

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

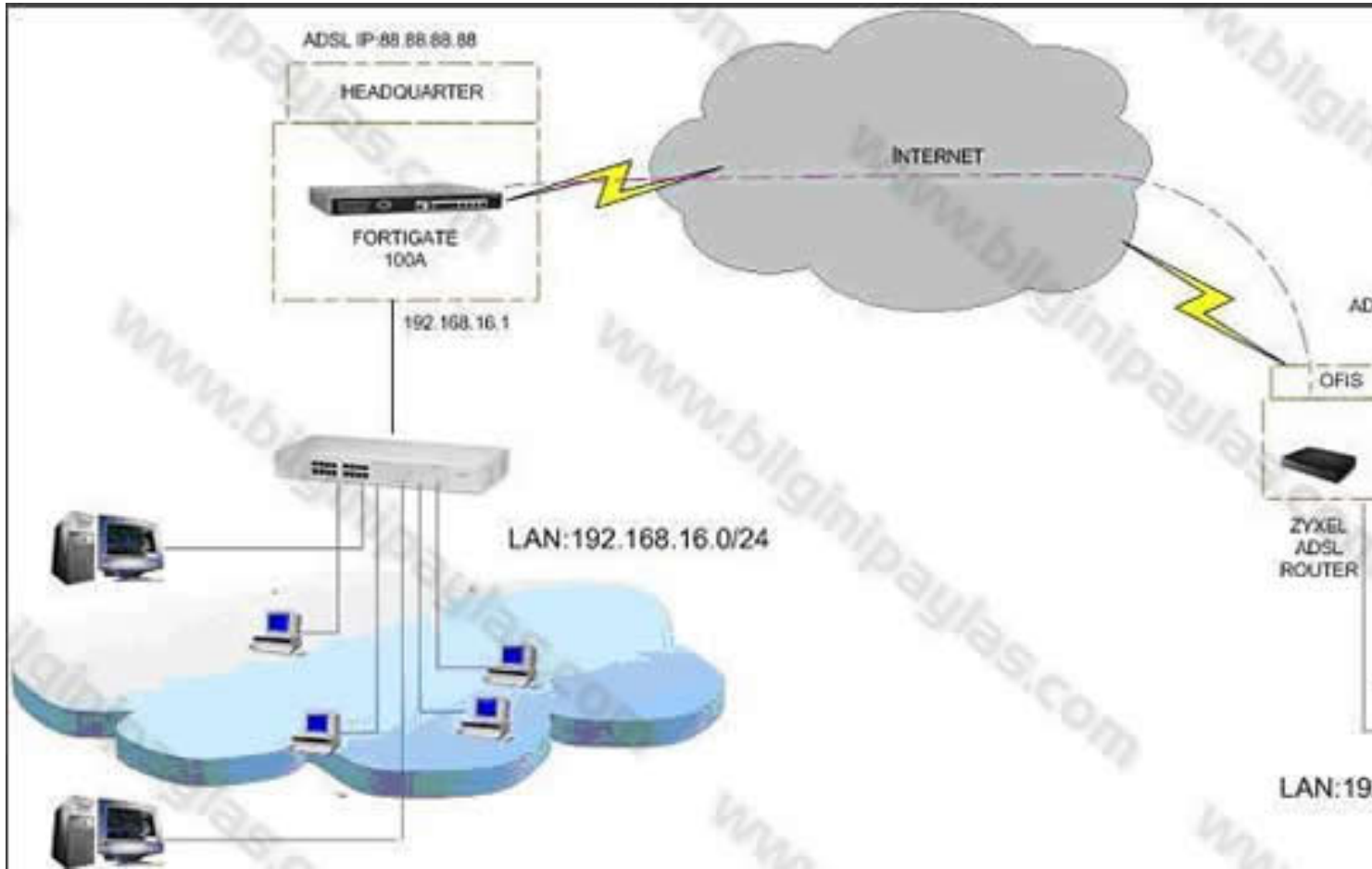
Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

Bu makalede fortigate firewalla zyxel marka adsl modem arasında noktadan noktaya IPSEC VPN bağlantısının nasıl yapıldığını anlatacağım.

{jcomments on}

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

öncelikle temel kural iki networkteki subnetler aynı olmaması gerekir. Makalede kullanılan topoloji aşağıda belirtilmiştir.



Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

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 Tarafında yapılan ayarlar:

Fortigate de IPSEC VPN konfigürasyonun yapılabilmesi için;

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

- 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 parametresi tanimlanir.
- 3.VPN tüneli içinden geçecek IP paketleri için kaynak ve hedef adresleri tanimlanir.
- 4.Kaynak ve hedef adresi arasında 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 Key (IKE) baglantisi için ayarlar yapilir.

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12



The image shows the Fortinet FortiGate web interface for configuring a VPN. The left sidebar contains a navigation menu with the following items: System, Router, Firewall, VPN (selected), IPSEC, PPTP, SSL, and Certificates. The main content area is titled 'Auto Key (IKE)' and 'Manual Key'. Below this, there are buttons for 'Create Phase 1' and 'Create Phase 2'. A dropdown menu shows 'Phase 1' selected. The 'New Phase 1' configuration page is displayed with the following fields:

- 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: *****

Below the main configuration fields, there is a section for 'Peer Options' with a radio button for 'Accept any peer ID'.

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

Enable IPsec Interface Mode

Local Gateway IP Main Interface IP
 Specify

P1 Proposal

1 - Encryption Authentication
2 - Encryption Authentication

DH Group 1 2 5

Keylife (120-172800 seconds)
Local ID (optional)

XAuth Disable Enable as Client Enable as Server

Nat-traversal Enable

Keepalive Frequency (10-900 seconds)

Dead Peer Detection Enable

OK Cancel
Phase 2 nin tanimlanmasi VPN - IPSEC - Auto Key kismina gelin Create Phase 2 ye

Auto Key (IKE) **Manual Key**

Phase 1

test_vpn

isim. kismina isim verilir ve Phase 1 kisminde bir adim once tanimladigimiz Phase 1 tanimi

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

Edit Phase 2

| | | | | | |
|----------------------------|--|-----------------|----------------------|------|----------|
| Name | vpn_tunnel | | | | |
| Phase 1 | test_vpn | | | | |
| Advanced... | | | | | |
| P2 Proposal | 1-Encryption: | 3DES | Authentication: SHA1 | | |
| | 2-Encryption: | 3DES | Authentication: MD5 | | |
| | <input checked="" type="checkbox"/> Enable replay detection | | | | |
| | <input checked="" type="checkbox"/> Enable perfect forward secrecy(PFS). | | | | |
| | DH Group | 1 | 2 | 5 | |
| Keylife: | Seconds | 1800 | (Seconds) | 5120 | (KBytes) |
| Autokey Keep Alive | <input checked="" type="checkbox"/> Enable | | | | |
| Quick Mode Selector | Source address | 192.168.16.0/24 | | | |
| | Source port | 0 | | | |
| | Destination address | 192.168.1.0/24 | | | |
| | Destination port | 0 | | | |
| | Protocol | 0 | | | |

Merkez network Internal interface inde olduğu için Internal seçilir.

Edit Address

| | |
|-------------------------|----------------------------|
| Address Name | merkeznetwork |
| Type | Subnet / IP Range |
| Subnet / IP Range | 192.168.16.0/255.255.255.0 |
| Interface | internal |
| OK Cancel | |

Merkez network Internal interface inde olduğu için Internal seçilir.

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

Edit Address

| | |
|-------------------|---------------------------|
| Address Name | vpnnetwork |
| Type | Subnet / IP Range |
| Subnet / IP Range | 192.168.1.0/255.255.255.0 |
| Interface | wan1 |

VPN tunnel için merkezi network için WAN 1 interface i secilir

Edit Policy

| | | |
|----------------------------|---------------|----------|
| Source Interface/Zone | internal | |
| Source Address | merkeznetwork | Multiple |
| Destination Interface/Zone | wan1 | |
| Destination Address | vpnnetwork | Multiple |
| Schedule | always | |
| Service | ANY | Multiple |
| Action | IPSEC | |

| | |
|--|---------------------------------------|
| VPN Tunnel | test_vpn |
| <input checked="" type="checkbox"/> Allow inbound | <input type="checkbox"/> Inbound NAT |
| <input checked="" type="checkbox"/> Allow outbound | <input type="checkbox"/> Outbound NAT |

| | |
|---|-----------------|
| <input type="checkbox"/> Protection Profile | [Please Select] |
| <input type="checkbox"/> Log Allowed Traffic | |
| <input type="checkbox"/> Traffic Shaping | |
| <input type="checkbox"/> User Authentication Disclaimer | |

| | |
|--------------|--|
| Redirect URL | |
|--------------|--|

VPN Tunnel için WAN 1 interface i secilir

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12



Çevreli bir VPN için bir VPN Tunnel oluşturulması ve istenilen VPN konumlarından erişilebilir olduğu

IPSec Setup

Active Keep Alive N

Name: merkez

IPSec Key Mode: IKE

Negotiation Mode: Main

Encapsulation Mode: Tunnel

DNS Server (for IPSec VPN): 0.0.0.0

Local

Local Address Type: Subnet

IP Address Start: 192.168.1.0

End / Subnet Mask: 255.255.255.0

Remote

Remote Address Type: Subnet

IP Address Start: 192.168.16.0

End / Subnet Mask: 255.255.255.0

IPSec için Main Negotiation, Keep Alive ve NAT Tunnel seçildi. IKE Key Modu IKE Fortigate

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

| 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 |
| <input checked="" type="radio"/> Pre-Shared Key | 12345678 |
| <input type="radio"/> Certificate | auto_generated_self_signed_cert |
| Encryption Algorithm | 3DES |
| Authentication Algorithm | SHA1 |
| <input type="button" value="Advanced"/> | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

www.bilginipaylas.com

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

VPN - IKE - Advanced Setup

| | |
|-------------------------|---------|
| Protocol | 0 |
| Enable Replay Detection | YES |
| Local Start Port | 0 End 0 |
| Remote Start Port | 0 End 0 |

Phase 1

| | |
|--------------------------|----------|
| Negotiation Mode | Main |
| Pre-Shared Key | 12345678 |
| Encryption Algorithm | 3DES |
| Authentication Algorithm | SHA1 |
| SA Life Time (Seconds) | 28800 |
| Key Group | DH2 |

Phase 2

| | |
|-------------------------------|--------|
| Active Protocol | ESP |
| Encryption Algorithm | 3DES |
| Authentication Algorithm | SHA1 |
| SA Life Time (Seconds) | 1800 |
| Encapsulation | Tunnel |
| Perfect Forward Secrecy (PFS) | DH2 |

Not: Perfect Forward Secrecy (PFS) aktif edilir çünkü fortigate in defaulunda Enable Replay Detection aktif değildir. Bu yüzden PFS de aktif yapılmalıdır.

Fortigate ile Zyxel Model Arasında Site to Site Vpn

Mustafa Demiröz tarafından yazıldı.

Pazartesi, 10 Ekim 2011 00:00 - Son Güncelleme Pazartesi, 10 Ekim 2011 10:12

| | | | | |
|----|------------------------|---------------------------------------|-------------|-------------|
| 2 | 01/01/2000 01:39:59 | Rule [1] Tunnel built successfully | 00100002100 | 00100002100 |
| 3 | 01/01/2000 01:39:59 | Adjust TCP MSS to 1390 | 05100000000 | 05100000000 |
| 4 | 01/01/2000 01:39:59 | Recv<:[HASH]> | 05100000000 | 05100000000 |
| 5 | 01/01/2000 01:39:59 | Send<:[HASH][SA][NONCE][KE][ID][ID]> | 05100000000 | 05100000000 |
| 6 | 01/01/2000 01:39:57 | Start Phase 2: Quick Mode | 00100002100 | 05100000000 |
| 7 | 01/01/2000 01:39:57 | Recv<:[HASH][SA][NONCE][KE][ID][ID]> | 00100002100 | 05100000000 |
| 8 | 01/01/2000 01:39:25 | Phase 1 IKE SA process done | 00100002100 | 05100000000 |
| 9 | 01/01/2000 01:39:25 | Send<:[ID][HASH][NOTFY:INIT_CONTACT]> | 00100002100 | 05100000000 |
| 10 | 01/01/2000 01:39:25 | Recv<:[ID][HASH][NOTFY:INIT_CONTACT]> | 00100002100 | 05100000000 |
| 11 | 01/01/2000 01:39:24 | Send<:[KE][NONCE]> | 00100002100 | 05100000000 |
| 12 | 01/01/2000 01:39:24 | Recv<:[KE][NONCE][UNKNOWN(130)][UNKN> | 00100002100 | 05100000000 |
| 13 | 01/01/2000 01:39:24 | Send<:[SA][VID][VID]> | 05100000000 | 05100000000 |
| 14 | 01/01/2000 01:39:23 | Recv<:[SA][VID][VID][VID][VID][VID]> | 05100000000 | 05100000000 |
| 15 | 01/01/2000 01:39:23 | Recv Mode request from <00100002100> | 00100002100 | 05100000000 |
| 16 | 01/01/2000 01:39:23 | Rule [1] Receiving IKE request | 00100002100 | 05100000000 |
| 17 | 01/01/2000 01:37:05 | Send<:[HASH][DEL]> | 00100002100 | 05100000000 |