

Содержание

[Вопрос](#)

[Среда](#)

[Признаки](#)

[Обходной путь 1](#)

[Обходной путь 2](#)

Вопрос

Когда SaaS с Идентификационным Поставщиком инициировала потоки и NTLM, почему пользователям предлагают для аутентификации?

Среда

- Cisco Web Security Appliance (WSA) рабочие версии AsyncOS 7.0 или позже
- NTLM используется для прозрачной аутентификации
- Управление доступом SaaS настроенное использование идентификационного поставщика инициировало поток
- SSO SaaS настроен

Мне настроили Управление доступом SaaS с моим внешним приложением, с помощью идентичности инициируемый поставщиками поток и SAML для единой точки входа. Я также использую NTLM для прозрачной аутентификации моих пользователей. Однако, как я могу препятствовать тому, чтобы они видели это приглашение?

Признаки

- Когда пользователи щелкают по своей закладке для URL SSO SaaS, они иногда видят опознавательные приглашения.
- Если пользователи обращаются к другому внешнему вебу - узлу и затем нажимают закладку URL SSO SaaS, доступ хорошо работает.

Эта проблема происходит, когда/потому что первый запрос, который WSA видит от клиента, к специальному URL SSO, который подается непосредственно от WSA.

Содержание, которое подается непосредственно от WSA - такого как страницы EUN или файлы PAC - обычно освобождено от аутентификации. В то время как функция SaaS может обратиться к опознавательным заместителям, поддержанным прокси, она не может самостоятельно запросить аутентификацию с помощью любого метода помимо основанной на форме аутентификации (NTLM или LDAP). Таким образом, наблюдаемое состояние на дизайн, но не является оптимальным решением.

Дефектный [CSCzv55859](#) подан, чтобы отследить эту проблему и предоставить лучший

механизм для решения этой проблемы.

Существует два доступные обходных пути.

Обходной путь 1

1. Первое должно использовать Иницируемый поставщиками услуг поток в конфигурации SaaS. В иницируемом в SP потоке пользователь запускает путем просмотра к целевому приложению SaaS, которое тогда выполняет перенаправление через URL SSO.
Поскольку этот начальный трафик проходит прокси, пользователь получит аутентифицируемый должным образом использующий NTLM. Если целевое приложение поддерживает иницируемые в SP потоки, этот обходной путь только работает.
2. Создайте новый URL SSO в политике WSA, вызвав аутентификацию и затем перенаправив клиента к "реальному" URL SSO.

Обходной путь 2

1. Выберите новый URL SSO. К этому URL никогда не будет фактически обращаться прокси; это будет просто действовать как точка для иницирования процесса входа в систему.

Например, если текущий URL SSO является "**wsa.mycompany.com/SSOURL/WebEx**", можно использовать "**wsa. пример. com/SSOURL/WebEx**". Важное рассмотрение удостоверяется часть имени хоста, которую вы используете, будет проксирован через WSA.

Когда WSA развернут как явный прокси, имя хоста может быть примерно чем-либо. Если WSA будет развернут как режим прозрачного прокси, то имя хоста должно будет быть реальным именем хоста, которое решает к внешнему IP - адресу.

2. Создайте пользовательскую категорию URL (**GUI > веб-Менеджер безопасности > Пользовательские категории URL**), который совпадает, новый URL. You должен будет создать одну пользовательскую категорию URL для каждого приложения SaaS, к которому необходимо применить обходной путь.
Используйте соответствие регулярного выражения для соответствия на полном URL.
3. Перейдите к политике доступа (**GUI > веб-Менеджер безопасности > Политика доступа**) и под столбцом фильтрации URL-адресов для политики доступа, с которой будет совпадать запрос пользователя. Это может быть глобальной политикой или другой политикой ранее в таблице.
Включайте новую пользовательскую категорию URL в эту политику доступа и заставьте ее действие **перенаправлять**. Цель перенаправления должна быть "реальным" URL SSO.

4. Отправьте и передайте изменения для применения новой конфигурации.

Пользователи должны теперь использовать новый URL SSO для доступа к приложению. Поскольку доступ к этому URL обработан прокси, аутентификация NTLM будет вызвана, и пользователь всегда будет регистрироваться прозрачно, избегая опознавательных приглашений.