Introduction to Sendmail for Firewalls

1

Sendmail Configs Needed

- Firewall
  - Must know to send mail for user@mumble.com to mailhub inside
  - Everything else goes out
- Mailhub
  - Must know to send mail for user@*anything-but*-mumble.com to firewall
  - Must accept mail for user@mumble.com

2

Sendmail Configs *(cont)*

- Other systems inside
  - Must send mail not for user@anything.mumble.com to mailhub

3

Sendmail Syntax

- Sendmail uses ***tabs*** as delimeters
  - Converting tabs to spaces can really mess you up!
  - Cut and paste via X-windows expands tabs! Be careful!
- Syntax designed to make it easy for computer to parse
  - Not for human

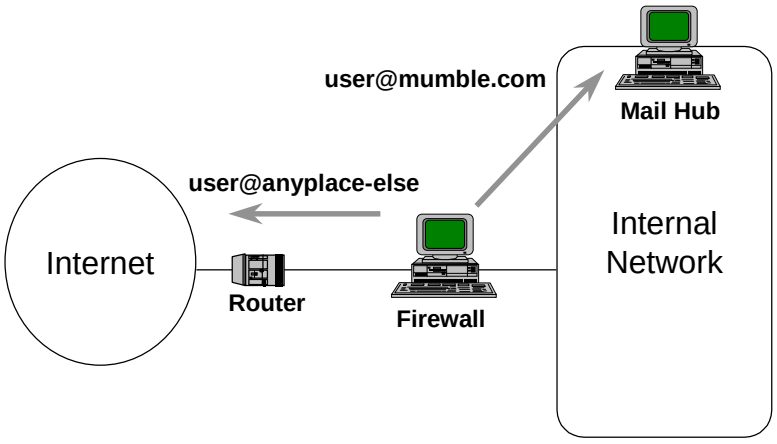
4

Sendmail Syntax *(cont)*

- Rules all have a left-hand-side and a right-hand-side
- Patterns match on left-hand-side product a rewrite to the right-hand-side
- This is dramatically oversimplified
  - If you need to do a lot with sendmail buy a book on the topic

5

This is easy! ☺



6

Some Codes

- $* - Match anything
- $+ - Match one or more tokens
- $# - Resolve to a mailer
- $1-$9 - Replace matched token
- $=L - A member of ‘L’
- S0 - Beginning of ruleset zero
- $w - Myself

7

Bad News

- All sendmail.cf files are not equal!
  - Some are huge and complicated
  - Some are stupid and out of date
  - Some are nicely parameterized
  - Some are incredibly cryptic
- Good idea on firewall is to use latest version of sendmail and sendmail.cf from the same distribution

8

Sendmail.cf Environment

- Some sendmail.cf files define various values that are easy to change
- When making changes, some programmers define values and then change them
  - Others (like me) just make changes in-line
- Good (but old) example:
  - decuac.dec.com:pub/sendmail-cf/generic.cf

9

Inside Ruleset Zero

```
# resolve locally connected UUCP links
R$* < @ $=Z . UUCP. > $*        $#uucp-uudom $@ $2 $: $1 <@$2.UUCP.> $3
R$* < @ $=Y . UUCP. > $*        $#uucp-new $@ $2 $: $1 <@$2.UUCP. > $3
R$* < @ $=U . UUCP. > $*        $#uucp-old $@ $2 $: $1 <@$2.UUCP. > $3


# deal with other remote names
R$* < @$* > $*          $#smtp $@ $2 $: $1 < @ $2 > $3


# handle locally delivered names
R$=L                    $#local $: @ $1
R$+                     $#local $: $1
```

10

Defining a Variable

```
# mjr - send mail to internal mail hub
DRmailhub.foo.com
```

... later, in Ruleset zero:

```
R$* < @foo.com > $*          $#smtp $@ $R $: $1 < @ foo.com > $2
```

11

Mailer Definitions

```
Mlocal, P=/usr/libexec/mail.local, F=lsDFMAw5:/|@rmn, S=10/30, R=20/40,
        T=DNS/RFC822/X-Unix,
        A=mail -d $u
Mprog,  P=/bin/sh, F=lsDFMoeu, S=10/30, R=20/40, D=$z:/,
        T=X-Unix,
        A=sh -c $u
```

12

Basic Rewrite

- In Ruleset zero:
  - Example traps mail for user@msmail.foo.com and sends it directly to msmail-gw.foo.com in form of user@foo.com

```
# resolve fake top level domains by forwarding to other hosts
R$*<@msmail.foo.com>$*    $#smtp $@ msmail-gw.foo.com $: $1<@foo.com>$3
```

13

Forwarding Mail In

- Some sendmail.cf files have a predefined domain value for you to fill in:

```
# EDIT--  this is added in answer to a question "What is your domain? "
# EDIT--  this is used for all hosts.
DDfoo.com
```

... later, in Ruleset zero:

```
R$*<@$-.$D>$*          $#smtp $@$2.$D$:$1<@$2.$D>$3
```

14

On the Mailhub

- Mailhub should forward mail out that is not for local domain

```
# EDIT--     this is added in answer to a question basically asked
# EDIT--     to determine what to do whenyou dont know how to deliver.
# EDIT--     Who gets the mail?  Can be empty...
# EDIT--     if for Tcpip host should be fully qualified name
DRfirewall.foo.com
```

... later, in Ruleset zero:

```
R$*<@$-.$D>$*           $#smtp $@$2.$D$:$1<@$2.$D>$3
R$*<@$+>$*              $#smtp $@$R$:$1<@$2>$3
```

15

Summary

- Sendmail is too much to cover in a firewall tutorial
- Making the actual changes to your sendmail.cf file depends on the sendmail.cf file you use to start
- Best to use a new version of sendmail and new .cf file
- Sendmail books exist

16