アウトバウンドのプロキシ認証 - Cisco IOS Firewall や NAT のない設定

目次

概要

認証プロキシ機能を使用した場合、ユーザはネットワークにログインするか、HTTP を使用してインターネットにアクセスできます。ユーザのアクセス プロファイルは RADIUS、または TACACS+ サーバから自動的に取得され、適用されます。 そのユーザ プロファイルは、認証済みユーザからのアクティブなトラフィックが存在する間だけ有効です。

この設定例は、認証プロキシを使用してブラウザの認証が行われるまで、内部ネットワーク上の（40.31.1.47 にある）ホスト デバイスからインターネット上のすべてのデバイスへのトラフィックをブロックします。 サーバから得られたアクセス コントロール リスト（ACL）（**permit tcp|IP|icmp any any**）は、許可後、ホスト PC からインターネットへのアクセスを一時的に許可するアクセス リスト 116 にダイナミック エントリを追加します。

認証プロキシの詳細については、認証プロキシの設定（英語）を参照してください。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.2(15)T
- Cisco 7206 ルータ

注: ip auth-proxy コマンドは、Cisco IOS ファイアウォール ソフトウェア リリース 12.0.5.T で導入されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。

設定

このドキュメントでは次の設定を使用しています。

7206 ルータ

```
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
```

PC での認証

このセクションでは、PC から取得したスクリーン キャプチャを使用して、認証手順を説明します。 ユーザは、次のウィンドウで認証用のユーザ名とパスワードを入力し、[OK] をクリックします。

認証が成功すると、次のウィンドウが表示されます。

適用されるプロキシ ACL を使って、RADIUS サーバを設定する必要があります。 この例では、次の ACL エントリが適用されます。 これにより、PC がデバイスに接続できるようになります。

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

この Cisco ACS ウィンドウは、プロキシ ACL を入力する場所を示しています。

注: RADIUS/TACACS+ サーバを設定する方法の詳細については、認証プロキシの設定（英語）を参照してください。

確認

このセクションでは、設定が正常に動作しているかどうかを確認する際に役立つ情報を示しています。

Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

- **show ip access-lists**：ファイアウォールに設定された標準および拡張 ACL を表示します（ダイナミック ACL エントリを含む）。 ダイナミック ACL エントリは、ユーザが認証されるかどうかに応じて、定期的に追加および削除されます。
- **show ip auth-proxy cache**：認証プロキシ エントリまたは実行中の認証プロキシ設定を表示します。 cache キーワードを使って、ホスト IP アドレス、送信元ポート番号、認証プロキシのタイムアウト値、および認証プロキシを使用する接続の状態を一覧表示します。 認証プロキシの状態が HTTP_ESTAB の場合、ユーザ認証は成功です。

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

これらのコマンド、およびその他のトラブルシューティング情報については、認証プロキシのトラブルシューティング（英語）を参照してください。

注: debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

関連情報

- IOS ファイアウォールのサポート ページ
- TACACS/TACACS+ に関するサポートページ
- IOS での TACACS+ に関するドキュメント
- RADIUS に関するサポート ページ
- IOS での RADIUS に関するドキュメント
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems