

Table of Contents

Table of Contents	1
Настройка удалённого доступа (VPN)	2
Настройка серверных правил	3
Настройка клиентских правил	5
Настройка сетей VPN	6
Настройка профилей безопасности VPN	7

Настройка серверных правил

Product: DCFW
Version: 8.x
Technology: VPN

Серверные правила настраиваются на уровне **vpn server-rules**. Подробнее о структуре команд настройки серверных правил читайте в разделе [UserGate Policy Language](#).

Для создания серверного правила VPN используется команда:

```
Admin@nodename# create vpn server-rules <position> upl-rule <parameters>
```

При настройке необходимо указать:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: • enabled(yes) или enabled(true). • enabled(no) или enabled(false). Если при создании правила не указывать, то правило будет включено после создания.
name	Название серверного правила VPN. Например: name("VPN server rule example") .
desc	Описание правила. Например: desc("VPN server rule example configured in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
vpn_network	Сеть VPN. Для указания сети: vpn_network("VPN network example") . О настройках сети VPN с использованием интерфейса командной строки читайте в разделе Настройка сетей VPN .
auth_profile	Профиль аутентификации для пользователей VPN. Допускается использовать тот же профиль аутентификации, что используется для авторизации пользователей для получения доступа к сети интернет. Следует учесть, что для авторизации VPN нельзя использовать методы прозрачной аутентификации, такие как Kerberos, NTLM, SAML IDP. Чтобы указать профиль аутентификации: auth_profile("Example user auth profile") . Подробнее о создании и настройке профилей аутентификации с использованием интерфейса командной строки читайте в разделе Настройка профилей аутентификации .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel1) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
ep_only	Опция (доступна начиная с релиза ПО 7.1.2) позволяет ограничить возможность подключения по данному правилу только для VPN-клиентов UserGate Client (true , false).
src.zone	Зона, с которой разрешено принимать подключения к VPN. Для указания зоны источника, например, Untrusted: src.zone = Untrusted . Подробнее о настройке зон с использованием интерфейса командной строки читайте в разделе Зоны .
src.ip	Добавление списков IP-адресов или доменов, с которых разрешено принимать подключения к VPN. Для указания списка IP-адресов: src.ip = lib.network() ; в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов . Для указания списка доменов источника: src.ip = lib.url() ; в скобках необходимо указать название URL, в который были добавлены необходимые домены. Подробнее о создании и настройке списков URL с использованием интерфейса командной строки читайте в разделе Настройка списков URL .

Параметр	Описание
user	Пользователи и группы пользователей, которым разрешено подключение по VPN. Для добавления LDAP групп и пользователей необходим корректно настроенный LDAP-коннектор (о настройке LDAP-коннектора через CLI читайте в разделе Настройка LDAP-коннектора). В следующей строке описано добавление локального пользователя (local_user) и группы (Local Group), пользователя (example.local\AD_user) и группы LDAP (AD group): <pre>user = (local_user, "CN=Local Group,DC=LOCAL", "example.loc\AD_user", "CN=AD group,OU=Example,DC=example,DC=loc")</pre> Заранее был настроен домен Active Directory example.loc. При добавлении пользователей и групп LDAP можно указать список путей на сервере, начиная с которых система будет осуществлять поиск пользователей и групп.
dst.ip	Добавление списков IP-адресов интерфейса, на который будет происходить подключение клиентов. Для указания списка IP-адресов: dst.ip = lib.network(); в скобках необходимо указать название списка. Подробнее о создании и настройке списков IP-адресов с использованием CLI читайте в разделе Настройка IP-адресов.

Пример создания серверного правила VPN:

```
Admin@nodename# create vpn server-rules 3 upl-rule OK\
...name("Test server VPN rule") \
...desc("Test server VPN rule description") \
...profile("New server VPN profile") \
...vpn_network("Test VPN network") \
...auth_profile(Local) \
...interface(tunnel3) \
...src.zone = Untrusted \
...dst.ip = lib.network("UG address") \
...user = ("CN=VPN servers,DC=LOCAL") \
...enabled(true) \
```

Для редактирования серверного правила VPN:

```
Admin@nodename# set vpn server-rules <position> upl-rule <parameters>
```

Для удаления серверных правил VPN:

```
Admin@nodename# delete vpn server-rules <position>
```

Для просмотра сконфигурированных серверных правил VPN:

```
Admin@nodename# show vpn server-rules <position>
```

Настройка клиентских правил

Product: DCFW
Version: 8.x
Technology: VPN

Клиентские правила настраиваются на уровне **vpn client-rules**. Подробнее о структурах команд настройки клиентских правил читайте в разделе [UserGate Policy Language](#).

Команда для создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules <position> upl-rule <parameters>
```

При настройке правил необходимо указать:

Параметр	Описание
PASS OK	Действие для создания правила с помощью UPL.
enabled	Включение/отключение правила: enabled(yes) или enabled(true). enabled(no) или enabled(false).
name	Название клиентского правила VPN. Например, name("VPN client rule example") .
desc	Описание клиентского правила VPN. Указывается, как desc("VPN client rule example set in CLI") .
profile	Профиль безопасности VPN, определяющий общий ключ шифрования (pre-shared key) и алгоритмы для шифрования и аутентификации. Например, profile("Client VPN profile") . Подробнее о добавлении и настройке профилей безопасности читайте в разделе Настройка профилей безопасности VPN .
interface	VPN-интерфейс, который будет использоваться для подключения клиентов VPN. Чтобы указать интерфейс, например, tunnel1: interface(tunnel3) . О добавлении и настройке интерфейсов VPN читайте в разделе Настройка VPN-адаптера .
server_address	IP-адрес VPN-сервера, куда подключается данный VPN-клиент. Как правило, это IP-адрес интерфейса в зоне Untrusted на NGFW, выполняющего роль VPN-сервера. Задаётся в формате: server_address("1.2.3.4") .

При отображении правил, помимо заданных условий и свойств, будут показаны последняя ошибка VPN, статус подключения и время соединения.

Пример создания клиентского правила VPN:

```
Admin@nodename# create vpn client-rules 2 upl-rule OK\  
...name("Test VPN client rule") \  
...desc("Test VPN client rule description") \  
...profile("Client VPN profile") \  
...interface(tunnel3) \  
...server_address("10.10.0.1") \  
...enabled(true) \  

```

Для редактирования клиентского правила VPN:

```
Admin@nodename# set vpn client-rules <position> upl-rule <parameters>
```

Для удаления клиентского правила VPN:

```
Admin@nodename# delete vpn client-rules <position>
```

Для просмотра параметров созданных клиентских правил VPN:

```
Admin@nodename# show vpn client-rules <position>
```

Настройка сетей VPN

Product: DCFW
Version: 8.x
Technology: VPN

Настройка VPN-сетей производится на уровне **vpn networks**.

Для создания сети VPN необходимо использовать следующую команду:

```
Admin@nodename# create vpn networks <parameters>
```

Настраиваемые параметры сети VPN:

Параметр	Описание
name	Название сети VPN.
description	Описание сети VPN.
ip-range	Диапазон IP-адресов, которые будут использованы клиентами и сервером; указывается в формате: <IP_start-IP_end>. Исключите из диапазона адреса, которые назначены VPN-интерфейсу, используемому совместно с данной сетью. Не указывайте здесь адреса сети и широковещательный адрес.
mask	Маска сети, например, 255.255.255.0.
use-system-dns	Назначение клиенту DNS-серверов, которые использует UserGate: • on: использовать системных DNS-серверов. • off: не использовать системных DNS-серверов.
dns-servers	DNS-серверы, которые будут переданы клиенту.
routes-ip	Маршрут VPN. Необходимо указать IP-адрес в формате "A.B.C.D" или "A.B.C.D/m".
routes-ip-list	Маршрут VPN. Необходимо указать группу IP-адресов. Подробнее о создании групп IP-адресов через CLI читайте в разделе Настройка IP-адресов .
all-routes	Отсутствие ограничений на маршрутизацию по VPN соединению при использовании UserGate VPN клиента.
include-routes-ip	IP-адреса, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
include-routes-ip-list	Список IP-адресов, доступ к которым должен маршрутизироваться через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip	IP-адреса, доступ к которым зарыт через VPN соединение при использовании UserGate VPN клиента.
exclude-routes-ip-list	Список IP-адресов, доступ к которым закрыт через VPN соединение при использовании UserGate VPN клиента.
restrict-lan-access	Запрет доступа к локальной сети при использовании UserGate VPN клиента.

Пример команды создания сети VPN:

```
Admin@nodename# create vpn networks name "Test VPN network" description "This is a new test VPN network" ip-range 10.10.3.2-10.10.2.200 mask 255.255.255.0
```

Редактирование параметров сети:

```
Admin@nodename# set vpn networks <network-name> <parameters>
```

Удаление сети VPN или отдельных параметров сети VPN:

```
Admin@nodename# delete vpn networks <network-name>
```

Просмотр информации о сети VPN:

```
Admin@nodename# show vpn networks <network-name>
```

Настройка профилей безопасности VPN

Product: DCFW
Version: 8.x
Technology: VPN

Начиная с версии nodename 7.1.0 определены два типа профилей безопасности VPN — серверные и клиентские.
Профили безопасности VPN настраиваются на уровне **vpn server-security-profiles** и **vpn client-security-profiles**.

Создание серверного профиля безопасности VPN

Для создания серверного профиля безопасности VPN предназначена следующая команда:
`Admin@nodename# create vpn server-security-profiles <parameters>`
Настраиваемые параметры серверного профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Версия протокола, используемого для создания защищённого канала связи между двумя сетями. Возможны следующие варианты: - ipsec — IPsec(IKEv1). - ipsec-l2tp — IPsec(IKEv1)/L2TP. - ikev2 — IPsec(IKEv2).
ike-mode	Режим IKE: - main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. - aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.
local-id-type	Тип параметра IKE local ID. Необходим для валидации реер-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: - none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. - IPv4 — IP-адрес узла. - FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). - CIDR — Адрес узла в формате бесклассовой адресации (CIDR).
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
authentication-mode	Метод аутентификации. Возможна аутентификация с помощью логина и пароля посредством метода EAP (AAA) или посредством сертификатов (PKI).
user-certificate-profile	При выборе метода аутентификации с PKI необходимо указать сконфигурированный ранее профиль клиентских сертификатов.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.

Параметр	Описание
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: • off — Механизм отключен. DPD запросы не отсылаются. • always — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. • idle — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. • Group 1 Prime 768 bit. • Group 2 Prime 1024 bit. • Group 5 Prime 1536 bit. • Group 14 Prime 2048 bit. • Group 15 Prime 3072 bit. • Group 16 Prime 4096 bit. • Group 17 Prime 6144 bit. • Group 18 Prime 8192 bit.
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn server-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifese-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifese	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifese), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off.

Параметр	Описание
nat-keepalive	Период отправки пакетов NAT keealive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keealive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keealive в сторону реер-узла для поддержания сессии NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn server-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: auth-alg: выбор алгоритма аутентификации. MD5. SHA1. SHA256. SHA384. SHA512. encrypt-alg: выбор алгоритма шифрования. DES. 3DES. AES128. AES192. AES256.

Создание клиентского профиля безопасности VPN

Для создания клиентского профиля безопасности VPN предназначена следующая команда:

```
Admin@nodename# create vpn client-security-profiles <parameter>
```

Настраиваемые параметры клиентского профиля безопасности VPN:

Параметр	Описание
name	Название профиля безопасности VPN.
description	Описание профиля безопасности VPN.
protocol	Протокол установления VPN канала. Возможны следующие варианты выбора поля: ipsec-l2tp — IPsec(IKEv1)/L2TP VPN. ipsec — IPsec(IKEv1) VPN с оборудованием сторонних производителей. ikev2 — IPsec(IKEv2) VPN.
ike-mode	Режим IKE: main — основной режим. В основном режиме происходит обмен шестью сообщениями. Во время первого обмена (сообщения 1 и 2) происходит согласование алгоритмов шифрования и аутентификации. Второй обмен (сообщения 3 и 4) предназначен для обмена ключами Диффи-Хеллмана (DH). После второго обмена служба IKE на каждом из устройств создаёт основной ключ, который будет использоваться для защиты проверки подлинности. Третий обмен (сообщения 5 и 6) предусматривает аутентификацию инициатора соединения и получателя (проверка подлинности); информация защищена алгоритмом шифрования, установленным ранее. aggressive — агрессивный режим. В агрессивном режиме происходит 2 обмена, всего 3 сообщения. В первом сообщении инициатор передаёт информацию, соответствующую сообщениям 1 и 3 основного режима, т.е. информацию об алгоритмах шифрования и аутентификации и ключ DH. Второе сообщение предназначено для передачи получателем информации, соответствующей сообщениям 2 и 4 основного режима, а также аутентификации получателя. Третье сообщение аутентифицирует инициатора и подтверждает обмен.

Параметр	Описание
local-id-type	Тип параметра IKE local ID. Необходим для валидации реер-узла при установлении VPN-соединения с оборудованием некоторых вендоров. Возможные значения параметра: none — значение поля по умолчанию. Используется в случае, когда для установления VPN-соединения не требуется использовать параметр IKE local ID. Например, для установления VPN-соединения между двумя узлами UserGate. IPv4 — IP-адрес узла. FQDN — Адрес узла в формате полностью определенного доменного имени (FQDN). CIDR — Адрес узла в формате бесклассовой адресации (CIDR).
local-id-value	Значение параметра IKE local ID в формате выбранного ранее типа.
psk	Общий ключ. Для аутентификации удаленного узла с использованием общего ключа (Pre-shared key). Строка, которая должна совпадать на сервере и клиенте для успешного подключения.
authentication-login	Логин, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.
authentication-password	Пароль, созданный ранее на VPN-сервере для аутентификации узла, работающего как VPN-клиент.
certificate	Сертификат VPN сервера для аутентификации посредством сертификатов.
vpn-local-network	IP-адрес разрешенной локальной подсети для организации VPN с узлом Cisco.
vpn-remote-network	IP-адрес разрешенной подсети со стороны удаленного VPN-сервера для организации VPN с узлом Cisco.
phase1-key-lifetime	Время жизни ключа. По истечению данного времени происходят повторные аутентификация и согласование настроек первой фазы.
dpd-state	Режимы работы механизма Dead Peer Detection, реализующего проверку работоспособности VPN канала и его своевременного отключения/переподключения при обрыве связи. Возможны 3 режима работы механизма: off — Механизм отключен. DPD запросы не отсылаются. always — DPD запросы всегда отсылаются через указанный интервал времени. Если ответ не пришел, последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если ответ есть, работа механизма возвращается к изначальному интервалу отправки DPD запросов, если нет ни одного ответа, соединение завершается. idle — DPD запросы не отсылаются, пока есть ESP трафик через созданные SA. Если в течение двойного указанного интервала времени нет ни одного пакета, тогда производится отсылка DPD запроса. При ответе новый DPD запрос будет отправлен снова через двойной интервал указанного времени. При отсутствии ответа последовательно с интервалом 5 сек отсылаются дополнительные запросы в количестве, указанном в параметре dpd-max-failures. Если нет ни одного ответа, соединение завершается.
dpd-interval	Интервал проверки механизма Dead Peer Detection. Минимальный интервал: 10 секунд. Для проверки состояния и доступности соседних устройств используется механизм Dead Peer Detection (DPD). DPD периодически отправляет сообщения R-U-THERE для проверки доступности IPsec-соседа (по умолчанию: 60 с.).
dpd-max-failures	Максимальное количество запросов обнаружения недоступных IPsec-соседей, которое необходимо отправить до того, как IPsec-сосед будет признан недоступным (по умолчанию: 5).
dh-groups	Группы Диффи-Хеллмана, которые будут использоваться для обмена ключами. Сам ключ не передаётся, а передаются общие сведения, необходимые алгоритму определения ключа DH для создания общего секретного ключа. Чем больше номер группы Диффи-Хеллмана, тем больше бит используется для обеспечения надёжности ключа. Group 1 Prime 768 bit. Group 2 Prime 1024 bit. Group 5 Prime 1536 bit. Group 14 Prime 2048 bit. Group 15 Prime 3072 bit. Group 16 Prime 4096 bit. Group 17 Prime 6144 bit. Group 18 Prime 8192 bit.

Параметр	Описание
phase1-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn client-security-profiles ... phase1-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.
phase2-key-lifetime	Время жизни ключа. По истечению данного времени узлы должны сменить ключ шифрования. Время жизни, заданное во второй фазе, меньше, чем у первой фазы, т.к. ключ необходимо менять чаще.
key-lifese-enabled	Включение режима настройки максимальный размер данных, шифруемых одним ключом.
key-lifese	Максимальный размер данных, шифруемых одним ключом; указывается в килобайтах. Если заданы оба значения (Время жизни ключа, phase2-key-lifetime и Максимальный размер данных, шифруемых одним ключом, key-lifese), то счётчик, первый достигнувший лимита, запустит пересоздание ключей сессии. Для отключения ограничения: off.
nat-keepalive	Период отправки пакетов NAT keealive в секундах (возможные значения 0 или больше 4). Применяется в сценариях, когда IPsec трафик проходит через узел с NAT. Записи в таблице трансляций NAT активны в течение ограниченного времени. Если за этот промежуток времени не было трафика по VPN туннелю, записи в таблице трансляций на узле с NAT будут удалены и трафик по VPN туннелю в дальнейшем не сможет проходить. С помощью функции NAT keealive VPN-сервер, находящийся за шлюзом NAT, периодически отправляет пакеты keealive в сторону реер-узла для поддержания сессии NAT активной.
phase2-security	Алгоритмы аутентификации и шифрования. Для указания алгоритмов аутентификации и шифрования: <pre>Admin@nodename# create vpn client-security-profiles ... phase2-security new auth-alg <auth-alg-name> encrypt-alg <encrypt-alg-name></pre> Доступны: • auth-alg: выбор алгоритма аутентификации. ◦ MD5. ◦ SHA1. ◦ SHA256. ◦ SHA384. ◦ SHA512. • encrypt-alg: выбор алгоритма шифрования. ◦ DES. ◦ 3DES. ◦ AES128. ◦ AES192. ◦ AES256.

Примеры создания и редактирования профилей безопасности VPN

Создание нового профиля безопасности VPN:

```
Admin@nodename# create vpn server-security-profiles <profile-name> <parameters>
```

```
Admin@nodename# create vpn client-security-profiles <profile-name> <parameters>
```

...

```
Admin@nodename# create vpn server-security-profiles name "New server VPN profile"
```

Редактирование параметров профиля безопасности VPN:

```
Admin@nodename# set vpn server-security-profiles <profile-name> <parameters>
```

```
Admin@nodename set vpn client-security-profiles <profile-name> <parameters>
```

...

```
Admin@nodename# set vpn server-security-profiles "New server VPN profile" phase1-security [ SHA1/AES128 SHA1/3DES ] phase2-security [ SHA1/AES128 SHA1/3DES ]
```

```
Admin@nodename# set vpn server-security-profiles "New server VPN profile" dh-groups [ "Group 16 Prime 4096 bit" ]
```

```
Admin@nodename# set vpn server-security-profiles "New server VPN profile" nat-keepalive 20
```

Удаление параметров профиля безопасности VPN:

```
Admin@nodename# delete vpn server-security-profiles <profile-name> <parameters>
```

```
Admin@nodename# delete vpn client-security-profiles <profile-name> <parameters>
```

...

```
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" phase1-security [ MD5/AES128 ]
```

```
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" phase2-security [ MD5/AES128 ]
```

```
Admin@nodename# delete vpn server-security-profiles "New server VPN profile" dh-groups [ "Group 16 Prime 4096 bit" ]
```

Просмотр информации о сконфигурированных профилях безопасности VPN:

```
Admin@nodename# show vpn server-security-profiles <profile-name>
```

```
Admin@nodename# show vpn client-security-profiles <profile-name>
```

...

```
Admin@nodename# show vpn client-security-profiles "New client VPN profile"
```

