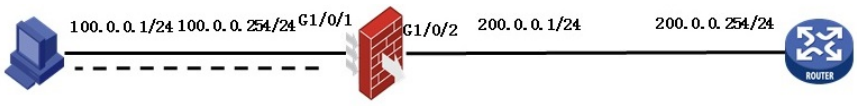
V7防火墙调用设备默认证书的IP接入本地SSL VPN认证典型配置

樊金帅 2018-03-10 发表

V7防火墙设备作为内网入口，客户PC通过iNode拨入，采用的认证类型为local、认证模式为密码认证，设备不导入ca.cer、server.pfx证书，调用默认证书（dir里看不到默认证书），认证成功后采用IP资源方式访问内网。



1.F1030上SSL VPN相关配置

配置PKI域sslvpn

[F1030] pki domain sslvpn

[F1030-pki-domain-sslvpn] public-key rsa general name sslvpn

[F1030-pki-domain-sslvpn] undo crl check enable

[F1030-pki-domain-sslvpn] quit

配置SSL VPN网关gw的IP地址为100.0.0.254，端口号为2000

[F1030] sslvpn gateway gw //默认情况下端口号即为443，建议修改，避免与https默认管理端口冲突

[F1030-sslvpn-gateway-gw] ip address 100.0.0.254 port 2000

开启SSL VPN网关gw

[F1030-sslvpn-gateway-gw] service enable

[F1030-sslvpn-gateway-gw] quit

创建地址池ippool，指定IP地址范围为10.1.1.1——10.1.1.10

[F1030] sslvpn ip address-pool ippool 10.1.1.1 10.1.1.10

创建SSL VPN AC接口1，配置接口的IP地址为10.1.1.100/24

[F1030] interface sslvpn-ac 1

[F1030-SSLVPN-AC1] ip address 10.1.1.100 24

[F1030-SSLVPN-AC1] quit

配置SSL VPN访问实例ctx引用SSL VPN网关gw

[F1030] sslvpn context ctx

[F1030-sslvpn-context-ctx] gateway gw

#调用ip接入地址池ippool

[F1030-sslvpn-context-ctx] ip-tunnel address-pool ippool mask 255.255.255.0

#创建路由列表rtlist，并添加路由表项200.0.0.0/24

[F1030-sslvpn-context-ctx] ip-route-list rtlist

[F1030-sslvpn-context-ctx-route-list-rtlist] include 200.0.0.0 255.255.255.0

[F1030-sslvpn-context-ctx-route-list-rtlist] quit

配置SSL VPN访问实例ctx引用SSL VPN AC接口1

[F1030-sslvpn-context-ctx] ip-tunnel interface sslvpn-ac 1

创建SSL VPN策略组pgroup，引用路由列表rtlist，并且通过acl限制，保证只有通过ACL检查的报文才可以访问IP资源

[F1030-sslvpn-context-ctx] policy-group pgroup

[F1030-sslvpn-context-ctx-policy-group-pgroup] ip-tunnel access-route ip-route-list rtlist

[F1030-sslvpn-context-ctx-policy-group-pgroup] filter ip-tunnel acl 3000 //必配

[F1030-sslvpn-context-ctx-policy-group-pgroup] quit

开启SSL VPN访问实例ctx。

[F1030-sslvpn-context-ctx] service enable

[F1030-sslvpn-context-ctx] quit

#创建SSLVPN本地用户

local-user h3c class network

 password cipher c3$UxwgdMpL62TJ3k1ftN3CAHz/CK73/uxD0A==

 service-type sslvpn

 authorization-attribute user-role network-operator

 authorization-attribute sslvpn-policy-group pgroup

2.F1030上域间策略相关配置
GigabitEthernet1/0/1、GigabitEthernet1/0/2加入Trust区域，SSLVPN-AC1加入SSLVPN区域，并放通策略。
#
security-zone name Trust
 import interface GigabitEthernet1/0/1
 import interface GigabitEthernet1/0/2
#
security-zone name SSLVPN
 import interface SSLVPN-AC1
#
acl number 3000
rule 0 permit ip
#
acl number 3010
 rule 0 permit ip source 10.1.1.0 0.0.0.255 destination 200.0.0.0 0.0.0.255
 rule 5 permit ip source 200.0.0.0 0.0.0.255 destination 10.1.1.0 0.0.0.255
#
zone-pair security source SSLVPN destination Trust
 packet-filter 3010
#
zone-pair security source Trust destination SSLVPN
 packet-filter 3010
#
zone-pair security source Trust destination Local
packet-filter 3000
#
zone-pair security source Local destination Trust

packet-filter 3000

3、验证

拨号成功后可以看到网关分配给主机的虚拟IP地址：

1、不需要导入CA证书ca.cer和服务器证书server.pfx
2、不需要配置SSL服务器端策略
3、网关不需要引用SSL服务器端策略
4、SSL VPN-AC需要加入安全域并放通策略