ASA 8.0：为 WebVPN 用户配置 RADIUS 身份验证

目录

简介

本文展示如何配置思科可适应安全工具(ASA)使用远程验证拨入用户服务(RADIUS)服务器WebVPN用户的验证。在本例中的RADIUS服务器是Cisco访问控制服务器(ACS)服务器，此配置用可适应安全设备管理器的版本4.1 (ASDM)执行6.0(2)在ASA运行软件版本8.0(2)。

注意： 在本示例中，为 WebVPN 用户配置了 RADIUS 身份验证，但此配置也可用于其他类型的远程访问 VPN。只需将 AAA 服务器组分配给所需的连接配置文件（隧道组）即可，如下所示。

先决条件

- 需要进行基本 WebVPN 配置。
- Cisco ACS 必须已为用户配置用户身份验证。有关详细信息，请参阅用户管理的添加基本用户帐户部分。

配置 ACS 服务器

本部分提供有关如何在 ACS 和 ASA 上配置 RADIUS 身份验证的信息。

完成以下步骤，以将 ACS 服务器配置为与 ASA 通信。

1. 从 ACS 屏幕的左侧菜单中选择 **Network Configuration**。
2. 在“AAA Clients”下，选择 **Add Entry**。
3. 提供客户端信息：**AAA客户端主机名**-您的选择名称**AAA Client IP Address**—安全设备与 ACS

联系的地址**Shared Secret**—在 ACS 和安全设备上配置的密钥

4. 在 **Authenticate Using** 下拉列表中，选择“RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)”。
5. 单击 **Submit+Apply**。

AAA 客户端配置示例

配置安全设备

ASDM

在 ASDM 中完成以下步骤，以将 ASA 配置为与 ACS 服务器通信并对 WebVPN 客户端进行身份验证。

1. 选择 **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups**。
2. 单击“AAA Server Groups”旁边的 **Add**。
3. 在显示的窗口中，为新的 AAA 服务器组指定名称并选择 **RADIUS** 作为协议。完成后单击 **OK**。
4. 确保在顶部窗格中选择了新组，并单击下部窗格右侧的 **Add**。
5. 提供服务器信息：**Interface Name**—ASA 必须用来连接 ACS 服务器的接口**Server Name or IP address**—ASA 必须用来连接 ACS 服务器的地址**Server Secret Key**—在 ACS 服务器上为 ASA 配置的共享密钥**ASA 上的 AAA 服务器配置示例**
6. 配置了 AAA 服务器组和服务器后，导航到 Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles，以将 WebVPN 配置为使用新的 AAA 配置。**注意**：尽管本示例使用 WebVPN，但您也可以将任何远程访问连接配置文件（隧道组）设置为使用此 AAA 设置。
7. 选择要配置 AAA 的配置文件，并单击 **Edit**。
8. 在 **Authentication** 下，选择之前创建的 RADIUS 服务器组。完成后单击 **OK**。

命令行界面

完成在命令行界面(CLI)的这些步骤为了配置ASA用ACS服务器通信和验证WebVPN客户端。

```
ciscoasa#configure terminal !--- Configure the AAA Server group. ciscoasa(config)# aaa-server
RAD_SRV_GRP protocol RADIUS ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA
Server. ciscoasa(config)# aaa-server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-
server-host)# key secretkey ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel
group to use the new AAA setup. ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group RAD_SRV_GRP
```

验证

使用本部分可确认配置能否正常运行。

使用 ASDM 测试

使用“AAA Server Groups”配置屏幕上的 **Test** 按钮验证您的 RADIUS 配置。提供用户名和口令后，使用此按钮可向 ACS 服务器发送测试身份验证请求。

1. 选择 **Configuration > Remote Access VPN > AAA Setup > AAA Server Groups**。
2. 在顶部窗格中选择所需的 AAA 服务器组。

3. 在下部窗格中选择要测试的 AAA 服务器。
4. 单击下部窗格右侧的 **Test** 按钮。
5. 在显示的窗口中，单击 **Authentication** 单选按钮，并提供要用来进行测试的凭据。完成后单击 **OK**。
6. 在 ASA 与 AAA 服务器联系后，将显示成功或失败消息。

使用 CLI 测试

可以在命令行中使用 **test** 命令测试您的 AAA 设置。向 AAA 服务器发送测试请求，并在命令行中显示结果。

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password
cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

故障排除

debug radius 命令可帮助您对此方案中的身份验证问题进行故障排除。此命令将启用 RADIUS 会话调试以及 RADIUS 数据包解码。在显示的每个调试输出中，解码的第一个数据包为从 ASA 发送到 ACS 服务器的数据包。第二个数据包为来自 ACS 服务器的响应。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

如果身份验证成功，则 RADIUS 服务器会发送一条 **access-accept** 消息。

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88
alloc_rip 0xd5627ae4 new request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x88 id 52 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ------------------------------------ Raw packet data (length =
62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73 30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b
61 74 65 02 12 0e c1 28 b7 | \e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 |
.&..{,z.|.s..... 01 01 05 06 00 00 00 34 3d 06 00 00 00 05 | .......4=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E)
Radius: Vector: 187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06
7c a3 73 19 | ..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
52 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88
request_id 0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
1 !--- Second Packet. Authentication Response. RADIUS packet decode (response) ----------------
---------------------- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5
31 78 59 | .4.25../..*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.........CACS
3a 30 2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet
data..... Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032)
Radius: Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type
= 25 (0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61
36 2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4 radius: send queue empty
```

如果身份验证失败，则 ACS 服务器会发送一条 **access-reject** 消息。

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85
```

```
alloc_rip 0xd5627ae4 new request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x85 id 49 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ------------------------------------ Raw packet data (length =
62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3 a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b
61 74 65 02 12 60 eb 05 32 | ..*...kate..`..2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 |
.ix.....K..7.... 01 01 05 06 00 00 00 31 3d 06 00 00 00 05 | .......1=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E)
Radius: Vector: 88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8
4b 0d c3 37 | `..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
49 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85
request_id 0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
1 !--- Second packet. Authentication Response. RADIUS packet decode (response) ----------------
---------------------- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df
a7 bd ff | .1. p.P.9....... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | ......Rejected..
Parsed packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length =
32 (0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-
Message Radius: Length = 12 (0x0C) Radius: Value (String) = 52 65 6a 65 63 74 65 64 0a 0d |
Rejected.. rad_procpkt: REJECT RADIUS_DELETE remove_req 0xd5627ae4 session 0x85 id 49 free_rip
0xd5627ae4 radius: send queue empty
```

相关信息

- 远程用户拨入认证系统(RADIUS)
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems