Archon CAMO: Covert Attribution Management and Orchestration

Mask assets’ identity, location, and destination server

Most identity-protection solutions create a cover identity for investigators or analysts. But adversaries can also identify assets by tracing their connections to government internet points of presence (PoPs). The problem is that the PoP is a fixed target.

Solution: Archon CAMO, for anonymization and misattribution

Archon CAMO is designed to prevent adversaries from associating mobile users with Commercial Solutions for Classified (CSfC) enclaves and other government servers. Archon CAMO obfuscates both the user device and the destination server in two ways:

- Makes IPsec VPN traffic look like another type of traffic, such as a YouTube video or IP camera stream.
- Routing traffic through a multi-hop path that’s created exclusively for the current session. For each session, Archon CAMO randomly selects servers from hundreds of private and popular commercial services around the world. (We can exclude specific countries or regions.) The options include major hosting providers that don’t attract attention, like Amazon Web Services (AWS) and VPN providers like NordVPN. At each hop, a VPN server is spun up just for the duration of the session. We will exclude countries or regions at your request.

With Archon CAMO, the government server in no longer a fixed target because it appears to move constantly.

How it works: “hiding in plain sight”

Set up

Install Archon CAMO software on the user’s device: desktop, laptop, tablet, phone, or thin or zero client. Tell us any countries or regions through which you don’t want traffic to travel. Otherwise, Archon CAMO randomly selects servers for each individual session from hundreds of private and popular commercial services around the world. These include major hosting providers that don’t attract attention, like Amazon Web Services (ASS) and VPN providers like NordVPN. We acquire the services anonymously so that they can’t be linked either to your organization or ours.

1. **The operator connects to the local Wi-Fi network.** The connection is routed through the Archon SideArm integrated retransmission device as requested by CSfC MA CPA.

2. **Archon CAMO software dynamically spins up and links temporary servers and commercial services to be used only for this session.** The inner VPN tunnel—from the end device to first server—is IPsec, as required by the CSfC Program (figure 1).
3. The file arrives at the first server, which Archon CAMO created exclusively for this session. Adversaries monitoring traffic entering the server cannot identify the originating device. Here, Archon CAMO adds an outer tunnel that makes the message look like common internet traffic, such as VPN, banking transaction, YouTube video stream, security camera feed, etc. The twice-encrypted traffic is forwarded to the next randomly selected server.

4. The file arrives at the second server—spun up on a private cloud service or commercial VPN service, commercial services to be used only for this session. The second server adds another encryption layer. The traffic exists looking like any other VPN traffic.

5. The file arrives at the destination, where it’s decrypted. An observer monitoring the user’s endpoint can see only the encrypted connection to the first server. The ultimate destination is hidden beneath multiple layers of encryption and obfuscation. An observer monitoring the government internet PoP can see only the encrypted traffic from a VPN server that’s not associated with the user device.

An example of a multi-hop path is from Tehran to AWS in Frankfurt, to Google Cloud in Los Angeles, to a USG location.

6. When the user disconnects, servers are wiped and terminated. Burned. No browser log are maintained—it’s as if the servers never existed. If the mission requires monitoring assets’ network activity without attribution, we can adapt Archon CAMO to comply.

The Archon CAMO user experience is the same as it is with an ordinary VPN connection. The only difference is a slight delay as Archon CAMO creates a multi-point connection (multiple servers and network segments) for the session. The result is a secure connection from anywhere—without attribution.

After

When the user disconnects, servers are wiped and terminated (burned). No browser logs are maintained: it’s as if the servers never existed. If the mission requires monitoring assets’ network activity—securely and without attribution, we can adapt Archon CAMO to comply.

Users do not know the server to which they connect—not even the country—giving them plausible deniability if someone later reports that the user accessed a website from a server in, say, Frankfurt.

The Archon CAMO difference

- **Asset identity protection.** Masks the fact that users are connecting via IPsec—a tip-off to adversaries that the user could be a high-value target.
- **Mission protection.** Obfuscated traffic makes it more difficult for adversaries to identify CSfC enclaves.
- **Server identity protection.** Masks the destination with multi-hop chains that include non-attention-getting commercial infrastructure and VPN providers.
- **Plausible deniability.** Private, one-time servers leave no trace.
- **Does not change user experience.** Just turn on the device and go. Archon is built into the Archon platform and integrated with CSfC-based architectures.