سیسکو به پارسی

آشنایی با Virtual Private Network

نوشته:

شفق زندی

سایت سیسکو به پارسی http://blog.shafagh.com/persian

انجمن سیسکو به پارسی http://forum.shafagh.com

Virtual Private Network

برای تشریح VPN ابتدا نگاهی به معنی لغوی آن می اندازیم:

Virtual Private Network به معنی شبکه خصوصی مجازی، شبکه ای است که بر روی شبکه ای دیگر تشکیل شده است. شبکه زیرین که کار زیرساخت را ایفا میکند معمولا شبکه ای عمومی (نظیر اینترنت) است...

برای توضیح واژگانی نظیر Transparent و Virtual میتوان مثال زیر را عنوان کرد:

اگر چیزی را دیدی و آنجا بود، حقیقی است = Real

اگر چیزی را دیدی اما بصورت حقیقی آنجا نبود مجازی است = Virtual

اگر چیزی را ندیدی اما آنجا بود Transparent است = شفاف

حال با توجه به تعاریف عنوان شده به مثالهای زیر رجوع میکنیم:

یک سرور که آدرسPublic داشته و درون Rack قرار دارد یک سرور حقیقی است = Real Server

یک سرور که قابل دسترسی از طریق IP است اما روی VMware نصب شده و روی سخت افزار مستقیما عمل نمی کند Virtual است.

یک Firewall که در مسیر Trace Route ما دیده نمیشود و قابل Ping و ردیابی نیست Transparent است.

Cisco in Persian

شبکه VPN همانطور که از اسمش پیداست Virtual است... بصورت فیزیکی ساختاری ندارد. وقتی مخابرات برای سازمانی با Frame Relay یا ATM و X.25 یا حتی بصورت Leased Line های مختلف ارتباط شبکه نقاط دوردست را فراهم میکند به آن Overlay Network یا Overlay VPN Model میگوییم. یعنی بنای شبکه شما روی شبکه سرویس دهنده نهاده شده است. اگر VPN بصوت Peer-to-peer باشد یعنی شبکه شما بصورت پویا با شبکه سرویس دهنده ارتباط برقرار میکند و از یک Routing Protocol برای اطلاع رسانی مسیرها استفاده میکند، نظیر MPLS VPN.

اما کاربرد عمومی واژه VPN بیشتر شبکه مجازی روی اینترنت است...

کلا دو مدل دسترسی به VPN در Internet پیدا سازی میشود:

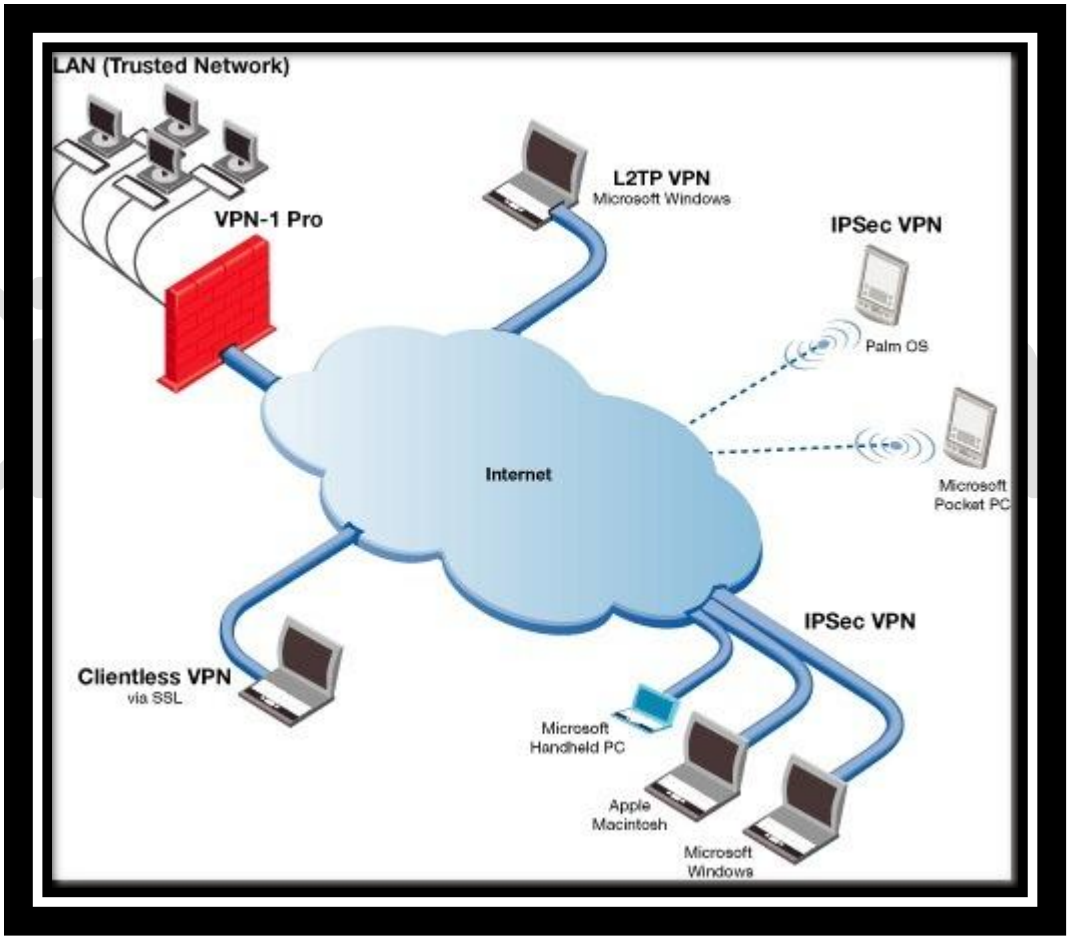
- Remote Access
- Site to Site

مدل Remote Access امکان دسترسی کاربر را از منزلش به شبکه محیط کار فراهم میکند. بطور مثال من خیلی از روز ها جلسات شرکت و کارهایم را از راه دور، از منزل یا در سفر انجام میدهم برای این کار از Cisco VPN Client یا Cisco Any Connectاستفاده میکنم.

در Remote Access بسته به نوع تکنولوژی و تولیدکننده از پروتکل های متنوعی استفاده میشود نظیر PPTP و PPTP.L2TP یا Point to Point Tunneling Protocol پروتکلی است که امکان VPN را البته بدون رمزنگاری و Encryption ایجاد میکند. در این روش PPP و GRE استفاده شده و روی پورت ۱۷۲۳ TCP کار میکند. از ویندوز ۹۵ پشتیبانی این پروتکل استاندارد در ویندوز گنجانده شد و با RFC2637 توسط IETF استاندارد شد:

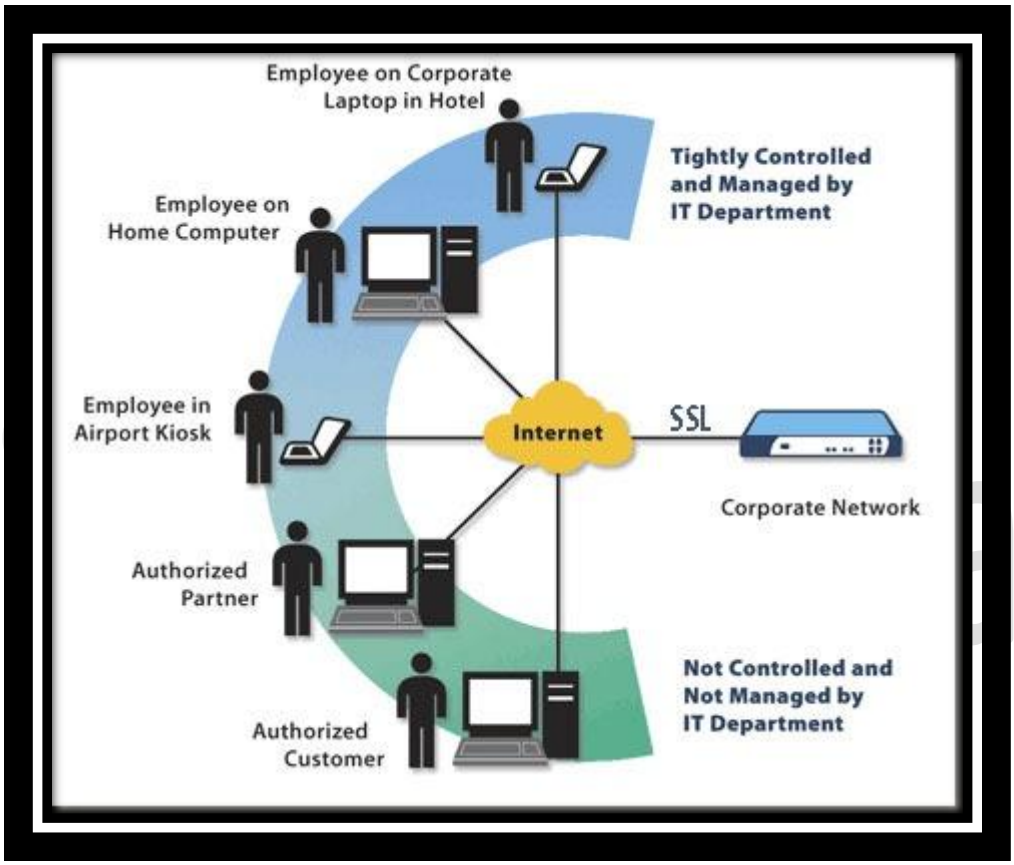
http://tools.ietf.org/html/rfc2637

PPTP را در سیسکو با دستورات VPDN میتوان فعال کرد هر چند که سیسکو پروتکل L2F را نیز ارائه کرد. در سمت دیگر برای Encryption و بالابردن امنیت و رمزنگاری L2TP در سال ۱۹۹۹ ارائه شد.



محبوبترین پروتکل برای VPN، IPSEC است. در سیسکو برای فعال کردن آن به نسخه ای از IOS با ویژگی های Advanced-Security نیاز داریم. سیسکو نرم افزار Cisco VPN Client را برای ویندوز، Mac، Linux و iPhone ارائه کرده تا بتوان از تمام کلاینت های موجود به VPN وصل شد و اطلاعات Encrypt شده را رد و بدل کرد.

جدیدترین نوع VPN استفاده از SSL و TLS است که بدون نیاز به نرم افزار خاصی در سمت کاربر و تنها به کمک مرورگر میتوان به آن وصل شد و شروع به کار کرد. بطور مثال SSL VPN را روی Cisco ASA در شرکت فعال میکنیم و از منزل با وصل شدن به صفحه Webpage شرکت و وارد کردن Username/Password به File Server و RDP های روی سرور درون صفحه Browser متصل میشویم. بدین صورت از Café Net ها و کامپیوترهایی که برنامه VPN ندارند نیز میتوان برای کار استفاده کرد.

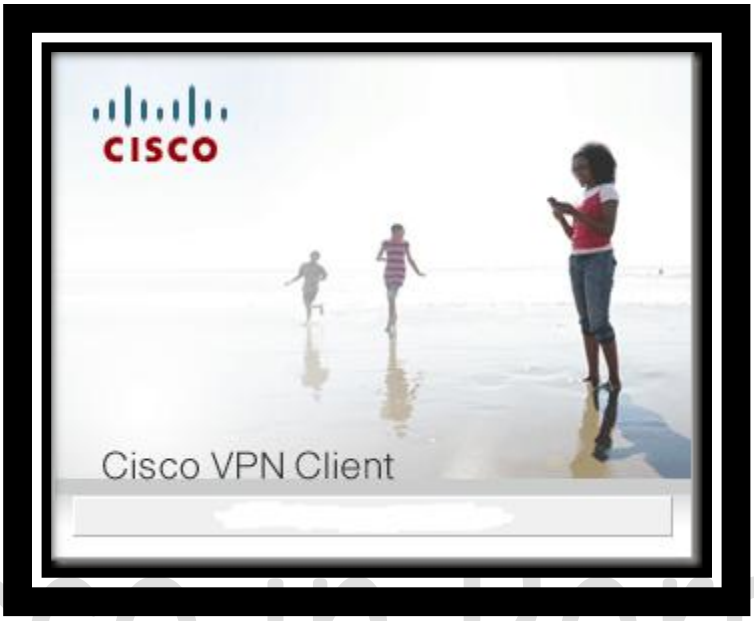


مدل دوم پیاده سازی VPN ، بنام Site to Site یا LAN to LAN برای ایجاد VPN بین دو یا چند شبکه است بطور مثال یک شعبه کوچک بانکی با پنج تا ده کلاینت به یک شعبه مرکزی VPN میکند (Tunnel)

در این مدل اگر نیازی به رمزنگاری نباشد میتوان از پروتکل GRE یا Generic Routing Encapsulation استفاده کرد. در صورتیکه به Encryption نیاز باشد از IPsec همراه با ISAKMP یا IKE برای رد و بدل کردن کلید و Certificate استفاده میشود. حالت ترکیبی استفاده از GRE همراه با IPsec امکان خوبی برای Routing و همچنین انتقال امن دیتا را فراهم میسازد.

سیسکو EZVPN را برای ساده کردن پیاده سازی Site to Site VPN ارائه کرده بدین صورت که با IP های Dynamic اینترنت نیز بتوان از VPN استفاده کرد.

DMVPN و GETVPN دو مدل دیگر VPN برای شبکه هایی است که میخواهند تعداد زیادی از شعب را روی اینترنت به هم متصل کنند در این مدل غیر از سایت های اصلی بقیه میتوانند از IP داینامیک و ADSL استفاده کنند که نیازی به آدرس استاتیک نباشد. (پایین آوردن هزینه)



Cisco in Persian

جالب اینجاست که تمامی تکنولوژی های VPN روی یک روتر سری ۱۸۰۰ یا ۲۸۰۰ سیسکو بهمراه IOS مورد نیاز، قابل پیاده سازی است. قبلا سیسکو محصولی بنام VPN Concentrator ارائه میکرد که با ارائه Cisco ASA تولید آن متوقف شد.