目 录

1 SSL

说明

设备运行于 FIPS 模式时，本特性部分配置相对于非 FIPS 模式有所变化，具体差异请见本文相关描述。有关 FIPS 模式的详细介绍请参见“安全配置指导”中的“FIPS”。

1.1 SSL简介

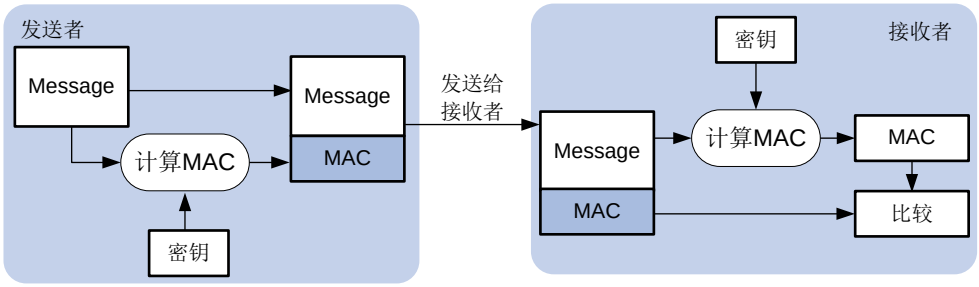
SSL（Secure Sockets Layer，安全套接字层）是一个安全协议，为基于 TCP 的应用层协议（如 HTTP）提供安全连接。SSL 协议广泛应用于电子商务、网上银行等领域，为应用层数据的传输提供安全性保证。

1.1.1 SSL安全机制

SSL 提供的安全连接可以实现如下功能：

- 保证数据传输的机密性：利用对称密钥算法对传输的数据进行加密，并利用密钥交换算法，如 RSA（Rivest Shamir and Adleman），加密传输对称密钥算法中使用的密钥。对称密钥算法、非对称密钥算法 RSA 的详细介绍请参见“安全配置指导”中的“公钥管理”。
- 验证数据源的身份：基于数字证书利用数字签名方法对 SSL 服务器和 SSL 客户端进行身份验证。SSL 服务器和 SSL 客户端通过 PKI（Public Key Infrastructure，公钥基础设施）提供的机制获取数字证书。PKI 及数字证书的详细介绍请参见“安全配置指导”中的“PKI”。
- 保证数据的完整性：消息传输过程中使用MAC（Message Authentication Code，消息验证码）来检验消息的完整性。MAC算法在密钥的参与下，将任意长度的原始数据转换为固定长度的数据，原始数据的任何变化都会导致计算出的固定长度数据发生变化。如 图 1-1 所示，利用MAC算法验证消息完整性的过程为：
  a. 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。
  b. 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。
  c. 如果二者相同，则接收者认为报文没有被篡改；否则，认为报文在传输过程中被篡改，接收者将丢弃该报文。

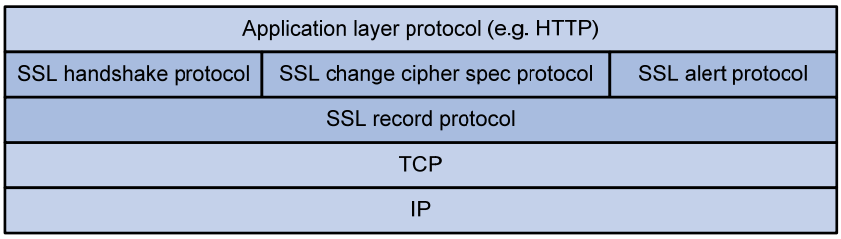
图1-1 MAC 算法示意图



1.1.2 SSL协议结构

如 图 1-2 所示，SSL协议可以分为两层：下层为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告警协议（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，最后把加密后的记录块传输给对方。
- SSL 握手协议：用来协商通信过程中使用的加密套件（数据加密算法、密钥交换算法和 MAC 算法等），实现服务器和客户端的身份验证，并在服务器和客户端之间安全地交换密钥。客户端和服务器通过握手协议建立会话。一个会话包含一组参数，主要有会话 ID、对方的数字证书、加密套件及主密钥。
- 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 告警协议：用来向对端报告告警信息，以便对端进行相应的处理。告警消息中包含告警的严重级别和描述。

1.2 SSL配置任务简介

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	请在SSL服务器端进行本配置	1.3
配置SSL客户端策略	请在SSL客户端进行本配置	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 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）等应用关联后，SSL 服务器端策略才能生效。

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**	-
（可选）禁止SSL服务器使用指定的SSL版本进行SSL协商	非FIPS模式下： **ssl version { ssl3.0 | tls1.0 | tls1.1 } * disable** FIPS模式下： **ssl version { tls1.0 | tls1.1 } * disable**	非FIPS模式下： 缺省情况下，允许SSL 服务器使用SSL3.0、TLS1.0、TLS1.1和TLS1.2版本的协商功能 FIPS模式下： 缺省情况下，允许使用TLS1.0、TLS1.1和TLS1.2版本的协商功能
（可选）配置SSL服务器端关闭SSL重协商	**ssl renegotiation disable**	缺省情况下，允许SSL重协商
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*	缺省情况下，设备上不存在任何SSL服务器端策略
（可选）配置SSL服务器端策略所使用的PKI域	**pki-domain** *domain-name*	缺省情况下，没有指定SSL服务器端策略所使用的PKI域 如果客户端需要对服务器端进行基于数字证书的身份验证，则必须在SSL服务器端使用本命令指定PKI域，并在该PKI域内为SSL服务器端申请本地数字证书 PKI域的创建及配置方法，请参见“安全配置指导”中的“PKI”

操作	命令	说明
配置SSL服务器端策略支持的加密套件	非FIPS模式下： **ciphersuite** { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha** | **dhe_rsa_aes_256_cbc_sha256** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } * FIPS模式下： **ciphersuite** { **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** } *	缺省情况下，SSL服务器端策略支持所有的加密套件
配置SSL服务器上缓存的最大会话数目和SSL会话缓存的超时时间	**session** { **cachesize** *size* | **timeout** *time* } *	缺省情况下，SSL服务器上缓存的最大会话数目为500个，SSL会话缓存的超时时间为3600秒
配置SSL服务器端对SSL客户端的身份验证方案	**client-verify** { **enable** | **optional** }	缺省情况下，SSL服务器端不要求对SSL客户端进行基于数字证书的身份验证 SSL服务器端在基于数字证书对SSL客户端进行身份验证时，除了对SSL客户端发送的证书链进行验证，还要检查证书链中的除根CA证书外的每个证书是否均未被吊销

说明

- 目前，SSL 协议版本主要有 SSL2.0、SSL3.0、TLS1.0、TLS1.1 和 TLS1.2（TLS1.0 对应 SSL 协议的版本号为 3.1）。设备作为 SSL 服务器时，缺省情况下，可以与 SSL3.0、TLS1.0、TLS1.1 和 TLS1.2 版本的 SSL 客户端通信，还可以识别同时兼容 SSL2.0/SSL3.0/TLS1.0/TLS1.1/TLS1.2 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/TLS1.1/TLS1.2 版本与 SSL 服务器通信。
- 当设备对系统安全性有较高要求时可以通过命令行关闭对应**版本号的** SSL 协**商**。

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，如 FTP（File Transfer Protocol，文件传输协议），关联后，SSL 客户端策略才能生效。FTP 的详细配置请参见“基础配置指导”中的“FTP 和 TFTP”。

表1-3 配置 SSL 客户端策略

配置任务	命令	说明
进入系统视图	**system-view**	-
（可选）配置SSL客户端关闭SSL重协商	**ssl renegotiation disable**	缺省情况下，允许SSL重协商
创建SSL客户端策略，并进入SSL客户端策略视图	**ssl client-policy** *policy-name*	缺省情况下，设备上不存在任何SSL客户端策略
（可选）配置SSL客户端策略所使用的PKI域	**pki-domain** *domain-name*	缺省情况下，没有指定SSL客户端策略所使用的PKI域 如果服务器端需要对客户端进行基于数字证书的身份验证，则必须在SSL客户端使用本命令指定PKI域，并在该PKI域内为SSL客户端申请本地数字证书 PKI域的创建及配置方法，请参见“安全配置指导”中的“PKI”

配置任务	命令	说明
配置SSL客户端策略支持的加密套件	非FIPS模式下： **prefer-cipher** { **dhe_rsa_aes_128_cbc_sha** | **dhe_rsa_aes_128_cbc_sha256** | **dhe_rsa_aes_256_cbc_sha** | **dhe_rsa_aes_256_cbc_sha256** | **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **exp_rsa_des_cbc_sha** | **exp_rsa_rc2_md5** | **exp_rsa_rc4_md5** | **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** } FIPS模式下： **prefer-cipher** { **ecdhe_ecdsa_aes_128_cbc_sha256** | **ecdhe_ecdsa_aes_128_gcm_sha256** | **ecdhe_ecdsa_aes_256_cbc_sha384** | **ecdhe_ecdsa_aes_256_gcm_sha384** | **ecdhe_rsa_aes_128_cbc_sha256** | **ecdhe_rsa_aes_128_gcm_sha256** | **ecdhe_rsa_aes_256_cbc_sha384** | **ecdhe_rsa_aes_256_gcm_sha384** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_cbc_sha256** | **rsa_aes_256_cbc_sha** | **rsa_aes_256_cbc_sha256** }	非FIPS模式下： 缺省情况下，SSL客户端策略支持的加密套件为**rsa_rc4_128_md5** FIPS模式下： 缺省情况下，SSL客户端策略支持的加密套件为**rsa_aes_128_cbc_sha**
配置SSL客户端策略使用的SSL协议版本	非FIPS模式下： **version** { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** } FIPS模式下： **version** { **tls1.0** | **tls1.1** | **tls1.2** }	缺省情况下，SSL客户端策略使用的SSL协议版本为TLS 1.0 对安全性要求较高的环境下，建议为不要为SSL 客户端指定SSL3.0 版本
配置客户端需要对服务器端进行基于数字证书的身份验证	**server-verify enable**	缺省情况下，SSL客户端需要对SSL服务器端进行基于数字证书的身份验证

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
显示算法库的版本号	**display crypto version**

操作	命令
显示SSL服务器端策略的信息	**display ssl server-policy** [*policy-name*]
显示SSL客户端策略的信息	**display ssl client-policy** [*policy-name*]