CYBERSECURITY FOR YOUR OFFICE: ENCRYPTION AND FIREWALLS

Louisiana Bar Association
Solo, Small Office & Tech Conference - 2019

Ron Chichester & Tony Ray

New Orleans, Louisiana

April 10, 2019

OVERVIEW

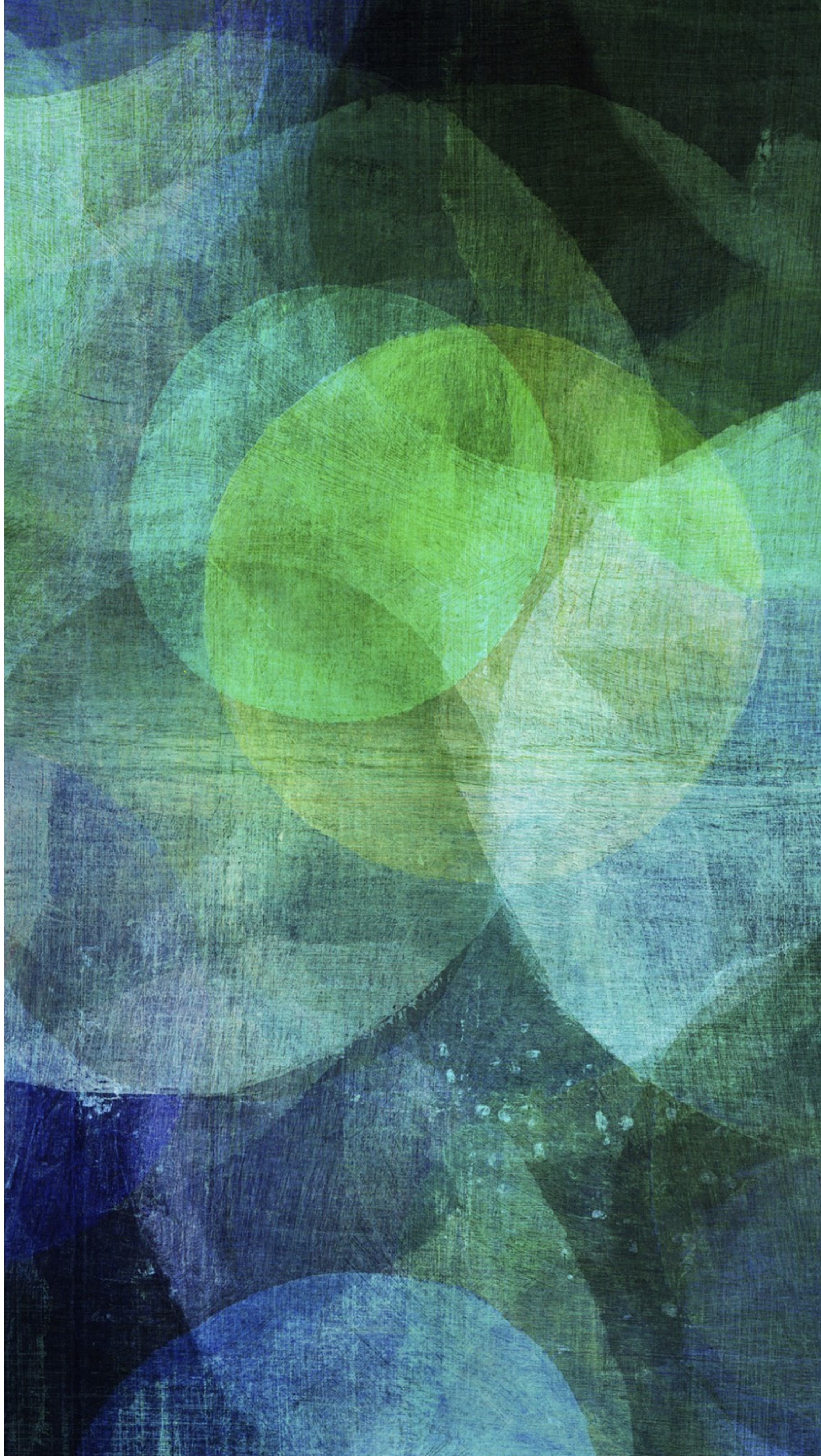
Why take the trouble?

Lay a foundation

Encryption

Firewalls

Questions



WHY TAKE THE TROUBLE?

- ALL states have breach/ notification laws for loss of sensitive data
- Law firms are businesses and so come under the breach/ notification laws
- In Louisiana, the breach/ notification laws are in La. Rev. Stat. §§ 51:3071 et seq.
- In addition — for attorneys — there is Louisiana Legal Ethics Rule **1.6** (Confidentiality of Information)

LAYING THE FOUNDATION

Do you have cyber-insurance?

*If not, this stuff can save your a***

The Problem

The Internet

bit

bit

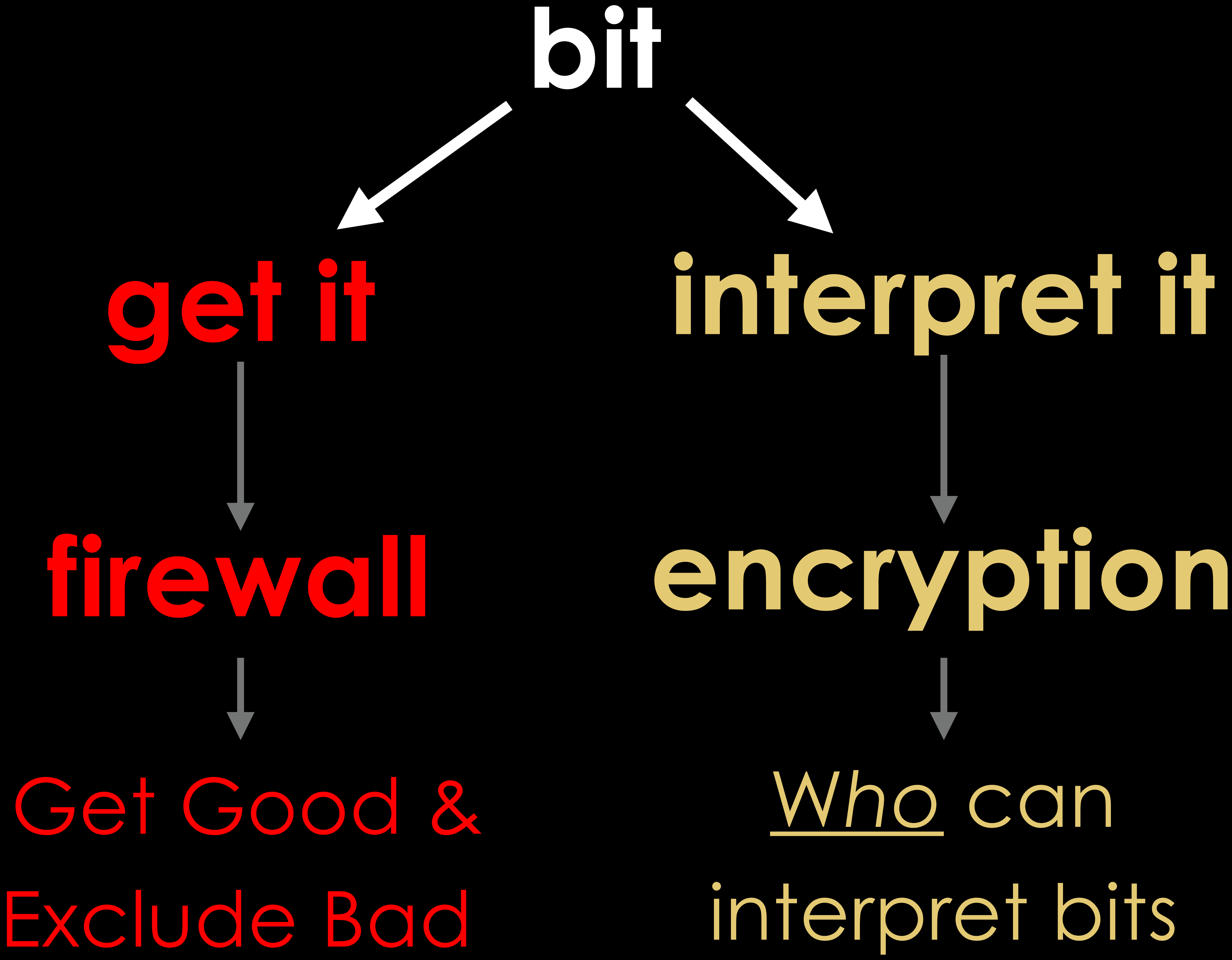
True False

bit

Yes No

bit

1 0



bit

get it

firewall

Get Good & Exclude Bad

interpret it

encryption

Who can interpret bits

ENCRYPTION

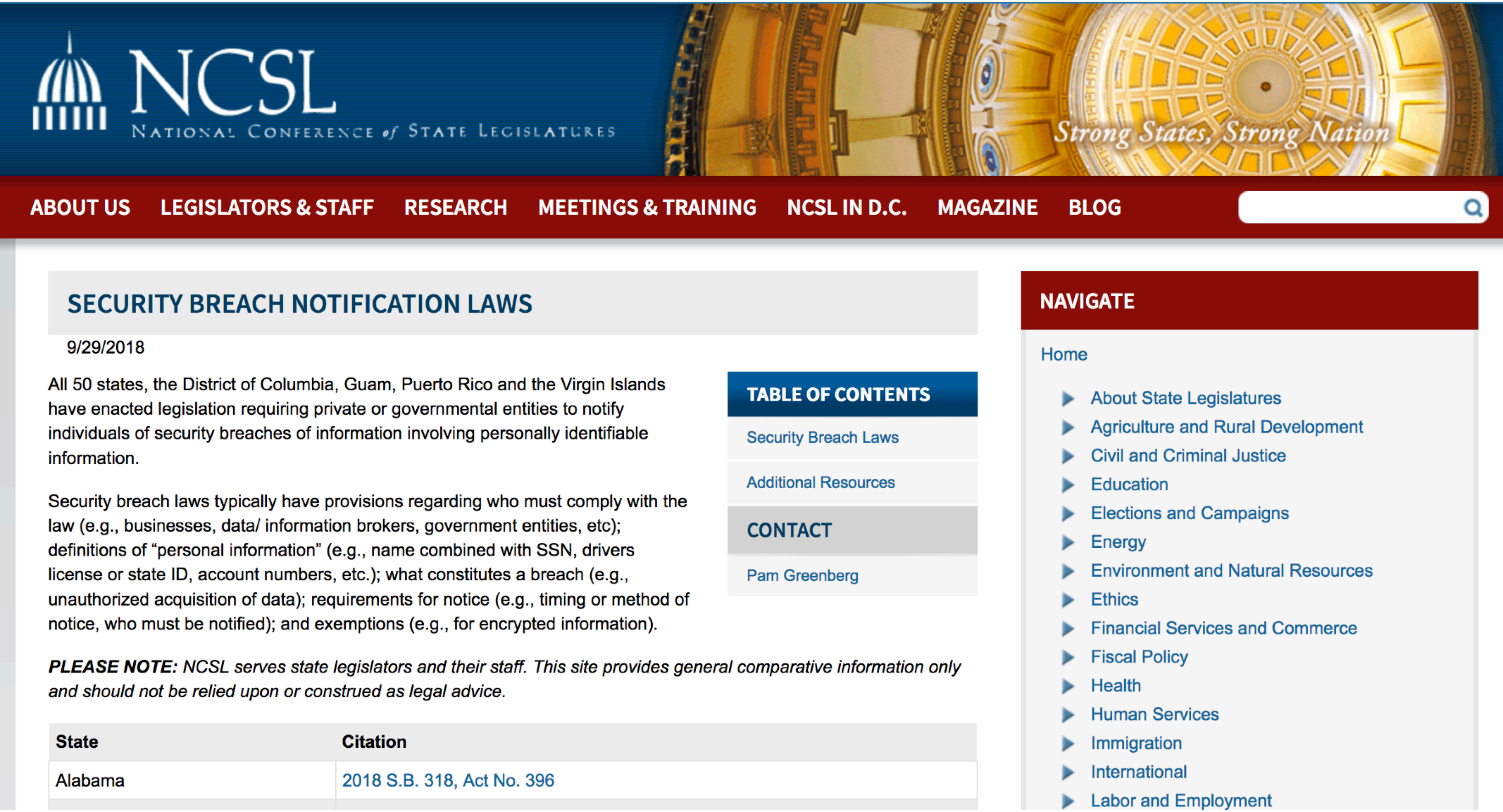
Chance

THIS ART MAY BE KEPT
UNTIL NEEDED, OR SOLD

**GET OUT OF JAIL
FREE**

> All 50 states have a safe harbor exception for encrypted data.
>
> *- Ronald Chichester*

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx



SECURITY BREACH NOTIFICATION LAWS

9/29/2018

All 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information.

Security breach laws typically have provisions regarding who must comply with the law (e.g., businesses, data/ information brokers, government entities, etc); definitions of "personal information" (e.g., name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified); and exemptions (e.g., for encrypted information).

***PLEASE NOTE:** NCSL serves state legislators and their staff. This site provides general comparative information only and should not be relied upon or construed as legal advice.*

State	Citation
Alabama	2018 S.B. 318, Act No. 396

“

But that safe harbor is limited in some states (such as Texas and Louisiana).

- Ronald Chichester

“

> In Texas, the safe harbor does not apply if the encryption was ***past*** tense or ***future*** tense.

- Ronald Chichester

Encrypted Data

+

an (available) Key

=

No *Safe Harbor*

Decrypted Data

+

Hack

=

No *Safe Harbor*

LA. REV. STAT. § 51:3074

§3074. Protection of personal information; disclosure upon breach in the security of personal information; notification requirements; exemption

A. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

B. Any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information shall take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

C. Any person that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, shall, following discovery of a breach in the security of the system containing such data, notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

D. Any agency or person that maintains computerized data that includes personal information that the agency or person does not own shall notify the owner or licensee of the information if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of security of the system containing such data, following discovery by the agency or person of a breach of security of the system.

LOUISIANA ETHICS RULE 1.6

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) …

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

TYPES OF DATA DIFFER

…between La. Rev. Stat. § 51:3073 and Rule 1.6

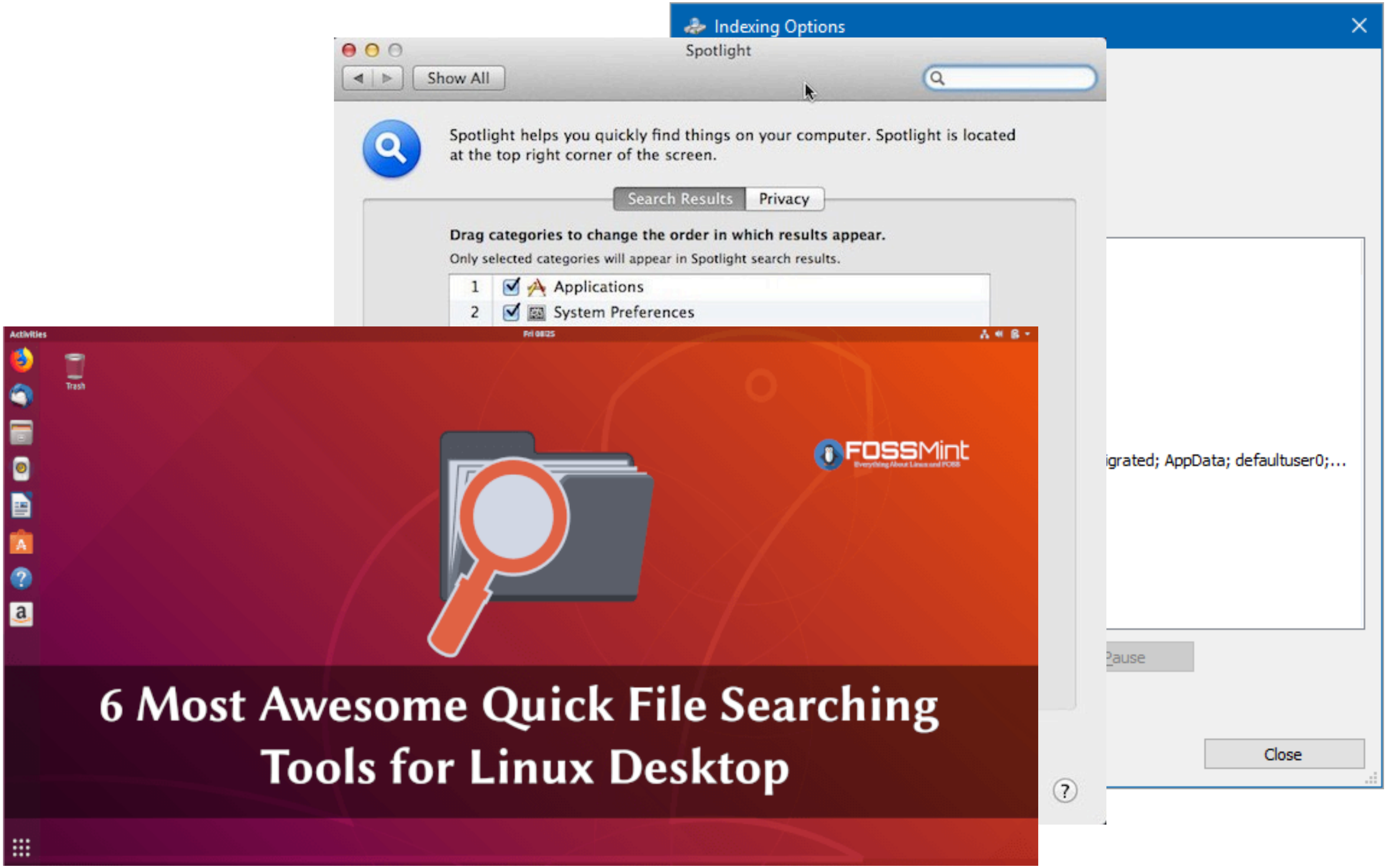
*In either case, **encryption** can **save** your **firm** and/or your **law license**…*

… **if** *you do it right*

DOING IT RIGHT…

- Two main types of encryption:
  - Single-key encryption (simpler)
  - Dual-key (more secure but more cumbersome)
- Determine client needs
  - Engagement letter
  - Software + Cost(?) + key/password management
- Devise practice/policy for handling data at the firm
  - Encrypt when not using the data! (*present* tense)
  - Encrypt backups!!
  - Don’t forget about the operating system indexes!!!

WATCH IT — OPERATING SYSTEM INDEXES



Spotlight helps you quickly find things on your computer. Spotlight is located at the top right corner of the screen.

Drag categories to change the order in which results appear.

Only selected categories will appear in Spotlight search results.

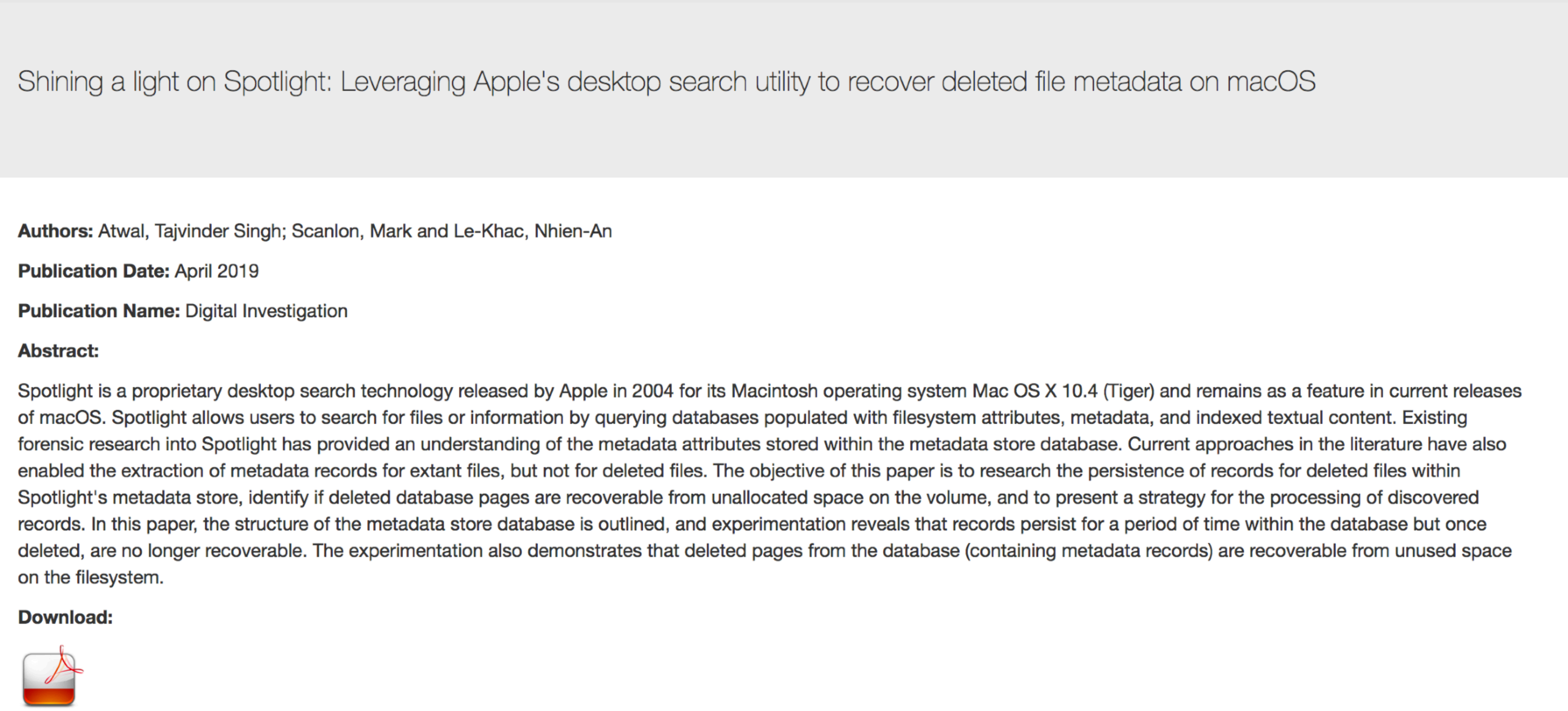
1 ☑ Applications

2 ☑ System Preferences

igrated; AppData; defaultuser0;...

6 Most Awesome Quick File Searching Tools for Linux Desktop

https://www.markscanlon.co/papers/SpotlightMacForensics.php



Shining a light on Spotlight: Leveraging Apple's desktop search utility to recover deleted file metadata on macOS

Authors: Atwal, Tajvinder Singh; Scanlon, Mark and Le-Khac, Nhien-An

Publication Date: April 2019

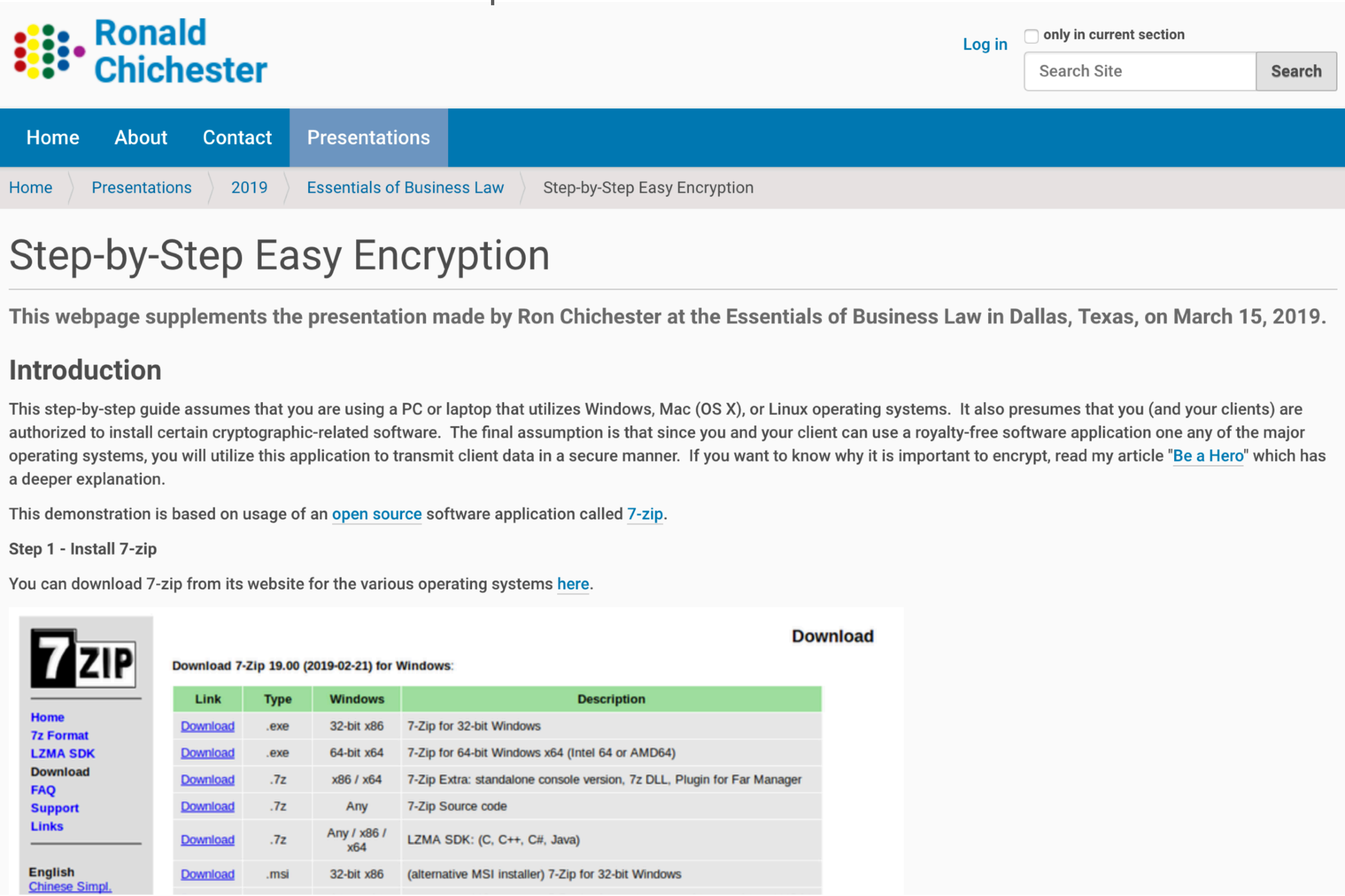
Publication Name: Digital Investigation

Abstract:

Spotlight is a proprietary desktop search technology released by Apple in 2004 for its Macintosh operating system Mac OS X 10.4 (Tiger) and remains as a feature in current releases of macOS. Spotlight allows users to search for files or information by querying databases populated with filesystem attributes, metadata, and indexed textual content. Existing forensic research into Spotlight has provided an understanding of the metadata attributes stored within the metadata store database. Current approaches in the literature have also enabled the extraction of metadata records for extant files, but not for deleted files. The objective of this paper is to research the persistence of records for deleted files within Spotlight's metadata store, identify if deleted database pages are recoverable from unallocated space on the volume, and to present a strategy for the processing of discovered records. In this paper, the structure of the metadata store database is outlined, and experimentation reveals that records persist for a period of time within the database but once deleted, are no longer recoverable. The experimentation also demonstrates that deleted pages from the database (containing metadata records) are recoverable from unused space on the filesystem.

Download:

http://ronaldchichester.com



Ronald Chichester

Log in ☐ only in current section

Search Site | Search

Home About Contact Presentations

Home › Presentations › 2019 › Essentials of Business Law › Step-by-Step Easy Encryption

Step-by-Step Easy Encryption

This webpage supplements the presentation made by Ron Chichester at the Essentials of Business Law in Dallas, Texas, on March 15, 2019.

Introduction

This step-by-step guide assumes that you are using a PC or laptop that utilizes Windows, Mac (OS X), or Linux operating systems. It also presumes that you (and your clients) are authorized to install certain cryptographic-related software. The final assumption is that since you and your client can use a royalty-free software application one any of the major operating systems, you will utilize this application to transmit client data in a secure manner. If you want to know why it is important to encrypt, read my article "Be a Hero" which has a deeper explanation.

This demonstration is based on usage of an open source software application called 7-zip.

Step 1 - Install 7-zip

You can download 7-zip from its website for the various operating systems here.

7ZIP

Home
7z Format
LZMA SDK
Download
FAQ
Support
Links

English
Chinese Simpl.

Download

Download 7-Zip 19.00 (2019-02-21) for Windows:

Link	Type	Windows	Description
Download	.exe	32-bit x86	7-Zip for 32-bit Windows
Download	.exe	64-bit x64	7-Zip for 64-bit Windows x64 (Intel 64 or AMD64)
Download	.7z	x86 / x64	7-Zip Extra: standalone console version, 7z DLL, Plugin for Far Manager
Download	.7z	Any	7-Zip Source code
Download	.7z	Any / x86 / x64	LZMA SDK: (C, C++, C#, Java)
Download	.msi	32-bit x86	(alternative MSI installer) 7-Zip for 32-bit Windows

THINGS TO THINK ABOUT IT

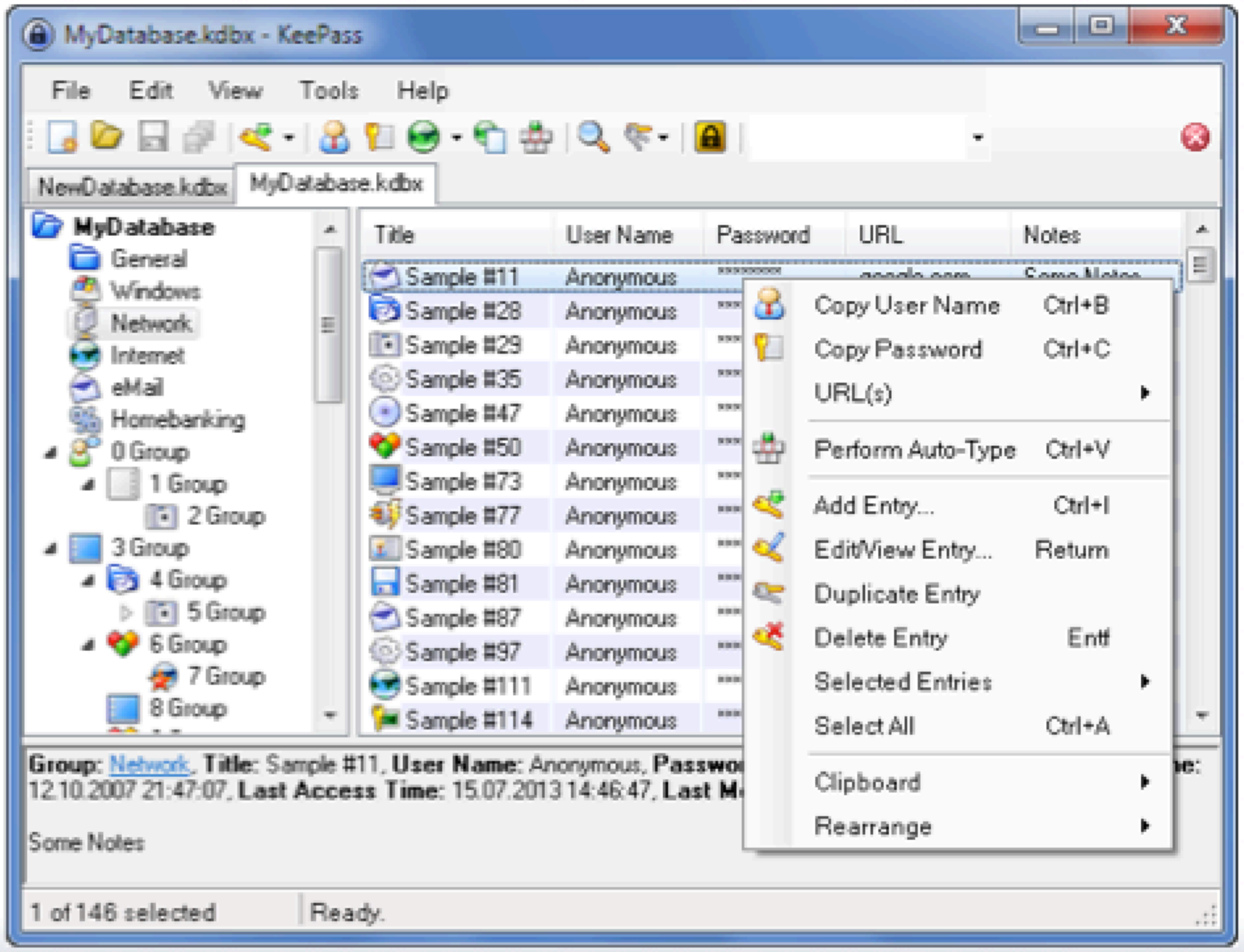
- Password management
  - for your clients
  - for you!
- Where is your data located?
  - Servers
  - Desktops
  - Backups
  - Laptops / Thumbdrives / External Drives

TOOLS YOU CAN USE

PASSWORD MANAGERS AND WHY YOU NEED THEM

- Login is simplified
- Secure notes
- Fill-in forms
- Share passwords
- Generate (secure) passwords
- Maintain digital assets
- Use across multiple devices
- 2-Factor authentication
- YubiKey authentication
- Example: A common password is: ji32k7au4a83

Keepass.info



Title	User Name	Password	URL	Notes
Sample #11	Anonymous	********	google.com	Some Notes
Sample #28	Anonymous	***		
Sample #29	Anonymous	***		
Sample #35	Anonymous	***		
Sample #47	Anonymous	***		
Sample #50	Anonymous	***		
Sample #73	Anonymous	***		
Sample #77	Anonymous	***		
Sample #80	Anonymous	***		
Sample #81	Anonymous	***		
Sample #87	Anonymous	***		
Sample #97	Anonymous	***		
Sample #111	Anonymous	***		
Sample #114	Anonymous	***		

Group: Network, **Title:** Sample #11, **User Name:** Anonymous, **Passwo**
12.10.2007 21:47:07, **Last Access Time:** 15.07.2013 14:46:47, **Last M**

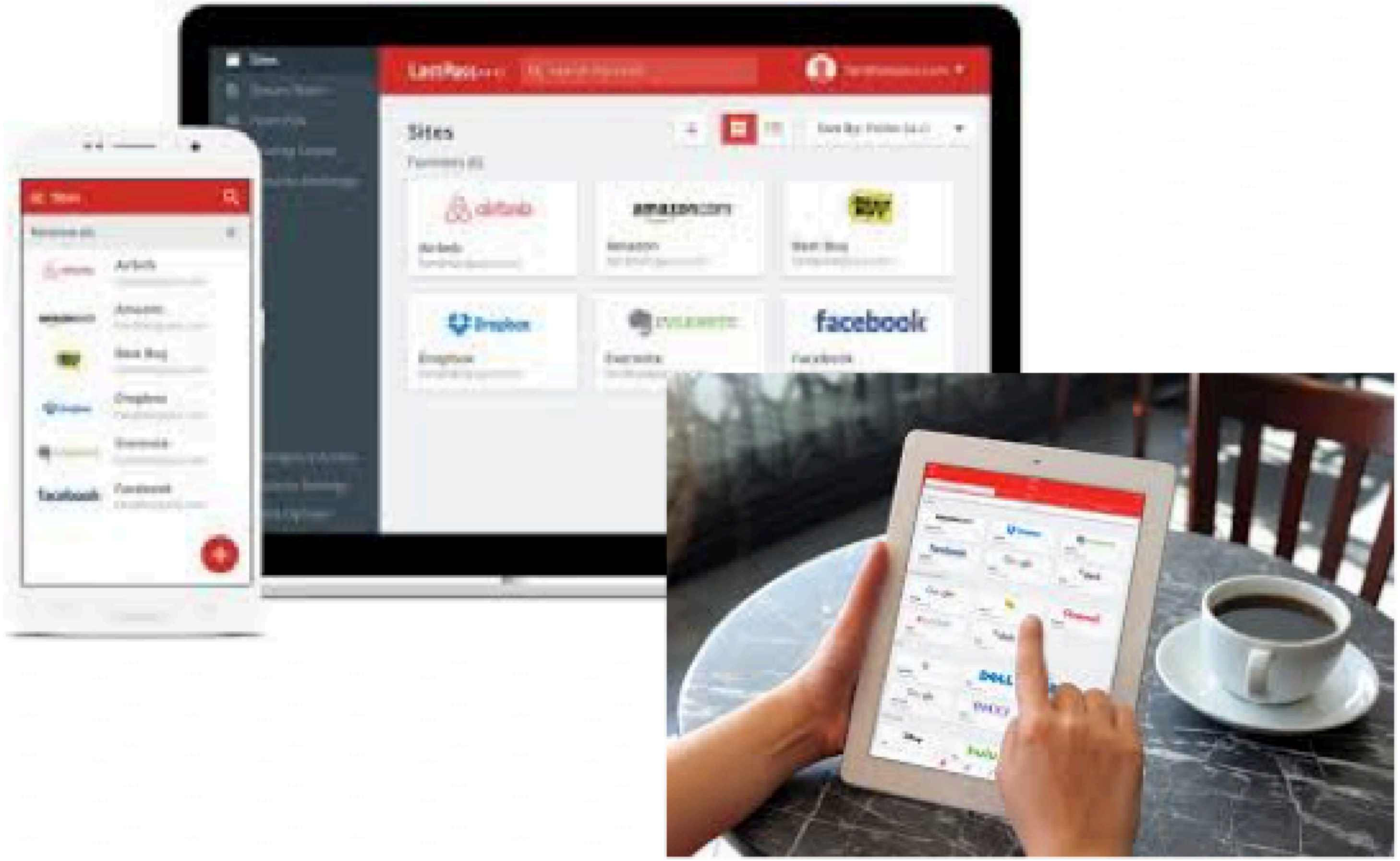
Some Notes

1 of 146 selected Ready.

Open Source Password Manager

- Free
- Open Source
- A Program on your computer
- Vault stored locally or on Dropbox

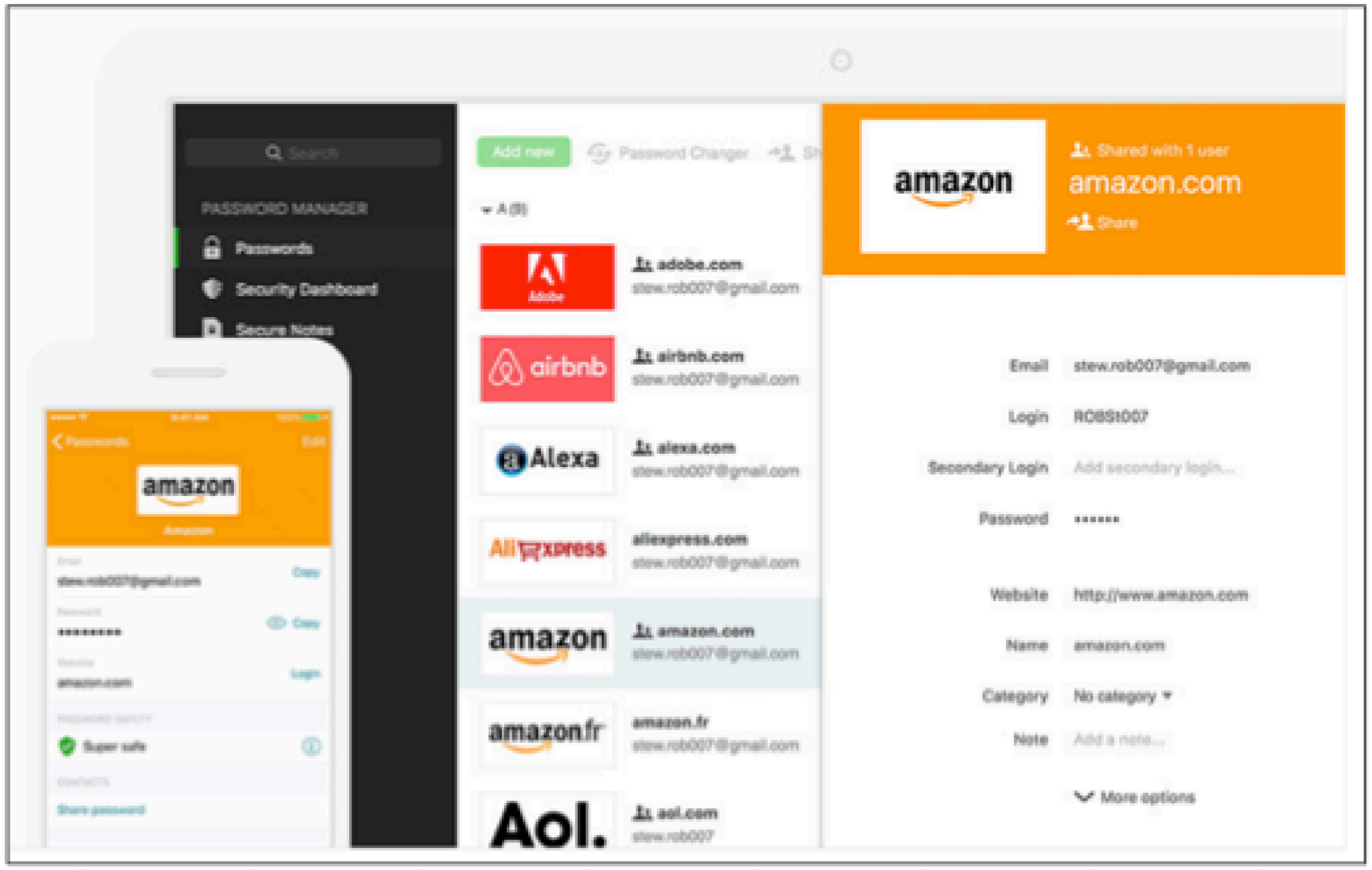
LastPass



Online Password Manager

- Free or Premium version for $36.00 or $48 a year
- A Web Browser Extension
- Vault stored on LastPass Server

Dashlane



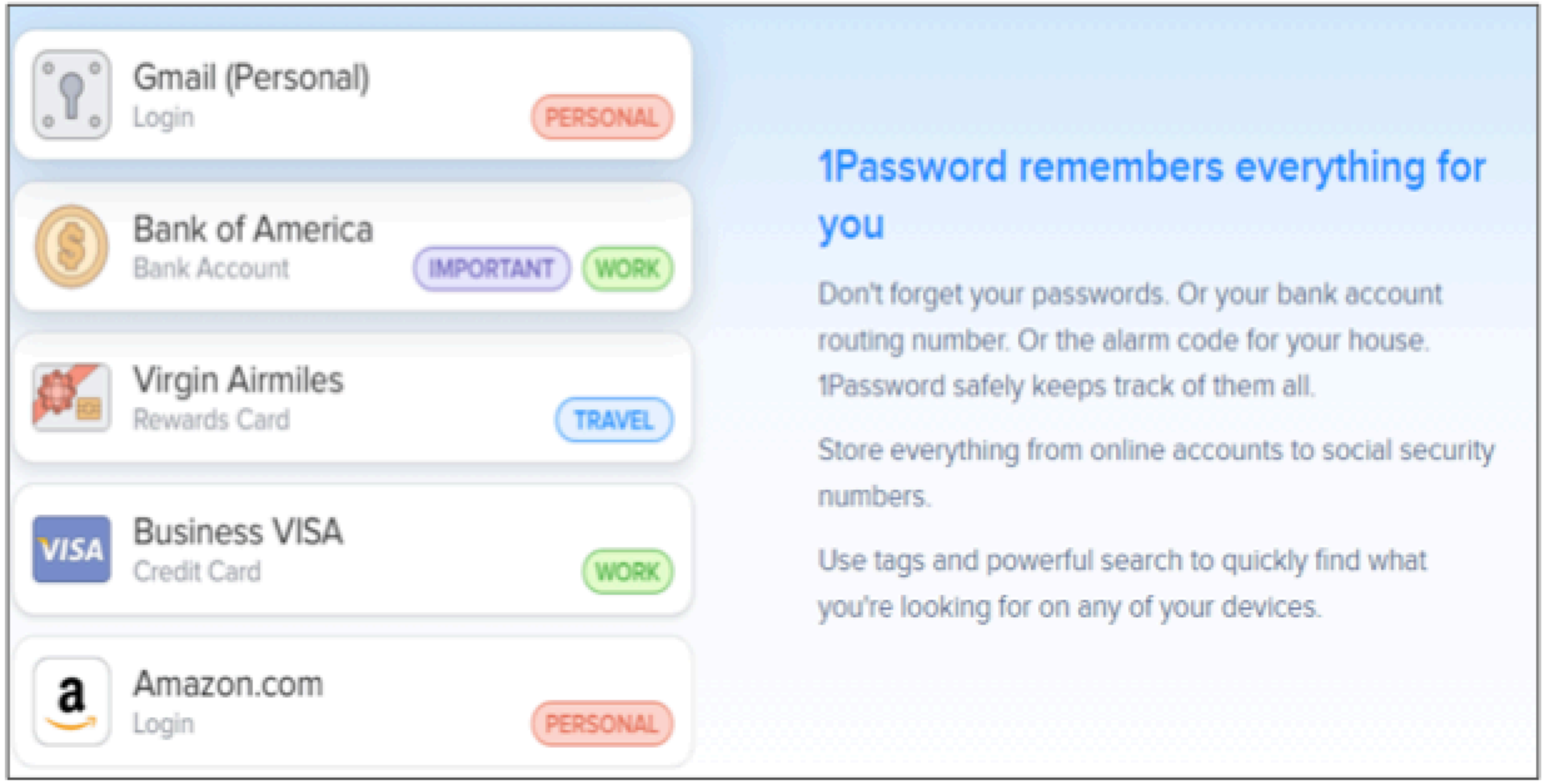
adobe.com stew.rob007@gmail.com
airbnb.com stew.rob007@gmail.com
alexa.com stew.rob007@gmail.com
aliexpress.com stew.rob007@gmail.com
amazon.com stew.rob007@gmail.com
amazon.fr stew.rob007@gmail.com
aol.com stew.rob007

Email stew.rob007@gmail.com
Login ROBSt007
Secondary Login Add secondary login...
Password ••••••
Website http://www.amazon.com
Name amazon.com
Category No category
Note Add a note...

Password manager

- Free or premium version for $60 or $120 a year
- A Web Browser Extension
- Vault stored on Dashlane Server

1Password.Com



Gmail (Personal)
Login
PERSONAL

Bank of America
Bank Account
IMPORTANT WORK

Virgin Airmiles
Rewards Card
TRAVEL

Business VISA
Credit Card
WORK

Amazon.com
Login
PERSONAL

1Password remembers everything for you

Don't forget your passwords. Or your bank account routing number. Or the alarm code for your house. 1Password safely keeps track of them all.

Store everything from online accounts to social security numbers.

Use tags and powerful search to quickly find what you're looking for on any of your devices.

Password Manager

- Premium version for $36 or $60 a year
- A Web Browser Extension
- Vault stored on your computer or Dropbox

COMPUTER AND TECHNOLOGY SECTION

Robert@TexasInheritance.Com

iOS ANDROID GOOGLE MICROSOFT $36

Encryption

- Any encryption is better than no encryption.
- How do you encrypt files, folders or drives?

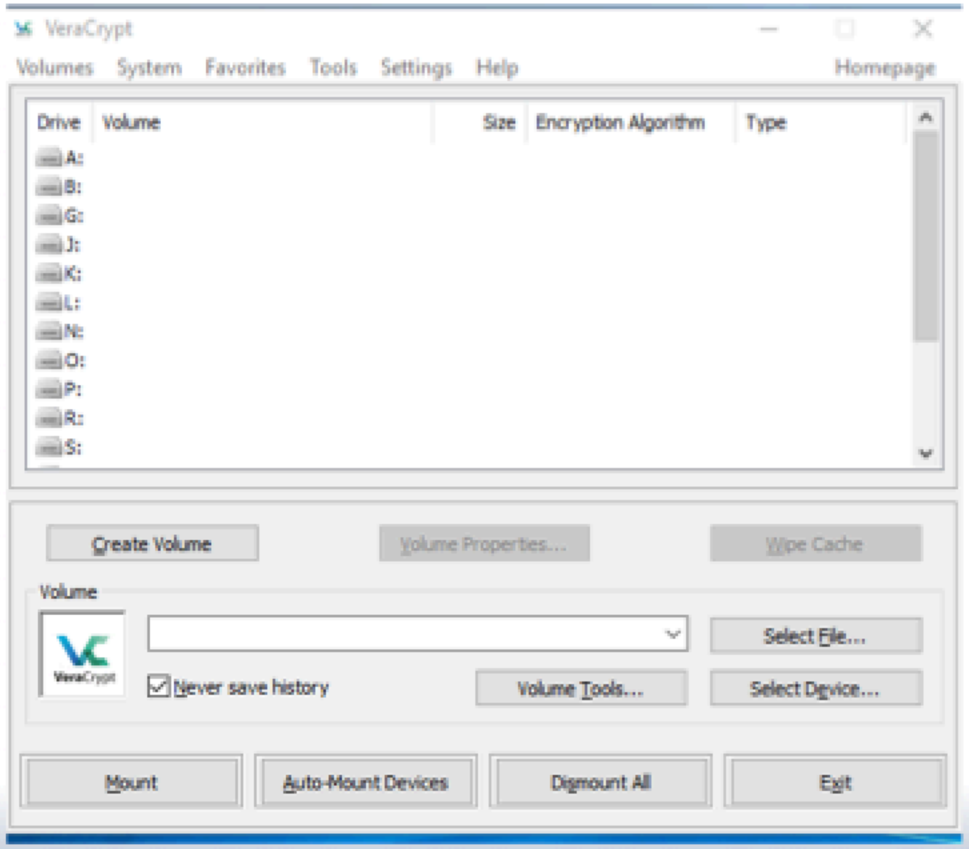
7-Zip by SourceForge.net

- A free zip tool – open source
- Password protect zip files

VeraCrypt by Idrix.fr

A secure, open source replacement for Truecrypt

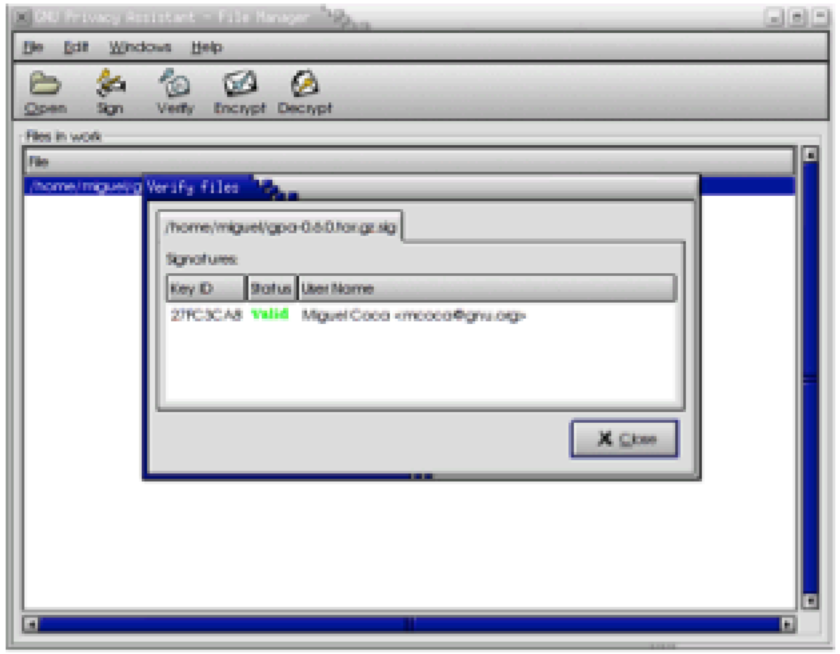
- Encrypt files, folders or drives



Gnupg.org

GPA - THE GNU PRIVACY ASSISTANT

- **PGP type program to encrypt files, messages, etc.**
- Works with Outlook
- Public and Private Keys



/home/miguel/gpa-0.6.0.tar.gz.sig

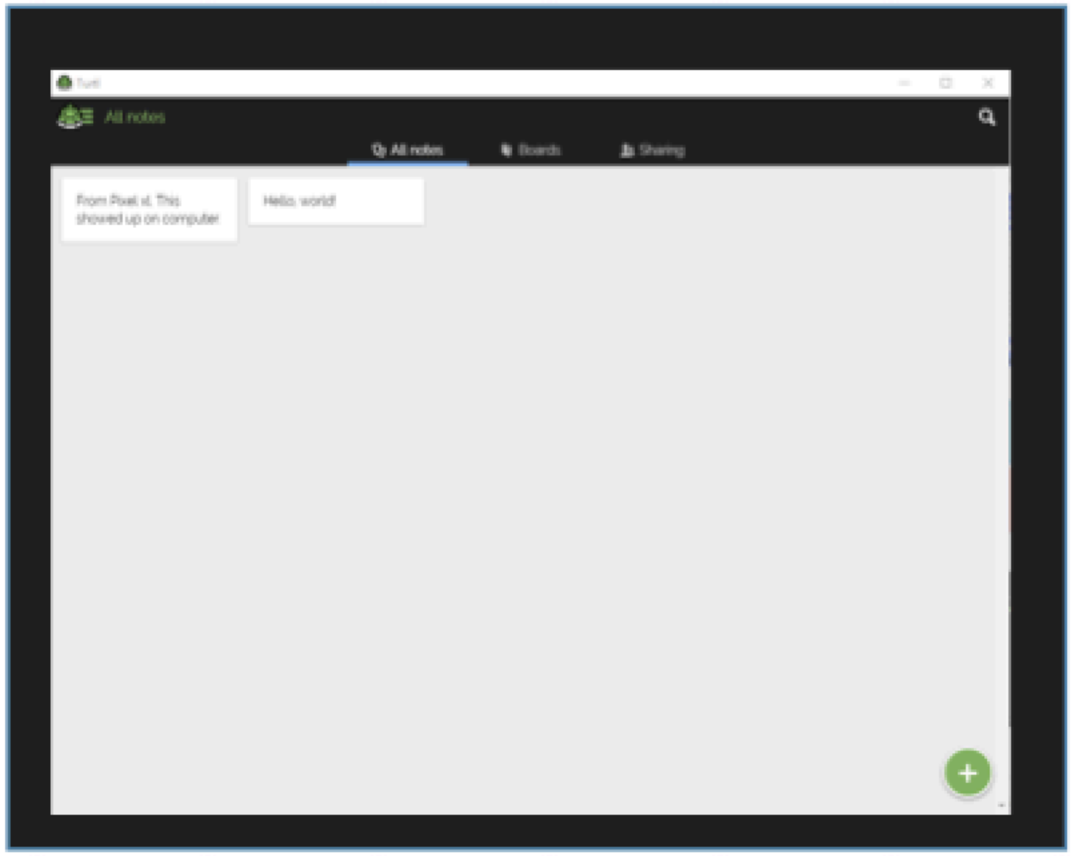
Signatures:

Key ID	Status	User Name
27FC3CA8	Valid	Miguel Coca <mcoca@gnu.org>

Turtlapp.com

Notes, bookmark websites, store documents, photos, research, passwords, etc.
(Like Evernote but encrypted)

- Can share notes with others and both make changes
- Open Source

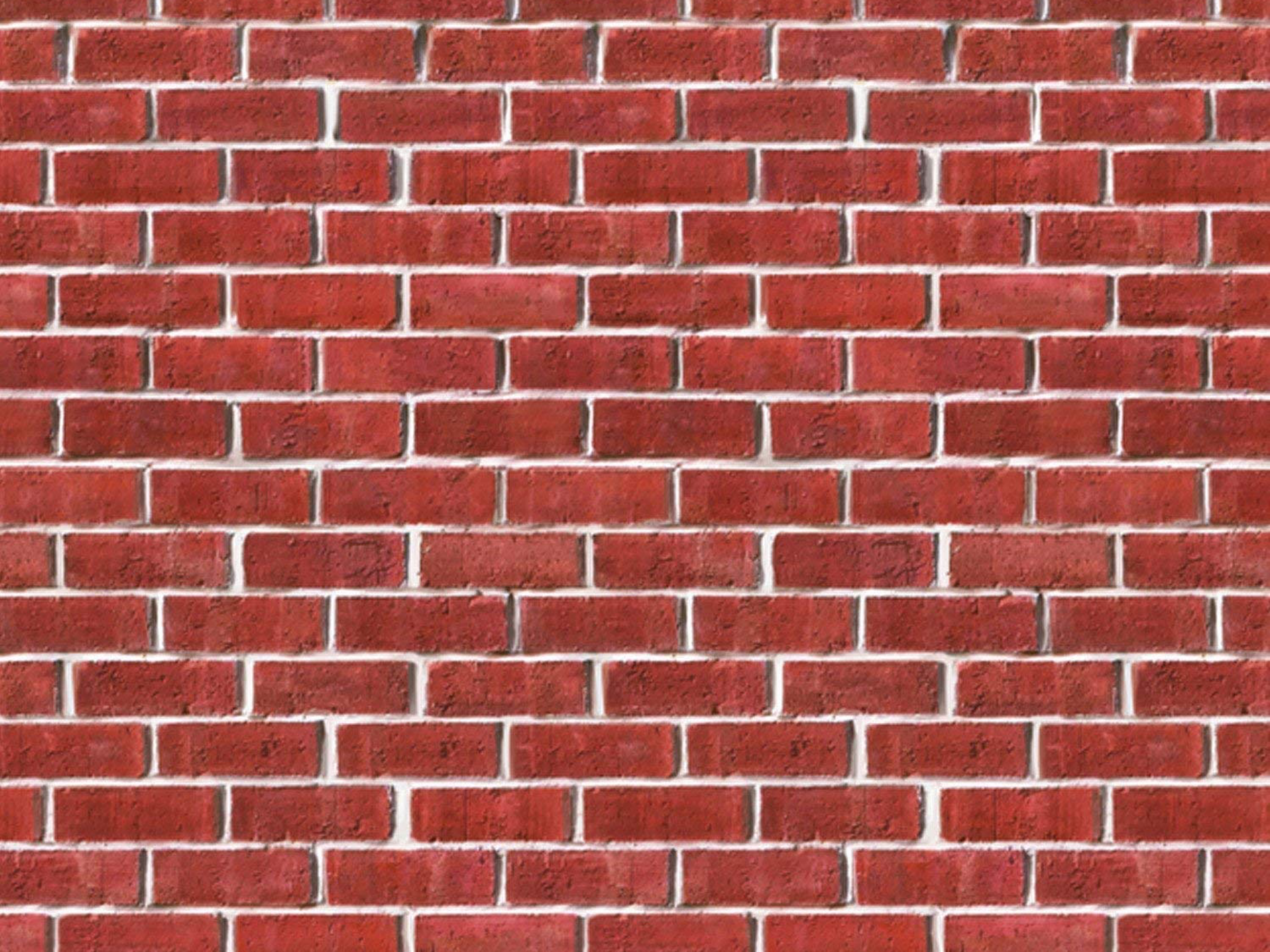


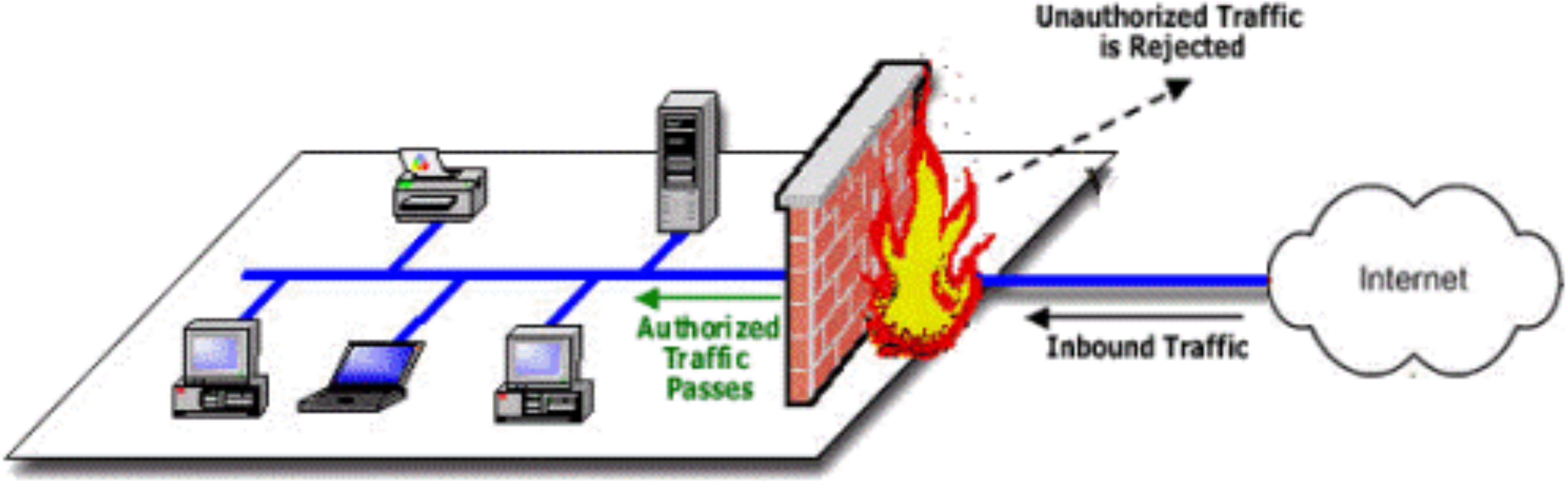
From Pixel xl. This showed up on computer

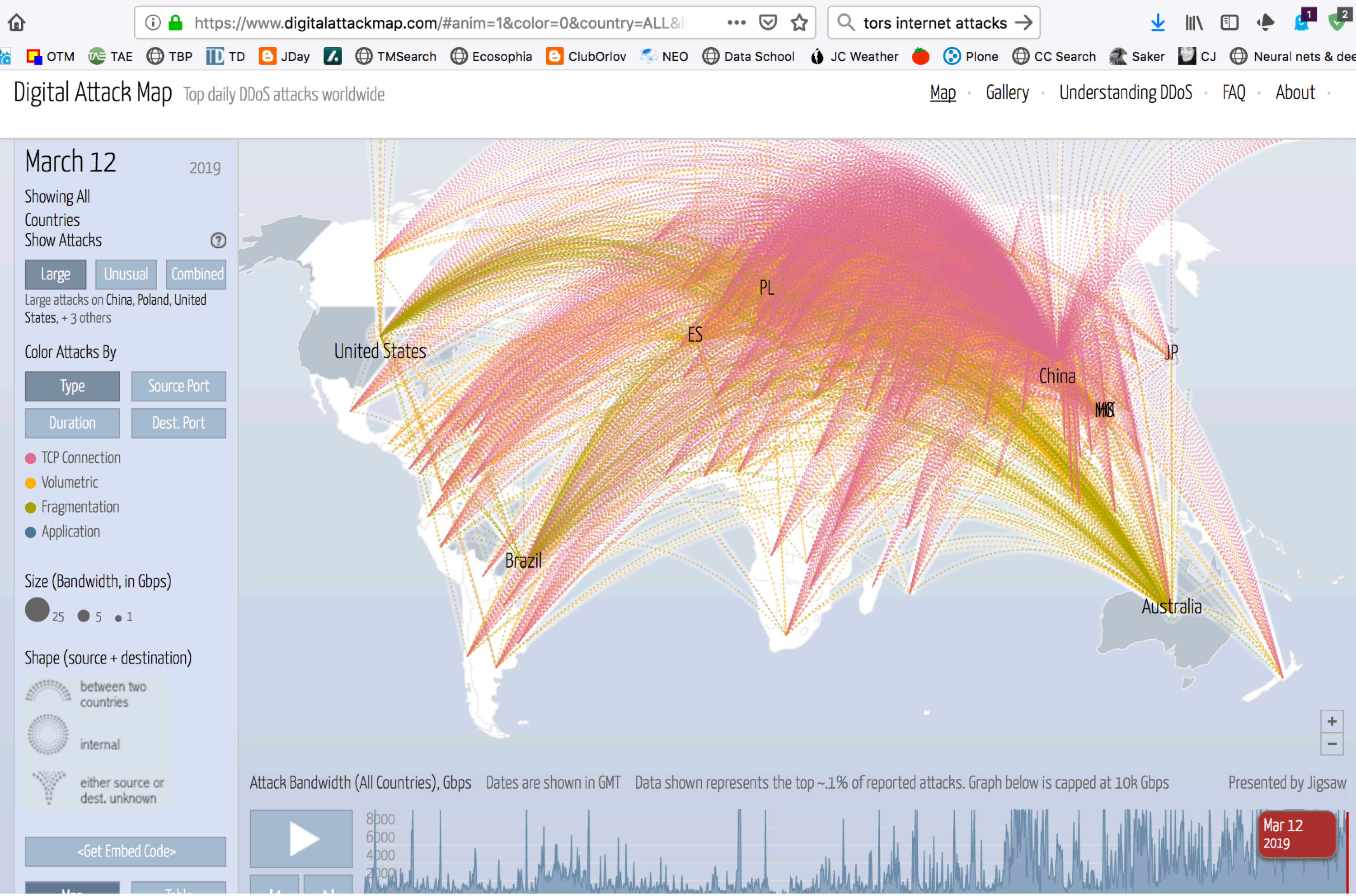
Hello, world!

Coming soon! iOS | ANDROID | GOOGLE | MICROSOFT | $0

FIREWALLS




Unauthorized Traffic
is Rejected
Internet
Authorized
Traffic
Passes
Inbound Traffic



https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&l

tors internet attacks

OTM TAE TBP TD JDay TMSearch Ecosophia ClubOrlov NEO Data School JC Weather Plone CC Search Saker CJ Neural nets & dee

Digital Attack Map Top daily DDoS attacks worldwide

Map · Gallery · Understanding DDoS · FAQ · About ·

March 12 2019

Showing All Countries

Show Attacks

Large Unusual Combined

Large attacks on China, Poland, United States, + 3 others

Color Attacks By

Type Source Port

Duration Dest. Port

- ● TCP Connection
- ● Volumetric
- ● Fragmentation
- ● Application

Size (Bandwidth, in Gbps)

● 25 ● 5 ● 1

Shape (source + destination)

between two countries

internal

either source or dest. unknown

<Get Embed Code>

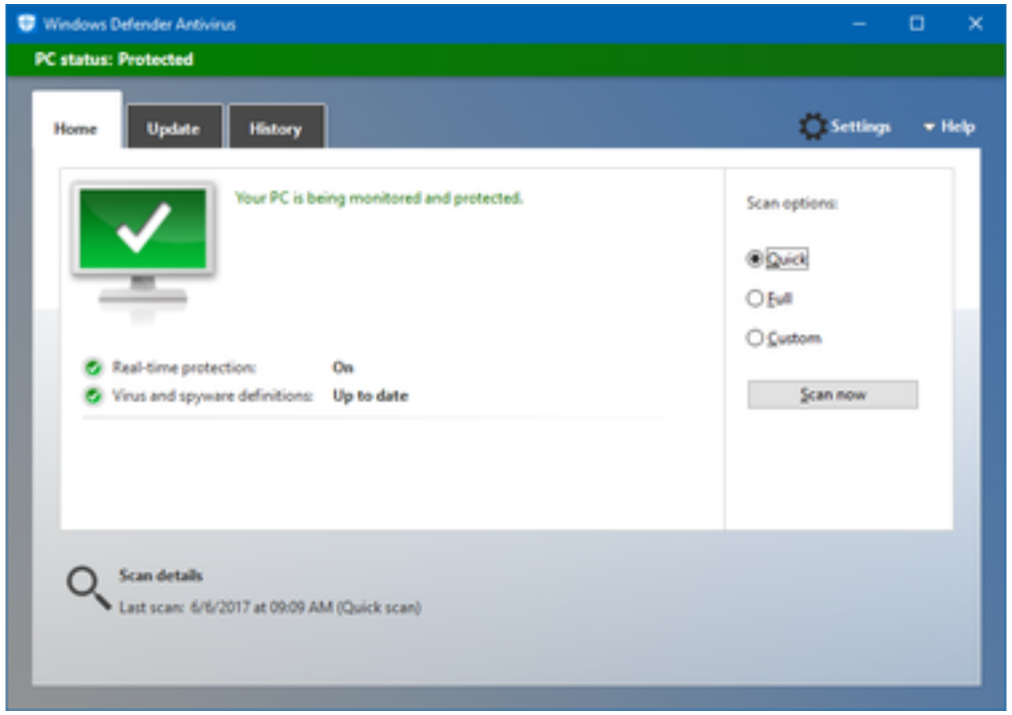
Attack Bandwidth (All Countries), Gbps   Dates are shown in GMT   Data shown represents the top ~.1% of reported attacks. Graph below is capped at 10k Gbps   Presented by Jigsaw

> “Well, I had talked to some experts, and I was fully expecting maybe a week, maybe never, certainly not less than a day," McGill told NPR's Ari Shapiro. "But it came a lot sooner. It was 41 minutes. [The second attempt was] within 10 or 15 minutes [and the third was] another 10 or 15."

-An Experiment Shows How Quickly The Internet Of Things Can Be Hacked

https://www.npr.org/sections/alltechconsidered/2016/11/01/500253637/an-experiment-shows-how-quickly-the-internet-of-things-can-be-hacked

Firewalls for Operating Systems



PC status: Protected

Your PC is being monitored and protected.

Real-time protection: On

Virus and spyware definitions: Up to date

Scan options:

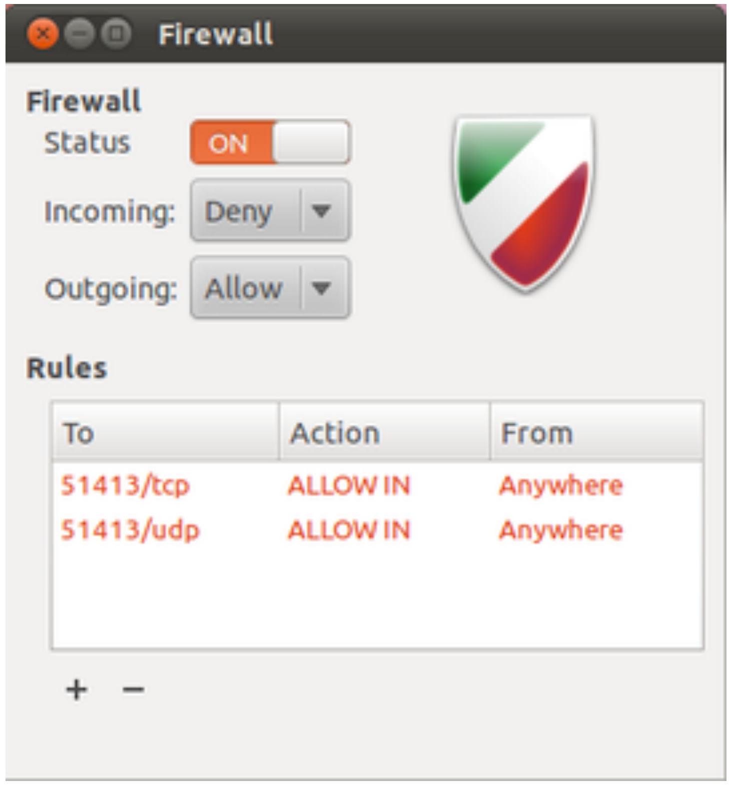
● Quick

○ Full

○ Custom

Scan details

Last scan: 6/6/2017 at 09:09 AM (Quick scan)



Firewall

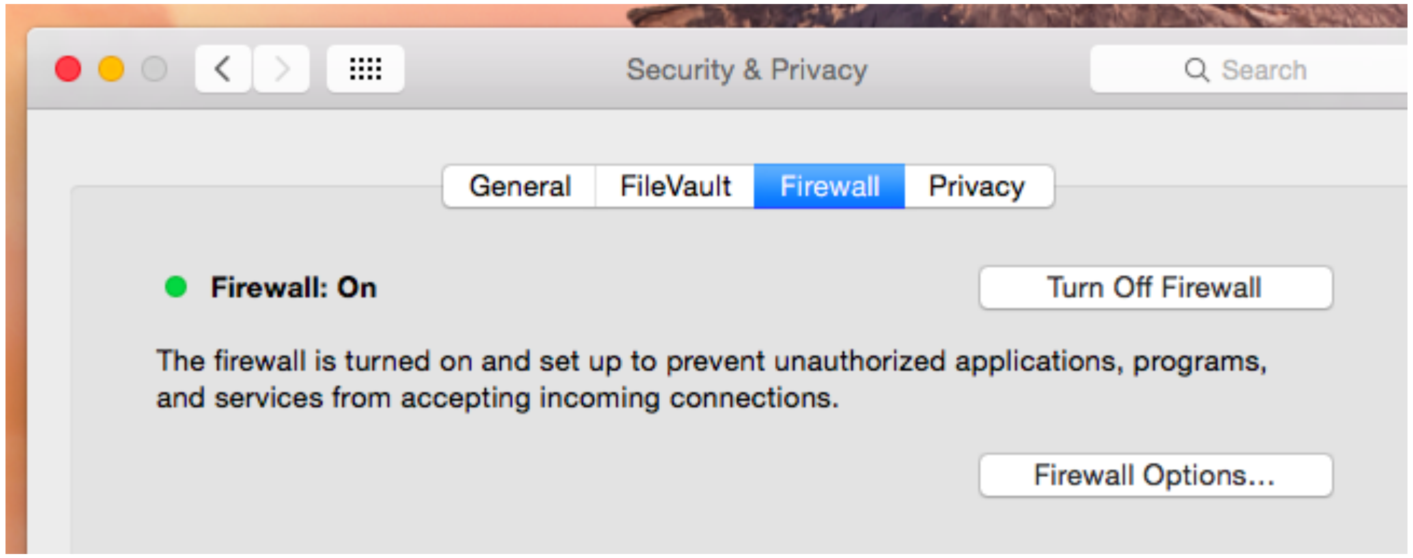
Status: ON

Incoming: Deny

Outgoing: Allow

Rules

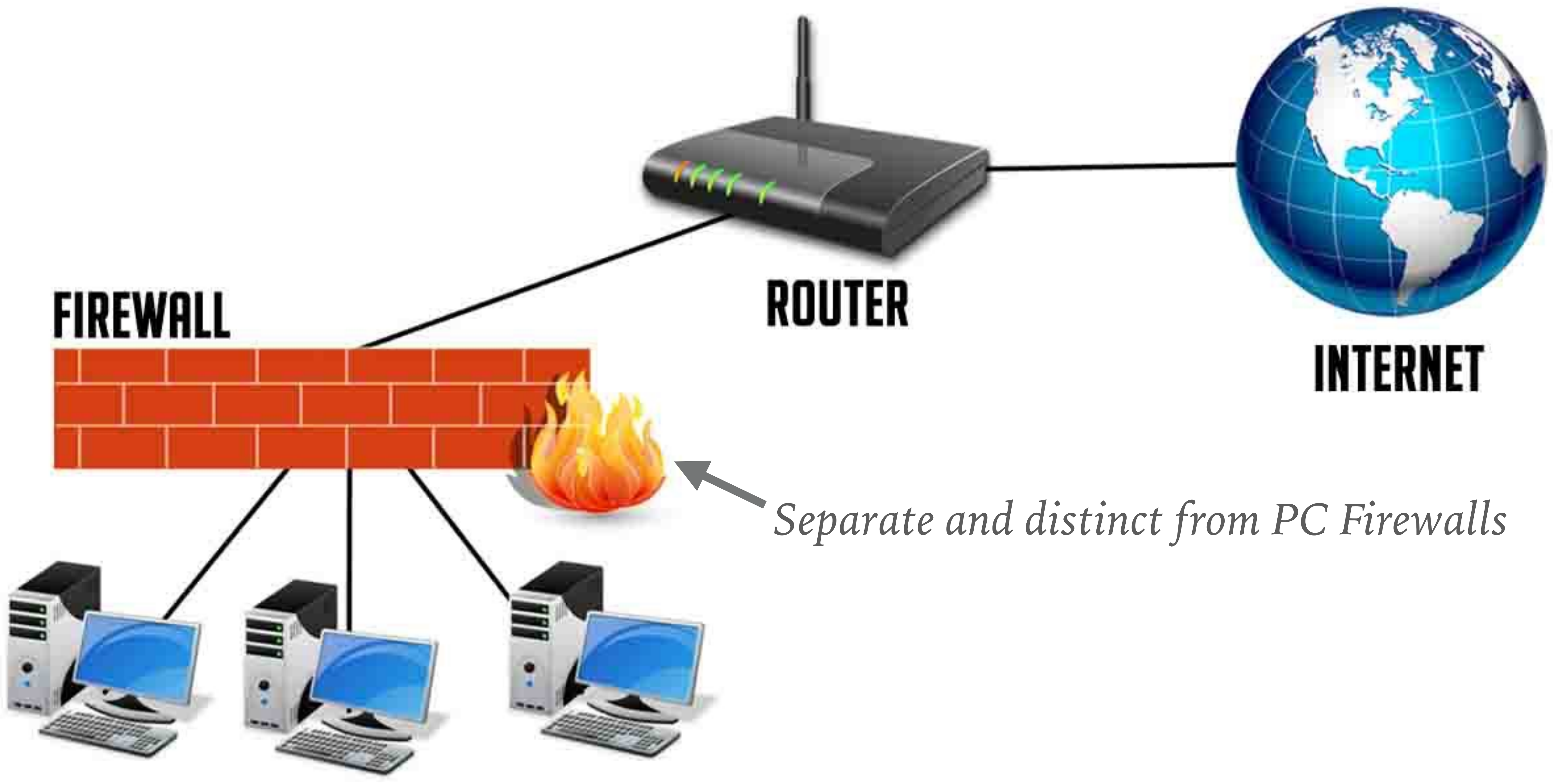
To	Action	From
51413/tcp	ALLOW IN	Anywhere
51413/udp	ALLOW IN	Anywhere



Firewall: On

The firewall is turned on and set up to prevent unauthorized applications, programs, and services from accepting incoming connections.

Stand-alone Firewall

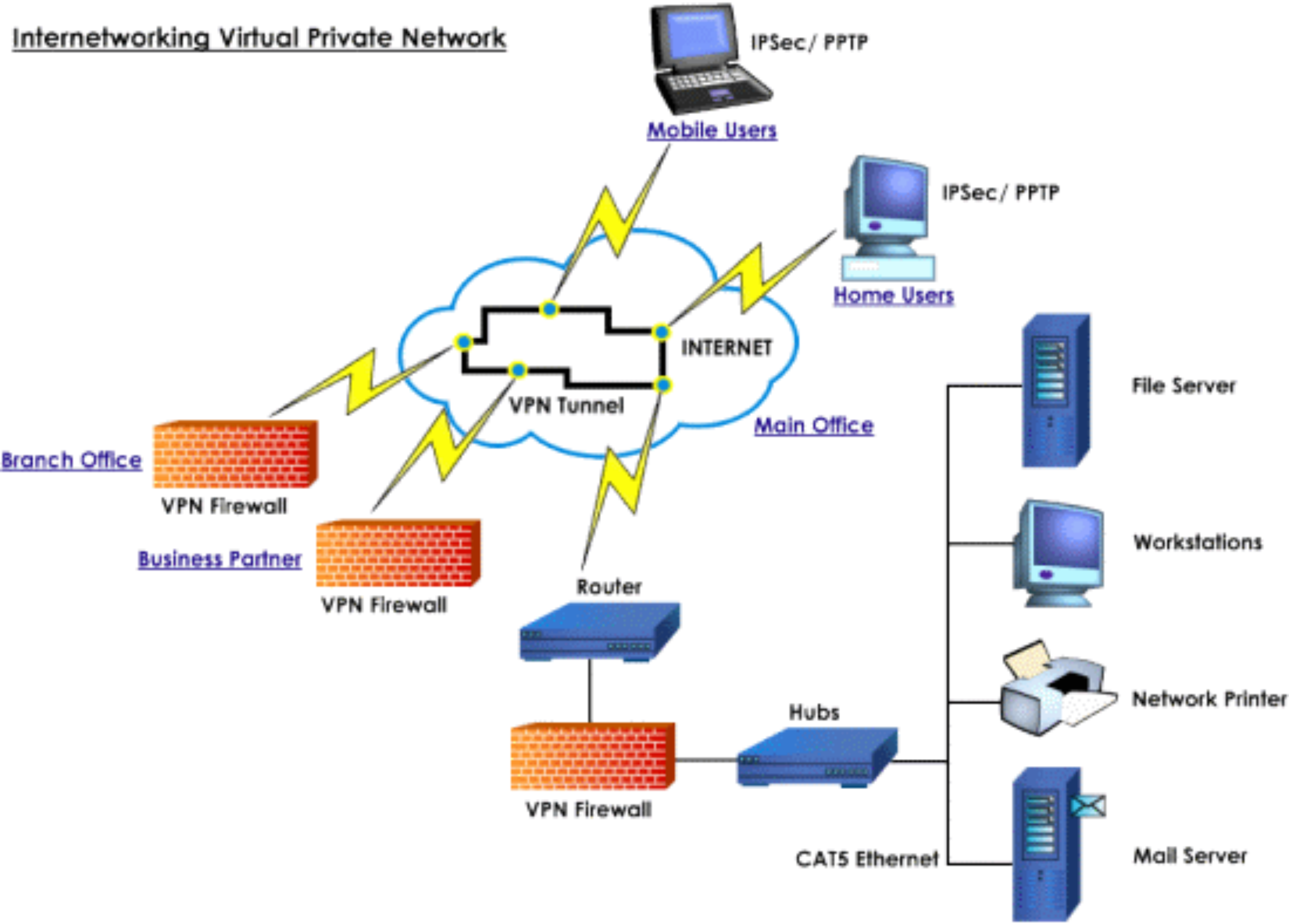


Separate and distinct from PC Firewalls

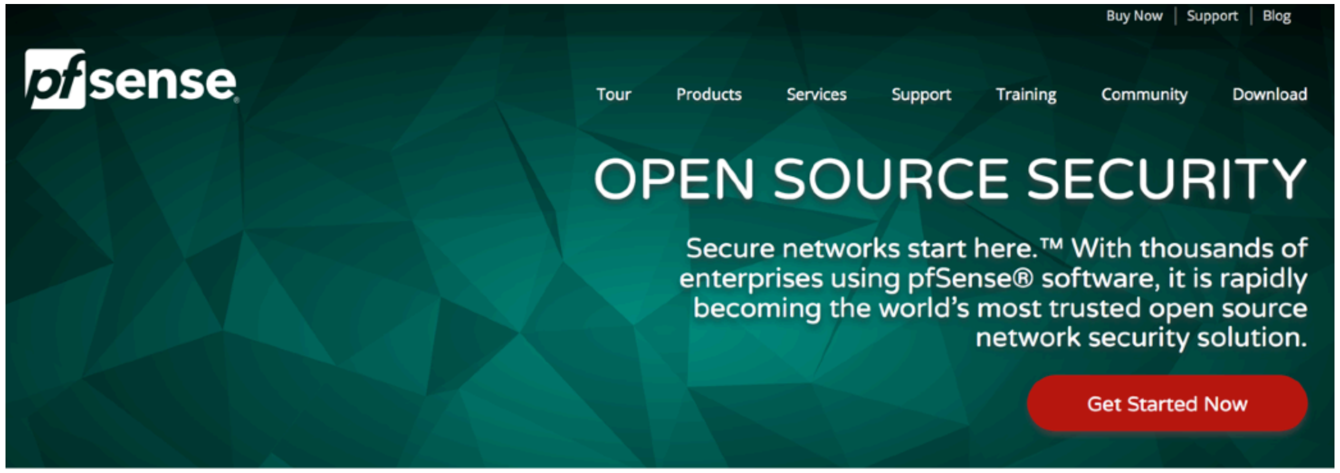
In addition…

…you can have your own VPN

Internetworking Virtual Private Network



OPEN SOURCE SOFTWARE



OPEN SOURCE SECURITY

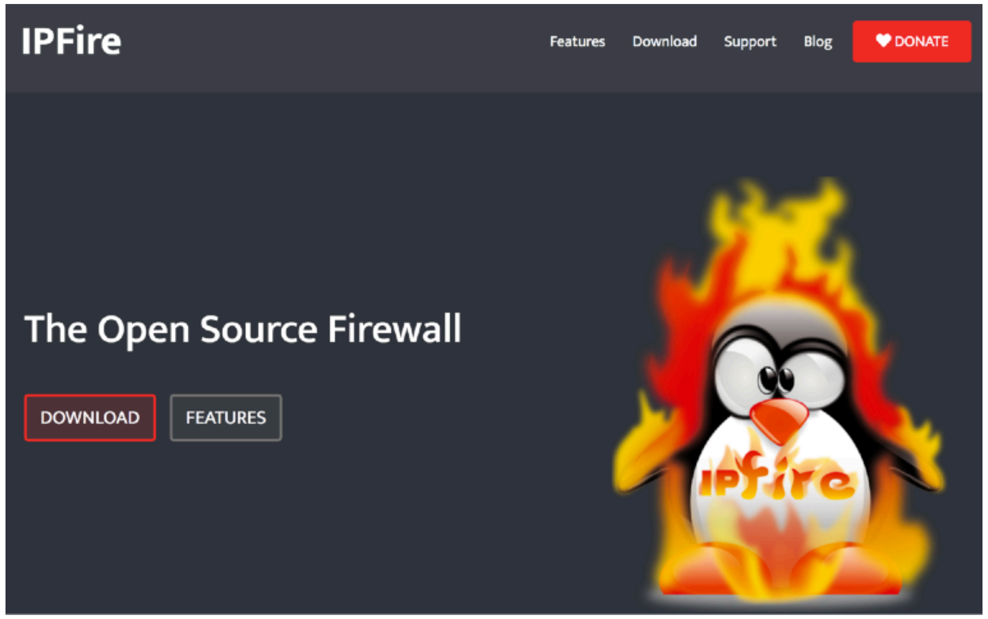
Secure networks start here.™ With thousands of enterprises using pfSense® software, it is rapidly becoming the world's most trusted open source network security solution.

https://www.pfsense.org/

Your Private Path to Access Network Resources and Services Securely

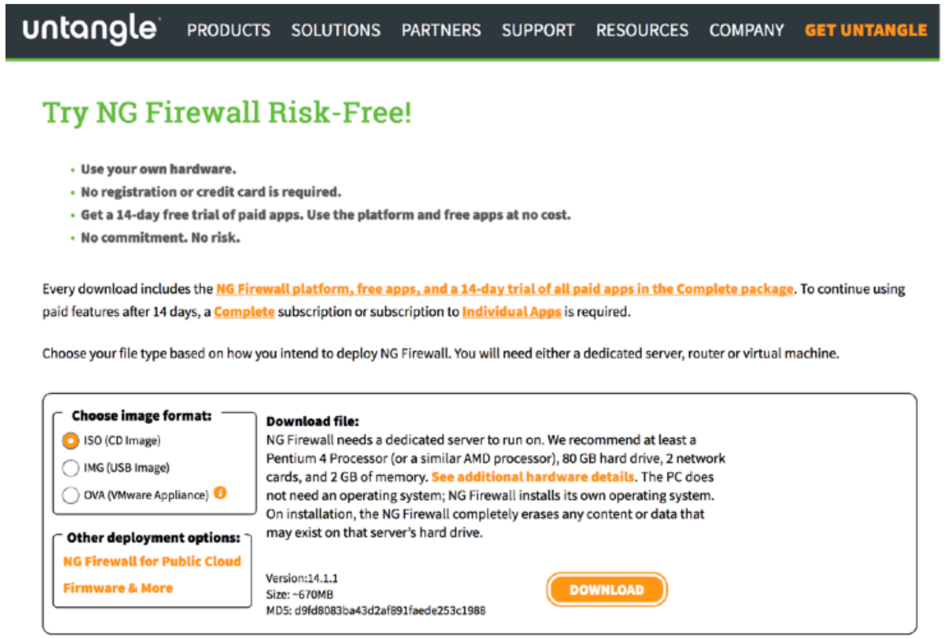
OpenVPN provides flexible VPN solutions to secure your data communications, whether it's for Internet privacy, remote access for employees, securing IoT, or for networking Cloud data centers. Our VPN Server software solution can be deployed on-premises using standard servers or virtual appliances, or on the cloud.

https://openvpn.net/



The Open Source Firewall

https://www.ipfire.org/



Try NG Firewall Risk-Free!

- Use your own hardware.
- No registration or credit card is required.
- Get a 14-day free trial of paid apps. Use the platform and free apps at no cost.
- No commitment. No risk.

Every download includes the NG Firewall platform, free apps, and a 14-day trial of all paid apps in the Complete package. To continue using paid features after 14 days, a Complete subscription or subscription to Individual Apps is required.

Choose your file type based on how you intend to deploy NG Firewall. You will need either a dedicated server, router or virtual machine.

Choose image format:

● ISO (CD Image)
○ IMG (USB Image)
○ OVA (VMware Appliance)

Other deployment options:

NG Firewall for Public Cloud
Firmware & More

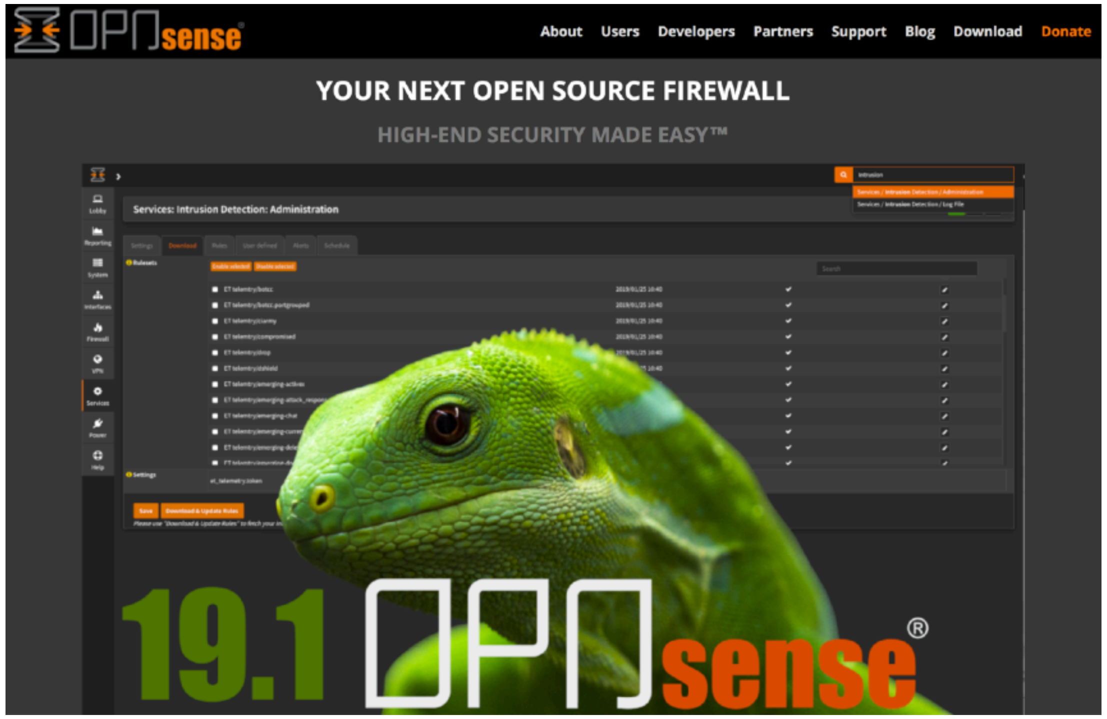
Download file:

NG Firewall needs a dedicated server to run on. We recommend at least a Pentium 4 Processor (or a similar AMD processor), 80 GB hard drive, 2 network cards, and 2 GB of memory. See additional hardware details. The PC does not need an operating system; NG Firewall installs its own operating system. On installation, the NG Firewall completely erases any content or data that may exist on that server's hard drive.

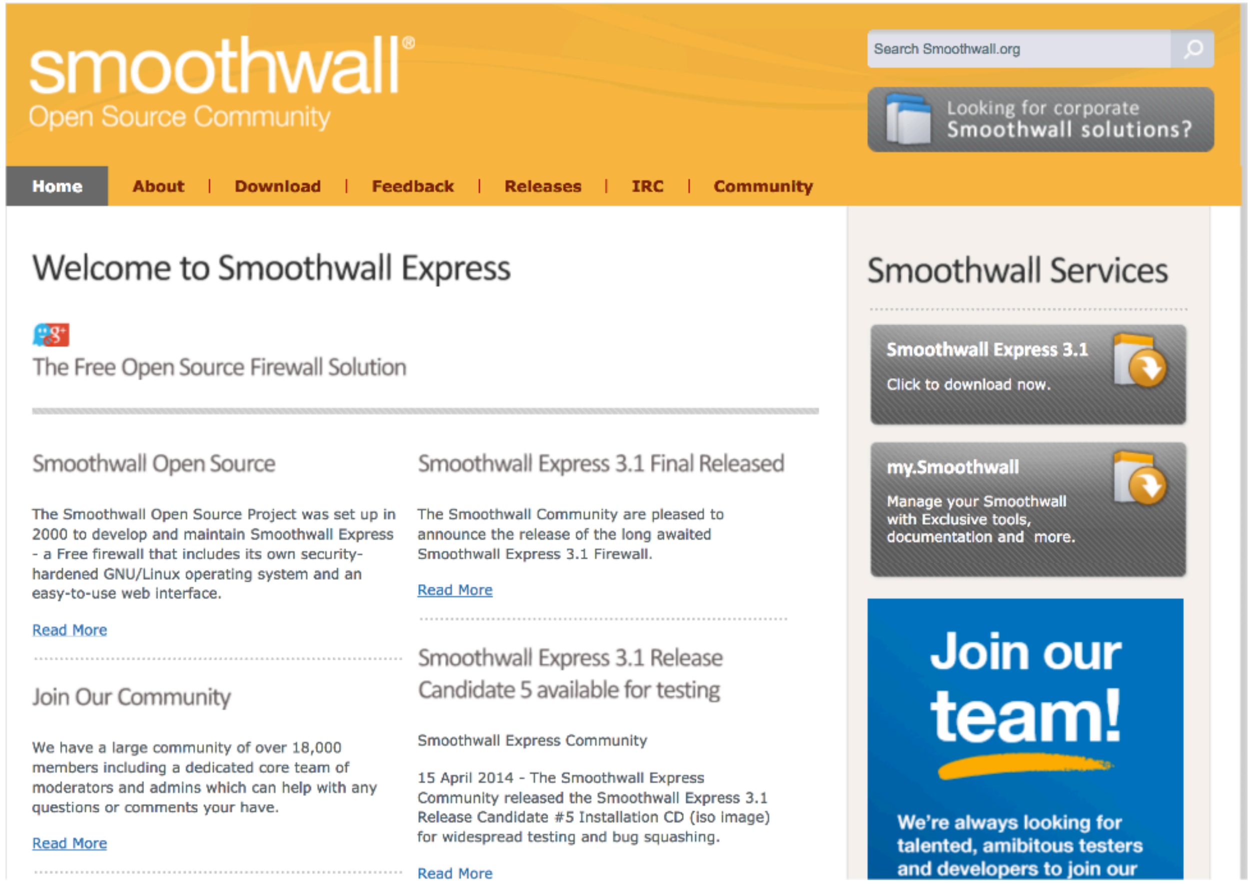
Version:14.1.1
Size: ~670MB
MD5: d9fd8083ba43d2af891faede253c1988

https://www.untangle.com/get-untangle/

OPEN SOURCE SOFTWARE…


OPNsense
About
Users
Developers
Partners
Support
Blog
Download
Donate
YOUR NEXT OPEN SOURCE FIREWALL
HIGH-END SECURITY MADE EASY™
Services: Intrusion Detection: Administration
19.1 OPNsense®

https://opnsense.org/



Welcome to Smoothwall Express

The Free Open Source Firewall Solution

Smoothwall Open Source

The Smoothwall Open Source Project was set up in 2000 to develop and maintain Smoothwall Express - a Free firewall that includes its own security-hardened GNU/Linux operating system and an easy-to-use web interface.

Read More

Join Our Community

We have a large community of over 18,000 members including a dedicated core team of moderators and admins which can help with any questions or comments your have.

Read More

Smoothwall Express 3.1 Final Released

The Smoothwall Community are pleased to announce the release of the long awaited Smoothwall Express 3.1 Firewall.

Read More

Smoothwall Express 3.1 Release Candidate 5 available for testing

Smoothwall Express Community

15 April 2014 - The Smoothwall Express Community released the Smoothwall Express 3.1 Release Candidate #5 Installation CD (iso image) for widespread testing and bug squashing.

Read More

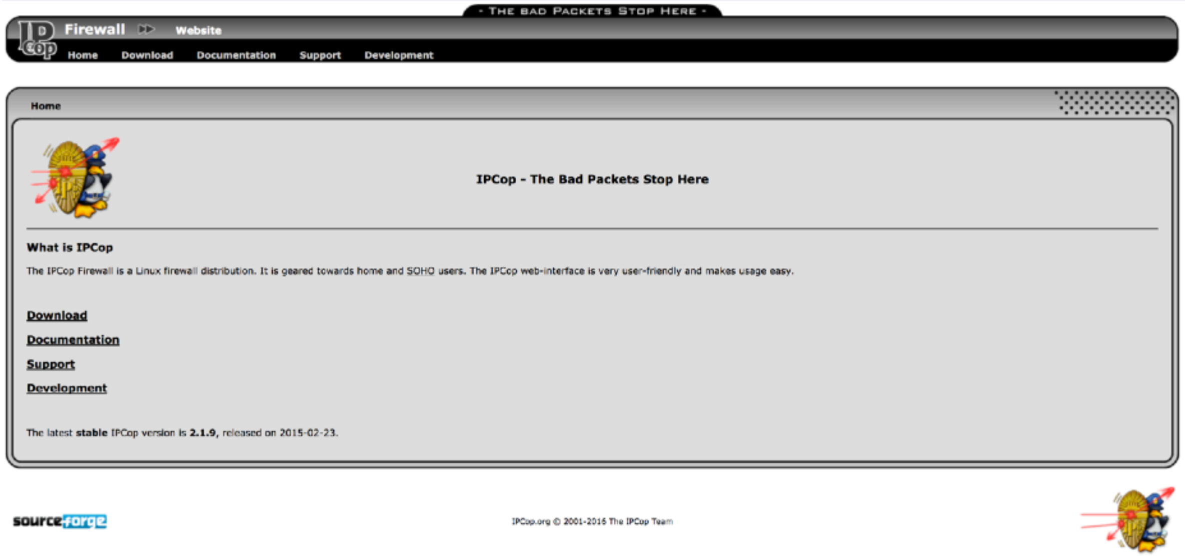
Smoothwall Services

Smoothwall Express 3.1
Click to download now.

my.Smoothwall
Manage your Smoothwall with Exclusive tools, documentation and more.

Join our team!
We're always looking for talented, amibitous testers and developers to join our

http://www.smoothwall.org/



IPCop - The Bad Packets Stop Here

What is IPCop

The IPCop Firewall is a Linux firewall distribution. It is geared towards home and SOHO users. The IPCop web-interface is very user-friendly and makes usage easy.

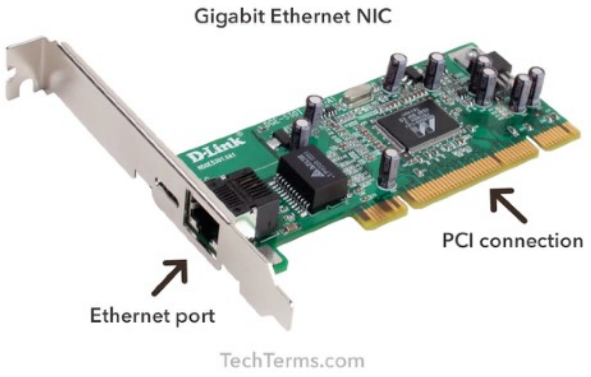
Download
Documentation
Support
Development

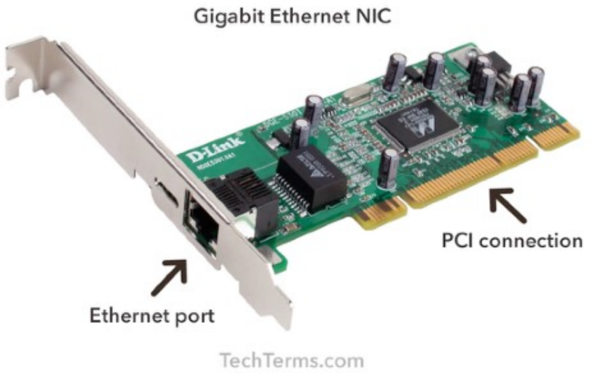
The latest **stable** IPCop version is **2.1.9,** released on 2015-02-23.

IPCop.org © 2001-2016 The IPCop Team

http://ipcop.sourceforge.net/

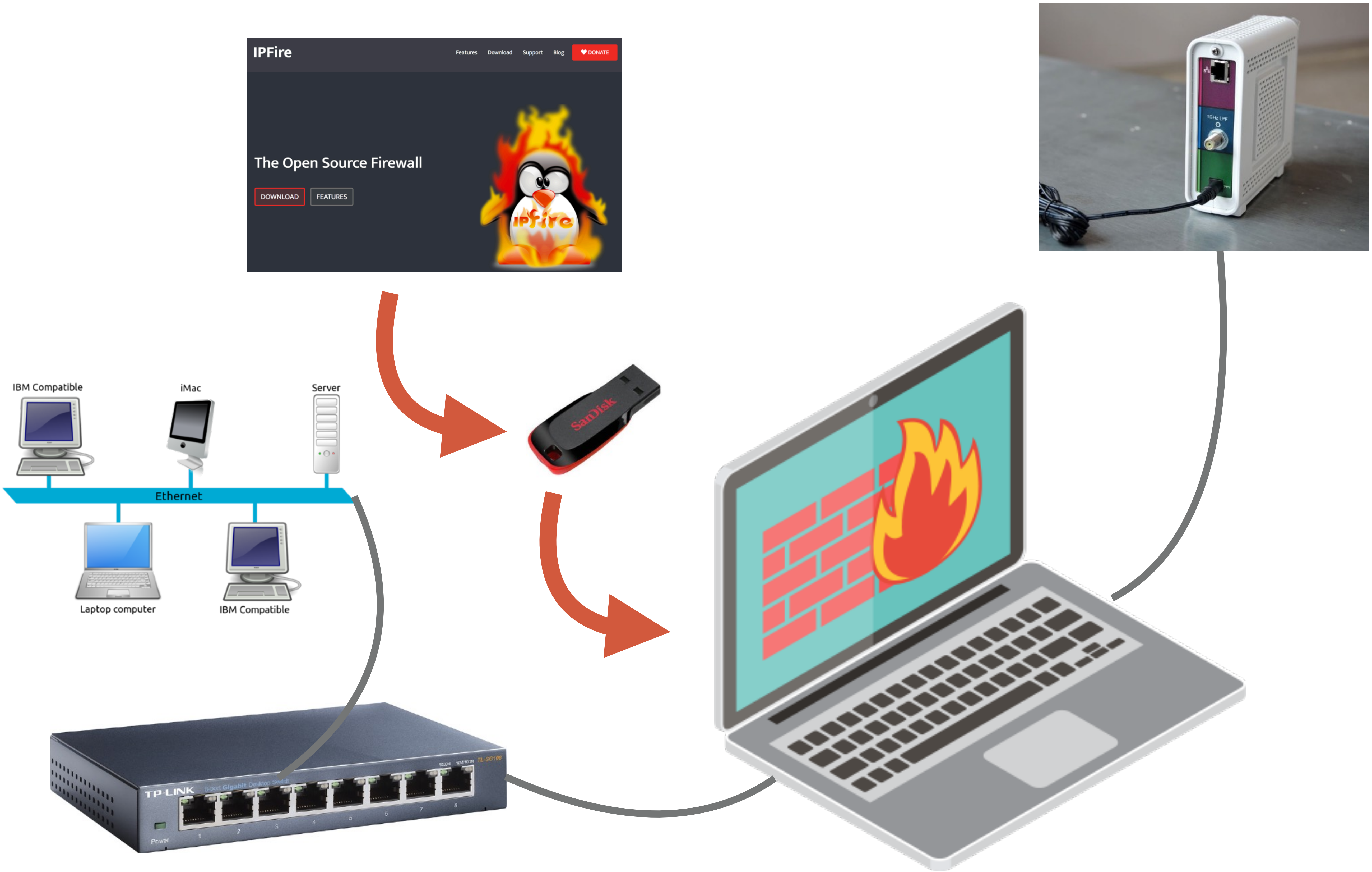
+ HARDWARE



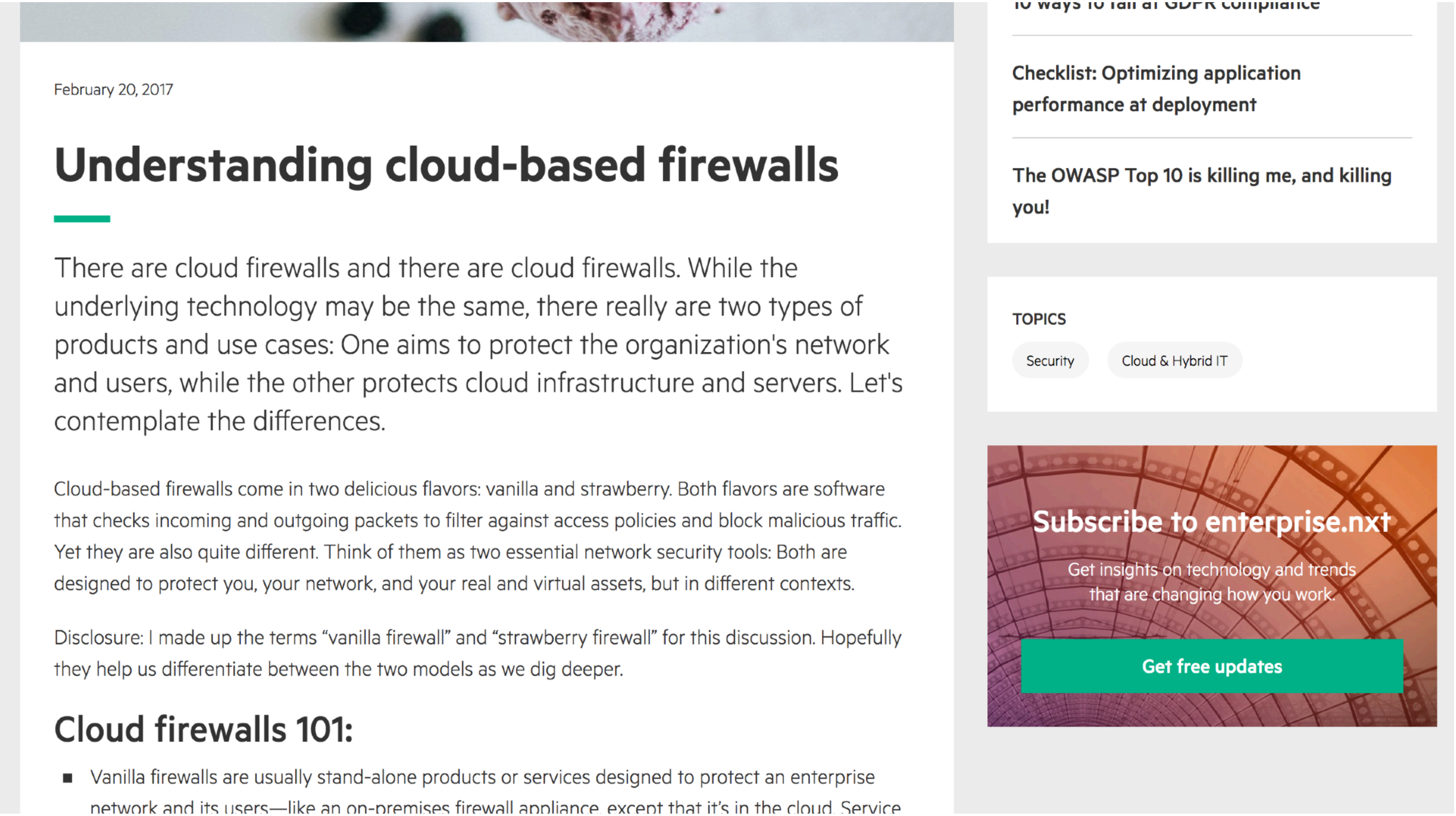


2 GB RAM + 1 USB Port or CD

RUN IT OFF A USB STICK (NO HARD DISK)…



YOU CAN EVEN HAVE CLOUD FIREWALLS



10 ways to fail at GDPR compliance

Checklist: Optimizing application performance at deployment

The OWASP Top 10 is killing me, and killing you!

TOPICS

Security

Cloud & Hybrid IT

February 20, 2017

Understanding cloud-based firewalls

There are cloud firewalls and there are cloud firewalls. While the underlying technology may be the same, there really are two types of products and use cases: One aims to protect the organization's network and users, while the other protects cloud infrastructure and servers. Let's contemplate the differences.

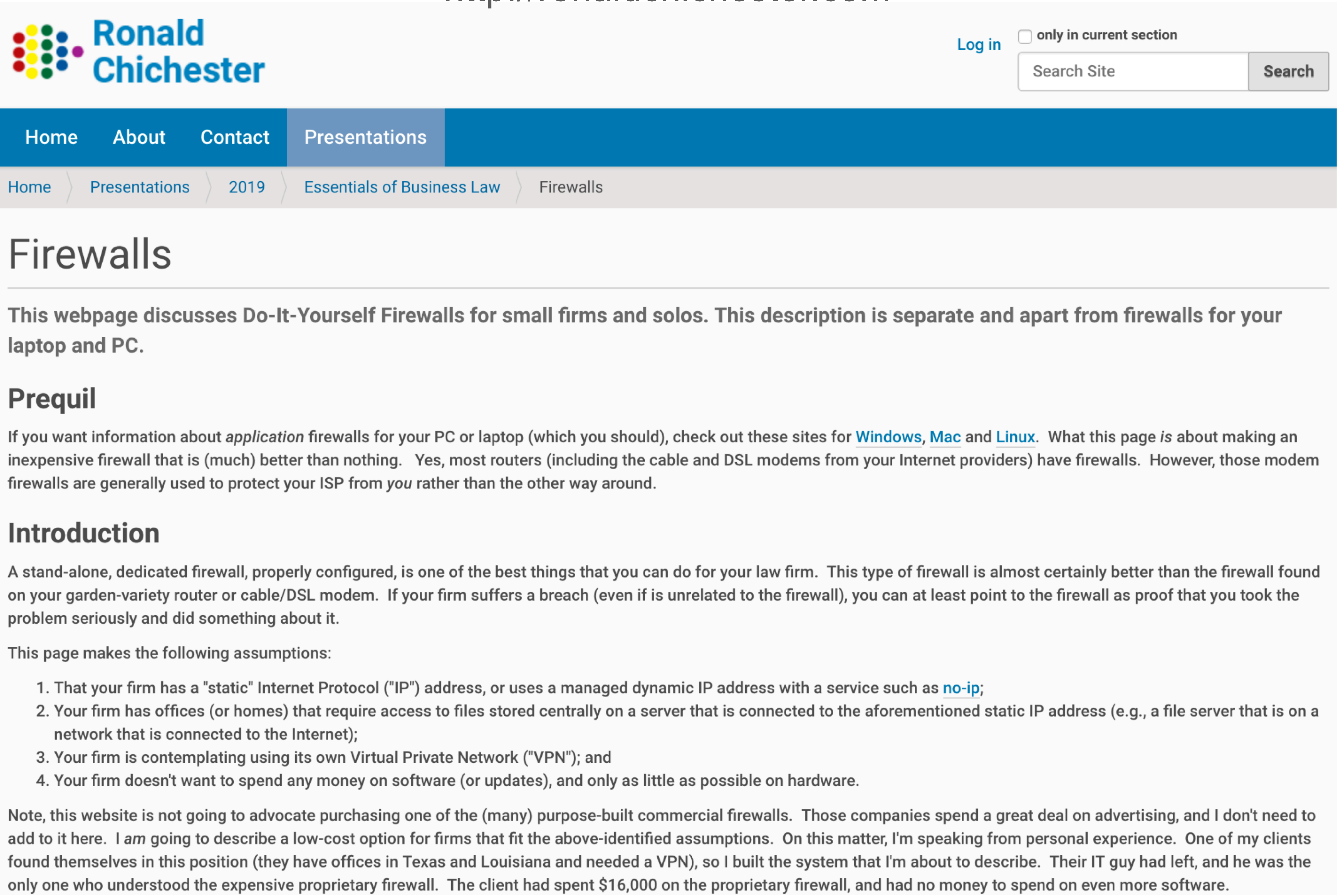
Cloud-based firewalls come in two delicious flavors: vanilla and strawberry. Both flavors are software that checks incoming and outgoing packets to filter against access policies and block malicious traffic. Yet they are also quite different. Think of them as two essential network security tools: Both are designed to protect you, your network, and your real and virtual assets, but in different contexts.

Disclosure: I made up the terms “vanilla firewall” and “strawberry firewall” for this discussion. Hopefully they help us differentiate between the two models as we dig deeper.

Cloud firewalls 101:

- Vanilla firewalls are usually stand-alone products or services designed to protect an enterprise network and its users—like an on-premises firewall appliance, except that it's in the cloud. Service

https://www.hpe.com/us/en/insights/articles/understanding-cloud-based-firewalls-1702.html http://ronaldchichester.com



Firewalls

This webpage discusses Do-It-Yourself Firewalls for small firms and solos. This description is separate and apart from firewalls for your laptop and PC.

Prequil

If you want information about *application* firewalls for your PC or laptop (which you should), check out these sites for Windows, Mac and Linux. What this page *is* about making an inexpensive firewall that is (much) better than nothing. Yes, most routers (including the cable and DSL modems from your Internet providers) have firewalls. However, those modem firewalls are generally used to protect your ISP from *you* rather than the other way around.

Introduction

A stand-alone, dedicated firewall, properly configured, is one of the best things that you can do for your law firm. This type of firewall is almost certainly better than the firewall found on your garden-variety router or cable/DSL modem. If your firm suffers a breach (even if is unrelated to the firewall), you can at least point to the firewall as proof that you took the problem seriously and did something about it.

This page makes the following assumptions:

1. That your firm has a "static" Internet Protocol ("IP") address, or uses a managed dynamic IP address with a service such as no-ip;
2. Your firm has offices (or homes) that require access to files stored centrally on a server that is connected to the aforementioned static IP address (e.g., a file server that is on a network that is connected to the Internet);
3. Your firm is contemplating using its own Virtual Private Network ("VPN"); and
4. Your firm doesn't want to spend any money on software (or updates), and only as little as possible on hardware.

Note, this website is not going to advocate purchasing one of the (many) purpose-built commercial firewalls. Those companies spend a great deal on advertising, and I don't need to add to it here. I *am* going to describe a low-cost option for firms that fit the above-identified assumptions. On this matter, I'm speaking from personal experience. One of my clients found themselves in this position (they have offices in Texas and Louisiana and needed a VPN), so I built the system that I'm about to describe. Their IT guy had left, and he was the only one who understood the expensive proprietary firewall. The client had spent $16,000 on the proprietary firewall, and had no money to spend on even more software.

YOU CAN
DO IT!
memegenerator.net

QUESTIONS?

Ronald Chichester

ron@texascomputerlaw.com

713-302-1679

Robert Ray

robert@texasinheritance.com

214-660-5700