Подлинные сбои через WSA, когда клиент использует NEGOEXTS

Содержание

Введение

Этот документ описывает, как к overocme проблема, когда Аутентификация отказывает через Cisco Web Security Appliance (WSA), когда клиент использует NEGOEXTS.

Общие сведения

Cisco Web Security Appliance (WSA) может аутентифицировать пользователей для применения политики на основе пользователя или группы. Один из методов, который доступен, является Kerberos. При использовании Kerberos как метод аутентификации в Идентичности WSA отвечает на запрос HTTP клиента с (прозрачными) 401 или 407 (явных) Ответов HTTP, которые содержат **WWW** заголовка **- Аутентифицируйтесь: Выполнить согласование**. На этом этапе клиент передает новый запрос HTTP с **Авторизацией: Выполните согласование** о заголовке, который содержит Прикладной программный интерфейс Сервиса безопасности Общего назначения (GSS-API) и Простой Защищенный Negotation (SPNEGO) протоколы. Под SPNEGO пользователь представляет **mechTypes**, который он поддерживает. Это mechTypes, который поддерживает WSA:

- метод аутентификации KRB5-Kerberos, который используется, если Kerberos поддерживается и настроенный правильно на клиенте и если допустимый билет Kerberos присутствует для сервиса, к которому обращаются
- NTLMSSP-метод Microsoft NTLM Security Support Provider, который используется, если никакие допустимые билеты Kerberos не доступны, но Выполняют согласование о подлинном методе, поддерживается

Проблема: Подлинные Сбои через WSA, когда клиент использует NEGOEXTS

В более свежем Windows версий Microsoft IE поддерживается новый подлинный метод, вызвал NegoExts, который является расширением к Выполнить согласование протоколу аутентификации. Когда единственные поддерживаемые методы являются NEGOEXTS и NTLMSSP, этот mechType считает более безопасным, чем NTLMSSP, и предпочитает клиент. Дополнительные сведения могут быть найдены в этой ссылке:

[Представление расширений к выполнить согласование пакету аутентификации](#)

Этот сценарий, как правило, происходит, когда Выполнить согласование подлинный метод выбран и существует № KRB5 mechType (скорее всего, из-за пропавших без вести допустимого билета Kerberos для сервиса WSA). Если клиент выбирает NEGOEXTS (может быть замечен как NEGOEX в wireshark), то WSA является unabled для обработки подлинной транзакции и подлинных сбоев для клиента. Когда это происходит, эти журналы замечены в подлинных журналах:

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP
packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

Когда аутентификация отказывает, это происходит:

Если гостевые полномочия включены - клиент классифицирован как **Не прошедший поверку подлинности** и перенаправленный к веб-сайту

Если гостевые полномочия отключены - клиенту предоставляют еще 401, или 407 (в зависимости от метода прокси) с остающимися подлинными методиками, представленными в заголовке ответа (выполните согласование, не представлен снова). Если NTLMSSP и/или Основная аутентификация будут настроены, подлинное приглашение, вероятно, произойдется. Если нет никаких других подлинных методов (Идентичность настроена только для Kerberos), то аутентификация просто отказывает.

Решение

Решение этой проблемы состоит в том, чтобы или удалить аутентификацию Kerberos из Идентичности - или исправляют клиента так, чтобы это получило допустимый билет Kerberos для сервиса WSA.