

**- Техническое описание -**

**Высокие технологии для  
виртуальных частных  
сетей**

**high technologie for  
virtual private network  
solution**

Версия документа:

Версия:

1.02

Дата:

22.04.2013

**Мы оставляем за собой право внесения технических изменений и наличия неточностей**

**Copyright© 2013 Мсм Нэт Майсснер. Все 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. Мы о себе
2. VPN-решения для стационарной техники
3. VPN-решения для мобильной техники
4. Типичные области применения VPN
5. Проектно-ориентированные решения
6. Сервис и техническое обслуживание
7. Подготовка, обучение и консультация
8. Контактная информация

## 1. Предисловие

Это «Техническое описание» предназначено для технически подготовленного персонала и для системных администраторов. Оно четко и ясно представляет важные технические показатели. На основании этого конспекта можно сделать быструю оценку возможных вариантов построения и системы интеграции. Мы предлагаем углубленный диалог всем заинтересованным лицам. В следующей главе, вы сможете прочитать об огромной возможности выбора масштаба.

## 2. Общие технические возможности

С помощью VPN - решений от „Мсм Нэт“ можно реализовать любое число структур VPN-сетей. При использовании Интернета можно выстроить классические звездообразные и беспроводные самоорганизующиеся сети, а также их комбинации. Это можно осуществить со статическими или динамическими IP - адресами в любой комбинации.

Основываясь на этих фактах, VPN-сети могут реализоваться как в стационарных, так и мобильных сферах. Любыми комбинации можно управлять из центрального пункта с помощью существующих административных инструментов.

Для технической реализации, как правило, существуют очень разные требования к аппаратному обеспечению. Технические решения «Мсм Нэт» открывают огромный диапазон. Для реализации используются стандартные аппаратные компоненты из компьютерной области.

Подключение к Интернету, как средству доставки, очень гибко с помощью нашего модульной концепции.

Само собой разумеется, каждый маршрутизатор VPN защищен брандмауэром.

### 3. Технические характеристики программного обеспечения VPN

Категория	Детали
ОС	Linux
Платформа аппаратной системы	Производственные компоненты ПК, Компоненты сервера, Изменяемые в зависимости от требований проекта
Количество возможных VPN-соединений	Ограничено только за счет платформы аппаратной системы .
Защита данных	<ul style="list-style-type: none"><li>• Ограничена только за счет применяемых методов защиты</li><li>• Ограничена за счет уровня мощности устройства</li></ul>
Методы аутентификации	<ul style="list-style-type: none"><li>• MD5</li><li>• SHA1</li><li>• SHA2-256</li><li>• SHA2-384</li><li>• SHA2-512</li></ul>
Алгоритмы кодирования	<ul style="list-style-type: none"><li>• 3DES 192</li><li>• AES 128 / 192 / 256</li><li>• Blowfish 128 / 192 / 256</li><li>• CAST6 128 / 192 / 256</li><li>• Twofish 128 / 192 / 256</li><li>• Serpent 128 / 192 / 256</li></ul>
Длина бита DH MODP-группы	<ul style="list-style-type: none"><li>• 786</li><li>• 1024</li><li>• 1536</li><li>• 2048</li><li>• 3072</li><li>• 4096</li><li>• 6144</li><li>• 8192</li></ul>

# Мсм Нэт Майсснер

компетентный - творческий - инновационный

Категория	Детали
Методы связи VPN-устройств	<ul style="list-style-type: none"><li>• IPSEC</li><li>• PPTP</li><li>• L2TP</li></ul>
Схема IP-адреса	<ul style="list-style-type: none"><li>• IPv4 и IPv6 (локальный)</li><li>• статический или динамический</li></ul>
Автоматическое прерывание связи	настраивается
Автоматическое обновление ключа	настраивается
Управление сертификатами	<ul style="list-style-type: none"><li>• Корневой CA или суб-CA сертификаты</li><li>• Проверка подлинности сертификатов</li><li>• CRL и OCSP</li><li>• Crypto Применение смарт-карт</li></ul>
Аутентификация	<ul style="list-style-type: none"><li>• X.509=сертификат настраивается с или без CRL и с или без OCSP</li><li>• Pre-Shared Key</li></ul>
Менеджмент файлов регистрации	<ul style="list-style-type: none"><li>• настраивается</li><li>• посылается по электронной почте</li><li>• посылается системным журналом (Syslog)</li></ul>
Общее резервирование	Управление общим для использования среды передачи и наличия техники VPN

## 4. Запрос на комментарий для программного обеспечения VPN

### Основные запрос на комментарий

- 2401 Security Architecture for the Internet Protocol
- 2411 IP Security Document Roadmap

### Основной протокол

- 2402 IP Authentication Header
- 2406 IP Encapsulation Security Payload (ESP)

### Управление ключами / Key Management

- 2367 PF\_KEY Key Management API, Version 2
- 2407 The Internet IP Security Domain of Interpretation for ISAKMP
- 2408 Internet Security Association and Key Management Protocol (ISAKMP)
- 2409 The Internet Key Exchange (IKE)
- 2412 The OAKLEY Key Determination Protocol
- 2528 Internet X.509 Public Key Infrastructure

### Детали к отдельно Вами использованным компонентам / Details of various things used

- 2085 HMAC-MD5 IP Authentication with Replay Prevention
- 2104 HMAC: Keyed-Hashing for Message Authentication
- 2202 Test Cases for HMAC-MD5 and HMAC-SHA-1
- 2207 RSVP Extensions for IPSEC Data Flows
- 2403 The Use of HMAC-MD5-96 within ESP and AH
- 2404 The Use of HMAC-SHA-1-96 within ESP and AH
- 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV
- 2410 The NULL Encryption Algorithm and Its Use With IPSEC
- 2451 The ESP CBC-Mode Cipher Algorithms
- 2521 ICMP Security Failures Messages

### Возможные отзывы о старых запрос на комментарий / Older RFCs which may be referenced

- 1321 The MD5 Message-Digest Algorithm
- 1828 IP Authentication using Keyed MD5
- 1829 The ESP DES-CBC Transform
- 1851 The ESP Triple DES Transform
- 1852 IP Authentication using Keyed SHA

### Сообщенные запрос на комментарий / Related RFCs

- 1750 Randomness Recommendations for Security
- 1918 Address Allocation for Private Internets
- 1984 IAB and IESG Statement on Cryptographic Technology and the Internet
- 2144 The CAST-128 Encryption Algorithm

## 5. Проектно-ориентированные решения

Для планирования и реализации VPN должны быть приняты во внимание все технические аспекты существующих сетей, а также технический доступ к Интернету и мобильной связи выездных сотрудников.

По этой причине очень важно провести первый фактический анализ на всех унифицируемых участках. Исходя из первого фактического анализа возможно поставить четкую цель со всеми требуемыми и заданиями для реализации.

Для реализации Вашей VPN, мы предлагаем следующие услуги:




- Услуги по консалтингу, планированию и проектированию при создании VPN на международных и национальных условиях
- Создание концепцию режима работы VPN – сетей
- Создание совокупность структуры для определения требований к оборудованию
- Установку, настройку и запуск в эксплуатацию аппаратных и программных компонентов VPN
- Мониторинг и оценка лог-файлов
- Регулярные проверки безопасности
- Сервис удаленный и на месте, техническое обслуживание
- Инструктаж и обучение местных администраторов

С помощью нашей техники возможно создание любое число местных сетей и подключить выездных работников через интернет к VPN.

Для получения дополнительной информации свяжитесь с нами в любое время.



## 6. Варианты VPN – маршрутизатора

<b>Mini-VPN-маршрутизатор</b>	
	<p>Mini VPN маршрутизатор предлагается в очень прочном алюминиевом корпусе размерами (ширина x глубина x высота) 15,5 x 15,5 x 2,5 см.</p> <p>возможный интерфейс:</p> <p style="text-align: center;">2 x 10/100 Мбит</p> <p>Интенсивность информационного потока:</p> <p style="text-align: center;">приблизительно 8 Мбит при 3DES-MD5-2048</p>
<b>Midi-VPN-маршрутизатор</b>	
	<p>Midi-VPN-маршрутизатор может быть использован как автономно, так и в качестве 19" варианта (с глубиной от 22см до 45 см).</p> <p>возможный интерфейс:</p> <p style="text-align: center;">2x 10/100 Мбит, ADSL, ISDN</p> <p>Интенсивность информационного потока:</p> <p style="text-align: center;">приблизительно 35 Мбит при 3DES-MD5-2048</p>
<b>Maxi-VPN-маршрутизатор</b>	
	<p>Maxi-VPN-маршрутизатор предлагается размером в 19" (с глубиной 45 см). При запросе также на серверной платформе.</p> <p>возможный интерфейс:</p> <p style="text-align: center;">2x 10/100/1000 Мбит</p> <p>Интенсивность информационного потока:</p> <p style="text-align: center;">более 200 Мбит при 3DES-MD5-2048</p>

# Мсм Нэт Майсснер

**компетентный - творческий - инновационный**

## Midi-HC-VPN-маршрутизатор



Midi-HC-VPN-маршрутизатор используют AES-шифрования и SHA-аутентификации в Padlock engine VIA C7-процессора.

возможный интерфейс:

2x 10/100/1000 Мбит, TP, SC, ST

Интенсивность информационного потока:

приблизительно 11 Мбит  
при AES128-SHA128-2048  
100 Мбит в зоне сети

приблизительно 25 Мбит  
при AES128-SHA128-2048  
в 1000 Мбит в зоне сети

## Maxi-HC-VPN-маршрутизатор



Midi-HC-VPN-маршрутизатор используют AES-шифрования и SHA-аутентификации в Padlock engine VIA C7-процессора.

возможный интерфейс:

2x 10/100/1000 Мбит, TP, SC, ST

Интенсивность информационного потока:

приблизительно 11 Мбит  
при AES128-SHA128-2048  
в 100 Мбит в зоне сети

приблизительно 110 Мбит  
при AES128-SHA128-2048  
в 1000 Мбит в зоне сети

Специальные требования к разъёмам могут быть реализованы по требованию.

Дополнительное оборудование	Mini маршрутизатор	Midi маршрутизатор	Maxi маршрутизатор
Crypto Применение смарт-карт	✓	✓	✓
Аппаратное шифрование (для приборов без VIA C7 процессора)	✓	✓	✓

Использованию аппаратного шифрования приводит к выполнению очень высоких требований по безопасности и повышению производительности.

## 7. Сервисные услуги и техническое обслуживание

«Мсм Нэт» предлагает для всех своих продуктов обширные сервисные услуги и техническое обслуживание, которые дифференцируются в зависимости от времени звонка и времени на гарантируемое устранение неисправности. Они предлагаются в рамках контракта по техническому обслуживанию.

## 8. Подготовка, обучение и консалтинг

Для эффективного достижения бизнес-целей, квалификация персонала играет большую роль. Мы с радостью обучим Ваших сотрудников по следующим темам:

- Администрация VPN
- Сети продажи и сервиса
- Приложения электронной почты
- Администрация сетей и систем
- Интернет и сбор информации
- Безопасность данных.

## 9. 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