Packet Tracer - Configure AAA Authentication on Cisco Routers

Topology

Addressing Table

<table>
<thead>
<tr>
<th>Device</th>
<th>Interface</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Default Gateway</th>
<th>Switch Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>G0/1</td>
<td>192.168.1.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S1 F0/1</td>
</tr>
<tr>
<td></td>
<td>S0/0/0 (DCE)</td>
<td>10.1.1.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R2</td>
<td>G0/0</td>
<td>192.168.2.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S2 F0/2</td>
</tr>
<tr>
<td></td>
<td>S0/0/0</td>
<td>10.1.1.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>S0/0/1 (DCE)</td>
<td>10.2.2.1</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>R3</td>
<td>G0/1</td>
<td>192.168.3.1</td>
<td>255.255.255.0</td>
<td>N/A</td>
<td>S3 F0/5</td>
</tr>
<tr>
<td></td>
<td>S0/0/1</td>
<td>10.2.2.2</td>
<td>255.255.255.252</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>TACACS+ Server</td>
<td>NIC</td>
<td>192.168.2.2</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
<td>S2 F0/6</td>
</tr>
<tr>
<td>RADIUS Server</td>
<td>NIC</td>
<td>192.168.3.2</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
<td>S3 F0/1</td>
</tr>
<tr>
<td>PC-A</td>
<td>NIC</td>
<td>192.168.1.3</td>
<td>255.255.255.0</td>
<td>192.168.1.1</td>
<td>S1 F0/2</td>
</tr>
<tr>
<td>PC-B</td>
<td>NIC</td>
<td>192.168.2.3</td>
<td>255.255.255.0</td>
<td>192.168.2.1</td>
<td>S2 F0/1</td>
</tr>
<tr>
<td>PC-C</td>
<td>NIC</td>
<td>192.168.3.3</td>
<td>255.255.255.0</td>
<td>192.168.3.1</td>
<td>S3 F0/18</td>
</tr>
</tbody>
</table>

Objectives

- Configure a local user account on R1 and configure authenticate on the console and vty lines using local AAA.
- Verify local AAA authentication from the R1 console and the PC-A client.
- Configure server-based AAA authentication using TACACS+.
- Verify server-based AAA authentication from the PC-B client.
Configure server-based AAA authentication using RADIUS.
Verify server-based AAA authentication from the PC-C client.

Background / Scenario

The network topology shows routers R1, R2 and R3. Currently, all administrative security is based on knowledge of the enable secret password. Your task is to configure and test local and server-based AAA solutions.

You will create a local user account and configure local AAA on router R1 to test the console and vty logins.

- User account: Admin1 and password admin1pa55

You will then configure router R2 to support server-based authentication using the TACACS+ protocol. The TACACS+ server has been pre-configured with the following:

- Client: R2 using the keyword tacacspa55
- User account: Admin2 and password admin2pa55

Finally, you will configure router R3 to support server-based authentication using the RADIUS protocol. The RADIUS server has been pre-configured with the following:

- Client: R3 using the keyword radiuspa55
- User account: Admin3 and password admin3pa55

The routers have also been pre-configured with the following:

- Enable secret password: ciscoenpa55
- OSPF routing protocol with MD5 authentication using password: MD5pa55

Note: The console and vty lines have not been pre-configured.

Note: IOS version 15.3 uses SCRYPT as a secure encryption hashing algorithm; however, the IOS version that is currently supported in Packet Tracer uses MD5. Always use the most secure option available on your equipment.

Part 1: Configure Local AAA Authentication for Console Access on R1

Step 1: Test connectivity.
- Ping from PC-A to PC-B.
- Ping from PC-A to PC-C.
- Ping from PC-B to PC-C.

Step 2: Configure a local username on R1.

Configure a username of Admin1 with a secret password of admin1pa55.

Step 3: Configure local AAA authentication for console access on R1.

Enable AAA on R1 and configure AAA authentication for the console login to use the local database.

Step 4: Configure the line console to use the defined AAA authentication method.

Enable AAA on R1 and configure AAA authentication for the console login to use the default method list.
Step 5: Verify the AAA authentication method.
Verify the user EXEC login using the local database.

Part 2: Configure Local AAA Authentication for vty Lines on R1

Step 1: Configure domain name and crypto key for use with SSH.
  a. Use ccnasecurity.com as the domain name on R1.
  b. Create an RSA crypto key using 1024 bits.

Step 2: Configure a named list AAA authentication method for the vty lines on R1.
Configure a named list called SSH-LOGIN to authenticate logins using local AAA.

Step 3: Configure the vty lines to use the defined AAA authentication method.
Configure the vty lines to use the named AAA method and only allow SSH for remote access.

Step 4: Verify the AAA authentication method.
Verify the SSH configuration SSH to R1 from the command prompt of PC-A.

Part 3: Configure Server-Based AAA Authentication Using TACACS+ on R2

Step 1: Configure a backup local database entry called Admin.
For backup purposes, configure a local username of Admin2 and a secret password of admin2pa55.

Step 2: Verify the TACACS+ Server configuration.
Click the TACACS+ Server. On the Services tab, click AAA. Notice that there is a Network configuration entry for R2 and a User Setup entry for Admin2.

Step 3: Configure the TACACS+ server specifics on R2.
Configure the AAA TACACS server IP address and secret key on R2.
  Note: The commands tacacs-server host and tacacs-server key are deprecated. Currently, Packet Tracer does not support the new command tacacs server.

  R2(config)# tacacs-server host 192.168.2.2
  R2(config)# tacacs-server key tacacspa55

Step 4: Configure AAA login authentication for console access on R2.
Enable AAA on R2 and configure all logins to authenticate using the AAA TACACS+ server. If it is not available, then use the local database.

Step 5: Configure the line console to use the defined AAA authentication method.
Configure AAA authentication for console login to use the default AAA authentication method.

Step 6: Verify the AAA authentication method.
Verify the user EXEC login using the AAA TACACS+ server.
Part 4: Configure Server-Based AAA Authentication Using RADIUS on R3

Step 1: Configure a backup local database entry called Admin.

For backup purposes, configure a local username of Admin3 and a secret password of admin3pa55.

Step 2: Verify the RADIUS Server configuration.

Click the RADIUS Server. On the Services tab, click AAA. Notice that there is a Network configuration entry for R3 and a User Setup entry for Admin3.

Step 3: Configure the RADIUS server specifics on R3.

Configure the AAA RADIUS server IP address and secret key on R3.

Note: The commands radius-server host and radius-server key are deprecated. Currently Packet Tracer does not support the new command radius server.

R3(config)# radius-server host 192.168.3.2
R3(config)# radius-server key radiuspa55

Step 4: Configure AAA login authentication for console access on R3.

Enable AAA on R3 and configure all logins to authenticate using the AAA RADIUS server. If it is not available, then use the local database.

Step 5: Configure the line console to use the defined AAA authentication method.

Configure AAA authentication for console login to use the default AAA authentication method.

Step 6: Verify the AAA authentication method.

Verify the user EXEC login using the AAA RADIUS server.

Step 7: Check results.

Your completion percentage should be 100%. Click Check Results to see feedback and verification of which required components have been completed.