Содержание

Введение

Если вы входите в удаленный хост с помощью Протокола удаленного рабочего стола (RDP), и удаленное имя пользователя является другим, чем пользователь, Системные изменения FireSIGHT IP-адрес пользователя, который привязан к IP-адресу на Центре управления FireSIGHT. Это вызывает изменение в разрешениях для пользователя относительно правил Управления доступом. Вы заметите, что неправильный пользователь привязан к рабочей станции. Этот документ предоставляет решение для этой проблемы.

Предварительные условия

Cisco рекомендует ознакомиться в Системе FireSIGHT и Клиенте User Agent.

> **Примечание:** Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Основная причина

Эта проблема происходит из-за пути Microsoft Active Directory (AD) попытки аутентификации RDP журналов к Входу в систему безопасности Windows Контроллера домена. AD регистрирует попытку аутентификации для сеанса RDP против IP-адреса вызывающего узла, а не оконечной точки RDP, с которой вы соединяетесь. Если вы войдете в удаленный хост с другой учетной записью пользователя, то это изменит пользователя, привязанного к IP-адресу вашей исходной рабочей станции.

Проверка

Для проверки это - то, что происходит, можно проверить, что IP-адрес от события входа в систему от исходной рабочей станции и удаленного хоста RDP имеет тот же IP-адрес.

Для обнаружения этих событий необходимо будет придержаться ниже шагов:

Шаг 1: Определите Контроллер домена, который вы размещаете, аутентифицируется против:

Используйте следующую команду:

Пример выходных данных:

Линия, которая запускает "DC": будет название Контроллера домена и линии, которая запускает "Адрес": будет IP-адрес.

Шаг 2: Использование RDP входит в Контроллер домена, определенный в Шаге 1

Шаг 3: Перейдите **к Пуску> Средства администрирования> Просмотр событий**.

Шаг 4: Выполните развертку к**> Security Windows Logs**.

Шаг 5: Фильтр для IP-адреса вашей рабочей станции путем нажатия Filter Current Log, нажатия вкладки XML и нажатия редактирует запрос.

Шаг 6: Введите следующий запрос XML, заменив вашим IP-адресом <ip address>

Шаг 7: Щелкните **по Событию Входа в систему** и щелкните по вкладке **Details**.

Пример вывода:

Выполните эти те же шаги после регистрации на пути RDP, и вы заметите получение другого события входа в систему (Идентификатор события 4624) с тем же IP-адресом как показано следующей линией от данных в XML события входа в систему от исходного входа в систему:

Решение

Для смягчения этой проблемы при использовании Клиента User Agent 2.1 или выше можно исключить любые учетные записи, что вы будете
используйте прежде всего для RDP в Конфигурации Клиента User Agent.

Шаг 1: Войдите в хост клиента User Agent.

Шаг 2: Запустите интерфейс пользователя Клиента User Agent.

Шаг 3: Щелкните по вкладке **Excluded Usernames**.

Шаг 4: Введите все имена пользователей, которые вы хотите исключить.

Шаг 5: **Нажмите Save.**

Пользователи ввели в этом списке, не генерируют события входа в систему на Центре управления FireSIGHT и не быть
привязанный к IP-адресам.