Cisco Advanced Phishing Protection: Implementation Process (On-Premises)

Published: June 22, 2018

Deploying Cisco Advanced Phishing Protection

Deploying Cisco Advanced Phishing Protection is a straightforward, well-defined process. The process has been refined based on years of experience supporting large organizations with their email security initiatives. Three primary project elements include: 1) Cisco Email Security Gateway 2) On-premises Cisco Advanced Phishing Protection Sensors and 3) Cisco Advanced Phishing Protection

These goals will be achieved:

- Understand the Messaging Architecture
- Deployment of Cisco Advanced Phishing Protection Sensors
- Confirmation of Message Traffic
- Verification of Accurate Message Scoring
- One Cisco Advanced Phishing Protection Policy in enforcement mode

Additional discrete steps are detailed.

Primary Project Tasks

The primary On boarding tasks consist of:

- Configure Cisco Email Security appliance for Dual Delivery of all messages to Cisco Advanced Phishing Protection Sensor. Enabling full visibility to the organization's inbound mail stream.
- Deployment of On-premises Cisco Advanced Phishing Protection Sensor. Providing the Cisco Advanced Phishing Protection Email Trust platform with the required message details (i.e. Authentication headers).

- Tune Policy & Data Model. Tuning to accurately identify your organizations valid messages. Adjusting policies to effectively identify malicious messages i.e. BEC.
- Enable Policy Enforcement.
- Enforcing policy to block malicious messages i.e. Friendly name spoofs.