Выходные данные Authentication Proxy - No Cisco IOS Firewall or NAT Configuration

Содержание

Введение

Функция Аутентификации прокси-сервера позволяет пользователям входить к сети или обращаться к Интернету через HTTP с их определенными профилями доступа, автоматически полученными и прикладными из RADIUS или TACACS + сервер. Профили пользователя активны только тогда, когда есть активный трафик от проверенных пользователей.

Этот трафик блоков примера конфигурации от основного устройства (в 40.31.1.47) на внутренней сети ко всем устройствам в Интернете до проверки подлинности обозревателя выполнен с использованием Аутентификации прокси-сервера. Список контроля доступа (ACL), переданный от сервера (**разрешают tcp|ip|icmp любого любой**), добавляет post-authorization динамических записей к списку доступа 116, которые временно предоставляют доступ от ПК хоста до Интернета.

См. Аутентификацию прокси-сервера Настройки для получения дополнительной информации об Аутентификации прокси-сервера.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Релиз 12.2 программного обеспечения Cisco IOS (15) T
- Маршрутизатор Cisco 7206

Примечание: Команда **ip auth-proxy** была представлена в Выпуске ПО межсетевого экрана Cisco IOS 12.0.5. T.

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

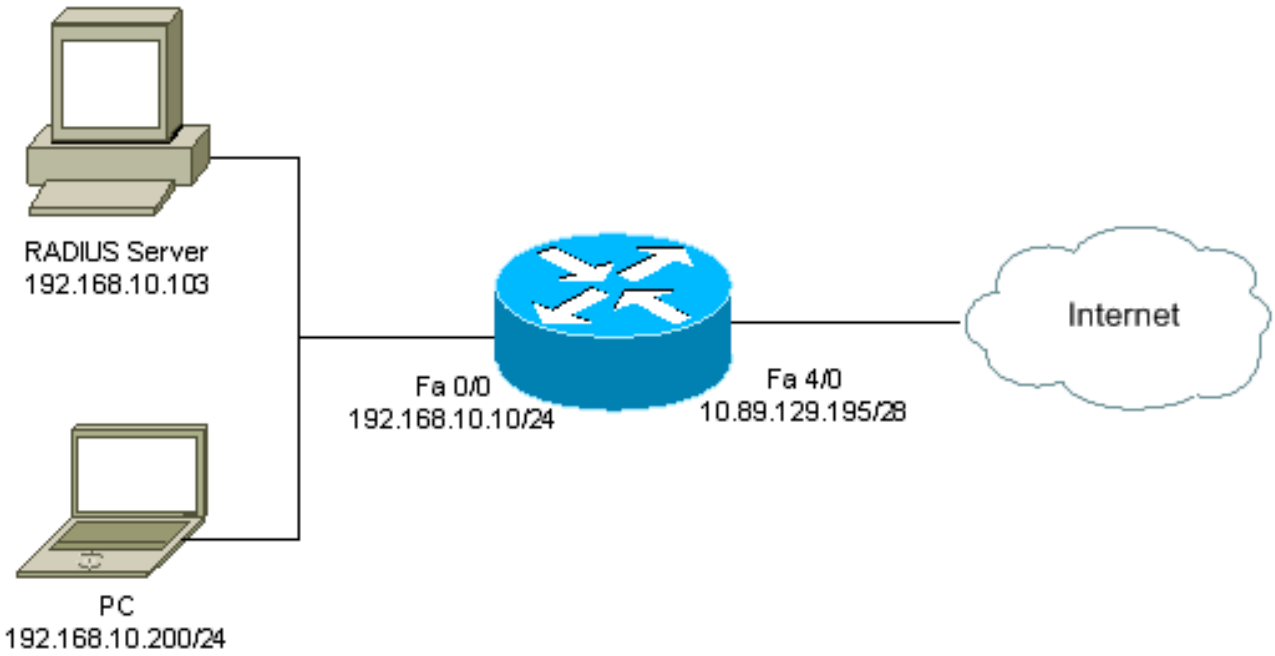
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



!--- конфигурацию

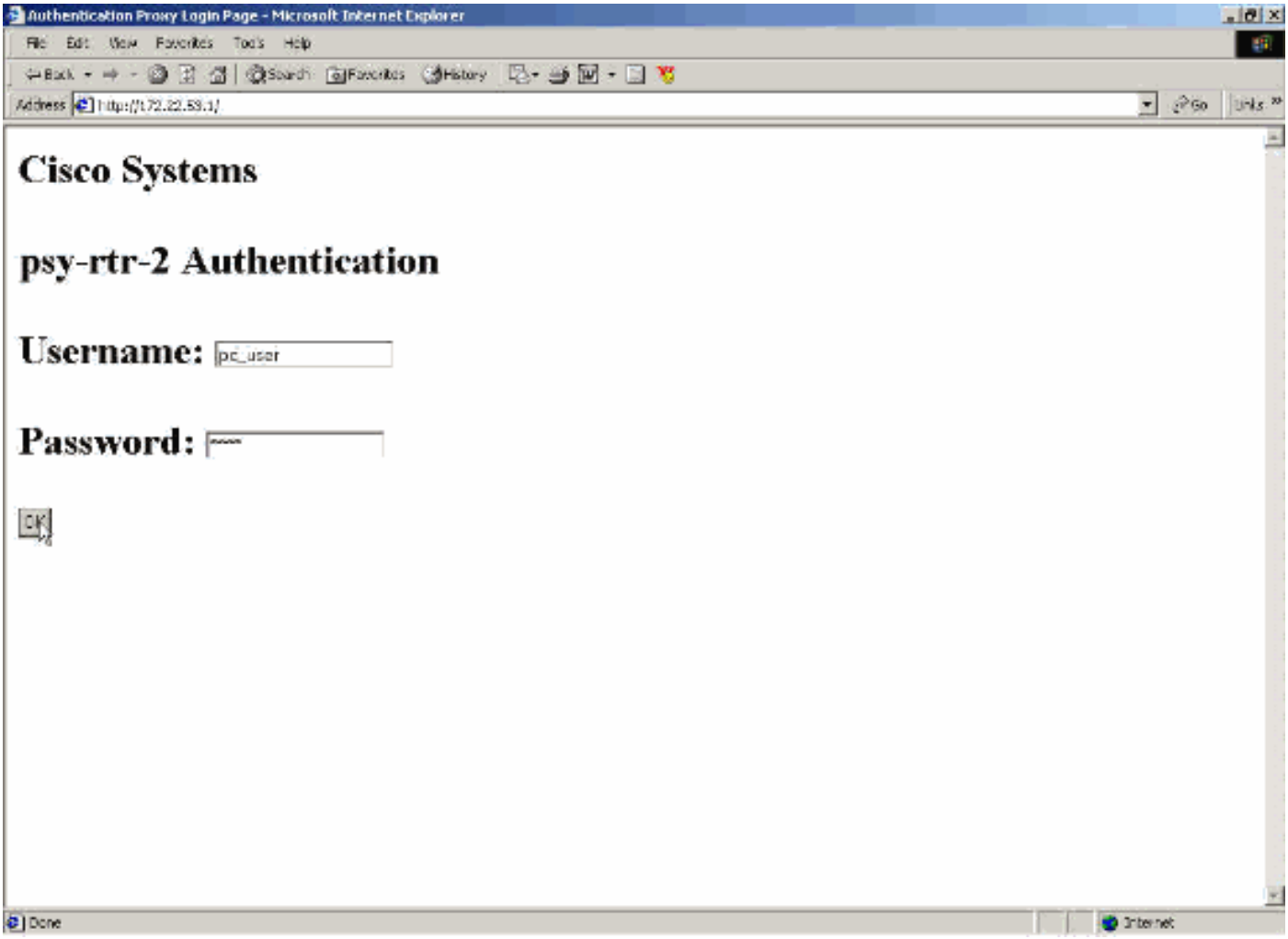
В данном документе используется следующая конфигурация:

7206 маршрутизаторов

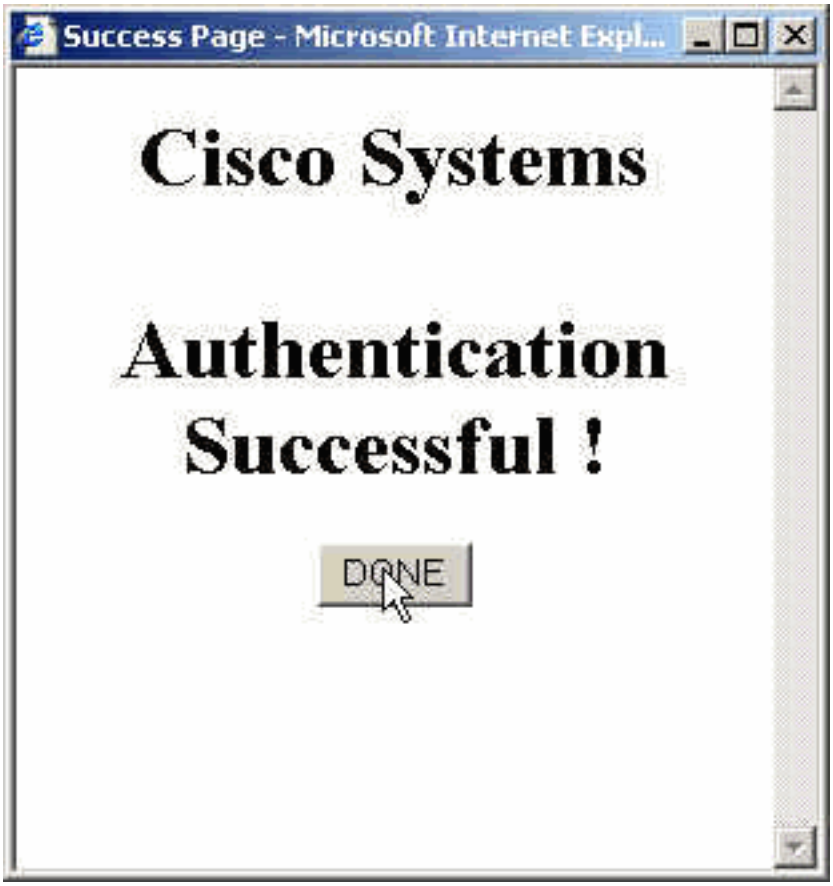
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- Enable AAA. aaa authentication login default group
radius none !--- Use RADIUS to authenticate users. aaa
authorization exec default group radius none aaa
authorization auth-proxy default group radius !---
Utilize RADIUS for auth-proxy authorization. aaa
session-id common ip subnet-zero ! ip cef ! ip auth-
proxy auth-proxy-banner !--- Displays the name of the
firewall router !--- in the Authentication Proxy login
page. ip auth-proxy auth-cache-time 10 !--- Sets the
global Authentication Proxy idle !--- timeout value in
minutes. ip auth-proxy name restrict_pc http !---
Associates connections that initiate HTTP traffic with
!--- the "restrict_pc" Authentication Proxy name. ip
audit notify log ip audit po max-events 100 ! no voice
hpi capture buffer no voice hpi capture destination !
mta receive maximum-recipients 0 ! ! interface
FastEthernet0/0 ip address 192.168.10.10 255.255.255.0
ip access-group 116 in !--- Apply access list 116 in the
inbound direction. ip auth-proxy restrict_pc !--- Apply
the Authentication Proxy list !--- "restrict_pc"
configured earlier. duplex full ! interface
FastEthernet4/0 ip address 10.89.129.195 255.255.255.240
duplex full ! ip classless ip http server !--- Enables
the HTTP server on the router. !--- The Authentication
Proxy uses the HTTP server to communicate !--- with the
client for user authentication. ip http authentication
aaa !--- Sets the HTTP server authentication method to
AAA. ! access-list 116 permit tcp host 192.168.10.200
host 192.168.10.10 eq www !--- Permit HTTP traffic (from
the PC) to the router. access-list 116 deny tcp host
192.168.10.200 any access-list 116 deny udp host
192.168.10.200 any access-list 116 deny icmp host
192.168.10.200 any !--- Deny TCP, UDP, and ICMP traffic
from the client by default. access-list 116 permit tcp
192.168.10.0 0.0.0.255 any access-list 116 permit udp
192.168.10.0 0.0.0.255 any access-list 116 permit icmp
192.168.10.0 0.0.0.255 any !--- Permit TCP, UDP, and
ICMP traffic from other !--- devices in the
192.168.10.0/24 network. ! radius-server host
192.168.10.103 auth-port 1645 acct-port 1646 key 7
<deleted> !--- Specify the IP address of the RADIUS !---
server along with the key. radius-server authorization
permit missing Service-Type call rsvp-sync ! ! line con
0 stopbits 1 line aux 0 stopbits 1 line vty 0 4 ! end
```

Аутентификация на ПК

Этот раздел предоставляет снимки экрана, полученные от ПК, которые показывают процедуру проверки подлинности. **Первый скриншот показывает окно, где пользователь вводит имя пользователя и пароль для аутентификации и нажимает OK.**



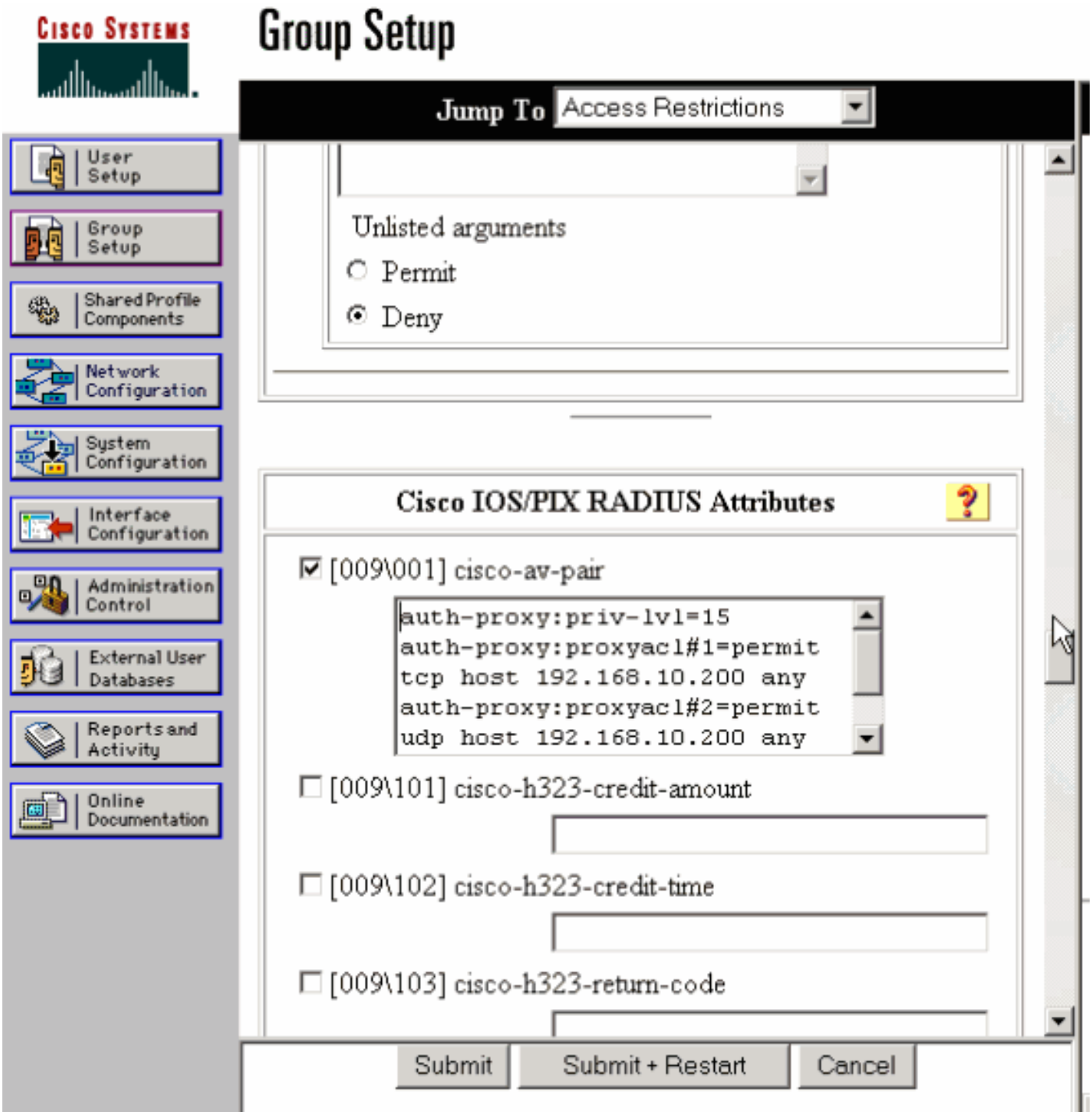
Если удостоверение подлинности успешно, то это окно появляется.



Сервер RADIUS должен быть настроен с ACL прокси, которые применены. В данном примере применены эти записи ACL. Это разрешает ПК соединяться с любым устройством.

```
permit tcp host 192.168.10.200 any
permit udp host 192.168.10.200 any
permit icmp host 192.168.10.200 any
```

Это окно ACS Cisco показывает, где ввести ACL прокси.



Примечание: См. Аутентификацию прокси-сервера Настройки для получения дополнительной информации о том, как настроить RADIUS/TACACS + сервер.

Проверка

В данном разделе содержатся сведения о проверке работы конфигурации.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show ip access-lists** — Отображает стандарт, и расширенные списки ACL, настроенные на межсетевом экране (включает динамические записи ACL). Динамические записи ACL добавлены и периодически удаляются на основе того, аутентифицируется ли

пользователь или нет.

- **кэш show ip auth-proxy** — Отображает или записи Аутентификации прокси-сервера или рабочую Конфигурацию аутентификации прокси-сервера. Ключевое слово кэша для распечатки адреса IP - адреса хоста, номера исходного порта, значения таймаута для Аутентификации прокси-сервера и состояния для соединений та Аутентификация прокси-сервера использования. Если состояние Аутентификации прокси-сервера является HTTP_ESTAB, проверка подлинности пользователя имеет успех.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Для этих команд, наряду с другими сведениями об устранении проблем, обращаются к Устранению проблем Аутентификации прокси-сервера.

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Дополнительные сведения

- Страница поддержки межсетевого экрана IOS
- Страница поддержки TACACS/TACACS+
- TACACS+ в документации по IOS
- Страница поддержки RADIUS
- RADIUS в документации по IOS
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация