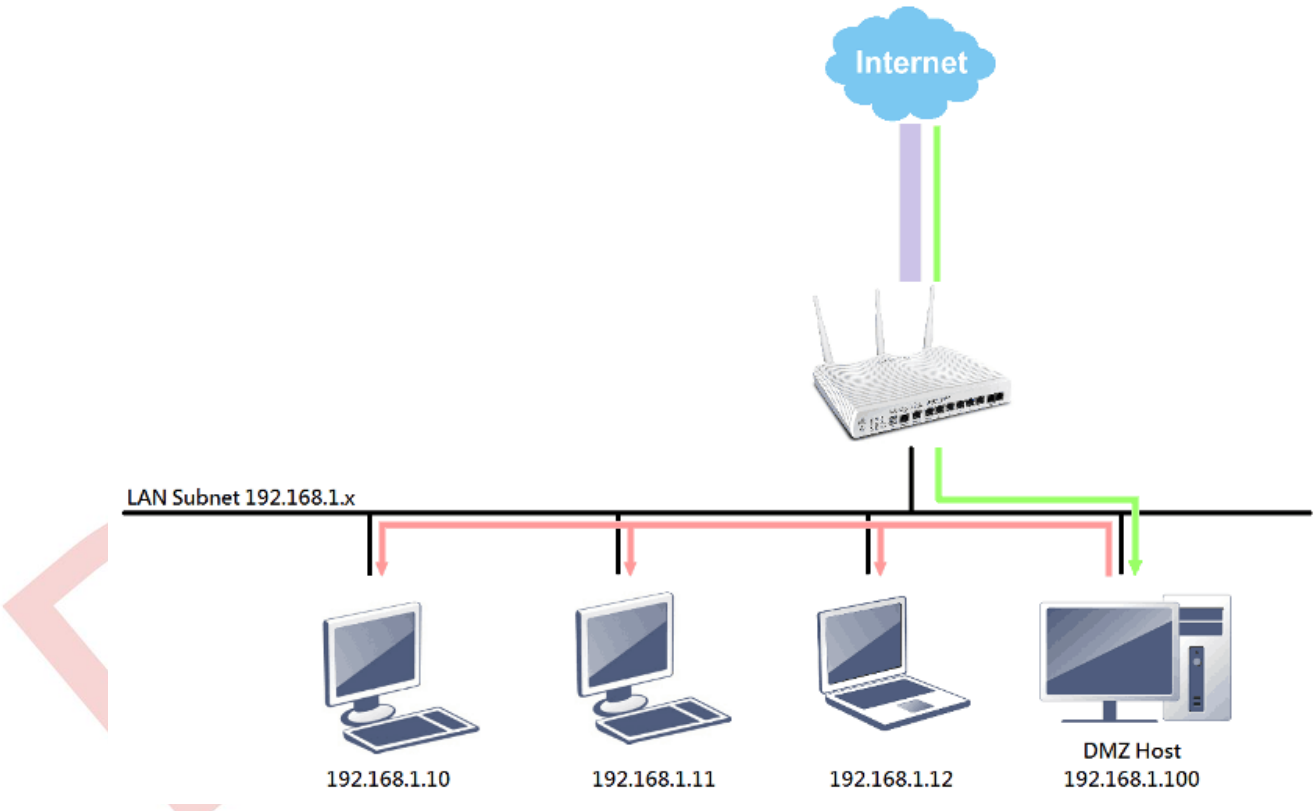
DMZ HOST VE DMZ SUBNET ARASINDAKİ FARK

Demilitarized Zone anlamına gelen DMZ, WAN ve LAN arasında ek bir güvenlik katmanıdır. DMZ subnetli bir router, LAN'ı hala firewall tarafından korunurken WAN'dan DMZ'e erişime izin verir. DMZ'in en yaygın uygulaması, posta sunucuları, HTTP / HTTPS web sunucuları ve FTP sunucuları gibi sunucuların, WAN'daki ana bilgisayarlara hizmet vermesine izin vermektir.

Vigor Router'da, DMZ'i kurmanın iki yolu vardır: DMZ host ve DMZ subnet. Bir DMZ ana bilgisayarı oluşturmak, tek bir ana bilgisayarı tamamen WAN'a açacaktır ve aşağıdakiler dışında tüm paketler bu tek ana bilgisayara iletilecektir:

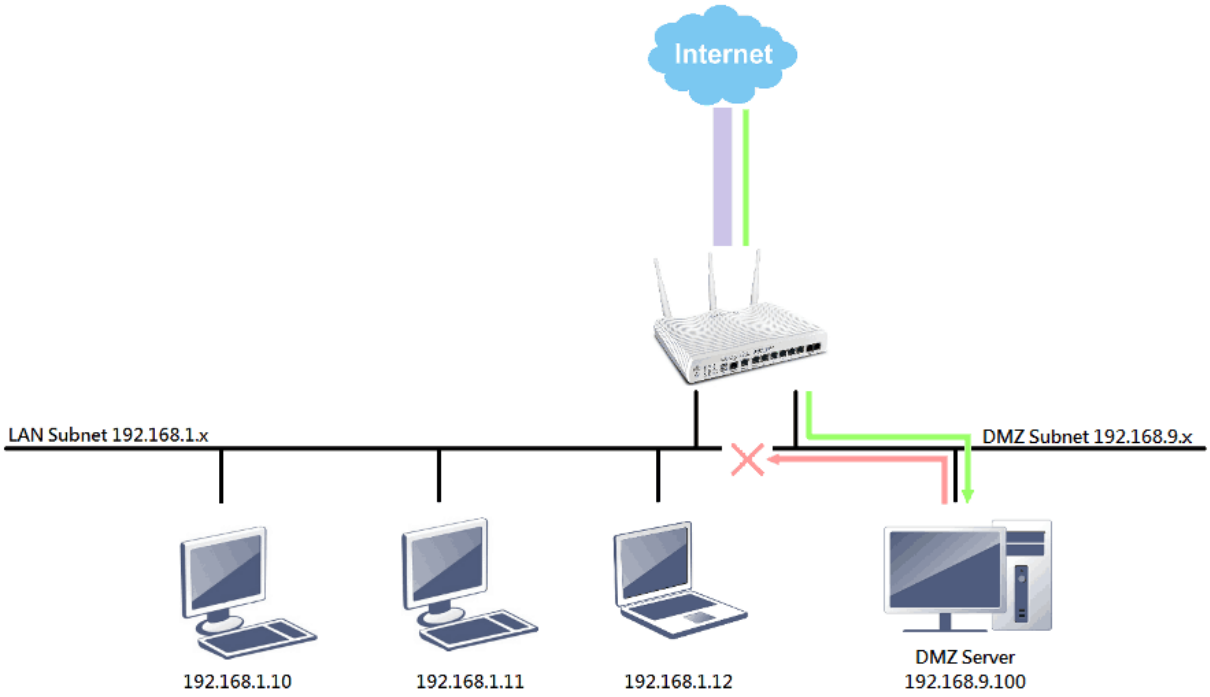
1. Paketler, port yönlendirmesi veya açık port kuralları ile eşleşir
2. Router'ın kendisinin aktif olarak dinlediği portlara yönlendirilmiş paketler. (Örneğin, telnet ve HTTP portlarındaki router üzerinde WAN yönetimi etkinse, 23 ve 80 numaralı portlara gelen paketler router tarafından yakalanır).

DMZ Host'un kurulumu ve kullanımı kolaydır. Ancak, DMZ host diğer LAN aygıtlarıyla aynı subnette olduğundan, bir saldırgan bu sunucunun güvenliğini ihlal ederse, tüm LAN'ın güvenliğini tehlikeye atabilir.

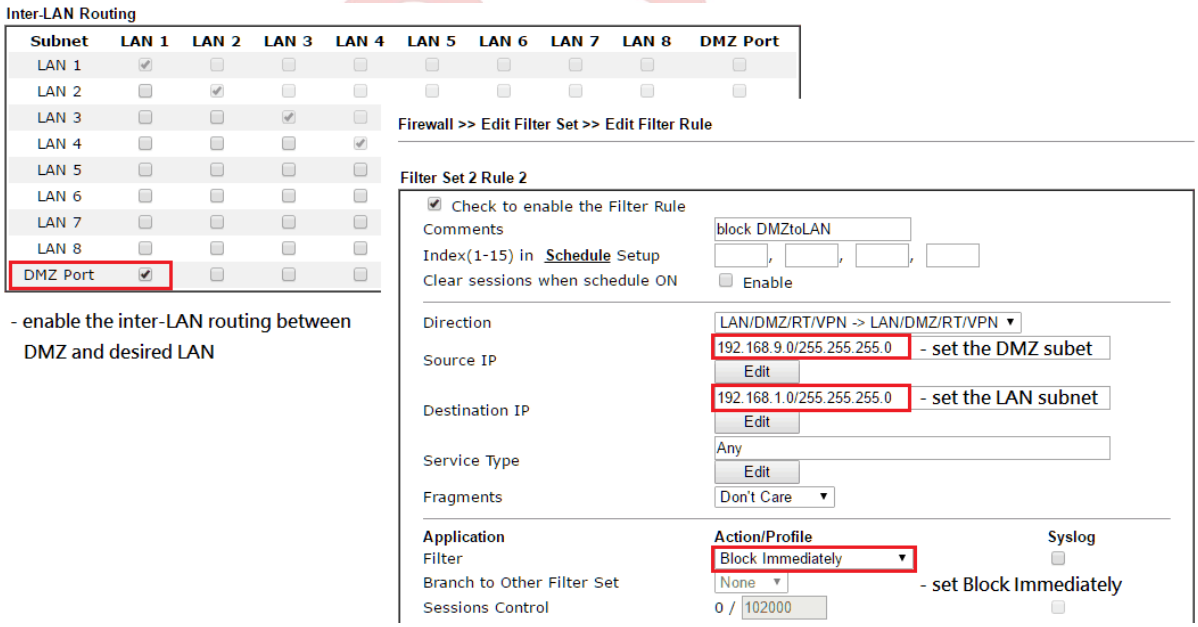


Yukarıdaki resimde yeşil ok, İnternet üzerindeki kullanıcıların routerın WAN IP adresini kullanarak DMZ Host'una erişebilecekleri DMZ Host'un normal kullanımını gösterir. Bir saldırgan DMZ Host'un güvenliğini ihlal ederse, saldırgan aynı subnetteki diğer ana bilgisayarlara kırmızı oklarla gösterilen yetkisiz erişim sağlayabilir.

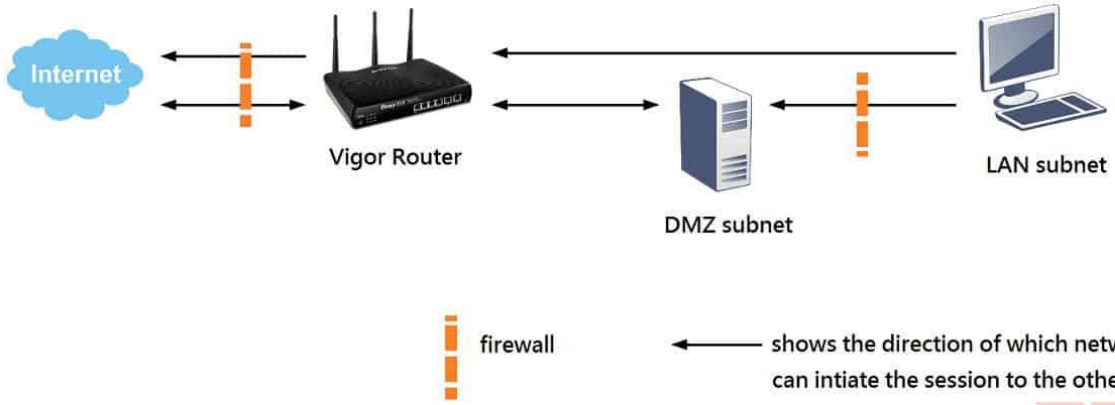
Bunun yerine DMZ subnetini kullanarak bu tür tehditlerden kaçınabiliriz. Bağımsız bir subnet olduğundan, DMZ Host'u ve diğer LAN subneti izole edilmiştir. Bu nedenle, eğer bir saldırgan DMZ subnetindeki bir Host'a girerse, diğer LAN subnetlerine erişemez.



WAN Hostlarının DMZ subnetindeki sunuculara erişmesine izin vermek için, ağ yöneticisinin bu sunuculara Port Redirection veya Open Ports kurallarını ayarlaması gerekir. Ayrıca, LAN subnetlerindeki kullanıcıların DMZ subnetindeki sunuculara erişmesine izin vermek için, inter-LAN routing etkin olmalı ve aşağıda gösterildiği gibi firewall kuralları ayarlanmalıdır.



Router daha sonra LAN subnetlerindeki hostların DMZ subnetine erişmesine izin verir, ancak DMZ subnetindeki hostun LAN subnetlerine session başlatmasını önler. Kural, hem routerı hem de LAN'ın geri kalanını DMZ'den yetkisiz erişime karşı korur.



DMZ subnetinin yapılandırması, DMZ Host'undakinden biraz daha karmaşık olsa da, daha güvenli bir ağ ortamına sahip olmanın sonucu onu değerli kılar.

Vigor3220'de Dedicated DMZ Portu

Birden çok LAN portuna sahip Vigor routerların çoğunda, router, DMZ subneti etkin olduğunda, LAN portlarından birini DMZ portu olarak bir kenara koyacaktır. Ancak Vigor3220 serisi routerlar, bir LAN portu ve her zaman etkin olan dedicated bir DMZ portu ile donatılmıştır.