目 录

1 SSL配置

说明

本特性仅集中式设备支持。

1.1 SSL简介

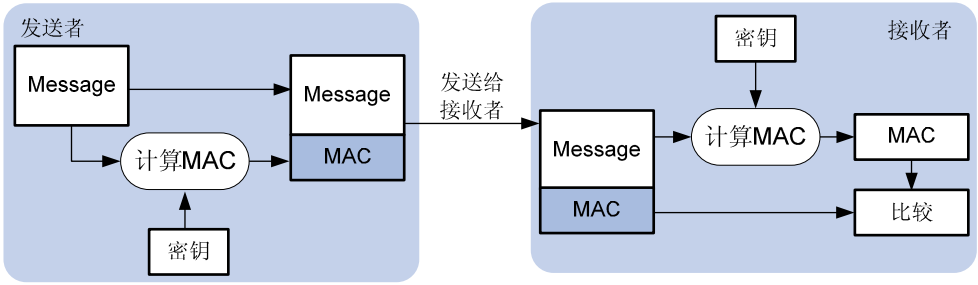
SSL（Secure Sockets Layer，安全套接层）是一个安全协议，为基于 TCP 的应用层协议提供安全连接，如 SSL 可以为 HTTP 协议提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为网络上数据的传输提供安全性保证。

1.1.1 SSL安全机制

SSL 提供的安全连接可以实现：

- 连接的私密性：利用对称加密算法对传输数据进行加密，并利用密钥交换算法——RSA（Rivest Shamir and Adleman，非对称密钥算法的一种）加密传输对称密钥算法中使用的密钥。
- 身份验证：基于证书利用数字签名方法对服务器和客户端进行身份验证。SSL 服务器和客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制从 CA（Certificate Authority，认证机构）获取证书。
- 连接的可靠性：消息传输过程中使用基于密钥的MAC（Message Authentication Code，消息验证码）来检验消息的完整性。MAC是将密钥和任意长度的数据转换为固定长度数据的一种算法。利用MAC算法验证消息完整性的过程如 图 1-1所示。发送者在密钥的参与下，利用MAC算法计算出消息的MAC值，并将其加在消息之后发送给接收者。接收者利用同样的密钥和MAC算法计算出消息的MAC值，并与接收到的MAC值比较。如果二者相同，则报文没有改变；否则，报文在传输过程中被修改，接收者将丢弃该报文。

图1-1 MAC 算法示意图



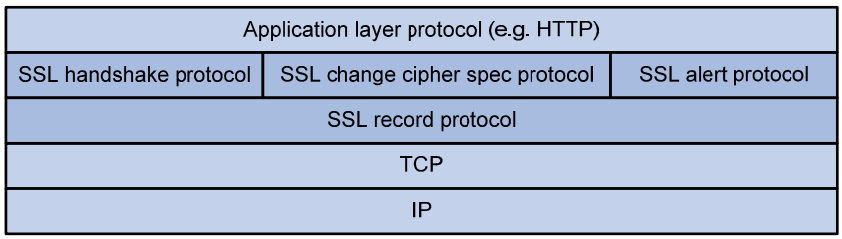
说明

- 对称密钥算法、非对称密钥算法 RSA 及数字签名的详细介绍请参见“安全配置指导”中的“公钥管理”；
- PKI 及证书、CA 的详细介绍请参见“安全配置指导”中的“PKI”。

1.1.2 SSL协议结构

如 图 1-2所示，SSL协议本身可以分为两层：底层为SSL记录协议（SSL record protocol）；上层为SSL握手协议（SSL handshake protocol）、SSL密码变化协议（SSL change cipher spec protocol）和SSL警告协议（SSL alert protocol）。

图1-2 SSL 协议栈



- SSL 记录协议：主要负责对上层的数据进行分块、计算并添加 MAC、加密，最后把记录块传输给对方。
- SSL 握手协议：是 SSL 协议非常重要的组成部分，用来协商通信过程中使用的加密套件（对称加密算法、密钥交换算法和 MAC 算法等）、在服务器和客户端之间安全地交换密钥，实现服务器和客户端的身份验证。客户端和服务器通过握手协议建立一个会话。会话包含一组参数，主要有会话 ID、对方的证书、加密套件（包括密钥交换算法、数据加密算法和 MAC 算法）及主密钥。
- SSL 密码变化协议：客户端和服务器端通过密码变化协议通知对端，随后的报文都将使用新协商的加密套件和密钥进行保护和传输。
- SSL 警告协议：用来允许一方向另一方报告告警信息。消息中包含告警的严重级别和描述。

1.2 SSL配置任务简介

SSL 服务器和客户端需要配置的参数不同，下面将分别介绍 SSL 服务器端策略和 SSL 客户端策略的配置方法。

表1-1 SSL 配置任务简介

配置任务	说明	详细配置
配置 SSL 服务器端策略	必选	1.3
配置 SSL 客户端策略	可选	1.4

1.3 配置SSL服务器端策略

SSL 服务器端策略是服务器启动时使用的 SSL 参数。只有与应用层协议（如 HTTP 协议）关联后，SSL 服务器端策略才能生效。

1.3.1 配置准备

配置 SSL 服务器端策略时，需要指定其使用的 PKI 域，以便通过该 PKI 域获取服务器端的证书。因此，在进行 SSL 服务器端策略配置之前，需要先配置 PKI 域。PKI 域配置方法的详细介绍，请参见“安全配置指导”中的“PKI”。

1.3.2 配置SSL服务器端策略

表1-2 配置 SSL 服务器端策略

操作	命令	说明
进入系统视图	**system-view**	-
创建 SSL 服务器端策略，并进入 SSL 服务器端策略视图	**ssl server-policy** *policy-name*	必选
配置 SSL 服务器端策略所使用的 PKI 域	**pki-domain** *domain-name*	必选 缺省情况下，没有配置 SSL 服务器端策略所使用的 PKI 域
配置 SSL 服务器端策略支持的加密套件	**ciphersuite** [**rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha**] *	可选 缺省情况下，SSL 服务器端策略支持所有的加密套件
配置服务器端 SSL 握手连接保持时间	**handshake timeout** *time*	可选 缺省情况下，服务器端 SSL 握手连接保持时间是 3600 秒
配置 SSL 连接关闭模式	**close-mode wait**	可选 缺省情况下，关闭模式为非 wait 模式
配置缓存的最大会话数目和会话缓存的超时时间	**session** { **cachesize** *size* | **timeout** *time* } *	可选 缺省情况下，缓存的最大会话数目为 500 个，会话缓存的超时时间为 3600 秒
配置 SSL 服务器端要求对 SSL 客户端进行基于证书的身份验证	**client-verify enable**	可选 缺省情况下，SSL 服务器端不要求对 SSL 客户端进行基于证书的身份验证

操作	命令	说明
使能 SSL 客户端弱认证功能	**client-verify weaken**	可选 缺省情况下，未使能 SSL 客户端弱认证功能 只有通过 **client-verify enable** 命令配置 SSL 服务器端要求对 SSL 客户端进行基于证书的身份验证后，本命令才会生效

说明

- 如果服务器端需要对客户端进行基于证书的身份验证，即配置了 **client-verify enable** 命令，则必须先为 SSL 客户端申请本地证书。
- 目前，SSL 协议版本主要有 SSL2.0、SSL3.0 和 TLS1.0（对应 SSL 协议的版本号为 3.1）。设备作为 SSL 服务器时，可以与 SSL3.0 和 TLS1.0 版本的 SSL 客户端通信，还可以识别同时兼容 SSL2.0 和 SSL3.0/TLS1.0 版本的 SSL 客户端发送的报文，并通知该客户端采用 SSL3.0/TLS1.0 版本与 SSL 服务器通信。

1.4 配置SSL客户端策略

SSL 客户端策略是客户端连接 SSL 服务器时使用的参数。只有与应用层协议关联后，SSL 客户端策略才能生效。

1.4.1 配置准备

如果 SSL 服务器要求验证 SSL 客户端的身份，则配置 SSL 客户端策略时，需要指定其使用的 PKI 域，以便通过该 PKI 域获取客户端的证书。因此，在进行 SSL 客户端策略配置之前，需要先配置 PKI 域。PKI 域配置方法的详细介绍，请参见“安全配置指导”中的“PKI”。

1.4.2 配置SSL客户端策略

表1-3 配置 SSL 客户端策略

操作	命令	说明
进入系统视图	**system-view**	-
创建 SSL 客户端策略，并进入 SSL 客户端策略视图	**ssl client-policy** *policy-name*	必选
配置 SSL 客户端策略所使用的 PKI 域	**pki-domain** *domain-name*	可选 缺省情况下，没有配置 SSL 客户端策略所使用的 PKI 域

操作	命令	说明
配置 SSL 客户端策略的首选加密套件	**prefer-cipher** { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }	可选 缺省情况下，SSL 客户端策略的首选加密套件为 **rsa_rc4_128_md5**
配置 SSL 客户端策略使用的 SSL 协议版本	**version** { **ssl3.0** | **tls1.0** }	可选 缺省情况下，SSL 客户端策略使用的 SSL 协议版本号为 TLS 1.0
使能基于证书的 SSL 服务器身份验证	**server-verify enable**	可选 缺省情况下，需要进行基于证书的 SSL 服务器身份验证

说明

如果服务器端需要对客户端进行基于证书的身份验证，则必须先在 SSL 客户端所属的 PKI 域内为 SSL 客户端申请本地证书。

1.5 SSL显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 SSL 的运行情况，通过查看显示信息验证配置的效果。

表1-4 SSL 显示和维护

操作	命令
显示 SSL 服务器端策略的信息	**display ssl server-policy** { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]
显示 SSL 客户端策略的信息	**display ssl client-policy** { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

1.6 常见配置错误举例

1.6.1 SSL握手失败

1. 故障现象

设备作为 SSL 服务器时，与 SSL 客户端握手失败。

2. 故障分析

SSL 握手失败，可能有以下原因：

- 客户端配置了必须对服务器端进行身份验证，但 SSL 服务器端证书不存在，或者证书不能被信任；

- 服务器端配置了必须对客户端进行身份验证，但 SSL 客户端的证书不存在或不能被信任；
- SSL 服务器端和客户端没有匹配的加密套件。

3. 故障排除

(1) 使用 **debugging ssl** 命令查看调试信息：

- 如果客户端配置了必须对服务器端进行身份验证，而 SSL 服务器端的证书不存在，请为 SSL 服务器申请证书；如果服务器端证书不能被信任，请在 SSL 客户端安装为 SSL 服务器颁发证书的 CA 服务器根证书，或服务器向 SSL 客户端信任的 CA 服务器重新申请证书；
- 如果服务器端配置了必须对客户端进行身份验证，而 SSL 客户端的证书不存在或不能被信任，请为客户端申请并安装证书。

(2) 使用 **display ssl server-policy** 命令查看 SSL 服务器端策略支持的加密套件。如果 SSL 服务器端和客户端没有匹配的加密套件，请用 **ciphersuite** 命令修改 SSL 服务器支持的加密套件。