VMWare NAT Sanal Makineye Ana Makineden Port Forwarding Yaparak Diğer Makinelerin Erişebilmesini Sağlama

VMWare sanal makinelerin ağ adatörleri nat ayarda iken sanal makine içerisindeki servislere (örn; ssh servisine, veya web sunucusu apache'nin web site hizmetine v.b.) ana makineden erişilebilir, ancak yerel ağdaki başka makineler tarafından erişilemez. Çünkü sanal makine sanal bir NAT ağı içerisindedir ve yerel ağda gerçek ip almak yerine sanal nat ağı içerisinde sanal bir ip almaktadır. Yerel ağda gerçek ip alan makineler birbirlerini görürler ve bu nedenle sadece ana makine görünür. İçerisindeki sanal makine görünmez. Örneğin sanal makine nat iken ana makineden sanal makinedeki ssh servisine bağlanılabilir, veya apache servisine bağlanılabilir, fakat yerel ağdaki başka makineler ilgili sanal makineyi görmediklerinden ssh servisine ulaşamazlar, veya apache servisine ulaşamazlar. Sanal makine yerel ağda gerçek bir ip almadığından bir adrese sahip değildir. Bridge yapılırsa bu noktada sanal makineler yerel ağda gerçek ip alırlar ve yerel ağa gerçek makineymiş gibi katılırlar. Bu sayede yerel ağdaki diğer makinelerin sanal makineyi görebilmesi mümkün olur.

Bazen sanal makineler yerel ağdaki güvenlik kısıtlaması gereği Bridge'de ip alamazlar. NAT veya HostOnly ile ip alabilirler. Bu sayede ana makine ile sanal makine arası haberleşme sağlanır. Ancak diğer makineler sanal makineyle haberleşemezler. Bridge'de ip alamamalarının nedeni ana makineye bağlanan fiziksel kablodan birden fazla yerel ip alınmasının normal koşullarda mantıksız olmasıdır. Bir kablo bir makineye bağlanır ve bir makine bir adet ip alır. Bu normal koşulun kural olarak konması makinede çalıştırılacak sanal makinelerin bridge'de yerel ip alamamasını sağlar. Bu normal koşul kural olarak belirlenmezse sanal makinelerin yerel ağa katılabilmesine yol açılmış olur ve bu güvenlik riski doğurur. Fakat bu kısıt varsa ana makinede çalışan sanal makine ip alamayacağı için sunduğu hizmetlere yerel ağdaki makineler erişemeyecektirler.

Örneğin müşteri kurumlara gidildiğinde sanal makineler ilk planda bridge'de ip alamazlar. IP alabilmeleri için sanal makinenin mac bilgisi paylaşılır ve tanımlanan izin doğrultusunda sanal makineler yerel ağda gerçek ip alırlar. Bu şekilde örneğin sanal makinedeki web hizmetlerine ortak bir şekilde diğer makinelerden erişim sağlanabilir. Fakat bu işleyişi, yani ağdaki makinelerin bir makinedeki sanal makineye erişebilmesini sanal makine yerel ağda gerçek ip alamasa da (örn; nat'ta çalışıyorsa da) uygulamak mümkündür. Ana makineye port forwarding kuralı girilebilir ve yerel ağdakiler ana makineye bağlanırken sanal makineye bağlanır hale girebilirler. Örneğin ana makinede port forward'lama kuralı oluşturarak yerel ağdaki makineler ana makineye ssh bağlantısı kurduklarında veya tarayıcıdan bağlandıklarında ana makine gelen paketleri sanal makineye yönlendirir ve ana makineye bağlananlar aslında sanal makineye bağlanmış olurlar. Yani yerel ağdaki makineler gerçek makineye ssh atarken, veya web sitesine bağlanıyormuş gibi tarayıcıdan ana makineye bağlanırken sanal makineye paketler gidip geleceğinden sanal makine servislerine bağlanılmış olur. Bu şekilde ana makineye girilecek port forward'lama kuralları ile nat'ta çalışan erişilmez sanal makine servislerine dolaylı yoldan erişim sağlanabilir.

Virtualbox ve VMWare yazılımlarında port forward'lama ayar ekranları mevcuttur ve bu ekranlardan dışarıdan erişilmez sanal makinelere dolaylı yoldan erişilebilme imkanı verilir. Bu şekilde ana makineye bağlananlar (örn; ana makinenin ssh portuna veya web portuna) sanal makineye (örn; sanal makinenin ssh portuna veya web portuna) bağlanmış olurlar.

VMWare'leri örnekleme ile gösterecek olursak ana makinede port forwarding kuralı ekleme şu şekilde gerçekleştirilir.

1. VMWare Workstation->Edit->Virtual Network Editor -> Change Settings

2. VMWare Workstation->Edit->Virtual Network Editor…->VMNet8 Nat->NAT

Settings->Add

3. Açılan pencerede ana makineye hangi portundan gelecek paketler sanal makineye yönlendirilsin bilgisi, ana makineye hangi türden (tcp mi udp mi) gelecek paketler sanal makineye yönlendirilsin bilgisi, ana makineye belirtilen kriterlerdeki gelecek paketler hangi sanal makineye yönlendirilsin bilgisi, ve ana makineye belirtilen kriterlerdeki gelecek paketler belirtilen sanal makinenin hangi portuna yönlendirilsin bilgisi girilir.

Bu şekilde port forwarding kuralı oluşturulur ve yerel ağdakiler ana makinenin sanal makinelerine erişebilirler.

Uygulama

(+) Birebir çukurambar ev ağında denenmiştir ve başarılı olunmuştur.

Gereksinimler

i) İş Laptop	// IP: 192.168.0.15
ii) Ev Masaüstü PC	// IP: 192.168.0.11
iii) Ev Masaüstü PC'deki XYZ Sanal Makine	// Bridge IP: 192.168.0.24 // NAT IP: 192.168.52.130

Ev ağında ev masaüstü pc'ye konulan xyz sanal makinesinin web hizmetine ev ağındaki başka makineden erişebilme noktasında Bridge ve NAT farkını gözlemleyelim ve NAT iken nasıl sanal makinenin web hizmetine dışarıdan erişim sağlanacağını uygulayalım.

Not: Ev masaüstü pc'den ev masaüstü pc'deki sanal makineye sanal makine hostonly, nat ve bridge iken herhalükarda web hizmetine erişim mümkündür. Bu yazının konusu sanal makine nat iken ana makinede port forward'lama ile dışarıdan nasıl erişilebileceğidir.

Şimdi ev masaüstü pc'deki sanal makina ağ adaptörünü Bridge yapalım ve yerel ağda adres almasını sağlayalım. Bu işlem sonrası iş laptop'ından ev masaüstü pc'deki sanal makinenin web hizmetine erişmeye çalışalım.

İş Laptop:

http://192.168.0.24	// Ev Masaüstü PC'deki Sanal Makine IP
[OK]	(*) Web sayfası görüntülendi.

Görüleceği üzere sorunsuz doğrudan sanal makine web hizmetine erişim sağlanacaktır. Şimdi ise ev masaüstü pc'deki sanal makina ağ adaptörünü NAT yapalım ve iş laptop'ından ev masaüstü pc'deki sanal makinenin web hizmetine tekrar erişmeye çalışalım.

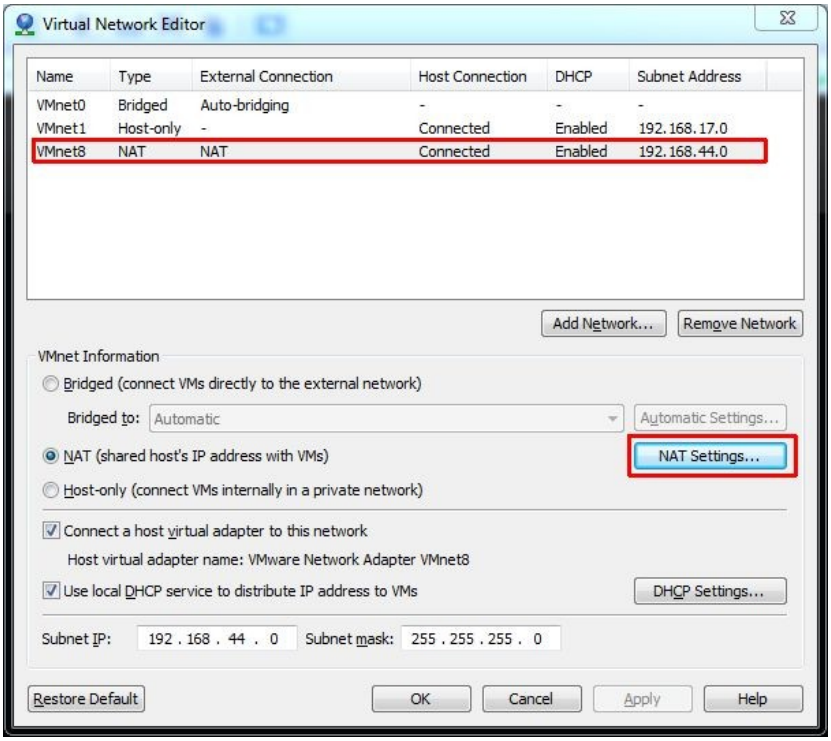
İş Laptop:

http://192.168.52.130	// Ev Masaüstü PC'deki Sanal Makine IP
[The website can't be reached]	(*) Web sayfasına erişilemedi.

Görüleceği üzere sanal makineye erişim sağlanamayacaktır. Normalde bir makinede sanal makine nat'ta çalışırsa dışardan sanal makineye doğru erişim mümkün değildir. Bu nedenle şimdi sanal makineyi bridge yapma şansımızın olmadığını düşünelim (ağdaki güvenlik kısıtlamaları nedeniyle) ve ev masaüstü pc'de port forward'lama kuralları ekleyelim. Port forward'lama ile ana makineye gelen web hizmetine bağlantı paketlerini sanal makinenin ilgili portuna yönlendirelim.

a) *VMware Workstation -> Edit -> Virtual Network Editor* seçeneğine gidilir ve *Change Settings* ile yapılacak değişiklikler için Administrator haklarına geçilir.

b) *VMnet8 NAT* seçilir ve aşağıdaki gösterildiği gibi *NAT Settings* butonuna tıklanır.



c) *Add* butonuna tıklanır ve gelen ekrana oluşturulacak kural bilgisi girilir. .

Host port	: 80	// Ana makine ip'sine erişenler ana makinenin
		// hangi portuna eriştiklerinde forward'lama
		// çalışsın bilgisi

Type	: TCP	// Ana makine ip'sine erişenler ana makineye
		// hangi türden paket gönderdiklerinde
		// forward'lama çalışsın bilgisi

Virtual machine IP address	: NAT Arkasındaki Sanal Makine IP Adresi	
		// Ana makineden forward'lanacak paketler // hangi sanal makineye forward'lanacak bilgisi.

Virtual machine port	: 80	// Ana makineden forward'lanacak paketler
		// belirtilen sanal makinenin hangi portuna
		// forward'lanacak bilgisi

Description : Port Forwarding for NAT VM - XYZ

d) Tüm pencerelere OK denir.

Ardından tekrar iş laptop'ından ev masaüstü pc'deki sanal makinenin web hizmetine erişmeye çalışalım.

> **(*) Not:** İş laptop'ında web tarayıcıya bu sefer sanal makinenin ip'si yerine - yerel ağda tanımlı adrese sahip olan - ev masaüstü pc'nin ip'si girilir. Port Forward'lama çalışacağından ev masaüstü pc'ye bağlantı sanal makineye yönlendirilecektir.

İş Laptop:

http://192.168.0.11	// Bu Sefer Ev Masaüstü PC'deki Sanal
	// Makine IP'si Değil, Ev Masaüstü PC
	// IP'si.

[OK]	(*) Sanal makine web sayfası görüntülendi.

Görüldüğü üzere ev masaüstü pc'deki port forward'lama kuralı çalışacaktır ve ev masaüstü pc kendine gelen 80 portlu paketleri sanal makinenin 80 portuna forward'layarak dışarının sanal makine ile haberleşmesini sağlayacaktır. Özetle yerel ağdaki makineler ana makinenin ip'sine bağlantı yaptıklarında ana makinedeki sanal makineye yönleneceklerdir.

Sanal makine bridge iken yerel ağda bir adrese sahip olduğundan doğrudan erişebilmekteyiz. Ancak NAT olduğunda yerel ağda bir adrese sahip olmadığından erişemeyiz. Bu durumda dolaylı yoldan erişmek ana makinede yapılacak port forward'lama ile mümkün hale gelir.

Port forward'lama kuralını sanal makinelerdeki apache servisi yerine ssh servisi için veya farklı servisler için de uygulamak mümkün durumda.