وثيقة متطلبات المشروع

إعداد اتصال Site-to-Site IPsec VPN (Cisco Routers)

وصف المشروع

المطلوب هو تنفيذ إعدادات شبكة خاصة افتراضية (VPN) من نوع Site-to-Site باستخدام بروتوكول IPsec لربط فرعين للشركة. يتم التنفيذ على أجهزة راوتر سيسكو (**R1** و **R3**) لتأمين حركة البيانات الصادرة والواردة بين الشبكات المحلية للفرعين.

المواصفات التقنية للشبكة

يجب الالتزام بالعناوين والبروتوكولات التالية لضمان نجاح الاتصال:

- **الشبكة المحلية للفرع الأول (R1 LAN):** 192.168.1.0/24
- **الشبكة المحلية للفرع الثاني (R3 LAN):** 192.168.3.0/24
- **خوارزمية التشفير (Encryption):** AES-256
- **بروتوكول التوثيق (Hashing):** SHA-256 أو SHA-1
- **مفتاح التشفير المشترك (Pre-shared Key):** vpnpa55
- **مجموعة ديفي-هيلمان (DH Group):** Group 5
- **بروتوكول الحماية:** IPsec ESP

المهام المطلوبة للتنفيذ

على المستقل تنفيذ الخطوات التالية بدقة:

1. **إعداد المرحلة الأولى (Phase 1):** تعريف ISAKMP Policy بالتشفير والتوثيق المطلوب.
2. **إعداد المرحلة الثانية (Phase 2):** إنشاء IPsec Transform-set (ESP-AES + ESP-SHA-HMAC).
3. **تحديد حركة البيانات (Interesting Traffic):** إنشاء قائمة تحكم بالوصول (ACL 110) لتحديد الترافيك المطلوب تشفيره بين الشبكتين.
4. **تطبيق الخريطة الأمنية (Crypto Map):** إنشاء Crypto Map وربطه بواجهة الـ WAN الخارجية لكل راوتر.
5. **التطابق (Mirroring):** التأكد من أن الإعدادات على R1 و R3 متطابقة بشكل عكسي لضمان نجاح المصافحة (Handshake).

الاختبار والتسليم

يُعتبر العمل منجزاً عند تحقيق النتائج التالية:

- نجاح إنشاء اتصال ISAKMP SA (الحالة: QM_IDLE).
- نجاح تبادل البيانات (Ping) بين الأجهزة في شبكة R1 وأجهزة شبكة R3.

- التأكد من أن حركة البيانات مشفرة عبر الأمر *show crypto engine connections active*.

ملاحظة: هذا المشروع يتطلب خبرة في أوامر *Cisco IOS Command Line*.