**Инструкция по обновлению менеджмента и нод Check Point R65 с установленным патчем ГОСТ до версии R75.40VS (версия патча ГОСТ 4.0) без переустановки с нуля, перевыпуска сертификатов и SiteKey**

**ПОДГОТОВКА И ПОРЯДОК ОБНОВЛЕНИЯ**

Обновление проводится в несколько этапов:

1. Подготавливаются необходимые лицензии для менеджмент сервера и межсетевых экранов. Это лицензии типа «Software blade» (тип лицензии для R65 – «NGX»), которые подходят к R75 и R75.40 VS. Это важно, без них не имеет смысла, производить обновление
2. Обновляется менеджмент-сервер в следующем порядке: **R65** 🡪 **R75** 🡪 **R75.40VS**.
3. Поочередно обновляются межсетевые экраны (ноды) в аналогичном порядке.
4. Проверяется работа обновленного кластера.

**ОБНОВЛЕНИЕ МЕНЕДЖМЕНТ-СЕРВЕРА**

1. Делаем backup, или image менеджмент-сервера и сохраняем себе его на ноутбук.
2. Запускаем установщик версии R75.

Если с диска, выполняем команду:

*patch add cd #запускаем установщик*

Если ставим с iso’шки, выполняем команды:

*mount –t iso9660 –o loop <адрес iso’шки> #монтируем iso-образ*

*patch add cd #запускаем установщик*

1. Экспортируем конфигурацию из меню установщика версии R75 (по умолчанию файл создается здесь: */var/tmp/cpexport.tgz*).

Копируем ее себе на ноутбук (не обязательно, при обновлении файл */var/tmp/cpexport.tgz* не затирается).

1. Устанавливаем R75.

|  |
| --- |
| !Примечание: По окончанию, обязательно нажмите букву «о», это избавит вас от выполнения пункта **«В»** из официальной инструкции по установке ГОСТ. |

1. Перезагружаемся.
2. Устанавливаем хотфикс R75\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tgz.

Создаем каталог для установки хотфикса:

*mkdir –p /var/hotfix\_install/R75HFGOST*

Копируем хотфикс в созданный каталог средствами WinSCP.
Выполняем следующие команды из данного каталога:

*gunzip R75\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tgz #распаковываем tgz архив*

*tar -xvf fw1\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tar #распаковываем tar архив*

*./fw1\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238\_979238001\_2 #запускаем скрипт*

Следуем инструкциям на экране во время установки.

1. Через консоль SmartUpdate R75 удаляем старую лицензию на менеджмент сервер.
2. Устанавливаем новую лицензию для менеджмент сервера:

*cplic put –l <путь к файлу лицензии \*.lic>*

1. Перезагружаемся.
2. Импортируем ранее сохраненную конфигурацию (*/var/tmp/cpexport.tgz*) средствами R75 migration tool:

*$FWDIR/bin/upgrade\_tools/migrate import <путь до файла>*

1. Запускаем установщик R75.40VS по аналогии с вторым пунктом.
2. Экспортируем конфигурацию из меню установщика версии R75.40VS по аналогии с третьим пунктом.
3. Устанавливаем CheckPoint версии R75.40VS.
Следуем инструкциям на экране во время установки.
4. Перезагружаемся.
5. Устанавливаем рекомендуемый хотфикс для Software Blades.
Создаем каталог для установки хотфикса:

*mkdir –p /var/hotfix\_install/fw1*

Копируем хотфикс в созданный каталог средставми WinSCP.
Выполняем следующие команды из данного каталога:

*tar -zxvf fw1\_wrapper\_HOTFIX\_GIZA\_HF\_BASE\_006.tgz #распаковываем tgz архив*

*./fw1\_wrapper\_HOTFIX\_GIZA\_HF\_BASE\_006\_988006030\_2 #запускаем скрипт*

1. Устанавливаем патч ГОСТ (v4.0) для CheckPoint версии R75.40VS.

Создаем каталоги для установки патчей ГОСТ (v4.0):

*mkdir –p /var/gost\_install/rpm*

*mkdir –p /var/gost\_install/kis*

При помощи WinSCP копируем архив *CryptoPro\_R75.40VS.tar* в папку */var/gost\_install/rpm*,

а архив *VPN\_R75.40VS\_HF\_GOST\_V4.0.tar* в папку */var/gost\_install/*.

Распаковываем архивы:

*tar –xvf /var/gost\_install/rpm/CryptoPro\_R75.40VS.tar*

*tar –xvf /var/gost\_install/VPN\_R75.40VS\_HF\_GOST\_V4.0.tar*

Перемещаем файл конфигурации генератора псевдослучайных чисел:

*mv /var/gost\_install/rpm/kis\_1 /var/gost\_install/kis*

Запускаем установку патчей ГОСТ (v4.0):

*./var/gost\_install/UnixInstallScript*

Следуем инструкциям на экране во время установки.

1. Перезагружаемся.
2. Импортируем ранее сохраненную конфигурацию (*/var/tmp/cpexport.tgz*) средствами R75.40VS migration tool:

*$FWDIR/bin/upgrade\_tools/migrate import <путь до файла>*

**ОБНОВЛЕНИЕ МЕЖСЕТЕВЫХ ЭКРАНОВ**

1. Определяем активную ноду через команду:

*cphaprob state*

В данном случае первая нода является активной, а вторая в режиме standby.

1. Производим обновление второй ноды (standby) по порядку, приведенному ниже:

|  |
| --- |
| !Примечание: Перед обновлением убедитесь, что в свойствах кластера консоли SmartDashboard первая нода по приоритету стоит выше второй, в противном случае, при обновлении может произойти переключение на ненастроенную вторую ноду, с последующим падением туннеля. |

1. Делаем backup, или image ноды и сохраняем себе его на ноутбук.
2. Запускаем установщик версии R75.

Если с диска, выполняем команду:

*patch add cd #запускаем установщик*

Если ставим с iso’шки, выполняем команды:

*mount –t iso9660 –o loop <адрес iso’шки> #монтируем iso-образ*

*patch add cd #запускаем установщик*

1. Устанавливаем R75.

|  |
| --- |
| !Примечание: По окончанию, обязательно нажмите букву «о», это избавит вас от выполнения пункта **«В»** из официальной инструкции по установке ГОСТ. |

1. Перезагружаемся.
2. Устанавливаем хотфикс R75\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tgz.

Создаем каталог для установки хотфикса:

*mkdir –p /var/hotfix\_install/R75HFGOST*

Копируем хотфикс в созданный каталог средствами WinSCP.
Выполняем следующие команды из данного каталога:

*gunzip R75\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tgz #распаковываем tgz архив*

*tar -xvf fw1\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238.tar #распаковываем tar архив*

*./fw1\_HOTFIX\_FOXX\_GOST\_UPGRADE\_238\_979238001\_2 #запускаем скрипт*

Следуем инструкциям на экране во время установки.

1. Через консоль SmartUpdate R75 удаляем старую лицензию на межсетевой экран.
2. Устанавливаем новую лицензию для межсетевого экрана:

*cplic put –l <путь к файлу лицензии \*.lic>*

1. Перезагружаемся.
2. Запускаем установщик R75.40VS по аналогии с четвертым пунктом.
3. Устанавливаем CheckPoint версии R75.40VS.
Следуем инструкциям на экране во время установки.
4. Перезагружаемся.
5. Устанавливаем рекомендуемые хотфиксы для Software Blades.
Создаем каталоги для установки хотфиксы:

*mkdir –p /var/hotfix\_install/fw1*

*mkdir –p /var/hotfix\_install/sim*

Копируем хотфиксы в соответствующие каталоги средствами WinSCP.
Выполняем следующие команды из каталога *fw1*:

*tar -zxvf fw1\_wrapper\_HOTFIX\_GIZA\_HF\_BASE\_006.tgz #распаковываем tgz архив*

*./fw1\_wrapper\_HOTFIX\_GIZA\_HF\_BASE\_006\_988006030\_*2 *#запускаем скрипт*

Выполняем следующие команды из каталога sim:

*tar- zxvf sim\_HOTFIX\_R75.40VS\_HF\_BASE\_006.tgz #распаковываем tgz архив*

*./sim\_HOTFIX\_GIZA\_HF\_BASE\_006\_988006004\_2 #запускаем скрипт*

|  |
| --- |
| !Примечание: Если на R65 не был установлен Perfomance Pack, то не получится установить хотфикс *sim\_HOTFIX\_R75.40VS\_HF\_BASE\_006*, поэтому в данном случае его установку можно пропустить. |

1. Удаляем rpm-пакеты от старых библиотек ГОСТ, для этого по порядку вводим следующие команды:

*rpm -e lsb-cprocsp-ipsec-ike-3.6.4-3.i486*

*rpm -e lsb-cprocsp-ipsec-genpsk-3.6.4-3.i486*

*rpm -e lsb-cprocsp-3.6.4-4.i486*

*rpm -e lsb-cprocsp-capilite-3.6.4-4.i486*

*rpm -e lsb-cprocsp-ipsec-esp-2.4.21-21cp-3.6.4-3.i486*

*rpm -e lsb-cprocsp-drv-2.4.21-21cp-3.6.4-4.i486*

*rpm -e lsb-cprocsp-ipsec-esp-2.4.21-21cpsmp-3.6.4-3.i486*

*rpm -e lsb-cprocsp-drv-2.4.21-21cpsmp-3.6.4-4.i486*

*rpm -e lsb-cprocsp-rdr-3.6.4-4.i486*

*rpm -e lsb-cprocsp-base-3.6.4-4.noarch*

*rpm -e cprocsp-compat-splat-1.0.0-1*

В процессе удаления могут выскакивать ошибки информационного содержания, но пакеты все равно удалятся.

1. Устанавливаем патч ГОСТ (v4.0) для CheckPoint версии R75.40VS.

Создаем каталоги для установки патчей ГОСТ (v4.0):

*mkdir –p /var/gost\_install/rpm*

*mkdir –p /var/gost\_install/kis*

При помощи WinSCP копируем архив *CryptoPro\_R75.40VS.tar* в папку */var/gost\_install/rpm*,

а архив *VPN\_R75.40VS\_HF\_GOST\_V4.0.tar* в папку */var/gost\_install/*.

Распаковываем архивы:

*tar –xvf /var/gost\_install/rpm/CryptoPro\_R75.40VS.tar*

*tar –xvf /var/gost\_install/VPN\_R75.40VS\_HF\_GOST\_V4.0.tar*

Перемещаем файл конфигурации генератора псевдослучайных чисел:

*mv /var/gost\_install/rpm/kis\_1 /var/gost\_install/kis*

Запускаем установку патчей ГОСТ (v4.0):

*./var/gost\_install/UnixInstallScript*

Следуем инструкциям на экране во время установки.

1. Проверяем командой:

*cphaprob state*

Должна отобразиться одна нода с состоянием *ready(\*).*

1. Заходим на менеджмент сервер через SmartDashboard R75.40VS.
2. В свойствах кластера в качестве версии выставляем *«R75.40VS»*, а в качестве операционной системы выставляем *«Gaia»*.
3. Нажимаем кнопку *«Install policy»*.
4. В открывшемся окне снимаем галку напротив: *«For Gateway Clusters install on all the members, if it fails do not install at all»*.
5. Устанавливаем политики. В итоге получаем сообщение, что политики были успешно установлены только на вторую ноду.
6. Переводим трафик на вторую ноду, для этого останавливаем кластерный сервис на первой ноде командой:

*cphastop*

|  |
| --- |
| !Примечание: Кластер по умолчанию работает в режиме «statefull failover», это означает, что при переключении, установленные сессии, идущие через кластер, не будут разорваны. Однако, в некоторых приложениях разрыв сессии возможен (зависит от специфики работы конкретного приложения), поэтому данное переключение рекомендуется согласовать с ответственными лицами на объекте. |

1. Проверяем, что трафик переключился на вторую ноду, для этого выполняем на ней команду:

*cphaprob state*

Статус *«Active attention»*, говорит о том, что мы на правильном пути и трафик перешел на вторую ноду.
Также, в консоли SmartView Monitor R75.40VS, в разделе *«Tunnels\Permanent Tunnels»* убеждаемся, что туннель жив и его работа перешла на вторую ноду.

1. Отключаем сетевые кабели (кроме management-интерфейса) от первой ноды для исключения возможности кластерного переключения на нее, что приведет к падению туннеля.

|  |
| --- |
| !Примечание: Рекомендуется использовать способ с отключением сетевых кабелей, так как он гарантирует стабильность туннеля. Даже не смотря на то, что вы понизите приоритет первой ноды в настройках кластера в SmartDashboard, туннель все-равно может переключиться на нее и это приведет к его падению. |

1. Повторяем процедуру обновления, описанную в пунктах 3-19 для первой ноды.
2. После обновления, проверям работу первой ноды, выполнив на ней команду:

*cphaprob state*

Должно отобразиться состояние, в котором указано, что первая нода находится в режиме *«Down»*, а вторая нода в режиме *«Active»*. Выполнение команды на другой ноде – даст аналогичный вывод.

1. Заходим на менеджмент сервер через SmartDashboard R75.40VS.
2. Нажимаем кнопку *«Install policy»*.
3. В открывшемся окне ставим галку напротив: *«For Gateway Clusters install on all the members, if it fails do not install at all»*.
4. Устанавливаем политики.
5. Через некоторое время проверяем кластер, выполнив на любой из нод команду:

*cphaprob state*

Должно отобразиться состояние, в котором указано, что первая нода находится в режиме *«Standby»*, а вторая нода в режиме *«Active»*.

**ПРОВЕРКА РАБОТЫ ОБНОВЛЕННОГО КЛАСТЕРА**

После обновления необходимо удостовериться в том, что кластер корректно переключается между нодами и корректно обновляет IKE SA и IPSec SA. Для этого:

1. На активной ноде запускаем диагностическую утилиту через команду:

*vpn tu*

Проверяем, что имеются IPsec SA, выбрав пункт «2».

В интерактивном меню данной утилиты производим удаление всех существующих SA (пункт «0»).

После удаления, сначала моментально должны создатьcя IKE SA, а затем IPsec SA.

Проверяем, что создались IKE SA, выбрав пункт «1».

Проверяем, что создались IPsec SA, выбрав пункт «2».

|  |
| --- |
| !Примечание: Данная процедура приводит к кратковременному обрыву туннеля. Возможна потеря нескольких пакетов туннельного трафика, или, в худшем случае, падение туннеля, при наличии неисправности в кластере. Перед ее выполнением запросите производственное окно на объекте. |

1. Переключаем туннель на другую ноду. Для этого приостанавливаем работу активной ноды через команду из режима expert:

*clusterXL\_admin down*

В консоли SmartView Monitor R75.40VS, в разделе *«Tunnels\Permanent Tunnels»* убеждаемся, что туннель жив и его работа перешла на другую ноду.

Выполняем аналогичные операции с утилитой «vpn tu» из первого пункта.

1. Переключаем туннель обратно. Для этого, на приостановленной ноде выполняем команду из режима expert:

*clusterXL\_admin up*

Туннель самостоятельно не переключится на восстановленную ноду, поэтому это нужно спровоцировать, выполнив на активной ноде команду:

*clusterXL\_admin down*

В консоли SmartView Monitor R75.40VS, в разделе *«Tunnels\Permanent Tunnels»* убеждаемся, что туннель жив и его работа перешла на другую ноду.

Включаем приостановленную ноду командой:

*clusterXL\_admin up*

|  |
| --- |
| !Примечание: Осуществлять переключение нод по аналогии с командами, описанными выше, можно также через графический интерфейс консоли SmartView Monitor, в разделе «Gateway Status\Firewalls» через пункты *«Cluster Member\Stop Member»* и «*Cluster Member\Start Member»* выпадающего меню. |

1. Проверяем настройки кластера в SmartDashboard: приоритет первой ноды должен быть выше второй.
2. Переключаем туннель на первую ноду по аналогии с вышеописанными пунктами и убеждаемся, что туннель работает через нее.