Содержание

[Вопрос](#)
[Среда](#)
[Признаки](#)
[Шаг 1: Создайте пользовательскую категорию URL](#)
[Шаг 2: Добавьте новую идентичность](#)
[Шаг 3: Добавьте новую идентичность к политике доступа](#)
[Обходной путь для Использования существующей политики доступа](#)
[Обходной путь для Использования новой политики доступа](#)

Вопрос

Когда аутентификация включена на Веб-безопасности Aplliance (WSA) Cisco, почему не работает Агент Teamviewer?

Среда

Cisco Web Security Appliance (WSA) и любая версия AsyncOS.

Признаки

Агент Teamviewer испытывает таймаут, и accesslog показывает записи, которые содержат 401 или 407 ошибок при указании "на Требуемую Проверку подлинности прокси-сервера".

Когда запросы WSA об аутентификации из приложения TeamViewer, приложение может не предоставить доменные учетные данные, Агенты Teamviewer не работают с аутентификацией - значение. Таким образом, необходимо исключить его из аутентификации.

Если WSA настроен для использования **Cookie** в качестве заместителей в Личностях (**GUI> веб-Менеджер безопасности> Личности**), опознавательное освобождение требуется.

Если Личности настроены заместителям **IP-адреса**, то ниже шагов может не требоваться, потому что учетные данные клиента кэшируются в течение периода, равного **Суррогатному Таймауту** (по умолчанию = 1 час), как только они обращаются к любому веб-сайту (веб-сайтам) с помощью своего браузера.

- **Примечание:** В Явном режиме (использующий файл PAC или параметры прокси браузера), гарантируйте, что проверено **Применение тех же суррогатных параметров настройки к явной прямой** опции **запросов**
- Если мы периодически видим 401s/407s в журналах доступа при доступе к Teamviewer, мы можем все еще использовать ниже шагов для обхода аутентификации.

Для настройки опознавательного освобождения для Teamviewer выполните эти действия:

Шаг 1: Создайте пользовательскую категорию URL

Агент Teamviewer соединяется с другими серверами с другими IP-адресами, таким образом, необходимо установить некоторые регулярные выражения.

1. Перейдите к **веб-GUI> веб-Менеджер безопасности> Пользовательские Категории URL**.

2. Нажмите **Add Custom Category...** кнопка.

3. Выберите название категории.

4. В поле Sites введите придерживающееся: **.teamviewer.com, dyngate.com**.

5. Нажмите **Advanced** и в поле Regular Expressions, добавьте придерживающееся:
   din\.aspx
   dout\.aspx

6. Подвергнитесь и Передача ваши изменения.

Шаг 2: Добавьте новую идентичность

1. Перейдите к **веб-GUI> веб-Менеджер безопасности> Личности**.

2. Нажмите **Add Identity...** кнопка.

3. Создайте идентичность **без аутентификации**.

4. Нажмите **Усовершенствованное** раскрывающееся меню и затем нажмите **None Selected link to the right of URL Categories**.

5. Добавьте недавно созданную **Пользовательскую Категорию URL** (посмотрите выше) к Идентичности путем выбора корректной строки.

6. Подвергнитесь и Передача ваши изменения.

Шаг 3: Добавьте новую идентичность к политике доступа

Существует две возможности сделать это; можно или использовать существующую Политику доступа или создать новую.

Обходной путь для Использования существующей политики доступа

1. Перейдите к **веб-GUI> веб-Менеджер безопасности> Политика доступа.**
2. Для Названия Политики доступа, где Пользовательский URL должен быть позволен, щелкните по ссылке под столбцом **URL Categories**.

3. Щелкните **по [включать]** ссылке на недавно созданной Пользовательской Категории и заставьте действие **Позволять** или **Контролировать**.

4. Подвергнитесь и Передача ваши изменения.

Обходной путь для Использования новой политики доступа

1. Перейдите к **веб-GUI> веб-Менеджер безопасности> Политика доступа**.

2. Щелкните **по Добавить Политике**... кнопка.

3. Выберите *<name> политики*.

4. Щелкните по выпадающему списку **Identities и Users** и выберите недавно созданную Идентичность.

5. Подвергнитесь и Передача ваши изменения.