Исправление DNS на примере конфигурации ASA

Содержание

Введение

Этот документ показывает, как Исправление DNS используется на Устройстве адаптивной защиты (ASA) для изменения встроенных IP - адресов в ответах Системы доменных имен (DNS) так, чтобы клиенты могли соединиться с правильным IP-адресом серверов.

Предварительные условия

Требования

Исправление DNS требует конфигурации Технологии NAT на ASA, а также включения проверки DNS.

Используемые компоненты

Сведения в этом документе основываются на Устройстве адаптивной безопасности.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

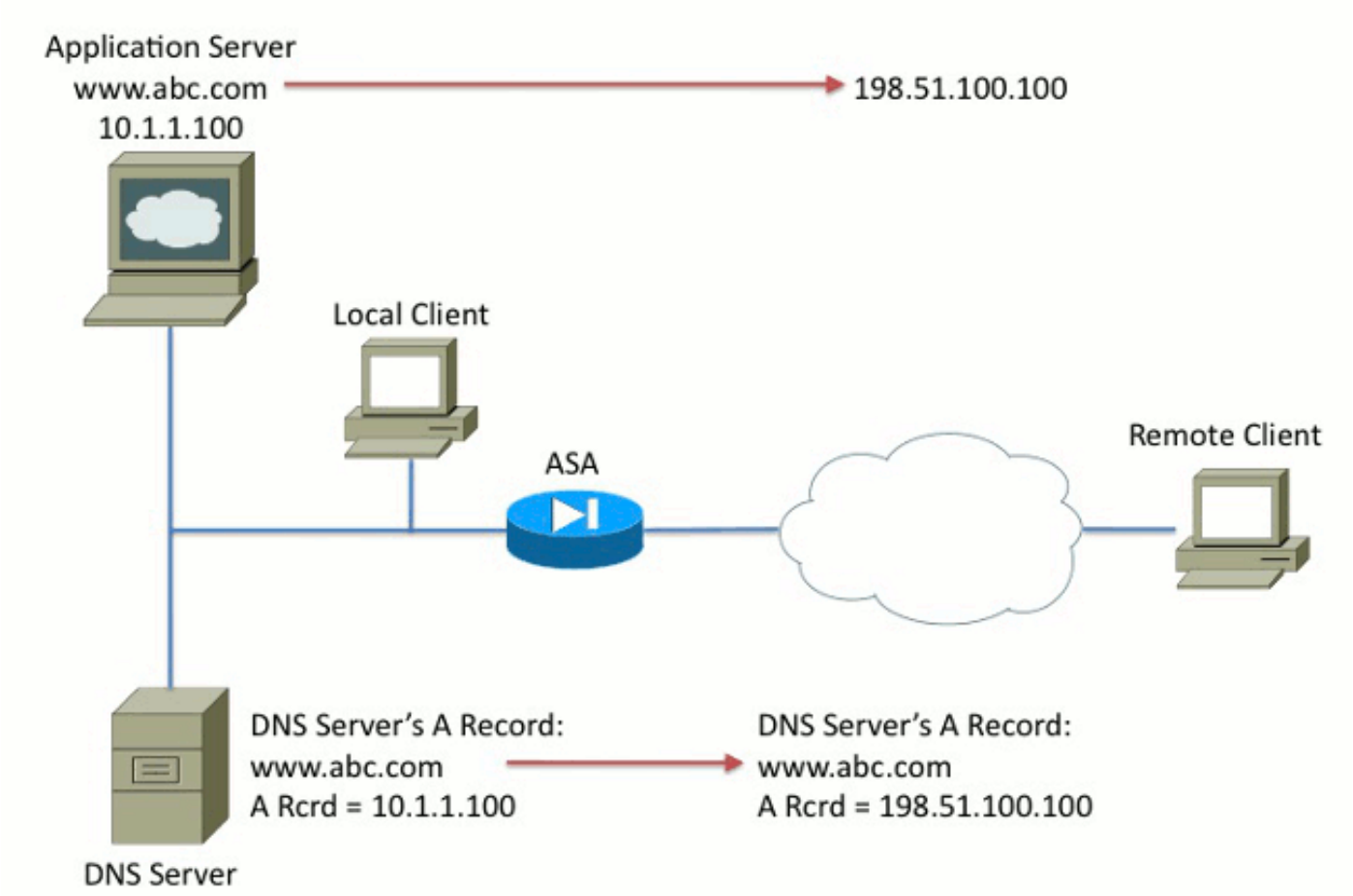
Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Примеры исправления DNS

Сервер DNS на внутренней части ASA

Рисунок 1



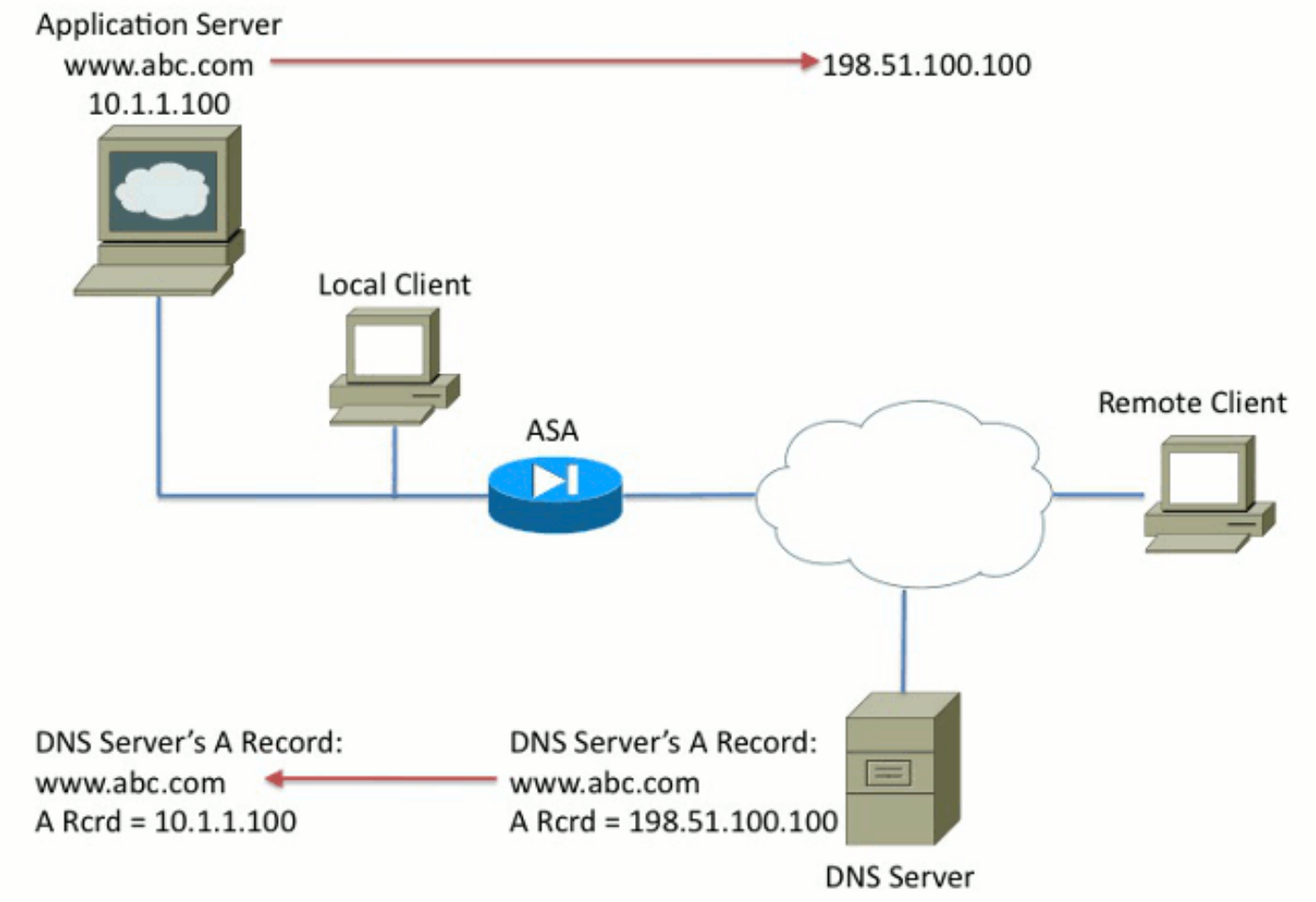

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

На рисунке 1 сервер DNS управляется локальным администратором. Сервер DNS должен раздать закрытый IP - адрес, который является *реальным IP - адресом*, назначенным на сервер приложений. Это позволяет локальному клиенту соединяться непосредственно с сервером приложений.

К сожалению, удаленный клиент не может обратиться к серверу приложений с частным адресом. В результате Исправление DNS настроено на ASA для изменения встроенного IP - адреса в пакете DNS - ответа. Когда удаленный клиент делает запрос DNS для www, это гарантирует это. а B C. com, ответ, который они получают, для транслированного адреса сервера приложений. Без ключевого слова DNS на Выражении NAT удаленный клиент пытается соединиться с 10.1.1.100, который не работает, потому что тот адрес не может маршрутизироваться в Интернете.

Сервер DNS за пределами ASA

Рис. 2



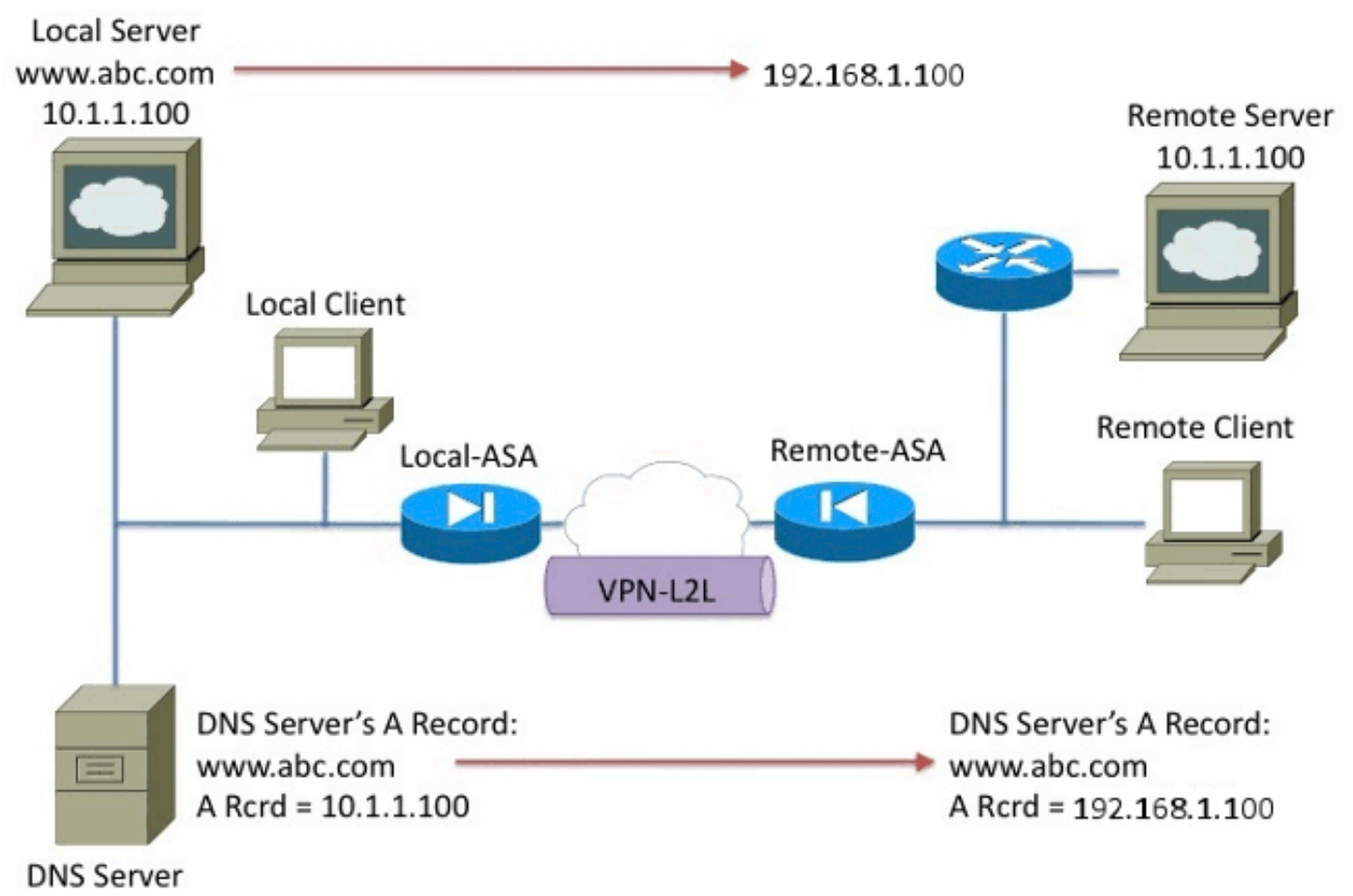

```
nat (inside,outside) source static 10.1.1.100 198.51.100.100 dns
!
policy-map global_policy
  class inspection_default
    inspect dns
```

На рисунке 2 сервер DNS управляется интернет-провайдером или подобным поставщиком услуг. Сервер DNS должен раздать открытый IP - адрес, т.е. *преобразованный IP-адрес* сервера приложений. Это позволяет всем интернет-пользователям обращаться к серверу приложений через Интернет.

К сожалению, локальный клиент не может обратиться к серверу приложений с общим адресом. В результате Исправление DNS настроено на ASA для изменения встроенного IP - адреса в пакете DNS - ответа. Когда локальный клиент делает запрос DNS для www, это гарантирует это. а B C. com, полученный ответ является действительным адресом сервера приложений. Без ключевого слова DNS на Выражении NAT локальный клиент пытается соединиться с 198.51.100.100. Это не работает, потому что этот пакет передан к ASA, который отбрасывает пакет.

VPN NAT и исправление DNS

Рис. 3



Рассмотрите ситуацию, где существуют сети то наложение. В этом условии, адрес 10.1.1.100 жизни и на удаленной стороне и на локальной стороне. В результате необходимо выполнить NAT на локальном сервере так, чтобы удаленный клиент мог все еще обратиться к нему с IP-адресом 192.1.1.100. Чтобы заставить это работать должным образом, Исправление DNS требуется.

Исправление DNS не может быть выполнено в этой функции. Ключевое слово DNS может только быть добавлено до конца объекта NAT или источника NAT. Дважды NAT не поддерживает ключевое слово DNS. Существует две возможных конфигурации и оба сбоя.

Ошибочная конфигурация 1: при настройке практического результата он преобразовывает 10.1.1.1 в 192.1.1.1, не только для удаленного клиента, но и для всех в Интернете. С тех пор 192.1.1.1 не маршрутизуемый Интернет, никто в Интернете не может обратиться к локальному серверу.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 dns
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
```

Ошибочная конфигурация 2: при настройке Исправления DNS линия NAT после необходимого дважды линия NAT это вызывает ситуацию, где никогда не работает Исправление DNS. В результате удаленный клиент пытается обратиться к www. a B C. com с IP-адресом 10.1.1.100, который не работает.

```
nat (inside,outside) source static 10.1.1.100 192.168.1.100 destination
   REMOTE_CLIENT REMOTE_CLIENT
nat (inside,outside) source static 10.1.1.100 64.1.1.100 dns
```

Дополнительные сведения

- CISCO ASA 5500 SERIES ADAPTIVE SECURITY APPLIANCES
- Многофункциональные устройства защиты Cisco ASA серии 5500> Загрузки программного обеспечения
- Cisco Systems – техническая поддержка и документация