

Kampüs Ağında Sanal Özel Ağ Yapılandırması

Mehmet Kemal Samur, Osman Saka

Akdeniz Üniversitesi Biyoistatistik ve Tıp Bilişimi Bölümü, Antalya
samur@akdeniz.edu.tr , saka@akdeniz.edu.tr

Özet: Sanal Özel Ağ (Virtual Private Network) (VPN), uzakta yer alan bir ağdan yerel ağa erişerek bilgisayarın yerel ağdaymış gibi çalışabilmesini sağlayan bir alt yapıdır. VPN platforma bağlı olmayan bir yapıdır ve çeşitli yazılımsal veya donanımsal çözümler kullanılarak farklı mimariler ile oluşturulabilir. Bu çalışmada VPN alt yapısının Internet Security and Acceleration (ISA) Server kullanarak nasıl yapılandırıldığı incelenmiştir. Elde edilen bilgiler Akdeniz Üniversitesine VPN alt yapısı kurulması sırasında elde edilen bilgilerden faydalanılarak oluşturulmuştur.

Anahtar Kelimeler: VPN, ISA Server, Uzaktan Yerel Ağ Erişimi.

Virtual Private Network Configuration in Campus Area Network

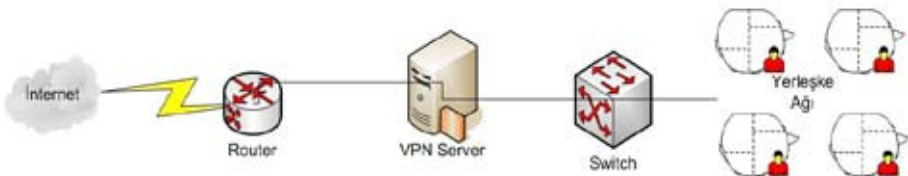
Abstract: VPN is connection infrastructure between local and remote network. VPN is platform independent and it's architecture use different software or hardware solutions. In this studying examined, how can VPN infrastructure configure to use ISA Server. Information in this study is formed from the data achived while setting up VPN infrastructure in Akdeniz University.

Keywords: VPN, ISA Server, Local Area Access to Remote

1. Giriş

VPN (Sanal Özel Ağ), bilgisayarların internet gibi genel bir ağ yapısını kullanarak kendilerine ait olan özel ağlara bağlanmasını sağlayan teknoloji altyapısıdır. Genel kullanıma açık olan ağ yapısını kullanıyor olması bir takım güvenlik endişeleri doğurabilir. Bu durum göz önünde bulundurularak bağlandığı nokta ile bilgisayar arasında adanmış ve şifreli bir tünel bağlantısı sayesinde bilgi akışının güvenliği artırılmıştır. Bir üniversite ağında VPN'in kullanımına basit örnekler verilebilir. Örneğin bütün üniversitelerde kullanılan ve hepsi için değerli olan, özellikle belirli dönemlerde sü-

rekli çevrimiçi kalması gereken bir veritabanı sunucusunun güvenlik gereçleri ile silahsızlandırılmış bölgede (Demilitarized zone) (DMZ) tutulması sakıncalar doğurabilir. Ancak bu veritabanı yöneticisi VPN ile istemci yerleşke içerisinde bir alt ağa alınarak yerleşke dışından da veritabanına müdahale edebilir. Başka bir örnek ile açıklayacak olursak; bir akademisyen bir bilimsel çalışmada bilgisayar altyapısını kullanıyor ve çalışma ile ilgili internet alt yapısı sağlanmış herhangi bir toplantıda nasıl çalıştığını göstermek istiyor. Ancak sadece yerel ağdan çalışacak şekilde tasarlanmış bir bilgisayar alt yapısı kullanılıyor. Bu durumda akademisyen, internet altyapısından VPN'i



Şekil 1.

kullanarak yerleşkenin yerel ağına dahil olabilir ve uygulamayı uzaktan rahatlıkla kullanabilir. VPN ile bilgisayarlar aynı yerel ağın bir parçası gibi olabileceğinden yerel ağlarda bir istemcinin yaptığı akla gelen her türlü örnek burada da kullanılabilir.

2. VPN Gereksinimleri

Bir VPN bağlantının sağlanabilmesi için VPN desteği sunabilecek bir altyapının bulunması gerekir. VPN ile yerel ağa bağlanacak istemci sayısı göz önüne alındığında bir takım maliyetler ortaya çıkmaktadır. Bunlardan en önemlisi sisteminizin internete açılırken kullandığı bağlantı hızıdır. Eğer bu hız düşük ise ve istemci sayınız hem içerde fazla hem de VPN için fazla ise bu sorunlar ortaya çıkarır. Örneğin özel bir kurum ortalama 150 VPN istemcisi için 2 Mb'lık bir bağlantı kullanmaktadır. Ancak bu değer VPN istemcilerinin ihtiyaçlarına göre değişmekte olduğundan bu bir standart sayılamaz. Günümüzde üniversitelerin çıkışlarının bu rakamın çok üzerinde olduğu düşünülür ise bağlantı açısından herhangi bir problemin yaşanmayacağı belirtilmektedir. Örnek VPN yapılandırmasında, VPN Server olarak Microsoft Windows Server 2003 işletim sistemi üzerinde yapılandırılmış bir Microsoft ISA Server 2004 kullanılmaktadır. İstemci olarak ise Windows XP işletim sistemine sahip bir bilgisayar kullanılmaktadır. [1]

Bu örnek yapılandırma zorunluluk belirtmemektedir. VPN için tasarlanmış birçok altyapı kullanılabilir olduğundan alt yapıya göre farklı sonucu ve istemciler kullanılabilir. [1]

3. Akdeniz Üniversitesinde ISA Server'ın VPN Server Olarak Yapılandırılması

Isa Server'ı yapılandırmak için yönetim ekranından rahatlıkla faydalanılabilir. VPN Server için yapılandırmada sırasıyla:

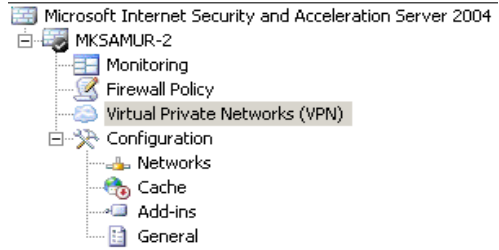
- VPN Server'ın Aktif Edilmesi
- VPN istemcileri için yerel ağa erişim ilkelinin ayarlanması

- Uzaktan erişim sağlayacak kullanıcı hesaplarının belirlenmesi
- Kullanılacak olan bağlantı protokolünün belirlenmesi (PPTP,L2TP,Sertifika)
- Bağlantıların test edilmesi ve izlenmesi [2]

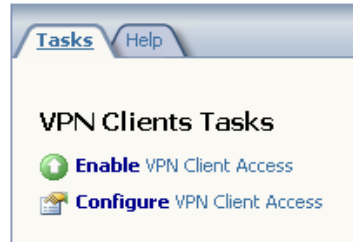
3.1. VPN Server'ın Aktif Edilmesi

ISA Server'ın varsayılan yapılandırmasında VPN aktif olarak gelmez. VPN' i aktifleştirmek için:

1. ISA Server 2004 yönetim konsolunda Virtual Private Network (VPN) alanına gelinir ve Enable VPN Client Access seçeneği seçilir.



Şekil 2



Şekil 3

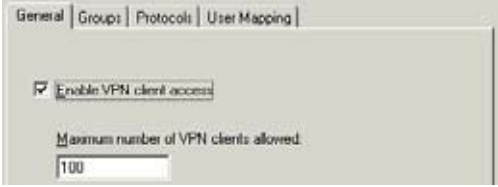
2. Yapılan değişikliklerin aktif olabilmesi için "Apply" butonuna basılır ve çıkan onay penceresinde "OK" butonu kullanılarak değişiklikler aktif hale getirilir.



Şekil 4

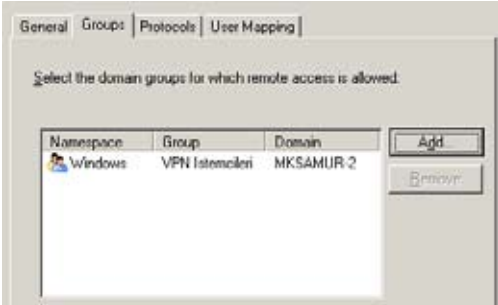
3. Görevler bölümünde "Configure VPN Client Access" linki kullanılır ve VPN istemcilerin özelliklerinin ayarlandığı pencere açılır. Açılan pencereyi incelenecek olursa:

a) Genel: Bu kısımda VPN bağlantının aktif edilip edilmeyeceği ve en fazla kaç istemciye kadar izin verileceği ile ilgili ayarlar yer almaktadır.



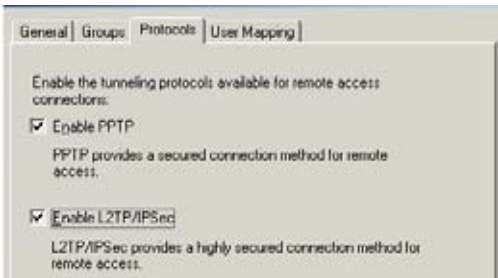
Şekil 5

b) Gruplar: Bu sekmede uzaktan erişime izin verilecek kullanıcı grubu sorulmaktadır. Uzaktan erişimlerine izin verilmesi istenen kullanıcılar bu gruba dahil edilmelidirler. Bu kullanıcılar ISA Server üzerindeki ilkeler ile denetlenmek isteniyorsa kullanıcı özelliklerinde “Uzaktan Erişim İlkesi aracılığıyla erişimi denetle” seçeneğinin aktif tutulması gerekir.



Şekil 6

c) Protokoller: Bu kısımda ise bağlantı için hangi protokolün kullanılacağı seçilebilmektedir.

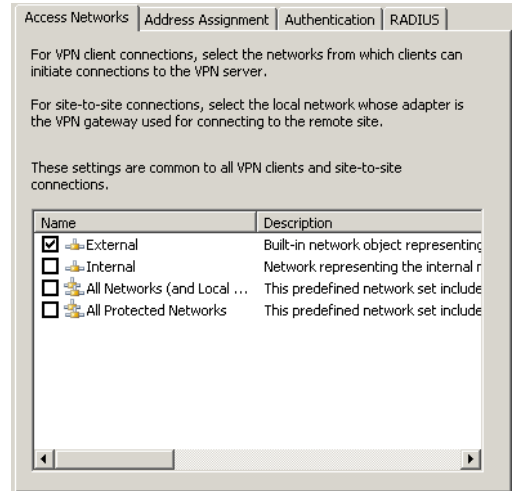


Şekil 7

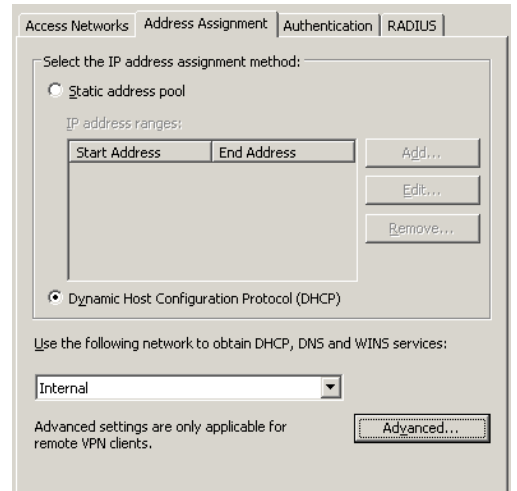
d) Kullanıcı Eşleştirme: Eğer Windows işletim sistemi haricinde bir alandan kullanıcılar kontrol edilmek istenirse bu seçenek kullanılacaktır.

4. Değişiklikler yapıldıktan ve onaylandıktan sonra tekrar görevler bölümünden “Select Access Networks” linkine tıklanılır ve açılan pencereden:

a. Erişilecek Ağ: Bu sekmede dışarıdan VPN istemcilerin yerel ağa hangi ara yüzü kullanarak bağlanacakları seçilir. ISA Server’ın dış erişime açık hangi ayağı üzerinden erişilmesi isteniyorsa burada o seçenek aktif edilmelidir.



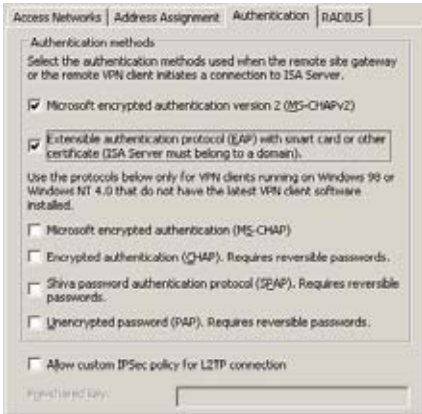
Şekil 8



Şekil 9

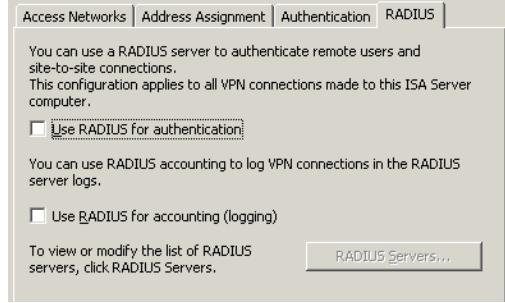
b. Adres Ataması: Bu sekmede VPN istemcilerin yerel ağa dahil edilirken kullanacakları network ayarları yapılabilmektedir. IP adresinin hangi metotla alınacağı kısmında istemcilerin statik mi yoksa dinamik mi alacağı belirlenmektedir. İkinci kısımda ise DHCP,DNS ve WINS sunucu için yerel ağ mı yoksa dış ağa ait sunucular mı kullanılacağı ayarı yapılmaktadır.

c. Kullanıcı Doğrulaması: Bu sekmede kullanıcı ağa bağlanırken hangi metot ile kullanıcı kimliği doğrulaması yapılacaksa belirlenir. Örneğin herhangi bir akıllı kart yardımı ile sertifika server kullanılarak kimlik doğrulaması yapılacaksa EAP seçilir. Eğer herhangi bir sertifika server kullanılmayacaksa ve VPN istemciler Windows 2000 ve sonrası bir işletim sistemi kullanıyorsa MS-CHAPv2 kullanılabilir. Diğer kimlik doğrulama seçenekleri: MS-CHAP, CHAP, SPAP, PAP. Eğer IPSec uygulayarak L2TP protokolü ile bağlantı sağlanacaksa bağlantının sorunsuz sağlanması için paylaşılan anahtarın da bu alanda belirtilmesi gerekir. Burada bir veya daha fazla kimlik doğrulama seçeneği aynı anda kullanılabilir.



Şekil 10

d. RADIUS: Bu seçenekte ise kullanıcı hesaplarının saklanması ve yönetilmesi için eğer bir radius server kullanılacaksa aktif edilebilir. İlk seçenek sadece doğrulama yapılacaksa, ikinci seçenek ise radius serverda yapılan doğrulamaların logları tutulacaksa kullanılmalıdır.



Şekil 11

3.2. VPN İstemcilerin Yerel Ağa Erişimi için Gerekli Kuralların Oluşturulması

ISA Server kullanarak VPN erişimine açılmış olan yerel ağa istemcilerin ulaşırken çeşitli erişim kuralları tanımlanabilir. Bu sayede yerel ağa erişmek isteyen istemcilere istenilirse ekstradan güvenlik tanımlamaları getirileceği gibi yerel ağda erişimine izin verilmeyen bir alana sadece VPN istemcilerin erişmesi de sağlanabilir. VPN istemcilere erişim ilkesi uygulamak için:

1. Yönetim ekranında “Firewall Policy” seçeneğine farenin sağ tuşu ile tıklanılır. Açılan menüden “New” seçeneği altında bulunan “Access Policy” seçeneği kullanılarak yeni bir erişim kuralı oluşturulmak için sihirbaz başlatılır.



Şekil 12

2. İlk aşamada oluşturulacak kural için bir isim verilmesi beklenmektedir.

3. İkinci adımda, ilerleyen adımlarda seçilecek olan protokollere izin mi verileceği, yoksa yasaklama mı getirileceği seçilmelidir.



Şekil 13

4. Protokoller ekranında izin verilecek olan ya da yasaklanacak olan protokoller belirlenmelidir. Ekle butonu kullanılarak istenilen protokoller eklenebilmektedir. Örnekte HTTP,HTTPS, Ping, POP3,POP3S protokollerine izin verilmiştir.



Şekil 14

5. Erişim Kuralı Kaynağı ekranında ise bu protokollere hangi ağdan istek gelmesi durumunda izin verileceği belirtilmektedir. Ekle butonu kullanılarak izin verilecek kaynak noktalar belirlenir. Örnekte, VPN istemcilerinden gelecek taleplere izin verilecek şekilde ayarlanmıştır.



Şekil 15

6. Erişim Kuralı Hedefi ekranında ise izin verilen protokoller kaynaktan hangi yöndeki ağlara erişebilecek bu belirtilmektedir. Yine ekle butonu yardımı ile izin verilecek yön seçilebilir. Örnekte yerel ağa erişim için izin verilmiştir.



Şekil 16

7. Kullanıcı Ayarları penceresinde ise bu kuralın uygulanacağı kullanıcı grupları belirlenmektedir. Örneğimizde belirtilen kaynak ve gidilecek ağ arasında çalışan bütün kullanıcılara izin verilmektedir.



Şekil 17

8. Bir sonraki pencerede ise bu kuralı oluşturmak için "Son" butonu kullanılmalıdır. Yönetim ekranında "Apply" butonu kullanılarak ISA üzerinde yapılan değişiklikler aktif duruma getirilir.



Şekil 18

Not: ISA Server'in bir özelliği olarak bilgisayar ağlarını ve kullanıcıları istenildiği gibi gruplanabilmektedir.

3.3. VPN İstemcisi için Kullanıcı Hesaplarının Aktif Edilmesi

Eğer uygulamada da görüldüğü gibi VPN Server olarak bir Windows Server kullanılacaksa ve Active Directory'den faydalanılmayacaksa VPN istemcilerin kullanıcı hesaplarının yerel sistemde oluşturulması gerekir ve oluşturulan bu kullanıcıların hesaplarında erişim için gerekli izinlerin verilmesi gerekir. Bunun için:

1. Bilgisayar yönetimi penceresinden, yerel kullanıcılar ve gruplar genişletilerek kullanıcı hesapları seçilir. Burada izin verilmek istenen kullanıcının hesabının özellikleri penceresi açılır.

2. Kullanıcının özellikleri ekranından “Dial-in” tabına geçilir ve buradan erişime izin verilir [2].

4. Sonuç

Bu VPN çalışması Akdeniz Üniversitesi Bilgi İşlem Dairesi tarafından test ortamında denedikten sonra gerçek zamanlı kullanıma alınmıştır. İlk aşamada Bilgi İşlem Dairesi çalışanları ve Akdeniz Üniversitesi Tıp Fakültesi Bilgi İşlem Birimi çalışanlarının kullanımına sunulmuştur. Sistem çalışanların işlerini daha düzenli takip edebilmelerine olanak sağlamıştır. Ayrıca çeşitli dönemlerde uzaktan kampus ağına erişmeye olanak sağladığı için sorunların giderilmesinde personele zaman kazandırmıştır.

tır. Birimlerde çalışma alanları belirli olan personellerin yıllık izin , resmi izin veya tatillerde kendi sorumlulukları dahilinde düzenli kontrollerini aksatmamaları ve olası sorunlara uzaktan da müdahale edebilmeleri sağlanmıştır. Sistemin network bant genişliğine getirmiş olduğu yükün çok fazla olmadığı ve alt yapıda kullanılan sunucunun çok üst düzey donanım yapısı gerektirmediği görülmüştür. Sistem bütün bu avantajları ile kullanılabilirliğini göstermiştir.

5. Kaynakça

[1] Shinder, T.W. , Shinder D.L. ve Grasdal M., “Dr. Tom Shinder’s Configuring ISA Server 2004”, Syngress Publishing, 2006

[2] Microsoft ISA Server Guides and Articles, <http://www.microsoft.com/isaserver/techinfo/guides-articles.msp>, Microsoft