Traefik HTTP TLS Documentation

- Configuration Example
- Configuration Options
- Certificate Resolver
- Custom Domains

When an HTTP router is configured to handle HTTPS traffic, include a `tls` field in its definition. This field tells Traefik that the router should process only TLS requests and ignore non-TLS traffic.

By default, an HTTP router with a TLS field will terminate the TLS connections, meaning that it will send decrypted data to the services. The TLS configuration provides several options for fine-tuning the TLS behavior, including automatic certificate generation, custom TLS options, and explicit domain specification.

!!! warning "Router TLS replaces entrypoint TLS"

```
Entrypoint `http.tls` settings apply only when a router does **not** define its own `tls`
section.
Defining a router `tls` section — even empty, or with any field such as `certResolver`,
`options`, or `domains` —
means Traefik does **not** merge that configuration with the entrypoint defaults for that
router. The router TLS
configuration replaces the entrypoint TLS configuration entirely.

For example, with entrypoint TLS options configured:

```yaml
entryPoints:
  websecure:
    address: :443
```
```

```
    http:
      tls:
        options: modern-tls@file
```

and a router that only sets a certificate resolver:

```yaml
http:
  routers:
    sample:
      rule: Host(`example.com`)
      service: sample
      tls:
        certResolver: letsencrypt
```

the entrypoint `options` (`modern-tls@file`) are **not** applied to `sample`.
To keep both, set them together on the entrypoint, or set both `options` and `certResolver` on the router.

Configuration Example

```
http:
  routers:
    my-https-router:
      rule: "Host(`example.com`) && Path(`/api`)"
      service: "my-http-service"
      tls:
        certResolver: "letsencrypt"
        options: "modern-tls"
        domains:
          - main: "example.com"
            sans:
              - "www.example.com"
              - "api.example.com"
```

```
[http.routers.my-https-router]
  rule = "Host(`example.com`) && Path(`/api`)"
  service = "my-http-service"

  [http.routers.my-https-router.tls]
    certResolver = "letsencrypt"
    options = "modern-tls"

    [[http.routers.my-https-router.tls.domains]]
      main = "example.com"
      sans = ["www.example.com", "api.example.com"]
```

```
labels:
  - "traefik.http.routers.my-https-router.rule=Host(`example.com`) && Path(`/api`)"
  - "traefik.http.routers.my-https-router.service=my-http-service"
  - "traefik.http.routers.my-https-router.tls=true"
  - "traefik.http.routers.my-https-router.tls.certresolver=letsencrypt"
  - "traefik.http.routers.my-https-router.tls.options=modern-tls"
  - "traefik.http.routers.my-https-router.tls.domains[0].main=example.com"
  - "traefik.http.routers.my-https-router.tls.domains[0].sans=www.example.com,api.example.com"
```

```
{
  "Tags": [
    "traefik.http.routers.my-https-router.rule=Host(`example.com`) && Path(`/api`)",
    "traefik.http.routers.my-https-router.service=my-http-service",
    "traefik.http.routers.my-https-router.tls=true",
    "traefik.http.routers.my-https-router.tls.certresolver=letsencrypt",
    "traefik.http.routers.my-https-router.tls.options=modern-tls",
    "traefik.http.routers.my-https-router.tls.domains[0].main=example.com",
    "traefik.http.routers.my-https-router.tls.domains[0].sans=www.example.com,api.example.com"
  ]
}
```

Configuration Options

Field	Description	Default	Required

`options`	The name of the TLS options to use for configuring TLS parameters (cipher suites, min/max TLS version, client authentication, etc.). See TLS Options for detailed configuration.	`""` (resolves to `default` at runtime)	No
`certResolver`	The name of the certificate resolver to use for automatic certificate generation via ACME providers (such as Let's Encrypt). See the Certificate Resolver section for more details.	""	No
`domains`	List of domains and Subject Alternative Names (SANs) for explicit certificate domain specification. See the Custom Domains section for more details.	[]	No

Certificate Resolver

The `tls.certResolver` option allows you to specify a certificate resolver for automatic certificate generation via ACME providers (such as Let's Encrypt).

When a certificate resolver is configured for a router, Traefik will automatically obtain and manage TLS certificates for the domains specified in the router's rule (in the `Host` matcher) or in the `tls.domains` configuration (with `tls.domains` taking precedence).

!!! important "Prerequisites"

```
- Certificate resolvers must be defined in the [static configuration](../../../install-configuration/tls/certificate-resolvers/acme.md)
- The router must have `tls` enabled
- An ACME challenge type must be configured for the certificate resolver
```

Custom Domains

When using ACME certificate resolvers, domains are automatically extracted from router rules, but the `tls.domains` option allows you to explicitly specify the domains and Subject Alternative Names (SANs) for which certificates should be generated.

This provides fine-grained control over certificate generation and takes precedence over domains automatically extracted from router rules.

Every domain must have A/AAAA records pointing to Traefik.

{% include-markdown "includes/traefik-for-business-applications.md" %}

□□□ #2
□ □□□ □□□ 2026-10-31 14:04:24 UTC
□ □□□ □□□ 2026-10-31 14:04:25 UTC