

DNS Güvenliđi

DNS Security , Domain Name System 'e (DNS) güvenlik eklemek için verilen bir özellik olan Domain Name System Security Extensions (DNSSEC)'a dayanmaktadır. Dijital imzaları kullanarak, DNS sunucusu, DNS istemcilerine DNS veri bütünlüğü ve kaynak kimlik doğrulaması sağlayabilir. Vigor Router'da DNSSEC'i etkinleştirirseniz, bir domain name sormadan önce, Router'ı DNSKEY ve RRSig için DNS sunucuları tarafından sağlanan bilgileri doğrulamak ve böylece sahte DNS yanıtları almamak için yinelemeli sorgular gerçekleştirecektir. WAN arayüzünde DNS Security'ı etkinleştirmek için:


1. Application >> DNS Security gidin, DNSSEC'in uygulanmasını istediđiniz WAN interfacesini seçin ve OK'a tıklayın.

Application >> DNS Security

DNS Security

General Setup		Domain Diagnose		Refresh
Enable	Interface	Primary DNS	Secondary DNS	Bogus DNS Reply
<input checked="" type="checkbox"/>	WAN1	---	---	Pass ▼
<input type="checkbox"/>	WAN2	---	---	Pass ▼
<input type="checkbox"/>	WAN3	---	---	Pass ▼
<input type="checkbox"/>	WAN4	---	---	Pass ▼

Note:

 The DNS server supports DNSSEC



 The DNS server does not support DNSSEC, function may not work as expected even if it is enabled

OK

2. Router, kullanılan DNS sunucusunun DNSSEC'yi destekleyip desteklemediđini kontrol edecektir. Bu birkaç saniye sürecek. Bundan sonra, DNS sunucusu IP'sinden önce yeşil bir kilit simgesi gösteriyorsa, DNS sunucusunun DNSSEC'yi desteklediđi anlamına gelir. Ancak bunun yerine gri bir kilit simgesi gösteriyorsa, bu, DNS sunucusunun DNSSEC'yi desteklemediđi anlamına gelir. DNS sunucusunu WAN >> Internet Access >> Details Page. değiştirebilirsiniz.

Application >> DNS Security

DNS Security

General Setup		Domain Diagnose		Refresh
Enable	Interface	Primary DNS	Secondary DNS	Bogus DNS Reply
<input checked="" type="checkbox"/>	WAN1	 168.95.1.1	 168.95.192.1	Pass ▼
<input type="checkbox"/>	WAN2	---	---	Pass ▼
<input type="checkbox"/>	WAN3	---	---	Pass ▼
<input type="checkbox"/>	WAN4	---	---	Pass ▼

3. Sahte bir DNS yanıtı için Policy'yi "Drop" olarak ayarlayın, böylece router imzasını doğrulayamazsa DNS yanıtını bırakacaktır.

Application >> DNS Security



DNS Security

General Setup		Domain Diagnose		Refresh
Enable	Interface	Primary DNS	Secondary DNS	Bogus DNS Reply
<input checked="" type="checkbox"/>	WAN1	168.95.1.1	168.95.192.1	Drop ▼
<input type="checkbox"/>	WAN2	---	---	Pass ▼
<input type="checkbox"/>	WAN3	---	---	Pass ▼
<input type="checkbox"/>	WAN4	---	---	Pass ▼

4. Domain Name DNSSEC ile uyumlu değilse, routerin DNS sorgusunu doğrulayamayacağını unutmayın. Domain Name'in DNSSEC'yi destekleyip desteklemediğini Domain Diagnose sekmesi üzerinden kontrol edebilirsiniz.

Application >> DNS Security



DNS Security

General Setup	Domain Diagnose	DNS Cache	
Domain: <input type="text" value="www.nctu.edu.tw"/>	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6		
Interface: <input type="text" value="WAN1"/>			
DNS Server: <input type="text" value="168.95.1.1"/>			
<input type="button" value="Diagnose"/>			
Note: If the domain have not been queried before, it will takes few seconds to process.			
Result <input type="button" value="Clear"/>			
Domain Name	IP Address	Interface	Verify Result
-----	-----	-----	-----
www.nctu.edu.tw	140.114.60.160	WAN1	Secure