CYBERSECURITY FOR YOUR OFFICE: ENCRYPTION AND FIREWALLS

Essentials of Business Law - 2019

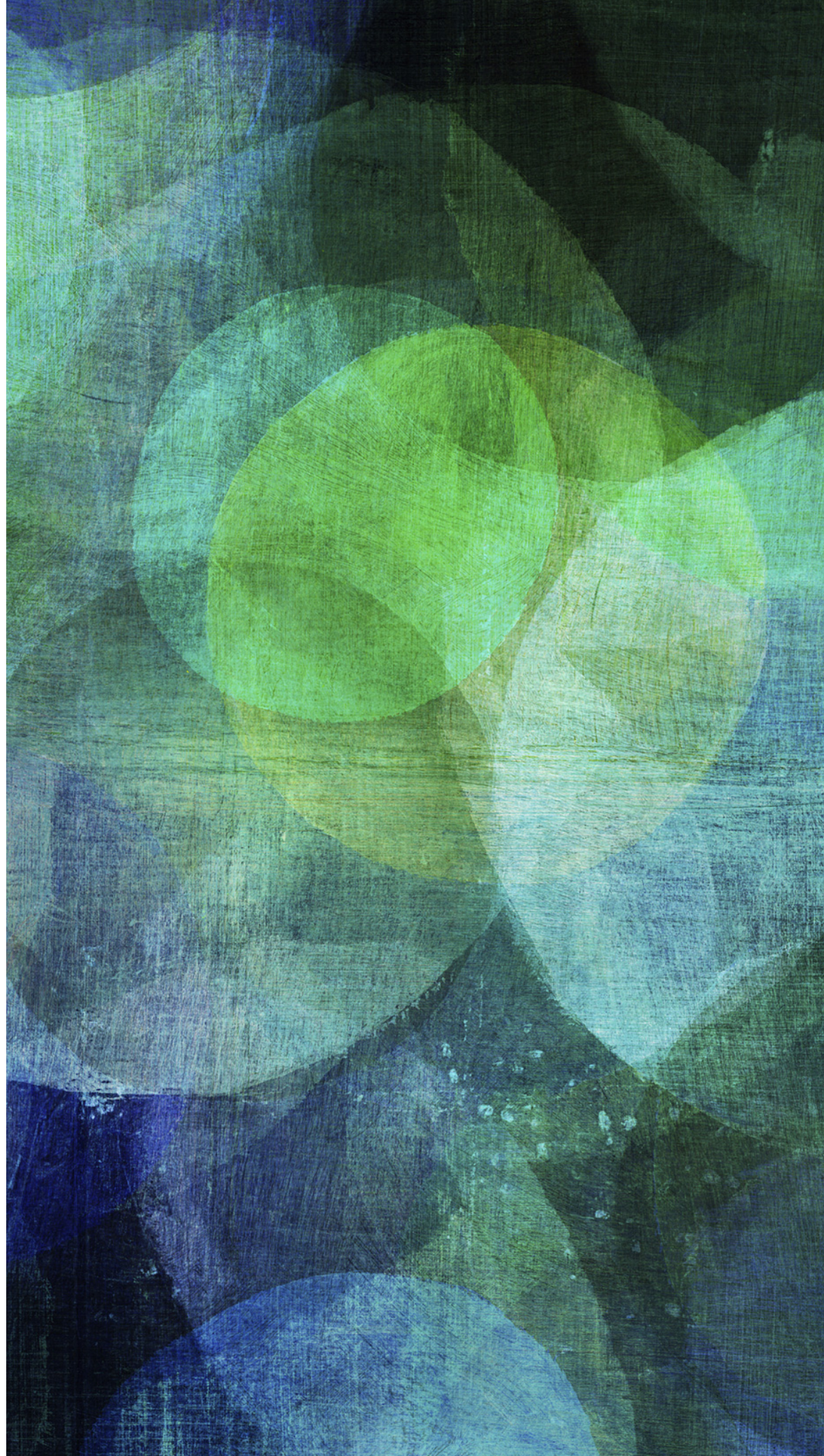
Ronald L. Chichester

Ronald Chichester, P.C.

March 15, 2019

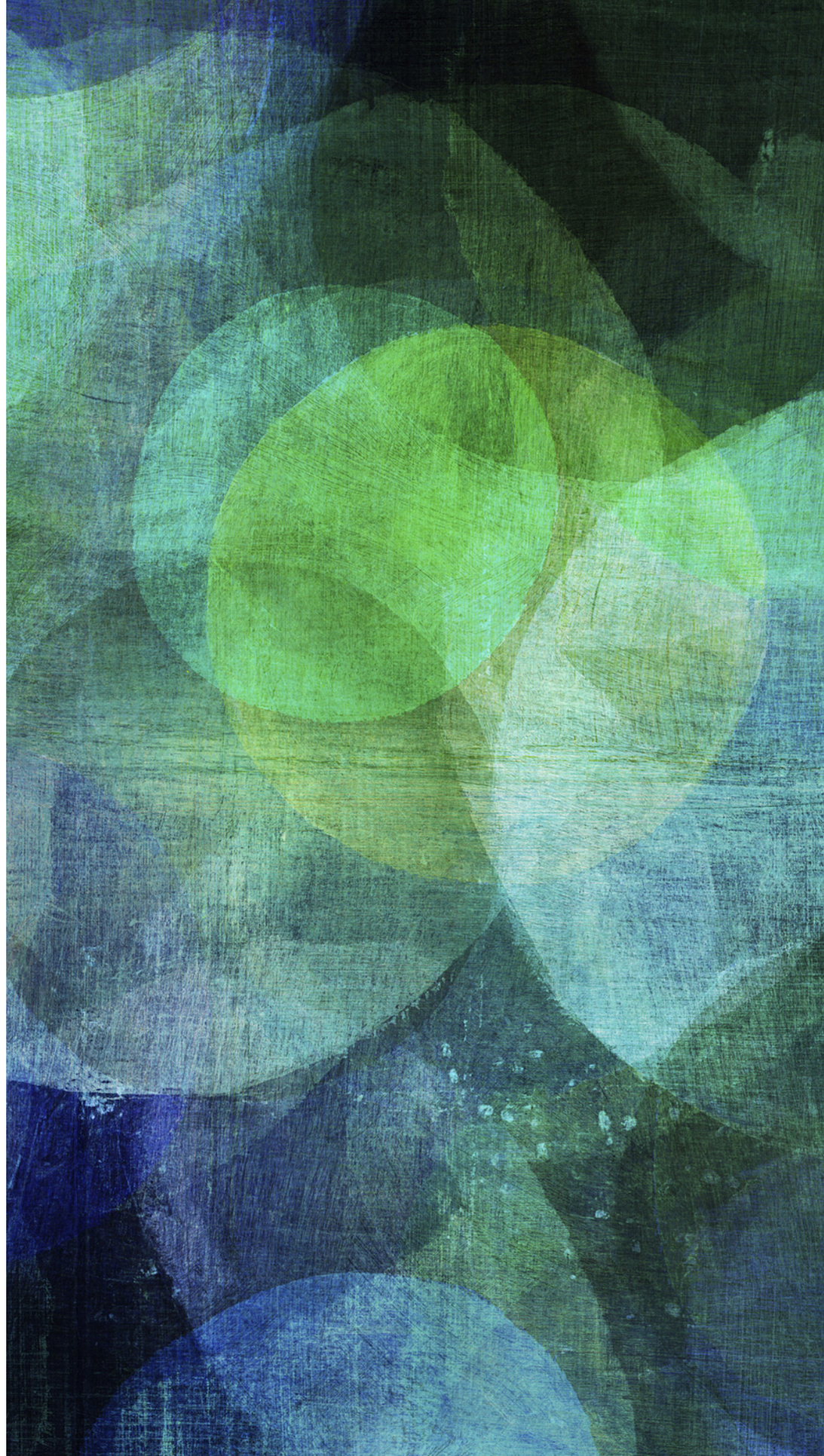
Dallas, Texas

OVERVIEW



OVERVIEW

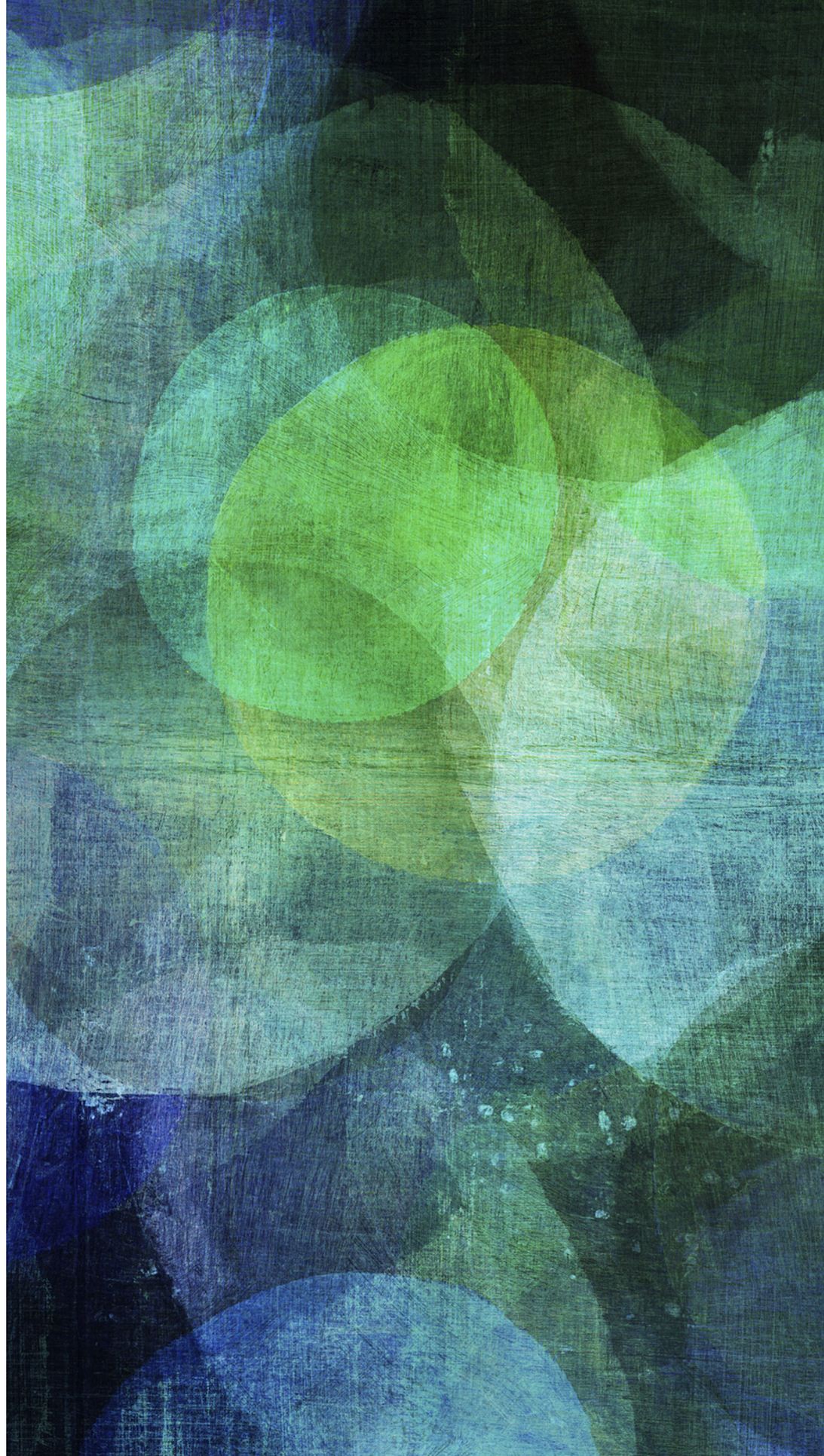
Why take the trouble?



OVERVIEW

Why take the trouble?

The aspects of cybersecurity

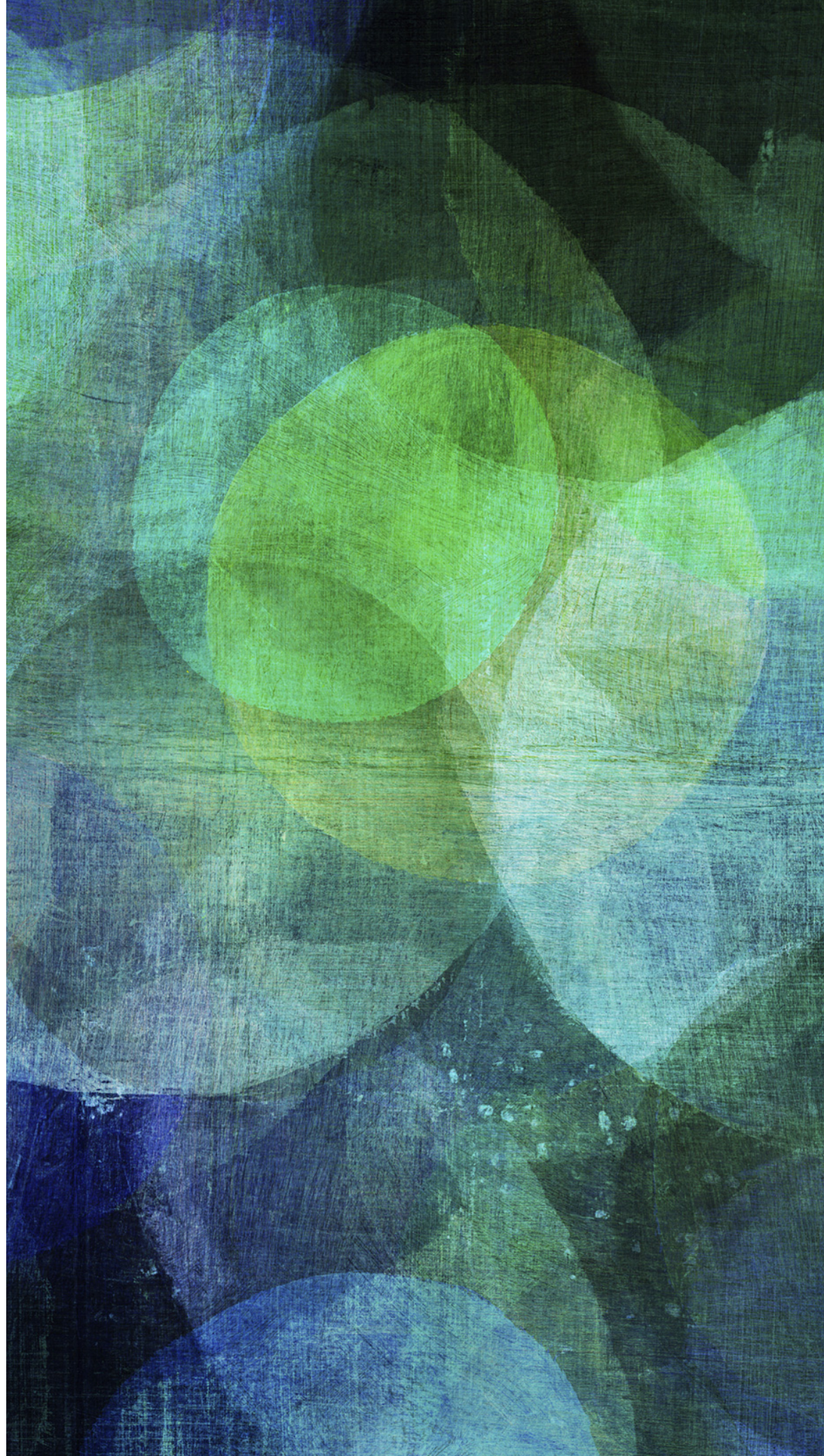


OVERVIEW

Why take the trouble?

The aspects of cybersecurity

Encryption



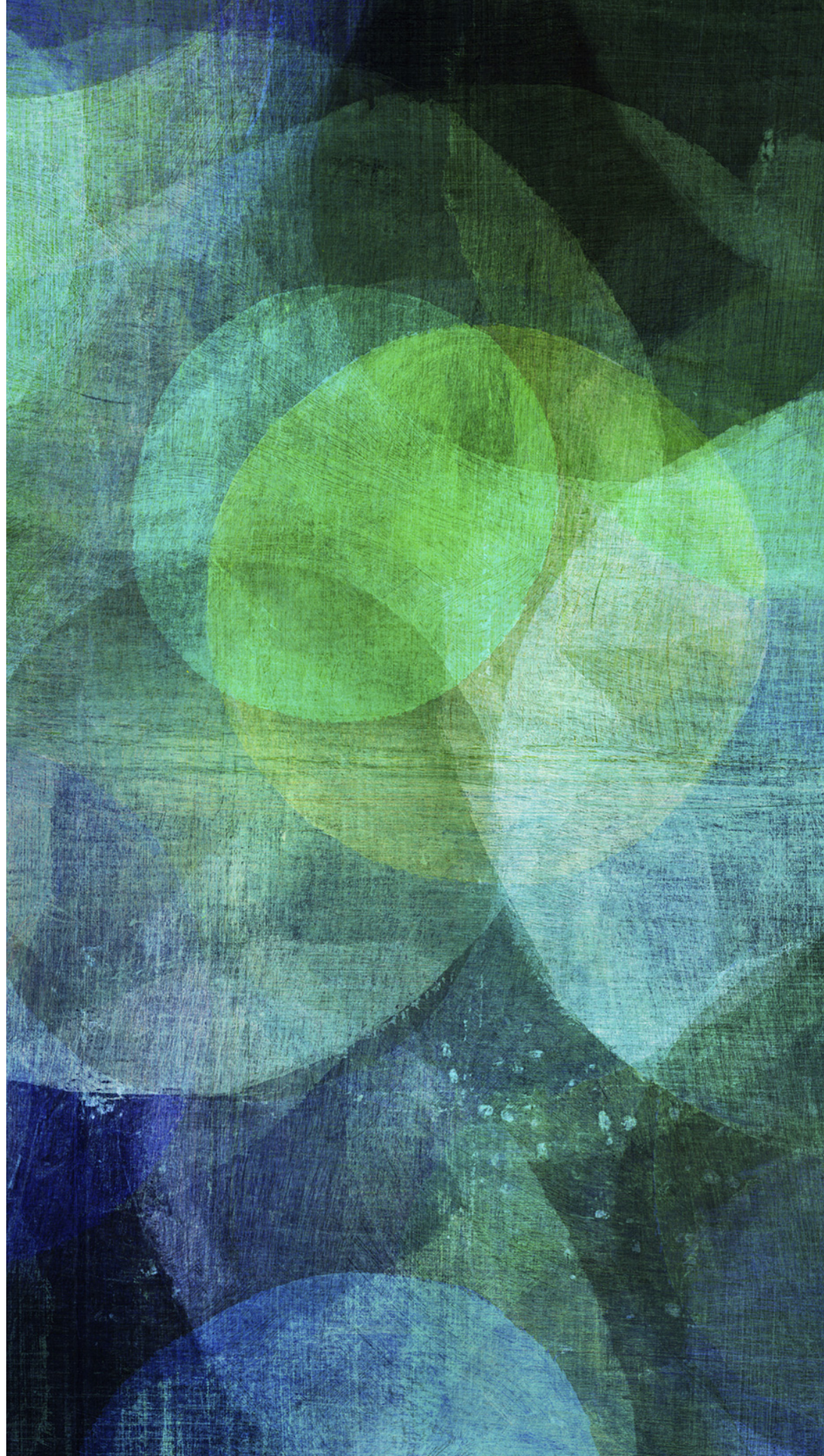
OVERVIEW

Why take the trouble?

The aspects of cybersecurity

Encryption

Firewalls



OVERVIEW

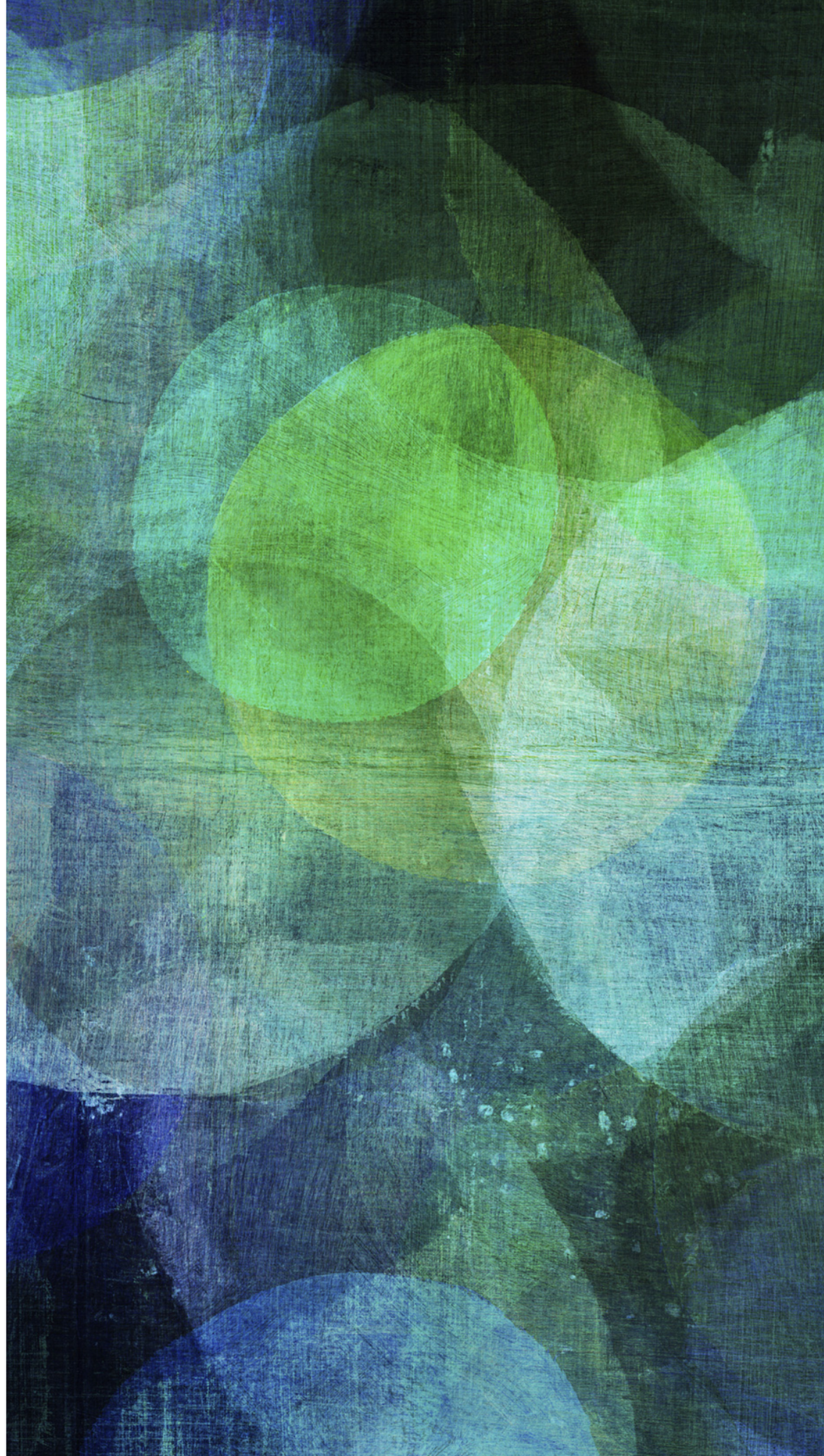
Why take the trouble?

The aspects of cybersecurity

Encryption

Firewalls

Questions



WHY TAKE THE TROUBLE?

WHY TAKE THE TROUBLE?

- ALL states have breach/ notification laws

WHY TAKE THE TROUBLE?

- ALL states have breach/ notification laws
- Law firms are businesses and so come under the breach/ notification laws

WHY TAKE THE TROUBLE?

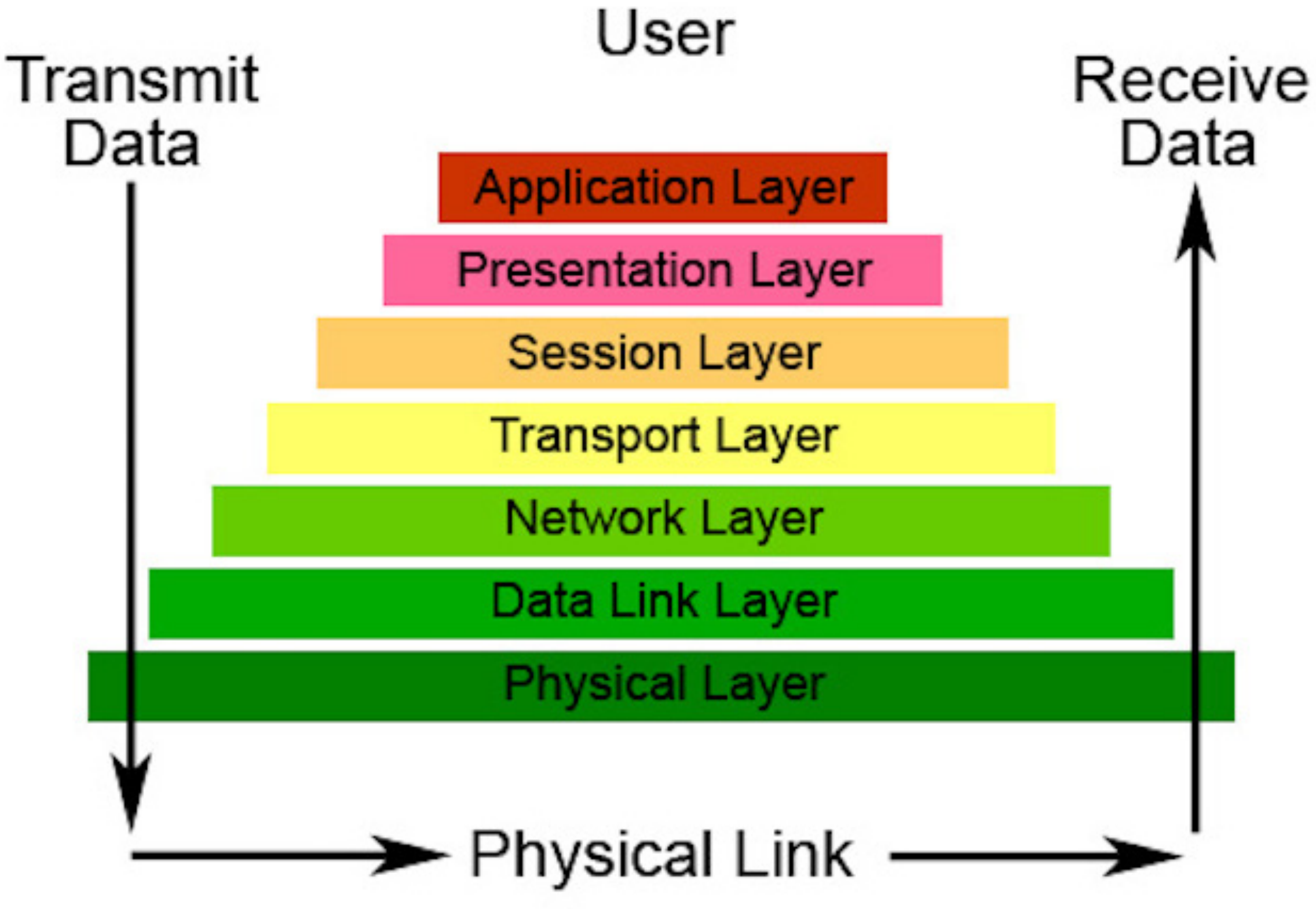
- ALL states have breach/ notification laws
- Law firms are businesses and so come under the breach/ notification laws
- In Texas, the breach/ notification laws are in Tex.Bus&Comm.Code

WHY TAKE THE TROUBLE?

- ALL states have breach/ notification laws
- Law firms are businesses and so come under the breach/ notification laws
- In Texas, the breach/ notification laws are in Tex.Bus&Comm.Code
- On top of that, there is Texas DR 1.05 (Confidentiality of Information)

THE ASPECTS OF CYBERSECURITY

The Seven Layers of OSI



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card —— Switch —— NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

PACKET FILTERING

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

PACKET FILTERING

Encryption

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	**User Applications** SMTP	GATEWAY Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting	**Routers** IP/IPX/ICMP		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control	**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts	**Hub**		

PACKET FILTERING

Encryption

Firewall

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).

CONTACT

Pam Greenberg

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

NAVIGATE

Home

- About State Legislatures
- Agriculture and Rural Development
- Civil and Criminal Justice
- Education
- Elections and Campaigns
- Energy
- Environment and Natural Resources
- Ethics
- Financial Services and Commerce
- Fiscal Policy
- Health
- Human Services
- Immigration
- International
- Labor and Employment

“

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

- Ronald Chichester

“

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

- Ronald Chichester

Encrypted Data

Encrypted Data

+

Encrypted Data

+

an (available) Key

Encrypted Data

+

an (available) Key

=

***No** Safe Harbor*

Decrypted Data

Decrypted Data

+

Decrypted Data

+

Hack

Decrypted Data

+

Hack

=

***No** Safe Harbor*

TEXAS DR 1.05

TEXAS DR 1.05

(a) “Confidential information” includes both “privileged information” and “unprivileged client information.” “Privileged information” refers to the information of a client protected by the lawyer-client privilege of Rule 503 of the Texas Rules of Evidence or of Rule 503 of the Texas Rules of Criminal Evidence or by the principles of attorney-client privilege governed by Rule 501 of the Federal Rules of Evidence for United States Courts and Magistrates. “Unprivileged client information” means all information relating to a client or furnished by the client, other than privileged information, acquired by the lawyer during the course of or by reason of the representation of the client.

TYPES OF DATA DIFFER

…between Tex.Bus.&Comm.Code and DR 1.05

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

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

… **<u>if</u>** *you do it right*

DOING IT RIGHT. . .

DOING IT RIGHT...

- Two main types of encryption:

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter
- Cost + key/password management

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter
  - Cost + key/password management
- Devise practice/policy for handling data at the firm

DOING IT RIGHT . . .

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter
  - Cost + key/password management
- Devise practice/policy for handling data at the firm
  - Encrypt at rest! (*present* tense)

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter
  - Cost + key/password management
- Devise practice/policy for handling data at the firm
  - Encrypt at rest! (*present* tense)
  - Encrypt backups!!

DOING IT RIGHT...

- Two main types of encryption:
  - Single-key encryption
  - Dual-key (aka public/private key encryption)
- Determine client needs
  - Engagement letter
  - Cost + key/password management
- Devise practice/policy for handling data at the firm
  - Encrypt at rest! (*present* tense)
  - Encrypt backups!!
  - Don't forget about the indexes!!!

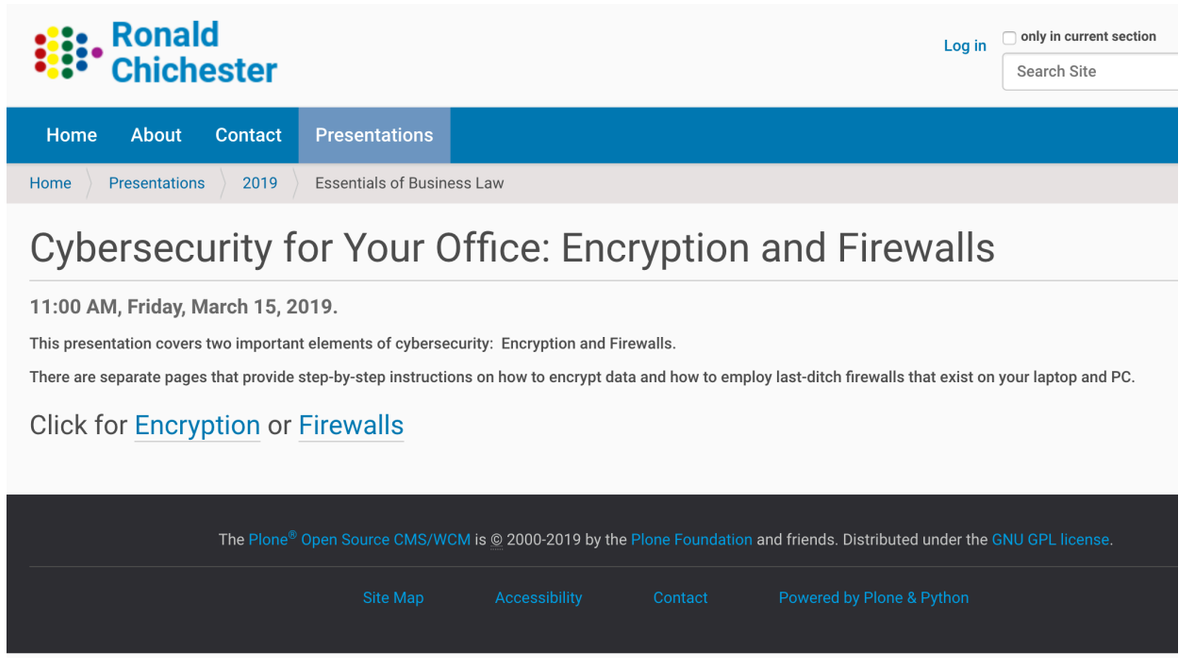
VERY SIMPLE (STEP-BY-STEP) EXAMPLE...

VERY SIMPLE (STEP-BY-STEP) EXAMPLE...

- ronaldchichester.com
  - Presentation
    - 2019
      - Essentials of Business Law
      - Encryption

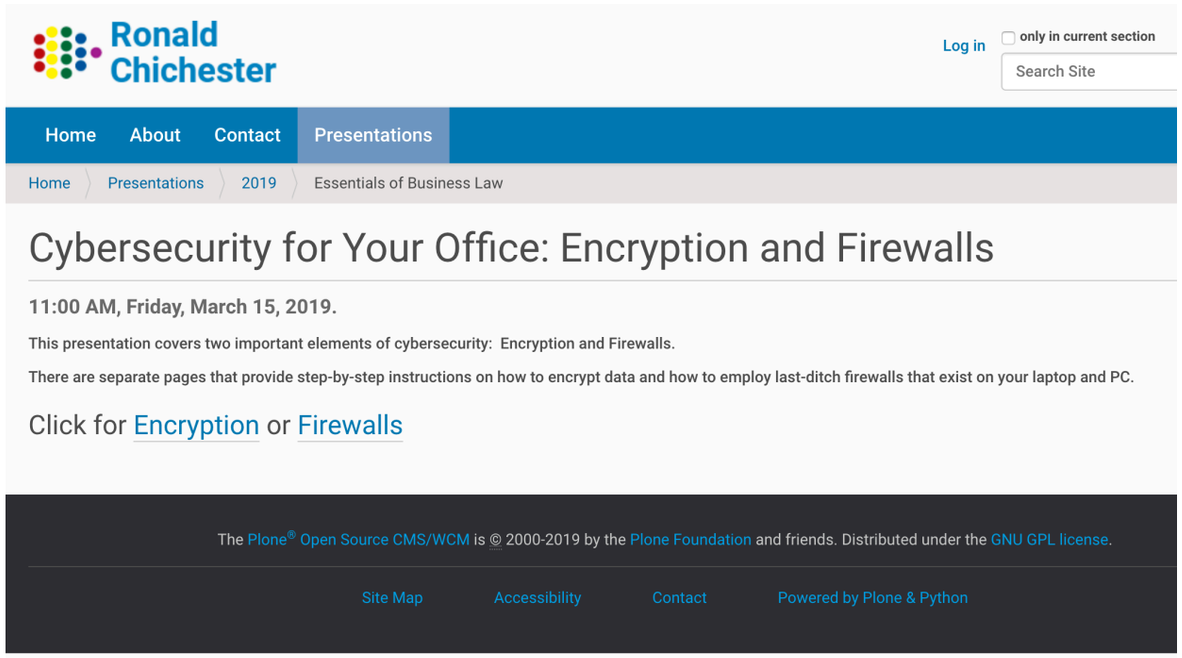
VERY SIMPLE (STEP-BY-STEP) EXAMPLE...

- ronaldchichester.com
  - Presentation
    - 2019
      - Essentials of Business Law
        - Encryption



VERY SIMPLE (STEP-BY-STEP) EXAMPLE...

- ronaldchichester.com
  - Presentation
    - 2019
      - Essentials of Business Law
        - Encryption



- This is an example of a single-key encryption scheme that can be used within your firm and your clients (at no cost)

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

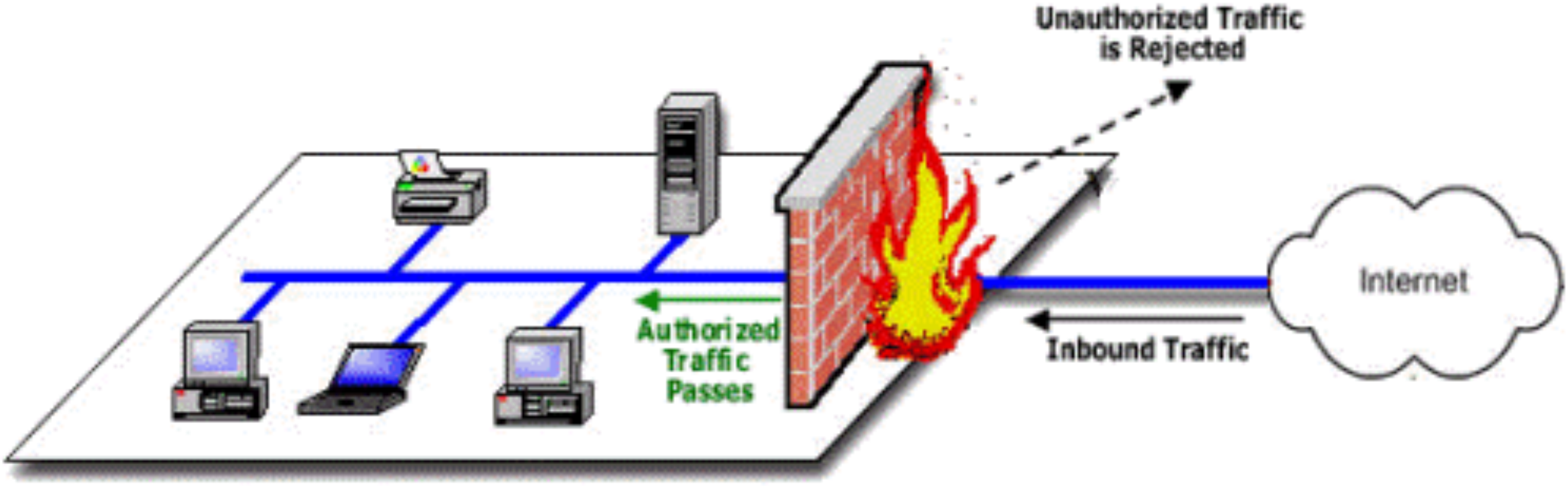
English
Chinese Simpl.

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

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

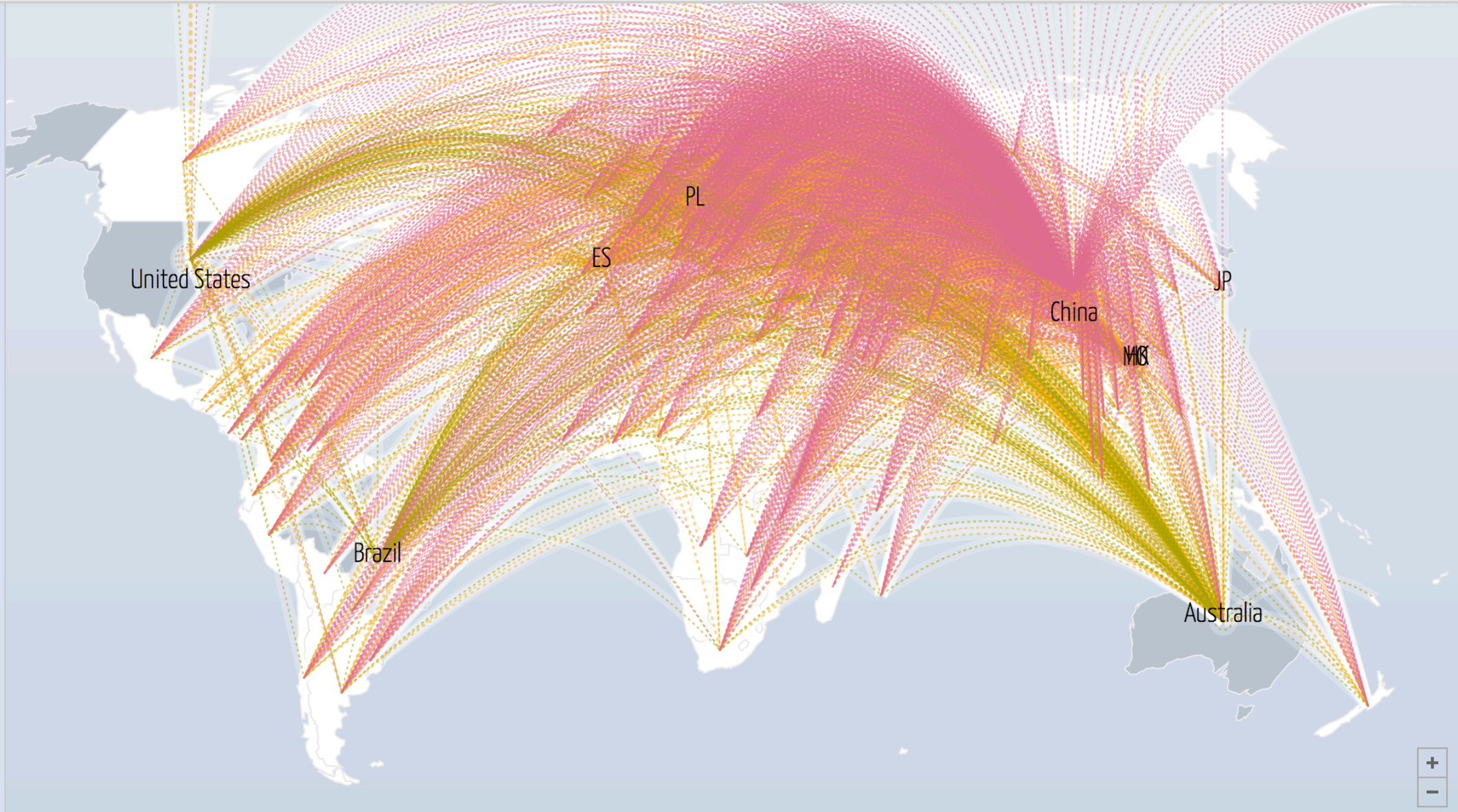
Shape (source + destination)

between two countries

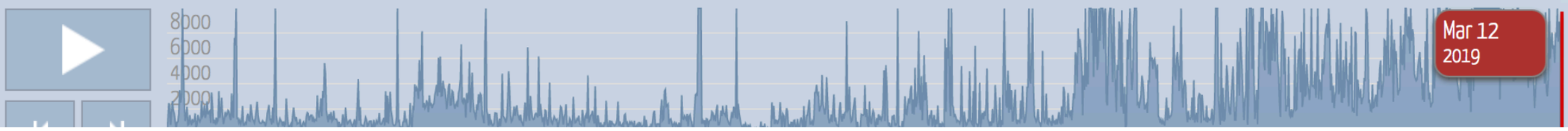
internal

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



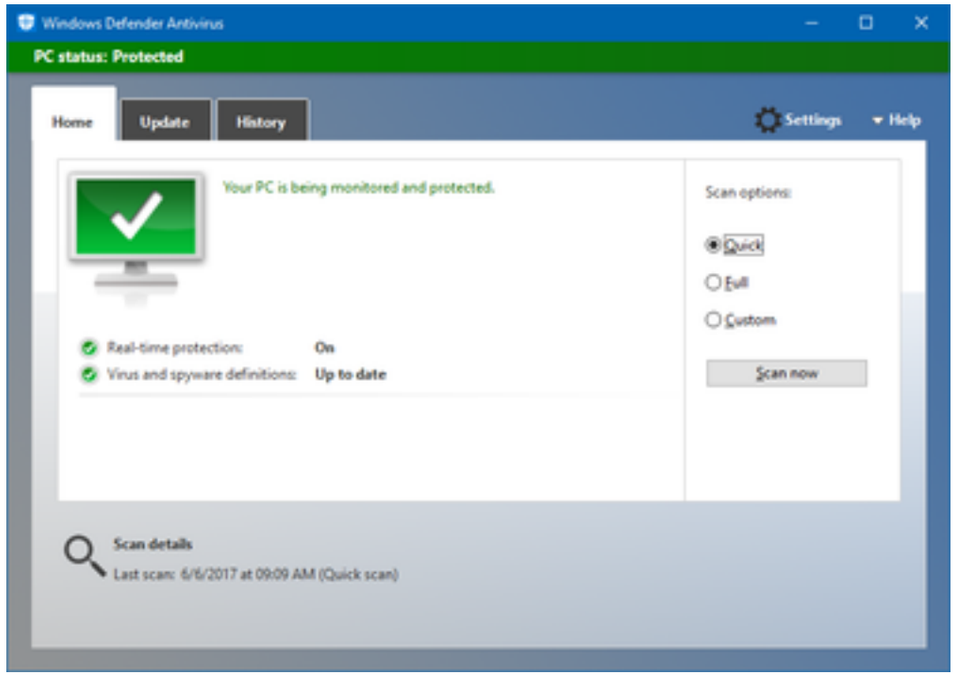
> “Well, I had talked to some experts, and I was fully expecting maybe a week, maybe never, certainly not less than a day," McGill told NPR's Ari Shapiro. "But it came a lot sooner. It was 41 minutes. [The second attempt was] within 10 or 15 minutes [and the third was] another 10 or 15."

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

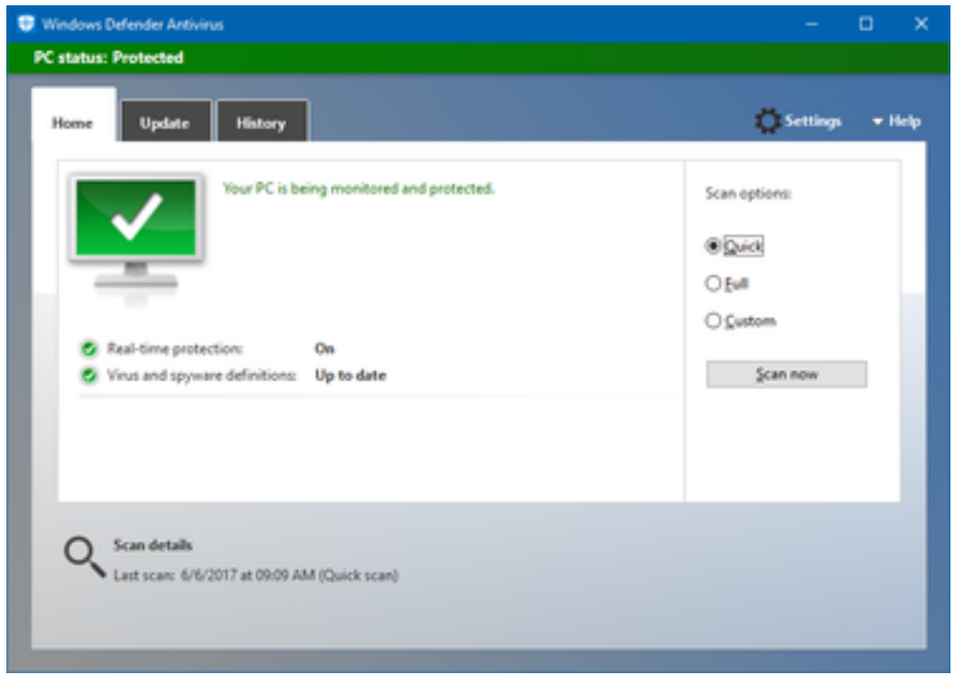
https://www.npr.org/sections/alltechconsidered/2016/11/01/500253637/an-experiment-shows-how-quickly-the-internet-of-things-can-be-hacked

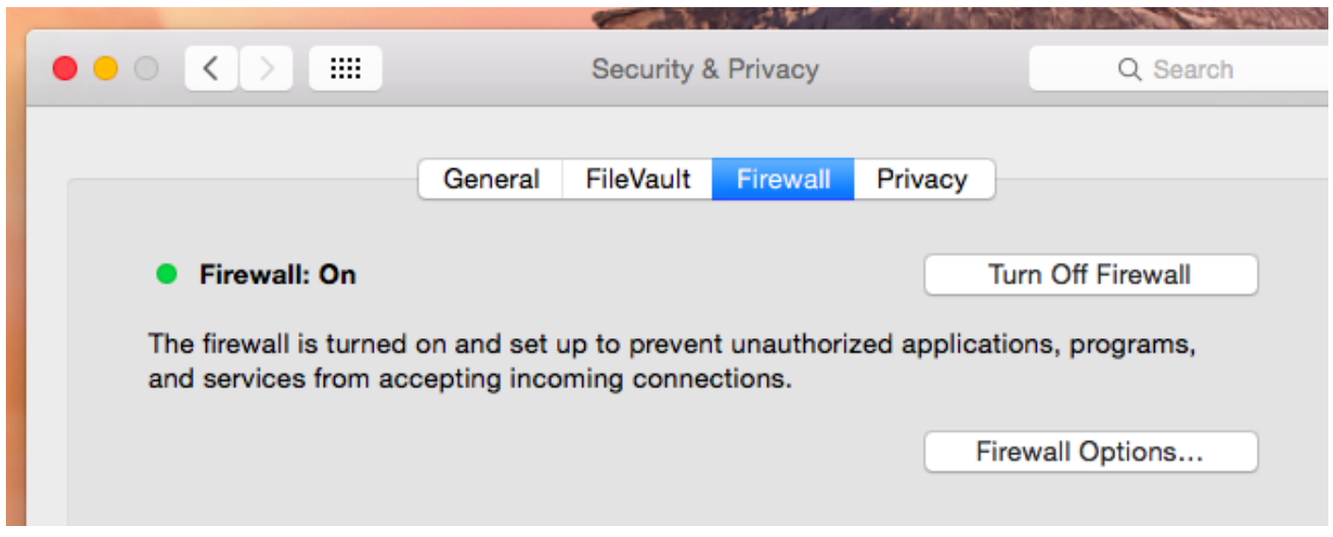
Firewalls for Operating Systems

Firewalls for Operating Systems

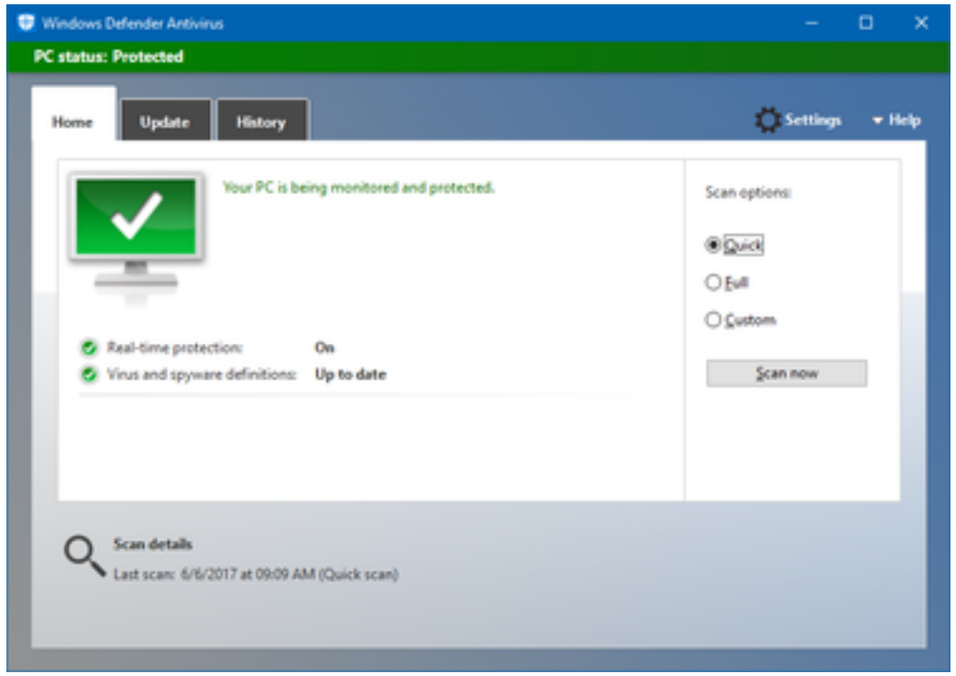


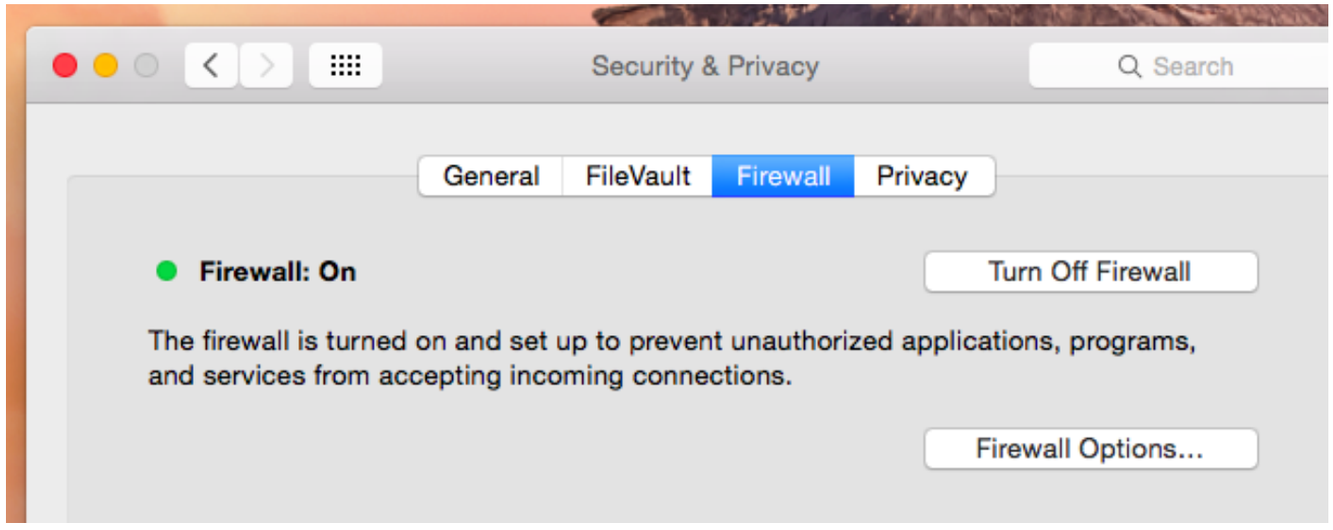
Firewalls for Operating Systems

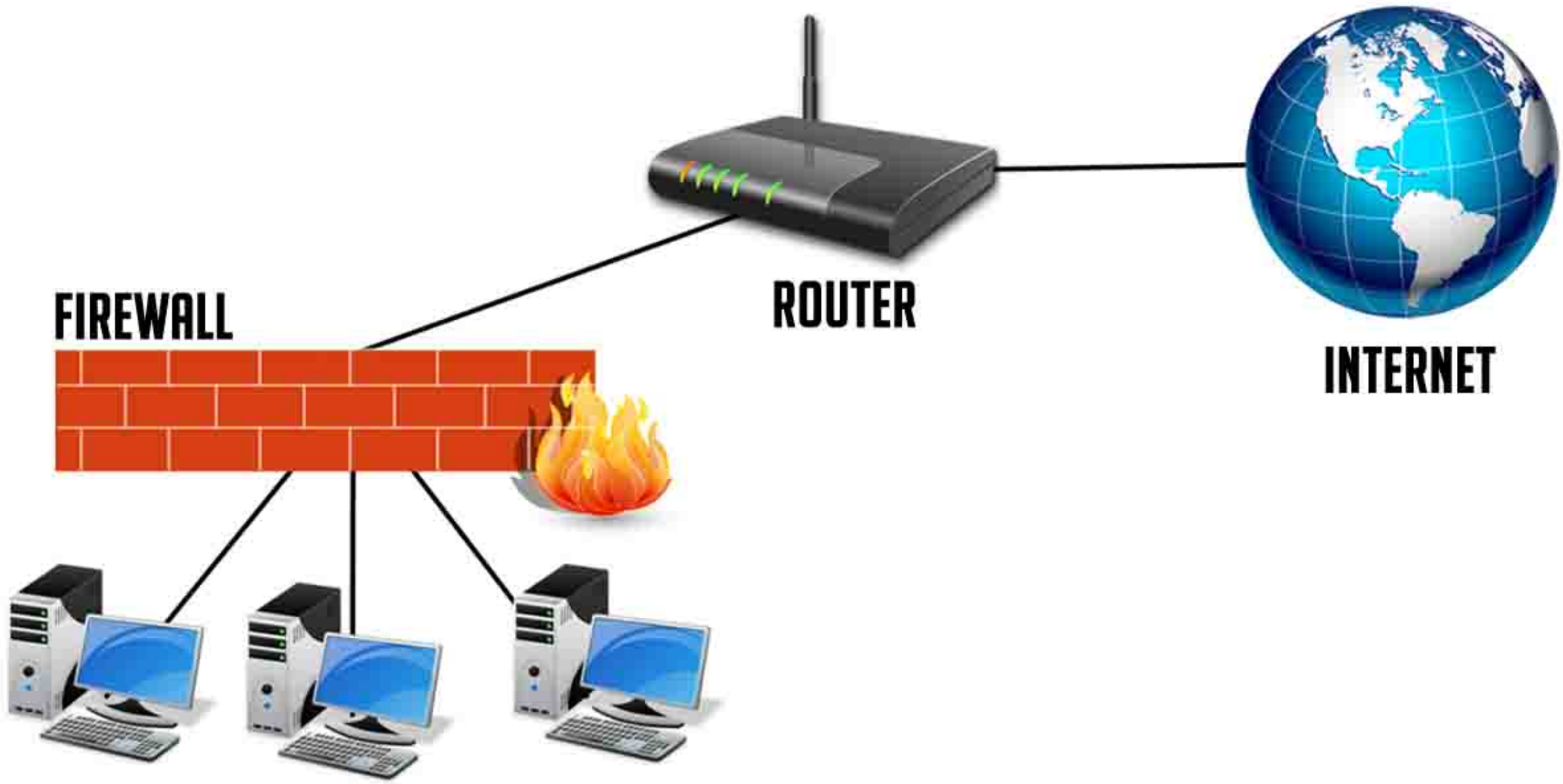




Firewalls for Operating Systems



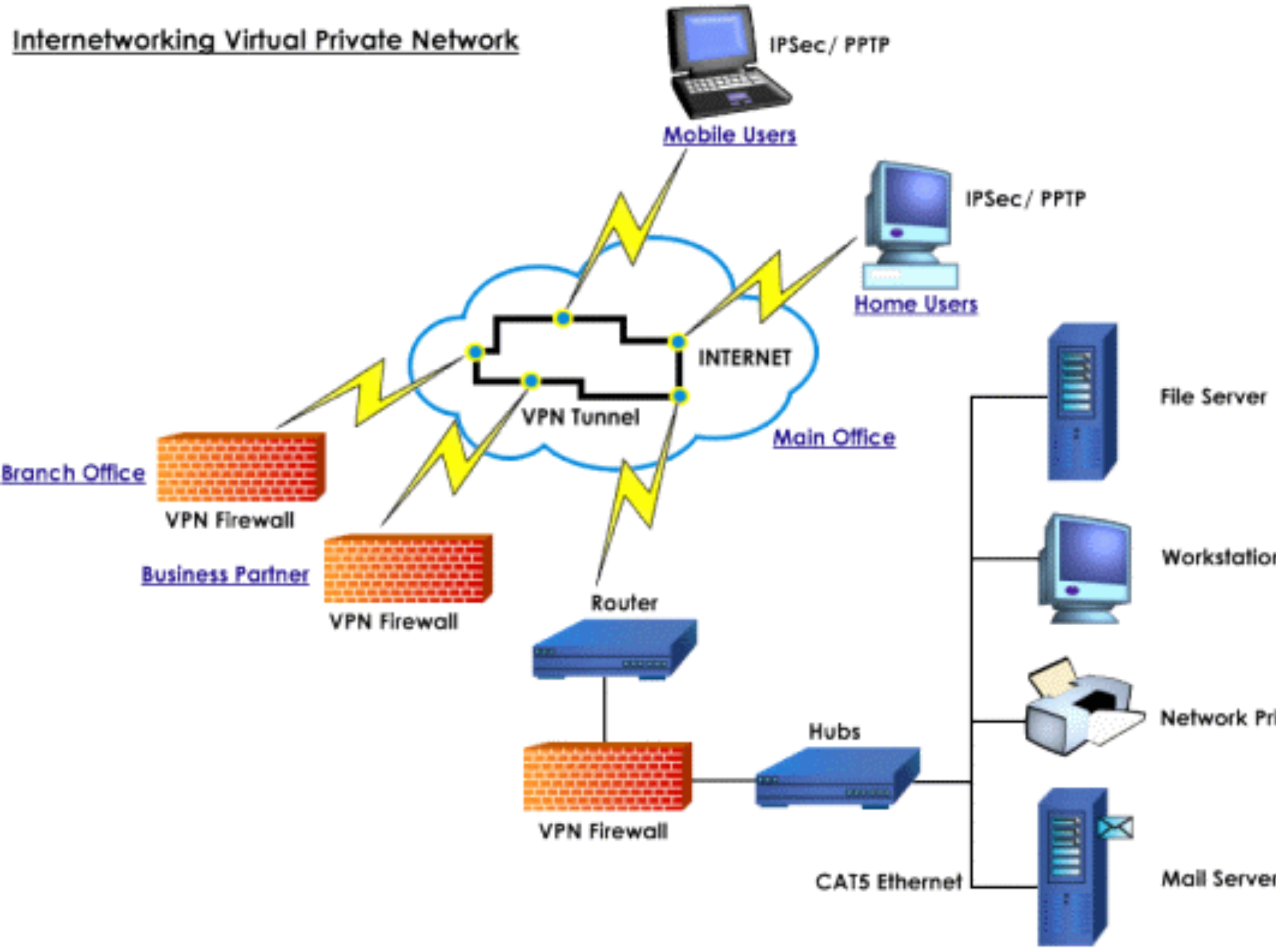



FIREWALL
ROUTER
INTERNET

In addition…

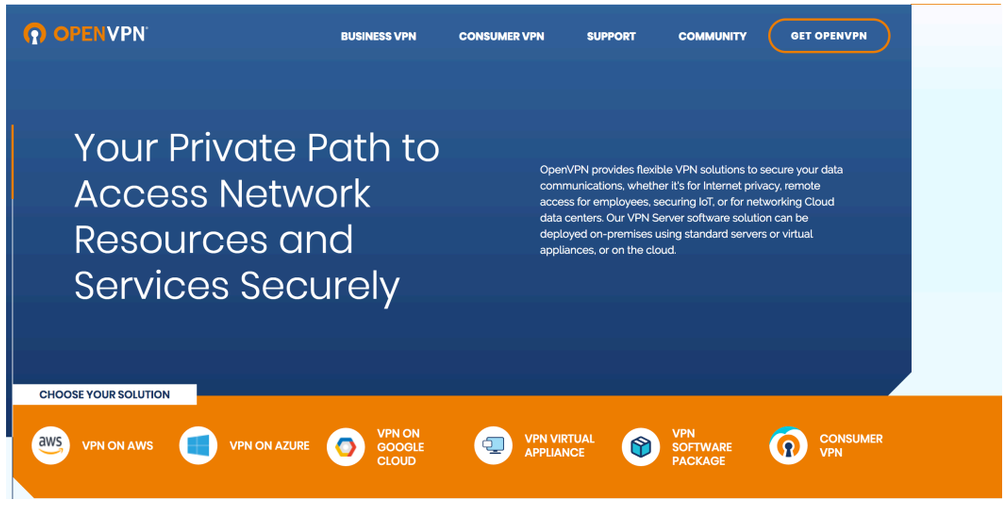
…you can have your own VPN

Internetworking Virtual Private Network



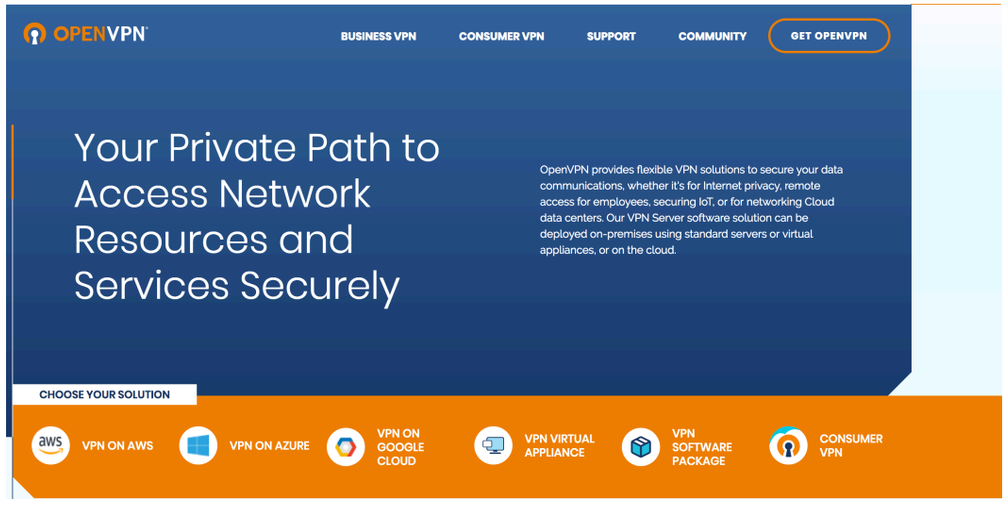
OPEN SOURCE SOFTWARE

OPEN SOURCE SOFTWARE

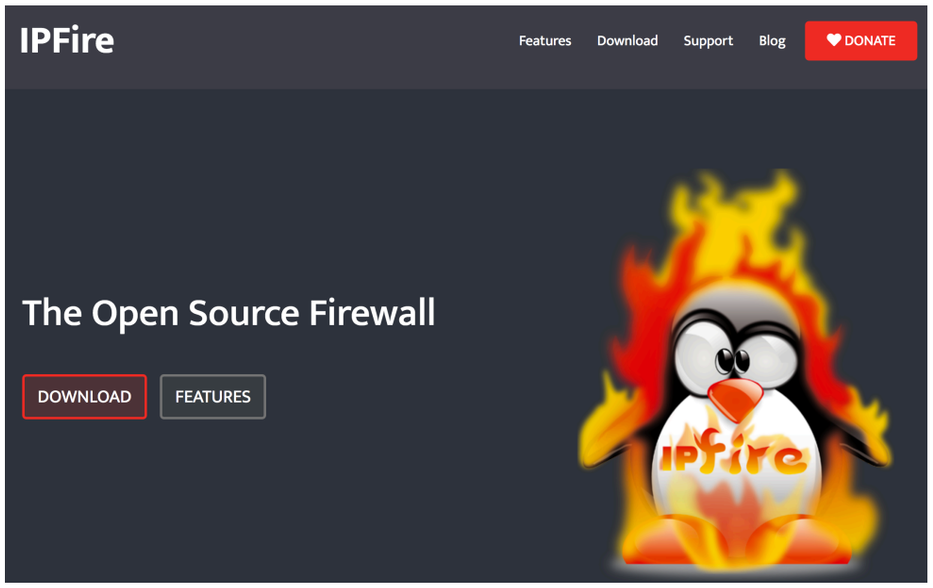


https://openvpn.net/

OPEN SOURCE SOFTWARE

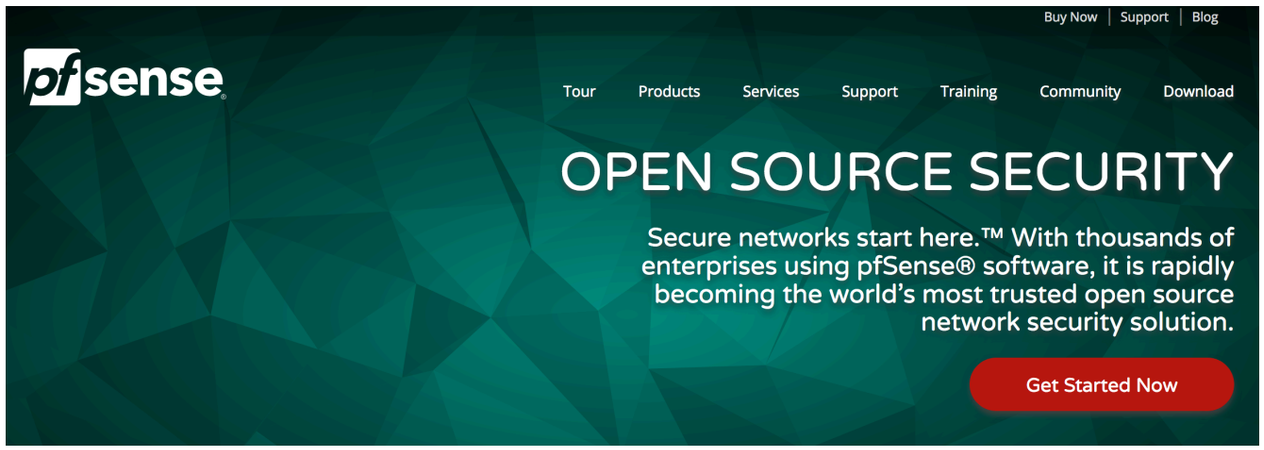


https://openvpn.net/



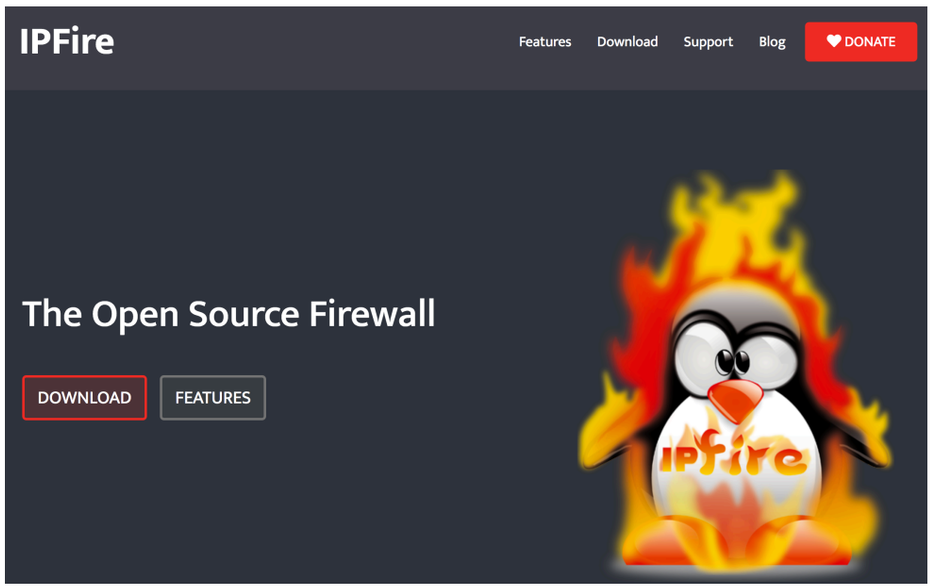
https://www.ipfire.org/

OPEN SOURCE SOFTWARE



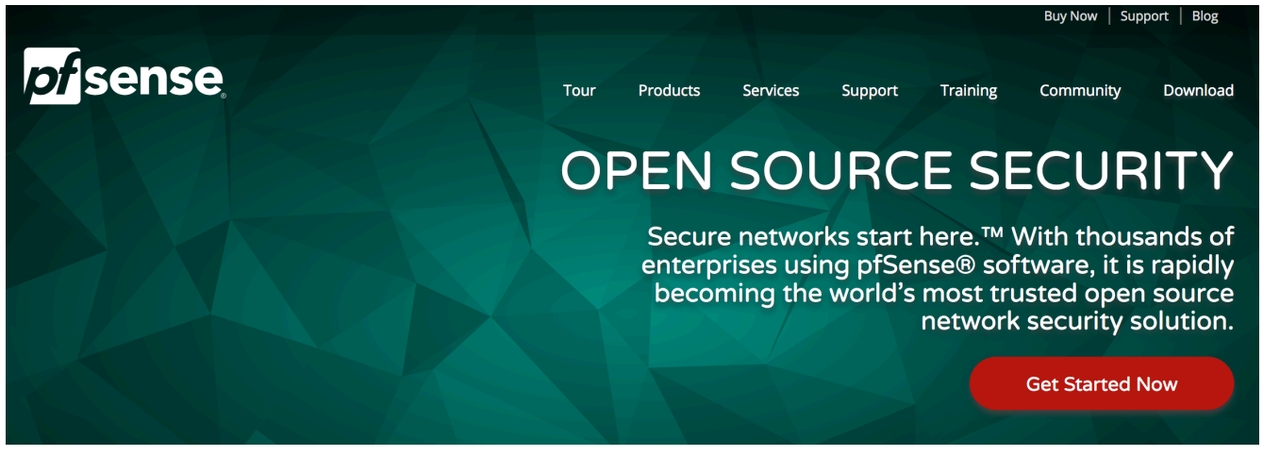
https://www.pfsense.org/

https://openvpn.net/



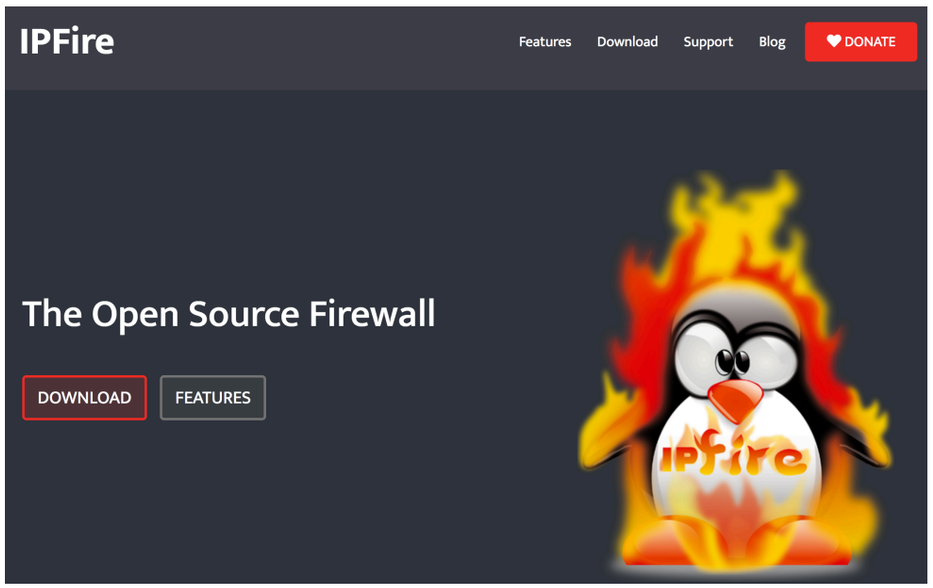
https://www.ipfire.org/

OPEN SOURCE SOFTWARE

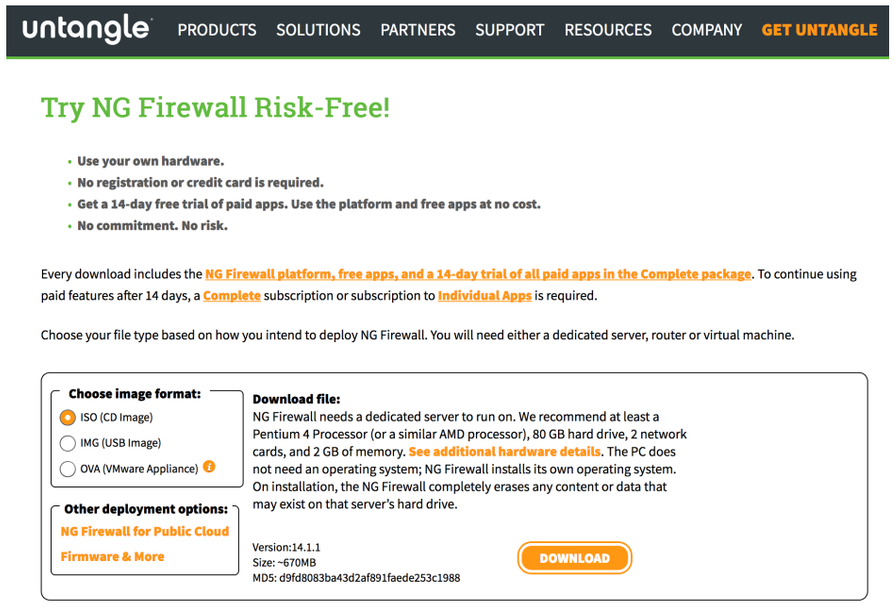


https://www.pfsense.org/

https://openvpn.net/



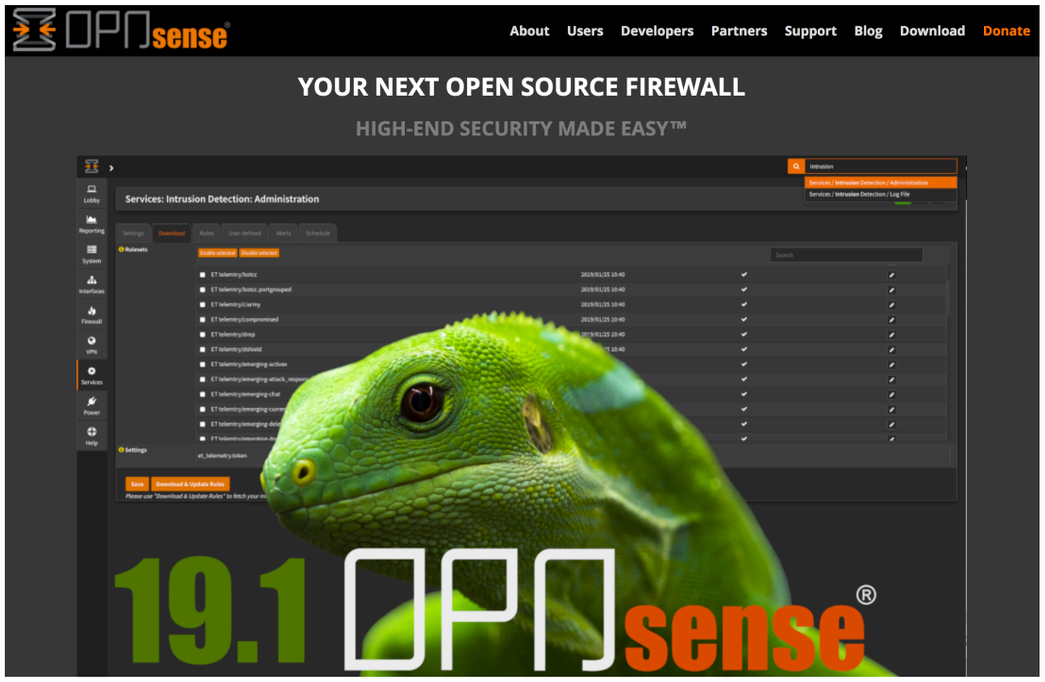
https://www.ipfire.org/



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

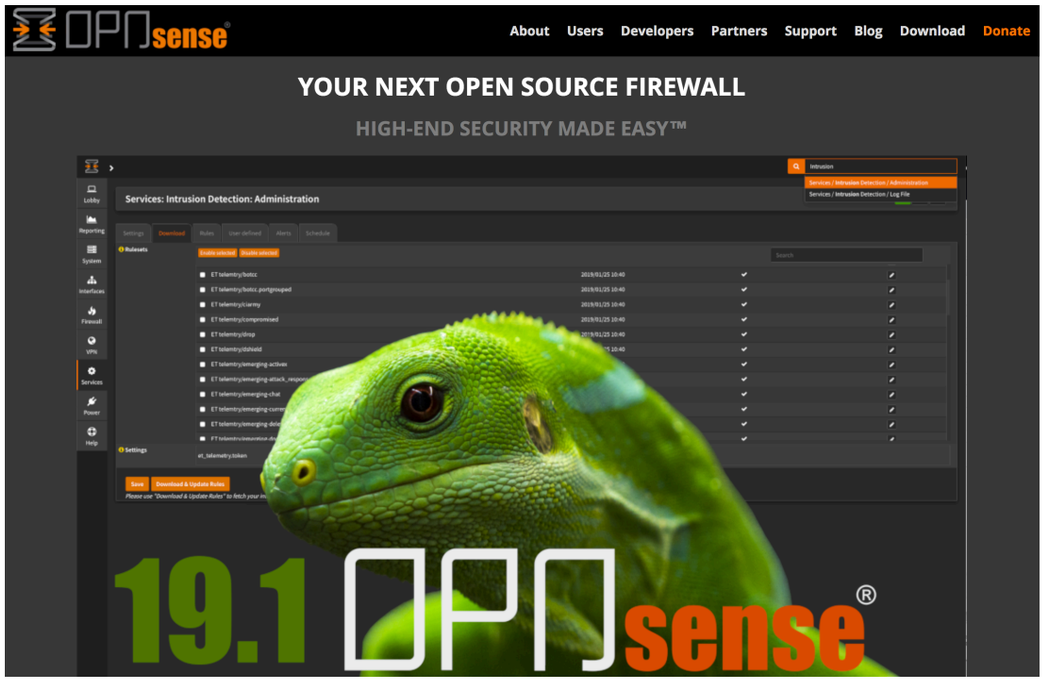
OPEN SOURCE SOFTWARE...

OPEN SOURCE SOFTWARE...

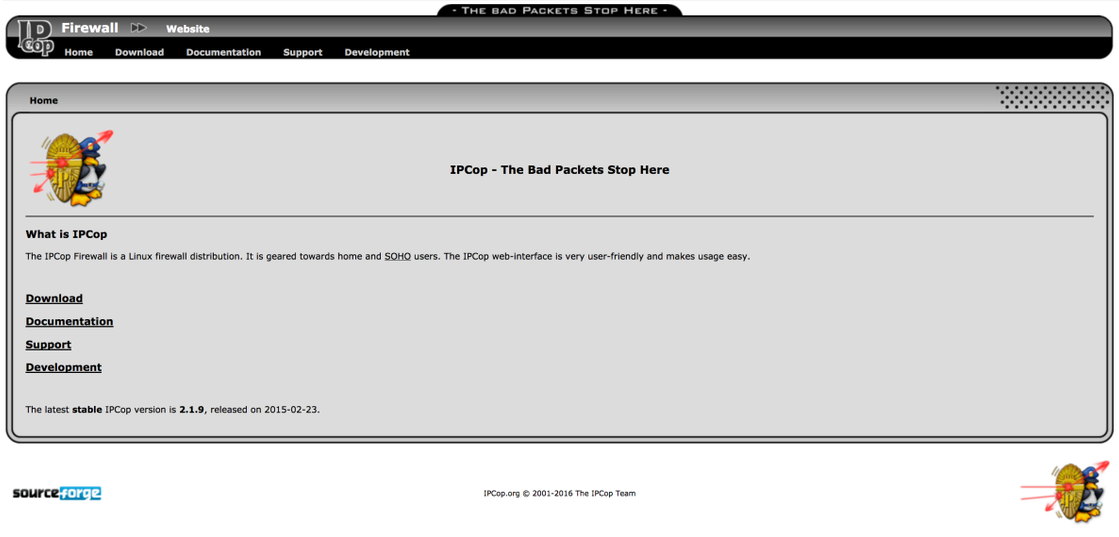


https://opnsense.org/

OPEN SOURCE SOFTWARE...

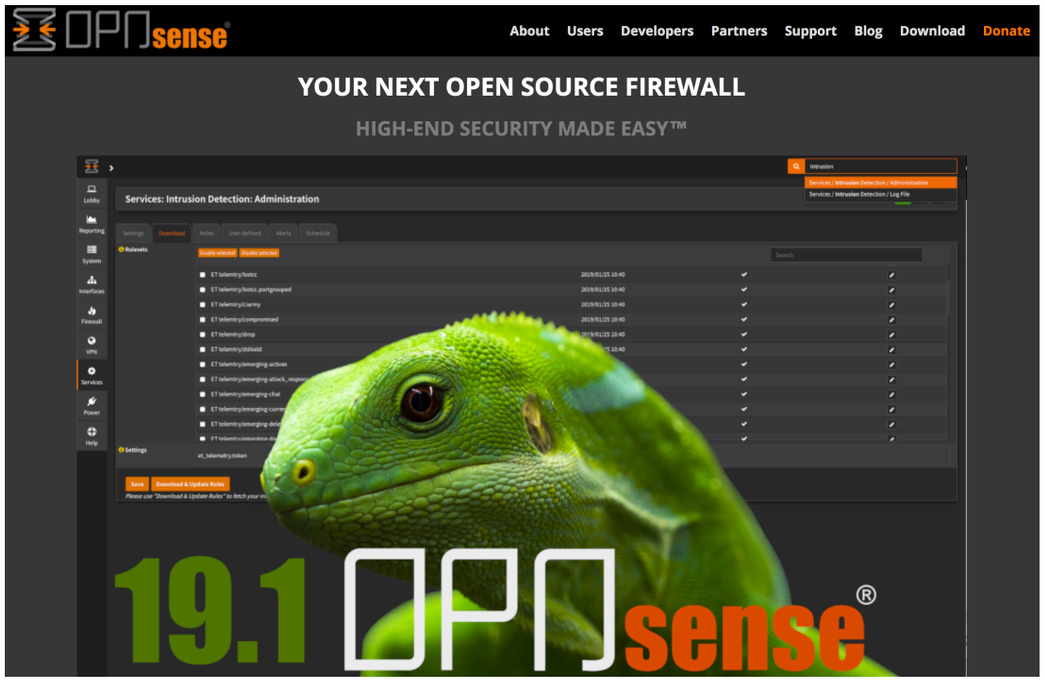


https://opnsense.org/

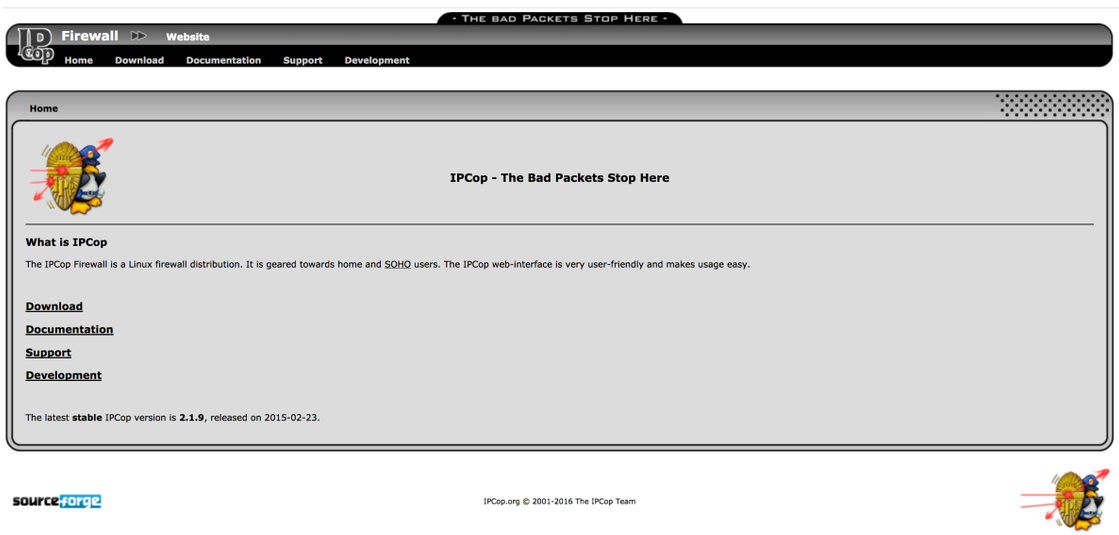


http://ipcop.sourceforge.net/

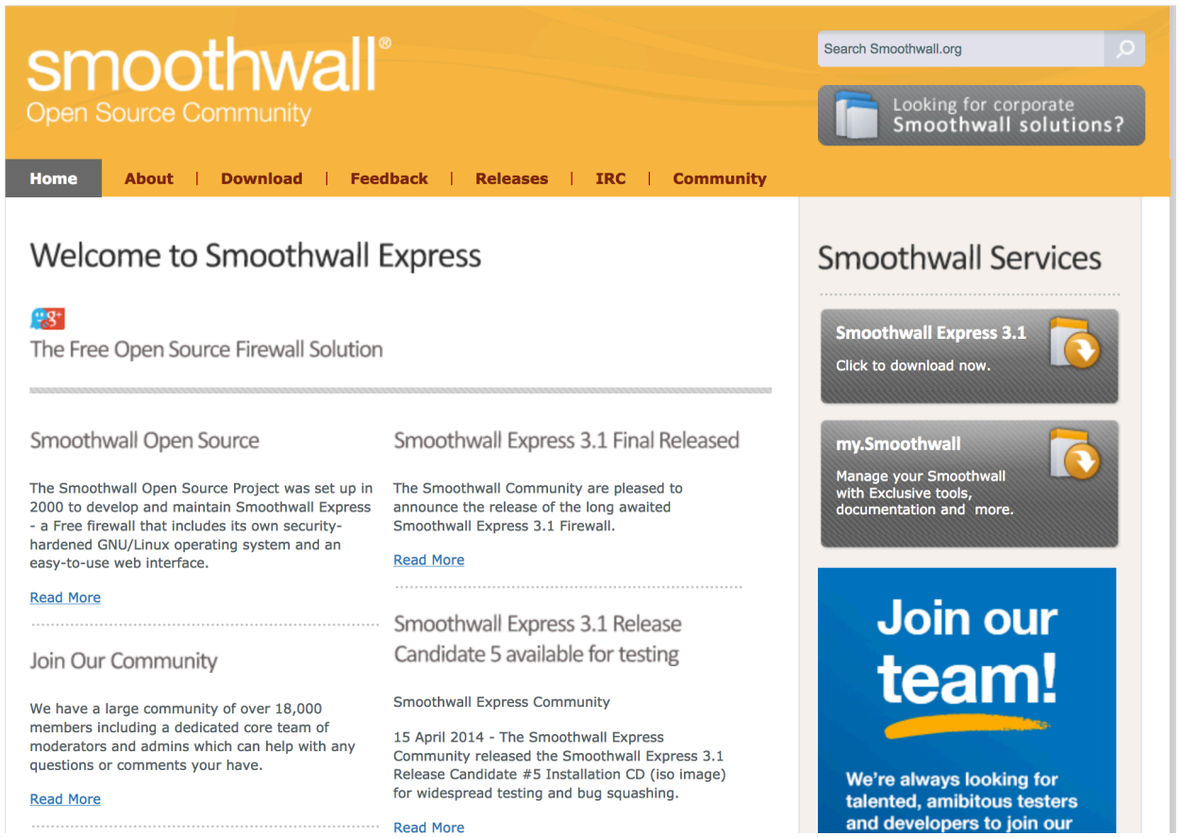
OPEN SOURCE SOFTWARE...



https://opnsense.org/



http://ipcop.sourceforge.net/

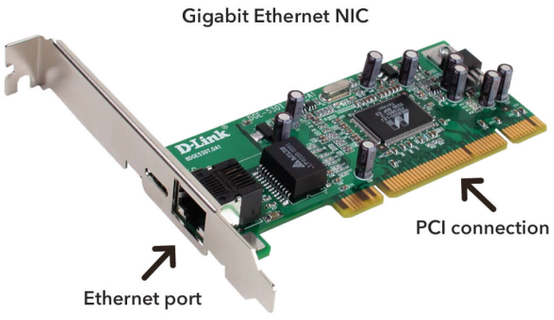


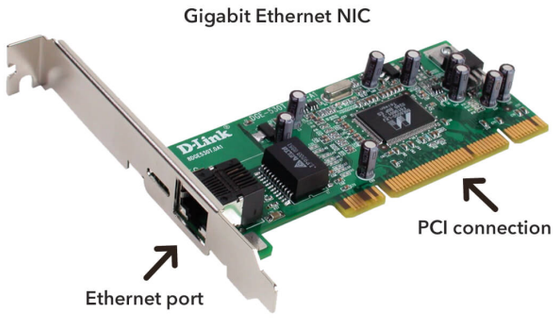
http://www.smoothwall.org/

+ HARDWARE

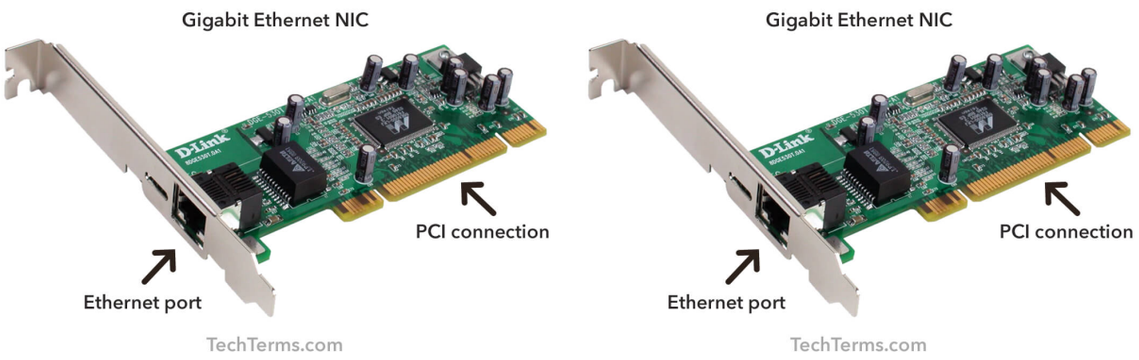
+ HARDWARE

+ HARDWARE


Gigabit Ethernet NIC
PCI connection
Ethernet port
TechTerms.com

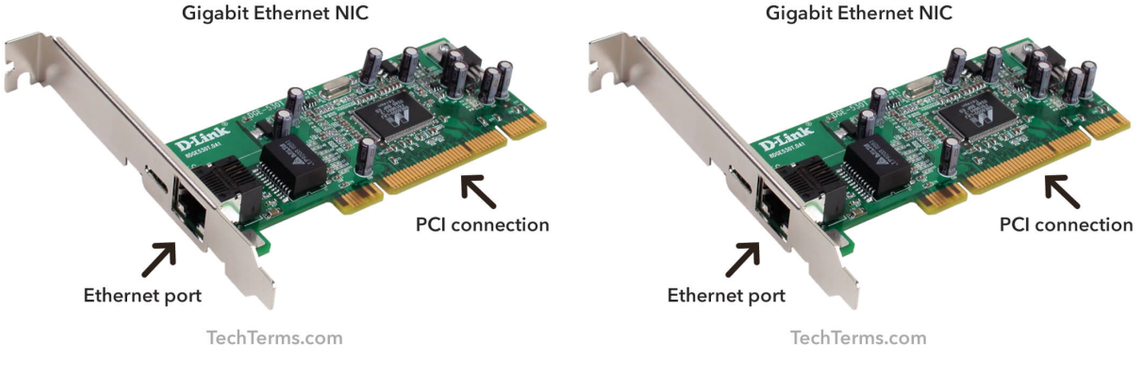

Gigabit Ethernet NIC
PCI connection
Ethernet port
TechTerms.com

+ HARDWARE



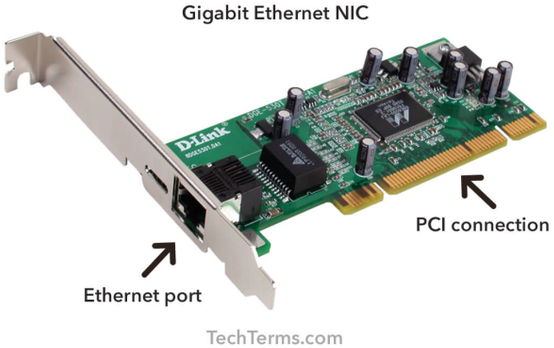
2 GB RAM + 1 USB Port or CD

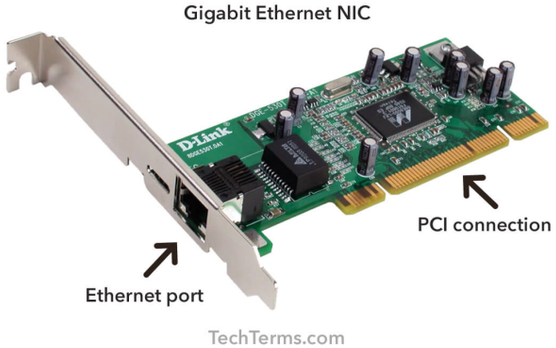
+ HARDWARE



2 GB RAM + 1 USB Port or CD

+ HARDWARE

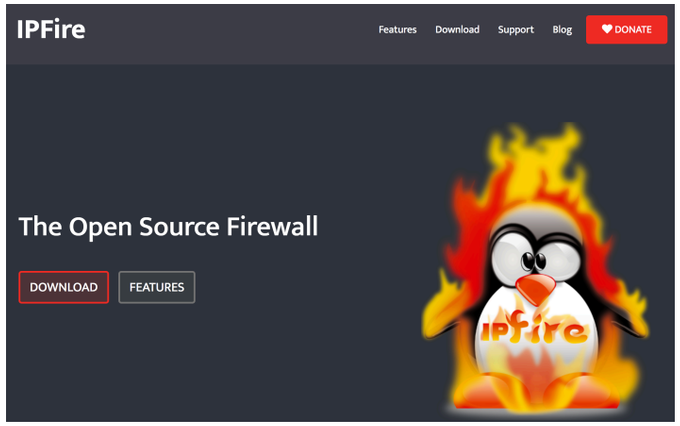




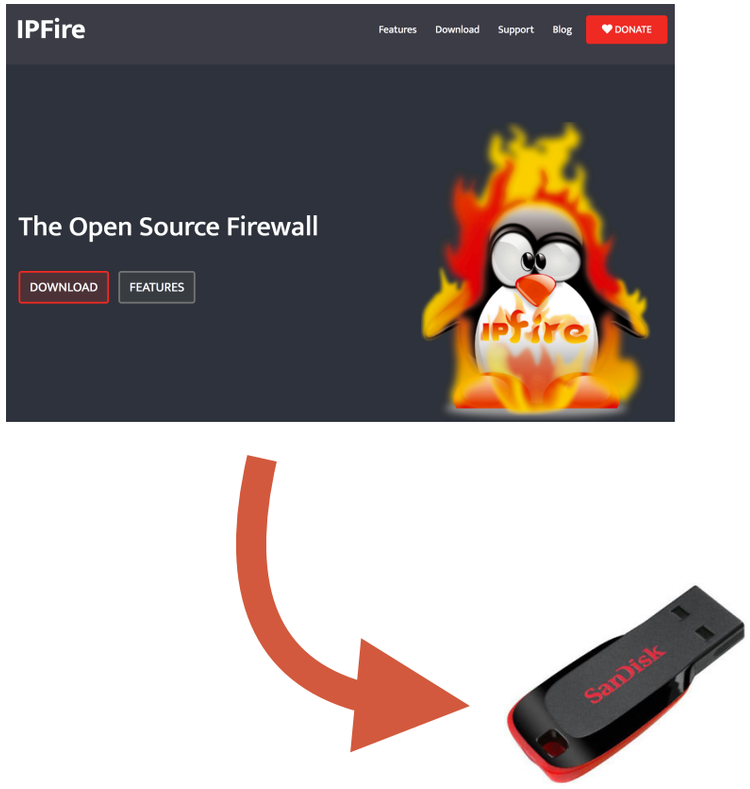
2 GB RAM + 1 USB Port or CD

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

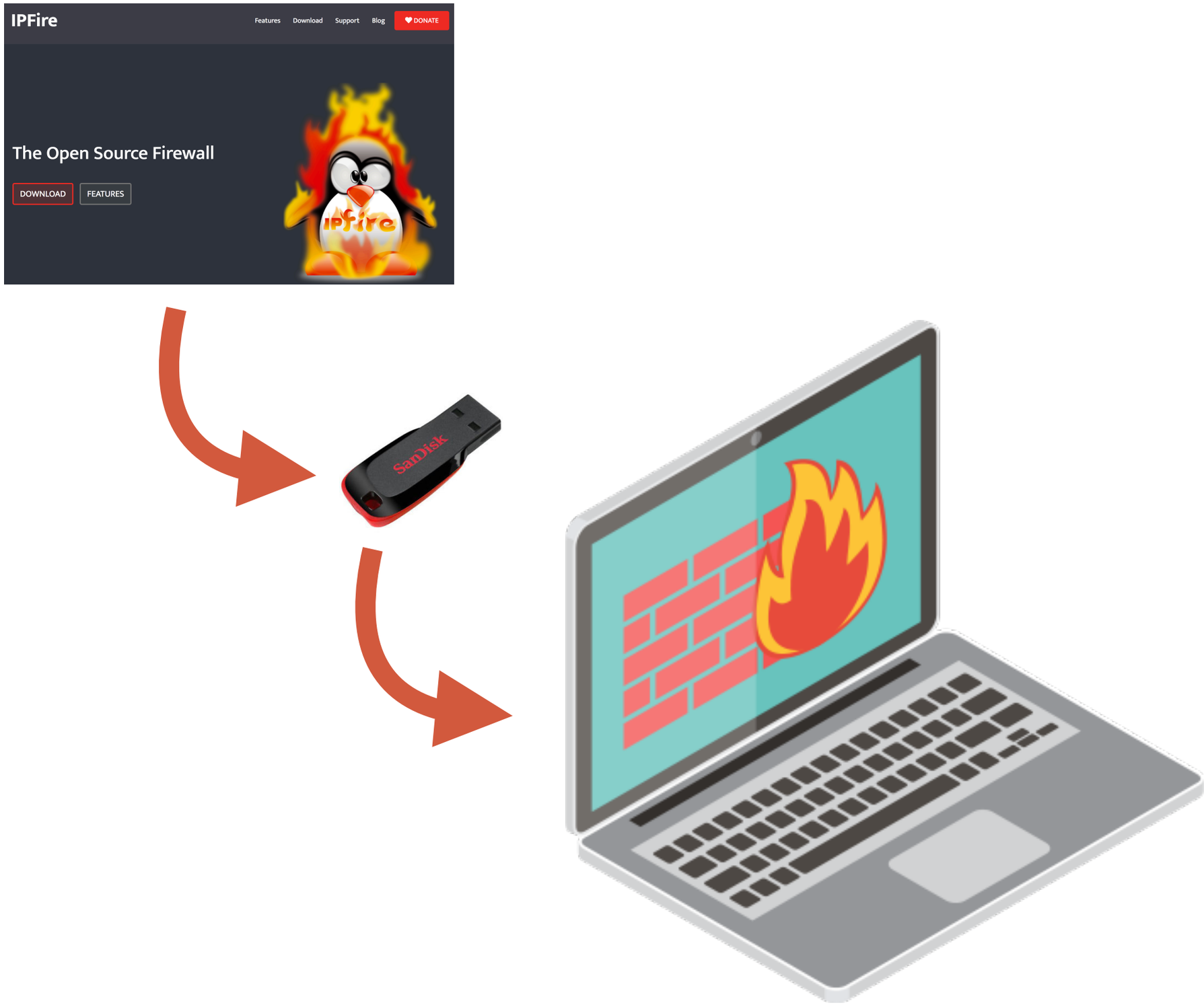
RUN IT OFF A USB STICK (NO HARD DISK)...



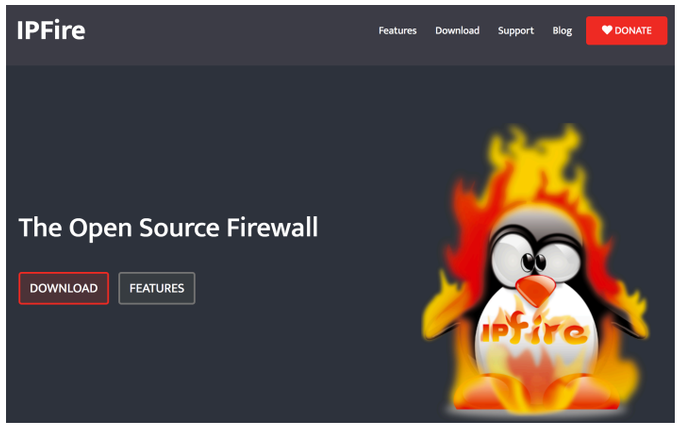
RUN IT OFF A USB STICK (NO HARD DISK)...



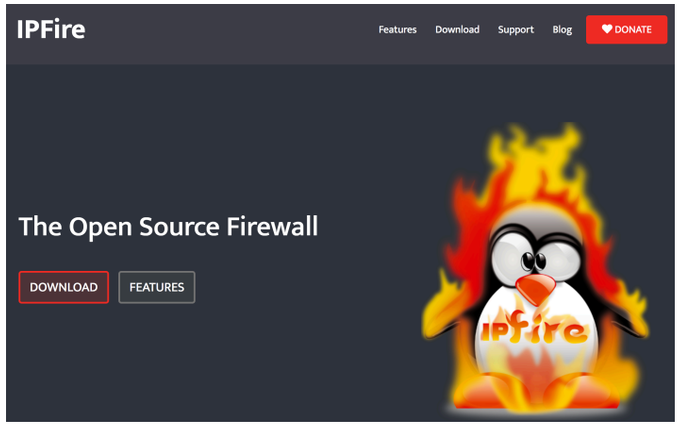
RUN IT OFF A USB STICK (NO HARD DISK)...

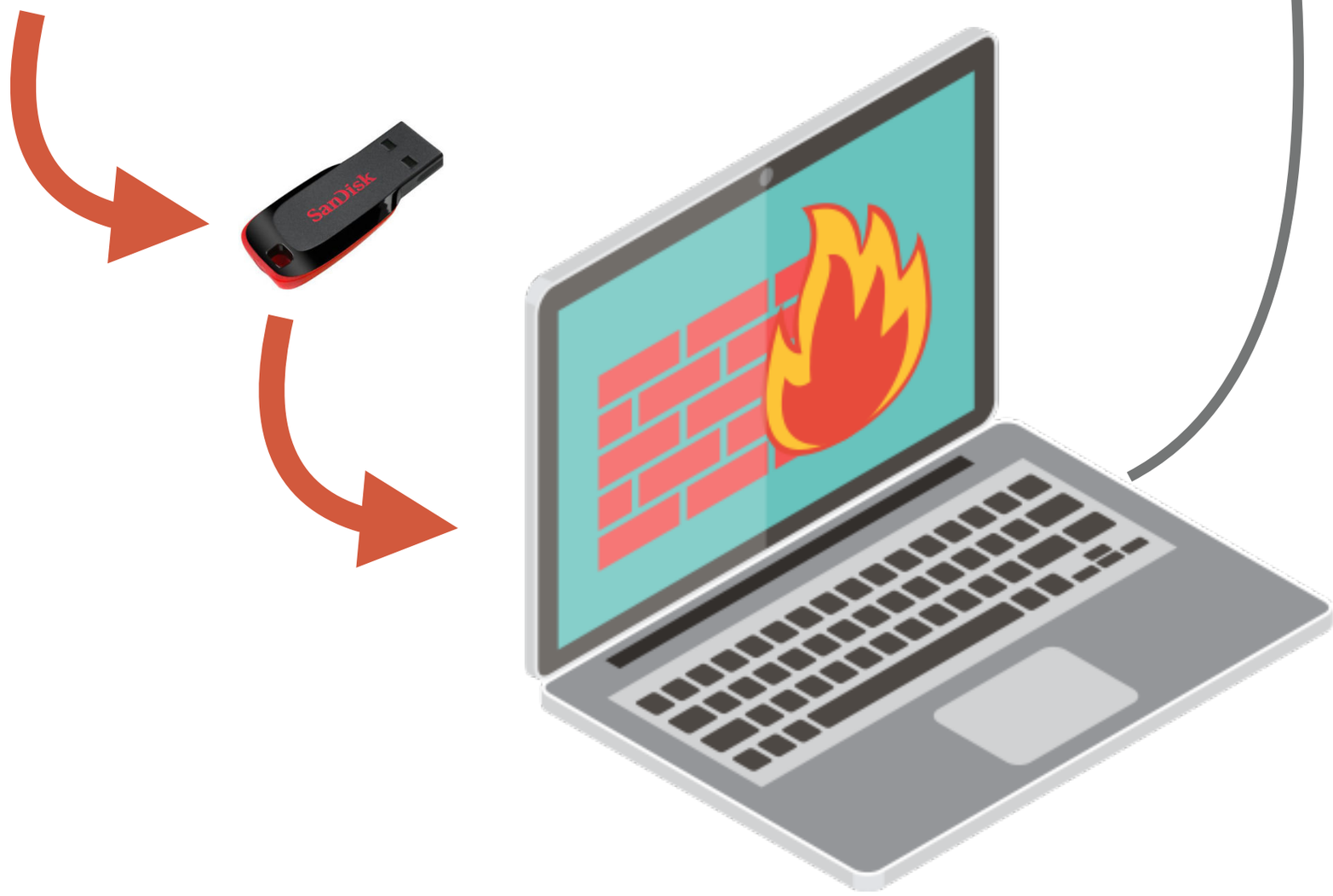


RUN IT OFF A USB STICK (NO HARD DISK)...

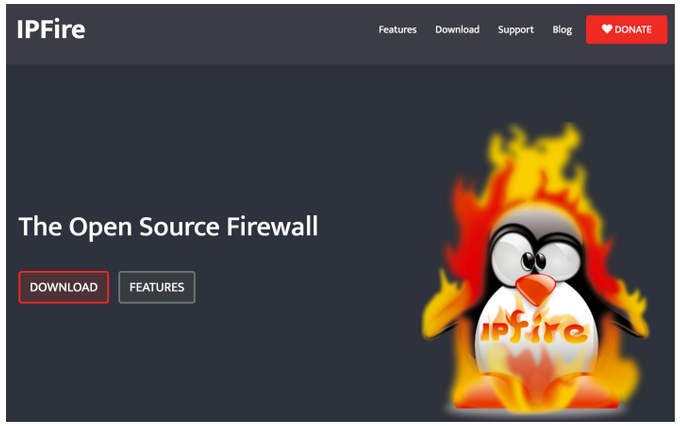


RUN IT OFF A USB STICK (NO HARD DISK)...

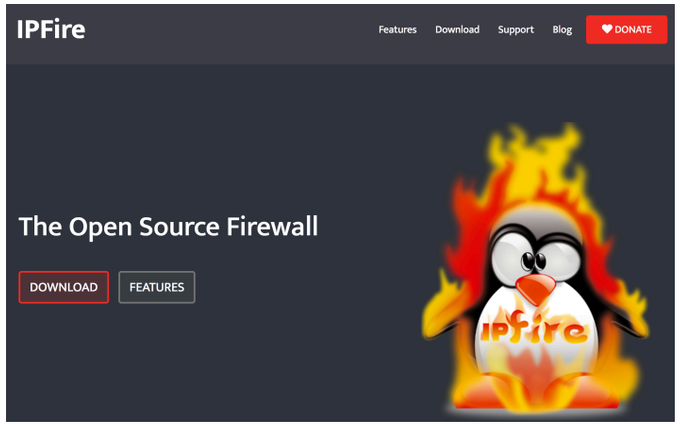




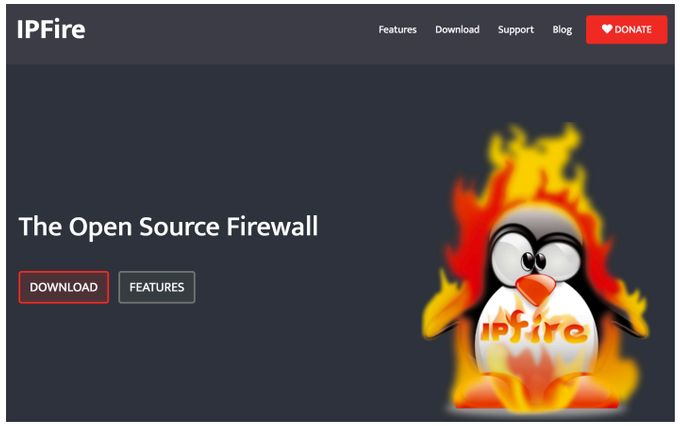
RUN IT OFF A USB STICK (NO HARD DISK)...

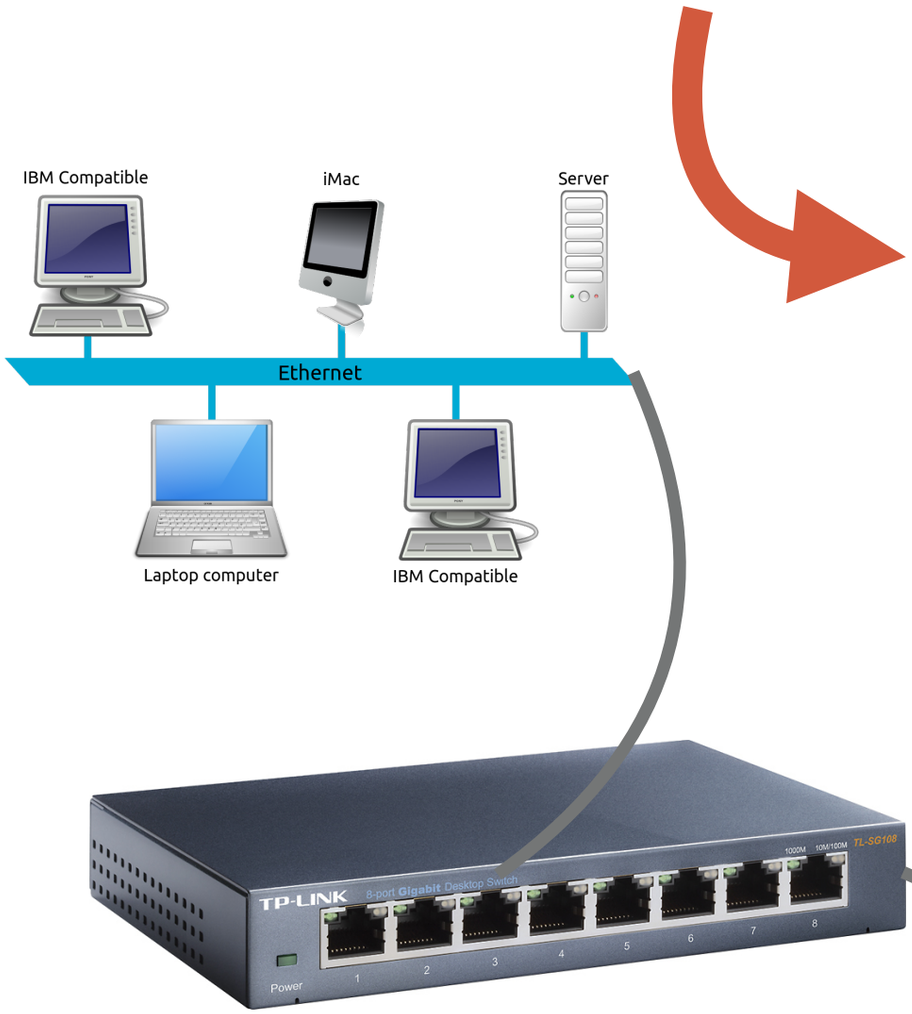


RUN IT OFF A USB STICK (NO HARD DISK)...



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





YOU CAN EVEN HAVE CLOUD FIREWALLS

YOU CAN EVEN HAVE CLOUD FIREWALLS

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

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

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