Настройка прокси-сервера аутентификации

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Как реализовать проверку подлинности прокси
Профили сервера
Cisco Secure UNIX TACACS+
Windows Cisco Secure (TACACS +)
Что видно пользователю
Дополнительные сведения

Введение

Прокси-сервер аутентификации (auth-proxy), доступный начиная с версии 12.0.5. T программного межсетевого экрана Cisco IOS®, используется для аутентификации пользователей входящих и (или) исходящих соединений. Эти пользователи обычно блокируются списком доступа. Однако в случае auth-proxy пользователи вызывают браузер для прохождения межсетевого экрана и аутентификации на сервере TACACS+ или RADIUS. Сервер передает маршрутизатору дополнительные записи списка доступа, чтобы пропускать пользователей после аутентификации.

Этот документ дает пользовательские общие советы для реализации auth-proxy, предоставляет некоторые профили Cisco Secure Server для подлинного прокси и описывает то, что видит пользователь, когда используется auth-proxy.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Как реализовать проверку подлинности прокси

Выполните следующие действия:

1. Удостоверьтесь, что трафики должным образом через межсетевой экран перед настройкой auth-proxy.
2. Для минимального ущерба сети при тестировании измените существующий список доступа, чтобы отказать в доступе одному тестовому клиенту.
3. Убедитесь, что один тестовый клиент не может проходить через межсетевой экран, а другие хосты могут.
4. Включите отладку с **exec-timeout 0 0** под консольным портом или виртуальными терминалами (VTY), в то время как вы добавляете **команды auth-proxy** и тест.

Профили сервера

Наше тестирование было сделано с Cisco Secure UNIX и Windows. Если используется аутентификация RADIUS, сервер RADIUS должен поддерживать атрибуты, заданные конкретным поставщиком (атрибут 26). Далее приведены примеры указанных серверов:

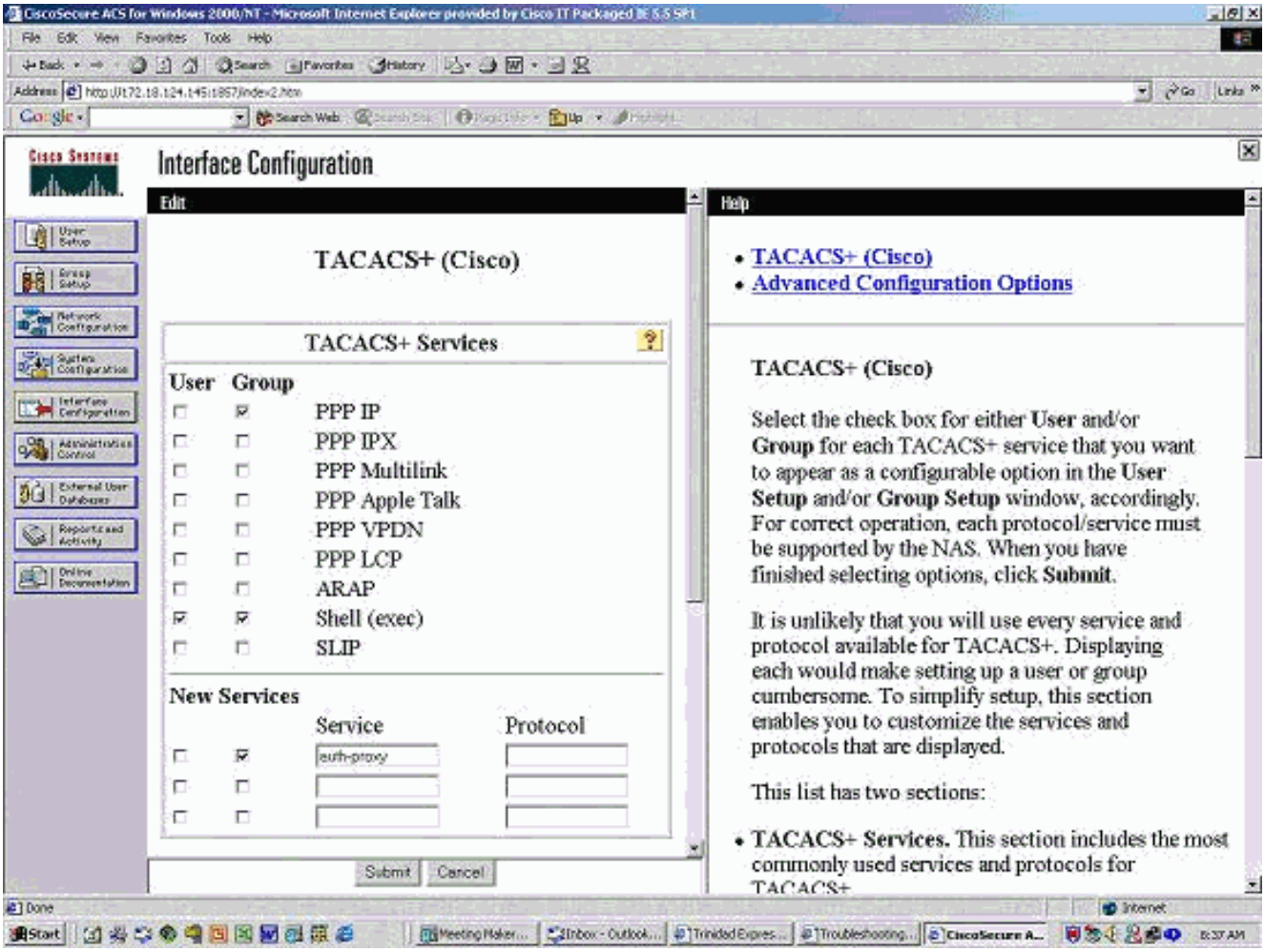
Cisco Secure UNIX TACACS+

```
# ./ViewProfile -p 9900 -u proxyonly
User Profile Information
user = proxyonly{
profile_id = 57
set server current-failed-logins = 1
profile_cycle = 2
password = clear "********"
service=auth-proxy {
set priv-lvl=15
set proxyacl#1="permit icmp any any"
set proxyacl#2="permit tcp any any"
set proxyacl#3="permit udp any any"
}
}
```

Windows Cisco Secure (TACACS +)

Придерживайтесь следующего порядка действий.

1. Введите имя пользователя и пароль (Cisco Secure или База данных Windows).
2. Для Конфигурации интерфейса выберите **TACACS +**.
3. Под New Services выберите опцию **Group** и введите **auth-proxy** в столбце Service. Не заполняйте столбец
   "Протокол".



4. Дополнительно – отображает окно для каждого сервиса – специальные атрибуты.
5. В Параметрах группы проверьте **auth-proxy** и введите эту информацию в окно:
   `priv-lvl=15 proxyacl#1=permit icmp any any proxyacl#2=permit tcp any any proxyacl#3=permit udp any any`

Cisco Secure UNIX RADIUS

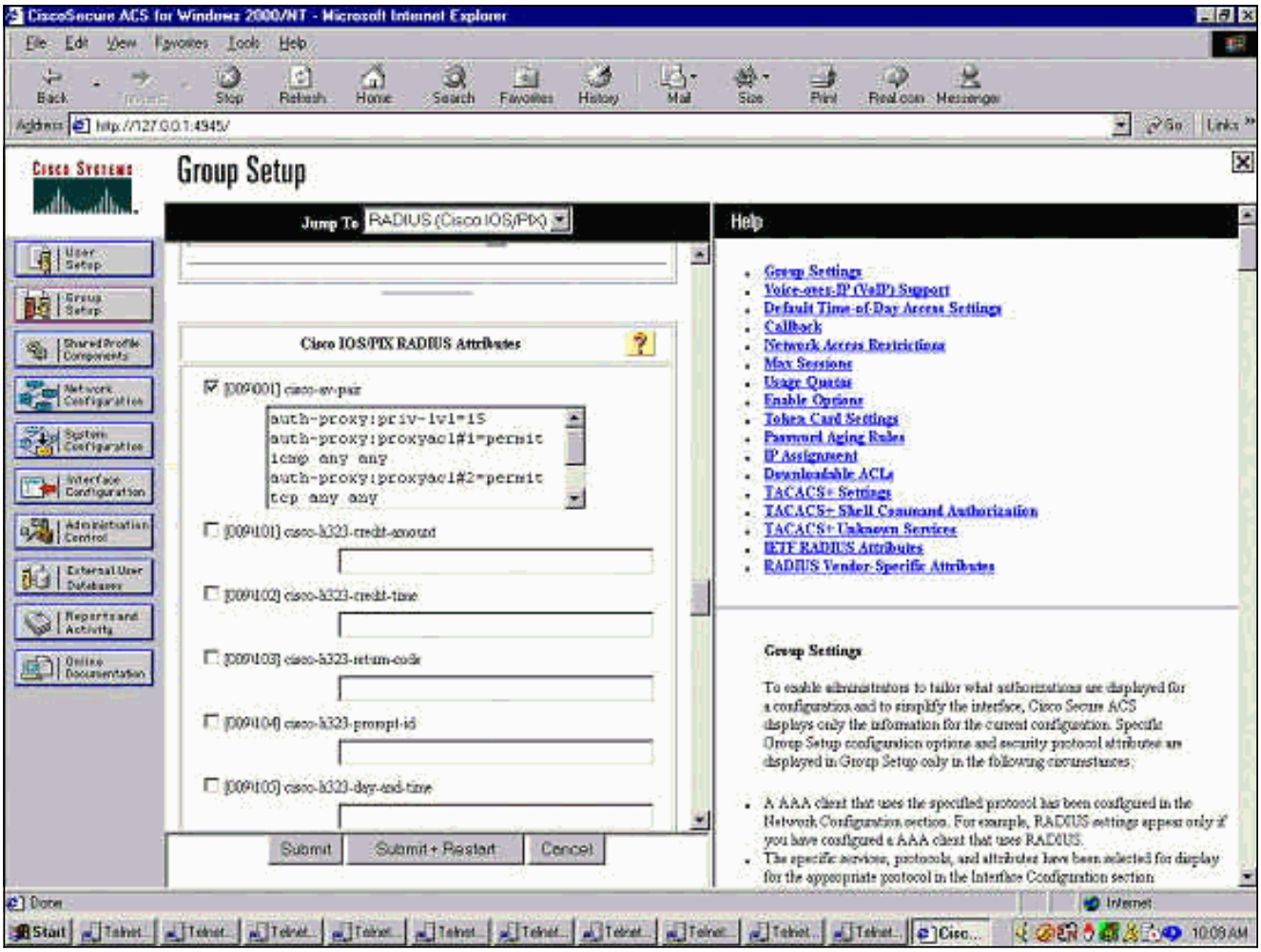
```
# ./ViewProfile -p 9900 -u proxy
User Profile Information
user = proxy{
profile_id = 58
profile_cycle = 1
radius=Cisco {
check_items= {
2="proxy"
}
reply_attributes= {
9,1="auth-proxy:priv-lvl=15"
9,1="auth-proxy:proxyacl#1=permit icmp any any"
9,1="auth-proxy:proxyacl#2=permit tcp any any"
9,1="auth-proxy:proxyacl#3=permit udp any any"
}
}

}
```

Windows Cisco Secure (RADIUS)

Придерживайтесь следующего порядка действий.

1. Конфигурация открытой сети. NAS должен быть Cisco RADIUS.
2. Если RADIUS Конфигурации интерфейса доступен, установите флажки **VSA**.
3. В Параметрах пользователя введите имя пользователя/пароль.
4. **В групповых настройках выберите опцию для пары "значение-атрибут" Cisco [009/001].** В текстовом поле под выбором введите это: **`auth-proxy:priv-lvl=15 auth-proxy:proxyacl#1=permit icmp any any auth-proxy:proxyacl#2=permit tcp any any auth-proxy:proxyacl#3=permit udp any any`** Это окно является примером этого шага.



Что видно пользователю

Пользователь пытается просмотреть что-то с другой стороны межсетевого экрана.

Окно отображается с этим сообщением:

```
Cisco <hostname> Firewall
Authentication Proxy
Username:
Password:
```

Если введены правильные имя пользователя и пароль, пользователь видит:

```
Cisco Systems
Authentication Successful!
```

Если аутентификация отказывает, сообщение:

```
Cisco Systems
Authentication Failed!
```

Дополнительные сведения

- Страница поддержки межсетевого экрана IOS
- Cisco Systems – техническая поддержка и документация