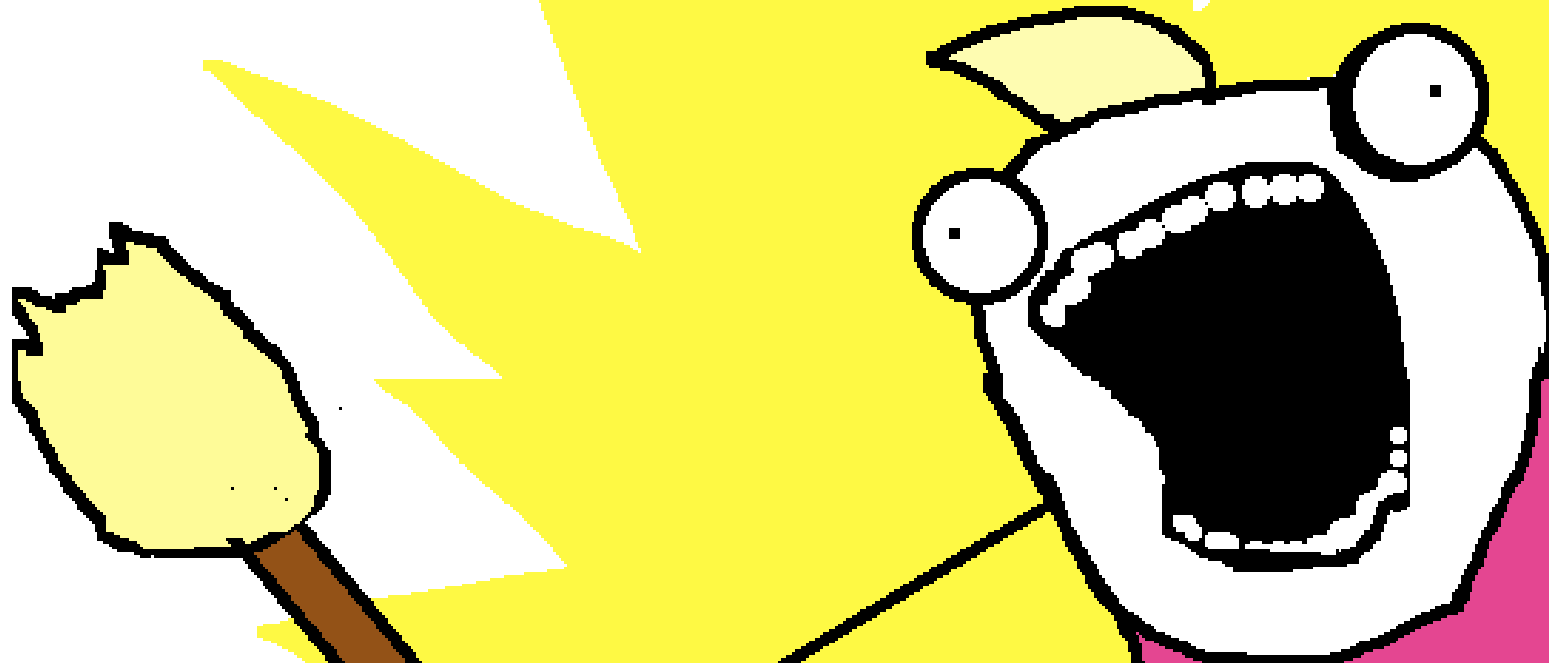


TOR



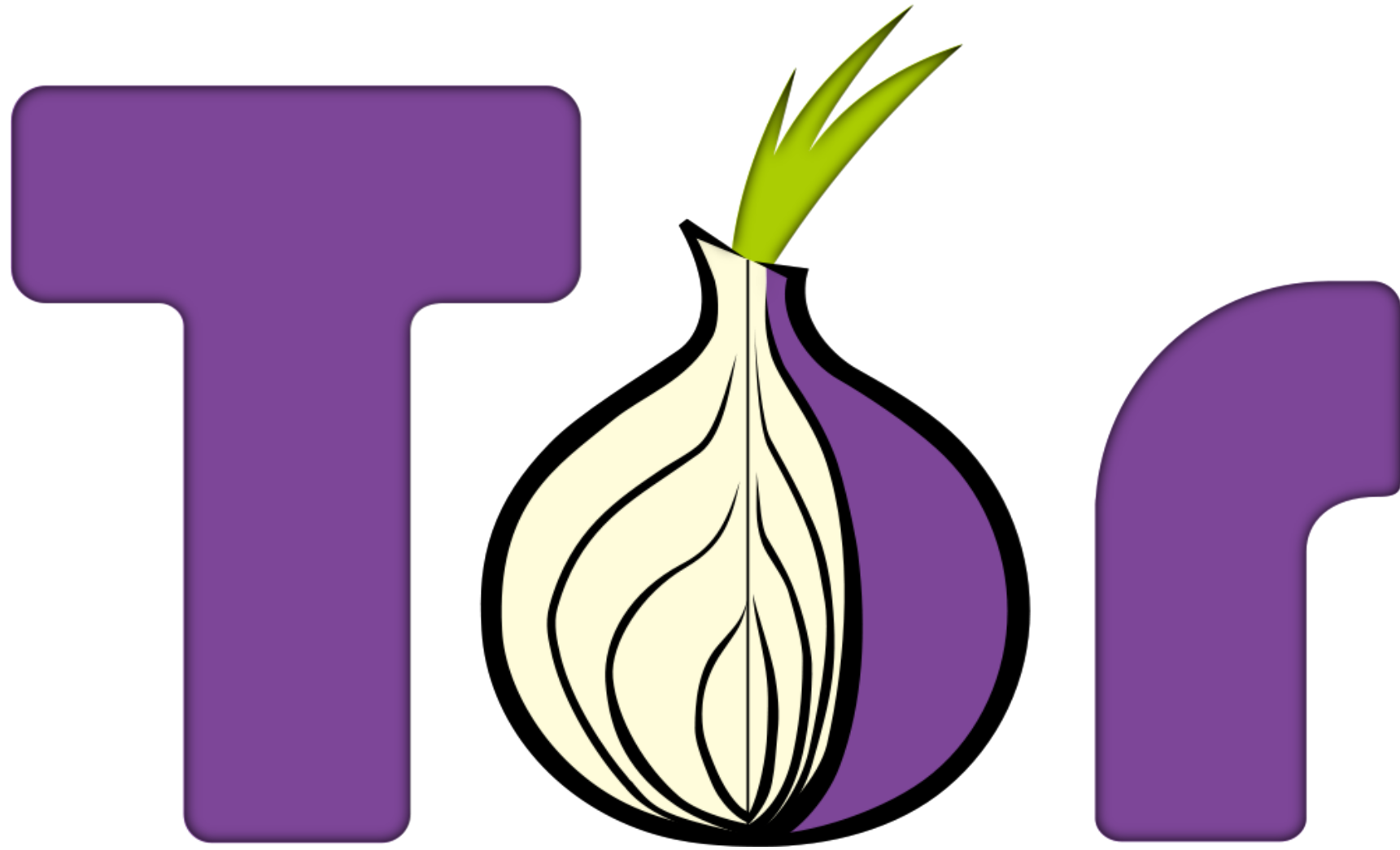
ALL THE THINGS

TOR... ALL THE THINGS!

Jason Geffner
Sr. Security Researcher
CrowdStrike, Inc.

Black Hat USA 2013



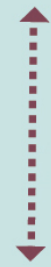





TORTILLA

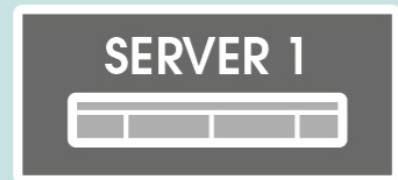
HOW TOR WORKS



Step 1
Tor client obtains a list of Tor nodes from a Tor directory server



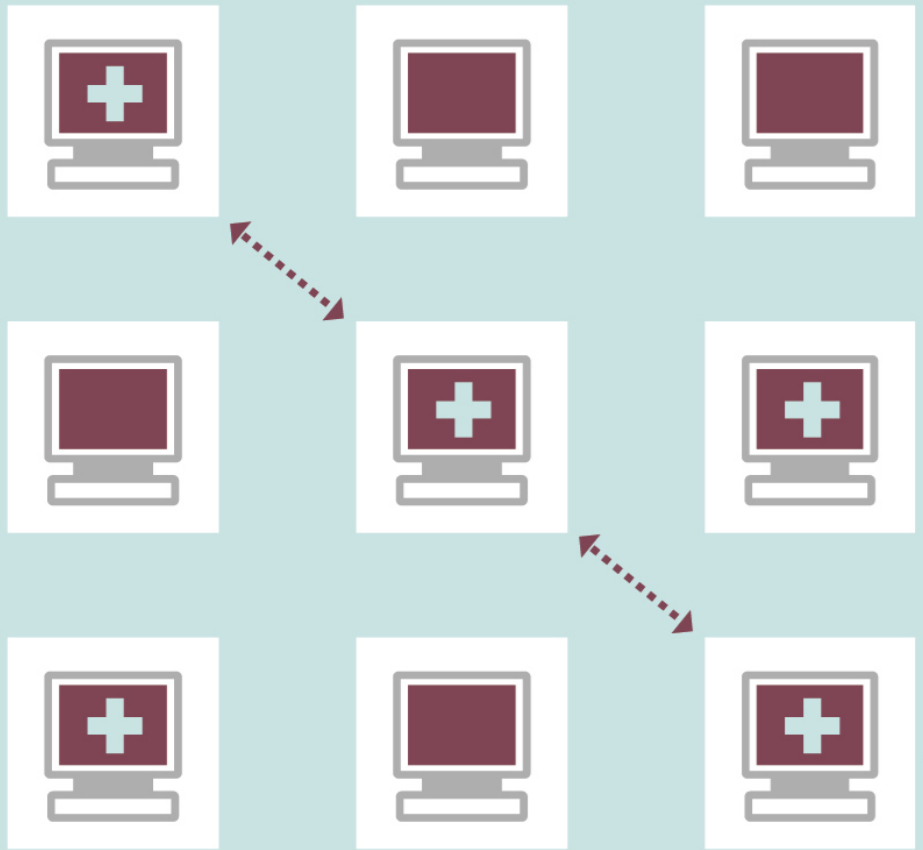
 TOR NODE
 UNENCRYPTED LINK
 ENCRYPTED LINK



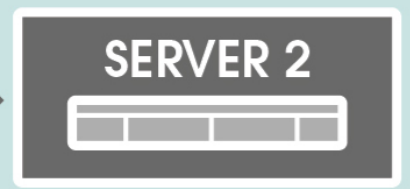
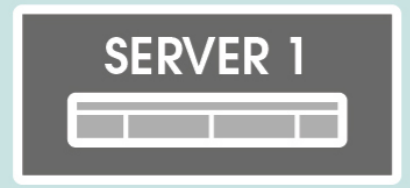
HOW TOR WORKS



Step 2
Tor client picks a random path to a destination server



+ TOR NODE
↔ UNENCRYPTED LINK
⋯ ENCRYPTED LINK

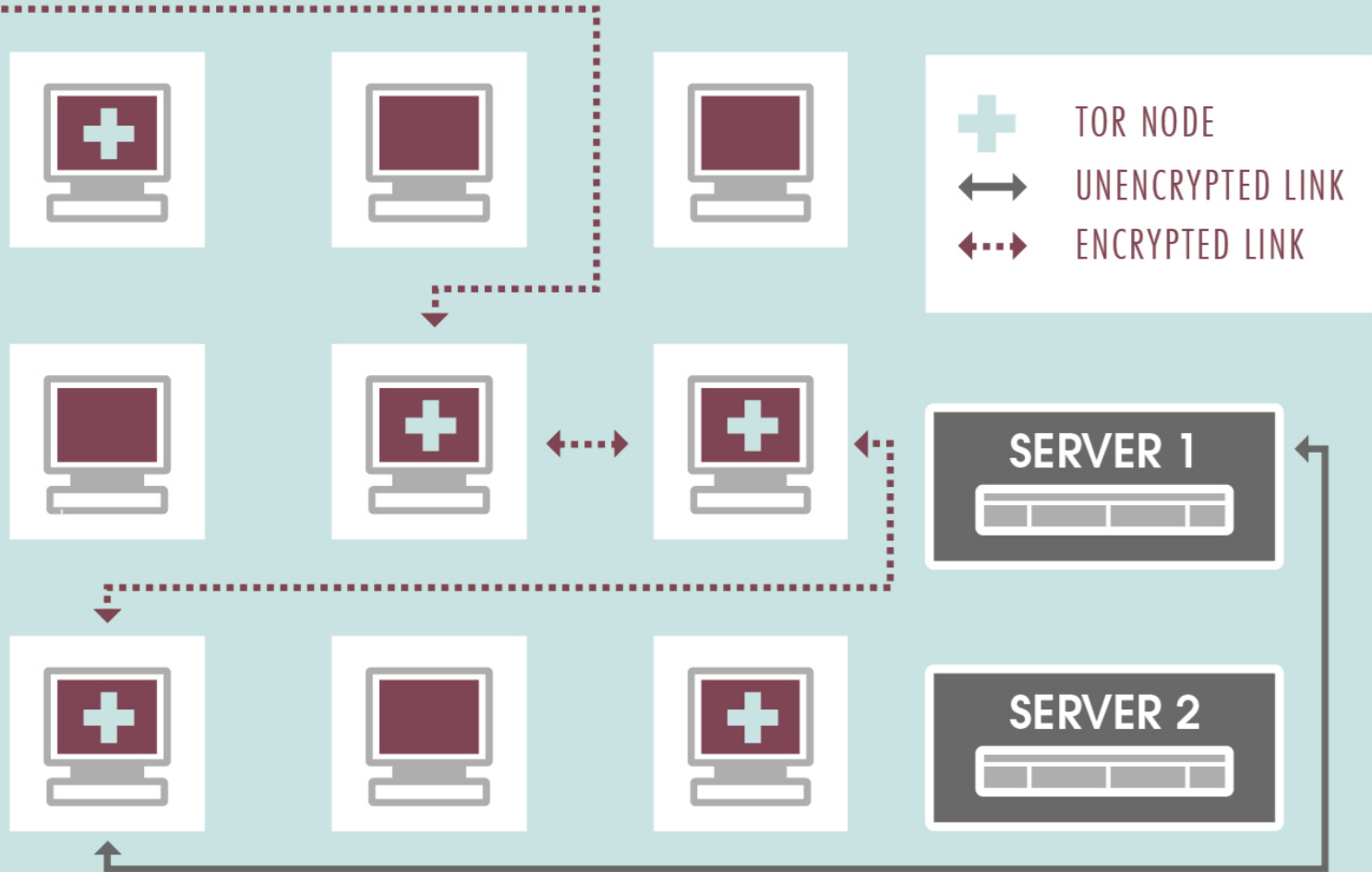


HOW TOR WORKS

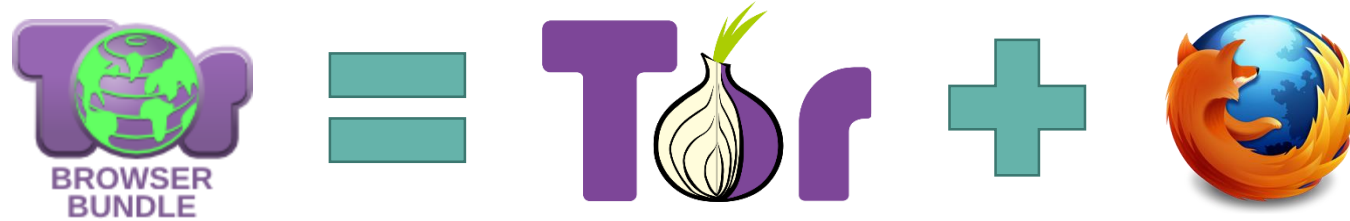


Step 3

Tor client picks another random path to connect to a different destination server



Tor Browser Bundle



- Tor
 - Runs a SOCKS server listening on TCP port 9050
 - SOCKS server routes traffic through global Tor network
- Modified Firefox ESR
 - Routes all web traffic through Tor's local SOCKS server
 - Disables Flash and all other plugins to deter identity leakage

Problems with Tor Browser Bundle

- Firefox only
 - No other browsers natively supported
 - No plugins allowed
- SOCKS server
 - Most software does not support TCP proxying via SOCKS
 - Even software that does support TCP proxying via SOCKS usually doesn't support DNS proxying via SOCKS

Ideal Tor Solution

1. Transparently route all TCP and DNS traffic through Tor
2. Do not allow any network traffic onto the Internet unless it goes through Tor
3. Do not require typical user to install an unfamiliar OS
4. Do not allow malware to circumvent Tor tunnel and communicate directly with the Internet
5. Do not require extra hardware or extra VMs

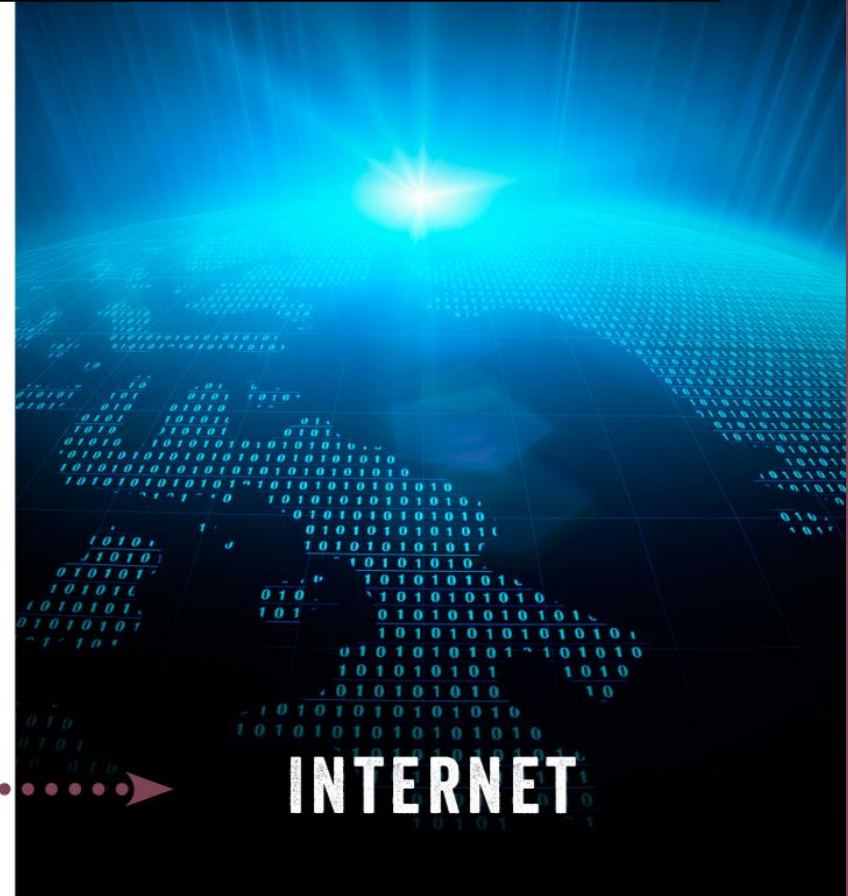
Existing Non-Ideal Solutions

- Hardware-Based Transparent Proxy
 - Solutions such as Onion Pi and P.O.R.T.A.L. require additional hardware
 - Malware could connect to a different WiFi network and circumvent Tor tunnel
- Software-Based Transparent Proxy
 - Tor does not support transparent proxying on Windows since it's implemented via `/dev/pf`
 - Requires non-Windows OS on a host system or additional VM such as Whonix
- Tails - Debian-based non-Windows OS
- Torcap - Malware can circumvent Winsock hooks

HOW CAN WE SECURELY WRAP TOR AROUND TRAFFIC?



COMPUTER



INTERNET



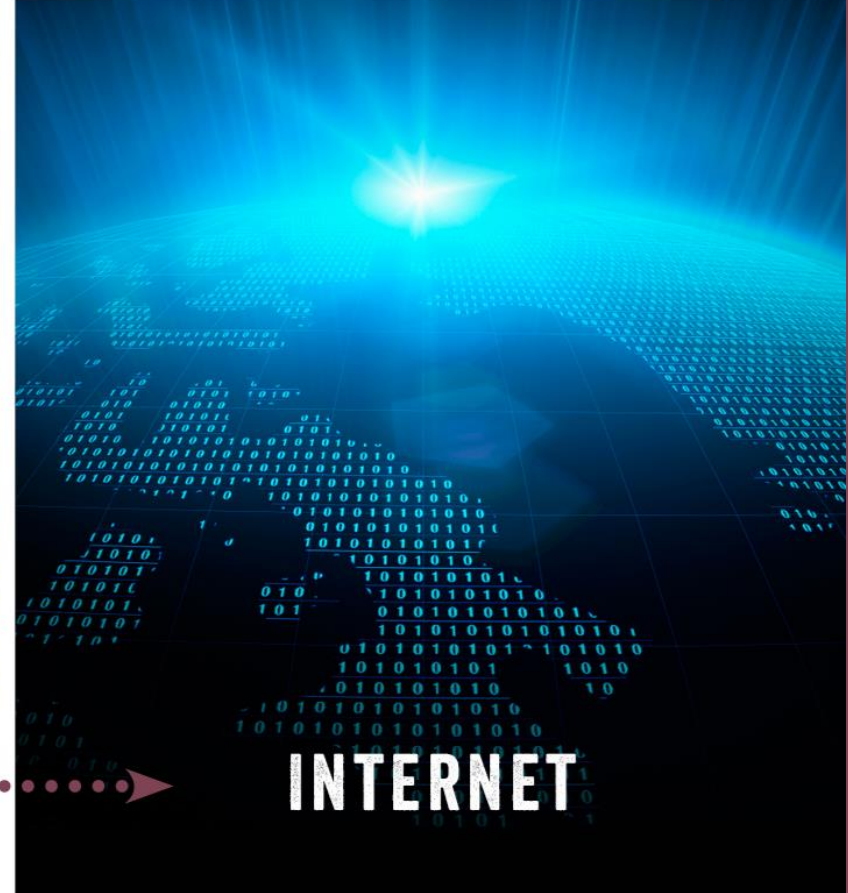
HOW CAN WE SECURELY WRAP TOR AROUND TRAFFIC?



COMPUTER



TORTILLA

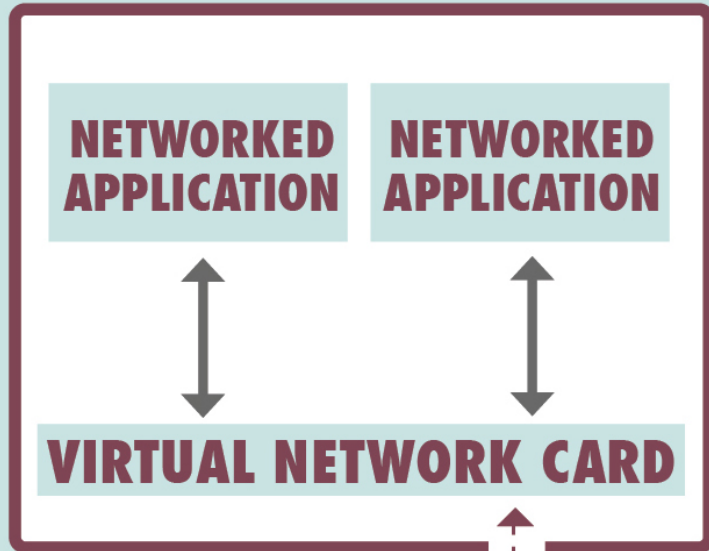


INTERNET

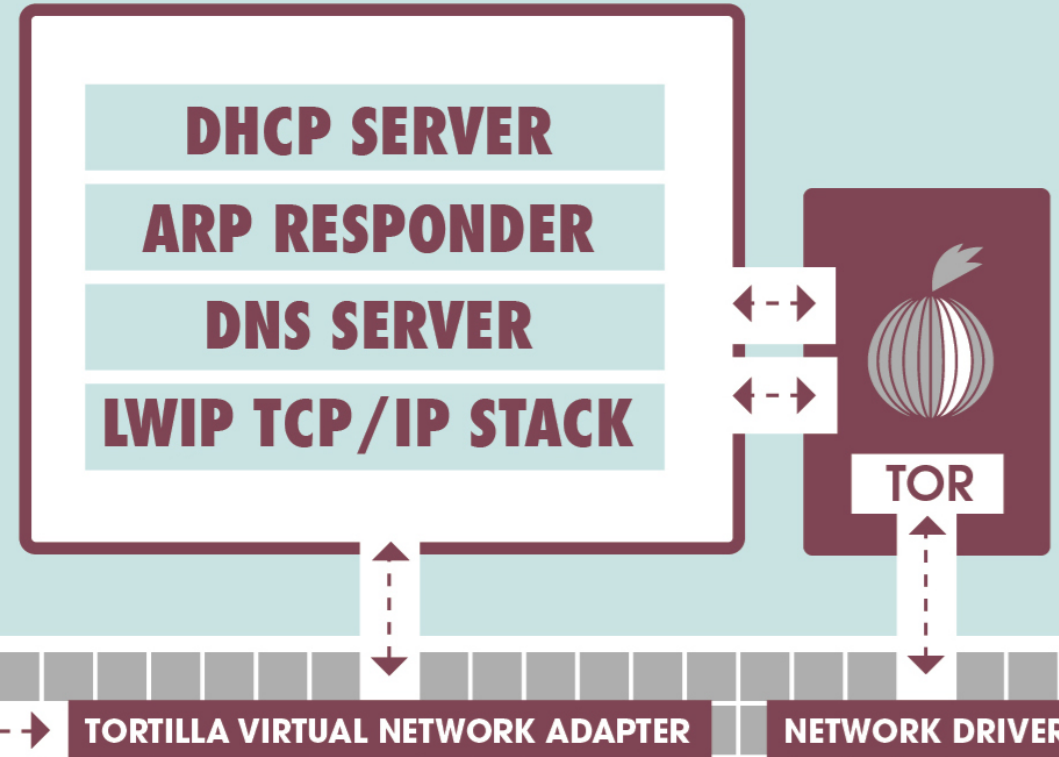
TORTILLA

TORTILLA ARCHITECTURE

VIRTUAL MACHINE



TORTILLA CLIENT



USER MODE

KERNEL MODE

VIRTUAL NETWORK BRIDGE

TORTILLA VIRTUAL NETWORK ADAPTER

NETWORK DRIVER

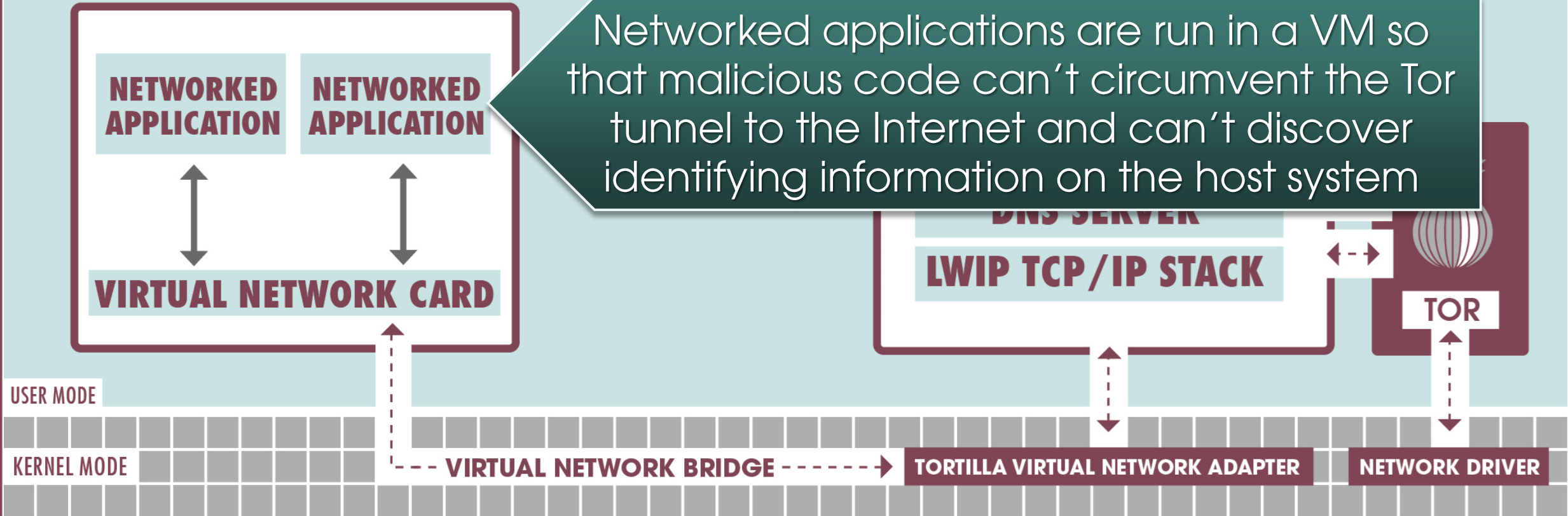
TORTILLA

TORTILLA ARCHITECTURE

VIRTUAL MACHINE

TORTILLA CLIENT

Networked applications are run in a VM so that malicious code can't circumvent the Tor tunnel to the Internet and can't discover identifying information on the host system

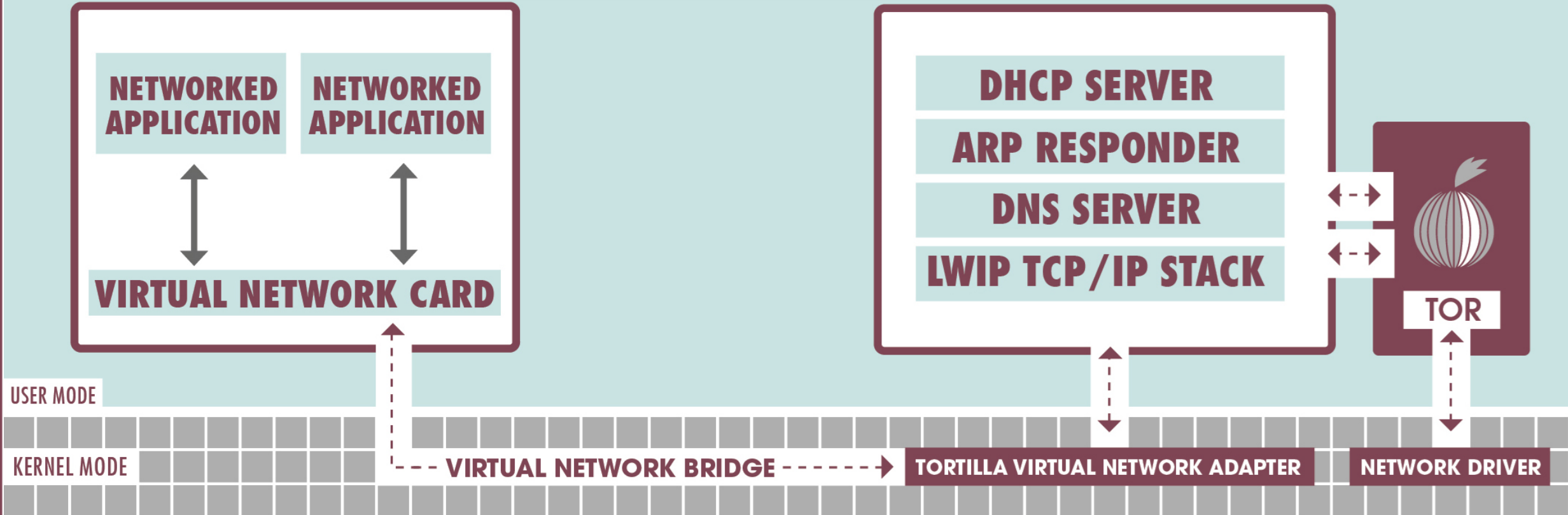


TORTILLA ARCHITECTURE

VIRTUAL MACHINE

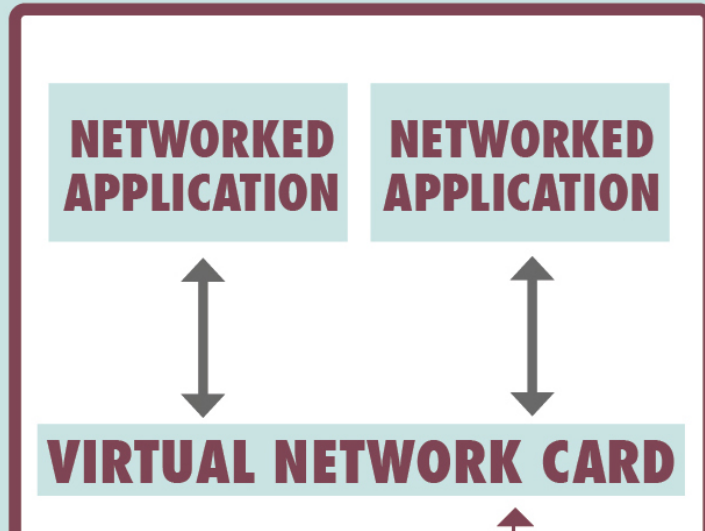
Tortilla is VM-platform agnostic and guest-OS agnostic

LLA NT

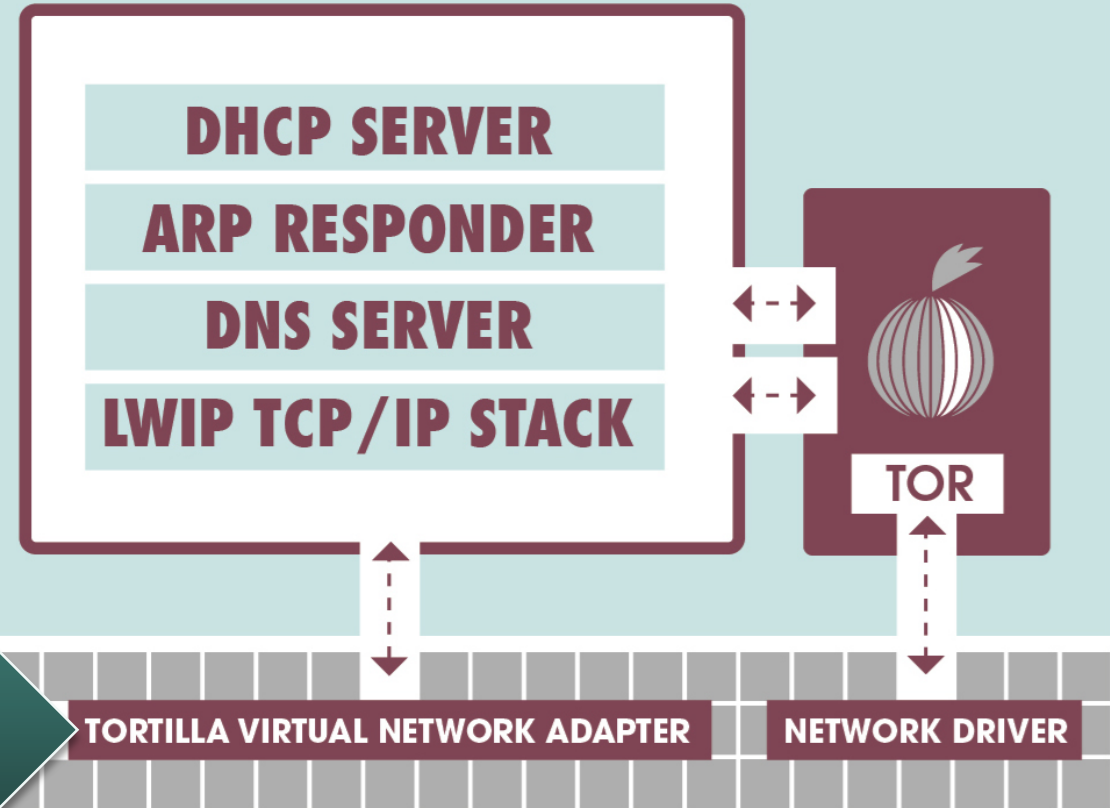


TORTILLA ARCHITECTURE

VIRTUAL MACHINE



TORTILLA CLIENT

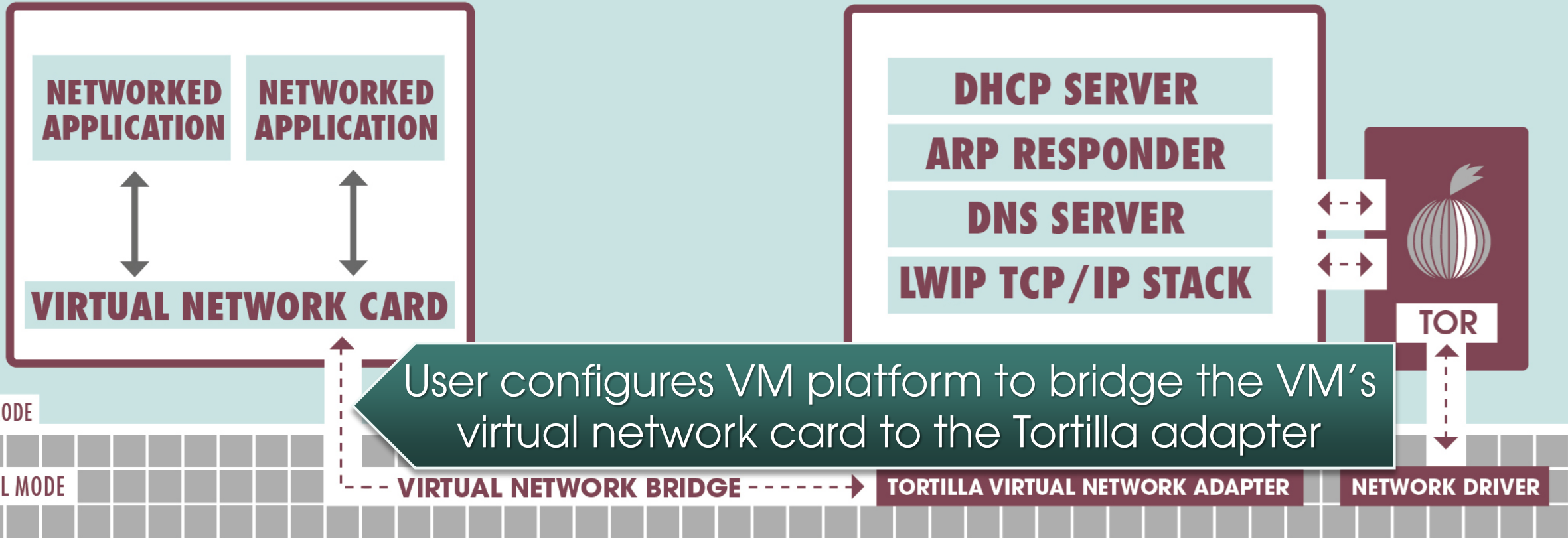


Tortilla installs a virtual network device & corresponding NDIS miniport driver, and disables all network component bindings except for that of the Virtual Network Bridge

TORTILLA ARCHITECTURE

VIRTUAL MACHINE

TORTILLA CLIENT



TORTILLA ARCHITECTURE

VIR
MAC

Tortilla Client receives all Layer 2 network traffic from the VM's virtual network card

TORTILLA CLIENT

NETWORKED APPLICATION

Basic DHCP server and ARP responder give the VM an IP address

DHCP SERVER

ARP RESPONDER

DNS SERVER

LWIP TCP/IP STACK

VIRTUAL NETWORK CARD



TOR

USER MODE

KERNEL MODE

VIRTUAL NETWORK BRIDGE

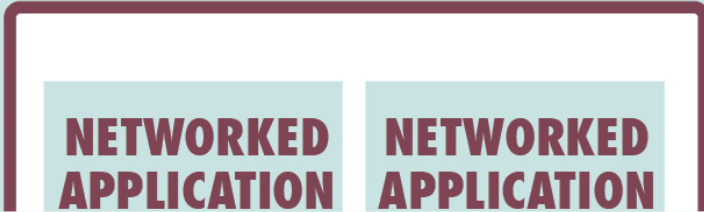
TORTILLA VIRTUAL NETWORK ADAPTER

NETWORK DRIVER

TORTILLA

TORTILLA ARCHITECTURE

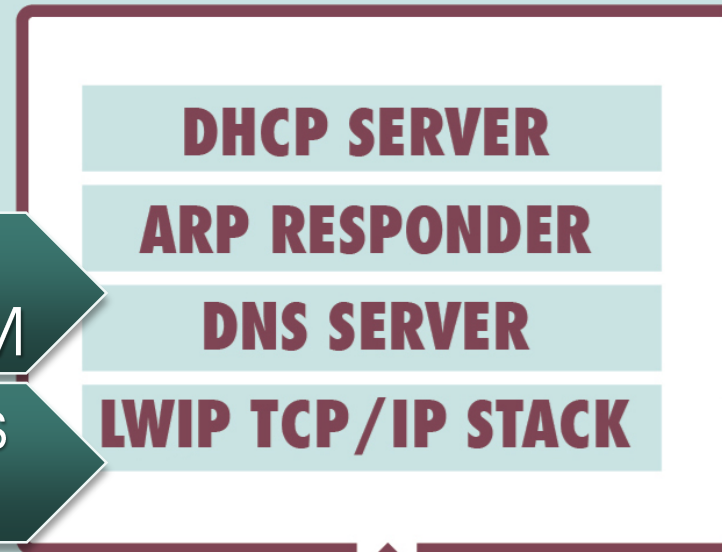
VIRTUAL MACHINE



DNS server parses DNS queries, requests lookups via Tor and sends responses to VM

Open-source Lightweight IP stack proxies TCP sessions between VM and Tor

TORTILLA CLIENT



USER MODE

KERNEL MODE

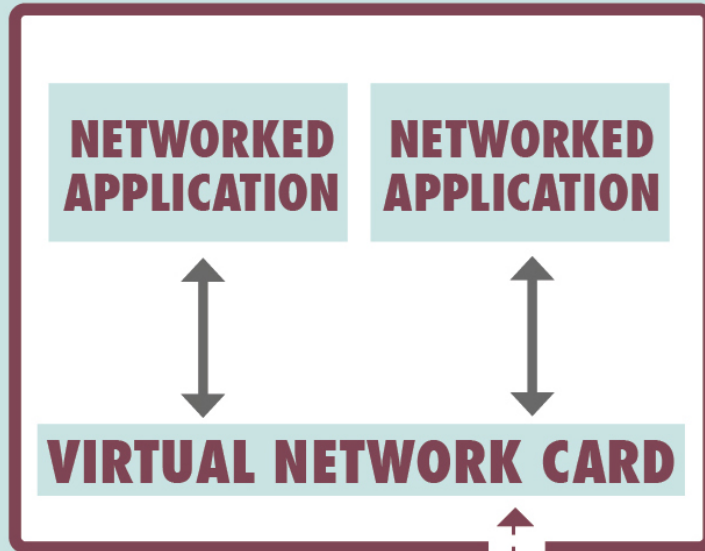
VIRTUAL NETWORK BRIDGE

TORTILLA VIRTUAL NETWORK ADAPTER

NETWORK DRIVER

TORTILLA ARCHITECTURE

VIRTUAL MACHINE

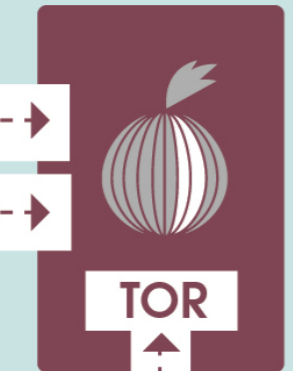
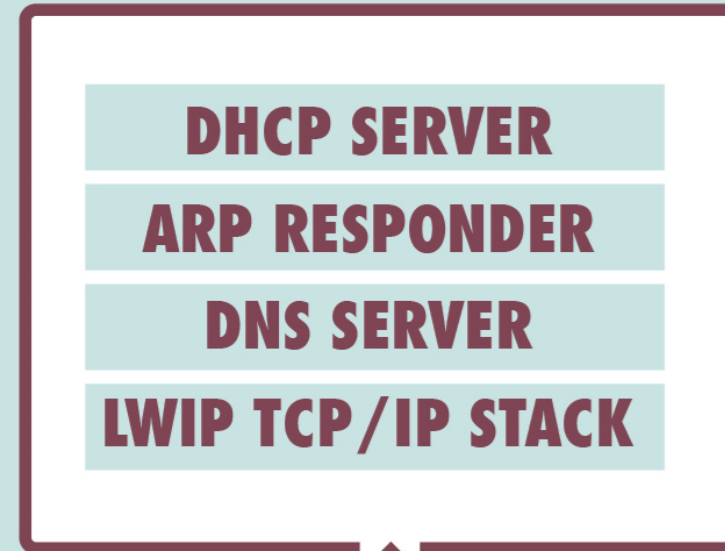


USER MODE

KERNEL MODE

VIRTUAL NETWORK BRIDGE

TORTILLA CLIENT



NETWORK DRIVER

No packets from the VM ever touch the host's actual network driver

TORTILLA

Tortilla is open-source
and supports
32-bit and 64-bit
Windows host
systems



Installation and Usage

- Tortilla ships as a single executable – Tortilla.exe
- When Tortilla.exe is executed on host system:
 - Extracts default Tortilla.ini file if not already on disk
 - Extracts 32-bit or 64-bit driver, depending on host OS
 - Extracts and executes driver installer
 - Installs Tortilla device and driver if not already installed
 - Disables all of the device's network component bindings except for that of the Virtual Network Bridge

Installation and Usage

- When Tortilla.exe is executed on host system:
 - Establishes secure communication channel between Tortilla client and driver
 - Begins listening for Layer 2 packets from VM
 - Acts on DHCP, ARP, DNS, and TCP packets, and drops everything else
 - Optionally stores all traffic to and from VM in a PCAP file on host

Complete Failsafe Functionality

- User can run Tor before or after starting Tortilla.exe
- User can run VM before or after starting Tortilla.exe
- User can configure VM platform's Virtual Network Bridge before or after starting Tortilla.exe (though Tortilla device must already be installed)

Minimal System Footprint

- No registry modifications (aside from Tortilla device and driver installation)
- No file system modifications (aside from Tortilla.ini and installed Tortilla driver)
- Can be uninstalled by just deleting Tortilla.exe and Tortilla.ini, and uninstalling Tortilla Adapter from Device Manager

Demo

Free and Open-Source

You can download Tortilla right now!

<http://www.crowdstrike.com/community-tools>

Summary

- Tortilla is a free and open-source solution for Windows that transparently routes all TCP and DNS traffic through Tor
- Tortilla does not allow any network traffic onto the Internet unless it goes through Tor
- Tortilla does not require extra hardware or extra VMs
- The Tortilla platform does not allow malware to circumvent the Tor tunnel to communicate directly with the Internet

Q & A

Special Thanks

- John Costello
- Cameron Gutman
- Alex Ionescu
- Sven Krasser
- Dan Kurc
- Kyle Larsen
- Aaron Putnam



@CrowdStrike