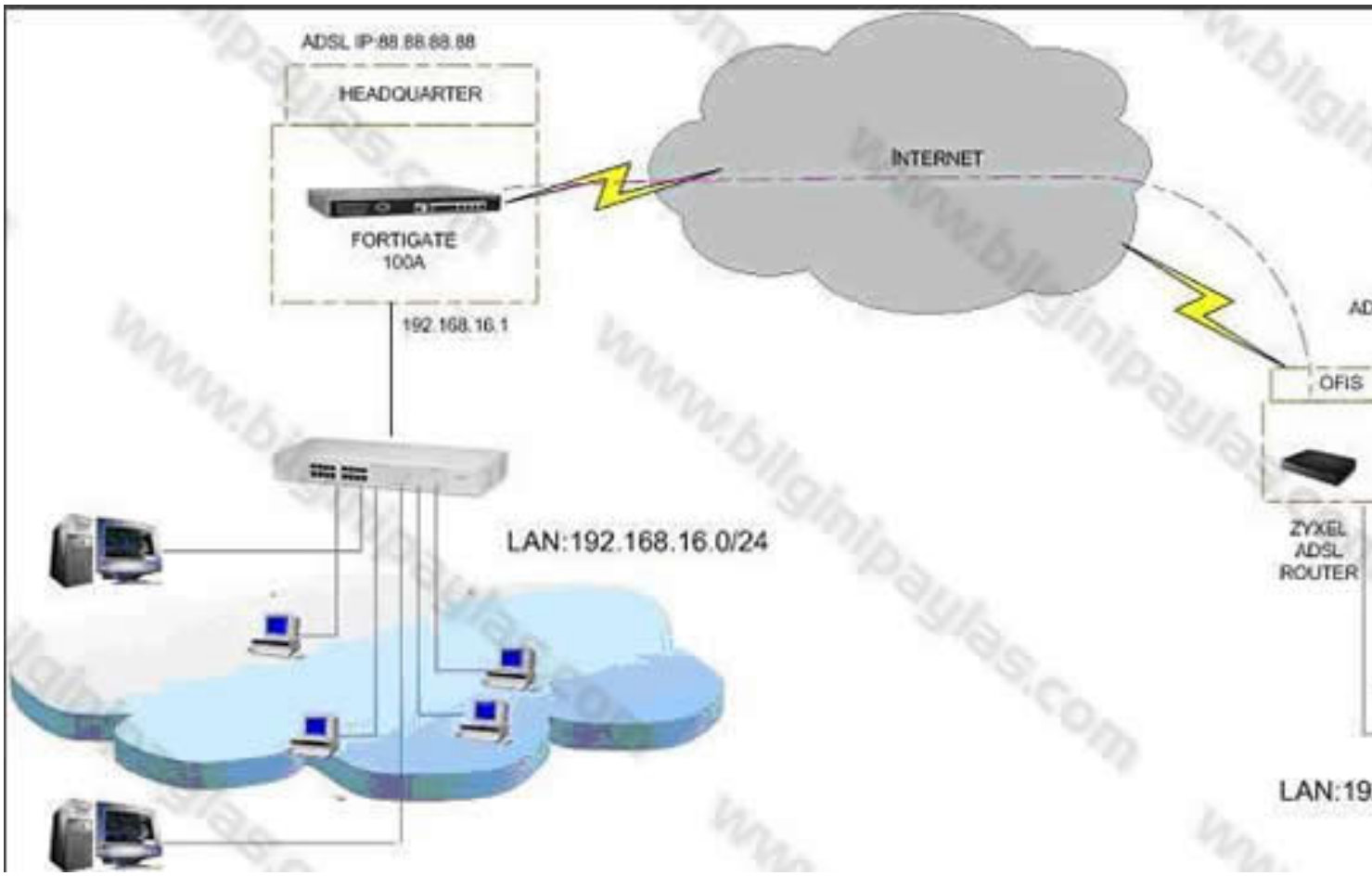
Bu makalede fortigate firewalla zyxel marka adsl modem arasinda noktadan noktaya IPSEC VPN baglantisinin nasil yapildigini anlatacagim.

{jcomments on}

Fortigate firewall merkezde yer alirken bölgelerde Zyxel P-662HW-D1 modeli adsl modem routerlar olan yapi kuruldu.

öncelikle temel kural iki newtorkteki subnetler ayni olmamasi gerekir.Makalede kullanilan topoloji asagida belirtilmittir.



Merkez Fortigate WAN IP:88.88.88.88

Fortigate Internal IP:192.168.16.1

Merkez Network.:192.168.16.0 /24

Bölge ADSL WAN IP:99.99.99.99

Bölge ADSL Internal IP:192.168.1.1

Bölge Network:192.168.1.0/24

Fortigate Tarafinda yapilan ayarlar:

Fortigate de IPSEC VPN konfigurasyonun yapilabilmesi için;

1.Fortigate in karsi ucun kimlik dogrulamasini yapabilmesi ve güvenli bir baglantinin saglanabilmesi için Phase 1 parametresi tanimlanir.

2.Fortigate in karsi uçla VPN tüneli kurabilmesi için Phase 2 paremetresi tanimlanir.

3.VPN tüneli içinden geçecek IP paketleri için kaynak ve hedef adresleri tanimlanir.

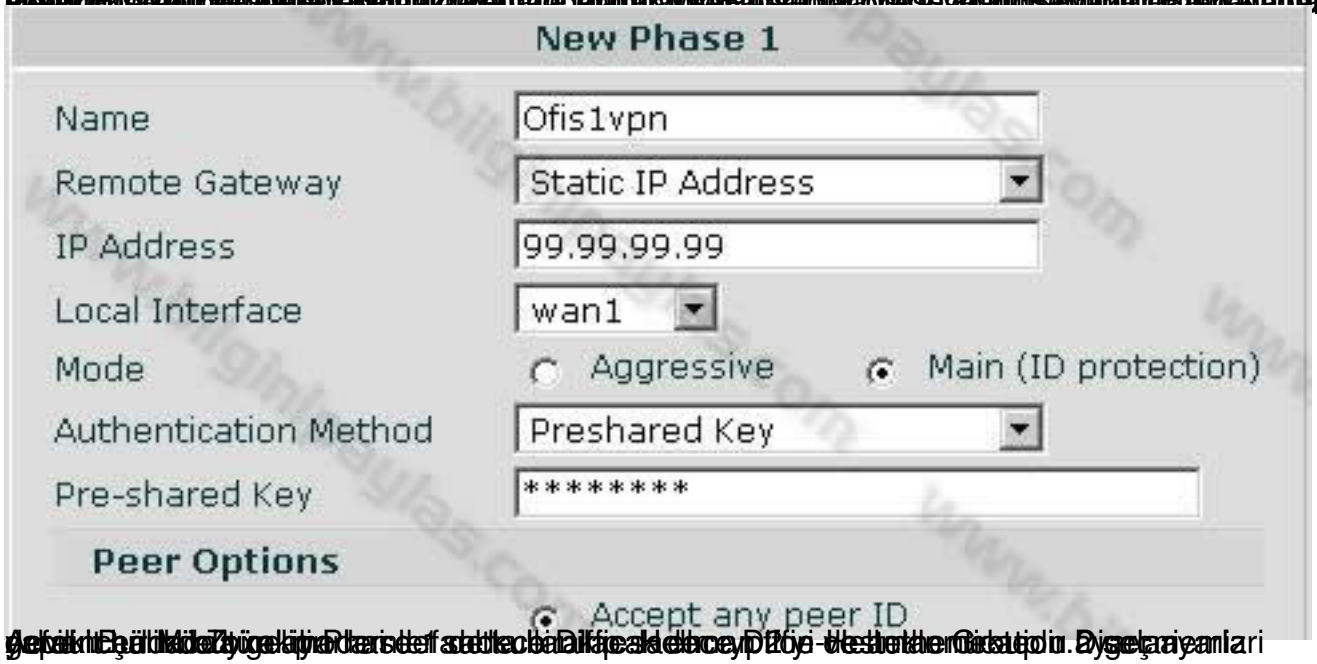
4.Kaynak ve hedef adresi arasinda sifreleme için kural tanimlanir ve izin verilen servisler firewallda belirtilir.

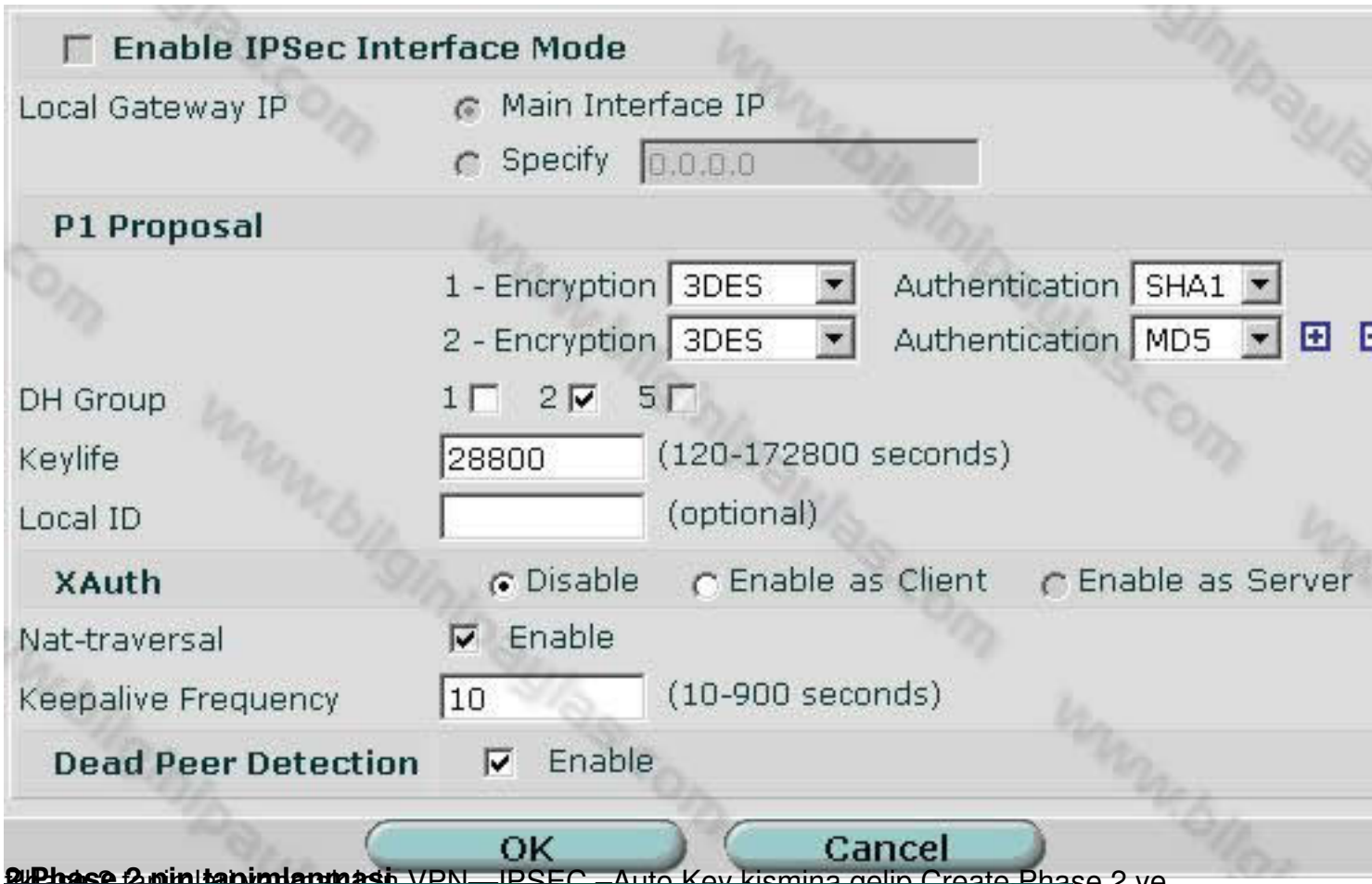
1.Phase 1 parametresinin tanimlanmasi:

Fortigate'in temel ayarlarinin yapildigi ve WAN1 bacaginda 88.88.88.88 ipsinin oldugu varsayilmistir.

Fortigate'in yönetim sayfasina gelip VPN kismindan öncelikle IPSEC baglantisi için Auto Kye (IKE) baglantisi için ayarlar yapilir.


System
Router
Firewall
VPN
IPSEC
PPTP
SSL
Certificates
Auto Key (IKE)
Manual Key
Co
Create Phase 1
Create Phase 2
Phase 1

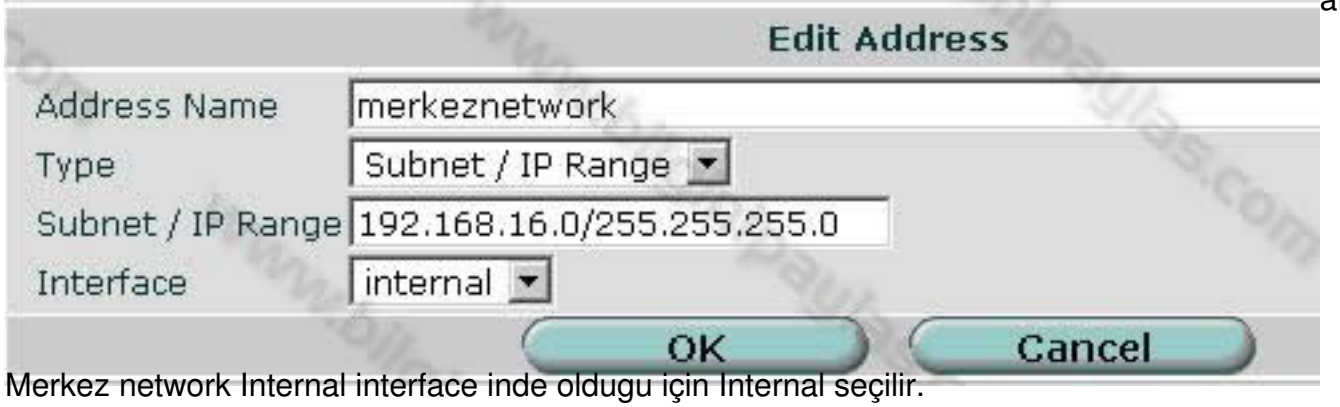

New Phase 1
Name
Ofis1vpn
Remote Gateway
Static IP Address
IP Address
99.99.99.99
Local Interface
wan1
Mode
Aggressive
Main (ID protection)
Authentication Method
Preshared Key
Pre-shared Key
****
Peer Options
Accept any peer ID



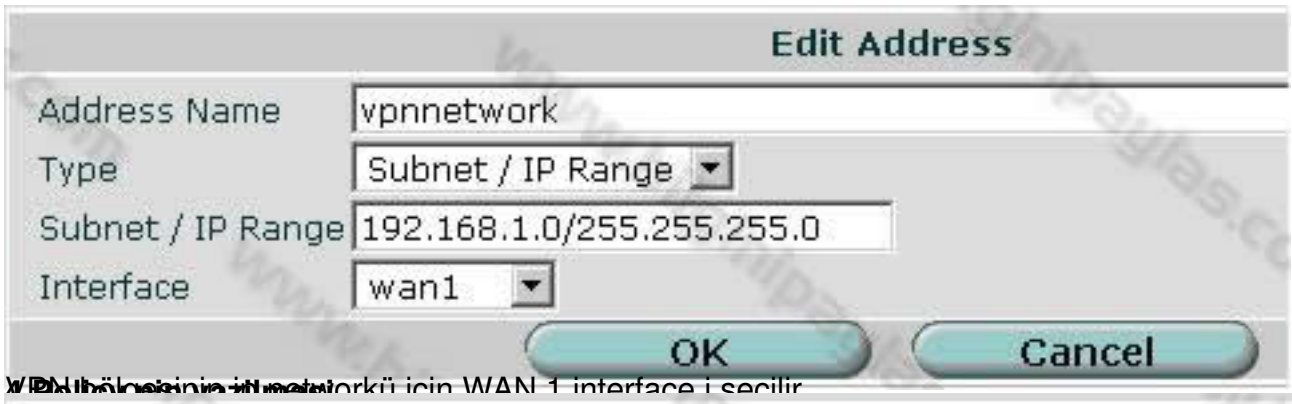
2Phase 2 nin tanimlanmasi VPN – IPSEC – Auto Key kismina gelip Create Phase 2 ye

tıklıyoruz. kismina isim verilir ve Phase 1 kisminda bir adim once tanimladigimiz Phase 1 tanimi saglıyoruz.

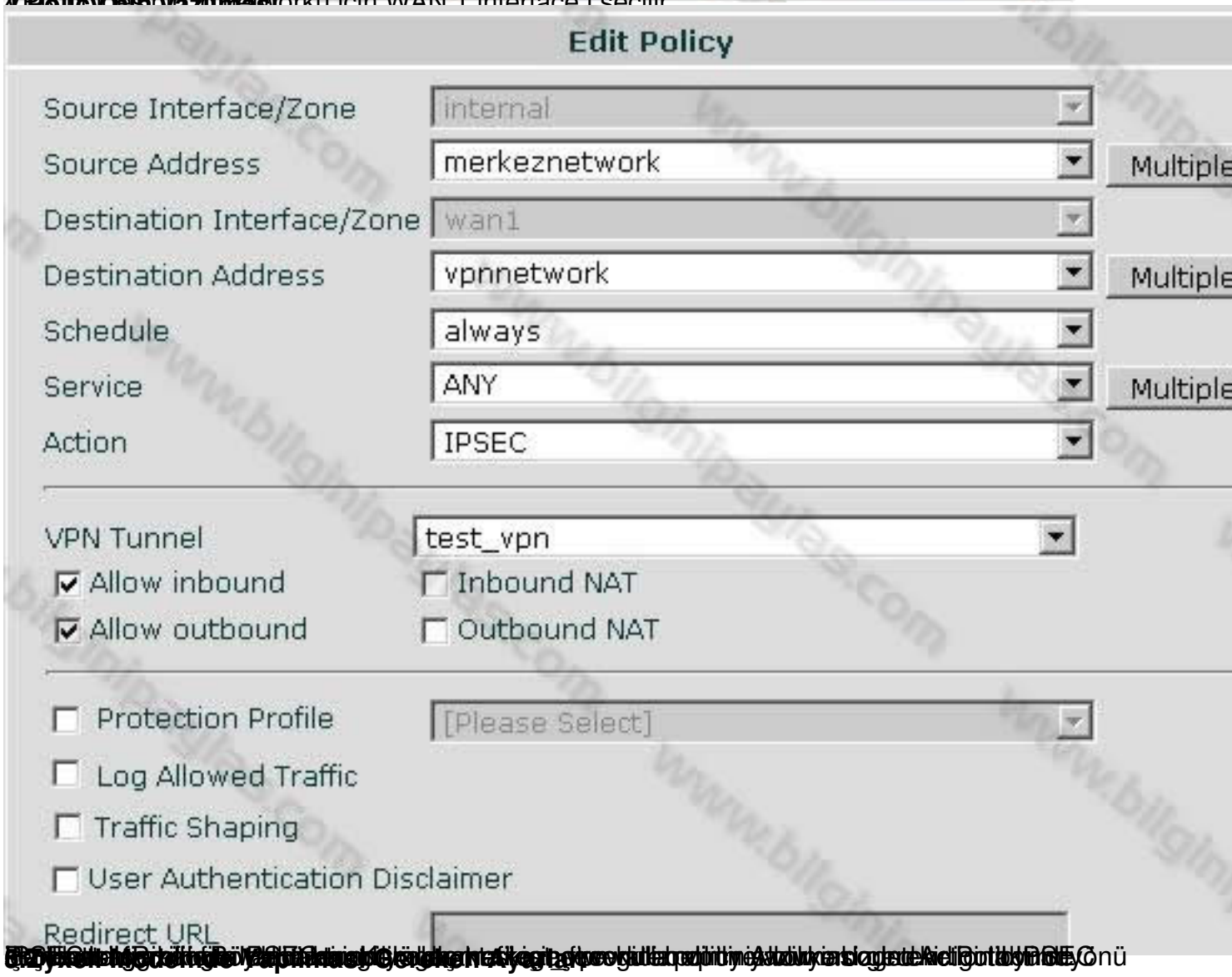
Create



Merkez network Internal interface inde oldugu için Internal seçilir.

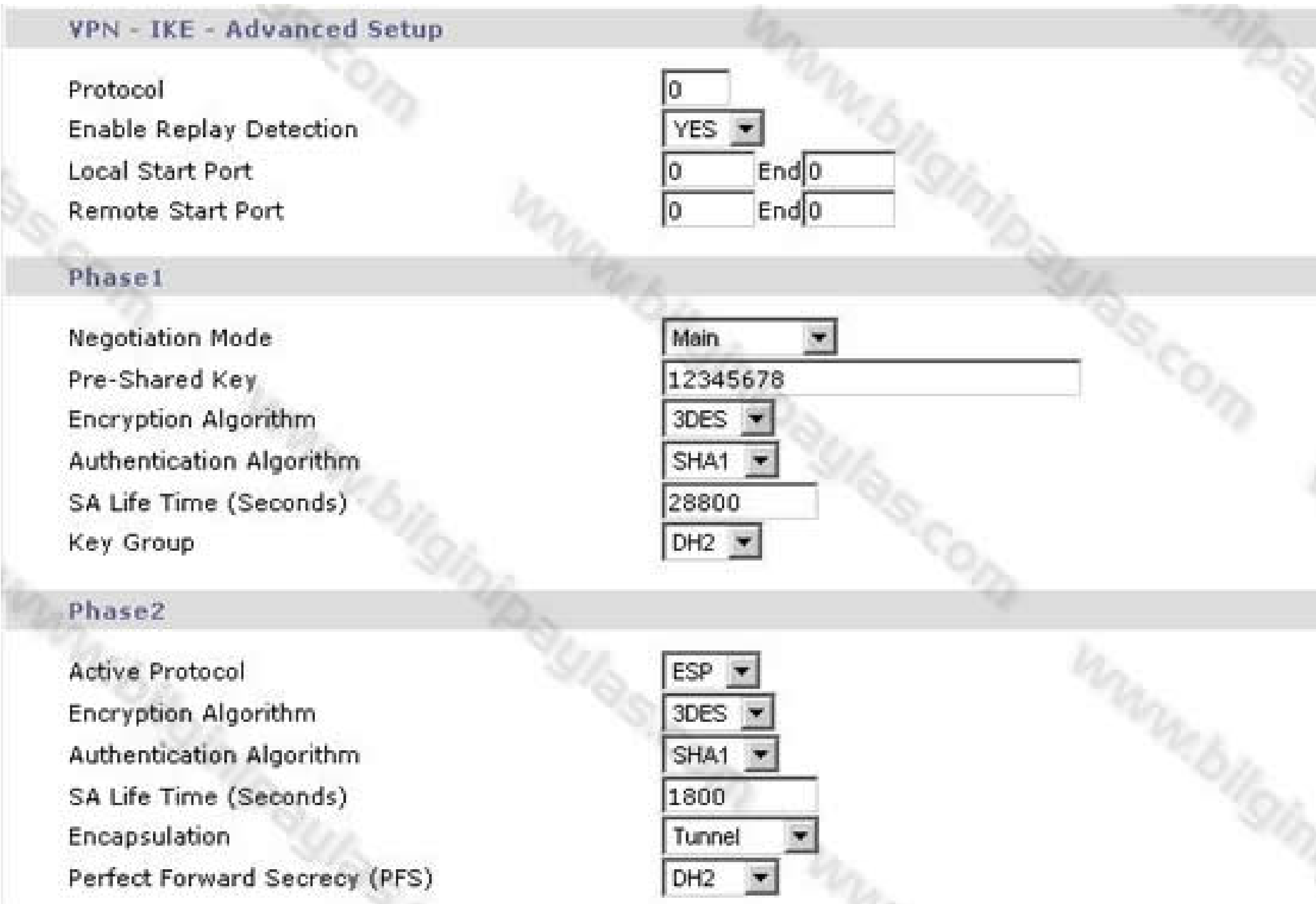


VPN bölgesinin ilgili networkü için WAN 1 interface i secilir



erişilebilir olduğu


Address Information
Local ID Type
E-mail
Content
99.99.99.99
My IP Address
99.99.99.99
Peer ID Type
IP
Content
88.88.88.88
Secure Gateway Address
88.88.88.88
Security Protocol
VPN Protocol
ESP
Pre-Shared Key
12345678
Certificate
auto_generated_self_signed_cert
Encryption Algorithm
3DES
Authentication Algorithm
SHA1
Advanced
Apply
Cancel



Enable Replay Detection aktif edilir çünkü fortigate in defaulunda Enable Replay Detection [illegible] ... dan IPSEC [illegible] bağlanti

2	01/01/2000 01:39:59	Rule [1] Tunnel built successfully		
3	01/01/2000 01:39:59	Adjust TCP MSS to 1390		
4	01/01/2000 01:39:59	Recv<:[HASH]>		
5	01/01/2000 01:39:59	Send<:[HASH][SA][NONCE][KE][ID][ID]>		
6	01/01/2000 01:39:57	Start Phase 2: Quick Mode		
7	01/01/2000 01:39:57	Recv<:[HASH][SA][NONCE][KE][ID][ID]>		
8	01/01/2000 01:39:25	Phase 1 IKE SA process done		
9	01/01/2000 01:39:25	Send<:[ID][HASH][NOTFY:INIT_CONTACT]>		
10	01/01/2000 01:39:25	Recv<:[ID][HASH][NOTFY:INIT_CONTACT]>		
11	01/01/2000 01:39:24	Send<:[KE][NONCE]>		
12	01/01/2000 01:39:24	Recv<:[KE][NONCE][UNKNOWN(130)][UNKN>		
13	01/01/2000 01:39:24	Send<:[SA][VID][VID]>		
14	01/01/2000 01:39:23	Recv<:[SA][VID][VID][VID][VID][VID][>		
15	01/01/2000 01:39:23	Recv Mode request from < >		
16	01/01/2000 01:39:23	Rule [1] Receiving IKE request		
17	01/01/2000 01:37:05	Send<:[HASH][DEL]>		