Содержание

Вопрос

Почему действительно торгует от Windows 7 / клиенты Vista показывают рабочую станцию вместо пользователя в журналах доступа?

Среда

Microsoft Windows 7, Microsoft Windows Vista, Cisco Web Security Appliance (все версии), Суррогатный Тип: IP-адрес

Признаки

Определенные строки журнала в журналах доступа показывают компьютерное имя машины вместо DOMAIN\USER.

Microsoft ввела новую характеристику в Windows 7 и Windows Vista, вызванный "Индикатор состояния Сетевого подключения" (NCSI), который обнаруживается как немного значка земного шара, который появляется по значку сетевого интерфейса в панели задач. Сразу после входа в систему, эта функция попытается запросить данные из Интернета, чтобы знать, существует ли интернет-соединение.

Существуют известные неполадки с NCSI, куда он передаст учетные данные машины вместо учетных данных пользователя, когда будет требоваться аутентификация NTLM.

Так как NCSI, скорее всего, отправит первый запрос от ПК до WSA, никакой заместитель еще не существует и новое на основе IP, заместитель с именем машины вместо названия реального пользователя создан. Этот заместитель используется для каждого запроса от исходного IP - адреса до суррогатных таймаутов, и пользователь должен пройти повторную проверку подлинности, на этот раз с реальными учетными данными.

Так как имя машины является по всей вероятности не участником первоначально намеченной AD группы, все запросы не инициируют корректный Доступ/Политику расшифровки, иногда приводящий к заблокированному запросу.

Для получения дополнительной информации относительно NCSI, см. следующую [статью Microsoft KB](#).

См. инструкции ниже для обхождения проблемы:

1. Запустите Редактор реестра путем поиска "regedit" из меню задач. Необходимо щелкнуть правой кнопкой мыши и выбрать "Run as Administrator".

2. Перейдите к: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet

3. Под интернет-ключом дважды нажмите "EnableActiveProbing", и затем в данных Значения, введите:0.
4. Нажмите кнопку OK.

5. Перезапустите компьютер.

Эти изменения могут быть выдвинуты всем клиентам как Объект глобальной политики (GPO) с помощью Контроллера домена.

Обходной путь на WSA

Создайте Идентичность для NCSI и освободите его от аутентификации на основе URL или его Клиента User Agent.

Известные URL те, к который Подключения NCSI

ncsi.glbdns.microsoft.com
newncsi.glbdns.microsoft.com
www.msftncsi.com

Клиент User Agent NCSI

Microsoft NCSI