

Взаимодействие SkyDNS и корпоративных систем

В корпоративной системе существует набор сервисов, использование которых упрощает администрирование сети, а на некоторые из них возлагают и функцию ограничения доступа пользователей к нежелательным ресурсам Интернета.

К являющимся частью инфраструктуры многих корпоративных систем можно отнести такие сервисы как **DHCP**, **DNS** и **контроллер домена**.

Одна из целей использования сервиса **DHCP** заключается в назначении сетевых реквизитов пользовательским системам.

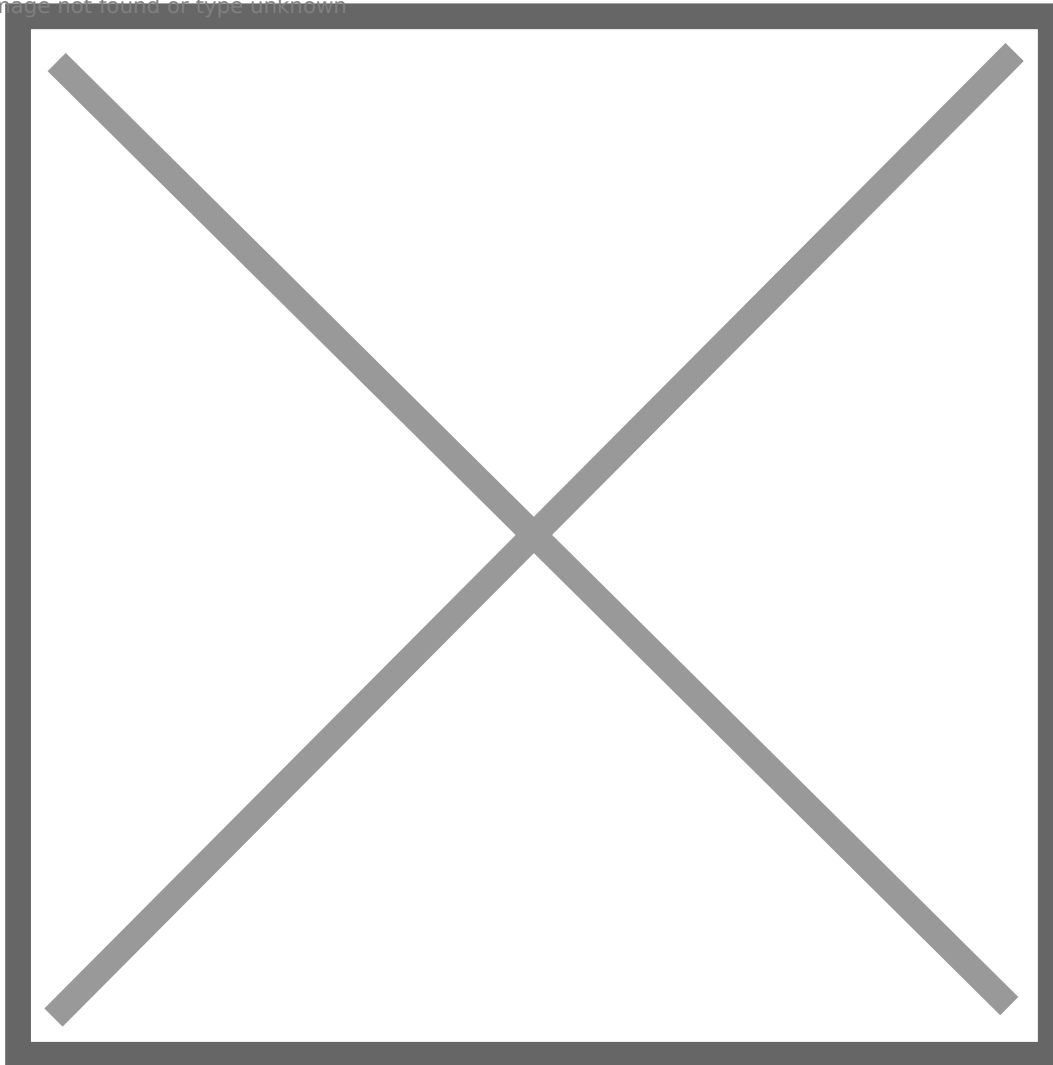
В задачи **контроллера домена** входит обеспечение централизованного управления ресурсами домена компании. К таким ресурсам относятся и доменные имена пользовательских и иных систем компании.

Разрешение доменных имён систем компании в их IP адреса для сетевого взаимодействия возлагается на **сервер DNS**. Кроме этого, DNS-сервер отвечает за обработку запросов, касающихся интернет доменов.

Дополнительно к вышеприведённым сервисам может применяться и **прокси-сервер**. Его основной функцией является транзит Веб-трафика (и трафика некоторых других протоколов) из Интернет в локальную сеть компании. Для выполнения запросов пользователей прокси-сервер выполняет разрешение имён используя сервис DNS.

Интернет-шлюз занимается маршрутизацией трафика между сетью компании и интернет. Очень часто на него возложены функции защиты локальной сети и блокировки нежелательных видов трафика в сторону Интернет.

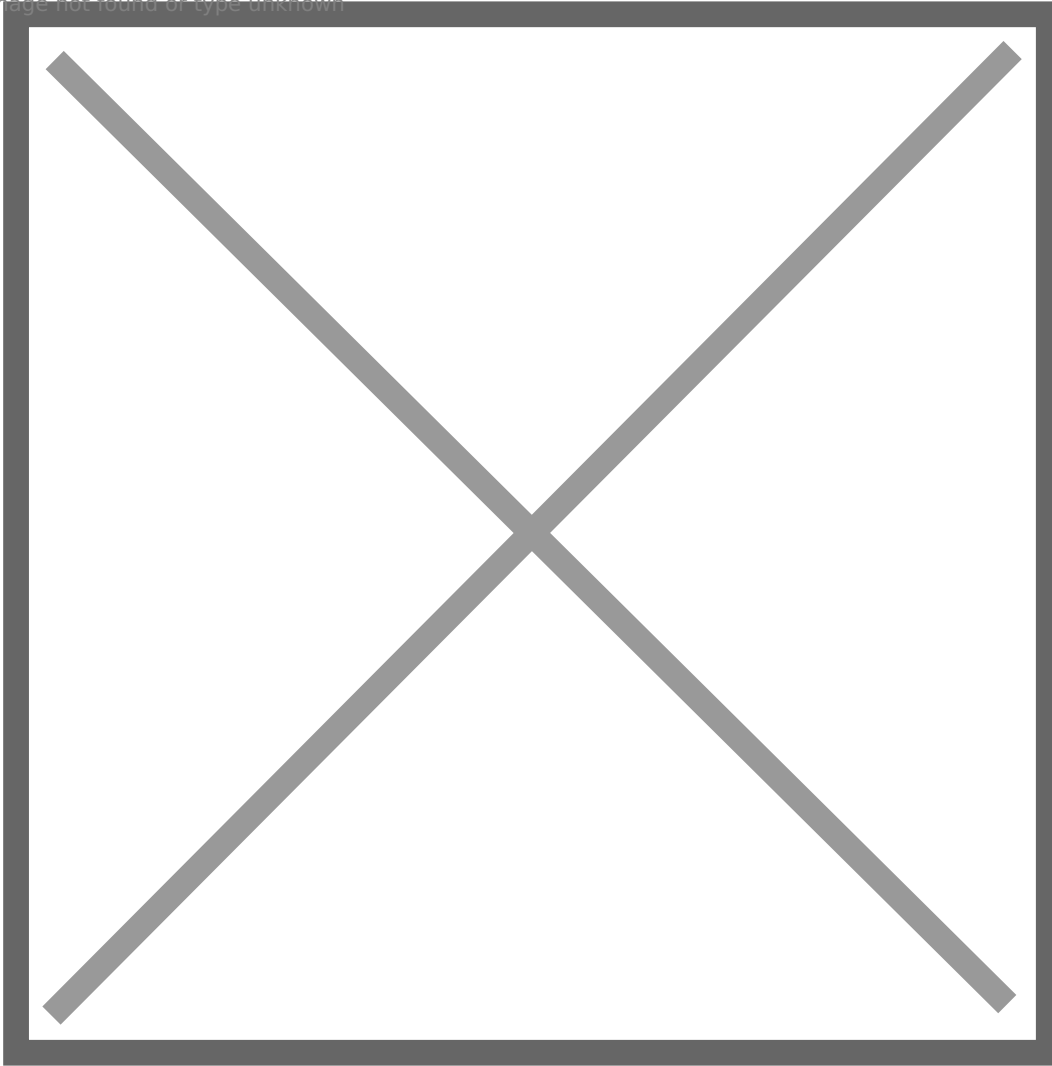
Image not found or type unknown



Рассмотрим варианты взаимодействия сервиса **SkyDNS** с каждым из вышеприведённых компонентов корпоративной системы.

DNS сервер компании: как правило, такие серверы настроены на передачу запросов соответствующим серверам провайдера и самостоятельным разрешением имён занимаются только в рамках корпоративного домена. Если для такого сервера в качестве сервиса реализующего фактическое разрешение имён для интернет указать **SkyDNS**, то в ответ на запросы, содержащиеся в заблокированных категориях, будет выдаваться один из адресов **SkyDNS**. Если при этом целью запроса к DNS-серверу компании было получение IP-адреса веб-страницы, то в браузере появится страница блокировки сервисом **SkyDNS** обращения к сайту. В данной конфигурации взаимодействия корпоративных систем со **SkyDNS** пользователи, использующие **DNS сервер** компании, будут вынуждены подчиняться тем или иным правилам политики безопасности или контроля использования интернет. А отражение правил будет установлено в личном кабинете сервиса **SkyDNS**.

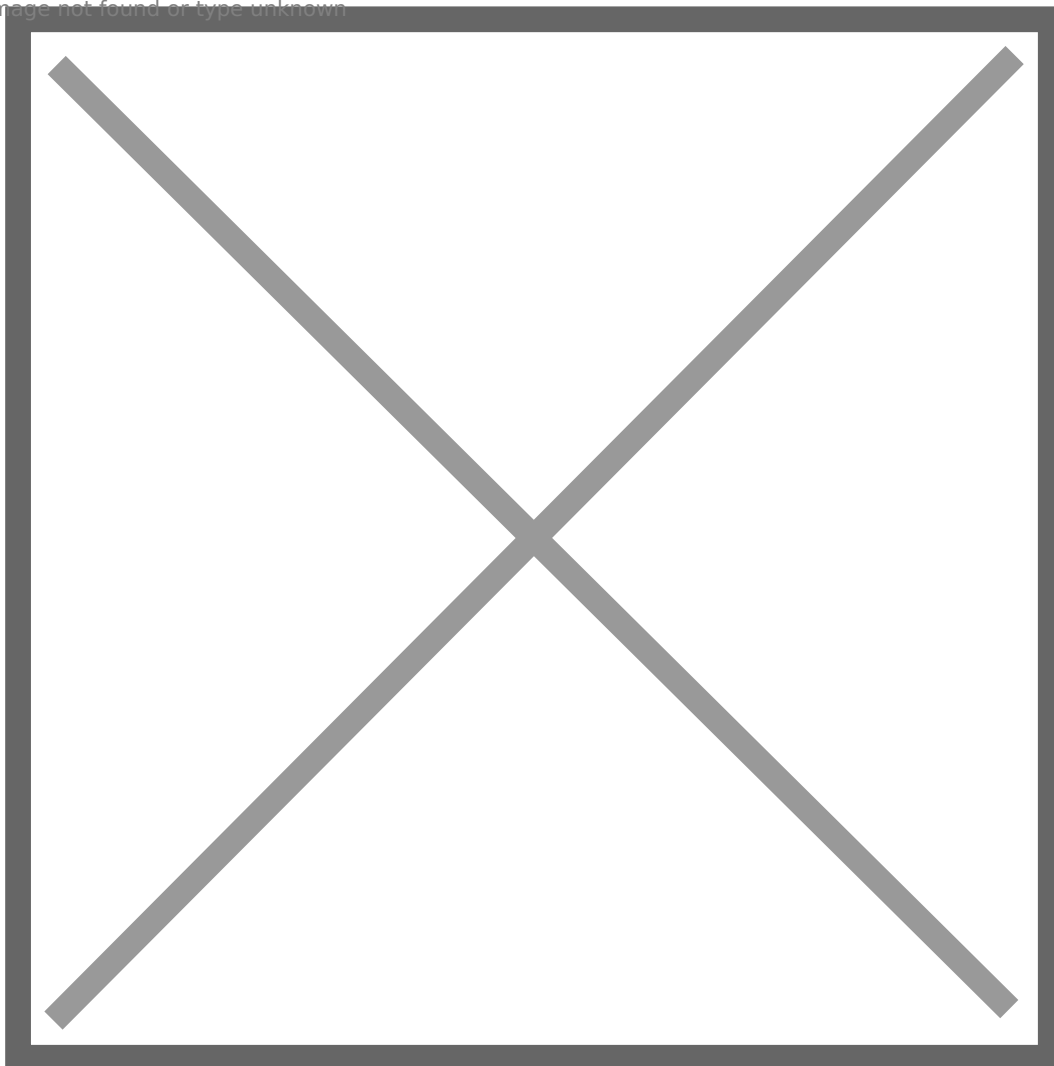
Image not found or type unknown



При этом, при правильной настройке разрешение имён корпоративного домена будет происходить только на стороне DNS-сервера компании.

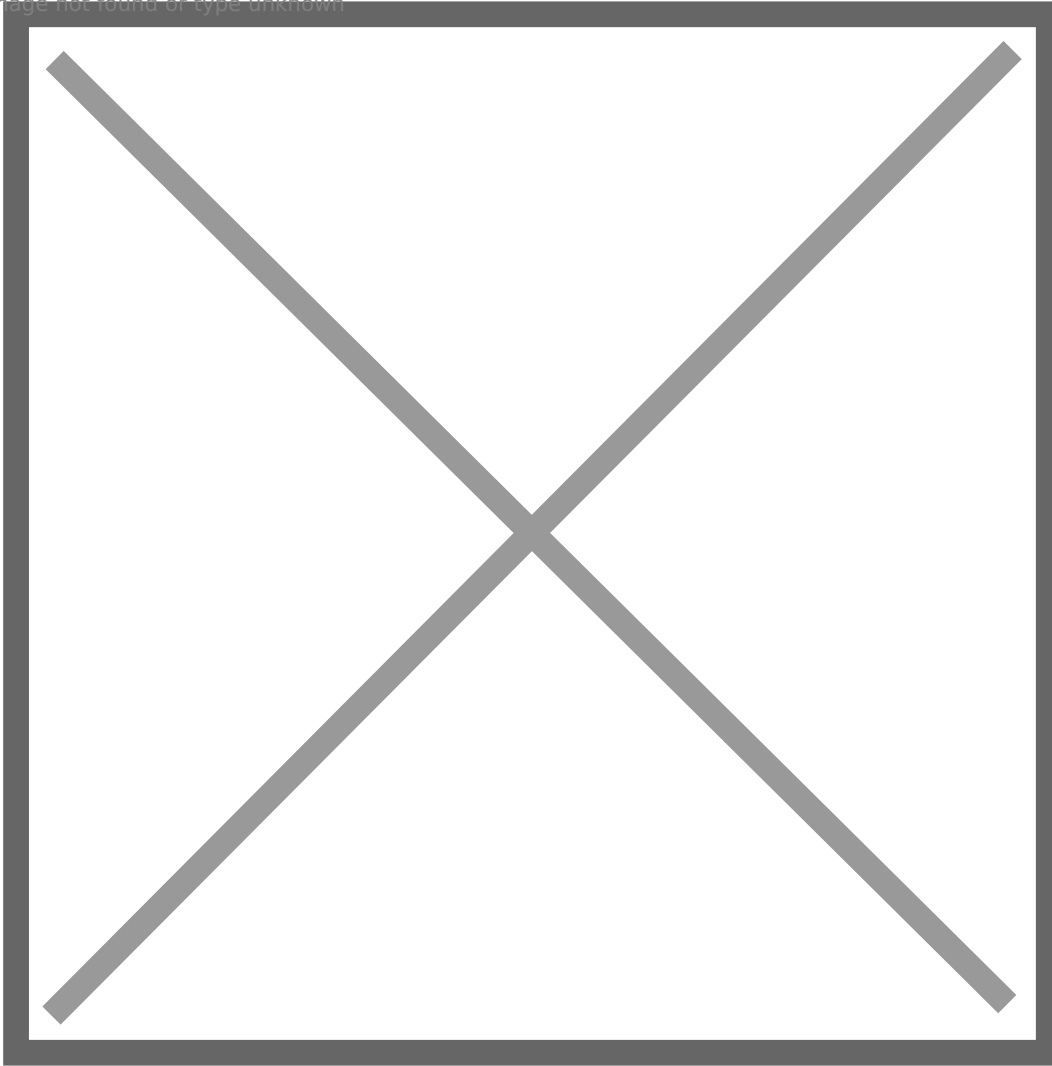
Далее рассмотрим конфигурирование **DHCP** таким образом, чтобы пользователям в качестве **DNS сервера** для компании выдавался адрес **SkyDNS**. При этом запросы тех пользователей, чьи системы используют **DHCP** для получения сетевых реквизитов, будут получать ответы напрямую от сервиса **SkyDNS**. Это ограничивает возможности использования корпоративного домена. Лучше такая конфигурация подходит когда он не используется в локальной сети компании. При возможности гибкой настройки **DHCP-сервера** можно назначать пользователям DNS без фильтрации или с ней.

Image not found or type unknown



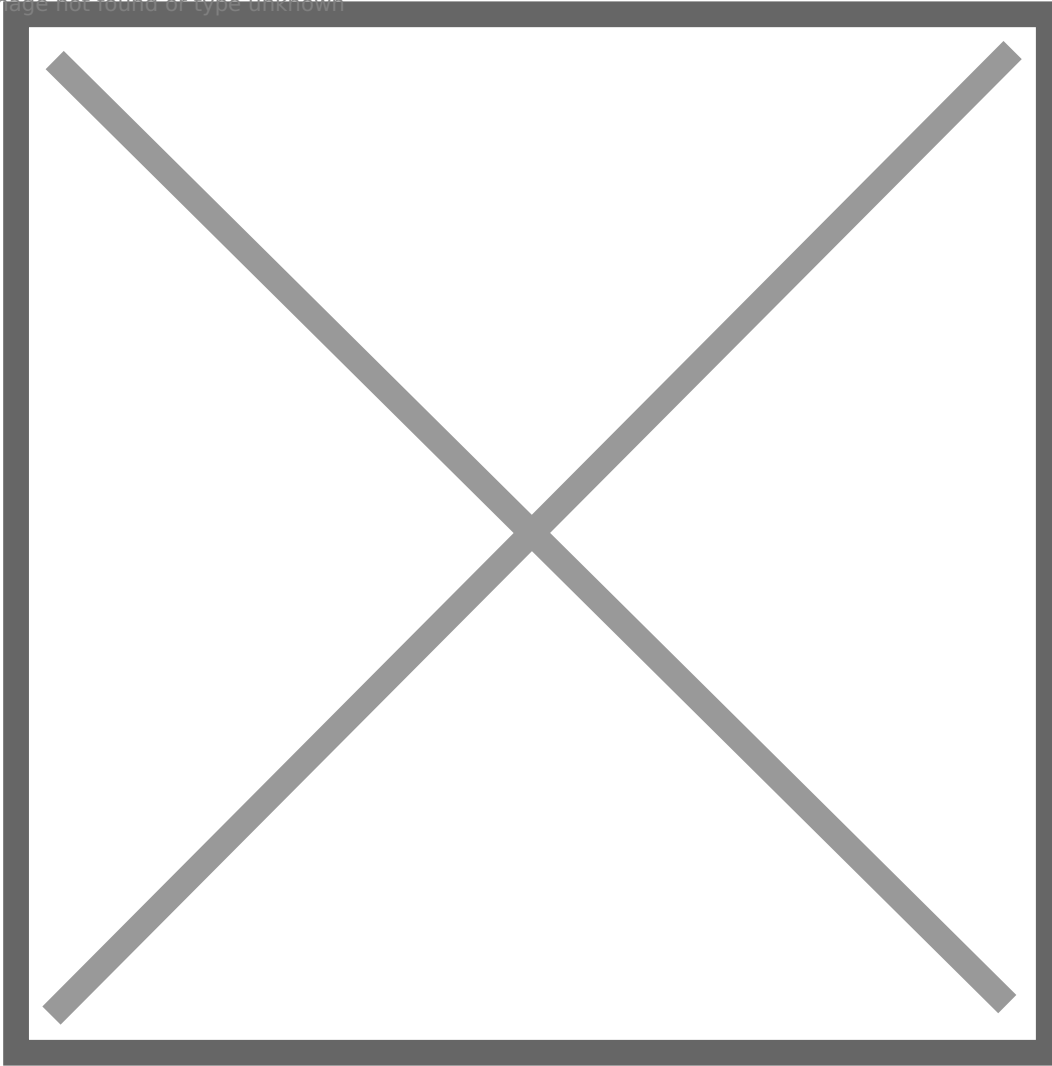
Если используется **прокси-сервер**, то настроив разрешение имён в нём через сервис **SkyDNS** можно получить аналогичный по своему эффекту взаимодействия **DNS** сервера компании с сервисом **SkyDNS** результат.

Image not found or type unknown



Лучший контроль над **DNS** запросами пользователей и соответствующую политике безопасности или ограничений реализацию взаимодействия с сервисом **SkyDNS** можно получить комплексным подходом, включающим в себя и настройку **интернет-шлюза** компании или филиала. При этом, в брандмауэре надо задать перенаправление **DNS** запросов на сервис **SkyDNS**. При желании можно и исключить те машины в сети, которые не должны проходить фильтрацию запросов.

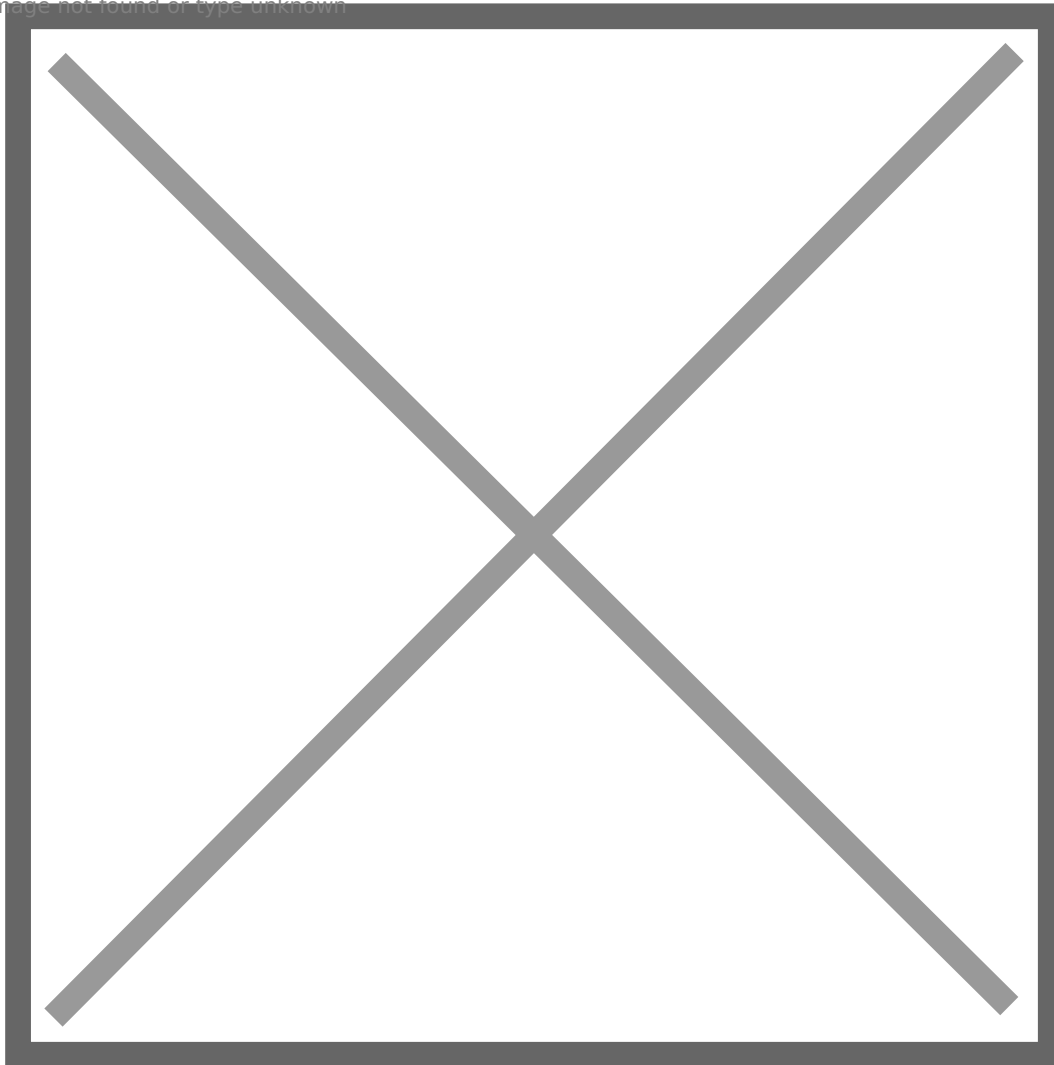
Image not found or type unknown



В качестве заключения можно привести вариант сценария взаимодействия с сервисом **SkyDNS**:

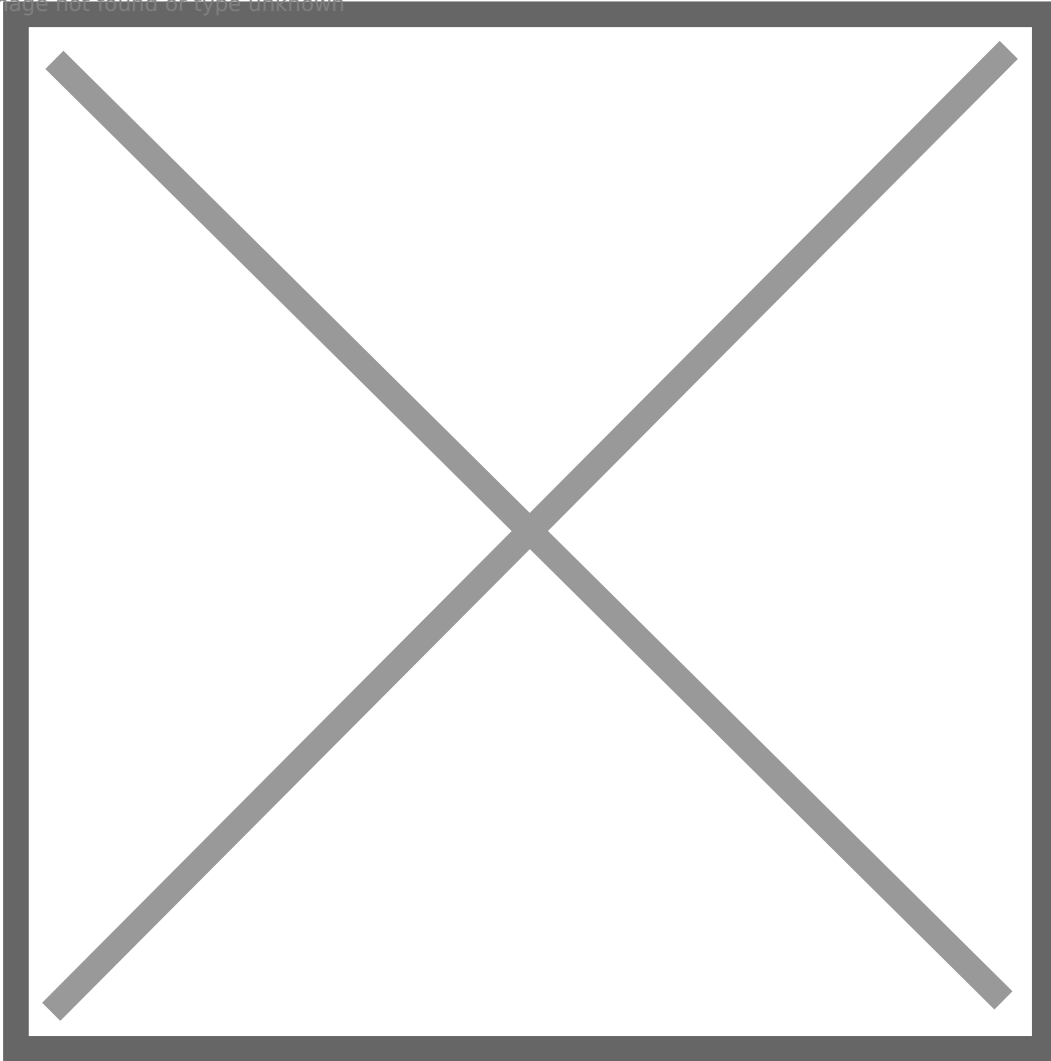
Среди сетевых реквизитов, получаемых по **DHCP** в качестве адреса **DNS-сервера**, пользовательская система получает адрес корпоративного **DNS сервера**.

Image not found or type unknown



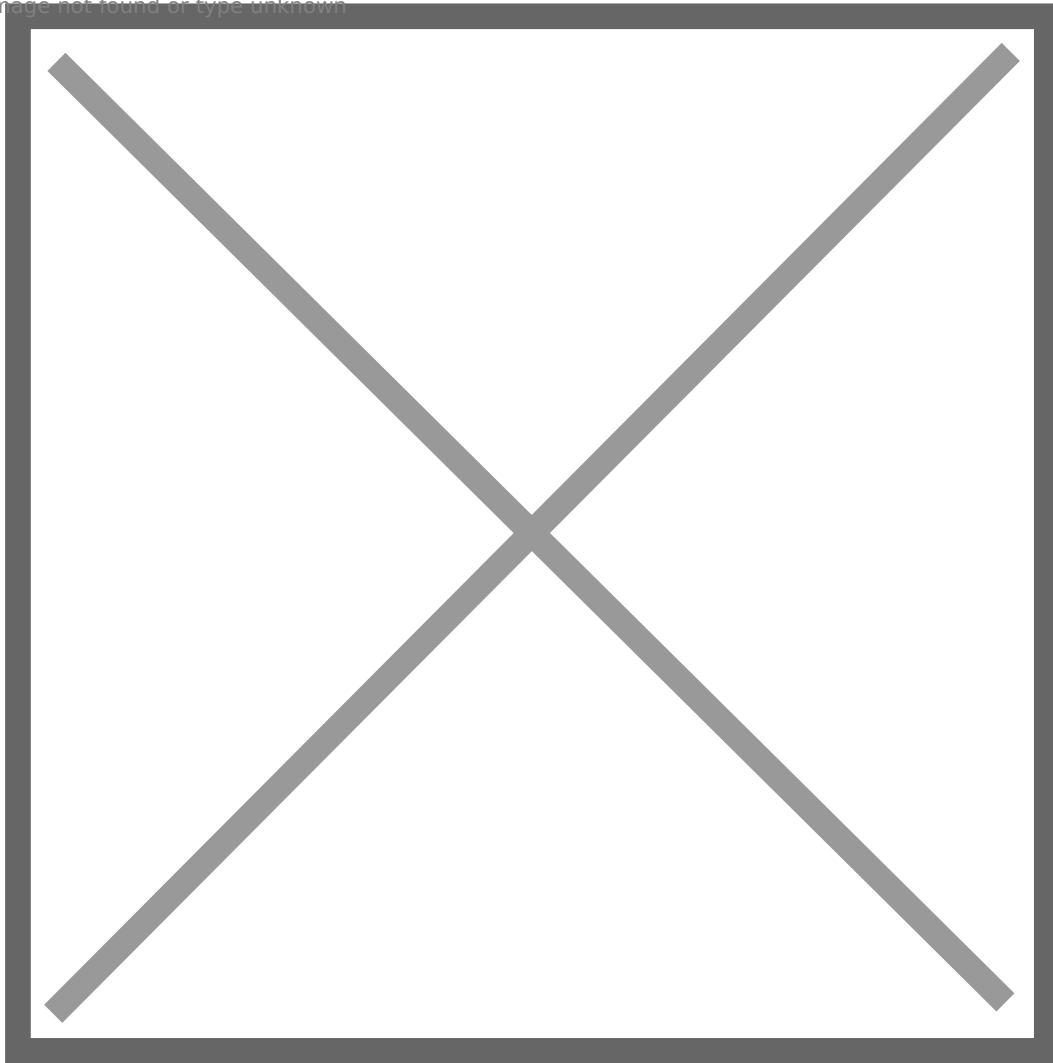
На корпоративном **DNS-сервере** запросы, касающиеся доменов интернет, передаются сервису **SkyDNS**. Ответы отфильтрованы в соответствии с настройками сервиса.

Image not found or type unknown



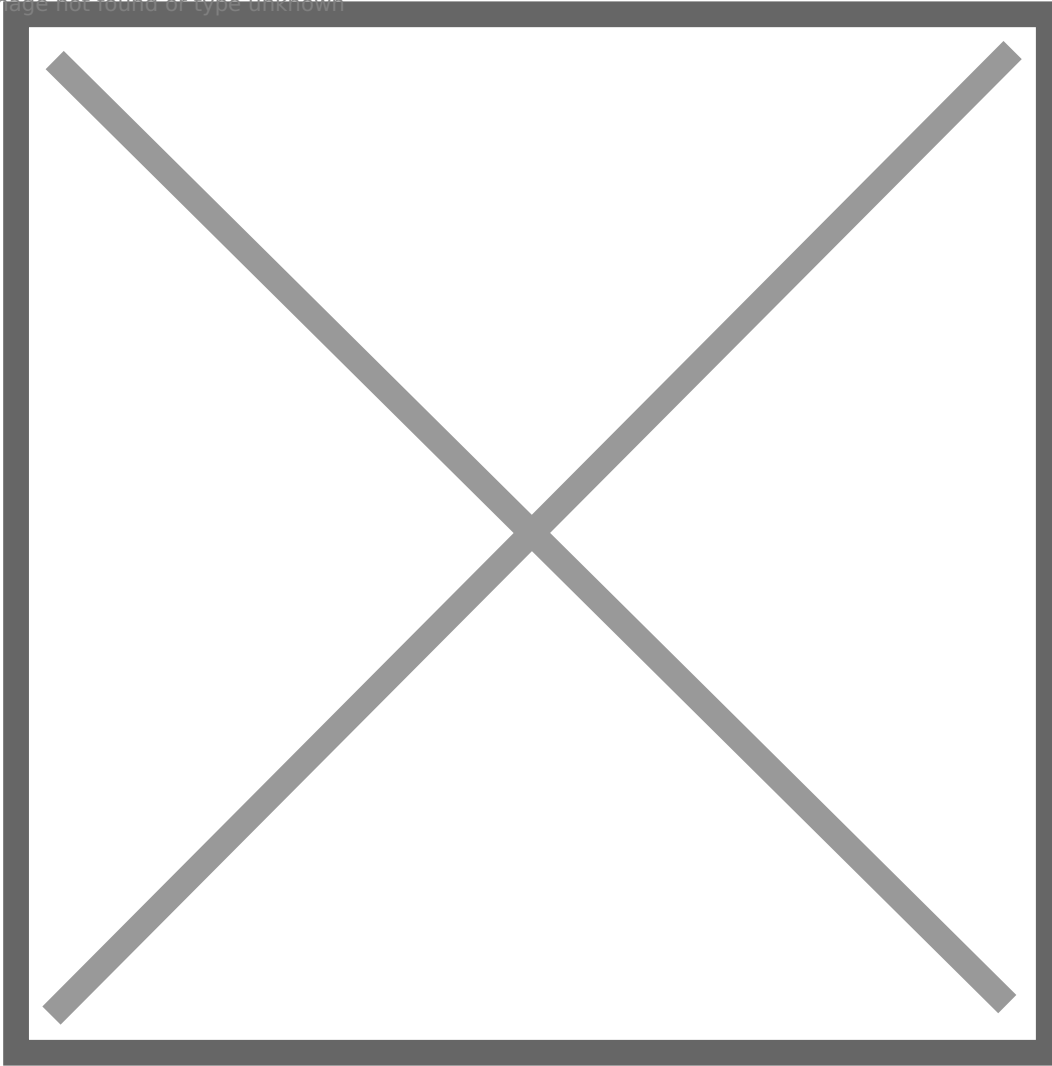
Преобразование адресов на **прокси-сервере** настроено на корпоративный **DNS сервер**.
Запросы к веб-серверам в сети проходят без изменений, а к Интернет-сайтам фильтруются на уровне **DNS**.

Image not found or type unknown



Дополнительно, или как вариант, на **Интернет-шлюзе** запросы, направляющиеся по протоколу **DNS**, перенаправляются в сторону сервиса **SkyDNS**.

Image not found or type unknown



Для успешного применения некоторых политик безопасности обязательно закрытие доступа пользователей к другим **DNS** на **Интернет-шлюзе**. При этом, если у компании есть несколько белых IP-адресов (например, для NAT), то возможно разделение профилей фильтрации.

Revision #3

Created 22 November 2023 12:02:15 by Виктор

Updated 7 February 2024 06:58:18 by Виктор