# HTTPS/secure on Port 443 ......

<VirtualHost 123.45.67.890:443>

ServerName somesite.com

ServerAlias www.somesite.com

DirectoryIndex index.php index.html

DocumentRoot /path/to/WP/webroot/directory

# copy and paste other existing variables here ...

# SSL directives ...

SSLEngine on

# Change these paths to find your certificate and key files

SSLCertificateFile /root/ssl/somesite.crt

SSLCertificateKeyFile /root/ssl/somesite.key

SetEnvIf User-Agent ".\*MSIE.\*" nokeepalive ssl-unclean-shutdown

# Route non-admins to HTTP

<IfModule mod\_rewrite.c>

RewriteEngine On

RewriteRule !^/wp-(admin|content|login|includes|signup)(.\*) - [C]

RewriteRule ^/(.\*) http://%{SERVER\_NAME}/$1 [QSA,L]

</IfModule>

</VirtualHost>

# HTTP/insecure on Port 80 ......

<VirtualHost \*:80>

ServerName somesite.com

ServerAlias www.somesite.com

ServerAdmin apache@somesite.com

DirectoryIndex index.php index.html

DocumentRoot /path/to/WP/webroot/directory

# more otions may be added here ...

<Directory /path/to/WP/webroot/directory >

<IfModule mod\_rewrite.c>

RewriteEngine On

RewriteBase /

# Route admins to HTTPS

RewriteCond %{REQUEST\_FILENAME} -f [OR]

RewriteCond %{REQUEST\_FILENAME} -d

RewriteRule ^wp-(admin|login|signup)(.\*) https://%{SERVER\_NAME}/wp-$1$2 [C]

# typical .htaccess file content goes last

RewriteRule ^.\*$ - [S=40]

RewriteRule ^index\.php$ - [L]

RewriteRule ^files/(.+) wp-includes/ms-files.php?file=$1 [L]

RewriteCond %{REQUEST\_FILENAME} -f [OR]

RewriteCond %{REQUEST\_FILENAME} -d

RewriteRule ^ - [L]

RewriteRule . index.php [L]

</IfModule>

</Directory>

</VirtualHost>

sudo -i

openssl version

aptitude install openssl

cd /etc/ssl/private

openssl genrsa -out somesite.key 1024

chmod 400 somesite.key

openssl req -new -key somesite.key -x509 -out somesite.crt -days 365

a2enmod ssl

a2enmod rewrite

cp /etc/apache2/sites-available/somesite.com /etc/apache2/sites-available/somesite.com.ORIGINAL

nano /etc/apache2/sites-available/somesite.com

# HTTPS/secure on Port 443 ......

<VirtualHost 123.45.67.890:443>

ServerName somesite.com

ServerAlias www.somesite.com

DirectoryIndex index.php index.html

DocumentRoot /path/to/WP/webroot/directory

# copy and paste other existing variables here ...

# SSL directives ...

SSLEngine on

# Change these paths to find your certificate and key files

SSLCertificateFile /root/ssl/somesite.crt

SSLCertificateKeyFile /root/ssl/somesite.key

SetEnvIf User-Agent ".\*MSIE.\*" nokeepalive ssl-unclean-shutdown

# Route non-admins to HTTP

<IfModule mod\_rewrite.c>

RewriteEngine On

RewriteRule !^/wp-(admin|content|login|includes|signup)(.\*) - [C]

RewriteRule ^/(.\*) http://%{SERVER\_NAME}/$1 [QSA,L]

</IfModule>

</VirtualHost>

# HTTP/insecure on Port 80 ......

<VirtualHost \*:80>

ServerName somesite.com

ServerAlias www.somesite.com

ServerAdmin apache@somesite.com

DirectoryIndex index.php index.html

DocumentRoot /path/to/WP/webroot/directory

# more otions may be added here ...

<Directory /path/to/WP/webroot/directory >

<IfModule mod\_rewrite.c>

RewriteEngine On

RewriteBase /

# Route admins to HTTPS

RewriteCond %{REQUEST\_FILENAME} -f [OR]

RewriteCond %{REQUEST\_FILENAME} -d

RewriteRule ^wp-(admin|login|signup)(.\*) https://%{SERVER\_NAME}/wp-$1$2 [C]

# typical .htaccess file content goes last

RewriteRule ^.\*$ - [S=40]

RewriteRule ^index\.php$ - [L]

RewriteRule ^files/(.+) wp-includes/ms-files.php?file=$1 [L]

RewriteCond %{REQUEST\_FILENAME} -f [OR]

RewriteCond %{REQUEST\_FILENAME} -d

RewriteRule ^ - [L]

RewriteRule . index.php [L]

</IfModule>

</Directory>

</VirtualHost>

exit

apache2ctl restart

openssl req -new -key somesite.key -out somesite.csr

ssh -p 54321 username@123.45.67.890

ssh localhost

sudo aptitude install ssh

cd ~/.ssh

ssh-keygen -t rsa

cat ~/.ssh/id\_rsa.pub > someFile.txt

cd ~

mkdir .ssh

nano .ssh/authorized\_keys

chown -R USER:USER .ssh­

chmod 700 .ssh

chmod 600 .ssh/authorized\_keys

nano /path/to/WP-root/wp-admin/.htaccess

order deny,allow

deny from all

allow from 123.45.67.890

AuthType Basic

AuthName "Protect me pretty please"

AuthUserFile "/home/USERNAME/.htpasswds/public\_html/protectme/passwd"

Require valid-user

htpasswd -c ~/.passwd mary-beth

htpasswd ~/.htpasswd someoneelse

AuthType Basic

AuthName "Welcome to the Whatnot Client Zone"

AuthUserFile "~/.htpasswd"

AuthGroupFile "~/.htgroup"

require group whatnot

sudo a2enmod auth\_digest

apache2ctl restart

htdigest -c ~/.htdigest\_pw realm user

htdigest -c ~/.htdigest\_pw "Private" bobcat

AuthType Digest

AuthName "Private"

AuthDigestFile /home/USERNAME/.htdigest\_pw

Require user bobcat

AuthType Digest

AuthName "Private"

AuthDigestFile /home/USERNAME/.htdigest\_pw

AuthDigestGroupFile /home/USERNAME/.htdigest\_groups

Require group admin

AuthName "Should You Be Here, I Mean, Reeeaaally?"

AuthType Basic

AuthMySQLEnable On

AuthMySQLHost localhost

AuthMySQLUser someUser

AuthMySQLPassword prettyPassword

AuthMySQLDB dbName

AuthMySQLUserTable userTableName

AuthMySQLNameField userNameField

AuthMySQLPasswordField userPasswordField

AuthMySQLPwEncryption md5

AuthMySQLAuthoritative On

require valid-user