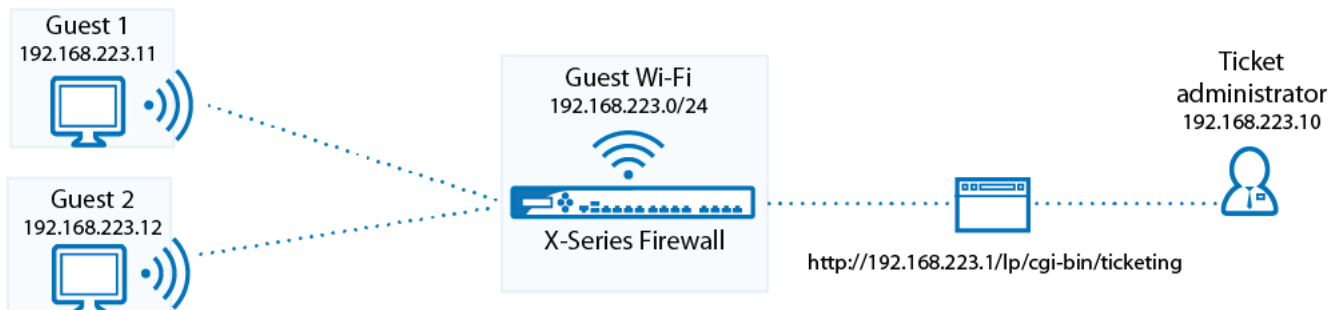


How to Set Up Guest Access with Ticketing

<https://campus.barracuda.com/doc/29327799/>

When you configure a guest network, you can set up a login or ticketing system to temporarily grant access to guests. Before guests can access the network, they must enter a username and password from tickets that are assigned to them. The tickets expire after a set period of time.

Before tickets can be created, you must configure the ticketing system and set up ticket administrators. If the ticket administrator is located in a different network segment, you must also create a firewall rule to allow access to the ticketing web interface.



Follow the instructions in this article to set up a guest network with ticketing.

Before You Begin

- Ensure that the Barracuda NextGen Firewall X-Series 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., 192.168.223.0/24).

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., 192.168.223.0/24).
- **Services to Allow** - Select **DNS Server**.
- **Classification** - Click **Trusted**.

Step 2. Enable the DHCP Server for 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 192.168.223.0 with a netmask of 255.255.255.0, set the **Beginning IP Address** to 192.168.223.10 and the **Ending IP Address** to 192.168.223.250. The IP address assigned to the network interface must not be part of the management network.
 - **DNS Servers** - The IP addresses of the DNS servers.
4. Click **Add Subnet**. 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

If you configured the guest network on a wired interface, specify that the network uses ticketing for guest access.

1. Go to the **USERS > Guest Access** page.
2. In the **Guest Networks** section, select your guest network (e.g., 192.168.223.1/24) from the **Network** column.
3. From the **Type** column, select **Ticketing**.
4. For wired interfaces, click **Add**.
5. Click **Save**. The network appears in the second **Network** table.

GUEST NETWORKS			
NETWORK	NETWORK NAME	TYPE	
172.16.0.100/24		Confirmation Message	Add
192.168.255.1/24	GuestNet	Ticketing	

Define networks for Guest Access or Landing Page here

Step 4. Set Up the Ticket Administrator

The ticket administrator can log into the ticketing system to create guest tickets but cannot log into the management interface of the X-Series Firewall.

1. Specify the ticketing system login credentials.
 1. Go to the **USERS > Guest Access** page.
 2. In the **Ticketing Administrator** section, enter the username and password for logging into the ticketing system.
 3. Click **Save**.
2. Ensure that ticket administrators have the following information:
 - The IP address of the ticketing web interface: <http://lp/cgi-bin/ticketing>
 - The [How to Manage Guest Tickets - User's Guide](#) on how to create guest tickets.

Step 5. Add a Redirect Firewall Rule

[Create a Network Object](#) for the gateway IP address of the guest access network, and then add a [Redirect to Service firewall rule](#).

Step 5.1 Create a Network Object

1. Go to the **FIREWALL > Network Objects** page.
2. Click **Add Network Object**. The **Add Network Object** window opens.
3. Enter a **Name** (e.g., GuestNetworkGW).
4. In the **Include Entries** section, enter the **Network Address** of the gateway IP address of the guest network. The guest network gateway IP address is the IP address that you assigned to the guest network interface in Step 1 (e.g., 192.168.223.1).

Add Network Object ?

Name:

Description:

Include Entries ?

Existing Network Object:

Include a set of networks, devices, interfaces or already existing network objects.

Description	Network Address	MAC Address	Interface	
<input type="text"/>	<input type="text" value="192.168.223.1"/>	<input type="text"/>	<input type="text" value="p4"/>	<input type="button" value="+"/>
	192.168.223.1		p4	<input type="button" value="-"/>

5. Click **Save**.

Step 5.2 Add a Redirect to Service Firewall Rule


1. Go to the **FIREWALL > Firewall Rules** page.
2. Click **Add Access Rule**.
3. In the **Add Access Rule** window, configure these settings:
 - o **Action** - Select **Redirect to Service**.
 - o **Name** - Enter a name.
 - o **Source** - Select the network that the ticket admin's computer is located in (e.g., **Trusted LAN Networks**).
 - o **Destination** - Select the Network Object for the guest network gateway IP address (e.g., **GuestNetworkAccess**).

Add Access Rule ?

General
Advanced

Action:

Redirect to Service



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:

TicketingWebInterfaceRedirect

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

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

Internet

Ref: Trusted LAN

Network Objects IP Address Geo Loc.

Redirect to Service Details

Guest Ticketing

The following protocols and port/protocol combinations are automatically selected upon the chosen Service **Guest Ticketing**:
 Redirects web requests to the guest ticketing page.
 Allows the ticketing admin to login from a non-guest network and create guest login accounts

Destination

DSL4 Local IP

Ref: GuestNetworkAccess

Network Objects IP Address Geo Loc.

4. Click **Save**.
5. [Move the access rule](#) above the BLOCKALL rule.

Step 6. (Optional) Configure the Login 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 cannot be larger than 1 MB and must be in JPG, GIF, or PNG format. The suggested image size is 170 x 40 pixels.


Step 7. 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.

- In the **Add Access Rule** window, enter a name for the rule. E.g.: GUEST-DNS-2-INTERNET
- Specify the following settings:

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

Edit Access Rule 

General

Advanced

Action:

Name:

Bi-directional: Yes No

Disable: Yes No

Description:

IPS: Yes No

Application Control: Yes No

URL Filter: Yes No

Safe Search: Yes No

Virus Protection: Yes No

SSL Inspection: Yes No

Connection:

Adjust Bandwidth:

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

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

Source:
Ref: GuestNetwork

Network Services:
DNS

Destination:
Ref: Internet



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.

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.

- At the top of the rule editor window, click **Save**.

Step 8. Create a PASS Access Rule for Authenticated Users

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

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

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

Edit Access Rule ?

General

Advanced

Action: Allow

Name: GUESTNET-2-INTERNET

Bi-directional: Yes No

Description:

Disable: Yes No

IPS: Yes No

Connection: Default (SNAT)

Application Control: Yes No

URL Filter: Yes No

Adjust Bandwidth: Internet

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

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 **+**.

General

Advanced

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 top 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	  	<input type="checkbox"/>
	GUESTNET-2-INTERNET	 	GuestNetwork	Internet	HTTP+S	Matching	  	<input type="checkbox"/>

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

Next Step

For instructions on how to create tickets for guests, see [How to Manage Guest Tickets - User's Guide](#).

Figures

1. guest_access.png
2. ticketing_page.png
3. GW_IP_Network_Object_67.png
4. Redirect_FW_GuestAccess_67.png
5. GuestDNS-2-INTERNET.png
6. GuestNET-2-INTERNET.png
7. user_access.png
8. rules_order.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.