# What breaks when you apply DNS at the root of network trust

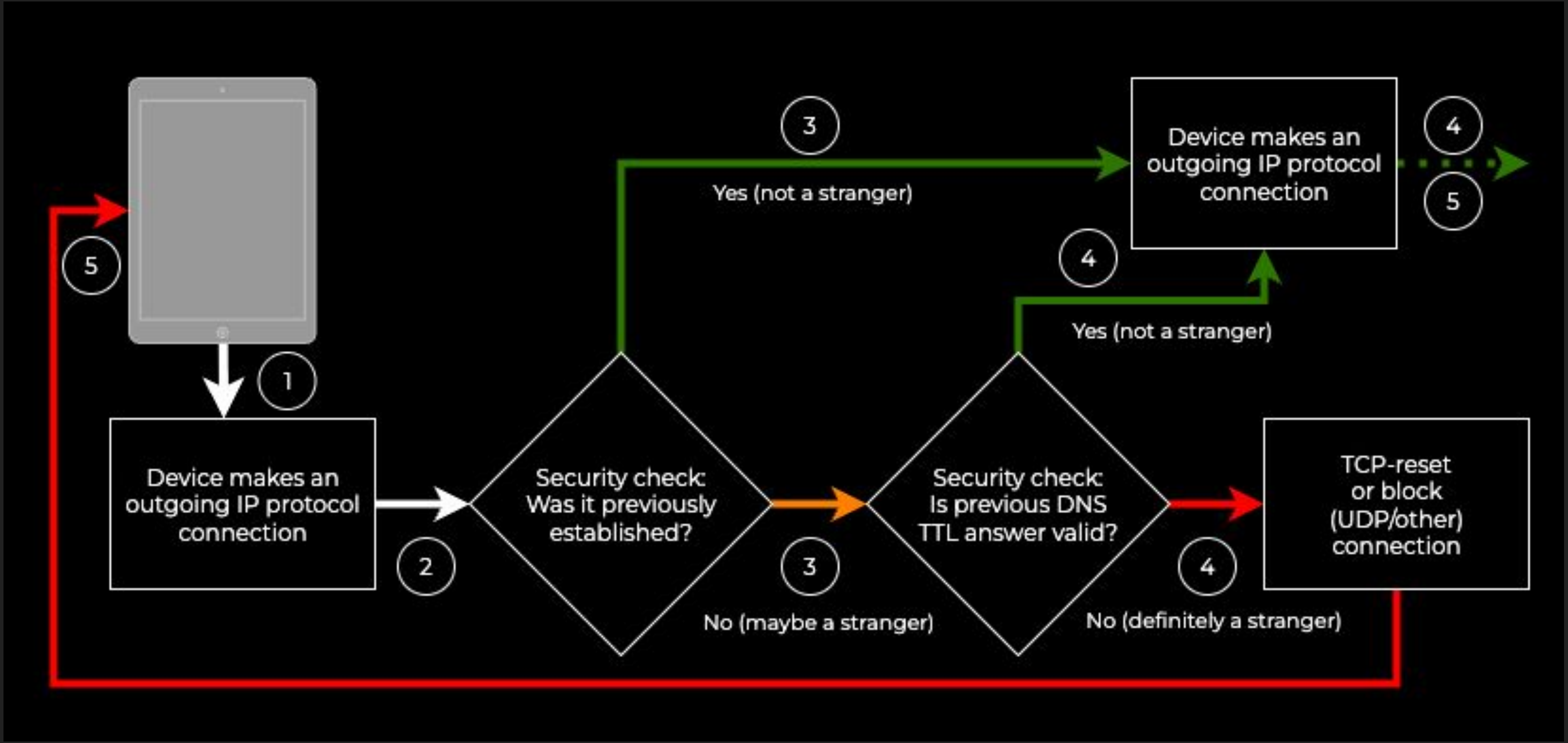
(lots, but it can all be fixed)

By David Redekop, ADAMnetworks

# What is DTTS/ZTDNS?

- Quick review:
- DTTS → Don’t Talk To Strangers (every IP not resolved by DNS is a stranger) at layer 3 security gateway
- ZTDNS → Microsoft naming convention for this application at Windows endpoint
- Essentially: DNS as the root of trust for egress traffic
- Expectation is that every destination IP will be resolved by DNS first
  - DNS to be answered by a Protective Resolver is assumed but technically optional
- Can run on a layer ⅔ gateway for static endpoints
- Can run on endpoint (for multi-homed or roaming devices)

# How Don’t Talk to Strangers | ZTDNS works



1
Device makes an outgoing IP protocol connection
2
Security check: Was it previously established?
3
Yes (not a stranger)
3
No (maybe a stranger)
Security check: Is previous DNS TTL answer valid?
4
Yes (not a stranger)
4
No (definitely a stranger)
Device makes an outgoing IP protocol connection
4
5
TCP-reset or block (UDP/other) connection
5

# Additional details on how DTTS/ZTDNS works

- For this to work, endpoints are enforced to use designated DNS *only
    - If browser attempts DoH by any other means, it will lose all DNS and therefore its connectivity
    - This is good for network defenders, thwarts typical threat actor network security circumvention
    - This is bad for end users and apps that want to do their own thing
- Once source → destination is allowed, any IP protocol, any port is allowed
    - Unless overridden by explicit block list by protocol and/or port and/or destination
- Time-bound (DTTS): if TTL is unreasonably long, the DNS answer may be modified and shortened
- Outgoing connection allow-rules are ephemeral; exist only for DNS TTL period, thereafter allow-rule is destroyed

# What all does this approach break?

- **LEGACY** Any direct-by-IP connection, typically legacy processes that ignore network-designated DNS server usage
  - Legacy application with hard-coded IPs in endpoint configurations
  - Hard-coded DNS servers (sometimes, administrators, sometimes manufacturer such as Chromecast)
  - Hard-coded NTP servers (this one is of particular concern because of UDP amplification attack surface)
  - Apps designed to circumvent protective DNS filtering (e.g. Telegram, Retail VPNs, P2P, Psiphon)
- **VOIP/P2P** Any modern application that includes connections to IP addresses that were not discovered via DNS - breaks some, but not all functionality
  - Video and voice apps using hard-coded IPs for SIP, RTP, STUN, TURN, etc
  - Online collaboration tools like zoom, Teams, Google Meet
  - P2P apps such as torrent clients cannot connect to peers
- **TIME BOUND** expiry - any application that uses DNS results beyond the TTL
  - Legacy Internet Explorer browser
  - Outlook caches IMAP beyond TTL

# The way to resolve and next steps

- Methods exist already to exempt trusted **prefixes + protocols + port** specifications to work, e.g. Google Meet uses:

```
{"destinations":["142.250.82.0/24","74.125.250.0/24","2001:4860:4864:5::0/64","2001:4860:4864:6::/64"],"ranges":[{"protocols":["udp"],"dst":{"start":19302,"end":19309}},{"protocols":["tcp"],"dst":{"start":443,"end":443}},{"protocols":["udp"],"dst":{"start":3478,"end":3478}}]}
{"destinations":["74.125.247.128"],"ranges":[{"protocols":["udp","tcp"],"dst":{"start":3478,"end":3478}}]}
{"destinations":["74.125.138.95"],"ranges":[{"protocols":["udp"],"dst":{"start":443,"end":443}}]}
```

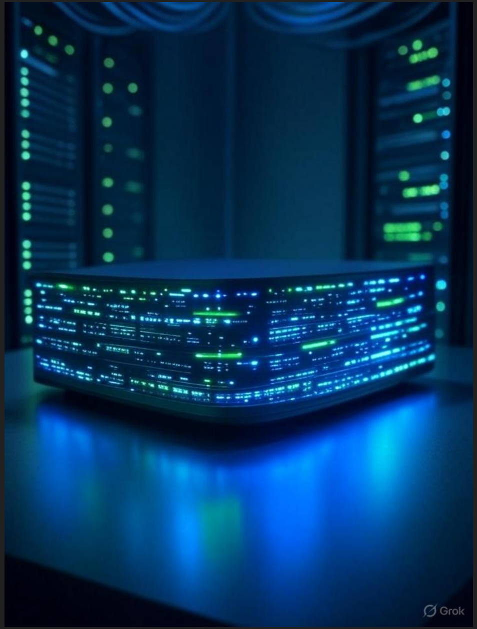
- RFC draft with co-authors Tommy Jensen, John Todd, David Redekop
- Call to app development to avoid DNSless connection attempts, use new rfc standard when adopted

# Other thoughts that make DTTS/ZTDNS worthwhile

- Encrypted Client Hello (ECH) has led to Proxy and DPI usage decline for good reasons (better privacy and security)
- DTTS/ZTDNS approach gives network edges the visibility they need for compliance and visibility

- Example #1 high value use case for DTTS: absolutely no reason any Active Directory domain controller needs to have internet access beyond NTP, Windows Update, combine with network seg
- Example #2 disrupt multi-stage attacks when C2 connection is made
- Example #3 solve IT/OT merger with a practical alternative to a unidirectional firewall

# Presentation Summary



- DTTS/ZTDNS is leak-proof DNS-based egress control
- It ensures all destination IPs are resolved by DNS
- Endpoints must use designated DNS servers to even have connectivity
- Some legacy apps will not function (until given explicit network permission)
- This approach improves network visibility
- Great for anti-circumvention and making C2 as impossible as you like