IPsec加密AC与AP间隧道配置举例

陈少华 2016-08-10 发表

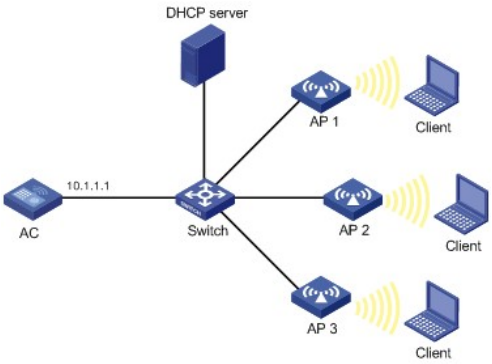
AP 1、AP 2和AP 3通过交换机与AC建立连接，接入的AP通过DHCP server获取IP地址。为了保证AC和某些AP之间的隧道安全性，使用IPsec加密AC与AP间隧道，具体要求如下：

(1). AP 1和AC之间的隧道不需要加密，即隧道间的数据和控制报文均使用明文方式传输。

(2). 为了保证AP 2和AC隧道之间控制报文的安全性，使用IPsec加密AC与AP间控制隧道。

(3). 为了保证AP 3和AC隧道之间控制报文和数据报文的安全性，使用IPsec加密AC与AP间控制和数据隧道。

图1 IPsec加密AC与AP间隧道配置组网图



(1)配置DHCP服务器

假设DHCP服务器为AP 1分配的IP地址范围为10.1.1.1～10.1.1.10，为AP 2分配的IP地址范围为10.1.1.11～10.1.1.20，为AP 3分配的IP地址范围为10.1.1.21～10.1.1.30。关于DHCP服务器的具体配置请参见“三层技术配置指导”中的“DHCP”。

(2)配置AC

创建并进入AP 2的配置视图，配置AP使用IPsec密钥12345来加密控制隧道，并将配置信息保存到AP的私有配置文件中。

<AC> system-view

[AC] wlan ap ap2 model WA2620E-AGN

[AC-wlan-ap-ap2] provision

[AC-wlan-ap-ap2-prvs] tunnel encryption ipsec pre-shared-key simple 12345

[AC-wlan-ap-ap2-prvs] save wlan ap provision name ap2

[AC-wlan-ap-ap2-prvs] quit

[AC-wlan-ap-ap2] quit

创建并进入AP 3的配置视图，配置AP使用IPsec密钥abcde来加密控制和数据隧道，并将配置信息保存到AP的私有配置文件中。

[AC] wlan ap ap3 model WA2620E-AGN

[AC-wlan-ap-ap3] provision

[AC-wlan-ap-ap3-prvs] tunnel encryption ipsec pre-shared-key simple abcde

[AC-wlan-ap-ap3-prvs] data-tunnel encryption enable

[AC-wlan-ap-ap3-prvs] save wlan ap provision name ap3

[AC-wlan-ap-ap3-prvs] return

手动重启AP 2和AP 3，使配置信息生效。

<AC> reset wlan ap name ap2

<AC> reset wlan ap name ap3

配置IPsec安全提议。

<AC> system-view

[AC] ipsec transform-set tran1

[AC-ipsec-transform-set-tran1] encapsulation-mode tunnel

[AC-ipsec-transform-set-tran1] transform esp

[AC-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128

[AC-ipsec-transform-set-tran1] esp authentication-algorithm sha1

[AC-ipsec-transform-set-tran1] quit

创建一个名称为1的ike提议。

[AC] ike proposal 1

[AC-ike-proposal-1]encryption-algorithm aes-cbc 128

[AC-ike-proposal-1] dh group2

[AC-ike-proposal-1] quit

配置ISAKMP SA向AP发送Keepalive报文的时间间隔为20秒。

[AC] ike sa keepalive-timer interval 20

配置ISAKMP SA等待AP发送Keepalive报文的超时时间为60秒。
[AC] ike sa keepalive-timer timeout 60
使能IPsec无效SPI恢复功能。
[AC] ipsec invalid-spi-recovery enable
配置IKE对等体ap2，对等体peer1用来为AP 2和AC协商SA，预共享密钥必须和AP 2上的预共享密钥保持一致。
[AC] ike peer ap2
[AC-ike-peer-ap2] remote-address 10.1.1.11 10.1.1.20
[AC-ike-peer-ap2] pre-shared-key 12345
[AC-ike-peer-ap2] proposal 1
[AC-ike-peer-ap2] quit
配置IKE对等体ap3，对等体peer1用来为AP 3和AC协商SA，预共享密钥必须和AP 3上的预共享密钥保持一致。
[AC] ike peer ap3
[AC-ike-peer-ap3] remote-address 10.1.1.21 10.1.1.30
[AC-ike-peer-ap3] pre-shared-key abcde
[AC-ike-peer-ap3] proposal 1
[AC-ike-peer-ap3] quit
创建一个模板名字为pt，顺序号为1的IPsec安全策略模板。配置IPsec安全策略所引用的安全提议为tran1，引用的IKE对等体为ap2。
[AC] ipsec policy-template pt 1
[AC-ipsec-policy-template-pt-1] transform-set tran1
[AC-ipsec-policy-template-pt-1] ike-peer ap2
[AC-ipsec-policy-template-pt-1] quit
创建一个模板名字为pt，顺序号为2的IPsec安全策略模板。配置IPsec安全策略所引用的安全提议为tran1，引用的IKE对等体为ap3。
[AC] ipsec policy-template pt 2
[AC-ipsec-policy-template-pt-2] transform-set tran1
[AC-ipsec-policy-template-pt-2] ike-peer ap3
[AC-ipsec-policy-template-pt-2] quit
引用IPsec安全策略模板pt创建名为map，顺序号为1的一条IPsec安全策略。
[AC] ipsec policy map 1 isakmp template pt
在VLAN接口上应用IPsec策略。
[AC] interface vlan-interface 1
[AC-Vlan-interface-1] ip address 10.1.1.1 24
[AC-Vlan-interface-1] ipsec policy map
在VLAN接口上应用IPsec策略，不会影响AP 1以明文方式和AC建立隧道。

结果验证，以AP 2为例，完成以上配置后，AP 2和AC之间如果有Join request控制报文通过，将触发IKE进行协商建立SA，使用**display ipsec sa**命令可以查看到建立的SA联盟。IKE协商成功并创建了SA后，AP 2和AC之间的控制报文将被加密传输。