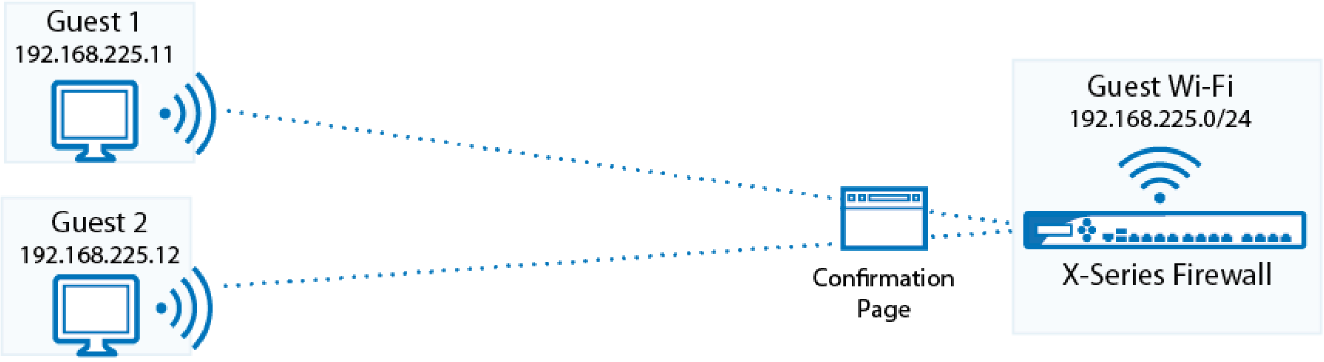
How to Set Up a Guest Access Confirmation Page

https://campus.barracuda.com/doc/11142138/

When setting up a guest network, you can configure the Barracuda NextGen Firewall X-Series to use a confirmation page that prompts guests to agree to the Terms of Service before they can access the network. A confirmation page is typically used to grant network access to anonymous users.



Before You Begin

- Ensure that the X-Series Firewall has one unused network interface (Wi-Fi, Ethernet, or virtual, e.g., ath3, p3, or p3.100).
- Identify the guest network that you want to use (e.g., 192.168.225.0/24).

Step 1. Set up the Guest Network Interface

You can use Wi-Fi or a wired network for guest access.

Configure a static network interface or a Wi-Fi interface. In the **Static Interface Configuration**, ensure that you specify the following settings:

- **Network** – The guest network (e.g., `192.168.225.0/24`).
- **Services to Allow** – Select **DNS Server**.
- **Classification** – Click **Trusted**.

Step 2. Enable the DHCP Server for the Guest Network

To automatically assign IP addresses for guests, enable a DHCP server for the guest network.

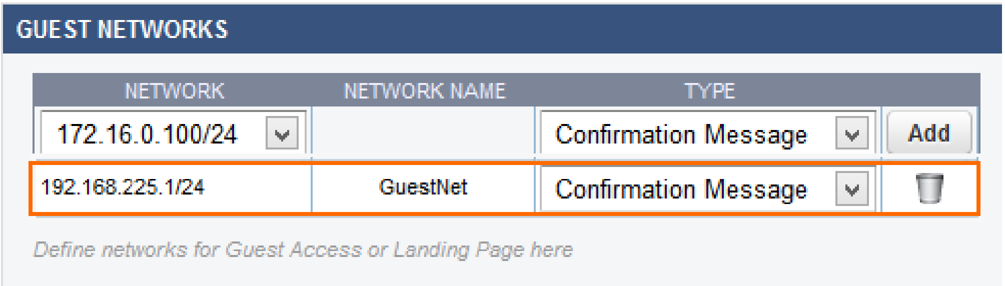
1. Go to the **NETWORK > DHCP Server** page.
2. In the **DHCP Server** section, enable the DHCP server.
3. In the **Add DHCP Server Subnet** section, configure the DHCP subnet. Ensure that you specify the following settings:
   - **Beginning IP Address** and **Ending IP Address** – The range of IP addresses to be assigned to clients. For example, if your guest network is 192.168.225.0 with a netmask 255.255.255.0, the **Beginning IP Address** is `192.168.225.1` and the **Ending IP Address** is `192.168.225.254`.
   - **DNS Servers** – The IP addresses of the DNS servers.
4. Click **Save**. The guest network subnet appears in the **DHCP Server Subnets** section.

For more information on setting up a DHCP server, see How to Configure the DHCP Server.

Step 3. Set up the Guest Network

Specify the network using the confirmation page for guest access.

1. Go to the **USERS > Guest Access** page.
2. In the **Guest Networks** section, select your guest network (e.g., `192.168.225.1/24`) from the **Network** column.
3. From the **Type** column, select **Confirmation Message**.
4. Click **Add**.
5. Click **Save**. The network then appears in the second **Network** table.


GUEST NETWORKS

NETWORK	NETWORK NAME	TYPE	
172.16.0.100/24		Confirmation Message	Add
192.168.225.1/24	GuestNet	Confirmation Message	🗑

Define networks for Guest Access or Landing Page here

Step 4. (Optional) Configure the Confirmation Page

On the **USERS > Guest Access** page, you can configure the page that is displayed to guests when they log into the network.

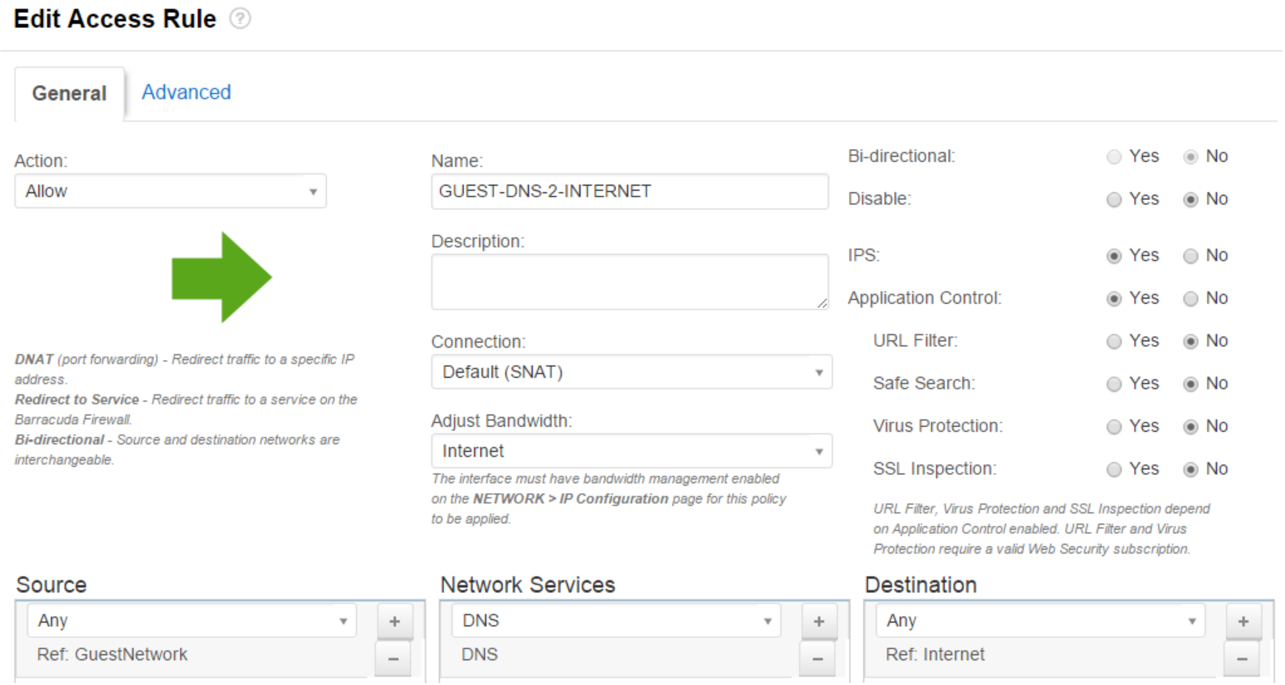
In the **Login Page Options** section, edit the **Welcome Message** and upload a **Welcome Image**. The image can be up to 1 MB and must be in JPG, GIF, or PNG format. The suggested image size is 170 x 40 pixels.

Step 5. Create a PASS Access Rule for DNS Traffic

Create an access rule to always allow DNS traffic from the guest network to the Internet.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name for the rule. E.g.: `GUEST-DNS-2-INTERNET`
4. Specify the following settings:

Action	**Connection**	**Adjust Bandwidth**	**Source**	**Network Services**	**Destination**
Allow	Default (SNAT)	Internet	Guest Network	DNS	Internet



Edit Access Rule

Action: Allow

Name: GUEST-DNS-2-INTERNET

Description:

Connection: Default (SNAT)

Adjust Bandwidth: Internet

*The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.*

Bi-directional: ○ Yes ● No

Disable: ○ Yes ● No

IPS: ● Yes ○ No

Application Control: ● Yes ○ No

URL Filter: ○ Yes ● No

Safe Search: ○ Yes ● No

Virus Protection: ○ Yes ● No

SSL Inspection: ○ Yes ● No

URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

***DNAT** (port forwarding) - Redirect traffic to a specific IP address.*
***Redirect to Service** - Redirect traffic to a service on the Barracuda Firewall.*
***Bi-directional** - Source and destination networks are interchangeable.*

Source: Any — Ref: GuestNetwork

Network Services: DNS — DNS

Destination: Any — Ref: Internet

To allow connections from the guest network to the Internet, the X-Series Firewall must perform source-based NAT. The source IP address of outgoing packets is changed from that of the client residing in the network to the WAN IP address of the X-Series Firewall, so the connection is established between the WAN IP address and the destination IP address. The destination address of reply packets belonging to this session is rewritten with the client's IP address.

5. At the bottom of the rule editor window, click **Save**.

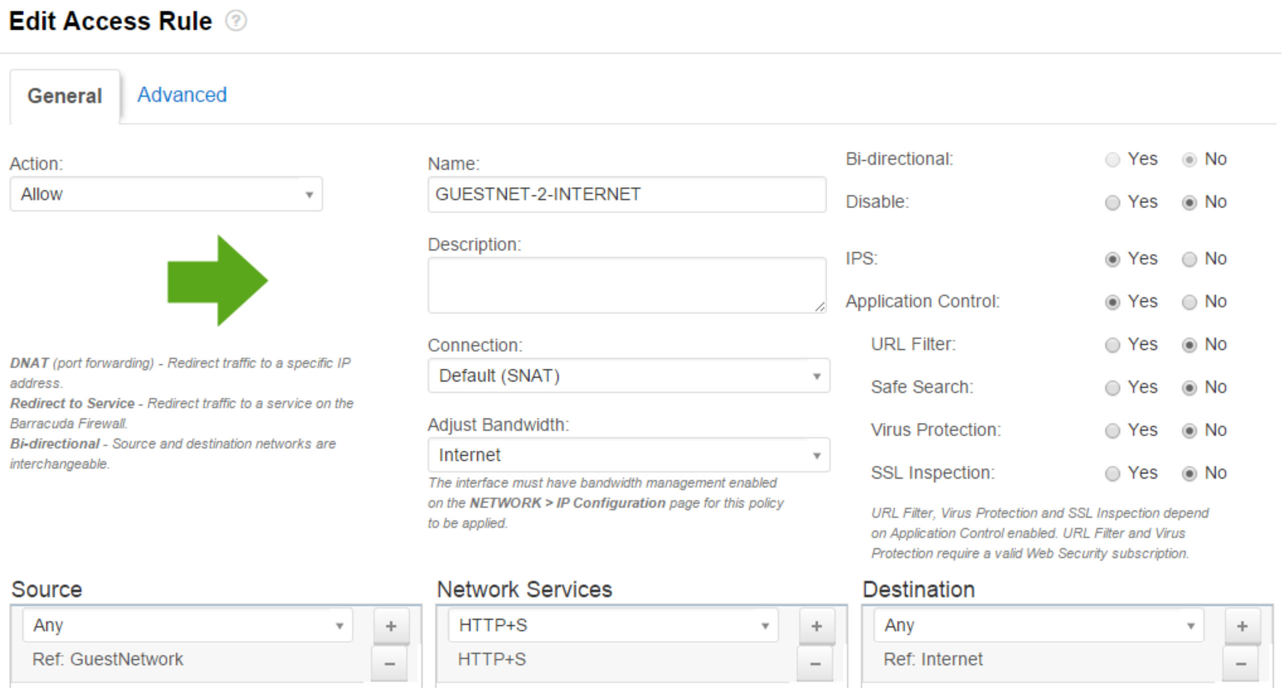
Step 6. Create a PASS Access Rule for Authenticated Users

Create an access rule to allow HTTP/S traffic from guest network users to the Internet.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule** to create a new access rule.

3. In the **Add Access Rule** window, enter a name for the rule. E.g.: `GUESTNET-2-INTERNET`
4. Specify the following settings:

Action	Connection	Adjust Bandwidth	Source	Network Services	Destination
Allow	Default (SNAT)	Internet	Guest Network	HTTP+S	Internet



Edit Access Rule

Action: Allow

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

Name: GUESTNET-2-INTERNET

Description:

Connection: Default (SNAT)

Adjust Bandwidth: Internet

*The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.*

Bi-directional: ○ Yes ● No

Disable: ○ Yes ● No

IPS: ● Yes ○ No

Application Control: ● Yes ○ No

URL Filter: ○ Yes ● No

Safe Search: ○ Yes ● No

Virus Protection: ○ Yes ● No

SSL Inspection: ○ Yes ● No

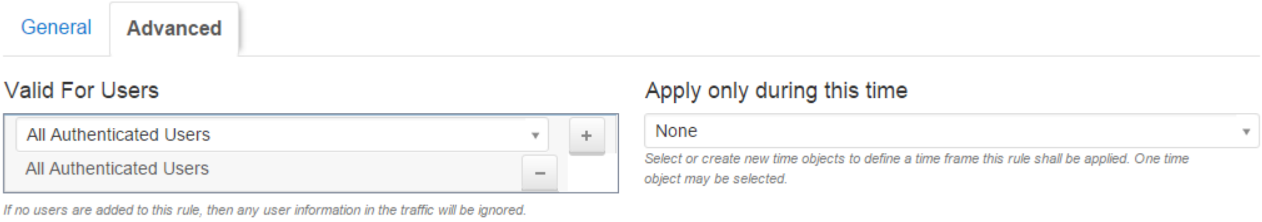
URL Filter, Virus Protection and SSL Inspection depend on Application Control enabled. URL Filter and Virus Protection require a valid Web Security subscription.

Source: Any; Ref: GuestNetwork

Network Services: HTTP+S; HTTP+S

Destination: Any; Ref: Internet

5. In the rule editor window, click the **ADVANCED** tab.
6. In the **Valid for Users** section, select **All Authenticated Users** and click **+**.



Valid For Users: All Authenticated Users; All Authenticated Users

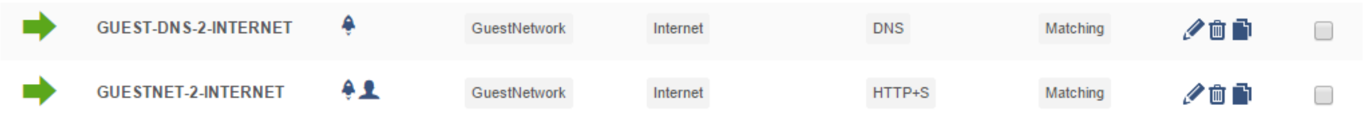
If no users are added to this rule, then any user information in the traffic will be ignored.

Apply only during this time: None

Select or create new time objects to define a time frame this rule shall be applied. One time object may be selected.

7. At the bottom of the rule editor window, click **Save**.

Because rules are processed from top to bottom in the rule list, ensure that the rule to allow DNS traffic is placed above the rule to allow users, and that both rules are placed above the BLOCKALL rule; otherwise, the rules are blocked. For more information, see Firewall Rules Order.



➡	GUEST-DNS-2-INTERNET		GuestNetwork	Internet	DNS	Matching		□
➡	GUESTNET-2-INTERNET		GuestNetwork	Internet	HTTP+S	Matching		□

After adjusting the order of the rules, click **Save**.

Figures