CNCS

Centro Nacional
de Cibersegurança
PORTUGAL

CIBERCRIME

Uma apróximação técnica

Ivo Vacas

Olá!

Eu sou o Ivo Vacas

Departamento de Operações.
Podem contatar em:

- Ivo.vacas@cncs.gov.pt

6,000,000,000,000$

Danos provocados pelo cibercrime (2021)

Possibilidade de duplicar devido ao COVID-19

46,000,000,000

Dispositivos ligados à Internet (2021)

fonte: CSOonline.com

prnewswire.com

300%

Crescimento de ataques phishing(2020)

CENTRO NACIONAL DE CIBERSEGURANÇA

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS)

- Estabelecido em 2014, é a Autoridade Nacional de Cibersegurança
- Treino, sensibilização e criação de capacidades
- Normas e regulação
- Cooperação nacional e internacional
- CERT.PT é o CSIRT Nacional
  - Coordenação da Resposta a Incidentes
  - Coordenação da Gestão de Vulnerabilidades
  - Alertas

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

CENTRO NACIONAL DE CIBERSEGURANÇA

CERT.PT
Centro Nacional
de Cibersegurança
PORTUGAL

MISSÃO

”(…) implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.”

Decree-Law Nº 3/2012 (16th Jan)

CERT.PT


ENTIDADES DO ESTADO
OPERADORES DE INFRAESTRUTURAS CRÍTICAS
CIBERESPAÇO NACIONAL

CERT.PT

- Coordenação da Resposta a Incidentes
- Análise Forense
- Gestão de Vulnerabilidades
- Cooperação (Inter)Nacional
- Capacitação de CSIRT

CSIRTs NETWORK

Rede Nacional CSIRT

POLICIA JUDICIÁRIA

ACCREDITED BY TI TRUSTED INTRODUCER

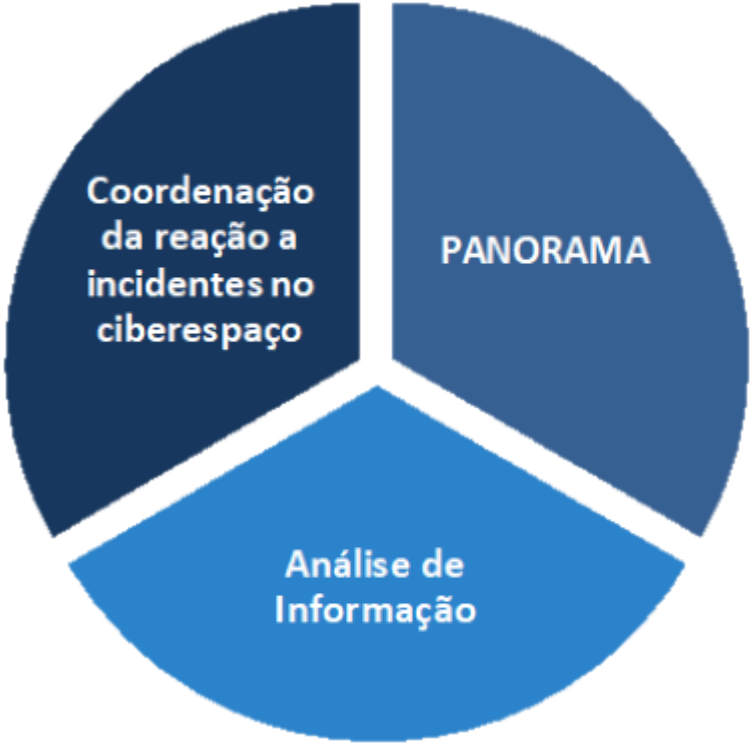
FIRST Improving Security Together

CERT.PT

- Troca de informação através de canais previligiados
- Grupos de trabalho
- Briefings
- Cooperação em casos (Inter)Nacionais

CERT.PT
Centro Nacional
de Cibersegurança
PORTUGAL

CERT.PT

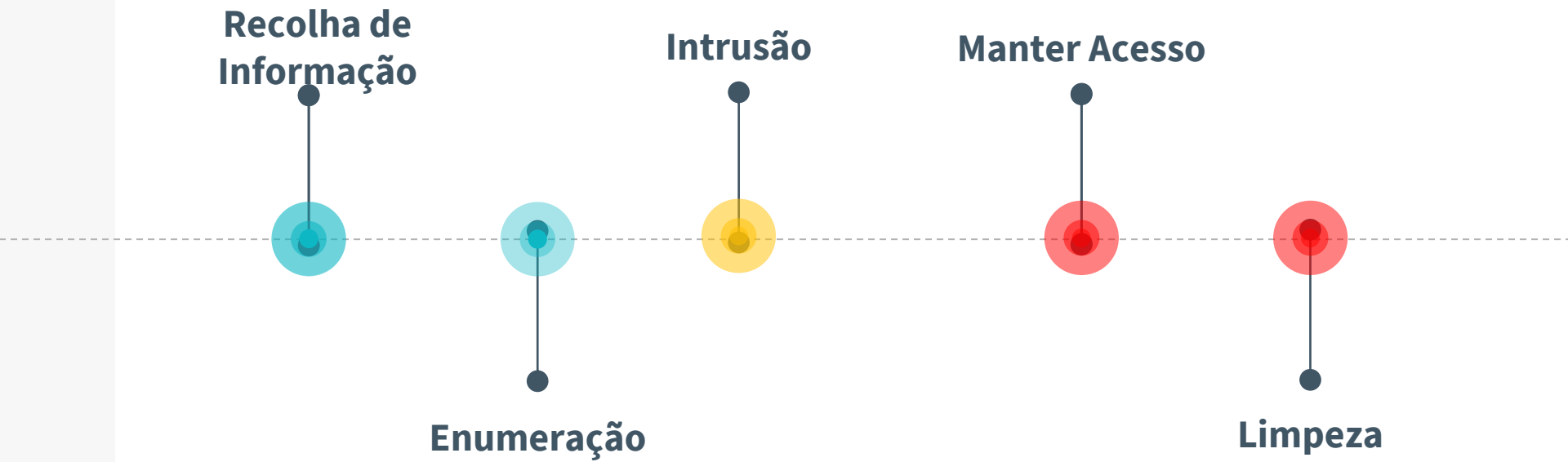


CERT.PT
Centro Nacional de Cibersegurança PORTUGAL

FASES DE UM ATAQUE

«Na guerra, o mais importante é atacar a estratégia do inimigo» – Sun Tzu

FASES DE UM ATAQUE



RECOLHA DE INFORMAÇÃO

«Se eu tivesse 8 horas para cortar uma árvore, gastava seis a afiar o meu machado» - Abraham Lincoln

- Conhecer a organização
- Conhecer colaboradores da organização
- Conhecer sistemas disponíveis publicamente

GOOGLE DORKS

site:www.cncs.gov.pt

Web | Imagens | Notícias | Mapas | Mais | Ferramentas de pesquisa

Cerca de 66 resultados (0,09 segundos)

Promoção Google

Experimente as Ferramentas do Google para Webmasters
www.google.com/webmasters/
É o proprietário de **www.cncs.gov.pt**? Receba da Google dados de indexação e de classificação de página.

CNCS | Centro Nacional de Cibersegurança
www.cncs.gov.pt/
Página inicial; SOBRE CNCS. Missão · Estrutura funcional · Contatos. CERT.PT. Coordenação da resposta a incidentes · Notificação de Incidentes · Suporte on- …

Sensibilização | CNCS
www.cncs.gov.pt/sensibilizacao/
O CNCS promove eventos no âmbito das iniciativas de divulgação, sensibilização e discussão aberta das temáticas relacionadas com a segurança e cidadania …

Sensibilização | CNCS
www.cncs.gov.pt/sensibilizacao2/
O CNCS promove eventos no âmbito das iniciativas de divulgação, sensibilização e discussão aberta das temáticas relacionadas com a segurança e cidadania …

GOOGLE DORKS

intitle:"webcam 7" inurl:'/gallery.html'

Tudo | Imagens | Mapas | Vídeos | Notícias | Mais | Definições | Ferramentas

4 resultados (0,25 segundos)

WHOIS

```
root@kali:~/tools/penteslab# whois google.pt
Nome de domínio / Domain Name: google.pt
Data de registo / Creation Date (dd/mm/yyyy): 09/01/2003
Data de expiração / Expiration Date (dd/mm/yyyy): 28/02/2018
Estado / Status: ACTIVE

Titular / Registrant
   Google, Inc.
   1600 Amphitheatre Parkway
   Mountain View
   94043 CA
   Email: ccops@markmonitor.com

Entidade Gestora / Billing Contact
   MarkMonitor Inc.
   Email: ccops@markmonitor.com

Responsável Técnico / Tech Contact
   MarkMonitor Inc.
   Email: ccops@markmonitor.com

Nameserver Information
   Nameserver: google.pt          NS      ns4.google.com.
   Nameserver: google.pt          NS      ns2.google.com.
   Nameserver: google.pt          NS      ns1.google.com.
   Nameserver: google.pt          NS      ns3.google.com.
```

ENUMERAÇÃO

Detetar possíveis vulnerabilidades dos sistemas:

- Portos abertos
- Serviços disponíveis
- Tecnologias usadas

NMAP

```
Nmap scan report for 192.168.56.102
Host is up (0.00028s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ET
RN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOS
A/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrPr
ovinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Not valid before: 2010-03-17T13:07:45+00:00
| Not valid after:  2010-04-16T13:07:45+00:00
| MD5:   dcd9 ad90 6c8f 2f73 74af 383b 2540 8828
|_SHA-1: ed09 3088 7066 03bf d5dc 2373 99b4 98da 2d4d 31c6
|_ssl-date: 2015-05-14T12:33:17+00:00; +1s from local time.
```

NIKTO

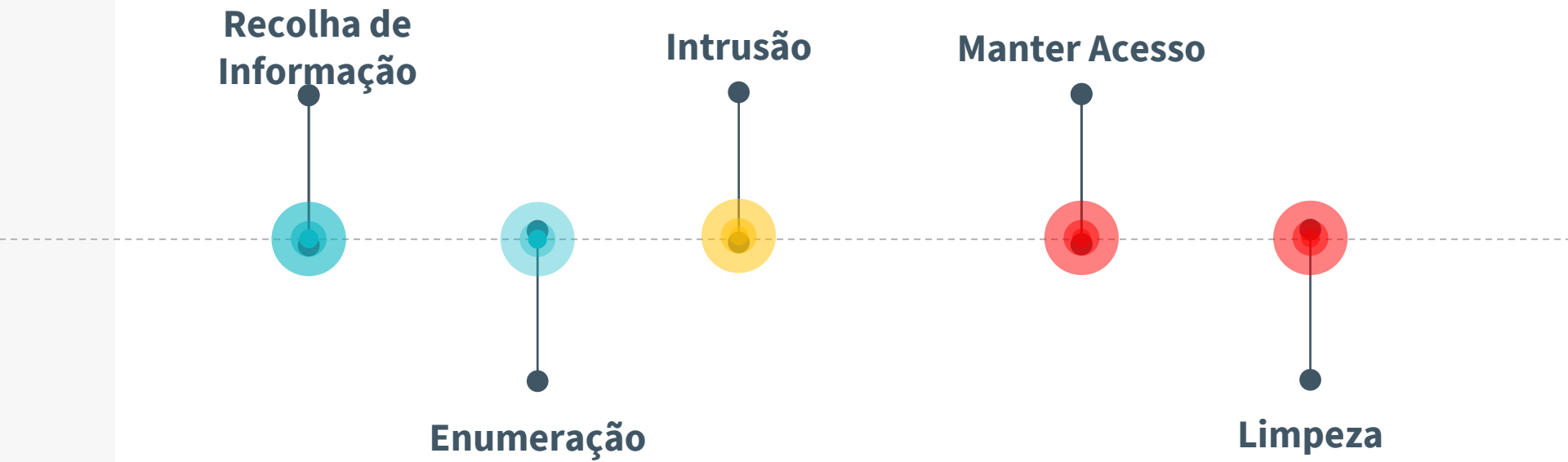
```
root@kali:~# nikto -h http://192.168.56.102
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2015-05-14 08:32:12 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.7). Apache
 2.0.65 (final release) and 2.2.26 are also current.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to e
asily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d1
5. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause fal
se positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potential
```

INTRUSÃO

Através da exploração da vulnerabilidades, garantir o acesso privilegiado (ou não).

- Metasploit
- Security-focus.com
- Exploit-DB
- SQLMap
- Burp
- Aircrack-ng

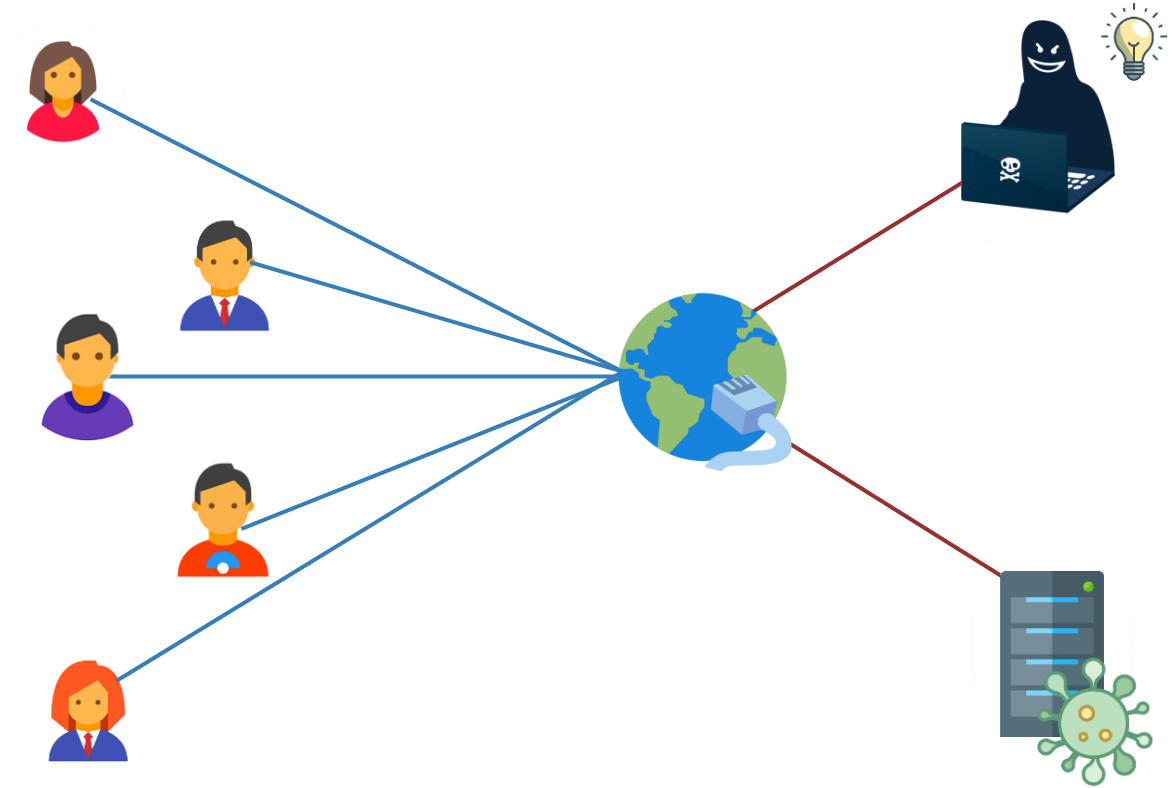
FASES DE UM ATAQUE



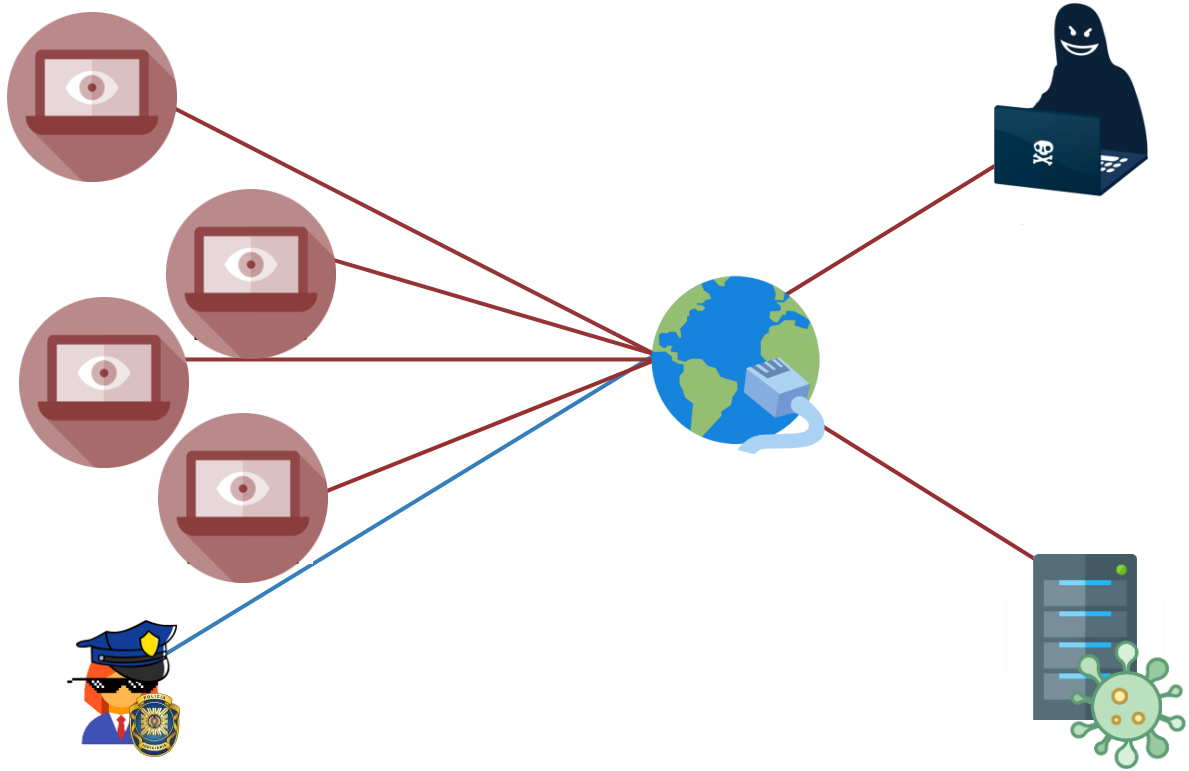
ANONIMIZAÇÃO

Now you see me! ……. now you don’t.

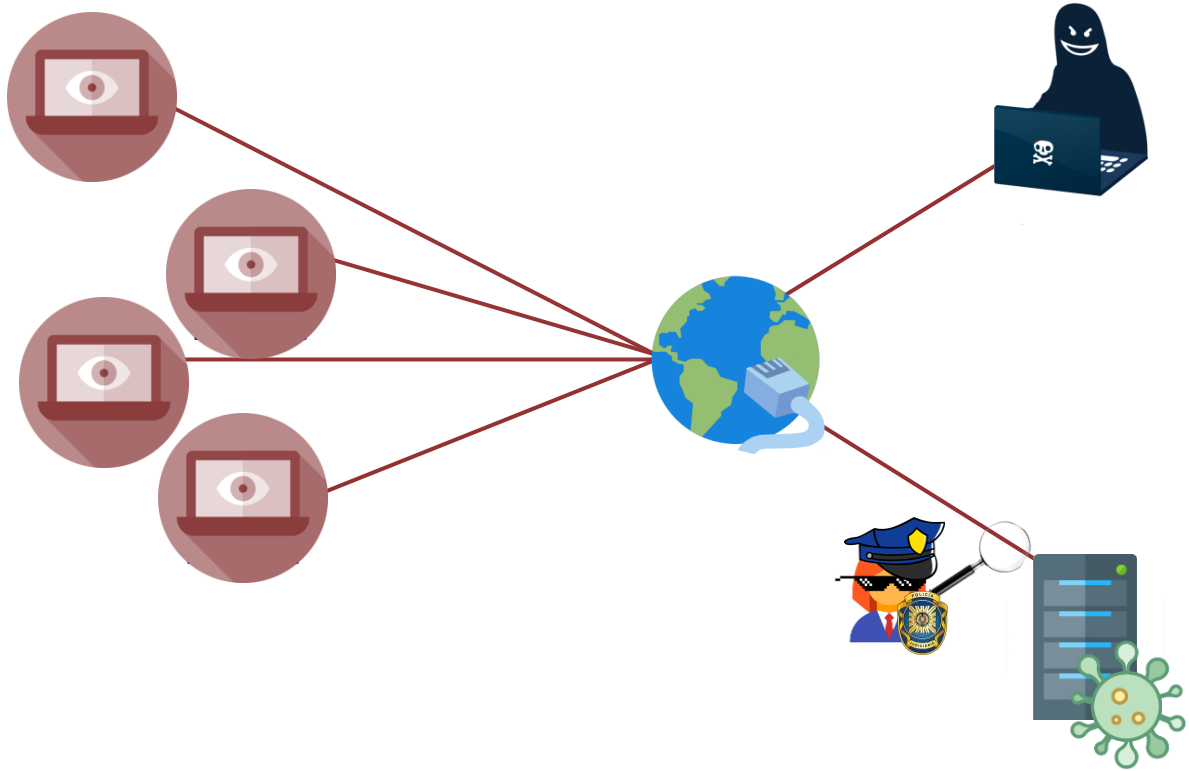
O DESAFIO DE UMA SITUAÇÃO REAL



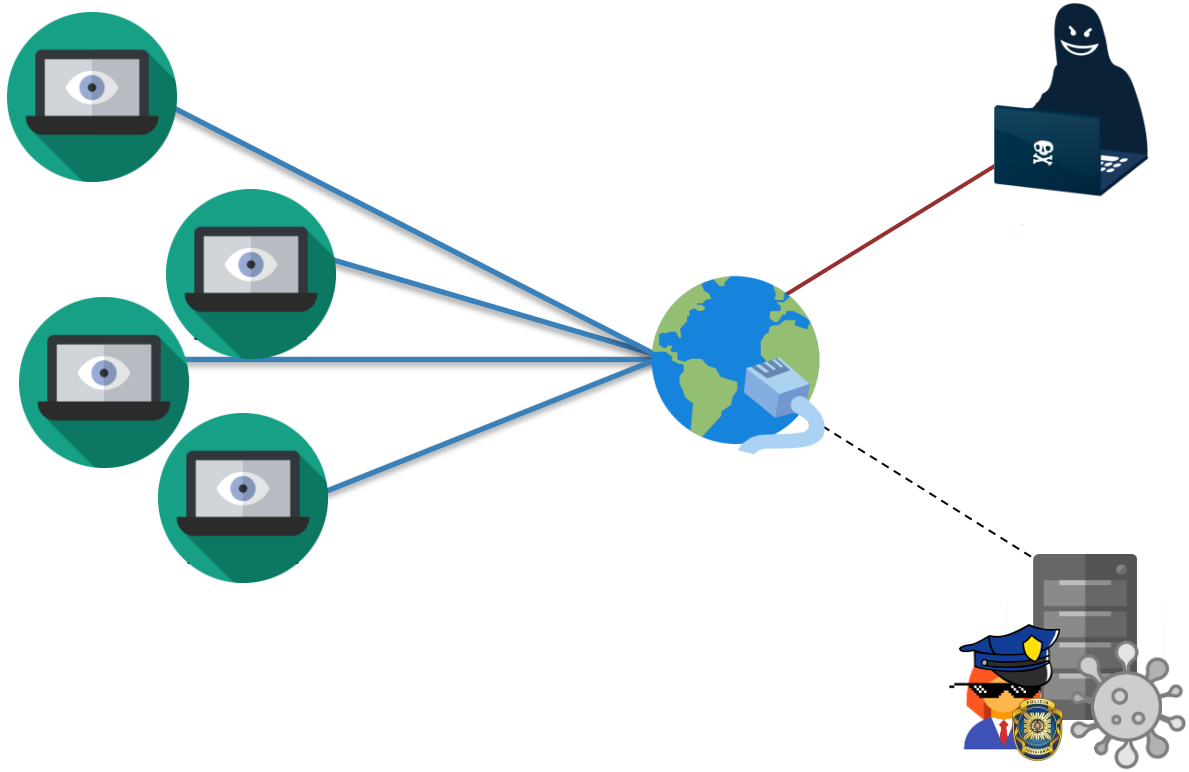
O DESAFIO DE UMA SITUAÇÃO REAL



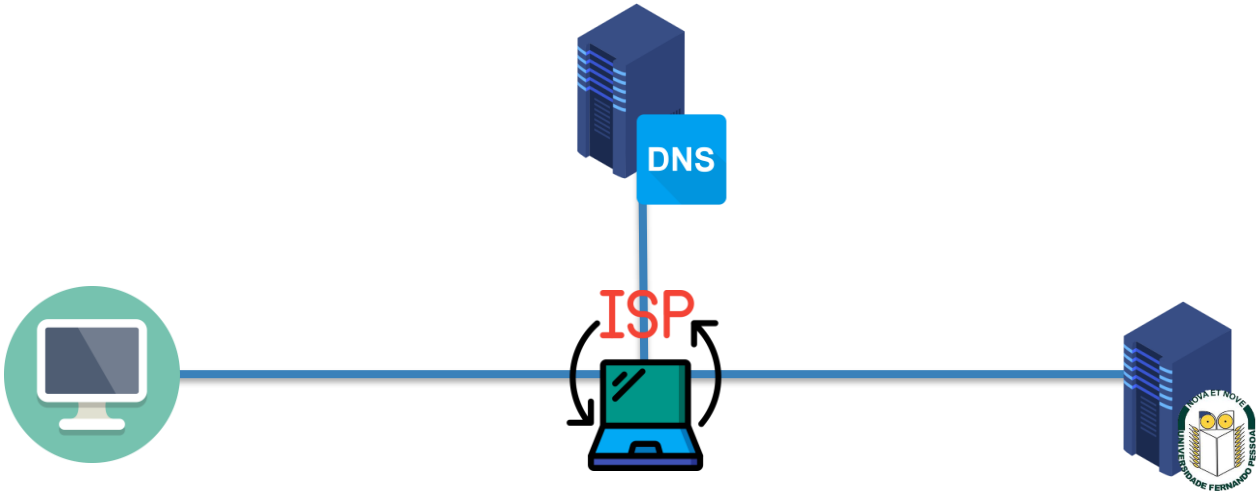
O DESAFIO DE UMA SITUAÇÃO REAL



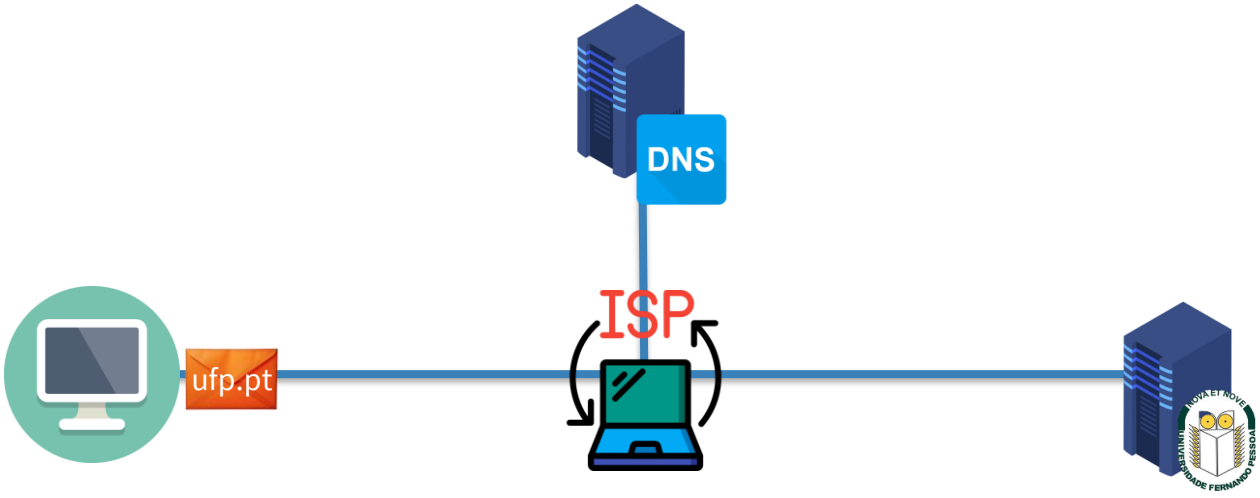
O DESAFIO DE UMA SITUAÇÃO REAL



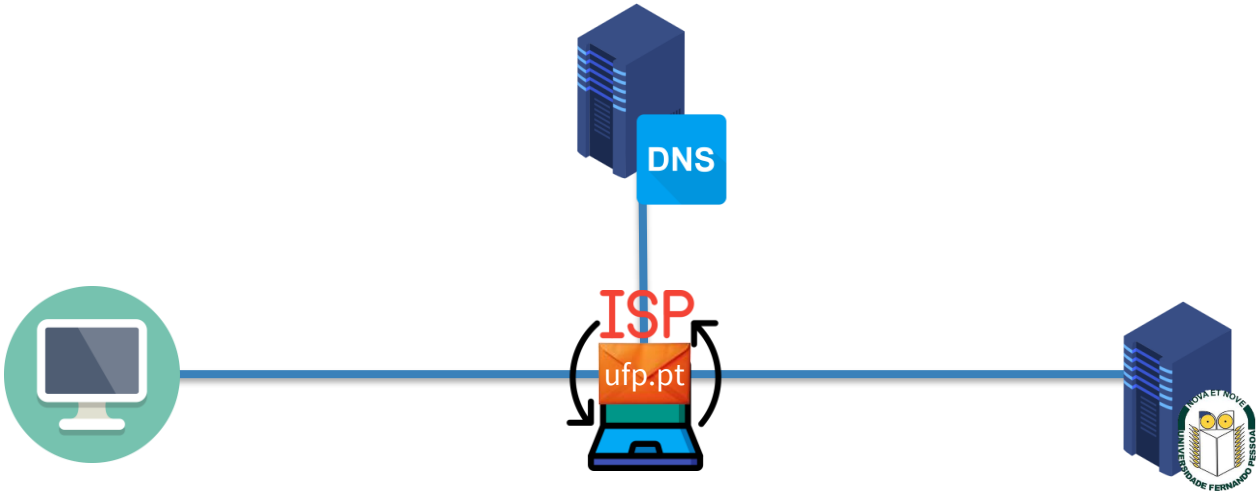
INTERNET COMUM



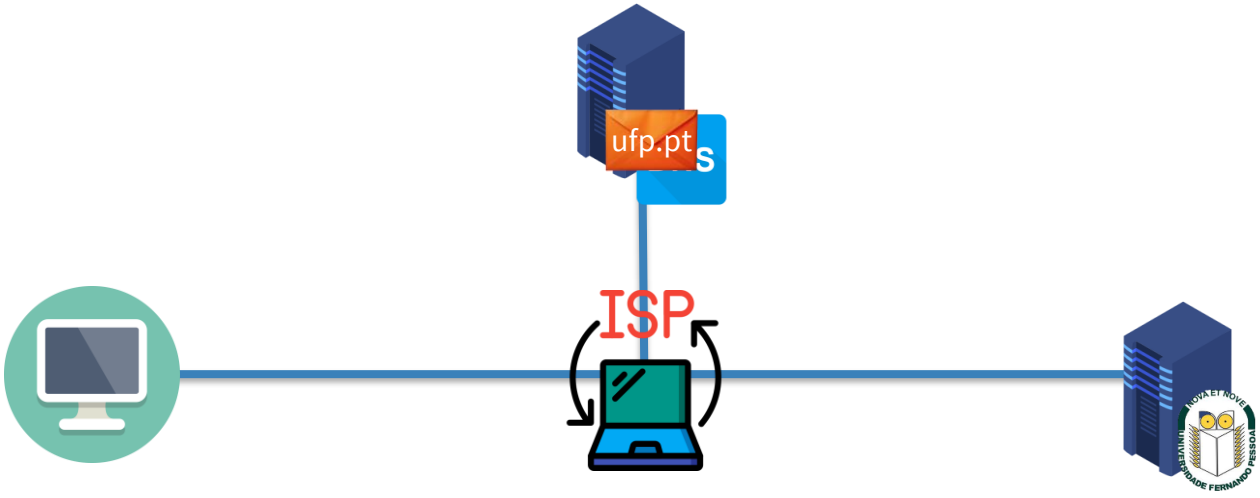
INTERNET COMUM



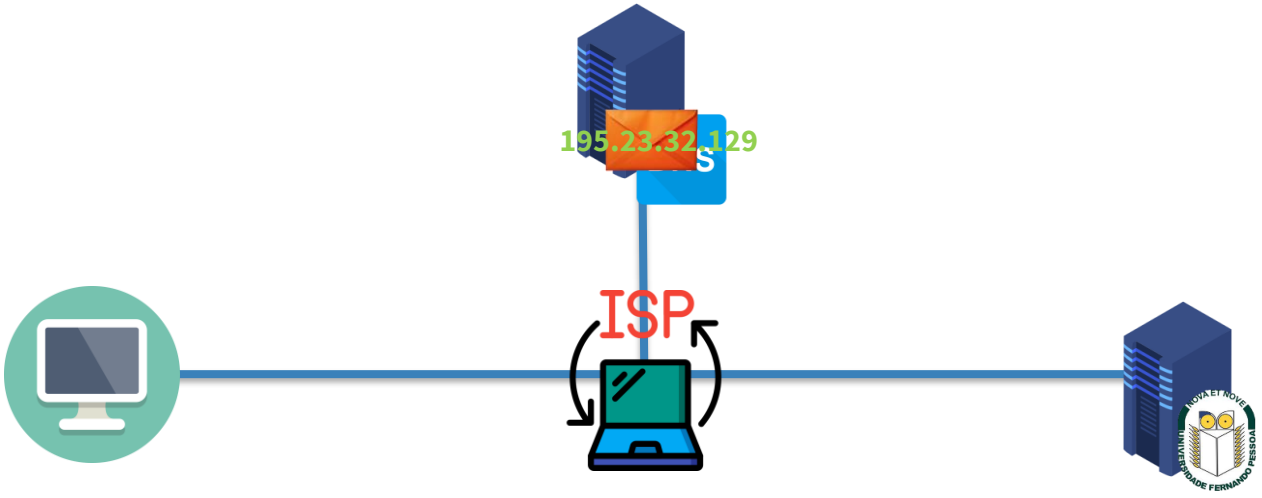
INTERNET COMUM



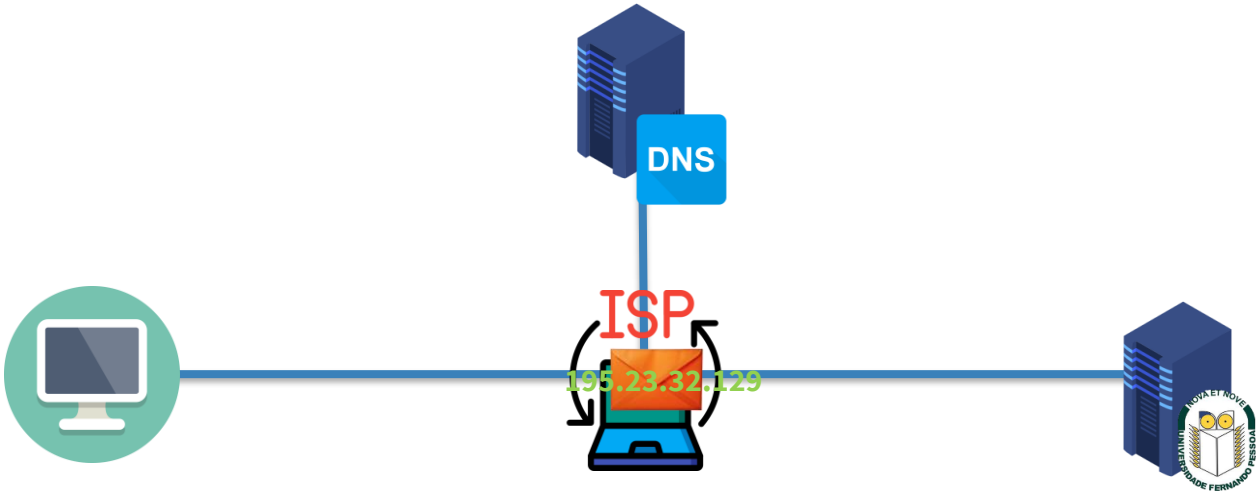
INTERNET COMUM



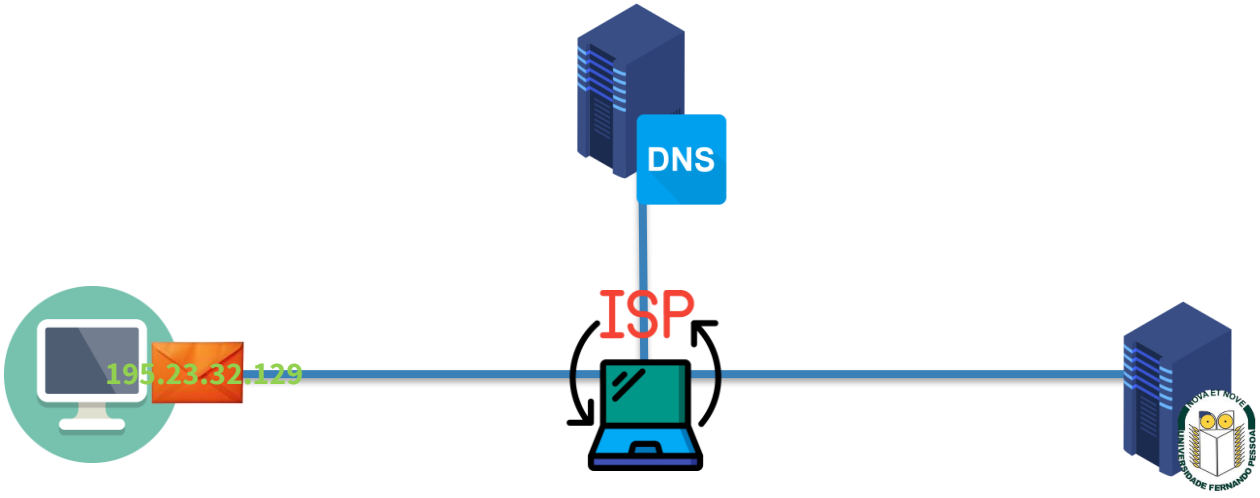
INTERNET COMUM



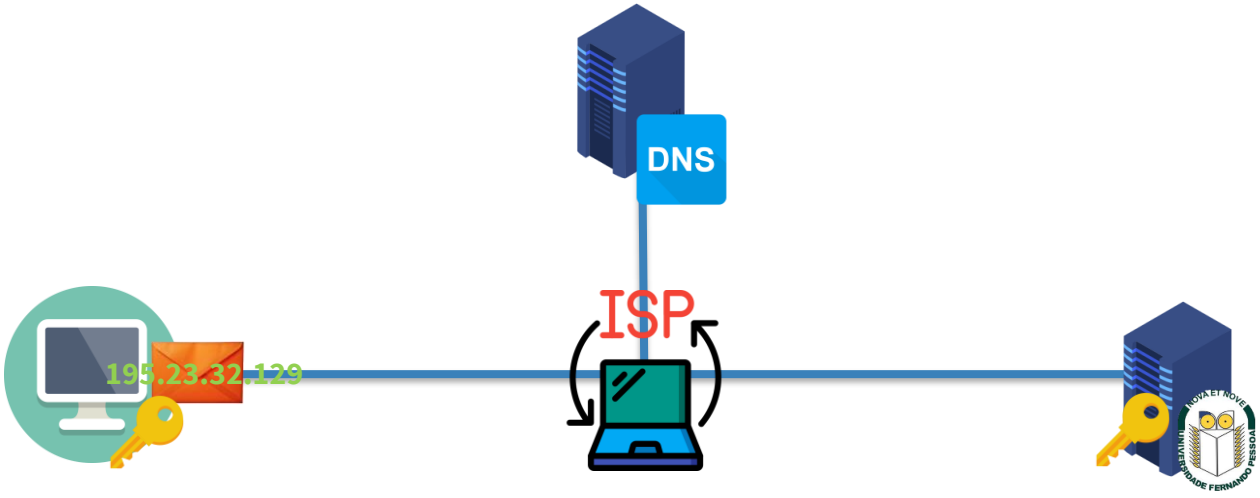
INTERNET COMUM



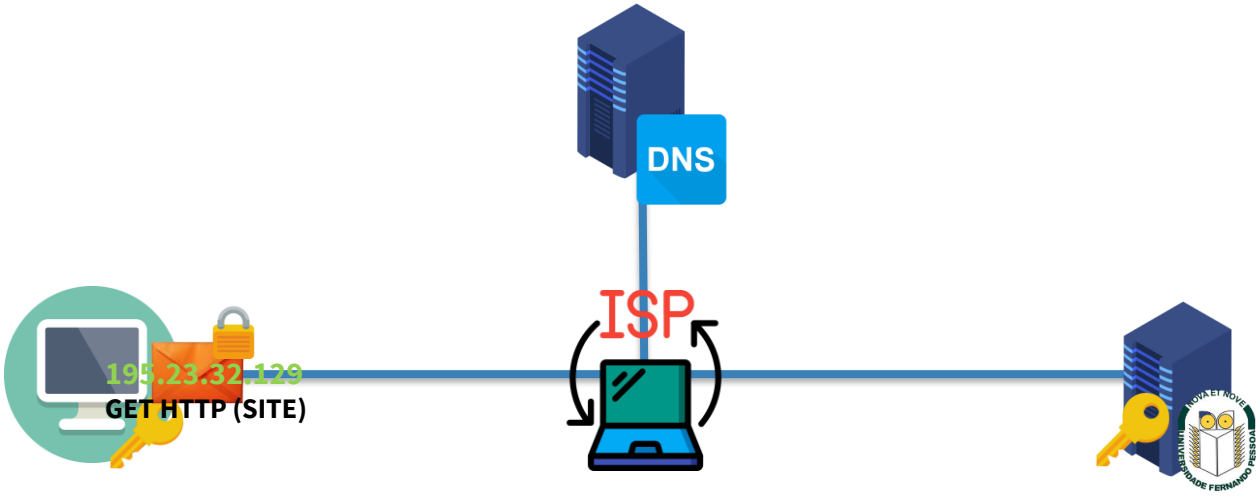
INTERNET COMUM



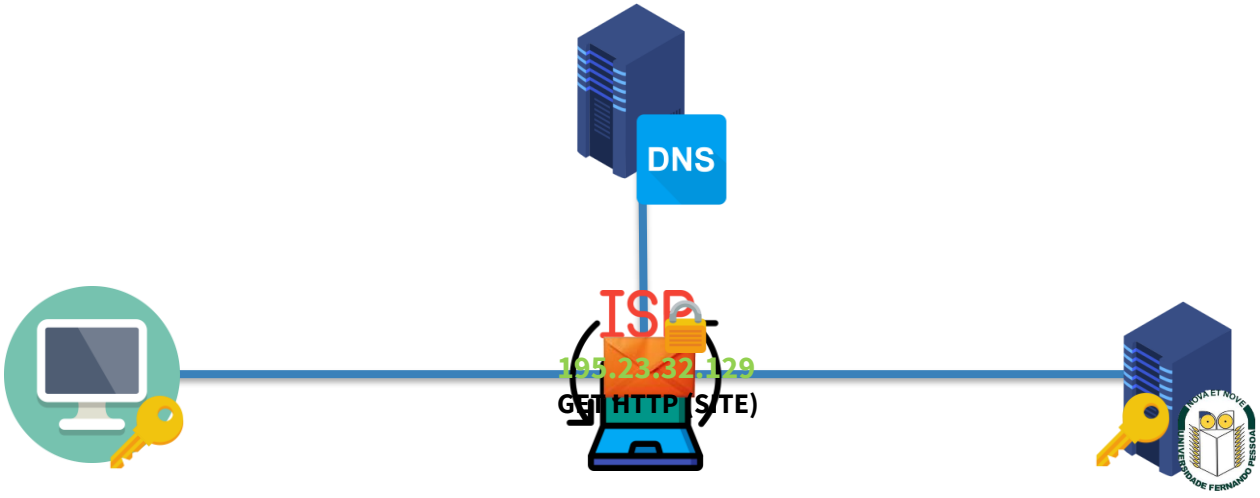
INTERNET COMUM



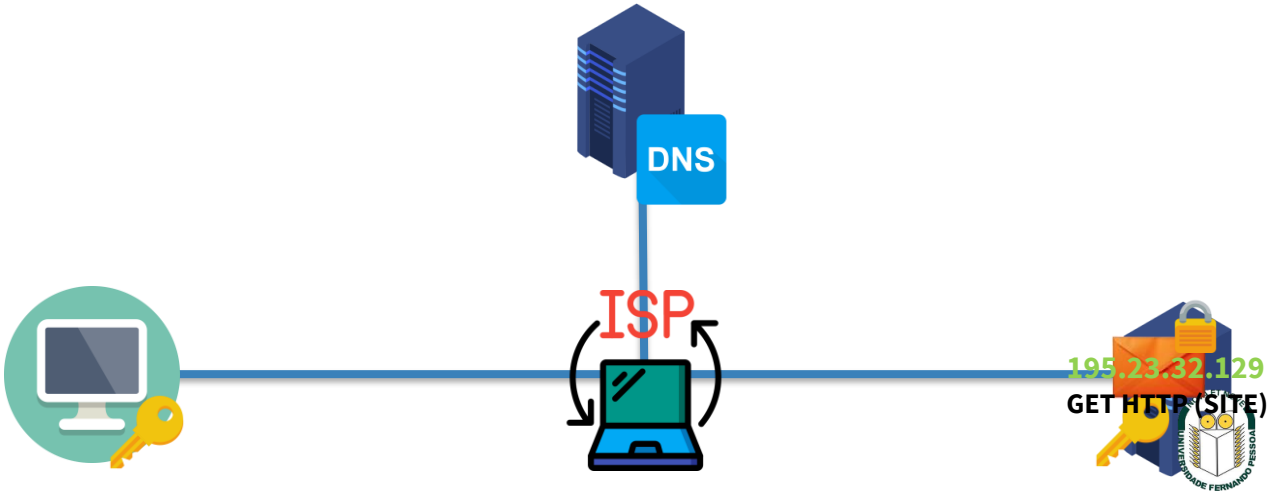
INTERNET COMUM



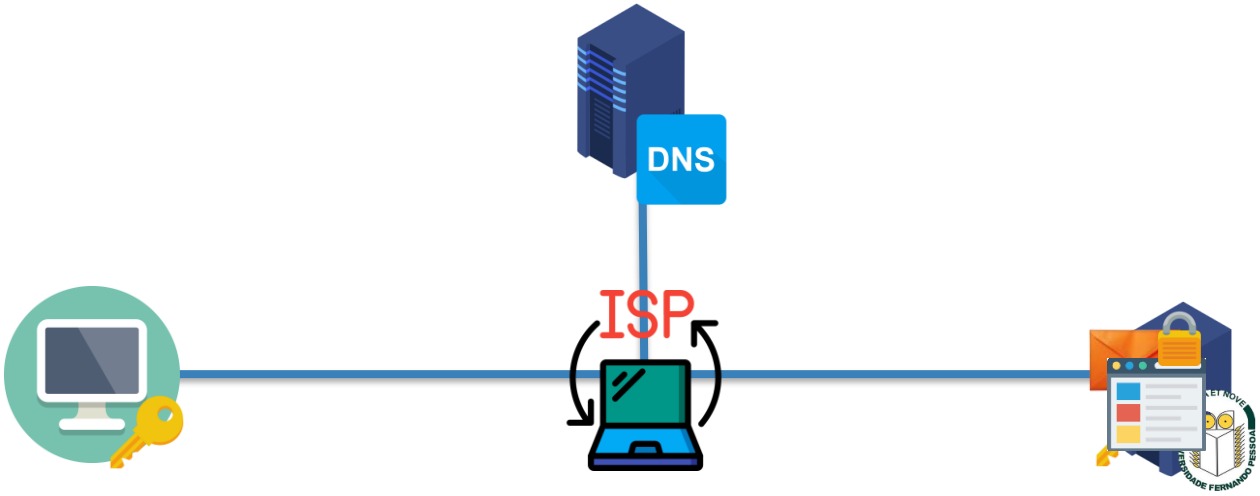
INTERNET COMUM



INTERNET COMUM

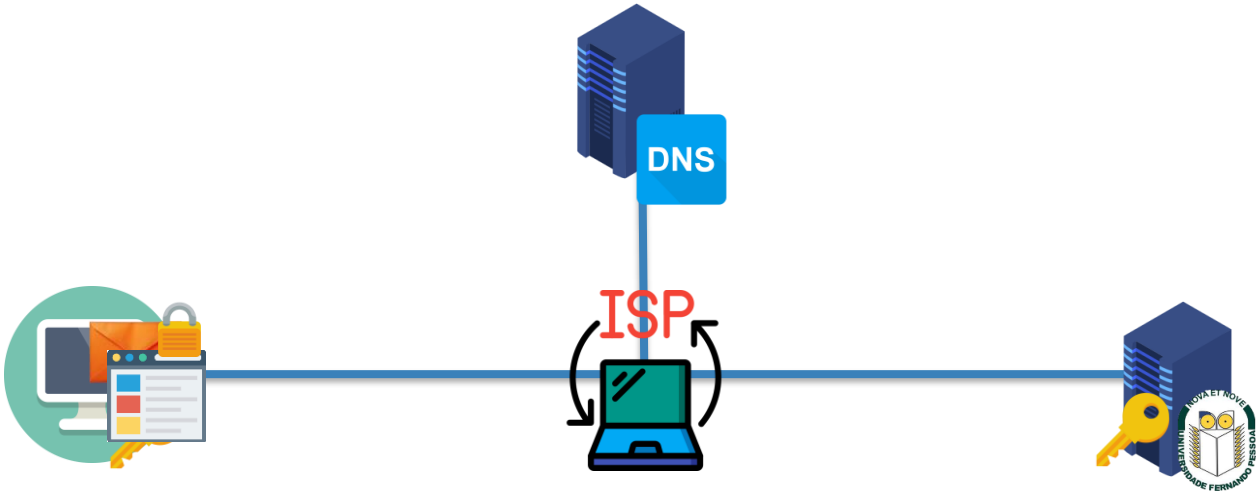


INTERNET COMUM

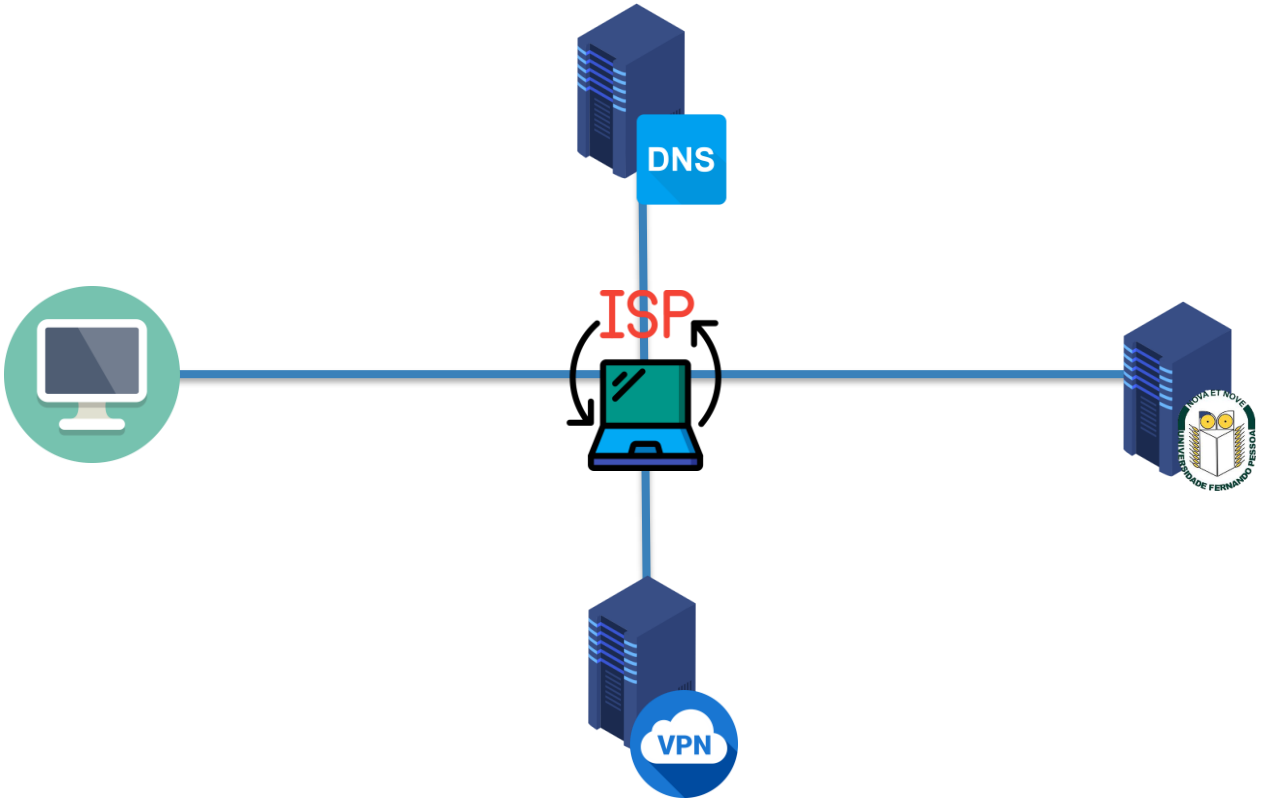


INTERNET COMUM

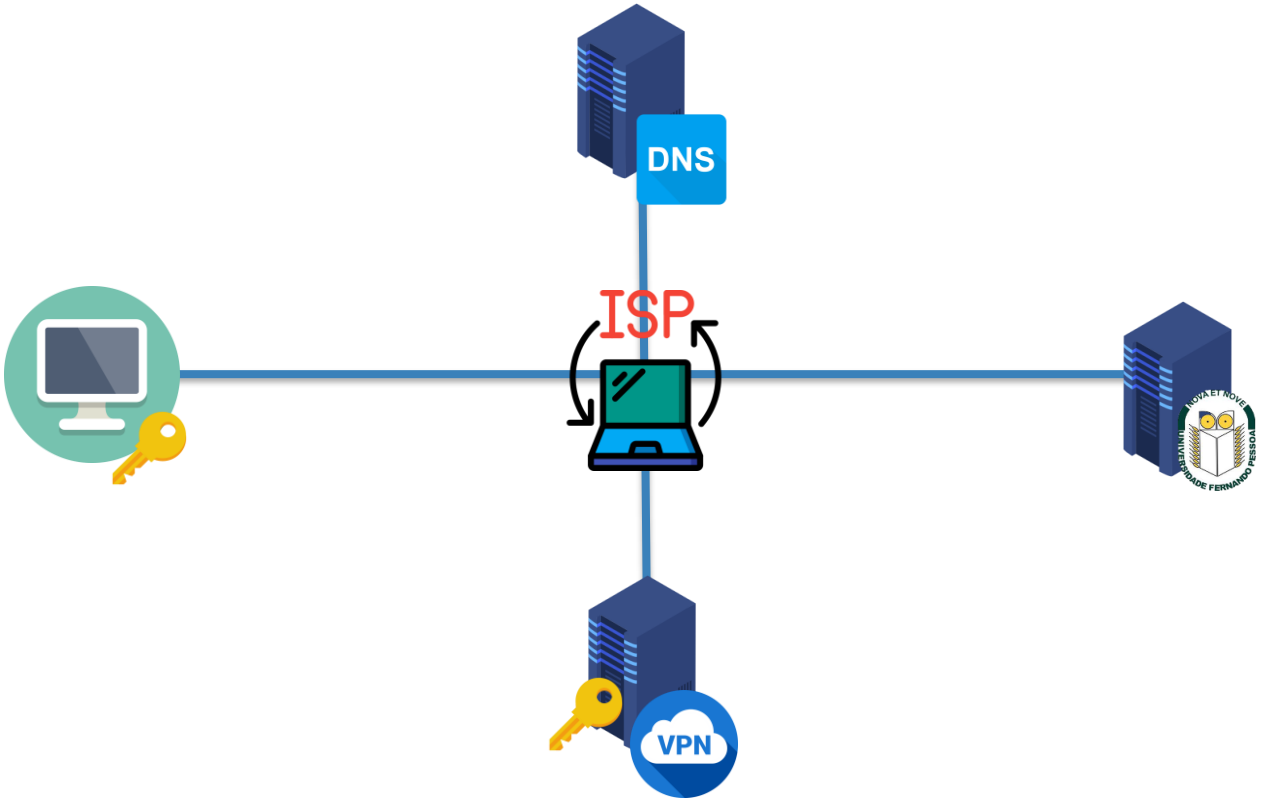
INTERNET COMUM



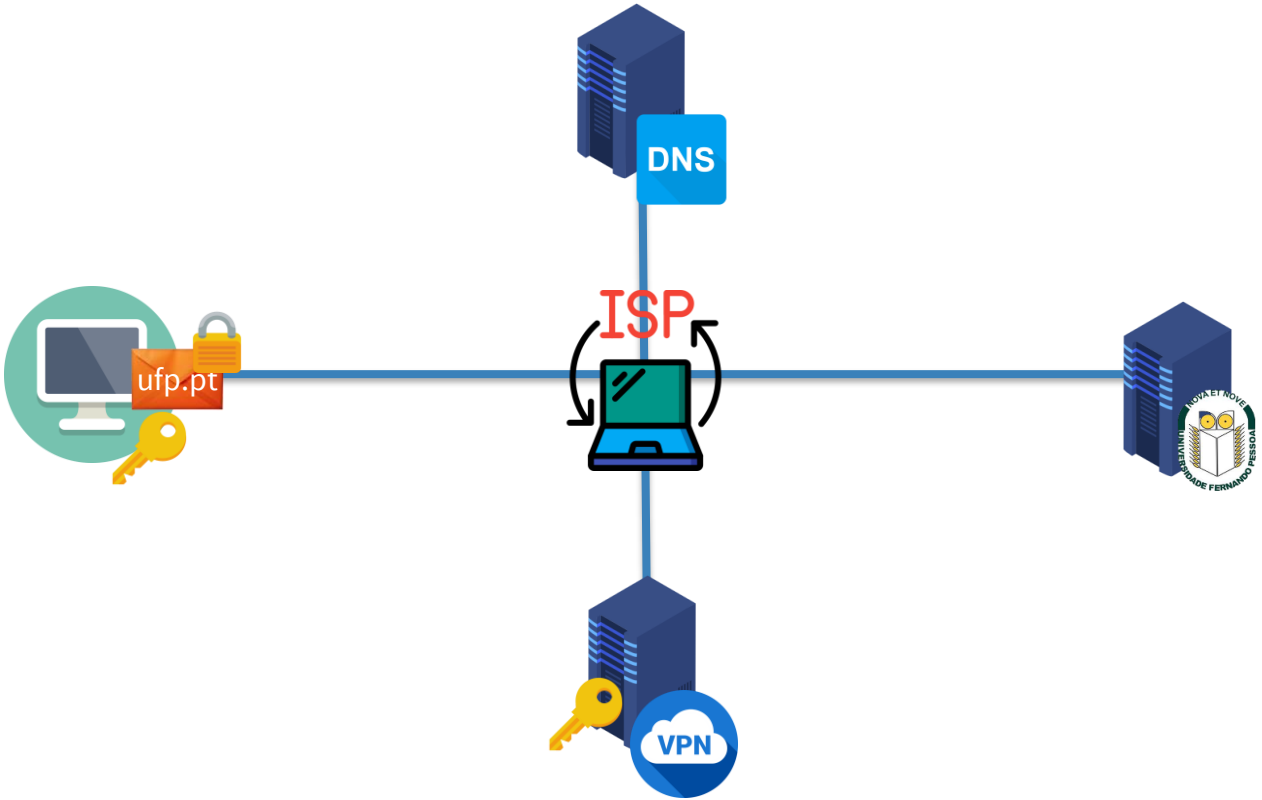
VPN (VIRTUAL PRIVATE NETWORK)



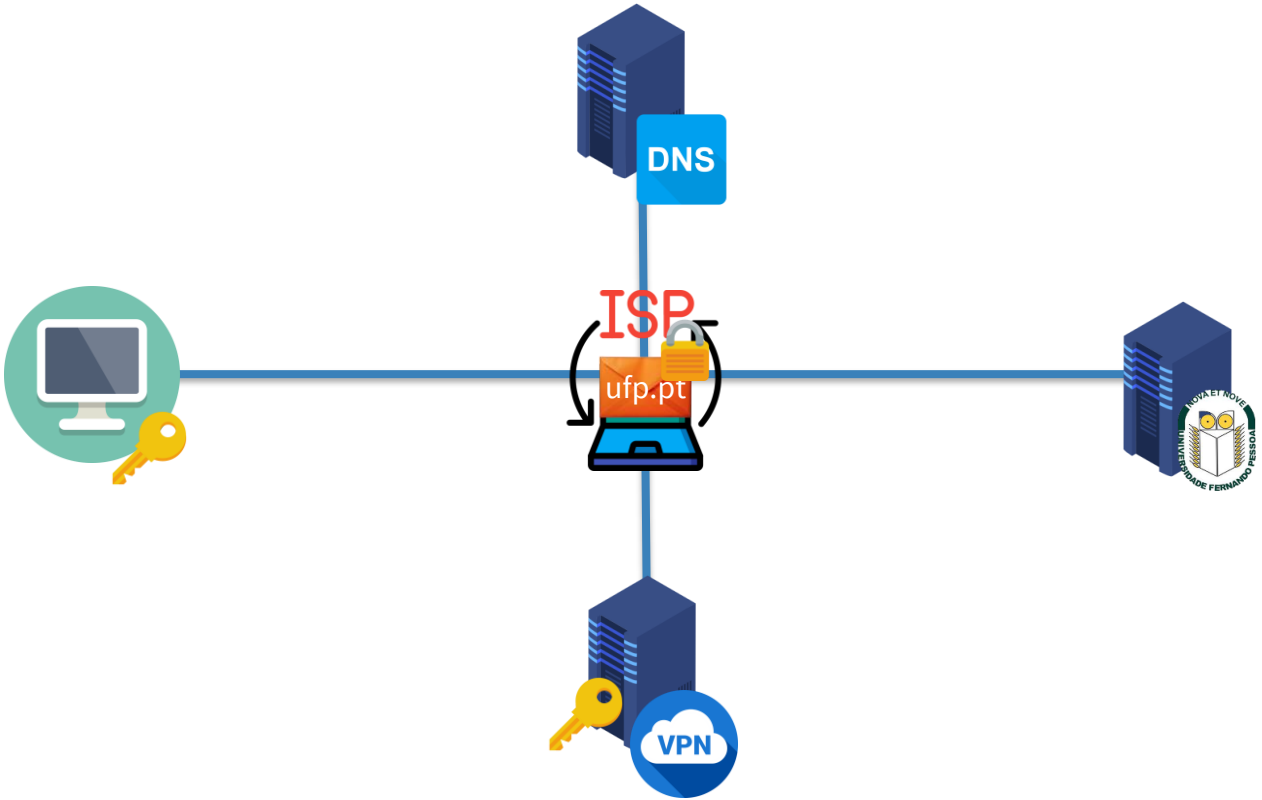
VPN (VIRTUAL PRIVATE NETWORK)



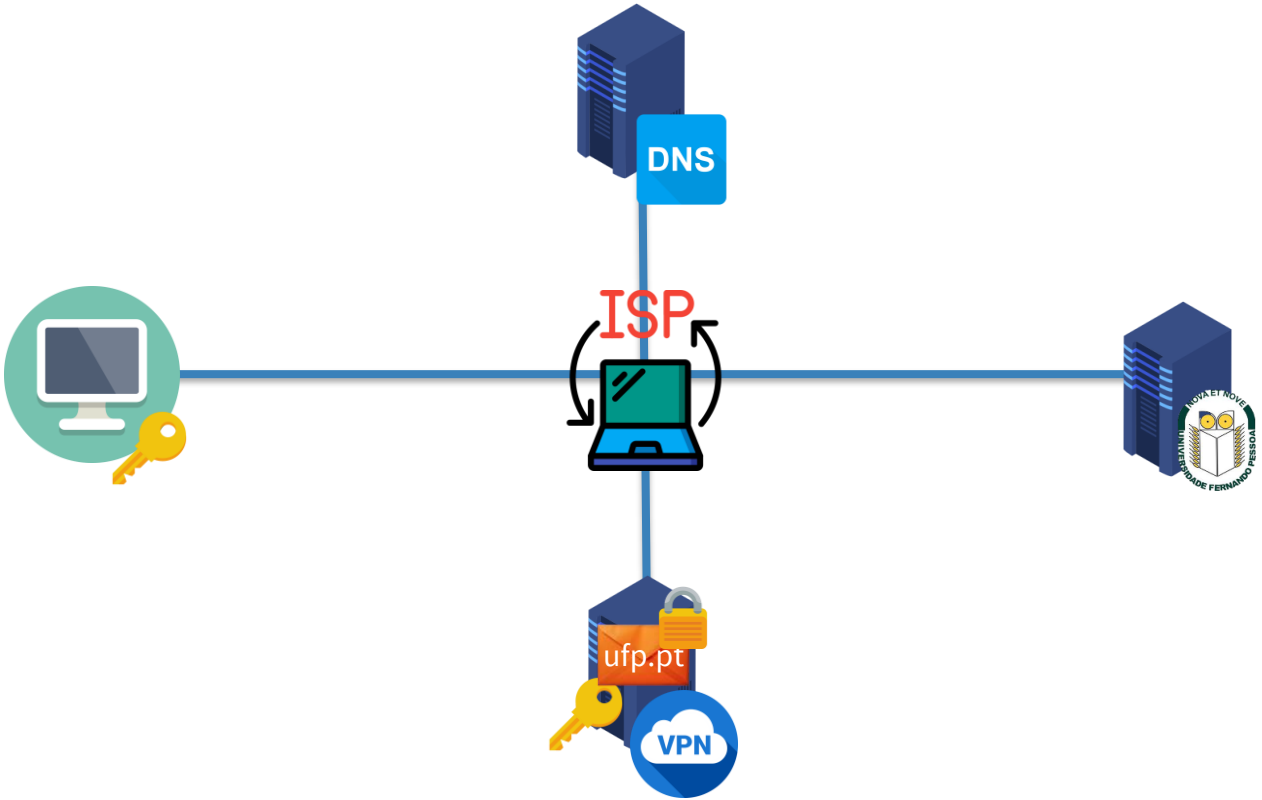
VPN (VIRTUAL PRIVATE NETWORK)



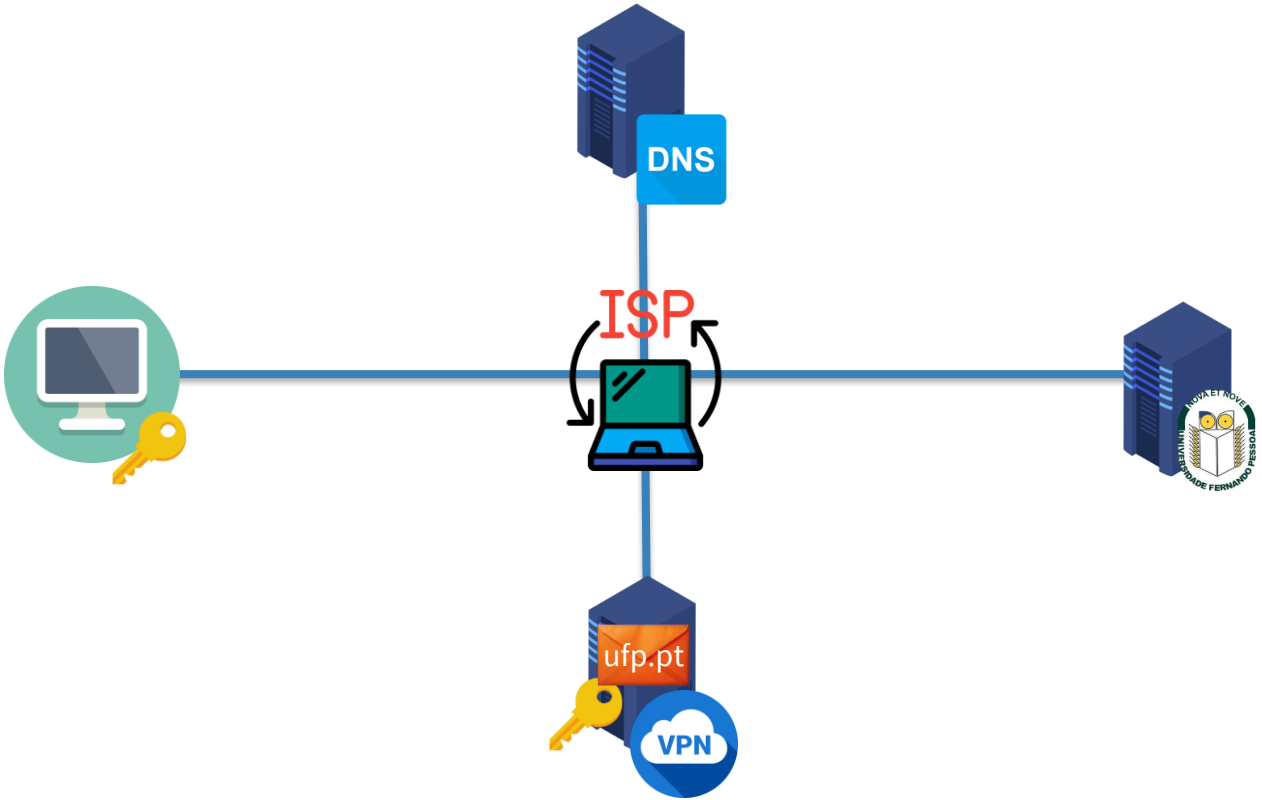
VPN (VIRTUAL PRIVATE NETWORK)



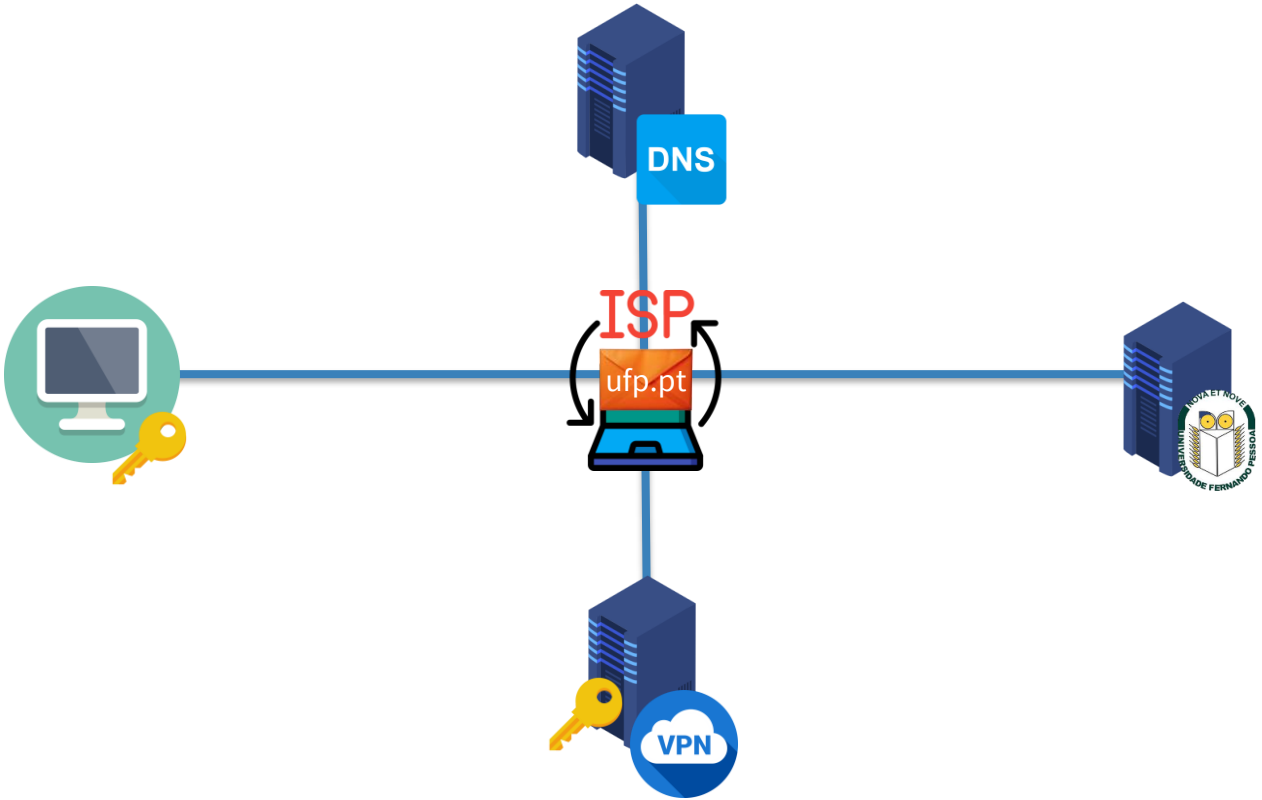
VPN (VIRTUAL PRIVATE NETWORK)



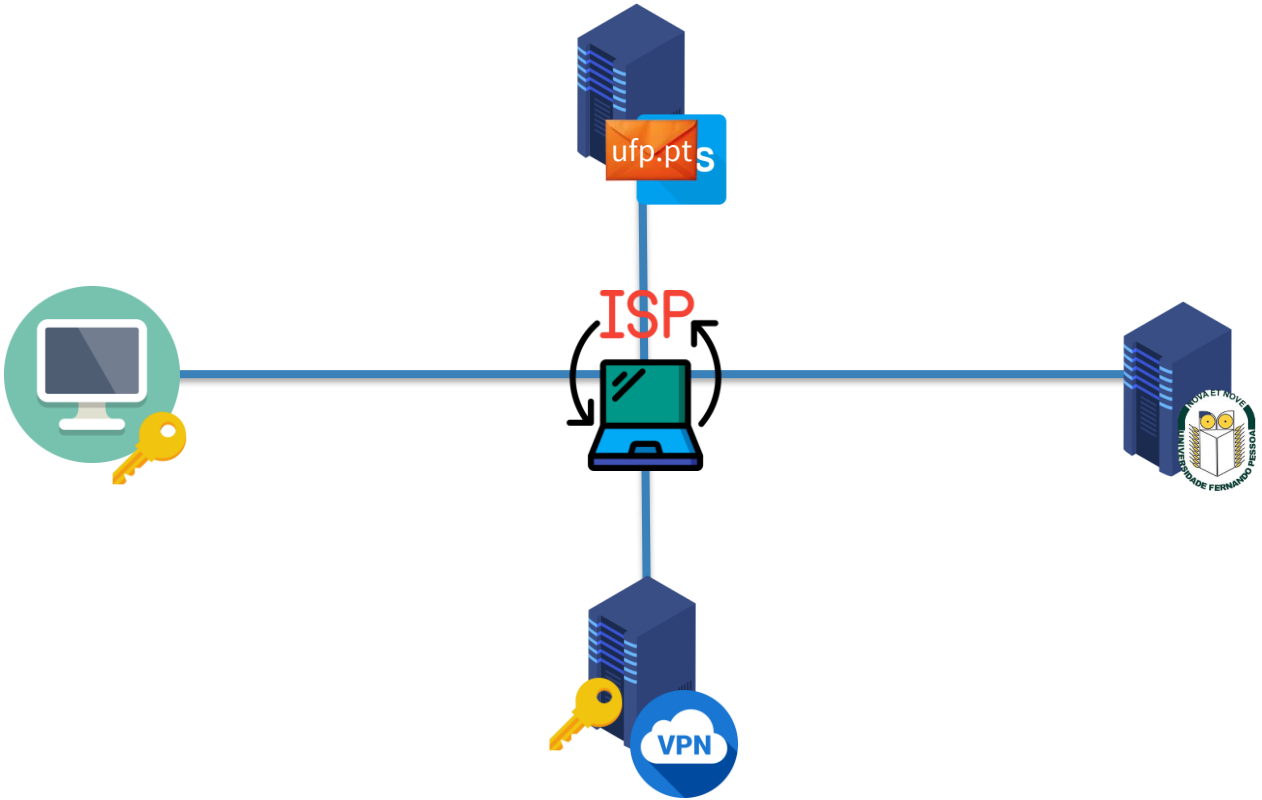
VPN (VIRTUAL PRIVATE NETWORK)



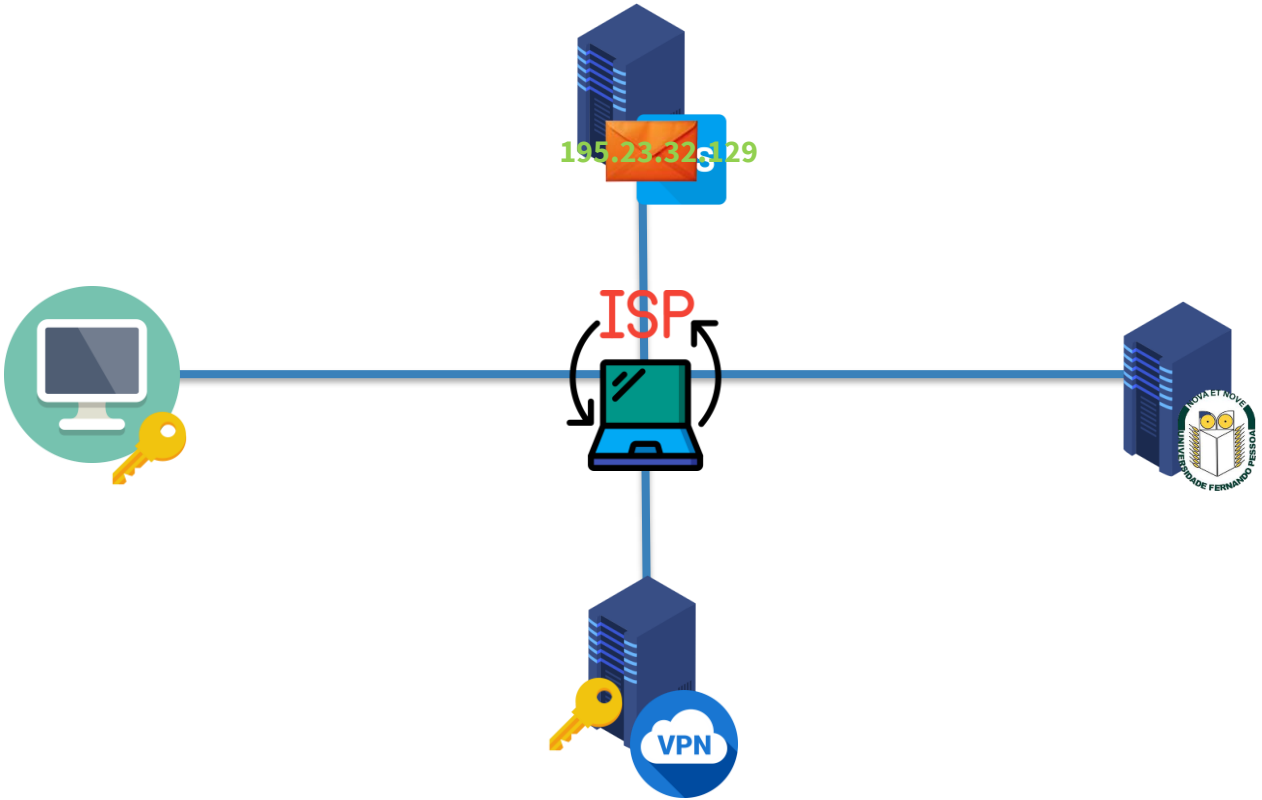
VPN (VIRTUAL PRIVATE NETWORK)



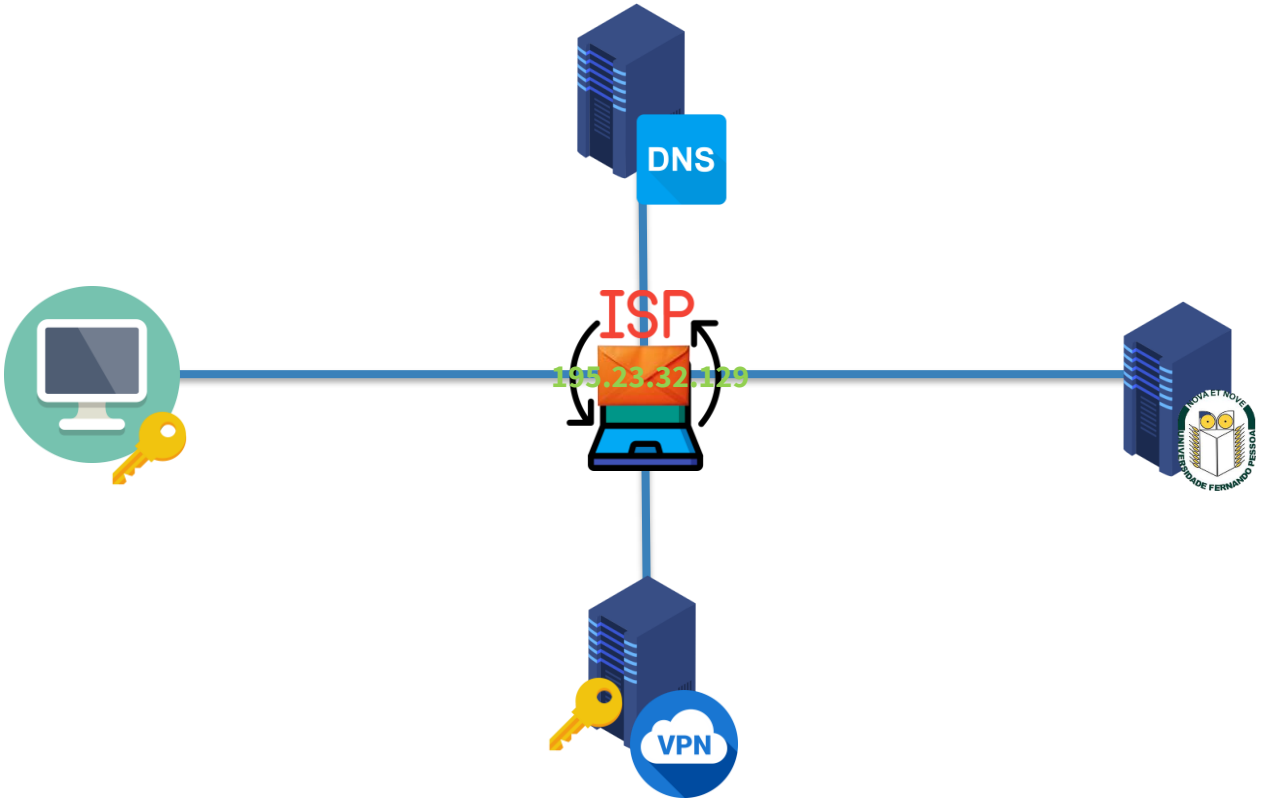
VPN (VIRTUAL PRIVATE NETWORK)



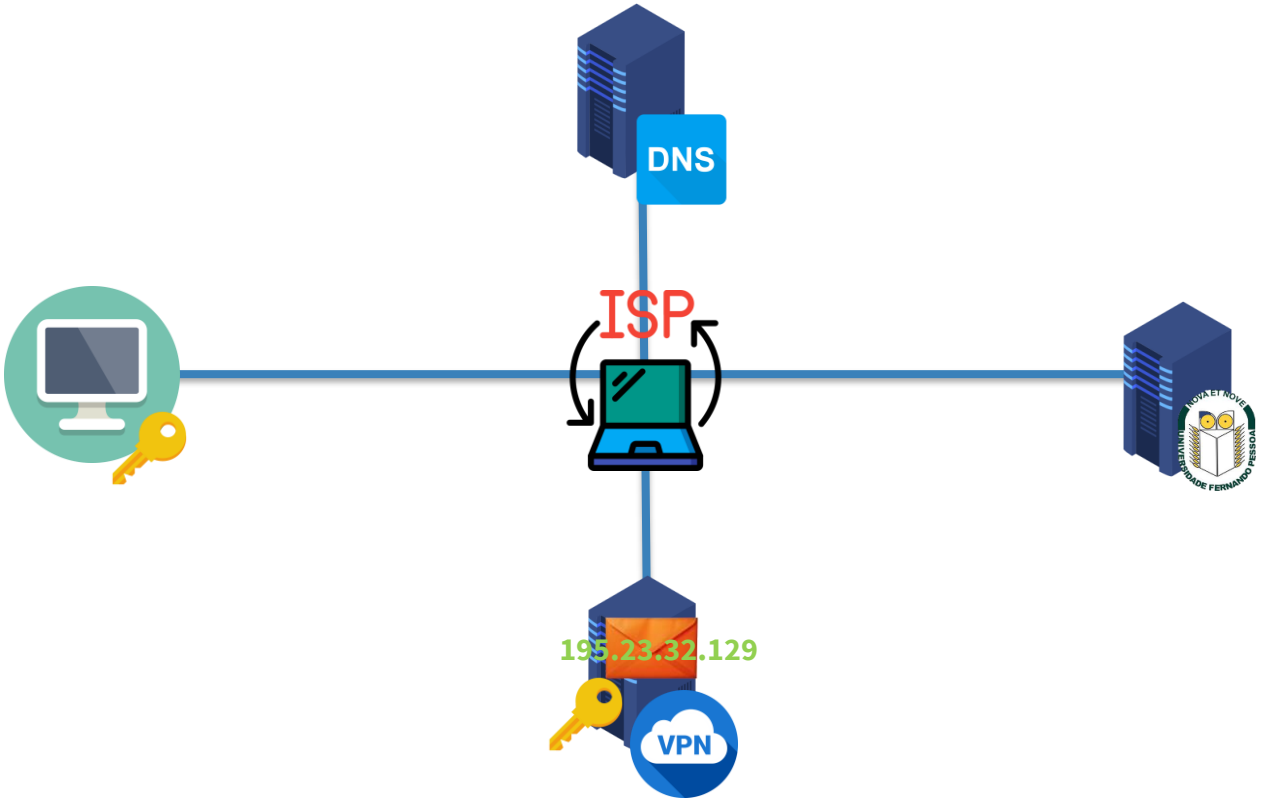
VPN (VIRTUAL PRIVATE NETWORK)



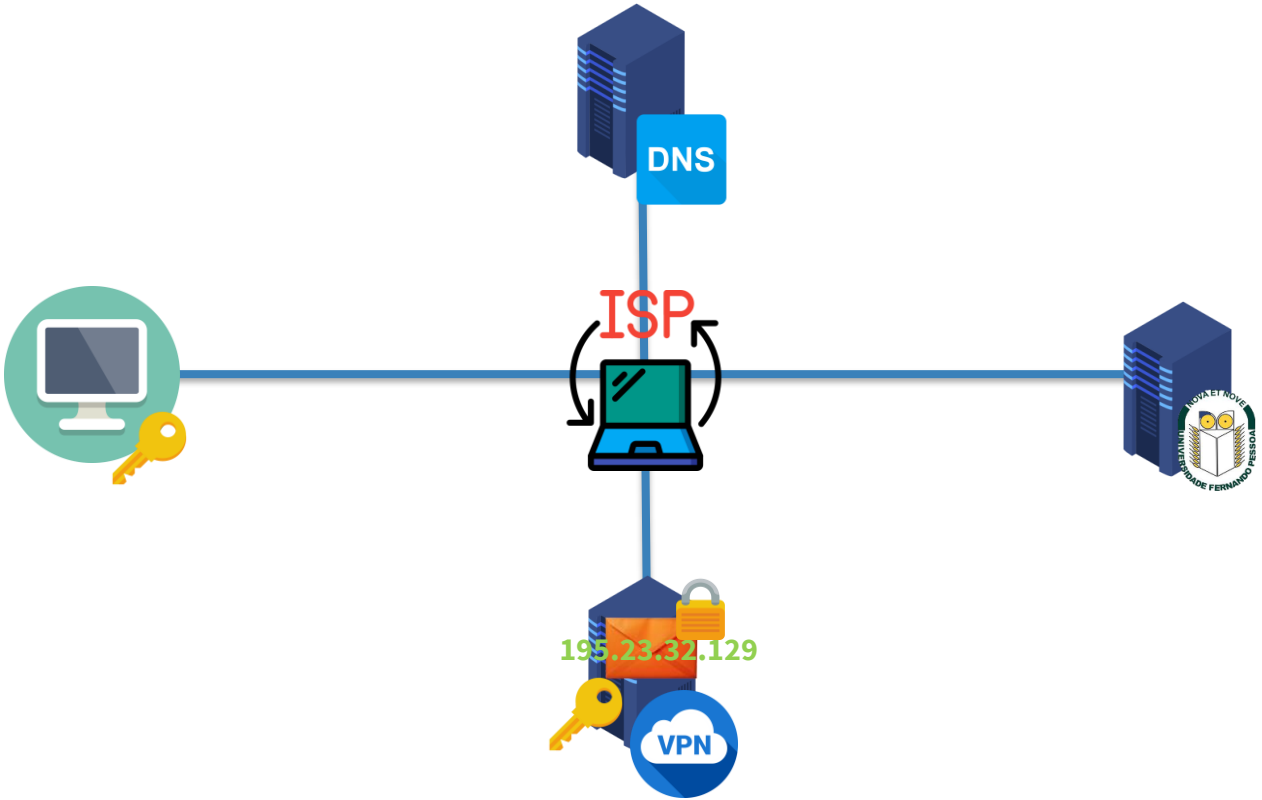
VPN (VIRTUAL PRIVATE NETWORK)



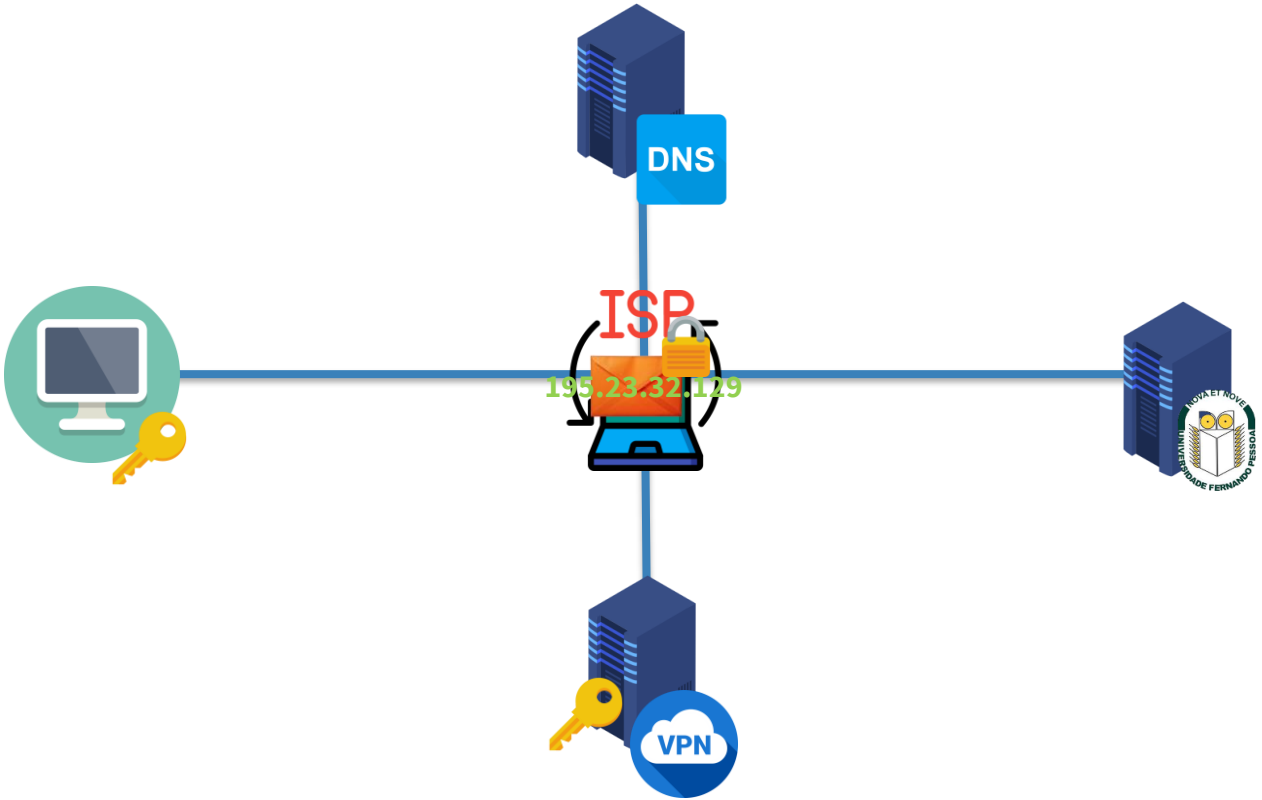
VPN (VIRTUAL PRIVATE NETWORK)



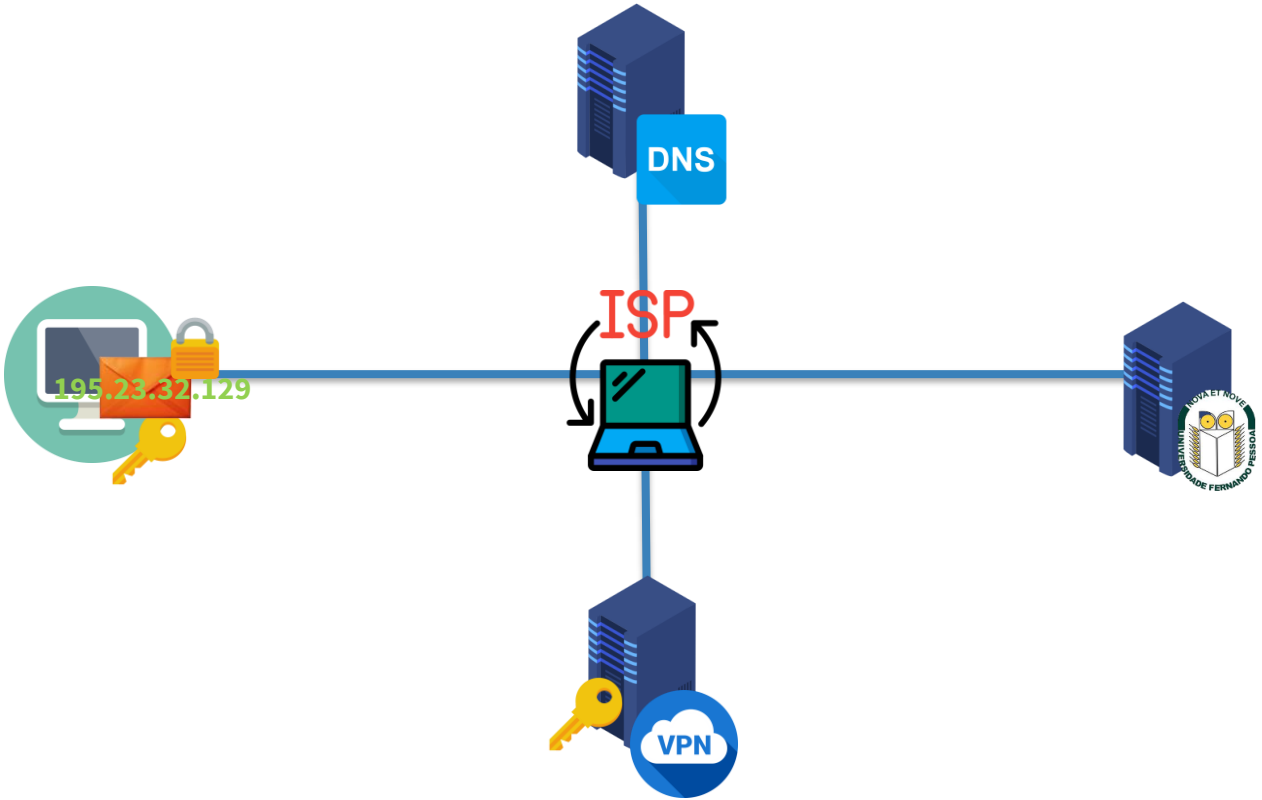
VPN (VIRTUAL PRIVATE NETWORK)



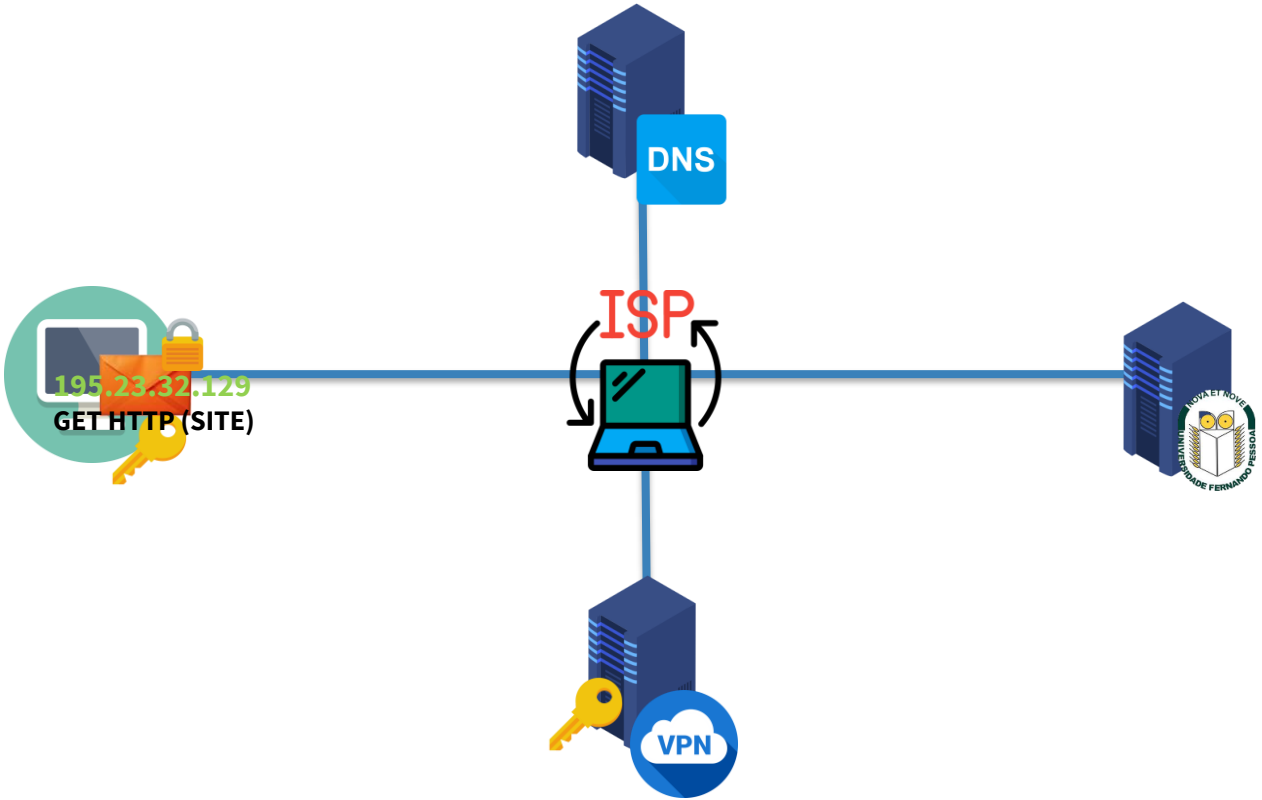
VPN (VIRTUAL PRIVATE NETWORK)



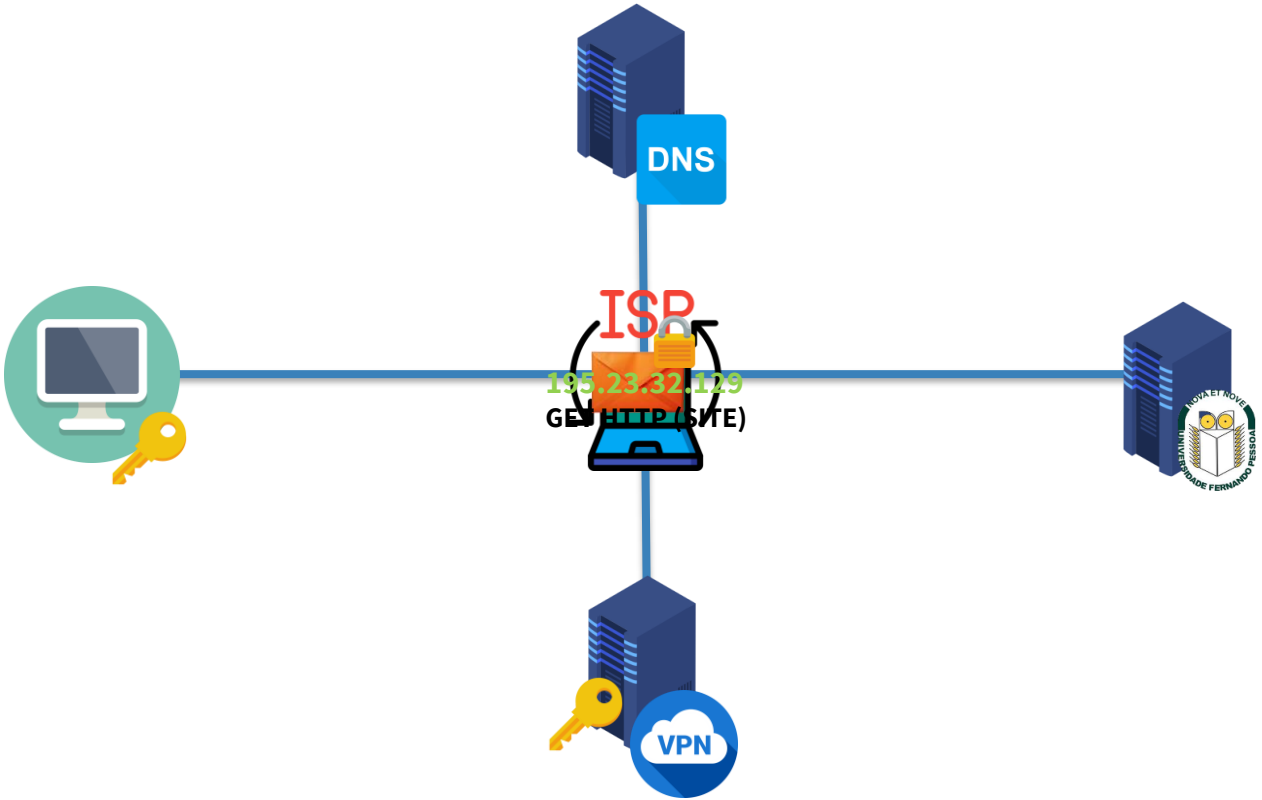
VPN (VIRTUAL PRIVATE NETWORK)



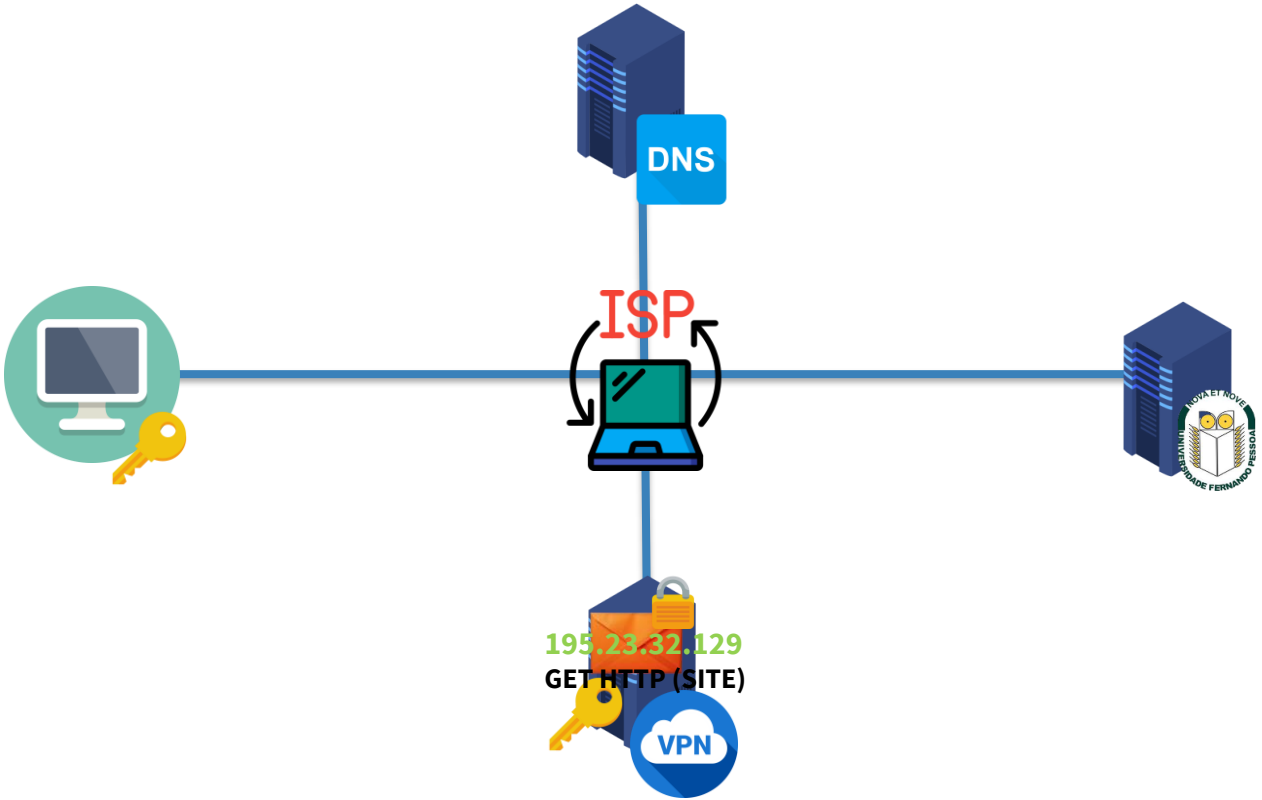
VPN (VIRTUAL PRIVATE NETWORK)



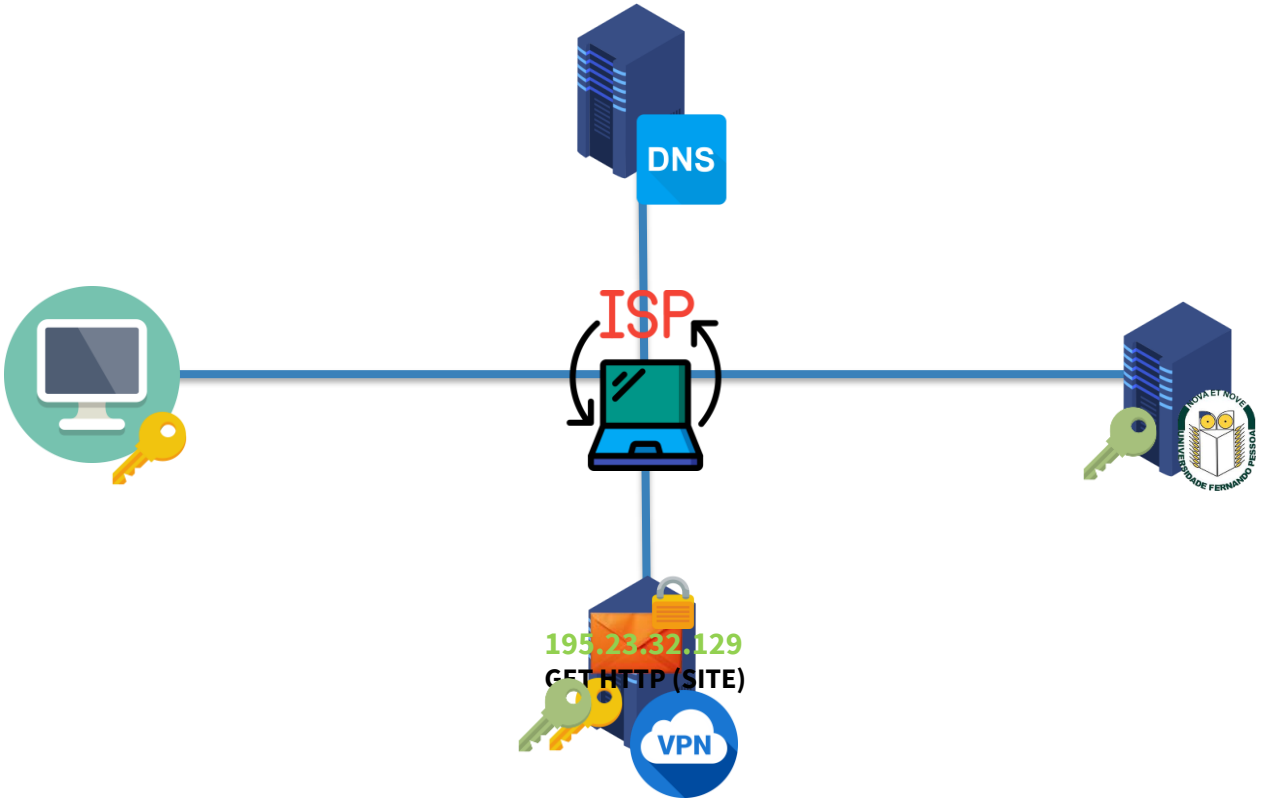
VPN (VIRTUAL PRIVATE NETWORK)



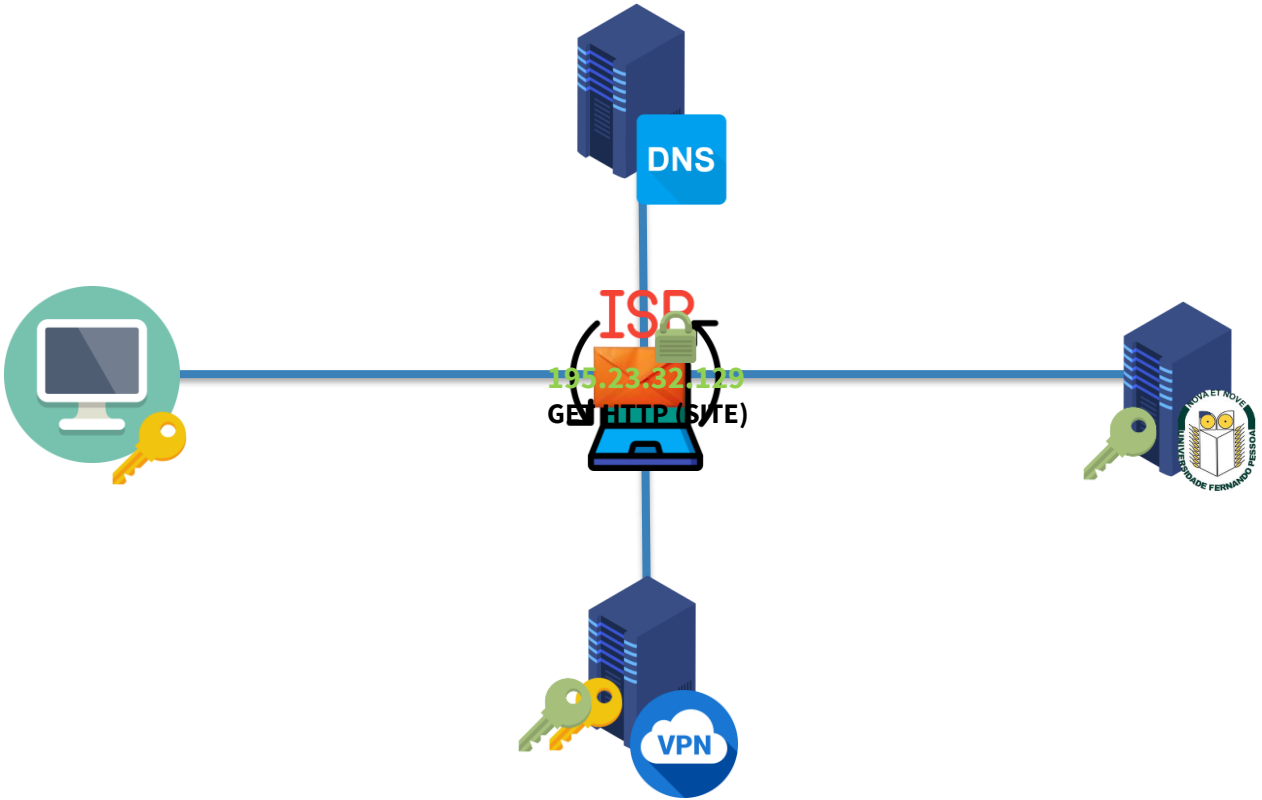
VPN (VIRTUAL PRIVATE NETWORK)



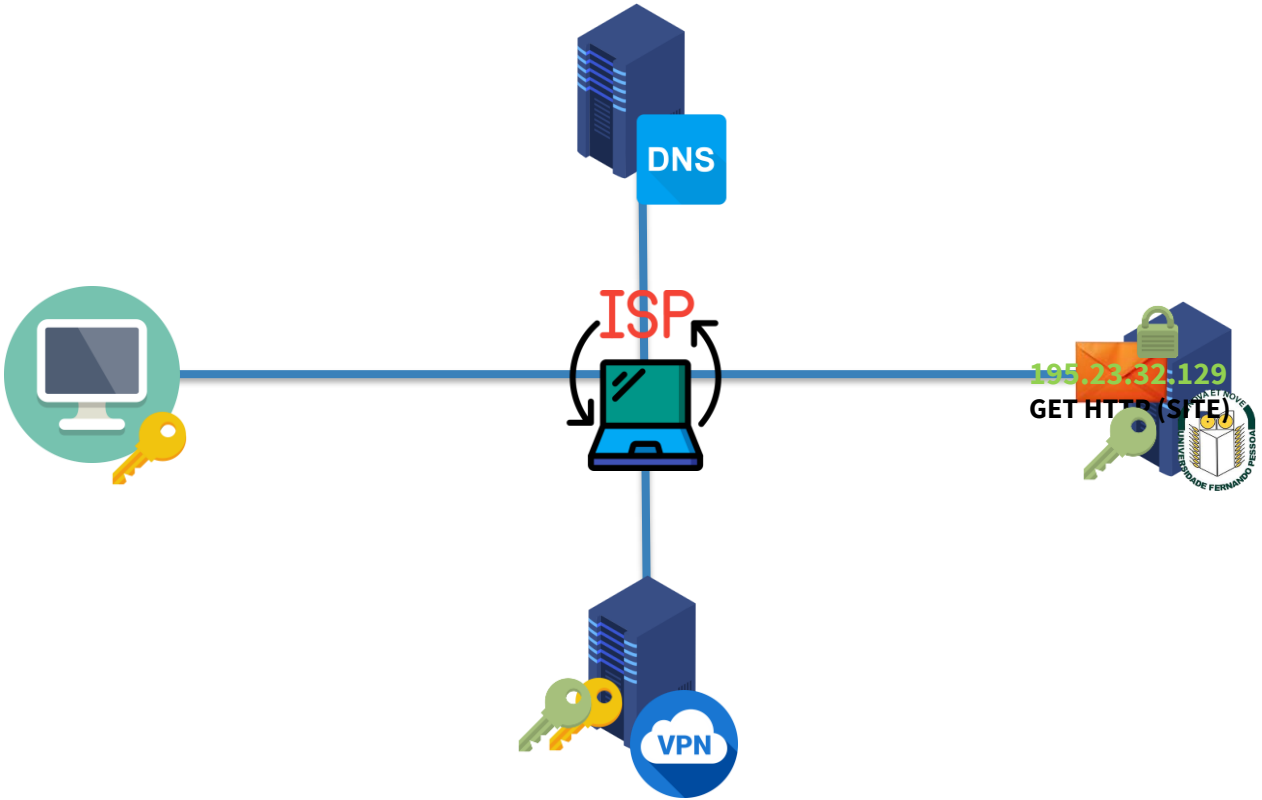
VPN (VIRTUAL PRIVATE NETWORK)



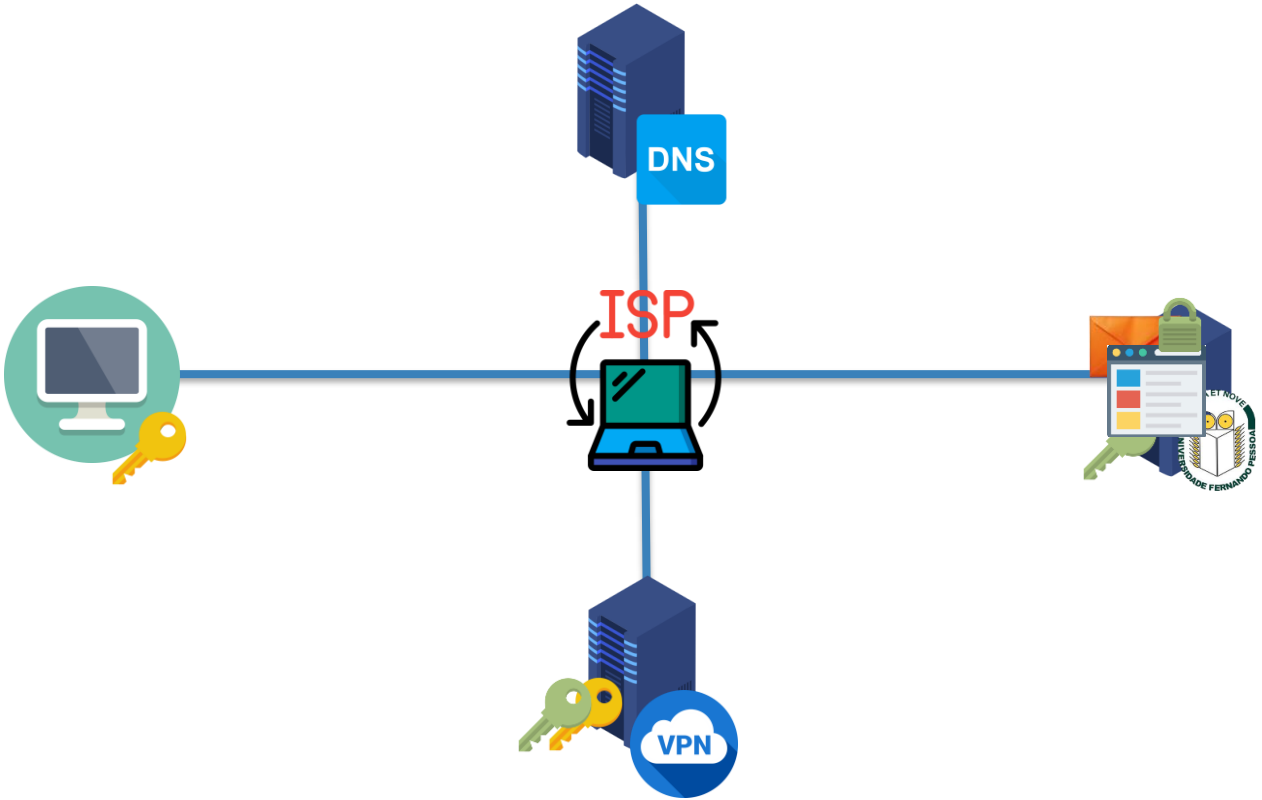
VPN (VIRTUAL PRIVATE NETWORK)



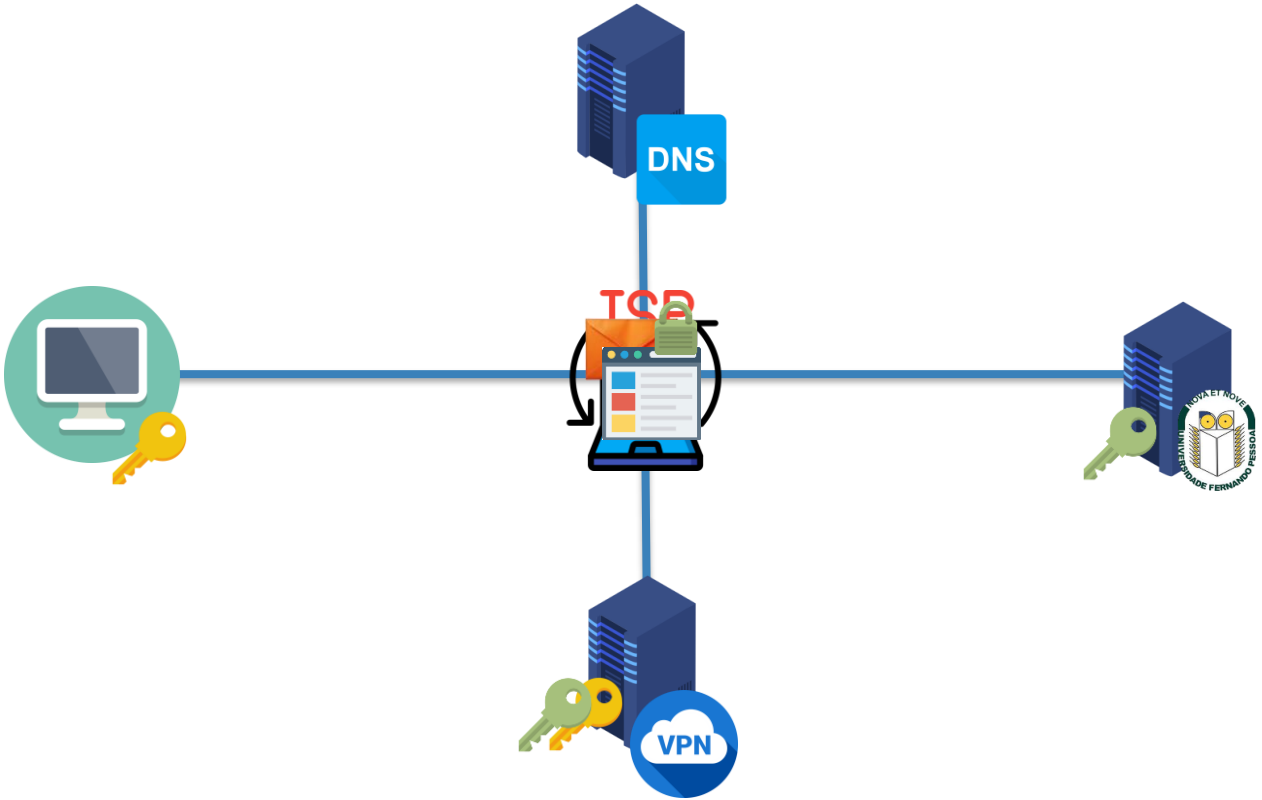
VPN (VIRTUAL PRIVATE NETWORK)



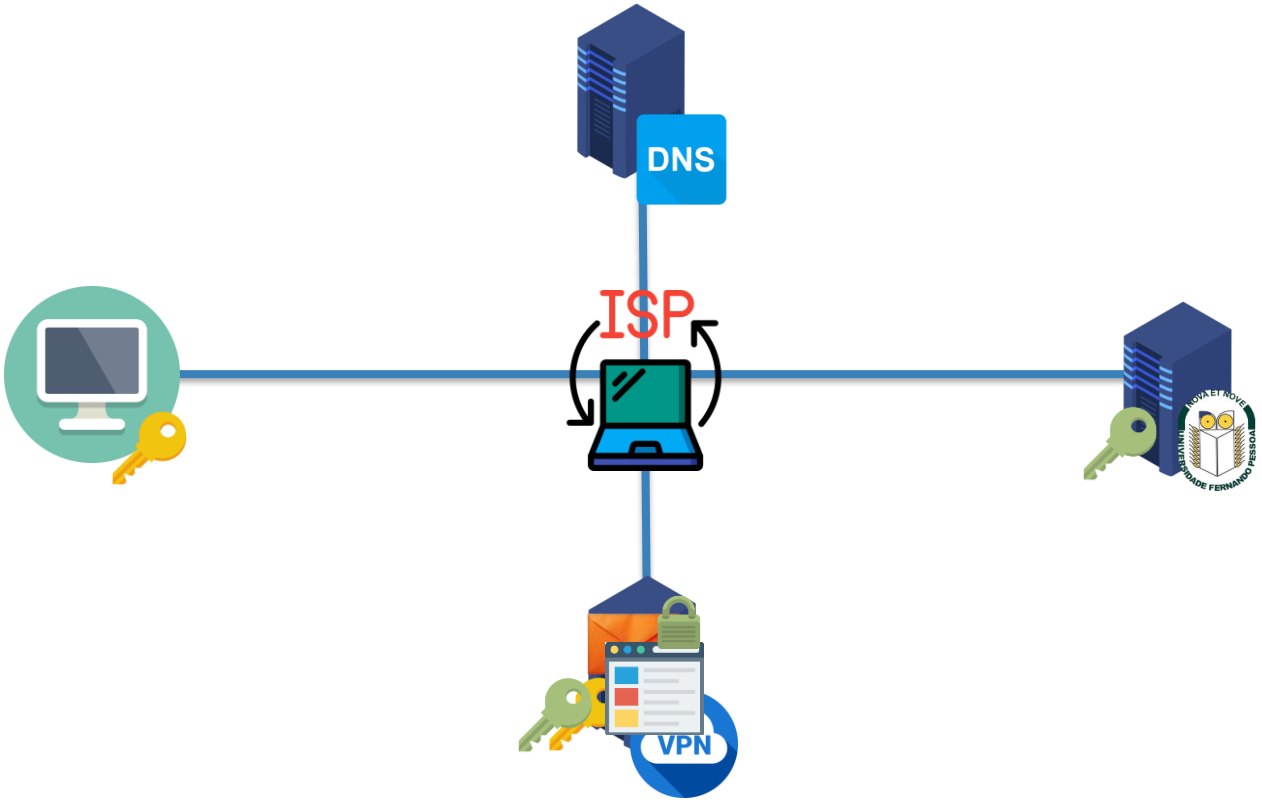
VPN (VIRTUAL PRIVATE NETWORK)



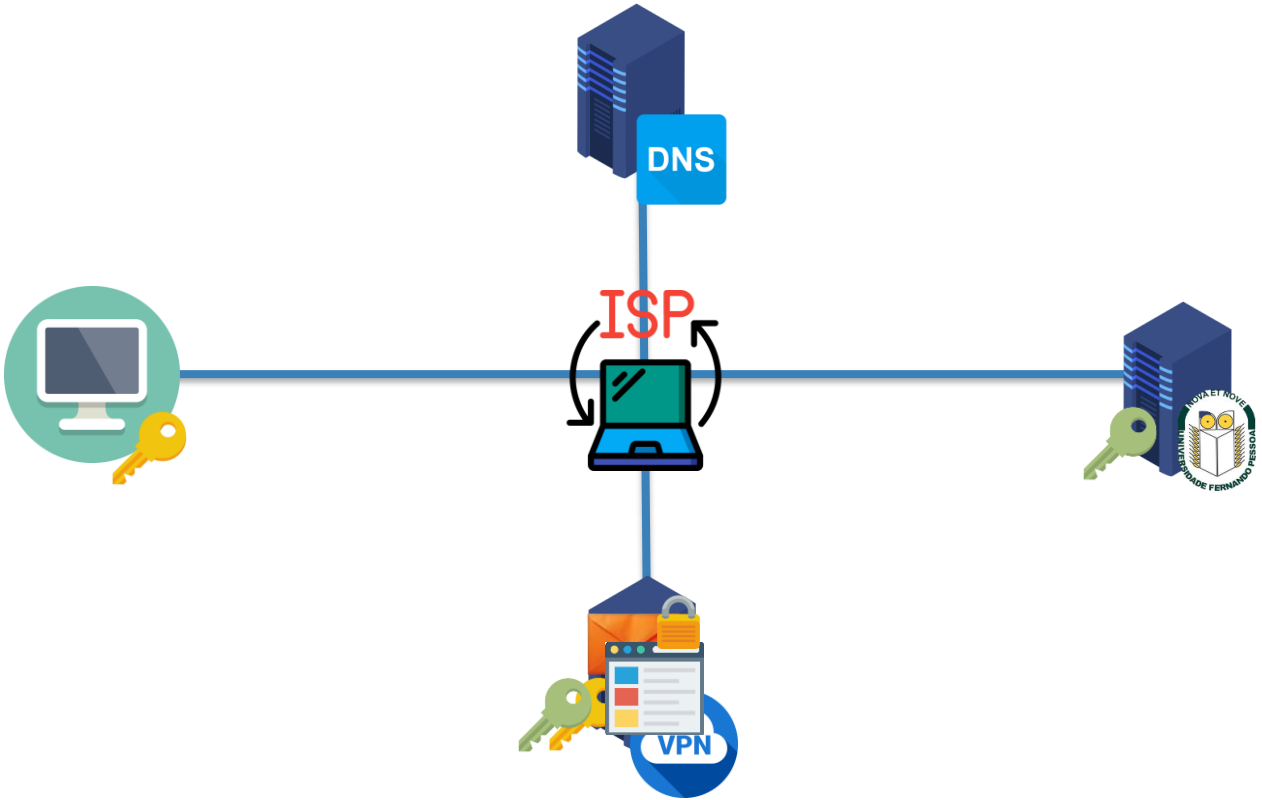
VPN (VIRTUAL PRIVATE NETWORK)



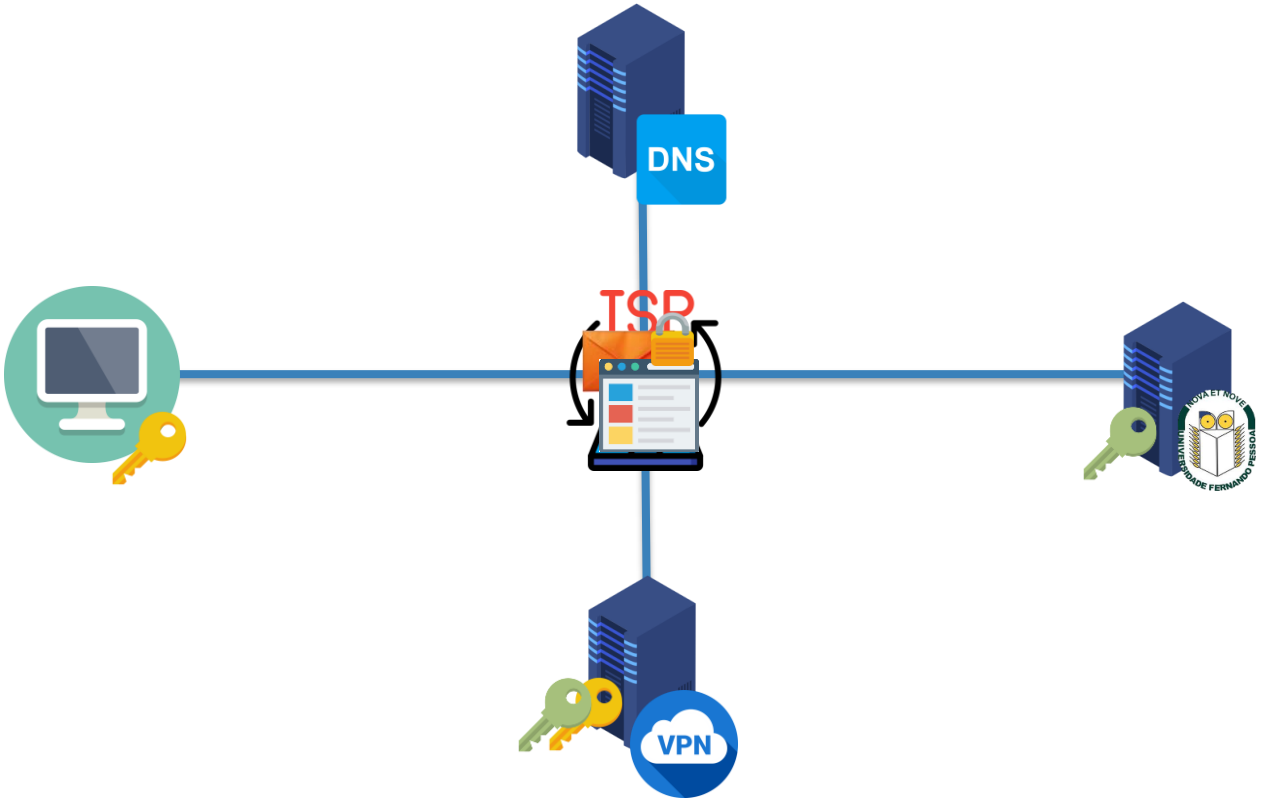
VPN (VIRTUAL PRIVATE NETWORK)



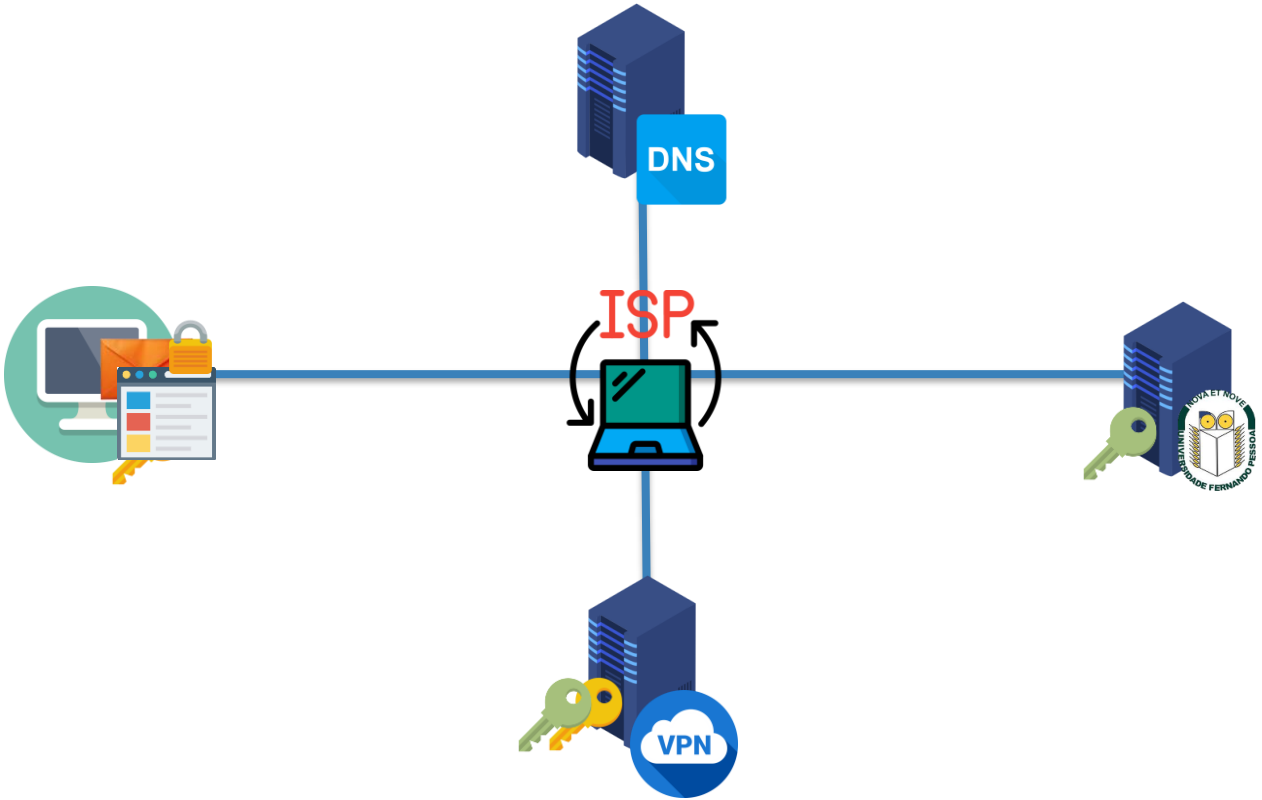
VPN (VIRTUAL PRIVATE NETWORK)



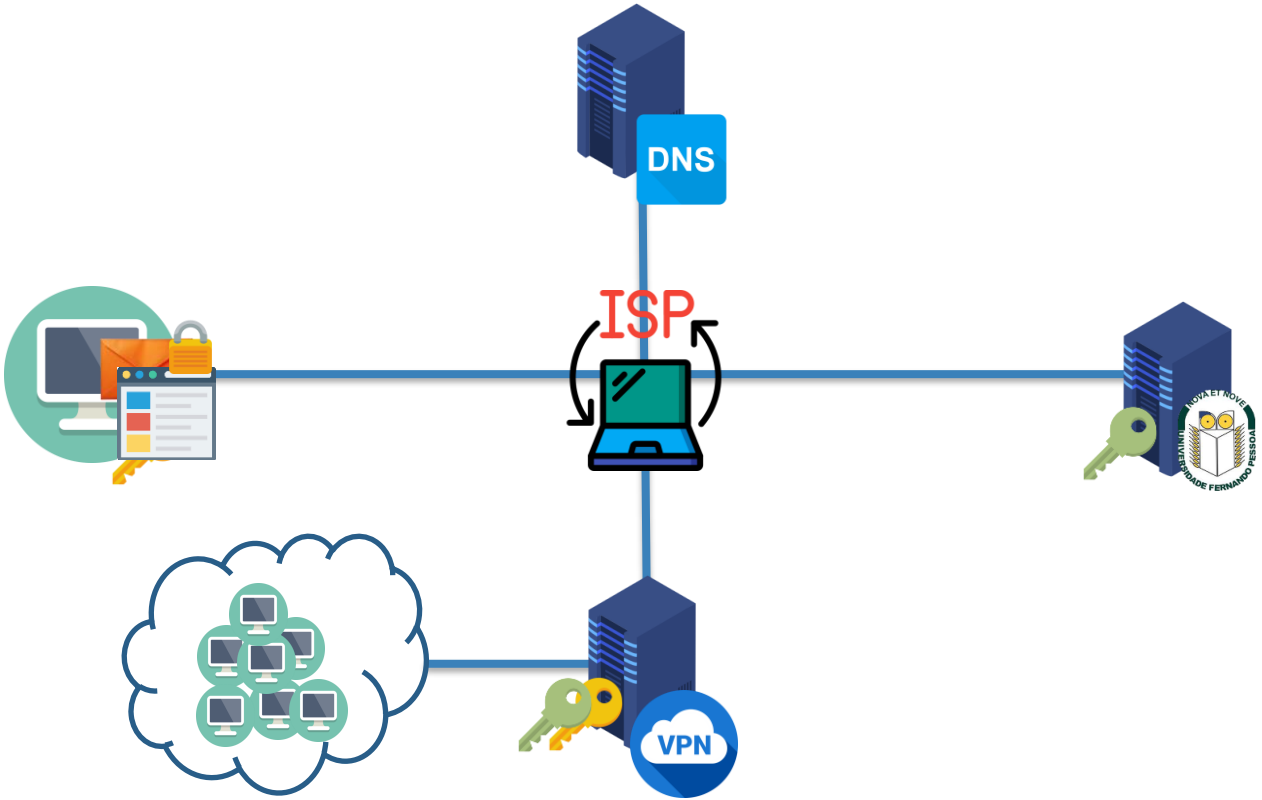
VPN (VIRTUAL PRIVATE NETWORK)



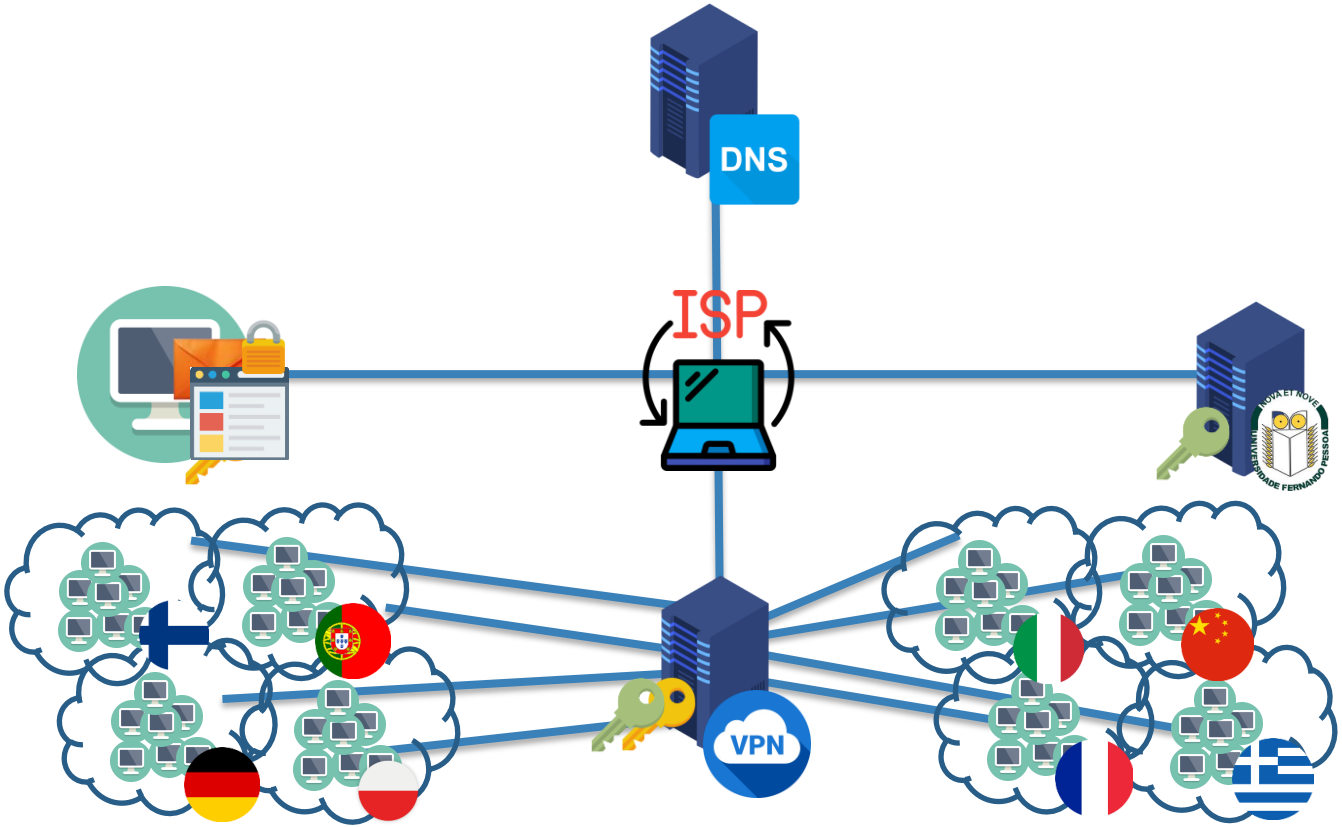
VPN (VIRTUAL PRIVATE NETWORK)



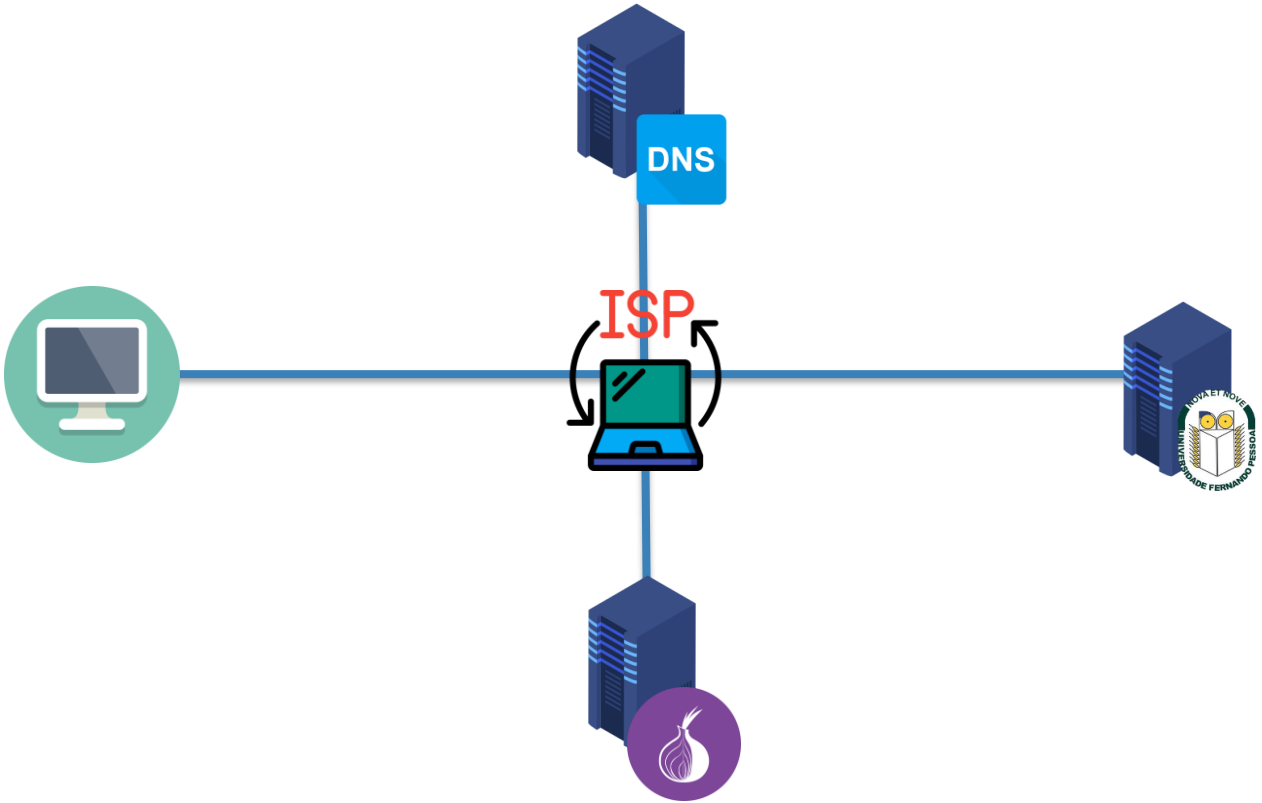
VPN (VIRTUAL PRIVATE NETWORK)



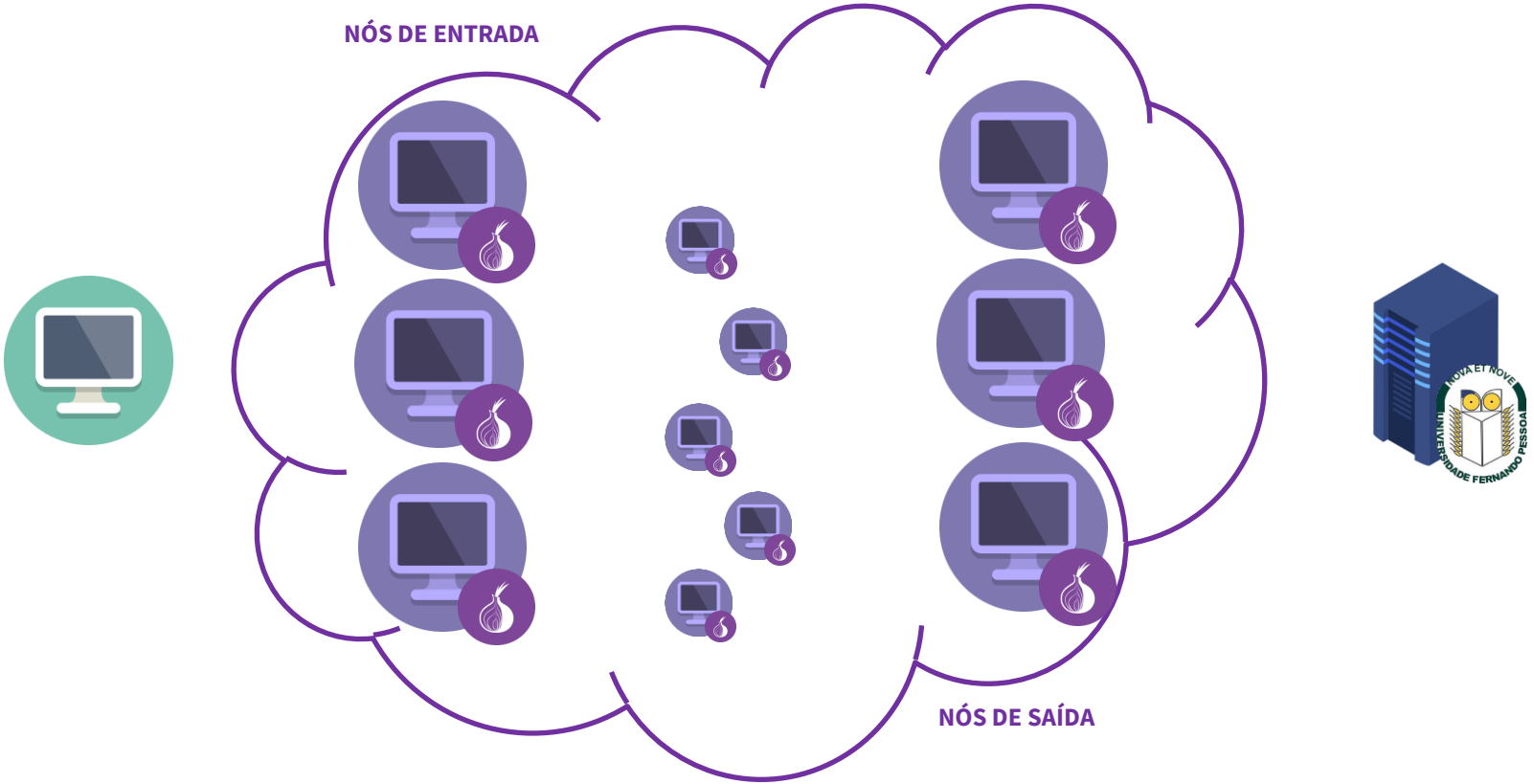
VPN (VIRTUAL PRIVATE NETWORK)



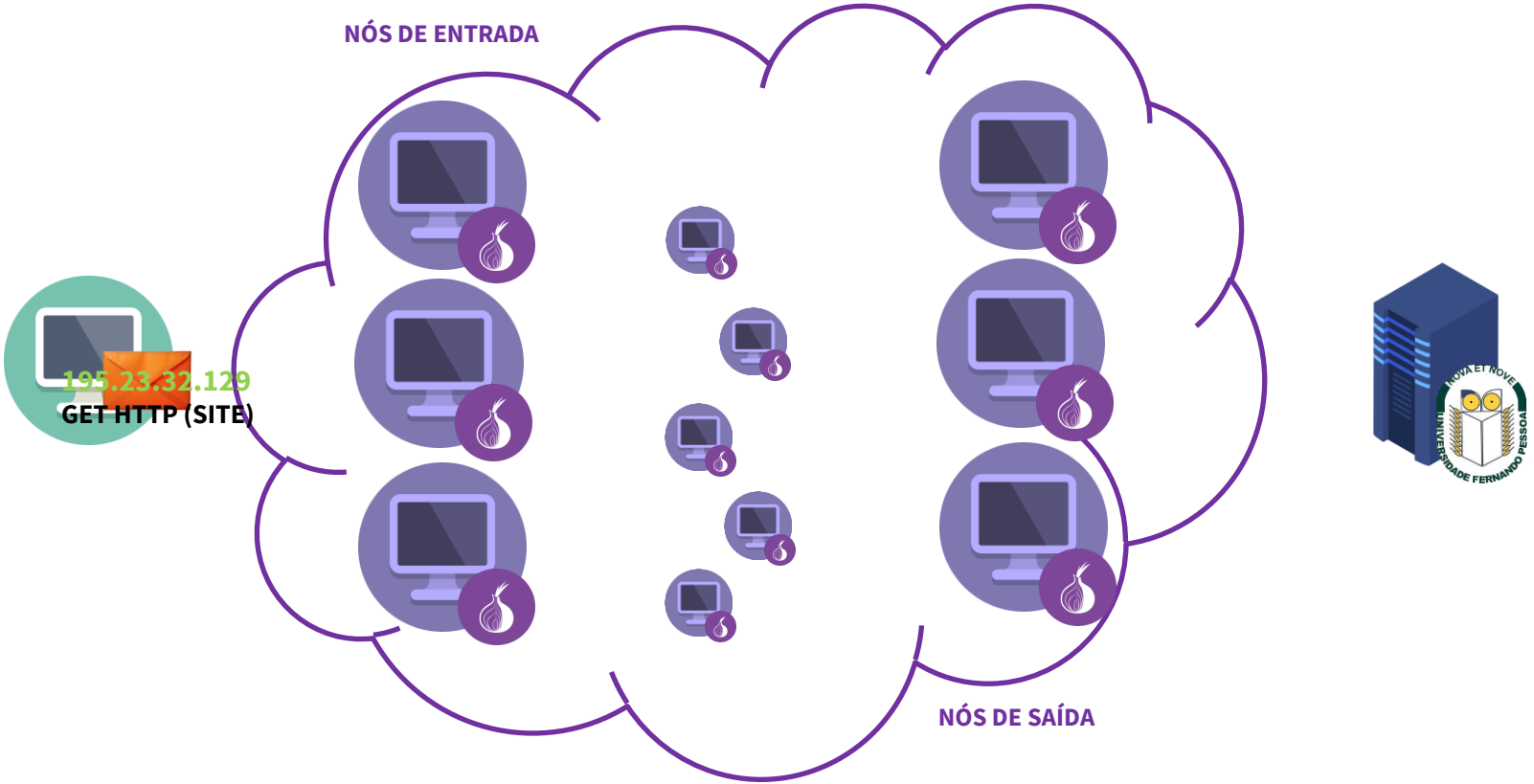
TOR



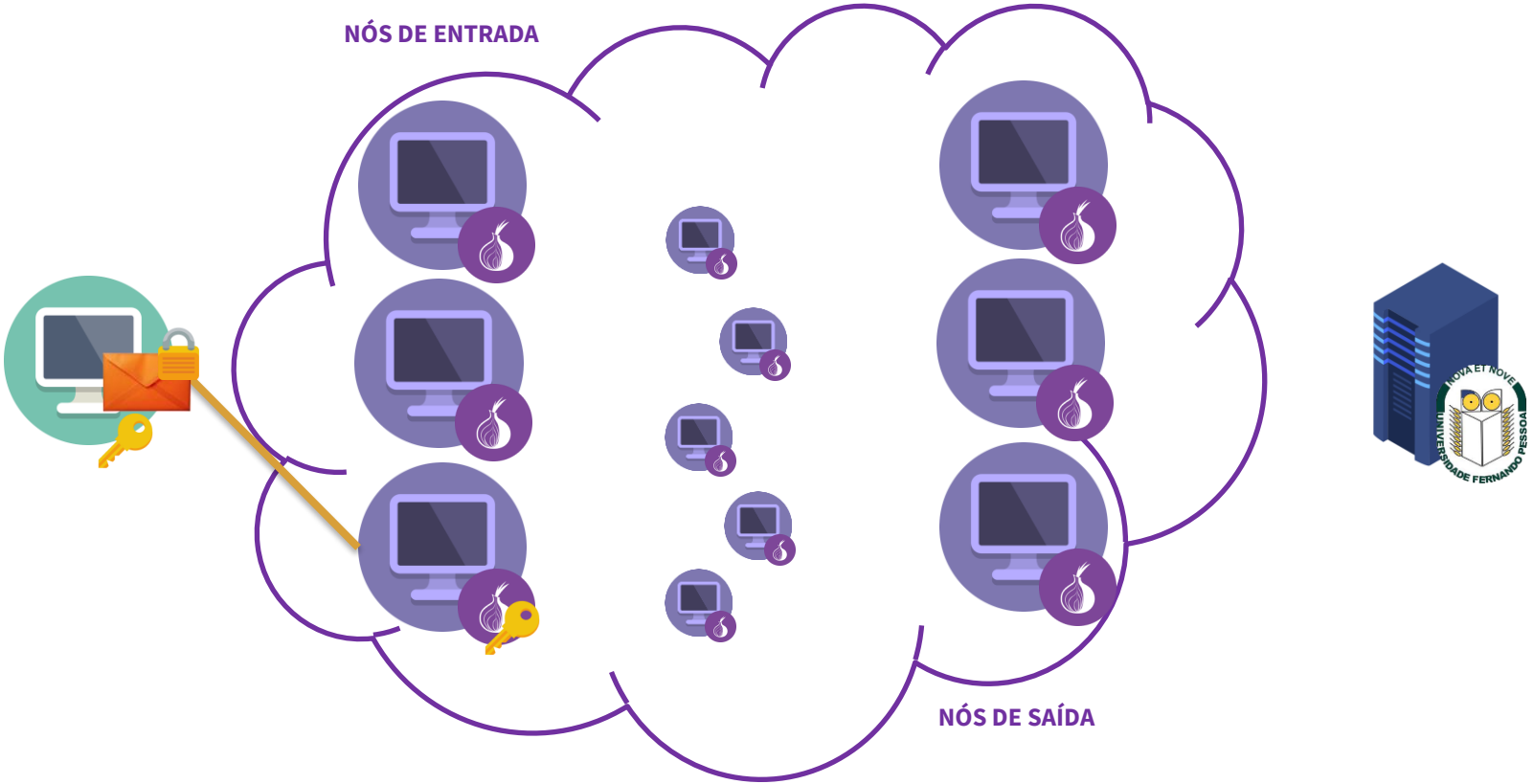
TOR


NÓS DE ENTRADA
NÓS DE SAÍDA
NOVA ET NOVÆ
UNIVERSIDADE FERNANDO PESSOA

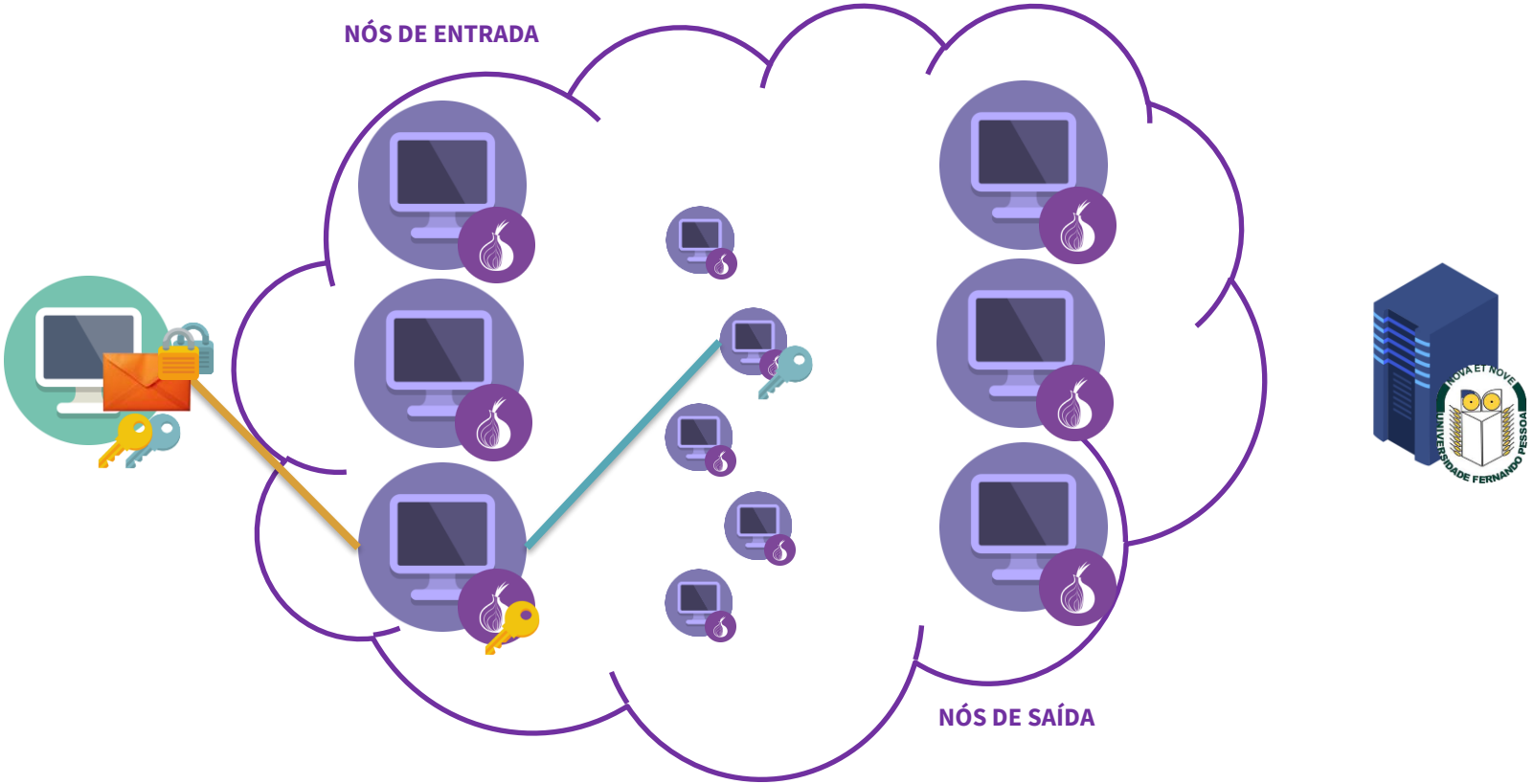
TOR


NÓS DE ENTRADA
195.23.32.129
GET HTTP (SITE)
NÓS DE SAÍDA
NOVA ET NOVÆ
UNIVERSIDADE FERNANDO PESSOA

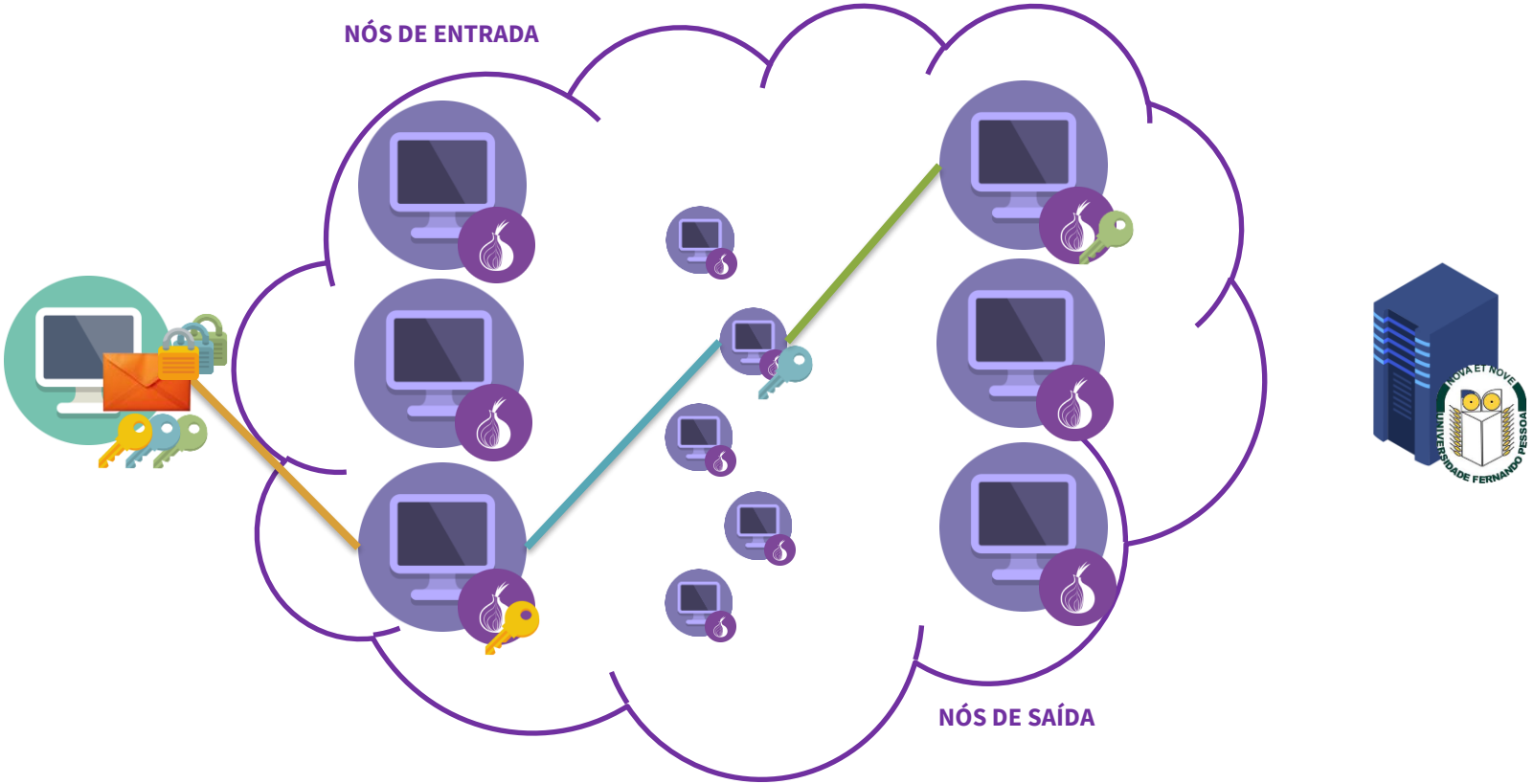
TOR



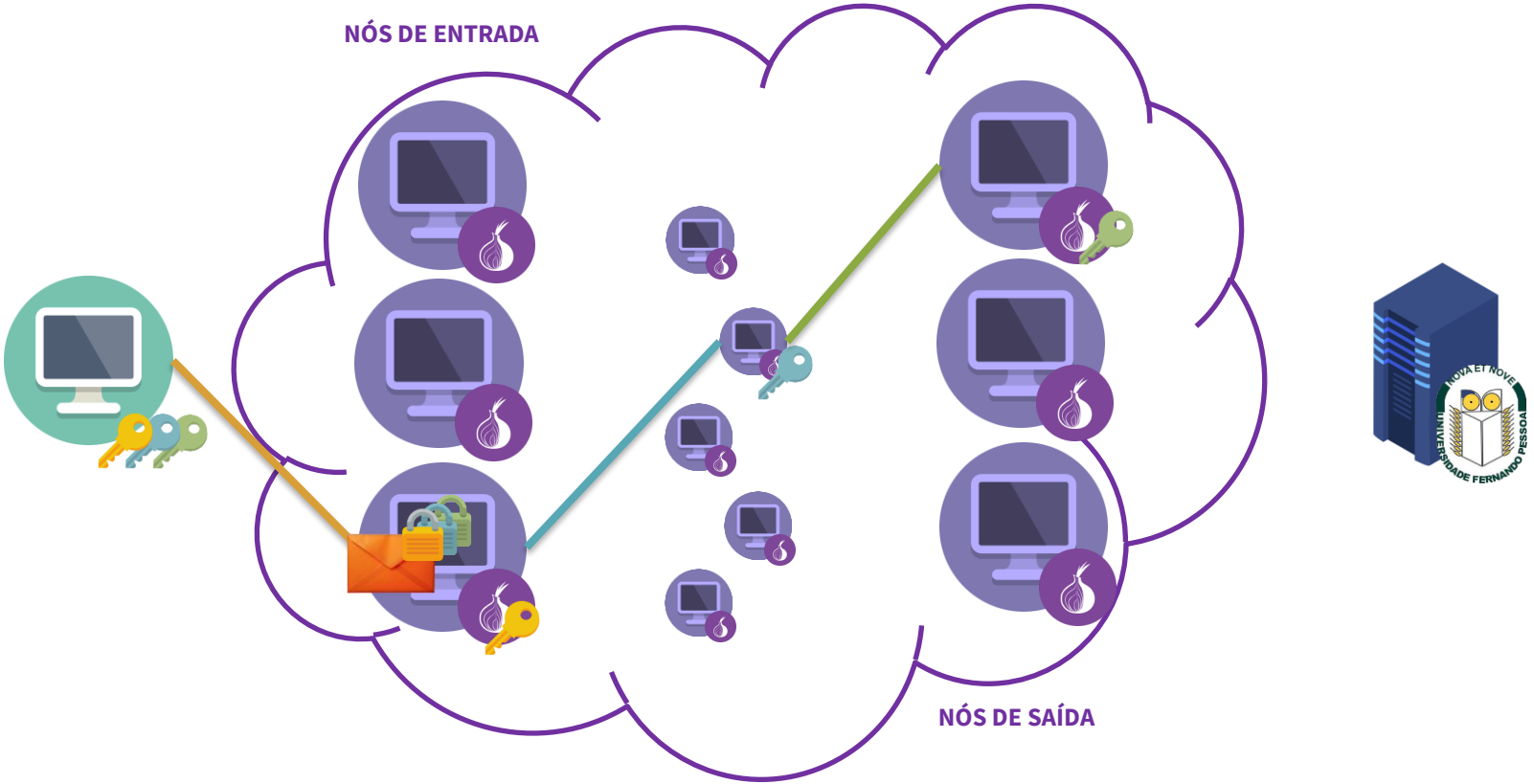
TOR



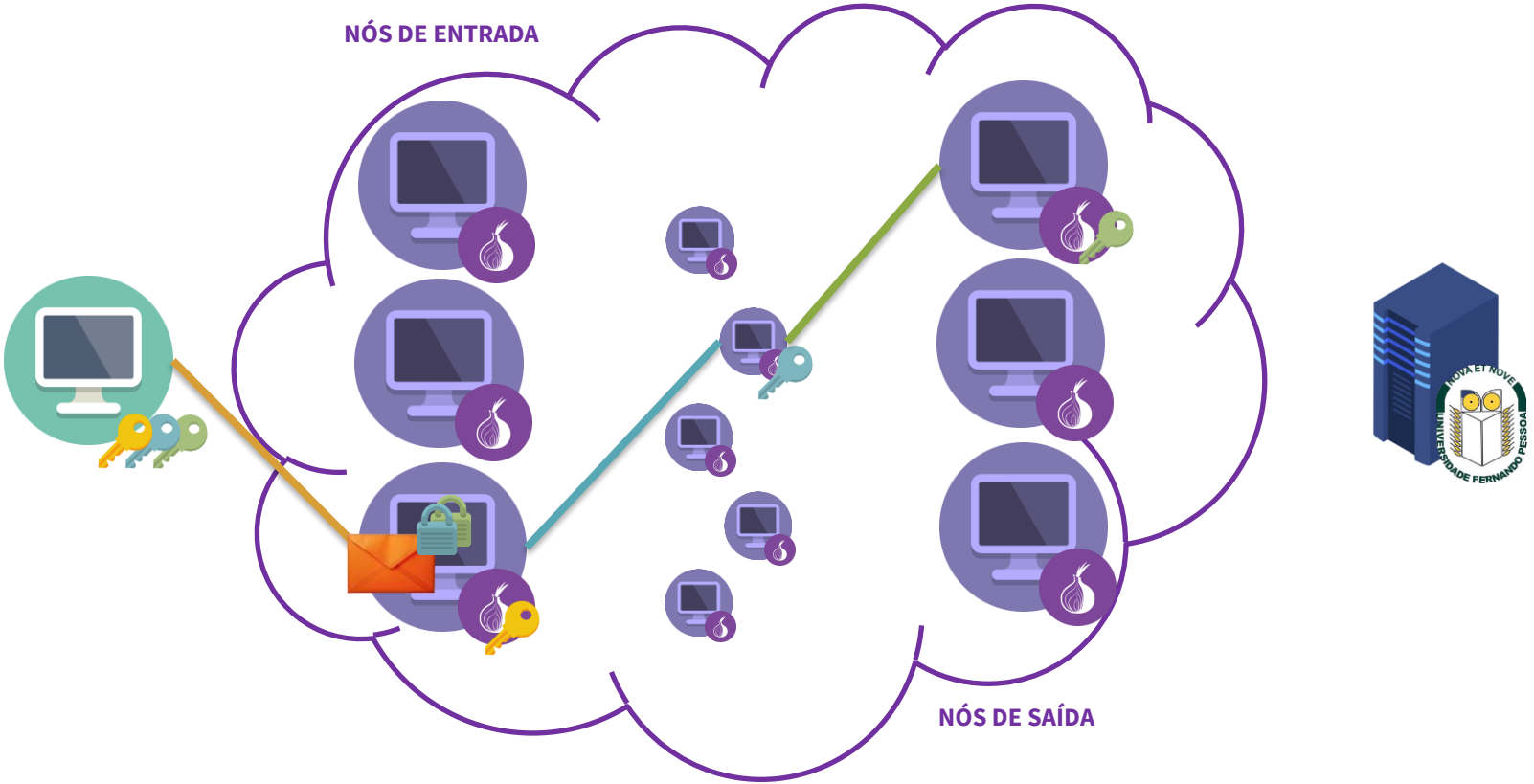
TOR



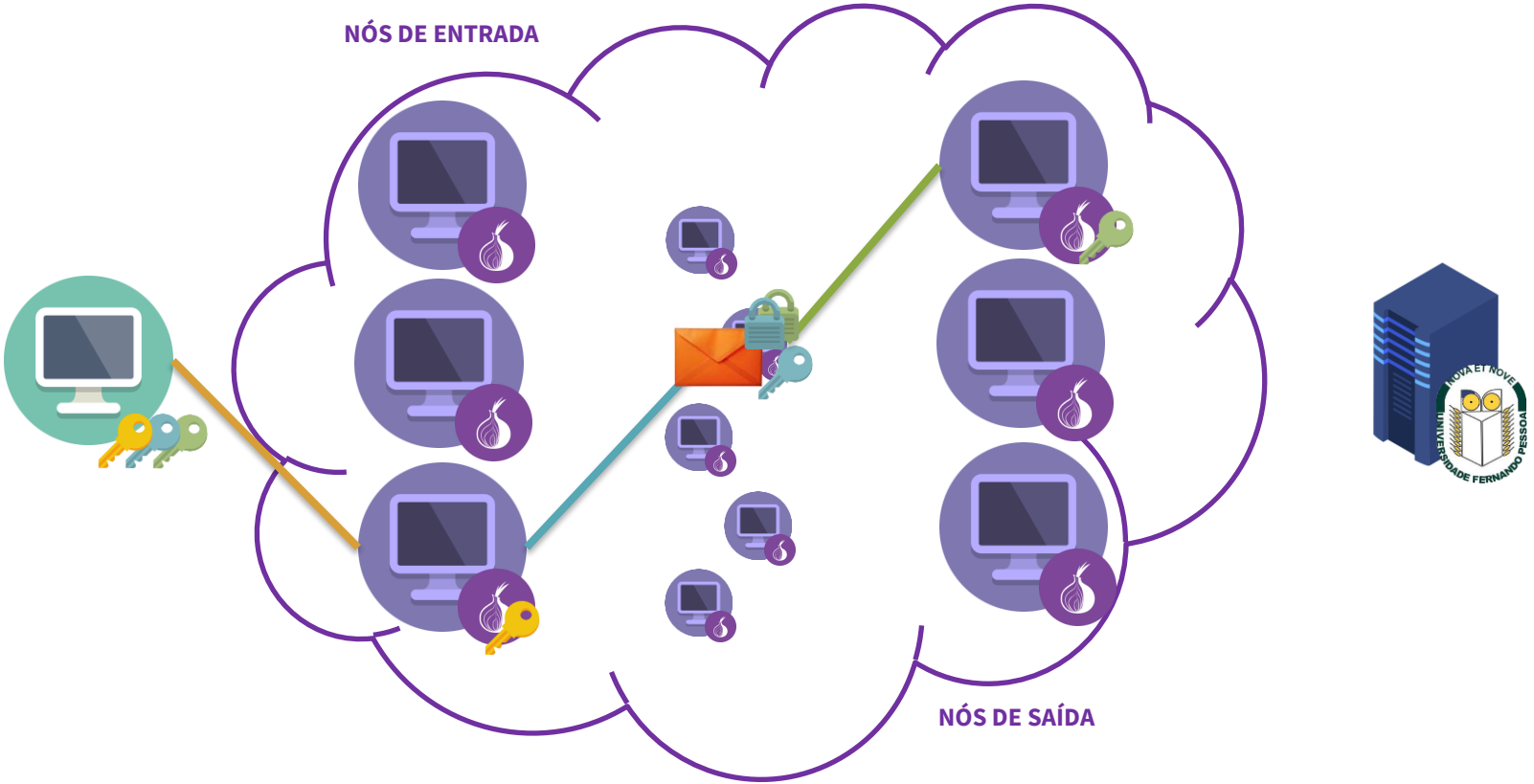
TOR



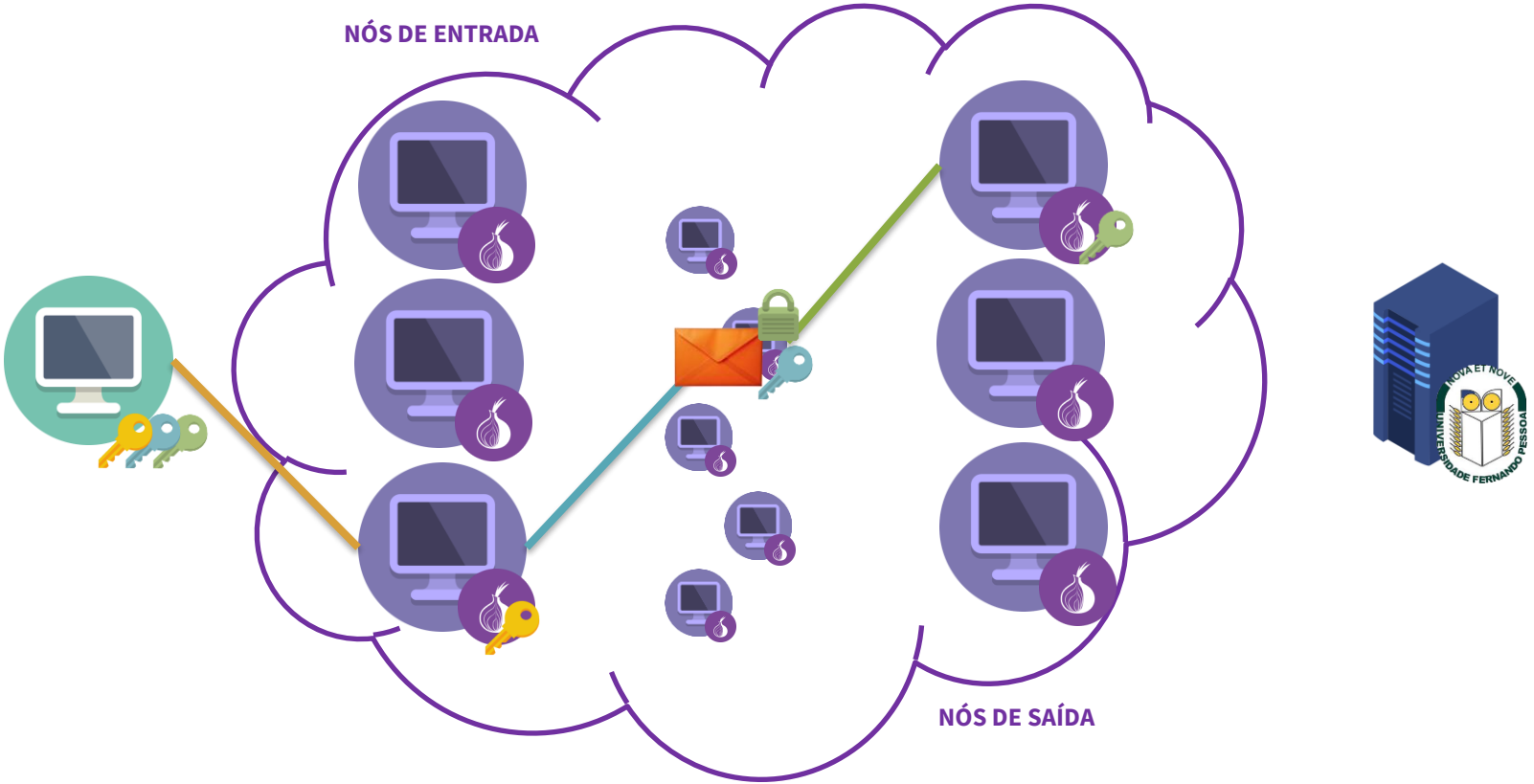
TOR



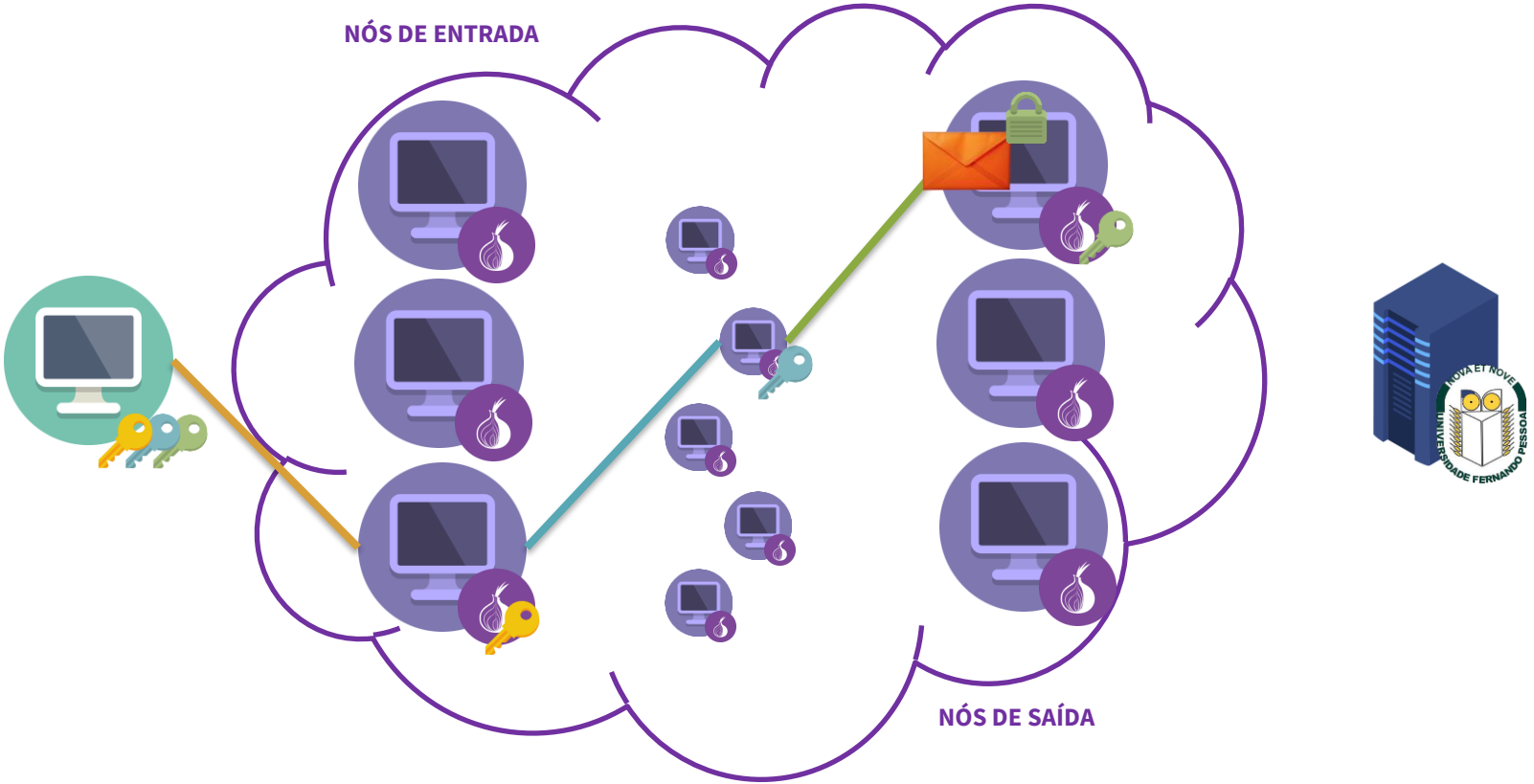
TOR



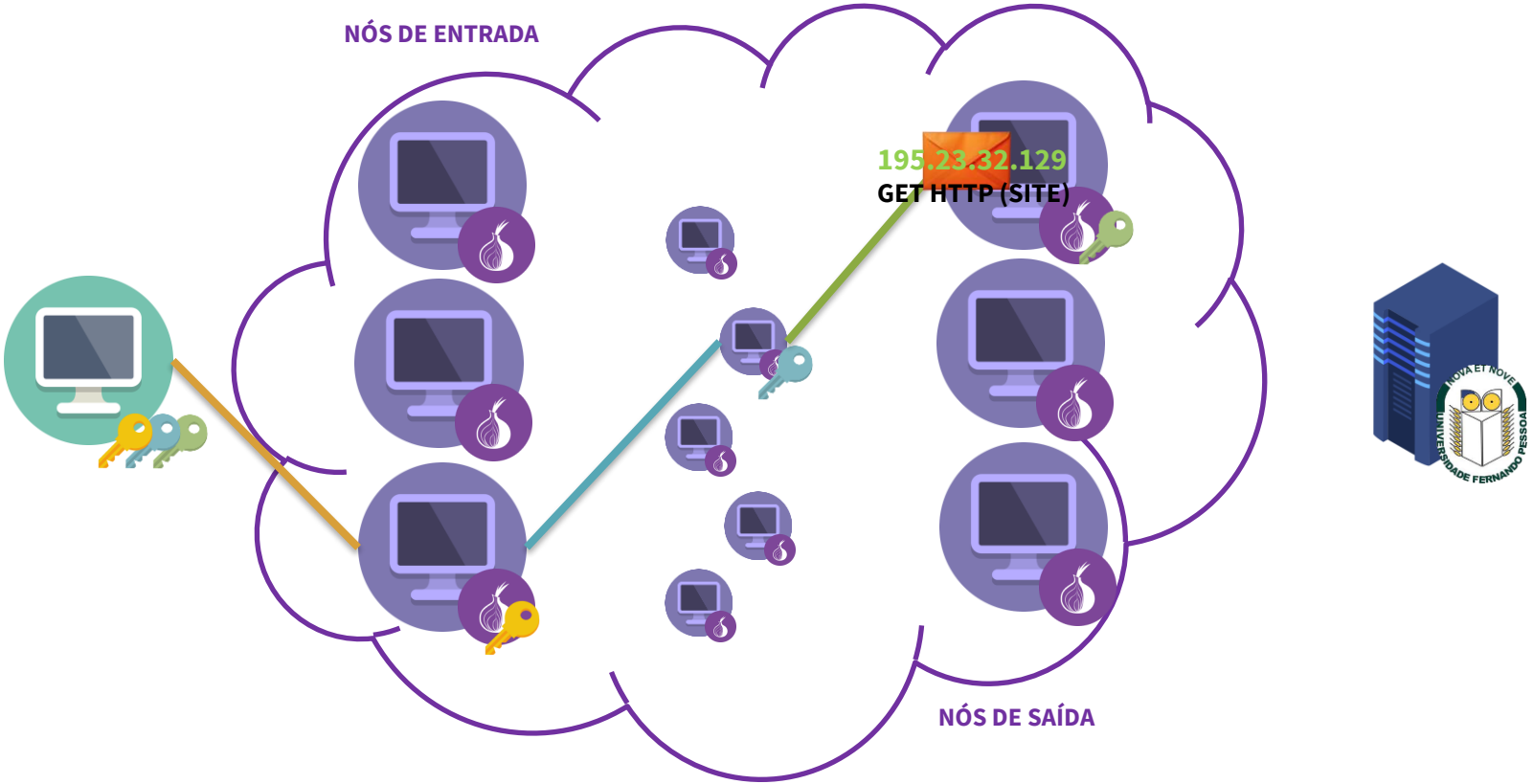
TOR



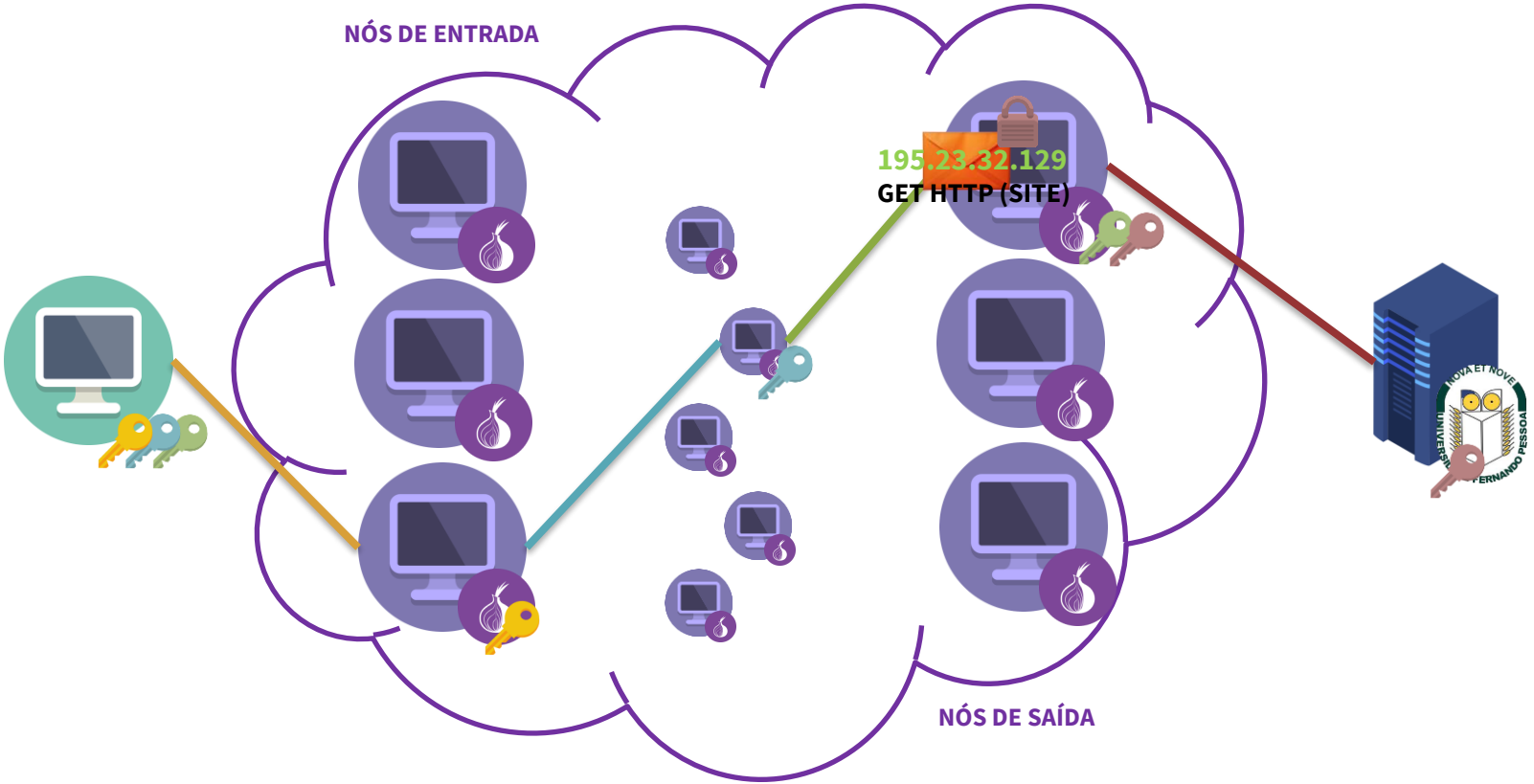
TOR



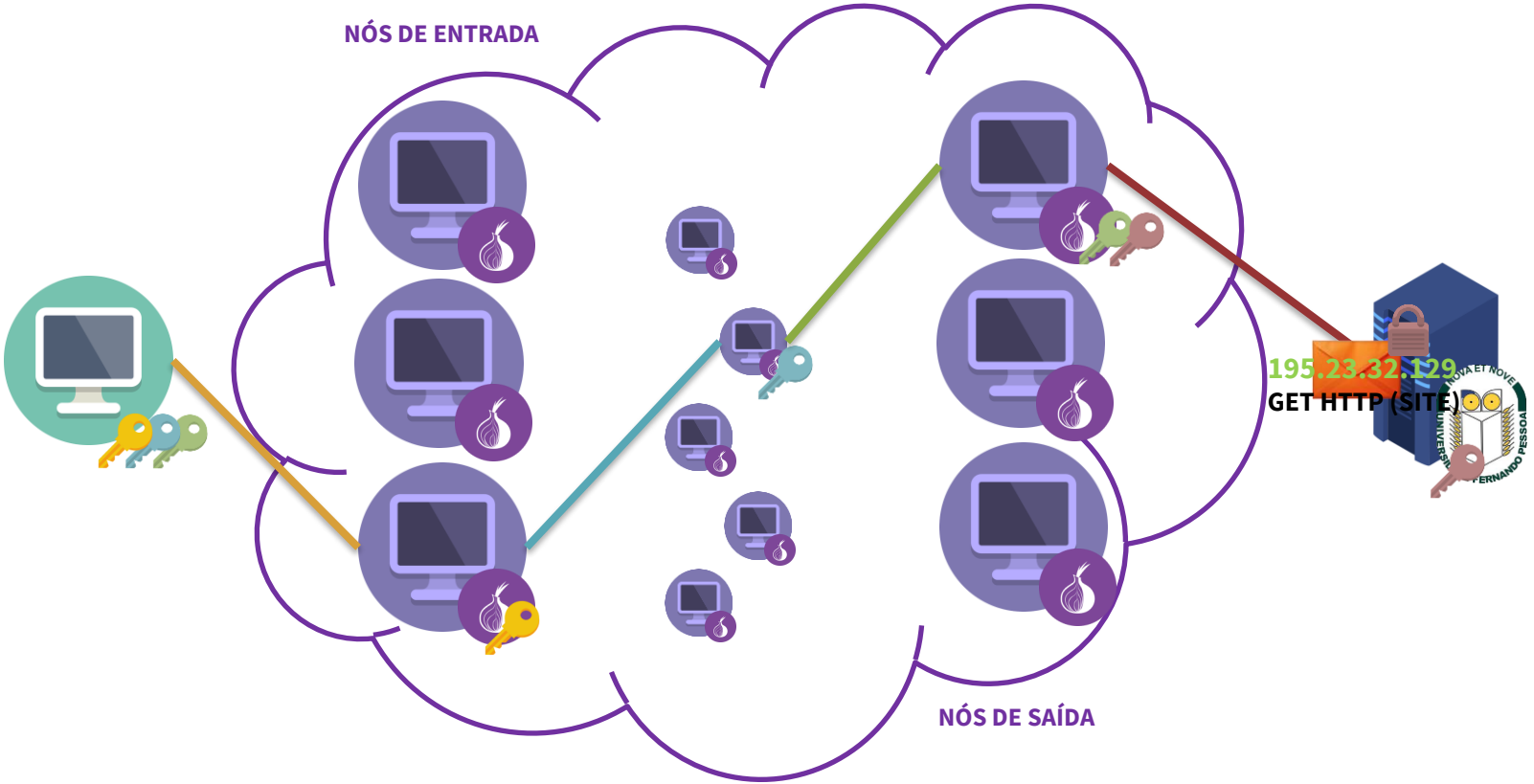
TOR



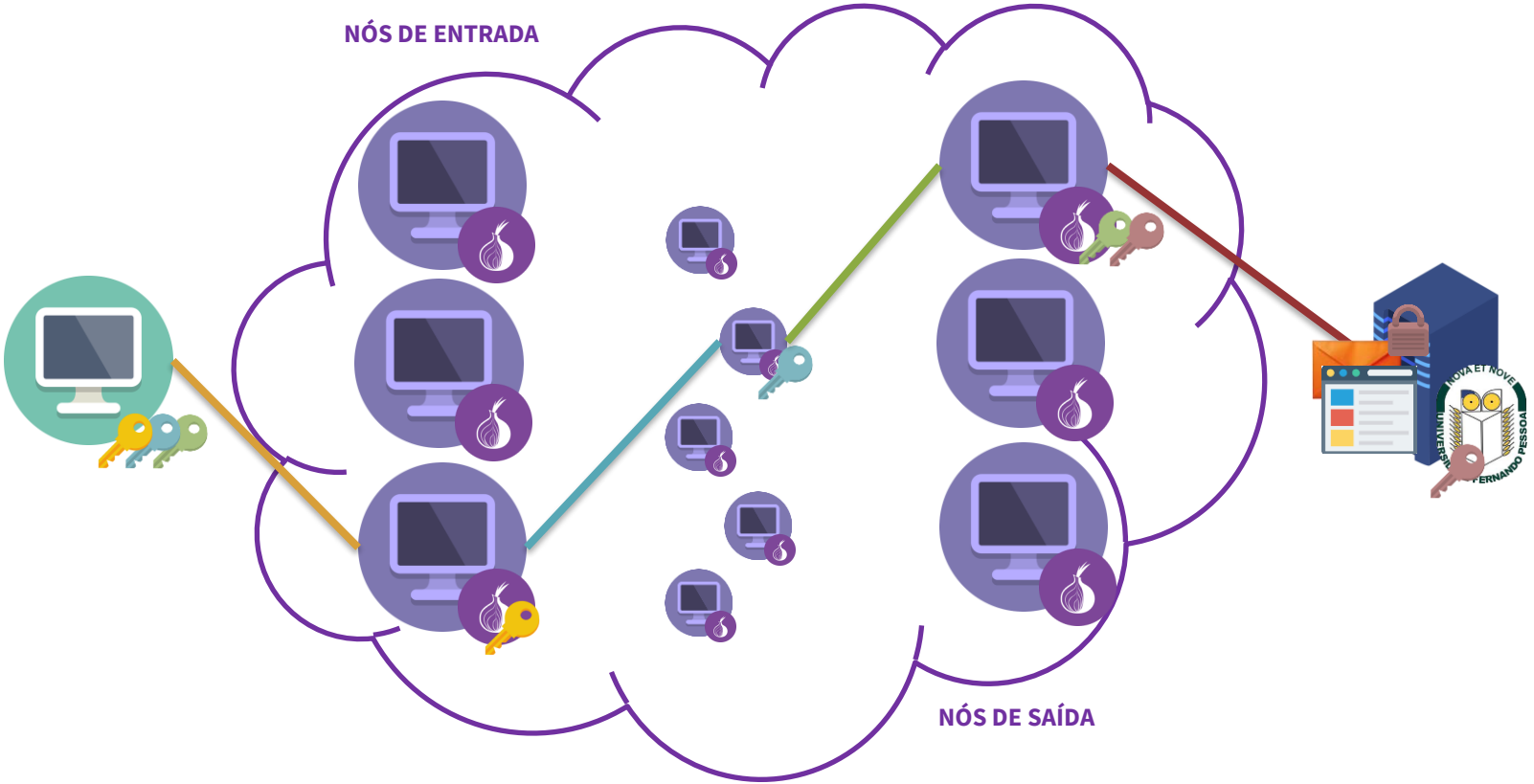
TOR



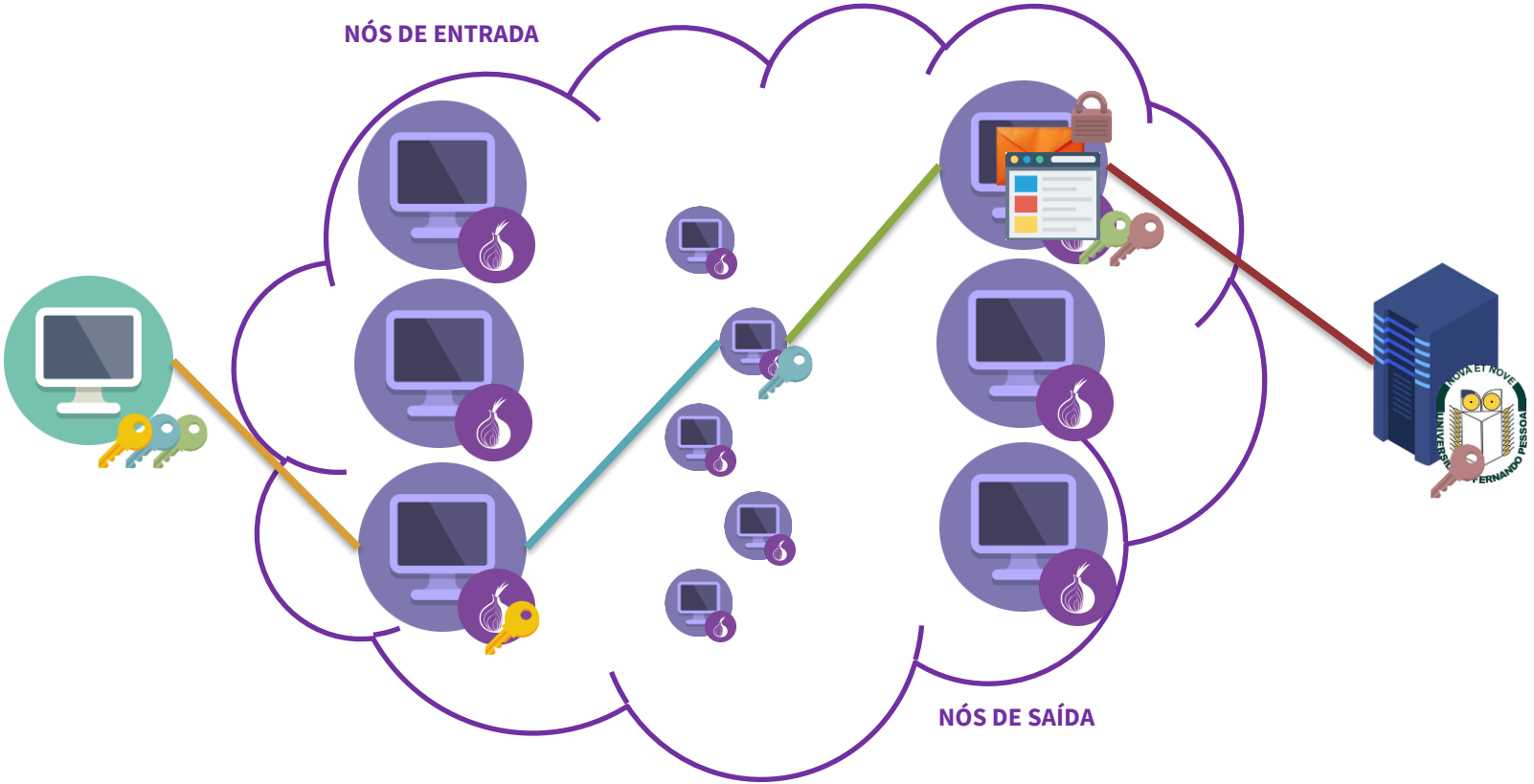
TOR



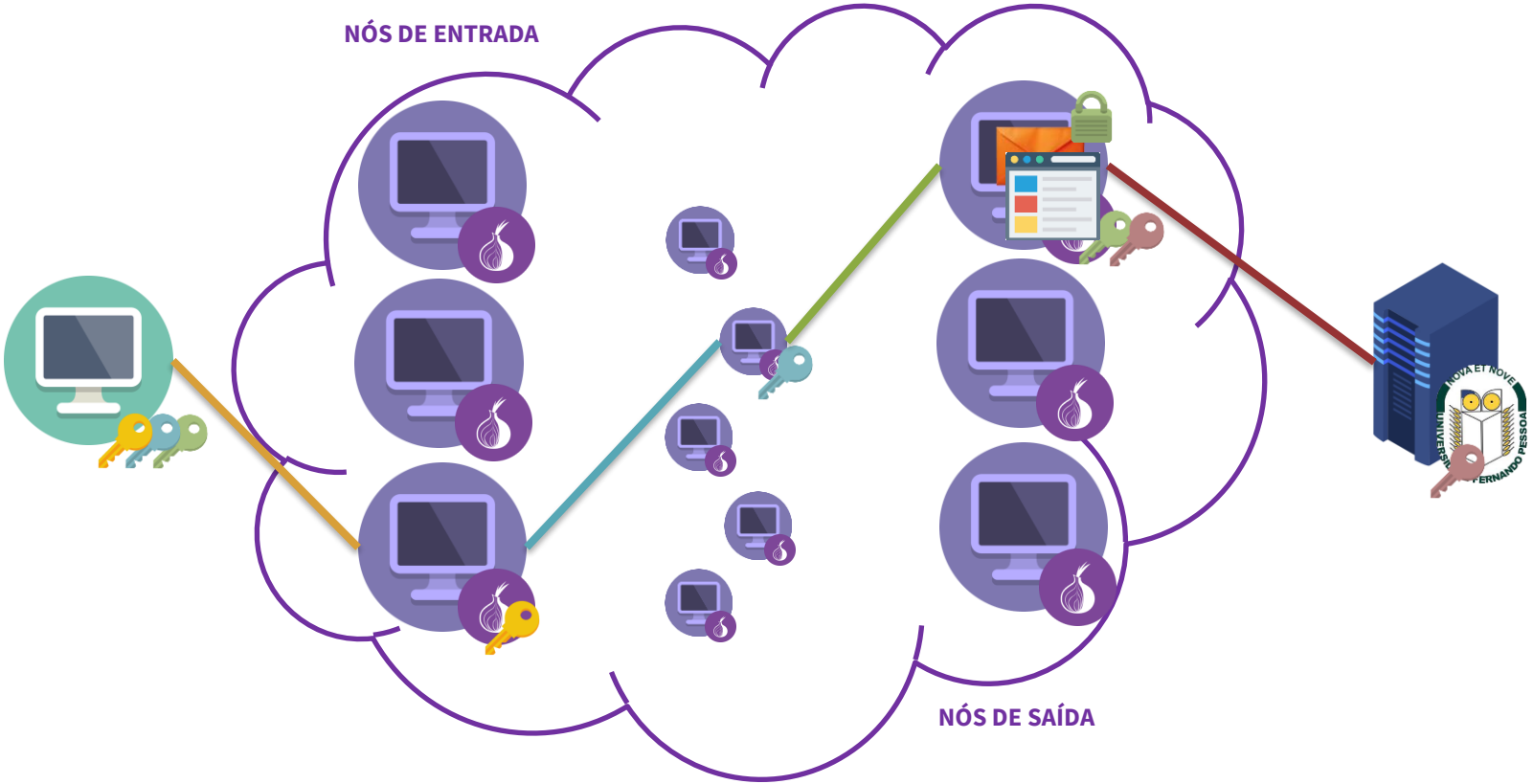
TOR



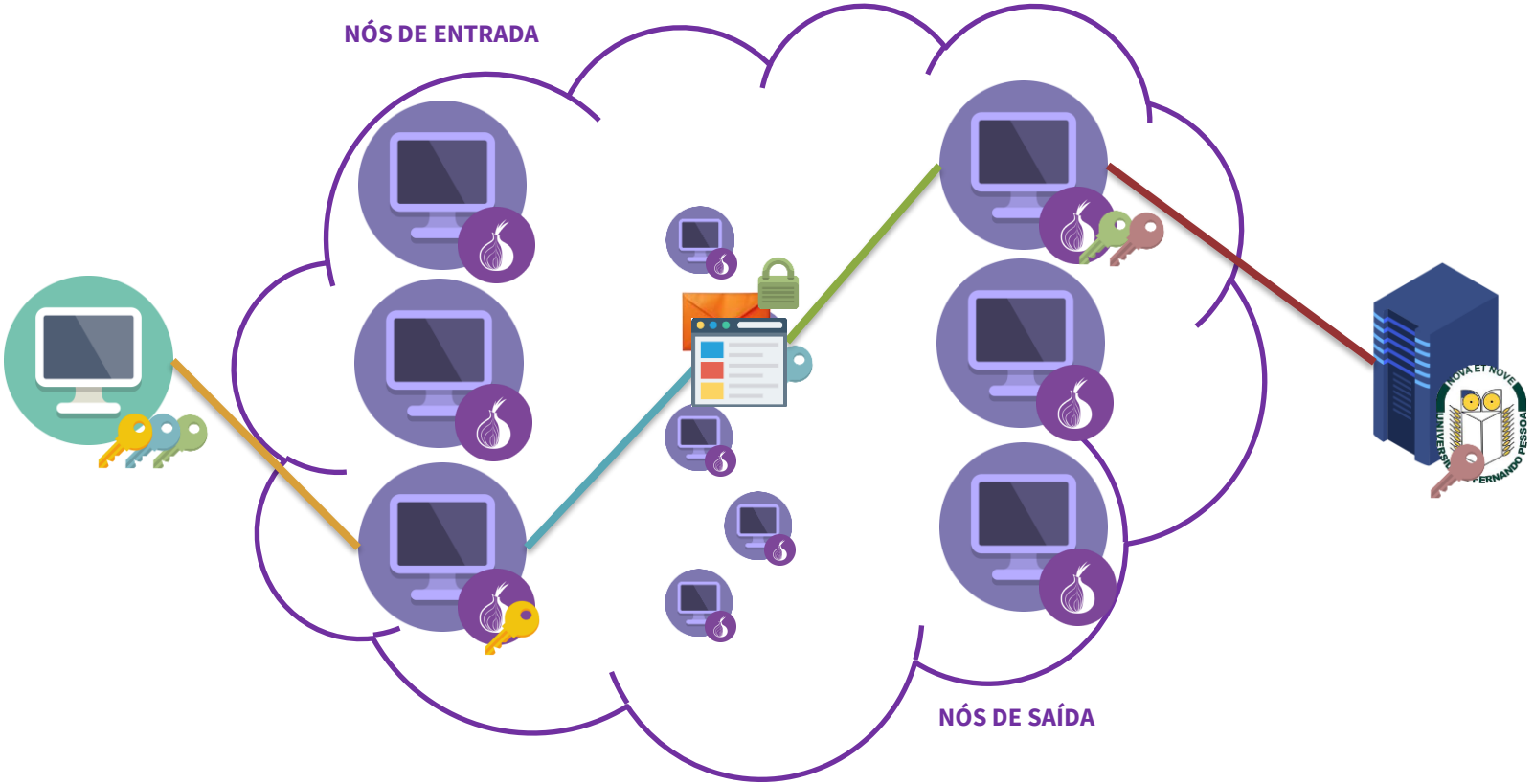
TOR



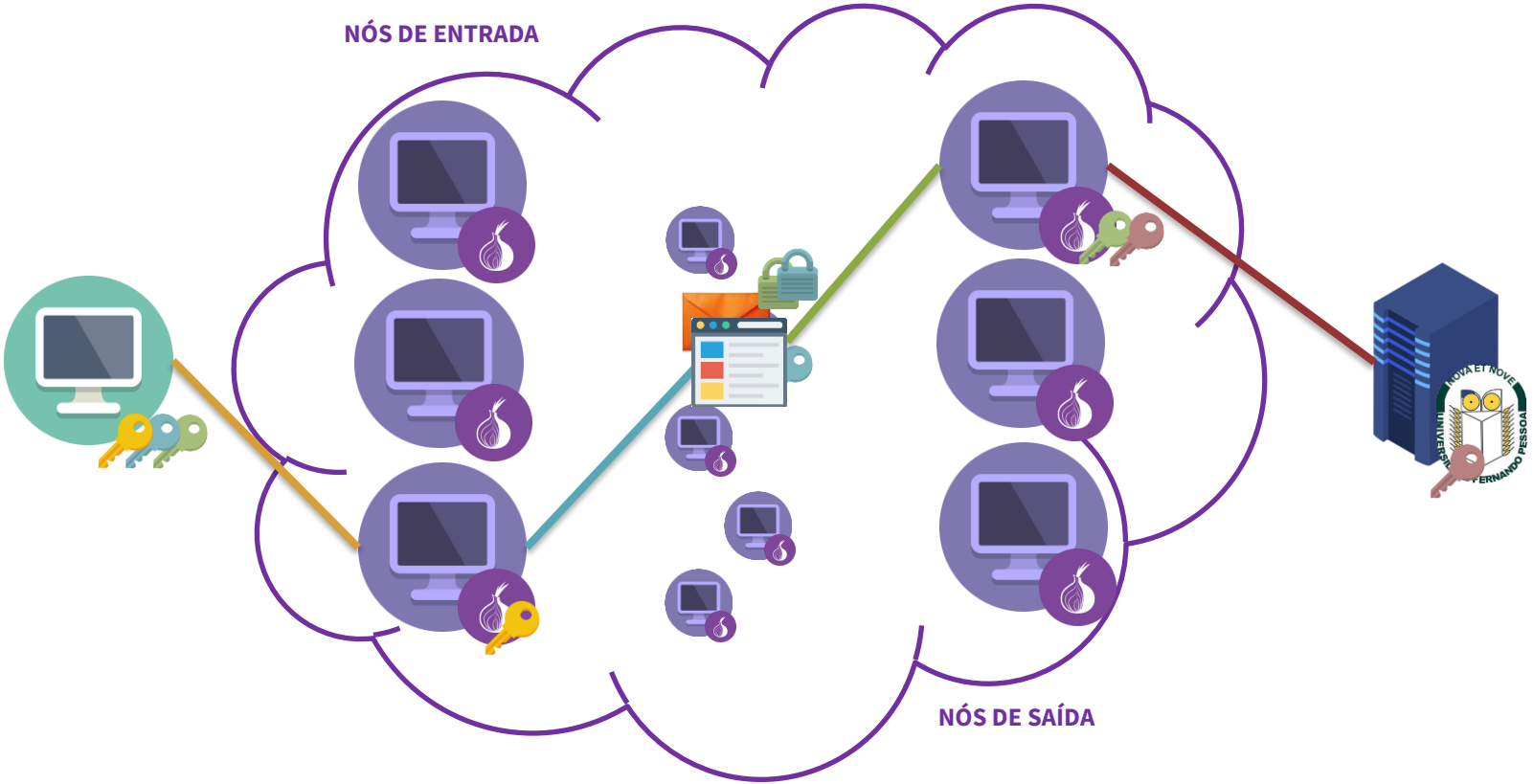
TOR



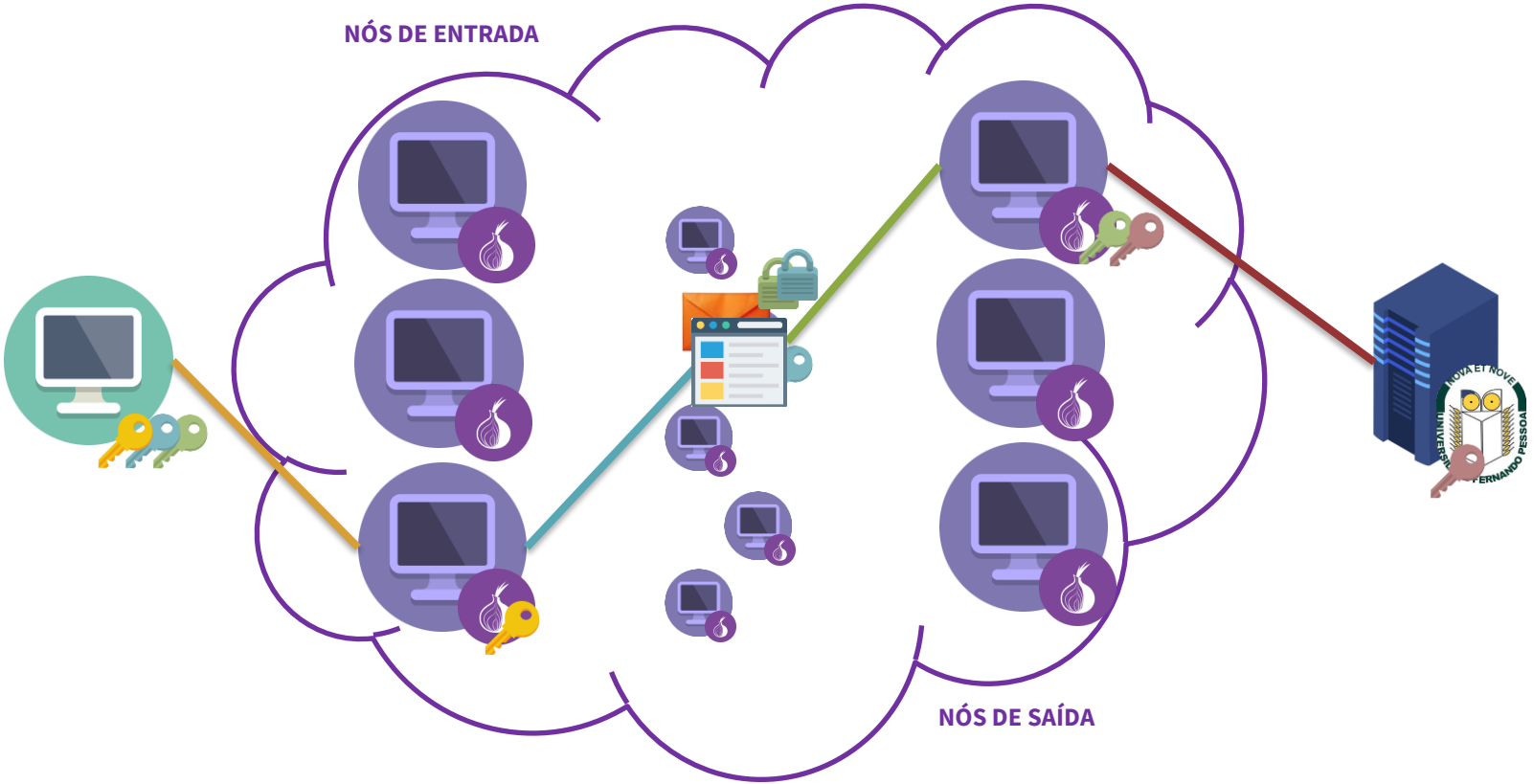
TOR



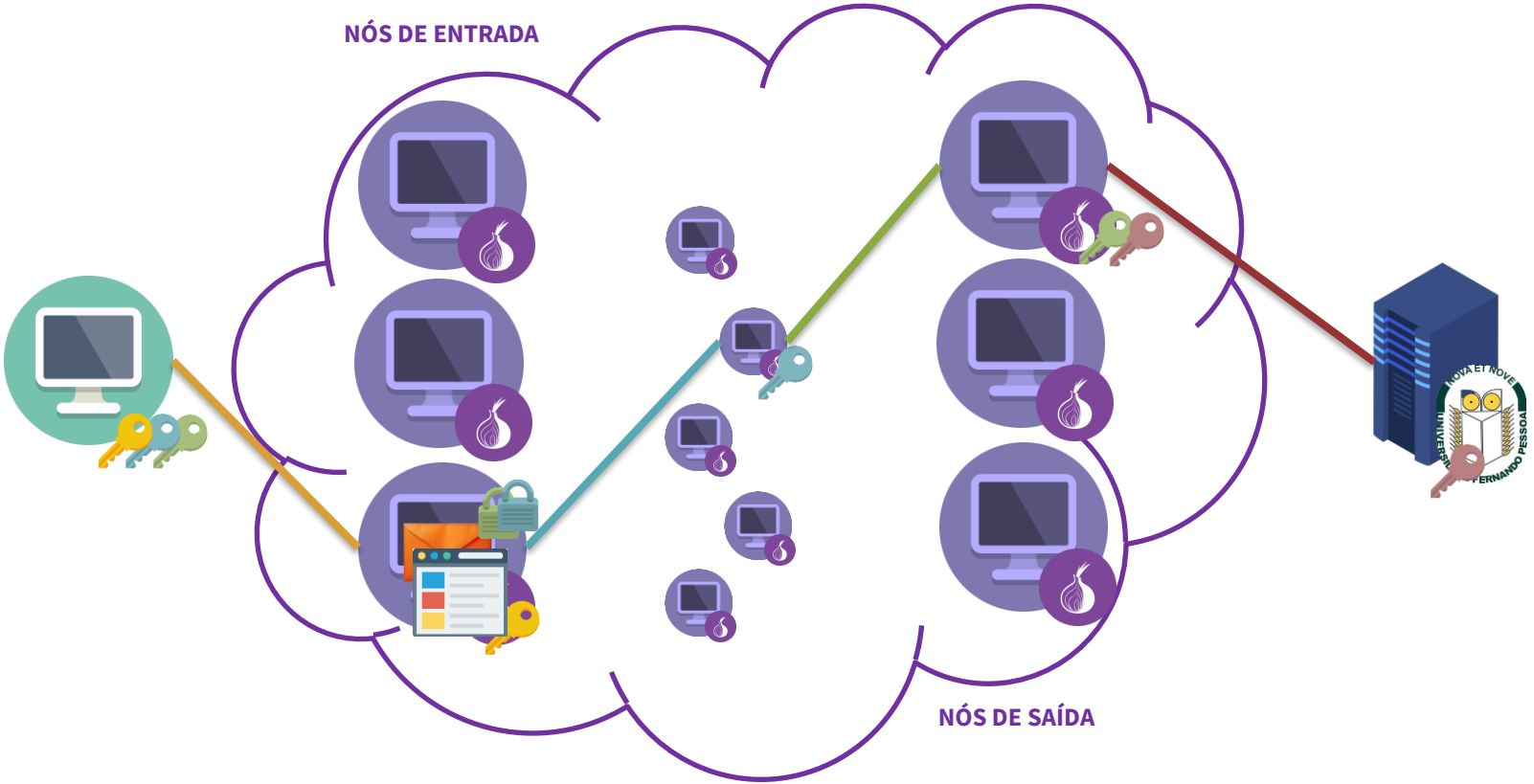
TOR



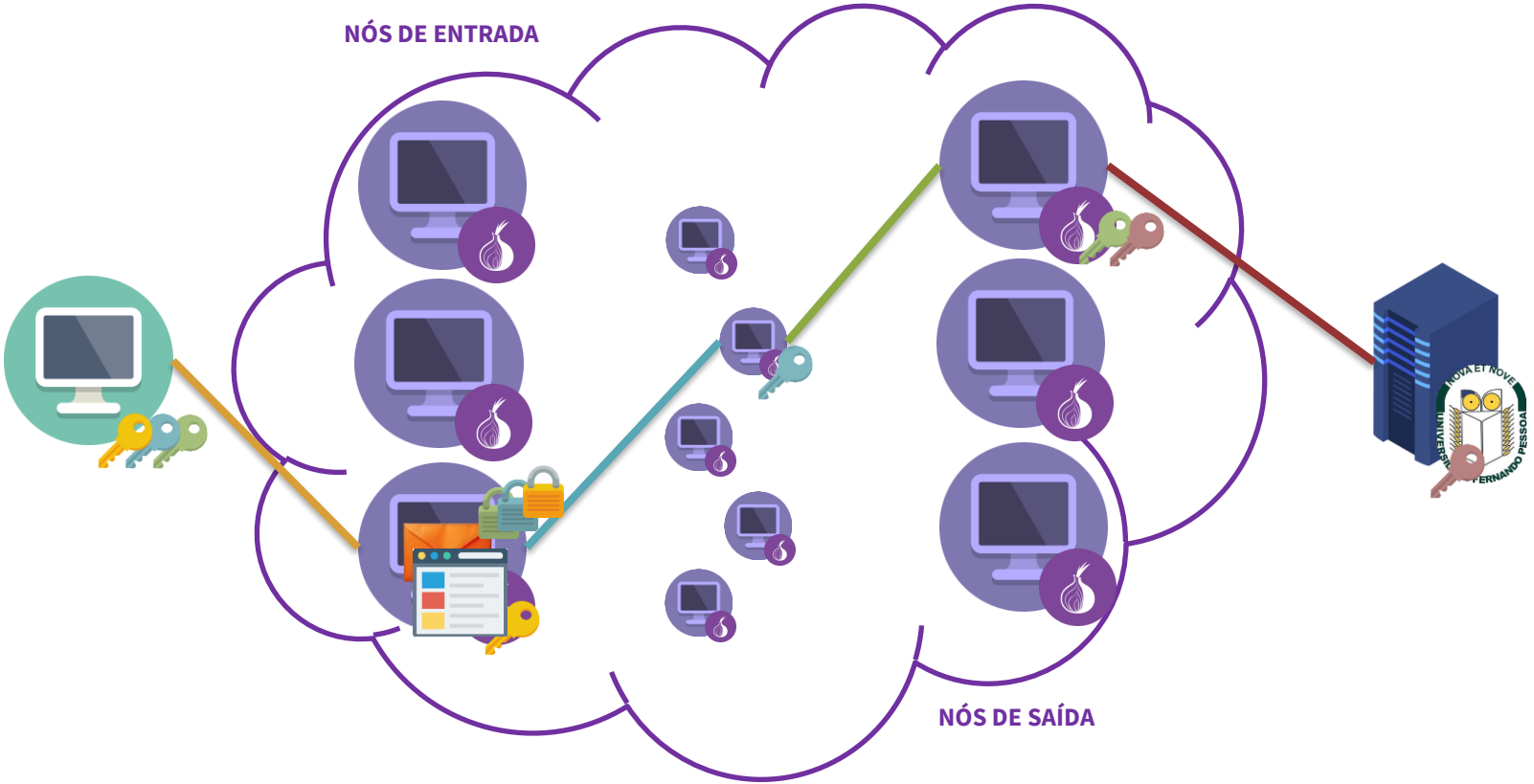
TOR



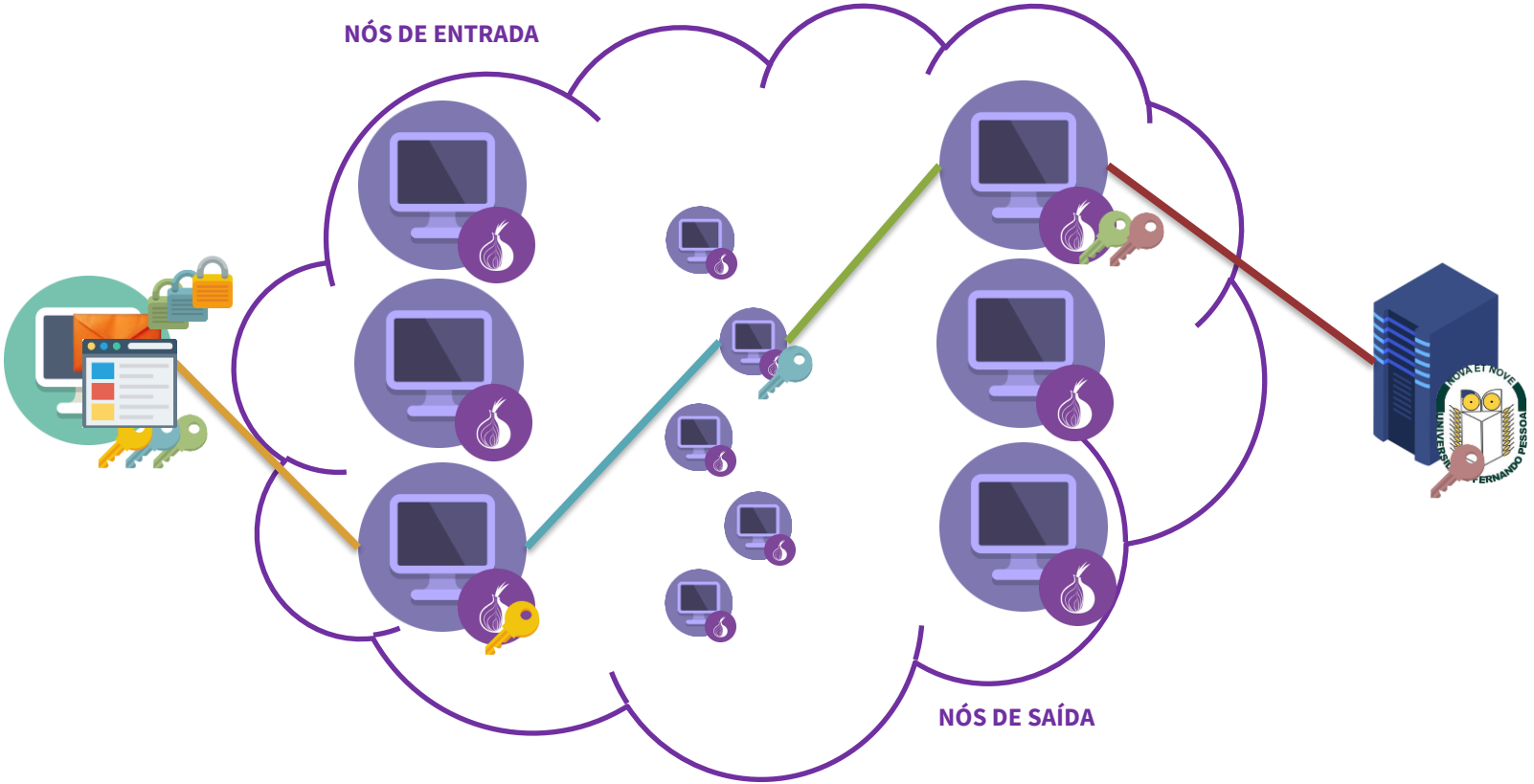
TOR



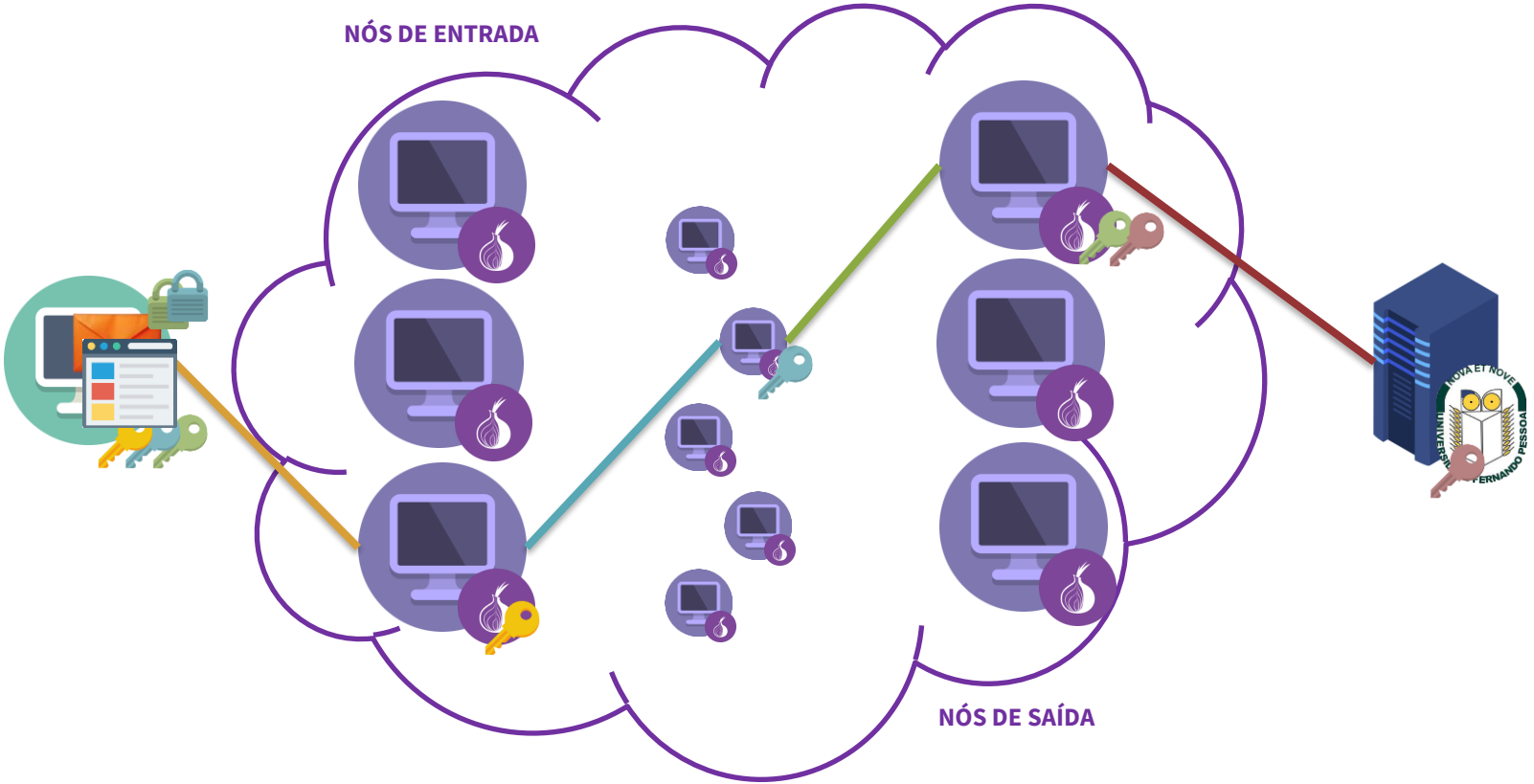
TOR



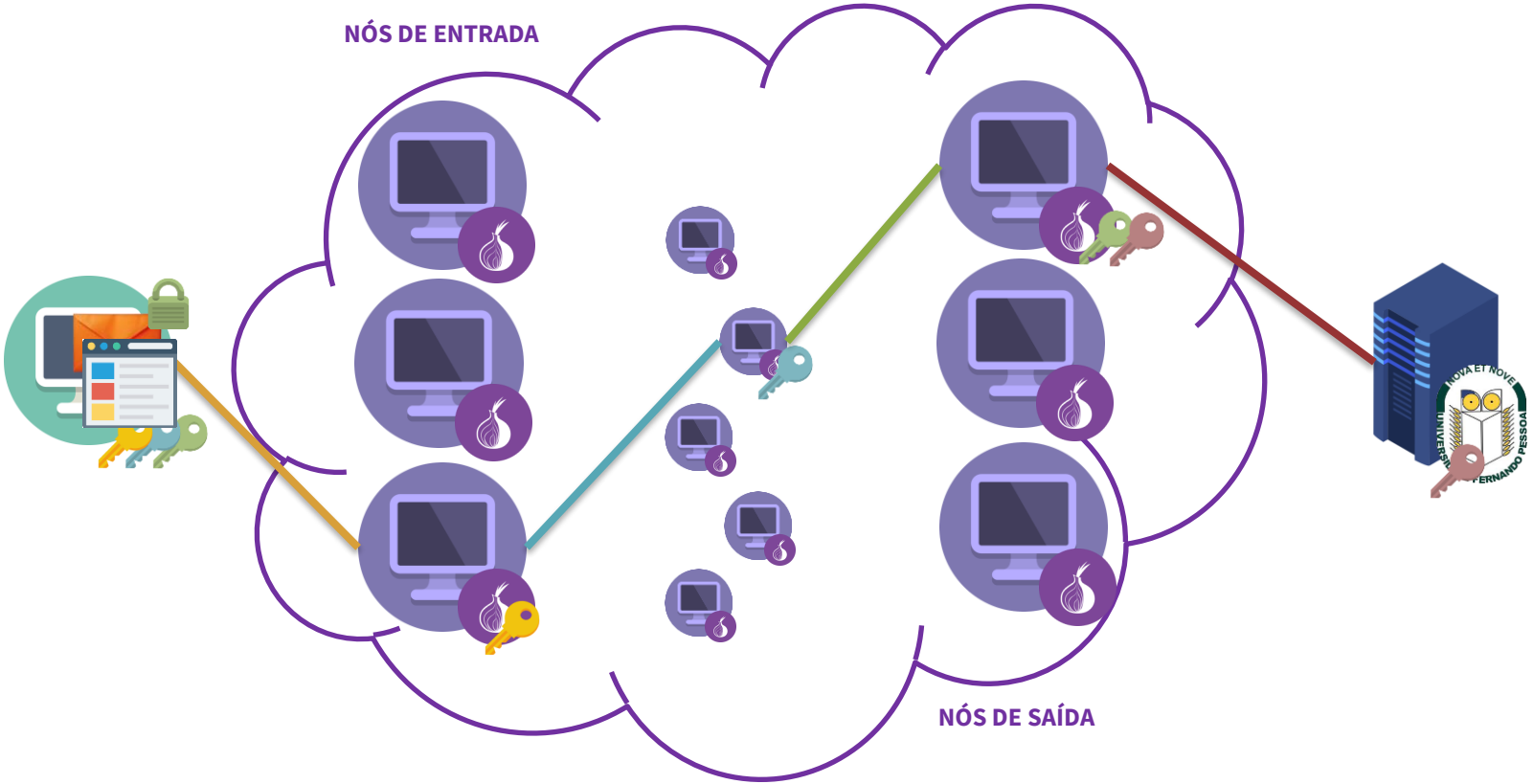
TOR



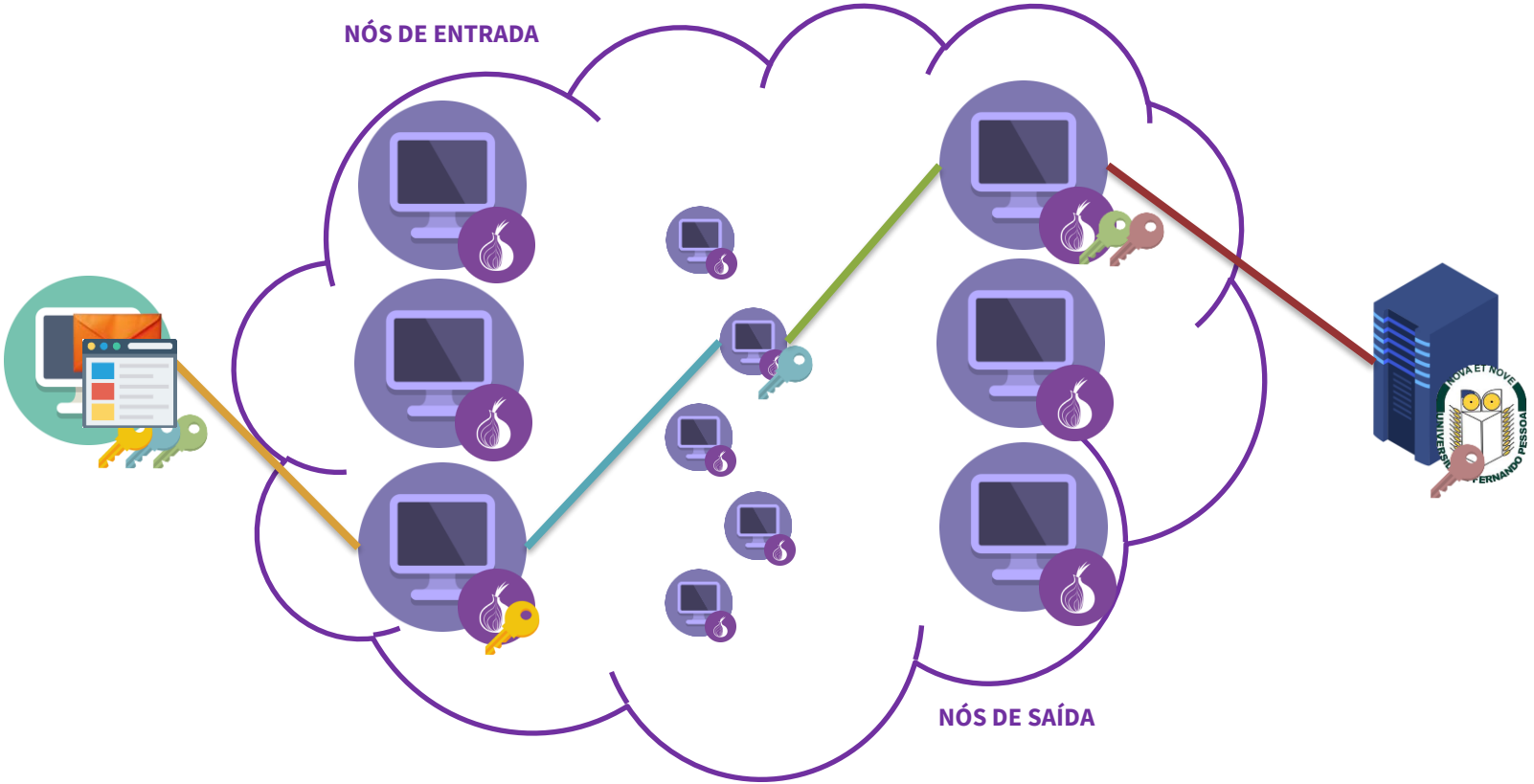
TOR



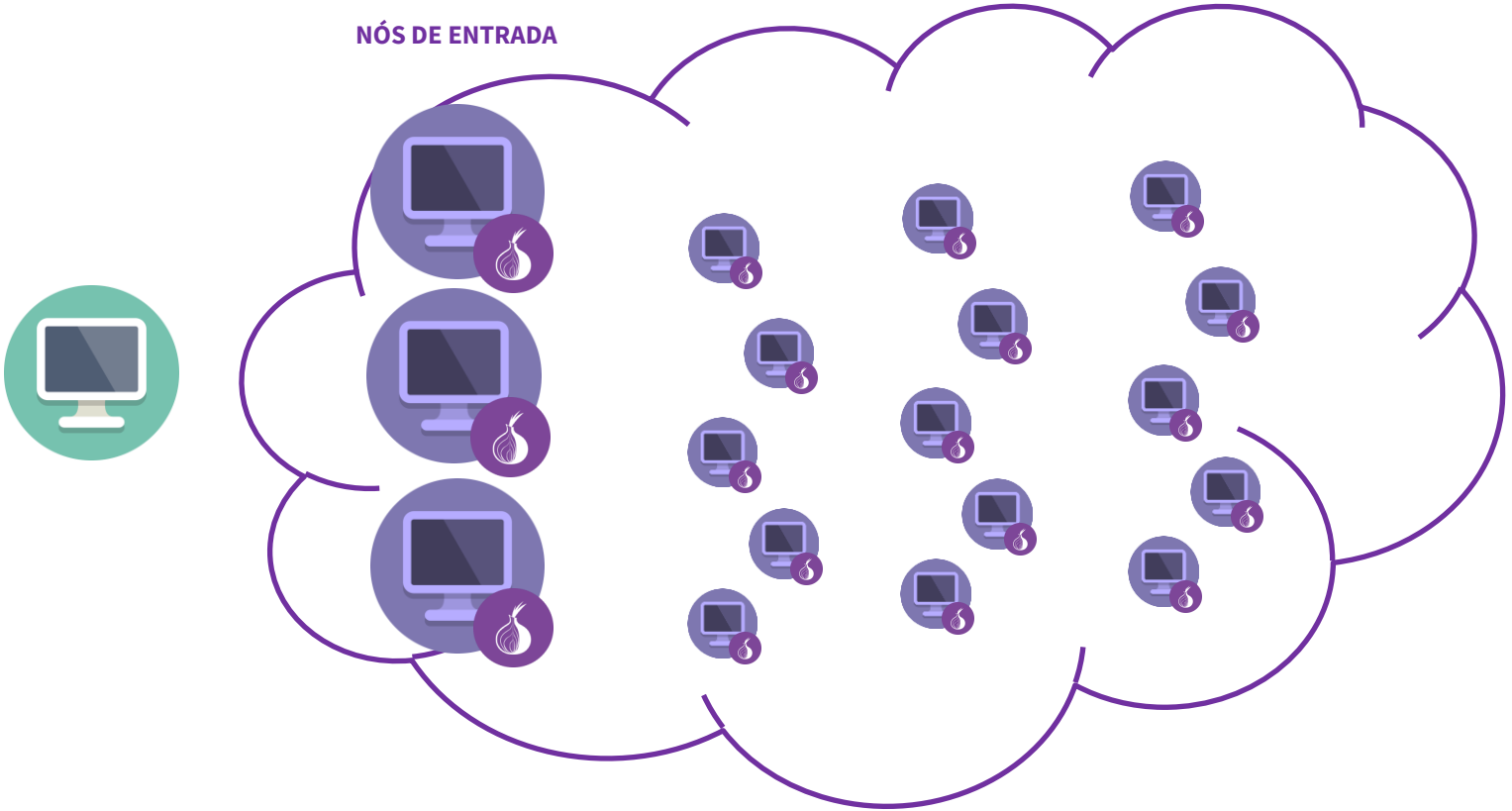
TOR



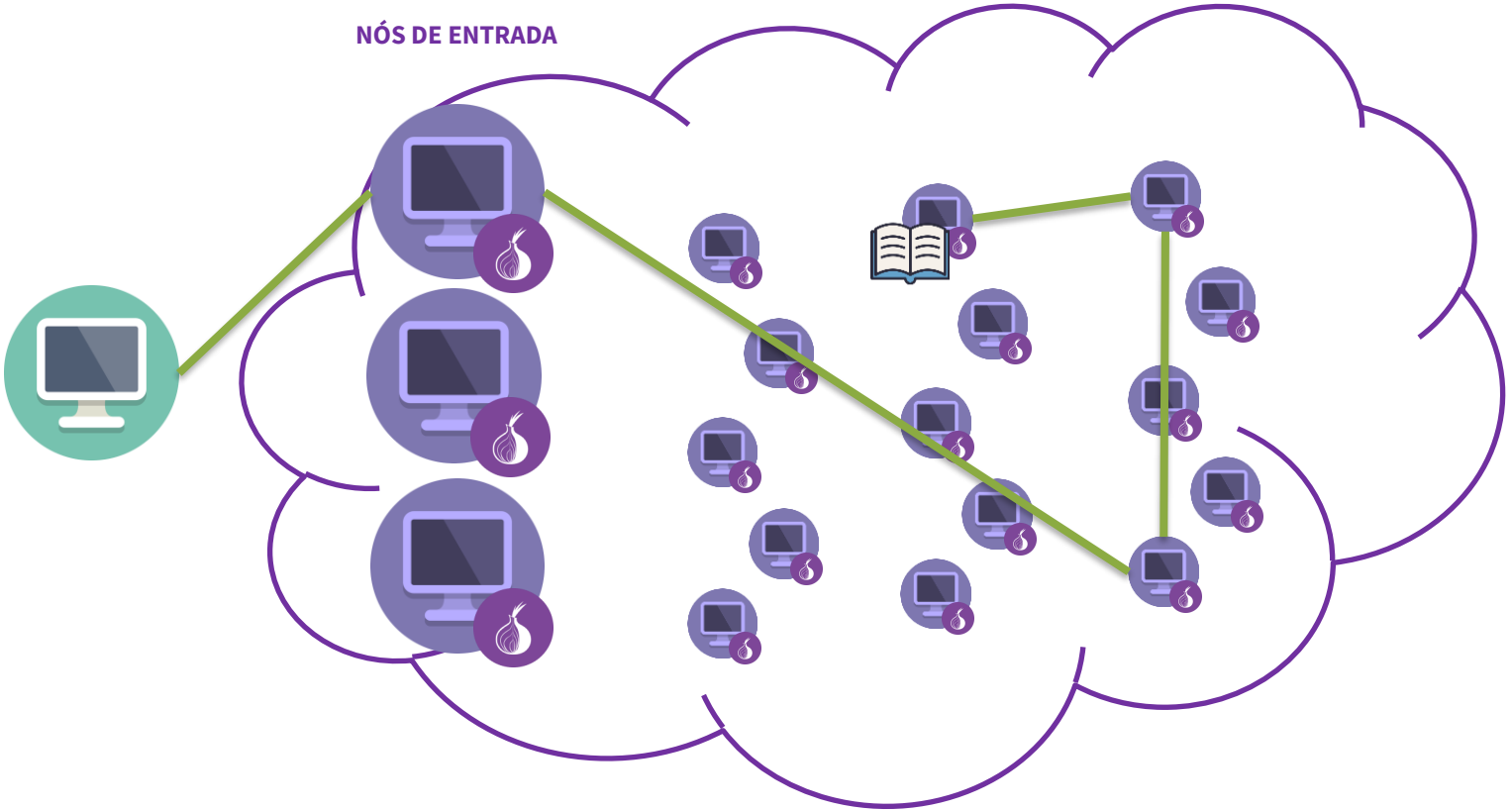
TOR



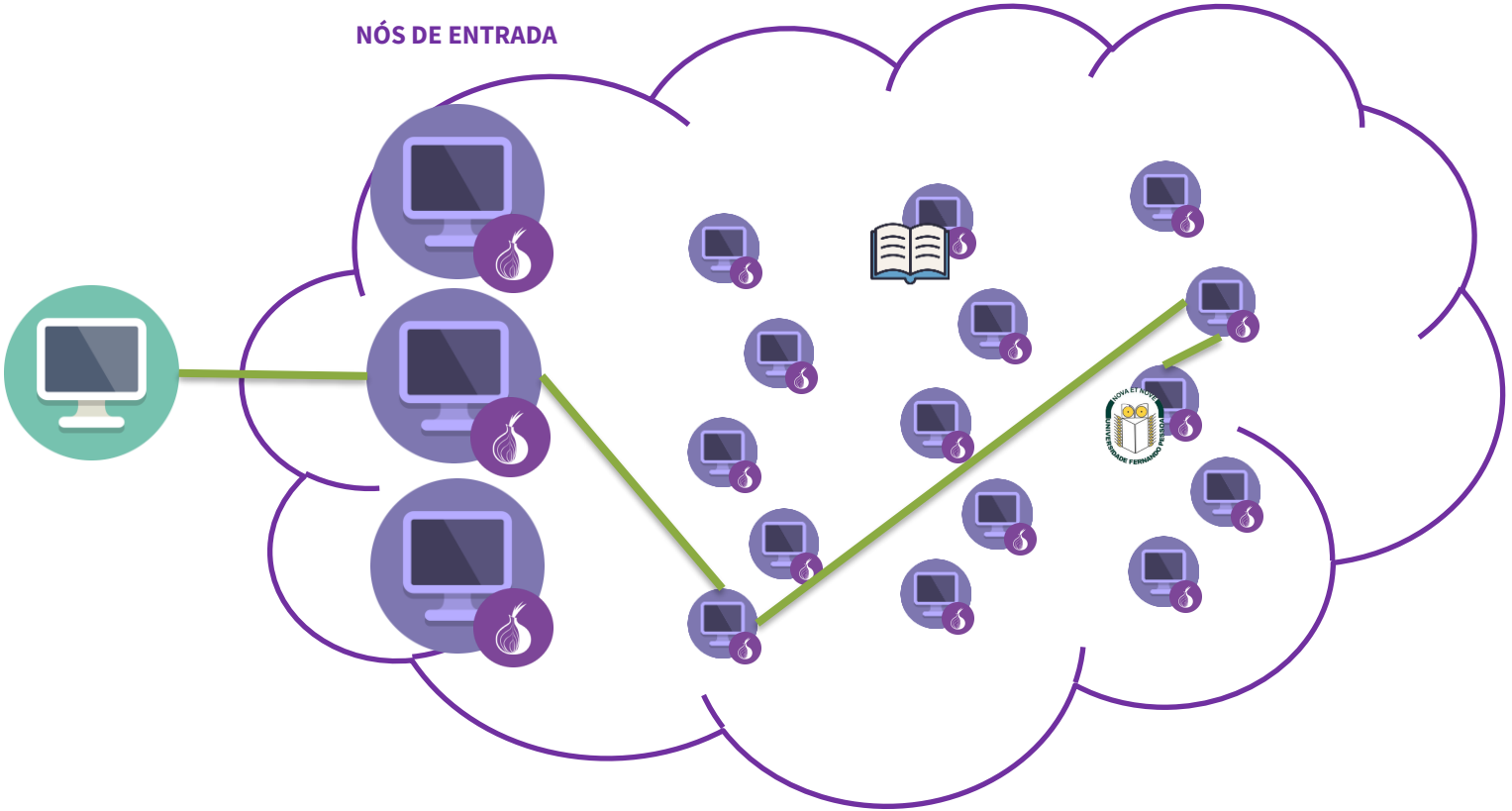
TOR



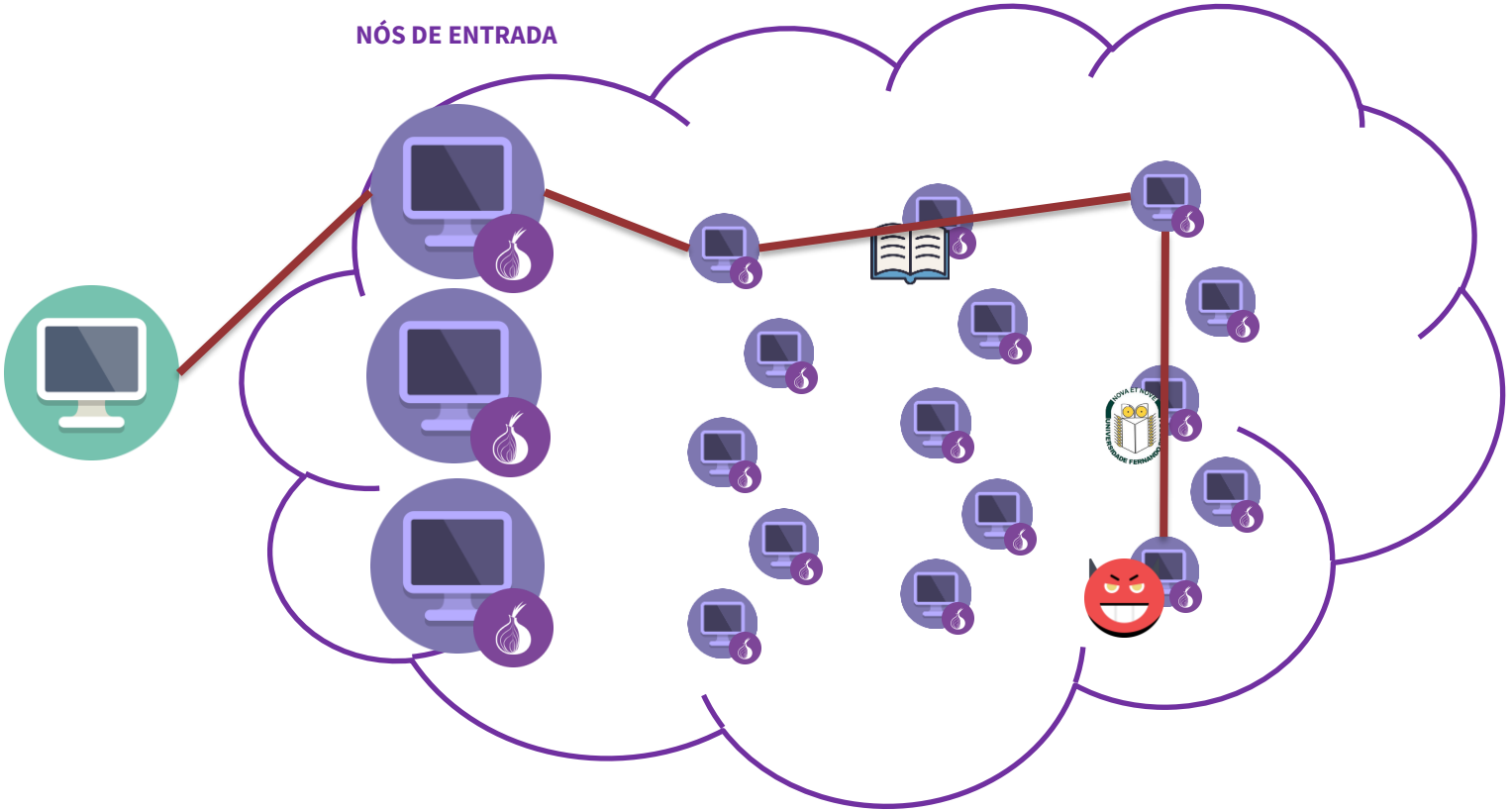
TOR



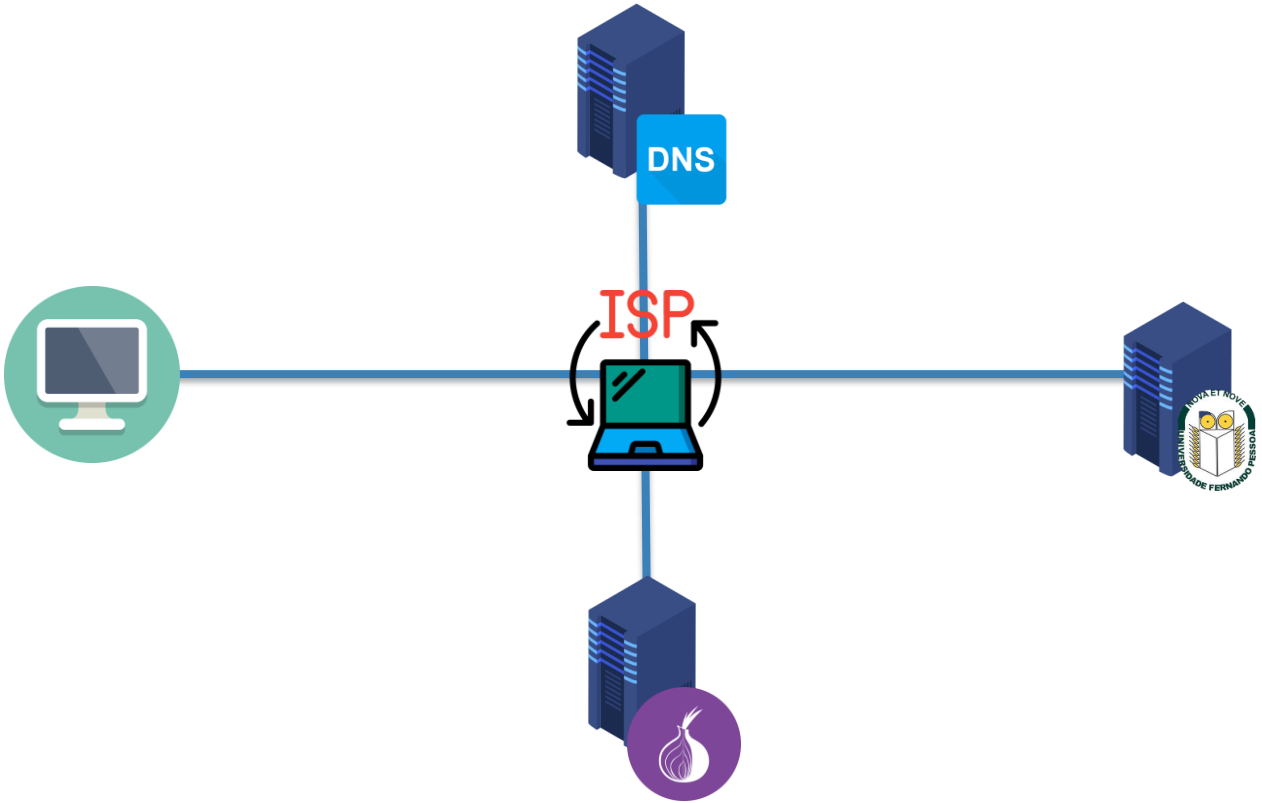
TOR



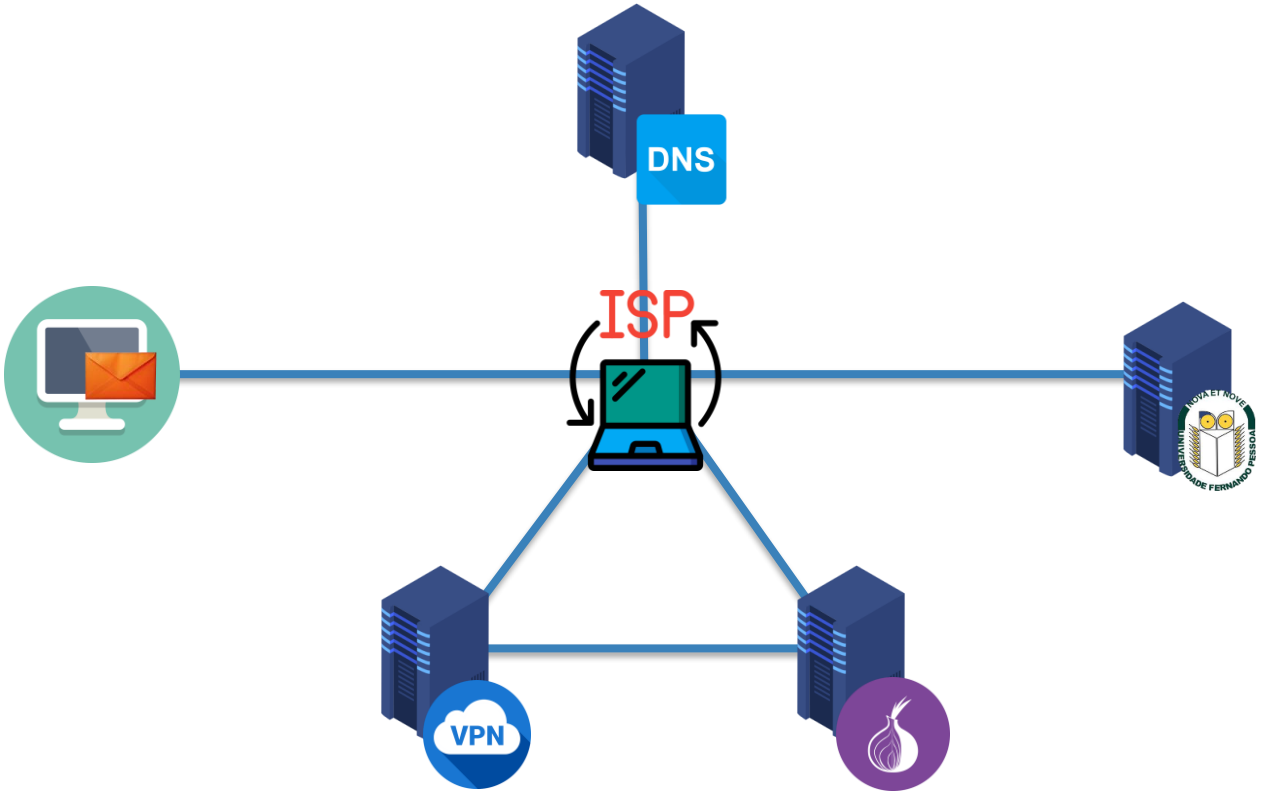
TOR



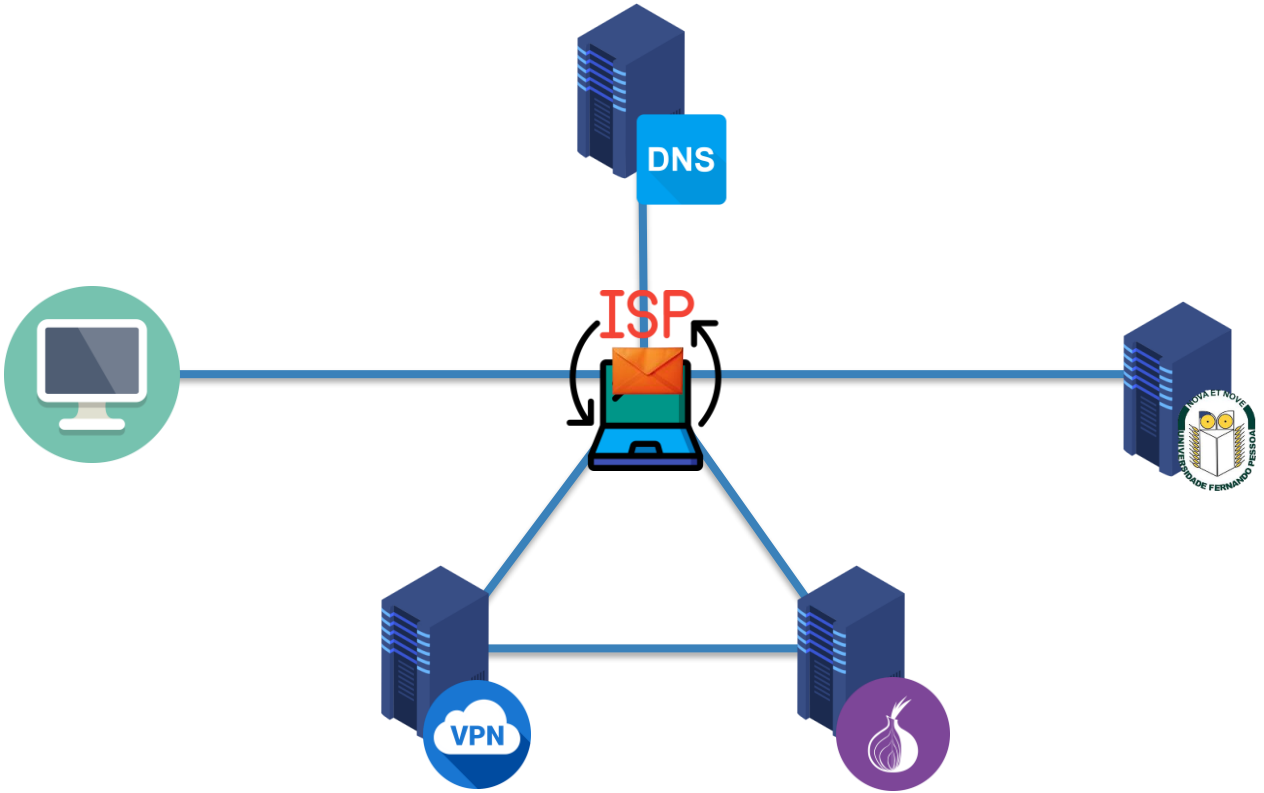
INTERNET COMUM



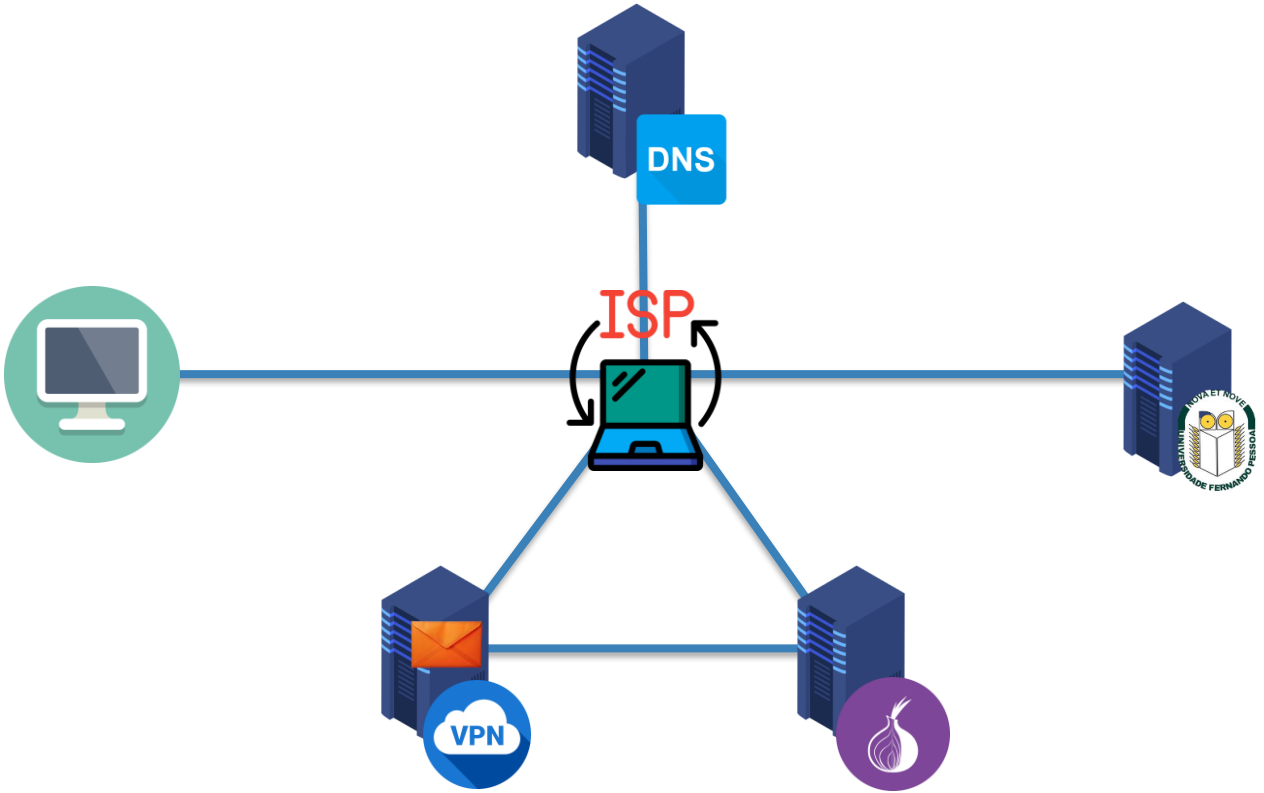
INTERNET COMUM



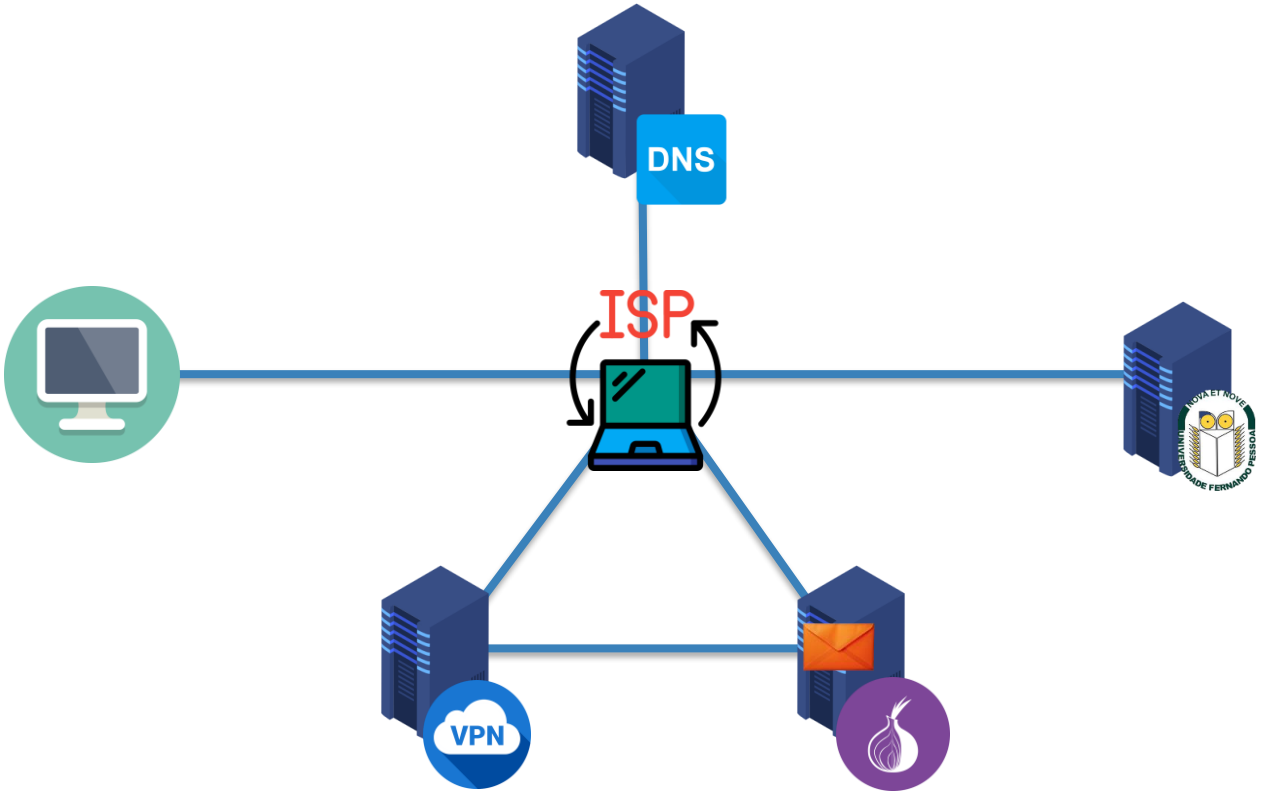
INTERNET COMUM



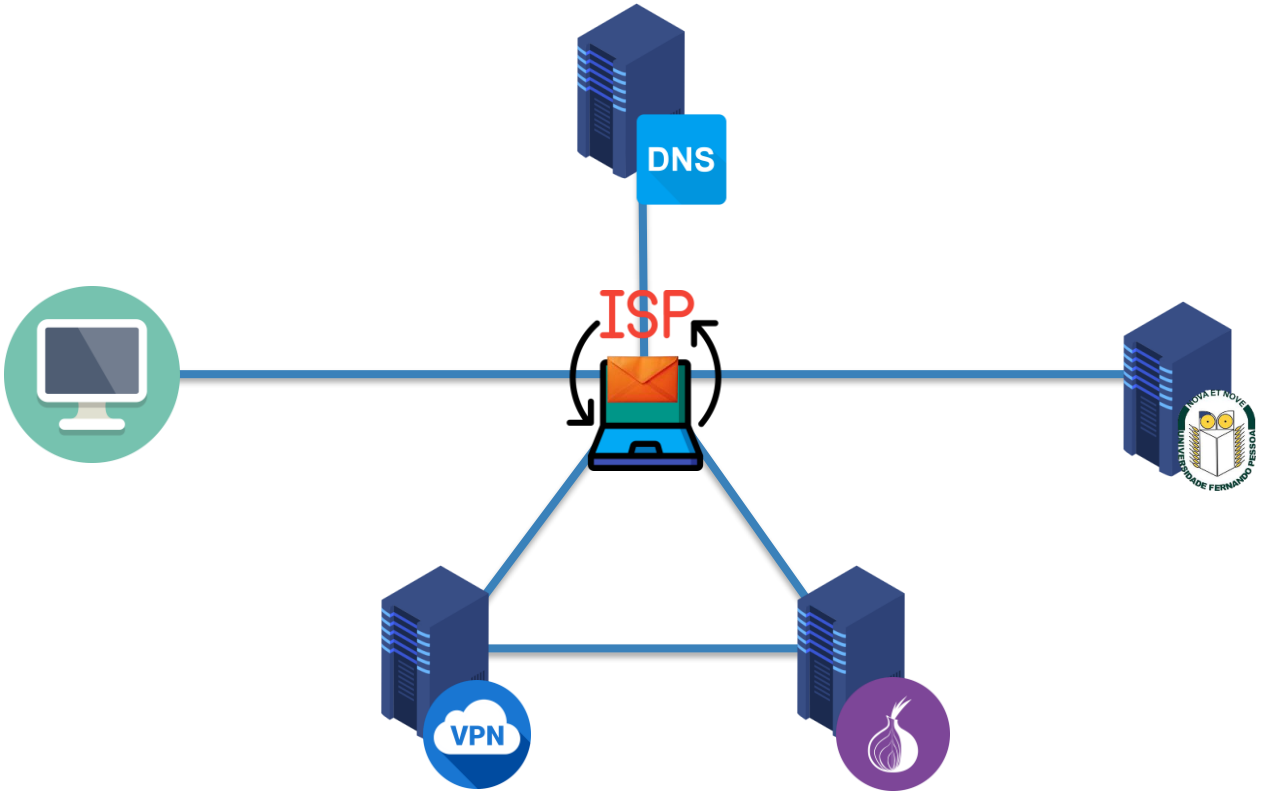
INTERNET COMUM



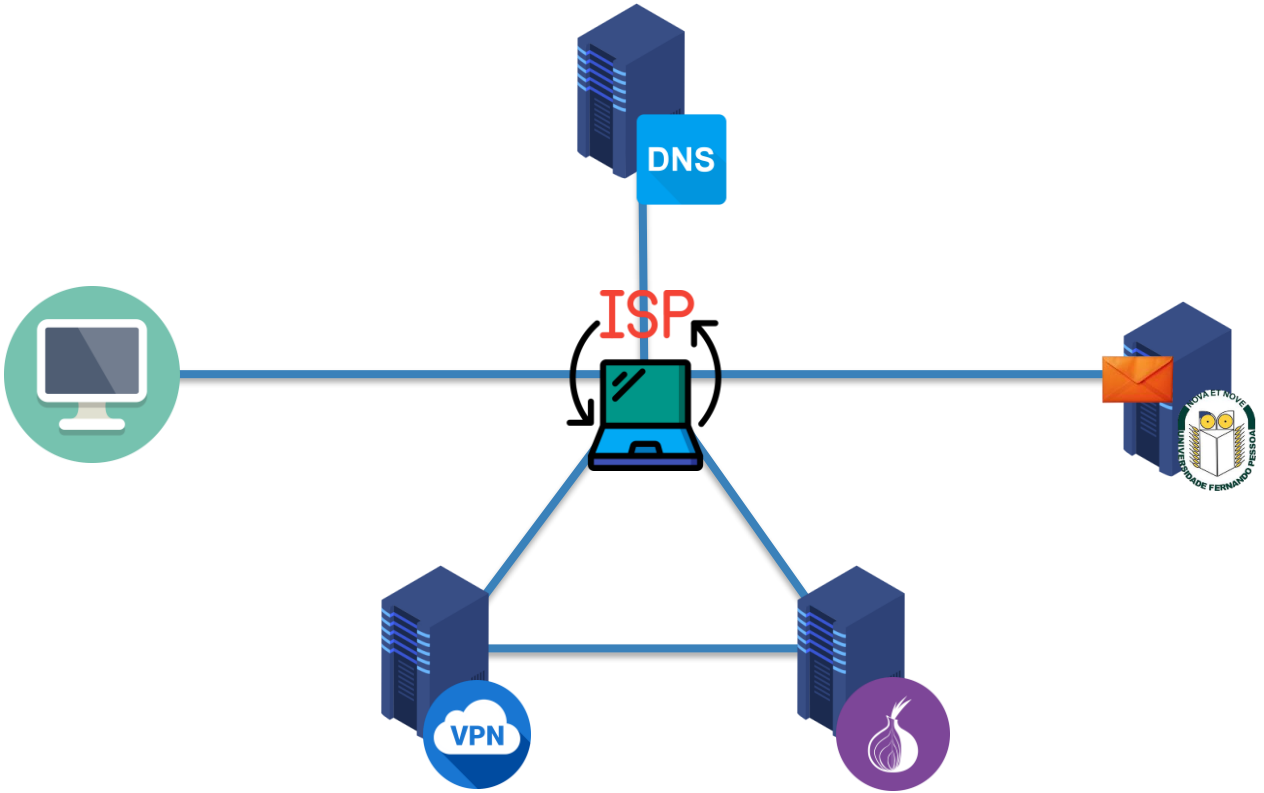
INTERNET COMUM



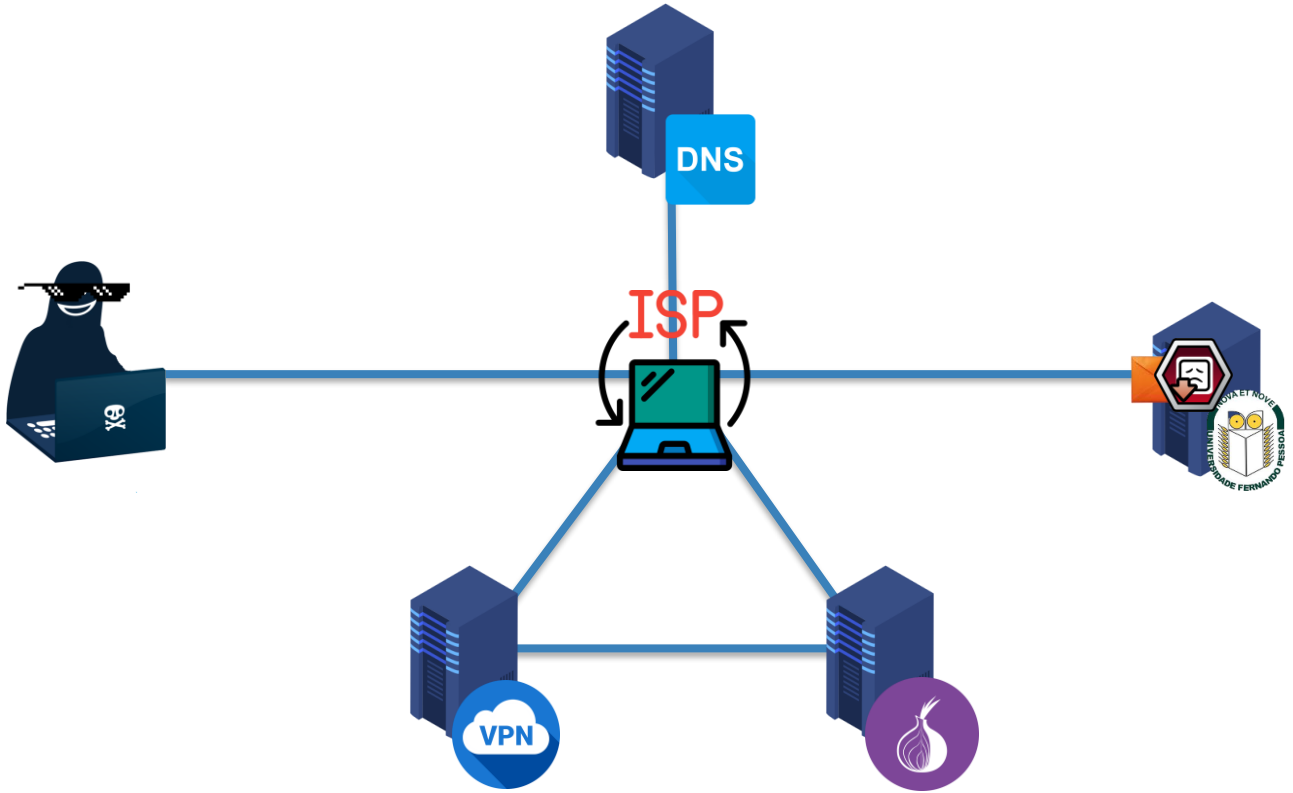
INTERNET COMUM



INTERNET COMUM



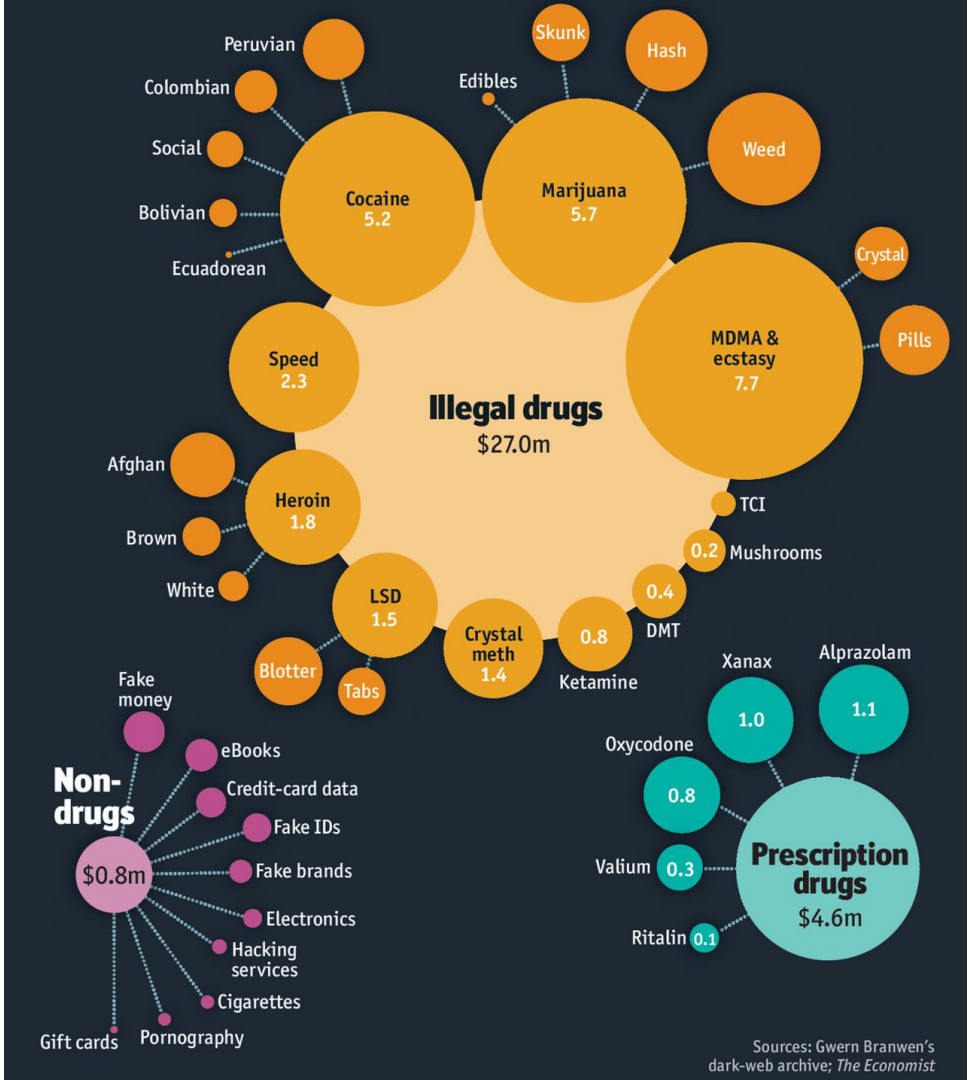
INTERNET COMUM



DARKWEB BUSINESS

Oh Evaristo! Tens cá disto?!

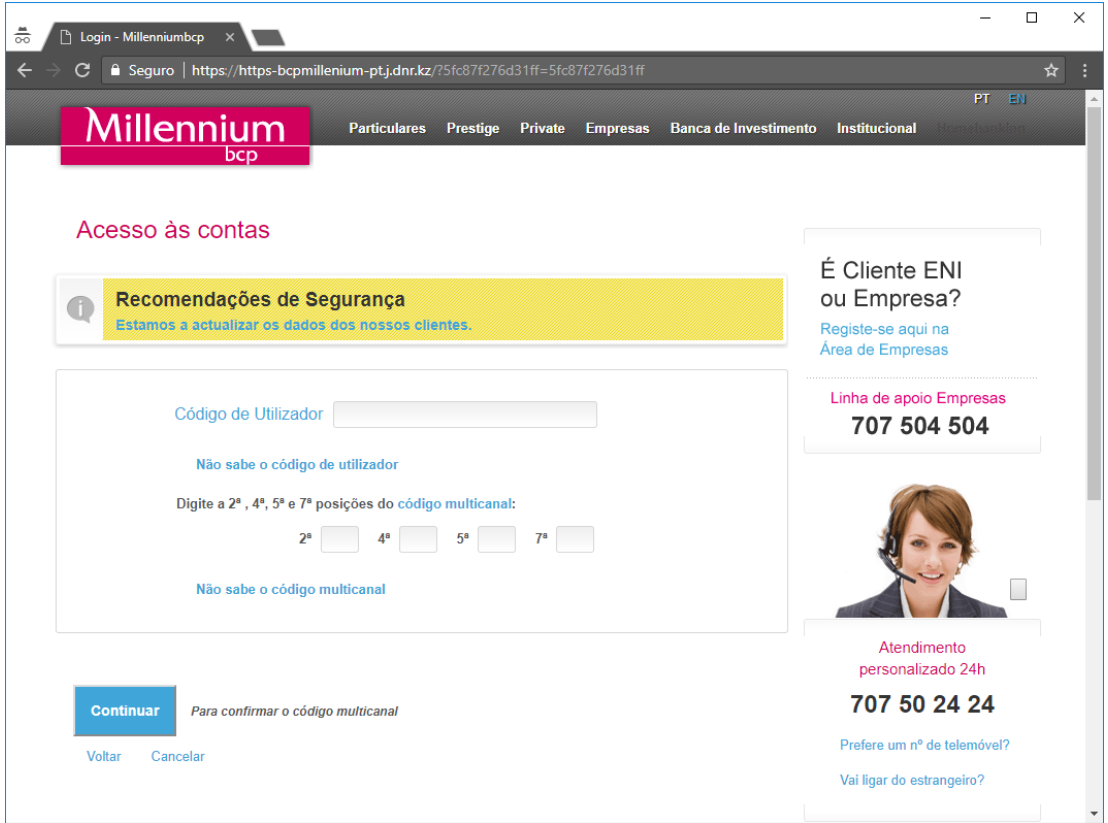
DARKWEB BUSINESS



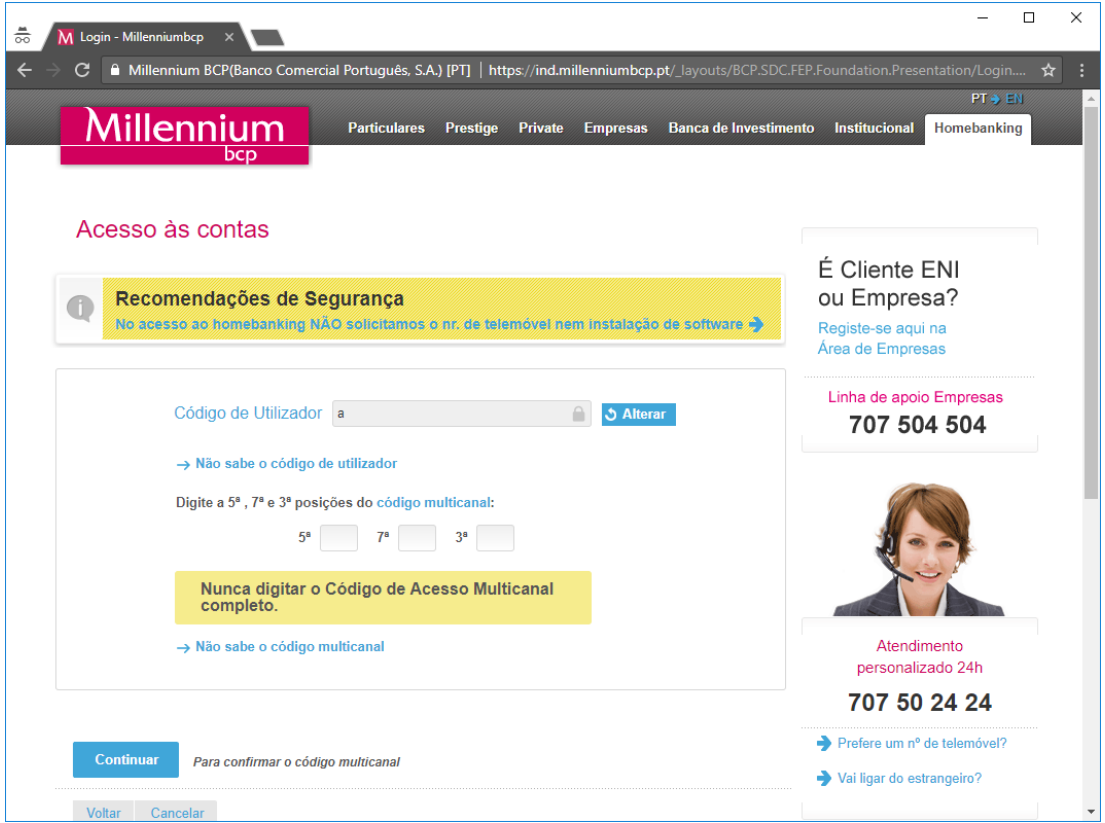
INCIDENTES

Mesmo com a webcam tapada viram-me?

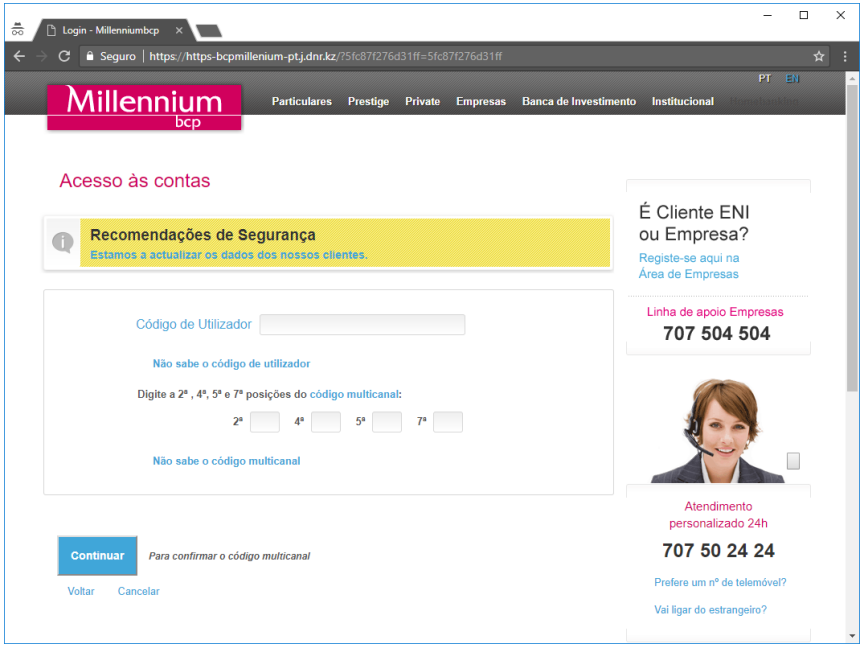
HOMEBANKING

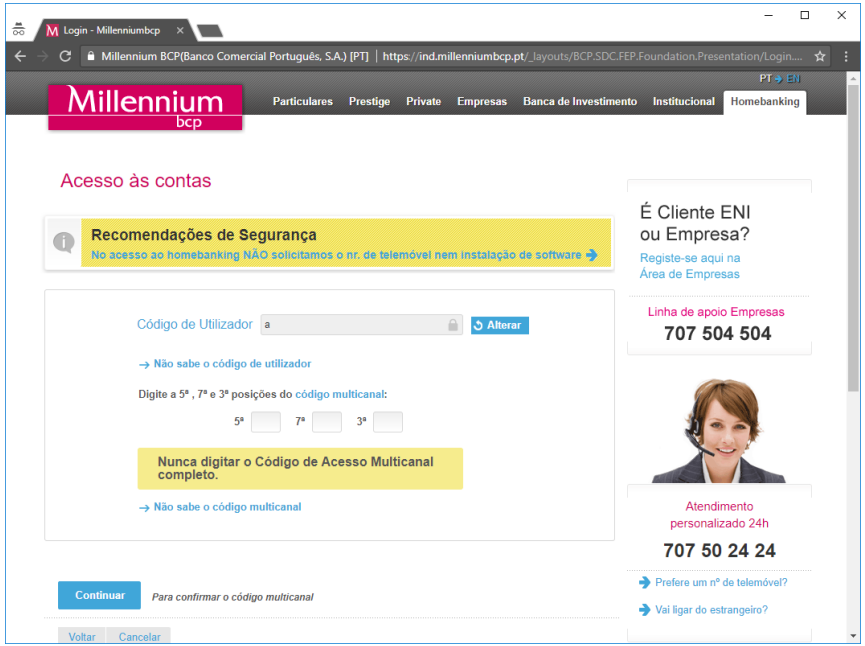


HOMEBANKING



PHISHING


Login - Millenniumbcp
Seguro | https://https-bcpmillenium-pt.j.dnr.kz/?5fc87f276d31ff=5fc87f276d31ff
PT EN
Millennium bcp
Particulares Prestige Private Empresas Banca de Investimento Institucional
Acesso às contas
Recomendações de Segurança
Estamos a actualizar os dados dos nossos clientes.
Código de Utilizador
Não sabe o código de utilizador
Digite a 2ª , 4ª, 5ª e 7ª posições do código multicanal:
2ª 4ª 5ª 7ª
Não sabe o código multicanal
Continuar
Para confirmar o código multicanal
Voltar Cancelar
É Cliente ENI ou Empresa?
Registe-se aqui na Área de Empresas
Linha de apoio Empresas
707 504 504
Atendimento personalizado 24h
707 50 24 24
Prefere um nº de telemóvel?
Vai ligar do estrangeiro?


Login - Millenniumbcp
Millennium BCP(Banco Comercial Português, S.A.) [PT] | https://ind.millenniumbcp.pt/_layouts/BCP.SDC.FEP.Foundation.Presentation/Login....
PT EN
Millennium bcp
Particulares Prestige Private Empresas Banca de Investimento Institucional Homebanking
Acesso às contas
Recomendações de Segurança
No acesso ao homebanking NÃO solicitamos o nr. de telemóvel nem instalação de software
Código de Utilizador a
Alterar
Não sabe o código de utilizador
Digite a 5ª , 7ª e 3ª posições do código multicanal:
5ª 7ª 3ª
Nunca digitar o Código de Acesso Multicanal completo.
Não sabe o código multicanal
Continuar
Para confirmar o código multicanal
Voltar Cancelar
É Cliente ENI ou Empresa?
Registe-se aqui na Área de Empresas
Linha de apoio Empresas
707 504 504
Atendimento personalizado 24h
707 50 24 24
Prefere um nº de telemóvel?
Vai ligar do estrangeiro?

SEXTORTION

From:
Sent: Friday, April 10, 2020 9:26:56 AM
To:
Subject: camif

Your password is camif. I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which proided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. The first part recorded the video you were viewing (you'e got an exceptional taste haha), and the next part recorded your webcam (Yep! t's you \doing nasty things!).

What should you do?

Well, I believe, $4900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (tf you don't know this, search "how to buy Bitcoin" in Google).

Bitcoin Address:

bc1qls8wknrwhvxlf36m cdekscjlpfry
(It is cAsE sensitive, so copy and paste it)

Important:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth.Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

RANSOMWARE

Data: 04.25.2020

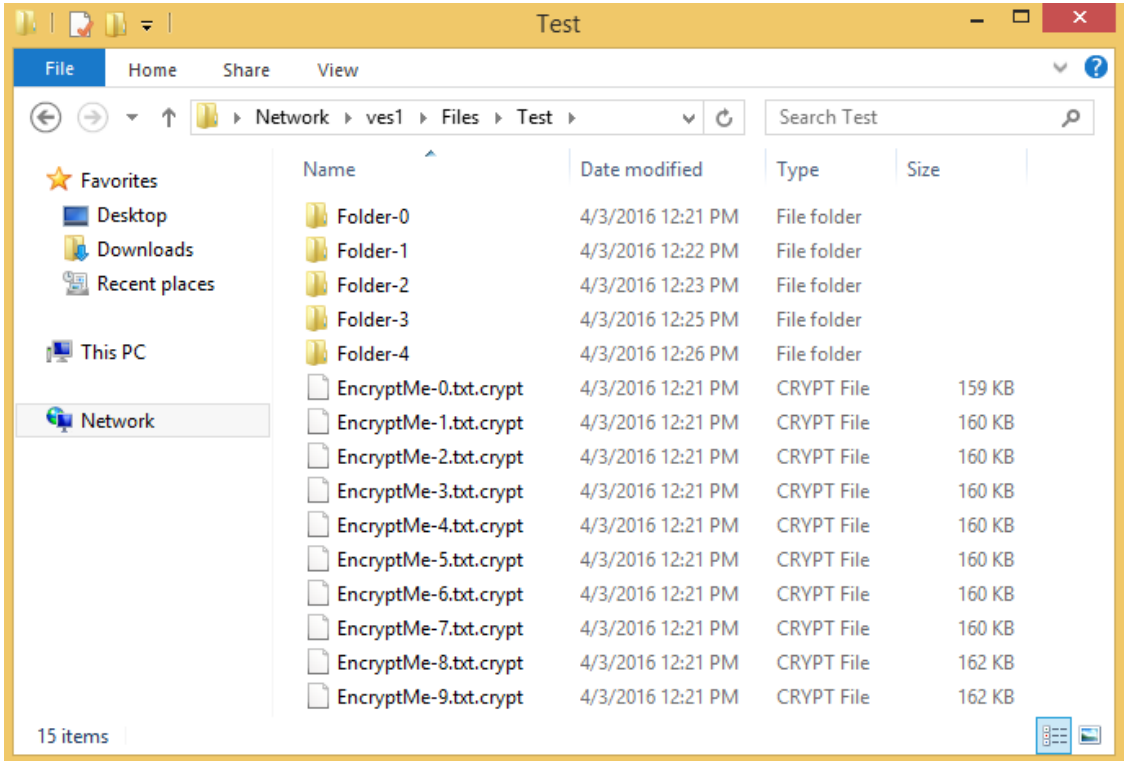
Tenho uma proposta comercial confidencial para você que vale uma quantia substancial. Após receber sua confirmação deste e-mail, divulgarei detalhes de minha intenção no e-mail da próxima página.

Por favor, responda / escreva em inglês, se possível, para melhor comunicação.

Cordial Saudações
Sir David E.J Ramsden
Tel: 075 1023 8901
Fax: 075 4446 9221
E-mail: davrs0842@aol.com

Secretário: Sr. Tomasson Oliver

RANSOMWARE


Test
File
Home
Share
View
Network ▸ ves1 ▸ Files ▸ Test ▸
Search Test
Favorites
Desktop
Downloads
Recent places
This PC
Network
Name
Date modified
Type
Size
Folder-0 4/3/2016 12:21 PM File folder
Folder-1 4/3/2016 12:22 PM File folder
Folder-2 4/3/2016 12:23 PM File folder
Folder-3 4/3/2016 12:25 PM File folder
Folder-4 4/3/2016 12:26 PM File folder
EncryptMe-0.txt.crypt 4/3/2016 12:21 PM CRYPT File 159 KB
EncryptMe-1.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-2.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-3.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-4.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-5.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-6.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-7.txt.crypt 4/3/2016 12:21 PM CRYPT File 160 KB
EncryptMe-8.txt.crypt 4/3/2016 12:21 PM CRYPT File 162 KB
EncryptMe-9.txt.crypt 4/3/2016 12:21 PM CRYPT File 162 KB
15 items

RANSOMWARE

!!! IMPORTANT INFORMATION !!!!

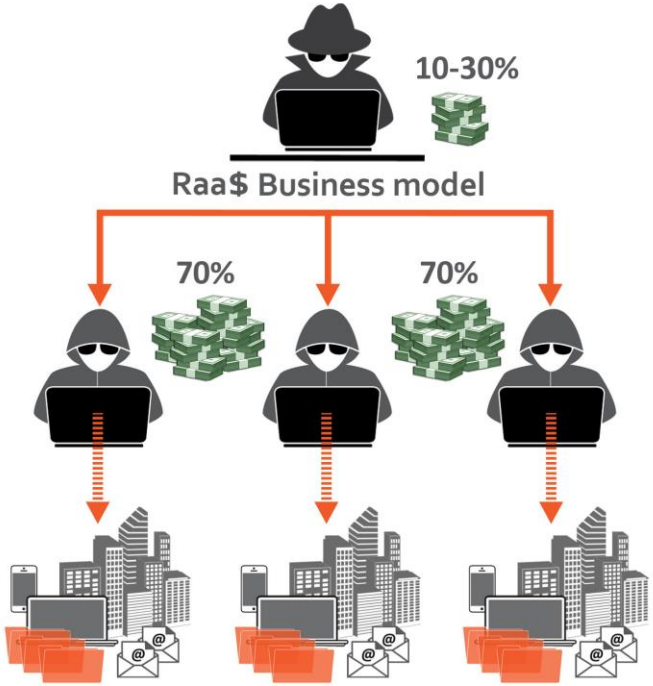
All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
http://en.wikipedia.org/wiki/RSA_(cryptosystem)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
1. http://6dtxgqam4crv6rr6.tor2web.org/ECCEADDE847A1F1A
2. http://6dtxgqam4crv6rr6.onion.to/ECCEADDE847A1F1A
3. http://6dtxgqam4crv6rr6.onion.cab/ECCEADDE847A1F1A

If all of this addresses are not available, follow these steps:
1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: 6dtxgqam4crv6rr6.onion/ECCEADDE847A1F1A
4. Follow the instructions on the site.

!!! Your personal identification ID: ECCEADDE847A1F1A !!!

RANSOMWARE-AS-A-SERVICE



ATAQUES

AVISO

Todos os exemplos são corridos num ambiente controlado e têm um objetivo educativo.

AVISO

Nenhum dos ataques será detalhado durante a apresentação!

TYPOSQUATTING

GOGGLE.COM

TYPOSQUATTING

MICORSOFT.COM

TYPOSQUATTING

WHITEHOUSE.COM

TYPOSQUATTING

HOTMAIL.CM

TYPOSQUATTING

apple.com

TYPOSQUATTING

xn--80ak6aa92e.com

TYPOSQUATTING

flytąp.com

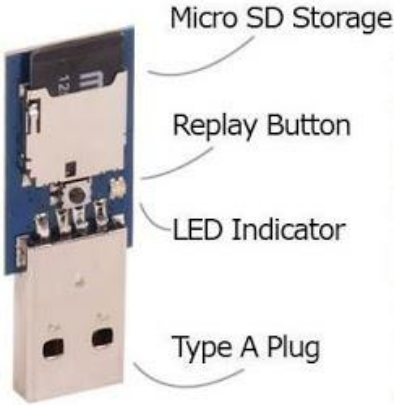
TYPOSQUATTING

xn--flytp-m11b.com

ATAQUE USB

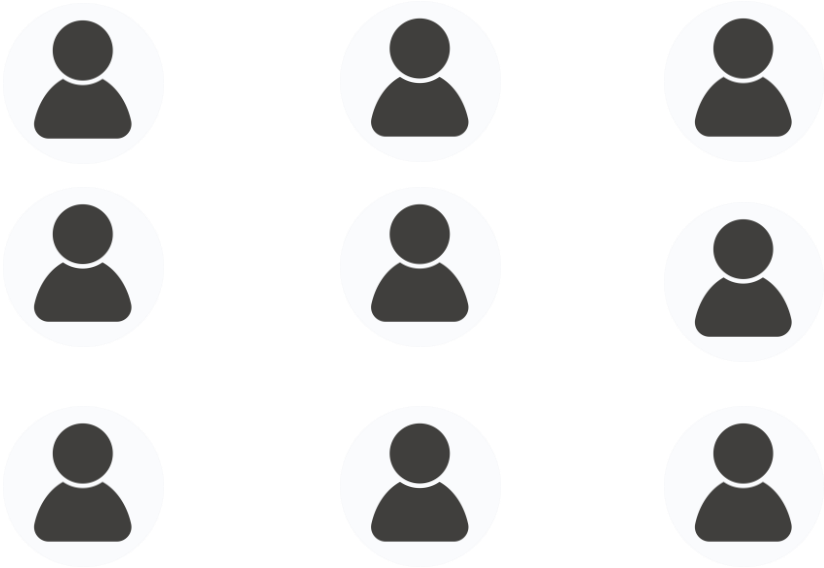
ATAQUE USB

ATAQUE USB

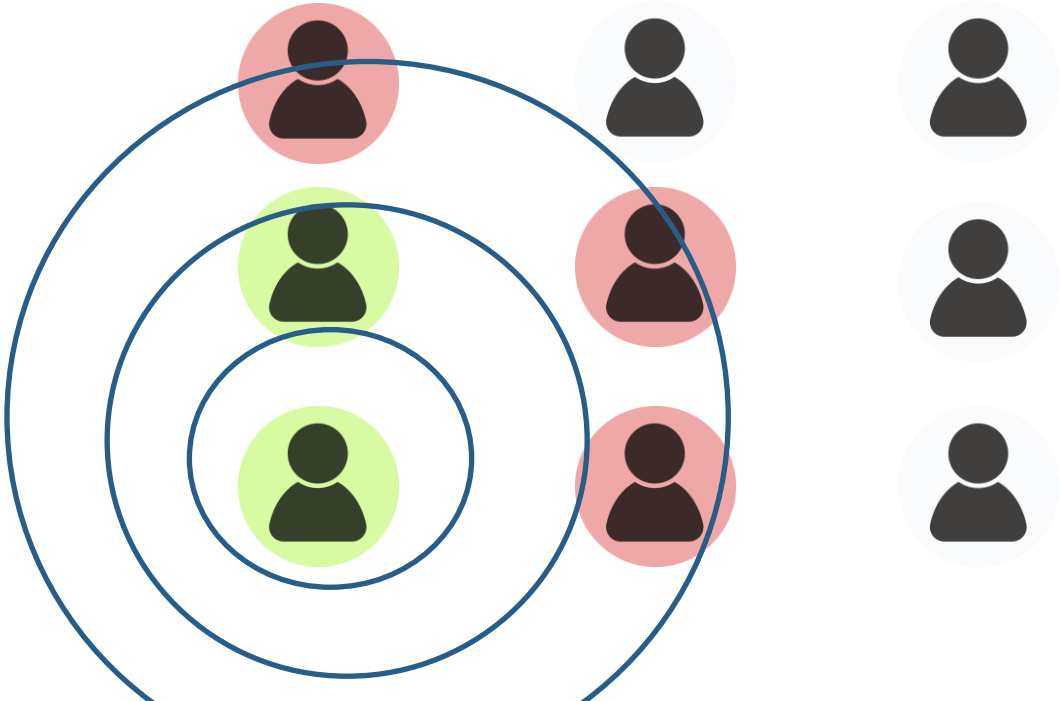

Micro SD Storage
Replay Button
LED Indicator
Type A Plug


60 MHz 32-Bit CPU

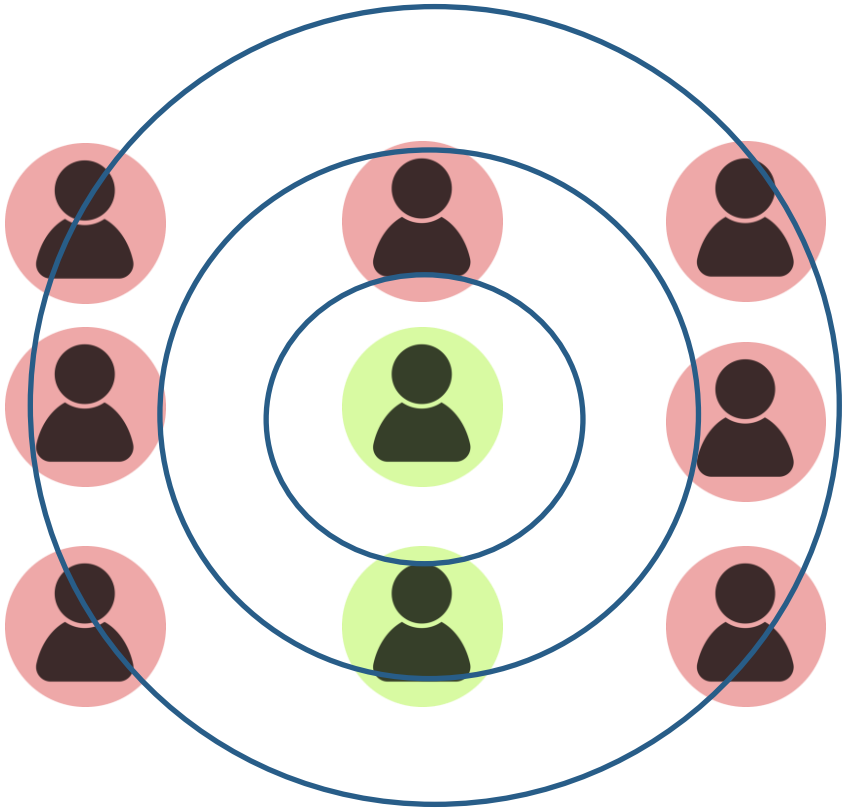
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



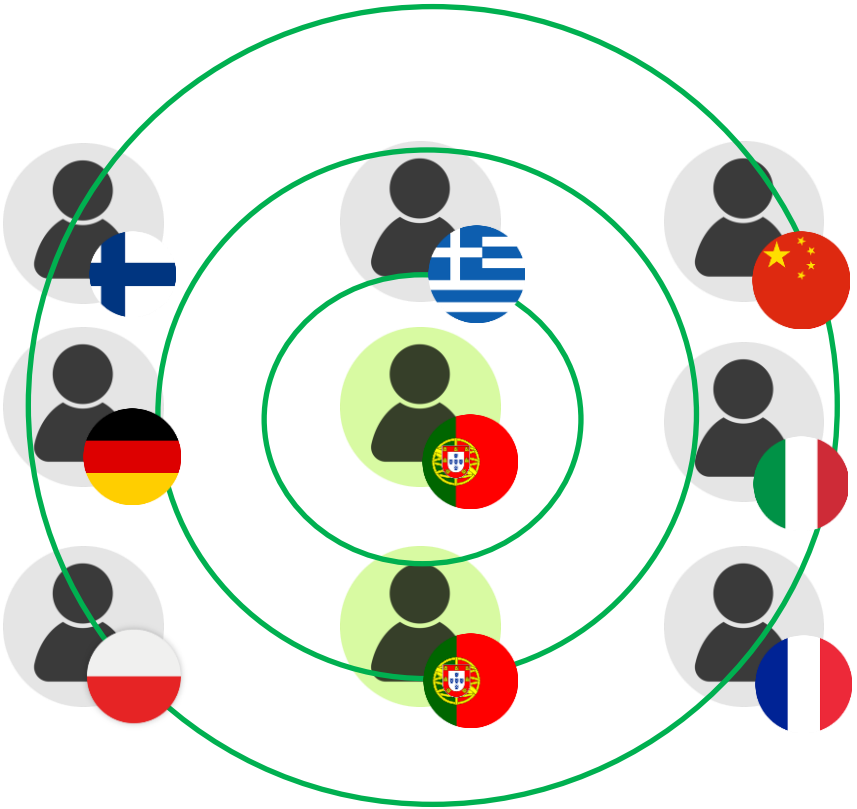
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



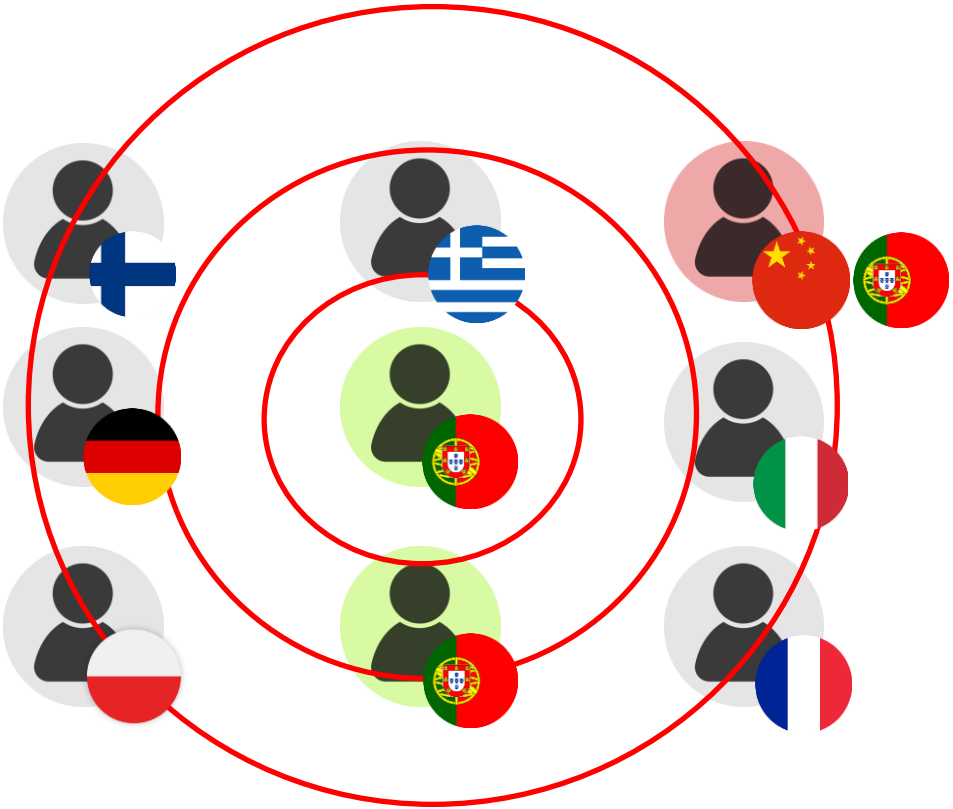
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



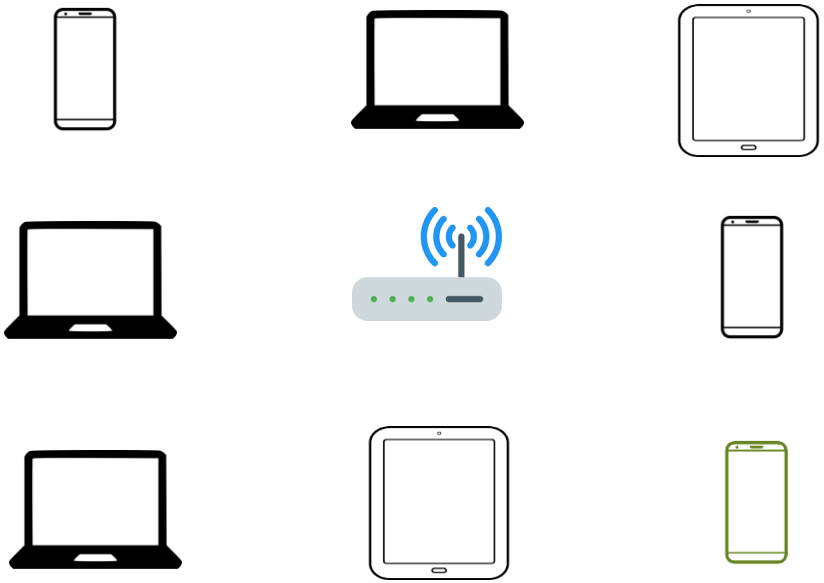
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



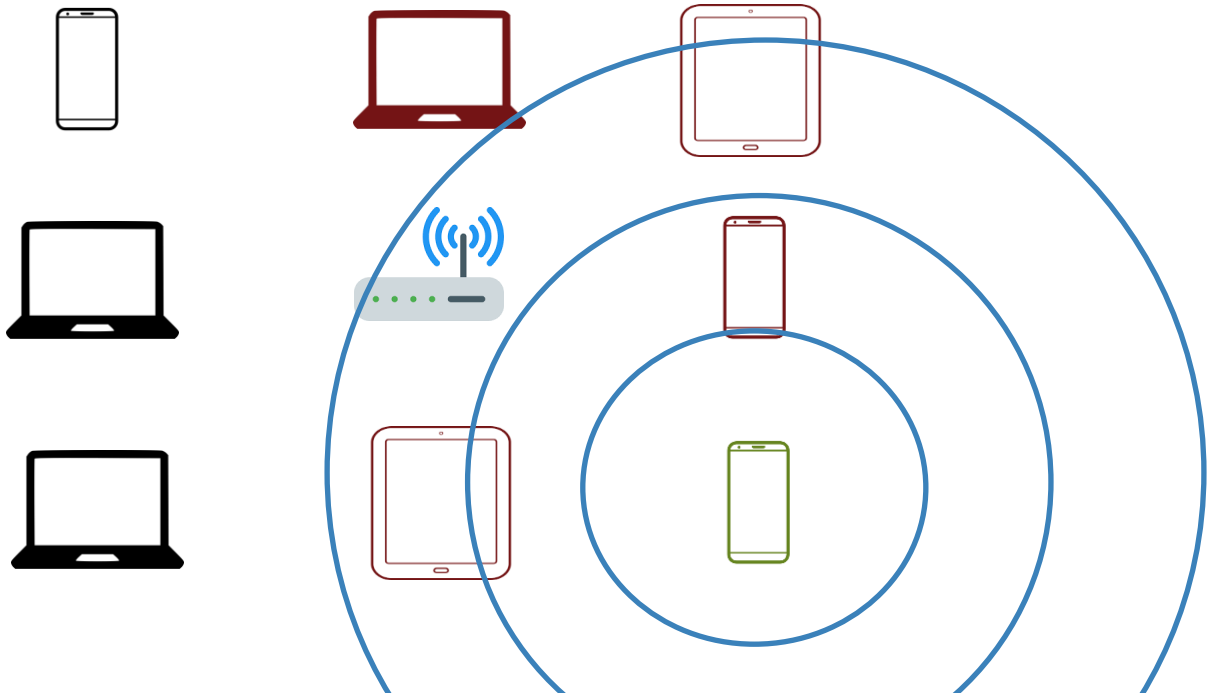
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



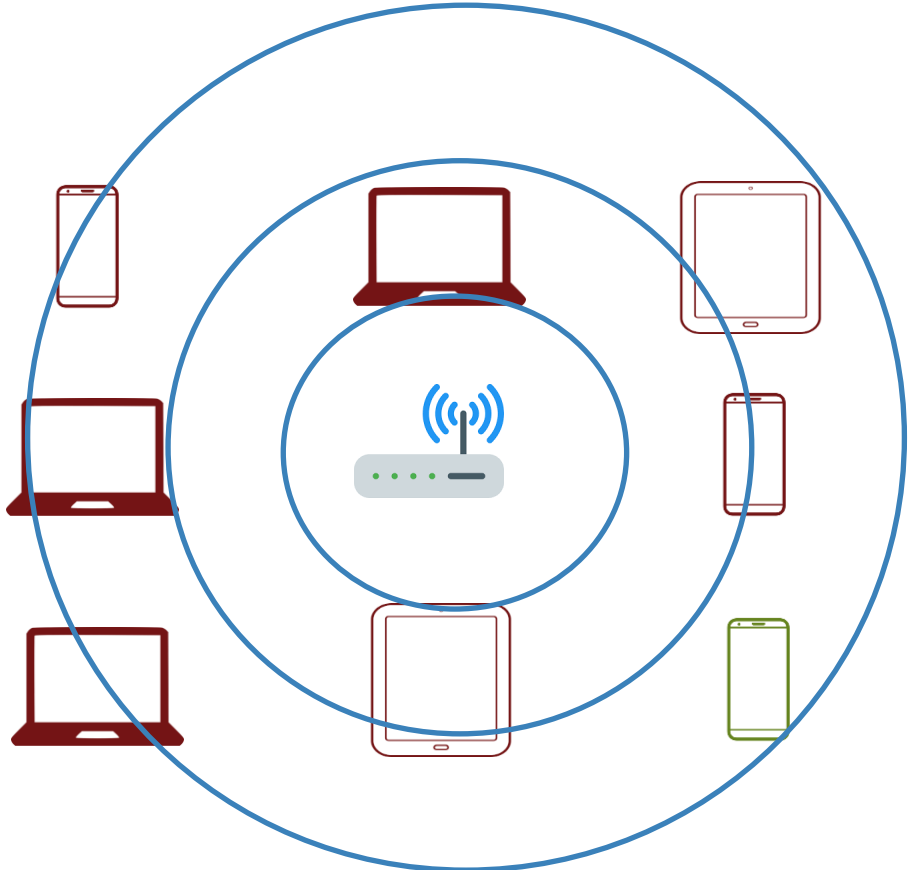
ATAQUE FORÇA-BRUTA WI-FI (WPA2)



ATAQUE FORÇA-BRUTA WI-FI (WPA2)



ATAQUE FORÇA-BRUTA WI-FI (WPA2)



8.
LOGS

Meu querido diário…

LOGS

Servem para registar eventos importantes na execução de um programa ou sistema com o objetivo de dar feedback ao Administrador de Sistemas.

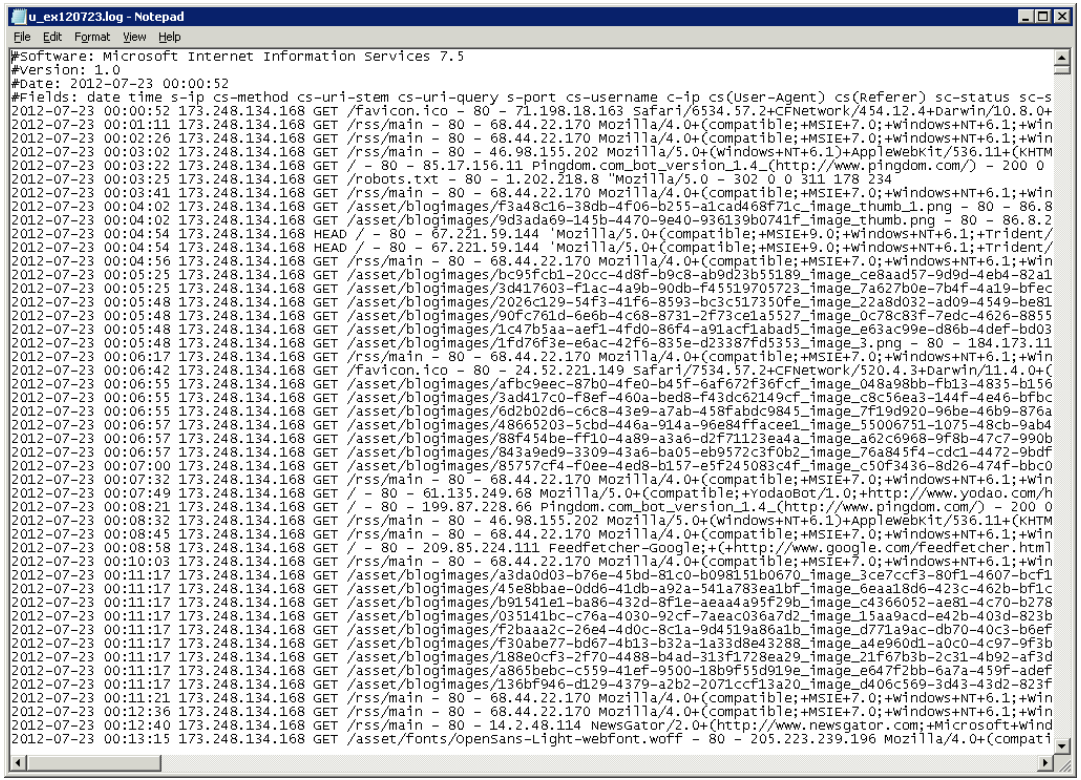
- Deteção de anomalias
- Configurações incorretas
- Validar o estado de funcionamento do sistema
- Ações que o sistema efetuou durante o seu funcionamento

LOGS

PROVAS FORENSES

LOGS

PROVAS FORENSES



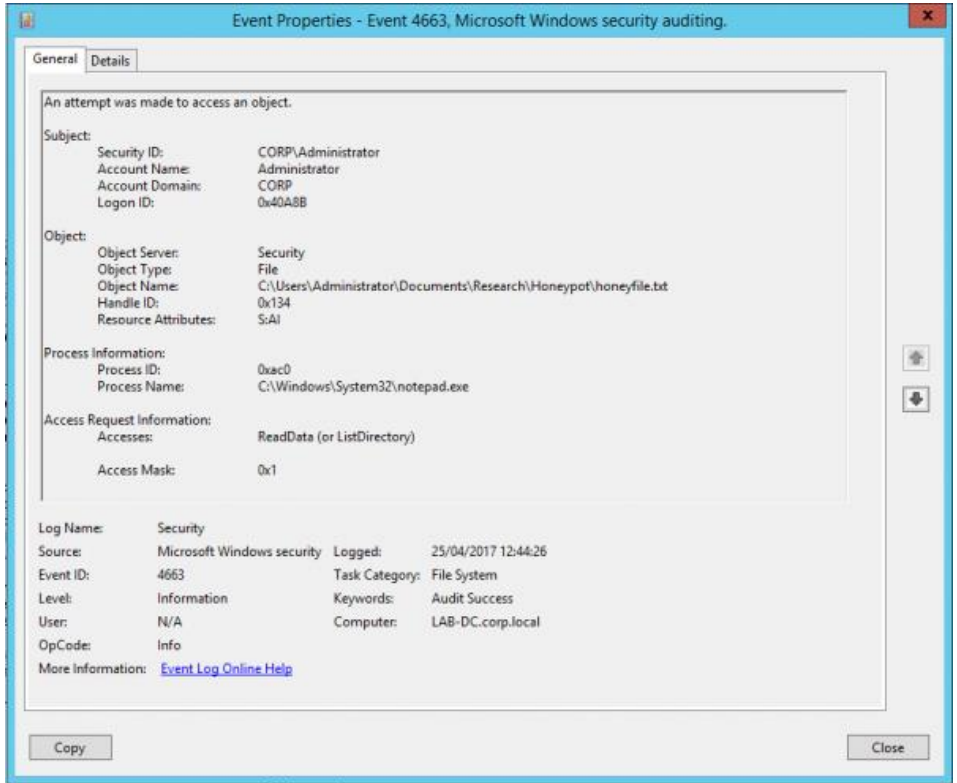
u_ex120723.log - Notepad

File Edit Format View Help

```
#Software: Microsoft Internet Information Services 7.5
#Version: 1.0
#Date: 2012-07-23 00:00:52
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-s
2012-07-23 00:00:52 173.248.134.168 GET /favicon.ico - 80 - 71.198.18.163 Safari/6534.57.2+CFNetwork/454.12.4+Darwin/10.8.0+
2012-07-23 00:01:11 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:02:26 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:03:02 173.248.134.168 GET /rss/main - 80 - 46.98.155.202 Mozilla/5.0+(Windows+NT+6.1)+AppleWebKit/536.11+(KHTM
2012-07-23 00:03:22 173.248.134.168 GET / - 80 - 85.17.156.11 Pingdom.com_bot_version_1.4_(http://www.pingdom.com/) - 200 0
2012-07-23 00:03:25 173.248.134.168 GET /robots.txt - 80 - 1.202.218.8 "Mozilla/5.0 - 302 0 0 311 178 234
2012-07-23 00:03:41 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:04:02 173.248.134.168 GET /asset/blogimages/f3a48c16-38db-4f06-b255-a1cad468f71c_image_thumb_1.png - 80 - 86.8
2012-07-23 00:04:02 173.248.134.168 GET /asset/blogimages/9d3ada69-145b-4470-9e40-936139b0741f_image_thumb.png - 80 - 86.8.2
2012-07-23 00:04:54 173.248.134.168 HEAD / - 80 - 67.221.59.144 'Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+Trident/
2012-07-23 00:04:54 173.248.134.168 HEAD / - 80 - 67.221.59.144 'Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;+Trident/
2012-07-23 00:04:56 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:05:25 173.248.134.168 GET /asset/blogimages/bc95fcb1-20cc-4d8f-b9c8-ab9d23b55189_image_ce8aad57-9d9d-4eb4-82a1
2012-07-23 00:05:25 173.248.134.168 GET /asset/blogimages/3d417603-f1ac-4a9b-90db-f45519705723_image_7a627b0e-7b4f-4a19-bfec
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/2026c129-54f3-41f6-8593-bc3c517350fe_image_22a8d032-ad09-4549-be81
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/90fc761d-6e6b-4c68-8731-2f73ce1a5527_image_0c78c83f-7edc-4626-8855
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/1c47b5aa-aef1-4fd0-86f4-a91acf1abad5_image_e63ac99e-d86b-4def-bd03
2012-07-23 00:05:48 173.248.134.168 GET /asset/blogimages/1fd76f3e-e6ac-42f6-835e-d23387fd5353_image_3.png - 80 - 184.173.11
2012-07-23 00:06:17 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:06:42 173.248.134.168 GET /favicon.ico - 80 - 24.52.221.149 Safari/7534.57.2+CFNetwork/520.4.3+Darwin/11.4.0+(
2012-07-23 00:06:55 173.248.134.168 GET /asset/blogimages/afbc9eec-87b0-4fe0-b45f-6af672f36fcf_image_048a98bb-fb13-4835-b156
2012-07-23 00:06:55 173.248.134.168 GET /asset/blogimages/3ad417c0-f8ef-460a-bed8-f43dc62149cf_image_c8c56ea3-144f-4e46-bfbc
2012-07-23 00:06:55 173.248.134.168 GET /asset/blogimages/6d2b02d6-c6c8-43e9-a7ab-458fabdc9845_image_7f19d920-96be-46b9-876a
2012-07-23 00:06:57 173.248.134.168 GET /asset/blogimages/48665203-5cbd-446a-914a-96e84ffacee1_image_55006751-1075-48cb-9ab4
2012-07-23 00:06:57 173.248.134.168 GET /asset/blogimages/88f454be-ff10-4a89-a3a6-d2f71123ea4a_image_a62c6968-9f8b-47c7-990b
2012-07-23 00:06:57 173.248.134.168 GET /asset/blogimages/843a9ed9-3309-43a6-ba05-eb9572c3f0b2_image_76a845f4-cdc1-4472-9bdf
2012-07-23 00:07:00 173.248.134.168 GET /asset/blogimages/85757cf4-f0ee-4ed8-b157-e5f245083c4f_image_c50f3436-8d26-474f-bbc0
2012-07-23 00:07:32 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:07:49 173.248.134.168 GET / - 80 - 61.135.249.68 Mozilla/5.0+(compatible;+YodaoBot/1.0;+http://www.yodao.com/h
2012-07-23 00:08:21 173.248.134.168 GET / - 80 - 199.87.228.66 Pingdom.com_bot_version_1.4_(http://www.pingdom.com/) - 200 0
2012-07-23 00:08:32 173.248.134.168 GET /rss/main - 80 - 46.98.155.202 Mozilla/5.0+(Windows+NT+6.1)+AppleWebKit/536.11+(KHTM
2012-07-23 00:08:45 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:08:58 173.248.134.168 GET / - 80 - 209.85.224.111 FeedFetcher-Google;+(+http://www.google.com/feedfetcher.html
2012-07-23 00:10:03 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/a3da0d03-b76e-45bd-81c0-b098151b0670_image_3ce7ccf3-80f1-4607-bcf1
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/45e8bbae-0dd6-41db-a92a-541a783ea1bf_image_6eaa18d6-423c-462b-bf1c
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/b91541e1-ba86-432d-8f1e-aeaa4a95f29b_image_c4366052-ae81-4c70-b278
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/035141bc-c76a-4030-92cf-7aeac036a7d2_image_15aa9acd-e42b-403d-823b
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/f2baaa2c-26e4-4d0c-8c1a-9d4519a86a1b_image_d771a9ac-db70-40c3-b6ef
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/f30abe77-bd67-4b13-b32a-1a33d8e43288_image_a4e960d1-a0c0-4c97-9f3b
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/188e0cf3-2f70-4488-b4ad-313f1728ea29_image_21f67b3b-2c31-4b92-af3d
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/a865bebc-c559-41ef-9500-18b9f55d919e_image_e647f2bb-6a7a-459f-adef
2012-07-23 00:11:17 173.248.134.168 GET /asset/blogimages/136bf946-d129-4379-a2b2-2071ccf13a20_image_d406c569-3d43-43d2-823f
2012-07-23 00:11:21 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:12:36 173.248.134.168 GET /rss/main - 80 - 68.44.22.170 Mozilla/4.0+(compatible;+MSIE+7.0;+Windows+NT+6.1;+Win
2012-07-23 00:12:40 173.248.134.168 GET /rss/main - 80 - 14.2.48.114 NewsGator/2.0+(http://www.newsgator.com;+Microsoft+Wind
2012-07-23 00:13:15 173.248.134.168 GET /asset/fonts/OpenSans-Light-webfont.woff - 80 - 205.223.239.196 Mozilla/4.0+(compati
```

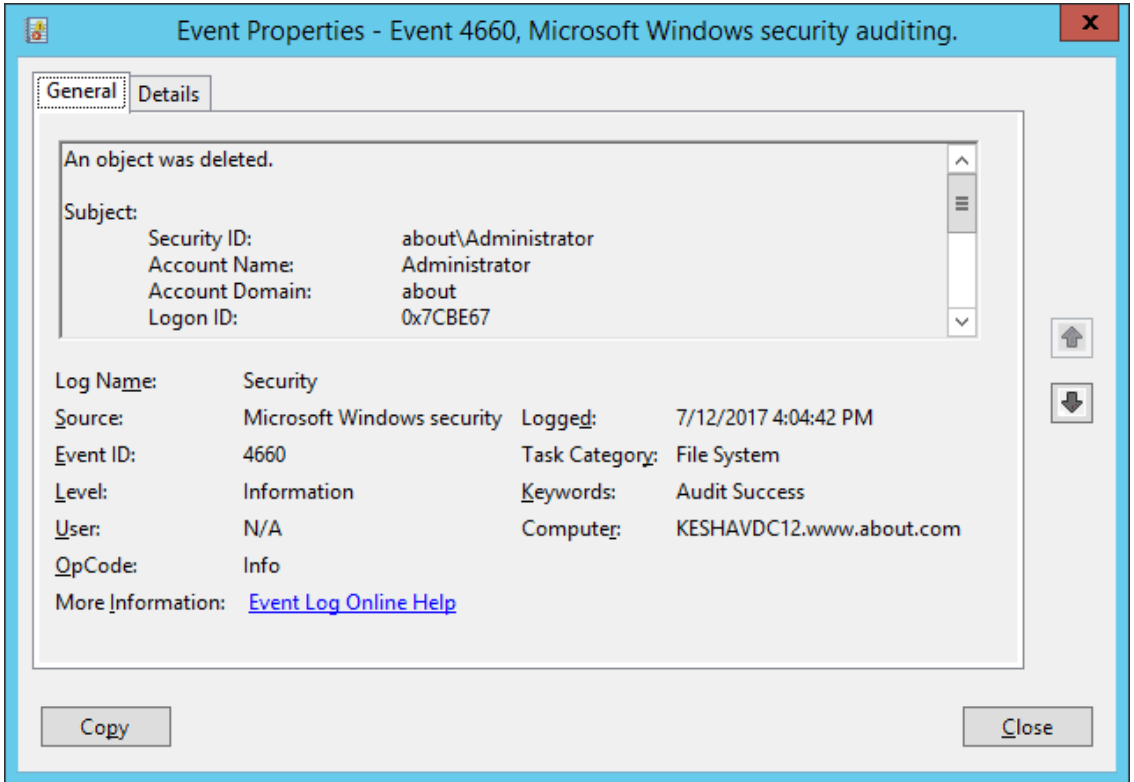
LOGS

PROVAS FORENSES



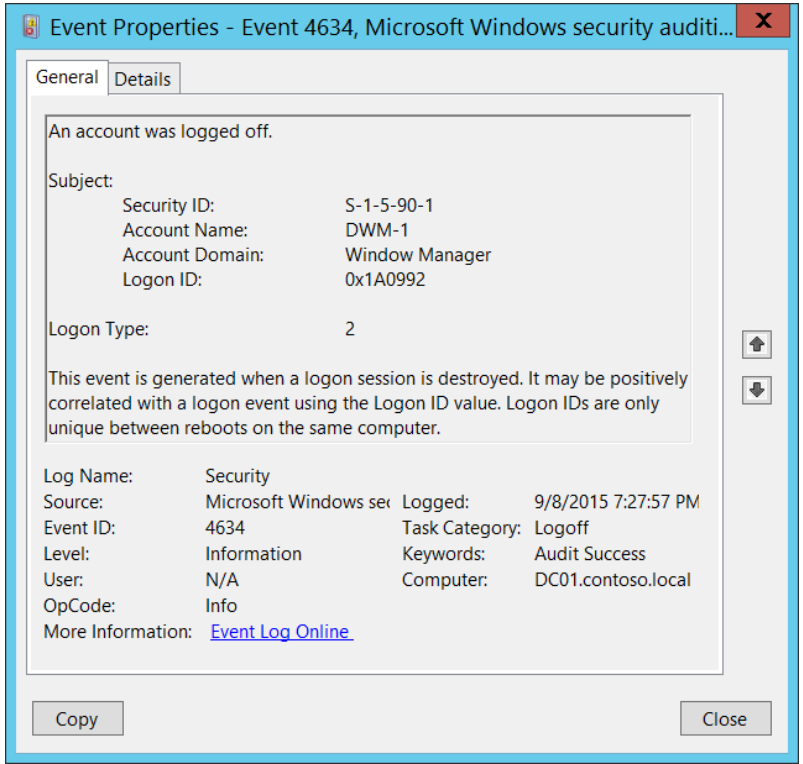
LOGS

PROVAS FORENSES



LOGS

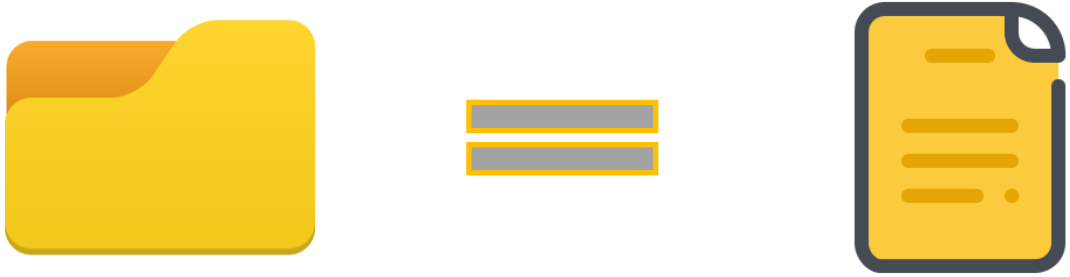
PROVAS FORENSES



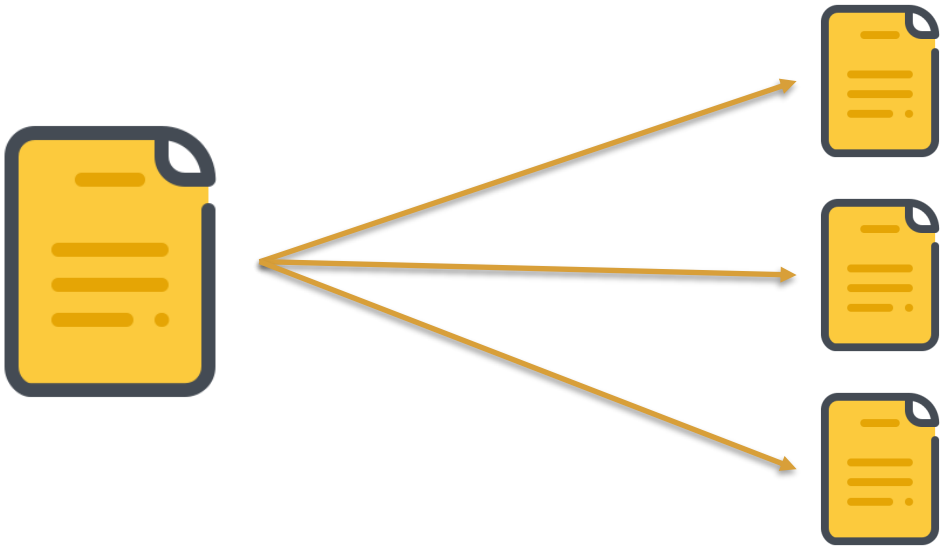
8.
FICHEIROS

Once it's gone, it's gone forever…… forever mesmo?

FICHEIROS



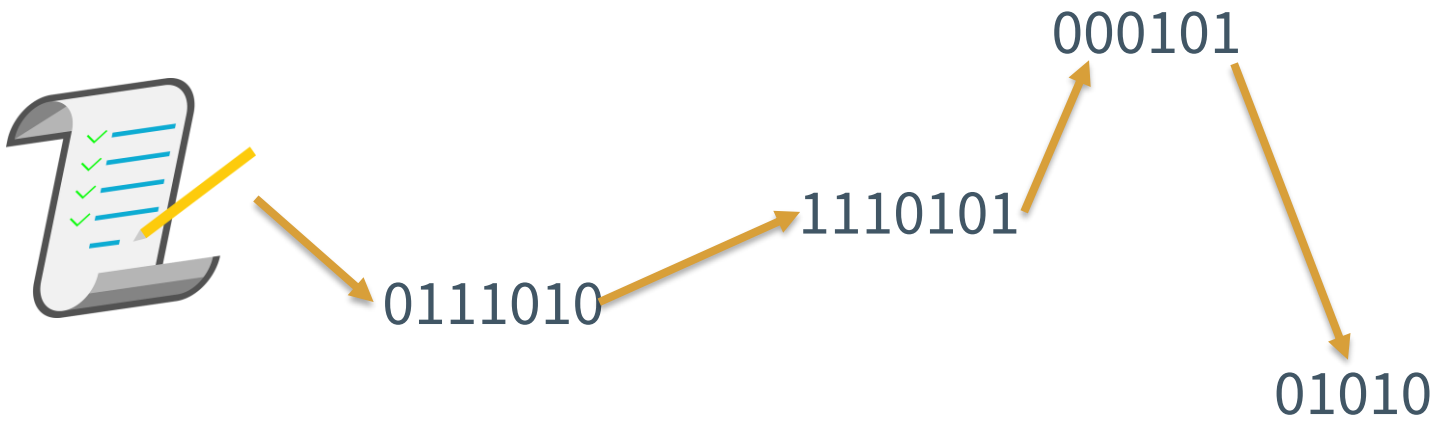
FICHEIROS



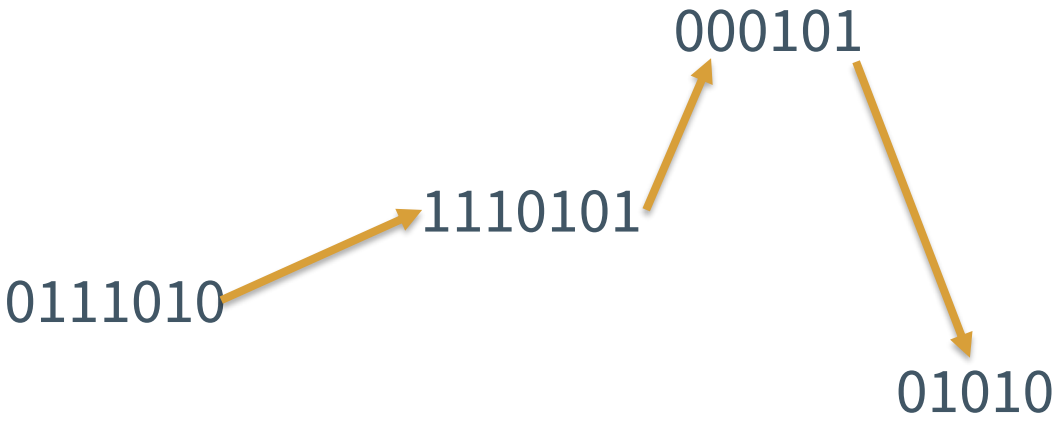
FICHEIROS

01110101110101000101010101

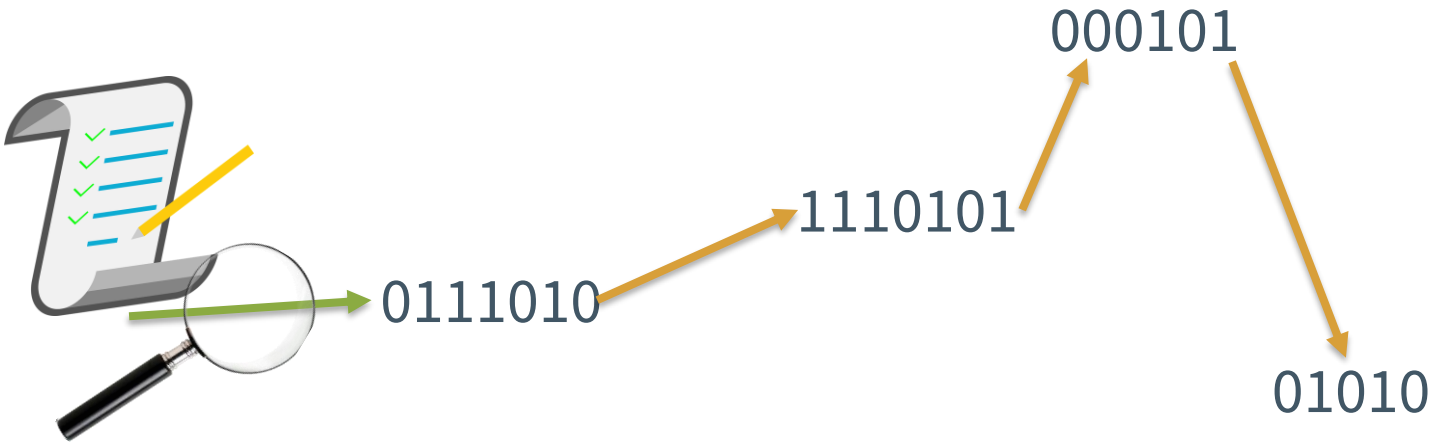
FICHEIROS



FICHEIROS



FICHEIROS



8.
EQUIPAMENTO FORENSE

Os utensílios do Chef.

EQUIPAMENTO FORENSE

EQUIPAMENTO FORENSE

EQUIPAMENTO FORENSE

EQUIPAMENTO FORENSE

EQUIPAMENTO FORENSE

WIRESHARK

ACCESSDATA
ForensicToolkit (FTK)

SIFT

Autopsy®
BASIS TECHNOLOGY

Hex-Rays
STATE-OF-THE-ART BINARY CODE ANALYSIS SOLUTIONS

VOLATILITY

E AGORA?

Persistência
É normal chegar-se a impasses devido ao volume de dados que é necessário analisar para tirar conclusões. É importante não desistir e não pensar de mais.

Ética
O que analisamos é o que os sistemas contém. Formulação de opiniões ou motivações extraordinárias podem ter impactos negativos na análise.

Atenção
A resposta que procuramos na nossa análise está no meio do palheiro. Atenção redobrada durante todas as fases da análise.

Aprendizagem
As tecnologias estão em constante evolução e os meios de analisar de forma forense evoluem também.

Partilha
É importante cooperar com quem realizamos a análise. Dois pares de olhos vêem sempre melhor que um.

Método
Seguir sempre as melhores práticas e o que está regulamentado para não por em causa a investigação.


FORENSIC SCIENCE?
MORE THAN A HOBBY FOR ME
imgflip.com

Hacking was about intellectual curiosity and pursuit of knowledge and thrill, and now is big business.

Kevin Mitnick

”

Obrigado.

Ivo.vacas@cncs.gov.pt

Departamento de Operações

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL