

## Securing Exchange checklist:

Before we began securing the Exchange environment we insure that the servers have a secured windows 2003 server environment first. To do so you must do the two following below.

1<sup>st</sup> Deploy the domain, domain controller, and member server baseline policy templates throughout the forest.

2<sup>nd</sup>. Deploy the exchange domain controller baseline policy templates (exchange\_2003-DC\_Incremental\_V1\_1.inf) to all domain controllers in the organization.. This allows exchange to operate in a secured environment.

To create the GPO and import the exchange domain controller policy template you will have to go in the active directory users and computers, right click domain controllers and properties. In group policy go to new and add new policy object. Title it Exchange DC Policy and enter. Edit, in computer configuration, right click the security setting and click import policy. Now go to the exchange 2003 import file and run the import. After this close and go to the domain controllers properties and select exchange dc policy. Click up till the DC policy is at the top and click apply and ok. Now wait for the replication to take once it does you can go to the event log and look for the Scecli 1704 log then verify communication to each DC.

## Exchange server

To secure the exchange server some services will need to be disabled. Below are the following ones:

Microsoft exchange IMap4  
Microsoft exchange Pop3  
Microsoft Search  
Microsoft exchange event  
Microsoft Exchange site replication service  
NNTP

However the HTTP SSL will need to be setup as a manual service

For front end services security the same processes will be disabled along with the following;

Microsoft exchange information store  
Exchange MTA stacks  
System attendant  
Exchange routing engine  
IIS admin service  
SMTP  
WWW publishing service

In doing these steps this will assist in a more secure mail services to our network clients both inside and outside of our facility.



Other steps that have been implemented have been:

Using patch management to help assist in making sure all security updates occur and are implemented to the exchange server

Setting up antivirus and spam blockers through third party software such as Norton antivirus.

Finally once everything is setup and functional our next step is to always educate our users. Hold a mandatory class once every two weeks going over security policies within the NSF organization is an ideal schedule. This way if new employees come into the company there won't be a missed opportunity to educate them as quickly as possible.

