双向NAT解决地址更改问题

说明：

通过IPSec的地址映射的方式来解决分支机构的IP地址混乱重叠等问题。

拓扑：

如下图所示，总部为固定IP，内网地址段位10.0.1.0/24, 分支机构为动态IP，内网地址段位192.168.1.0/24。我们给分支机构分配了地址段为10.0.2.0/24，用于VPN互联，也就是说凡是192.186.1.0网段均需映射到10.0.2.0网段，才能访问总部内网。



步骤：

首先配置中心防火墙的IPsec VPN，配置方法与正常配置相同。

（一）首先配置阶段1。远程网关选择“连接用户”，本地接口选择公网接口。“接口模式”也可以启用也可以不启用。本例中不启用。



（二）然后配置。阶段2。设置“保持存活”。在快速模式匹配器中，设置源地址为总部内网“10.0.1.0/24”，目标地址是分支机构的内网地址。因为分支机构很多，可能是10.0.2.0， 也可能是10.0.3.0，所以我们干脆用10.0.0.0/8来替代它。



（三）配置IPSec防火墙策略，源地址设置成总部内网地址，目标地址设置成涵盖分支机构的所有地址段10.0.0.0。动作选为ipsec，通道则选为前面所设置成的阶段1.



然后配置分支机构，以10.0.2.0为例。分支机构采用接口模式，目的是方便映射。

(一) 首先设置阶段1。设置远程网关为静态IP地址，IP地址为总部公网地址。启用接口模式。



(二) 设置阶段2， 启用保持存活， 源地址设置成分配给分支机构的网段，目标地址设置成总部内网。



（三）设置地址转换。在防火墙的虚拟IP中，做10.0.2.1到192.168.1.0网段的映射，接口选为vpn的虚拟接口“分支”



（四）设置从内到VPN的防火墙策略，源接口设置内网接口，目标接口为VPN虚拟接口，设置启用NAT。



（五）设置从总部到分支的VPN策略。源接口为VPN虚拟接口，目标接口为内网接口，目标地址是所建立的虚拟IP。



（六） 配置路由。设置目标地址为10.0.1.0网段，接口为VPN虚拟接口。



完成如上配置后，VPN就可以通了。分支访问总部采用的是10.0.2.0网段。