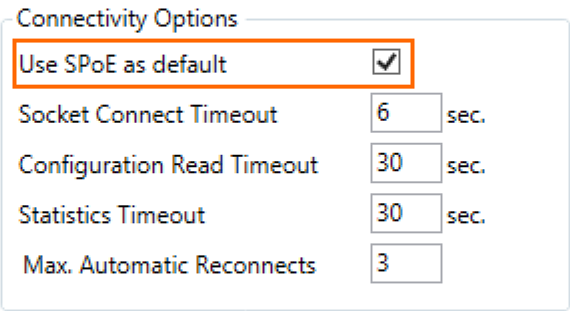
Week 1 Lab

Lab 1: Connect to the Barracuda network.

1. Download the Barracuda NG Firewall Admin 5.4
2. Launch NG Admin
3. In the upper left hand corner, click the Barracuda logo ( ) then click Settings
4. Select the check box for **SPoE as default**.



Connectivity Options

Use SPoE as default ☑

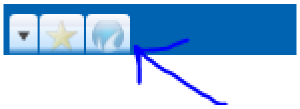
Socket Connect Timeout 6 sec.

Configuration Read Timeout 30 sec.

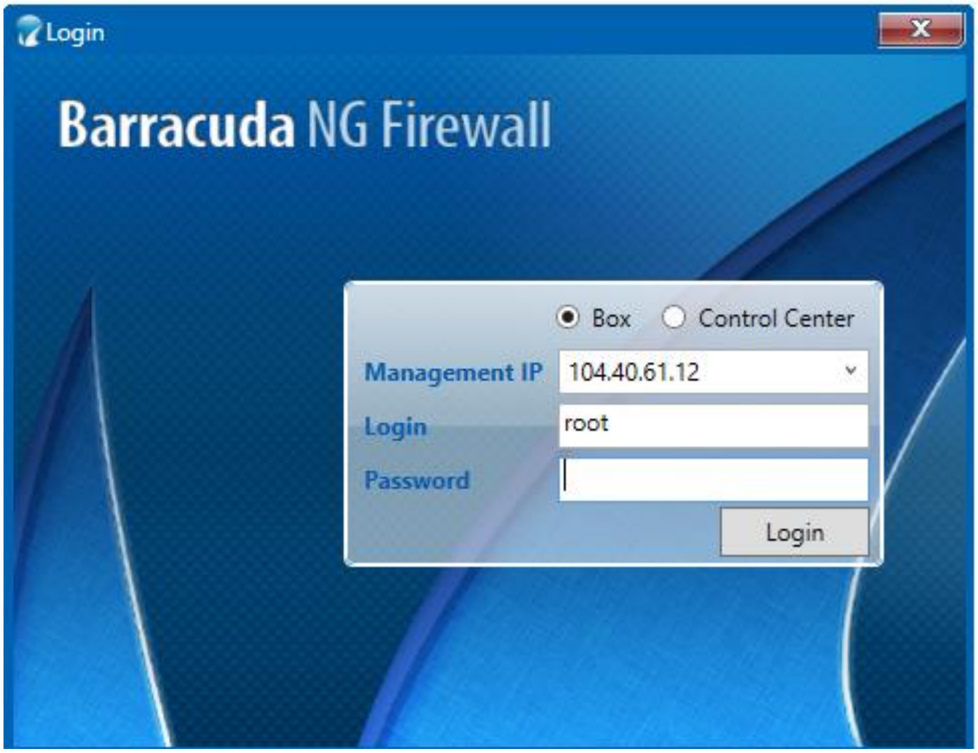
Statistics Timeout 30 sec.

Max. Automatic Reconnects 3

5. Click the new login button.



6. Enter the ip address, root as the user name, and password. You can get this information from your instructor.



● Box ○ Control Center

Management IP 104.40.61.12

Login root

Password

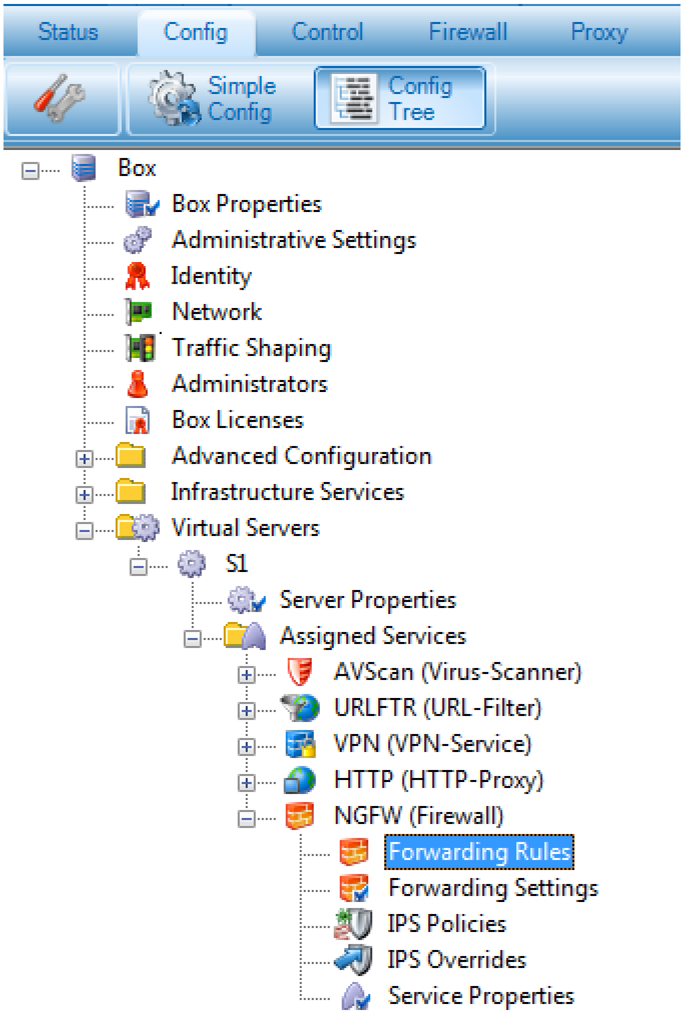
Click login. Once logged in take a screenshot, paste it in a word document, and upload.

Week 2 Lab

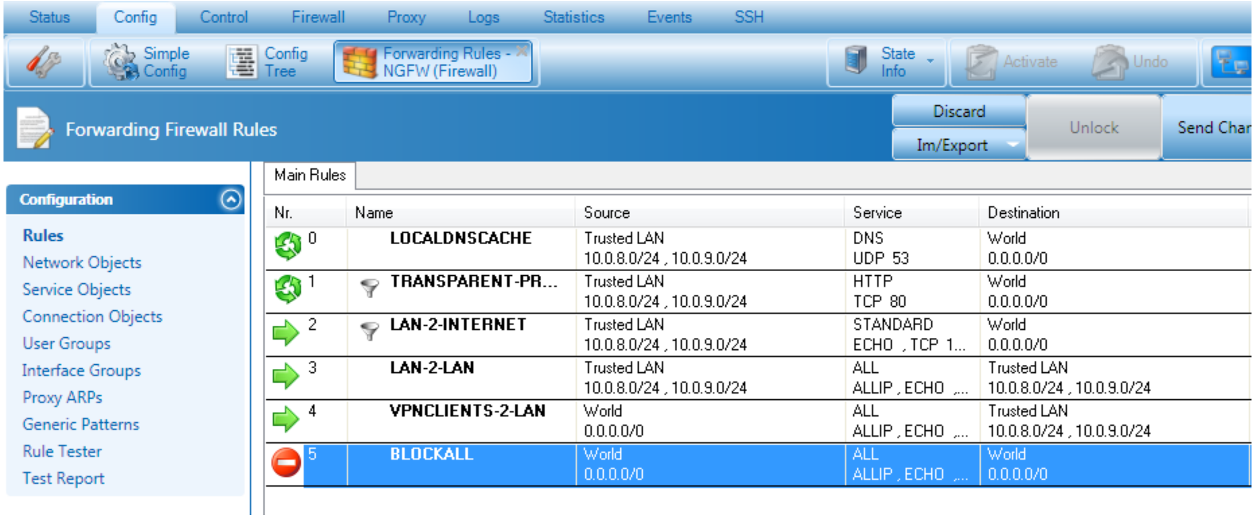
Lab 1: Allow Internet Access for Typical Users

Firewall rules are arranged in a ruleset table from top to bottom in order of precedence. The forwarding Firewall service has a rule that allows the following traffic: HTTP and HTTPS, ICMP, FTP, DNS, NTP, SMTP, POP3, IMAP, and TELNET. By default, this traffic is blocked by the BLOCKALL rule. To allow this traffic, you must drag the BLOCKALL rule to the bottom of the rule set.

1. Log into the Barracuda NG Firewall
2. Click on the config tab.
3. In the **Config Tree**, Full Config, expand the Forwarding Firewall Service and double-click **Forwarding Rules**.



4. In the upper right of the page, click **Lock**.
5. In the **Main Rules** table, select and drag the **BLOCKWALL** firewall rule to the bottom of the rule set.



Nr.	Name	Source	Service	Destination
0	LOCALDNSCACHE	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24	DNS UDP 53	World 0.0.0.0/0
1	TRANSPARENT-PR...	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24	HTTP TCP 80	World 0.0.0.0/0
2	LAN-2-INTERNET	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24	STANDARD ECHO , TCP 1...	World 0.0.0.0/0
3	LAN-2-LAN	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24	ALL ALLIP , ECHO ,...	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24
4	VPNCLIENTS-2-LAN	World 0.0.0.0/0	ALL ALLIP , ECHO ,...	Trusted LAN 10.0.8.0/24 , 10.0.9.0/24
5	BLOCKALL	World 0.0.0.0/0	ALL ALLIP , ECHO ,...	World 0.0.0.0/0

6. In the upper right of the page, click **Send Changes**, then click **Activate**. Take a screenshot of the rules showing BLOCKALL at the bottom, paste it in a word document, and upload.

Week 3 Labs

Lab 1: Create a VPN Service

1. Log into the Barracuda NG Firewall
2. In the Config Tree, navigate to and expand Assigned Services (Config > Full Config > Box > Virtual Servers > your virtual server > Assigned Services).
3. Right-click Assigned Services and select Create Service.
4. In the wizard, specify the type of service that you are creating and configure your service settings. Service name: VPN Software Module: VPN. Leave the rest as default.
5. Click Finish to close the wizard. The service is created on the Barracuda NG Firewall.
6. Take a screenshot showing the VPN service, paste to a word document, and submit.

Lab 2: Client to site VPN

To let mobile workers securely connect to corporate information resources, you can configure a client-to-site TINA VPN. To connect to this type of VPN, clients require the Barracuda VPN Client, an optionally password-protected certificate license file, and a server password.

1. Log into the Barracuda NG Firewall
2. Open the **VPN Settings** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **VPN-Service** > **VPN Settings**).
3. Click **Lock**.
4. Go back to the Config Tree tab and select SSL VPN
5. From the **Enable SSL VPN** list, select *yes*.
6. In the **Listen IP** table, add the listen IP addresses for SSL VPN. . (put in the public IP you connect to the with NG Admin. Click the **+** icon and enter the external IP address. For example, *131.77.12.129*.)

7. In the **Service Identification** section, configure the certificates and private keys that are used by the SSL VPN.
8. From the **Identification Type** list, select one of the following options: (select Generated Certificate).
    - *Self-Signed-Certificate* - Create the **Self-Signed Private Key** and the **Self-Signed Certificate**.
    - *External-Certificate* - Import the CA-signed **External Certificate** and the **External-Signed Private Key**.
    - *Generated-Certificate* - The certificate and the private key is created by the Barracuda NG Firewall.
9. Generate or import your keys and certificates.
10. Click **Send Changes** and then click **Activate**.
11. Capture a screenshot and paste in Microsoft Word.
12. When updating or changing certificates, the SSL VPN service needs to be restarted. Set **Enable SSL VPN** to **no**, click **Send Changes** and **Activate**, and enable the service again.
13. Open the **SSL-VPN** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **VPN-Service**).
14. From the **Configuration** menu in the left navigation pane, click **Authentication & Login**.
15. Click **Lock**.
16. From the **Authentication Scheme** list, select your authentication method. In this case, we will use Microsoft Active Directory.
17. In the **Corporate ID** section, enter a message in the **Login Message** field. For example, *Welcome to SSL VPN*.
18. Click **Send Changes** and then click **Activate**
19. **Take another screenshot, add it to the word document below the first screenshot. Save document and turn in.**

Week 4 Lab

Lab 1: Manage Virtual Servers and Services

To monitor and control virtual servers and services, go to the **Control > Server** page. The page is divided into the following sections:

- Server Status - Upper table that displays the status of all available servers.
- Service Status – Lower table that displays the status of available services.

1. Take a screenshot of the server status and paste in Word. Green means the server is up. Yellow means the server is blocked. Red means the server is stopped, and a Grey X means the server is disabled.
2. To start and stop a virtual server, click it in the Server Status table. (You can also right-click the server) and then select the Stop Server option. Take a screenshot and paste in the word document. Start the server back up again.
3. Upload document.

Week 5 Lab

Monitoring

1. Log into the Barracuda NG Firewall.
2. Open the **Control** page (**Config** > **Full Config** > **Box** > **Infrastructure Services, Control**).
3. Click **Lock**.
4. In the **Monitoring Parameters** section, specify the monitoring interval and which services or daemons should not be monitored:

- **Startup Poll Interval [Secs] -** The period of time that has to expire after booting or activating the network until a HA action can take place (default: *10*). This is important especially with "slow learning" NICs that need quite a time after booting/activating until the link is activated.
- **Regular Poll Interval [Secs] -** The number of seconds between HA heartbeats. This setting also specifies the reaction time for activating and deactivating routes and the server (Monitor IPs). For faster HA failovers, you can decrease the default poll interval of *5*seconds

5. **Note** -** To deactivate an unnecessary service or daemon, add it to this table. For an overview of box services, see Understanding the Barracuda NG Firewall Layers.
6. In the **HA Monitoring Parameters** section, define a translation table specifying the IP addresses to use for communication in network setups that provide a private uplink between two HA partners. In the **Translated HA IP** table, specify the following settings for each entry:

7. **Translated HA IP -** The primary management IP address of the HA unit as specified in the **Management IP** field on the **Network** page (**Config** > **Full Config** > **Box**). (Just click the + sign and then click insert).
8. In the **ICMP Gateway Monitoring Parameter** section, specify DHCP.
9. Click **OK**.
10. Click **Send Changes** and then click **Activate.**
11. Take a screenshot of the screen and paste to a word document.

Lab 2: CPU Load Monitoring

To monitor the CPU load of the Barracuda NG Firewall, you can set a limit on the number of processes that may simultaneously wait for the execution (In either inbound or outbound direction) within and average of 1, 5, and 15 minutes before the High System Load [30] and Excessive System Load [31] events are generated.

1. Log into the Barracuda NG Firewall.
2. Open the **Control** page (**Config > Full Config > Box > Infrastructure Services**).
3. From the **Configuration** menu in the left navigation pane, select **CPU Load Monitoring**.
4. Click **Lock**.
5. To collect system performance data, select yes from the **Performance Statistics** list in the **Performance** section.
6. In the following sections, specify the CPU thresholds (your choice) before event notifications are generated:

   a. **CPU-Load Warning Thresholds** – The maximum number of waiting processes that is allowed within the average of 1, 5, 15 minutes before the **High System Load [30]** event is generated.
   b. **CPU-Load Error Thresholds** – The maximum number of waiting processes that is allowed within an average of 1, 5, and 15 minutes before the **Excessive System Load [31]** event is generated. For example, if you enter 24 in the **Critical 1 Min. Average** field of the CPU Load Error Thresholds section, the **Excessive System Load [31]** event is created when there are at least 24 waiting processes within an average of 1 minutes.

7. Click Send Changes and then click **Activate**.
8. Take a screenshot and paste it in a Word document and upload.