

epati

IPSEC VPN Yapılandırma

Ürün: Antikor v2 - Yeni Nesil Güvenlik Duvarı
Yapılandırma Örnekleri

IPSEC VPN Yapılandırma

Kısa Anlatım

İnternet Protokolü Güvenliği (IPSec), İnternet Protokolü (IP) kullanılarak sağlanan iletişimlerde her paket için doğrulama ve şifreleme kullanarak koruma sağlayan bir protokoldür. IPsec, içinde bulundurduğu protokoller sayesinde, oturum başlarken karşılıklı doğrulama ve oturum sırasında anahtar değişimlerini gerçekleştirme yetkisine sahiptir. İki bilgisayar arasında (host-to-host), iki güvenlik kapısı arasında (network-to-network), bir güvenlik kapısı ve bir bilgisayar arasında (network-to-host) sağlanan bağlantıdaki veri akışını korumak için kullanılır.

Network Şeması



Konfigürasyon

İlk olarak **VPN Ayarları** sekmesinden **IPSec VPN Ayarları** seçeneğine tıklanır.



Ekle butonuna tıklanarak IPSec için ayarlamalar yapılır.

IPsec VPN Ayarları		Profiller				
		Yenile + Ekle				
XLS	CSV	PDF	Göster/Gizle			
Sayfa Başı Kayıt Sayısı		Tamam	Filtrele			
		Filtreyi Temizle				
#	Durum	Bağlantı Adı	Kaynak IP	Hedef IP	Bağlantı Durumu	İşlemler
< > Götür						

IPsec VPN Ayarları - Yeni Kayıt

x

Uç Bilgileri

Bağlantı Adı

Durum Aktif

Kaynak IP **Antikor WAN IP**

Hedef IP **Modem WAN IP**

ID Yapılandırması

Kaynak ID Türü IP Adresi
 Domain(FQDN)

Kaynak ID

Hedef ID Türü IP Adresi
 Domain(FQDN)

Hedef ID

Faz 1

Takas Modu

Kriptolama Algoritması

Hash Algoritması

Kimlik Doğrulama Metodu

DH Grubu

Ön Paylaşımlı Anahtar

Faz 2

PFS Grubu

Kriptolama Algoritması

Kimlik Doğrulama Algoritması

Sıkıştırma Algoritması

İptal

Kaydet

Uç Bilgileri	Açıklama
Bağlantı Adı	IPsec Vpn bağlantısı için herhangi bir isim girilir.
Durum	Aktif/Pasif durum ayarı yapılır.
Kaynak IP	Antikor WAN IP yazılır.
Hedef IP	Modem Dış IP yazılır.

ID Yapılandırması	Açıklama
Kaynak ID Türü	IP adresi seçildiyse Kaynak IP'de yazılı olan IP geçerlidir.
Kaynak ID	Domain (FQDN) seçildiyse ilgili IP yazılır.
Hedef ID Türü	IP adresi seçildiyse Hedef IP'de yazılı olan IP geçerlidir.
Hedef ID	Domain (FQDN) seçildiyse ilgili IP yazılır.

Faz 1	Açıklama
Takas Modu	Modemde girilen ayara göre main, base ve aggressive seçeneklerinden biri seçilir.
Kriptolama Algoritması	Modemde girilen ayara göre des, 3des, aes, camilia vb seçeneklerinden biri seçilir.
Hash Algoritması	Modemde girilen ayara göre sha1, md5, sha254, sha384, sha512 seçeneklerinden biri seçilir.
Kimlik Doğrulama Metodu	Modem tarafında girilen Key ile aynı olmak zorundadır.
DH Grubu	Modemde girilen DH grubuna göre ayarlama yapılır.
Ön Paylaşımlı Anahtar	Ön paylaşımlı anahtar girilmelidir, bu anahtar remote ayarlarında da girilecektir.

Faz 2	Açıklama
PFS Grubu	Modem tarafında girilen ayara göre düzenleme yapılır.
Kriptolama Algoritması	Modemde girilen ayara göre aes, des, 3des vb seçeneklerinden biri seçilir.
Kimlik Doğrulama Algoritması	Modemde girilen algoritmaya göre hmac sha1, hmacmd5 vb seçeneklerinden biri seçilir.
Sıkıştırma Algoritması	Deflate olarak ayar seçilir.

Gerekli ayarlamalar yapıldıktan sonra **Erişimler**'e tıklanarak haberleşmesi gereken iç IP'ler yazılır.

IPsec VPN Ayarları		Profiller					
XLS	CSV	PDF	Göster/Gizle	Sayfa Başı Kayıt Sayısı	Tamam	Filtrele	Filtreyi Temizle
#	Durum	Bağlantı Adı	Kaynak IP	Hedef IP	Bağlantı Durumu	İşlemler	
1	Aktif	IPsec_VPN			Yok	Düzenle Sil Erişimler	
« < 1 > »							
Git							

Erişim Listesi - Yeni Kayıt

Kaynak IP 10.33.72.0/21

Hedef IP 192.33.80.0/24

Protokol

Mod

Açıklama

Antikor tarafında gerekli ayarlar yapıldıktan sonra **Gösterge Panelinden, IPsec VPN Servisi** başlatılır.

Ayrıca Profiller bölümünden IPSEC Bağlantıları için hazır profil yaratabilirsiniz. Bu yarattığınız profili IPSEC VPN Ayarlarında kullanabilirsiniz.

IPsec VPN Ayarları **Profiller**

Sayfa Başı Kayıt Sayısı

#	Durum	Profil Adı	İşlemler
<input type="button" value="<"/> <input type="button" value="<"/> <input type="button" value=">"/> <input type="button" value=">"/>			

Uç Bilgileri

Bağlantı Adı

Durum Aktif

Kaynak IP

Hedef IP

ID Yapılandırması

Kaynak ID Türü IP Adresi Domain(FQDN)

Kaynak ID

Hedef ID Türü IP Adresi Domain(FQDN)

Hedef ID

Elle Ayarla Profil Kullan

Modem Tarafında Yapılandırma

Modem tarafında IPsec ayarlarına girdikten sonra **Antikor v2**'de yapmış olduğumuz ayarlarla aynı ayarlar olmalıdır.

IPSec Ayarları

IPSec Bağlantı Adı: Merkez HBYS
Uzak IPsec Ağgeçidi Adresi (URL): Antikor WAN IP

LAN IP adresinden Tünel Erişimi: Ağ Maskesi
VPN için IP adresi: 192.33.80.0
IP alt ağ Maskesi: 255.255.255.0

WAN IP adresinden Tünel erişimi: Ağ Maskesi
VPN için IP adresi: 10.33.72.0
IP alt ağ Maskesi: 255.255.248.0

Anahtar Değişirme Metodu: Oto (IKE)
Doğrulama Metodu: PSK Anahtar
PSK Anahtar: EpatiIPSEC*
Kusursuz İletim Gizliliği: Etkin

Hide Advanced Settings

'==Faz 1==:

Mod: Temel
Kimlik Tanımlayıcı Türü: Yerel WAN IP
Kimlik Tanımlayıcı:
Uzak Kimlik Tanımlayıcı Türü: Uzak WAN IP
Uzak Tanımlayıcı:
Encryption Algorithm: 3DES
Integrity Algorithm: MD5
Anahtar Değişimi için Diffie-Hellman Grubu Seçin: 1024bit
Anahtar Ömrü: (Saniye): 3600

'==Faz 2==:

Encryption Algorithm: 3DES
Integrity Algorithm: MD5
Anahtar Değişimi için Diffie-Hellman Grubu Seçin: 1024bit
Anahtar Ömrü: (Saniye): 3600

VPN Oturumları Sayfasında IPSEC VPN'in Bağlantı durumlarını görebilirsiniz.

VPN Oturumları

SSL VPN L2TP VPN Site to Site VPN **IPSec VPN**

Sayfada 50 kayıt göster Ara :

#	Mod	Yerel Adres	Uzak Adres	Gelen Bayt	Giden Bayt	Yaşam Süresi	İşlemler
1	TUNNEL			76630317	27168880	782	Oturumu Sonlandır
1	TUNNEL			3562799	5067200	930	Oturumu Sonlandır
1	TUNNEL	1		34618	7208	2243	Oturumu Sonlandır
1	TUNNEL			70465943	3029032	2913	Oturumu Sonlandır
1	TUNNEL	1		116159	89312	3444	Oturumu Sonlandır

5 kayıttan 1 - 5 arasındaki kayıtlar gösteriliyor

Önceki 1 Sonraki

Sorun Giderme

1. Tüm ayarlar yapıldıktan sonra **Gösterge Panelinde VPN-İpsec** servisi açılır.
Antikor SSH'ta **ipsecDebug** komutu ile bağlantı durumu görülebilir. Örnek olarak ;

```
2018-01-23 13:59:34: INFO: received Vendor ID: draft-ietf-ipsec-nat-t-ike-00
2018-01-23 13:59:34: INFO: received Vendor ID: DPD
2018-01-23 13:59:34: ERROR: no suitable proposal found.
2018-01-23 13:59:34: ERROR: failed to get valid proposal.
2018-01-23 13:59:34: ERROR: failed to pre-process ph1 packet (side: 1, status 1).
2018-01-23 13:59:34: ERROR: phase1 negotiation failed.
```

Faz1'de uyumsuzluklar olduğu görünmektedir. Antikor < Modem ve Modem < Antikor Tarafı faz 1 ayarları tekrar gözden geçirilmelidir. (Aynı durum faz2 ayarları içinde geçerlidir.)

2. Gerekli tüm ayarlar sağlandıktan sonra, modem-Antikor ve Antikor-modem arasında ping atmak gerekecektir.
Bağlantı resmi ;

```
Foreground mode.
2018-01-23 11:20:49: INFO: @(#)ipsec-tools 0.8.2 (http://ipsec-tools.sourceforge.net)
2018-01-23 11:20:49: INFO: @(#)This product linked OpenSSL 1.0.1s-freebsd 1 Mar 2016 (http://www.openssl.org/)
2018-01-23 11:20:49: INFO: Reading configuration from "/usr/local/etc/racoon/racoon.conf"
2018-01-23 11:20:49: INFO: [500] used as isakmp port (fd=5)
2018-01-23 11:20:52: INFO: respond new phase 1 negotiation:
2018-01-23 11:20:52: INFO: begin Identity Protection mode.
2018-01-23 11:20:53: INFO: ISAKMP-SA established 40a0502010080:485aa411d492226f
2018-01-23 11:20:53: INFO: respond new phase 2 negotiation:
2018-01-23 11:20:54: INFO: IPsec-SA established: ESP/Tunnel spi=231620864(0xdce4100)
2018-01-23 11:20:54: INFO: IPsec-SA established: ESP/Tunnel spi=2401189535(0x8f1f3e9f)
```

ePati Siber Güvenlik Teknolojileri A.Ş.
Mersin Üniversitesi Çiftlikköy Kampüsü
Teknopark İdari Binası Kat: 4 No: 411
Posta Kodu: 33343 Yenişehir / MERSİN

www.epati.com.tr
bilgi@epati.com.tr
+90 324 361 02 33
+90 324 361 02 39

