

Email Non Delivery Receipts (NDR)

also known as Bounce Messages

As an increasing number of organizations implement anti-spam and anti-virus solutions, it has become more important to understand how and why email non-delivery receipts (NDRs) or bounce messages are generated. By understanding how NDRs work, organizations are better equipped to create useful NDRs that help legitimate emails reach their intended recipients.

This whitepaper gives an overview of NDRs and discusses how they relate to the Barracuda Spam Firewall.

What are NDRs?

NDRs, also known as bounce messages, are the email messages that are sent to an email's sender when an email can not be delivered. Nearly all users of email have received an NDR at one time or another.

There is no standard format for NDRs, and no standards for what must be included in an NDR. Different email servers have different formats. Some NDRs include the original email message (either in the body of the NDR or as an attachment); others do not. Some NDRs include text that clearly explains why the email message could not be delivered; others do not. There are also NDRs that simply inform the sender that their email message has not been delivered yet but an email server is still trying to deliver it.

Although there are some standards for how and when an NDR is generated, not all email servers follow the standard. Different email servers typically have different ways of generating NDRs. However, most email servers will generate an NDR when an email is not delivered.

When are NDRs generated?

In order for an email to reach its recipient, the email typically travels from one server to another until it reaches the destination server. Each of the servers along the path chooses to either accept the email (for delivery to the next server or the end user) or reject the email either permanently or temporarily. The Barracuda Spam Firewall can be viewed as one of the servers along the path and thus can either accept or reject the email as well.

NDRs are generated and emails are bounced back to the sender for a variety of reasons. Historically, the most common reasons have included:

- the destination email server is down and there is no response
- the email address is invalid
- the domain name is invalid
- an email server is incorrectly configured
- the message was rejected for an unknown reason.

However, with the increasing amounts of spam being sent, there are now a number of other reasons to reject an email. These reasons include:

- a virus was detected
- the email includes obscene language or other banned words
- the email looks like spam according to pre-determined rules
- the email has a faked sender
- the email includes a banned file type
- and many others.

How are NDRs generated?

There are two fundamental ways that an NDR may be generated.

When a server receives an email from another server (the sending server), it can either accept or reject the email. If the server rejects the email, the sending server is responsible for generating a NDR to the sender. The sending server will typically try to incorporate into the NDR the reason the receiving server gave for rejecting the email. This reason is typically difficult to decipher by end users since the servers tend to provide cryptic messages.

The second fundamental way of generating an NDR occurs if the destination server accepts the email and then later decides that it does not want to forward it on to the next server. In this case the destination server must create the NDR and send it to the originator of the email.

NDRs and the Barracuda Spam Firewall

Because the Barracuda Spam Firewall is one of the servers that an email passes through when going from sending server to destination server, it can also accept or reject an email message. If the Barracuda Spam Firewall determines that the email is spam before the email is fully received, it will reject the email. The sending server is then responsible for generating the NDR. In this case, the Barracuda Spam Firewall has little control over the format and content of this message. If, however, the Barracuda Spam Firewall fully accepts the message and then determines it is spam or contains a virus, it will generate the NDR. In this case, the Barracuda Spam Firewall has complete control over the content of the NDR.

The Barracuda Spam Firewall has been especially optimized to reduce the chance of blocking a legitimate email (a false positive). But as with all spam and virus solutions, there is a small probability that a false positive may occur. There is a higher probability of a false positive when users include their own "blocking" rules based on keywords and have not taken into account all the repercussions. Nevertheless, whenever an email is blocked by the Barracuda Spam Firewall, an NDR is generated and sent to the originator of the email (if the originator has a legitimate email address).

Best Practices for NDRs

NDR messages can be quite cryptic and unfriendly at times. However, with the Barracuda Spam Firewall, users may create clear, useful, and courteous NDRs that are appropriate for professional environments.

Barracuda Networks ■ Email Non Delivery Receipts (NDR)

Here are a number of best practice rules that we have developed for creating NDR messages:

- NDRs should be in a language that the recipient can understand. Note that many systems only send NDRs in English. If your primary business is in another language, your NDRs should be as well.
- NDRs should contain appropriate polite wording. It is best to include an apology and a polite explanation.
- NDRs should tell the sender what is wrong with the message. It is best to tell the sender why the message was rejected so that they have information to correct the problem if it is a legitimate message.

- NDRs should tell the sender how to get the message delivered if it is legitimate.

One common and useful technique is to have the receiving destination add a special word to their Barracuda Spam Firewall's white list. However, we do not recommend using the company name or anything that can be determined from the company's email addresses or domains. The NDRs can then be customized to say something such as: To make sure this email is delivered, please place the word spamfirewall in the subject of your email.

Legitimate emails that were blocked will now be delivered, provided that they do not contain a virus. In the unlikely scenario that a spammer obtains the special word to spam the company, the company can simply change the special word in its white list.

- NDRs should tell the sender who to contact (i.e. phone number) if they are unable to get their message delivered.

Nearly all spammers do not accept NDRs, ignore NDRs, or route NDRs to other domains. Because of this, it is typically safe to provide useful information in your NDRs in case a person actually is trying to legitimately send an email.

Here is an example of a good NDR message. This is a message from a Barracuda Spam Firewall located at the fictitious "Smith Company47"

```
Subject: **Message blocked by Barracuda Spam Firewall at Smith
Company47**
```

```
We apologize, but your message to:
john DOE@smithcompany47.com
was blocked by our Barracuda Spam Firewall. The email you sent with the
following subject has NOT BEEN DELIVERED:
```

```
Subject: Need to get a Viagra prescription
```

```
If this is a legitimate message and you would like it to be delivered,
please add the word "farmplowmodel44" to the subject and the message
will be allowed through.
```

```
We apologize for any inconvenience.
```

```
If you have any further questions or are unable to get your email
delivered please contact us at 999-999-9999 (USA) and ask for Martin.
```

```
Sincerely,
```

```
SmithCompany47
```

Conclusion

With the large amounts of spam and viruses being sent through the Internet, and the increasing number of organizations implementing anti-spam and virus solutions, organizations are now paying more attention to NDRs. To date, there are few implemented standards for NDRs. Most NDRs are unfriendly and cryptic, making them useless in helping the sender get his email delivered. However, for companies using the Barracuda Spam Firewall, friendly, clear and useful NDRs can be created to help ensure that legitimate emails actually arrive at their intended destinations.



Barracuda Networks

10040 Bubb Road

Cupertino, CA 95014

+1 408 . 342 . 5400

+1 888 . 268 . 4772

www.barracudanetworks.com

info@barracudanetworks.com