Uitgaande verificatie van verificatieproxy - geen Cisco IOS-firewall of NAT-configuratie

Inhoud

Inleiding

De functie Verificatieproxy stelt gebruikers in staat om in te loggen op het netwerk of via HTTP toegang te krijgen tot het internet, waarbij hun specifieke toegangsprofielen automatisch worden opgeroepen en toegepast vanaf een RADIUS- of TACACS+ server. De gebruikersprofielen zijn alleen actief wanneer er actief verkeer is van de geauthentiseerde gebruikers.

Deze voorbeeldconfiguratie blokkeert het verkeer van het host-apparaat (op 40.31.1.47) op het interne netwerk naar alle apparaten op het internet totdat browser-verificatie wordt uitgevoerd met het gebruik van Verificatieproxy. De toegangscontrolelijst (ACL) die van de server is doorgegeven (**laat tcp|ip|icmp elke willekeurige**) voegt dynamische items na autorisatie toe aan toegangslijst 116 die tijdelijk toegang van de host-pc tot het internet toestaan.

Raadpleeg Verificatieproxy configureren voor meer informatie over verificatieproxy.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS®-softwarerelease 12.2(15)T
- Cisco 7206 router

Opmerking: De **ip** opdracht **voor automatische proxy** is geïntroduceerd in Cisco IOS-softwarerelease 12.0.5.T.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

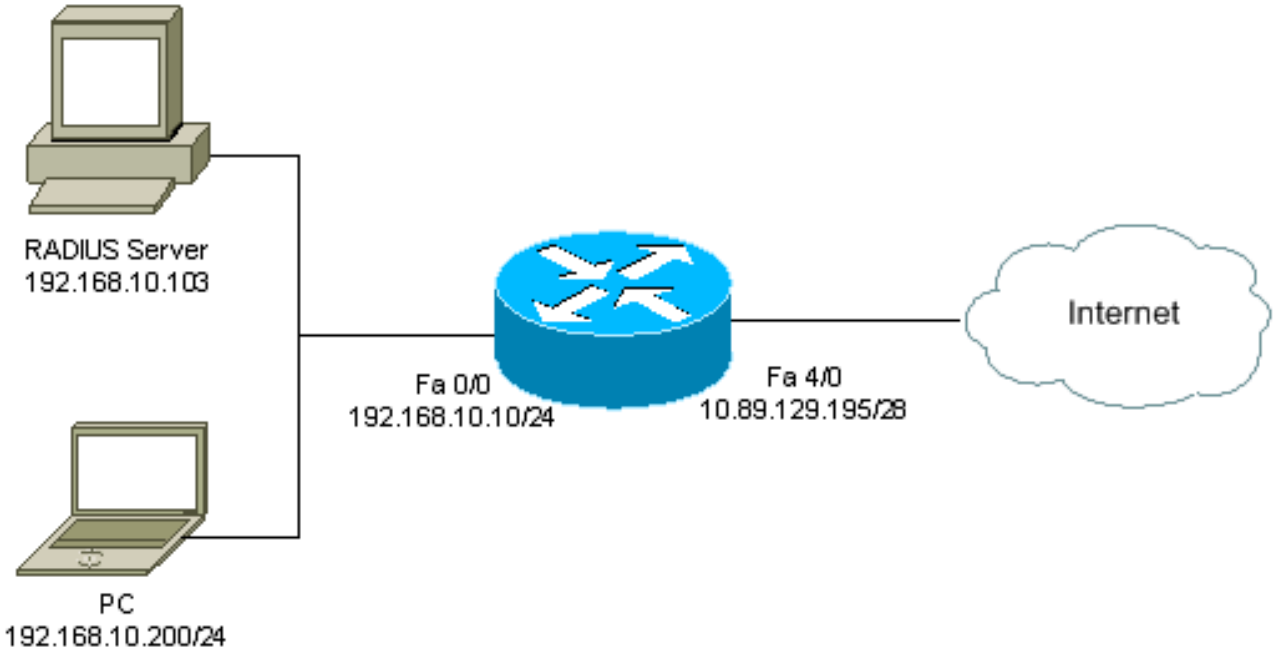
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuratie

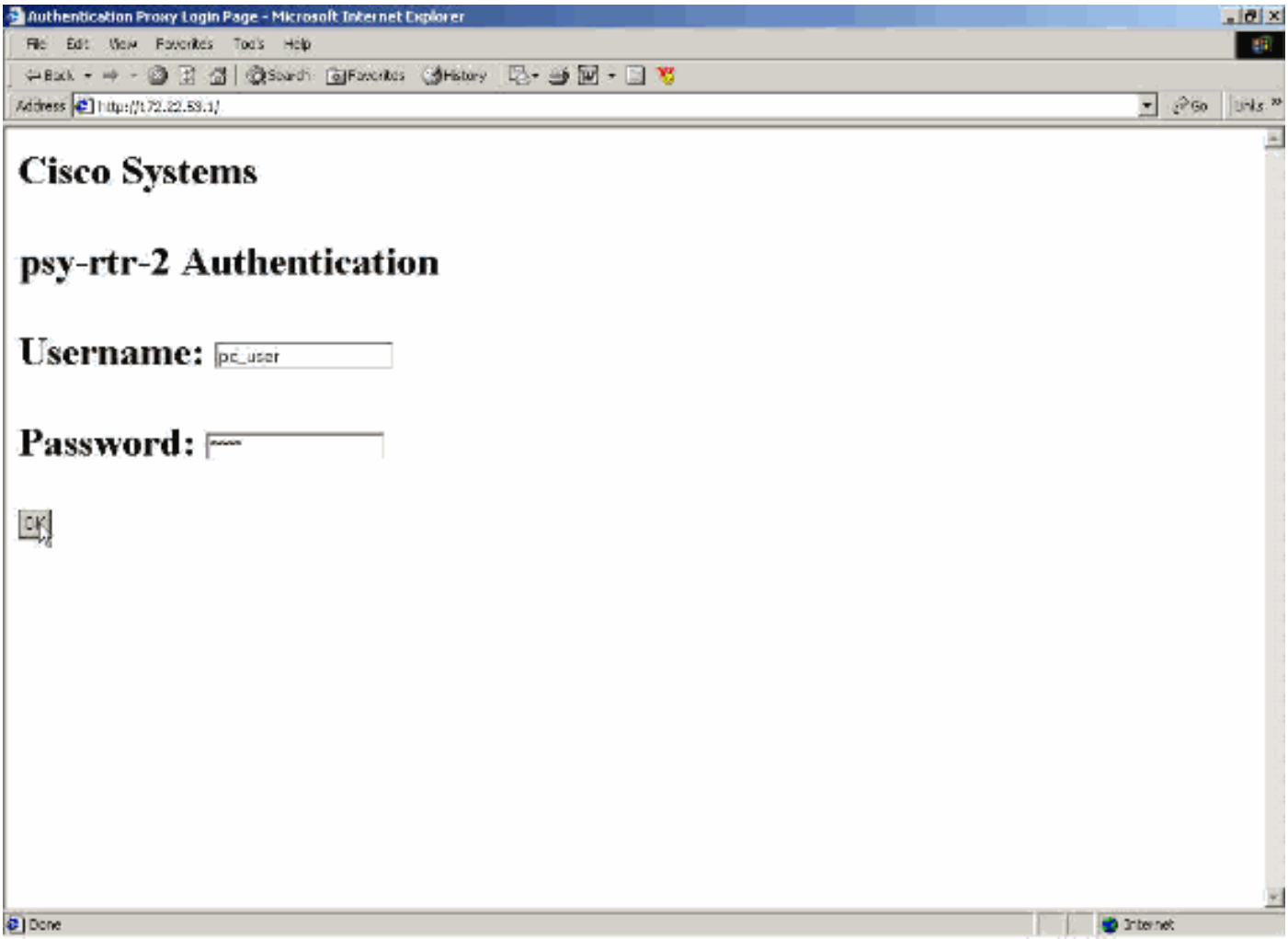
Dit document gebruikt deze configuratie:

7206 router

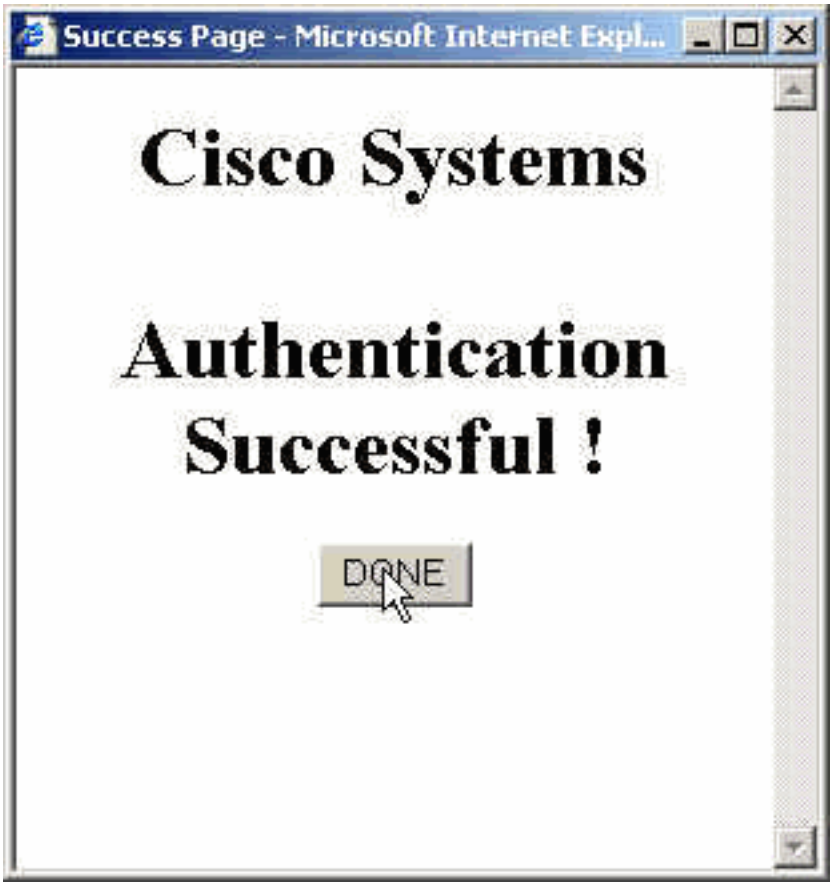
```
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname psy-rtr-2
!
logging queue-limit 100
!
username admin password 7 <deleted>
aaa new-model

 !--- 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
```

Verificatie op de PC

Deze sectie verschaft screenshot's van de PC die de authenticatieprocedure tonen. De eerste opname toont het venster waarin een gebruiker de gebruikersnaam en het wachtwoord voor verificatie invoert en op **OK** drukt.



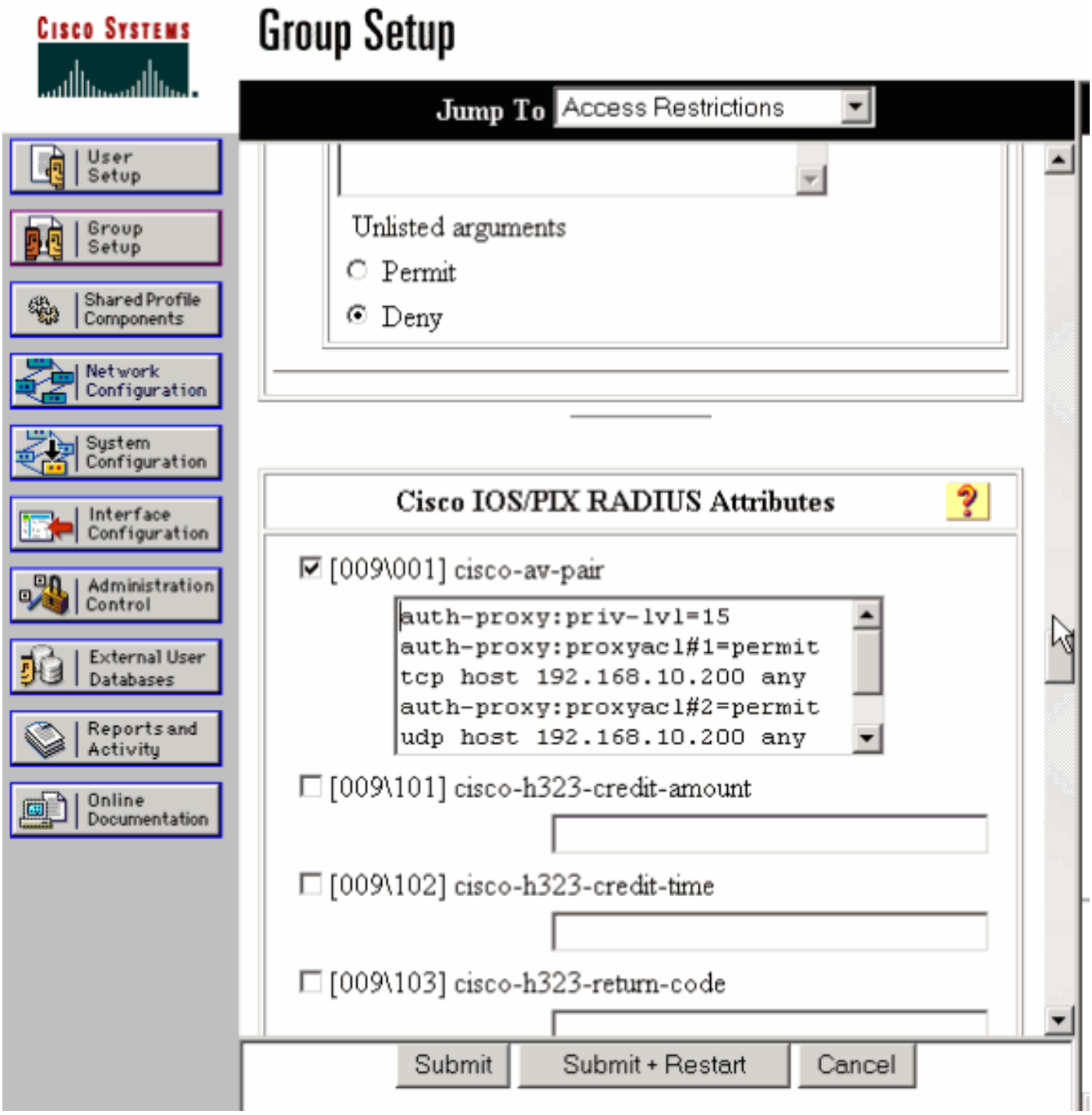
Als authenticatie succesvol is, verschijnt dit venster.



De RADIUS-server moet worden geconfigureerd met de proxy-ACL's die worden toegepast. In dit voorbeeld worden deze ACL-items toegepast. Hiermee kan de PC op elk apparaat worden aangesloten.

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

Dit venster van Cisco ACS toont waar om de volmacht ACLs in te gaan.



Opmerking: Raadpleeg Verificatieproxy voor meer informatie over het configureren van de RADIUS/TACACS+ server.

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Toon ip toegang-lijsten**-Toont de standaard en uitgebreide ACLs die in de firewall zijn ingesteld (omvat dynamische ACL-items). De dynamische ACL-items worden toegevoegd en periodiek verwijderd op basis van of de gebruiker echt is geworden.

- **Toon ip auth-proxy cache**-displays of de verificatieproxy-items of de actieve configuratie van Verificatieproxy. Het cache-trefwoord om een lijst op te geven van het IP-adres van de host, het bronpoortnummer, de tijdelijke waarde voor de verificatieproxy en de staat voor verbindingen die verificatieproxy gebruiken. Als de verificatieproxy-status HTTP_ESTAB is, is de gebruikersverificatie een succes.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Raadpleeg voor deze opdrachten, samen met andere informatie over probleemoplossing, de verificatieproxy voor probleemoplossing.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Gerelateerde informatie

- IOS-ondersteuningspagina
- Ondersteuningspagina voor TACACS/TACACS+
- TACACS+ in IOS-documentatie
- RADIUS-ondersteuningspagina
- RADIUS in IOS-documentatie
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems