Endian Proxy / Firewall

Created October 27, 2006
by Bruce A. Westbrook

Revisions:

Introduction

This document describes the step by step process of installing and configuring the Endian Firewall, Community Edition (e.g. free!), with Advanced Proxy for LDAP authentication and very granular proxy control, plus DansGuardian for URL & content filtering.

For the purposes of these procedures, we are installing Endian to be used as a content filtering server for an internal network in conjunction with another firewall. Endian will be placed between the inside network and the Internet firewall.

There is also a section detailing how to use Endian as a proxy on the internal network and routing back to the internal firewall, without any network segmentation.

Useful Websites:

Home
http://www.endian.it/en/

Install and Configure:
http://www.endian.it/fileadmin/documentation/efw-admin-guide/en/index.html

Install Endian

√		Description
	Create ISO	Go to http://www.endian.it/en/community/download/iso/ and download the ISO image for Endian Firewall. For these installation and configuration procedures we are using version 2.0 RESPIN from October 2006. Other versions may obviously have differences in their installation, configuration and use.
	Boot with CD	Once you've downloaded and burned your CD, boot with it in the PC of your choice. Your PC MUST have at least 2 NICs to install and use Endian properly (unless you plan on configuring it as a proxy ONLY on the internal network).

	Install	1. At the initial **boot** prompt, **[ENTER]** 2. Select your **Language**, **OK** 3. Partitioning explanation, **OK** 4. Set your inside **IP address** and mask for this NIC, **OK** 5. The initial installation process will complete. Remove the CD and select **OK** 6. Select your **keyboard mapping**, **OK** 7. Select your **timezone**, **OK** 8. Enter a **hostname** for your box, **OK** 9. Enter a **domain name** for your box, **OK** 10. Set a **root** password (note that you will not see typing or even see the cursor move), **OK** 11. Now set the **admin** user password, **OK** 12. Setup is now complete! Select **OK** to reboot

Configure Endian Basics

√		Description
	Login	Now that your systems is setup and running (did you hear the cool little beeps when it booted? :) you perform all of your administration from the web interface. 1. To login, open a web browser on a machine located on the inside interface's network and go to https://endian_ip_address:10443 2. You will be prompted about the SSL certificate since it's a self-signed cert. Accept it permanently (varies depending on your browser). 3. The Endian interface will come up. Click Connect. The authentication is the username **admin** with the password you created during setup
	SSH	We'll probably want to run this box headless, so for advanced features and functions we'll want SSH enabled 1. Under **System**, select **SSH Access** 2. Select **Enabled** 3. Click **Save**
	Setup Outside Interface	1. Under **System**, select **Network Configuration** 2. Choose the **RED**, WAN Internet connection. We'll assume for these procedures that it's an **Ethernet Static** IP connection. Click **Next** 3. If you have more then 2 NICs, you will be prompted to choose what type of additional network zone(s) you would like. For these procedures we'll assume a **BLUE** wireless network. Click **Next** 4. Now set both your **GREEN** and **BLUE** IP addresses, network masks and choose the correct card. Your GREEN should already be correct, although verify the correct card is selected. 5. You can also change the **Hostname** and **Domain** if you're so inclined.

		6. Click **`Next`** 7. Configure your **`RED`** Internet IP information. Click **`Next`** 8. Configure your **`DNS servers`**. If you only have one DNS server, you'll need to enter the same IP address for both **`DNS 1`** and **`DNS 2`**. Click **`Next`** 9. Click **`OK, apply configuration`**
	Verify Routing	Verify the box itself can route. 1. SSH to your Endian – note that the SSH port is set to **`222`** (not 22) by default 2. Login as **`root`** 3. Ping your gateway IP address 4. Ping something on the inside by name 5. Ping something on the Internet by name If you have any networking problems, you'll obviously need to resolve these. To check things you can use basic linux commands like • **`ifconfig`** – check interface IP addresses & masks • **`route`** – check the gateway If you need to change any basic settings, like IP addresses, DNS, gateways, etc. simply go back into the **`Network Configuration`** page and make your changes. Or if you're adventurous and think you know what you're doing ☺ you can edit the **`/var/efw/ethernet/settings`** file to change IP addresses, DNS, gateway, etc.

Configure Advanced Web Proxy

√		Description
	Configure	There are a lot of settings that we can configure in the web proxy. I suggest getting yourself configured with all of them with the administrative guide, but for now, we'll configure what usually use. 1. Click the **Proxy** tab at the top of the screen 2. By default you will be on the **HTTP Advanced Web Proxy** page 3. Under **Common settings**, click **Enabled on Green** 4. If you have a Wireless zone as well, you'll want to click **Enabled on Blue** also 5. For the **Cache Administrator e-mail**, type in your email address. You don't have to do this, but if your user's get a message page from the proxy at least it won't have your boxes root email address. 6. Click to enable the **Contentfilter** 7. Under Upstream proxy, click to enable **Client IP address forwarding**. This will populate the Source IP in the content filtering logs. 8. Under **Log settings**, click to enable all four log settings. You can back this off later after you've become comfortable with your customization. 9. Under **Cache management** you may want to add domains that you don't want cached. All domains must be entered with a leading dot and be entered on separate lines, such as: **.google.com** **.cnn.com** 10. Under **Network based access contro**l, for the **Allowed subnets**, add any additional subnets on your internal network that will be allowed to use the proxy, one on each line, such as: **10.0.0.0/255.0.0.0** **172.16.0.0/255.255.224.0** **192.168.0.0/255.255.0.0** 11. The other settings you can research on your own, with the exception of the Authentication method. We'll go through the separately. 12. Click **Save and Restart**

Configure DansGuardian Content Filtering

√		Description
	Configure	1. Click the **`Proxy`** tab at the top of the screen, then select **`Content filter`** 2. Under **`Content filter (Dansguardian)`**, click to **`Enable logging`** 3. You might also consider increasing the **`Max. score for phrases`**. I found that the default of 160 blocked some news sites, such as Foxnews. **`200`** seems to be ok. 4. Click **`Save`** 5. The first time you do this it may take several minutes for the content filter to start. Wait for it and then continue. 6. Under **`Block pages which contain…`** select your content based blocking categories. 7. Click **`Save`** 8. Under **`Block pages known to have…`** select your URL based blocking categories. 9. Click **`Save`**

Backup Settings

√		Description
	Create Backup of Configuration	Now that we have our settings configured and verified, let's backup the configuration. 1. Under **`System`**, select **`Backup`** 2. You can choose to backup to a floppy or locally. For now, we'll just back up locally and then copy them off 3. Under **`Backup Configuration`**, click **`Create`** 4. You will now see a **`Backup Set`** with today's date & timestamp. 5. You will also see an **`Unencrypted`** file with an **`Export`** link next to it. Click the **`Export`** link for the **`Unencrypted`** file and save it to your workstation 6. This is the same information that would go onto the backup floppy.

Setup Browsers

√		Description
	Setup Browsers	You can now use Endian to perform content filtering. Simply configure your workstation browsers to use the proxy server using the IP address (or name if you configured a host record in your internal DNS properly) and port **`8080`**.

LDAP Authentication with Active Directory

√		Description
	Configure LDAP User in Active Directory	First, we need to configure a basic user account that will be used to query Active Directory. This is because AD doesn't allow anonymous browsing of the LDAP tree: 1. Open **Active Directory Users and Computers** 2. Create a new user named **ldap4proxy** with the following attributes: a. DO NOT put in a first name – just enter **ldap4proxy** as the last name only b. Make sure there are NO SPACES in the username or full name c. Select **User cannot change password** d. Select **Password never expires** 3. Once created, add the your ldap4proxy user to the **Everyone-1** group so it can logon. 4. Now still in **AD Users & Computers**, right-click the domain 5. Select **Delegate Control** 6. Click **Next** 7. Click **Add** and select your **ldap4proxy** user, click **OK** 8. Click **Next** 9. Select **Create a custom task to delegate** and click **Next** 10. Select **Only the following objects…** and then select **User Objects** all the way at the bottom of the list 11. Click **Next** 12. For **Permissions**, **General** will already by selected. In the Permissions box select only **Read All Properties** (note that the Property–specific permission will also then be automatically selected. Leave it as is.) 13. Click **Next** 14. Click **Finish**
	Configure AD Internet Group	We'll also want to configure a group for our Internet users. Simply go into AD and create a group called **InternetAccess** in the **C1_Users** OU. Yes, I said the **C1_Users** OU. Endian is not able to look at the group in one OU while the users are in another. So we need to put the Internet group in the same OU as the users. You also want to be sure not to put spaces in the group name to make it simple. Otherwise you'll have to escape the space with a \ in Endian.

	Configure LDAP Authentication	Now back to your browser and the Endian administrative interface: 1. Under **Proxy**, select **Proxy** and expand the **Authentication method** 2. Select **LDAP** and click **Save** 3. Expand **Authentication method** again 4. In the **Global authentication settings**: a. For **Authentication realm prompt**, enter **Corporate One Internet Access** b. Under Domains without authentication, depending on the environment, you may want to enter the sites for Windows Update. Domain names must be entered with a leading dot and one per line, such as: **.corpone.org** **.download.microsoft.com** **.windowsupdate.com** **.windowsupdate.microsoft.com** 5. In the **Common LDAP settings**: a. For Base DN, enter the following: **OU=C1_Users,DC=corpone,DC=org** b. LDAP Type should be **Active Directory** and the port should be **389** c. For the LDAP Server enter the <u>IP address</u> (not host name) of the local domain controller 6. In the **Bind DN settings**: a. Set the **Bind DN username** to the following: **CN=ldap4proxy,DC=corpone,DC=org** b. Note: If you placed the user in a sub-OU and not at the root of the domain, you'll need to include that in the DN (Distinguised Name). For instance, if you put the user in the C1_Users group, the DN username would be: **CN=ldap4proxy,OU=C1_Users,DC=corpone,DC=org** c. For the **Bind DN password** enter the ldap4proxy user password 7. In the **Group based access control**: a. For the **Required group** enter **InternetAccess** b. For **Advanced Group Selections**, choose **Enabled** 8. Click **Save and Restart**

	Configure Groups	1. Now click the **Group Management** link. If you see the error **No Connection to the ADS/LDAP Directory**, then you have something amiss in the DN sections. Otherwise, you should see a list of the CorpOne user group – which given that there is only one group in our C1_Users OU, you should only see **InternetAccess**. 2. Select **InternetAccess** and click the arrow to move it into the **Proxy Groups**. 3. Click **Save** 4. Now click the **Activated Groups** link 5. Click enabled next to **InternetAccess** 6. Click **Save and Restart** 7. Go configure a browser and test it out.

Endian with One NIC & Internal Routing

√		Description
	Overview	So, what if you'd like to use Endian as a proxy for filtering on your internal network, but you still want to route all traffic out your normal firewall? And, you want to keep Endian on your internal network without any segmentation – that is, you don't want to have to have both a GREEN (inside) NIC and a RED (outside) NIC? Well, here's the answer!
	Routing	After you have Endian installed, you'll need to make a couple changes. 1. First, add your inside gateway. At the command prompt type: **`route add –net 0.0.0.0 netmask 0.0.0.0 gw IP br0`** …where **`IP`** is the IP address of your internal router, firewall, or gateway 2. Second, configure your nameservers. **`vi /etc/resolv.conf`** Add your nameservers in the following format: **`nameserver 207.169.53.69`** **`nameserver 207.169.53.70`** 3. Check your routing/resolution by issuing the command: **`ping www.google.com`** 4. If it resolve, then add your gateway route permanently by editing the /etc/rc.d/rc.local file: **`vi /var/efw/inithooks/start.local`** Add the same route you entered at the command prompt here: **`route add –net 0.0.0.0 netmask 0.0.0.0 gw IP br0`** …where **`IP`** is the IP address of your internal 5. Reboot Endian and verify again that you can still route & resolve properly: **`ping www.cnn.com`**
	Client	Your clients will be setup the same – just point them to the Endian as their proxy on port 8080. Try one and see!

Edit Various Files

√		Description
	DansGuardian Configuration Files	Located in: **`/etc/dansguardian`** **`/var/efw/dansguardian`**
	DansGuardian Access Denied	If you want to edit the “Access Denied” page for the banned sites, edit the following file: **`/etc/dansguardian/languages/ukenglish/template.html`** After editing the page you’ll need to **`Save and Restart`** the proxy server.
	Other Error Pages	Most other error pages are located in the following location: **`/etc/havp/templates/en`**
	Squid Error Pages	The Squid error pages are located in the following location: **`/usr/share/squid/errors/English`** After editing the page you’ll need to **`Save and Restart`** the proxy server.
	Login Prompt	Want to change the **`Endian Firewall release 2`** login prompt to something else? Simply edit the **`/etc/issue`** file and change to whatever you like.