Stop Email Spoofing Using MDaemon's

Improved IP Shield Feature

What is IP Shield?

IP Shield is a security feature in MDaemon that protects local accounts by preventing malicious users from spoofing, or pretending, to be a local user on your MDaemon server. IP Shield works by pairing an IP address/IP range with your local domain. If a sending user claims to be a user of a domain entered into IP Shield then the user must be sending their message from the supplied IP address/IP range. Below is an example of an IP Shield entry.

Yourdomain.com 192.168.0.*

*****Be sure to read the important notes at the end of this article.

What does the above example mean?

If a sending user is claiming to be a user of the Yourdomain.com domain then they must be sending their message from the 192.168.0.* IP range.

What if the user is not coming from the IP address/IP range specified and they are a valid user?

Enabling SMTP authentication in the user's email client will bypass the IP Shield security check. By default any authenticated SMTP sessions will not have IP Shield applied to them.

IP Shield Standard Behaviour

IP Shield is applied to the domain name given in the MAIL FROM command during the SMTP session. Below is an example of a rejection that failed to meet the requirements of IP Shield.

```
Tue 2012-06-26 14:17:12: Accepting SMTP connection from [173.239.156.252:11063] to [173.239.156.253:25]
Tue 2012-06-26 14:17:12: --> 220 mail.robobak.ca ESMTP MDaemon 12.5.6; Tue, 26 Jun 2012 14:17:12 -0400
Tue 2012-06-26 14:17:14: <-- ehlo mike
Tue 2012-06-26 14:17:14: --> 250-mail.robobak.ca Hello mike, pleased to meet you
Tue 2012-06-26 14:17:14: --> 250-ETRN
Tue 2012-06-26 14:17:14: --> 250-AUTH LOGIN CRAM-MD5 PLAIN
Tue 2012-06-26 14:17:14: --> 250-8BITMIME
Tue 2012-06-26 14:17:14: --> 250-STARTTLS
Tue 2012-06-26 14:17:14: --> 250 SIZE
Tue 2012-06-26 14:17:24: <-- MAIL FROM:<mike@yourdomain.com>
```

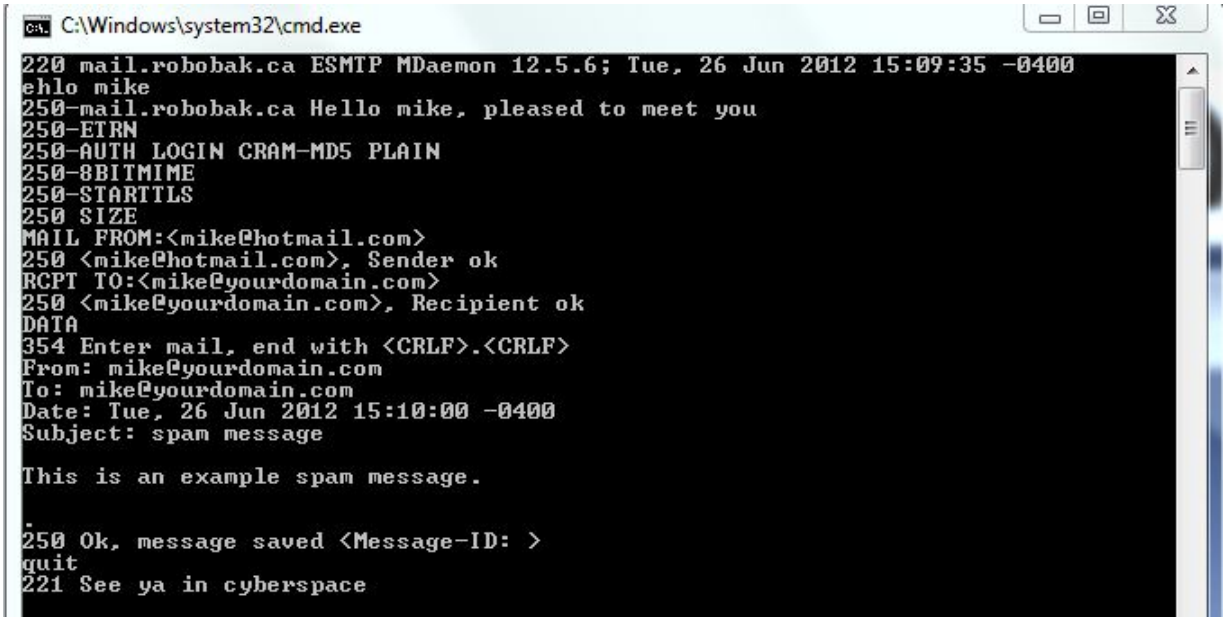
```
Tue 2012-06-26 14:17:24: --> 530 Authentication required to send mail from 173.239.156.252
Tue 2012-06-26 14:17:26: <-- quit
Tue 2012-06-26 14:17:26: --> 221 See ya in cyberspace
Tue 2012-06-26 14:17:26: SMTP session terminated (Bytes in/out: 50/296)
Tue 2012-06-26 14:17:26: ----------
```

As we can see, the domain name used in the MAIL FROM command was Yourdomain.com so MDaemon expects the session to be coming from the 192.168.0.* IP range. Since the session did not come from this IP range the connection is rejected with a "530 Authentication required..." error. The wording of the error will hopefully let a valid user know to enable authentication in their email client to be able to send their message to MDaemon.

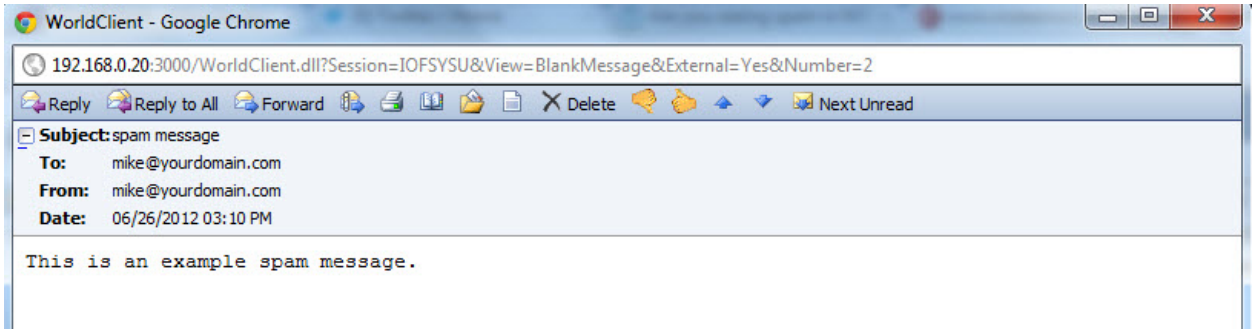
If you have ever received a spam message that appeared to be From and To yourself then you may be wondering how the message was accepted by MDaemon even if you were using IP Shield. Most spammers are smart enough to know not to use a local address in the MAIL FROM command because most email servers require some form of verification in order for the email server to accept their email (i.e. require SMTP authentication). So the spammer will give an external address in the MAIL FROM command, which MDaemon cannot apply IP Shield to.

It's after the DATA command is given during the SMTP session is when the actual message is being transferred to the server. This is where the From, To, Subject, Date headers (and others) along with the body of the message are formed. Here the spammer can make the message appear to be From and To the local user.

Below is a screenshot of a telnet session. In this session I'm pretending to be an external sender while forming both the From and To headers to contain the local users address.



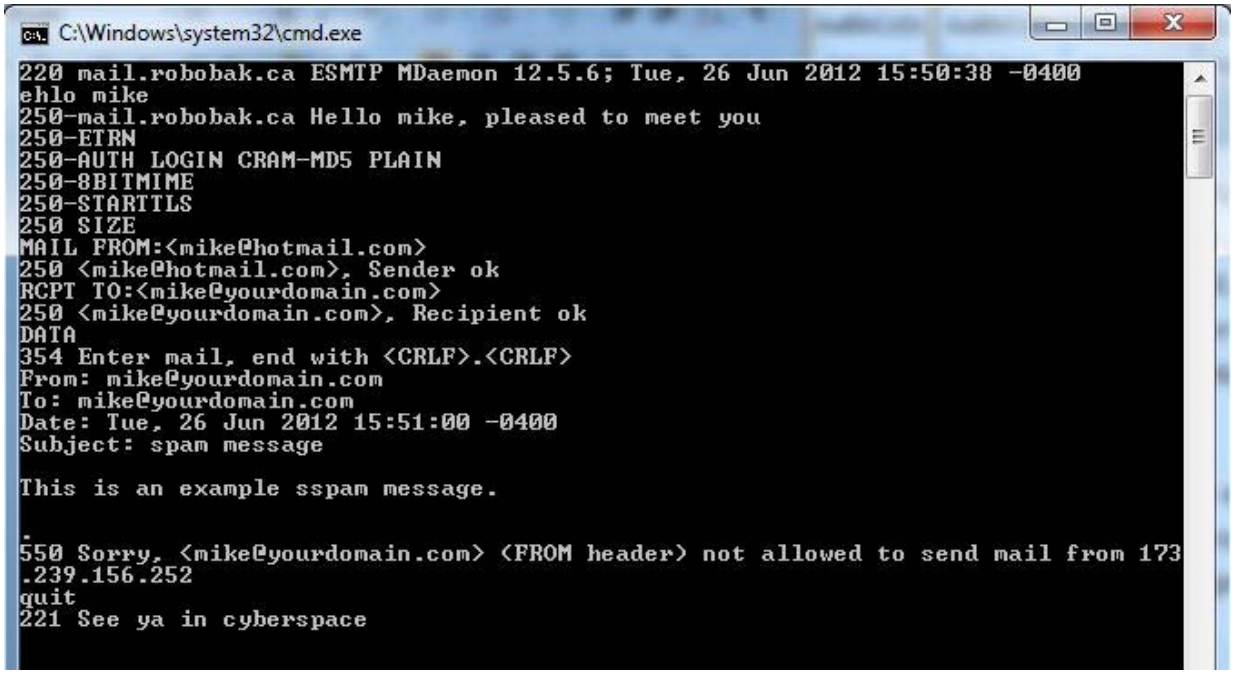
Under the old IP Shield behaviour this email is accepted. Below is what this email looks like when viewed through WorldClient.



Improved IP Shield Behaviour

If you are still with me, and I hope you are, here's how Alt-N improved the IP Shield feature. IP Shield can now be set to also look at the From header of an email and apply IP Shield to the domain used. IP Shield will still look at the domain name given in the MAIL FROM command but now it can also look at the From header. Since the From header is formed after the DATA command is given we'll see the rejection near the end of the session.

Below is a screenshot of a telnet session where MDaemon's IP Shield feature is set to check the From header.



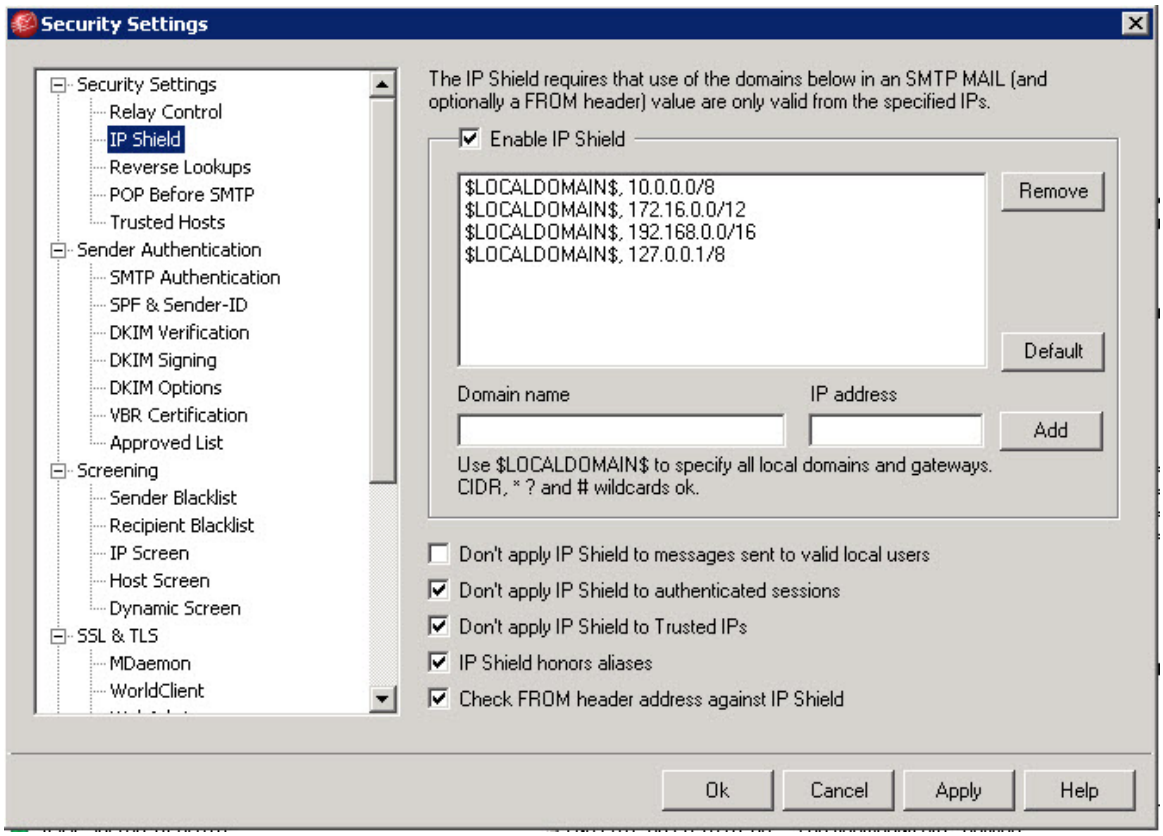
We can see that MDaemon rejected this spoofed email and the error is a bit different which indicates to the admin why the email was rejected.

Important Notes

In order to benefit from the IP Shield feature, MDaemon must be accepting email from external sources directly. This means that the MX record for your domain will point directly to MDaemon. MDaemon has to be able to see the connecting IP address of the SMTP sessions in order to apply its IP Shield settings.

Alt-N Technologies improved the IP Shield feature in MDaemon v12.5.0. You may need to update your MDaemon installation in order to take advantage of this improved security feature. You can download your MDaemon update from here: http://www.ccsoftware.ca/mdaemon/download.cfm.

To turn on the IP Shield feature, access the MDaemon GUI and click Security | Security Settings | IP Shield. Below is a screenshot of the IP Shield options on a typical set up.



The new option that will give us the improved spoof checking is “Check FROM header address against IP Shield”. It is also good to note here that MDaemon can use the $LOCALDOMAIN$ macro. This is handy for MDaemon servers that have multiple domains configured so that the admin doesn’t have to manually add every domain. The entries you see in the above screenshot can be made automatically by MDaemon by clicking the Default button on the right hand side.

Feel free to ask us any questions by directing them to support@ccsoftware.ca.

We’re always happy to help you get the most from your MDaemon software!