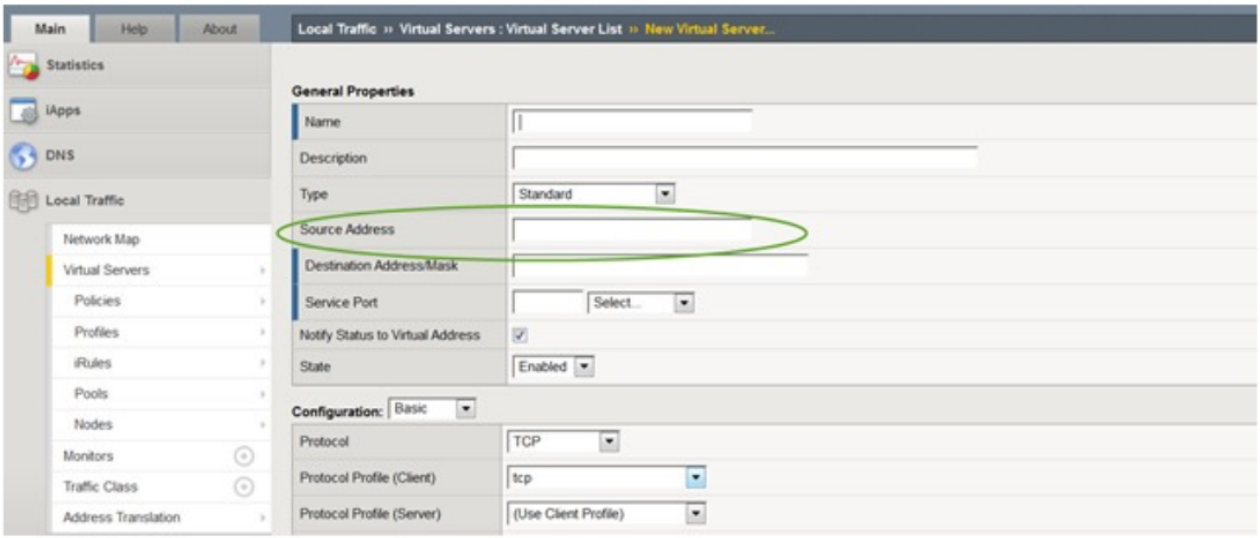
ИСПОЛЬЗОВАНИЕ SOURCE ADDRESS

В прошлой версии TMOS v11.3 поле Source Address было добавлено к настраиваемым параметрам Виртуального Сервера. Как вы вероятно знаете, адрес источника (source address) определяет IP-адрес или подсеть, из которой Виртуальный Сервер принимает трафик, который, в свою очередь, разрешает соединения только от одного из этих IP-адресов. Вам не обязательно использовать эту настройку. Вы можете просто оставить это поле пустым для того, чтобы принимать трафик с любого адреса. Чтобы использовать настройку эффективно, вы должны задать значение, отличное от 0.0.0.0/0 или ::/0 (соответственно, any/0, any6/0).

Для получения максимальной пользы от этой настройки вы должны предельно точно задать адреса, чтобы включить всех пользователей и исключить всех остальных. IP-адреса записываются в формате бесклассовой адресации (CIDR): адрес/префикс, значение префикса обозначает количество единичных бит в маске подсети. Например, IPv4 адреса будет выглядеть следующим образом: 10.0.0.1/32 или 10.0.0.0/24, а IPv6 адреса будет выглядеть так: ffe1::0020/64 или 2001:ed8:77b5:2:10:10:100:42/64. Вы определяете Source Address при создании Виртуального Сервера (Virtual Server).



Кажется, что эта настройка должна быть вписана в Carrier-Grade Network Address Translation (CGNAT), но она может быть использована и в некоторых довольно полезных случаях, и кроме CGNAT.

Я имел возможность присутствовать на F5 Tech Summit, и один из докладчиков (Don Flinspach) в своем замечательном докладе вдохновил всех «Посмотреть изнутри коробки» — со стороны F5 BIG-IP. Основная мысль его доклада была сконцентрирована на том факте, что, пока некоторые функции добавляются в BIG-IP, время от времени бывает полезно понять существующий функционал и использовать его более креативно. Откровенно говоря, это относится к любой функции BIG-IP... в то время, как она была разработана для одних целей, она может (и должна) быть использована во всех нестандартных, творческих идеях. В этой статье мы рассмотрим Source Address (адрес источника).

ИСПОЛЬЗОВАНИЕ SOURCE ADDRESS

Очередность Виртуальных Серверов

Как я упоминал ранее, настройка Source Address проверяет IP-адрес клиента, пославшего запрос и, если адрес совпадает с разрешенными, клиенту дается доступ к этому Виртуальному Серверу. Разумеется, есть много сценариев, при которых клиент посылает запрос, предназначенный для одного виртуального сервера, однако возможно, что их несколько и они имеют одинаковые адреса назначения (и, возможно, те же номера портов). В TMOS существует серия предшествующих проверок, которые используются для определения, какой из виртуальных серверов будет обрабатывать соединение. Порядок их очередности описан в таблице ниже.

Order	Destination	Source	Service port
1	<host address>	<host address>	<port>
2	<host address>	<host address>	*
3	<host address>	<network address>	<port>
4	<host address>	<network address>	*
5	<host address>	*	<port>
6	<host address>	*	*
7	<network address>	<host address>	<port>
8	<network address>	<host address>	*
9	<network address>	<network address>	<port>
10	<network address>	<network address>	*
11	<network address>	*	<port>
12	<network address>	*	*
13	*	<host address>	<port>
14	*	<host address>	*
15	*	<network address>	<port>
16	*	<network address>	*
17	*	*	<port>
18	*	*	*

В этом видео объясняется первоочередность виртуальных серверов более детально: https://www.youtube.com/watch?v=i0Ggz2w19Xc

Также, по этой ссылке вы найдете статью K14800 на портале поддержки о старшинстве виртуальных серверов: Order of precedence for virtual server matching (11.3.0 and later)

Необычные способы использования Source Address

Один из способов использования адреса источника (source address) является создание более целевого виртуального сервера, который можно использовать для упрощения конфигурации (возможно, для исключения iRules или политик LTM, которые запрещают трафик). Как указывал Дон в своем докладе, создание более специфичного Виртуального Сервера может потребовать немного больше усилий для первоначального планирования, но его элементы значительно проще изменять, чем iRules или политики.

ИСПОЛЬЗОВАНИЕ SOURCE ADDRESS

Другой необычный способ использования Source Address – помощь при поиске проблем (troubleshooting). Вы можете просто создать равнозначный виртуальный сервер для расследования, но ограничить Source Address, чтобы протестировать IP-адрес или подсеть клиента. Изменения могут быть произведены даже тогда, когда продуктивный виртуальный сервер продолжает работать. Это также может использоваться при оркестрации.

И, наконец, вы можете использовать поле адреса источника для альтернативной конфигурации «глобального SNAT» как виртуального сервера. Приятель из F5 как-то сказал: «Не существует существенной причины не делать этого (сложность настройки такая же, но с более простым траблшутингом)». Самый простой случай — создание Виртуального Сервера с адресом 0.0.0.0 и с Source Address с изначальным SNAT и SNAT пулом из новых адресов. Ниже пример конфигурации:

```
ltm virtual NAT_192.0.2.1_TO_10.0.2.1 {
destination 0.0.0.0:0
ip-forward
source 192.0.2.1/32
source-address-translation {
pool 10.0.2.1
type snat
}
translate-address disabled
translate-port disabled
}
ltm snatpool 10.0.2.1 {
members {
10.0.2.1
}
```

ИСПОЛЬЗОВАНИЕ SOURCE ADDRESS

Если бы вы спросили Дона, он бы ответил, что это правильный вариант того, как это должно быть сделано. Ниже приведены его аргументы ()

1. Если SNAT включен, IP-адрес клиента всегда транслируется, даже если он подключается к Виртуальному Серверу. Например, возьмите простую конфигурацию, в которой IP клиента 192.0.2.1 транслируется в 10.0.2.1. Это работает хорошо, пока 192.0.2.1 пытается подключиться к виртуальному серверу (например, 192.0.3.1:80).

   - Член пула может принять адрес SNAT (10.0.2.1), но для этого он должен быть в состоянии принять соединения от этой подсети.

   - Если первая причина не подходит, (например, член пула находится в другом VLAN, используя, к примеру, self IP 11.0.2.1/24), передача данных оборвется только для этого одного клиента. В этом случае довольно легко отследить эту причину, но большинство заказчиков ощущают себя загнанными в угол. Часто неясно, как изменить этот адрес обратно или сделать «как должно быть»
     .
   - Если вы внедряете SNAT в виде Виртуального Сервера, он следует всем предшествующим правилам, актуальным для Виртуальных Серверов, [L1] [II2] следовательно, для соединений 192.0.2.1 → 192.0.3.1:80, BIG-IP использует 11.0.2.1 для подключения к члену пула, иначе происходит трансляция через SNAT виртуального сервера, и используется 10.0.2.1.
     [L1]Не знаю, яким синонімом можна замінити...
     Тут и не надо менять. Виртуальный Сервер - это объект в F5. Специфичный. [II2]

2. Если включен NAT/SNAT, транслируется только IP клиента и BIG-IP может тогда попытаться маршрутизировать нетранслируемый трафик. Например, возьмем ту же конфигурацию что мы брали выше: изначальный IP 192.0.2.1 будет транслирован в 10.0.2.1. Если 192.0.2.2 пытается подключиться к BIG-IP, может произойти следующее:

   - Согласно правилам Firewall, адресу 192.0.2.2 запрещено подключение. Этот сценарий встречается, когда BIG-IP – внешнее устройство и это может быть лучшим вариантом.

   - 192.0.2.2 подключается к BIG-IP и перенаправляется на адрес назначения:

     - У получателя прописан обратный маршрут. Это позволит 192.0.2.2 подключиться к сервису, хотя скорее всего это подключение должно было бы быть запрещено.

     - У получателя не прописан обратный маршрут. Трафик будет отброшен, но этот сервер остается подверженным SYN флуду и другим ненужным ему подключениям.

     - Устройство назначения является роутером, который возвращает нетранслированный трафик на BIG-IP прямым или непрямым образом. В результате образуется петля маршрутизации.

   - Если вы применяете SNAT в виде виртуального сервера, будет принят только трафик, подпадающий под заданный адрес источника. Весь остальной трафик будет отброшен.

ИСПОЛЬЗОВАНИЕ SOURCE ADDRESS

Вышенаписанное не является исчерпывающим перечнем вариантов использования Source Address, и я надеюсь, что это, как минимум, немного вдохновит вас на поиск нестандартных и творческих вариантов использования функционала BIG-IP.