

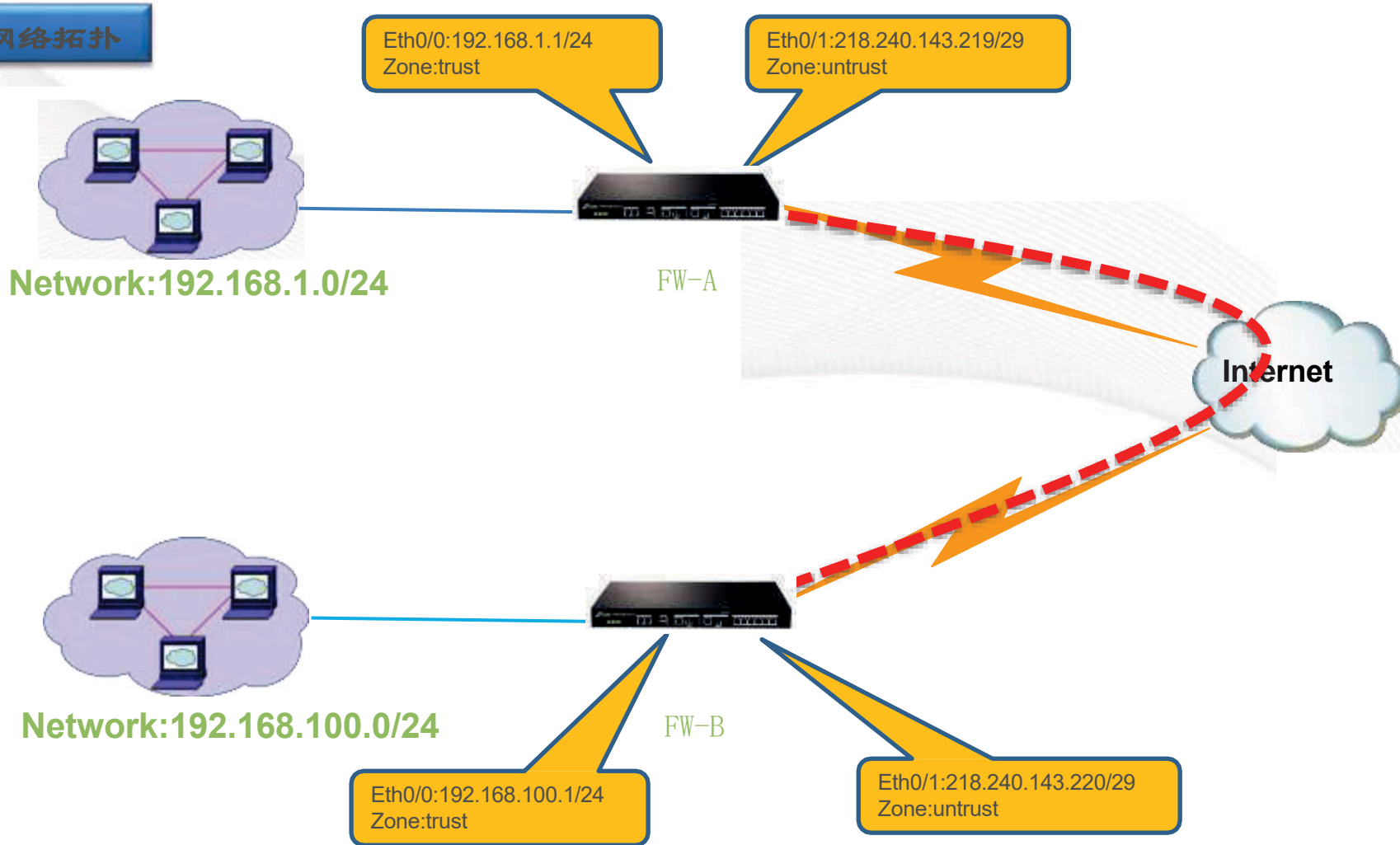
IPSEC配置示例 FOR4.0R4

柳 鑫

DCN 客户服务中心

示例功能描述

网络拓扑



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。

The screenshot illustrates the configuration process for an IKE Phase 1 proposal in a firewall management system. It is divided into three main sections:

- Left Panel (Navigation):** A tree view with categories like System, Objects, Users, Network, Firewall, and VPN. The **VPN** category is expanded, and **IPSec VPN** is selected, indicated by a red circle labeled '1'.
- Top Panel (Proposal List):** Shows tabs for 'IPSec VPN', 'VPN对端', 'P1提议', and 'P2提议'. The 'P1提议' tab is active, showing a list with a '新建...' (New...) button, indicated by a red circle labeled '3'.
- Bottom Panel (Configuration):** The '阶段1提议配置' (Phase 1 Proposal Configuration) dialog box is open. It contains the following fields:
 - 提议名称 (Proposal Name):** 'P1' (1~31 characters), indicated by a red circle labeled '4'.
 - 认证 (Authentication):** Radio buttons for Pre-shared Key (selected), RSA Signature, MD5, SHA-1 (selected), SHA256, SHA384, and SHA512.
 - 验证算法 (Verification Algorithm):** Radio buttons for 3DES, DES, AES-128, AES-192, and AES-256.
 - 加密算法 (Encryption Algorithm):** Radio buttons for Group 1, Group 2 (selected), and Group 5.
 - 生存时间 (Lifetime):** '86400' (300~86400 seconds, default 86400).At the bottom of the dialog are '确认' (Confirm) and '取消' (Cancel) buttons, with a red circle labeled '5' around the Confirm button.

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/976214025105010212>