ЦЕНТРАЛИЗОВАННЫЙ УДАЛЕННЫЙ ДОСТУП БЕЗ ПРОБЛЕМ

ИНТЕГРАЦИЯ CISCO ISE С РЕШЕНИЯМИ С-ТЕРРА ШЛЮЗ И С-ТЕРРА КЛИЕНТ

Алина СИДОРОВА
инженер отдела технических решений защиты информации АМТ-ГРУП

В современном мире деятельность организаций становится более динамичной, и для повышения эффективности и гибкости работы сотрудников многие наши клиенты применяют технологии удаленного решения корпоративных задач. Традиционно удаленный доступ к корпоративной сети реализуется на основе решений, обеспечивающих построение VPN. Существует достаточно большое количество VPN-клиентов — каждый со своими плюсами и минусами.

Зачастую использовать произвольное решение по предоставлению удаленного доступа невозможно, так как при обработке в информационной системе информации, подлежащей обязательной защите в соответствии с законодательством (например, персональные данные), необходимо использовать сертифицированные средства защиты, прошедшие процедуру оценки соответствия регуляторами — ФСБ России и/или ФСТЭК России.

Также во многих организациях используются решения по контролю физических подключений к ЛВС, позволяющие реализовать функции идентификации и аутентификации пользователей по протоколу IEEE802.1x с помощью внутренней базы учетных записей или службы каталогов Microsoft Active Directory, при этом проблема состоит в том, что аутентификация при подключении по 802.1x и по VPN зачастую осуществляется независимо, что существенно снижает информативность журналов доступа и затрудняет расследование инцидентов и устранение неполадок.

В связи с этим у администраторов сети возникают вопросы о том, как одновременно обеспечить:

- выполнение требований российского законодательства по защите персональных данных при организации подключений удаленного доступа;
- централизованный контроль доступа к ресурсам сети удаленных пользователей;
- централизованный контроль физических подключений к ЛВС.

ТЕХНИЧЕСКИЕ РЕШЕНИЯ

Во многих организациях используется многофункциональное решение по реализации в корпоративной ИТ-инфраструктуре средств аутентификации и авторизации пользователей — система контроля доступа к сети Cisco Identity Services Engine (Cisco ISE).

В свою очередь, одним из решений, позволяющим реализовывать VPN-туннель, по которому передается зашифрованный с применением ГОСТ-алгоритмов трафик, являются ПАК С-Терра Шлюз и ПО С-Терра Клиент, традиционно используемые для соответствия требованиям законодательства РФ по защите персональных данных.

Решить задачу обеспечения удаленного доступа сотрудников с соблюдением всех вышеописанных требований позволяет интеграция С-Терра Шлюз и С-Терра Клиент версии 4.2, в которой появилась возможность аутентификации пользователей по доменному логину и паролю на RADIUS-сервере, с Cisco ISE версии 2.3, которые выступает в качестве данного сервера.

При этом использование доменной учетной записи при аутентификации позволяет организовать более строгую аутентификацию. Преимущество заключается в том, что даже если злоумышленник каким-либо образом получит доступ к компьютеру пользователя, то для входа в сеть ему необходимо ввести дополнительно аутентификационные данные. Также при утере устройства, с которого осуществлялся удаленный доступ, становится возможным не только отзыв сертификата пользователя, но и блокировка доменной УЗ.

Система контроля доступа Cisco ISE, которая выступает в качестве RADIUS-сервера, позволяет осуществлять интеграцию со службой каталогов Microsoft Active Directory, благодаря чему пользователь может использовать свою доменную учетную запись при подключении к сети.

ОДНИМ ИЗ РЕШЕНИЙ, ПОЗВОЛЯЮЩИМ РЕАЛИЗОВЫВАТЬ VPN-ТУННЕЛЬ, ПО КОТОРОМУ ПЕРЕДАЕТСЯ ЗАШИФРОВАННЫЙ С ПРИМЕНЕНИЕМ ГОСТ-АЛГОРИТМОВ ТРАФИК, ЯВЛЯЮТСЯ ПАК С-ТЕРРА ШЛЮЗ И ПО С-ТЕРРА КЛИЕНТ

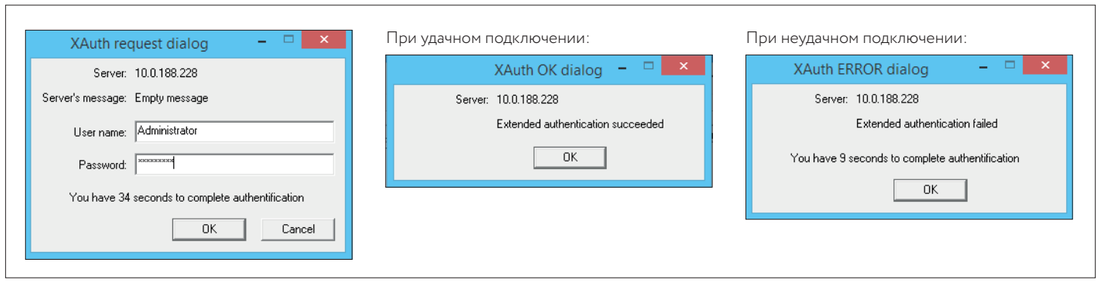


Рисунок 1. Окно запроса аутентификационных данных

ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ

Тестирование описанных выше решений проводилось в лаборатории АМТ-ГРУП. Для этого использовались С-Терра Шлюз и С-Терра Клиент версии 4.2, Cisco ISE версии 2.3 и служба каталогов Microsoft Active Directory.

Были произведены настройки по взаимодействию шлюза с RADIUS-сервером и использование XAuth. При построении IKE-сессии от клиента до шлюза на клиенте выводится окно «XAuth request dialog» (рис. 1). Введенные в окне данные передаются на RADIUS-сервер для аутентификации. При удачной аутентификации происходит построение IKE и IPsec туннелей между клиентом и шлюзом. При неудачной аутентификации будет выдаваться окно «XAuth ERROR dialog» с сообщением «Extended authentication failed», а также окно для повторной аутентификации.

Как только пользователь успешно проходит процедуры аутентификации и авторизации и получает доступ в сеть, на Cisco ISE появляется полная информация об этом пользователе, включающая IP-адрес пользователя и его учётную запись. В случае неудачной процедуры аутентификации и авторизации в журнале Cisco ISE появляется запись о неудачной попытке доступа к сети (рис. 2).

При просмотре детальной информации о подключении можно убедиться, что пользователь подключился к сети через С-Терра Шлюз, взаимодействие с которым настроено на сервере Cisco ISE (рис. 3).

Для выполнения данной задачи достаточно базовой лицензии Cisco ISE (Base).

При просмотре информации о подключении на С-Терра Шлюз дополни-

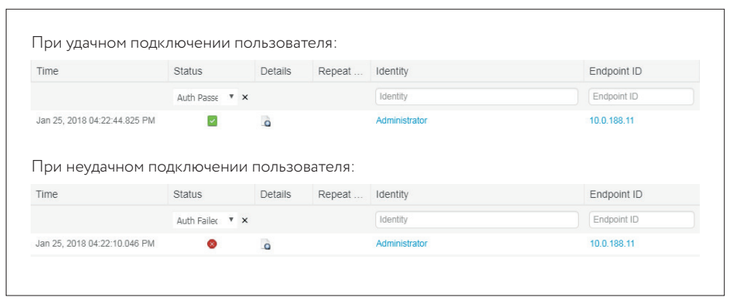


Рисунок 2. Radius live log

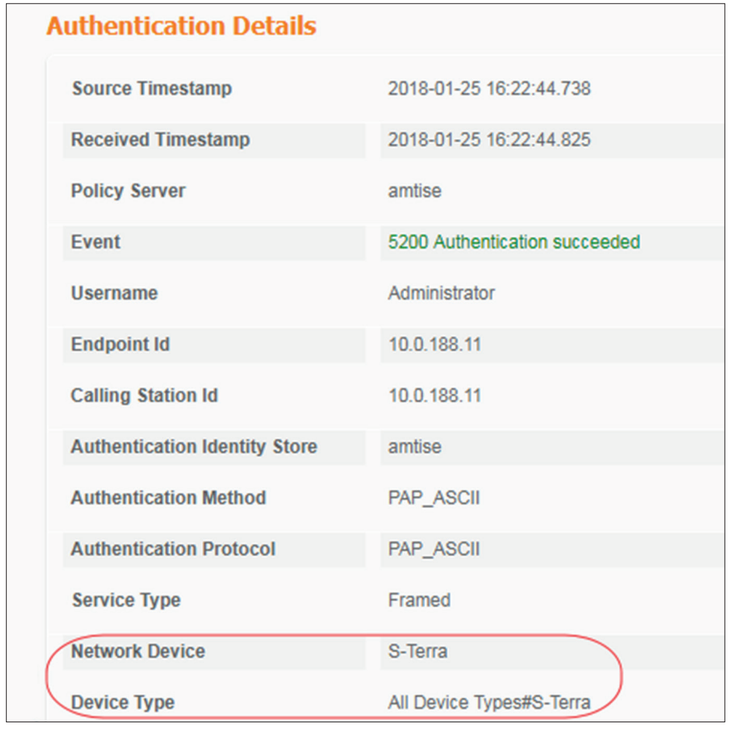


Рисунок 3. Детальный просмотр Radius live log

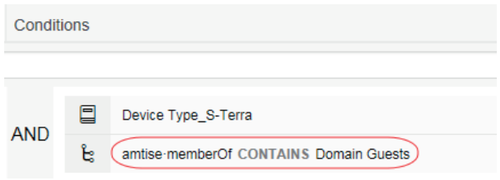
```
root@sterragate:~# sa_mgr show -detail
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connection id: 7
    cookies: 9710726B2A450753.D0DC273CCF7383A5
    local  peer (addr/port): 10.0.188.228/500
    remote peer (addr/port): 10.0.188.11/500
    IKECFG address: 10.0.1.1

    local identity (DN): CN=Certificate of gate
    remote identity (DN): CN=Certificate of client
    IKERule name: IKERule:CMAP:1:DMAP:1
    auth: gost signature + xauth (client as initiator)
    mode: main
```

Рисунок 4. Информация о подключении на С-Терра Шлюз

Указание группы AD в условии применения профиля авторизации:



Radius live log при неудачном подключении пользователя, не состоящего в группе Domain Guest:

Status	Details	Repeat...	Identity	Endpoint ID	Authorization Profiles
Auth Failed					
			Administrator	10.0.188.11	DenyAccess

Атрибуты пользователя, не состоящего в группе Domain Guest:

memberOf	CN=Group Policy Creator Owners,CN=Users,DC=sblcise,DC=com
memberOf	CN=Domain Admins,
memberOf	CN=Enterprise Admins,
memberOf	CN=Schema Admins,
memberOf	CN=Administrators,CN=Builtin,

Рисунок 5

Radius live log при удачном подключении пользователя, состоящего в группе Domain Guest:

Status	Details	Repeat...	Identity	Endpoint ID	Authorization Profiles
Auth Passed					
			iivanov	10.0.188.15	PermitAccess_S-Terra

Атрибуты пользователя, состоящего в группе Domain Guest:

memberOf	CN=Domain Guests,CN=Users,DC=sblcise,DC=com
RADIUS Username	iivanov

Рисунок 6

тельно отображается метод аутентификации XAuth (рис. 4).

При этом при подключении удаленных пользователей к сети С-Терра Шлюз и С-Терра Клиент имеется возможность применения профилей авторизации на основе принадлежности к определенной группе в AD.

В данном случае используется проверка атрибута memberOf и указание условия принадлежности к выбранной группе в политики авторизации.

Например, при указании группы Domain Guest в политике авторизации (рис. 5), пользователь, не состоящий в данной группе, доступа к сети не получит, если для него не создана отдельная политика для подключения.

Пользователь, который состоит, в указанной группе, получит доступ к сети на основе указанного профиля авторизации (рис. 6).

Дополнительно возможно создание учетной записи на сервере Cisco ISE и применение профилей авторизации на основе группы пользователя, в которую помещена учетная запись, а также настройка таких атрибутов, как IP-адрес, выдаваемый по IKECFG, IP-адреса DNS-сервера и DNS-суффикса.

Для выдачи IP-адреса с помощью сервера Cisco ISE необходимо использовать атрибут Radius: Framed-IP-Address = <IP> (рис. 7), где IP- — адрес, выдаваемый удаленному пользователю. При этом на С-Терра Шлюз пул адресов в крипто-карте не указывается.

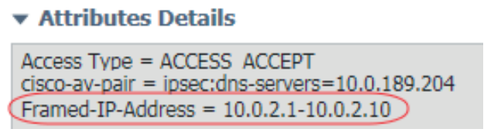
Для определения адреса DNS-сервера с помощью сервера Cisco ISE указывается дополнительный атрибут Cisco-av-pair = «ipsec: dns-servers=<IP1>», где IP1 адрес DNS-сервера (рис. 8).

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ КОНТРОЛЯ

Вышесказанное демонстрирует, что интеграция решений по контролю доступа с решением по предоставлению удаленного доступа предоставляет возможность настройки параметров удаленных пользователей в зависимости от атрибутов, определяемых при аутентификации.

Становится возможным применение тонких настроек для конкретных пользователей и групп пользователей, под-

Атрибут, настроенный в профиле авторизации, для выдачи адреса по IKECFG:



Адрес, выданный пользователю, при подключении через С-Терра Клиент:

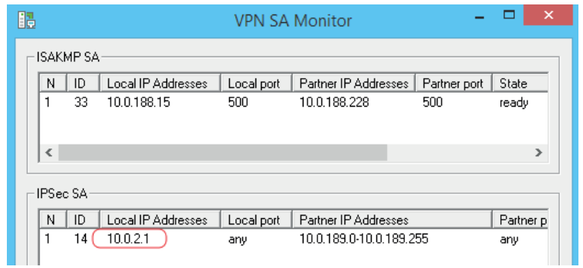
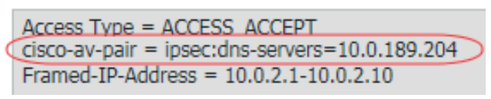


Рисунок 7

Атрибут, настроенный в профиле авторизации, для выдачи DNS-сервера:



Адрес DNS-сервера, выданный пользователю, при подключении через С-Терра Клиент:

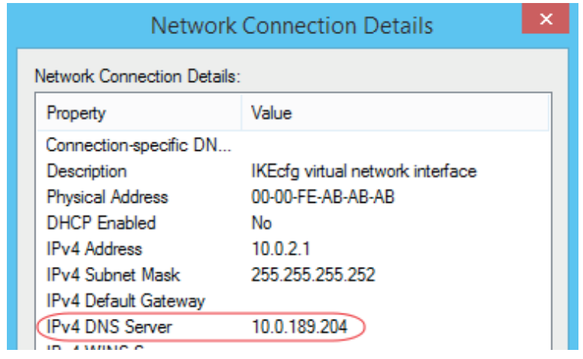


Рисунок 8

ключаемых посредством С-Терра Шлюз и С-Терра Клиент, через централизованную консоль, а также решается задача по мониторингу состояния подключений к сети в реальном времени и ретроспективе.

Полученная при VPN-подключении пользователя к сети информация может быть использована в технологии Cisco Platform Exchange Grid (pxGrid), посредством которой осуществляется взаимодействие различных продуктов Cisco, а также связь решений Cisco с системами других вендоров. Данная технология предлагает общий язык взаимодействия для обмена информации между различными системами, например, FirePOWER, ISE, WSA, Cyber Threat Defense (CTD) и т.д. Тем самым, появляется возможность использовать результаты профилирования Cisco ISE, например, в правилах доступа межсетевых экранов производства компаний Cisco, Check Point и др.

Помимо pxGrid Cisco ISE позволяет реализовать архитектуру Cisco TrustSec. Cisco TrustSec позволяет разграничивать доступ в сети по меткам, называемым Security Group Tags (SGT). Метка назначается как результат авторизации сессии оконечного подключившегося устройства, уникально его идентифицирует и переносится через всю сеть вместе с трафиком оконечного устройства. Тегирование дает возможность каждому устройству, поддерживающему работу с SGT, на пути следования пакета видеть, принимать решение по фильтрации и логировать события о прохождении данного трафика.

* * *

Таким образом, возможность совместного использования решений Cisco ISE и С-Терра Шлюз и С-Терра Клиент позволяет не только повысить уровень защиты сети при подключении удаленных пользователей к внутренним ресурсам и снизить риски связанные с безопасностью информации, но и соответствовать требованиям российского законодательства по защите персональных данных в части организации VPN для подключения к сети удаленных пользователей, снизить трудозатраты на инвентаризацию используемых конечных устройств, отправлять информацию о подключении удаленных пользователей в систему управления информацией и событиями о безопасности (SIEM), а также помогает отслеживать и расследовать инциденты информационной безопасности.