

Решение с резервированием канала. Аутентификация на Preshared Key

Описание стенда

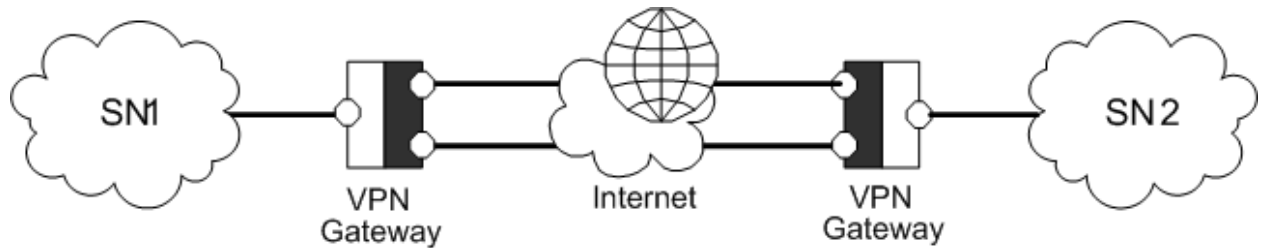


Рис. 1. Общая схема подключения

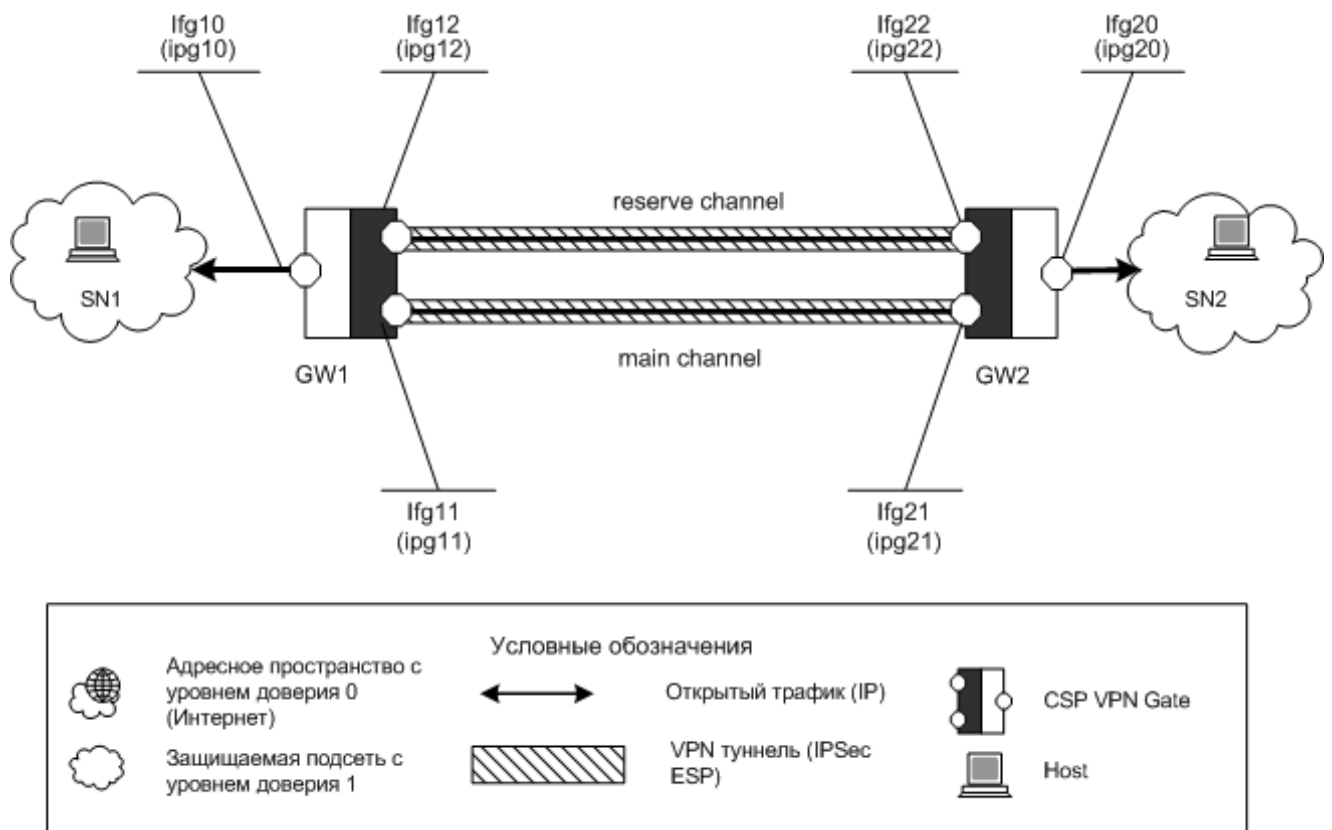


Рис. 2 Схема стенда

В представленном сценарии два шлюза безопасности GW1 и GW2, защищающие подсети SN1 и SN2, соединены между собой двумя разными каналами: main channel (например Ethernet) и reserve channel (например GPRS), по которым идет защищенный трафик.

Примечание: здесь и далее предполагаем, что все интерфейсы шлюзов безопасности имеют фиксированные имена.

Логика работы решения

В предложенном решении реализована следующая логика:

- На шлюзах безопасности GW1 и GW2 установлен продукт CSP VPN Gate
- Основной режим работы (при отсутствии сбоев) – защищенный трафик между двумя подсетями идет по основному каналу через GW1 и GW2.
- Во время работы осуществляется постоянный мониторинг состояния основного канала (с помощью ping). В случае, если основной канал не работает (отсутствует ping), происходит переключение защищенного трафика на резервный канал.
- Во время работы по резервному каналу мониторинг состояния основного канала продолжается. Если обнаружено, что основной канал заработал, происходит обратное переключение защищенного трафика с резервного канала на основной.
- Предложено решение с переключением LSP. Существуют две LSP: одна для работы по основному каналу, другая – по резервному. Различие в этих LSP состоит в разных туннельных адресах.
- Для мониторинга состояния основного канала по нему производится периодический ping.
 - В случае стабильного отсутствия ping (единичные потери игнорируются во избежание случайных срабатываний), происходит переключение на резервный канал:
 - Прописывается роутинг между двумя подсетями так, чтобы он проходил через резервный канал.
 - Загружается LSP, в которой прописан альтернативный туннельный адрес (резервный канал).
 - Если идет трафик по резервному каналу и обнаружено, что связь по основному каналу восстановлена (в этом случае достаточно единичного успешного ping) – происходит обратное переключение на основной канал:
 - Прописывается роутинг между двумя подсетями так, чтобы он проходил через основной канал.
 - Загружается LSP, в которой прописан основной туннельный адрес (основной канал).
 - Переключение каналов, запуск и остановка резервного канала производится с помощью скриптов, устанавливаемых на шлюзы безопасности.

Параметры защищенного соединения

Параметры защищенного соединения между подсетями SN1 и SN2:

- Аутентификация на Preshared Key.
- IKE parameters:
 - Encryption algorithm – GOST
 - Hash algorithm – GOST
 - DH-group – group1 (768)
- IPSec parameters:
 - ESP encryption algorithm – GOST

Основные шаги по настройке устройств стенда

Настройку каждого из шлюзов безопасности GW1 и GW2 проведем по следующему плану:

- Установка скрипта для переключения каналов, настройка его параметров
- Установка скрипта для запуска и остановки резервного каналов

- Регистрация в продукте Preshared Key
- Создание политики безопасности (LSP) для работы по основному каналу. Настройка параметров.
- Создание политики безопасности (LSP) для работы по резервному каналу. Настройка параметров.

Настройка шлюза безопасности GW1

Установка скриптов

На шлюз безопасности GW1 нужно установить два скрипта. Один скрипт будет отвечать за переключение каналов (`vpn_reserve_channel`), а второй - за запуск и остановку резервного канала (`vpn_reserve_chan_init`).

Скрипт `vpn_reserve_channel`

В данном скрипте [настраиваем некоторые параметры](#), сохраняем его в директории `/etc/init.d` под именем `vpn_reserve_channel` и выполняем для него:

```
chmod a+x vpn_reserve_channel
```

Текст скрипта `vpn_reserve_channel`:

```
#!/bin/ksh

LOCAL_MAIN_NAME=pcn1
LOCAL_MAIN_PARAM=10.1.1.1/24

LOCAL_RESERVE_NAME=pcn2
LOCAL_RESERVE_PARAM=10.2.1.1/24

REMOTE_MAIN_IP=10.1.1.2
REMOTE_RESERVE_IP=10.2.1.2

REMOTE_NET=10.0.2.0/24

CHECK_N=3

PING=/usr/sbin/ping
ROUTE=/usr/sbin/route

MAIN_CHANNEL_LSP=main_channel_lsp.txt
RESERVE_CHANNEL_LSP=reserve_channel_lsp.txt

do_ping()
{
    $PING $REMOTE_MAIN_IP 1 > /dev/null
}
```

```
notify()
{
    logger -p local0.notice "$1"
    echo `date` "$1" > /dev/console
}

on_fail()
{
    route delete $REMOTE_NET $REMOTE_MAIN_IP > /dev/null
    route add $REMOTE_NET $REMOTE_RESERVE_IP > /dev/null
    ./lsp_mgr load -f $RESERVE_CHANNEL_LSP > /dev/null
    notify 'Reserve channel is used'
}

on_ok()
{
    route delete $REMOTE_NET $REMOTE_RESERVE_IP > /dev/null
    route add $REMOTE_NET $REMOTE_MAIN_IP > /dev/null
    ./lsp_mgr load -f $MAIN_CHANNEL_LSP > /dev/null
    notify 'Main channel is used'
}

cd /opt/VPNagent/bin

ifconfig $LOCAL_MAIN_NAME $LOCAL_MAIN_PARAM broadcast + up 2> /dev/null
ifconfig $LOCAL_RESERVE_NAME $LOCAL_RESERVE_PARAM broadcast + up 2> /dev/null

if do_ping; then
    RETRY_COUNT=$CHECK_N
    on_ok
else
    RETRY_COUNT=0
    on_fail
fi

while true; do
    if [[ $RETRY_COUNT -gt 0 ]]; then
        if do_ping; then
            RETRY_COUNT=$CHECK_N
        else
            RETRY_COUNT=$((RETRY_COUNT-1))
            if [ $RETRY_COUNT -eq 0 ]; then
                on_fail
            fi
        fi
    fi
done
```

```

fi

if [[ $RETRY_COUNT -gt 0 ]]; then
    sleep 1
fi
else
    if do_ping; then
        RETRY_COUNT=$CHECK_N
        on_ok
    fi
fi
done

```

Описание настраиваемых параметров скрипта `vpn_reserve_channel`

Внутри скрипта необходимо настроить следующие параметры:

`LOCAL_MAIN_NAME` - имя сетевого интерфейса, подключенного к основному каналу (`ifg11` на схеме).

`LOCAL_MAIN_PARAM` - параметры интерфейса `ifg11`: IP-адрес (`ipg11`) и длина префикса (количество единиц в сетевой маске).

`LOCAL_RESERVE_NAME` - имя сетевого интерфейса, подключенного к резервному каналу (`ifg12`).

`LOCAL_RESERVE_PARAM` - параметры интерфейса `ifg12`: IP-адрес (`ipg12`) и длина префикса (количество единиц в сетевой маске).

`REMOTE_MAIN_IP` - IP-адрес интерфейса `GW2`, подключенного к основному каналу (`ipg21`).

`REMOTE_RESERVE_IP` - IP-адрес интерфейса `GW2`, подключенного к резервному каналу (`ipg22`).

`REMOTE_NET` - параметры сети, защищаемой `GW2` (`net2`): адрес сети и длина префикса (количество единиц в сетевой маске).

`CHECK_N` - количество неуспешных попыток `ping-a`, после которых считается, что связи нет. Чем меньше данное число, тем быстрее срабатывает переключение интерфейсов, но тем больше вероятность ложных срабатываний.

Функция `notify` задает команды оповещения о переключениях на резервный канал с основного и наоборот – с резервного на основной. В данную функцию передается строка сообщения для вывода. В командах эта строка задается как `$1`. В данном примере заданы две команды: одна отправляет сообщение в `syslog` с `facility local0` и `severity notice`, а другая - выдает сообщение на системную консоль.

Скрипт для запуска и остановки скрипта `vpn_reserve_channel` (одинаковый для обоих гейтов)

Данный скрипт надо сохранить в директории `/etc/init.d` под именем `vpn_reserve_chan_init` и выполнить для него:

```
chmod a+x vpn_reserve_chan_init
```

Тело скрипта `vpn_reserve_chan_init`:

```
#!/bin/sh

RESERVE_CHANNEL_SCRIPT=/etc/init.d/vpn_reserve_channel

```

```

PS=/usr/bin/ps
GREP=/usr/bin/grep
KILL=/usr/bin/kill
AWK=/usr/bin/awk

case $1 in
'start')
    $RESERVE_CHANNEL_SCRIPT &
    ;;
'stop')
    PID=`$PS -ef | $GREP -v grep | $GREP $RESERVE_CHANNEL_SCRIPT | $AWK '{print $2}'`
    if [ ! -z "$PID" ] ; then
        /usr/bin/kill $PID 1> /dev/null 2>&1
    fi
    ;;
*)
    echo "Usage: vpn_reserve_chan_init { start | stop }"
    ;;
esac

```

Для того, чтобы скрипт вызывался при StartUp-е и останавливался при Shutdown-е, необходимо сделать линки на скрипт `vpn_main_gate_init`:

```

ln -s /etc/init.d/vpn_reserve_chan_init /etc/rc2.d/S22vpn_reserve_chan_init
ln -s /etc/init.d/vpn_reserve_chan_init /etc/rc0.d/K91vpn_reserve_chan_init

```

При необходимости скрипт `vpn_reserve_chan_init` можно запускать и останавливать вручную:

```

/etc/init.d/vpn_reserve_chan_init start | stop

```

Регистрация Preshared Key

Перед регистрацией ключа запишите значение ключа в файл. Для регистрации ключа с именем `reserve_channel_key` используйте утилиту `key_mgr import`, входящую в состав CSP VPN Gate:

```

/opt/VPNagent/bin/key_mgr import -n reserve_channel_key -f <key_file_path>,

```

где `<key_file_path>` – путь к файлу, содержащему значение ключа. На шлюзе безопасности GW2 должен регистрироваться ключ, имеющий такое же значение.

Создание LSP для работы по основному каналу для GW1

Приступим к настройке CSP VPN Gate, установленного на шлюзе безопасности GW1. Создадим конфигурацию (LSP), по которой:

- Разрешается открытый доступ по SSH (для удаленного управления GW1).
- Разрешается открытый трафик по протоколу ICMP между двумя гейтами по основному каналу (ping для мониторинга состояния канала).

- Защищенный трафик (ESP, ГОСТ) между двумя подсетями. Используется аутентификация (ГОСТ) на `preshared key`.
- Весь остальной трафик запрещен.

Описанную ниже LSP положите в файл `main_channel_lsp.txt`, [настройте некоторые параметры](#), а затем доставьте на шлюз безопасности GW1 в `/opt/VPNagent/bin/`.

```
const LOCAL_MAIN_IP=10.1.1.1
const REMOTE_MAIN_IP=10.1.1.2
const LOCAL_MAIN_NAME="pcn1"
const INNER_IFS_NAME="pcn0"
const LOCAL_NET=10.0.1.0/24
const REMOTE_NET=10.0.2.0/24

GlobalParameters(
    Title                = "Main channel LSP (GW1)"
    Version              = "2.1"
)

IKETransform IKETransform_10(
    CipherAlg    *= "G2814789CPR01-K256-CBC-65534"
    HashAlg     *= "GR341194CPR01-65534"
    GroupID     *= MODP_768
    LifetimeSeconds = 86400
)

ESPProposal transform1(
    Transform* = ESPTransform(
        CipherAlg*      = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodPreshared IKE_auth_key(
    LocalID = IdentityEntry(
        IPv4Address *= LOCAL_MAIN_IP
    )
    RemoteID = IdentityEntry(
        IPv4Address *= REMOTE_MAIN_IP
    )
    SharedIKESecret = "reserve_channel_key"
)

IKERule IKE_cmap_1(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_key
    MainModeAuthMethod *= IKE_auth_key
    DoAutopass         = TRUE
)

IPsecAction cmap_1(
```

```

    TunnelingParameters *= TunnelEntry(
        LocalIPAddress = LOCAL_MAIN_IP
        PeerIPAddress = REMOTE_MAIN_IP
    )
    ContainedProposals *= ( transform1 )
    IKERule = IKE_cmap_1
)
# SSH clear traffic to allow management of the gate
FilteringRule FilterSshPass(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 Port *= 22 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 )
    Action *= ( PASS )
)
# Ping to check main channel
FilteringRule FilterCheckPingPass(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_MAIN_IP ProtocolID *= 1 )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_MAIN_IP ProtocolID *= 1 )
    NetworkInterfaces *= LOCAL_MAIN_NAME
    Action *= ( PASS )
)
FilteringRule FilterTunnel(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_NET )
    NetworkInterfaces *= LOCAL_MAIN_NAME
    Action *= ( cmap_1 )
)
FilteringRule FilterInnerPass(
    LocalIPFilter *= FilterEntry( IPAddress *= REMOTE_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= LOCAL_NET )
    NetworkInterfaces *= INNER_IFS_NAME
    Action *= ( PASS )
)
FilteringRule FilterDrop(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    Action *= ( DROP )
)

```

Настройка параметров LSP в файле main_channel_lsp.txt

В конфигурации, записанной в файл `main_channel_lsp.txt`, настройте следующие параметры:

LOCAL_MAIN_IP - IP-адрес локального интерфейса, подключенного к основному каналу (ipg11).

REMOTE_MAIN_IP - IP-адрес интерфейса GW2, подключенного к основному каналу (ipg21).

LOCAL_MAIN_NAME - имя сетевого интерфейса, подключенного к основному каналу (ifg11).

INNER_IFS_NAME - имя сетевого интерфейса, подключенного в защищаемую подсеть (ifg10).

LOCAL_NET - параметры защищаемой сети SN1: адрес сети и длина префикса (количество единиц в сетевой маске).

REMOTE_NET - параметры сети SN2, защищаемой GW2: адрес сети и длина префикса (количество единиц в сетевой маске).

Создание LSP для работы по резервному каналу для GW1

Описанную ниже LSP положите в файл `reserve_channel_lsp.txt`, [настройте некоторые параметры](#), а затем доставьте на шлюз безопасности GW1 в `/opt/VPNagent/bin/`.

```
const LOCAL_MAIN_IP=10.1.1.1
const REMOTE_MAIN_IP=10.1.1.2
const LOCAL_RESERVE_IP=10.2.1.1
const REMOTE_RESERVE_IP=10.2.1.2
const LOCAL_MAIN_NAME="pcn1"
const LOCAL_RESERVE_NAME="pcn2"
const INNER_IFS_NAME="pcn0"
const LOCAL_NET=10.0.1.0/24
const REMOTE_NET=10.0.2.0/24

GlobalParameters(
    Title                = "Reserve channel LSP (GW1)"
    Version              = "2.1"
)

IKETransform IKETransform_10(
    CipherAlg    *= "G2814789CPR01-K256-CBC-65534"
    HashAlg     *= "GR341194CPR01-65534"
    GroupID     *= MODP_768
    LifetimeSeconds = 86400
)

ESPProposal transform1(
    Transform* = ESPTransform(
        CipherAlg*      = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
)

AuthMethodPreshared IKE_auth_key(
    LocalID = IdentityEntry(
        IPv4Address *= LOCAL_RESERVE_IP
    )
    RemoteID = IdentityEntry(
```

```

        IPv4Address *= REMOTE_RESERVE_IP
    )
    SharedIKESecret = "reserve_channel_key"
)
IKERule IKE_cmap_1(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_key
    MainModeAuthMethod *= IKE_auth_key
    DoAutopass          = TRUE
)
IPsecAction cmap_1(
    TunnelingParameters *= TunnelEntry(
        LocalIPAddress = LOCAL_RESERVE_IP
        PeerIPAddress  = REMOTE_RESERVE_IP
    )
    ContainedProposals *= ( transform1 )
    IKERule = IKE_cmap_1
)
# SSH clear traffic to allow management of the gate
FilteringRule FilterSshPass(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 Port *= 22 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 )
    Action *= ( PASS )
)
# Ping to check main channel
FilteringRule FilterCheckPingPass(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_MAIN_IP ProtocolID *= 1 )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_MAIN_IP ProtocolID *= 1 )
    NetworkInterfaces *= LOCAL_MAIN_NAME
    Action *= ( PASS )
)
FilteringRule FilterTunnel(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_NET )
    NetworkInterfaces *= LOCAL_RESERVE_NAME
    Action *= ( cmap_1 )
)
FilteringRule FilterInnerPass(
    LocalIPFilter *= FilterEntry( IPAddress *= REMOTE_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= LOCAL_NET )
    NetworkInterfaces *= INNER_IFS_NAME
    Action *= ( PASS )
)
FilteringRule FilterDrop(

```

```

LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
Action *= ( DROP )
)

```

Настройка параметров LSP в файле `reserve_channel_lsp.txt`

В конфигурации, записанной в файл `reserve_channel_lsp.txt`, настройте следующие параметры:

LOCAL_MAIN_IP - IP-адрес локального интерфейса, подключенного к основному каналу (ipg11).

REMOTE_MAIN_IP - IP-адрес интерфейса GW2, подключенного к основному каналу (ipg21).

LOCAL_RESERVE_IP - IP-адрес локального интерфейса, подключенного к резервному каналу (ipg12).

REMOTE_RESERVE_IP - IP-адрес интерфейса GW2, подключенного к резервному каналу (ipg22).

LOCAL_MAIN_NAME - имя сетевого интерфейса, подключенного к основному каналу (ifg11).

LOCAL_RESERVE_NAME - имя сетевого интерфейса, подключенного к резервному каналу (ifg12).

INNER_IFS_NAME - имя сетевого интерфейса, подключенного в защищаемую подсеть (ifg10).

LOCAL_NET - параметры защищаемой сети SN1: адрес сети и длина префикса (количество единиц в сетевой маске).

REMOTE_NET - параметры сети SN2, защищаемой GW2: адрес сети и длина префикса (количество единиц в сетевой маске).

Настройка шлюза безопасности GW2

Установка скриптов

На шлюз безопасности GW2 нужно установить два скрипта. Один скрипт будет отвечать за переключение каналов (`vpn_reserve_channel`), а второй - за запуск и остановку резервного канала (`vpn_reserve_chan_init`).

Скрипт `vpn_reserve_channel`

В данном скрипте [настройте некоторые параметры](#), сохраните в директории `/etc/init.d` под именем `vpn_reserve_channel` и выполните для него:

```
chmod a+x vpn_reserve_channel
```

Текст скрипта `vpn_reserve_channel`:

```

#!/bin/ksh

LOCAL_MAIN_NAME=pcn1
LOCAL_MAIN_PARAM=10.1.1.2/24

LOCAL_RESERVE_NAME=pcn2
LOCAL_RESERVE_PARAM=10.2.1.2/24

REMOTE_MAIN_IP=10.1.1.1

```

```
REMOTE_RESERVE_IP=10.2.1.1

REMOTE_NET=10.0.1.0/24

CHECK_N=3

PING=/usr/sbin/ping
ROUTE=/usr/sbin/route

MAIN_CHANNEL_LSP=main_channel_lsp.txt
RESERVE_CHANNEL_LSP=reserve_channel_lsp.txt

do_ping()
{
    $PING $REMOTE_MAIN_IP 1 > /dev/null
}

notify()
{
    logger -p local0.notice "$1"
    echo `date` "$1" > /dev/console
}

on_fail()
{
    route delete $REMOTE_NET $REMOTE_MAIN_IP > /dev/null
    route add $REMOTE_NET $REMOTE_RESERVE_IP > /dev/null
    ./lsp_mgr load -f $RESERVE_CHANNEL_LSP > /dev/null
    notify 'Reserve channel is used'
}

on_ok()
{
    route delete $REMOTE_NET $REMOTE_RESERVE_IP > /dev/null
    route add $REMOTE_NET $REMOTE_MAIN_IP > /dev/null
    ./lsp_mgr load -f $MAIN_CHANNEL_LSP > /dev/null
    notify 'Main channel is used'
}

cd /opt/VPNagent/bin

ifconfig $LOCAL_MAIN_NAME $LOCAL_MAIN_PARAM broadcast + up 2> /dev/null
ifconfig $LOCAL_RESERVE_NAME $LOCAL_RESERVE_PARAM broadcast + up 2> /dev/null

if do_ping; then
```

```

    RETRY_COUNT=$CHECK_N
    on_ok
else
    RETRY_COUNT=0
    on_fail
fi

while true; do
    if [[ $RETRY_COUNT -gt 0 ]]; then
        if do_ping; then
            RETRY_COUNT=$CHECK_N
        else
            RETRY_COUNT=$((RETRY_COUNT-1))
            if [ $RETRY_COUNT -eq 0 ]; then
                on_fail
            fi
        fi
    fi

    if [[ $RETRY_COUNT -gt 0 ]]; then
        sleep 1
    fi
else
    if do_ping; then
        RETRY_COUNT=$CHECK_N
        on_ok
    fi
fi
done

```

Описание настраиваемых параметров скрипта `vpn_reserve_channel`

Внутри скрипта необходимо настроить следующие параметры:

`LOCAL_MAIN_NAME` - имя сетевого интерфейса, подключенного к основному каналу (`ifg21`).

`LOCAL_MAIN_PARAM` - параметры интерфейса `ifg21`: IP-адрес (`ipg21`) и длина префикса (количество единиц в сетевой маске).

`LOCAL_RESERVE_NAME` - имя сетевого интерфейса, подключенного к резервному каналу (`ifg22`).

`LOCAL_RESERVE_PARAM` - параметры интерфейса `ifg22`: IP-адрес (`ipg22`) и длина префикса (количество единиц в сетевой маске).

`REMOTE_MAIN_IP` - IP-адрес интерфейса `GW1`, подключенного к основному каналу (`ipg11`).

`REMOTE_RESERVE_IP` - IP-адрес интерфейса `GW1`, подключенного к резервному каналу (`ipg12`).

`REMOTE_NET` - параметры сети `SN1`, защищаемой `GW1`: адрес сети и длина префикса (количество единиц в сетевой маске).

`CHECK_N` - количество неуспешных попыток ping-а, после которых считается, что связи нет.

Скрипт для запуска и остановки скрипта `vpn_reserve_channel`

Тело этого скрипта и размещение является таким же, как и для шлюза безопасности GW1.

Регистрация Preshared Key

Перед регистрацией ключа запишите значение ключа в файл. Для регистрации ключа с именем `reserve_channel_key` используйте утилиту `key_mgr import`, входящую в состав CSP VPN Gate:

```
/opt/VPNagent/bin/key_mgr import -n reserve_channel_key -f <key_file_path>
```

где `<key_file_path>` – путь к файлу, содержащему значение ключа. На шлюзе безопасности GW1 должен регистрироваться ключ, имеющий такое же значение.

Создание LSP для работы по основному каналу для GW2

Приступим к настройке CSP VPN Gate, установленного на шлюзе безопасности GW2. Создадим конфигурацию (LSP), по которой:

- Разрешается открытый доступ по SSH (для удаленного управления GW2).
- Разрешается открытый трафик по протоколу ICMP между двумя гейтами по основному каналу (ping для мониторинга состояния канала).
- Защищенный трафик (ESP, ГОСТ) между двумя подсетями. Используется аутентификация (ГОСТ) на preshared key.
- Весь остальной трафик запрещен.

Описанную ниже LSP положите в файл `main_channel_lsp.txt`, [настройте некоторые параметры](#), а затем доставьте на шлюз безопасности GW2 в `/opt/VPNagent/bin/`.

```
const LOCAL_MAIN_IP=10.1.1.2
const REMOTE_MAIN_IP=10.1.1.1
const LOCAL_MAIN_NAME="pcn1"
const INNER_IFS_NAME="pcn0"
const LOCAL_NET=10.0.2.0/24
const REMOTE_NET=10.0.1.0/24
GlobalParameters (
    Title                = "Main channel LSP (GW2) "
    Version              = "2.1"
)
IKETransform IKETransform_10 (
    CipherAlg            *= "G2814789CPR01-K256-CBC-65534"
    HashAlg              *= "GR341194CPR01-65534"
    GroupID              *= MODP_768
    LifetimeSeconds      = 86400
)
ESPProposal transform1 (
    Transform*           = ESPTransform (
        CipherAlg*       = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds  = 3600
    )
)
```

```

        LifetimeKilobytes    = 4608000
    )
)
AuthMethodPreshared IKE_auth_key(
    LocalID = IdentityEntry(
        IPv4Address *= LOCAL_MAIN_IP
    )
    RemoteID = IdentityEntry(
        IPv4Address *= REMOTE_MAIN_IP
    )
    SharedIKESecret = "reserve_channel_key"
)

IKERule IKE_cmap_1(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_key
    MainModeAuthMethod *= IKE_auth_key
    DoAutopass          = TRUE
)

IPsecAction cmap_1(
    TunnelingParameters *= TunnelEntry(
        LocalIPAddress = LOCAL_MAIN_IP
        PeerIPAddress  = REMOTE_MAIN_IP
    )
    ContainedProposals *= ( transform1 )
    IKERule = IKE_cmap_1
)

# SSH clear traffic to allow management of the gate
FilteringRule FilterSshPass(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 Port *= 22 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 )
    Action *= ( PASS )
)

# Ping to check main channel
FilteringRule FilterCheckPingPass(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_MAIN_IP ProtocolID *= 1 )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_MAIN_IP ProtocolID *= 1 )
    NetworkInterfaces *= LOCAL_MAIN_NAME
    Action *= ( PASS )
)

FilteringRule FilterTunnel(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_NET )
    NetworkInterfaces *= LOCAL_MAIN_NAME

```

```

    Action *= ( cmap_1 )
)
FilteringRule FilterInnerPass(
    LocalIPFilter *= FilterEntry( IPAddress *= REMOTE_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= LOCAL_NET )
    NetworkInterfaces *= INNER_IFS_NAME
    Action *= ( PASS )
)
FilteringRule FilterDrop(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    Action *= ( DROP )
)

```

Настройка параметров LSP в файле main_channel_lsp.txt

В конфигурации, записанной в файл `main_channel_lsp.txt`, настройте следующие параметры:

`LOCAL_MAIN_IP` - IP-адрес локального интерфейса, подключенного к основному каналу (`ipg21`).

`REMOTE_MAIN_IP` - IP-адрес интерфейса `GW1`, подключенного к основному каналу (`ipg11`).

`LOCAL_MAIN_NAME` - имя сетевого интерфейса, подключенного к основному каналу (`ifg21`).

`INNER_IFS_NAME` - имя сетевого интерфейса, подключенного в защищаемую подсеть (`ifg20`).

`LOCAL_NET` - параметры защищаемой сети `SN2`: адрес сети и длина префикса (количество единиц в сетевой маске).

`REMOTE_NET` - параметры сети `SN1`, защищаемой `GW1`: адрес сети и длина префикса (количество единиц в сетевой маске).

Создание LSP для работы по резервному каналу для GW2

Описанную ниже LSP положите в файл `reserve_channel_lsp.txt`, [настройте некоторые параметры](#), а затем доставьте на шлюз безопасности `GW2` в `/opt/VPNagent/bin/`.

```

const LOCAL_MAIN_IP=10.1.1.2
const REMOTE_MAIN_IP=10.1.1.1
const LOCAL_RESERVE_IP=10.2.1.2
const REMOTE_RESERVE_IP=10.2.1.1
const LOCAL_MAIN_NAME="pcn1"
const LOCAL_RESERVE_NAME="pcn2"
const INNER_IFS_NAME="pcn0"
const LOCAL_NET=10.0.2.0/24
const REMOTE_NET=10.0.1.0/24

GlobalParameters(
    Title = "Reserve channel LSP (GW2)"
    Version = "2.1"
)

```

```

IKETransform IKETransform_10(
    CipherAlg    *= "G2814789CPR01-K256-CBC-65534"
    HashAlg      *= "GR341194CPR01-65534"
    GroupID      *= MODP_768
    LifetimeSeconds = 86400
)
ESPProposal transform1(
    Transform* = ESPTransform (
        CipherAlg*      = "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
        LifetimeKilobytes = 4608000
    )
)
AuthMethodPreshared IKE_auth_key(
    LocalID = IdentityEntry(
        IPv4Address *= LOCAL_RESERVE_IP
    )
    RemoteID = IdentityEntry(
        IPv4Address *= REMOTE_RESERVE_IP
    )
    SharedIKESecret = "reserve_channel_key"
)
IKERule IKE_cmap_1(
    Transform* = IKETransform_10
    AggrModeAuthMethod *= IKE_auth_key
    MainModeAuthMethod *= IKE_auth_key
    DoAutopass          = TRUE
)
IPsecAction cmap_1(
    TunnelingParameters *= TunnelEntry(
        LocalIPAddress = LOCAL_RESERVE_IP
        PeerIPAddress  = REMOTE_RESERVE_IP
    )
    ContainedProposals *= ( transform1 )
    IKERule = IKE_cmap_1
)
# SSH clear traffic to allow management of the gate
FilteringRule FilterSshPass
(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 Port *= 22 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255
    ProtocolID *= 6 )
    Action *= ( PASS )
)
# Ping to check main channel

```

```

FilteringRule FilterCheckPingPass(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_MAIN_IP ProtocolID *= 1 )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_MAIN_IP ProtocolID *= 1 )
    NetworkInterfaces *= LOCAL_MAIN_NAME
    Action *= ( PASS )
)
FilteringRule FilterTunnel(
    LocalIPFilter *= FilterEntry( IPAddress *= LOCAL_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= REMOTE_NET )
    NetworkInterfaces *= LOCAL_RESERVE_NAME
    Action *= ( cmap_1 )
)
FilteringRule FilterInnerPass(
    LocalIPFilter *= FilterEntry( IPAddress *= REMOTE_NET )
    PeerIPFilter  *= FilterEntry( IPAddress *= LOCAL_NET )
    NetworkInterfaces *= INNER_IFS_NAME
    Action *= ( PASS )
)
FilteringRule FilterDrop(
    LocalIPFilter *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    PeerIPFilter  *= FilterEntry( IPAddress *= 0.0.0.0..255.255.255.255 )
    Action *= ( DROP )
)

```

Настройка параметров LSP в файле `reserve_channel_lsp.txt`

В конфигурации, записанной в файл `reserve_channel_lsp.txt`, настройте следующие параметры:

LOCAL_MAIN_IP - IP-адрес локального интерфейса, подключенного к основному каналу (ipg21)

REMOTE_MAIN_IP - IP-адрес интерфейса GW1, подключенного к основному каналу (ipg11)

LOCAL_RESERVE_IP - IP-адрес локального интерфейса, подключенного к резервному каналу (ipg22)

REMOTE_RESERVE_IP - IP-адрес интерфейса GW1, подключенного к резервному каналу (ipg12)

LOCAL_MAIN_NAME - имя сетевого интерфейса, подключенного к основному каналу (ifg21)

LOCAL_RESERVE_NAME - имя сетевого интерфейса, подключенного к резервному каналу (ifg22)

INNER_IFS_NAME - имя сетевого интерфейса, подключенного в защищаемую подсеть (ifg20)

LOCAL_NET - параметры защищаемой сети SN2: адрес сети и длина префикса (количество единиц в сетевой маске)

REMOTE_NET - параметры сети SN1, защищаемой GW1: адрес сети и длина префикса (количество единиц в сетевой маске).