Содержание

Вопрос:

Вопрос:

Что означают другие Коды ответа HTTP?

Среда: Cisco Web Security Appliance (WSA), выполняющий любую версию AsyncOS

HTTP всегда имеет запрос клиента и ответ сервера. Ответы сервера классифицированы числовым кодом ответа. Коды ответа указывают на причины позади успешных и отказавших запросов HTTP.

Для полных подробных сведений относительно Кодов ответа HTTP посмотрите (HTTP) RFC 2616, разделите 10.

Ниже подробные данные относительно наиболее распространенного кода ответа, с которым вы, вероятно, столкнетесь:

1xx коды: Информационный

100 Продолжите: Как правило, замеченный в отношении протокола ICAP. Это - информационный ответ который, позвольте нам, клиент знает, что он может продолжить передавать данные. В отношении сервисов ICAP (таких как поиск вирусов), сервер может только хотеть видеть первую x сумму байтов. Когда это будет сделано, просматривая первый набор байтов и не обнаружило вирус, это передаст 100, Продолжают сообщать клиенту для передачи остатка объекта.

2xx коды: Успешный

200 OK: наиболее распространенный код ответа. Это показывает, что запрос успешен без любых проблем.

3xx коды: Перенаправление

302 Найденных: Это - временное перенаправление. Клиент проинструктирован для выполнения нового запроса для объекта, заданного в Местоположении: заголовок.

304 Не Модифицированный: Это в ответ на **GIMS** (If-modified-since GET). Это - буквально стандартный GET HTTP, который включает **If-modified-since** заголовка**: <дата>.** Этот заголовок говорит серверу, что у клиента есть копия запрашиваемого объекта в, он - локальный кэш, и включенный дата, объект был выбран. Если объект модифицировался с тех пор, сервер ответит 200 OK и свежей копией объекта. Если объект не изменился начиная с выбранной даты сервер передаст 304 обратно Не Модифицированный ответ.

307 Временных Перенаправлений: Для всех намерений и целей, это имеет то же значение как 302. Если более подробная информация обнаружена, эта статья может быть обновлена.

4xx коды: Ошибка клиента

400 Плохих Запросов: Это означает, что что-то в запросе HTTP не придерживается правильного синтаксиса. Возможные причины могли произойти из-за множественных заголовков, находящихся на той же линии, пробелах в заголовке, никаком HTTP/1.1 в URI, так дальше. На RFC 2616 нужно сослаться для собственного синтаксиса.

401 Неавторизованный: объект, который запрашивают, требует аутентификации для доступа. Эти 401 используются для аутентификации к целевому Web-серверу. Когда аутентификация включена на прокси, при использовании Cisco Web Security Appliance (WSA) в прозрачном режиме 401 передают обратно клиенту. Это вызвано тем, что устройство имитирует себя, как будто это был OCS (сервер содержания происхождения).

Доступные методы проверки подлинности заданы в **www - аутентифицируйтесь**: заголовок Ответа HTTP. Это скажет клиенту, просит ли этот сервер NTLM, основные, или другие методы проверки подлинности.

403 Запрещенных: клиент запрещен от доступа к запрашиваемому объекту. Существует много причин для того, почему сервер может запретить доступ к объекту. Как правило, сервер будет включать своего рода описание причины в данных HTTP (ответ HTML).

404 Не Найденный: запрашиваемый объект не существует на сервере.

407 Требуемых Проверок подлинности прокси-сервера: Это совпадает с 401, за исключением того, что это в частности для аутентификации к прокси, не OCS. Это передается, только если запрос был отправлен явно к прокси. 407 не могут быть переданы клиенту при использовании WSA в качестве режима прозрачного прокси, поскольку клиент не знает, что существует прокси. Если это верно, клиент будет наиболее вероятный FIN или RST TCP - сокет.

Вместо того, чтобы использовать www - аутентифицируйтесь: заголовки для определения, какие методы аутентификации доступны, **прокси - аутентифицируются**: заголовок используется.

5xx коды: Ошибка сервера

500 Внутренних ошибок сервера: сбой Общего сервера

502 Недопустимых шлюза: Вы будете, как правило, видеть это при использовании WSA как прокси, где шлюз отвечает неправильно.

503 Недоступные Сервиса: Когда OCS по обремененному, это, как правило, передается. Попытка запроса снова в более позднее время должна быть успешной.

504 Таймаута шлюза: Если WSA не получил ответ от своего шлюза, 504 будут передаваться.