Ask-a-Muse: Follow up on FQDN in CFMAIL

Posted At : February 13, 2009 6:10 PM | Posted By : Mark Kruger
Related Categories: ColdFusion

Muse reader **Eric Cobb**, whose **CFgears** blog is an great read, made an excellent point regarding my statement that the designated server for a CFMAIL tag should be a full qualified domain name instead of just an IP address.

> *Eric wrote:*
> To me, this seems like it would be a problem with your mail server, not CF. The mail server is responsible for telling the world the FQDN the email is coming from, not CF. All the mail server settings in the CF Administrator do is tell CF who to pass the mail to so it can be sent, right? The mail server does the actual sending of the mail, and should have everything set up to report its FQDN. So if you specify the mail server's IP address in the CF Administrator, that should be fine since the mail server itself is the one actually sending the email. All CF needs to know is which machine to pass the mail to so it can be sent.
>
> I may have a misunderstanding of how things work, but CF isn't a mail server, it just connects to one and lets it do its job, right?

I got to thinking about this and I wanted to be sure - so I ran a test. Here's what I found.

The Test

I set up a test by sending 2 mail messages through the same relay. One I sent using the IP address and the other using a fully qualified domain name. Both were exactly the same.

```
<cfmail from="*muse email*"
        to="*muse email*"
            subject="test from ip address"
            server="10.4.2.18">
This message comes from the IP address relay.

</cfmail>

<cfmail from="*muse email*"
        to="*muse email*"
            subject="test from ip address"
            server="internalrelay.cfwebtools.com">
This message comes from the FLQDN relay.

</cfmail>
```

When the 2 emails arrived I took some time to examine the headers of each of them. I wanted to see if that IP address shows up anywhere in the header information. I suspect that Eric is right and that the email server reports it's own FLQDN, but that doesn't mean the IP doesn't show up right? And if it shows up anywhere I'm guessing it's a tipoff to a spam filter some how. Here are the 2 headers (with some stuff removed):

Sent Via IP Address

```
1: Authentication-Results: ...
2: DomainKey-Status: ...
3: Authentication-Results: ...
4: Return-Path:
5: Received: from internalrelay.cfwebtools.com [10.4.2.18]
6:  by mail.cfwebtools.com with SMTP;
7:    ...
8: Received: from web-dev3.cfwebtools.com (web-dev3 [10.4.2.211])
9:  by internalrelay (8.13.1/8.13.8) with ESMTP id n1DK4tKs028292
10:  for; Fri, 13 Feb 2009 14:04:55 -0600
11: Date: Fri, 13 Feb 2009 14:04:55 -0600 (CST)
12: From: *muse email*
13: To:   *muse email*
14: Message-ID:
15: Subject: test from ip address
16: MIME-Version: 1.0
17: Content-Type: text/plain; charset=UTF-8
18: Content-Transfer-Encoding: 7bit
19: X-Mailer: ColdFusion 8 Application Server
```

Hmmm... it looks as if Eric is correct. The mail server identied itself as "internalrelay" on lines 5 and line 9. So yes, the relay server is writing into the header the information to correctly identify the origin. But take a look at line 14.

```
14: Message-ID:
```

Perhaps what Declude is clued into is the messageID (a sort of unique signature used by mail servers). The message ID seems to source the message by the IP address of the mail server instead of its FLQDN. If I examine the other message - the one sent using the FLQDN - I'm betting that line will look different, right?

Sent Via FLQDN

```
1: Authentication-Results: ...
2: DomainKey-Status: ...
3: Authentication-Results: ...
4: Return-Path:
5: Received: from internalrelay.cfwebtools.com [10.4.2.18]
6:  by mail.cfwebtools.com with SMTP;
```

```
7:    ...
8: Received: from web-dev3.cfwebtools.com (web-dev3 [10.4.2.211])
9:  by internalrelay(8.13.1/8.13.8) with ESMTP id n1DK4tKs028292
10:  for; Fri, 13 Feb 2009 14:04:55 -0600
11: Date: Fri, 13 Feb 2009 14:04:55 -0600 (CST)
12: From: *muse email*
13: To:   *muse email*
14: Message-ID:
15: Subject: test from ip address
16: MIME-Version: 1.0
17: Content-Type: text/plain; charset=UTF-8
18: Content-Transfer-Encoding: 7bit
19: X-Mailer: ColdFusion 8 Application Server
```

Huh? Even though I was prepared to see a FLQDN in the message ID, I have to say this is *not what I expected*. What I had expected to see was "*unique signature*@internalrelay.cfwebtools.com". Instead, the signature actually shows the FLQDN of the server where the message *originated*. In other words, the web server. Somehow, specifying the domain of the server I was relaying through caused that server to reassign my message ID domain to be the FLQDN of the server which was making contact. It's more information to be sure and I can understand why Declude might see it as more legit since so much spam relays through agents on desktops and TOR etc. Still, it came as a surprise.

Now since this is news to me I would love for some savvy Muse Readers to set me straight on what is actually going on here. If you have a clue please fire away.