Содержание

Вопрос:

Почему мы видим 502 / 504 ошибки GATEWAY_TIMEOUT при просмотре к определенным сайтам?

Признаки: Пользователи получают 502 или 504 ошибки времени ожидания шлюза от Cisco WSA при просмотре к определенным веб-сайтам

Пользователи получают 502 или 504 ошибки времени ожидания шлюза при просмотре к веб-сайтам. Журналы доступа или показали бы 'NONE/504' или 'NONE/502'

Типовая строка журнала Доступа:

1233658928.496 153185 10.10.70.50 GET 17:29 **NONE/504** http://www. пример. com / - ПРЯМОЙ/WWW. пример. com-.....

Существует много причин, почему WSA может возвратить 502 или 504 ошибки времени ожидания шлюза. Несмотря на то, что эти ошибочные ответы подобны, важно понять небольшие различия между ними.

Вот несколько примеров типов сценариев, которые могут произойти:

- **502:** WSA попытался установить TCP - подключение с Web-сервером, но не получил SYN/ACK.
- **504:** WSA получает сброс TCP (RST), завершающий соединение с Web-сервером.
- **504:** WSA не получает ответ от требуемого сервиса до связи с Web-сервером, таким как DNS отказывает.
- **504:** WSA установил TCP - подключение с Web-сервером и отправил запрос GET, но WSA никогда не получает Ответ HTTP.

Ниже примеры каждого сценария и большего количества подробных данных относительно потенциальных проблем:

502: WSA попытался установить TCP - подключение с Web-сервером, но не получил SYN/ACK.
Если Web-сервер не отвечает на SYN - пакеты WSA, после того, как определенная величина попыток, клиент будет передаваться 502 Ошибки времени ожидания шлюза. Типичные причины для этого: **1.** Сеть Web-сервера или Web-сервера имеет проблемы. **2.** Сетевая проблема в сети WSA препятствует тому, чтобы SYN - пакеты добрались до Интернета. **3.** Устройство с функциями межсетевого экрана или аналогичное устройство отбрасывают

или SYN - пакеты WSA или SYN/ACK Web-сервера
4. IP-спуфинг включен на WSA, но должным образом не настроен (никакое перенаправление адреса возврата)

Шаги по устранению неполадок:

Первый шаг должен проверить, может ли WSA Функция проверки связности ICMP ping Web-сервер. Это может быть сделано при помощи следующей команды CLI:
WSA> *пропинговывают www. пример. com*
Если эхо-запрос отказывает, это не означает, что сервер не работает. Это может означать, что пакеты ICMP становятся заблокированными где-нибудь в пути. Если эхо-запрос успешно выполняется, то мы можем знать наверняка, что WSA имеет основной layer3 уровень подключения на Web-сервер.
Тест telnet проверит, имеет ли WSA способность установить TCP - подключение на порту 80 на Web-сервер. См. инструкции далее в этой статье для выполнения теста telnet.

Сетевые проблемы или блок Межсетевого экрана
Если эхо-запрос успешен, но сбои telnet, существует хорошая возможность, что фильтрующее устройство, такое как межсетевой экран, препятствует тому, чтобы этот трафик прошел через сеть. Рекомендуется, чтобы журналы межсетевого экрана и/или захваты пакета от межсетевого экрана были проанализированы для получения дальнейшей информации.
IP-спуфинг включает, но не должным образом настроенный
Если явное проксирование через WSA или тест telnet успешно, это показывает, что WSA может связаться непосредственно с Web-сервером, но когда клиент проксирует через WSA с IP-спуфингом, существует проблема.

Без спуфинга IP-адреса клиента:
- WSA передает SYN к Web-серверу с помощью собственного IP-адреса в качестве источника. Когда пакет возвращается, он идет непосредственно в WSA.

Со спуфингом IP-адреса клиента:
- WSA передает SYN, но вместо этого, использует IP клиента в качестве источника. Без специальной сетевой установки возвращаемый пакет будет передаваться клиенту вместо WSA.
- Для использования спуфинга IP-адреса клиента сеть должна быть настроена в очень особенном методе для упрощения этого, пакеты перенаправлены должным образом. Если пакеты адреса возврата Web-сервера будут переданы клиенту вместо WSA, то WSA никогда не будет видеть SYN/ACK серверов и передаст 502 Ошибки времени ожидания шлюза обратно клиенту.

504: WSA получает сброс TCP (RST), завершающий соединение с Web-сервером.

Если WSA получит пакет сброса TCP на своем восходящем подключении на Web-сервер, то WSA передаст 504 Ошибки времени ожидания шлюза клиенту.

Типичные причины для этого:
1. Cisco Layer 4 Traffic Monitor (L4TM) блокирует прокси WSA от соединения Web-сервера.
2. Межсетевой экран, IDS, IPS или другое устройство проверки пакетов блокируют WSA.

Шаги по устранению неполадок:
Сначала определите, прибывает ли RST TCP из L4TM или из другого устройства.

Если L4TM заблокирует этот трафик, то трафик обнаружится в отчётах о GUI под "*Монитором-> Монитор трафика L4*". В противном случае RST прибывает из другого устройства.

Блокирование L4TM:

Рекомендуется, чтобы, если L4TM блокируется, не блокируйтесь на портах, на которых также работает прокси WSA. Существуют множественные причины для этого:

1. Прокси WSA предоставляет сообщение дружественной ошибки в случае проблемы вместо просто TCP, перезагружающего соединение. Это поможет ограничивать беспорядок от конечных пользователей, когда они будут заблокированы.

2. Прокси WSA имеет способность просмотреть и заблокировать определенное содержание, тогда как L4TM блокирует весь трафик, совпадающий с помещенным в черный список IP-адресом.

Для настройки L4TM для не блокирования на прокси - портах, перейдите "*к GUI-> Security Сервисы-> Монитор трафика L4*".

Если узел является известным плохим веб-сайтом, но существуют причины, почему трафик должен быть позволен, узел может быть белый перечисленный в:
"*GUI-> веб-Менеджер безопасности-> Монитор трафика L4-> Позволяет Список*"

Межсетевой экран / IDS / Блокирование IPS:

Если другое устройство на сетях блокирует WSA от соединения до Web-сервера, рекомендуется проанализировать придерживающееся:

1. Журналы блока межсетевого экрана

2. Вход / Исходящий пакет перехватывает во время проблемы

Блочные журналы могут быстро подтвердить, блокирует ли устройство WSA. Иногда межсетевой экран, IPS или IDS заблокируют трафик и НЕ регистрируют его соответственно. Если это верно, единственный способ доказать, куда RST TCP прибывает из, состоит в том, чтобы получить входные и выходные перехваты из устройства. Если RST отсылается, входной интерфейс и никакие пакеты переместились через выходную сторону, устройство безопасности является определенно причиной.

504: WSA установил TCP - подключение с Web-сервером и отправил запрос GET, но WSA никогда не получает Ответ HTTP.

Если WSA передаст GET HTTP, но никогда не будет получать ответ, то он передаст 504 Ошибки времени ожидания шлюза клиенту.

Типичные причины для этого:

- Межсетевой экран, IDS, IPS или другое устройство проверки пакетов позволяют TCP - подключение, но блокируют содержание HTTP от достижения Web-сервера. В этом случае тест telnet может помочь изолировать, какой вид данных HTTP блокируется.

Журналы блока межсетевого экрана могут быстро подтвердить, если / почему устройство блокирует WSA. Иногда межсетевой экран, IPS или IDS заблокируют трафик и НЕ регистрируют его соответственно. Если это верно, единственный способ доказать, куда RST TCP прибывает из, состоит в том, чтобы получить входные и выходные перехваты из устройства. Если RST отсылается, входной интерфейс и никакие пакеты переместились через выходную сторону, устройство безопасности является определенно причиной.

Тестирование подключения с Web-сервером с помощью telnet

От CLI WSA выполните **команду telnet**:
WSA> **telnet**
Выберите, от какого интерфейса вы хотите к telnet.
1. Auto
2. Менеджмент (192.168.15.200/24: wsa. host name. com)
3. P1 (192.168.113.199/24: data.com)
[1]> **3**

Введите удаленное имя хоста или IP-адрес.
[]> www. пример. com

Введите удаленный порт.
[25]> **80**

Попытка 10.3.2.99...
Связанный с www. пример. com.
Символ выхода является '^]'.

Примечание: "Связанное" сообщение красного цвета, указывает, что TCP успешно установил между WSA и Web-сервером.

Запрос HTTP может вручную быть передан через этот сеанс Telnet также. Ниже приводится типовой запрос, который может быть введен после "Связанного" сообщения:

GET http://www. пример. **HTTP/1.1** com
ХОСТ: www. пример. com
Введите

Примечание: Удостоверьтесь, что добавили дополнительный возврат каретки в конце, иначе сервер не ответит на запрос.