

Using MX Records and Spam Firewalls

This whitepaper defines MX records and provides information about effectively using MX records in conjunction with a spam firewall, such as the Barracuda Spam Firewall.

MX Records

MX records are DNS entries that are used by sending email servers to locate destination email servers. An email server sending an email to a particular domain will look up the MX record for that destination domain. The MX record provides a machine name or an IP address for the destination domain. For example, if an email server wants to send an email to bob@mydomain.com, it would perform an MX record look up on mydomain.com to determine the destination IP address. Once the sending email server has the destination IP address, it would then be able to contact the destination machine to deliver the email.

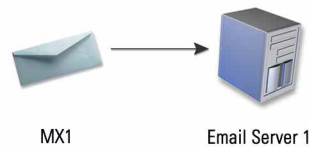


Figure 1: Basic MX Record Setup

Multiple MX Records

Some domains have several MX records associated with it. Each MX record has a different priority associated with it and each one points to a different server.

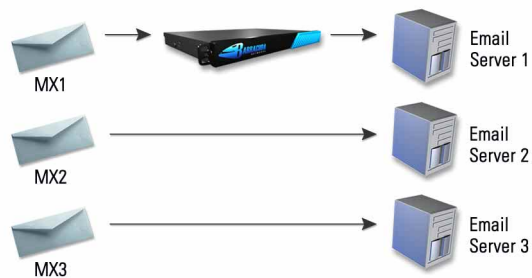


Figure 2: Domain with Multiple MX Records

When a sending email server performs an MX record lookup on a destination domain, it obtains the complete list of MX records and their associated priorities. Under normal circumstances, the sending email server will attempt to send the email to the highest priority destination first and only proceed down the list if the higher priority machine is down, overloaded or cannot take the email for some reason. This is particularly useful when building robust and high availability systems. The email is delivered according to the highest priority MX record. If the email server specified in that record is down, then the email is routed according to the next highest priority MX record.

Using a Spam Firewall

To help block spam, some organizations may have their email server's highest priority MX record point to a spam firewall rather than the email server itself. This way the first machine to receive the email would be the spam firewall. The spam firewall would then process the email and determine if the email is legitimate. If it is, then it would forward the email to the destination email server.



Figure 3: Spam Firewall and MX Record

To protect against the case of the spam firewall going down, some organizations have a lower priority or backup MX record that points directly to the email server.



Figure 4: Wrong Method for Obtaining High Availability

This, however, is not a recommended way to protect against a spam firewall failing. Why? Spammers know about this method and will take advantage of the lower priority MX record that bypasses the spam firewall. Spammers will send spam directly to the lower priority MX record so that they will always bypass the spam firewall and get through to the email server.

Barracuda Networks ■ Using MX Records and Spam Firewalls

For organizations who wish to protect against a spam firewall failing, we recommend having both the first and second priority MX records point to a spam firewall and the spam firewall pointing to an email server. This way all email, regardless of which MX record is being used, is always processed by a spam firewall first.



Figure 5: Correct Method for Obtaining High Availability

Summary

To effectively use MX records with spam firewalls, we recommend having the highest priority MX record point to the spam firewall and the spam firewall point to the email server.

To have a high availability environment, we recommend having a lower priority MX record point to another spam firewall and the spam firewall point to an email server. It is not effective to have the lower priority MX record point directly to an email server since spammers will simply bypass the higher priority MX record and use the lower priority MX record to send spam directly to the email server.



Barracuda Networks

10040 Bubb Road
Cupertino, CA 95014
+1 408 . 342 . 5400
+1 888 . 268 . 4772

www.barracudanetworks.com
info@barracudanetworks.com