{%- if site.ssl is defined %}

{%- if site.ssl.enabled %}

SSLEngine on

{%- if site.ssl.key\_file is defined %}

SSLCertificateFile {{ site.ssl.cert\_file }}

SSLCertificateKeyFile {{ site.ssl.key\_file }}

{%- if site.ssl.chain\_file is defined %}

SSLCertificateChainFile {{ site.ssl.chain\_file }}

{%- endif %}

{%- else %}

{%- if pillar.letsencrypt is defined %}

SSLCertificateFile /etc/letsencrypt/live/{{ site.host.name }}/cert.pem

SSLCertificateKeyFile /etc/letsencrypt/live/{{ site.host.name }}/privkey.pem

SSLCertificateChainFile /etc/letsencrypt/live/{{ site.host.name }}/fullchain.pem

{%- else %}

SSLCertificateFile /etc/ssl/certs/{{ site.host.name }}.crt

SSLCertificateKeyFile /etc/ssl/private/{{ site.host.name }}.key

SSLCertificateChainFile /etc/ssl/certs/{{ site.host.name }}-ca-chain.crt

{%- endif %}

{%- endif %}

{%- if site.ssl.get('strict\_transport\_security', False) %}

Header always set Strict-Transport-Security "max-age=63072000; includeSubdomains; preload"

{%- endif %}

{%- set ssl\_mode = site.ssl.get('mode', 'secure') %}

{%- if ssl\_mode not in ['normal', 'secure'] %}

{%- if site.ssl.protocols is defined %}

{%- set \_protocols = [] %}

{%- for protocol\_name, protocols in site.ssl.get('protocols', {}).iteritems() %}

{%- if protocols.get('enabled', False) %}

{%- do \_protocols.append(protocols.name) %}

{%- endif %}

{%- endfor %}

SSLProtocol {{ ' '.join(\_protocols) }}

{%- endif %}

{%- if site.ssl.ciphers is defined %}

{%- set \_ciphers = [] %}

{%- for cipher\_name, ciphers in site.ssl.get('ciphers', {}).iteritems() %}

{%- if ciphers.get('enabled', False) %}

{%- do \_ciphers.append(ciphers.name) %}

{%- endif %}

{%- endfor %}

SSLCipherSuite {{ ':'.join(\_ciphers) }}

{%- endif %}

{%- if site.ssl.prefer\_server\_ciphers is defined %}

SSLHonorCipherOrder {{ site.ssl.prefer\_server\_ciphers }}

{%- endif %}

{%- if site.ssl.get('crl', {'enabled': False}).enabled %}

{%- if site.ssl.crl.value is defined %}

SSLCARevocationCheck {{ site.ssl.crl.value }}

{%- endif %}

{%- if site.ssl.crl.file is defined %}

SSLCARevocationFile {{ site.ssl.crl.file }}

{%- endif %}

{%- if site.ssl.crl.path is defined %}

SSLCARevocationPath {{ site.ssl.crl.path }}

{%- endif %}

{%- endif %}

{%- if site.ssl.compression is defined %}

SSLCompression {{ site.ssl.compression }}

{%- endif %}

{%- if site.ssl.ssl\_engine is defined %}

SSLEngine {{ site.ssl.ssl\_engine }}

{%- endif %}

{%- if site.ssl.insecure\_renegotiation is defined %}

SSLInsecureRenegotiation {{ site.ssl.insecure\_renegotiation }}

{%- endif %}

{%- if site.ssl.get('ocsp', {'enabled': False}).enabled %}

{%- if site.ssl.ocsp.default\_responder is defined %}

SSLOCSPDefaultResponder {{ site.ssl.ocsp.default\_responder }}

{%- endif %}

{%- if site.ssl.ocsp.ocsp\_enable is defined %}

SSLOCSPEnable {{ site.ssl.ocsp.ocsp\_enable }}

{%- endif %}

{%- if site.ssl.ocsp.noverify is defined %}

SSLOCSPNoverify {{ site.ssl.ocsp.noverify }}

{%- endif %}

{%- if site.ssl.ocsp.proxy\_url is defined %}

SSLOCSPProxyURL {{ site.ssl.ocsp.proxy\_url }}

{%- endif %}

{%- if site.ssl.ocsp.override\_responder is defined %}

SSLOCSPOverrideResponder {{ site.ssl.ocsp.override\_responder }}

{%- endif %}

{%- if site.ssl.ocsp.cert\_file is defined %}

SSLOCSPResponderCertificateFile {{ site.ssl.ocsp.cert\_file }}

{%- endif %}

{%- if site.ssl.ocsp.responder\_timeout is defined %}

SSLOCSPResponderTimeout {{ site.ssl.ocsp.responder\_timeout }}

{%- endif %}

{%- if site.ssl.ocsp.max\_age is defined %}

SSLOCSPResponseMaxAge {{ site.ssl.ocsp.max\_age }}

{%- endif %}

{%- if site.ssl.ocsp.time\_skew is defined %}

SSLOCSPResponseTimeSkew {{ site.ssl.ocsp.time\_skew }}

{%- endif %}

{%- if site.ssl.ocsp.nonce is defined %}

SSLOCSPUseRequestNonce {{ site.ssl.ocsp.nonce }}

{%- endif %}

{%- endif %}

{%- if site.ssl.get('dhparam', {'enabled': False}).enabled %}

SSLOpenSSLConfCmd DHParameters "/etc/ssl/dhparams\_apache\_{{ site\_name }}.pem"

{%- endif %}

{%- if site.ssl.ecdh\_curve is defined %}

{%- set \_ecdh\_curve = [] %}

{%- for ecdh\_curve\_name, ecdh\_curve in site.ssl.get('ecdh\_curve', {}).iteritems() %}

{%- if ecdh\_curve.get('enabled', False) %}

{%- do \_ecdh\_curve.append(ecdh\_curve.name) %}

{%- endif %}

{%- endfor %}

SSLOpenSSLConfCmd Curves {{ ':'.join(\_ecdh\_curve) }}

{%- endif %}

{%- if site.ssl.conf\_cmd is defined %}

{%- for conf\_cmd\_name, conf\_cmd in site.ssl.get('conf\_cmd', {}).iteritems() %}

{%- if conf\_cmd.get('enabled', False) %}

SSLOpenSSLConfCmd {{ conf\_cmd.command\_name }} {{conf\_cmd.command\_value }}

{%- endif %}

{%- endfor %}

{%- endif %}

{%- if site.ssl.ssl\_options is defined %}

{%- for ssl\_options\_name, ssl\_options in site.ssl.get('ssl\_options', {}).iteritems() %}

{%- if ssl\_options.get('enabled', False) %}

SSLOptions {{ ssl\_options.option }}

{%- endif %}

{%- endfor %}

{%- endif %}

{%- if site.ssl.proxy is defined %}

{%- include "apache/files/\_ssl\_proxy.conf" %}

{%- endif %}

{%- if site.ssl.session\_timeout is defined %}

SSLSessionCacheTimeout {{ site.ssl.session\_timeout }}

{%- endif %}

{%- if site.ssl.get('ticket\_key', {'enabled': False}).enabled %}

SSLSessionTicketKeyFile /etc/ssl/ticket\_apache\_{{ site\_name }}.key

{%- endif %}

{%- if site.ssl.session\_tickets is defined %}

SSLSessionTickets {{ site.ssl.session\_tickets }}

{%- endif %}

{%- if site.ssl.srp\_unknown\_seed is defined %}

SSLSRPUnknownUserSeed {{ site.ssl.srp\_unknown\_seed }}

{%- endif %}

{%- if site.ssl.srp\_verifier\_file is defined %}

SSLSRPVerifierFile {{ site.ssl.srp\_verifier\_file }}

{%- endif %}

{%- if site.ssl.ssl\_stapling is defined %}

{%- include "apache/files/\_ssl\_stapling.conf" %}

{%- endif %}

{%- if site.ssl.sniv\_host\_check is defined %}

SSLStrictSNIVHostCheck {{ site.ssl.sniv\_host\_check }}

{%- endif %}

{%- if site.ssl.stapling is defined %}

SSLUseStapling {{ site.ssl.stapling}}

{%- endif %}

{%- if site.ssl.verify\_client is defined %}

SSLVerifyClient {{ site.ssl.verify\_client }}

{%- endif %}

{%- if site.ssl.verify\_depth is defined %}

SSLVerifyDepth {{ site.ssl.verify\_depth }}

{%- endif %}

{%- else %}

{%- include "apache/files/\_ssl\_"+ssl\_mode+".conf" %}

{%- endif %}

{%- endif %}

{%- endif %}