



Oregon

State Data Center

Email Hub Replacement Technical Forum

Presented by: Bill Donaldson, SDC Security

Date: August 14, 2008



Why Are We Here?

Directory synchronization and email transport is working well but...

- A significant increase in email volume could impact email flow (again)
- The dirsync process is varied and running on an old application and on non-SDC-standard hardware/OS
- Email and dirsync issues are difficult to trouble-shoot





Agenda

- Project Goals
- Email Directory Synchronization
 - Current process
 - Future process
- Central Email Infrastructure
 - Current environment
 - Future environment
- Implementation Plan
- Questions and Answers





Project Goals – What Are We Looking For?

- Scalable – email processing power and filtering features to handle increases in email volume
- Secure – increased anti-virus protection
- Simple – use standard methods and protocols for global address book updates to / from agencies
- Supportable – give more agency control and ease trouble-shooting



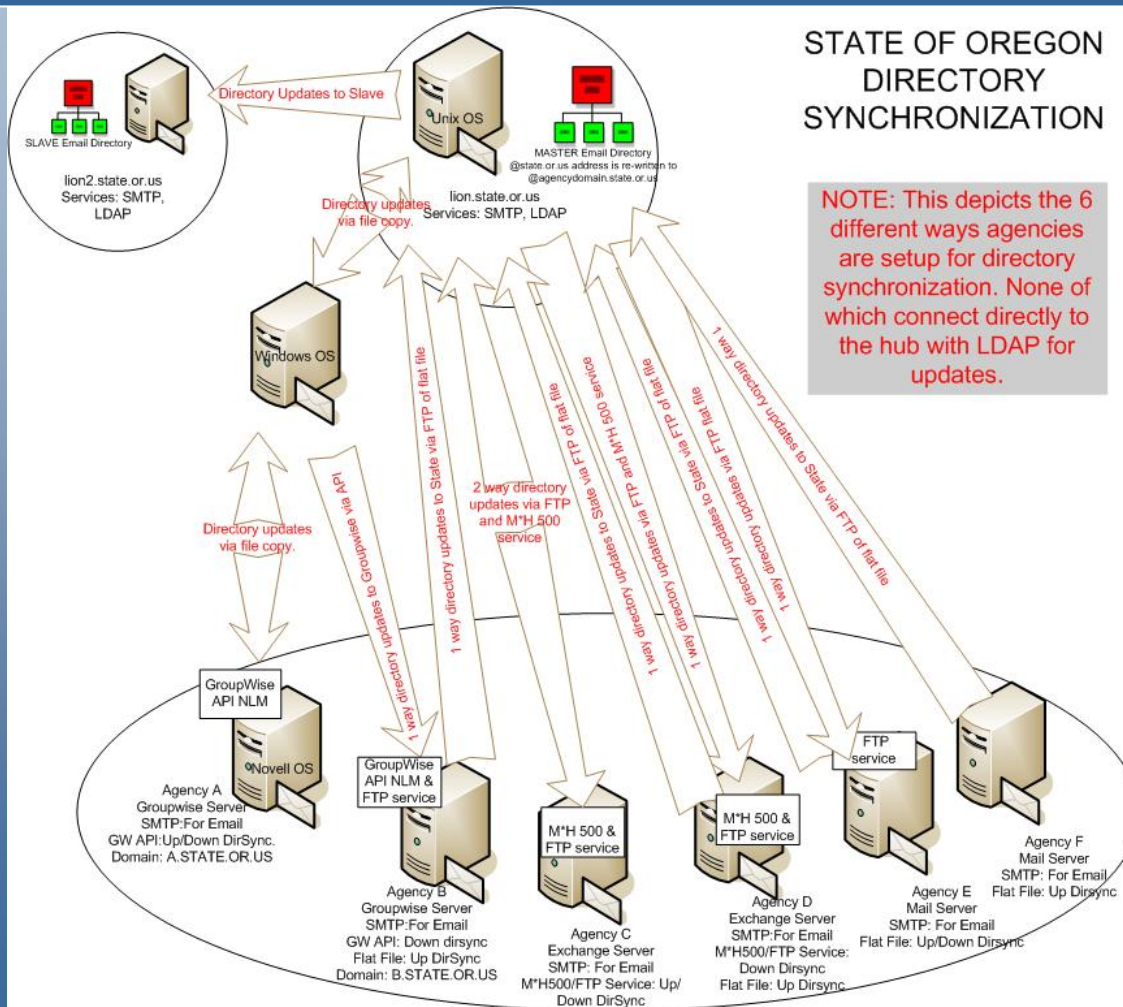


Email Directory Synchronization Replacement

- Standardize the process across agencies
- Provide as much agency control as possible



Current Directory Synchronization





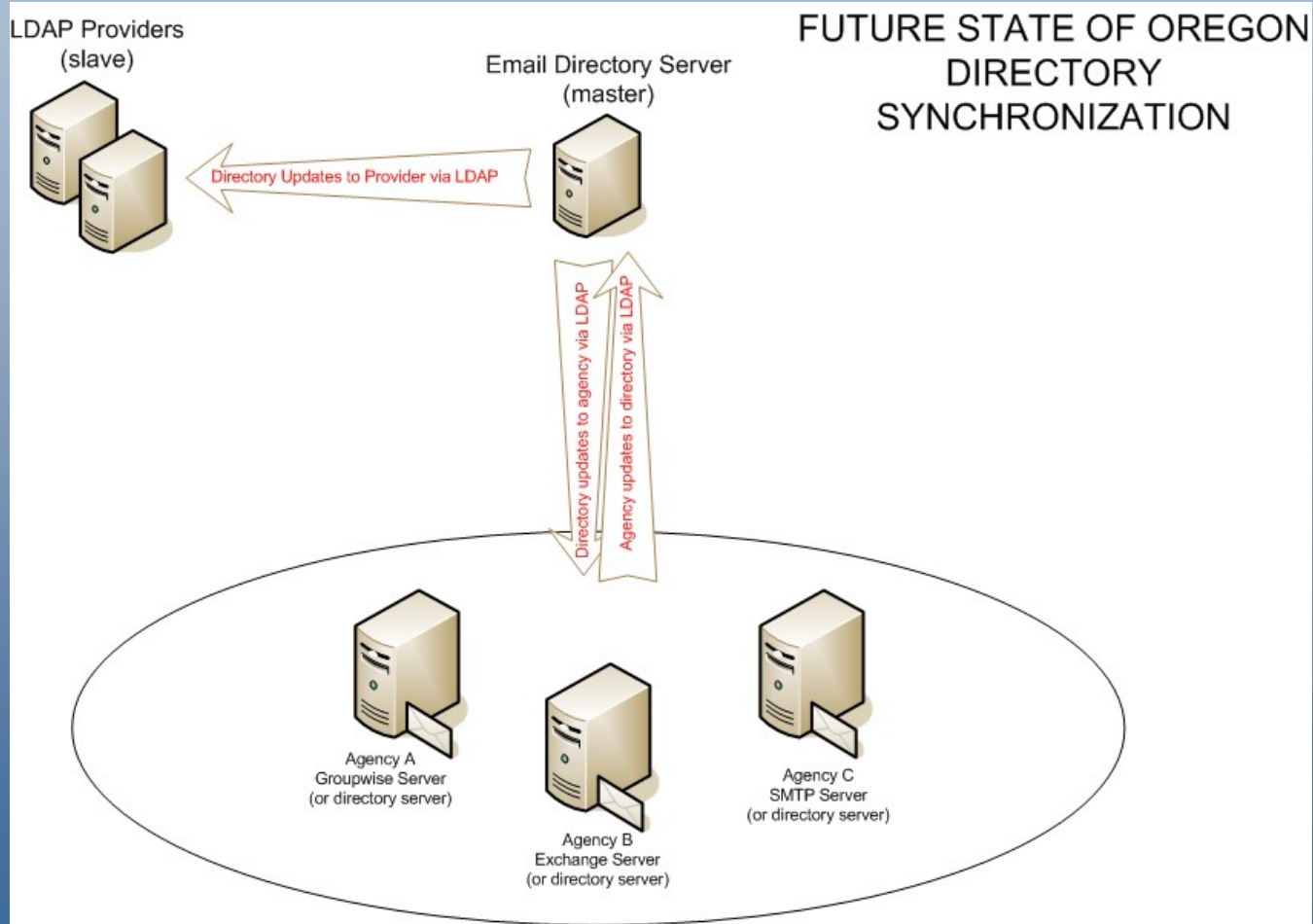
Directory Synchronization Enabling Technologies


- Email directory synchronization tool
 - Contracted application development
 - Standard synchronization process
- LDAP provider
 - LAMP stack (Linux, Apache, MySQL, PHP)
 - OpenLDAP





Future Directory Synchronization



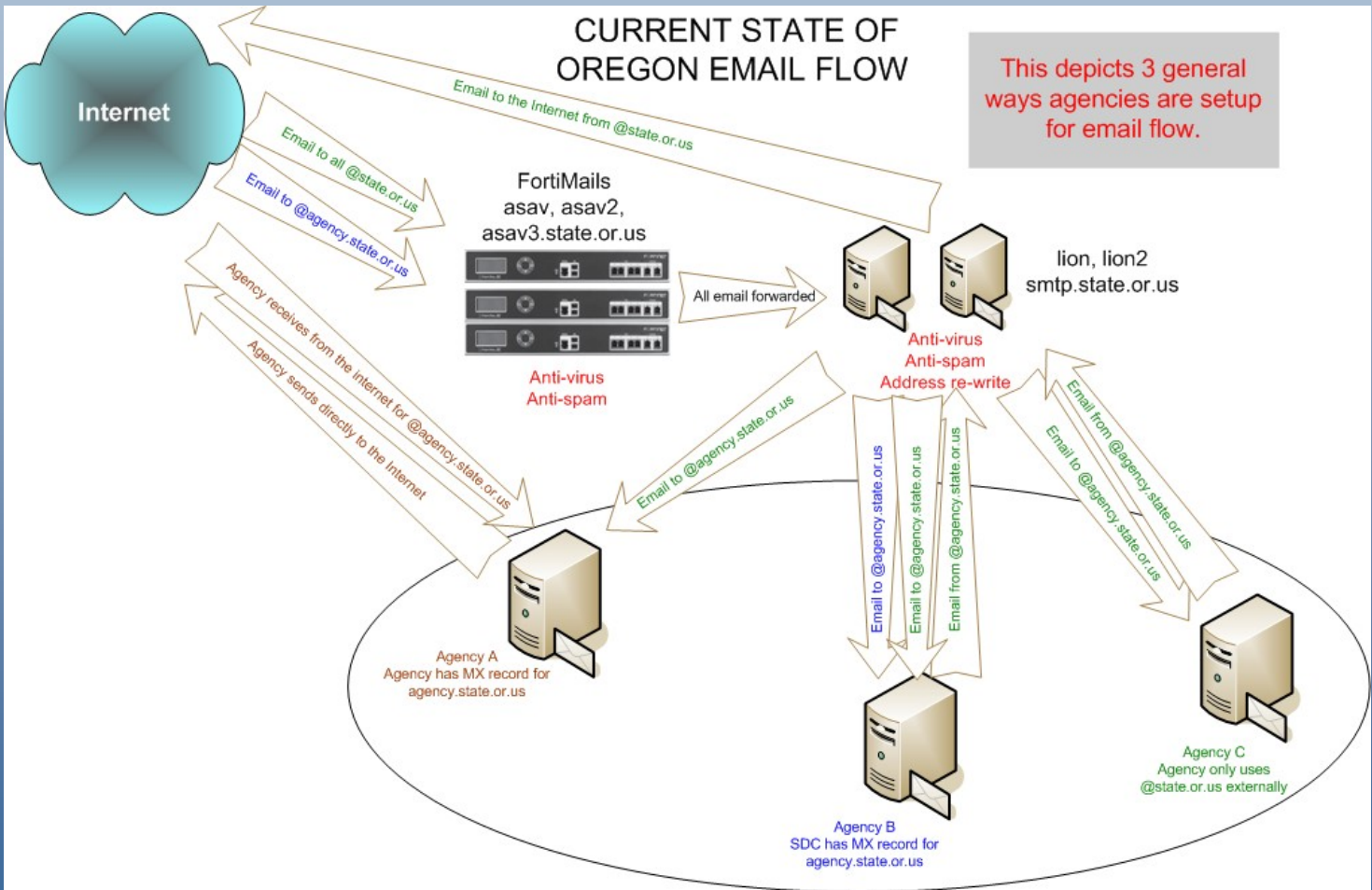


Current Central Email Infrastructure

- Hardware
 - Two Sun Solaris servers (lion and lion2)
 - Three Email Firewalls (FortiMail)
- Software
 - An old application (Mail*Hub) that will be end of support by February 2009
- Processing
 - Currently processing approximately 10 million emails / day



Current Environment: Email Flow





Email Hub Enabling Technologies

- FortiGate 3810A security device
 - Email filtering and network anti-virus
- FortiMail 2000A email firewall
 - Email routing, filtering, anti-virus
- FortiAnalyzer 4000A manager
 - Central logging, reporting, and quarantining
- LDAP provider





FortiGate 3810A



- Transparent mode
- Anti-Virus
 - signature-based and heuristic detection of virus and spyware
 - Only enabled for agency HTTP, FTP traffic
- Email firewall
 - Block known-bad senders (DNSBL)
- High Availability - Failover





FortiMail 2000A



- Email firewall
 - SURBL to check URIs in an email
 - Sender Reputation
 - Available: dictionary, image, greylist, Bayesian, black/white listing, etc.
 - Messages marked as spam are quarantined
- Anti-Virus
 - Signature-based and heuristic detection of virus and spyware
- High Availability - cluster





FortiAnalyzer 4000A



- Central Quarantine
 - Central location to quarantine email from multiple email filters (FortiGates/FortiMails)
 - Agency/user can release quarantined email
- Log Analysis, Reporting and Archiving
 - Track fate of an email more easily when using multiple email filters (FortiGates/FortiMails)
 - Summary reports on email actions, senders, volume, quarantining, etc.



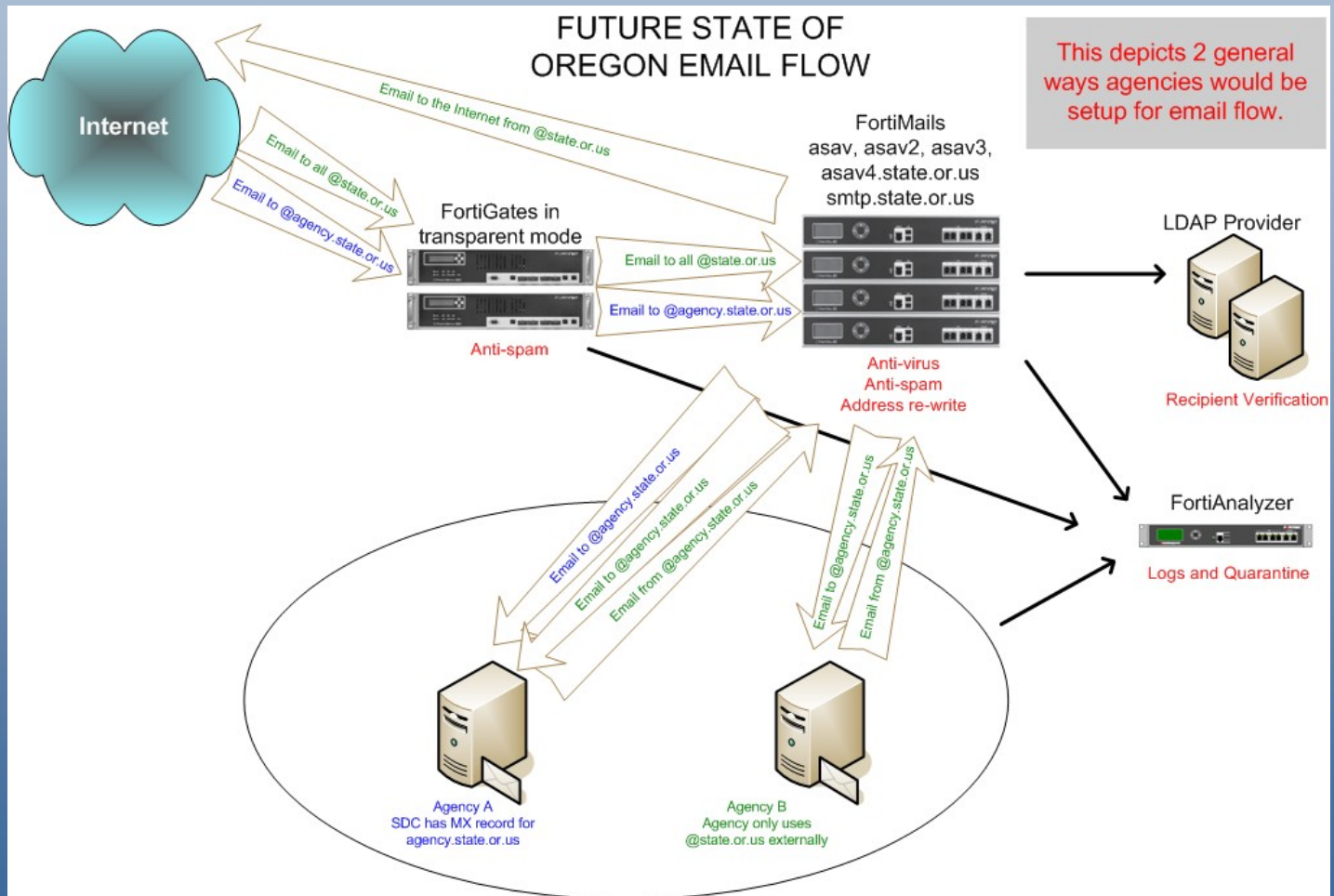


LDAP Provider

- LAMP stack
- OpenLDAP
- Directory of valid email recipients for the central email infrastructure
 - Email address re-writing
 - Sender reputation more efficient
 - Quarantining more efficient
- High Availability - cluster



New Environment –





Management Features for Agency Email Administrators

- Email directory updates
 - Conflicts
 - Manual / automatic updates
- Anti-Spam Options
 - Dictionary
 - Image
 - Greylist
 - Bayesian
 - Black/white listing
- Manage quarantined email





Implementation Plan

- Phase 1
 - Dirsync Replacement
- Phase 2
 - LDAP provider
- Phase 3
 - Fortinet assistance
- Can be simultaneous – although there are some dependencies





Implementation – DirSync Replacement

- Contractor to start early September
- Requirements gathering with agencies
- Build custom application
- Integrate with
 - lion, lion2
 - LDAP provider
- Pilot / Test with a few Agencies





Implementation – LDAP Provider

- Clean-up of Aliases on lion
- Identifying all uses of lion's LDAP directory
- Configuration
 - 2 prod and 1 dev
- Test





Implementation - Fortinet

- Test and implement
 - FortiGates
 - FortiMails
 - FortiAnalyzer
- Upgrade and cluster old FortiMails with new ones
- Fortinet onsite mid-September





Implementation – Complete....

- Bring in remaining agencies after testing and pilots
- All email flowing through the new architecture
- Decommission lion and lion2





Agency Interaction

- Workshops
 - Microsoft Exchange
 - September 9th
 - Novell GroupWise
 - September 10th
 - Others
 - September 22nd
- Pilots / Testing



Questions?

Contacts:

Marshall Wells

Bill Donaldson

Carol Johnson



Q&A – Email Hub Replacement

8/14/08

Q: Will the agencies see a dramatic increase in spam filtering after the FortiGate is implemented?

A: No – we are trying to offload the filtering from the FortiMails so they can do more. The FortiMails have a lot of anti-spam features that we are planning to push down to the agencies for management.

Q: Are we going to increase the blacklist services?

A: We currently use Fortinet's service to identify known bad senders. We may add more but this does add more complexity in troubleshooting problems and getting addresses/sites removed promptly if needed.

Q: How do we deal with servers that have been blacklisted, but at times do send valid emails? Are they going to be able to manage the blacklists to manage this?

A: We are looking into the level of management that the agencies can have to manage blacklists. We typically will get a site removed within 24 hours. However, if a network/domain has machines within it sending spam, they will usually be blacklisted again. Then the process will have to be repeated. The best answer is for the problem itself of sending spam to be dealt with by the entity.

Q: Who do we actually use for blacklists?

A: Fortinet. The Fortinet list is a combined list that they have put together from their international offices.

Q: Does FortiMail have an option for anti-spoofing?

A: Yes – there is an option for anti-spoofing that will be available to the agencies.

Q: If we give the agencies the capability of adding / subtracting to the blacklist does it just impact that agency?

A: If you are removing yourself from the blacklist – it is just an impact to you. We do have whitelists for senders / receivers that are agency specific available now. That option will continue.

Q: What is the difference between the FortiGate anti-spam and the FortiMail anti-spam?

A: The FortiGates will only block known bad senders. The FortiMails will inspect the content of the messages and is also where the agencies can customize the feature sets.

Q: Will ftp services within the SDC be running through the FortiGates?

A: No

Q: Will agencies be able to see what is being dropped at the FortiGates?

A: With the FortiAnalyzer, yes.

Q&A – Email Hub Replacement

8/14/08

Q: Does the FortiMail have the ability to set up an email where you can forward ham / spam (i.e.: spam@state.or.us) for learning and heuristic scanning.

A: There is an option for Bayesian scanning for learning. As the project progresses we will be working with our test domain and pilot agencies to see which features can be managed by agencies. This feature would be one of those being addressed.

Q: Does it have the ability to scan for different languages / special characters?

A: Yes – and we hope to push that to the agency level.

Q: How are the agencies going to interface with the FortiMails?

A: It is web-based. Training sessions will be scheduled with our customers (Train the trainer approach).

Q: How long is the quarantined spam currently retained?

A: 1 week - which approaches a Terabyte of storage at this time. Most of them are just invalid state email address emails.

Q: Does the quarantine give the end-user the ability to release quarantined mail?

A: Yes, it has the capability for that specific user. We believe this will be an option that can be chosen at the agency level too.

Q: Will the agencies be able to manage the quarantine options by agency?

A: Yes, although there will be some variations to this, such as the amount of time we can quarantine. This could take disk space needs to an unrealistic level.

Q: Do the FortiGates log to the FortiAnalyzer also?

A: Yes

Q: The change to outbound email flow to go through the FortiMail devices instead of straight out to the internet does what?

A: Allows us to help eliminate internal devices from sending spam and/or virus' outbound. The devices would still be able to send to the user@agency.state.or.us email addresses.

Q: Are we going to allow exceptions to that?

A: We will have a process for reviewing exception requests. Our intent is to meet agency business needs while also working to better control outbound viruses and SPAM in order to improve the reputation of the state in regard to email.

Q: A TLS tunnel from agency to the mail hub and then out – will that still continue?

A: Yes

Q&A – Email Hub Replacement

8/14/08

Q: If you are an SDC agency – will you be involved in the appliance pilots as they are brought up?

A: Yes, on a volunteer basis.

Q: Do we have any timelines?

A: We hope to have it done by end of the year

Q: Is Feb 09 a drop dead date because of the support?

A: Yes. Although the functionality will not cease at that time, only our ability to utilize support options.

Q: Some of the agencies MX records are pointed to the agency's mail server. Do we have the ability to point an MX record to the FortiMails?

A: Yes – we are currently doing that for most agencies.

Q: How much extra mail will we be receiving from agencies that have their own email servers?

A: There aren't a lot of other agencies that have their MX records pointing to their own servers. There would be an increase but it is not expected to be significant in regards to our capacity planning.

Q: ODOT has their own MX record – when do we see them being moved over to the FortiMails?

A: This will be completely coordinated with each agency, but because the agency has the control over the features on the FortiMails – they would go through the devices and just not turn any features on.

Q: What is the benefit to the agency?

A: For agencies that currently host their own MX record, email can arrive from two different paths. One would be direct from the Internet if the sender uses the user@agency.state.or.us in addressing. The other path would be through the FortiMails if the sender uses an address without specifying the agency (user@state.or.us). Moving the MX record to the FortiMails would create a single path and provide the ability to better troubleshoot email issues.

Another benefit would be that the agency does not necessarily need to keep increasing their capacity to handle the increase in SPAM volume as we are doing that. Also, the agency can restrict outside access to their email servers, only allowing the FortiMails to talk to them, which reduces risk.

Q: Are the agencies going to be charged for the spam filtering even if they aren't using it?

A: There isn't a rate for enterprise mail management, so you shouldn't see one. Also – the cost for the anti-spam on these devices is not a per user cost, but a per device cost.

Q&A – Email Hub Replacement

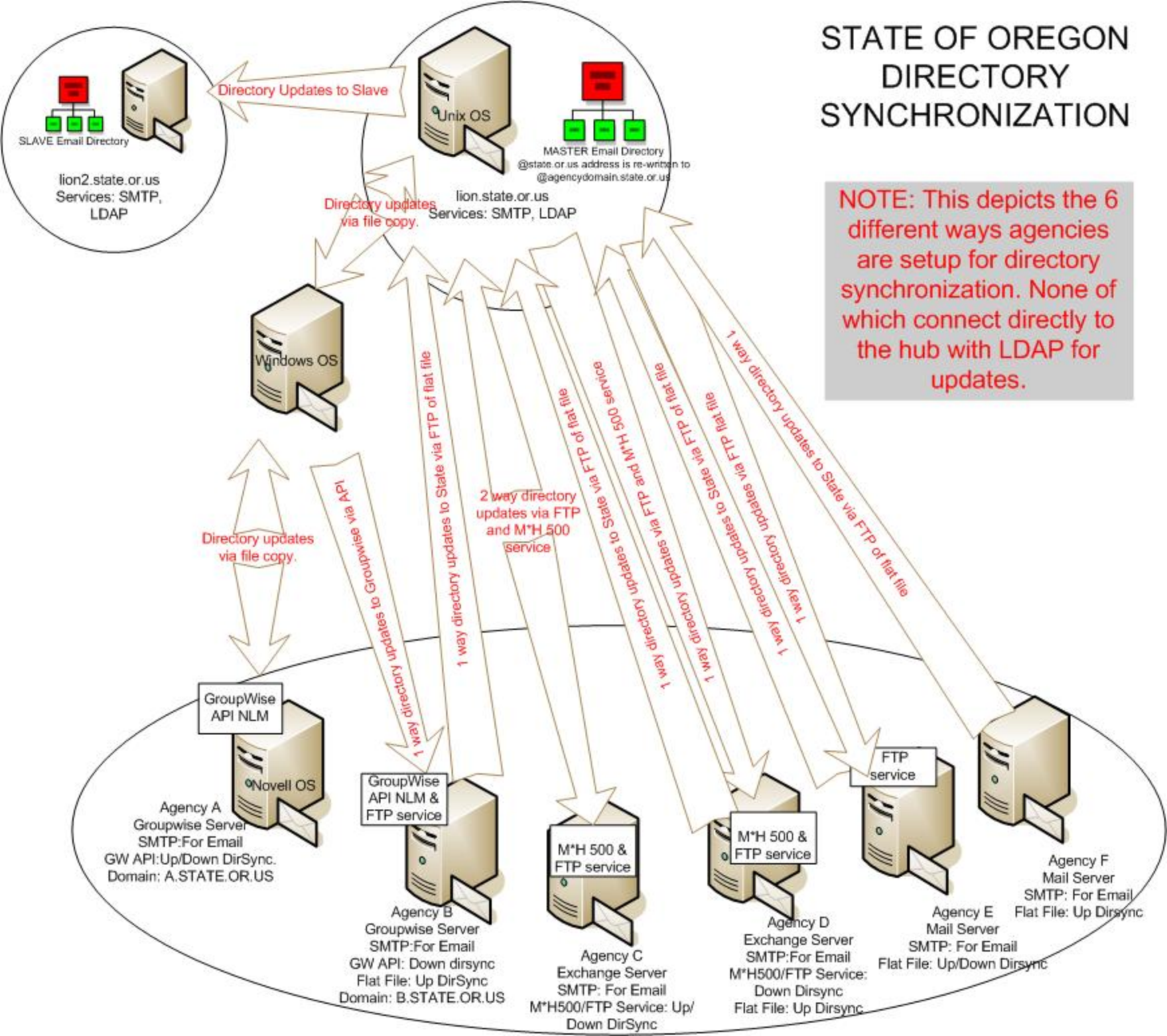
8/14/08

Q: Does the anti-spam on the current FortiMails work the way the new ones will? (Customizing the feature set).

A: We currently don't have the ability to customize it on the FortiMails at an agency level per se. We will with the new infrastructure.

STATE OF OREGON DIRECTORY SYNCHRONIZATION

NOTE: This depicts the 6 different ways agencies are setup for directory synchronization. None of which connect directly to the hub with LDAP for updates.



LDAP Providers
(slave)



Email Directory Server
(master)

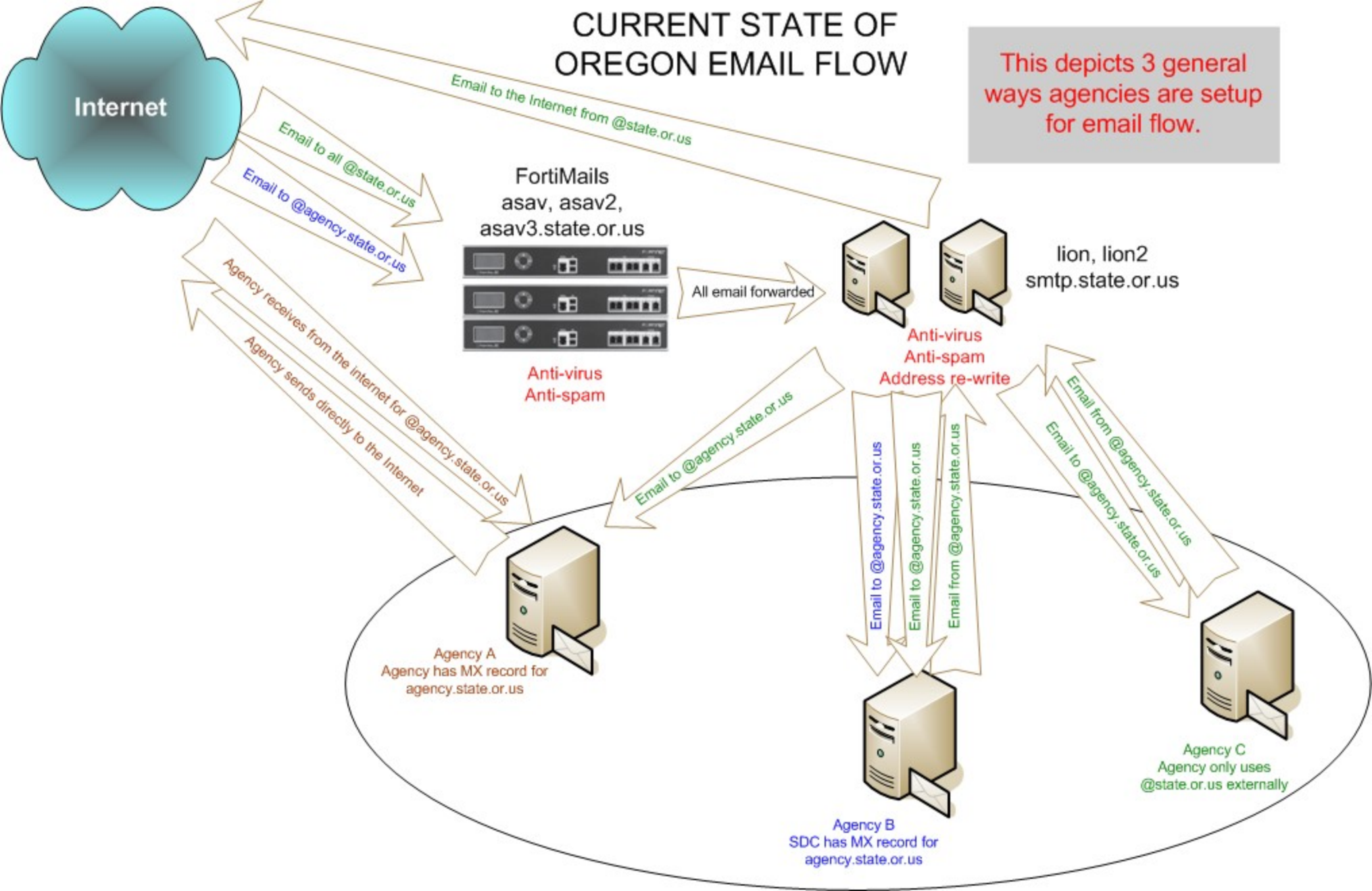


FUTURE STATE OF OREGON DIRECTORY SYNCHRONIZATION



CURRENT STATE OF OREGON EMAIL FLOW

This depicts 3 general ways agencies are setup for email flow.



Internet

Email to the Internet from @state.or.us

Email to all @state.or.us

Email to @agency.state.or.us

FortiMails
asav, asav2,
asav3.state.or.us



Anti-virus
Anti-spam

All email forwarded



lion, lion2
smtp.state.or.us

Anti-virus
Anti-spam
Address re-write

Agency receives from the internet for @agency.state.or.us

Agency sends directly to the Internet

Email to @agency.state.or.us

Email to @agency.state.or.us

Email to @agency.state.or.us

Email to @agency.state.or.us

Email from @agency.state.or.us

Email from @agency.state.or.us

Email to @agency.state.or.us

Agency A
Agency has MX record for
agency.state.or.us



Agency B
SDC has MX record for
agency.state.or.us



Agency C
Agency only uses
@state.or.us externally



FUTURE STATE OF OREGON EMAIL FLOW

