مبانی امنیت شبکه

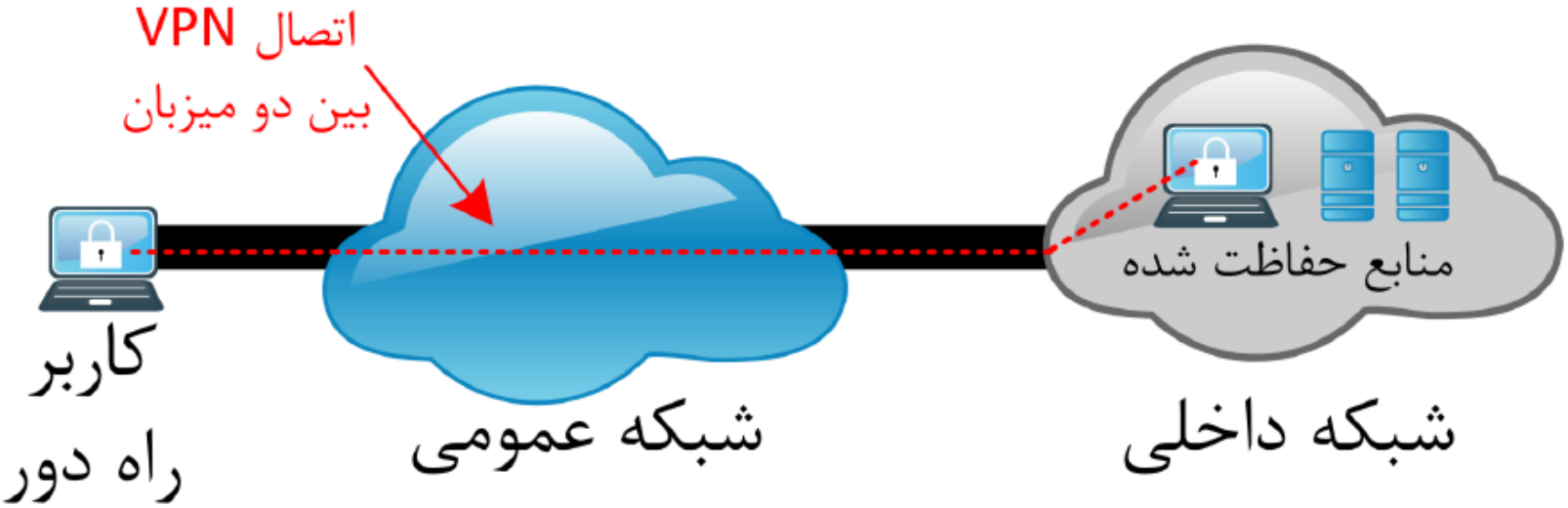
گردآوری: محمدعلی عظیمی

شبکه های خصوصیVPN

دو راهکار برای حفظ امنیت در سطح شبکه

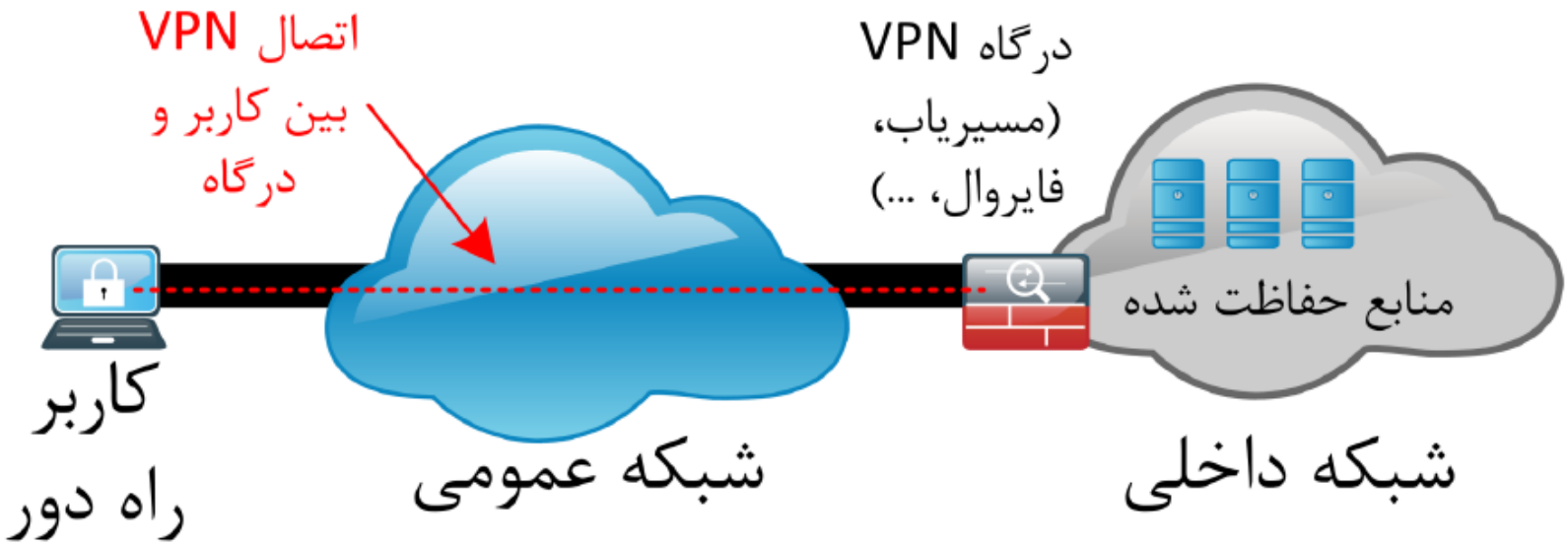
- به کار گیری شبکه ای کاملاً خصوصی و حفاظت فیزیکی از آن
  مثال: خطوط اجاره ای (Leased Line)
  حفاظت فیزیکی از شبکه امر دشواری است.
  این راهکار بسیار گران است.
- استفاده از یک شبکه وعمومی و به کار گیری الگوریتمها و پروتکلهای رمزنگاری روی آن برای حفاظت از اطلاعات
  شبکه خصوصتی مجازی) Virtual Private Network

انواع اتصالات – VPNمیزبان به میزبان



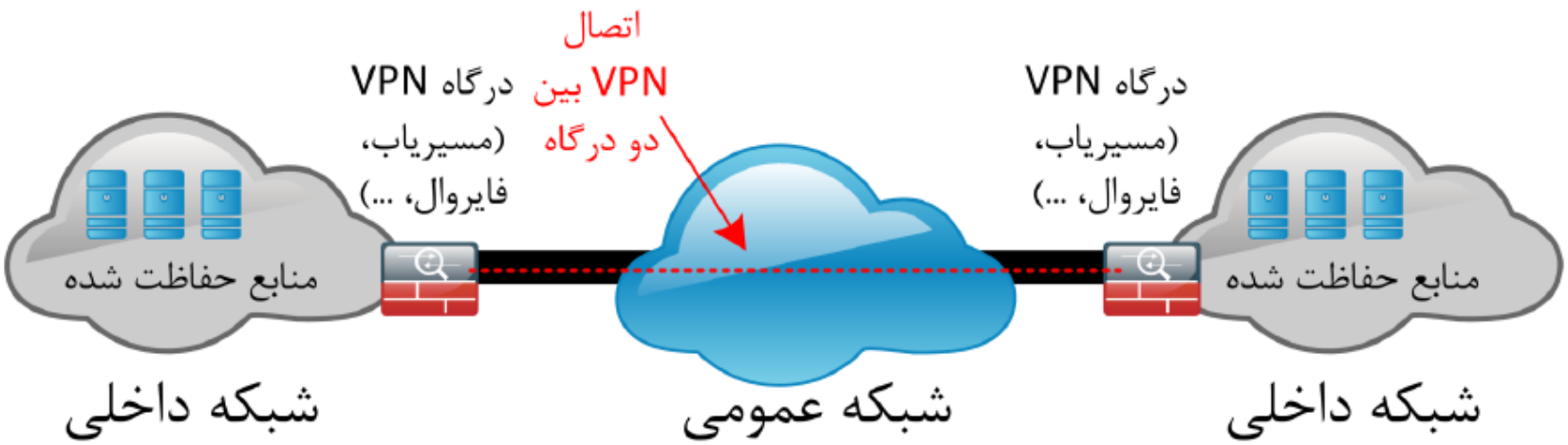
Host to Host (H2H)

انواع اتصالات VPN – میزبان به شبکه



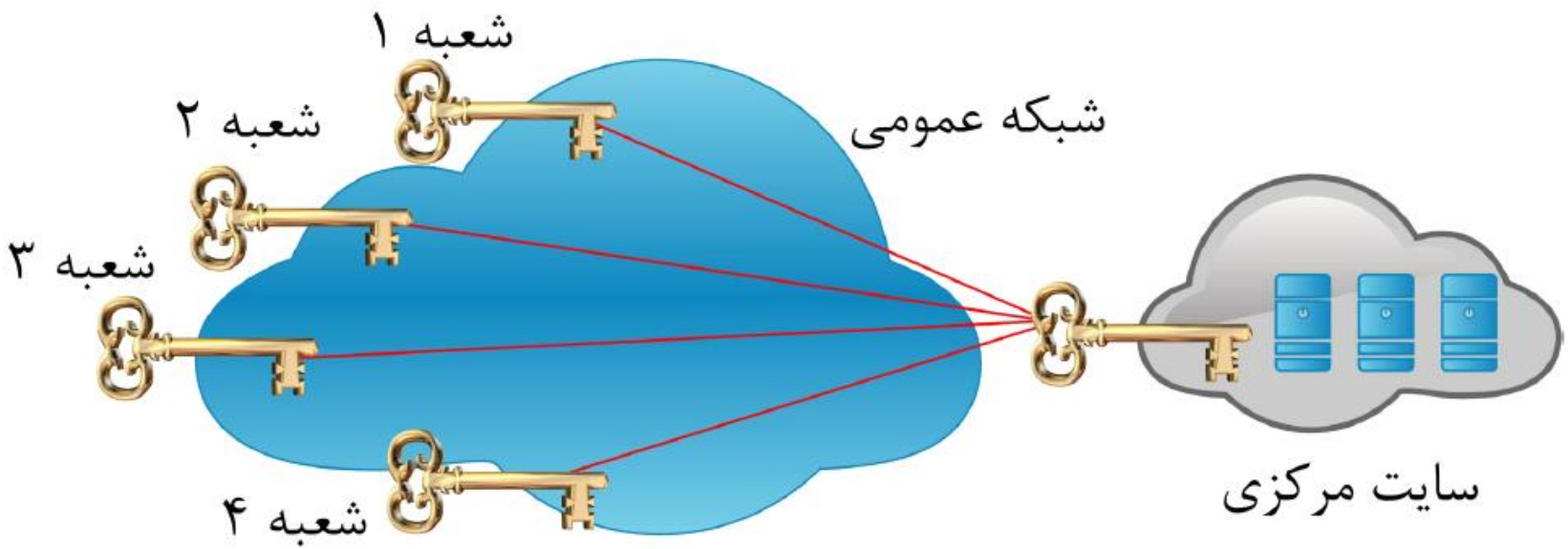
Host to Net (H2N)

انواع اتصالات VPN – شبکه به شبکه



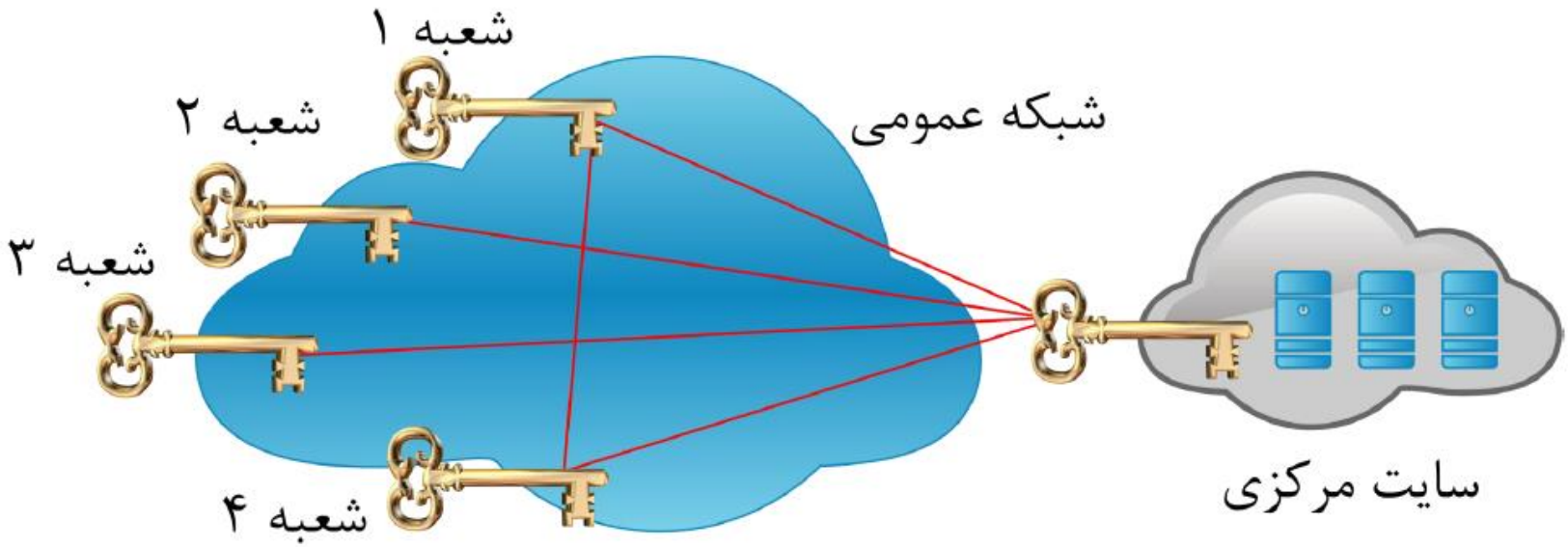
Net to Net (N2N)

انواع توپولوژی – اتصال مرکزیN2N



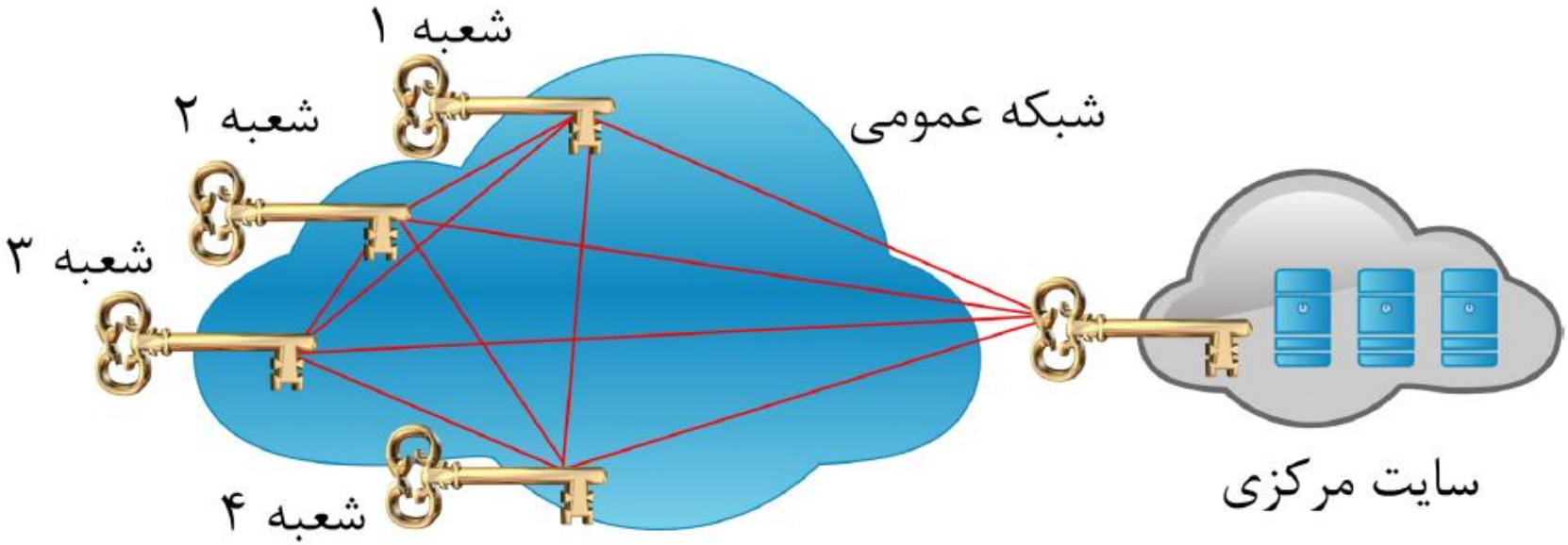
Hub and Spoke

انواع توپولوژی - اتصال ناقصN2N



Partial Mesh

انواع توپولوژی – اتصال کامل N2N



Full Mesh

سایر انواع توپولوژی N2N

- **همبندی تلفیقی:** تعدادی سایت مرکزی داریم، و هر سایت مرکزی تعدادی شعبه دارد. مثال: مراکز استان و شهرستانهای کوچکتر

معمولاً سایتهای مرکزی به هم اتصال کامل دارند.

اتصال شعبه ها با سایت مرکزی خود به صورت اتصال مرکزی یا اتصال ناقص است.

- همبندی پویا Dynamic Multipoint VPN یا DMVPN

ایجاد اتصالات VPN به صورت پویا و نه ایستا

سایت مرکزی به عنوان واسط برقراری VPN (و نه واسط ارتباطات بعدی)

VPN: شبکه خصوصی مجازی

- خصوصی بودن در مقابل عمومی بودن: هر شبکه آدرس‌های خود را داشته باشد و اطلاعات یک سازمان برای سازمان دیگر قابل شنود نباشد و پهنای‌باند اختصاصی داشته باشد
- مجازی بودن در مقابل حقیقی بودن: کاربران سازمان در شعبه‌های مختلف احساس کنند در یک شبکه محلی باهم ارتباط دارند
- ارتباط بین شعب مختلف از طریق زیرساخت عمومی موجود انجام می شود.

مزایای VPN

- امنیت
- ارزان
- سرویس سیار
- کیفیت سرویس
- برقراری ساده و اتوماتیک
- اضافه کردن و حذف کردن به صورت نرم‌افزاری
- استفاده بهینه از منابع شبکه

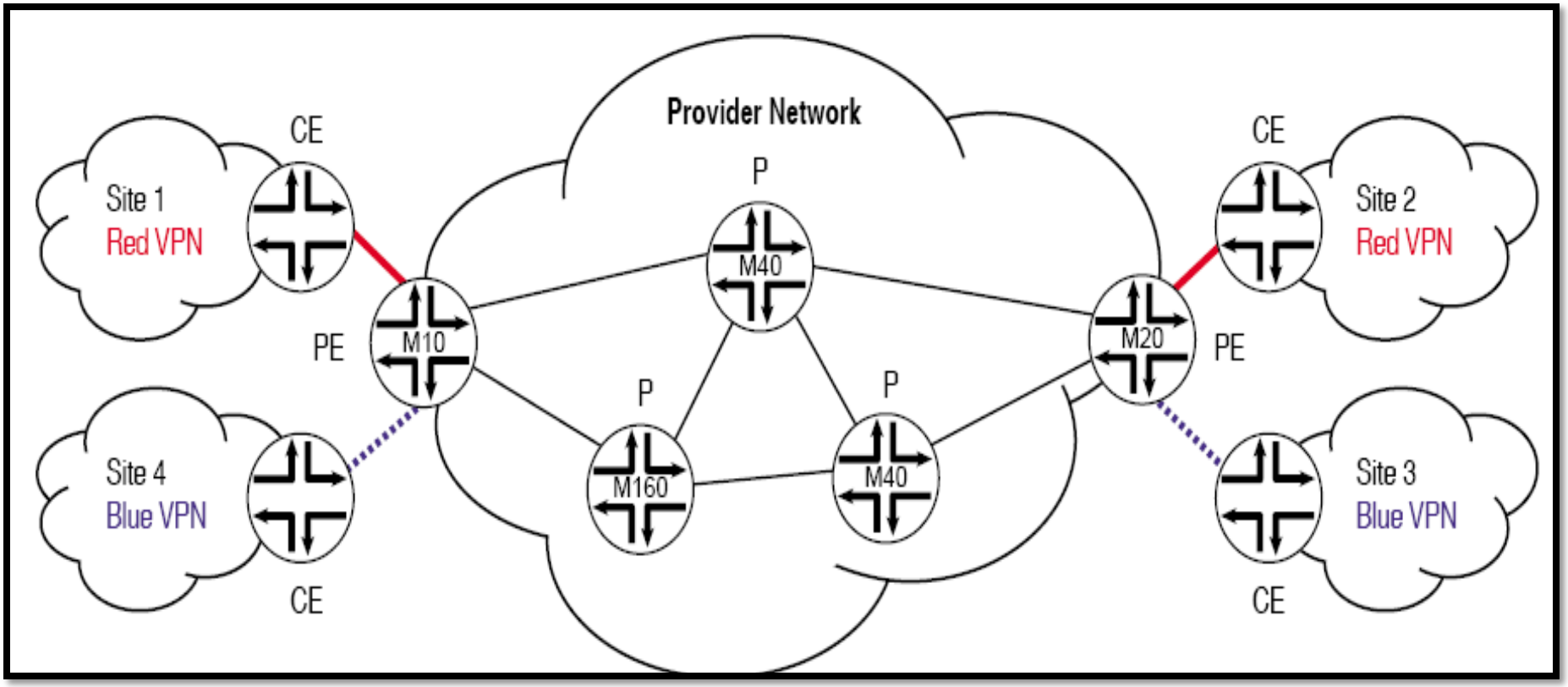
معیارهای ارزیابی VPN

- مسائل امنیتی
- تعداد سایت‌ها
- تعداد کاربران
- پیچیدگی مسیریابی
- برنامه‌های کاربردی حساس و کیفیت سرویس
- میزان ترافیک و الگوی ترافیک
- تخصص شبکه مورد نیاز برای مشتری
- قابلیت گسترش
- هزینه

تجهیزات شبکه VPN

- تجهیزات لبه شبکه مشتری (CE)– مسیریاب و یا سوئیچ لبه شبکه مشتری تجهیز یا تجهیزاتی است که مستقیما با تجهیزات شبکه تامین‌کننده سرویس متصل است.
- تجهیزات لبه شبکه تامین‌کننده سرویس (PE)– این تجهیز متعلق به Provider است که اولین سطح از تجمیع را برای CEهای مختلف انجام می‌دهد. تجهیزات PE به طور منطقی VPNهای مختلفی را که در آنها شرکت دارد از هم جدا می‌سازد.
- تجهیزات تامین‌کننده سرویس(P)– این تجهیز معمولا یک مسیریاب هسته است که دومین سطح از تجمیع را برای PE ها انجام می‌دهد. تجهیزات P در هیچ یک از عملیات VPN شرکت نداشته و معمولا از وجود VPNها بی‌اطلاع می‌باشد.

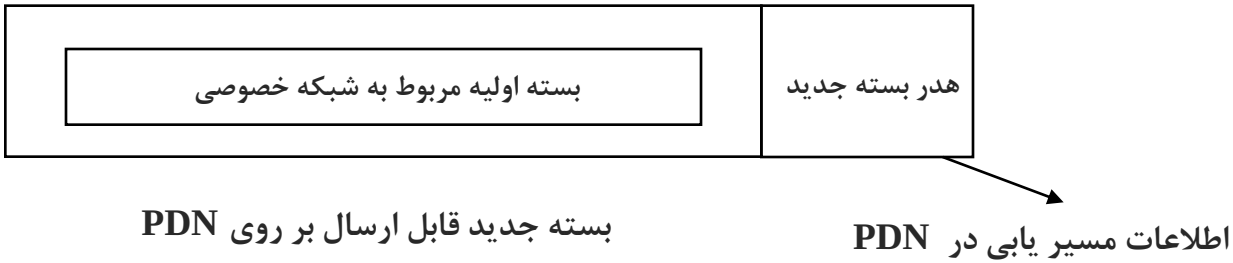
تجهیزات شبکه VPN



پروتکلهای VPN

VPN ها از دو جنبه محرمانگی (خصوصی بودن) و مجازی بودن برخوردارند. محرمانگی با استفاده از رمزنگاری بدست می‌آید. مجازی سازی به معنای ایجاد ارتباط بین دو بخش یک شبکه خصوصی از طریق شبکه عمومی است بنحوی که از دید شبکه خصوصی یک ارتباط مستقیم (بی واسطه) بین دو بخش آن دیده شود.

اینکار با روش تونل زنی یا Tunneling انجام می شود. تونل زنی با استفاده از Encapsulation پیاده سازی می شود.



پروتکلهای VPN

ادامه

با استفاده از Encapsulation، بسته ارسالی از یک بخش شبکه خصوصی به بخش دیگر درون یک بسته جدید قرار می‌گیرد که در هدر آن اطلاعات مسیریابی از درون شبکه PDN (عمومی) از نقطه A به نقطه B ثبت می گردد. بنابراین یک مسیر مجازی از نقطه A به B ایجاد می شود. بسته های ارسالی بین دو بخش یک شبکه خصوصی در این مسیر و درون بسته‌های جدید، حمل می‌شوند. بنابراین مکانیزم ارسال دورن PDN از دید شبکه خصوصی پنهان می ماند. این امر مانند این است که یک تونل از درون شبکه عمومی بین دو بخش شبکه خصوصی زده شده باشد و لذا لفظ تونل زنی استفاده می‌شود. تونل ها و به تبع آن VPN ها به سه دسته اصلی تقسیم می‌شوند:

- تونل های لایه ۲
- تونل های لایه ۳ - برای یک پرتکل مشخص از لایه ۳
- تونل های لایه ۴ - برای یک پرتکل مشخص از لایه ۴

تونل لایه ۲

بین دو عنصر کناری (Edge Device) بخش A و B شبکه خصوصی ایجاد شده و یک مسیر از پیش تعیین شده بین نقطه A و B ایجاد می‌شود. از آنجا که مسیر عبور بسته‌های encapsulate شده از پیش تعیین شده است، به آن تونل لایه ۲ گفته می شود. هدر بسته های encapsulate کافی است اطلاعات مسیر تعیین شده (مانند برچسب مسیر) را حمل کنند و نه آدرس شبکه مبداء و مقصد را.

در گیرنده بسته اولیه از درون بسته encapsulate شده استخراج و بر اساس آدرس مقصد، درون شبکه خصوصی مسیریابی شده و در مقصد بر حسب شماره پورت لایه ۴ به پروسه کاربرد مربوطه تحویل می‌گردد.

پروتکلهای اصلی تونلینگ لایه ۲ عبارتند از MPLS، PPP، PPTP، L2TP.

مشکل قابلیت گسترش: اگر یک شبکه خصوصی از M قسمت تشکیل شده باشد و بخواهیم تمام بخش ها بصورت مجازی مستقیماً بهم متصل باشند، لازم است M(M-1)/2 تونل بین آنها ایجاد شود. که با افزایش M بصورت توان ۲ از M افزایش می یابد.

تونل لایه ۳

- بین دو عنصر کناری(Edge Device) بخش A و B شبکه خصوصی ایجاد می شود ولی مسیر عبور بسته‌های encapsulate شده از پیش تعیین شده نیست و لذا هدر بسته‌های encapsulate شده باید حاوی آدرس شبکه مبداء و مقصد باشد. چون این بسته‌ها توسط پروسه های لایه ۳ توسط عناصر PDN پردازش می شوند، به این روش تونلینگ لایه ۳ گفته می‌شود.
- هر بخش از شبکه خصوصی، کافی است دارای یک آدرس شبکه عمومی باشد.
- عمل مسیریابی در VPN Gateway انجام می شود تا مقصد بسته تعیین شود و بر اساس آن آدرس عمومی بخش مقصد برای encapsulate کردن بسته ها استفاده می شود.
- در طرف گیرنده، بسته اولیه استخراج و درون شبکه خصوصی مسیریابی می شود.
- اگر عناصر شبکه خصوصی دارای آدرس های عمومی باشند، تونل لایه ۳ می‌تواند بین تک تک تجهیزات در دو بخش A و B برقرار شود.

تونل لایه ۳

ادامه

- در صورتی که عناصر شبکه خصوصی دارای آدرس‌های عمومی نباشد، برای ایجاد تونل بین یک تجهیز در بخش A و B، باید عناصر کناری (Edge Devices) نقش واسط را بازی کنند و در واقع تونل از سه بخش تشکیل می گردد.

تونل لایه ۴

بین دو پروسه نرم افزاری ایجاد می شود و لذا هدر بسته های جدید باید حاوی هدر لایه ۳ و هدر لایه ۴ باشد.

پروتکل IPSec برای ایجاد تونل لایه سه و پروتکلهای SSL و TLS برای تونل‌های لایه ۴ تعریف شده اند.

انواع پروتکلهای ایجاد VPN

- IPsec (IP Security)
- MPLS (Multiprotocol Label Switching)
- L2TP (Layer Two Tunneling Protocol)
- GRE (Generic Routing Encapsulation)
- PPTP (Point-to-Point Tunneling Protocol)
- OpenVPN (مبتنی بر پروتکل SSL/TLS)
- SSTP (Secure Socket Tunneling Protocol)

نیازمندیهای پروتکلهای تونلینگ

نیازمندیهای اصلی یک پروتکل تونلینگ عبارت است از:

1. **تعریف فرمت بسته های encapsulate شده و تعیین اطلاعات حمل شده در هدر بسته‌ها (تعریف عملکرد مکانیسم encapsulation).**
2. **ایجاد تونل شامل تعریف نقاط ابتدا و انتهای تونل و handshaking بین آنها برای توافق در مورد ایجاد تونل و نیز انجام عمل تصدیق اصالت (Authentication).** بحث signaling
3. **پیکربندی تونل شامل تعریف پارامترهای مربوط به عملکرد نقاط ابتدا و انتهایی مانند تعیین مد کاری، تعیین روش تصدیق اصالت و تعیین پارامترهای رمز نگاری (شامل تبادل کلید).**
4. **مدیریت تونل شامل اطمینان از برقرار بودن تونل (keep alive) و ارسال پیغام‌های خطا در صورت وقوع.**

دسته بندی فناوری های VPN

انواع شبکه های خصوصی مجازی

- چهار نوع VPN در RFC 2764 تعریف شده است:
  - Virtual Leased Lines (VLL) :
    - لینک های نقطه به نقطه و اتصال گرا بین سایت های مشتریان فراهم می کند.
    - مشتری هر VLL را به عنوان یک لینک خصوصی (فیزیکی) ملاحظه می کند.
  - Virtual Private LAN Segments (VPLS):
    - یک شبکه محلی را بین سایت های VPLS شبیه سازی می کند.
    - یک VPLS نیازمند استفاده از تونل های IP است که برای پروتکلی که در LAN شبیه سازی شده شفاف می باشد.
    - شبکه محلی ممکن است بوسیله یک مش از تونلها بین سایت های مشتری و یا نگاشت هر VPLS به یک آدرس همه پخشی جداگانه ، شبیه سازی شود.

انواع شبکه های خصوصی مجازی

- Virtual Private Routed Networks (VPRNs)
  - یک شبکه مسیریابی شده بر پایه IP را بین سایت های مشتری تقلید می کند.
  - باید به عنوان یک دامنه مسیریابی جداگانه از شبکه SP اصولی رفتار شود.
  - احتمال دارد VPRN از آدرس IP های غیر یکتا که توسط مشتری تعیین شده است، استفاده کند.
  - این آدرسها نباید در خارج از VPRN انتشار یابند.

انواع شبکه های خصوصی مجازی

- Virtual Private Dial-in Network (VPDN)
  - VPDN امکان اتصال کاربران راه دور را به شبکه سازمانی از طریق یک تونل را فراهم می کند.
  - نیازمند authentication & security است.

انواع دسته‌بندی VPN

- Site-to-site/Remote access/Host-to-Host
- CE-Based(Overlay)/PE-Based(Peer-to-Peer)
- Managed/Unmanaged
- Layer1/Layer2/Layer3/Layer4
- Intranet/Extranet/Access

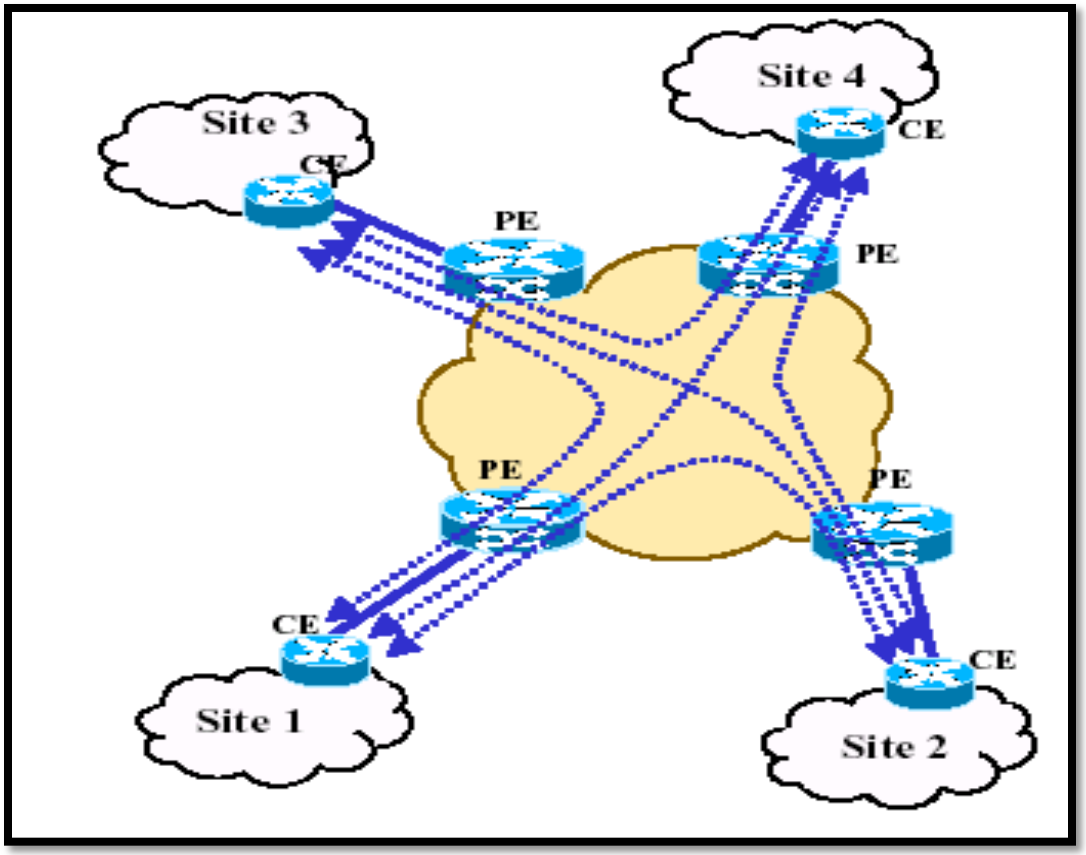
دسته بندی فناوری های VPN از نظر لایه ای

OSI Layer	VPN Protocol
Application Layer 7	
Transport Layer 4	• Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
Network Layer 3	• IP Security (IPSec)
Data Link Layer 2	• Point-to-Point-Tunneling Protocol (PPTP) • Layer 2 Tunneling Protocol (L2TP) • Multi Protocol Label Switching (MPLS)
Physical Layer 1	

CE-Based VPN

- انتهای تونل در تجهیزات لبه شبکه مشتری
- به این مدل overlay نیز گفته می‌شود
- تجهیزات مشتری باید امکانات تونل‌زنی داشته باشد
- از پروتکل‌های تونل‌زنی مختلف مثل PPTP, L2TP, IPSec, IPIP, GRE, و ... می‌توان استفاده کرد

CE-Based VPN



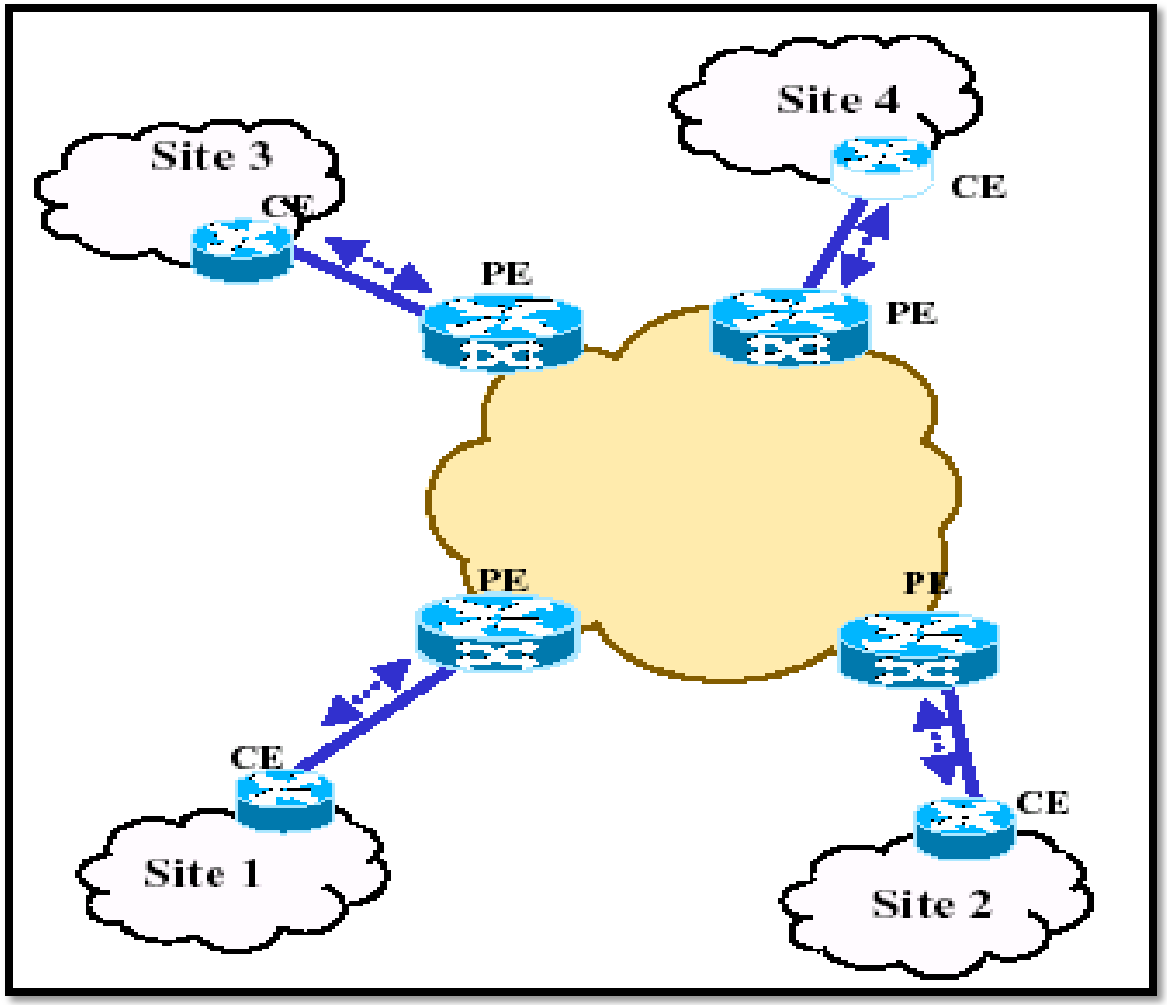
CE-Based VPN

- معایب:
  - لزوم دخالت کاربر در پیکربندی شبکه
  - عدم امکان استفاده از مهندسی ترافیک
  - عدم توسعه‌پذیری
- مزایا:
  - امکان رمزنگاری و تصدیق هویت قوی به دلیل استفاده از امکانات پروتکل‌هایی نظیر IPSec و L2TP

PE-Based VPN

- انتهای تونل در تجهیزات لبه شبکه تامین‌کننده است
- به این مدل Peer-to-Peer نیز گفته می‌شود زیرا تجهیزات مشتری با تجهیزات تامین‌کننده باید یک ارتباط Peer-to-Peer داشته باشد
- معمولا توسط پروتکل MPLS ایجاد می‌شود

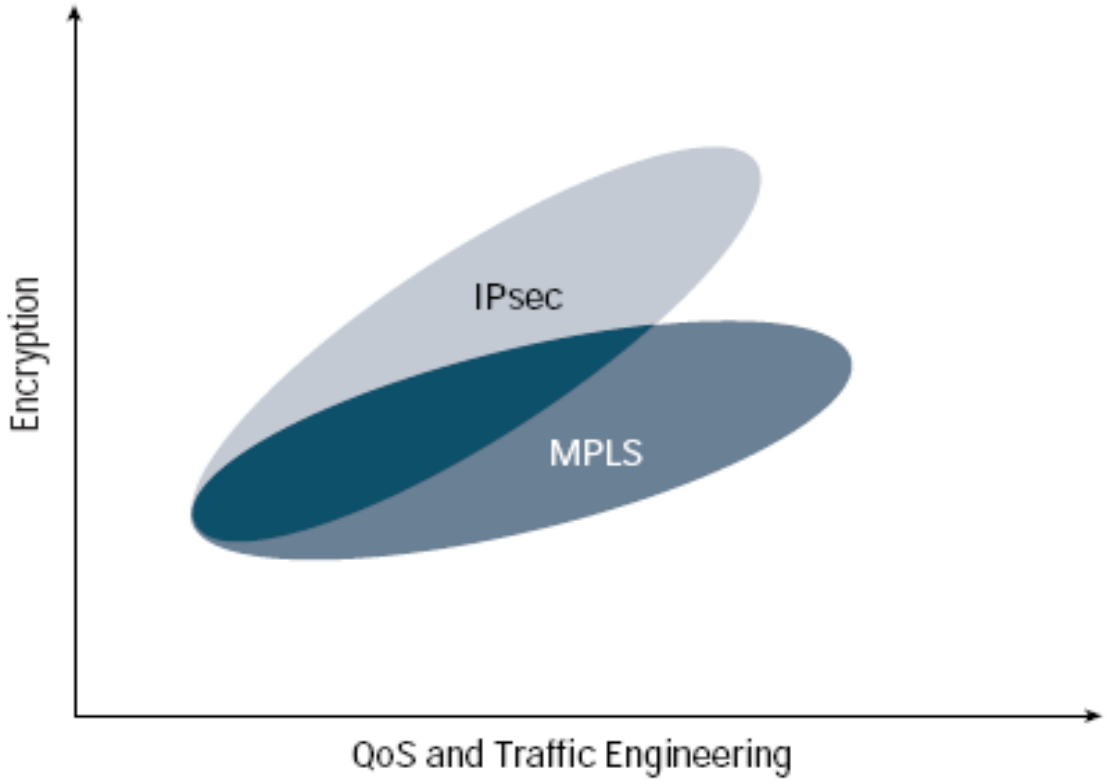
PE-Based VPN



PE-Based VPN

- معایب:
  - عدم امکان رمزنگاری و امنیت پایین نسبت به CE-Based VPN
- مزایا:
  - امکان استفاده بهینه از شبکه و مهندسی ترافیک
  - امکان ارائه کیفیت سرویس به سادگی
  - توسعه‌پذیری بسیار بالا
  - عدم دخالت کاربر در پیکربندی و سادگی واسط کاربر
  - سهولت افزودن سایت‌های جدید به شبکه برای کاربر
  - مناسب برای ایجاد شبکه‌های خصوصی مجازی بزرگ

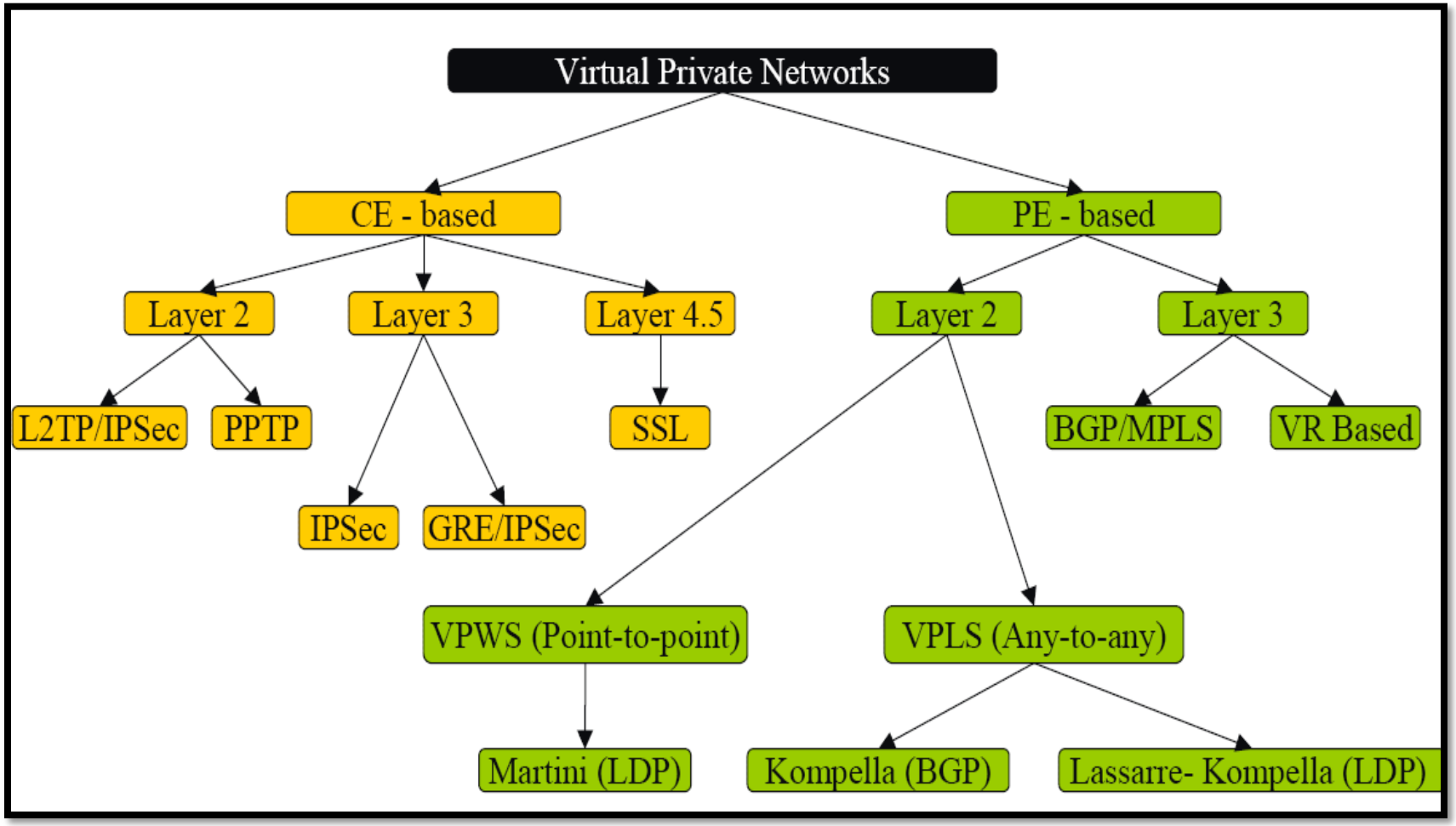
تلفیق دو نوع VPN



تقسیم وظایف بین PE و CE

- اصولا هدف این است که تا حد ممکن مسئولیت CE را کم کنیم و کارها را برعهده PE قرار دهیم
- در Leased line تنها نقش PE ایجاد ارتباط فیزیکی است و عملیات لایه‌های بالاتر همه برعهده CE می‌باشد
- در Unmanaged CE-Based تجهیزات کاربر باید توانایی تونل زدن و ایجاد ارتباط با سایت دیگر را داشته باشد و مدیریت این کار نیز برعهده مشتری است
- در Managed CE-Based مدیریت تجهیزات لبه‌ای مشتری بر عهده تامین‌کننده است
- در PE-Based تجهیزات کاربر دیگر در تونل‌زنی دخیل نیست و این کار برعهده تامین‌کننده است

VPN Taxonomy



فناوری های VPN مبتنی بر CE

Layer 2 CE-Based VPN

- در این نوع VPN انتهای تونل در سایت مشتری قرار دارد و با استفاده از پروتکل‌های لایه دو تونل زده می‌شود
- پروتکل‌های متداول مورد استفاده L2TP و PPTP هستند

Layer 3 CE-Based VPN

- در این نوع VPN انتهای تونل در سایت مشتری قرار دارد و با استفاده از پروتکل‌های لایه سه تونل زده می‌شود
- پروتکل متداول مورد استفاده IPSec است
- از مزایای این پروتکل امنیت رمزنگاری است ولی خود رمزنگاری و رمزگشایی زمان‌بر است و باعث کاهش توسعه‌پذیری این روش می‌شود

پروتکل RFC1661 : Point-to-point protocol (PPP)

- از فریم بندی شبیه HDLC استفاده می‌کند.
- ۸ بایت سربار اضافه می‌کند که می تواند به ۴ یا ۲ بایت (در صورت نیاز) کاهش یابد (Compression).
- از پروتکل‌های کنترلی Link Control Protocol (LCP) برای وظایف کنترلی استفاده می کند.
- برای تسهیل در ایجاد و استفاده از کانال با پارامترهای پیش فرض طراحی شده است.
- امکان مذاکره پارامترهای کانال بین دو طرف وجود دارد.

فرمت بسته PPP

HDLC Header	Protocol 8 or 16 bit	Header Information	Padding	Payload	HDLC Trailer

پرتکل Framing لایه ۲ است

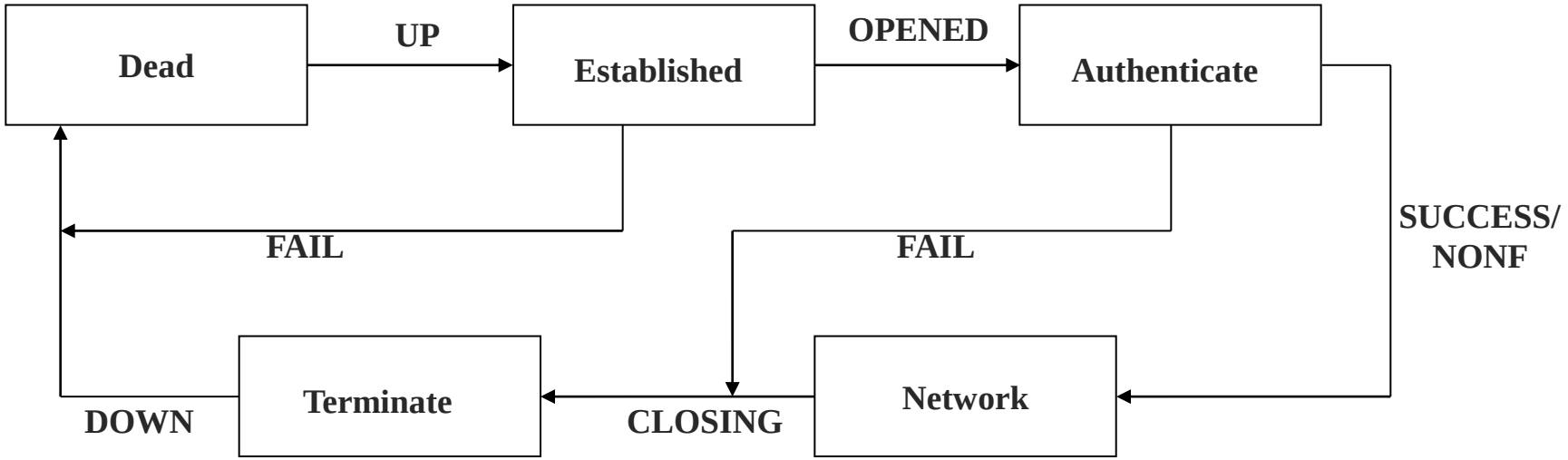
فرمت بسته PPP

ادامه

کد های تعریف شده در حال حاضر:

00cf	**PPP NLPID**
C021	**Link control protocol**
C023	**Password Auth. Protocol**
C025	**Link Quality Report**
C223	**CHAP Auth. Protocol**

دیاگرام FSM پروتکل PPP



عملکرد PPP

عملکرد PPP از چهار فاز تشکیل می شود:

1. فاز برقراری تونل با استفاده از LCP انجام می شود. Link Establishment Phase
2. فاز تصدیق اصالت اجباری نیست . Authentication Phase
3. فاز برقراری ارتباط در سطح لایه شبکه Network Layer Protocol Phase

از آنجا که ترافیک پروتکل های مختلف مانند IP و IPX میتواند بر روی یک تونل PPP مالتی پلکس شود، ارتباط در سطح هر پروتکل می‌تواند مستقلاً برقرار یا بسته شود. حال بسته‌های داده می تواند در PPP Payload حمل گردد.

4. فاز قطع ارتباط Link Terminate

پروتکل Password Authentication Protocol (PAP) : RFC1334

- پس از فاز برقراری لینک، کلمه رمز وId مکرراً ارسال می شود تا زمانی که تصدیق اصالت از طرف مقابل Ack شود.
- کلمه رمز بصورت متن ساده ارسال می شود، لذا روش قوی برای تصدیق اصالت نیست .

پروتکل RFC 1994 : Challenge handshake /Auth. Protocol (CHAP)

Chap از روش 3-way handshake استفاده می کند .

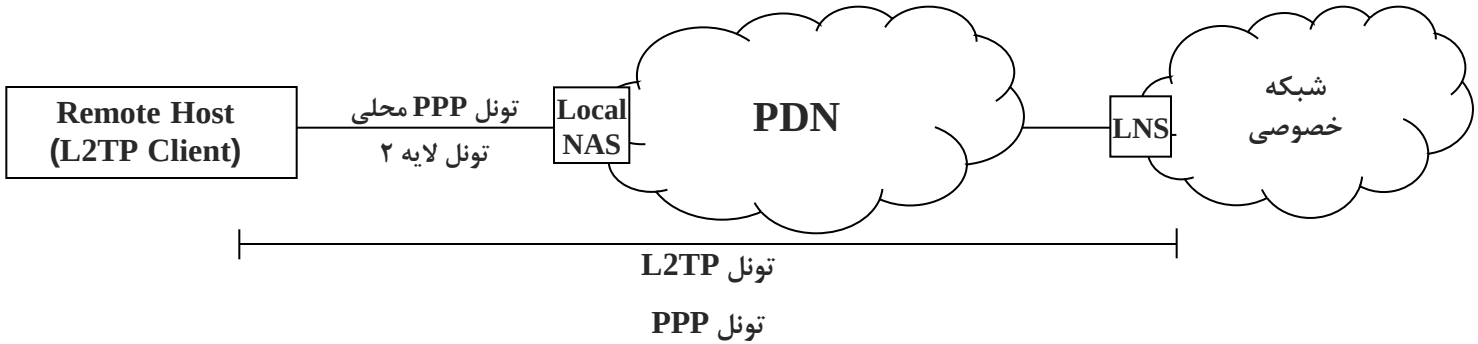
- پس از برقراری لینک، طرف مقابل (Authenticator) یک پیغام Challenge ارسال می کند .
- طرف Authenticating Peer در پاسخ مقداری را که با استفاده از یک one-way hash function محاسبه شده است، ارسال می کند. این مقدار وابسته به یک کلمه رمز مشترک (Secret) بین دو طرف است.
- در صورت درست بودن مقدار Response ،تصدیق اصالت صورت می پذیرد.
- در الگوریتم CHAP طول کلمه رمز حداقل باید یک بایت باشد ولی بهتر است حداقل برابر طول Hash تولید شده باشد (۱۶ بایت در صورتیکه از MD5) استفاده شود. بدین ترتیب می‌توان مقاومت در برابر Exhaustive Search Attack را افزایش داد.
- مقدار challenge ارسال شده باید غیر قابل پیش بینی بوده و تکراری نباشد .

RFC2661 Layer 2 Tunneling Protocol L2TP

یک روش **encapsulate** کردن برای ارسال بسته های انواع پروتکل های لایه ۳ بر روی خطوط نقطه – به نقطه لایه ۲ است.

در حالت **PPP** تونل لایه ۲ از طریق شبکه ای انتقال مانند شبکه تلفنی ایجاد می شود و انتهای تونل **PPP** همان انتهای تونل لایه ۲ یعنی **Network Access Server (NAS)** است.

L2TP امکان این را فراهم می آورد که تونل **PPP** بتواند بین **Remote Host** و یک سرور دور برقرار شود در حالیکه تونل **L2** در اولین **NAS** خاتمه می یابد.



Layer 2 Tunneling Protocol : RFC2661

ادامه

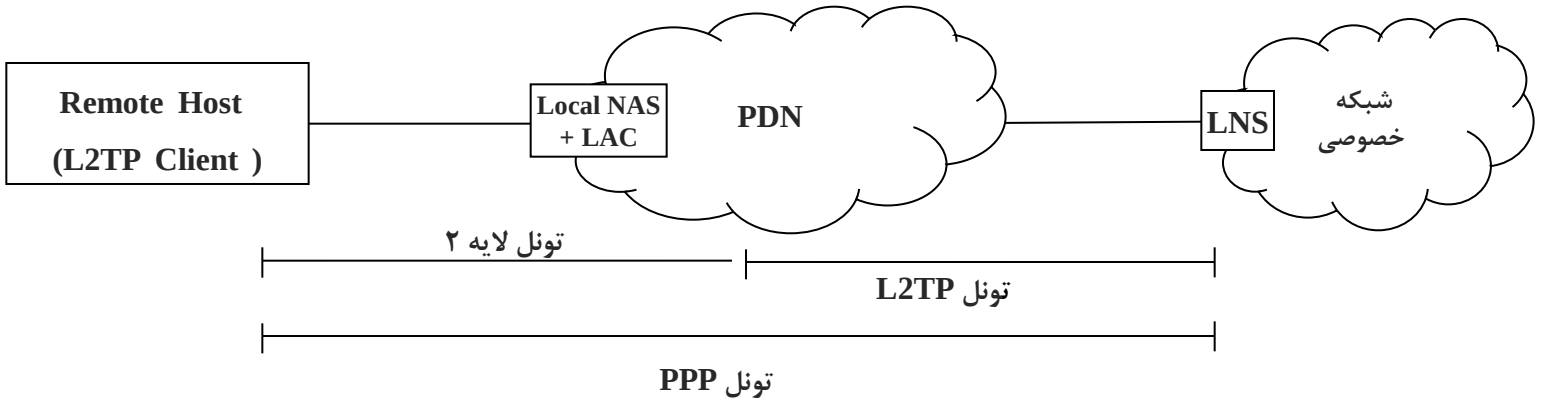
پردازش بسته های PPP در سرور راه دور (LNS) انجام می گیرد و نه در اولین سرور دسترسی(Local NAS). در حالت Multilink PPP نیز، هر لینک می تواند از طریق یک Local NAS برقرار شود و نیاز نیست که همه از طریق یک سرور برقرار شوند. کافی است همه لینک ها به سرور راه دور (LNS) منتهی شوند.

Control Connection

روش in-band سیگنالینگ برای ایجاد، حذف و نگهداری تونل (نشست) است.

تونل L2TP بین L2TP Access Controller (LAC) و یک L2TP Network Server (LNS) برقرار می شود و پیغامهای کنترلی بین آنها برای ایجاد حذف و نگهداری تونل تبادل می شود.

هر تونل L2TP می تواند چندین نشست را حمایت کند. هر نشست دارای یک کد مشخصه است. Remote Hostممکن است به عنوان LAC عمل نکند بلکه LAC با Local NAS هم محل باشند. در اینصورت Remote Host ارتباط PPP را با LAC برقرار می کند . LAC فریمهای PPP دریافتی را به LNS تونل می کند. آدرس شبکه به Remote Host از طرف LNS و از طریق NCP به PPP داده می شود. عمل Authentication، Authorization و حسابرسی توسط LNS انجام می‌گیرد.



Local NAS عمل تصدیق اصالت و... را انجام نمی دهد و طبق قرارداد این کار را به LNS می‌سپارد.

عملکرد پروتکل

عملکرد پروتکل: از دو فاز تشکیل شده است:

1. **ایجاد تونل و یک Control Connection و تعیین یک Tunnel ID برای آن.**
2. **ایجاد نشست (Session) بر اساس Call Requestهای دریافتی.**

تونل های PPP از درون نشست های L2TP ارسال می شوند.

امنیت در L2TP: در سطح تونل، در سطح بسته ها

پروتکل PPTP RFC 2637

این پروتکل امکان ارسال بسته های PPP از طریق شبکه IP را فراهم می کند بدون آنکه پروتکل PPP تغیری کرده باشد.

PAC: PPTP Access Concentrator

PNS: PPTP Network Server

برای ارسال بسته های کنترلی از TCP استفاده می کنند ولی برای داده از

GRE (Generic Routing Encapsulate) استفاده می شود که اطلاعات اضافی مانند کنترل ازدحام را حمل کند.

نشست : PPTP از نوع Connection- oriented است و برای هر کاربر که به PAC وصل می شود، حالت نگهداری می شود. هرگاه یک نشست PPP بخواهد بوجود آید، یک نشست PPTP ایجاد می شود.

عملکرد پروتکل :

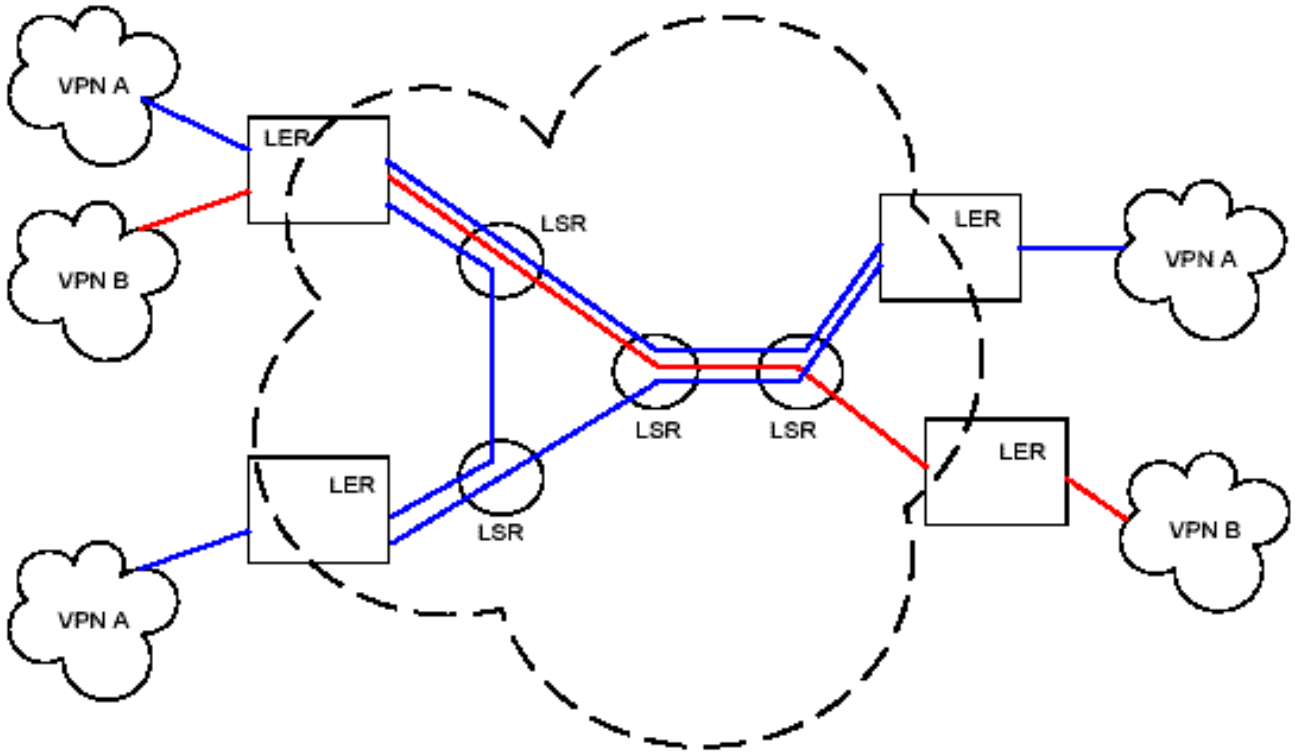
از دو فاز تشکیل شده است :

1. **یک Control Connection بین PAC و PNS که از TCP استفاده می کند.**
2. **یک تونل IP که از GRE برای Encapsulateکردن بسته های PPP استفاده می کند.**

فناوری های VPN مبتنی بر PE

MPLS VPNs

- غیر از VPDN که توسط L2TP ایجاد می شود، MPLS می تواند برای ایجاد VPN از نوع VLL ، VPLS و VPRN بکار رود.
- اینکار بر اساس تکنیک تونلهای LSP انجام می شود که در مورد VLL و VPLS بصورت دستی ایجاد می شوند و در مورد VPRN بصورت خودکار با استفاده از پروتکلهای مسیریابی انجام می شود.



MPLS VPN

- از نوع PE-Based هستند
- انواع مختلف لایه دو و لایه سه دارند
- Layer2 MPLS VPN
  - VPWS
  - VPLS
- Layer3 MPLS VPN
  - BGP/MPLS VPN
  - VR-Based VPN

مزایای MPLS VPN

- با یک زیرساخت واحد سرویس دهنده می‌تواند انواع سرویس MPLS L2VPN ، BGP/MPLS VPN و IP Routing را ارائه دهد
- می‌توان از پشته برچسب استفاده کرد و بنابراین روترهای P تنها اطلاعات یک برچسب را نگهداری می‌کنند و بنابراین توسعه‌پذیری بالایی دارد ولی در ATM و FR همه روترها باید اطلاعات همه برچسب‌ها را داشته باشند
- آدرس‌دهی لایه ۳ نداریم و بنابراین نباید نگران overlap آدرس‌های کاربران باشیم. این مساله در BGP/MPLS VPN وجود دارد