Table of Contents

Основные процессы

Клиентам недоверенной не-3GPP-сети шлюз предоставляет интерфейс SWu посредством протокола IPSec, обеспечивая интерфейс авторизации SWa посредством протокола IKEv2 и интерфейс шифрованных защищенных туннелей SWn посредством протокола ESP.

1. Аутентификация и авторизация

Шлюз в целях аутентификации и авторизации клиентов поддерживает два режима взаимодействия с компонентами AAA и HSS ядра сети посредством протокола Diameter: с использованием интерфейса SWm для взаимодействия с компонентом AAA и с использованием интерфейса SWx для взаимодействия с компонентом HSS.

При работе в режиме с использованием интерфейса SWm, плагин осуществляет авторизацию пользователей при взаимодействии с компонентом AAA.

При работе в режиме SWx, плагин осуществляет авторизацию пользователей при прямом взаимодействии с компонентом HSS, аналогично компоненту AAA.

Для эмуляции функций компонента AAA, шлюз поддерживает серверные интерфейсы S6b для поддержки запросов авторизации от компонента PGW, а также SWa (SWm) для подключений внешних компонентов сторонних вендоров.

Запросы взаимодействия шлюза с компонентами посредством протокола Diameter могут балансироваться между клиентскими подключениями к множеству серверов используемого интерфейса, также в таком случае поддерживается обход отказа клиентских подключений.

Балансировка осуществляется распределением активных сессии аутентификации и авторизации клиентов шлюза между серверами используемого интерфейса в пропорции указанных приоритетов серверов исходя из общей суммы равной 100.

Обход отказа производится направлением неотложного запроса повтора процесса аутентификации и авторизации всем клиентам шлюза, имеющим активные сессии, связанные с отказавшим клиентским подключением. При повторе процесса аутентификации и авторизации клиентом шлюза, сессия аутентификации и авторизации клиента шлюза будет распределена и привязана в соответствии с балансировкой между функционирующими клиентскими подключениями к серверам. В случаях отсутствия функционирующих клиентских подключений к серверам или отказа аутентификации и авторизации клиента, клиент шлюза будет отключен в одностороннем порядке.

Серверные интерфейсы, предоставляемые шлюзом посредством протокола Diameter, поддерживают множественные подключения от соответствующих клиентов.

В качестве транспортного протокола для прикладного протокола Diameter поддерживается использование протоколов TCP/SCTP/TLS2/DTLS2.

2. Туннелирование

Шлюз поддерживает два режима взаимодействия с компонентом PGW ядра сети посредством протокола GTP: с использованием интерфейса S5/S8 и с использованием интерфейса S2b.

При работе с использованием интерфейса S5/S8 используются клиентские запросы аналогично компоненту SGW.

При работе с использованием интерфейса S2b используются клиентские запросы компонента EPDG.

При взаимодействии с компонентом PGW шлюз использует выбранный интерфейс в целях создания GTP-U туннелей посредством протокола GTP-C для авторизованных клиентов шлюза между EPDG и пакетной сетью, обслуживаемой PGW. Посредством протокола GTP-U обеспечивается обмен трафиком между ассоциированными SWn туннелями клиентов шлюза и GTP-U туннелями в соответствии с заданными QoS.

Запросы взаимодействия с компонентом PGW посредством протокола GTP-C могут балансироваться между клиентскими подключениями к множеству серверов.

Алгоритм балансировки и обхода отказа аналогичен алгоритму описанному для процесса аутентификации и авторизации, за отличием, что обход отказа производится направлением неотложного запроса повтора установки SWn туннелей всем клиентам шлюза, имеющим активные ассоциированные GTP-U туннели, связанные с отказавшим клиентским подключением.

В качестве транспортного протокола для прикладного протокола GTP поддерживается использование протокола UDP со стандартными номерами портов 2123 для протокола GTP-C и 2152 для протокола GTP-U.

3. Назначение IP-адресов

Шлюз поддерживает два источника назначения адреса туннеля SWn, адресов DNS серверов, адресов P-CSCF клиенту шлюза: полученные посредством протокола Diameter и полученные посредством протокола GTP.