Cisco ISE and 802.1x Deployment
Statement of Work

EXECUTIVE SUMMARY

FireOwls is an All-CCIE Certified team and a Cisco Partner. FireOwls will install a Cisco ISE server and configure 802.1x on 50 production access switches.

STATEMENT OF WORK

- Assumptions
  - This scope will be based on an assumption of 50 Production User Access switches
  - Each Client switch is compliant with ISE and no hardware or code upgrades are required
  - Fireowls' Engineer will have direct VPN access, access into the ISE servers, and to the switches as well
  - ISE Wireless authentication efforts will be focused on Client's primary Corp-Wireless SSID
- Exclusions
  - Meraki Guest-SSID and user authentication is not in this scope and currently serviced by the Meraki guest portal
  - VPN Radius authentication is not in this scope and currently serviced via AD/LDAP
- Define High Level Design
  - Discuss administration policies
  - Discuss client authentication policies (username/certificate)
  - Discuss AD groups and roles (employees, vendors, contractors, guests, etc)
- Critical Access Control List
  - Discuss 802.1x Authentication policy protocols
  - Discuss authentication methodologies & certificate requirements
  - Create deployment of 802.1x supplicant/certificate to endpoint devices
- Assumption – Client will be responsible for
  - Desktop/Laptop/Windows/MAC/Printers/VoIP Phones/any other User or IoT device connecting to the wired network
  - Client will be responsible for rolling this out
  - Discuss 1x on Cisco IP Phone
  - Discuss Client Trust – Network switches, Model, and Code version
  - Provide ISE implementation design
- Install ISE servers configured for HA - DeployVM/Upgrade/ConfigureHA
  - Deploy (2) ISE servers in Primary DC in HA mode
  - Configure mode - Admin Node, Monitor Node, and Policy Service Node (PSN),
  - Deploy optional redundant set of (2) servers in a Secondary DC
  - Configure mode - Admin Node, Monitor Node, and Policy Service Node (PSN)
  - Integrate with Active Directory
- Configure ISE management access
  - Setup administration access and policies
  - Install ISE licenses
  - Install certificates, AD integration, Email integration, Configure Alerts, Configure Backups. Assumption: Customer has CA server and access
- Configuring ISE Policies
  - Configure Policy Sets
  - Create up to 5 Policy Sets

For more info, contact:
FireOwls Corporation – All-CCIE Team
16755 Von Karman Ave, #200, Irvine, CA 92602
info@fireowls.com | 1(833) Fire-Owl

  - Configure Authentication Policies
  - Create up to 5 Authentication policies
  - Create MAB list and policies
- Integrating and Configuring Wired Access Devices (Template for 1 switch)
  - Identify list of all Wired Network Switch, Model, and Version
  - Create configuration template for the switches
  - Create MOP for adding network switch into ISE
  - Deploy configuration to network switch
- Deployment Phase
  - (Crawl) Designate a Test Lab switch and configure ISE for network access and .1x authentication on the ports
    - Implement/Test MAB authentication/policies
    - Implement/Test Device .1x authentication/policies
    - Test ISE Failure and HA redundancy
    - Test ISE issues and support methods
  - (Walk) Designate the least critical user access switch
    - Implement/Test MAB authentication/policies
    - Implement/Test Device .1x authentication/policies
  - (Rollout) Implementing on a site by site basis
- Documentation and Handoff
  - As built documentation of ISE design, configuration, and support procedure
  - Handoff Meeting with Client team
  - Provide FireOwls best practice and optimization report for ISE/Security/Network
- Configurating Wireless ISE authentication for CorpSSID and policy testing
  - Design & Configure ISE for wireless auth
  - Define wireless auth method – Corp SSID, ad+certificates
  - Review meraki group policies, review ISE groups to map to Meraki Group Policy
  - Configure Meraki to point to ISE meraki group policy
  - Implementing Test SSID & Test Authentication
  - Implementing Corp SSID & Test Authentication

Responsibilities and Assumptions:

- Client will be responsible for procurement of hardware and software licensing for this project.
- Client will be responsible for all cabling and physical installation
- Client will be responsible for any necessary base IP addressing needed for remote connectivity to equipment.
- Client will provide with direct VPN access (non-Webex or screen-sharing) for remote access to equipment.
- FireOwls must review all BOMs prior to contract acceptance.
- Out of Scope: Any work not explicitly detailed in this SOW is out of scope unless there is an appropriate Change Order.
- Client will provide a project contact with decision-making authority to support the scope of services described in this SOW and ensure the proper personnel are scheduled to review each completed Service or Deliverable upon notification of completion by Client.
- Client will provide the necessary hardware, software, and tools required for the successful completion of the project.

For more info, contact:
FireOwls Corporation – All-CCIE Team
16755 Von Karman Ave, #200, Irvine, CA 92602
info@fireowls.com | 1(833) Fire-Owl

- All work will be performed during normal business hours, Monday through Friday, 8am to 5pm, except holidays unless otherwise agreed upon.
- Provider is not liable for any data loss.
- Work to be completed within 120 days from when the Provider receives Customer PO.

For more info, contact:
FireOwls Corporation – All-CCIE Team
16755 Von Karman Ave, #200, Irvine, CA 92602
info@fireowls.com | 1(833) Fire-Owl