

Техническое описание

Примеры конфигурации

для

VPN-маршрутизаторов

Версия этой документации:

Версия:

1.02

Дата:

23.04.2013

Мы оставляем за собой право внесения технических изменений и наличия неточностей

Copyright© 2013 Мсм Нэт Майсснер. Вс права защищены.

В этом руководстве Мсм Нэт будет использоваться в качестве синонима для инженерного бюро Мсм Нэт Майсснер, а так же для Мсм Нэт Майсснер GmbH.

Все другие в этом документе использованные торговые знаки служат для идентификации. Все торговые знаки, марки и марки фирм являются собственностью их предъявителей.

Мсм Нэт Майсснер GmbH отказывается от права владения торговыми знаками и торговыми обозначениями, не являющихся ее собственностью.

Содержание:

1. X.509 для управление сертификатами.....	4
1.1. Основы для использования управление сертификатами.....	4
1.2. Создание центра сертификации (CA Вариант 1).....	5
1.3. Создание пользовательских сертификатов (Вариант 1).....	5
1.4. Блок сертификата пользователя (Вариант 1).....	6
1.5. Экспорт сертификатов для пользователей (Вариант 1).....	6
1.6. Импорт сертификатов X.509 в формате PKCS12 (Вариант 1).....	7
1.7. Создание CRL и их экспорт (Вариант 1).....	7
1.8. Публикация и использование CRL (Вариант 1).....	8
1.9. Управление сертификатами в варианте 2.....	8
2. Способы соединения и примеры.....	9
2.1. Основы для VPN-подключения.....	9
2.2. Соединение сеть-сеть со статическим IP-адресом через IPSEC nativ с PSK.....	10
2.3. Соединение сеть-сеть со статическим IP-адресом через IPsec nativ с X.509.....	11
2.4. Соединение сеть-сеть со статическим и динамическим IP-адресами.....	12
2.5. Соединение сеть-сеть с двумя динамическими IP-адресами (версия 1, с использованием динамического DNS).....	13
2.6. Соединение сеть-сеть с двумя динамическими IP-адресами (версия 2, используя ISDN).....	14
2.7. Соединение сеть-сеть со статичными IP-адресами через IPsec-gre с X.509.....	15
2.8. Удаленное подключение для технического обслуживания.....	16
2.9. Протокол туннельных соединений.....	17
3. Конфигурационные варианты подключения VPN.....	18
3.1. Настройка параметров.....	18
3.2. Соединение в целом.....	20
3.3. Соединения с автоматически снабженные ключом параметрами	21
3.4. Соединения с снабженными вручную ключом параметрами.....	23
4. Конфигурация структурограмма (примеры).....	24
4.1. Централизованная VPN (конфигурация).....	24
4.2. Логическая конфигурация централизованной VPN.....	25
4.3. Централизованное управление.....	26
Контактная информация.....	27

1. X.509 для управление сертификатами

1.1. Основы для использования управление сертификатами

Каждый маршрутизатор VPN от Мсм Нэт снабжен полной версией сертификата X.509.

Вариант 1

Этот сертификат дает возможность создать и управлять любым количеством центров сертификации (Root CA). Кроме того, есть возможность для создания любого количества сертификатов для пользователя. Создание сертификата для пользователя осуществляется таким образом, что сертификат пользователя автоматически подписывается центром сертификации (Root CA) по умолчанию. То есть, сертификат пользователя может быть использован сразу же после создания. Благодаря иерархической связи центра сертификации с сертификатом пользователя любая компания в состоянии легко, независимо и бесплатно создать и управлять действующим PKI.

Вариант 2

С помощью управления сертификатами могут быть создано и подписано любое количество запросов и сертификатов (RootCA, SubCA и сертификат идентификации). С помощью интеграции приложения CryptoSmartcard (в настоящий момент как eToken от Aladdin) возможно реализовать безопасные структуры PKI. Аналогично с «вариантом 1» реализованы обширные функции экспорта и импорта.

В обоих вариантах интегрированы сложные CRL-приложения (создание, импорт, экспорт и автоматический заказ). В подписании RootCA-сертификатов «вариантом 2» так же интегрирован OCSP (Online Certificate Status Protocol).

1.2. Создание центра сертификации (CA Вариант 1)

После успешной регистрации в маршрутизаторе VPN в качестве администратора перейдите в пункт меню VPN соединения, а там к управлению сертификатами. На этой странице в левой части Вы получите список всех существующих центров сертификации. С правой стороны вам предлагаются дальнейшие варианты. С нажатием кнопки «Создание центра сертификации» открывается новая страница. На этой странице вам надо ввести все данные для создания нового центра сертификации. Все данные, которые Вы вводите, перед созданием нового центра сертификации проверяются на допустимые символы и длину. Нажатием кнопки «Сохранить» после проверки ваших введенных данных создается новый центр сертификации. В списке центров сертификации теперь стоит имя Вами созданного центра сертификации. Выбрав его и нажав кнопку «Подробности к центру сертификации» Вы можете посмотреть Root CA. Если Вы прокрутите в этом окне вниз, то увидите строку с названием: CA: TRUE.

Это указывает на то, что это действительно центр сертификации.

1.3. Создание пользовательских сертификатов (Вариант 1)

Если Вы хотите создать новый сертификат пользователя, выберите сначала в обзоре один из центров, в котором Вы хотите создать новый сертификат. Далее, нажмите кнопку «Выбор центра сертификации».

Если центр сертификации был создан на этом VPN-маршрутизаторе, то Вы можете теперь создать сертификат пользователя. Если VPN-маршрутизатор не тот, на котором был создан этот центр сертификации, то есть он импортирован, то Вы не имеете доступ к нескольким дальнейшим функциям. При возможном выборе уже существующего сертификата Вы можете по желанию посмотреть его в деталях. Нажатием кнопки «Создать новый сертификат» открывается новая страница, на которой задаются данные, необходимые для создания сертификата пользователя. При сохранении и при достоверности данных (проверка автоматически) создается новый сертификат пользователя. В списке сертификатов центра сертификации Вы сможете найти имя нового сертификата.

1.4. Блок сертификата пользователя (Вариант 1)

Если по каким либо причинам возникнет потребность для блокировки сертификата пользователя, то выберите сертификат из списка нажатием на него. Следующим шагом нажмите на «Заблокировать выбранный сертификат».

Далее вас спросят еще раз, хотите ли Вы действительно заблокировать этот сертификат. Если Вы уверены, пожалуйста, подтвердите. Тогда сертификат блокируется. В изображении это можно определить за счет того, что перед названием сертификата пользователя находится значок «#» и вся строка выделена красным. С блокировкой сертификата автоматически создается новый CRL (список отозванных сертификатов). Этот список Вы можете посмотреть в любой момент нажатием на «Список отозванных сертификатов».

Там Вы увидите развернуто все заблокированные сертификаты пользователей этого центра сертификации.

1.5. Экспорт сертификатов для пользователей (Вариант 1)

Для того, чтобы пользоваться вами созданные сертификаты и на других приборах, Вы должны их экспортировать. Для этого требуются следующие шаги. Откройте страницу органов сертификации и нажмите «Выбор центра сертификации» («Zertifizierungsstelle auswählen»). Далее выберите «Экспортные сертификаты» («Zertifikate exportieren»). Потом откроется страница, на которой находятся все сертификаты этого центра сертификации, которые можно экспортировать. Пожалуйста, выберите сертификат, который Вы хотите экспортировать, и введите соответствующий пароль. Если Вы выбрали одинаковый пароль для всех сертификатов, то Вы можете воспользоваться соответствующей сборной функцией. Когда Вы закончили ввод, нажмите кнопку «Далее» («Weiter»). В следующем окне Вы увидите все выбранные сертификаты для скачивания в формате «PKCS12».

Нажмите контекстной кнопкой мыши (правая кнопка) на каждый сертификат и выберите сохранить как «...». Все так сохраненные сертификаты могут теперь быть легко импортированы на соответствующий VPN-маршрутизатор. Также импортировать в другие системы (например в Windows X, Linux, ..) возможно в этом формате, потому что все данные, необходимые для использования сертификата, включены в этот файл.

1.6. Импорт сертификатов X.509 в формате PKCS12 (Вариант 1)

Для импорта экспортированных или других сертификатов в формате «PKCS12» нажмите, пожалуйста «импортировать чужие сертификаты (PKCS12)» («Fremdzertifikate importieren (PKCS12)») на странице центра сертификации.

Пожалуйста, введите необходимые данные в формуляр, и нажмите «импорт» («importieren»). Через импорт создается полноценный центр сертификации и сопряженные с ним сертификат пользователя. Вы можете импортировать несколько сертификатов пользователя в центр сертификации. При условии, что сертификат пользователя был подписан центром сертификации. Если это не так, то создается новый центр сертификации. Выберите вновь созданный (импортированный) центр сертификации, и Вы увидите, что доступна только часть функций нормального центра сертификации. Если Вы хотите использовать механизмы управления «CRL», то Вы должны их настроить.

1.7. Создание CRL и их экспорт (Вариант 1)

Каждый центр сертификации, с помощью которого Вы можете создать сертификат пользователя, имеет свой список отозванных сертификатов (CRL). Этот CRL создается автоматически при генерации центра сертификации. При создании центра сертификации введите цикл, когда должен быть создан новый CRL. Всегда после окончания этого цикла на VPN-маршрутизаторе создается автоматически новый CRL этого центра сертификации.

Кроме того, независимо от цикла, создается новый CRL после блокирования сертификата пользователя. CRL может быть загружен с VPN-маршрутизатора для дальнейшего использования.

Пожалуйста, выполните следующие действия:

- Выберите центр сертификации
- Выберите CRL
- Выберите экспорт

Таким образом, CRL скачан на ваш локальный компьютер и доступен для дальнейшего использования.

1.8. Публикация и использование CRL (Вариант 1)

CRL может быть опубликован на веб-сервере или FTP-сервере в Интернете. Чтобы это осуществить, CRL загружается на сервер и встраивается в соответствующее место. Чтобы убедиться, что все VPN-маршрутизаторы пользуются сертификатами центра сертификации, надо установить этот CRL на VPN-маршрутизаторе.

- Выберите импортированный CA
- Выберите CRL

У вас есть выбор между двумя способами по загрузке CRL:

1. Вы можете скачать CRL прямо с вашего компьютера.
2. Введите полный URL к CRL.

Если Вы настроили автоматическое обновление через сеть, то у вас есть доступ к услугам HTTP, FTP и wget. Это означает, что ваш URL может выглядеть следующим образом:

`http://www.msm-net.de/zertifizierungsstellename.crl`

`ftp://1.2.3.4/zertifizierungsstellename.crl`

`wget://hostname/zertifizierungsstellename.crl`

Если Вы настроили обновление через сеть, то CRL ежечасно загружается с сервера. По желанию этот цикл может быть произвольно изменен. Вы также можете импортировать CRL и одновременно настроить загрузку с единого указателя ресурсов (URL).

1.9. Управление сертификатами в варианте 2

Во втором варианте управления сертификатами действуют общие административные правила сертификатов X.509. Это означает:

1. Создать запрос
2. Подписать запрос в соответствие с целью
3. Экспортировать или импортировать сертификаты в различных форматах

В целях ужесточения требований к безопасности по отношению к варианту 1 была убрана автоматическая установка пароля сертификата администрации и введена полная интеграция шифрования смарт-карт с помощью приложения CryptoSmartcard. Это приложение может быть использовано для CA-администрации, а также для идентификации локальных и удаленных компьютеров. Соответствующие этому требования принимаются при создании соединений. Кроме того, с помощью независимой административной структуры возможно импортировать, создавать администрировать и использовать в маршрутизаторе системы любые Sub-CA-структуры.

2. Способы соединения и примеры

2.1. Основы для VPN-подключения

Вполне возможно, создать 3 различных типа подключений VPN.

Типы:

- постоянно двусторонние
- двусторонние по требованию и
- одностороннее подключение (только входящие)

Кроме того, может быть подключено неактивное соединение. Двухнаправленные (постоянное и по требованию) соединения-соединения, которые могут быть установлены между VPN-маршрутизаторами. Входящие соединения – соединения, которые могут быть использованы между VPN-маршрутизаторами, а также VPN-маршрутизатором и мобильным клиентом.

Получаются следующие комбинации:

маршрутизатор 1		маршрутизатор 2		применение при
IP-адрес	соединения	IP-адрес	соединения	
постоянный	постоянно двусторонние	постоянный	постоянно двусторонние	Маршрутизатор к маршрутизатору
постоянный	одностороннее	динамический	постоянно двусторонние	Маршрутизатор к маршрутизатору, Маршрутизатор 2, к напримеру, с DSL
постоянный	одностороннее	динамический	двусторонние по требованию	Маршрутизатор к маршрутизатору, Маршрутизатор 2, к напримеру, с DSL

Соответственно, список можно продолжать в сочетании с динамическими клиентами. Если соединения работают с динамическими IP адресами, уделите особое внимание настройкам DPD (dead peer detection)! Эта опция может быть отредактирована только в меню для экспертов.

Возможные варианты:

1. **hold** (рекомендуется для маршрутизаторов с динамическим IP)
2. **clear** (рекомендуется для маршрутизатора со статическим IP и динамическим IP клиента)
3. **restart** (рекомендуется для маршрутизатора с постоянной двухнаправленной связью)

См. также 3.3

Устанавливаются связи с использованием аутентификации сертификата, пожалуйста, обратите внимание на следующее:

В настройке соединения выберите сертификат, с которым Вы хотите работать. В ниже стоящем поле ввода внесите субъект («Subject») партнерского сертификата. Замены на '*' при этом допустимы.

Таким образом, могут получиться следующие вводы:

C=Ваша страна, ST=Ваш регион, L=место жительства, O=организация, OU=*/Email=Ваш электронный адрес

На VPN-маршрутизаторе во втором варианте управления сертификатами это может быть один способом из многих! Если Вы хотите, использовать PSK для аутентификации, то Вы должны учитывать следующее:

Маршрутизатор будет пытаться вызвать идентификацию (ID) с помощью DNS. Если Вы хотите избежать этого, вставьте @ перед Вашим ID. (Например, @192.168.6.254)

2.2. Соединение сеть-сеть со статическим IP-адресом через IPSEC nativ с PSK

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN 1.1.1.2	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Pre Shared Key verwenden» («использовать PSK») @192.168.6.254 @192.168.7.254	«Pre Shared Key verwenden» («использовать PSK») @192.168.7.254 @192.168.6.254
«IPSEC nativ»	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.3. Соединение сеть-сеть со статическим IP-адресом через IPSec nativ с X.509

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN 1.1.1.2	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.4. Соединение сеть-сеть со статическим и динамическим IP-адресами

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«eingehend» («одностороннее»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN %any	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.5. Соединение сеть-сеть с двумя динамическими IP- адресами (версия 1, с использованием динамического DNS)

Если Вы пользуетесь двумя или более VPN-маршрутизаторами с подключением через DSL или ISDN и они не имеют постоянного IP-адреса, тогда имеет смысл зарегистрироваться у провайдера услуг DNS и в последствие использовать зарегистрированное полностью определённое имя домена (FQDN) для конфигурации. Для конфигурации динамического DNS-клиента выберите IP-провайдера в сервисном меню. Таким образом, Вы можете использовать полную VPN с динамическим клиентом и динамическим IP-адресом.

Для более подробной информации, пожалуйста, см. таблицу:

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN fqdnrouter2	IP или FQDN fqdnrouter1
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.6. Соединение сеть-сеть с двумя динамическими IP-адресами (версия 2, используя ISDN)

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN vpnrouter2.dyndns.org	IP или FQDN vpnrouter1.dyndns.org
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.0/24 192.168.7.0/24	192.168.7.0/24 192.168.6.0/24
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.7. Соединение сеть-сеть со статичными IP-адресами через IPSec-gre с X.509

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN 1.1.1.2	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Pre Shared Key verwenden» («использовать PSK») @192.168.6.254 @192.168.7.254	«Pre Shared Key verwenden» («использовать PSK») @192.168.6.254 @192.168.7.254
«IPSEC nativ»		
«GRE über IPSEC» («GRE через IPSEC»)	192.168.6.0/24 192.168.7.0/24 Если требуется, возможно, больше вариантов	192.168.7.0/24 192.168.6.0/24 Если требуется, возможно, больше вариантов
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.8. Удаленное подключение для технического обслуживания

Техническое обслуживание должно быть выполнено на компьютере с IP 192.168.6.10 через маршрутизатор 1 на маршрутизаторе 2. Не забывайте, что компьютер требует соединение к 192.168.7.254 через 192.168.6.254 (внутренний IP маршрутизатор 1).

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN 1.1.1.2	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.10/32 192.168.7.254/32	192.168.7.254/32 192.168.6.10/32
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

2.9. Протокол туннельных соединений

Протоколы туннельной связи служат VPN-маршрутизаторам для параллельного сохранения внесенных в протокол данных в базе данных SQL. Для этого задайте на странице «Общее» («Allgemein») IP-адрес Log-сервера (например, 192.168.6.2). Этот адрес должен быть доступен в следующем примере конфигурации для VPN-маршрутизатора 2 через VPN-маршрутизатор 1.

Название поля	Значение маршрутизатора 1	Значение маршрутизатора 2
«Verbindungstyp» («Тип соединения»)	«bidirektional permanent» («постоянно двусторонние»)	«bidirektional permanent» («постоянно двусторонние»)
«ESP»	одинаковые настройки	
«IKE»	одинаковые настройки	
«Local Port/Protokoll» («Локальный порт / протокол»)	Только для L2TP соединения через IPSEC и зависит от версии Windows	
«Remote Port/Protokoll» («Удаленный порт / протокол»)		
«Kompression» («Сжатие »)	Должно быть сразу настроено	
«Partner IP, FQDN» («Партнер IP, FQDN»)	IP или FQDN 1.1.1.2	IP или FQDN 1.1.1.1
«Authentifizierung» («аутентификация»)	«Zertifikat verwenden» («использовать сертификат») Сертификат 1 Субъект Сертификата 2	«Zertifikat verwenden» («использовать сертификат») Сертификат 2 Субъект Сертификата 1
«IPSEC nativ»	192.168.6.2/32 192.168.7.254/32	192.168.7.254/32 192.168.6.2/32
«GRE über IPSEC» («GRE через IPSEC»)		
«Filterregel» («правило фильтра»)	По требованию	По требованию

3. Конфигурационные варианты подключения VPN

3.1. Настройка параметров

Параметр	Описания	Значение	Комментарии	Исп.
also	Включает все опции других секций в актуальную секцию	Имя другой секции		
interfaces	Назначение виртуально-реального интерфейса	<virtual>=<real> %defaultroute (quoted string)		
forwardcontrol	Forwarding должен быть включен, если еще не активирован	yes no (да/нет)		
syslog	Используемая Syslog-facility	facility.level <u>facilities (средства):</u> auth, authpriv, cron, daemon, kern, lpr, mail, news, syslog, user, uucp and local(0-7) <u>levels:</u> debug, info, notice, warning, err, crit, alert, emerg		
klipsdebug	Ipssec-Debugging	tunnel, tunnel-xmit, pfkey, xform, eroute, spi, radij, esp, ah, ipcomp, verbose (zu finden in /proc/net/ipsec_klipsdebug) -> special: all, none		
plutodebug	IKE-Debugging	raw, crypt, parsing, emitting, control, lifecycle, klips, dns, private, nat_t -> special: all, none		
dumpdir	Каталог для дампа памяти (Core-Dump)	Указание пути		
dump	Core-Dump (Дамп памяти)	no yes (да/нет)		
manualstart	Предназначенные к запуску соединения в manual mode (ручном режиме)	Список секций (quoted String)		
pluto	Pluto должен быть запущен	yes no (да/нет)		
plutoload	Соединение, которое Pluto должен загрузить при запуске	Список секций (quoted String) -> special: %search (все самозапускающиеся соединения= add route start)		
plutostart	Соединение, которое Pluto должен запустить при запуске	Список секций (quoted String) -> special: %search Все соединения с auto= route start (все соединения для: auto= route start)		
plutowait	Pluto должен ждать, пока одно соединение отключится, перед тем как начать другое.	yes no (да/нет)		
plutobackground-load	Игнорируется (устарело)			
prepluto	shell-command, должен быть выполнен перед папуском Pluto.	Путь к скрипту		
postpluto	shell-command, должен быть выполнен перед запуском Pluto.	Путь к скрипту		

Мсм Нэт Майсснер

КОМПЕТЕНТНЫЙ - ТВОРЧЕСКИЙ - ИННОВАЦИОННЫЙ

Параметр	Описания	Значение	Комментарии	Исп.
fragicmp	Фрагментированные пакеты должны быть представлены отправителем, для того что бы он мог уменьшить PMTU	yes no (да/нет)		
no_eroute_pass	Неполная версия 'packetdefault' будет игнорирована, если 'packetdefault' опеределено.	yes (да) -> packetdefault=pass no (нет) -> packetdefault=drop		
opportunistic	opportunistic encryption	yes no-default (да/нет)		
hidetos	Должно ли значение TOS быть скрыто туннельным пакетом?	yes no (да/нет) (если нет, то значение TOS перенимается в туннельного пакета ESP / AH)		
uniqueids	Точный ID-партнер	yes no (да/нет) (Если да, то существующее соединение с партнером с таким же ID, как и у партнера с новым соединением, будет удалено.)		
packetdefault	Процедура для пакетов, входящих в виртуальный IPSEC-интерфейс и не имеющие eroute	pass drop reject (пройти сбросить отвергнуть)		
overridemtu	Указывает PMTU из виртуального IPSEC - интерфейса	Целое число (MTU-значение)		
nocrsend	<u>Не должен</u> при установлении соединения посылать запрос сертификату (Certificate-Request)	yes no (да/нет) (для партнеров, которые не поддерживают и прерывают аутентификацию подлинности сертификата, и)		
strictcrlpolicy	тщательный анализ сертификата идентификации с помощью CRL	yes no (да/нет) (Если да, то должен существовать действительный CRL.) (Если нет и CRL с заблокированным сертификатом существует, будет ли это)		
crlcheckinterval		Целое число (long) (секунды)		
nat_traversal	Включение NAT-T патчи (ESP в UDP)	yes no (да/нет)		
keep_alive	Время между keepalive пакетами	Целое число (секунды)		
force_keepalive	Вынуждение keepalive пакета	yes no (да/нет)		
disable_port_floating		yes no (да/нет)		
virtual_private	Общесистемный список частных сетей	Пример: virtual_private= %v4:10.0.0.0/8,%v4:172.16.0.0/12, %v4:192.168.0.0/16, %v4:!192.168.2.0/24, %v4:!192.168.15.128/25		
xauth	Аутентификация пользователя / пароль против PAM (/etc/pam.d/pluto)	yes no (да/нет)		

3.2. Соединение в целом

Параметр	Описания	Значение	Комментарии	Исп.
also	Включает все опции других секций в актуальную секцию	Имя другой секции		
type	Тип связи	(transport tunnel passthrough) (only manual-mode)		
authby	Аутентификация через	Secret rsasig		
_plutodevel				
left/right	Адрес	<ipaddress> %any %opportunistic		
left/rightsubnet	Туннелизируемая сеть	left=<netaddress> %defaultroute right=<netaddress> %any %vhost <u>vhost:</u> %no (no virtual IP, accept public IP) %dhcp (accept DHCP SA of affected IP [not impl]) %ike = accept affected IKE Config Mode IP [not impl] %priv = accept system-wide private net list %v4:x = accept ipv4 in list 'x' %v6:x = accept ipv6 in list 'x' %all = accept all ips [only for testing]		
left/rightprotoport	Выбор протокола / порта для IPSEC SA	< Имя/номер протокола>/(< номер протокола>) %any как Wildcard		
leftnexthop	Маршрутизатор IPsec-пакетов через ...	<ipaddress> %defaultroute %direct		
leftfirewall	если соединение с хостом защищено брандмауэром, то используется правило Forward	yes no (да/нет)		
leftupdown	Скрипт запускается при изменении статуса связи	Путь к скрипту + аргументация (quoted String)		
esp	Алгоритмы кодирования / Алгоритмы аутентификации	enc-auth(!) <u>enc:</u> 3des cast128 aes(128..256) blowfish(128..256) twofish(128..256) serpent(128..256) <u>auth:</u> md5 sha sha2_256 sha2_512 <u>!:</u> exclusive, не признает других вариантов		
ah	Методы аутентификации	auth(!) <u>auth:</u> md5 sha sha2_256 sha2_512 <u>!:</u> exclusive, не признает других вариантов		

Мсм Нэт Майсснер

КОМПЕТЕНТНЫЙ - ТВОРЧЕСКИЙ - ИННОВАЦИОННЫЙ

3.3. Соединения с автоматически снабженные ключом параметрами

Параметр	Описания	Значение	Комментарии	Исп.
auto	Операции при запуске	add route start ignore		
keyexchange	Метод обмена ключа	ike		
auth	Протокол для аутентификации	esp ah		
pfs	Perfect Forward Secrecy of keys	yes no (да/нет)		
pfsgroup	PFS- группа, если pfs=yes	modp(768,1024,1536,2048,3072,4096,6144,8192)		
keylife	Срок службы аутентификации / ключа шифрования через IPSEC	елое число из последующих s (секунд) m (минут) h (часов), максимум 24h		
rekey	Стоит ли перед окончанием действия ключ сделать обновление ключа?	yes no (да/нет)		
rekeymargin	За сколько времени до окончания действия ключа должен быть сделан новый обмен ключами	Целое число из последующих s (секунд) m (минут) h (часов)		
rekeyfuzz	Процент, с которым повторный обмен ключа случайно продляется. (Результат не должен превышать keylife)	Целое число % (в процентах)		
dpddelay	Время ожидания между пакетами	Целое число (в секундах)		
dpdtimeout	Тайм-аут ожидания ответа пакетов	Целое число (в секундах)		
dpdaction	Действия, когда соединение прервано	hold clear		
aggrmode	позволен агрессивный режим, или основной режим	yes no (да/нет)		
xauth	???????????? (мы не используем)			
compress	Сжатие данных пользователей	yes no (no = никогда не сжимать, IKE предложение отклонить, yes = если возможно)		
keyingtries	Количество попыток установки соединения	Целое число (0 = никогда не сдавайся)		
ikelifetime	Время работы IKE ключа	Целое число из последующих s (секунд) m (минут) h (часов)), максимум 8h		
disablearrivalcheck	???????	yes no (да/нет)		
ike	Алгоритм кодирования / алгоритм аутентификации Бит длины DH	enc- auth(-dh) (!) enc: 3des cast128 aes(128..256) blowfish(128..256) twofish(128..256) serpent(128..256) auth: md5 sha sha2_256 sha2_512 dh: modp(768,1024,1536,2048,3072,4096,6144,8192) !: исключающий, не принимающий другие методы		

Мсм Нэт Майсснер

КОМПЕТЕНТНЫЙ - ТВОРЧЕСКИЙ - ИННОВАЦИОННЫЙ

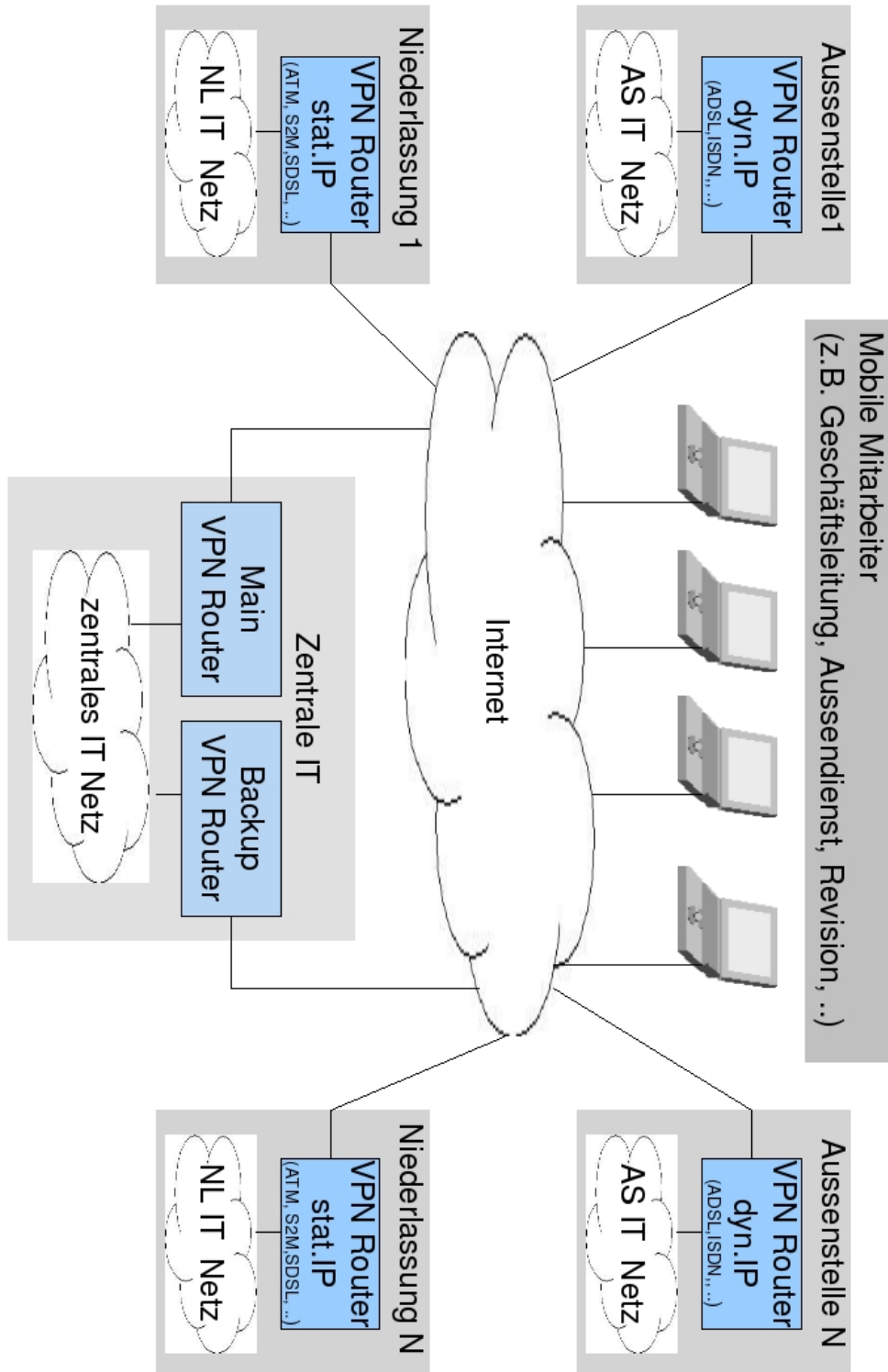
Параметр	Описания	Значение	Комментарии	Исп.
lifetime	устарелло для 'keylife'			
rekeystart	устарелло для 'rekeymargin'			
rekeytries	Количество новых попыток обмена ключа	Целое число (0 никогда не сдавайся)		
left/rightsasig-key	установка RSA public keys, то есть как определить	<rsakey> %cert %none %dnsondemand %dnsonload		
left/rightsasig-key2	установка RSA public keys, , то есть как определить (полезно для обновления ключа)	<rsakey> %cert %none %dnsondemand %dnsonload		
left/rightid	ID партнеров	<ip> <fqdn> @<user_fqdn> <distinguished name>		
left/rightcert	сертификат, который будет использоваться (PEM-формат)	<задать путь относительно /etc/ipsec.d/>		
rightca	CA сертификат, который будет использоваться для проверки подлинности сертификата	<distinguished name> %same (если не специфицировано, все возможные CA's)		
rightsubnetwithin	Удаленная подсеть должна находиться в заданной сети	<net adress>		

3.4. Соединения с снабженными вручную ключом параметрами

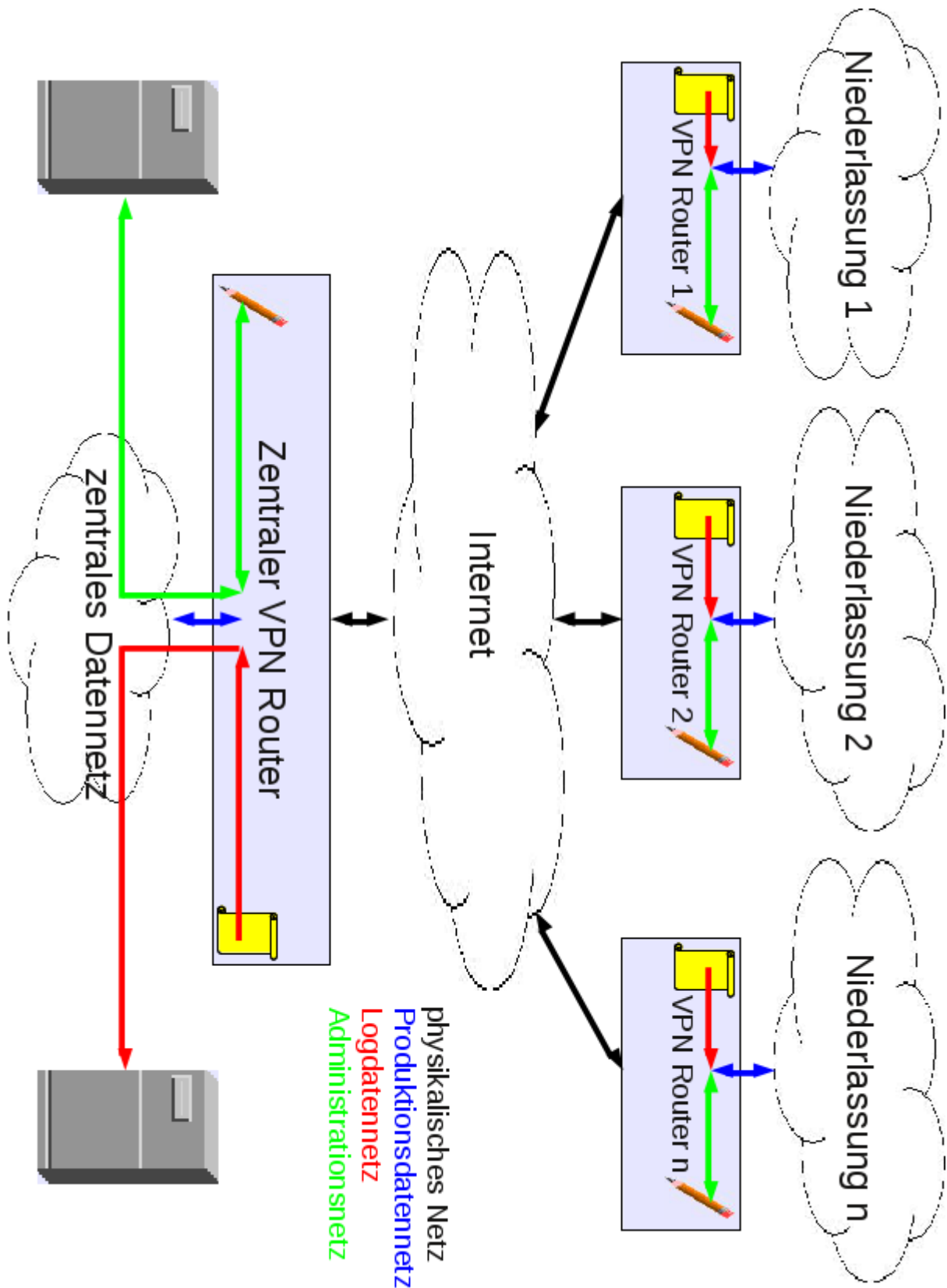
Параметр	Описания	Значение	Комментарии	Исп.
spibase	SPI базовое значение, самое малое значение бита направление (in/out) (exclusiv or 'spi')	Шестнадцатеричное число (3 цифры, последняя должна быть 0) 0x..0 (советуется 0x100-0xff0)		
spi	Используйте SPI-номер для всех SA (включающий или 'spibase')	Шестнадцатеричное число (3 Stellen) 0x... (советуется 0x100-0xffff)		
left-/rightespsi	автоматически перезаписать ESP SA значение с величиной...	Шестнадцатеричное число 0x...		
left-/rightahspi	автоматически перезаписать AH SA значение с величиной...	Шестнадцатеричное число 0x...		
(left/right/-)espenckey	Ключ шифрования может быть установлен отдельно независимо для обоих направлений	действительный ключ (разрядность) в hex- форме: 0x...		
(left/right/-)espauthkey	Ключ шифрования может быть установлен отдельно независимо для обоих направлений	действительный ключ (разрядность) в hex- форме: 0x...		
espreplay_window	Ответ в новом окне браузера	Целое число между 0..64		
(left/right/-)ahkey	Ключ шифрования может быть установлен отдельно независимо для обоих направлений	действительный ключ (разрядность) в hex- форме: 0x...		
ahreplay_window	Ответ в новом окне браузера	Целое число между 0..64		

4. Конфигурация структурограмма (примеры)

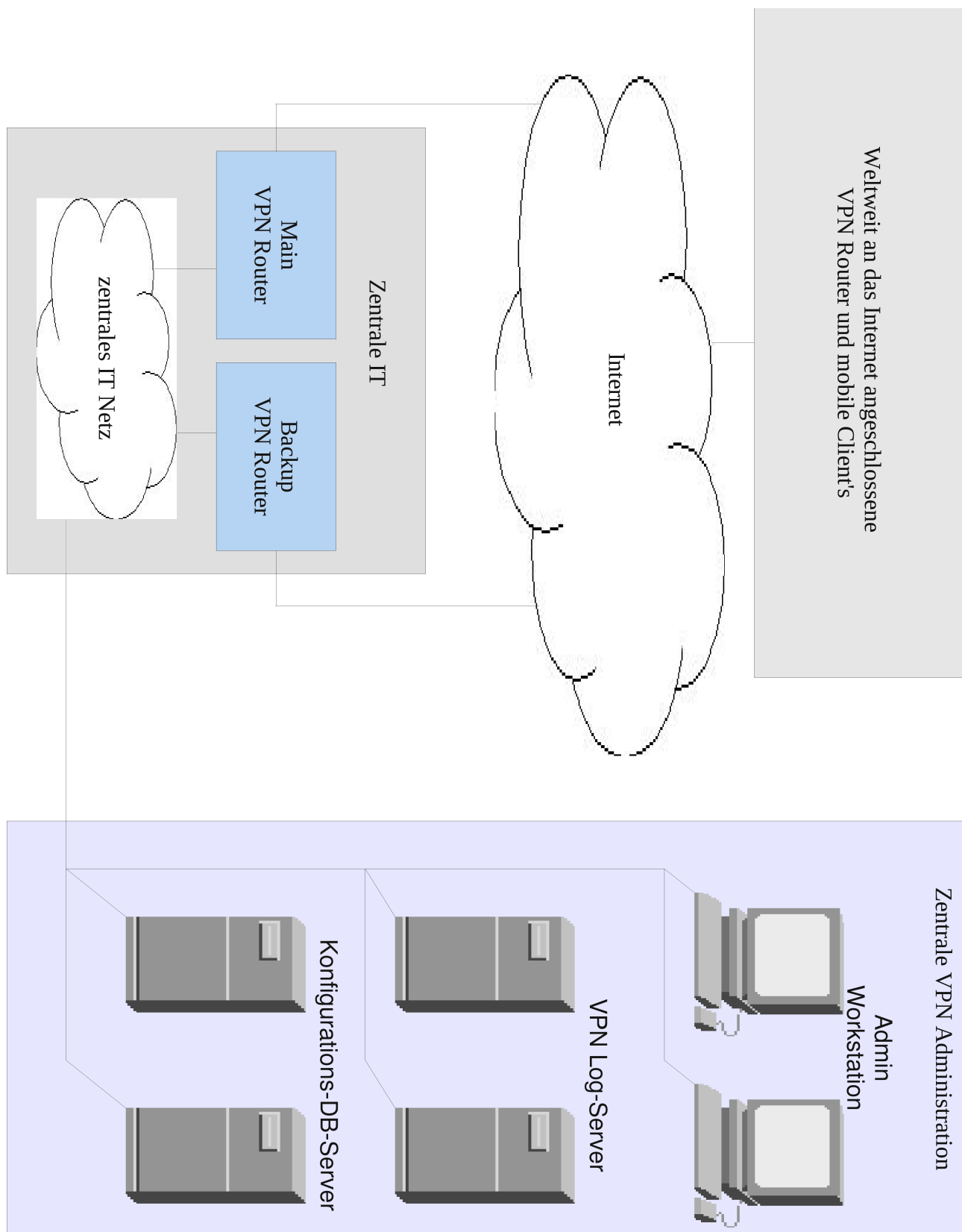
4.1. Централизованная VPN (конфигурация)



4.2. Логическая конфигурация централизованной VPN



4.3. Централизованное управление



Контактная информация

Адрес	
	Инженерного бюро Мсм Нэт Майсснер Ам Банхоф 10 07570 Нидэргёллнитц ФРГ
Контакт	
телефон:	+49 (0) 36628 9571 0
факс:	+49 (0) 36628 9571 130
сотовый телефон:	+49 (0) 0170 24190 25
электронный адрес:	service@msm-net.de
интернет:	www.msm-net.de