目 录

1 SSL 1-1
1.1 SSL配置命令 1-1
1.1.1 ciphersuite 1-1
1.1.2 client-verify enable 1-1
1.1.3 client-verify weaken 1-2
1.1.4 close-mode wait 1-3
1.1.5 display ssl client-policy 1-3
1.1.6 display ssl server-policy 1-4
1.1.7 handshake timeout 1-6
1.1.8 pki-domain 1-6
1.1.9 prefer-cipher 1-7
1.1.10 server-verify enable 1-8
1.1.11 session 1-8
1.1.12 ssl client-policy 1-9
1.1.13 ssl server-policy 1-9
1.1.14 version 1-10

1 SSL

1.1 SSL配置命令

1.1.1 ciphersuite

【命令】

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**] *

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

rsa_3des_ede_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC、MAC 算法采用 SHA。

rsa_des_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 DES_CBC、MAC 算法采用 SHA。

rsa_rc4_128_md5：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 MD5。

rsa_rc4_128_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4、MAC 算法采用 SHA。

【描述】

ciphersuite 命令用来配置 SSL 服务器端策略支持的加密套件。

缺省情况下，SSL 服务器端策略支持所有的加密套件。

需要注意的是：

- 如果不指定任何参数，则 SSL 服务器端策略支持上述所有加密套件。
- 如果多次执行本命令，则新的配置覆盖原有配置。

相关配置可参考命令 **display ssl server-policy**。

【举例】

指定 SSL 服务器端策略支持的加密套件为 **rsa_rc4_128_md5** 和 **rsa_rc4_128_sha**。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

1.1.2 client-verify enable

【命令】

client-verify enable

undo client-verify enable

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

client-verify enable 命令用来配置 SSL 服务器端要求对 SSL 客户端进行基于证书的身份验证。**undo client-verify enable** 命令用来恢复缺省情况。

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。

执行本命令后：

- 如果通过 **client-verify weaken** 命令使能了 SSL 客户端弱认证功能，则由客户端决定是否对客户端进行身份验证。客户端选择进行身份验证时，只有身份验证通过后，SSL 客户端才能访问 SSL 服务器；客户端选择不进行身份验证时，SSL 客户端可以直接访问 SSL 服务器。
- 如果未使能 SSL 客户端弱认证功能，则必须对客户端进行身份验证。只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。

相关配置可参考命令 **client-verify weaken** 和 **display ssl server-policy**。

【举例】

配置服务器端要求对客户端进行基于证书的身份验证。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

1.1.3 client-verify weaken

【命令】

client-verify weaken

undo client-verify weaken

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

client-verify weaken 命令用来使能 SSL 客户端弱认证功能。**undo client-verify weaken** 命令用来恢复缺省情况。

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。

- 使能 SSL 客户端弱认证功能后，由客户端决定是否对客户端进行身份验证。如果客户端选择进行身份验证，则只有身份验证通过后，SSL 客户端才能访问 SSL 服务器；如果客户端选择不进行身份验证，则 SSL 客户端可以直接访问 SSL 服务器。

- 如果未使能 SSL 客户端弱认证功能，则必须对客户端进行身份验证。只有身份验证通过后，SSL 客户端才能访问 SSL 服务器。

相关配置可参考命令 **client-verify enable** 和 **display ssl server-policy**。

【举例】

使能 SSL 客户端弱认证功能。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
[Sysname-ssl-server-policy-policy1] client-verify weaken
```

1.1.4 close-mode wait

【命令】

close-mode wait

undo close-mode wait

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

close-mode wait 命令用来配置 SSL 连接的关闭模式为 wait 模式，即发送 close-notify 警告消息给客户端后，等待客户端的 close-notify 警告消息，在接收到客户端的 close-notify 警告消息后才能关闭连接。**undo close-mode wait** 命令用来恢复缺省情况。

缺省情况下，服务器发送 close-notify 警告消息给客户端，不等待客户端的 close-notify 警告消息，直接关闭连接。

相关配置可参考命令 **display ssl server-policy**。

【举例】

设定 SSL 连接的关闭模式为 wait 模式。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

1.1.5 display ssl client-policy

【命令】

display ssl client-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

policy-name：显示指定的 SSL 客户端策略的信息，为 1～16 个字符的字符串，不区分大小写。

all：显示所有 SSL 客户端策略的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssl client-policy 命令用来显示 SSL 客户端策略的信息。

【举例】

显示名为 policy1 的 SSL 客户端策略信息。

```
<Sysname> display ssl client-policy policy1
 SSL Client Policy: policy1
     SSL Version: SSL 3.0
     PKI Domain: 1
     Prefer Ciphersuite:
         RSA_RC4_128_SHA
     Server-verify: enabled
```

表1-1 display ssl client-policy 命令显示信息描述表

字段	描述
SSL Client Policy	SSL客户端策略名
SSL Version	SSL客户端策略使用的协议版本号，取值包括SSL 3.0和TLS 1.0
PKI Domain	SSL客户端策略使用的PKI域
Prefer Ciphersuite	SSL客户端策略的首选加密套件
Server-verify	SSL客户端策略的服务器验证模式，取值包括： • disabled：不需要对服务器端进行身份验证 • enabled：需要对服务器端进行身份验证

1.1.6 display ssl server-policy

【命令】

display ssl server-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

1：监控级

【参数】

policy-name：显示指定的 SSL 服务器端策略的信息，为 1～16 个字符的字符串，不区分大小写。

all：显示所有 SSL 服务器端策略的信息。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display ssl server-policy 命令用来显示 SSL 服务器端策略的信息。

【举例】

显示名为 policy1 的 SSL 服务器端策略的信息。

```
<Sysname> display ssl server-policy policy1
 SSL Server Policy: policy1
     PKI Domain: domain1
     Ciphersuite:
         RSA_RC4_128_MD5
         RSA_RC4_128_SHA
         RSA_DES_CBC_SHA
         RSA_3DES_EDE_CBC_SHA
         RSA_AES_128_CBC_SHA
         RSA_AES_256_CBC_SHA
     Handshake Timeout: 3600
     Close-mode: wait disabled
     Session Timeout: 3600
     Session Cachesize: 500
     Client-verify: disabled
     Client-verify weaken: disabled
```

表1-2 display ssl server-policy 命令显示信息描述表

字段	描述
SSL Server Policy	SSL服务器端策略名
PKI Domain	SSL服务器端策略使用的PKI域 如果显示为空，则表示未指定SSL服务器端策略使用的PKI域，SSL服务器自己生成证书，而无需从CA获取证书
Ciphersuite	SSL服务器端策略支持的加密套件
Handshake Timeout	SSL服务器端策略的握手连接保持时间，单位为秒
Close-mode	SSL服务器端策略的关闭模式，取值包括： • wait disabled：SSL 连接的关闭模式为非 wait 模式，即服务器发送 close-notify 警告消息给客户端，不等待客户端的 close-notify 警告消息，直接关闭连接 • wait enabled：SSL 连接的关闭模式为 wait 模式，即发送 close-notify 警告消息给客户端后，等待客户端的 close-notify 警告消息，在接收到客户端的 close-notify 警告消息后才能关闭连接
Session Timeout	SSL服务器端策略会话缓存的超时时间，单位为秒
Session Cachesize	SSL服务器端策略可以缓存的最大会话数目
Client-verify	SSL服务器端策略的客户端验证模式，取值包括： • disabled：不要求对客户端进行身份验证 • enabled：要求对客户端进行身份验证

字段	描述
Client-verify weaken	是否使能SSL客户端弱认证功能，取值包括 • disabled：未使能该功能 • enabled：使能该功能

1.1.7 handshake timeout

【命令】

handshake timeout *time*

undo handshake timeout

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

time：握手连接的保持时间，取值范围为 180～7200，单位为秒。

【描述】

handshake timeout 命令用来配置 SSL 服务器端策略的握手连接保持时间。**undo handshake timeout** 命令用来恢复缺省情况。

缺省情况下，SSL 服务器端策略的握手连接保持时间为 3600 秒。

如果 SSL 服务器在握手连接保持时间内没有收到 SSL 客户端的报文，则 SSL 服务器将终止当前的 SSL 握手过程。

相关配置可参考命令 **display ssl server-policy**。

【举例】

配置 SSL 服务器端策略的握手连接保持时间为 3000 秒。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

1.1.8 pki-domain

【命令】

pki-domain *domain-name*

undo pki-domain

【视图】

SSL 服务器端策略视图/SSL 客户端策略视图

【缺省级别】

2：系统级

【参数】

domain-name：PKI 域的域名，为 1～15 个字符的字符串，不区分大小写。

【描述】

pki-domain 命令用来配置 SSL 服务器端策略或 SSL 客户端策略所使用的 PKI 域。**undo pki-domain** 命令恢复缺省情况。

缺省情况下，没有配置 SSL 服务器端策略和 SSL 客户端策略所使用 PKI 域。

需要注意的是，如果没有配置 SSL 服务器端策略所使用的 PKI 域，则 SSL 服务器自己生成证书，而无需从 CA 获取证书。

相关配置可参考命令 **display ssl server-policy** 和 **display ssl client-policy**。

【举例】

配置 SSL 服务器端策略所使用的 PKI 域为 server-domain。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

配置 SSL 客户端策略所使用的 PKI 域为 client-domain。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

1.1.9 prefer-cipher

【命令】

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** }

undo prefer-cipher

【视图】

SSL 客户端策略视图

【缺省级别】

2：系统级

【参数】

rsa_3des_ede_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 3DES_EDE_CBC 算法、MAC 算法采用 SHA。

rsa_aes_128_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位 AES_CBC 算法、MAC 算法采用 SHA。

rsa_aes_256_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 256 位 AES_CBC 算法、MAC 算法采用 SHA。

rsa_des_cbc_sha：密钥交换算法采用 RSA、数据加密算法采用 DES_CBC 算法、MAC 算法采用 SHA。

rsa_rc4_128_md5：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4 算法、MAC 算法采用 MD5。

rsa_rc4_128_sha：密钥交换算法采用 RSA、数据加密算法采用 128 位的 RC4 算法、MAC 算法采用 SHA。

【描述】

prefer-cipher 命令用来配置 SSL 客户端策略的首选加密套件。**undo prefer-cipher** 命令用来恢复缺省情况。

缺省情况下，SSL 客户端策略的首选加密套件为 **rsa_rc4_128_md5**。

相关配置可参考命令 **display ssl client-policy**。

【举例】

配置 SSL 客户端策略的首选加密套件为 **rsa_aes_128_cbc_sha**。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

1.1.10 server-verify enable

【命令】

server-verify enable

undo server-verify enable

【视图】

SSL 客户端策略视图

【缺省级别】

2：系统级

【参数】

无

【描述】

server-verify enable 命令用来使能基于证书的 SSL 服务器身份验证，即在 SSL 握手过程中，客户端需要对服务器端进行基于证书的身份验证。**undo server-verify enable** 命令用来关闭基于证书的 SSL 服务器身份验证功能，默认 SSL 服务器身份合法。

缺省情况下，需要进行基于证书的 SSL 服务器身份验证。

相关配置可参考命令 **display ssl client-policy**。

【举例】

配置握手过程中，客户端需要对服务器端进行基于证书的身份验证。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] server-verify enable
```

1.1.11 session

【命令】

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

【视图】

SSL 服务器端策略视图

【缺省级别】

2：系统级

【参数】

cachesize *size*：缓存的最大会话数目，*size* 取值范围为 100～1000。

timeout *time*：会话缓存的超时时间，*time* 取值范围为 1800～72000，单位为秒。

【描述】

session 命令用来配置缓存的最大会话数目和会话缓存的超时时间。**undo session** 命令用来恢复缓存的最大会话数目或会话缓存超时时间为缺省情况。

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。

通过 SSL 握手协议协商会话参数并建立会话的过程比较复杂。为了简化 SSL 握手过程，SSL 允许重用已经协商过的会话参数建立会话。为此，SSL 服务器上需要保存已有的会话信息。保存的会话信息的数目和保存时间具有一定的限制：

- 如果缓存的会话数目达到最大值，SSL 将拒绝缓存新的会话；
- 会话保存的时间超过设定的时间后，SSL 将删除该会话的信息。

相关配置可参考命令 **display ssl server-policy**。

【举例】

配置会话缓存的超时时间为 4000 秒，缓存的最大会话数目为 600 个。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

1.1.12 ssl client-policy

【命令】

ssl client-policy *policy-name*

undo ssl client-policy { *policy-name* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：SSL 客户端策略名，为 1～16 个字符的字符串，不区分大小写，该字符串不能是“a”，“al”和“all”。

all：所有 SSL 客户端策略。

【描述】

ssl client-policy 命令用来创建 SSL 客户端策略，并进入 SSL 客户端策略视图。**undo ssl client-policy** 命令用来删除已创建的 SSL 客户端策略。

相关配置可参考命令 **display ssl client-policy**。

【举例】

创建名为 policy1 的 SSL 客户端策略，并进入该 SSL 客户端策略视图。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

1.1.13 ssl server-policy

【命令】

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

policy-name：SSL 服务器端策略名，为 1～16 个字符的字符串，不区分大小写，该字符串不能是“a”，“al”和“all”。

all：所有的 SSL 服务器端策略。

【描述】

ssl server-policy 命令用来创建 SSL 服务器端策略，并进入 SSL 服务器端策略视图。**undo ssl server-policy** 命令用来删除已创建的 SSL 服务器端策略。

需要注意的是，SSL 服务器端策略与应用层协议关联后，无法删除该策略。

相关配置可参考命令 **display ssl server-policy**。

【举例】

创建名为 policy1 的 SSL 服务器端策略，并进入该 SSL 服务器端策略视图。

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

1.1.14 version

【命令】

version { **ssl3.0** | **tls1.0** }

undo version

【视图】

SSL 客户端策略视图

【缺省级别】

2：系统级

【参数】

ssl3.0：版本号为 SSL 3.0。

tls1.0：版本号为 TLS 1.0。

【描述】

version 命令用来配置 SSL 客户端策略使用的 SSL 协议版本。**undo version** 命令恢复缺省情况。

缺省情况下，SSL 客户端策略使用的 SSL 协议版本号为 TLS 1.0。

相关配置可参考命令 **display ssl client-policy**。

【举例】

配置 SSL 客户端策略使用的 SSL 协议版本号为 SSL 3.0。

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version ssl3.0
```