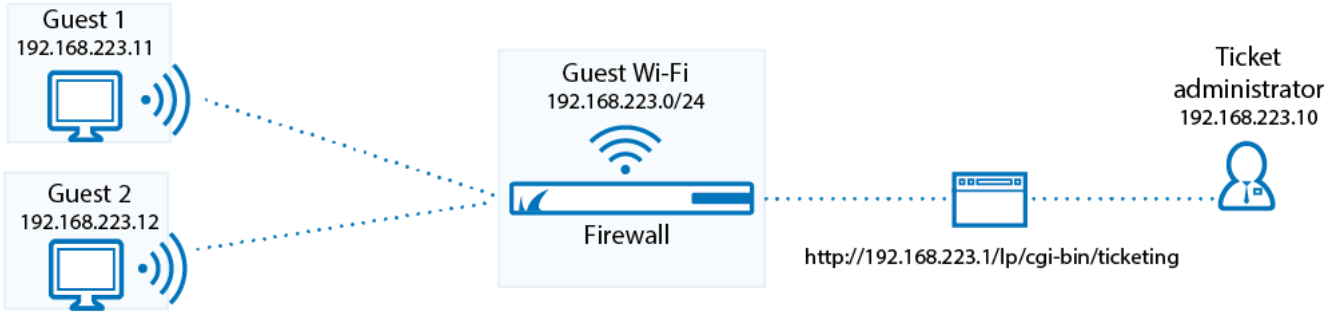
How to Configure Guest Access with the Ticketing System

https://campus.barracuda.com/doc/73008356/

When you configure a guest network, you can set up a login or ticketing system to temporarily grant access to guests. You can use Wi-Fi or a wired network for guest access. 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 an access rule to allow access to the ticketing web interface.



Before You Begin

- Ensure that the 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., 192.168.223.0/24).
- Create or upload an SSL certificate for the ticketing interface. For more information, see How to Use and Manage Certificates with the Certificate Manager.

Step 1. Set Up the Guest Network Interface

Configure a static network interface or a Wi-Fi interface. For more information, see How to Configure Static Network Interfaces and Wi-Fi.

In the **Static Interface Configuration** section, ensure that you specify the following settings:

- **IP Address** – The IP address of the guest network. E.g., `192.168.223.0/24`
- **Classification** – Select **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 **NETWORK > DHCP Server**.
2. In the **DHCP Server** section, enable the DHCP server.
3. Click **Add DHCP Server Subnet**. The **Add DHCP Server Subnet** window opens.
4. 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.
5. Click **Save**.

The guest network subnet appears in the **DHCP Server Subnets** section.

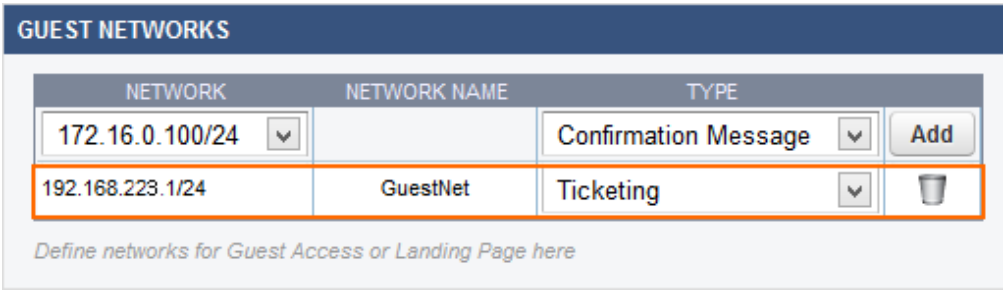
For more information on setting up a DHCP server, see How to Configure the DHCP Service.

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 **USERS > Guest Access**.
2. In the **Guest Networks** section, select your guest network from the **Network** column. E.g., `192.168.223.1/24`
3. From the **Type** column, select **Ticketing**.
4. Click **Add**.
5. Click **Save**.

The network appears in the second **Network** table.



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 firewall.

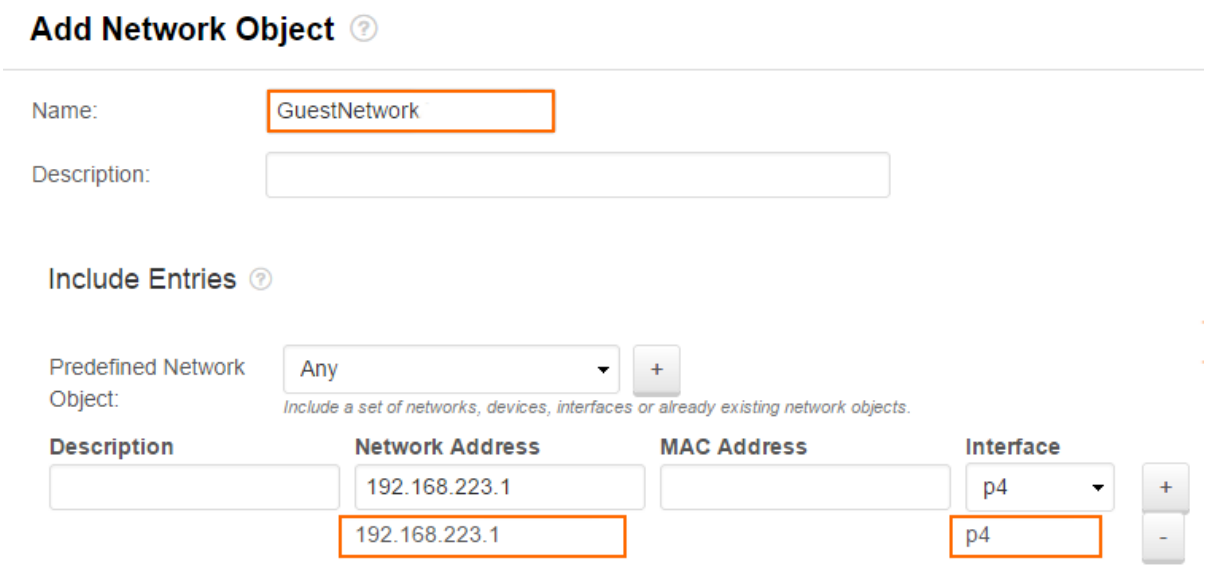
1. Specify the ticketing system login credentials.
   1. Go to **USERS > Guest Access**.
   2. In the **Ticketing Administrator** section, enter the **Username** and **Password** for logging into the ticketing system.
   3. Click **Save**.
2. Ensure that ticket administrators have the following information: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

Step 5. Add a Redirect to Service Access Rule

Create a network object for the gateway IP address of the guest access network, and then add a Redirect to Service access rule.

Step 5.1 Create a Network Object

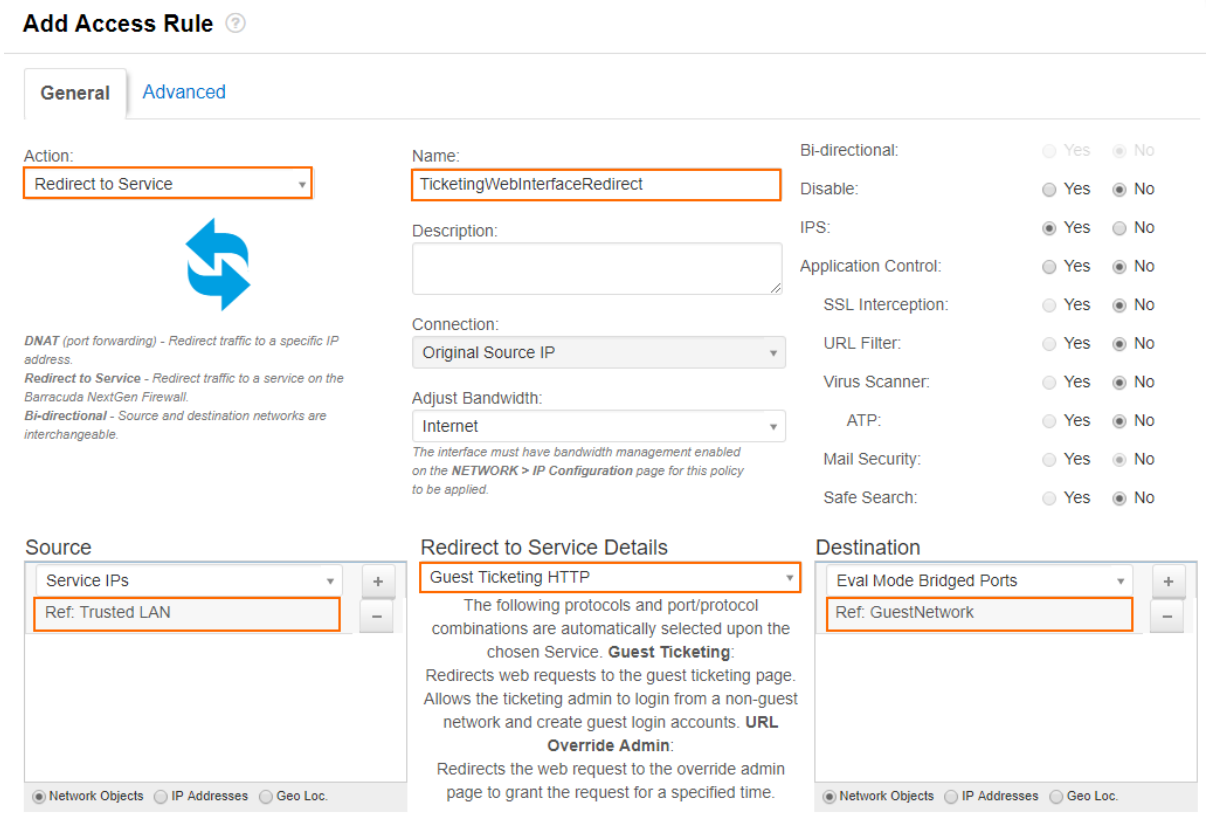
1. Go to **FIREWALL > Network Objects**.
2. Click **Add Network Object**. The **Add Network Object** window opens.
3. Enter a **Name**. E.g., `GuestNetworkGW`
4. In the **Include Entries** section, enter the **Network Address** of the gateway IP address of the guest network. The guest network gateway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



5. Click **Save**.

Step 5.2 Add a Redirect to Service Access Rule

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule**. The **Add Access Rule** window opens.
3. Specify the following settings:
   - **Action** – Select **Redirect to Service**.
   - **Name** – Enter a name for the rule. E.g., `TicketingWebInterfaceRedirect`
   - **Source** – Select the network that the ticket admin's computer is located in. E.g., **Trusted LAN**
   - **Network Services** – Select **Guest Ticketing**.
   - **Destination** – Select the network object for the guest network gateway IP address. E.g., **GuestNetwork**



1. Click **Save**.
2. 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.

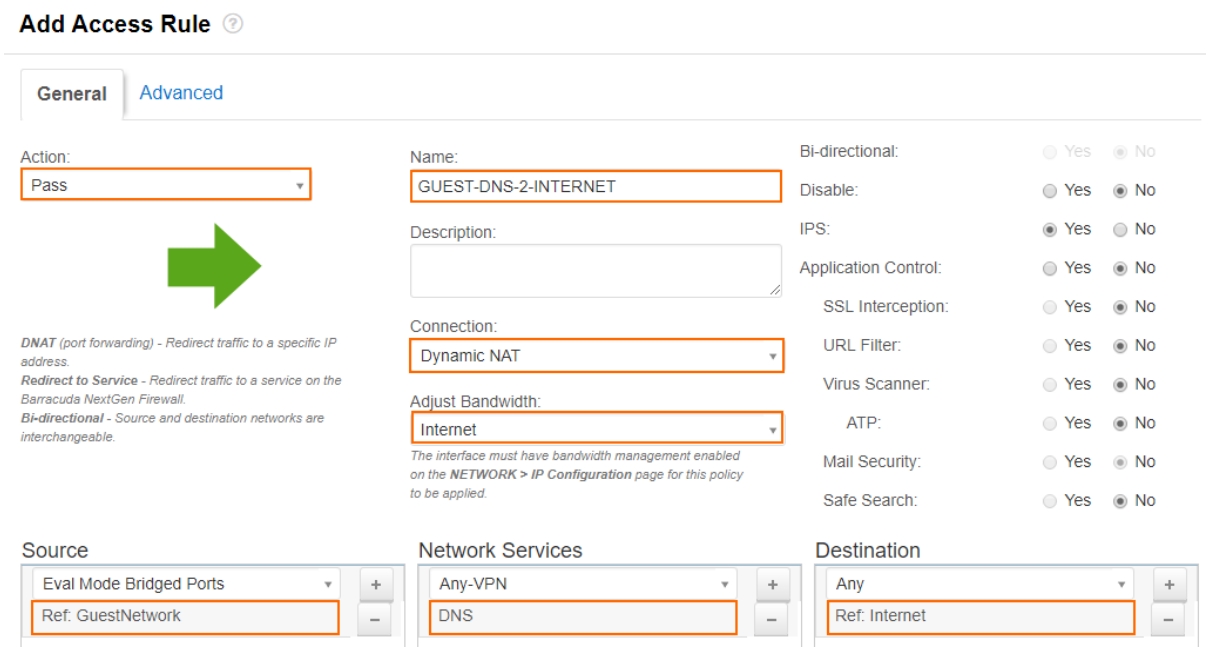
In the **Login Page Options** section, edit the **Welcome Message** and upload a **Welcome Image**. The image cannot be larger than 1 MB and must be in JPG, GIF, or PNG format. The suggested image size is 170 x 40 pixels.

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 **FIREWALL > Access Rules**.
2. Click **Add Access Rule**. The **Add Access Rule** window opens.
3. Specify the following settings:

- **Action** – Select **Pass**.
- **Name** – Enter a name for the rule. E.g., `GUEST-DNS-2-INTERNET`
- **Connection** – Select **Dynamic NAT**.
- **Adjust Bandwidth** – Select **Internet**.
- **Source** – Select the Network Object for the guest network gateway IP address. E.g., **Guest Network**
- **Network Services** – Select **DNS**.
- **Destination** – Select **Internet**.



To allow connections from the guest network to the Internet, the 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 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.

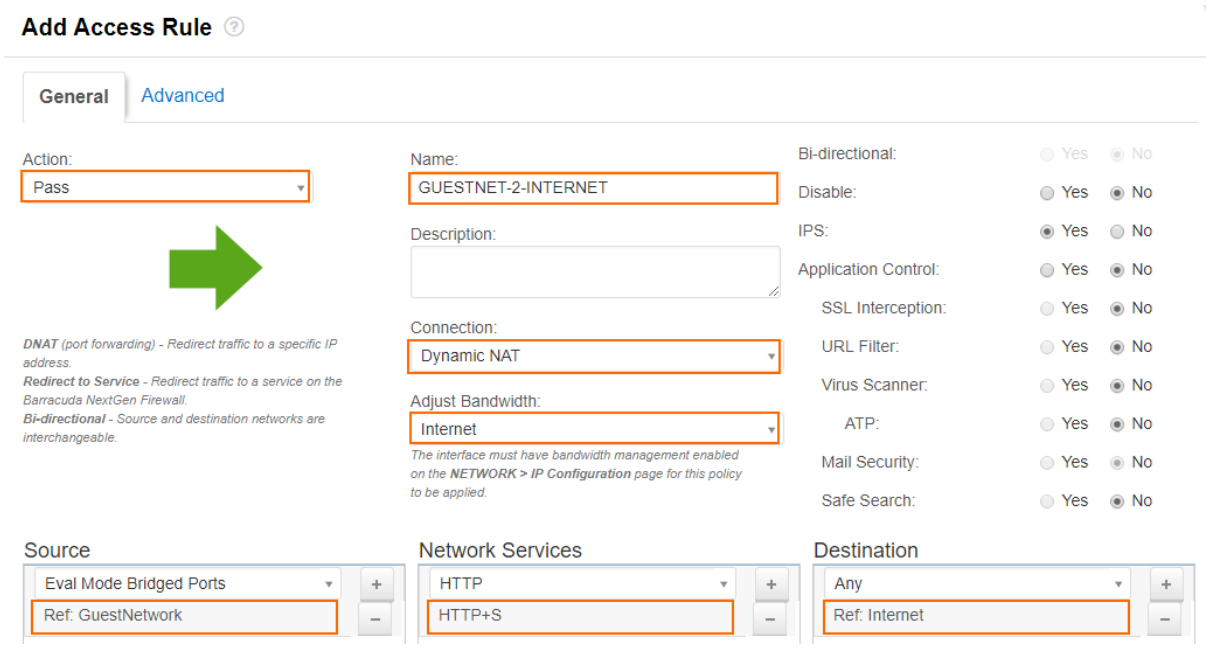
4. At the top of the rule editor window, click **Save**.

Step 8. Create a PASS Access Rule for Authenticated Users

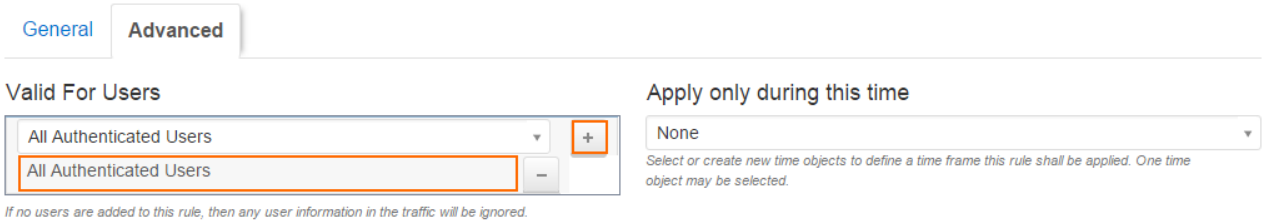
Create an access rule to allow HTTP/S traffic from guest network users to the Internet.

1. Go to **FIREWALL > Access Rules**.
2. Click **Add Access Rule**. The **Add Access Rule** window opens.
3. Specify the following settings:
   - **Action** – Select **Pass**.
   - **Name** – Enter a name for the rule. E.g., `GUESTNET-2-INTERNET`
   - **Connection** – Select **Dynamic NAT**.
   - **Adjust Bandwidth** – Select **Internet**.

- **Source** – Select the Network Object for the guest network gateway IP address. E.g., **GuestNetwork**
- **Network Services** – Select **HTTP+S**.
- **Destination** – Select **Internet**.

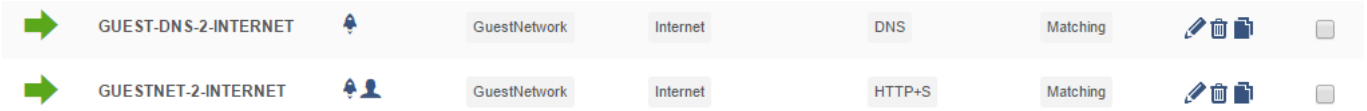


1. In the rule editor window, click the **ADVANCED** tab.
2. In the **Valid for Users** section, select **All Authenticated Users** and click **+**.



3. 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.



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_network_object_ticket.png
4. Redirect_FW_GuestAccess.png
5. GuestDNS-2-INTERNET_01.png
6. GuestNET-2-INTERNET_01.png
7. user_access.png
8. rules_order.png