Configuring RADIUS Authentication for WebVPN

So we decided that we have too many users to keep track of locally on the ASA. What are some other options? There are a variety of AAA methods we can use. My personal favorite is RADIUS attached to a Microsoft/Windows IAS (Internet Authentication Server). In Server 2008 I believe it’s called NPS (Network Policy Server) which we will hopefully cover how to configure at some point. Right now we are going to configure RADIUS with a 2003 domain controller for authentication. Another option would be LDAP but I’m not a huge fan of it; It seems to work well until it breaks, then it’s a huge pain to troubleshoot and get working again. So let’s get right into the configuration.

Notes
- Insert your relevant information between <>
- Console prompts are show in green
- Text in blue are variable names I made up, feel free to change them

Define an AAA server
ASA(config)# aaa-server WindowsIAS protocol radius
ASA(config-aaa-server-group)# aaa-server WindowsIAS host <IAS Server IP Address>
ASA(config-aaa-server-host)# key <IAS Key>

Configure RADIUS on the MS Server
The first thing we need is a server 2003 domain controller. Once we have that, we need to install IAS on top of it. IAS will do the RADIUS processing for us. In order to install IAS go to Control Panel, Add or Remove Programs, and select ‘Add/Remove Windows Components’ from the left-hand side bar. In the Windows Component Wizard scroll down to ‘Networking Services’ and double click on it.

Note: Prior to beginning this configuration I created two users in AD. One called marketing and one called sales. Additionally I have two groups configured SalesGroup and MarketingGroup. Each user is a member of their respective group. If you want to follow along with the example please add these users and groups now.
Double clicking on ‘Networking Services’ should bring up a second window. On the second window find IAS and select the check box next to it. Then press OK to close the Networking Services window. Back on the Windows Components Wizard window press NEXT to begin the installation.

Wait for the installation to complete.
Once the installation is complete press FINISH and close Add/Remove programs.

Now that IAS is installed we can begin configuring it. To open IAS locate it under Administrative Tools.
The first thing to do is to configure a new RADIUS client. In our case this client will be the ASA. To configure the client right-click on RADIUS clients and select ‘New RADIUS Client’.

On the New Radius Client window enter a name for the RADIUS client as well as the devices IP Address. Then press NEXT.
On the next screen select ‘Cisco’ from the Client-Vendor drop down and then enter the secret you configured on the ASA when you defined the AAA server. Then press FINISH.

Technically the next step here would be to configure logging. I usually don’t configure logging beyond what’s configured in the default settings. All of the requests (approved and denied) are logged in the servers system event log. That’s usually good enough for me. So let’s jump right into configuring the remote access policy for our connection. Select ‘Remote Access Policies’ from the left-hand side bar. On the right you should see the two default policies. Let’s start from scratch; right-click on each and select DELETE. Then right-click on the Remote Access Policies and select ‘New Remote Access Policy’
Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.
On the next screen select the option for ‘Setup a custom policy’ and give it a name. Keeping with our example, I’ll call this policy ‘Sales’. Then press NEXT.

On the next window press ADD to add a new policy condition
In the Select Attribute window scroll down to ‘Windows Group’ and press ADD.

After you press ADD, a new window will pop up called ‘Groups’. Click the ADD button once again and select a windows security group from Active Directory.
Press OK on the Select Groups window and OK on the Groups window to return to the New Remote Access Policy Wizard. You should now see your group listed in the Policy Conditions window as shown below. Press NEXT.
On the next screen press the EDIT PROFILE

On the Edit Dial-in Profile window select the Authentication tab and ensure that ‘Unencrypted authentication (PAP, SPAP)’ is checked.
Now select the Encryption tab and check the ‘No Encryption’ check mark. Then Press OK.

When you press OK, you will receive the following error message. Just press NO to return to the wizard.
Press Next on the wizard window

Then press FINISH to create the policy
Now that we have successfully configured RADIUS let’s test it on the ASA to ensure that it’s working correctly.

**Testing the RADIUS Configuration**

ASA# test aaa-server authentication WindowsIAS username <username> password <password>
Server IP Address or name: <IP address of RADIUS Server that you defined>
INFO: Attempting Authentication test to IP address <IP you entered> (timeout: 12 seconds)
INFO: Authentication Successful

**Checking the server's system log for IAS events**

When you perform any sort of authentication (including the test we did above) against IAS it logs an event in the server’s System log. Let’s take a brief look at a couple of events that can appear in the log and I’ll show you how easy it is to troubleshoot IAS/RADIUS issue. The below screen shot is of my system log.

As you can see there are two events from IAS. Successful RADIUS authentication requests are logged as type informational and event ID 1. Failures are logged as type warning and event ID 2. Let’s look at both of the actual events and see why the first one failed.
The failure is shown on the left. To determine the cause of the failure, I scrolled down to the ‘Reason’ part of the event. I simulated this error by checking the ‘User must change password at next logon’ attribute underneath the users AD account settings. Once I unchecked the settings and ran the test on the ASA again, I got the event on the right. The first line indicates my user was granted access. Bottom line, if you are having IAS issues, check the system log. If there aren’t any IAS events it’s most likely a misconfig on the ASA or the IAS server. If there are events, it’s usually pretty easy to determine the issue.

As I mentioned in my last post, an advantage of using RADIUS configured with a MS domain is that you get it’s password policies along with it. For instance a default domain group policy on a 2003 MS Server requires that the password uses ‘password’ complexity’. In other words it has to meet certain standards such as containing a certain number of letters, numbers, and symbols. Additionally, you get the password expiration policy which forces the user to change their password every so often. The screen shot below shows the password policies that are available in the default domain policy on a MS Server. I’m not going to dig into configuring group policies on a MS server on this blog, but I will give you piece of advice: download the ‘group policy management tool’ if you are working in server 2003.
However a problem does exist with this configuration. If you have RADIUS setup on the portal and you have some users defined in AD just for portal authentication, they might never logon to a windows PC (on the domain) to see warnings about their password expiring. At the very least, they wouldn’t have the facilities to change the password. No fear, Cisco built this functionality into the ASA. One simple command enables password management that processes all of the warnings and errors to the user at the logon prompt. Password management is a function of a tunnel group.

**Enable Password Management on the Logon page**

ASA(config)# tunnel-group <Tunnel Group Name> general-attributes
ASA(config-tunnel-general)# password-management

OR

ASA(config-tunnel-general)# password-management password-expire-in-days <Days prior to expiration you want to warn the user>

If you just enable password management by simply entering ‘password-management’, the ‘password-expire-in-days’ value is defaulted to a value of 14. If you want to warn the user on the day of expiration enter a value of 0 in the ‘password-expire-in-days’ value.

Now that we have all of this configured, let’s configure our tunnel group to use RADIUS.

**Modify your tunnel group to add the AAA server**

ASA(config)# tunnel-group <Tunnel Group name> general-attributes
ASA(config-tunnel-general)# authentication-server-group WindowsIAS

Now let’s browse externally to the ASA logon page and test it all out. I applied the AAA server to my sales tunnel group. Remember, AAA is defined per tunnel group. If you want all of your users to use RADIUS and have multiple tunnel groups you need to define RADIUS in each.
After entering the credentials and clicking ‘Login’ I was able to successfully gain access to the portal page. A quick check of the IAS server’s system log confirmed that my RADIUS request was granted access. As a last note, try out the password management feature if you enabled it. Go into AD and check the ‘User must change password at next logon’ under the sales user’s account settings. Now let’s try logging in again.

The ASA caught onto the fact that the users password was expiring in AD and is giving us the opportunity to change it now. Additionally since it’s an AD password it needs to meet all of the AD password policies. Pretty slick huh? After I entered my new password, I confirmed that it changed on the AD side by logging in to a local computer on the domain with my new credentials. In the next post we’ll be talking about pulling attributes from AD and processing them during logon.