Table of Contents

Table of Contents 1
Авторизация и аутентификация 2
- Определение пользователей при авторизации с помощью NTLM 3
- Разрешения доступа администраторов 4
- Настройка браузера Chrome на Linux для авторизации Kerberos/Captive portal 5
- Некорректная работа правил UserGate NGFW при работе с доменными пользователями 6
- Периодические разрывы связи при работе с потоковыми сервисами 7
- Проблемы с авторизацией при использовании нескольких методов аутентификации 8
- Загрузка сертификатов на клиентское устройство с ОС Windows 11 9
- Как настроить прозрачную аутентификацию Kerberos в нескольких доменах? 10

Авторизация и аутентификация

Определение пользователей при авторизации с помощью NTLM

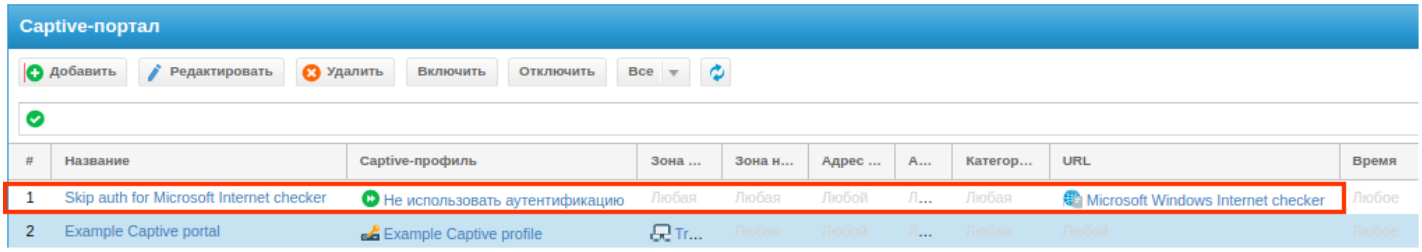
Product: UserGate NGFW

Задача

После авторизации на captive-портале с помощью NTLM для части запросов определяется только тип пользователей **Known**/**Unknown**.

Решение

При авторизации с использованием NTLM некоторые GET-запросы приходят от системы, а не от пользователя. В этом случае идентификация пользователя невозможна, поэтому такому пользователю присваивается тип **Known**. Для исправления данной ситуации необходимо в списке правил captive-портала включить и поставить первым правило **Skip auth for Microsoft Internet checker**, созданное по умолчанию для исключения подобных запросов из captive-портала.



Примечание В список URL Microsoft Windows Internet checker, возможно, необходимо будет добавить домены ipv6.msftncsi.com и *.microsoft.com.
Важно! В качестве зоны источника следует указать зону, назначенную на интерфейсах, через которые доступны сети с пользовательским трафиком, например, Trusted.
Важно! После добавления правила пользователям необходимо повторно авторизоваться (можно сбросить авторизацию всех пользователей или подождать истечения срока жизни авторизованного пользователя).

Разрешения доступа администраторов

Version: 7.0.0, 6.x
Product: UserGate NGFW

Задача

Администратору даны права доступа **Чтение и запись** на раздел **Политики сети → Межсетевой экран**. При попытке редактирования правил данного раздела отображается ошибка: **У вас нет прав доступа**.

Решение

Необходимы дополнительные разрешения на объекты: сценарии, серверы ICAP, профили защиты DoS и т.п.

Для возможности внесения изменений в политику межсетевого экранирования, помимо прав **Чтение и запись** на раздел **Межсетевой экран**, администратору необходимы разрешения на просмотр раздела **Политики безопасности → Сценарии**.

Данное разрешение необходимо для работы с разделами **Межсетевой экран**, **NAT и маршрутизация**, **Пропускная способность**, **Фильтрация контента**, **Правила защиты DoS** (для раздела **Правила защиты DoS** также необходимы права на раздел **Политики безопасности → Профили DoS**).

Настройка браузера Chrome на Linux для авторизации Kerberos/Captive portal

Product: UserGate NGFW

Задача

В браузере Chrome (и его вариациях) не отображается портал авторизации. Пользователь видит пустое окно со следующим содержимым:

Заголовок:

HTTP/1.1 407 Authorization Required

Содержимое страницы

<html> <!-- please auth via kerberos/NTLM ➔ </html>

Решение

Для подробной информации по работе с политиками в браузере, обратитесь к документации по адресу: https://www.chromium.org/administrators/linux-quick-start

1. В соответствии с инструкцией, нужно создать json-файл в директории managed:

touch /etc/opt/chrome/policies/managed/test_policy.json

Содержимое файла должно быть следующего вида:

{

"AuthServerWhitelist": "*.usergate.demo",

"AuthSchemes": "ntlm,negotiate"

}

"usergate.demo" необходимо заменить на доменное имя вашего домена.

2. В браузере Chrome открыть страницу политик about:policy.

Вы должны увидеть настройки прописанные в файле на открытой странице:

Chrome Policies

Policy name	Policy value
AuthSchemes	ntlm,negotiate
AuthServerWhitelist	*.usergate.demo

Если этих строк нет, значит браузеру не удалось загрузить политики из созданного файла. Проверьте права доступа, и другие возможные причины. Обратите внимание, различные браузеры имеют особенности в загрузке политик. Например браузер Chromium на Kali Linux автоматически не загружает описанные политики.

После проведенных манипуляций, браузер не способный произвести прозрачную Kerberos аутентификацию, будет перенаправлять пользователя на портал авторизации.

Некорректная работа правил UserGate NGFW при работе с доменными пользователями

Version: 5.x, 6.x, 7.x
Technology: Identification and Authentication
Product: UserGate NGFW

Задача

При изменении членства пользователя в доменных группах, UserGate NGFW не учитывает эти изменения.

Решение

Для того, чтобы UserGate NGFW обновил информацию о членстве в группах для пользователя, нужно:

1. В CLI выполнить команду: cache ldap-clear
2. Произвести переподключение пользователя на клиентской станции (Вход-Выход).
3. Произвести процедуру выхода пользователю на UserGate NGFW.

После этого работа с обновленным пользователем нормализуется.

Периодические разрывы связи при работе с потоковыми сервисами

Technology: Identification and Authentication
Version: 5.x, 6.x, 7.x
Product: UserGate NGFW

Задача

При работе с потоковыми сервисами (например, видеоконференция) периодически происходит обрыв связи.

Решение

Это штатное поведение, описанное в Руководстве Администратора. Параметр *Время жизни авторизованного пользователя* - это таймер, устанавливаемый при аутентификации пользователя. По его истечении сбрасываются все установленные с IP-адреса пользователя соединения.

Вы можете:

1. увеличить этот таймер до нужных значений;
2. создать для пользователя отдельное правило Captive-портала с дополнительным условием, например, IP-адрес источника, с указанием другого профиля авторизации;
3. установить на компьютер пользователя агент авторизации.

Проблемы с авторизацией при использовании нескольких методов аутентификации

Technology: Identification and Authentication
Version: 6.x, 7.x
Product: UserGate NGFW

Задача

Настроены несколько методов аутентификации (Kerberos, NTLM, локальный пользователь); используются несколько правил captive-портала без дополнительных условий (источник, назначение и т.п.), т.е. всегда срабатывает первое правило, для которого совпали все условия.

Решение

Добавьте в используемый профиль аутентификации сразу три метода аутентификации: **Kerberos**, **NTLM** и **локальный пользователь**. В соответствии с данным профилем:

- для доменных пользователей и комьютеров будет работать авторизация с использованием Kerberos;
- для доменных пользователей, но недоменных компьютеров можно будет вводить учетные данные домена;
- локальные пользователи смогут авторизоваться на Captive-портале с логином/паролем.

О применении политик UserGate к пользователя читайте в соответствующей статье: Применение к пользователям политик UserGate .

Загрузка сертификатов на клиентское устройство с ОС Windows 11

Technology: Identification and Authentication

Задача

Как автоматизировать загрузку сертификатов на клиентское устройство с ОС Windows 11.

Решение

При тестировании технических решений бывает необходимо автоматизировать процесс загрузки пользовательских сертификатов на клиентское устройство с ОС Windows. Часто для этих целей в скриптах используется системная утилита certutil. Однако в Windows 11 утилита certutil загружает пользовательский сертификат некорректно. В качестве альтернативного метода загрузки сертификата на клиентском устройстве с ОС Windows 11 можно использовать следующую последовательность команд в PowerShell:

```
$pfx = new-object System.Security.Cryptography.X509Certificates.X509Certificate2
$pfx.import("C:\cert.pfx","1234","MachineKeySet, PersistKeySet")
$store = new-object System.Security.Cryptography.X509Certificates.X509Store("My","LocalMachine")
$store.open("MaxAllowed")
$store.add($pfx)
$store.close()
```

Подробнее об использованных атрибутах смотрите в статье: https://learn.microsoft.com/en-us/dotnet/api/system.security.cryptography.x509certificates.x509keystorageflags?view=net-8.0

Как настроить прозрачную аутентификацию Kerberos в нескольких доменах?

Technology: Identification and Authentication
Version: 6.x, 7.x
Product: NGFW

Задача

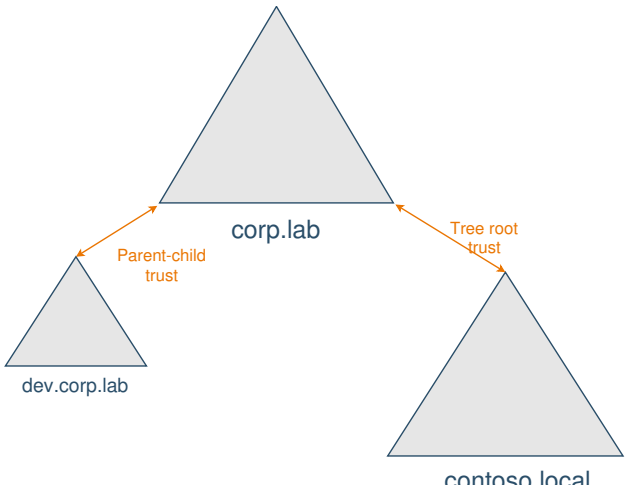
Как настроить прозрачную аутентификацию Kerberos в нескольких доменах?

Решение

На самом прокси-сервере никаких дополнительных настроек производить не требуется. Для корректной работы аутентификации Kerberos в нескольких доменах необходимо настроить некоторые параметры доменов. А именно, потребуется произвести следующие настройки:

- Убедиться, что между всеми деревьями и лесами доменов, а также между всеми доменами в дереве установлено транзитивное двунаправленное доверие.
- Во всех доменах синхронизировано время.
- Хосты во всех доменах доверяют прокси-серверу.

Возьмём для примера инфраструктуру Active Directory со следующей конфигурацией:



Хосты из всех доменов пользуются прокси-сервером с FQDN auth.corp.lab, который разрешается в IP-адрес интерфейса UserGate NGFW. Keytab-файл также создан в домене corp.local и привязан к принципалу HTTP/auth.corp.local.

Хосты из леса corp.lab, по умолчанию будут доверять запросам аутентификации Kerberos от хоста auth.corp.lab, так как все они находятся в рамках единого домена. Чтобы хосты из домена contoso.local также начали предоставлять данные аутентификации хосту из другого домена, нужно добавить FQDN прокси-сервера в зону доверенных хостов. Сделать это удобно при помощи групповых политик:

- User Configuration ➜ Policies ➜ Administrative Templates ➜ Windows Components ➜ Internet Explorer ➜ Internet Control Panel ➜ Security Page \ Site to Zone Assignment List.

  В данной конфигурации прописать FQDN прокси-сервера и задать значение 2:

- User Configuration ➜ Policies ➜ Administrative Templates ➜ Windows Components ➜ Internet Explorer ➜ Internet Control Panel ➜ Security Page \ Trusted Sites Zone \ Logon Options. Установить в значение "Automatic logon with current username and password".

Для браузера FireFox возможно потребуется дополнительная настройка доверенных FQDN хостов для аутентификации. Подробнее читайте в статье Авторизация с помощью Kerberos.