Инструкция по подготовительным действиям и подключению к услуге Internet Umbrella, вариант предоставления Cloud Protection

1. Подготовительные действия на стороне клиента до подключения услуги

1.1 Действия перед изменением DNS записи

Перед заменой DNS записи необходимо произвести подготовительные действия для того, чтобы минимизировать время перерыва сервиса клиента при подключении услуги. Изменения настроек описанные ниже влияют на скорость подключения услуги, а также на скорость приостановки и восстановления услуги Internet Umbrella Cloud Protection для защищаемого ресурса.

При перенастройке A-записи нужно изменить TTL-запись заранее. Рекомендуется установить время TTL-записи равное 15 минутам. Настройки TTL распространятся по всем серверам зоны в течение времени TTL, изначально выставленного у клиента. По прошествии значения времени, равному предыдущей TTL-записи - зона обновляется на всех серверах домена и TTL-таймер становится равным 15 минутам. Например, если выставлен TTL 24 часа, а мы меняем TTL на 15 минут обновленный TTL 15 минут применится только через 24 часа. Время отчитывается с момента обновления зоны на всех Primary и Secondary NS серверах. Это необходимо выполнить для того, чтобы DNS-зона успела обновиться на всех на всех кеширующих серверах интернета.

Команды для проверки параметров refresh и TTL DNS записи находятся. в п.3.

Существует правило, что при каждом изменении настроек зоны, необходимо дополнительно изменять серийный номер зоны. Обратите также внимание, что уменьшение времени TTL увеличивает нагрузку на DNS сервера зоны.

Рекомендуем не использовать DNS записи типа CNAME, где можно узнать реальный IP адрес защищаемого Ресурса, отключите такие записи.

Если вы используете почтовые ретрансляторы, то уберите указание IP адресов защищаемого Ресурса из записей типа TXT.

1.2 Рекомендации

Для снижения вероятности получение злоумышленником реального IP адреса защищаемого ресурса, рекомендуется:

- Убедится, что в коде HTTP заголовков не указан реальный IP адрес, который злоумышленники могут узнать, также проверить альтернативные места в публичном доступе, где в явном виде прописан реальный IP адрес защищаемого ресурса.
- Разместите защищаемые ресурсы на выделенном хостинге, доступ в интернет для офисных сотрудников не должен быть на том же канале, что и защищаемый ресурс.
- В случае наличия мониторинга непосредственно IP адресов защищаемых ресурсов из публичной сети добавить выданные Orange IP адреса из выделенного диапазона 194.84.46.0/23 на ваших системах мониторинга как дополнительные, либо заменить реальные IP адреса на выданные.

Во избежание блокировок легитимного трафика к защищаемому ресурсу, рекомендуется:

- Для защиты WEB ресурсов учесть повышенное количество TCP соединений с подсети 195.151.68.0/23 во избежание блокировки по превышению количества TCP соединений с одного IP адреса.

Orange Restricted

2. Действия при подключении услуги

2.1 Изменение DNS записи.

2.1.1 В случае если DNS сервер находится под управлением клиента

При подключении ресурса к услуге, необходимо заменить A-запись и PTR-запись на выданный Orange IP адрес из выделенного диапазона 194.84.46.0/23 в DNS-зоне клиента. DNS-зона представляет собой файл, в котором описано соответствие хостов домена и IP-адресов. За каждую DNS-зону отвечает не менее двух серверов. Один из них является первичным (primary), остальные — вторичными (secondary) серверами.

После чего primary сервер должен распространить запись на secondary сервера зоны. Рекомендуется сразу же настроить автоматический апдейт записей на все сервера зоны NOTIFY. Если автоматический апдейт записей зоны не настроен, то все secondary сервера зоны обратятся к primary серверу и обновят свои A-записи по прошествии времени, указанному в параметре refresh в SOA-записи. Время, через которое обновятся все DNS-записи зоны равно сумме параметров refresh + TTL, настроенные ранее на primary сервере зоны.

При необходимости временно приостановить, либо отключить услугу Internet Umbrella Cloud Protection для защищаемого ресурса можно вернуть изначальные значение A-записи и PTR-записи и через 15 минут DNS зона обновится.

2.1.2 DNS сервер находится под управлением Orange.

В таком случае уже имеется подключенная услуга Internet Direct Registration. Все дальнейшие действия по обслуживанию DNS записи будут производиться инженерами Orange, никакие дальнейшие действия с вашей стороны не требуются.

2.1.3 Защищаемый ресурс не имеет DNS записи.

Вам будет передан IP адрес при подключении услуги из выделенного диапазона 194.84.46.0/23. С вашей стороны требуется перенастроить доступ всех конечных пользователей защищаемого ресурса на полученный от Orange IP адрес.

2.2 Ограничение доступа к защищаемому ресурсу из сети Интернет

Закрыть доступ со всех публичных IP адресов Интернет-пространства, кроме двух подсетей 195.151.68.0/23, на каждый защищаемый ресурс. Данная подсеть будет выступать в качестве Proxy pool IP адресов, в которую будут транслироваться все внешние подключения к защищаемым ресурсам. Также закрыть ICMP трафик.

3. Команды для проверки параметров DNS записи

Проверять, правильно ли настроены параметры для подключения услуги имеет смысл смотреть не ранее, чем через время, по истечению которого обновятся все DNS-записи зоны. Это время соответствует сумме параметров **refresh** + **TTL**, которые были актуальными до совершения конфигураций.

3.1 Пример команд для Linux:

Вначале следует собрать информацию по зоне, смотрим SOA запись. В SOA можно увидеть значение параметра **refresh**.

Orange Restricted

```
[root@inoventica ~]#  dig -t SOA gin.ru

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.sp6.7 <<>> -t SOA gin.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4331
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;gin.ru.                                IN      SOA

;; ANSWER SECTION:
gin.ru.                 1831    IN      SOA     master.rosprint.net. dnsmaster.rosprint.net. 2024030601 28800 7200 604800 86400

;; AUTHORITY SECTION:
gin.ru.                 3414    IN      NS      master.rosprint.net.
gin.ru.                 3414    IN      NS      ns2.rosprint.net.
gin.ru.                 3414    IN      NS      ns1.rosprint.net.

;; ADDITIONAL SECTION:
master.rosprint.net.    306     IN      A       195.151.241.2
ns1.rosprint.net.       86059   IN      A       185.128.196.254
ns2.rosprint.net.       86059   IN      A       194.84.23.125

;; Query time: 3 msec
;; SERVER: 172.16.255.1#53(172.16.255.1)
;; WHEN: Fri Mar 29 15:55:04 2024
;; MSG SIZE  rcvd: 187
```

Команда dig на Linux машине показывает нужное значение **TTL** таймера в секундах.

Для получения значения параметра **refresh** в первую очередь необходимо проверить какой сервер является авторитетным:

```
dig -t NS gin.ru
```

```
[root@inoventica ~]#  dig -t NS gin.ru

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.sp6.7 <<>> -t NS gin.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57513
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;gin.ru.                                IN      NS

;; ANSWER SECTION:
gin.ru.                 3530    IN      NS      master.rosprint.net.
gin.ru.                 3530    IN      NS      ns2.rosprint.net.
gin.ru.                 3530    IN      NS      ns1.rosprint.net.

;; ADDITIONAL SECTION:
master.rosprint.net.    422     IN      A       195.151.241.2
ns1.rosprint.net.       86175   IN      A       185.128.196.254
ns2.rosprint.net.       86175   IN      A       194.84.23.125

;; Query time: 4 msec
;; SERVER: 172.16.255.1#53(172.16.255.1)
;; WHEN: Fri Mar 29 15:53:09 2024
;; MSG SIZE  rcvd: 141
```

Далее на выбранном авторитетном сервере смотрим значение TTL таймера в секундах:

```
dig @ns1.rosprint.net www.gin.ru
```

Orange Restricted

```
[root@inoventica ~]# dig @ns1.rosprint.net www.gin.ru

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.sp6.7 <<>> @ns1.rosprint.net www.gin.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54061
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.gin.ru.                    IN      A

;; ANSWER SECTION:
www.gin.ru.             3600    IN      CNAME   home.global-one.ru.
home.global-one.ru.     86400   IN      A       185.128.196.7

;; Query time: 2 msec
;; SERVER: 185.128.196.254#53(185.128.196.254)
;; WHEN: Fri Mar 29 15:53:17 2024
;; MSG SIZE  rcvd: 74
```

3.2 Пример команд на Windows (если нет Linux машины)

Примечание: Параметр TTL на Windows машине указан на весь домен, а не на конкретную запись, поэтому на Windows машине можно узнать только значение параметра **refresh**.

При выводе команд на Windows машине следует обратить внимание на точку после ввода имени. Если точку не указать, к имени будет добавлен домен по умолчанию из DNS Search настроек сети и будет осуществлен неправильный запрос.

Вначале следует собрать информацию по зоне, для этого посмотреть SOA запись. Из вывода SOA записи на Windows машине можно узнать значение настроенного параметра **refresh**.

```
Microsoft Windows [Version 10.0.19042.1645]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\Users\                    >nslookup
╤хЁтхЁ яю єьюыўрэш■:  ns.in.rosprint.ru
Address:  172.16.255.1

> set type=SOA
> gin.ru.
╤хЁтхЁ:  ns.in.rosprint.ru
Address:  172.16.255.1

Не заслуживающий доверия ответ:
gin.ru
        primary name server = master.rosprint.net
        responsible mail addr = dnsmaster.rosprint.net
        serial  = 2024030601
        refresh = 28800 (8 hours)
        retry   = 7200 (2 hours)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)

gin.ru  nameserver = master.rosprint.net
gin.ru  nameserver = ns2.rosprint.net
gin.ru  nameserver = ns1.rosprint.net
master.rosprint.net     internet address = 195.151.241.2
ns1.rosprint.net        internet address = 185.128.196.254
ns2.rosprint.net        internet address = 194.84.23.125
>
```

Orange Restricted