آموزش راه اندازی IPSec VTI در روتر سیسکو (نسخه PDF)

یک روش tunnelling و ارتباط امن و نسخه انعطاف پذیر تر پروتکل IPsec با پیاده سازی آسان تر، قابلیت های بیشتر، و ارائه خدمات بهتر در واقع IPsec VTI برای ما برقراری ارتباط در سطح WAN و ارسال و مسیریابی Packet ها و Data های مارا به صورت Multicast و Unicast به صورت Encrypted (رمزنگاری) شده را فراهم می آورد. قابلیت اعمال NAT, Quality Of Service و access control list در واقع VTI در دو نوع DVTI و SVTI ارائه شده است

SVTI مخفف Static Virtual Tunnel Interface وقتی مـا از برای یک ارتباط Site-T-Site از VTI اسـتفاده میکنیم در واقع یک Tunnel برای ارتباط دو شـبکه باهم اینکار را انجام میدهیم.زمانی که از SVTI اسـتفاده میکنیم توانایی پیاده سازی یک routing protocol در بین دو شبکه را خواهیم داشت که ترافیک کاربران دو شبکه به سمت هم دیگر مسیریابی شود بدون نیاز به ۴ bite اضافی پروتکل GRE اینکار موجب بالارفتن پهنای باند کاربران می شود.

DVTI مخفف Dynamic Virtual Tunnel Interface ارتباط بسـیار مقایس پذیر و امن تر استفاده از مکانیزم Hub-And-Spoke به منظور Tunnel establishing داشتن قابلیت انجام remote-access VPN توانایی استفاده از Radius server، Firewall، NefFlow، QoS توانایی تعریف Per-group و Per-user group و بسیاری از قابلیت های دیگر که DVTI در اختیار ما قرار میدهد

چندین نکته

۱. پشتیبانی نکردن از IPv۶
۲. توانایی اعمال ACL
۳. کپسوله سازی پکت های ESP و IKE در UDP در مواقع استفاده از NAT در شبکه
۴. به صورت default تمامی traffic های که از VTI عبور میکنند به صورت encrypted هستند
۵. توانایی استفاده از static routing و Dynamic routing

سناریو ما به شکل زیر میباشد که ما نیاز داریم یک S-VTI بین R۱ و R۲ برقرار کنیم و ارتباط آن هارا به صورت encrypted ردوبدل کنیم

تعریف Profile و تنظیم پارامتر های مختلف برای Tunnelling

```
crypto isakmp policy 1
encryption 3des
authentication pre-share
group 2
crypto isakmp key Amirhosein address 10.1.1.1 255.255.255.0
crypto IPsec transform-set Cisco1 esp-3des esp-md5-hmac
crypto IPsec profile Cisco
set transform-set Cisco1
```

تعریف interface tunnel:

```
interface tunnel 100
tunnel source fasteth 0/0
tunnel destination 50.50.50.1
tunnel mode ipsec ipv4
tunnel protection ipsec profile Cisco
crypto isakmp policy 1
encryption 3des
```

```
encryption aes
authentication pre-share
group 2
crypto isakmp key Amirhosein address 10.1.1.2 255.255.255.0
crypto IPsec transform-set Cisco1 esp-3des esp-md5-hmac
crypto IPsec profile Cisco
set transform-set Cisco1
```

تعریف interface tunnel:

```
interface tunnel 100
tunnel source fasteth 0/0
tunnel destination 50.50.50.2
tunnel mode ipsec ipv4
tunnel protection ipsec profile Cisco
```

نوشتن یک Static-Route برای ارتباط site ها باهم در هر دو روتر

```
ip route 0.0.0.0 0.0.0.0 tunnel 100
```

پیاده سازی S-VTI به پایان رسـید به بخش verification و دستورات troubleshooting ان میپردازیم:دسـتور زیر اطلاعات کاملی در رابطه با tunnel که ایجاد کرده اییم به ما میدهد

```
show interface tunnel 100
```

دستور زیر نیز session های ایجاد شده را برای ما نشان میدهد

```
show crypto session
```

نویسنده: امیرحسین تنگسیری نژاد

مطلب اصلی