Настройка NTP (Network Time Protocol) на «С-Терра Шлюз»

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.
Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Логика работы NTP

NTP – протокол для синхронизации внутренних часов компьютера по сети.

«С-Терра Шлюз» версии 5.0 (далее криптошлюз) может выступать одновременно в качестве NTP клиента и сервера.

В данной инструкции предполагается, что NTP сервер (который также является клиентом) настраивается на криптошлюзе (его IP-адрес `192.168.1.1`) в условном центре, а NTP клиентами являются криптошлюзы, установленные в условных филиалах.

В случае если на ПАК настроен DHCP клиент, если DHCP сервер передаёт ему настройки NTP, сервера, с которыми будет происходить синхронизация, будут определяться DHCP сервером.
- Для того, чтобы игнорировать настройки NTP от DHCP сервера, следует в файле `/etc/default/ntpsec` выставить опцию `IGNORE_DHCP` в значение `yes` (`IGNORE_DHCP="yes"`);
- Если же требуется, чтобы применялись настройки от DHCP сервера, рекомендуется к прочтению пункт главы «Примечание» Получение настроек NTP через DHCP.
В общем случае рекомендуется настраивать NTP **либо** через Cisco-like, **либо** через файлы конфигурации, **либо** получать настройки по DHCP.

Рассматривается два основных варианта настроек – при помощи Cisco-like консоли (без аутентификации) и через системные файлы конфигурации (с возможностью настройки аутентификации по симметричному ключу).

Настоятельно рекомендуется защищать обмен протокола NTP при помощи IPsec, так как встроенной аутентификации в протоколе NTP недостаточно для обеспечения надлежащей защиты.

Особенность использования NTP

Особенность связана с использованием сервиса NTP (например, реализации `ntpsec` или `ntp`).

Независимо от того, работает ли сервис NTP в роли клиента или сервера, синхронизация времени выполняется периодически и только в том случае, если разница между локальным временем устройства и временем сервера не превышает 1000 секунд.

Если смещение превышает указанный порог, сервис завершает работу и фиксирует ошибку в системном журнале (в файл `/var/log/syslog` по умолчанию).

Для восстановления корректной работы достаточно перезапустить сервис NTP — при запуске (или перезапуске) ограничение по смещению времени не применяется, и синхронизация выполняется успешно.

Пример настройки NTP при помощи Cisco-like

- На данный момент через Cisco-like консоль аутентификация NTP сервера не настраивается. Также как и ограничения доступа по адресу;
- Если для настройки NTP используется Cisco-like консоль, вносить изменения в файлы конфигурации вручную не рекомендуется.

Пример настройки NTP клиента

В данной главе настройки NTP клиента предполагается, что NTP сервер уже настроен.

Предварительные требования

Устройства С-Терра Шлюз должны быть инициализированы (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Инициализация С-Терра Шлюз»).

Настройки

1. Перейдите в Cisco-like консоли в режим конфигурирования и добавьте нужный NTP сервер, с которым будет производиться синхронизация по времени:

```
administrator@sterragate] configure
sterragate login: cscons
Password:
```

```
S-Terra Gate 5.0.XXXXX (amd64)
Linux sterragate X.X.X-XstX-amd64 #1 SMP PREEMPT_DYNAMIC Debian X.X.X-X+bX+sterraX
(XXXX-XX-XX) x86_64
```

```
sterragate#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
sterragate(config)#ntp server 192.168.1.1 iburst
sterragate(config)#exit
sterragate#
```

После проведённой конфигурации сервис NTP будет перезапущен и впоследствии будет автоматически запускаться после перезагрузки криптошлюза.

2. Для проверки подождите 1 – 3 минуты и выполните команду:

```
sterragate#show ntp associations
```

```
     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
*192.168.1.1     81.200.28.110    3 u  183 1024  377   0.3669   2.1033   2.0665
```

Обратите внимание на звездочку (*), которая говорит о том, что синхронизация производится с данного сервера.

Пример настройки NTP сервера

Предварительные требования

1. Устройства С-Терра Шлюз должны быть инициализированы (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз 5.0 -> «Инициализация С-Терра Шлюз»).
2. На криптошлюзе должен быть открыт порт 123 протокола UDP (по умолчанию открыт).
3. На криптошлюзе должен быть настроен соответствующий часовой пояс:

```
root@sterragate:~# dpkg-reconfigure tzdata
root@sterragate:~# exit
```

4. На криптошлюзе должны быть заданы рабочие DNS сервера:

```
administrator@sterragate] configure
sterragate login: cscons
Password:
```

```
S-Terra Gate 5.0.XXXXX (amd64)
Linux sterragate X.X.X-XstX-amd64 #1 SMP PREEMPT_DYNAMIC Debian X.X.X-X+bX+sterraX
(2023-11-03) x86_64
```

```
sterragate#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
sterragate(config)#ip name-server 77.88.8.8 77.88.8.1
sterragate(config)#exit
sterragate#exit
root@sterragate:~# exit
```

В примере заданы DNS сервера Яндекс (https://dns.yandex.ru/).

Настройки

1. Перейдите в Cisco-like консоли в режим конфигурирования и добавьте нужные NTP сервера, с которыми будет производиться синхронизация по времени (сервера представлены только в качестве примера):

```
administrator@sterragate] configure
sterragate login: cscons
Password:
```

```
S-Terra Gate 5.0.XXXXX (amd64)
Linux sterragate X.X.X-XstX-amd64 #1 SMP PREEMPT_DYNAMIC Debian X.X.X-X+bX+sterraX
(XXXX-XX-XX) x86_64
```

```
sterragate#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
sterragate(config)#ntp server 0.ru.pool.ntp.org iburst
sterragate(config)#ntp server 1.ru.pool.ntp.org iburst
sterragate(config)#ntp server 2.ru.pool.ntp.org iburst
sterragate(config)#ntp server 3.ru.pool.ntp.org iburst
sterragate(config)#exit
sterragate#
```

Если не требуется задание специфичных серверов, можно вместо команд `ntp server <имя_сервера>` воспользоваться следующей командой `ntp default servers`
Команда добавит в конфигурацию Cisco-like сервера `vniiftri.ru`.
Также эту команду можно ввести в дополнение к уже имеющимся серверам.
Данная команда не отображается в конфигурации Cisco-like и не имеет отменяющего аналога (команды `no ntp default servers` не существует). Если требуется удалить эти сервера, следует посмотреть конфигурацию Cisco-like и удалить их, используя команды `no ntp server <имя_сервера>`.

После проведённой конфигурации сервис NTP будет перезапущен и впоследствии будет автоматически запускаться после перезагрузки криптошлюза.

2. Для проверки подождите 1 – 3 минуты и выполните следующую команду (пример вывода приведён без `ntp default servers`):

```
sterragate#show ntp associations
```

```
     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
 0.ru.pool.ntp.o .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 1.ru.pool.ntp.o .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 2.ru.pool.ntp.o .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 3.ru.pool.ntp.o .POOL.          16 p    -  256    0   0.0000   0.0000   0.0001
 95.31.7.160     .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
```

```
 37.79.216.163   83.143.51.50     2 u    5   64    1  31.3153  -2.0856   1.2279
*188.120.233.26  130.173.91.58    2 u    5   64    1   3.4317  -3.2398   0.6456
 185.5.250.181   94.198.132.184   2 u    5   64    1   3.4447  -1.1361   0.1489
 213.234.203.30  .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
+162.159.200.123 10.216.8.4       3 u    4   64    1  43.9884  -3.2611   1.0092
 213.33.141.134  204.9.54.119     2 u    4   64    1  10.5654  -1.4555   0.9358
-94.229.247.207  118.143.17.83    2 u    4   64    1 113.8545  -4.0258   0.9184
+193.192.36.3    194.190.168.1    2 u    3   64    1  18.5498  -3.1771   1.2279
 185.68.101.2    10.0.10.101      2 u    1   64    1  29.5622  -2.8393   0.4346
 195.218.227.230 .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
 91.207.136.55   .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
 2606:4700:f1::1 .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
 2a00:ab00:203:9 .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
 2a01:230:4:8d0: .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
 2a00:1390:5:722 .STEP.          16 u    -   64    0   0.0000   0.0000   0.0001
+217.10.42.30    89.109.251.22    2 u   19   64    1  15.9403  -5.8266   1.0320
-82.142.168.18   204.9.54.119     2 u   23   64    1   9.6860   0.2271   0.9221
```

Обратите внимание на звездочку (*), которая говорит о том, что синхронизация производится с данного сервера.

Примеры конфигураций

Ниже приведены частичные выводы команды `show running-config`, относящиеся к настройкам NTP.

Клиент

```
...
!
ntp server 192.168.1.1
...
```

Сервер

Без `ntp default servers`

```
...
!
ntp server 0.ru.pool.ntp.org
ntp server 1.ru.pool.ntp.org
ntp server 2.ru.pool.ntp.org
ntp server 3.ru.pool.ntp.org
...
```

После выполнения `ntp default servers`

```
...
!
ntp server 0.ru.pool.ntp.org
ntp server 1.ru.pool.ntp.org
ntp server 2.ru.pool.ntp.org
ntp server 3.ru.pool.ntp.org
ntp server ntp1.vniiftri.ru iburst
ntp server ntp2.vniiftri.ru iburst
ntp server ntp3.vniiftri.ru iburst
ntp server ntp4.vniiftri.ru iburst
...
```

Пример настройки NTP через системные файлы конфигурации

- Для криптошлюза «С-Терра Шлюз» версии (5.0 KB) настройки, описанные в данной главе, отличаются от настроек для других версий криптошлюза. Отличие связано с использованием службы `ntp` вместо

`ntpsec`. При выполнении настроек NTP клиента и сервера необходимо учитывать используемую версию криптошлюза.

- Если настройка NTP производится через системные файлы конфигурации, вносить изменения в конфигурацию с использованием Cisco-like консоли не рекомендуется.
- Настройки NTP рекомендуется проводить в директории `/etc/ntpsec/ntp.conf.d/` в отдельном файле. Если используете криптошлюз версии (5.0 KB), то настройки NTP рекомендуется проводить в директории `/etc/ntp.conf.d/` также в отдельном файле. В примере настроек ниже это файл `custom_ntp.conf`

Пример настройки NTP клиента

В данной главе настройки NTP клиента предполагается, что NTP сервер уже настроен.

Предварительные требования

Требования соответствуют требованиям из раздела «Предварительные требования» главы с настройками NTP клиента при помощи Cisco-like.

Настройки

1. Проверьте, что в выводе команды `show running-config` в Cisco-like консоли нет настроек NTP.

   Если настройки имеются, то перейдите в Cisco-like консоли в режим конфигурирования и удалите все NTP сервера.

2. Проверьте, что в конфигурационном файле `/etc/ntpsec/ntp.conf.d/st_ntp.conf` службы `ntpsec` нет настроек NTP. Если настройки есть, удалите их.

   Если используете криптошлюз версии (5.0 KB), то проверьте конфигурационный файл `/etc/ntp.conf.d/st_ntp.conf` на наличие настроек NTP. Если настройки есть, удалите их.

3. Добавьте в конфигурационный файл `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` (если файл отсутствует, создайте его самостоятельно) следующие строки:

   ```
   root@sterragate:~# vim.tiny /etc/ntpsec/ntp.conf.d/custom_ntp.conf
   server 192.168.1.1 iburst
   ```

   где:

   - `server 192.168.1.1 iburst` – указываем сервер, с которым будет производиться синхронизация времени (`192.168.1.1` – IP- адрес криптошлюза с настроенным NTP сервером).
   - Опция `iburst` позволяет запускать быструю последовательность пакетов в случае, если сервер недоступен. В частности, при старте сервиса. Это позволяет пройти начальную синхронизацию быстрее.
     Для бóльших подробностей смотрите описание параметров по ссылке: https://manpages.debian.org/bookworm/ntpsec/ntp.conf.5.en.html

   Если используете криптошлюз версии (5.0 KB), то добавьте в конфигурационный файл `/etc/ntp.conf.d/custom_ntp.conf` (если файл отсутствует, создайте его самостоятельно) следующие строки:

   ```
   root@sterragate:~# vim.tiny /etc/ntp.conf.d/custom_ntp.conf
   server 192.168.1.1 iburst
   ```

4. Перезагрузите службу `ntpsec`:

   ```
   root@sterragate:~# systemctl restart ntpsec.service
   ```

   Если используете криптошлюз версии (5.0 KB), то перезагрузите службу `ntp`:

   ```
   root@sterragate:~# systemctl restart ntp.service
   ```

5. Подождите 1 – 3 минуты и выполните команду:

   ```
   root@sterragate:~# ntpq -p
   ```

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.1.1     81.200.28.110    3 u   21   64    3    0.2171  -2.9221   5.3415
```

Обратите внимание на звездочку (*), которая говорит о том, что синхронизация производится с данного сервера.

6. Для того чтобы служба `ntpsec` запускалась после перезагрузки системы, выполните команду:

```
root@sterragate:~# systemctl enable ntpsec.service
```

Если используете криптошлюз версии (5.0 КВ), то для того чтобы служба `ntp` запускалась после перезагрузки системы, выполните команду:

```
root@sterragate:~# systemctl enable ntp.service
```

Пример настройки NTP сервера

Предварительные требования

Требования соответствуют требованиям из раздела «Предварительные требования» главы с настройками NTP сервера при помощи Cisco-like.

Настройки

1. Проверьте, что в выводе команды `show running-config` в Cisco-like консоли нет настроек NTP.

   Если настройки имеются, то перейдите в Cisco-like консоли в режим конфигурирования и удалите все NTP сервера.

2. Проверьте, что в конфигурационном файле `/etc/ntpsec/ntp.conf.d/st_ntp.conf` службы `ntpsec` нет настроек NTP. Если настройки есть, удалите их.

   Если используете криптошлюз версии (5.0 КВ), то проверьте конфигурационный файл `/etc/ntp.conf.d/st_ntp.conf` на наличие настроек NTP. Если настройки есть, удалите их.

3. Добавьте в конфигурационный файл `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` (если файл отсутствует, создайте его самостоятельно) следующие строки:

```
root@sterragate:~# vim.tiny /etc/ntpsec/ntp.conf.d/custom_ntp.conf
```

```
pool 0.ru.pool.ntp.org iburst
pool 1.ru.pool.ntp.org iburst
pool 2.ru.pool.ntp.org iburst
pool 3.ru.pool.ntp.org iburst
```

где:

- `pool 0.ru.pool.ntp.org iburst` – указываем сервер, с которым будет производиться синхронизация времени.

`pool` здесь используется вместо `server` по той причине, что за указанным адресом может находиться набор NTP серверов. Тем не менее, даже если это не так, настройка будет работать нормально.

Для бóльших подробностей смотрите описание параметров по ссылке: https://manpages.debian.org/bookworm/ntpsec/ntp.conf.5.en.html

Если используете криптошлюз версии (5.0 КВ), то добавьте в конфигурационный файл `/etc/ntp.conf.d/custom_ntp.conf` (если файл отсутствует, создайте его самостоятельно) следующие строки:

```
root@sterragate:~# vim.tiny /etc/ntp.conf.d/custom_ntp.conf
```

```
pool 0.ru.pool.ntp.org iburst
pool 1.ru.pool.ntp.org iburst
```

```
pool 2.ru.pool.ntp.org iburst
pool 3.ru.pool.ntp.org iburst
```

4. Перезагрузите службу `ntpsec`:

```
root@sterragate:~# systemctl restart ntpsec.service
```

Если используете криптошлюз версии (5.0 KB), то перезагрузите службу `ntp`:

```
root@sterragate:~# systemctl restart ntp.service
```

5. Подождите 1 – 3 минуты и выполните команду:

```
root@sterragate:~# ntpq -p
```

```
     remote           refid      st t when poll reach   delay   offset   jitter
==============================================================================
 0.ru.pool.ntp.o .POOL.          16 p    -  256    0    0.0000    0.0000   0.0001
 1.ru.pool.ntp.o .POOL.          16 p    -  256    0    0.0000    0.0000   0.0001
 2.ru.pool.ntp.o .POOL.          16 p    -  256    0    0.0000    0.0000   0.0001
 3.ru.pool.ntp.o .POOL.          16 p    -  256    0    0.0000    0.0000   0.0001
+tms04.deltatele .GPS.            1 u    9   64    1   38.3147   -0.3201   1.9198
+dynamicip-176-2 89.109.251.22    2 u    9   64    1    7.3458   -2.0897   2.9438
+188.126.46.67   89.109.251.21    2 u    9   64    1    7.8056   -1.4804   2.9773
#195.218.227.230 85.21.78.91      3 u    9   64    1   31.3259    0.6234   1.8605
+89-179-240-219. 89.109.251.24    2 u    8   64    1    9.9406   -1.2590   1.8534
+nsa.lds.net.ua  194.190.168.1    2 u   10   64    1   18.1762   -1.2162   0.8712
#217.10.42.30    89.109.251.22    2 u   10   64    1   15.5988   -4.8764   0.7180
+95-31-7-160.sta 82.209.210.87    2 u    8   64    1    9.5143   -1.1946   1.5446
#yggnode.cf      194.190.168.1    2 u    7   64    1   22.3861    1.3434   2.2339
#time100.stupi.s .PPS.            1 u    9   64    1  135.9212  -35.4851   0.5526
+atomail.ru      130.173.91.58    2 u    9   64    1    7.8867   -2.9506   2.1651
+time.cloudflare 10.214.8.6       3 u    7   64    1   44.3837   -1.3591   2.0419
 2a03:aa00::136: .INIT.          16 u    -   64    0    0.0000    0.0000   0.0001
 time.cloudflare .INIT.          16 u    -   64    0    0.0000    0.0000   0.0001
 2a00:ab00:203:9 .INIT.          16 u    -   64    0    0.0000    0.0000   0.0001
 2a00:1390:5:722 .INIT.          16 u    -   64    0    0.0000    0.0000   0.0001
-home.ostankin.n 89.109.251.24    2 u    6   64    1   17.5403   -1.0695   1.1166
*ntp.ix.ru       .GLN.            1 u    6   64    1   47.5017    0.2976   1.2444
#h195-3-218-2.ke 185.68.101.2     3 u    6   64    1   56.3700   -3.1215   1.8400
+time.cloudflare 10.216.8.4       3 u    6   64    1   45.4619   -1.7648   1.0959
```

Обратите внимание на звездочку (*), которая говорит о том, что синхронизация производится с данного сервера.

6. Для того чтобы служба `ntpsec` запускалась после перезагрузки системы, выполните команду:

```
root@sterragate:~# systemctl enable ntpsec.service
```

Если используете криптошлюз версии (5.0 KB), то для того чтобы служба `ntp` запускалась после перезагрузки системы, выполните команду:

```
root@sterragate:~# systemctl enable ntp.service
```

Пример настройки аутентификации

В случае, если требуется, чтобы связь между клиентом и сервером была аутентифицирована, можно воспользоваться симметричным ключом, добавив в конфигурацию настройки, приведённые ниже.

Настройки, приведенные ниже, требуется провести как на клиенте, так и на сервере.

1. Создайте файл `/etc/ntpsec/ntp.keys` с ключами и добавьте в него ключ:

Идентификатор ключа `key ID`, алгоритм хеширования `hash algorithm` и сам ключ `key` должны быть одинаковыми как на сервере, так и на клиенте (в данном примере ключ это слово `secret`).

```
root@sterragate:~# vim.tiny /etc/ntpsec/ntp.keys
```

```
# key ID | hash algorithm | key
1 MD5 secret
```

В качестве алгоритма хеширования поддерживается только MD5. Длина пароля ограничена 20 символами ASCII.

Если используете криптошлюз версии (5.0 KB), то создайте файл `/etc/ntp.keys` с ключами и добавьте в него ключ:

```
root@sterragate:~# vim.tiny /etc/ntp.keys
```

```
# key ID | hash algorithm | key
1 MD5 secret
```

2. Добавьте в конфигурационный файл `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` следующие строки:

```
root@sterragate:~# vim.tiny /etc/ntpsec/ntp.conf.d/custom_ntp.conf
```

```
keys /etc/ntpsec/ntp.keys
trustedkey 1
```

где:

- `keys /etc/ntpsec/ntp.keys` – файл с ключами;
- `trustedkey 1` – список доверенных ключей `key ID` из файла с ключами (если ключей несколько, то укажите их через пробел `trustedkey 1 2 3`).

Если используете криптошлюз версии (5.0 KB), то добавьте в конфигурационный файл `/etc/ntp.conf.d/custom_ntp.conf` следующие строки:

```
root@sterragate:~# vim.tiny /etc/ntp.conf.d/custom_ntp.conf
```

```
keys /etc/ntp.keys
trustedkey 1
```

Только для клиента:

2.1. Также требуется в конец строки `server 192.168.1.1 iburst` добавить настройку, указывающую какой ключ использовать для синхронизации. В результате данная настройка должна выглядеть следующим образом:

```
server 192.168.1.1 iburst key 1
```

где:

- `1` - `key ID` из файла с ключами.

2.2. Если требуется, чтобы подключения могли происходить только с аутентифицированным сервером, нужно добавить в файле `custom_ntp.conf` следующую строку:

```
restrict default notrust
```

Важно заметить, что данная строка не заменяет опции `restrict default`, а дополняет их (если они есть к моменту конфигурирования).

3. Перезагрузите службу `ntpsec`:

```
root@sterragate:~# systemctl restart ntpsec.service
```

Если используете криптошлюз версии (5.0 KB), то перезагрузите службу `ntp`:

```
root@sterragate:~# systemctl restart ntp.service
```

4. Для того чтобы убедиться в том, что соединение между клиентом и сервером NTP установлено с аутентификацией, можно воспользоваться приведенной ниже командой на клиенте NTP и убедиться, что соединение имеет статус `auth` в значении `ok`:

```
root@sterragate:~# ntpq -c associations
```

```
ind assid status  conf reach auth condition  last_event cnt
===========================================================
  1 17767  f61a   yes   yes   ok   sys.peer    sys_peer  1
```

Примеры конфигураций

Ниже приведены примеры результирующих конфигурационных файлов с настроенной аутентификацией `custom_ntp.conf`

Клиент

Пример конфигурационного файла `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` выглядит следующим образом.

```
server 192.168.1.1 iburst key 1
keys /etc/ntpsec/ntp.keys
trustedkey 1
restrict default notrust
```

Если используете криптошлюз версии (5.0 KB), то пример конфигурационного файла `/etc/ntp.conf.d/custom_ntp.conf` выглядит следующим образом.

```
server 192.168.1.1 iburst key 1
keys /etc/ntp.keys
trustedkey 1
restrict default notrust
```

Сервер

Пример конфигурационного файла `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` выглядит следующим образом.

```
pool 0.ru.pool.ntp.org iburst
pool 1.ru.pool.ntp.org iburst
pool 2.ru.pool.ntp.org iburst
pool 3.ru.pool.ntp.org iburst
keys /etc/ntpsec/ntp.keys
trustedkey 1
```

Если используете криптошлюз версии (5.0 KB), то пример конфигурационного файла `/etc/ntp.conf.d/custom_ntp.conf` выглядит следующим образом.

```
pool 0.ru.pool.ntp.org iburst
pool 1.ru.pool.ntp.org iburst
pool 2.ru.pool.ntp.org iburst
pool 3.ru.pool.ntp.org iburst
keys /etc/ntp.keys
trustedkey 1
```

Примечание

Получение настроек NTP через DHCP

Данные настройки не являются для инструкции основными, потому вынесены отдельно. Настройки носят рекомендательных характер.

- Для криптошлюза версии (5.0 KB) получение настроек NTP через DHCP игнорируется, при этом в файл журнала `/var/log/cspvpngate.log` выводится соответствующее сообщение.
- В случае если требуется получать настройки NTP от DHCP сервера, на нём должны быть заранее проведены соответствующие настройки, позволяющие отдавать их, а также на интерфейсе криптошлюза настроено получение адреса по DHCP. Данные настройки в сценарии приводиться не будут;

- Подразумевается, что пользователь не проводил настроек NTP ни через Cisco-like, ни через системные файлы конфигурации.

1. Проверьте, что в выводе команды `show running-config` в Cisco-like консоли нет настроек NTP.

   Если настройки имеются, то перейдите в Cisco-like консоли в режим конфигурирования и удалите все NTP сервера.

2. Проверьте, что в конфигурационном файле `/etc/ntpsec/ntp.conf.d/st_ntp.conf` службы `ntpsec` нет настроек NTP. Если настройки есть, удалите их.

3. Очистите конфигурационный файл `/etc/ntpsec/ntp.conf.d/custom_ntp.conf` службы `ntpsec`, выполнив команду:

   ```
   root@sterragate:~# echo > /etc/ntpsec/ntp.conf.d/custom_ntp.conf
   ```

4. **Если специфических настроек `ntpsec` не требуется, рекомендуется сразу переходить к следующему пункту.**

   Настройки `server`, `peer`, `pool` и `tos`, проведённые в файле `/etc/ntpsec/ntp.conf`, не будут восприниматься в случае получения настроек NTP по DCHP. Это связано с особенностями реализации NTP (в частности взаимодействия NTP с DHCP клиентом). Если есть необходимость их всё-таки добавить/изменить, это можно сделать в файле `/etc/ntpsec/ntp.conf.d/custom_ntp.conf`, но делать этого **не рекомендуется**. Так же можно при необходимости поступить и с настройками `restrict` и другими.

   Желательно чтобы все возможные настройки NTP принимались от DHCP сервера.

5. Перезагрузите службу `ntpsec`:

   ```
   root@sterragate:~# systemctl restart ntpsec.service
   ```

6. Для того чтобы служба `ntpsec` запускалась после перезагрузки системы, выполните команду:

   ```
   root@sterragate:~# systemctl enable ntpsec.service
   ```

7. Для того чтобы получить сетевые настройки по DHCP можно перезапустить службу `networking` (**выполнение команды может сбросить текущие соединения**):

   ```
   root@sterragate:~# systemctl restart networking.service
   ```

Настройка межсетевого экрана

Настройки ниже описаны для случаев, когда нужно заблокировать любые обмены данными по протоколу NTP, не инициированные устройством (в данном случае криптошлюзом).

Данные настройки могут иметь смысл на внешнем интерфейсе сервера. Для примера считается, что `172.16.100.2` – адрес внешнего интерфейса криптошлюза.

1. Создайте сетевой `object-group` с именем `SELF` для хранения в нем WAN адресов криптошлюза с целью дальнейшего его использования в ACL:

   ```
   root@sterragate:~# su cscons
   sterragate#configure terminal
   Enter configuration commands, one per line.  End with CNTL/Z.
   sterragate(config)#object-group network SELF
   sterragate(config-network-group)# remark WAN IP
   sterragate(config-network-group)# host 172.16.100.2
   sterragate(config-network-group)#exit
   ```

2. Создайте ACL с именем `FW_INPUT_WAN` для входящего на WAN интерфейс трафика:

   ```
   sterragate(config)#ip access-list extended FW_INPUT_WAN
   sterragate(config-ext-nacl)# deny udp any object-group SELF eq ntp
   sterragate(config-ext-nacl)# permit ip any any
   sterragate(config-ext-nacl)# exit
   ```

Данный ACL блокирует пакеты только для случая, когда криптошлюз является ответчиком по протоколу NTP **впервые**. Если криптошлюз является инициатором или ответчиком в рамках ранее созданной сессии, то ответные пакеты будут разрешены в силу принципов работы stateful фильтрации (включается в пункте 3) – динамические разрешающие правила более приоритетны чем статические. Данные правила в Cisco-like консоли НЕ отображаются, их можно посмотреть при помощи утилиты `fwconn_mgr` с параметром `show`.

3. Создайте правила инспектирования UDP трафика и задайте необходимое максимальное количество сессий (в версии 5.0 данная команда устанавливает максимальное количество сессий для IPv4 и IPv6):

```
sterragate(config)#ip inspect name INSPECT udp
sterragate(config)#ip inspect udp sessions-max 65536
```

Максимальное количество сессий настраивается в зависимости от условий, потребностей и производительности аппаратной платформы. Суммарное максимальное рекомендуемое значение для количества сессий – 10 000 000 (для Gate 7000+). Также может потребоваться увеличить значение `fw_storage_hash_bits` в `drv_mgr`, но более 22 ставить не рекомендуется.

4. Прикрепите правила межсетевого экранирования на WAN интерфейс `GigabitEthernet0/0` (обратите особое внимание на направление правил фильтрации, список доступа `FW_INPUT_WAN` прикрепляется для входящих через интерфейс пакетов – **`in`**, а правило `INSPECT` stateful фильтрации прикрепляется для исходящих через интерфейса пакетов – **`out`**):

```
sterragate(config)#interface GigabitEthernet0/0
sterragate(config-if)# ip access-group FW_INPUT_WAN in
sterragate(config-if)# ip inspect INSPECT out
sterragate(config-if)#exit
sterragate(config-if)#end
```