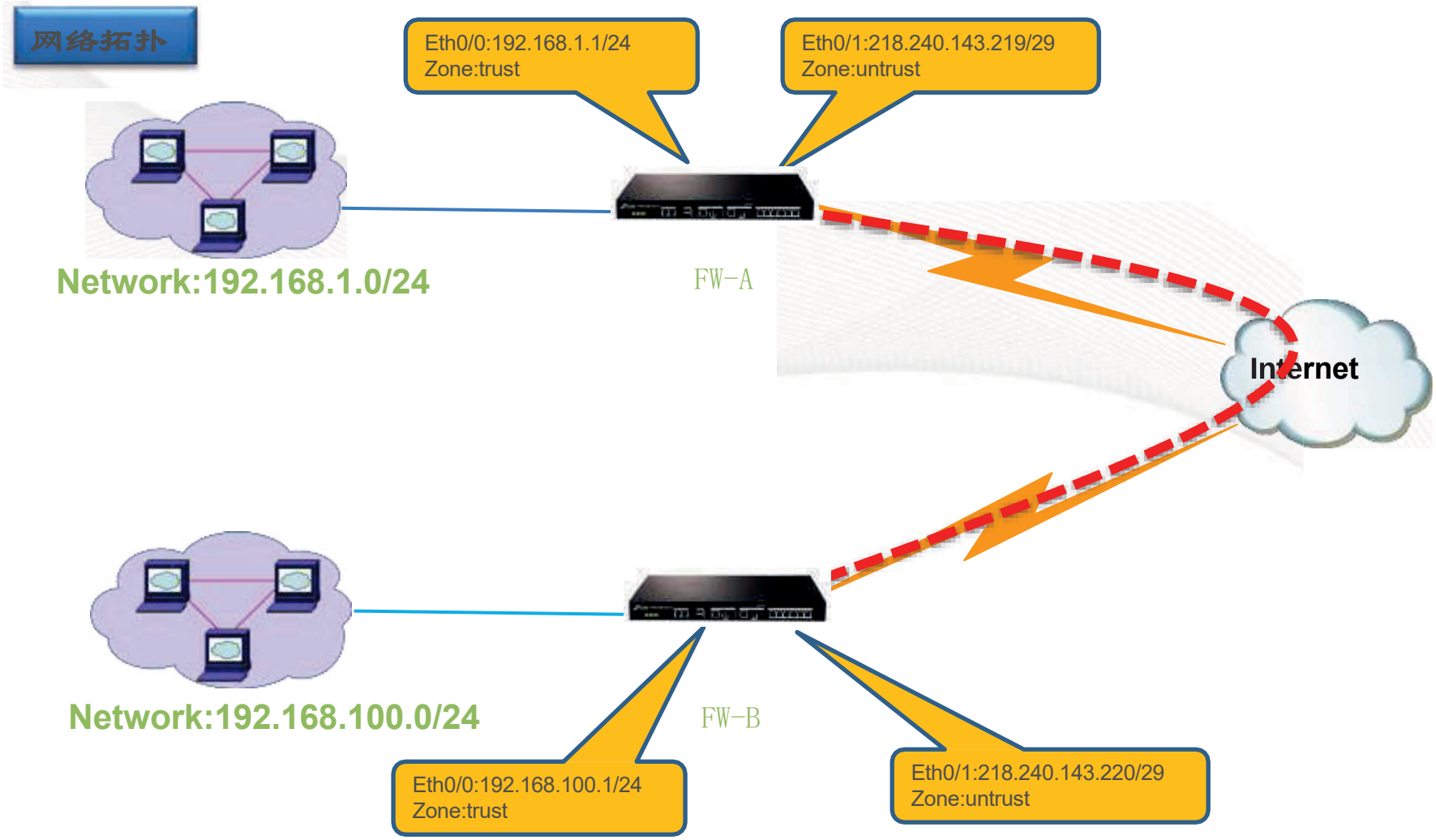
DCN | 神州数码 Digital China

IPSEC配置示例 FOR4.0R4

柳　鑫

DCN 客户服务中心

示例功能描述



注：该案例假设防火墙已完成了基本的上网配置

拓扑环境描述

- 防火墙FW-A和FW-B都具有合法的静态IP地址
- 其中防火墙FW-A的　　保护子网为192.168.1.0/24
- 防火墙FW-B的　　保护子网为192.168.100.0/24。

要求在FW-A与FW-B之间创建IPSec VPN，使两端的保护子网能通过VPN隧道互相访问。

FW-A 防火墙配置步骤

本案例采用“预共享密钥认证”机制

- 第一步，创建IKE第一阶段提议
- 第二步，创建IKE第二阶段提议
- 第三步，创建VPN对端
- 第四步，创建IPSEC隧道
- 第五步，创建基于隧道的安全策略
- 第六步，创建源NAT策略

第一步，创建IKE第一阶段提议

- 定义IKE第一阶段的协商内容，两台防火墙的IKE第一阶段协商内容需要一致。