

ДИАГНОСТИКА NAT C УСТАНОВЛЕННЫМ TRAFFIC INSPECTOR

Перед диагностикой NAT необходимо отключить службу Traffic Inspector.

Подготовка к диагностике NAT, отключение Traffic Inspector

1. Для отключения Traffic Inspector, запустите консоль управления Traffic Inspector. Нажмите правой кнопкой мыши на разделе «Traffic Inspector [LOCAL]» и в контекстном меню выберите пункт «Свойства».

2. На вкладке «Сетевой драйвер» снимите галку с «Блокировать внешнюю сеть при остановке службы программы».

	Общие настройки программы
Общие н	настройки программы
Сетевой драйвер	✓ Учитывать заголовки Ethernet
Параметры очередей	Учитываются допольнительные 14 байт заголовка пакета. Отключите, если необходимо учитывать чистый IP трафик.
Сетевая статистика	□Блокировать фрагменты IP пакетов
Распознавание имен	Блокировать внешнюю сеть при остановке службы
Журналы	программы
Оповещение	Включите для предотвращения бесконтрольного потребления трафика при остановке службы программы.
Автоматизация	Блокировка производится на уровне драйвера программы только для интерфейсов, назначенных как внешние.
Счетчики скорости	□ Пропускать IPv6 пакеты
Дополнительно	Правило обработки IPv6 трафика. Отключите, если необходимо блокировать IPv6 пакеты на внешнем интерфейсе.
	Вести учет отбращений во внешнюю сеть от неавторизованных пользователей
Помощь	ОК Отмена

3. Остановите службу. Это можно сделать в самой консоли Traffic Inspector, выделив корень консоли Traffic Inspector [LOCAL] и нажав кнопку «Стоп», или через консоль «Службы» операционной системы (Панель управления → Администрирование → Службы).



		Службы				- 🗆 X
⊉айл Действие	<u>Вид С</u> правка					
• 🔿 🗖 🗇 (Q 😼 🚺 📰 🕨 💷 🕪					
Службы (локаль	Службы (локальные)					
	Traffic Inspector	Имя	Описание	Состояние	Тип запуска	Вход от имен
		ОНСР-клиент	Регистрирует и обновляет IP-адреса	Выполняется	Автоматиче	Локальная с
	Остановить службу	🖏 DNS-клиент	Служба DNS-клиента (dnscache) кэш	Выполняется	Автоматиче	Сетевая слу
	Приостановить службу	🔍 KtmRm для координатора распределенных	Координирует транзакции между MS		Вручную (ак	Сетевая слу
	Перезапустить службу	🕞 Plug and Play	Позволяет компьютеру распознават	Выполняется	Вручную	Локальная с
		🍓 SMP дисковых пространств (Майкрософт)	Служба узла для поставщика управл		Вручную	Сетевая слу:
	Описание:	💁 Superfetch	Поддерживает и улучшает производ		Вручную	Локальная с
	Прокси сервер, контроль трафика,	Caraffic Inspector	Прокси сервер, контроль трафика, с	Выполняется	Автоматиче	Локальная с
	сетевой экран	🔍 VirtualBox Guest Additions Service	Manages VM runtime information, tim	Выполняется	Автоматиче	Локальная с
		🔍 Windows Audio	Управление средствами работы со з		Вручную	Локальная с
		🔍 Windows Driver Foundation - User-mode Driv	Создает процессы драйверов пользо		Вручную (ак	Локальная с
		🔍 Агент защиты сетевого доступа	Агент службы защиты доступа к сети		Вручную	Сетевая слу
		🔍 Агент карантина для удаленного доступа	Удаляет проверенные клиенты удале		Вручную	Локальная с
		🔍 Агент политики IPsec	Безопасность протокола IP (IPsec) по	Выполняется	Вручную (ак	Сетевая слу
		Адаптер производительности WMI	Предоставляет сведения библиотеки		Вручную	Локальная о
		🔍 Брандмауэр Windows	Брандмауэр Windows помогает пред	Выполняется	Автоматиче	Локальная о
		🔍 Браузер компьютеров	Обслуживает список компьютеров в		Отключена	Локальная
		🔍 Брокер системных событий	Координирует выполнение фоновой	Выполняется	Автоматиче	Локальная
		🔍 Быстрая проверка	Проверяет потенциальные поврежде		Вручную (ак	Локальная
		🔍 Виртуальный диск	Предоставление служб управления д		Вручную	Локальная о
		🔍 Внутренняя база данных Windows	Обеспечивает поддержку служб внут	Выполняется	Вручную	NT SERVICE
		🏐 Вспомогательная служба IP	Обеспечивает возможность туннель	Выполняется	Автоматиче	Локальная с
		<	2 III			>
m N	Расширенный (Стандартный /					

Traffic Inspector остановлен и можно производить диагностику настроек ОС.

Диагностика NAT

Для проверки правильности настроек NAT используется «Командная строка». Проверку производят на клиентской машине, но, если вы в чем-то сомневаетесь, не поленитесь проверить на всех.

1. Зайдите в Пуск \rightarrow Программы \rightarrow Стандартные, и запустите «Командную строку». Также можете её открыть, набрав cmd в Пуск \rightarrow Выполнить. Путь, который высветиться по умолчанию не важен.



2. Сначала проверим доступность сервера с Traffic Inspector, пусть он у нас находиться по адресу 10.0.1.1, для этого напишем «ping 10.0.1.1». Если пинг прошел (см рис.), то локальная сеть у нас работает без проблем. Если пишет «Превышен интервал ожидания для запроса» или «Заданный узел не доступен», необходимо проверить настройки сети.

C:\Win	dows\system32\cmd.exe	_ 🗆 X
Microsoft Windows [Version 6.3.960 (с) Корпорация Майкрософт (Microso	0] ft Corporation), 2013. Все права	защищены. 🔒
C:\Users\Test_Admin>ping 10.0.1.1		
Обмен пакетами с 10.0.1.1 по с 32 Ответ от 10.0.1.1: число байт=32 в Ответ от 10.0.1.1: число байт=32 в Ответ от 10.0.1.1: число байт=32 в Ответ от 10.0.1.1: число байт=32 в	байтами данных: ремя<1мс TTL=128 ремя<1мс TTL=128 ремя<1мс TTL=128 ремя<1мс TTL=128 ремя<1мс TTL=128	
Статистика Ping для 10.0.1.1: Пакетов: отправлено = 4, получ (Ох потерь)	ено = 4, потеряно = 0	
Приблизительное время приема-перед Минимальное = Омсек, Максималь	ачи в мс: ное = О мсек, Среднее = О мсек	
C:\Users\Test_Admin>		
		×

3. Далее надо проверить доступность внешнего интерфейса сервера, для этого мы должны знать его адрес. Если он вам известен – данный пункт можно пропустить. Иначе его можно узнать, набрав в командной строке на сервере «ipconfig/all».

Здесь мы увидим название нашего подключения к Интернету и его IP адрес.

```
x
C:4.
                    Администратор: C:\Windows\system32\cmd.exe
                                                                               ~
C:\Users\Администратор>ipconfig /all
Настройка протокола IP для Windows
  ..... WIN-GJ2891FSOGS
Ethernet adapter WAN:
  Ethernet adapter Office:
  DNS-суффикс подключения . . . .
  Описание. . . . . . . . . . . . Адаптер рабочего стола Intel(R) PRO/1000
MT
  Физический адрес. . . . . . . . . .
                                     08-00-27-0E-1C-0B
  Основной шлюз.
NetBios через TCP/IP. . . . . . : Включен
Туннельный адаптер isatap.{C116F327-65C3-4A7A-BC61-77558C5CE806}:
  Состояние среды. . . . . . . Среда передачи недоступна.
  Адаптер Microsoft ISATAP
00-00-00-00-00-00-00-00-E0
Нет
                                     Дa
Туннельный адаптер isatap.office.local:
                                                                              Ξ
  Состояние среды. . . . . . : Среда передачи недоступна.
DNS-суффикс подключения . . . . : office.local
Описание. . . . . . : Адаптер Microsoft ISATAP #2
Физический адрес. . . . . . : 00-00-00-00-00-00-E0
DUCP вистический адрес. . . . . . : 00-00-00-00-00-00-E0
  Нет
C:\Users\Администратор}_
```

Также можно зайти в Пуск → Панель Управления → Центр управления сетями и общим доступом → Изменение параметров адаптера, далее перейти в свойства интересующего адаптера нажать «Сведения...»

Q	Состояние -	WAN	x
Общие			
Подключен	ие		-
IPv4-под	ключение:	Интернет	
IPv6-под	ключение:	Без доступа к сети	
Состоян	ие среды:	Подключено	
Длитель	ность:	00:37:13	
Скорости	ь:	1.0 Гбит/с	
<u>С</u> веден Активность	ия		_
	Отправлено —	— Принято	
Байт:	9 813 693	69 112 262	
Свойст	гва <u>இ</u> Отключить	Диа <u>г</u> ностика	
		<u>З</u> акры	ть

4. Предположим, IP-адрес внешнего интерфейса – 10.0.2.2. На клиентской машине в командной строке набираем «ping 10.0.2.2». Если на запросы приходит стабильный ответ, то связь с внешним интерфейсом установлена. Если ответа нет, необходимо проверить настройки ICS или RRAS, а также проверить, прописаны ли шлюз и DNS на клиентской машине (в настройках протокола TCP/IP).

C:\Windows\system32\cmd.exe	_ 🗆 X
C:\Users\Test_Admin>ping 10.0.2.2 Обмен пакетами с 10.0.2.2 по с 32 байтами данных: Ответ от 10.0.2.2: число байт=32 время=14мс TTL=124 Ответ от 10.0.2.2: число байт=32 время<1мс TTL=124	
Приблизительное время приема-передачи в мс: Минимальное = Омсек, Максимальное = 14 мсек, Среднее = 3 мсе C:\Users\Test_Admin>	к

5. Проверим доступность сети Интернет. Для этого запустим пинг до IP 8.8.8.8 с клиента: «ping 8.8.8.8». В случае стабильного ответа можно сделать вывод, что NAT сконфигурирован правильно.



6. Запустим пинг до google.com с клиента: «ping google.com». В случае стабильного ответа можно сделать вывод, что DNS сконфигурирован правильно. Если в командной строке сообщение «google.com: неизвестный узел» нужно проверить настройки DNS. В случае если пишет «Превышен интервал ожидания для запроса»: запустите пинг до «google.com» с сервера.

Car.	C:\Windows\system32\cmd.exe	 x
C:\Users\Test_Admin>ping	google.com	^
Обмен пакетами с google.c Ответ от 87.245.196.59: ч Ответ от 87.245.196.59: ч Ответ от 87.245.196.59: ч Ответ от 87.245.196.59: ч Ответ от 87.245.196.59: ч	от [87.245.196.59] с 32 байтами данных: исло байт=32 время=11мс TTL=58 исло байт=32 время=10мс TTL=58 исло байт=32 время=10мс TTL=58 исло байт=32 время=11мс TTL=58	Ξ
Статистика Ping для 87.24 Пакетов: отправлено = (О% потерь) Приблизительное время при Минимальное = 10мсек, C:\Users\Test_Admin}_	5.196.59: 4, получено = 4, потеряно = 0 ема-передачи в мс: Максимальное = 11 мсек, Среднее = 10 мсек	
		~

Далее следует проверить работу приложения, оно должно работать без каких-либо особенных настроек (используется прямое подключение).

Если приложение сообщает об ошибках соединения, вам необходимо отделить проблемы Интернет от проблем самого клиентского приложения. Для этого используйте telnet (имеется на всех версиях Windows, утилита telnet.exe) для проверки доступности TCP-соединений с сервером.

Пример:

Проверка SMTP (протокол отправки почтовых сообщений) с сервера mail.ru.



При проблемах с соединением у вас появиться сообщение о неудаче, а в случае успеха соединения – сообщение следующего вида:

	Telnet smtp.mail.ru	 x
220 smtp42.i.mail.ru ESMTP ready		^
		=
		~

Для проверки соединения, которое использует ваша программа, необходимо знать имя сервера и используемый порт (протокол). Сама проверка будет в таком виде:

telnet <имя сервера> <номер порта>

Если соединение устанавливается, то проблем с настройками сети нет, проверьте настройки Вашего приложения.

Если соединение не устанавливается, возможна проблема с тем сервером, которое использует приложение.

После проведения диагностики запустите службу Traffic Inspector на сервере, включите обратно «Блокировать внешнюю сеть при остановке службы программы». Если проблема с приложением опять появилась, то следующим шагом вам необходимо проверить авторизацию пользователя, который работает с этим приложением.