

# Advanced Network Security

## VPN Security

**Dr. Yaeghoobi**

PhD. Computer Science & Engineering, Networking, India  
[dr.yaeghoobi@gmail.com](mailto:dr.yaeghoobi@gmail.com)



**00** | **Introduction**

**01** | **How a VPN Protects You**

**02** | **VPN Protocols**

**03** | **VPN Log Handling**

**04** | **Killswitches & DNS Leaks**

**05** | **Types of VPNs for Companies**

**Introduction**

**00**



# VPN

- A virtual private network, or VPN, is an **encrypted connection** over the Internet from a device to a network.
- The encrypted connection helps **ensure that sensitive data is safely transmitted**.

- یک شبکه خصوصی مجازی یا VPN یک اتصال رمزگذاری شده اینترنتی از یک دستگاه به شبکه است.

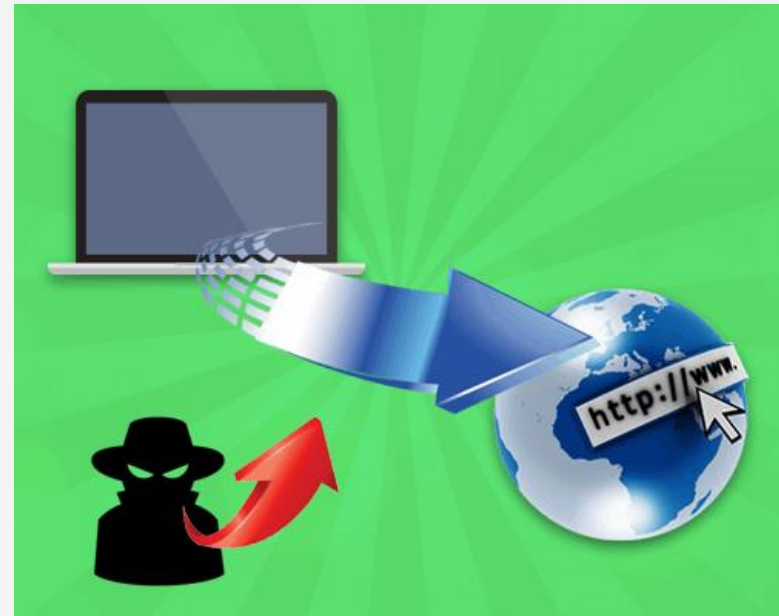
- اتصال رمزگذاری شده به اطمینان از انتقال ایمن داده های حساس کمک می کند.

# VPN ...

- It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.
- VPN technology is widely used in corporate environments.

این امر مانع از استراق سمع افراد غیرمجاز در ترافیک می شود و به کاربر امکان می دهد کار را از راه دور انجام دهد.

فناوری VPN به طور گسترده در محیط های شرکت مورد استفاده قرار می گیرد.



# Private/Public Network

- Your home network has a physical connection.
- If, for **example**, you have **three computers** that are all connected through a **network switch and not to the internet**, that would be known as a private network.
- **The internet**, on the other hand, is a **public network** where files can be transferred from one private machine to another.

- شبکه خانگی شما ارتباط فیزیکی دارد.
- به عنوان مثال ، اگر سه رایانه دارید که همه از طریق سوئیچ شبکه متصل هستند و به اینترنت متصل نیستند، این به عنوان یک شبکه خصوصی شناخته می شود.
- از طرف دیگر اینترنت یک شبکه عمومی است که می توان فایل ها را از یک ماشین خصوصی به دستگاه دیگر منتقل کرد.

# Private/Public Network and VPN

- A VPN restores that “private” moniker to your network, but for use with the internet.
- You’re creating a private network virtually, hence the name “virtual private network.”

- یک VPN این خصوصیات را به شبکه شما بازگرداند اما برای استفاده با اینترنت.

- شما در حال ایجاد یک شبکه خصوصی هستید ، از این رو نام آن "شبکه خصوصی مجازی" است.

**VPN is a network**, a connection between machines, it's virtual as there's no physical connection to the remote server and it's private through password protection and encryption.

VPN یک شبکه است، یک ارتباط بین دستگاه ها، بصورت مجازی، زیرا هیچ ارتباط فیزیکی با سرور از راه دور وجود ندارد و از طریق رمز عبور محافظت می شود و رمزگذاری آن خصوصی است.



# VPN Trick

- Originally, VPNs were **created as a way** for businesses to remotely access other machines.
- You'd essentially **trick the remote machine** into thinking it was on the same physical network.
- Now that VPNs have evolved for commercial use, they can be used for other purposes.

- در ابتدا، VPNها به عنوان راهی برای دسترسی به سایر ماشین ها از راه دور ایجاد شده اند.
- در اصل شما می توانید ماشین را از راه دور فریب دهید تا فکر کند در همان شبکه فیزیکی است.
- اکنون که VPNها برای استفاده تجاری تکامل یافته اند، می توانند برای مقاصد دیگر استفاده شوند.

# VPN/Proxy

- You can connect to a remote server which sends data out on your behalf, such as a proxy would.
- The difference between a VPN and proxy, though, is that **VPNs provide more security** with **encryption** and take randomizing measures at the remote server to make sure you're anonymous.
- ما می‌توانید به یک سرور از راه دور متصل شوید که داده‌ها را از طرف شما ارسال می‌کند، مانند یک پروکسی.
- تفاوت بین VPN و پروکسی در این است که VPNها امنیت بیشتری را با رمزگذاری فراهم می‌کنند و اقدامات تصادفی در سرور راه دور را انجام می‌دهند تا مطمئن شود ناشناس هستید.

# VPN works for a Company

- Because the traffic is encrypted between the device and the network, traffic remains private as it travels.
- An employee can work outside the office and still securely connect to the corporate network. Even smartphones and tablets can connect through a VPN.



- از آنجا که ترافیک بین دستگاه و شبکه رمزگذاری شده است، هنگام حرکت، ترافیک خصوصی باقی می ماند.
- یک کارمند می تواند در خارج از شرکت کار کند و هنوز هم با اطمینان به شبکه شرکت متصل شود. حتی تلفن های هوشمند و تبلت ها می توانند از طریق VPN متصل شوند.

# Commonly use of VPN

- Once your IP and location is hidden, you can safely browse the web.

پس از پنهان کردن IP و موقعیت مکانی، می توانید با خیال راحت وب را مرور کنید.

- VPNs are most commonly used today to reclaim online privacy and bypass nasty geo-blocks, a common distribution hurdle for TV shows, movies and streaming services that restricts access to a certain part of the world.

امروزه از VPN برای بازیابی حریم خصوصی آنلاین و دور زدن شرایط جغرافیایی ناخوشایند، یک مانع توزیع مشترک برای نمایش های تلویزیونی، فیلم ها و سرویس های پخش استفاده می شود که دسترسی به بخش خاصی از جهان را محدود می کند.

**How a VPN  
Protects  
You**

**01**



# Process of Connect to Website

- As you send that request, though, your **internet service provider (ISP)** takes a **log of what URL** you're trying to access and **your IP address**.
- In the event you're doing something that you shouldn't be, such as copyright piracy or other pursuits, the **ISP has a record of it**.



# PRISM

- Outside of trying to download a couple of movies, the fact that your **ISP can record all of your browsing data is a major privacy concern.**
- In the U.S., there are worries about those records being shared with the NSA as part of the PRISM project (surveillance\_program), and there are even more major concerns abroad.

- خارج از تلاش برای بارگیری چند فیلم، این واقعیت که ISP شما می تواند تمام داده های مرور شما را ضبط کند، یک نگرانی مهم در مورد حفظ حریم خصوصی است.
- در ایالات متحده آمریکا، نگرانی هایی در مورد به اشتراک گذاری سوابق با NSA به عنوان بخشی از پروژه PRISM (surveillance\_program) وجود دارد، و حتی نگرانی های مهم دیگری نیز در خارج از کشور وجود دارد.

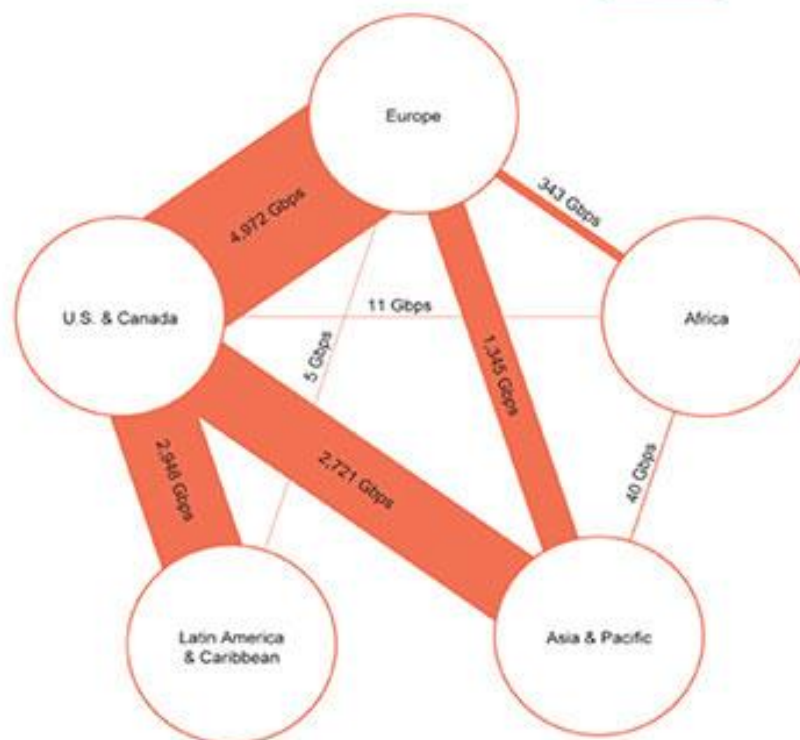


# (TS//SI//NF) Introduction

## U.S. as World's Telecommunications Backbone



- Much of the world's communications flow through the U.S.
- A target's phone call, e-mail or chat will take the **cheapest** path, **not the physically most direct** path – you can't always predict the path.
- Your target's communications could easily be flowing into and through the U.S.



International Internet Regional Bandwidth Capacity in 2011

Source: Telegeography Research

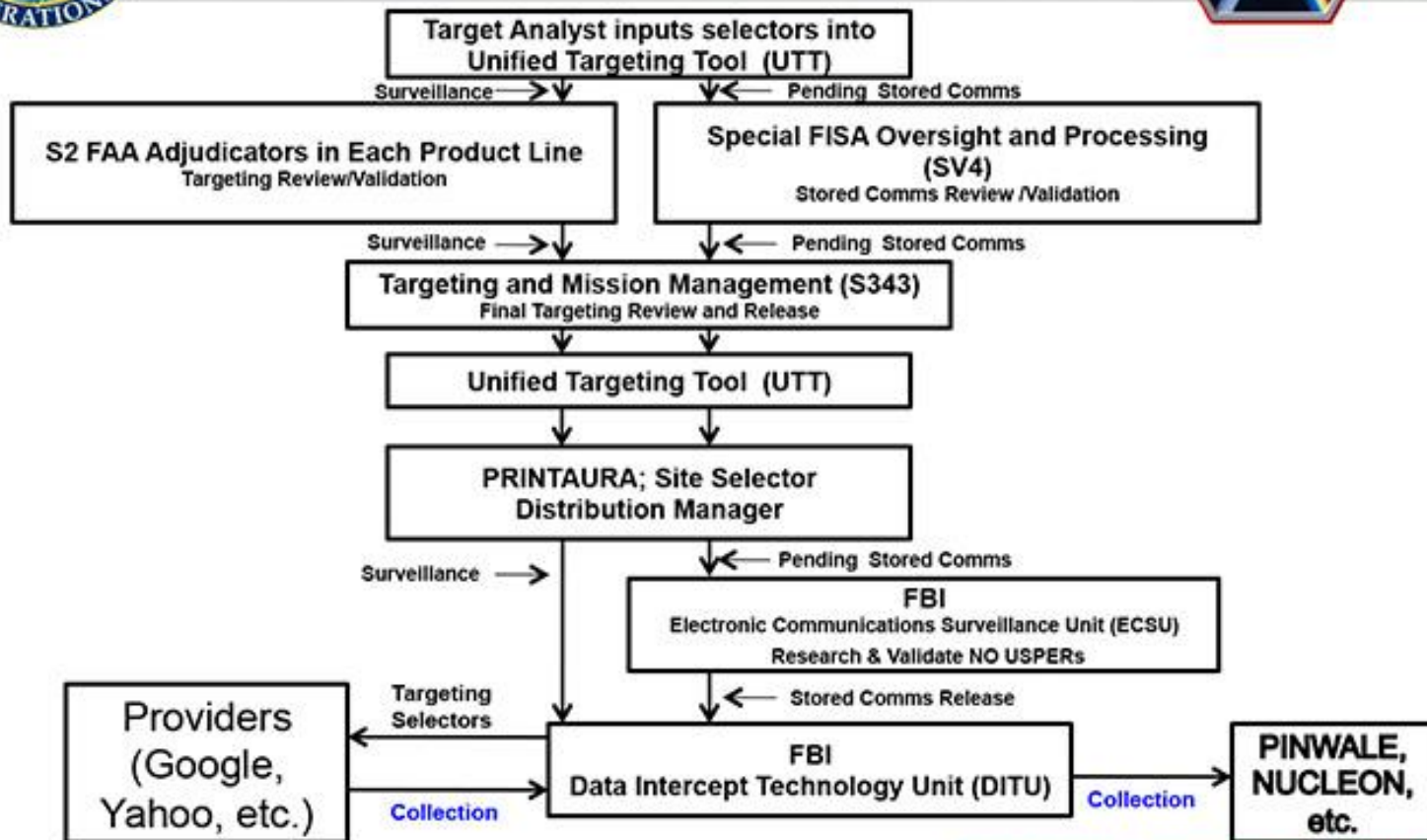




Hotmail

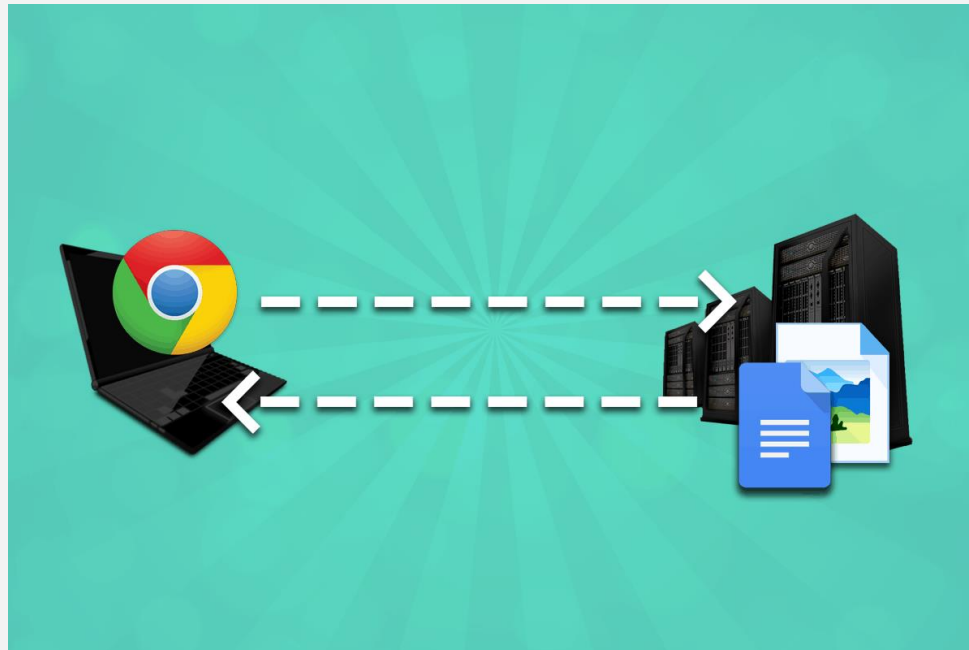


# (TS//SI//NF) PRISM Tasking Process



# Layers of Protection

- There are **two layers of protection** that a VPN uses to protect against this sort of snooping.
- Tunnelling
- Encryption



# *Tunnelling*

- Tunnelling, essentially, is a **virtual tunnel** that your **data travels through** so your ISP, or any other eyes, can't see it.
- All data running to and from your machine is sent in data packets. Packets include the **request** you're sending, the **protocol** and the sender's **IP address**.

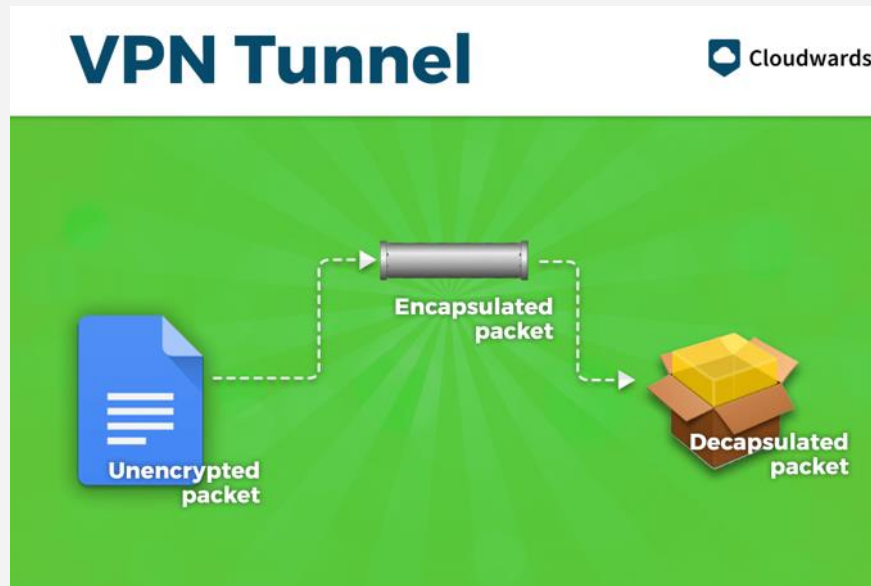
• تونلینگ، اساساً، یک تونل مجازی است که داده های شما از آن عبور می کنند، بنابراین ISP یا هر چشم دیگر قادر به دیدن آن نیستند.

• کلیه داده های در حال اجرا از طریق دستگاه شما در بسته های داده ارسال می شود. بسته ها شامل درخواستی که شما می فرستید، پروتکل و آدرس IP فرستنده است.

# *Tunnelling - Encapsulation*

- A **VPN puts a data packet inside of another data packet.** The process is known as encapsulation, and it's the first level of security a VPN uses to **keep you anonymous.**

• یک VPN بسته داده را درون یک بسته داده دیگر قرار می دهد. این فرایند به عنوان کپسوله سازی شناخته می شود، و این اولین سطح امنیتی است که VPN برای ناشناس ماندن شما از آن استفاده می کند.



# *Tunnelling ...*

- The VPN uses a **remote access server** which you connect to when using a VPN. Your computer will provide the **required credentials to log into this server**. The computer you're using has a **client software** that's used to establish this tunnelled connection. Once it's done, all browser activity will appear as if it's coming from the remote server and not your machine.

- VPN از سرور دسترسی از راه دور استفاده می کند که هنگام استفاده از VPN به آن متصل می شوید. رایانه شما اعتبار لازم را برای ورود به این سرور فراهم می کند. رایانه ای که شما از آن استفاده می کنید دارای یک نرم افزار مشتری است که برای برقراری این اتصال تونل استفاده می شود. پس از اتمام این کار، تمام فعالیت های مرورگر به نظر می رسد که از سرور راه دور و نه دستگاه شما برمی گردد.

# *Encryption*

- VPNs encrypt the data packets you send to the remote server to add an extra form of **security and anonymity**.
- Your data is **encrypted locally**.

• VPN بسته های داده ای را که برای سرور از راه دور می فرستید رمزگذاری می کنند تا یک شکل اضافی از امنیت و ناشناس بودن به آن اضافه شود.

• داده های شما بصورت محلی رمزگذاری می شوند.



## *Example*

- The best VPN providers, such as ExpressVPN use 256-bit AES encryption. It's the industry standard encryption method that's virtually impossible to crack. A 256-bit key can spit out  $1.1 \times 10^{77}$  possible combinations.

- بهترین ارائه دهندگان VPN مانند ExpressVPN از رمزگذاری AES 256 بیتی استفاده می کنند. این روش رمزگذاری استاندارد صنعتی است که شکستن آن تقریباً غیرممکن است. یک کلید ۲۵۶ بیتی می تواند ترکیبات احتمالی  $1.1 \times 10^{77}$  باشد.

# *Encryption ...*

- Only the data sent to the server is encrypted, though, as it has the proper decoder to make your data accessible.
- Once data is sent from the remote server to the website you're trying to access, it will not be encrypted as the receiving website doesn't have the key to decrypt that data.

- فقط داده هایی که به سرور ارسال می شوند رمزگذاری شده اند، سرور دارای رمزگشایی مناسب برای دستیابی به داده های شما دارد.

- هنگامی که داده ها از سرور راه دور به وب سایتی که می خواهید دسترسی داشته باشید ارسال می شود، رمزگذاری نمی شود زیرا وب سایت دریافت کننده کلید رمزگشایی آن داده ها را ندارد.



# Is VPN traffic encrypted?

- Yes, traffic on the virtual network is sent securely by establishing an encrypted connection across the Internet known as a tunnel.
- Offsite employees can then use the virtual network to access the corporate network.

• بله، ترافیک در شبکه مجازی با ایجاد اتصال رمزگذاری شده در اینترنت که به عنوان یک تونل شناخته می شود ترافیک رمزگذاری می شود.

• سپس کارمندان خارج از کشور می توانند از شبکه مجازی برای دسترسی به شبکه شرکت ها استفاده کنند.

# VPN Protocols

# 02

---

# VPN Protocols

- A key part of understanding VPN security is learning the **common protocols VPNs** use and **difference between** them.
- While an automatic VPN connection should keep you anonymous, some providers use a **more secure protocol** than others.

بخش اصلی درک امنیت VPN، یادگیری پروتکل های متداول استفاده شده در VPN ها و تفاوت بین آنها است.

در حالی که یک اتصال خودکار VPN باید شما را ناشناس نگه دارد، برخی از ارائه دهندگان از پروتکل امن تری نسبت به سایرین استفاده می کنند.



# *OpenVPN*

- OpenVPN is an open source VPN protocol that's known for **being quick and having excellent security**.
- It's **built on an SSL/TLS secure connection**, the same way your browser verifies a web site with an SSL certificate.

• OpenVPN پروتکل VPN منبع باز است که به سرعت و امنیت عالی معروف است.

• این سرویس بر روی یک اتصال ایمن SSL / TLS ساخته شده است، به همان روشی که مرورگر شما یک وب سایت را با گواهی SSL تأیید می کند.

# *OpenVPN ...*

- It's a go-to choice for **many VPN providers** because it can support nearly an operating system, has decent speeds out of the gate and supports top-notch encryption. ***It may not be the best protocol to use for every task, but it's rarely a bad one.***

- این گزینه برای بسیاری از ارائه دهندگان VPN انتخاب خوبی است زیرا می تواند از سیستم عامل پشتیبانی کند، سرعت مناسب و از رمزگذاری درجه یک پشتیبانی می کند. ممکن است بهترین پروتکل مورد استفاده برای هر کار نباشد، اما بندرت یک نسخه بد است.

# *OpenVPN ...*

- OpenVPN is a great protocol to use for **bypassing geo-blocks**.
- It's highly **configurable** and can **used on any port**, meaning you can get through most network restrictions and firewalls without a hitch.

• OpenVPN پروتکل عالی برای استفاده برای دور زدن بلوک های جغرافیایی است.

• بسیار قابل تنظیم است و می تواند در هر پورت مورد استفاده قرار گیرد ، بدین معنی که می توانید بدون هیچ مشکلی بیشتر محدودیت های شبکه و فایروال ها را دور بزنید.

# SSTP

- SSTP, or **Secure Socket Tunneling Protocol**, is owned by Microsoft and, thus, only **available for Windows**. Even so, it's one of the most secure VPN protocols available, sitting alongside OpenVPN.
- SSTP transfers data through an SSL channel, hence the name. It uses SSL over TCP port 443, so it's less likely to get blocked by a firewall, as well.
- SSTP یا پروتکل Tunneling Secure Socket، متعلق به **مایکروسافت** است و بنابراین فقط برای ویندوز در دسترس است. با این وجود، یکی از امن ترین پروتکل های VPN موجود است که در کنار OpenVPN قرار دارد.
- SSTP داده ها را از طریق کانال SSL انتقال می دهد. از SSL بر روی پورت TCP 443 استفاده می کند، بنابراین احتمال مسدود شدن توسط فایروال نیز کمتر است.

# PPTP

- The **Point-to-Point Tunnelling Protocol** is the oldest VPN protocol still in use. It's developed by Microsoft and, while there are some **major security vulnerabilities**, PPTP still has its place.
- **It's simple.** That makes it **very fast**, a huge advantage over other VPN protocols. It's an **ideal choice for high data transfer tasks**, such as streaming, and older machines with underpowered hardware.

• پروتکل تونلینگ Point-to-Point قدیمی ترین پروتکل VPN است که هنوز در حال استفاده است. توسط مایکروسافت توسعه یافته است و با وجود برخی آسیب پذیری های امنیتی مهم، PPTP هنوز جایگاه خود را دارد.

• ساده است. این امر باعث می شود خیلی سریع باشد، مزیت بزرگی نسبت به سایر پروتکل های VPN. این یک انتخاب ایده آل برای کارهای انتقال داده بالا، مانند پخش و ماشین های قدیمی تر با سخت افزار کم قدرت است.



# PPTP ...

- It usually uses the **MS-CHAP-v1 authentication protocol** which is **insecure**. It's been **cracked multiple times** since it was introduced. **PPTP is a fine choice for tasks where security is irrelevant, such as streaming Netflix .**
- The downside, at least when compared to OpenVPN, is that it's Windows-only and not open source. As long as you're a Microsoft user, there's no harm in trying it as you should have a similar level of protection as if you were using OpenVPN.

- معمولاً از پروتکل احراز هویت MS-CHAP-v1 استفاده می کند که ناامن است. از زمان معرفی ، چندین بار شکسته شده است. PPTP یک انتخاب خوب برای کارهایی است که امنیت مهم نیست، مانند پخش Netflix

- نکته منفی، حداقل در مقایسه با OpenVPN، فقط منبع ویندوز است و منبع باز نیست. تا زمانی که شما یک کاربر مایکروسافت باشید، هیچ ضرری در استفاده از آن ندارید ، زیرا باید از سطح محافظ مشابهی برخوردار باشید، گویی که از OpenVPN استفاده می کنید.

# *L2TP/IPsec*

- This “protocol” is actually **two protocols that are commonly used together**.
- L2TP, or Layer 2 Tunnelling Protocol, was introduced in 1999 as an upgrade L2F and PPTP. It provides weak encryption alone, so it’s often paired with IPsec for a more secure connection.

- این "پروتکل" در واقع دو پروتکل است که معمولاً با هم استفاده می‌شوند.
- پروتکل تونلینگ L2TP یا Layer 2 در سال ۱۹۹۹ به عنوان به روزرسانی شده L2F و PPTP معرفی شد. به تنهایی رمزنگاری ضعیف را فراهم می‌کند، بنابراین اغلب برای ارتباط امن تر با IPsec همراه می‌شود.

# *L2TP/Ipsec ...*

- IPsec is an **end-to-end security protocol that authenticates and encrypts** each packet of data individually.
- When used together, L2TP and IPsec is **much more secure** than PPTP while still have some of the **speed advantages**. It's still **slower than OpenVPN**, though.
- This protocol pair also has some **issues with firewalls** as it uses **UDP port 500**, a port that many firewalls are known to block.

• IPsec یک پروتکل امنیتی پایان به پایان است که هر بسته از داده را بصورت جداگانه تأیید و رمزگذاری می کند.

• L2TP و IPsec هنگام استفاده باهم، بسیار امن تر از PPTP هستند در حالی که هنوز برخی از مزایای سرعت را دارند. با این وجود هنوز کندتر از OpenVPN است.

• این جفت پروتکل همچنین در رابطه با فایروال ها نیز مشکلاتی دارند، استفاده از درگاه UDP 500 که بسیاری از فایروال ها آن را مسدود می کنند.

# IKEv2

- **Internet Key Exchange Version 2 isn't a VPN protocol**, but many VPN applications list it as one. It's a separate version of the L2TP/IPsec combo that has a **higher level of encryption** and, thus, is **more secure**.

- It supports up to **AES-256 encryption** and supports a **variety of operating systems**, including iOS.

- تبادل کلید اینترنتی نسخه ۲ پروتکل VPN نیست، اما بسیاری از برنامه های VPN آن را به عنوان یکی ذکر می کنند. این یک نسخه جداگانه از L2TP / IPsec است که از سطح رمزگذاری بالاتری برخوردار است و در نتیجه امنیت بیشتری دارد.

- این سیستم از رمزگذاری AES-256 پشتیبانی می کند و انواع سیستم عامل ها از جمله iOS را پشتیبانی می کند.

# *IKEv2 ...*

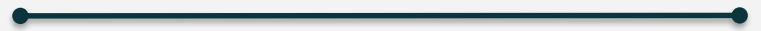
- It has a long track record of **secure and reliable connection**, reconnecting **very quickly** in the event you drop from the server.
- It's a close second to OpenVPN and you can use either if one is causing issues. It's faster and more secure than PPTP, building upon IPsec for a "protocol" that's close, but not as good, as OpenVPN.

- دارای سابقه طولانی در ارتباط امن و قابل اعتماد است، در صورتی که از سرور قطع شوید خیلی سریع وصل می شوید.

- پروتکلی نزدیک به OpenVPN است و اگر مشکل ایجاد کند می توانید از آن استفاده کنید. سریعتر و ایمن تر از PPTP است، و بنا بر IPsec ساخته شده است.

# VPN Log Handling

# 03



# Log Handling

- All of the effort a VPN provider goes through would be in vain **if there were still logs of your activity**. You're simply moving it from one company to another.
- Good VPN providers take steps to anonymize you at their remote servers and don't log any of your incoming activity.
- تمام تلاشهایی که ارائه دهنده VPN از طریق آن انجام می شود در صورت وجود گزارش های مربوط به فعالیت شما بیهوده خواهد بود. شما به سادگی آن را از یک شرکت به شرکت دیگر منتقل می کنید.
- ارائه دهندگان خوب VPN برای ناشناس کردن شما در سرورهای از راه دور خود اقداماتی انجام می دهند و هیچ یک از فعالیت های دریافتی خود را ثبت نمی کنند.

# Log Handling ...

- You'd think this would be common sense, but some VPN provider do, in fact, keep logs of your activity. **Hotspot Shield**, for example, states that it can **collect your IP address to identify your location and share that with government agencies in its privacy policy.**

- برخی از ارائه دهندگان VPN، در واقع گزارش های مربوط به فعالیت شما را حفظ می کنند. به عنوان مثال Hotspot Shield اظهار داشت که می تواند آدرس IP شما را برای شناسایی مکان شما جمع کند و آن را با آژانس های دولتی در سیاست حفظ حریم خصوصی خود به اشتراک بگذارد.



# **Killswitches & Leaks**

# **04**



# Killswitches & DNS Leaks

- There are two other important parts of VPN security that wouldn't fit neatly into any other sections:
  1. leaks and
  2. kill switches.

- دو بخش مهم دیگر از امنیت VPN وجود دارد که به راحتی در هر بخش دیگر قرار نمی گیرند:
- نشت و
- از بین بردن سوئیچ

# Killswitch

- A killswitch is a **security feature** that *allows you to cut your connection to the internet in the event you get disconnected from the remote server*. That way, you won't get caught
- A lot of VPN providers offer a killswitch, but some of the more mediocre options on the market do not. PIA, AirVPN, IPVanish and ExpressVPN are just a few of the many providers that offer a killswitch.

- killswitch یک ویژگی امنیتی است که به شما امکان می دهد در صورت قطع اتصال از سرور، اتصال خود را به اینترنت قطع کنید. به این ترتیب ، شما گرفتار نمی شوید.

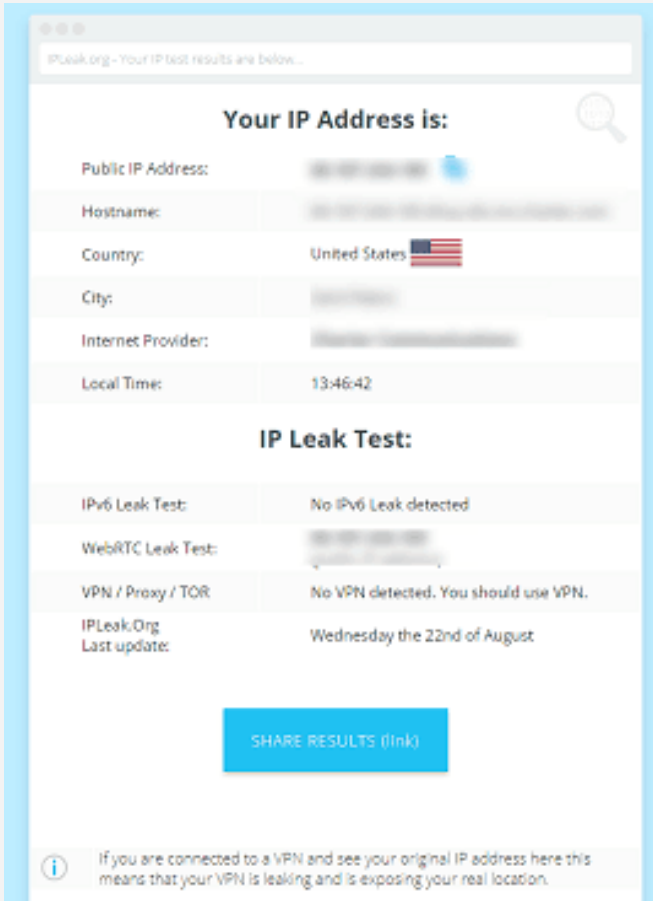
- بسیاری از ارائه دهندگان VPN یک killswitch را پیشنهاد می دهند، اما برخی از گزینه های متوسط تر در بازار این کار را نمی کنند. PIA ، AirVPN ، IPVanish و ExpressVPN تنها معدودی از ارائه دهندگان بسیاری هستند که یک killswitch را ارائه می دهند.

# Leaks


- Leaks are a serious problem when using a VPN.
- The two main leaks you'll encounter are **IP leaks and DNS leaks**.

• نشت هنگام استفاده از VPN یک مشکل جدی است.

• دو نشت اصلی که با آنها روبرو می شوید نشت IP و نشت DNS است.



The screenshot shows the IPLeak.org website interface. At the top, it says "Your IP Address is:". Below this, there is a table of information:

Public IP Address:	[Redacted]
Hostname:	[Redacted]
Country:	United States 
City:	[Redacted]
Internet Provider:	[Redacted]
Local Time:	13:46:42

Below the table, there is a section titled "IP Leak Test:" with the following results:

IPv6 Leak Test:	No IPv6 Leak detected
WebRTC Leak Test:	[Redacted]
VPN / Proxy / TOR:	No VPN detected. You should use VPN.
IPLeak.Org Last update:	Wednesday the 22nd of August

At the bottom, there is a blue button labeled "SHARE RESULTS (link)".

At the very bottom, there is a small information icon and a note: "If you are connected to a VPN and see your original IP address here this means that your VPN is leaking and is exposing your real location."

# IP Leaks

- **IP leaks are when you're connected to the VPN, but your IP address still points back to your location.**
- In most cases, IP leaks are the cause of a WebRTC bug. VPNs that work in browser extensions should disable WebRTC when you enable the extension, but you can go and disable it yourself using another extension.
- نشت IP هنگام اتصال به VPN زمانیکه آدرس IP شما هنوز به موقعیت مکانی شما بازمی‌گردد.
- در بیشتر موارد، نشت IP علت اشکال WebRTC است. VPN‌هایی که در پسوندهای مرورگر کار می‌کنند باید WebRTC را هنگام فعال کردن برنامه افزودنی غیرفعال کنند، اما می‌توانید با استفاده از یک برنامه افزودنی دیگر، آن را غیرفعال کنید.

# DNS Leaks

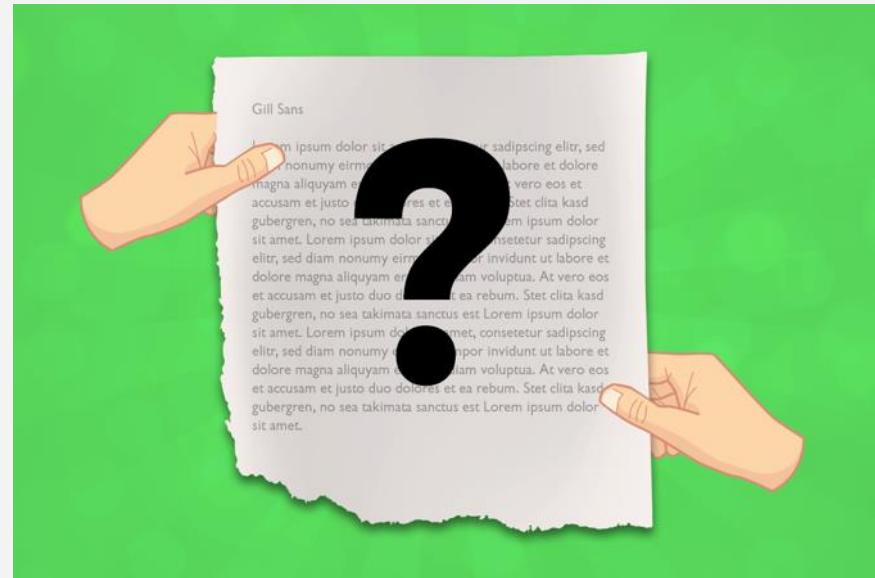
- **DNS leaks are when you connect to the VPN's DNS servers but your web browser sends the request directly to your ISP anyway.**
- DNS, the domain name system, is what allows IP addresses and domains to work. When you type a URL into your web browser, DNS translates your IP address and the server's IP address so the two can connect.
- نشت DNS هنگام اتصال به سرورهای DNS VPN اس ، اما مرورگر وب شما درخواست را مستقیماً به ISP شما ارسال می کند.
- DNS، سیستم نام دامنه، چیزی است که به آدرس ها و دامنه های IP اجازه کار می دهد. وقتی URL را در مرورگر وب خود وارد می کنید، DNS آدرس IP شما و آدرس IP سرور را ترجمه می کند تا این دو بتوانند به هم وصل شوند.

# Types of VPNs

05

---

- Types of VPNs :
  - Remote Access
  - Site-to-site





# What is secure remote access?

- It includes **VPN technology** that uses **strong ways to authenticate the user or device**.
- VPN technology is available to **check whether a device meets certain requirements**, also called a **device's posture**, before it is allowed to connect remotely.
- این شامل فناوری VPN است که از روشهای محکمی برای تأیید اعتبار کاربر یا دستگاه استفاده می کند.
- فناوری VPN برای بررسی اینکه آیا یک وسیله از الزامات خاصی برخوردار است، به آن حالت استقرار دستگاه نیز گفته می شود، قبل از اینکه اجازه برقراری ارتباط از راه دور را داشته باشد، موجود است.

# *Remote Access*

- A remote access VPN securely connects a device outside the corporate office. These devices are known as endpoints and may be laptops, tablets, or smartphones.
- Advances in VPN technology have allowed **security checks to be conducted on endpoints** to make sure they **meet a certain posture** before connecting.

- یک VPN با دسترسی از راه دور به طور ایمن دستگاهی را در خارج از دفتر شرکت ها متصل می کند. این دستگاه ها به عنوان نقاط پایانی شناخته می شوند و ممکن است لپ تاپ، تبلت یا تلفن هوشمند باشند.

- پیشرفت های فن آوری VPN باعث شده است که بررسی های امنیتی بر روی نقاط پایانی انجام شود تا اطمینان حاصل شود که آنها قبل از اتصال از وضعیت خاصی استفاده می کنند

# *Site-to-site*

- A site-to-site VPN connects the corporate office to branch offices over the Internet. Site-to-site VPNs are used when distance makes it impractical to have direct network connections between these offices.
- Dedicated equipment is used to establish and maintain a connection. Think of site-to-site access as network to network.
- یک VPN سایت به سایت، دفتر شرکت را به شعبات از طریق اینترنت متصل می کند. از VPN های سایت به سایت استفاده می شود که از راه دور، ارتباط مستقیم شبکه ای بین این دفاتر غیر عملی باشد.
- از تجهیزات اختصاصی برای برقراری و حفظ ارتباط استفاده می شود. به دسترسی به سایت به عنوان شبکه به شبکه فکر کنید.

# Security Policy

- What are the classes of users?
- What level of access is allowed to a class?
- Which devices are allowed to connect to the corporate network through a VPN?
- Which authentication method will be used and how will it be implemented?
- How will you counter sloppy practices?
- What are the Standard Operating Procedures (SOPs) in case of a network breach?
- What is the maximum idle VPN connection time allowed before automatic termination?

# VPN in the corporate world

1. Remote Access Server (RAS)
2. Internet Protocol Security (IPSec)
3. Secure Sockets Layer (SSL)



# RAS

- The **most basic form of VPN** remote access is through a RAS.
- The **client-side software is responsible for establishing a tunnelling connection to the RAS and for the encryption of data.**
- RAS VPNs are appropriate **for small companies**, requiring a remote access for a few employees. However, most serious businesses have moved on from this basic form of VPN connection.

• ابتدایی ترین شکل دسترسی از راه دور VPN از طریق RAS است.

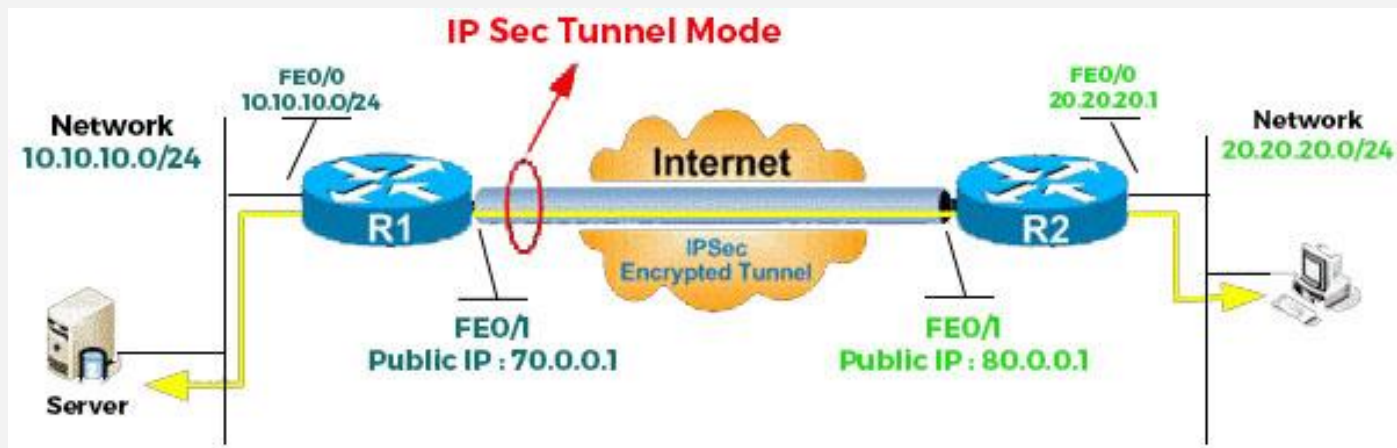
• نرم افزار سمت مشتری وظیفه ایجاد اتصال تونلینگ به RAS و رمزگذاری داده ها را بر عهده دارد.

• RAS VPN برای شرکت های کوچک مناسب است و نیاز به دسترسی از راه دور برای چند کارمند دارد. با این حال ، جدی ترین مشاغل از این شکل اصلی اتصال VPN حرکت کرده اند.

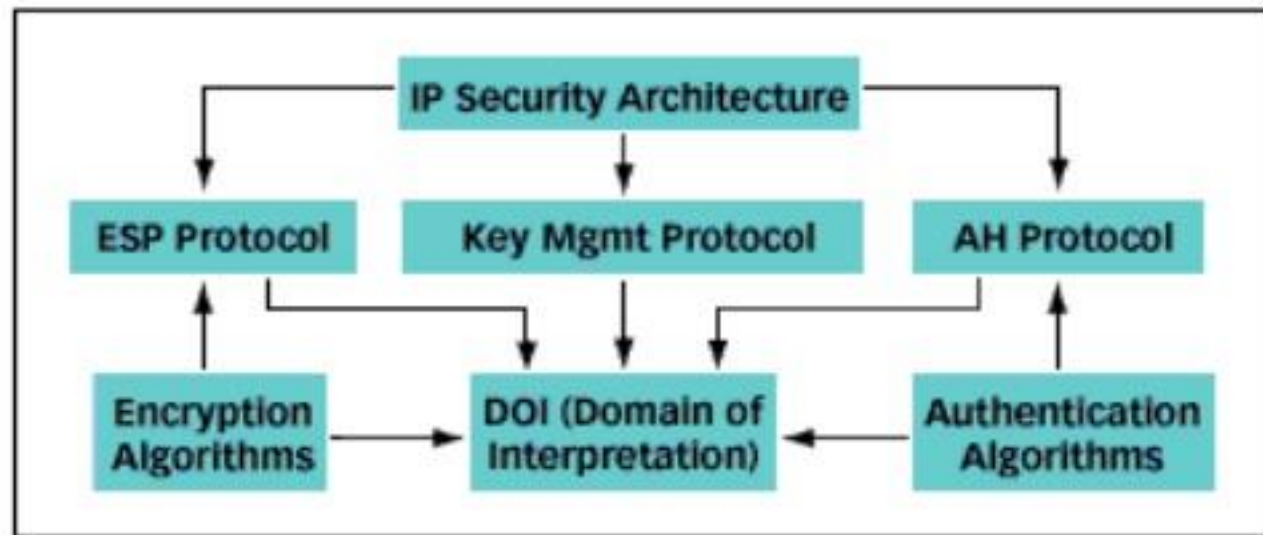
# IPSec

- A company should go for IPSec VPN remote access if it has a strong networking department with the ability to configure each employee's hardware device individually (installing client software, enforcing security policies etc.).

• برای یک شرکت با شبکه قوی و امکان پیکربندی دستگاه سخت افزاری هر کارمند بطور جداگانه (نصب نرم افزار مشتری، اجرای سیاست های امنیتی و غیره)، باید به دسترسی از راه دور IPSec VPN مراجعه کند.



# IPSEC ARCHITECTURE





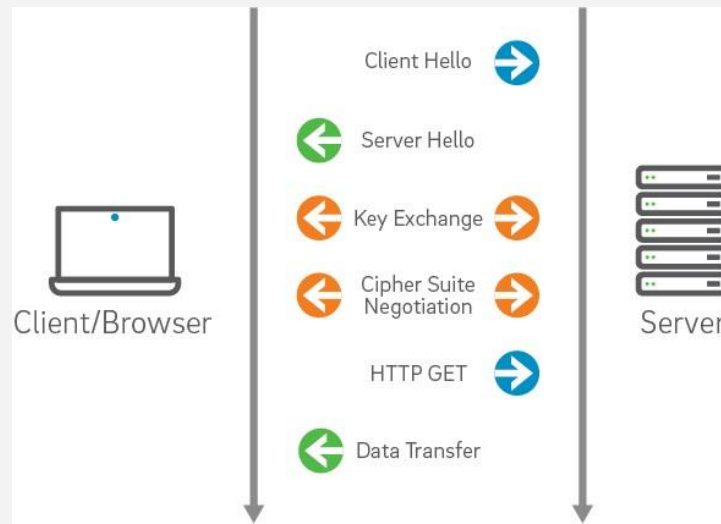
# Warning

- If you are using IPSec VPN for remote access, but you are not deploying Internet Key Exchange (IKE, certificates) as an authentication method, the connection will be vulnerable.
- For many use cases, XAUTH and L2TP methods of IPSec authentication are prone to security lapses.
- اگر از IPSec VPN برای دسترسی از راه دور استفاده می کنید، اما از Internet Key Exchange (IKE, certificates) به عنوان یک روش تأیید اعتبار استفاده نمی کنید، این اتصال آسیب پذیر خواهد بود.
- برای بسیاری از موارد استفاده، روشهای XAUTH و L2TP احراز هویت IPSec مستعد خطرات امنیتی هستند.

# SSL

- A lot of corporations worldwide have adopted SSL VPNs for their remote access needs. This method provides VPN access through any regular browser! It requires no special software to be installed on the employee's device.

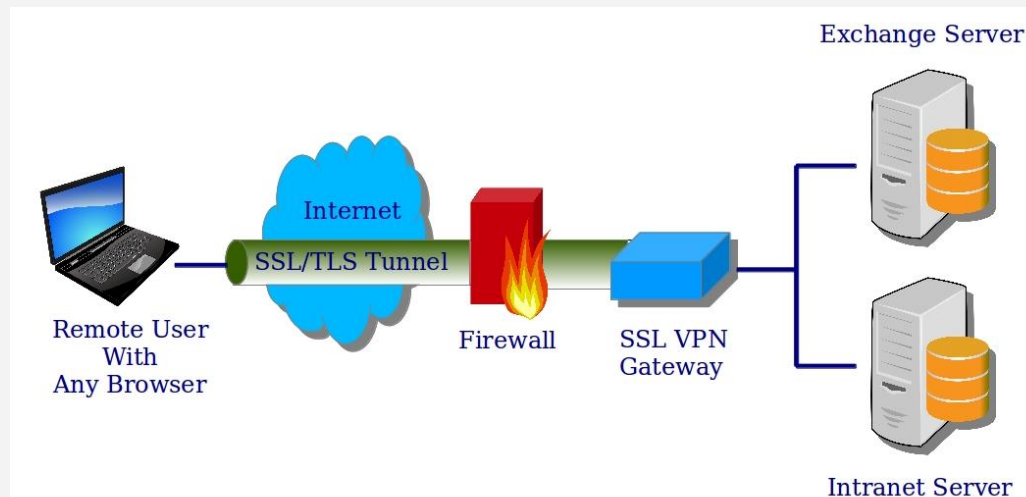
• بسیاری از شرکتها در سراسر جهان برای نیازهای دسترسی از راه دور خود SSL VPN را تصویب کرده اند. این روش دسترسی VPN را از طریق هر مرورگر معمولی فراهم می کند! نیازی به نصب نرم افزار خاصی در دستگاه کارمند نیست.



# SSL ...

- A Secure Sockets layer connection operates at the Transport Layer or Application Layer of the OSI Model of protocols. SSL VPN gateways are deployed behind the perimeter firewall, with rules which grant or deny access to specific applications.

• اتصال لایه Secure Sockets در لایه Transport یا Application Layer مدل OSI پروتکل ها کار می کند. گیتوی SSL VPN در پشت دیوار آتش محیطی مستقر می شوند، با قوانینی که دسترسی به برنامه های خاص را مجاز یا رد می کنند.



**Thanks for your Attention.**