

TOBB Ekonomi ve Teknoloji Üniversitesi

Bilgisayar Mühendisliği Bölümü

Teknik Rapor 2016-03

Ağ Savunma Sistemleri: StrongSwan Ipsec VPN

Batuhan Karataş 151111021

Ağustos 1, 2016

Özet

VPN günümüzde kullanımı giderek artış gösteren bir internet ağ teknolojisidir. Bu teknoloji sıradan internet kullanıcıları dâhil birçok farklı profildeki kullanıcı tarafından farklı amaçlar doğrultusunda kullanılan bir ihtiyaç haline gelmiştir. Teknik olarak kısaca VPN (Virtual Private Network) internet ya da başka bir açık ağ üzerinden özel bir ağa bağlanmayı sağlayan bir bağlantı çeşididir. VPN üzerinden bir ağa bağlanan kişi, o ağın fonksiyonel, güvenlik ve yönetim özelliklerini kullanmaya da devam eder. VPN sanal bir ağ uzantısı oluşturduğu için; VPN kullanarak o ağa bağlanan cihaz fiziksel olarak bağlıymış gibi o ağ üzerinden veri alışverişinde bulunabilir. Bu teknik rapor VPN teknolojisini gerçekleyen uygulamalardan biri olan StrongSwan'nin Kali Linux işletim sistemi üzerinde ki kurulumu, kullanımını ve uygulamanın temel alt yapısını içermektedir.

İçindekiler

1. Giriş	3
2. Kurulum Kılavuzu	3
3. Kullanım Kılavuzu.....	4
4. Sonuç	12
5. Referanslar	13

1. Giriş

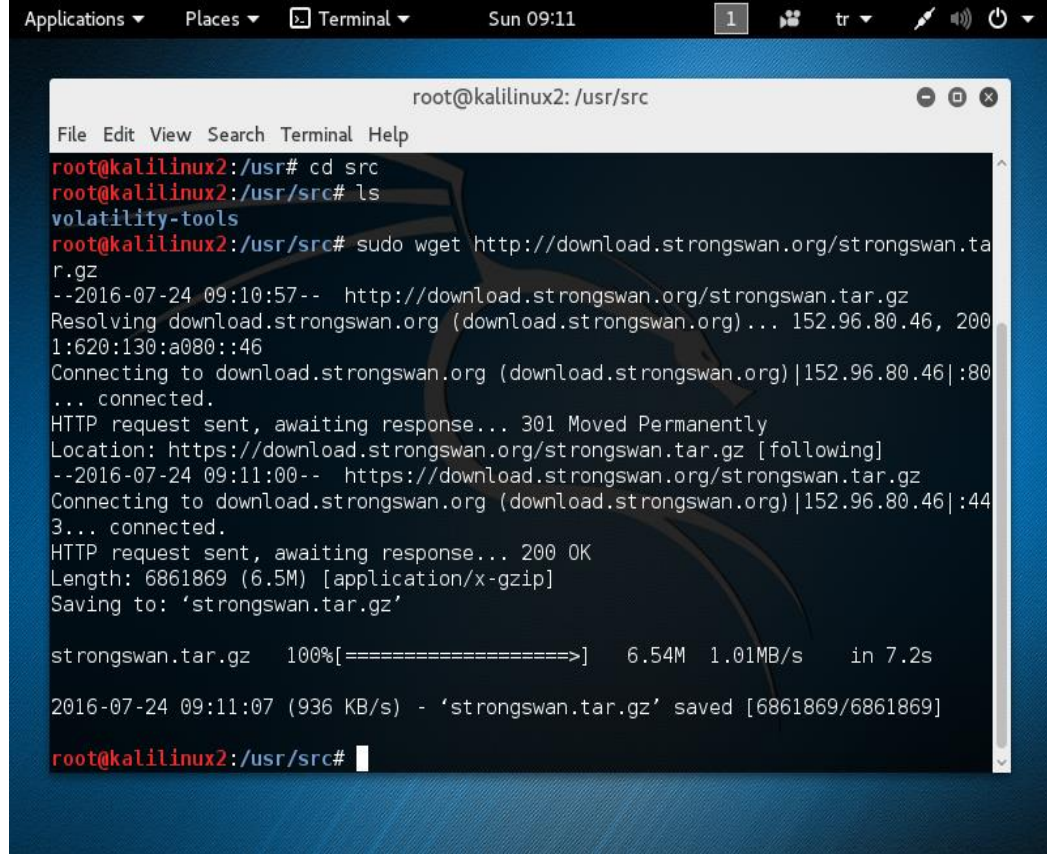
VPN güvenli ve özel ağ bağlantıları oluşturmamızı sağlar. İnternetteki güvenlik ve esneklik ihtiyaçlarından dolayı ortaya çıkmıştır. Strongswan VPN'ni Ipsec protokolünü kullanarak gerçekleştirmektedir. Bu uygulama Linux tabanlı (2.x, 3.x, 4.x), Android, FreeBSD, OS x ve Windows işletim sistemlerini desteklemektedir. IKEv1 ve IKEv2 anahtar paylaşım protokollerini kullanabilmektedir. IPv4 ve IPv6 altyapısını kullanarak çalışabilmektedir. Ipsec tabanlı firewall kuralları otomatik olarak eklenip silinebilir. Virtual ip adresleri ile çalışabilir.

Rapor içerisinde anlatılmakta olan kılavuzlar; Windows işletim sisteminde kurulu VMware programı üzerinde yaratılan Kali Linux 2016.1 sanal makinesi temel alınarak oluşturulmuşlardır.

2. Kurulum Kılavuzu

Strongswan 5.5.0 uygulamasının kurulumu Kali Linux 2016.1 işletim sistemi üzerinde gerçekleştirilmiştir.

Adım 1;



```
root@kalilinux2: /usr/src
File Edit View Search Terminal Help
root@kalilinux2:/usr# cd src
root@kalilinux2:/usr/src# ls
volatility-tools
root@kalilinux2:/usr/src# sudo wget http://download.strongswan.org/strongswan.tar.gz
--2016-07-24 09:10:57-- http://download.strongswan.org/strongswan.tar.gz
Resolving download.strongswan.org (download.strongswan.org)... 152.96.80.46, 2001:620:130:a080::46
Connecting to download.strongswan.org (download.strongswan.org)|152.96.80.46|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://download.strongswan.org/strongswan.tar.gz [following]
--2016-07-24 09:11:00-- https://download.strongswan.org/strongswan.tar.gz
Connecting to download.strongswan.org (download.strongswan.org)|152.96.80.46|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6861869 (6.5M) [application/x-gzip]
Saving to: 'strongswan.tar.gz'

strongswan.tar.gz 100%[=====>] 6.54M 1.01MB/s in 7.2s

2016-07-24 09:11:07 (936 KB/s) - 'strongswan.tar.gz' saved [6861869/6861869]

root@kalilinux2:/usr/src#
```

Resim 1

Öncelikle terminalden “wget” komutu ile <http://download.strongswan.org/strongswan.tar.gz> bağlantısından strongSwan'nin son release'ini indiriyoruz. Bizim burada kullandığımız sürüm 5.5.0'dır.

Adım 2:

```

root@kalilinux2:/usr/src# ls
strongswan.tar.gz  volatility-tools
root@kalilinux2:/usr/src# ls
strongswan-5.5.0  strongswan.tar.gz  volatility-tools
root@kalilinux2:/usr/src# cd strongswan-5.5.0/
root@kalilinux2:/usr/src/strongswan-5.5.0# ./configure --enable-aes --enable-charon --enable-ikev1 --enable-ikev2 --enable-md5 --enable-pem --enable-sha1 --enable-x509

```

Resim 2

Sıkıştırılan dosyayı açtıktan sonra yapmamız gereken işlem program yapılandırmasını gerçekleştirmek. Bu kısımda configure script'i parametre verilmeden çalıştırılıp strongSwan'nin default ayarları tercih edilebilir veya Resim-2'de görüldüğü üzere parametreler vererek Strongswan'nin bize sağladığı özellikleri enable – disable yapılabilir veya dosya konum ayarlamalarında bulunabilirsiniz. <https://wiki.strongswan.org/projects/strongswan/wiki/Autoconf#> bu bağlantıdan strongSwan default yapılandırma ayarları görülebilir. Raporun giriş kısmında da bahsedildiği üzere strongSwan'nin birçok farklı işlevi yerine getirebilme fonksiyonları mevcuttur. Bu programla neler gerçekleştirmek istediğinize bağlı olarak ihtiyaç duyacağınız fonksiyonları bu aşamadaki yapılandırmada aktif hale getirebilirsiniz.

```

config.status: creating config.h
config.status: executing depfiles commands
config.status: executing libtool commands

strongSwan will be built with the following plugins
-----
libstrongswan: aes des rc2 sha2 sha1 md5 random nonce x509 revocation constraint
s pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dnskey sshkey pem fips-prf gmp xcbc cmac h
mac
libcharon: attr kernel-netlink resolve socket-default stroke vici updown xau
th-generic
libnccs:
root@kalilinux2:/usr/src/strongswan-5.5.0#

```

Resim 3

Adım 3:

Yapılandırma işlemini gerçekleştirdikten sonra yapmamız gereken diğer işlem programın build edilmesidir. Bunu gerçekleştirmek için; “make sudo make install” komutları terminal’den çalıştırılır. Bu işlemle tamamlanmasıyla kurulum tamamlanmış olur. Biz programı “usr/src” konumuna kurduk. Bu işlem sonunda önemli olan bir husus; “usr/local/etc” konumunda ipsec ve strongSwan yapılandırma dosyaları oluşur. Bu dosyalar üzerinde değişiklik yapılarak strongSwan ile farklı fonksiyonel özellikler gerçekleştirilebilir. Bu işlemler kullanım kılavuzu kısmında anlatılacaktır.

3. Kullanım Kılavuzu

StrongSwan IpSec tabanlı bir çözümdür ve 3 temel yapılandırma seçeneği sunmaktadır. Bunlar; Remote Access, Site-Site ve Host-Host yapılarıdır. Bu yapıları kullanırken hangi anahtar değişim protokolü kullanılmalı, yetkilendirmeyi hangi metodu kullanarak yapmalıyım, iletişim kuracak iki uç için sertifika, ip, subnet vb. ne olarak tanımlanmalıdır gibi birçok farklı ince ayarın yapılması gerekmektedir. StrongSwan’ini kullanmaya başlamadan önce genel olarak ne yapmak istiyorsunuz ve yapacağınız şeyi hangi yapıları kullanarak ve kimler arasında yapacaksınız gibi sorulara cevap bulmanız gerekmektedir. Bunları tespit ettikten sonra gerekli yapılandırmaları oluşturup programı kullanmaya başlayabilirsiniz. Strongswan’nin kendi sitesinde bol miktarda yapılandırma ayar örnekleri mevcuttur. <https://wiki.strongswan.org/projects/strongswan/wiki/ConfigurationExamples> Aynı zamanda uygulamada geliştiricilere yönelik bir yapı oluşturulmuştur. Çünkü uygulama yukarıda belirtilen yapılandırma örneklerini gerçeklemenizi sağlayan bir test yapısı kurmanıza olanak sağlamaktadır. Ayrıca ayarlar konusunda son kullanıcıyı özgür bırakması geliştirici için gerekli fonksiyonel çeşitliliği sağlamıştır ama normal kullanıcı için bu yapı bir zorluk oluşturmaktadır.

StrongSwan'da kullanılan önemli terminal komutları;

ipsec start: IKE daemon charon'u başlatır. ipsec.conf dosyasını kullanmaya başlar.

ipsec stop: IKE daemon charon'u ve tüm Isec bağlantılarını sonlandırır.

ipsec update: ipsec.conf dosyasında bir değişiklik yapıldıysa IKE daemon charon'u yeni ipsec konfigürasyonuna göre çalıştırmaya başlar.

ipsec up <name>: ipsec.conf dosyasında tanımlı "conn <name>" ipsec bağlantısını başlatır ve bu ipsec bağlantı durum bilgilerinin görüntülenmesini sağlar.

ipsec down <name>: ipsec.conf dosyasında tanımlı "conn <name>" bağlantısını sonlandırır.

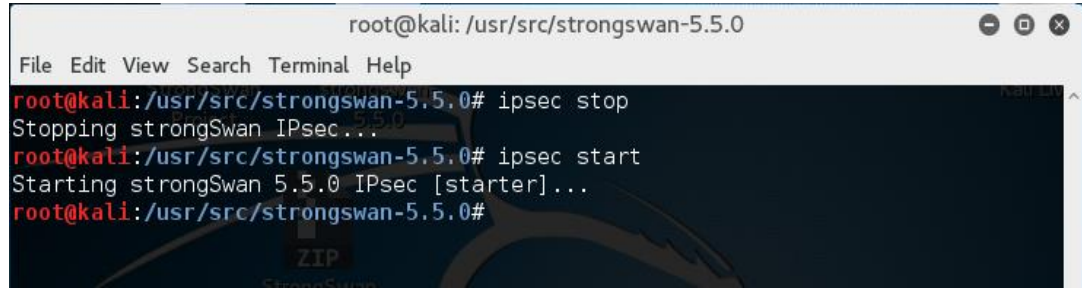
ipsec status <name>: conn <name> bağlantı ile ilgili özet bilgi döner.

ipsec statusall <name>: conn <name> bağlantı ile ayrıntılı bilgi döner.

ipsec restart: ipsecstop ve sonra ipsecstart yapar.

ipsec listaacerts: usr/local/etc/ipsec.d/aacerts konumundaki X509 sertifikalarını görüntüler.

ipsec listcacerts: usr/local/etc/ipsec.d/cacerts konumundaki X509 sertifikalarını görüntüler.



Resim 4

StrongSwan yapılandırma dosyaları (usr/local/etc);

ipsec.conf : Isec bağlantı yapılandırmalarını içeren dosyadır.

ipsec.secrets: Private ve pre-shared anahtarların tutulduğu dosyadır.

ipsec.d: Sertifikalar (Ca, Aa) ve private anahtarlar bu dosyadadır.

strongswan.conf: Genel strongswan ayarlarını içerir.

StrongSwan ile sertifika yönetimi:

Bunun için StrongSwan'nin içerisindeki PKI tool'unu kullanabilirsiniz.

CA sertifikası için:

Öncelikle sertifikayı imzalamak için bir private key üretiyoruz. Bu key default olarak 2048 bit RSA anahtarı olarak üretilmektedir.

- ipsec pki --gen > caKey.der

Şimdi kendi oluşturduğumuz caKey private key ile imzalanmış bir CA sertifikası oluşturabiliriz.

- ipsec pki --self --in caKey.der --dn "C=CH, O=strongSwan, CN=strongSwan CA" --ca > caCert.der

End entity sertifikası için:

Bu sertifika strongSwan'da peer'lar içindir örneğin; VPN client'lari veya VPN Gateway'leri için.

- ipsec pki --gen > peerKey.der
- ipsec pki --pub --in peerKey.der | ipsec pki --issue --cacert caCert.der --cakey caKey.der \ --dn "C=CH, O=strongSwan, CN=peer" > peerCert.der

Ara not: RSA private key'den public key üretmek için:

- ipsec pki --pub --in myKey.der > myPub.der

SubjectAltName'i üretilecek sertifikada tanımlamak için aşağıdaki parametre pki komutuna eklenebilir.

--san vpn.strongswan.org

X509 sertifikasını der tipinden pem'e dönüştürmek için;

- openssl x509 -inform der -outform pem -in caCert.der -out caCert.pem

RSA anahtarını der tipinden pem'e dönüştürmek için;

- openssl rsa -inform der -outform pem -in peerKey.der -out peerKey.pem

Sertifikalar sistemde nereye yüklenmeli?

Strongswan kullanımı için sertifika ve anahtarların tutulması gereken konum“
usr/local/etc/swanctl”

/etc/swanctl/(rsa|ecdsa|pkcs8)/peerKey.der: Peer'in private key'i tutulur.

/etc/swanctl/x509/peerCert.der: Peer'in sertifikaları tutulur.

/etc/swanctl/x509/caCert.der: CA sertifikaları tutulur.

/etc/ipsec.d/private/peerKey.der: Peer'in private key'i tutulur. Ipsec.secrets script'inde değişiklik yapmak gerekir.

/etc/ipsec.secrets - strongSwan IPsec secrets file

192.168.0.1 : PSK "v+NkxY9LLZvwj4qCC2o/gGrWDF2d21jL"

: RSA moonKey.pem

alice@strongswan.org : EAP "x3.dEhgN"

carol : XAUTH "4iChxLT3"

dave : XAUTH "ryftzG4A"

get secrets from other files

include ipsec.*.secrets

/etc/ipsec.d/certs/peerCert.der: Peer'in sertifikaları tutulur. Ipsec.conf script'inde değişiklik yapmak gerekir.

/etc/ipsec.conf - strongSwan IPsec configuration file

config setup

cachecrls=yes

strictcrlpolicy=yes

ca strongswan #define alternative CRL distribution point

cacert=strongswanCert.pem

crluri=http://crl2.strongswan.org/strongswan.crl

auto=add

conn %default

keyingtries=1

keyexchange=ikev2


```

conn roadwarrior
    leftsubnet=10.1.0.0/16
    leftcert=moonCert.pem
    leftid=@moon.strongswan.org
    right=%any
    auto=add

```

/etc/ipsec.d/cacerts/caCert.der: CA sertifikaları tutulur.

CA private anahtarı; oluşabilecek güvenlik açıkları sebebiyle internet erişimi olan bir makine ve korumasız bir konum üzerinde tutulmamalıdır.

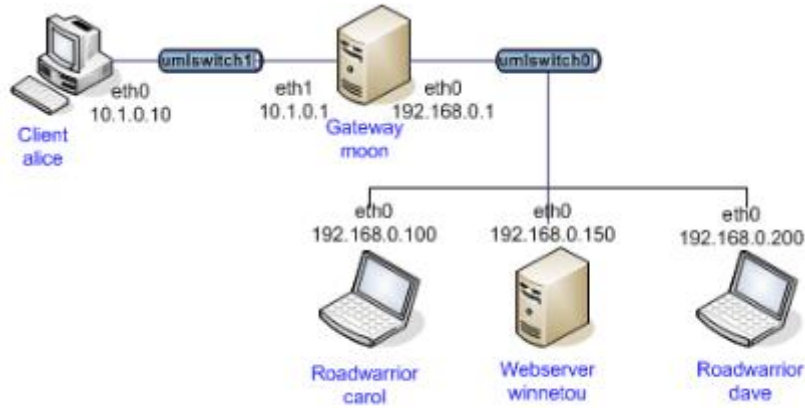
Örnek yapılandırmalar:

Gizli ve güvenli bir bağlantı VPN tüneli açmadan önce bu ayarların yapılması gerekmektedir.

Ö1:

Yaygın olarak kullanılan bir uç noktadan(Mobile Client) uzaktaki bir ağa bağlanmamızı sağlayan (Evden şirket ağına bağlanmak veya Kısıtlamaların olduğu bir web sitesine VPN bağlantısı kullanarak erişmek vb.) yapılandırma ayarlarını inceleyelim;

Anahtar Paylaşım Tipi: IKEv1
 Bağlantı Tipi: Remote Access
 Yetkilendirme Tipi: X509 sertifikaları doğrulanarak
 Yetkilendirme Algoritması: RSA
 IP versiyonu: IPV4



Şekil 1

Bu yapıda Carol ve Dave adında iki mobil client Moon gateway'nin (Uzaktaki ağ) ardındaki alice client'ına erişmek istiyor. Bunu yapmaları için Moon gateway'i ile aralarında bir VPN bağlantısı oluşturmaları lazım. Bunu gerçeklerken VMWare'de iki farklı Kali linux sanal makinası oluşturdum.

Kali Linux bilgileri;

```

root@kali: /usr/local/etc# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:26:2b:b2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.172.128/24 brd 192.168.172.255 scope global dynamic eth0
        valid_lft 1284sec preferred_lft 1284sec
    inet6 fe80::20c:29ff:fe26:2bb2/64 scope link
        valid_lft forever preferred_lft forever

```

Resim 5

Kali Linux 2 bilgileri;

```
root@kali:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:6a:99:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.172.129/24 brd 192.168.172.255 scope global dynamic eth0
        valid_lft 1661sec preferred_lft 1661sec
    inet6 fe80::20c:29ff:fe6a:9907/64 scope link
        valid_lft forever preferred_lft forever
```

Resim 6

Ayarlarda bahsedilen left = Local'i, Right ise Remote'ı temsil etmektedir. Bu ayarlar usr/local/etc konumunda bulunmalıdır

Moon Gateway Yapılandırma dosya içerikleri:

ipsec.conf

/etc/ipsec.conf - strongSwan IPsec configuration file

config setup

conn %default

ikelifetime=60m
keylife=20m
rekeymargin=3m
keyingtries=1
keyexchange=ikev1

conn rw

left=192.168.0.1
leftcert=moonCert.pem
leftid=@moon.strongswan.org
leftsubnet=10.1.0.0/16
leftfirewall=yes
right=%any
auto=add

conn %default kısmında Anahtar Değişim Protokolü olarak hangi versiyonun tercih edildiği ve bağlantıyı şifreleyen bu anahtarın hangi sıklıkla değiştirileceği ile ilgili ayarlamalar mevcuttur.

conn rw kısmında ise left field'ında moon'nun ipv4 adresi görülmektedir. Yetkilendirmede kullanılacak X509 sertifikasının ismi leftcert'de belirtilmiştir.

LeftSubnet: Moon gateway'inin subnet mask'ı yazılmaktadır.

Leftfirewall = yes ise ip tabloları ile ilgili firewall kurallarının otomatik olarak eklenmesini sağlamak içindir. Bununla birlikte tünel bağlantısından gelen paketler firewall'dan geçebilecektir.

ipsec.secrets

/etc/ipsec.secrets - strongSwan IPsec secrets file

: RSA moonKey.pem

strongswan.conf

/etc/strongswan.conf - strongSwan configuration file


```

charon
{
    load = test-vectors aes des sha1 sha2 md5 pem pkcs1 pkcs8 gmp random nonce x509 curl
    revocation hmac xcbc ctr ccm gcm stroke kernel-netlink socket-default updown

    dh_exponent_ansi_x9_42 = no
    integrity_test = yes

    crypto_test
    {
        on_add = yes
    }
}

```

Carol Mobile Client yapılandırma dosya içerikleri:

ipsec.conf

/etc/ipsec.conf - strongSwan IPsec configuration file

config setup

```

conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    keyexchange=ikev1

```

```

conn home
    left=192.168.0.100
    leftcert=carolCert.pem
    leftid=carol@strongswan.org
    leftfirewall=yes
    right=192.168.0.1
    rightid=@moon.strongswan.org
    rightsubnet=10.1.0.0/16
    auto=add

```

ipsec.secrets

/etc/ipsec.secrets - strongSwan IPsec secrets file

```
: RSA carolKey.pem "nH5ZQEWtku0RJEZ6"
```

strongswan.conf

/etc/strongswan.conf - strongSwan configuration file

```

charon
{
    load = test-vectors aes des sha1 sha2 md5 pem pkcs1 pkcs8 gmp random nonce x509 curl
    revocation hmac xcbc ctr ccm gcm stroke kernel-netlink socket-default updown

    dh_exponent_ansi_x9_42 = no
    integrity_test = yes

    crypto_test {
        on_add = yes
    }
}

```

VPN bağlantısı üzerinden paket alışverişinin başlatılması;

Bu örnekte Carol ve Moon arasında bağlantı oluşturacağız ve bu ipsec bağlantısı üzerinden Moon'a ping atacağız.

Bunları yapmak için terminal'den şu komutların girilmesi gerekmektedir;

Adım 1:

```
moon# tcpdump -l -i eth0 not port ssh and not port domain >/tmp/tcpdump.log
2>/tmp/tcpdump.err.log &
```

Moon VM'deki eth0'i ileride test amaçlı kontrol etmek amacıyla tcpdump komutunu kullanarak sniff edip log'luyoruz.

Adım 2:

```
moon# ipsec start
Starting strongSwan 5.5.0 IPsec [starter]...
No leaks detected, 1 suppressed by whitelist
```

Moon, IKE daemon charon'u kendi içinde tanımladığımız ipsec.conf dosyasını kullanarak başlatır. Master virtual makinamızı moon olarak belirledik.

Adım 3:

```
carol# ipsec start
Starting strongSwan 5.5.0 IPsec [starter]...
No leaks detected, 1 suppressed by whitelist
```

Carol, IKE daemon charon'u kendi içinde tanımladığımız ipsec.conf dosyasını kullanarak başlatır. Carol virtual makinamızı slave olarak düşünelim.

Adım 4:

```
carol# ipsec up home
```

Bu komut ile ipsec.conf içerisinde tanımlamış olduğumuz home bağlantısı ile yetkilendirilmiş ve şifrelenmiş bir şekilde başlatılır. Böylece bir VPN bağlantısını kurmuş oluruz. Bu bağlantı yapılandırma dosyalarında belirtilen parametre değerlerine göre şekillenir. Eğer yapılandırma dosyalarında bir değişiklik olursa "ipsecupdate" komutu ile bağlantı güncellenmelidir.

Cevap:

```
initiating Main Mode IKE_SA home[1] to 192.168.0.1
generating ID_PROT request 0 [ SA V V V V ]
sending packet: from 192.168.0.100[500] to 192.168.0.1[500] (216 bytes)
received packet: from 192.168.0.1[500] to 192.168.0.100[500] (136 bytes)
parsed ID_PROT response 0 [ SA V V V ]
received XAuth vendor ID
received DPD vendor ID
received NAT-T (RFC 3947) vendor ID
generating ID_PROT request 0 [ KE No NAT-D NAT-D ]
sending packet: from 192.168.0.100[500] to 192.168.0.1[500] (524 bytes)
received packet: from 192.168.0.1[500] to 192.168.0.100[500] (600 bytes)
parsed ID_PROT response 0 [ KE No CERTREQ NAT-D NAT-D ]
received cert request for 'C=CH, O=Linux strongSwan, CN=strongSwan Root CA'
sending cert request for "C=CH, O=Linux strongSwan, CN=strongSwan Root CA"
authentication of 'carol@strongswan.org' (myself) successful
sending end entity cert "C=CH, O=Linux strongSwan, OU=Research,
CN=carol@strongswan.org"
generating ID_PROT request 0 [ ID CERT SIG CERTREQ N(INITIAL_CONTACT) ]
sending packet: from 192.168.0.100[500] to 192.168.0.1[500] (1500 bytes)
received packet: from 192.168.0.1[500] to 192.168.0.100[500] (1388 bytes)
parsed ID_PROT response 0 [ ID CERT SIG ]
received end entity cert "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
using certificate "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
using trusted ca certificate "C=CH, O=Linux strongSwan, CN=strongSwan Root CA"
```

```

checking certificate status of "C=CH, O=Linux strongSwan, CN=moon.strongswan.org"
  fetching crl from 'http://crl.strongswan.org/strongswan.crl' ...
  using trusted certificate "C=CH, O=Linux strongSwan, CN=strongSwan Root CA"
  crl correctly signed by "C=CH, O=Linux strongSwan, CN=strongSwan Root CA"
  crl is valid: until Aug 12 08:18:18 2016
certificate status is good
  reached self-signed root ca with a path length of 0
authentication of 'moon.strongswan.org' with RSA_EMSA_PKCS1_NULL successful
IKE_SA home[1] established between
192.168.0.100[carol@strongswan.org]...192.168.0.1[moon.strongswan.org]
scheduling reauthentication in 3411s
maximum IKE_SA lifetime 3591s
generating QUICK_MODE request 1667714920 [ HASH SA No ID ID ]
sending packet: from 192.168.0.100[500] to 192.168.0.1[500] (220 bytes)
received packet: from 192.168.0.1[500] to 192.168.0.100[500] (188 bytes)
parsed QUICK_MODE response 1667714920 [ HASH SA No ID ID ]
connection 'home' established successfully
No leaks detected, 1 suppressed by whitelist

```

Bu bağlantıyı test etmek için;

Adım 5:

```

carol# ipsec status 2> /dev/null | grep
'home.*ESTABLISHED.*carol@strongswan.org.*moon.strongswan.org' [YES]
  home[1]: ESTABLISHED 0 seconds ago,
192.168.0.100[carol@strongswan.org]...192.168.0.1[moon.strongswan.org]

carol# ping -c 1 10.1.0.10 | grep '64 bytes from 10.1.0.10: icmp_.eq=1' [YES]
64 bytes from 10.1.0.10: icmp_seq=1 ttl=63 time=0.649 ms

```

Strongswan ipsec status komutu ve ping ile paket alışverişi sağlandığı görülmektedir.

Adım 6:

```
moon# killall tcpdump
```

Tcpdump sniff işlemlerini sonlandırıyoruz.

```
moon# ipsec stop
Stopping strongSwan IPsec...
```

```
carol# ipsec stop
Stopping strongSwan IPsec...
```

Ipsec bağlantısı her iki taraftanda kapatılarak işlem sona erdirilir.

Moon TCPDump Log'ları:

```

08:31:19.607495 STP 802.1d, Config, Flags [none], bridge-id 8000.fe:54:00:3b:0c:d7.8004, length
35
08:31:20.081056 IP carol.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase
1 I ident
08:31:20.090105 IP moon.strongswan.org.isakmp > carol.strongswan.org.isakmp: isakmp: phase
1 R ident
08:31:20.106575 IP carol.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase
1 I ident
08:31:20.121219 IP moon.strongswan.org.isakmp > carol.strongswan.org.isakmp: isakmp: phase
1 R ident
08:31:20.147098 IP carol.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase
1 I ident[E]

```

```

08:31:20.160592 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [S], seq
227407066, win 29200, options [mss 1460,sackOK,TS val 4294955836 ecr 0,nop,wscale 4], length
0
08:31:20.160781 IP winnetou.strongswan.org.http > moon.strongswan.org.53276: Flags [S.], seq
3692254122, ack 227407067, win 28960, options [mss 1460,sackOK,TS val 4294955561 ecr
4294955836,nop,wscale 4], length 0
08:31:20.160808 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [.] , ack 1,
win 1825, options [nop,nop,TS val 4294955836 ecr 4294955561], length 0
08:31:20.161109 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [P.], seq
1:72, ack 1, win 1825, options [nop,nop,TS val 4294955836 ecr 4294955561], length 71
08:31:20.161493 IP winnetou.strongswan.org.http > moon.strongswan.org.53276: Flags [.] , ack
72, win 1810, options [nop,nop,TS val 4294955561 ecr 4294955836], length 0
08:31:20.161504 IP winnetou.strongswan.org.http > moon.strongswan.org.53276: Flags [P.], seq
1:1935, ack 72, win 1810, options [nop,nop,TS val 4294955561 ecr 4294955836], length 1934
08:31:20.161511 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [.] , ack
1935, win 2067, options [nop,nop,TS val 4294955836 ecr 4294955561], length 0
08:31:20.161650 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [F.], seq
72, ack 1935, win 2067, options [nop,nop,TS val 4294955836 ecr 4294955561], length 0
08:31:20.161742 IP winnetou.strongswan.org.http > moon.strongswan.org.53276: Flags [F.], seq
1935, ack 73, win 1810, options [nop,nop,TS val 4294955561 ecr 4294955836], length 0
08:31:20.161751 IP moon.strongswan.org.53276 > winnetou.strongswan.org.http: Flags [.] , ack
1936, win 2067, options [nop,nop,TS val 4294955836 ecr 4294955561], length 0
08:31:20.173298 IP moon.strongswan.org.isakmp > carol.strongswan.org.isakmp: isakmp: phase
1 R ident[E]
08:31:20.198067 IP carol.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase
2/others I oakley-quick[E]
08:31:20.201944 IP moon.strongswan.org.isakmp > carol.strongswan.org.isakmp: isakmp: phase
2/others R oakley-quick[E]
08:31:20.214561 IP carol.strongswan.org.isakmp > moon.strongswan.org.isakmp: isakmp: phase
2/others I oakley-quick[E]

```

Bunun dışında birçok farklı yapılandırma ayarları mevcuttur. Remote Access örneğinin seçilmesinin temel sebebi yaygın kullanımı ve strongswan'da kapsamlı ayarlara sahip olmasıdır.

StrongSwan Test Ortamı

StrongSwan içerisinde belli senaryoları gerçekleyebileceğimiz test script'leri bulunmaktadır. Bunları çalıştırabilmek için tıpkı programın kurulumunu yaptığımızda olduğu gibi bazı komutları terminalden girip bir kurulum yapmamız gerekir. Bunun için;

Proje dosyasının olduğu konuma gelip ./testing.conf komutunu girerek test ortamı konfigürasyonunu gerçekleştiriyoruz. Build işlemini gerçekleştirmek için ise ./make-testing komutunu giriyoruz. Test ortamını başlatmak için ./start-testing komutunu giriyoruz. Daha sonra hangi senaryoyu test etmek istiyorsak ./do-tests <testnames> komutuna konumu parametre olarak giriyoruz. Raporda anlatılan bir VPN bağlantısı başlatma senaryosundaki adımlar gerçekleştirilip, sonuçlar testing.conf script'i içerisinde testresultdir konumunda oluşturuluyor. Bu test ortamının strongSwan'da yer alması geliştiriciler için programın yapısının ve kullanımının anlaşılması açısından faydalı olmuştur.

4. Sonuç

Bu raporda StrongSwan temel yapısı, kurulumu ve kullanım süreçleri anlatılmıştır. StrongSwan'nin sağladığı fonksiyonel çeşitlilik birçok farklı işlemi gerçekleştirmenize olanak sağlamaktadır. Fakat kullanıcı arayüzü ve yapılandırma işlemleri sıradan internet kullanıcılarına yönelik değildir. Bu konuda pek dost canlısı olduğu söylenemez. Bu durum geliştiriciler için olumlu sonuçlar doğurmaktadır. Test altyapısının olması ve uygulamanın her adımının iyi bir şekilde dökümanite edilmesi hem öğretici olması açısından hem de programa hakimiyet açısından önemli katkı sağlamaktadır. Sonuç olarak; Strongswan bir VPN uygulamsından beklenen; Maliyet etkinlik, Güvenlik, Kısıtlamaların Aşılması, Esneklik gibi özellikleri ipsec yapısını kullanarak karşılamaktadır.

5. Referanslar

<https://wiki.strongswan.org/projects/strongswan/wiki/InstallationDocumentation>
https://raymii.org/s/tutorials/IPSEC_vpn_with_Ubuntu_15.04.html
<https://wiki.strongswan.org/projects/strongswan/wiki/IntroductiontostrongSwan>
<https://wiki.strongswan.org/projects/strongswan/wiki/Testingenvironment>
<https://www.youtube.com/watch?v=G07Jhuy6RFY>
<https://wiki.strongswan.org/projects/strongswan/wiki/ConfigurationExamples>