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.

İçerik

|  |  |  |
| --- | --- | --- |
| 1 | Giriş . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ………. | 4 |
| 2 | How to Proceed . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 4 |
|  | 2.1 How to Invoke the LLNCS Document Class . . . . . . . . . . . . . . . . . . . | 4 |
|  | 2.2 Contributions Already Coded with LATEX without the LLNCS  document class . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
| 3 | General Rules for Coding Formulas . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 5 |
|  | 3.1 Italic and Roman Type in Math Mode . . . . . . . . . . . . . . . . . . . . . . . | 6 |
| 4 | How to Edit Your Input (Source) File . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
|  | 4.1 Headings . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
|  | 4.2 Capitalization and Non-capitalization . . . . . . . . . . . . . . . . . . . . . . . . | 6 |
|  | 4.3 Abbreviation of Words . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 7 |
| 5 | How to Code the Beginning of Your Contribution . . . . . . . . . . . . . . . . . . | 7 |
| 6 | Special Commands for the Volume Editor . . . . . . . . . . . . . . . . . . . . . . . . . | 9 |
| 7 | How to Code Your Text . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 10 |
| 8 | Predefined Theorem like Environments . . . . . . . . . . . . . . . . . . . . . . . . . . . | 10 |
| 9 | Defining your Own Theorem like Environments . . . . . . . . . . . . . . . . . . . . | 11 |
|  | 9.1 Method 1 (preferred) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 11 |
|  | 9.2 Method 2 . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
|  | 9.3 Unnumbered Environments . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
| 10 | Program Codes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 12 |
| 11 | Fine Tuning of the Text . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 16 |
| 12 | Special Typefaces . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 16 |
| 13 | Footnotes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 17 |
| 14 | Lists . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 17 |
| 15 | Figures . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 17 |
| 16 | Tables . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 18 |
|  | 16.1 Tables Coded with LATEX . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 19 |
|  | 16.2 Tables Not Coded with LATEX . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 19 |
|  | 16.3 Signs and Characters . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 20 |
| 17 | References . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 21 |
|  | 17.1 References by Letter-Number or by Number Only . . . . . . . . . . . . . | 21 |
|  | 17.2 Author-Year System . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . | 22 |

## Giriş

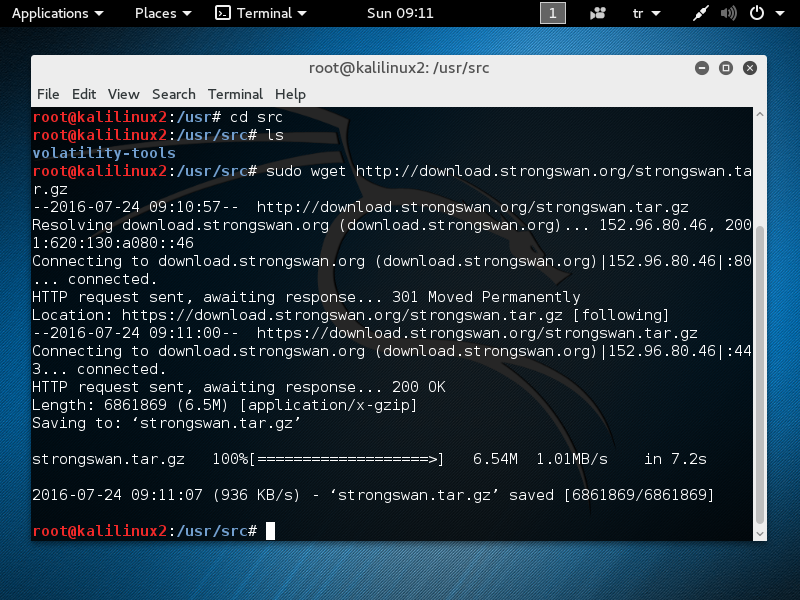
Strongswan Ipsec tabanlı bir Vpn uygulamasıdır. Bu uygulama Linux tabanlı ( 2.x, 3.x, 4.x ), Android, FreeBSD, OS x ve Windows işletim sistemlerini desteklemektedir. IKEv1 ve IKEv2 anahtar paylaşım protokollerini kullanabilmektedir. IPv6 altyapısını kullanarak çalışabilmektedir. Ipsec tabanlı firewall kurallarını otomatik olarak eklenip silinebilir. Dead peer detection sistemi dangling tunnel durumlarını saptayabilir…. ( Devamı gelecek )

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

## Kurulum Kılavuzu

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

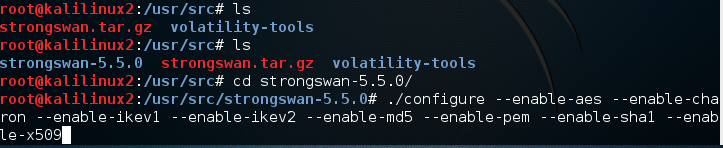
**Adım 1;**



Resim 1

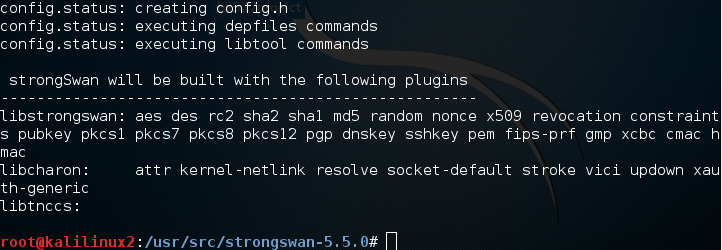
Öncelikle terminalden “wget” komutu ile <http://download.strongswan.org/strongswan.tar.gz> bağlantısından strongSwan’nin son release’ini indiriyoruz. Bizim burada kullandığımız sürüm 5.5.0’dır.

**Adım 2:**



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#](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 duyacağız fonksiyonları bu aşamadaki yapılandırmada aktif hale getirebilirsiniz.



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 işleminde tamamlanmasıyla kurulum tamamlanmış olur. Biz programı “usr/scr” 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.

## Kullanım Kılavuzu

StrongSwan bir 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 Ipsec 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>” bağlantısını başlatır ve bu ipsec bağlantı durum bilgilerinin görüntülenmesini sağlar.

**ipsec down <name>:** ipsec.conf dosyasında tanımlı “conn <name>” bağlantısını sonlandırır.

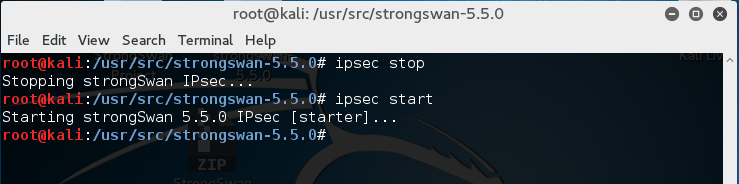
**ipsec status <name>**: conn <name> bağlantı ile ilgili özet bilgi döner.

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

**ipsecrestart:** 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.**



StrongSwan yapılandırma dosyaları ( usr/local/etc );

**ipsec.conf** : Ipsec 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.

Örnek yapılandırmalar:

## Conclusion

References

[NLTK] Bird, Steven, Edward Loper and Ewan Klein (2009), Natural Language Processing with Python. O’Reilly Media Inc.