HOW-TO – SETUP ASSP WITH IBM LOTUS DOMINO

This HOW-TO is provided free (as in speech) and without warrantee. If you follow these directions, you are solely responsible for the results. I recommend you stop now. Do not even read the rest of this document. If you do read more, and you follow these directions – perfectly or not – and things go wrong, it is your fault not mine. If you break something by following these directions, you own all the pieces. You may not sue me, because I'm telling you right now that these instructions are just a theory and you should not actually use them.

WHO AM I, AND WHY AM I WRITING THIS?

I'm a Lotus Domino Zealot, and the President of Northern Collaborative Technologies. I make my living using Lotus Domino to save companies a ton of money on workflow systems and secure extranets. I'm writing this because I like the product and I know a lot of Domino Administrators really feel abandoned in the antispam market simply because a big product like Domino cannot change fast enough to keep up with the spammers.

http://www.thenorth.com

http://www.thenorth.com/apblog

WHAT IS ASSP

ASSP (http://assp.sourceforge.net) is essentially just an SMTP proxy that does some really great in-line processing to block inbound spam and viruses as they're being transmitted. The first of two big wins here, are that it ends up being almost totally vendor neutral because it happens at the protocol layer before the mail servers get the message and do proprietary things with it. The second is that because the denial happens during the connection, legitimate users who sends you mail that is mistakenly classified as spam and thus denied will get a report from their own server indicating that the message didn't go through, while at the same time your Domino server isn't stuck spending its time sending bounce reports to users that don't really exist.

WHY RUN IT ON DOMINO?

Domino is an incredibly powerful tool and its messaging really is state of the art for enterprise scale mail systems. I don't want to make this a marketing document for IBM or argue with Microsoft people about Exchange –suffice it to say that depending on what day you read the analyst reports and which reports you choose to believe, IBM Lotus Domino has about half the corporate mail users in the world, with MS having about the other half. In the US, it's very close to even and in Europe and Asia Domino is ahead by some percentage points. You can disagree or choose different reports – it doesn't matter. There are well over 120 million people who use it so believing it to be number one or number two makes no difference. It's a good product and it is not going away.

The downside to being so big and widely adopted is that you can't make quick changes. Domino is pretty good about blocking obvious spam, but beyond that you need a third party tool. I believe ASSP serves that role very well for the small to medium sized companies. I'm not yet convinced that it will scale well enough to handle a fortune 1000 company—but who cares? They have other solutions and funds to spend on them.

WHAT ABOUT SPAMJAM?

SpamJam (http://www.gsw.com) rocks when it comes to end-users interacting with their spam. Its biggest advantage is that users feel comfortable about getting back messages that were blocked,

and its reporting and retrieval tools help sell the idea of blocking messages to corporate users. On the back end, I don't find it to be quite as effective as ASSP.

The best case, in my opinion, is to use ASSP at the front end set in "test" mode for questionable mail so that it does the job but instead of blocking those questionable emails it marks them and then SpamJam can pick those marks up and do its thing with users.

OVERVIEW – WHAT WE'RE ACCOMPLISHING WITH THIS SETUP

For ASSP to work right, it needs to do two things. First, it needs to be the front end, listening on port 25 for inbound SMTP connections and acting as a pass-through proxy for those connections so that it can process the inbound mail as it goes to your server. Next, it needs to be the first outbound relay point for your mail so that it can keep track of who you send mail to, thus building a "whitelist" of people who are already corresponding with you – these are very likely to be non-spam.

To accomplish this, we need three things. First, we need ASSP to be the inbound SMTP listener on port 25. Next, we need Domino to listen for SMTP on some other port, and we need to tell ASSP to use that other port to pass the message along to Domino. If you're using separate machines, you can leave the ports alone and just change your MX records but that's not how I did it so it is not how I'm writing this document. Finally, since ASSP isn't really an outbound MTA and we don't want to tie up Domino doing that through ASSP (if that even works), we need an outbound SMTP relay.

The result of all this is that inbound mail hits ASSP, which acts as a filtering proxy to Domino. If its spam, ASSP severs the connection, otherwise the message passes through ASSP to Domino which delivers the message. On the outbound side, Domino relays the SMTP mail to ASSP which grabs all the addressee data from it and uses it to update the white list, then hands off the message to your outbound SMTP relay for transfer to the intended recipient.

Sure, its sounds complicated, but it is not too bad once you get to know it. Its not like you have to write the stuff yourself after all.

NOTE: You'll see we're doing SMTP internally on this machine on ports 125, 325, and 425 for various things. Make sure you firewall this machine so those ports are blocked for everyone else. You don't want someone exploiting those as relay points.

MAKE SURE PERL IS INSTALLED AND YOU'VE ADDED ANY MISSING MODULES

I'm running my Domino server on Fedora Core 3 Linux, and it came with Perl already installed. If you don't have Perl, go get it and install it. It's available for Windows as well. You should also make sure you install the additional modules to use all the features of ASSP. On my machine, I had to install the following additional modules: NET::DNS, NET::CIDR::Lite, Mail::Address, Sys::Hostname::Long, Mail::SPF::Query, and Email::Valid. These were available from http://search.cpan.org/~maurice/ . Each one had a README file and installation wasn't hard at all.

INSTALL AN OUTBOUND SMTP RELAY SERVER IF YOU DO NOT ALREADY HAVE ONE

NOTE: You'll see we're doing SMTP internally on this machine on ports 125, 325, and 425 for various things. Make sure you firewall this machine so those ports are blocked for everyone else. You don't want someone exploiting those as relay points.

ASSP needs to see the mail as it goes out to build its white lists, but it is not an MTA and you don't want to make Domino do that. On my machine, I just configured SENDMAIL to do this job. I changed its port to 425 from 25 so that it wouldn't interfere with ASSP, and I configured it to send all local mail traffic to 127.0.0.1:25 (where ASSP is listening). You can do this on Windows even using Microsoft's SMTP task or find some other one. You could even configure another Domino server to do this and allow relaying on that server. Its overkill, but it would work.

So, to review – I've set up SENDMAIL to listen on port 425 instead of 25, and to forward all local traffic to 127.0.0.1:25 where ASSP is listening and can pass it through to Domino.

INSTALL ASSP ACCORDING TO ITS INSTRUCTIONS

Follow the regular destructions for installing ASSP. It is not hard, just run the Perl script and connect to it with a web browser on port 55555. Change the password or you're an idiot who deserves to have all your mail routed to your competitors. When you start it up, configure it according to the settings below.

USE THE FOLLOWING ASSP SETTINGS IN ADDITION TO ANY OF YOUR OWN

NOTE: You'll see we're doing SMTP internally on this machine on ports 125, 325, and 425 for various things. Make sure you firewall this machine so those ports are blocked for everyone else. You don't want someone exploiting those as relay points.

Network Setup: SMTP Destination: 127.0.0.1:125 -- in my case, I'm using port 125 on my Domino server to listen for SMTP traffic now. Since my Domino server is actually partitioned, I used the IP address of that partition instead of just localhost, but you get the idea. This is where ASSP will connect to pass through the inbound SMTP connections. Your Domino server has to be there. If you're using separate boxes, you could just use the IP of that box and leave the Domino sever on port 25, but make sure to not allow yourself to be a relay.

Relaying: ISP/Secondary MX Servers: 127.0.0.1|nn.nn.nn.nn|… This is a pipe separated list of all the IP addresses on this box. If you're using multiple boxes, put those addresses here.

Relaying: Accept All Mail: 127.0.0.1|nn.nn.nn.nn|… This is a pipe separated list of all the IP addresses on this box. If you're using multiple boxes, put those addresses here.

Relaying: Relay Host: 127.0.0.1:425 -- Notice the 425 there? This is the IP and Port of my outbound SMTP relay host. In my case, the sendmail I configured earlier. If you have another relay host, put it here. This is were outbound mail will go after Domino hands it to ASSP.

Relaying: Relay Port: 127.0.0.1:325 -- This is where ASSP will listen for mail from your Domino server before it gets passed off to your relay server. This is what you tell Domino is your outbound relay host. Mail comes from Domino to here, then goes to the outbound relay host.

MAKE THE FOLLOWING CHANGES TO YOUR DOMINO SERVER'S MAIL SETUP

NOTE: You'll see we're doing SMTP internally on this machine on ports 125, 325, and 425 for various things. Make sure you firewall this machine so those ports are blocked for everyone else. You don't want someone exploiting those as relay points.

On your configurations document (not the server document, this is separate from that) you need to change the following:

1. Router/SMTP: Basics: Relay host for messages leaving the local internet domain: 127.0.0.1:325 – this matches what you put in on the ASSP configuration for its "Relaying: Relay Port".

2. Router/SMTP: Advanced: Commands and Extensions: Turn off "Pipelining" for outbound messages. This causes problems in this situation – I have no idea why and don't really care.

On your server document itself, change the following:

1. Ports: Internet Ports: Mail: Outbound SMTP – set this to 325, which is what I told ASSP to listen for mail from Domino on.

2. Ports: Internet Ports: Mail: Inbound SMTP – set this to 125, which is what I told ASSP to send mail to Domino on.

Of course, make sure everything else about your Domino server is set correctly so you're not a relay. Don't find yourself on an RBL. Its painful.

MAKE SURE ALL YOUR OUTBOUND SMTP MAIL ROUTES THROUGH THIS ONE SERVER

This is really a who different topic, but its critical in this case because all your outbound messages have to go through this or your white lists wont be any good and you'll end up with more false positives than you need. Here are instructions:

http://www.thenorth.com/apblog4.nsf/0/67623CFC361554FB85256FCE006B5EE0

Follow those directions so your mail routes properly, please!

START IT UP AND TELL YOUR USERS TO REJOICE!

If you've followed these directions, it should work. If it doesn't – start hacking on it. It works for me. Read the rest of the instructions for ASSP and configure it to do what you want. It's a good tool, but you'd better set it up right.

ADDITIONAL SETUP I'VE DONE TO MAKE LIFE EASIER FOR ME

In addition to the items described above to "get it working", I've done a few things to make my installation just so much sweeter. Primarily, I've set ASSP to use "test mode" for mail that fails "Bayesian" filtering. That is the most likely to be a false positive. It is really good, but not perfect. I've set it so ASSP puts a header indicating the spam likelihood on the message. I've also had it put [PossibleSpam] in the subject line.

In my mail file, I've created a rule that says if the subject line starts with [PossibleSpam] then put the message in a folder called "NCTSPAM".

Also in my mail file, I've created an on-delivery agent which on each delivered message. If the subject starts with "[PossibleSpam]" it gets marked as if I've already read the message. That keeps my new mail icon quiet. Also, if the spam probability is less than 90%, I put the message back in my inbox. It is still marked as read, but its there for my attention. Very few end up that way.

If you're paying attention, you realize that these "possible" spam messages are now out of my inbox and marked as read. They're easy for me to find, but otherwise out of the way. Sometimes I scan through them to see if I've missed something. Often if I subscribe to something new, or buy something from a new site, the mail ends up in that folder. Fine, that's easy to deal with.

Here's the code I'm using:

```
Sub Initialize

        On Error Goto errorHandle
        Dim session As New notessession
        Dim thisDb As NotesDatabase
        Dim thisDoc As NotesDocument
        Set thisdb = session.CurrentDatabase
        Set thisdoc = session.DocumentContext
        If thisdoc.hasitem("X_Assp_Spam_Prob") Then
                Dim s As String
                Dim i As notesitem
                Dim n As Double
                Set i = thisdoc.getfirstitem("X_Assp_Spam_Prob")
                s = i.text
                n = Cdbl(s)
                thisdoc.spamprob = s
                thisdoc.spampct = n
                Call thisdoc.save(True, False, True)
                If n < 0.9 Then thisdoc.PutInFolder("($Inbox)")
        End If
done:
        Exit Sub
errorHandle:
        Print "Error handling document mail delivery"
        Resume done
End Sub
```