ОБНОВЛЕНО 16 МАР

TCP авторизация

TCP-авторизация предназначена для защиты сетевой инфраструктуры от атак, связанных с подменой IP-адресов (IP-spoofing), а также от ситуаций, когда злоумышленник не может установить полноценное TCP-соединение. Данный механизм позволяет проверить подлинность отправителя TCP-пакетов и минимизировать риски несанкционированного доступа.

Основные команды и их назначение

Проверка наличия IP-адреса в таблице доверенных узлов

```
-c insert -- ! -m hmark id 77 status valid -j TCPAUTH 1 type hs atype hs
```

Если IPv4-адрес отправителя отсутствует в таблице "host mark" ID 77 или его статус "valid" истёк, выполняется TCP-авторизация с применением RST на SYN и RST на SYN+ACK.

Добавление IP-адреса в доверенную таблицу

```
-c insert -- -m verdict tcpauth valid -j HMARK id 77 value 1 lifetime 3600
```

При успешном прохождении TCP-авторизации IPv4-адрес отправителя добавляется в "host mark" ID 77 со значением "1" и временем жизни 3600 секунд.

Обработка неудачной авторизации

```
-c insert -- -m verdict tcpauth invalid -j STATS TCP_AUTH -j DROP
```

В случае неуспешной авторизации пакет фиксируется в статистике с тегом "TCP_AUTH" и отбрасывается.

Полный пример конфигурации:

```
-c insert -- ! -m hmark id 77 status valid -j TCPAUTH 1 type hs atype hs
-c insert -- -m verdict tcpauth valid -j HMARK id 77 value 1 lifetime 3600
-c insert -- -m verdict tcpauth invalid -j STATS TCP_AUTH -j DROP
-c insert -- -j VERDICT clear
```

Рекомендации по применению

Выбор метода TCP-авторизации определяется характеристиками сервиса и параметрами сети, инициирующей или принимающей подключение. В зависимости от этих факторов рекомендуется применять различные механизмы проверки.

Настоящий документ предоставляет сведения о применении TCP-авторизации в различных сетевых инфраструктурах. Перед внедрением рекомендуется тестирование специфических сценариев, включая нестандартные приложения.

Определение совместимости: Авторизация считается прозрачной для пользователя, если выполняется автоматически и не требует дополнительных действий, таких как обновление страницы или повторное установление соединения.

Веб-приложения

Браузер	Операционная система	Исходящая сеть	Совместимость SA-авторизации	Совместимость RST-авторизации
PC				
Google Chrome	Windows 10,11	РТК-бизнес		
Google Chrome	Mac OS 13.4	РТК-бизнес		
Google Chrome	Linux Ubuntu 22.04.2 LTS	РТК-бизнес		
Atom	Windows 10,11	РТК-бизнес		
Safari	Mac OS 13.4	РТК-бизнес		Требуется перезагрузка страницы
Яндекс Браузер	Windows 10,11	РТК-бизнес		
Яндекс Браузер	Mac OS 13.4	РТК-бизнес		

Браузер	Операционная система	Исходящая сеть	Совместимость SA-авторизации	Совместимость RST-авторизации
Mozilla Firefox	Windows 10,11	РТК-бизнес		
Opera	Windows 10,11	РТК-бизнес		
TOR Browser	Windows 11	РТК-бизнес	Отсутствует	
Brave Browser	Windows 11	РТК-бизнес		
Mobile				
Google Chrome	Android 11,12,13	РТК-бизнес, МТС, Билайн, Мегафон		
Google Chrome	iOS 16	РТК-бизнес, МТС, Билайн, Мегафон		
Safari	iOS 16	РТК-бизнес, МТС, Билайн, Мегафон		Требуется перезагрузка страницы
Яндекс Браузер	Android 11,12,13	МТС, Билайн, Мегафон		

Последнее обновление рекомендаций: 13 июля 2023 г.