

How to Configure Web Authentication on a ProCurve Switch



Contents

1. Introduction	2
2. Prerequisites	2
3. Network diagram	2
4. Configuring the ProCurve Switch 5400zl	2
4.1 Configure the VLANs	2
4.2 Configure access to the RADIUS server	3
4.3 Configure the ProCurve switch for Web authentication	3
5. Configuring the RADIUS server	4
5.1 Configure the policy	4
5.2 Configure IAS clients	11
6. Configuring users	12
7. Reference documents	13

1. Introduction

This document describes how to configure Web authentication using a ProCurve switch and a RADIUS server (Microsoft IAS). The switch used in this example is an HP ProCurve Switch 5400zl, but most ProCurve switches can be configured in the same manner.

2. Prerequisites

This procedure assumes you have an already configured RADIUS server (Microsoft IAS, on Windows Server 2003), and have created the necessary users and groups.

3. Network diagram

Figure 1 details the configuration referenced in this section.



Figure 1. Setup for Web authentication

Using this topology, you will configure the clients, switch, and RADIUS server to allow access to the network via Web authentication. You will use two VLANs to separate traffic between authorized and unauthorized users.

4. Configuring the ProCurve Switch 5400zl

As stated in the previous section, to keep the unauthorized and authorized traffic separate and secure, you will divide them into two separate VLANs. The first VLAN, ID=2, will be used to hold the unauthorized traffic. The second VLAN, ID=3, will be used to hold the authorized traffic.

4.1 Configure the VLANs

In order to support the authorized and unauthorized VLANs on the HP ProCurve Switch 5400zl, you need to create the VLANs and assign the uplink ports to the designated VLANs.

Connect to the 5400zl switch and enter the following commands:

```
5400zl> en
5400zl# config term
5400zl(vlan-1)# vlan 2
5400zl(vlan-2)# name "unauth"
5400zl(vlan-2)# untag all
5400zl(vlan-2)# vlan 3
5400zl(vlan-3)# name "auth"
5400zl(vlan-3)# ip addr 10.24.3.80/24
```

```
5400zl(vlan-3)# exit
5400zl(config)# ip default-gateway 10.24.3.1
5400zl(config)# exit
5400zl# write mem
```

4.2 Configure access to the RADIUS server

Now that you have created the VLANs, you need to tell the HP ProCurve Switch 5400zl how to authorize clients and how to handle client traffic. Connect to the 5400zl switch and enter the following commands to tell the switch to access a RADIUS server:

```
5400zl# config term
5400zl(config) # radius-server host 10.24.3.10 key hpsecret
5400zl(conifg) # show radius
Status and Counters - General RADIUS Information
 Deadtime(min) : 0
 Timeout(secs) : 5
 Retransmit Attempts : 3
 Global Encryption Key :
                         Auth
                                      Acct
 Server IP Addr
                        Port
                                      Port
                                                    Encryption Key
                         _____
                                       ____
                                                     _____
 10.24.3.10
                        1812
                                      1813
                                                    hpsecret
5400zl(config) # exit
5400zl# write mem
5400zl# ping 10.24.3.10
10.24.3.10 is alive, time = 25 ms
5400zl#
```

4.3 Configure the ProCurve switch for Web authentication

After the 5400zl switch knows the address of the RADIUS server, you next restrict the security on the switch and enable Web authentication. Restricting the access to the switch and specifying secure communication to it is necessary to create a secure environment.

The following steps create local usernames, set up SSL communications, and set the Web authentication parameters to the switch:

```
5400zl# config term
5400zl(config)# password manager user-name admin
New password for Manager: procurve
Please type new password for Manager: procurve
5400zl(config)# crypto key gen cert 1024
Installing new RSA key. If the key/entropy cache is
depleted, this could take up to a minute.
```

```
5400zl(config)# aaa port-access web-based a2-a4
LACP has been disabled on 'port-access' enabled port(s).
5400zl(config)# aaa port-access web-based a2-a4 auth-vid 3
5400zl(config)# aaa port-access web-based a2-a4 unauth-vid 2
5400zl(config)# aaa port-access web-based a2-a4 redirect-url http://www.hp.com/go/
procurve
5400zl(config)# aaa port-access web-based a2-a4 ssl-login
5400zl(config)# exit
5400zl(config)# exit
```

5. Configuring the RADIUS server

With the switch configured, the next step is to configure the Windows 2003 IAS RADIUS server.

5.1 Configure the policy

You first need to define a policy to allow Web authentication to work. To configure the policy:

1. In IAS, right-click Remote Access Policies and choose New Remote Access Policy. The New Remote Access Policy Wizard pops up:



New Remote Access Policy W	izard	×
	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.	
	< <u>Back</u> <u>Next</u> > Canc	el

2. Click Next. You see the Policy Configuration Method screen:

New Remote Acces	ss Policy Wizard	×
Policy Configur The wizard c	ration Method an create a typical policy, or you can create a custom policy.	ŷ
How do you w	ant to set up this policy?	
⊂ <u>U</u> se the	wizard to set up a typical policy for a common scenario	
Set up :	a custom policy	
Type a name th <u>P</u> olicy name:	hat describes this policy. Web and 802.1X	_
	Example: Authenticate all VPN connections.	
	< <u>B</u> ack <u>Next</u> >	Cancel

3. Click the button Set up a custom policy, and enter a name in the Policy name field. Then click Next. You see the Policy Conditions window:

Remote Acce	ss Policy Wizard
Policy Condition To be authe	ons enticated, connection requests must match the conditions you specify.
Specify the o	conditions that connection requests must match to be granted or denied
Policy condit	tions:
Add	Edt Bemove

Policy conditions are used to determine whether connection requests should be handled by this policy. It is best to choose something that can be easily controlled.

4. In the Policy Conditions window, click Add to see the options. You see a list of names and attributes:

Constitution that also an unstant distant but the use
specifies the phone number dialed by the usi
Specifies the phone number from which the c
Specifies the friendly name for the RADIUS c
Specifies the IP address of the RADIUS clier
Specifies the manufacturer of the RADIUS pr
Specifies the time periods and days of week
Specifies the protocol that is used.
Description not yet defined
Specifies the string that identifies the NAS th.
Specifies the IP address of the NAS where the
Specifies the type of physical port that is user
Specifies the type of service that the user ha
Specifies the tunneling protocols used.
Specifies the Windows groups that the user h

You will use Windows-Groups, since it allows you to select everyone at once and does not restrict the connection request to one device (type).

5. In the Select Attributes window, click select Windows-Groups, and click Add. You see the Groups windows, which allows you to choose which Windows Groups will be handled by this remote access policy:

Groups		<u>? ×</u>
The following groups are currently in	this condition.	
<u>G</u> roups:		
Name		
, 		
Add <u>R</u> emove		
	OK	Cancel

6. In the Groups window, no groups are selected yet, so click Add. You see the Select Groups window that allows you to enter object names:

elect Groups		?
Select this object type:		
Groups	Object Type	s
From this location:		
ProCurve.demo	Locations	
		_
Enter the object names to select (<u>examples</u>):		
Enter the object names to select (<u>examples)</u> ; domain users	Check Nam	es
Enter the object names to select (<u>examples)</u> : domain users	<u>Check Nam</u>	es

7. In the Select Groups window, type in Domain users and click Check Names. This should verify the group. By default, every user in the domain is a member of domain users.

8. After checking the name, in the Select Groups window click OK. You see the Groups window with the new group added:

Groups		?>
The following groups are currently in the	his condition.	
Name		
PROCURVE \Domain Users		
Add		
	OK	Cancel

9. After confirming that the group has been added to the Groups window, click OK. You see the Permissions window, showing the policy condition:

New Remote Access Policy Wizard	×
Permissions A remote access policy can either grant or deny access to users who match the specified conditions.	ŷ
If a connection request matches the specified conditions:	
<u>G</u> rant remote access permission	
< <u>B</u> ack <u>Next</u> >	Cancel

10. Since you will only use this one, click Next.

This determines whether connection requests are granted or denied. Since you raised the functional level of the domain, this is the only setting that determines whether or not users are authorized. If you had not raised the functional level, it would be necessary for each user to have the Remote Access Permission set to Allow access in the user properties.

Instead, choose Grant remote access permission, then click Next. You see the Profile window for this policy:

New Remote Access Policy Wizard	
Profile You can make changes to the profile for the	his policy.
A profile is a collection of settings applied t authenticated. To review or change the de	to connection requests that have been efault profile for this policy, click Edit Profile.
Edit Profile	
	< <u>B</u> ack <u>N</u> ext > Cancel

11. Next, you will edit the profile of the remote access policy so that it suits your needs. Click Edit Profile. You see the Edit Profile window:

Dial-in Profile		1
Dial-in Constraints	IP	Multilink
Authentication	Encryption	Advanced
Select the authentication me	ethods you want to allo	w for this connection.
Microsoft Encrypted A	uthentication version ;	2 (MS-CHAP ∨2)
User can chang	je password after it ha	s expired
Microsoft Encrypted A	uthentication (MS-CH/	AP)
🔽 Uger can chang	je password after it ha	s expired
Encrypted authenticat	ion (CHAP)	
✓ Unencrypted authentic	cation (PAP, SPAP)	
- Unauthenticated access-		
Allow clients to conner method.	ct without negotiating	an authentication
	OK	Cancel Apply

- 12. In the Edit Profile window, choose the Authentication tab. Make sure at least Encrypted authentication (CHAP) is checked. This means that Web authentication from the ProCurve switch will use CHAP.
- 13. You have finished configuring the profile. Click OK to return to the wizard.
- 14. This completes the New Remote Access Policy Wizard and the IAS configuration. Click Finish.

5.2 Configure IAS clients

You now need to configure the IAS server to recognize the RADIUS client and users making the requests. This means that you need to identify the ProCurve Switch 5400zl as a RADIUS client. To do this in a Windows 2003 environment, you add the switch to the IAS client table, as follows:

1. To load the IAS management console on the IAS server, go to Start > Programs > Administrative Tools > Internet Authentication Service. You see the Welcome page:



2. Right-click on RADIUS Clients and select New Client. You see the Add Client window:

d Client		
Name and Protocol Assign a name and proto	col for the client.	
Type a friendly name and	I protocol for the client.	
Friendly name:	5400Static	
Protocol:	RADIUS	

3. In the Add Client window, enter a name for the HP ProCurve 5400zl (for example, 5400Static) in the Friendly name text box and click Next. You see the Add RADIUS Client window:

Client address (IP or DNS):		
10.24.3.80 Ve		Verify
Client-Vendor:		
RADIUS Standard		
Client must always send	the signature attribute in the request	
Shared secret:		
Confirm shared secret:	ххххххх	

- 4. In the Add RADIUS Client window:
 - o Enter the IP Address or DNS Name of the HP ProCurve Switch 5400zl (for example, 10.24.3.80).
 - o Select RADIUS Standard as the Client-Vendor.
 - Enter a secret (for example, hpsecret) in the Shared secret field.
 - And make sure the check box next to Client must always send the signature attribute in the request is *not* selected.
- 5. Then click Finish to complete adding the RADIUS client.

6. Configuring users

When using Web authentication, no detailed changes or detailed configuration need to be performed on any of the clients. If you followed the instructions in "5. Configuring the RADIUS server " you have the user defined, with a remote access policy also defined.

For proper operation of the client during the authorization step, the client's Web browser proxy setting should be off. After the client has been authorized, you can reinstate the proxy setting to allow for accessing a firewall or proxy server.

7. Reference documents

This concludes the procedure for configuring Web authentication.

For further information about how to configure ProCurve switches to support security, please refer to the following links:

- For user manuals for ProCurve 3500yl-5400zl-8212zl switches: http://www.hp.com/rnd/support/manuals/3500-6200-5400-ChapterFiles.htm
- For ProCurve Switch 2610 series manuals: http://www.hp.com/rnd/support/manuals/2610.htm
- For PCM+ and IDM manuals: <u>http://www.hp.com/rnd/support/manuals/ProCurve-Manager.htm</u> <u>http://www.hp.com/rnd/support/manuals/IDM.htm</u>

For further information, please visit www.procurve.eu



© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.