Authentifizierungsproxyauthentifizierung - Ausgehend - keine Cisco IOS-Firewall oder NAT-Konfiguration

Inhalt

Einführung

Die Authentifizierungsproxyfunktion ermöglicht es Benutzern, sich über HTTP beim Netzwerk anzumelden oder auf das Internet zuzugreifen, wobei ihre spezifischen Zugriffsprofile automatisch von einem RADIUS- oder TACACS+-Server abgerufen und angewendet werden. Die Benutzerprofile sind nur aktiv, wenn der aktive Datenverkehr der authentifizierten Benutzer vorhanden ist.

Diese Beispielkonfiguration blockiert den Datenverkehr vom Hostgerät (bei 40.31.1.47) im internen Netzwerk zu allen Geräten im Internet, bis die Browser-Authentifizierung unter Verwendung des Authentifizierungsproxys erfolgt. Die vom Server übergebene Zugriffskontrollliste (ACL) (**permit tcp|ip|icmp any any**) fügt dynamische Einträge nach der Autorisierung hinzu, um auf die Liste 116 zuzugreifen, die temporär den Zugriff vom Host-PC auf das Internet ermöglichen.

Weitere Informationen zum Authentifizierungsproxy finden Sie unter Konfigurieren des Authentifizierungsproxys.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.2(15)T
- Cisco 7206-Router

Hinweis: Der Befehl **ip auth-proxy** wurde in Version 12.0.5.T der Cisco IOS Firewall-Software eingeführt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

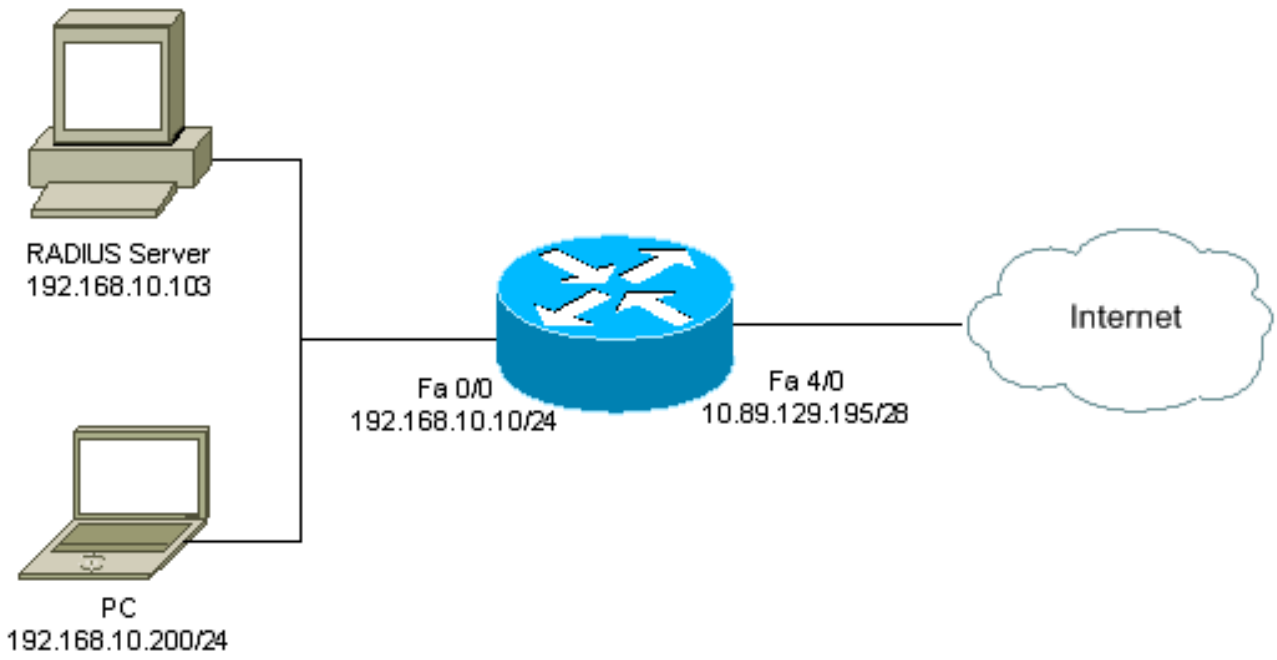
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfiguration

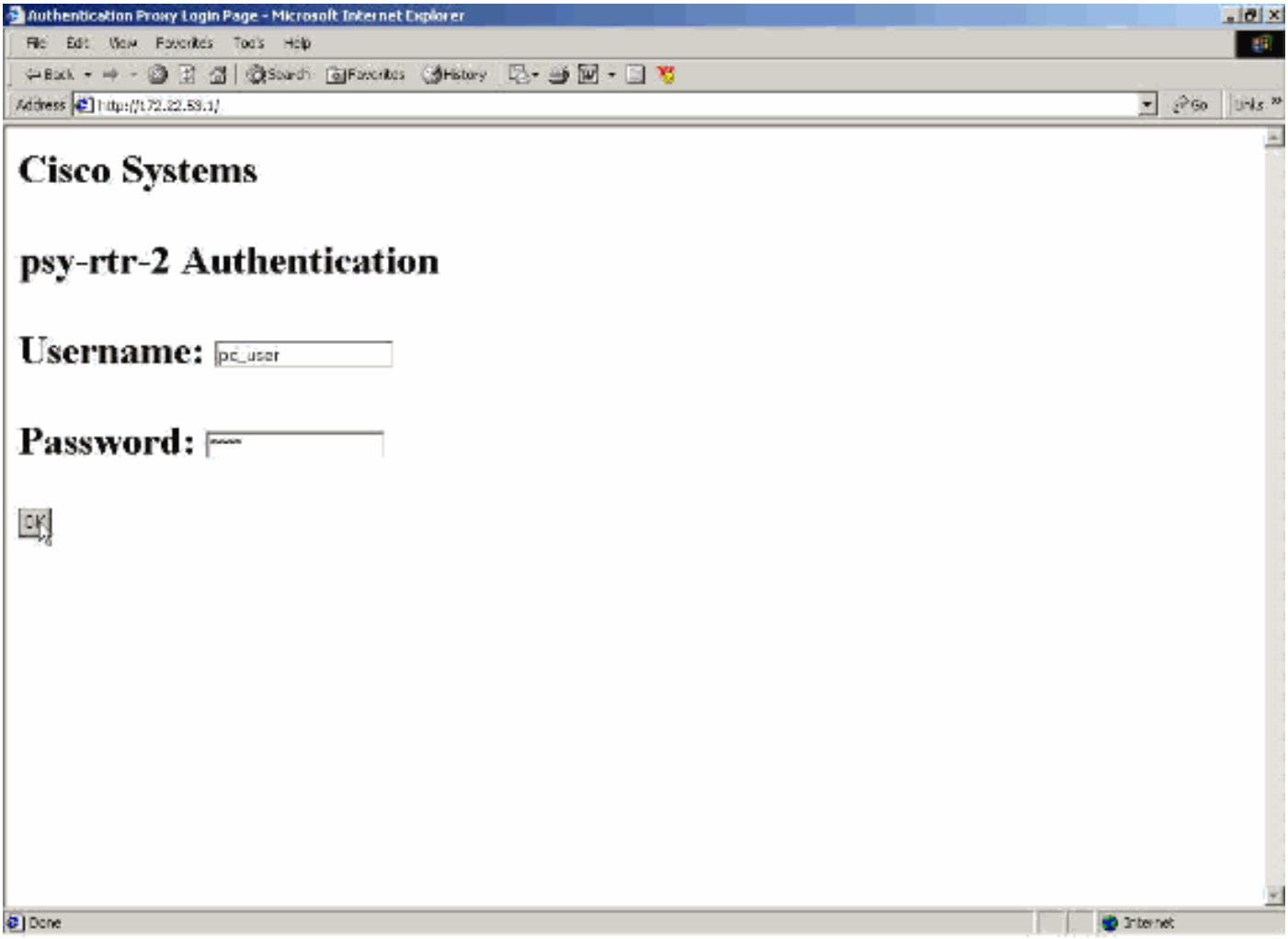
In diesem Dokument wird diese Konfiguration verwendet:

7206-Router

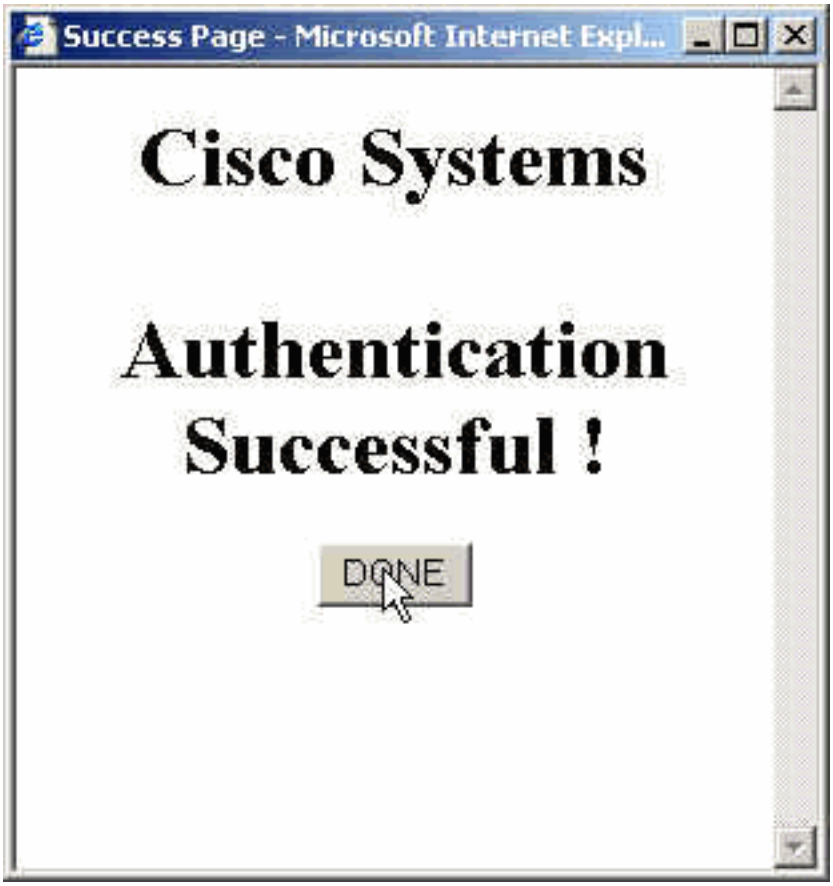
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

Authentifizierung auf dem PC

Dieser Abschnitt enthält Screenshots des PCs, die die Authentifizierungsverfahren anzeigen. Die erste Erfassung zeigt das Fenster, in dem ein Benutzer den Benutzernamen und das Kennwort für die Authentifizierung eingibt, und drückt **OK**.



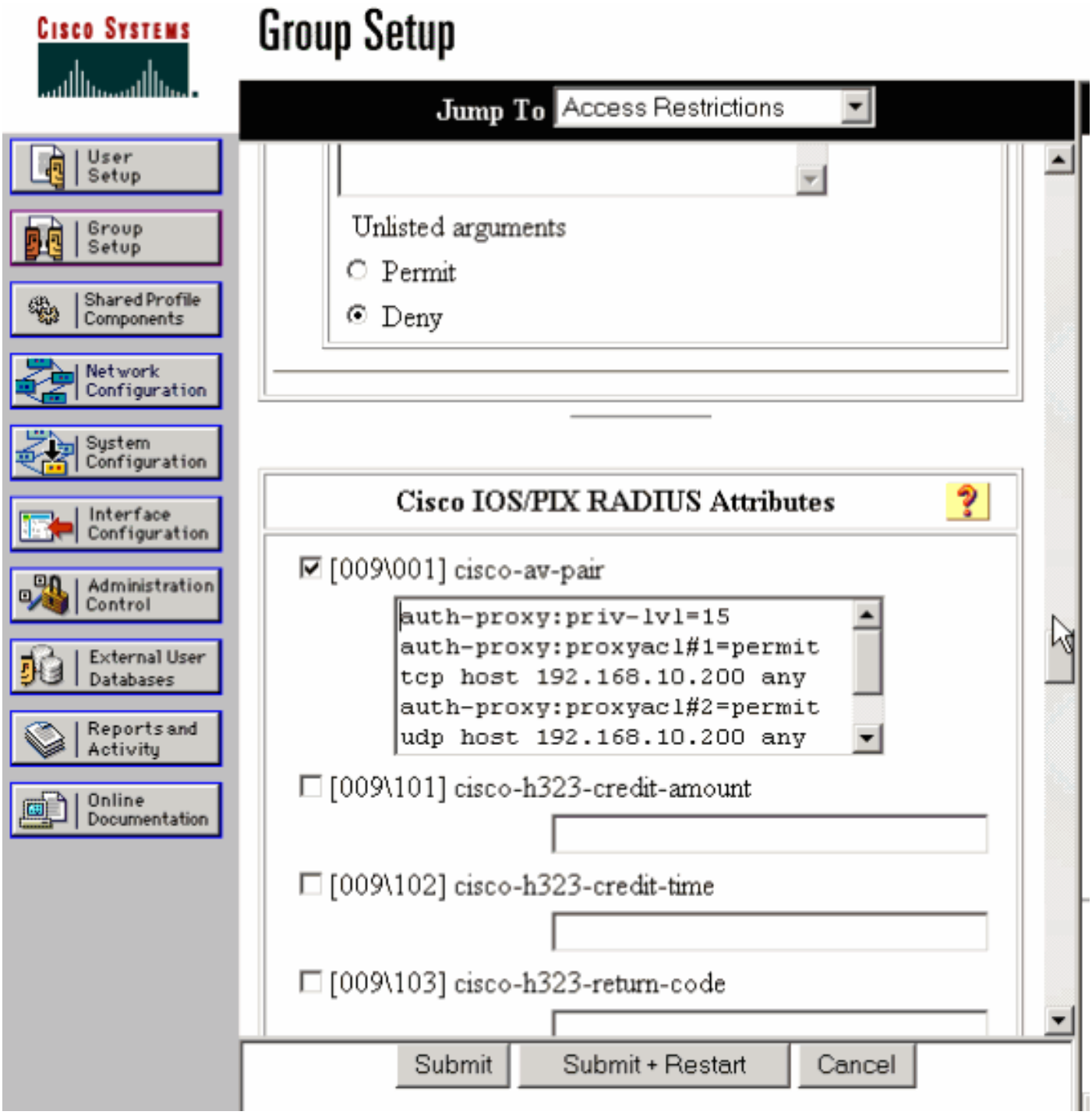
Wenn die Authentifizierung erfolgreich ist, wird dieses Fenster angezeigt.



Der RADIUS-Server muss mit den angewendeten Proxy-ACLs konfiguriert werden. In diesem Beispiel werden diese ACL-Einträge angewendet. Dadurch kann der PC eine Verbindung zu einem beliebigen Gerät herstellen.

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

Dieses Fenster von Cisco ACS zeigt an, wo die Proxy-ACLs eingegeben werden müssen.



Hinweis: Weitere Informationen zum Konfigurieren des RADIUS-/TACACS+-Servers finden Sie unter Konfigurieren des Authentifizierungsproxys.

Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show ip access-lists**: Zeigt die auf der Firewall konfigurierten Standard- und erweiterten ACLs an (einschließlich dynamischer ACL-Einträge). Die dynamischen ACL-Einträge werden regelmäßig hinzugefügt und entfernt, je nachdem, ob sich der Benutzer authentifiziert oder

nicht.

- **show ip auth-proxy cache**: Zeigt entweder die Authentifizierungsproxyeinträge oder die aktuelle Authentifizierungsproxykonfiguration an. Das Cache-Schlüsselwort zur Auflistung der Host-IP-Adresse, der Quell-Port-Nummer, des Timeout-Werts für den Authentifizierungsproxy und des Zustands für Verbindungen, die den Authentifizierungsproxy verwenden. Wenn der Authentifizierungsproxystatus HTTP_ESTAB lautet, ist die Benutzerauthentifizierung ein Erfolg.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Weitere Informationen zu diesen Befehlen sowie weitere Informationen zur Fehlerbehebung finden Sie unter Troubleshooting Authentication Proxy.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Zugehörige Informationen

- Support-Seite für IOS-Firewall
- Support-Seite für TACACS/TACACS+
- TACACS+ in der IOS-Dokumentation
- RADIUS-Support-Seite
- RADIUS in IOS-Dokumentation
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems