Example - Handling SMTP Traffic

https://campus.barracuda.com/doc/16680425/

You must configure at least one access rule to control mail traffic. Direct SMTP traffic to your Barracuda Email Security Gateway or your mail server. If your mail server supports POP/IMAP access, configure a rule that allows this access. If you have more than one external IP address, configure a access rule to ensure that outgoing traffic uses the correct IP address.

Incoming Traffic

If your mail server or Barracuda Email Security Gateway is on the public network, you might want to allow your Barracuda NextGen X-Series Firewall to provide protection and move your mail system onto the internal network. The mail traffic passes through the firewall in both directions.

If the advertised method of receiving email is a dynamically-assigned IP address, use a service such as DynDNS to make a permanent identifier for your mail server or Email Security Gateway. For more information on the DynDNS service, see http://dyn.com/dns/.

As you can see on the **FIREWALL > Service Objects** page, the Any-EMAIL service object contains the following email protocols: POP2, POP3S, POP3, IMAP, IMAPS, and SMTP. You can use this object or just the protocols that you want to support. The rules below specify the protocols explicitly. Configure the access rules for the cases that match your scenario, and then verify your access rule order.

Case 1 – Barracuda Email Security Gateway

Configure a rule to redirect incoming mail traffic for the Barracuda Email Security Gateway. If you have an Email Security Gateway and your mail server does not support POP or IMAP, this is the only rule that you will need for incoming email traffic.

Go to the **FIREWALL > Firewall Rules** page and configure the following rule to redirect the incoming mail traffic:

SMTP-2-SPAMFW Values:

Action	Source	Destination	Service	Connection	Redirected To

DNAT	Either the **Internet** network object or a specific public IP address. For example, the IP address of the hosting provider.	The destination depends on the advertised method of receiving email. • If it is one or more external static IP addresses, enter those addresses (a CIDR summarization of addresses can also be used). • If it is a domain name which maps to a dynamically-assigned IP address, select the network object named **Any** .	**SMTP**	**No SNAT** (the original source IP address is used)	The internal static IP address of the Barracuda Email Security Gateway.

Case 2 – Barracuda Email Security Gateway and a POP/IMAP Mail Server

If you have a Barracuda Email Security Gateway and you also want to support POP/IMAP traffic from your mail server, then you must add this rule in addition to the above rule for the Email Security Gateway.

Go to the **FIREWALL > Firewall Rules** page and configure the following rule to redirect the incoming POP/IMAP traffic only to the mail server:

POP-2-INTERNAL Values:

Action	Source	Destination	Service (select relevant ones)	Connection	Redirected To

DNAT	Either the **Internet** network object or a specific public IP address. For example, the IP address of the hosting provider.	The destination depends on the advertised method of receiving email. • If it is one or more external static IP addresses, enter those addresses (a CIDR summarization of addresses can also be used). • If it is a domain name which maps to a dynamically assigned IP address, select the network object named **Any**.	**POP2** **POP3** **POP3S** **IMAP** **IMAPS**	**No SNAT** (the original source IP address is used)	The internal static IP address of the mail server.

Case 3 – Mail Server Only

If you do not have a Barracuda Email Security Gateway, you can redirect the incoming traffic to the mail server that is on your internal network.

Go to the **FIREWALL > Firewall Rules** page and configure the following rule to redirect the incoming mail traffic:

EMAIL-2-MAIL-SERVER Values:

Action	Source	Destination	Service (select relevant ones)	Connection	Redirected To

DNAT	Either the **Internet** network object or a specific public IP address. For example, the IP address of the hosting provider.	The destination depends on the advertised method of receiving email. • If it is one or more external static IP addresses, enter those addresses (a CIDR summarization of addresses can also be used). • If it is a domain name which maps to a dynamically assigned IP address, select the network object named **Any**.	**SMTP** **POP2** **POP3** **POP3S** **IMAP** **IMAPS**	**No SNAT** (the original source IP address is used)	The internal static IP address of the mail server.

Verify the Order of the Access Rules

New rules are created at the bottom of the firewall rule set. Because rules are processed from top to bottom in the rule set, arrange your rules in the correct order. You must especially ensure that your rules are placed above the BLOCKALL rule; otherwise, the rules are blocked. After adjusting the order of rules in the rule set, click **Save Changes**.

Outgoing Traffic

Outgoing SMTP traffic (for outgoing email) must also be allowed to pass. Depending on the location of your mail server, this traffic might already be allowed by the pre-installed LAN-2-INTERNET rule. If it is not, or if you want to make an explicit rule anyway, you must add a rule.

Configure the access rules for the case that matches your scenario. If you have multiple public IP addresses, follow the instructions in Case 2 - Multiple Public IP Addresses to ensure that the traffic leaves on the same IP address that the public MX record points to. If you do not have multiple IP addresses, follow the instructions in Case 1 - Mail Server Not on Trusted LAN. After configuring the required access rule, verify your access rule order.

Case 1 – Mail Server Not on Trusted LAN

Go to the **FIREWALL > Firewall Rules** page and configure the following rule to allow outgoing SMTP traffic:

SMTP-2-INTERNET Values:

Action	Source	Destination	Service (select relevant ones)	Connection
Allow	The internal IP address of the mail server	**Internet**	**SMTP**	**Default (SNAT)**

Case 2 – Multiple Public IP Addresses

If you have multiple external IP addresses and want to force outbound SMTP traffic to use a specific IP address :

1. Go to the **FIREWALL > Connection Objects** page and create a connection object that specifies the IP address that is in the MX record.
2. Go to the **FIREWALL > Firewall Rules** page and add the following rule to direct the outgoing mail traffic:

SMTP-2-INTERNET Values:

Action	Source	Destination	Service	Connection
Allow	The internal IP address of the mail server	**Internet**	**SMTP**	A connection object with the IP address used for email.

Verify the Order of the Firewall Rules

Move the firewall rule above the pre-installed LAN-2-INTERNET rule. If this rule is under the LAN-2-INTERNET rule, traffic goes out on the primary IP address, which might not be the correct path. After adjusting the order of rules in the rule set, click **Save Changes**.