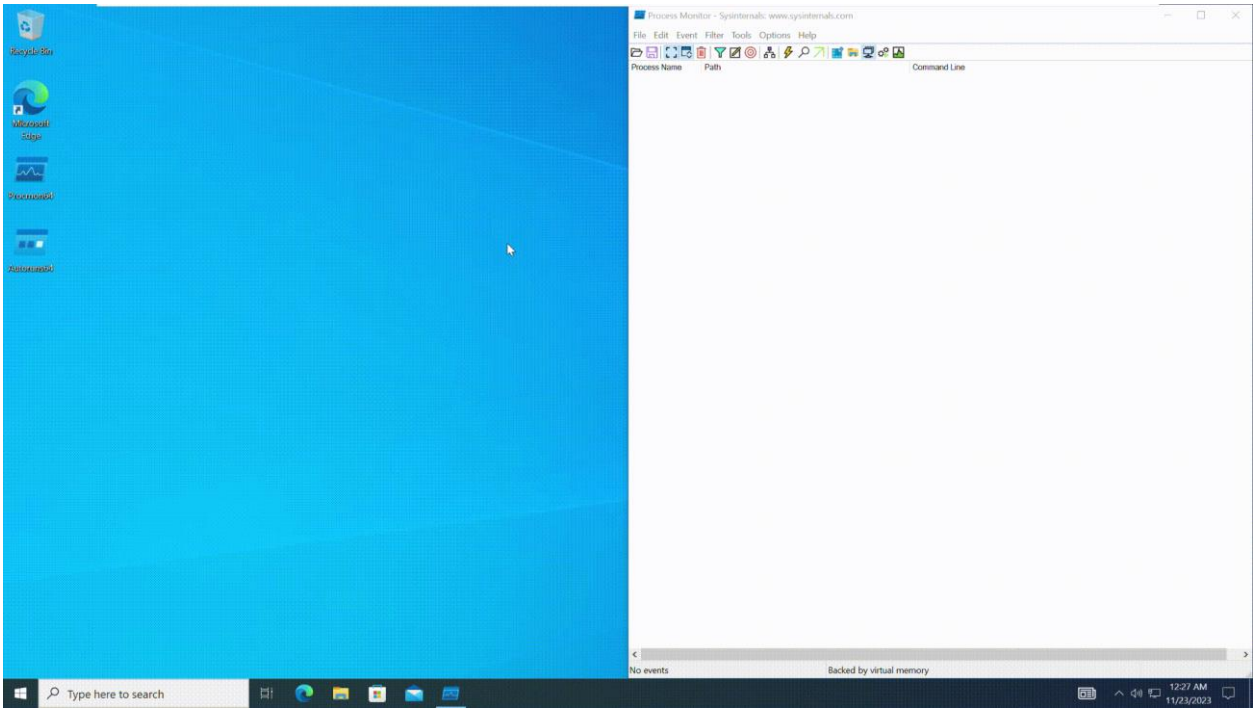
3. Настроим главный экран, что бы он отображал только то, что нам нужно. Открываем Options > Select columns и ставим галки только напротив пунктов: «Process name», «Command Line» и «Path»

В результате всех этих экзерциций при анализе сетевого трафика мы сможем увидеть процесс, инициирующий соединение, сетевой адрес назначения, и имена сетевых служб, запускаемых через специализированный процесс svchost.exe.



Первый замер

Наш первый замер будет самый простой. Мы дождёмся чуда, когда Windows перестанет передавать что-либо в Интернет, после чего пробежимся по стандартным настройкам ОС и посмотрим, какой трафик при этом будет генерироваться.



(анимированный GIF https://habrastorage.org/webt/go/zq/fw/gozqfwyqmn-fvvbp6dglmcuc-ns.gif)

Смотрите, как здорово. В Интернет передаётся информация практически о каждом нашем клике. Приватность? Не, не слышал… Что ж, мы научились детектировать «паразитный» трафик. Теперь будем разбираться, как его

блокировать.

Вариант блокировки № 1 – Windows Firewall

Наиболее логичным вариантом блокировки выглядит использование штатного межсетевого экрана — Windows Firewall. По логике вещей мы должны каким-то образом идентифицировать паразитный трафик и затем его заблокировать. Сделать это можно двумя способами:

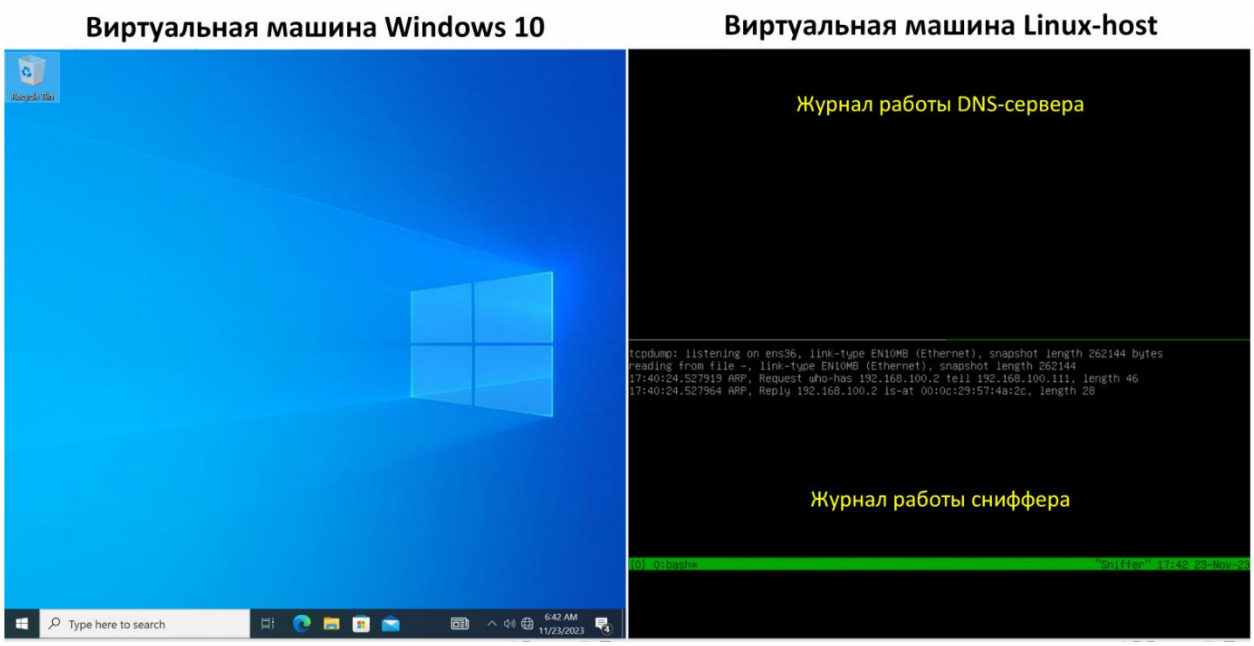
1. Оставить разрешённым весь исходящий трафик и при этом блокировать только тот, что мы сочтём паразитным.
2. Запретить весь исходящий трафик, а затем разрешить только тот, что сочтём нужным (не паразитным).

Но поскольку мы работаем в недоверенной системе, то нам нужно убедиться, что Windows Firewall в принципе на это способен. В частности, нам нужно удостовериться, что:

1. Windows Firewall может разрешать или запрещать системный траффик ОС.
2. Windows Firewall может разрешать или запрещать траффик с гранулярностью до системных служб.
3. Windows Firewall самостоятельно не отменит сделанные нами правила или другим образом не проявит излишнюю самостоятельность.

Тест для Windows Firewall № 1. Может ли он блокировать системный трафик?

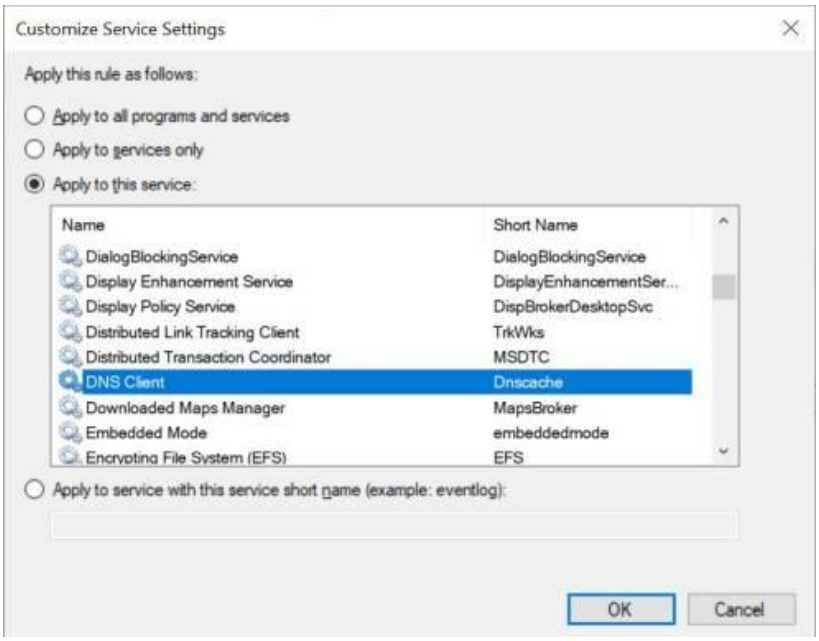
Идея эксперимента очень проста. Мы запретим любую сетевую активность и посмотрим, какой трафик будет проходить через этот запрет. Для этого в настройках Windows Firewall установим по умолчанию блокировку всего исходящего и входящего трафика, после чего удалим все правила исключения. Данные со шлюза говорят о том, что «паразитный» Интернет-трафик отсутствует, и фиксируются только ARP-запросы.



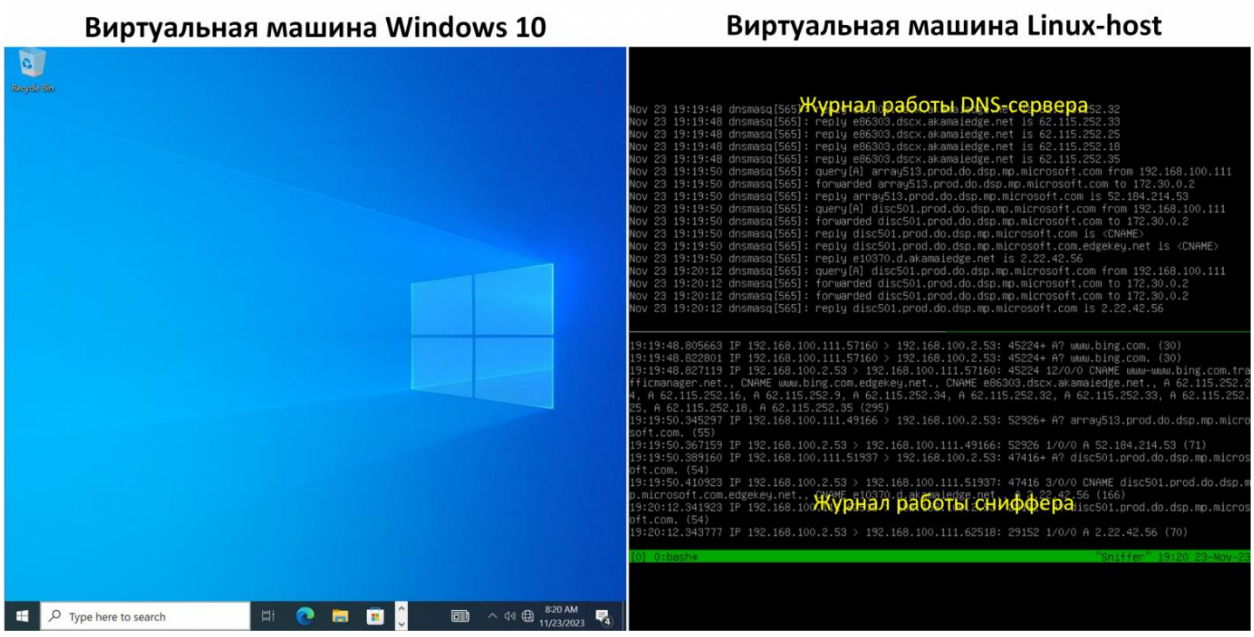
Получается, Windows Firewall может действительно заблокировать весь Интернет-трафик. Звучит обнадёживающе.

Тест для Windows Firewall № 2. Может ли он управлять трафиком конкретной сетевой службы?

В этом эксперименте мы должны убедиться, что Windows Firewall может управлять трафиком с гранулярностью до сервиса. Для этого попробуем разрешить трафик для системного DNS-клиента (имя этой службы – Dnscache). С помощью мастера настройки создадим исходящее правило, разрешающее весь трафик, и укажем, чтобы оно применялось к данной службе.



Смотрим, что там на шлюзе.



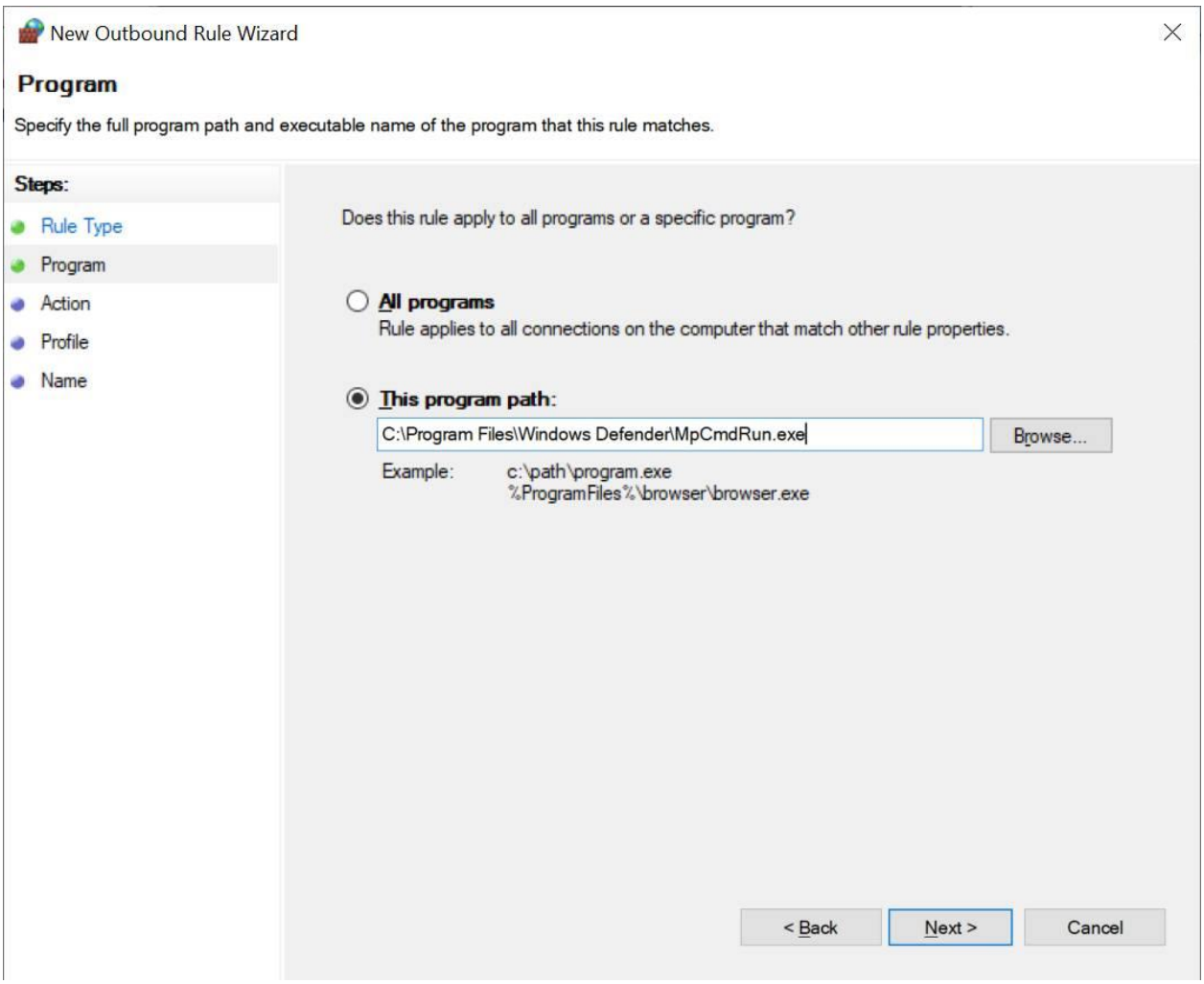
Словно человек, изнывающий от жажды при виде бутылки чистой воды, Windows 10 после разрешения работы DNS-клиента сразу же бросилась пытаться что-нибудь передать или получить из Интернета, ведь она не была в онлайне уже несколько минут. Мало ли что там могло произойти!

Windows Firewall прошёл и это испытание. Остался последний шаг.

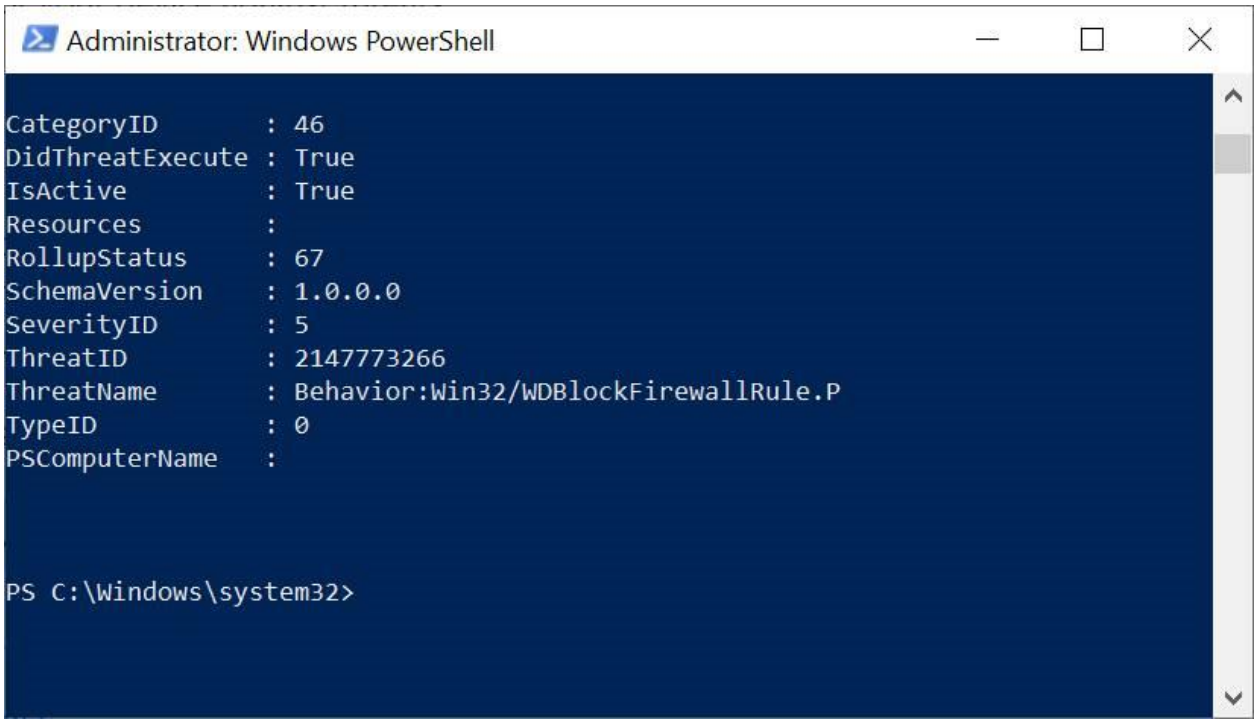
Тест для Windows Firewall № 3. Будет ли Windows Firewall самостоятельно исправлять правила, созданные пользователем?

Одним из генераторов «паразитного» трафика является встроенный антивирус Windows Defender. Он качает обновления баз, а также передаёт в облачный сервис (который судя по групповым политикам, называется SpyNet) принадлежащие вам файлы. В качестве теста попробуем заблокировать эту сетевую активность.

Для схемы с разрешённым по умолчанию исходящим трафиком создадим правило блокировки Windows Defender. Для этого в правиле блокировки укажем путь к блокируемой программе: «C:\Program Files\Windows Defender\MpCmdRun.exe»



В момент записи правила сразу же срабатывает Windows Defender с обнаружением угрозы (WDBlockFirewallRule) и удаляет сделанное нами правило.



Таким образом, последний тест Windows Firewall провалил. Конечно, правила удалил не Windows Firewall, а другой компонент ОС, тем не менее мы в очередной раз убедились, что наш компьютер нам не принадлежит.

Итог по Windows Firewall

Несмотря на все выкрутасы, использование Windows Firewall для блокировки паразитного трафика возможно. Единственной доступной в данном случае схемой будет блокировка по умолчанию всего исходящего трафика с созданием разрешающих правил для трафика, который мы сочтём нужным. Тем не менее осадочек остался, и использовать Windows Firewall дальше мы не будем.

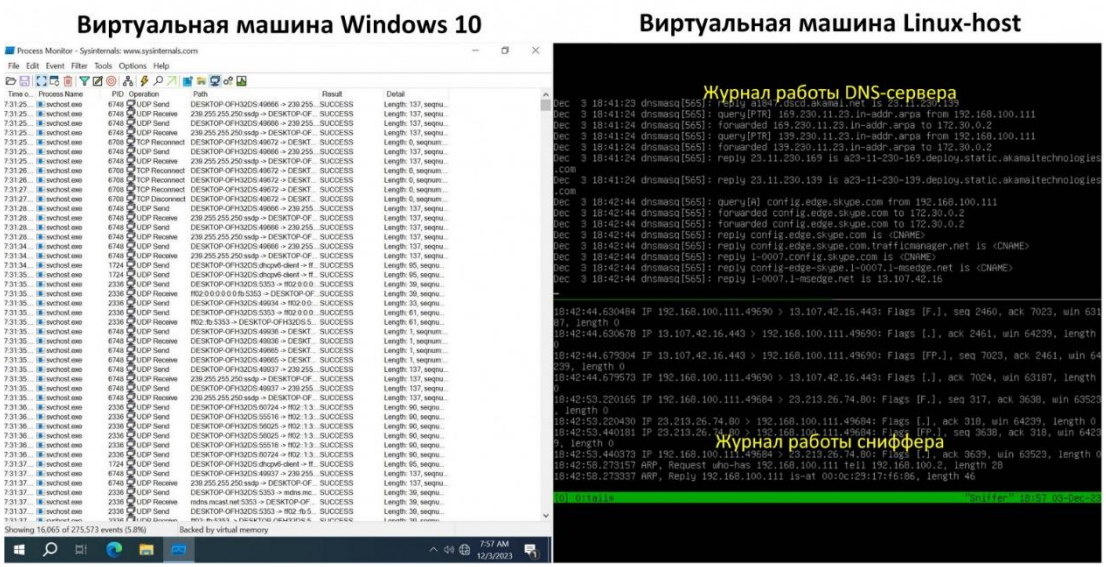
Вариант блокировки № 2 – рекомендации Microsoft

Корпорацию Microsoft наверно так задолбали с наездами по поводу не в меру ретивой сетевой активности Windows, что она выпустила гайд «Manage connections from Windows 10 and Windows 11 operating system components to Microsoft services» о том, как немного притормозить её пыл. В гайде приведены инструкции, как с помощью групповых политик или манипуляций с реестром отключить часть сетевых возможностей ОС. Также Microsoft предлагает удалить некоторые встроенные приложения. Реализация гайда Приведена в Приложениях:

Приложение 1. REG-файл уровня пользователя user.reg
Приложение 2. REG-файл уровня компьютер comp.reg
Приложение 3. PowerShell-скрипт, удаляющий ВСЕ встроенные приложения

Применим все эти файлы, перезагрузимся и посмотрим, что станет с трафиком.

Важно! Перед применением REG-файлов необходимо отключить самозащиту Windows Defender (Tamper protection). О том, как это сделать, будет в конце статьи.



«Паразитный» трафик уменьшился в разы, но, ожидаемо, не пропал полностью. Анализ фонового трафика находящейся в простое ВМ выявил следующих «болтунов»:

1. MS Edge;
2. Сервис Delivery Optimization (DoSvc);
3. Сервис AppX Deployment Service (AppXSVC);
4. Сервис Windows Update (wuauserv).

С большей частью болтунов можно разобраться, указав в свойствах сетевого подключения, что оно лимитированное (mettered). Для проводных (Ethernet) соединений сделать это можно с помощью скрипта в Приложении.

Приложение 4. PowerShell-скрипт, устанавливающий признак лимитированного соединения

После применения этого скрипта объём передаваемого трафика снизится ещё больше (~1Mb/час), а единственным болтуном останется MS Edge. Если вы планируете использовать этот браузер в дальнейшем, то на этом можно и успокоиться. Для тех же, кто хочет полной приватности, необходимо победить финального босса — MS Edge.

Чтобы прикрыть ему рот, необходимо с помощью штатных средств (Menu > Settings) настроить браузер таким образом, чтобы он использовал облачные службы, синхронизировался и выполнял прочую сетевую активность по минимуму. Если требуется настроить несколько машин, то можно только на одной настроить пользовательский профиль в браузере, а потом копировать его на все другие машины. Профиль хранится в "%LOCALAPPDATA%\Microsoft\Edge\User Data".

После настройки браузера необходимо отключить службы Edge, отвечающие за обновления, и удалить задания из системного планировщика. Сделать всё это можно следующим скриптом из приложения:

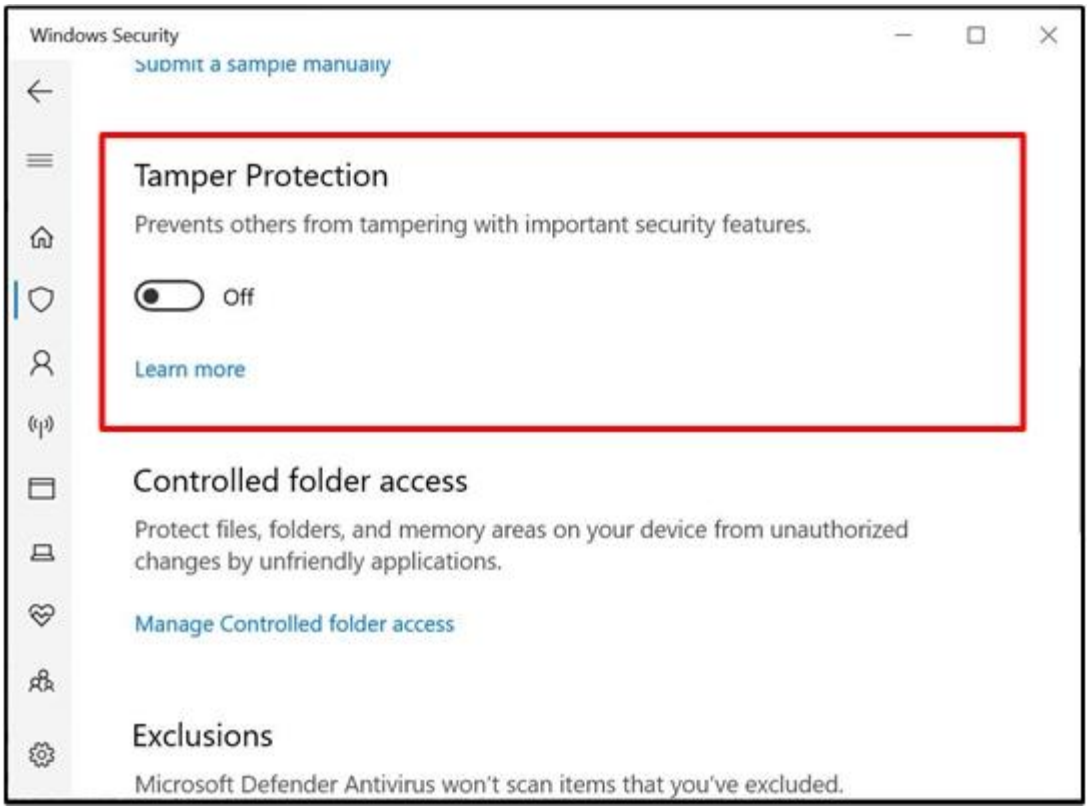
Приложение 5. PowerShell-скрипт, отключающий службы обновления MS Edge

После всех этих манипуляций с MS Edge система полностью прекратит генерировать фоновый Интернет-трафик (при измерении в режиме простоя). Важно отметить, что любой неосторожный запуск MS Edge приведёт к тому, что он снова будет втихаря стучаться в Интернет. Так что будьте осторожны.

Отключение Windows Defender

Данный шаг является опциональным, поскольку болтливость встроенного антивируса существенно ограничится REG-файлами, приведёнными выше. Однако, в условиях, когда антивирус не обновляется, он теряет всякую актуальность и жрёт ресурсы впустую. Чтобы его отключить, нужно сделать следующее:

1. Руками, с помощью GUI в настройках антивируса необходимо отключить опцию «Tamper protection» (Settings > Update & Security > Windows Security > Virus & Threat protection > Virus & Threat protection settings > Tamper protection off).



2. Затем следует применить следующий REG-файл из Приложения.

[Приложение 6. REG-файл, отключающий Windows Defender]

Краткая инструкция применения данного способа блокировки

1. Загрузить REG-файлы уровня пользователя user.reg и уровня компьютера comp.reg.
2. Запустить скрипт, удаляющий встроенные приложения.
3. Запустить скрипт, устанавливающий признак лимитированного соединения.
4. Провести настройку браузера MS Edge.
5. Запустить скрипт, отключающий механизмы обновления MS Edge.

Послевкусие и стратегия использования

Как уже отмечалось выше, любые попытки отключения сетевых возможностей ОС Windows 10 приводят к проблемам. Данный способ не исключение.

Практика показала, что после проведения всех этих манипуляций некоторые

программы, например, Mozilla Firefox, отказываются инсталлироваться. Тем не менее ранее установленные программы, тот же Firefox, продолжают работать. Всё это говорит о том, что стратегия «затыкания рта Windows» должна быть такой:

1. Полностью обновить ОС.
2. Инсталляция и настройка требуемых сторонних программ.
3. Отключение «паразитного» сетевого трафика.

Приложение 1. REG-файл уровня пользователя user.reg

Примечание. Будьте аккуратны с переносами строк.

```
Windows Registry Editor Version 5.00

; 8. Internet Explorer. Turn off the home page
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main]
"Start Page"="about:blank"

; 8. Internet Explorer. Turn off the home page
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Control
Panel]
"HomePage"=dword:1

; 8. Internet Explorer. Disable first run wizard
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main]
"DisableFirstRunCustomize"=dword:1

; 8. Internet Explorer. Set about:blank in new tab
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet
Explorer\TabbedBrowsing]
"NewTabPageShow"=dword:0

; 8.1 ActiveX control blocking. Disable periodocally download a list of out-
of-date ActiveX controls
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\VersionManager]
"DownloadVersionList"=dword:0

; 18.1 General. Disable websites access to my language list
[HKEY_CURRENT_USER\Control Panel\International\User Profile]
"HttpAcceptLanguageOptOut"=dword:00000001

; 18.1 General. Disable track app launches
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advance
d]
"Start_TrackProgs"=dword:00000000

; 18.1 General. Turn off SmartScreen check of URLs what Microsoft Store apps
use:
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\AppHost]
"EnableWebContentEvaluation"=dword:00000000

; 18.6 Speech. Prevent sending your voice input to Microsoft Speech services:
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Speech_OneCore\Settings\OnlineSpeechPri
vacy]
"HasAccepted"=dword:00000000

; 18.16 Feedback & diagnostics. Turn off tailored experiences
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CloudContent]
"DisableTailoredExperiencesWithDiagnosticData"=dword:1

; 18.21 Inking & Typing. Turn off Inking & Typing data collection
[HKEY_CURRENT_USER\Software\Policies\Microsoft\InputPersonalization]
"RestrictImplicitTextCollection"=dword:0

; 18.21 Inking & Typing. Turn off Inking & Typing data collection
[HKEY_CURRENT_USER\Software\Policies\Microsoft\InputPersonalization]
"RestrictImplicitInkCollection"=dword:0
```

```
; 18.21 Inking & Typing. Turn off Inking & Typing data collection
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\InputPersonalization]
"RestrictImplicitInkCollection"=dword:00000001

; 18.21 Inking & Typing. Turn off Inking & Typing data collection
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\InputPersonalization]
"RestrictImplicitTextCollection"=dword:00000001

; 21. Sync your settings
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Messaging]
"CloudServiceSyncEnabled"=dword:00000000

; 25. Personalized Experiences. Disable feature
[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CloudContent]
"DisableWindowsSpotlightFeatures"=dword:1

; !!! This must be done within 15 minutes after Windows 10 or Windows 11 is
installed.
; 25. Personalized Experiences. Disable feature
[HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CloudContent]
"DisableCloudOptimizedContent"=dword:00000001

; 29. Windows Update. Turn off
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Windows
Update]
"DisableWindowsUpdateAccess"=dword:1

; 29. Windows Update. Turn off
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Windows
Update]

"DisableWindowsUpdateAccessMode"=dword:0
```

Приложение 2. REG-файл уровня компьютер comp.reg

Примечание. Будьте аккуратны с переносами строк.

```
Windows Registry Editor Version 5.00

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\AuthRoot]
"DisableRootAutoUpdate"=dword:1

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\ChainEngin
e\Config]
"ChainUrlRetrievalTimeoutMilliseconds"=dword:15000

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\ChainEngin
e\Config]
"ChainRevAccumulativeUrlRetrievalTimeoutMilliseconds"=dword:20000

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\ChainEngin
e\Config]
"Options"=dword:0

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\ChainEngin
e\Config]
"CrossCertDownloadIntervalHours"=dword:168

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\DPNGRA\Cer
tificates]

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\DPNGRA\CRL
s]

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\DPNGRA\CTL
s]

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\FVE\Certif
icates]

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\FVE\CRLs]

; 1. Automatic Root Certificates Update. Disable auto update
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\SystemCertificates\FVE\CTLs]

; 2.1 Cortana and Search Group Policies. Turn off Cortana
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Windows Search]
"AllowCortana"=dword:0

; 2.1 Cortana and Search Group Policies. Block access to location information
for Cortana
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Windows Search]
```

```
"AllowSearchToUseLocation"=dword:0

; 2.1 Cortana and Search Group Policies. Remove the option to search the
Internet from Cortana
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Windows Search]
"DisableWebSearch"=dword:1

; 2.1 Cortana and Search Group Policies. Stop web queries and results from
showing in Search
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Windows Search]
"ConnectedSearchUseWeb"=dword:0

; 2.1 Cortana and Search Group Policies. Firewall block rule
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\FirewallRules
]
"{0DE40C8E-C126-4A27-9371-
A27DAB1039F7}"="v2.25|Action=Block|Active=TRUE|Dir=Out|Protocol=6|App=%windir
%\\SystemApps\\Microsoft.Windows.Cortana_cw5n1h2txyewy\\searchUI.exe|Name=Blo
ck outbound Cortana|"

; !!!!!!!!!
; 3. Date & Time. Disable NTP
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters]
"Type"="NoSync"

; !!!!!!!!!
; 3. Date & Time. Disable NTP
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\W32time\TimeProviders\NtpClie
nt]
"Enabled"=dword:0

; 4. Device metadata retrieval. Prevent
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Device Metadata]
"PreventDeviceMetadataFromNetwork"=dword:1

; 5. Find My Device. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\FindMyDevice]
"AllowFindMyDevice"=dword:0

; 6. Font streaming. Disable download on demand
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"EnableFontProviders"=dword:0

; 7. Insider Preview builds. Turn off Insider Preview builds
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PreviewBuilds]
"AllowBuildPreview"=dword:0

; 7. Insider Preview builds. Turn off Insider Preview builds
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"ManagePreviewBuildsPolicyValue"=dword:1

; 7. Insider Preview builds. Turn off Insider Preview builds
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"BranchReadinessLevel"=-

; 8. Internet Explorer. Disable suggested Sites
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Suggested
Sites]
```

```
"Enabled"=dword:0

; 8. Internet Explorer. Disable enhanced suggestion in Address Bar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer]
"AllowServicePoweredQSA"=dword:0

; !!!!!!!!!
; 8. Internet Explorer. Disable auto complete
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Explor
er\AutoComplete]
"AutoSuggest"="no"

; 8. Internet Explorer. Disable geolocation
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\Geolocation]
"PolicyDisableGeolocation"=dword:1

; 8. Internet Explorer. Prevent managing Microsoft Defender SmartScreen
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\PhishingFilter]
"EnabledV9"=dword:0

; 8. Internet Explorer. Turn off Compatibility View
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet
Explorer\BrowserEmulation]
"DisableSiteListEditing"=dword:1

; 8. Internet Explorer. Turn off the flip ahead with page prediction feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\FlipAhead]
"Enabled"=dword:0

; 8. Internet Explorer. Turn off background synchronization for feeds and Web
Slices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Feeds]
"BackgroundSyncStatus"=dword:0

; 8. Internet Explorer. Disallow Online Tips
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explor
er]
"AllowOnlineTips"=dword:0

; 9. License Manager. Turn off related traffic
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LicenseManager]
"Start"=dword:00000004

; 10. Live Tiles. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\PushNo
tifications]
"NoCloudApplicationNotification"=dword:1

; 11. Mail synchronization. Turn off the Windows Mail app
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Mail]
"ManualLaunchAllowed"=dword:00000000

; 12. Microsoft Account. Disable Microsoft Account Sign-In Assistant:
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\wlidsvc]
"Start"=dword:00000004
```

```
13.1 Microsoft Edge Group Policies. Disable Address Bar drop-down list
suggestions
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\ServiceUI]
"ShowOneBox"=dword:0

13.1 Microsoft Edge Group Policies. Disable configuration updates for the
Books Library
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\BooksLibrary]
"AllowConfigurationUpdateForBooksLibrary"=dword:0

13.1 Microsoft Edge Group Policies. Turn off autofill
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\Main]
"Use FormSuggest"="no"

13.1 Microsoft Edge Group Policies. Don't send "Do Not Track"
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\Main]
"DoNotTrack"=dword:1

13.1 Microsoft Edge Group Policies. Disable password manager
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\Main]
"FormSuggest Passwords"="no"

13.1 Microsoft Edge Group Policies. Turn off search suggestion in address bar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\SearchScopes]
"ShowSearchSuggestionsGlobal"=dword:0

13.1 Microsoft Edge Group Policies. Turn off SmartScreen
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\PhishingFilter]
"EnabledV9"=dword:0

13.1 Microsoft Edge Group Policies. Open blank new tab
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\ServiceUI]
"AllowWebContentOnNewTabPage"=dword:0

13.1 Microsoft Edge Group Policies. Set blank homepage
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\Internet
Settings]
"ProvisionedHomePages"="<<about:blank>>"

13.1 Microsoft Edge Group Policies. Prevent the First Run webpage from
opening
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\Main]
"PreventFirstRunPage"=dword:1

13.1 Microsoft Edge Group Policies. Disable compatibility mode
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MicrosoftEdge\BrowserEmulatio
n]
"MSCompatibilityMode"=dword:0

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"SearchSuggestEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"AutofillAddressEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"AutofillCreditCardEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"ConfigureDoNotTrack"=dword:00000001

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"PasswordManagerEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"DefaultSearchProviderEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"HideFirstRunExperience"=dword:00000001

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"SmartScreenEnabled"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"NewTabPageLocation"="about:blank"

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge]
"RestoreOnStartup"=dword:00000005

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\RestoreOnStartupURLs]
"1"="about:blank"

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate]
"UpdateDefault"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate]
"AutoUpdateCheckPeriodMinutes"=dword:00000000

; 13.2 Microsoft Edge Enterprise.
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Edge\EdgeUpdate]
"ExperimentationAndConfigurationServiceControl"=dword:00000000

; 14. Network Connection Status Indicator. Turn off active probe
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\NetworkConnectivitySt
atusIndicator]
"NoActiveProbe"=dword:1

; 15. Offline maps. Disable download and update offline maps
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Maps]
"AutoDownloadAndUpdateMapData"=dword:0

; 15. Offline maps. Disable download and update offline maps
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Maps]
```

```
"AllowUntriggeredNetworkTrafficOnSettingsPage"=dword:0

; 16. OneDrive. Prevent the usage of OneDrive for file storage
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\OneDrive]
"DisableFileSyncNGSC"=dword:1

; 16. OneDrive. Prevent OneDrive from generating network traffic until the
user signs in to OneDrive
[HKEY_LOCAL_MACHINE\Software\Microsoft\OneDrive]
"PreventNetworkTrafficPreUserSignIn"=dword:1

; 18.1 General. Turn off advertising ID
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\AdvertisingInfo
]
"Enabled"=dword:00000000

; 18.1 General. Turn off advertising ID
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AdvertisingInfo]
"DisabledByGroupPolicy"=dword:1

; 18.1 General. Disable continue experiences
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"EnableCdp"=dword:0

; 18.2 Location. Prevent apps from accessing the location
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\LocationAndSensors]
"DisableLocation"=dword:1

; 18.2 Location. Prevent apps from accessing the location
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessLocation"=dword:2

; 18.2 Location. Prevent apps from accessing the location
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessLocation_UserInControlOfTheseApps"=hex(7):00,00

; 18.2 Location. Prevent apps from accessing the location
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessLocation_ForceAllowTheseApps"=hex(7):00,00

; 18.2 Location. Prevent apps from accessing the location
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessLocation_ForceDenyTheseApps"=hex(7):00,00

; 18.3 Camera. Prevent apps from accessing the camera
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCamera"=dword:2

; 18.3 Camera. Prevent apps from accessing the camera
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCamera_UserInControlOfTheseApps"=hex(7):00,00

; 18.3 Camera. Prevent apps from accessing the camera
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCamera_ForceAllowTheseApps"=hex(7):00,00

; 18.3 Camera. Prevent apps from accessing the camera
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
```

```
"LetAppsAccessCamera_ForceDenyTheseApps"=hex(7):00,00

; 18.4 Microphone. Prevent apps from accessing the microphone
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMicrophone"=dword:2

; 18.4 Microphone. Prevent apps from accessing the microphone
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMicrophone_UserInControlOfTheseApps"=hex(7):00,00

; 18.4 Microphone. Prevent apps from accessing the microphone
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMicrophone_ForceAllowTheseApps"=hex(7):00,00

; 18.4 Microphone. Prevent apps from accessing the microphone
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMicrophone_ForceDenyTheseApps"=hex(7):00,00

; 18.5 Notifications. Turn off cloud notifications notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\PushNo
tifications]
"NoCloudApplicationNotification"=dword:1

; 18.5 Notifications. Prevent apps from accessing my notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessNotifications"=dword:2

; 18.5 Notifications. Prevent apps from accessing my notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessNotifications_UserInControlOfTheseApps"=hex(7):00,00

; 18.5 Notifications. Prevent apps from accessing my notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessNotifications_ForceAllowTheseApps"=hex(7):00,00

; 18.5 Notifications. Prevent apps from accessing my notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessNotifications_ForceDenyTheseApps"=hex(7):00,00

; 18.6 Speech. Turn off updates to the speech recognition and speech
synthesis models
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Speech]
"AllowSpeechModelUpdate"=dword:0

; 18.6 Speech. Turn off updates to the speech recognition and speech
synthesis models
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\InputPersonalization]
"AllowInputPersonalization"=dword:0

; 18.7 Account info. Prevent apps from accessing account info
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessAccountInfo"=dword:2

; 18.7 Account info. Prevent apps from accessing account info
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessAccountInfo_UserInControlOfTheseApps"=hex(7):00,00

; 18.7 Account info. Prevent apps from accessing account info
```

```
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessAccountInfo_ForceAllowTheseApps"=hex(7):00,00

; 18.7 Account info. Prevent apps from accessing account info
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessAccountInfo_ForceDenyTheseApps"=hex(7):00,00

; 18.8 Contacts. Prevent apps from accessing contacts
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessContacts"=dword:2

; 18.8 Contacts. Prevent apps from accessing contacts
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessContacts_UserInControlOfTheseApps"=hex(7):00,00

; 18.8 Contacts. Prevent apps from accessing contacts
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessContacts_ForceAllowTheseApps"=hex(7):00,00

; 18.8 Contacts. Prevent apps from accessing contacts
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessContacts_ForceDenyTheseApps"=hex(7):00,00

; 18.9 Calendar. Prevent apps from accessing calendar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCalendar"=dword:2

; 18.9 Calendar. Prevent apps from accessing calendar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCalendar_UserInControlOfTheseApps"=hex(7):00,00

; 18.9 Calendar. Prevent apps from accessing calendar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCalendar_ForceAllowTheseApps"=hex(7):00,00

; 18.9 Calendar. Prevent apps from accessing calendar
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCalendar_ForceDenyTheseApps"=hex(7):00,00

; 18.10 Call history. Prevent apps from accessing call history
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCallHistory"=dword:2

; 18.10 Call history. Prevent apps from accessing call history
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCallHistory_UserInControlOfTheseApps"=hex(7):00,00

; 18.10 Call history. Prevent apps from accessing call history
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCallHistory_ForceAllowTheseApps"=hex(7):00,00

; 18.10 Call history. Prevent apps from accessing call history
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessCallHistory_ForceDenyTheseApps"=hex(7):00,00

; 18.11 Email. Prevent apps from accessing emails
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessEmail"=dword:2
```

```
; 18.11 Email. Prevent apps from accessing emails
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessEmail_UserInControlOfTheseApps"=hex(7):00,00

; 18.11 Email. Prevent apps from accessing emails
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessEmail_ForceAllowTheseApps"=hex(7):00,00

; 18.11 Email. Prevent apps from accessing emails
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessEmail_ForceDenyTheseApps"=hex(7):00,00

; 18.12 Messaging. Prevent apps from accessing messages
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMessaging"=dword:2

; 18.12 Messaging. Prevent apps from accessing messages
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMessaging_UserInControlOfTheseApps"=hex(7):00,00

; 18.12 Messaging. Prevent apps from accessing messages
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMessaging_ForceAllowTheseApps"=hex(7):00,00

; 18.12 Messaging. Prevent apps from accessing messages
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMessaging_ForceDenyTheseApps"=hex(7):00,00

; 18.12 Messaging. Turn off Message Sync
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Messaging]
"AllowMessageSync"=dword:0

; 18.13 Phone calls. Prevent apps from accessing phone calls
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessPhone"=dword:2

; 18.13 Phone calls. Prevent apps from accessing phone calls
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessPhone_UserInControlOfTheseApps"=hex(7):00,00

; 18.13 Phone calls. Prevent apps from accessing phone calls
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessPhone_ForceAllowTheseApps"=hex(7):00,00

; 18.13 Phone calls. Prevent apps from accessing phone calls
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessPhone_ForceDenyTheseApps"=hex(7):00,00

; 18.14 Radios. Prevent apps from accessing radio
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessRadios"=dword:2

; 18.14 Radios. Prevent apps from accessing radio
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessRadios_UserInControlOfTheseApps"=hex(7):00,00

; 18.14 Radios. Prevent apps from accessing radio
```

```
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessRadios_ForceAllowTheseApps"=hex(7):00,00

; 18.14 Radios. Prevent apps from accessing radio
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessRadios_ForceDenyTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with unpaired devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsSyncWithDevices"=dword:2

; 18.15 Other devices. Prevent communications with unpaired devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsSyncWithDevices_UserInControlOfTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with unpaired devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsSyncWithDevices_ForceAllowTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with unpaired devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsSyncWithDevices_ForceDenyTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with tursted devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTrustedDevices"=dword:2

; 18.15 Other devices. Prevent communications with tursted devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTrustedDevices_UserInControlOfTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with tursted devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTrustedDevices_ForceAllowTheseApps"=hex(7):00,00

; 18.15 Other devices. Prevent communications with tursted devices
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTrustedDevices_ForceDenyTheseApps"=hex(7):00,00

; 18.16 Feedback & diagnostics. Turn off Feedback notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection]
"DoNotShowFeedbackNotifications"=dword:1

; 18.16 Feedback & diagnostics. Disable telemetry
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection]
"AllowTelemetry"=dword:0

; 18.16 Feedback & diagnostics. Turn off tailored experiences
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CloudContent]
"DisableWindowsConsumerFeatures"=dword:1

; 18.17 Background apps. Turn off background app
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsRunInBackground"=dword:2

; 18.17 Background apps. Turn off background app
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsRunInBackground_UserInControlOfTheseApps"=hex(7):00,00
```

```
; 18.17 Background apps. Turn off background app
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsRunInBackground_ForceAllowTheseApps"=hex(7):00,00

; 18.17 Background apps. Turn off background app
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsRunInBackground_ForceDenyTheseApps"=hex(7):00,00

; 18.18 Motion. Prevent apps from accessing motion data
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMotion"=dword:2

; 18.18 Motion. Prevent apps from accessing motion data
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMotion_UserInControlOfTheseApps"=hex(7):00,00

; 18.18 Motion. Prevent apps from accessing motion data
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMotion_ForceAllowTheseApps"=hex(7):00,00

; 18.18 Motion. Prevent apps from accessing motion data
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessMotion_ForceDenyTheseApps"=hex(7):00,00

; 18.19 Tasks. Prevent apps from accessing tasks
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTasks"=dword:2

; 18.19 Tasks. Prevent apps from accessing tasks
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTasks_UserInControlOfTheseApps"=hex(7):00,00

; 18.19 Tasks. Prevent apps from accessing tasks
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTasks_ForceAllowTheseApps"=hex(7):00,00

; 18.19 Tasks. Prevent apps from accessing tasks
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsAccessTasks_ForceDenyTheseApps"=hex(7):00,00

; 18.20 App Diagnostics. Prevent apps from accessing diagnostic information
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsGetDiagnosticInfo"=dword:2

; 18.20 App Diagnostics. Prevent apps from accessing diagnostic information
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsGetDiagnosticInfo_UserInControlOfTheseApps"=hex(7):00,00

; 18.20 App Diagnostics. Prevent apps from accessing diagnostic information
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsGetDiagnosticInfo_ForceAllowTheseApps"=hex(7):00,00

; 18.20 App Diagnostics. Prevent apps from accessing diagnostic information
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsGetDiagnosticInfo_ForceDenyTheseApps"=hex(7):00,00

; 18.21 Inking & Typing. Turn off Inking & Typing data collection
```

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\TextInput]
"AllowLinguisticDataCollection"=dword:0

; 18.22 Activity History. Turn off tracking of your Activity History
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"EnableActivityFeed"=dword:0

; 18.22 Activity History. Turn off tracking of your Activity History
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"PublishUserActivities"=dword:0

; 18.22 Activity History. Turn off tracking of your Activity History
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"UploadUserActivities"=dword:0

; 18.23 Voice Activation. Turn Off apps ability to listen for a Voice keyword
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsActivateWithVoice"=dword:2

; 18.23 Voice Activation. Turn Off apps ability to listen for a Voice keyword
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\AppPrivacy]
"LetAppsActivateWithVoiceAboveLock"=dword:2

; 18.24 News and interests. Disable Windows Feeds
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Feeds]
"EnableFeeds"=dword:00000000

; 19. Software Protection Platform. Turn off sending KMS client activation data to Microsoft
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform]
"NoGenTicket"=dword:1

; 20. Storage health. Turn off downloading updates to the Disk Failure Prediction Model
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\StorageHealth]
"AllowDiskHealthModelUpdates"=dword:0

; 21. Sync your settings. Turn off settings sync
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync]
"DisableSettingSync"=dword:2

; 21. Sync your settings. Turn off settings sync
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\SettingSync]
"DisableSettingSyncUserOverride"=dword:1

; 22. Teredo. Disable Teredo
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\TCPIP\v6Transition]
"Teredo_State"="Disabled"

; 23. Wi-Fi Sense. Turn off the feature
[HKEY_LOCAL_MACHINE\Software\Microsoft\wcmsvc\wifinetworkmanager\config]
"AutoConnectAllowedOEM"=dword:0

; 24. Microsoft Defender Antivirus. Disconnect from the Microsoft Antimalware Protection Service
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet]
```

```
"SpynetReporting"=dword:0

; 24. Microsoft Defender Antivirus. Stop sending file samples back to
Microsoft
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Spynet]
"SubmitSamplesConsent"=dword:2

; 24. Microsoft Defender Antivirus. Stop downloading Definition Updates
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Signature
Updates]
"FallbackOrder"="FileShares"

; 24. Microsoft Defender Antivirus. Stop downloading Definition Updates
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Signature
Updates]
"DefinitionUpdateFileSharesSources"="Nothing"

; 24. Microsoft Defender Antivirus. Turn off Malicious Software Reporting
Tool (MSRT) diagnostic data:
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\MRT]
"DontReportInfectionInformation"=dword:00000001

; 24. Microsoft Defender Antivirus. Turn off Enhanced Notifications
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\Reporting]
"DisableEnhancedNotifications"=dword:1

; 24.1 Microsoft Defender SmartScreen. Disable feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"EnableSmartScreen"=dword:0

; 24.1 Microsoft Defender SmartScreen. Disable feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\SmartScreen]
"ConfigureAppInstallControlEnabled"=dword:1

; 24.1 Microsoft Defender SmartScreen. Disable feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows Defender\SmartScreen]
"ConfigureAppInstallControl"="Anywhere"

; 24.1 Microsoft Defender SmartScreen. Disable feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"ShellSmartScreenLevel"=-

; 25. Personalized Experiences. Disable feature
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CloudContent]
"DisableCloudOptimizedContent"=dword:1

; 26. Microsoft Store. Disable all apps from Microsoft Store
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsStore]
"DisableStoreApps"=dword:1

; 26. Microsoft Store. Turn off Automatic Download and Install of updates.
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsStore]
"AutoDownload"=dword:2

; 27. Apps for websites. Turn off apps for websites
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"EnableAppUriHandlers"=dword:0
```

```
; 28.3. Delivery Optimization. (simple mode) prevent P2P traffic
; Value is Hex 63 = 99 decimal
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeliveryOptimization]
"DODownloadMode"=dword:63

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"DoNotConnectToWindowsUpdateInternetLocations"=dword:1

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"DisableWindowsUpdateAccess"=dword:1

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"WUServer"=" "

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"WUStatusServer"=" "

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"UpdateServiceUrlAlternate"=" "

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU]
"UseWUServer"=dword:1

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"FillEmptyContentUrls"=-

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"DoNotEnforceEnterpriseTLSCertPinningForUpdateDetection"=-

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate]
"SetProxyBehaviorForUpdateDetection"=dword:0

; 29. Windows Update. Turn off
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsStore\Wi
ndowsUpdate]
"AutoDownload"=dword:00000005

; 30. Cloud Clipboard
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System]
"AllowCrossDeviceClipboard"=dword:0

; 31. Services Configuration. Turn off
[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DataCollection]
"DisableOneSettingsDownloads"=dword:00000001
```

Приложение 3. PowerShell-скрипт, удаляющий ВСЕ встроенные приложения

Примечание. Будьте аккуратны с переносами строк.

```
get-AppxPackage | Remove-AppxPackage
$packs = Get-AppxProvisionedPackage -online | Select-Object PackageName
foreach ($pack in $packs) {Remove-AppxProvisionedPackage -online -PackageName
$pack.PackageName}
get-AppxPackage -allusers | Remove-AppxPackage

'Uninstalling OneDrive...'
taskkill.exe /F /IM "OneDrive.exe"
& "$env:systemroot\SysWOW64\OneDriveSetup.exe" /uninstall
'... waiting until OneDrive will be uninstalled ....'
while (Test-Path $env:LOCALAPPDATA\Microsoft\OneDrive\OneDrive.exe) { Start-
Sleep 1 }
'... OneDrive Uninstalling complete!'
```

Приложение 4. PowerShell-скрипт, устанавливающий признак лимитированного соединения

Примечание. Будьте аккуратны с переносами строк.

```
<#
.SYNOPSIS : PowerShell script to set Ethernet connection as metered or not
metered

.AUTHOR : Michael Pietroforte

.SITE : https://4sysops.com
#>

#We need a Win32 class to take ownership of the Registry key
$definition = @"
using System;
using System.Runtime.InteropServices;

namespace Win32Api
{

public class NtDll
{
[DllImport("ntdll.dll", EntryPoint="RtlAdjustPrivilege")]
public static extern int RtlAdjustPrivilege(ulong Privilege, bool Enable,
bool CurrentThread, ref bool Enabled);
}
}
"@

Add-Type -TypeDefinition $definition -PassThru | Out-Null
[Win32Api.NtDll]::RtlAdjustPrivilege(9, $true, $false, [ref]$false) | Out-
Null

#Setting ownership to Administrators
$key =
[Microsoft.Win32.Registry]::LocalMachine.OpenSubKey("SOFTWARE\Microsoft\Windo
ws
NT\CurrentVersion\NetworkList\DefaultMediaCost",[Microsoft.Win32.RegistryKeyP
ermissionCheck]::ReadWriteSubTree,[System.Security.AccessControl.RegistryRigh
ts]::takeownership)
$acl = $key.GetAccessControl()
$acl.SetOwner([System.Security.Principal.NTAccount]"Administrators")
$key.SetAccessControl($acl)

#Giving Administrators full control to the key
$rule = New-Object System.Security.AccessControl.RegistryAccessRule
([System.Security.Principal.NTAccount]"Administrators","FullControl","Allow")
$acl.SetAccessRule($rule)
$key.SetAccessControl($acl)

#Setting Ethernet as metered or not metered
$path = "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\NetworkList\DefaultMediaCost"
$name = "Ethernet"
$metered = Get-ItemProperty -Path $path | Select-Object -ExpandProperty $name
```

```
New-ItemProperty -Path $path -Name $name -Value "2" -PropertyType DWORD -
Force | Out-Null
Write-Host "Ethernet is now set to metered."
```

Приложение 5. PowerShell-скрипт, отключающий службы обновления MS Edge

Примечание. Будьте аккуратны с переносами строк.

```
'Killing MS Edge processes...'
C:\Windows\System32\taskkill.exe /F /IM "msedge.exe"

'Stroping MS Edge update related services...'
C:\Windows\System32\net.exe stop MicrosoftEdgeElevationService
C:\Windows\System32\net.exe stop edgeupdate
C:\Windows\System32\net.exe stop edgeupdatem

'Disabling MS Edge update related services...'
C:\Windows\System32\sc.exe config MicrosoftEdgeElevationService obj= .\Guest
start= disabled
C:\Windows\System32\sc.exe config edgeupdate obj= .\Guest start= disabled
C:\Windows\System32\sc.exe config edgeupdatem obj= .\Guest start= disabled

'Removing MS Edge update related Scheduler Tasks...'
Get-ScheduledTask -TaskName "*EdgeUpdate*" | Unregister-ScheduledTask -
Confirm:$false
```

Приложение 6. REG-файл, отключающий Windows Defender

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender]
"DisableAntiSpyware"=dword:00000001
```