SHADOW GRID

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Downrange: Past Performance

- Multiple existing deployments across multiple customers
  - All Global
  - 99.99% SLA
  - Over 100 servers managed in three data centers and the cloud
  - Zero intrusions
- 12 current deployments of research (non-collaborative) NA networks
- Experience:
  - 10 years experience designing, developing, deploying and maintaining Cov-Comm capabilities and NA infrastructure
  - 12 years experience as a network/software architect in diverse positions
  - 21 years experience as an Intelligence Professional/Soldier

What is ShadowGrid?

ShadowGrid is secure communications and collaboration platform designed for use by forward deployed elements. Its main purpose is to facilitate collaboration between elements from *across the street or across the ocean* with zero attribution to the elements using the system.

- **Shadow-Wire:** An encrypted email platform designed to facilitate secure, private, real-time communications between individuals and organizations
- **Shadow-Voice:** A mis-attributable voice communication system designed to evade LE and LI through the intelligent employment of high-volume call trunking services, dynamic call routing and redirection
- **Ricochet:** A software suite used to dynamically create on-demand, non-attributable communication nodes, in near-real time, around the world
- **Shadow-Desk:** A web-based Virtual Desktop Environment. Useful for client-less, NA web browsing and persona management. **Does not require any client software.**

SHADOW GRID

DOWNRANGE TECHNOLOGIES

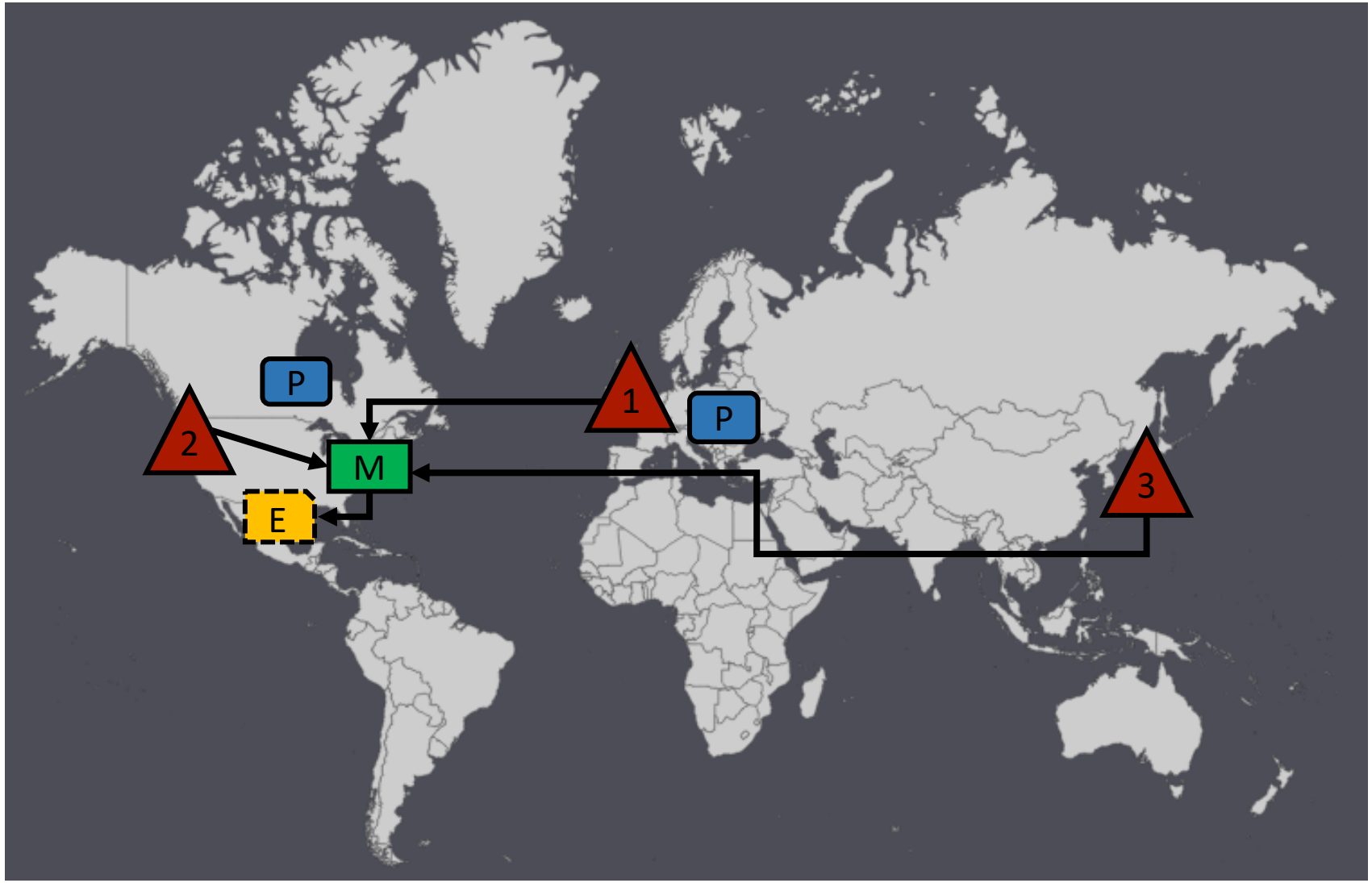
Basic Functionality

- Users log in to ShadowGrid using a VPN client and pre-shared keys
  - Clients: Mac, Windows, Linux, Android, iOS, freely available
- Users can enter the network from a Forwarding Server or directly into the Main Server
  - Forwarding Servers simply re-route traffic to the main server. They do not have any crypto keys on them
- Once on the network, all client traffic passes from the client through the VPN. Any external routing is attributable to the main server (or exit server, as designed)
  - The network can be configured to block outgoing traffic
- The internal network offers multiple services for collaboration
- The network employs standard enterprise-grade services
  - Backup, Monitoring, Redundancy, Failover, etc

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Typical Deployment



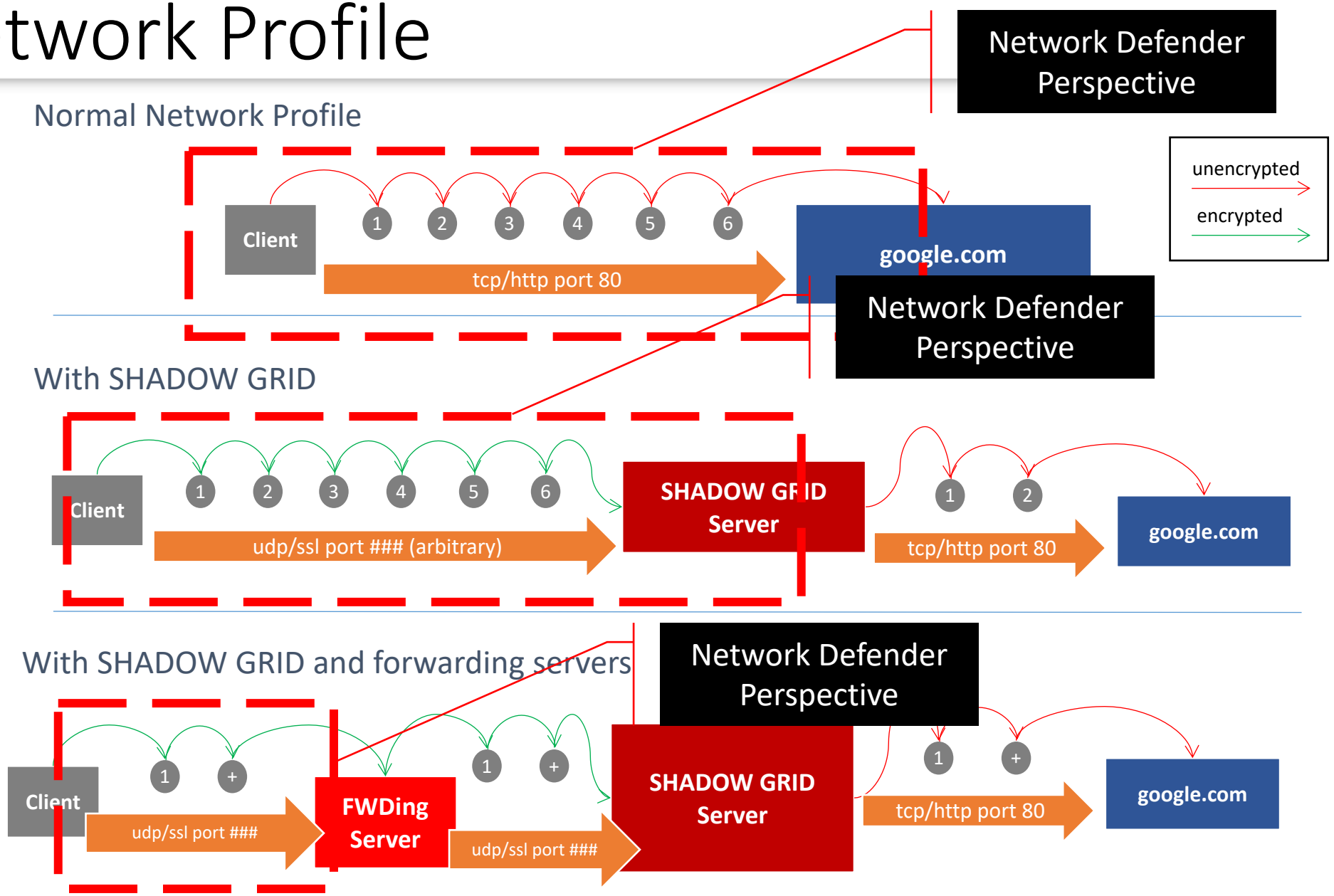
Forwarding Server

Main Server

PBX

Exit Server

Network Profile



SHADOW GRID

DOWNRANGE TECHNOLOGIES

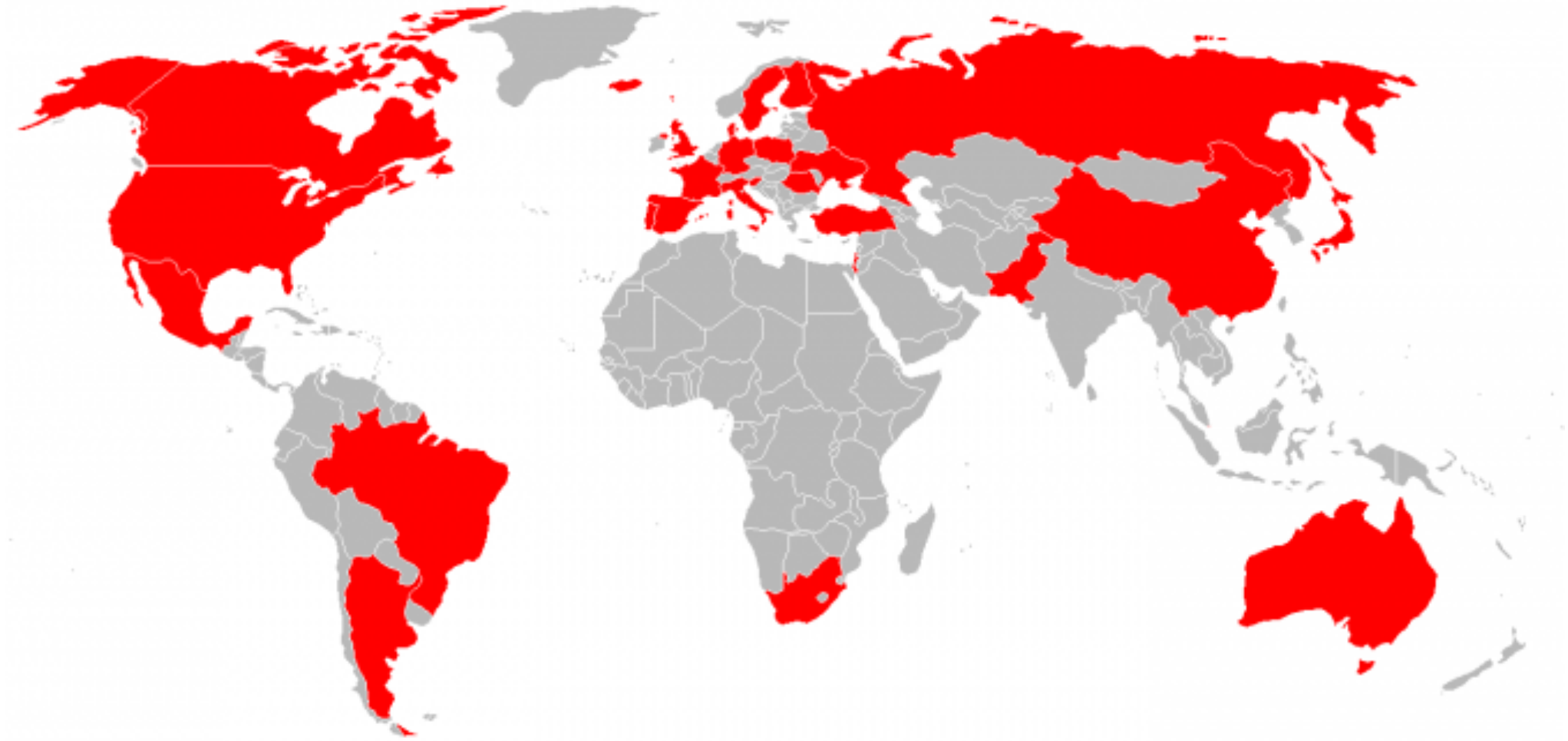
Network Attribution: A Tiered Approach

Tier	Location	Datacenter	Server Ownership	Type	Cost	Attributability
1	US	Private	Owned	Physical	Highest	Extremely High
		Commercial	Owned	Physical	Highest	High
			Rented	Physical	Higher	High
			Rented Virtual		Medium	Low
2	N. America Europe	Commercial	Owned	Physical	High	Medium
			Rented	Physical	High	Medium
			Rented Virtual		Lowest	Low
3	Other Areas	Commercial	Rented	Physical	Medium	Medium
			Rented Virtual		Medium	Low

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Server Deployment Areas



SHADOW GRID

DOWNRANGE TECHNOLOGIES

Passive Services and Benefits

- **False Positive Generator**
  - **Active:** Portable Software that Users can run to generate bogus traffic to throw off a network defender (automates the Soccer Mom profile)
  - **Passive:** Runs behind the scenes and generates the same traffic from all servers
- **Antivirus:** All email is scanned by *clamav* before being sent to the user's mailbox
- **Proxy Services:** Automatically block/deny known malware sites for users as they browse the web.
- **Automatic Patching:** Servers are configured to automatically patch themselves with critical security updates two times a day
- We employ multiple hot-spares (Servers and Phone Numbers)
- **All resources are purchased non or mis-attributably**

Shadow-Wire: Features

- Email
  - Multi-layer encryption (2,048-bit for data, 256-bit for Control Channel)
  - Two-Factor Authentication available
  - Accessible via web interface or Mail Client
  - Real-Time Chat (web or w/client)
  - Web-Based video Chat (no software needed)
  - **Internal Only**; No external mail delivery allowed
    - Users have an *@shadowgrid.vpn* email address (or domain of your choice)
  - Globally Accessible
    - When using a forwarding server, the main server's location is obfuscated
  - Nothing left on the client
  - Extremely easy to use

Shadow-Voice: Features

- International: Able to allocate local numbers in over 60 countries
- Call Mis-Direction
  - Person A calls Person B, but two (2) CDRs are generated
  - Person B does not know Person A's true phone number
- Caller Mis-Attribution
  - Person A calls a pre-defined number and enters their password
  - They are given a dial tone and can call any number they want
  - CID is set to a specific callback number or "Unknown".
- Internal to Internal calling, completely secure

Scenario #1: Person to User

Scenario:
Person wants to call **User**.
Person's phone number is **(123) 456-7890**
User has a forwarding number of **(890) 123-4567**
User's actual phone number is **(456) 789-0123**
Person calls **User** at **(890) 123-4567**.
User's phone rings. The caller ID shows **(000) 000-9999**.
Person and **User** are now talking

How does it work?

1. **Person's** call gets routed via their standard PSTN.
2. From the PSTN, the call reaches our PBX through an inbound SIP Trunk.
   - A single CDR is generated from **(123) 456-7890 -> (890) 123-4567**.
3. Our PBX generates a new call from an outgoing SIP Trunk to **(456) 789-0123** (via PSTN)
   - A second CDR is generated from **(000) 000-9999 -> (456) 789-0123**.

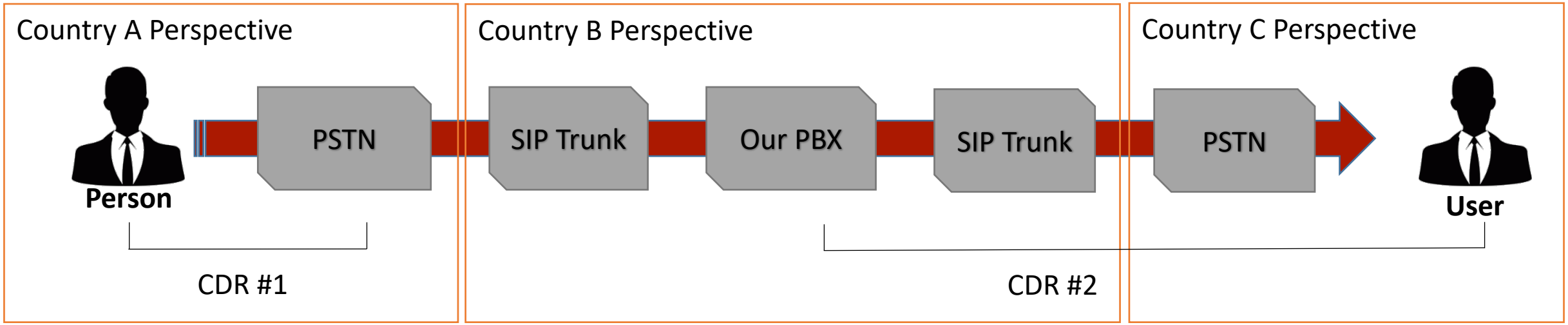
Important Considerations:

- The incoming and outgoing SIP Trunks are not the same (server and provider)
- There is an artificial delay between the incoming call and outgoing call (defeats rudimentary automated analysis)
- There are no location limitations; **Person** and **User** can be in disparate locations. As long as the forwarding number is in the same region as **Person's** incoming number, the call is not international.

What have we achieved?

- **Person** does not know **User's** true phone number
- **User** is aware that he is receiving a call from a non-standard person.
- The location of the PBX is not seen by LE/LI and is transparent to a network defender.
- Multiple CDRs are generated (good)
- No international call is made over the PSTN.

A Deeper Understanding



CDR #1: (123) 456-7890 -> (890) 123-4567 @ 14 DEC 14 -08:20:55
CDR #2: (000) 000-9999 -> (456) 789-0123 @ 14 DEC 14 -08:21:17

Scenario #2: User to Person

User wants to call **Person**.
User's phone number is **(123) 456-7890**
Person's actual phone number is **(456) 789-0123**
User calls his entry number at **(890) 123-9876** and enters his passcode.
User is given a dial-tone and enter **(456) 789-0123**
Person's phone rings. The caller ID shows **(890) 123-4567**.
Person and **User** are now talking.

How does it work?

1. User's call gets routed through our PBX and SIP Trunk.
2. From the SIP Trunk, the call reaches Person via their PSTN. , the call reaches our PBX through an inbound SIP Trunk.
   - A single CDR is generated from **(123) 456-7890 -> (890) 123-4567**.
3. Our PBX generates a new call from an outgoing SIP Trunk to **(456) 789-0123**.
   - A second CDR is generated from **(000) 000-9999 -> (456) 789-0123**.

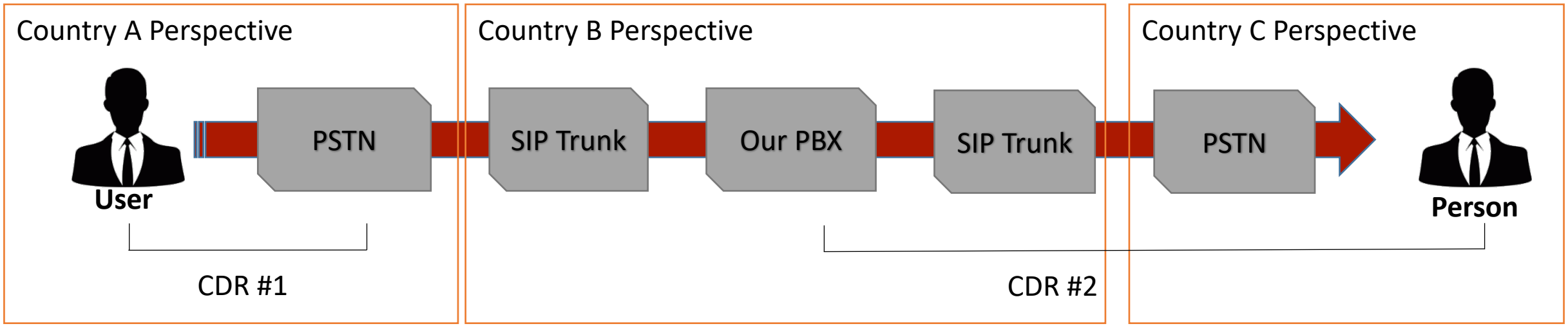
Important Considerations:

- The incoming and outgoing SIP Trunks are not the same (server and provider)
- There is an artificial delay between the incoming call and outgoing call (defeats rudimentary automated analysis)
- There are no location limitations; **Person** and **User** can be in disparate locations. As long as the forwarding number is in the same region as **Person's** incoming number, the call is not international.

What have we achieved?

- **User** can reach **Person**, from a seemingly local number.
- **Person** is unaware of **User's** location or true number.
- The location of the PBX is not seen by LE/LI and is transparent to a network defender.
- Multiple CDRs are generated (good)
- No international call is made over the PSTN.

A Deeper Understanding



CDR #1: (123) 456-7890 -> (890) 123-9876 @ 14 DEC 14 -08:20:55
CDR #2: (890) 123-4567 -> (456) 789-0123 @ 14 DEC 14 -08:21:17

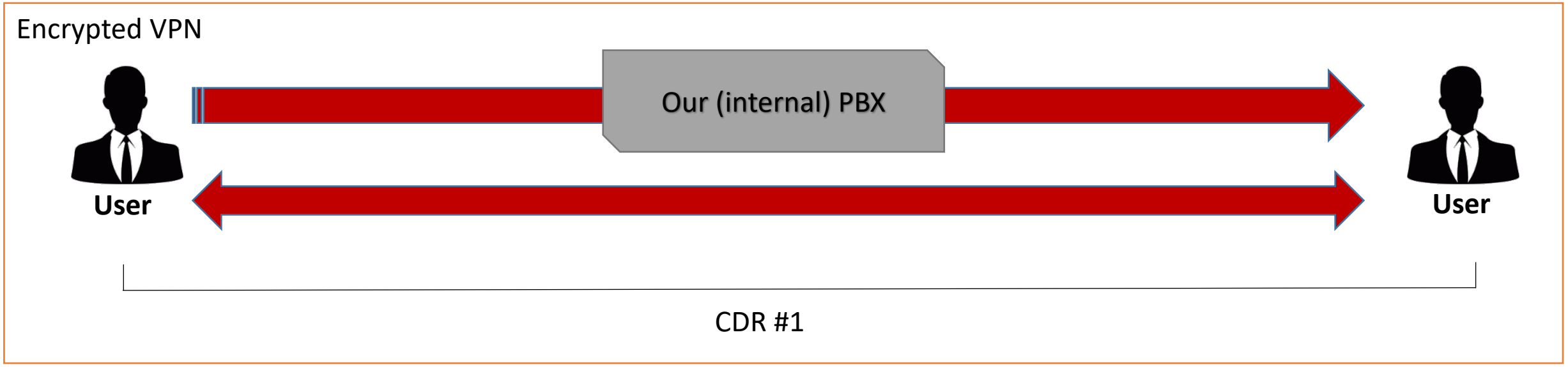
SHADOW GRID

DOWNRANGE TECHNOLOGIES

Scenario #3: User to User

- User 1 wants to call User 2
- User 1 has an extension (1001) and User 2 has an extension (1002).
- User 1 calls User 2
- User 1's handset calls the PBX. If User 2 is online, The PBX tells User 2's handset about User 1. It then passes the call off and voice data is routed directly between User 1 and User 2.
- If User 2 is not online, User 1 can leave a voicemail.
  - The voicemail will be emailed to User 2 within the internal email system (shadowgrid.vpn)
- Everything is handled internal to the VPN and is 100% secure
  - Double encryption is possible, but adds latency

A Deeper Understanding



CDR #1: 1001 -> 1002 @ 14 DEC 14 -08:20:55

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Ricochet

- Ricochet is a software toolkit engineered to dynamically provision, configure, and enable global secure communications on-demand. The toolkit allows users to quickly and easily standup global virtual communications infrastructure to enable secure data services, such as Anonymization, Anti-virus and encrypted communications.
- The software toolkit is designed for use by a beginner-to-intermediate operator and does not require in-depth technical knowledge to operate.
- The toolkit facilitates the immediate provisioning of 'ephemeral' virtual private servers (VPS) throughout the world.

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Ricochet: Features

- **Offers secure communications:** 1,024-bit RSA encryption and higher (FIPS 140-2 available)
- **Globally available:** Hosts can be placed in over 23 countries
- **Hosts secure:** Hosts are automatically secured using industry standard hardening techniques
- **On-The-Fly Host Generation:** Hosts are created on-demand and are never staged for use.
- **Self-Destruct:** Hosts are (optionally) securely destroyed upon logoff.
- **Multi-Hop Capable:** The Operator is capable of choosing the number and location of hops needed; Entry and exit points
- **Communications are Encrypted End-to-End:** Hop-Hosts do not contain crypto keys and cannot decrypt traffic; They are blind forwarders
- **Multiple Vendors Diversity:** Ricochet supports over twenty (20) VPS and Datacenter providers.
- **Active and Passive Countermeasures:** Client-side traffic production agent and server side data services.
- **Early-Warning-System capable:** Ricochet-created hosts contain an (optional) lightweight IDS (bro) to monitor non-Secure communications for third-party probing and introspection.
- **Not Attributable:** All resources are purchased using non-attributable funds over non-attributable communication mediums.

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Ricochet: Video Demonstration

Additional Capabilities

SHADOW GRID

DOWNRANGE TECHNOLOGIES

ShadowBox: Features

- All traffic is securely routed through the VPN
  - Your first hop after the router is our VPN, not your ISP
  - Router chooses the most intelligent path to the internet
  - Chosen path changes at a specified or random interval
- 5-Port Router (4-ports available)
  - PoE capable (for SIP phone, WAP, etc)
- Internally offers DHCP/DNS/Routing Services
- **No client software required**
- Commercially available hardware
  - Can be programmed in the field
  - Can be re-packaged

UBIQUITI NETWORKS

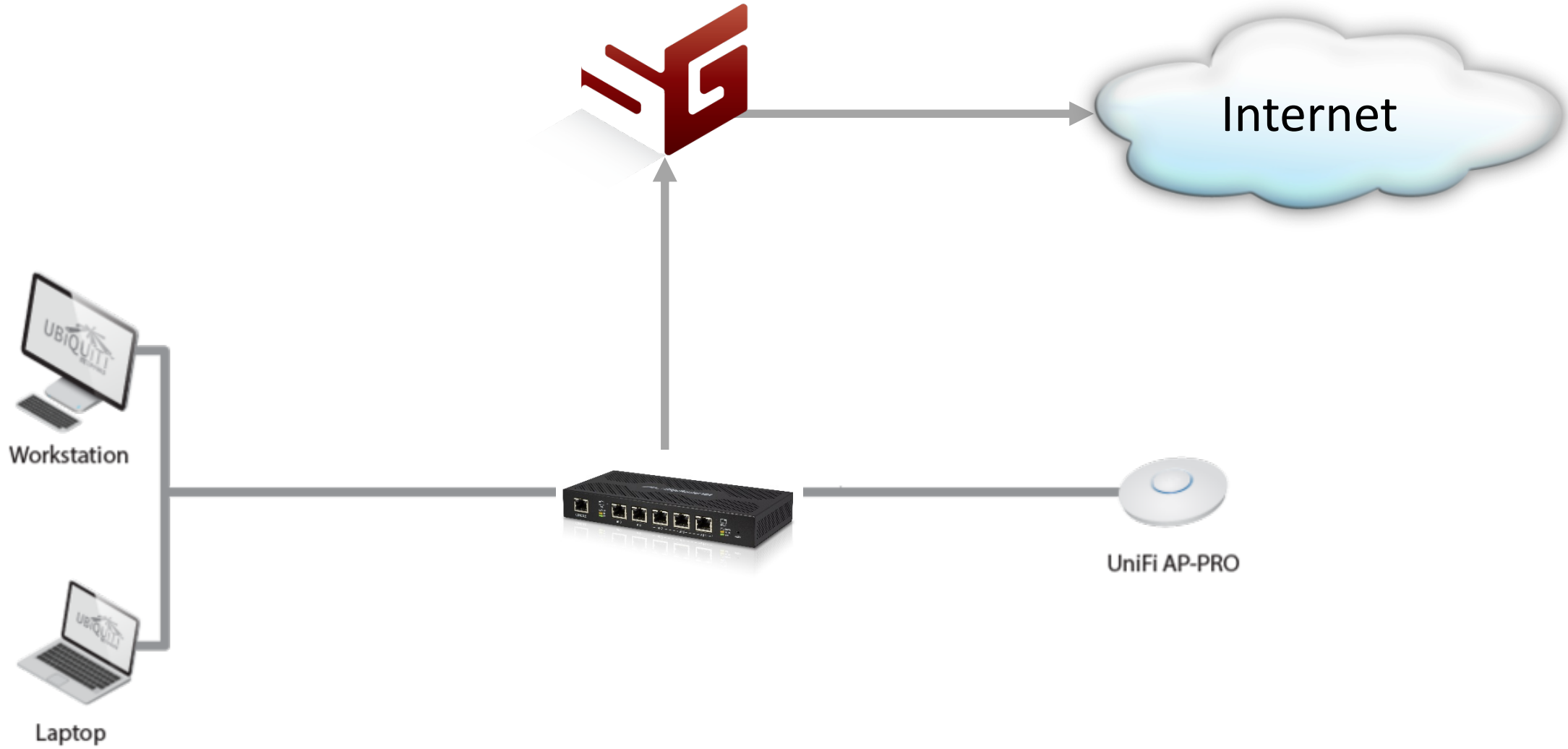
ShadowBox: Add-ons

- **SIP Phone**
  - Call Types Available:
    - Internal to Internal
    - External to Internal
    - Internal to External
  - Video Capable
  - Internal Calls are Secure
  - Location is Obfuscated
  - Fully featured Android platform
- **Wireless Access Point**
  - Enables Wireless Client Access
  - Encrypted and does not Broadcast

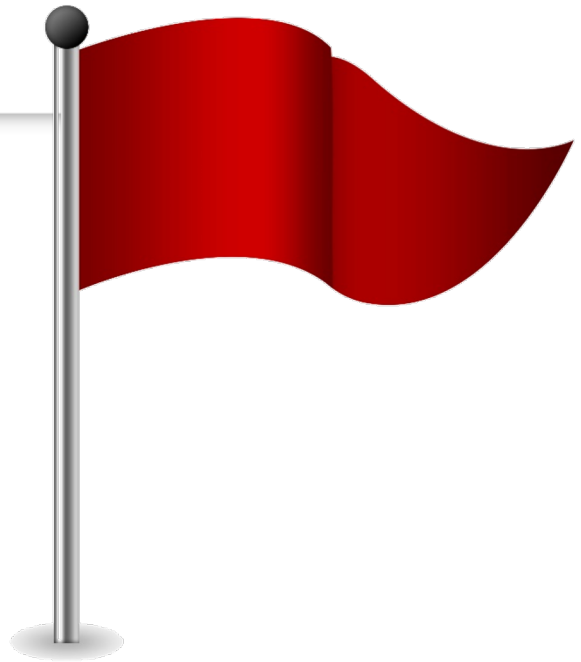
SIP Phones

Wifi Adapter

ShadowBox: Network Architecture



RedFlag



RedFlag is a general capability that enables Users to report periods of duress through active use or passive misuse. Every implementation is customer specific.

Implementation:

- **False VPN Authentication:** In the event a User is artificially motivated to log into the VPN, they can provide a duress password. The duress password will allow temporary access to the network, but will alert the user's leadership. Follow-on actions can be programmed IAW the operational scenario. Location data is collected.
- **SMS or Voice check-in:** A user calls or messages a pre-defined number on a set schedule. The user is able to report duress during the check-in. Failure to check-in will alert the user's leadership. Historic location data is collected.

SHADOW GRID

DOWNRANGE TECHNOLOGIES

LOKI

LOKI is an asset validation and verification system.

Users are assigned “Keys”, which are unique URLs assigned to a specific user, area, or topic of interest.

On demand, a User accesses the URL. The location, IP, Browser profile and DTG of the visit is logged and immediately sent to the User’s supervisor for validation/verification via SMS and/or email.

The User is instantaneously redirected to an innocuous webpage.

The Key can be programmed to be disabled for a set period of time after initial use.

LOKI is in production (1-year) with two clients.

Mr. Fusion

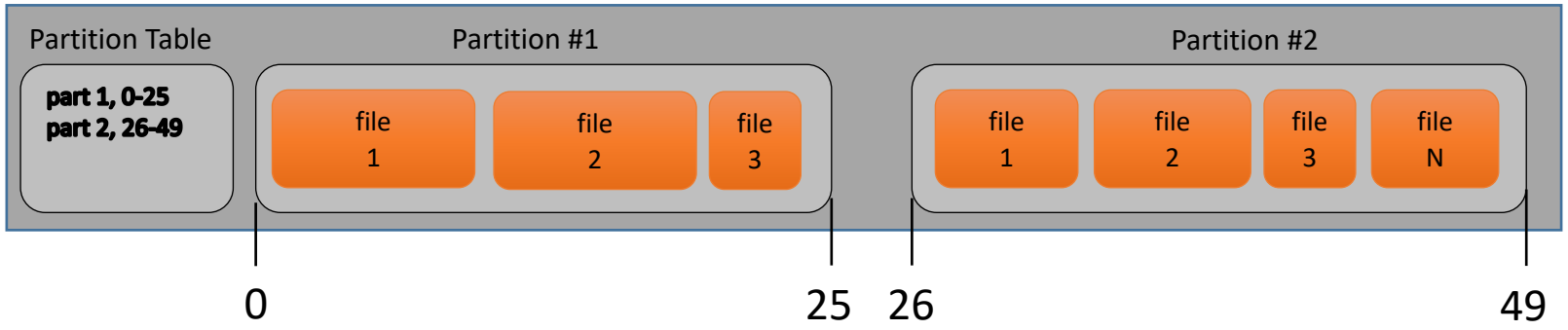
Mr. Fusion is a proof of concept hidden file system capability.

Using **Mr. Fusion**, an entire file system can be hidden within an existing binary file.

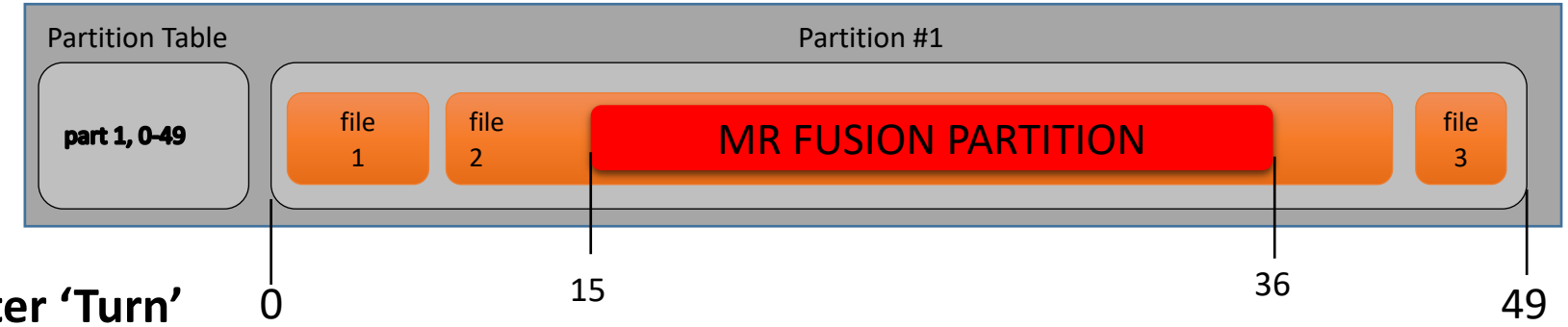
Currently in the proof of concept stage, it is running in Windows, with consideration for Mac taken during development.

file1 = Movie Player (VLC)
file2 = A Charlie Brown's Christmas
file3 = Mr. Fusion executable

Standard Partition Layout



Mr. Fusion Layout



After 'Turn'

Mr. Fusion: Employment Implementations

We can trigger the "Turn" multiple ways; each depends on the customer's operational scenarios:

- ***Method 1:*** Utilities are embedded on the 'Open' Partition.

- ***Method 2:*** Embedded in an existing Binary, such as VLC
  - Affects the binary's hash, which may trigger a "Second Look"

- ***Method 3:*** Code is embedded within the **Mr. Fusion** partition as shell-code. 0-day is discovered in publicly accessible version of open-source software. When that software opens our partition file, we exploit the 0-day and execute our turn shell-code.
  - Binary's hash is not affected.

SHADOW GRID

DOWNRANGE TECHNOLOGIES

Bottom Line

- We have past performance
  - Our architecture is sound
  - Zero Intrusions
- We are really serious about the stuff you don't see
  - Backup
  - Redundancy
  - SLA/Uptime
  - Monitoring

Questions?

joe@downrange.tech