Managed Cloud Email Security [MCES] Client Side Setup

Network Box USA'S (NWB) List of IPs

Any time the instructions below require you to open ports inbound in your firewall; traffic should always be limited only to the following subnets:

69.7.162.176/28

69.7.160.24/29

192.159.123.0/25

Inbound Email

In order for NWB to deliver emails to your email server, you will need to open port TCP/25 inbound, allowing access only from the IP addresses mentioned above, and redirect said port to the local eMail server.

Please do NOT allow any traffic on port TCP/25 inbound from other source IP addresses, unless you have set up a separate email scanner to intercept emails that aren't going through the NWB MCES service.

TLS

We will be delivering your emails to you via the internet. To guarantee your privacy, and in most cases, also compliance with existing law and regulations, we will only deliver such emails using TLS, to ensure they are encrypted. To that end, you will need to ensure the email server is set to support STARTTLS and open port 25 inbound to the server *only* from the IP addresses mentioned at the beginning of this document. Documentation on how to set up STARTTLS on your specific server is available online.

You can easily verify if STARTTLS is set up by using telnet on port 25 to the IP of your server; once you obtain the initial prompt, type an EHLO line (i.e., ehlo me); the reply from the server should contain, among other lines, one showing "250 STARTTLS".

Envelope Verify via LDAP

NWB email scanner verifies the existence of the recipient before accepting an email. In order to allow such verification, you will need to create a user within the LDAP structure, and provide NWB with the following information:

- distinguishedName of the Network Box user
- Password
- distinguishedName of the LDAP root domain
- public IP to which NWB will send the LDAP queries

NWB will use this LDAP connection to verify that the recipients of inbound emails actually exist, before accepting emails.

Supported protocols are LDAP for AD, Open LDAP and Radius.

LDAP

LDAP transactions exchange information such as usernames and passwords. Since this connection is via the internet, we require that the transmission be encrypted. You will need to ensure LDAP is using encryption, and, specifically, LDAPS on port TCP/636 or, for MS Exchange, TCP/3269.

You will need to open inbound traffic on the appropriate port and restrict access to the list of IP addresses mentioned above.

Envelope Verification Based on Static List

If your company is not running LDAP, you can provide NWB a list of your email addresses; this will be imported in the MCES and used for envelope verification. It is important that this list be comprehensive, as any email address left out of the list will be considered DHA and emails to that address will be rejected. The list can be updated from time to time upon your request.

Outbound Email

As part of the MCES service, you have the option to relay your outbound email through NWB's cloud. Outbound emails will be scanned for viruses, spam and, optionally, also DLP. Email traffic outbound will need to be redirected to any of the IP addresses corresponding to mces.networkboxusa.com. In order to facilitate this, set up a smarthost on your email server, using mces.networkboxusa.com as the destination, and provide NWB with the IP address from which such emails will be sourced.

Outbound 4245

NWB's MCES generates eMail portal reports which allow users to release emails quarantined in error, and to create personal whitelists and blacklists. In order for this feature to work, you will need to open port TCP/4245 outbound to the IP addresses corresponding to mces.networkboxusa.com.

SPF Record

If you do not already have one, you will need to create an SPF record and include the following in it:

include:mces.networkboxusa.com

NOTE: ideally the SPF record should end in -all; client can include anything else necessary in the SPF record, as long as the include line above is part of it. For more information on SPF records, please see http://www.openspf.org/SPF_Record_Syntax

Your emails will not be accepted by our scanning system if the SPF record is incorrectly created or does not include the above line.

MX Record

For every domain protected by NWB, you will point the MX record to a name constructed as follows:

- replace the dots with dashes in your primary domain name
- add mces.networkboxusa.com. to it

For example, for our own domain we have:

networkboxusa.com. 86400 IN MX 10 networkboxusa-com.mces.networkboxusa.com.

10 is the priority and can be set to any number since there will be only 1 MX record

86400 is the TTL (time to live) and specifies the DNS resolver cache. The value shown here serves merely as an example.

NOTE the period at the very end of the line:

networkboxusa-com.mces.networkboxusa.com.

That period is very important because it tells the DNS resolver that the name is to be used 'as is'. Otherwise, any DNS resolver will append the name of your domain to it, and the result would be a value that has no meaning.