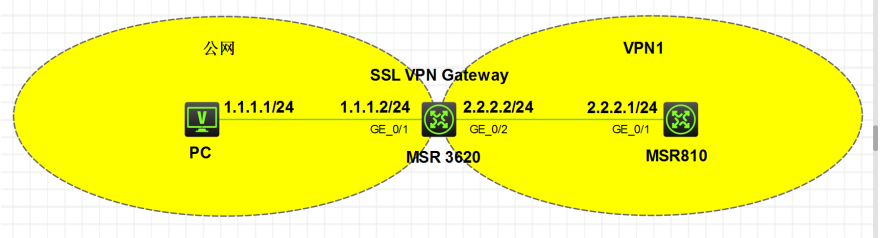
SSL VPN Web接入典型配置

李政 2017-12-21 发表

SSL VPN常见接入方式包括web接入方式、TCP接入方式以及IP接入方式，常见的部署方式包括单臂模式和双臂模式。本文介绍采用web接入方式的SSL VPN双臂模式参考配置



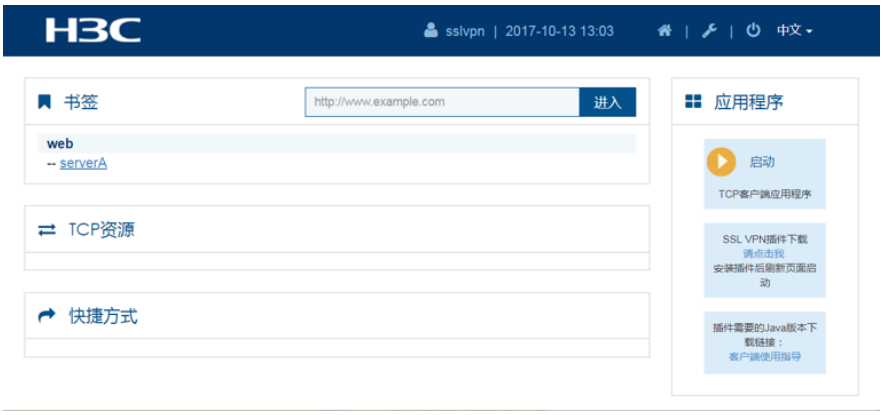
在配置之前首先确认如下信息：

1. SSL VPN网关设备已创建VPN实例
2. SSL VPN网关已获取CA证书ca.cer和服务器证书server.pfx
3. SSL VPN网关与其他设备路由可达

配置PKI域sslvpn。
<Gateway> system-view
[Gateway] pki domain sslvpn
[Gateway-pki-domain-sslvpn] public-key rsa general name sslvpn
[Gateway-pki-domain-sslvpn] undo crl check enable
[Gateway-pki-domain-sslvpn] quit
导入CA证书ca.cer和服务器证书server.pfx。
[Gateway] pki import domain sslvpn der ca filename ca.cer
[Gateway] pki import domain sslvpn p12 local filename server.pfx
配置SSL服务器端策略ssl。
[Gateway] ssl server-policy ssl
[Gateway-ssl-server-policy-ssl] pki-domain sslvpn
[Gateway-ssl-server-policy-ssl] quit
配置SSL VPN网关gw的IP地址为1.1.1.2，端口号为2000，并引用SSL服务器端策略ssl。
[Gateway] sslvpn gateway gw
[Gateway-sslvpn-gateway-gw] ip address 1.1.1.2 port 2000
[Gateway-sslvpn-gateway-gw] ssl server-policy ssl
开启SSL VPN网关gw。
[Gateway-sslvpn-gateway-gw] service enable
[Gateway-sslvpn-gateway-gw] quit
配置SSL VPN访问实例ctx1引用SSL VPN网关gw，指定域名为domain1，并配置SSL VPN访问实例关联的VPN实例为VPN1。
[Gateway] sslvpn context ctx1
[Gateway-sslvpn-context-ctx1] gateway gw domain domain1
[Gateway-sslvpn-context-ctx1] vpn-instance VPN1
创建URL列表urllist。
[Gateway-sslvpn-context-ctx1] url-list urllist
配置URL列表标题为web。
[Gateway-sslvpn-context-ctx1-url-list-urllist] heading web
添加一个URL表项，链接名为serverA，对应的URL为2.2.2.1。
[Gateway-sslvpn-context-ctx1-url-list-urllist] url serverA url-value http://2.2.2.1
[Gateway-sslvpn-context-ctx1-url-list-urllist] quit
SSL VPN访问实例ctx1下创建策略组pgroup，引用Web资源，并指定其为缺省策略组。
[Gateway-sslvpn-context-ctx1] policy-group pgroup
[Gateway-sslvpn-context-ctx1-policy-group-pgroup] resource url-list urllist
[Gateway-sslvpn-context-ctx1-policy-group-pgroup] quit
[Gateway-sslvpn-context-ctx1] default-policy-group pgroup
开启SSL VPN访问实例ctx1。
[Gateway-sslvpn-context-ctx1] service enable
[Gateway-sslvpn-context-ctx1] quit
创建本地SSL VPN用户sslvpn，密码为111111，用户角色为network-operator，授权用户的SSL VPN策略组为pgroup。
[Gateway] local-user sslvpn class network
[Gateway-luser-network-sslvpn] password simple 111111

[Gateway-luser-network-sslvpn] service-type sslvpn
[Gateway-luser-network-sslvpn] authorization-attribute user-role network-operator
[Gateway-luser-network-sslvpn] authorization-attribute sslvpn-policy-group pgroup
[Gateway-luser-network-sslvpn] quit
4. 验证配置
在Gateway上查看SSL VPN网关状态，可见SSL VPN网关gw处于Up状态。
[Gateway] display sslvpn gateway
Gateway name: gw
  Operation state: Up
  IP: 1.1.1.2 Port: 2000
  SSL server policy configured: ssl
  SSL server policy in use: ssl
  Front VPN instance： Not configured
在Gateway上查看SSL VPN访问实例状态，可见SSL VPN访问实例ctx1处于Up状态。
[Gateway] display sslvpn context
Context name: ctx1
  Operation state: Up
  AAA domain： Not specified
  Certificate authentication: Disabled
  Dynamic password: Disabled
  Verify code validation: Disabled
  Default policy group: pgroup
  Associated SSL VPN gateway:gw
  Domain name: domain1
  SSL client policy configured: ssl
  SSL client policy in use: ssl
  Maximum users allowed: 1048575
  VPN instance: VPN1
  Idle timeout: 30 min

验证：
在浏览器上输入https://2.2.2.1



1. 配置前需确认导入CA证书以及服务器证书，CA证书获取方式可参考

2. web接入方式利用浏览器直接登录即可