Identity Services Engine (ISE)

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

CCIE Security

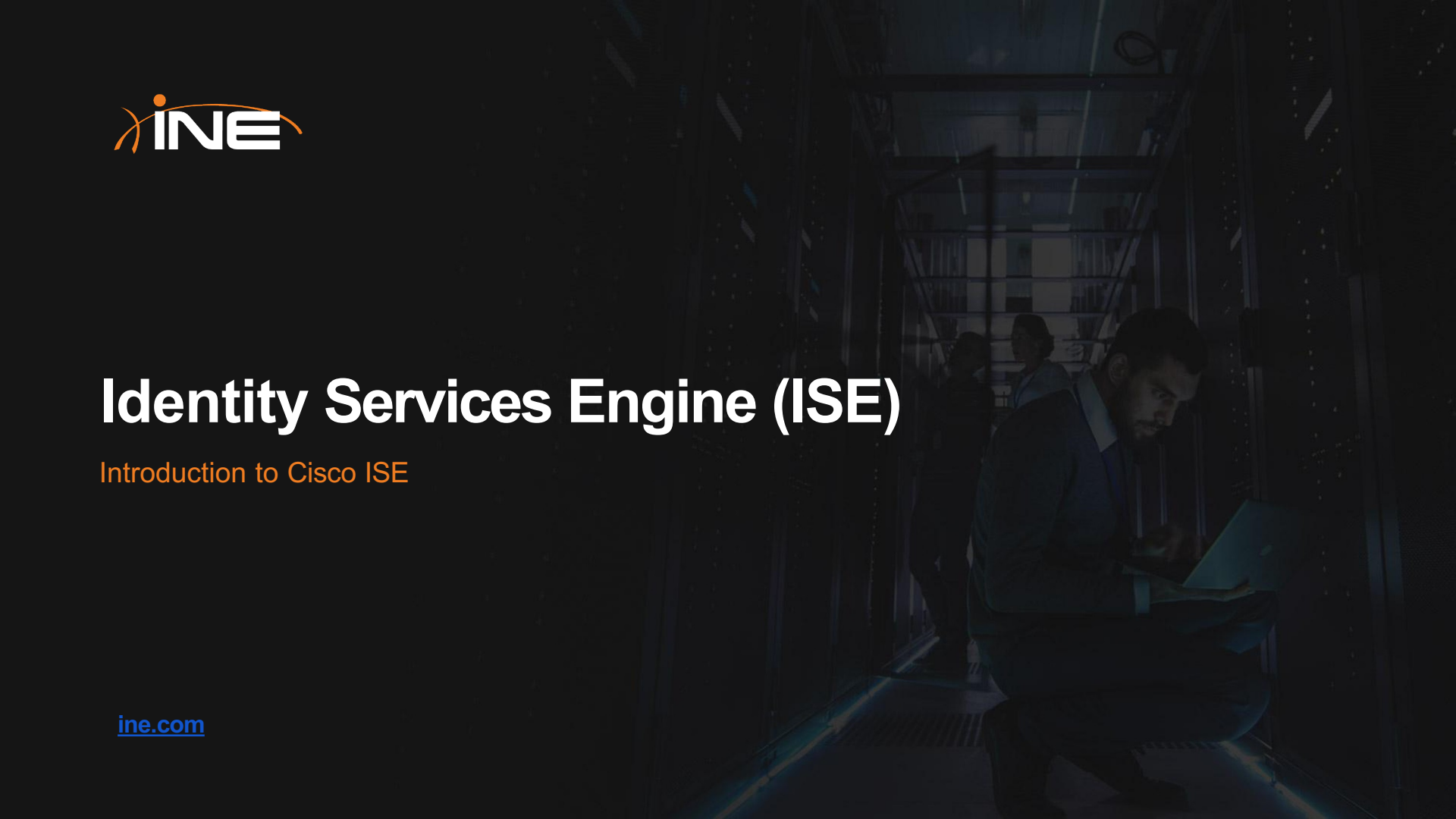
Course Prerequisites

- General security concepts
- Cryptography basics

Course Overview

+ Module 1	Introduction to Cisco ISE
+ Module 2	The Policies
+ Module 3	Integrating with Active Directory
+ Modules 4 - 6	AAA & Device Administration
+ Modules 7 - 10	Profiling & related topics
+ Modules 10 - 14	802.1x
+ Module 15	Guest Services
+ Modules 16 - 17	Scalability & redundancy


INE



Identity Services Engine (ISE)

Introduction to Cisco ISE

ine.com

Module Overview

+ System overview

Identity Services Engine (ISE) Overview

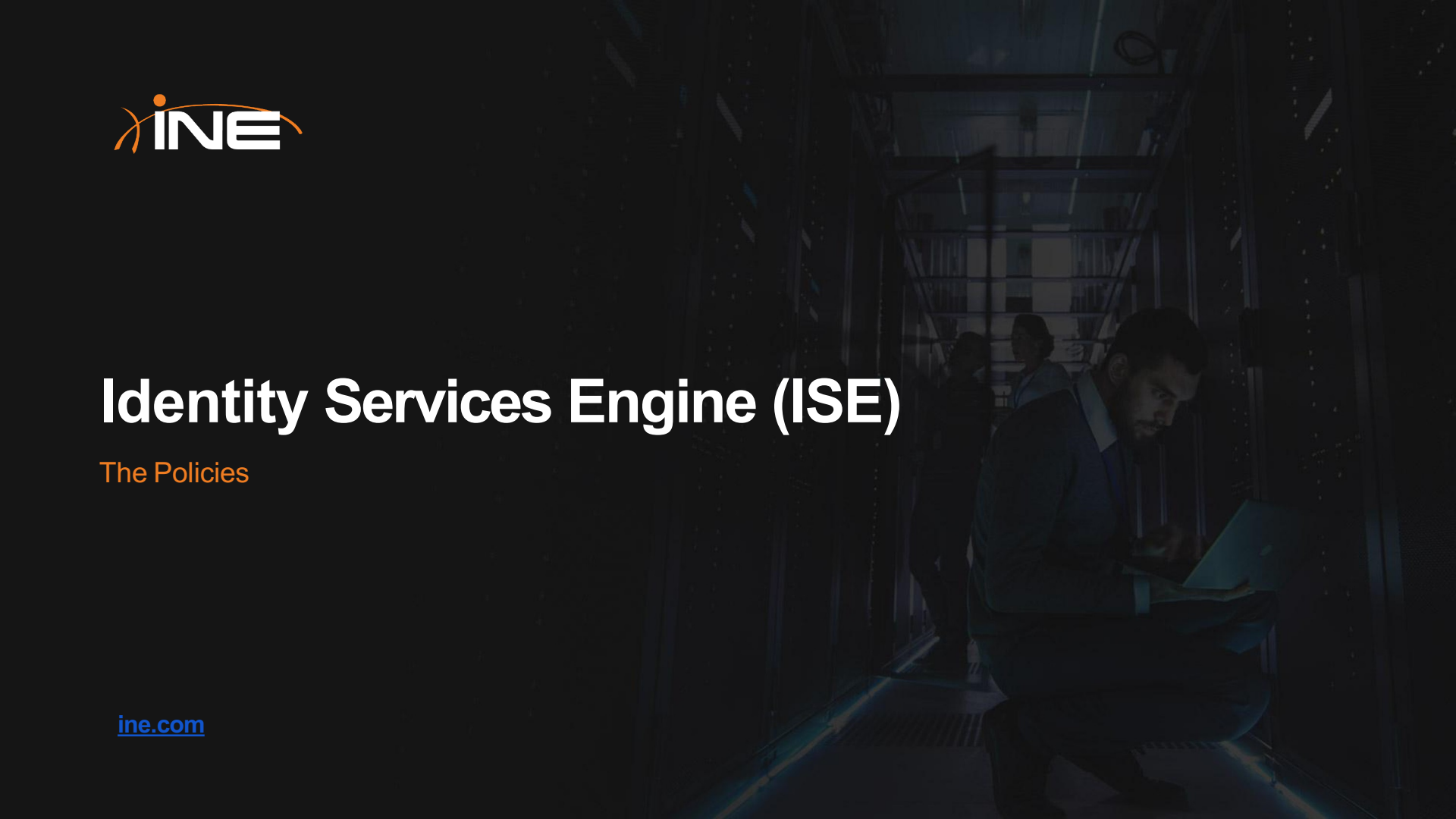
- Next-generation Identity Management system
  - Similar to ACS but much more powerful
    - Context-based access
    - Network visibility
    - Centralized policy enforcement
    - Guest & endpoint management
- Available as a physical or virtual appliance
  - 1 RU 3600-series Secure Network Server (SNS)
  - VMware ESXi/Red Hat KVM/Microsoft Hyper-V software image

Identity Services Engine (ISE) Overview

- Main features (2.4)
  - Centralized Management & AAA
    - Flexible rule-based policies
    - RADIUS & TACACS+
    - External Databases
  - Profiling
  - BYOD
  - Guest Services
  - Posture Assessment
  - TrustSec
  - Platform Exchange Grid (pxGrid) Integration
  - Internal Certificate Authority (CA)

ISE Documentation

- Cisco Documentation -> Security -> Identity Services Engine
  - https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html
  - See "Documentation Roadmaps"



Identity Services Engine (ISE)

The Policies

ine.com

Module Overview

- Policies overview
- Policy Elements
- Policy Sets
- Authentication & Authorization Policies

Policies Overview

- ISE services are controlled through Policies
  - Authentication, Authorization, Posture, Profiler & more
  - Policies consist of rules that are generally processed top-down*
    - Default Rule (if exists) acts as a catch-all

- Policies and/or Policy Rules are made of two types of Policy Elements:
  - Conditions
    - Matching criteria
  - Results
    - Action(s)

Policy Elements

- ISE offers a large set of predefined Policy Elements
  - **Policy -> Policy Elements**
    - Vary depending on the policy type
  - The structure of most elements is well-defined through Dictionaries
    - **Policy -> Policy Elements -> Dictionaries**
    - Catalogs of objects ISE understands, their attributes & allowed values
      - System vs User
  - Some elements come from external sources
    - E.g. Posture Updates
  - Useful Policy Conditions can be stored in the Library (Condition Studio)
    - **Policy -> Policy Elements -> Conditions -> Library Conditions**

Policy Sets

- Logical groupings of Authentication & Authorization policies
  - Default in ISE 2.3+
  - Simplify policy structure
    - Separate sets for wired/wireless/guest/etc. access
  - Processing
    - Policy-set-level rules are evaluated first (top-down) until a match
      - The Default Set is checked last
    - For the set to be processed, Allowed Protocols must be met
      - Rules within the processed set follow top-down first-match evaluation
  - Available for network access & device administration

Authentication (AuthC) Policy

- Establishes an Identity
- Matched Rule Processing
  - Identity Store Selection
    - E.g. Identity Source Sequence
  - Identity Validation
    - PASS
    - FAIL

Authentication Policy

- Successful Authentication (PASS) leads to Authorization
  - Failure Scenarios (FAIL)
    - Authentication failed
    - User not found
    - Process failed

- Failover Options
  - Reject
  - Drop
  - Continue

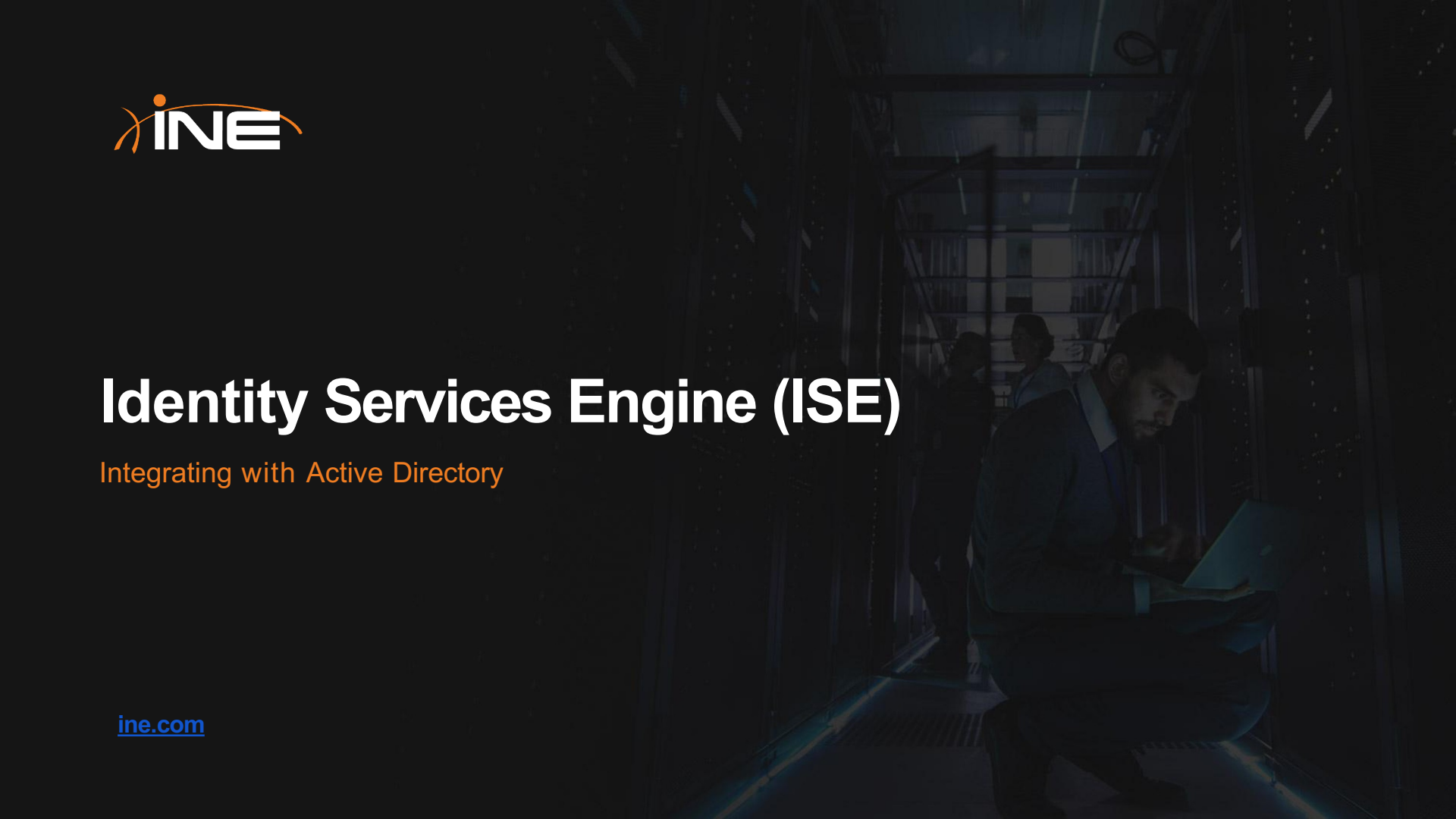
Authorization (AuthZ) Policy

- Determines access to the network/device
  - Authorization Policy Types
    - Standard
    - Exception
      - Local vs Global
  - Exception rules take precedence over Standard rules
    - Top-down, first-match
    - The "Multiple Matched" option is deprecated since 2.3

- A matching rule returns an Authorization Profile
  - Set of permissions to be enforced on the session

Authorization Policy

- Policy Enforcement Methods
  - Downloadable ACL (dACL)
  - VLAN Segmentation
  - Web Authentication
    - Central or Local
  - Security Group Tag (SGT)
  - Any other RADIUS AV Pairs (including VSAs)
    - MACsec Policy, Reauthentication, Smartport Macros & more



Identity Services Engine (ISE)

Integrating with Active Directory

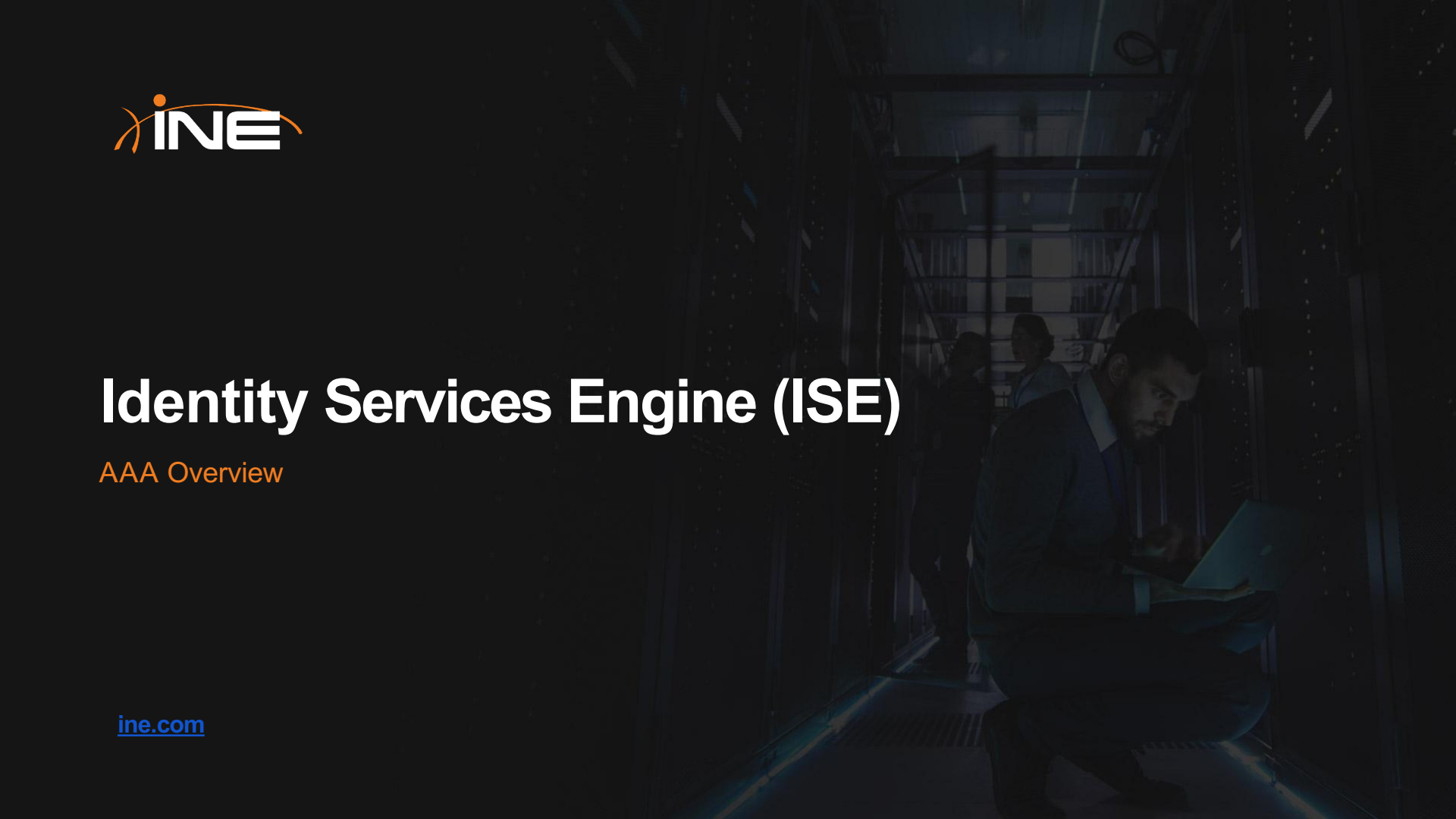
ine.com

Module Overview

+ Prerequisites
+ Example

AD Integration

- Prerequisites
  - ISE Super/System User account
  - Time synchronization (NTP)
  - Port openings
    - DNS
    - MS-RPC
    - Kerberos
    - LDAP & LDAP (GC)
    - NTP
    - IPC



Identity Services Engine (ISE)

AAA Overview

ine.com

Module Overview

- Authentication, Authorization and Accounting (AAA)
- AAA Security Protocols

AAA Overview

- AAA is a framework for configuring three different security functions
  - Authentication is a process of providing and verifying an identity
    - May involve multiple factors/elements
      - Something you know (e.g. password)
      - Something you have (e.g. token)
      - Something you are (e.g. biometrics)
  - Authorization enforces a policy
    - Privileges, access level/scope etc.
  - Accounting is a process of tracking and recording activities
    - What and when

AAA Security Protocols

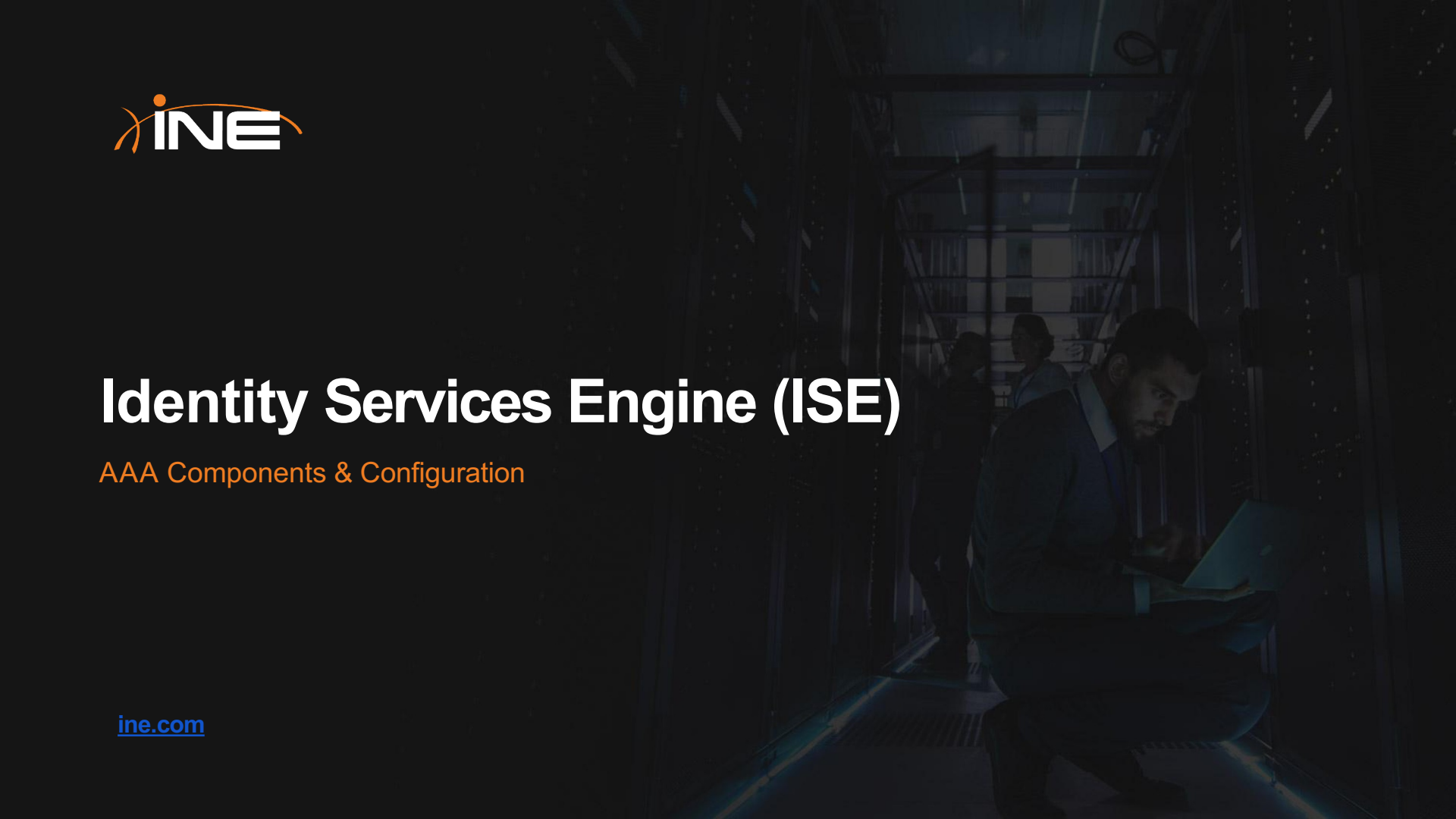
- AAA could be deployed directly on Network Access Devices (NADs)
  - Not scalable, limited AAA functionality
  - Centralized AAA is only possible with RADIUS or TACACS+
    - A client device (NAD) does AAA with a RADIUS/TACACS+ server

- RADIUS vs TACACS+
  - Primary Purpose : network access (R) <-> device administration (T)
  - Transport : UDP 1812/1813 or 1645/1646 (R) <-> TCP 49 (T)
  - Security : user password (R) <-> entire payload (T) encryption
  - Protocol Design : authC + authZ (R) <-> separate AAA functions (T)
  - Standardization : industry standard (R) <-> Cisco proprietary (T)
  - EAP Support : yes (R) <-> no (T)

AAA Security Protocols

- RADIUS & TACACS+ exchange the client-server info using Attributes
  - Each Attribute is designed to carry a certain type of info (Value is the data)
  - TACACS+ Attributes & Values (AVs) are both Strings defined by Cisco

- RADIUS Attributes
  - Supports 255 possible main numbered attributes (most IETF pre-defined)
  - Vendor Specific Attribute (VSA) allows vendors to carry proprietary data
    - VSA is IETF attribute 26 & consists of a Vendor Type, ID & Length
    - Cisco AV-Pair (Vendor ID 9, Type 1) is a well-known Cisco's VSA originally created to extend basic RADIUS functionality with some TACACS+ capabilities
      - *protocol:attribute=value*, e.g. shell:priv-level=15



Identity Services Engine (ISE)

AAA Components & Configuration

ine.com

Module Overview

- AAA configuration components

AAA Configuration Overview

- IOS AAA framework is by default disabled
  - Activate it with **aaa new-model**

- AAA functions are controlled with Method Lists
  - Default
  - Custom (user-defined)
    - Must be activated
    - Overrides a corresponding Default List

aaa [authentication | authorization | accounting] *service* **[***name* **| default]** *method*

AAA Configuration Overview

- AAA Method (database)
  - RADIUS
    - **radius-server**
  - TACACS+
    - **tacacs-server**

- Database configuration
  - ACS
  - ISE
  - LOCAL

Authentication (AuthC)

- A process of verifying an identity
  - Commonly authenticated services
    - IEEE 802.1x (**dot1x**)
    - Enable password (**enable**)
    - Login (**login**)
      - To activate a custom list use **login authentication** under a line

- Fallback Authentication
  - More than one method can be defined (backup)
    - **aaa authentication login default group tacacs+ local**

Authorization (AuthZ)

- A process of enforcing a policy
  - Commonly authorized services
    - Network (**network**)
    - EXEC/Shell (**exec**)
      - To activate a custom list use **authorization exec**
    - Commands (**command**)
      - To activate a custom list use **authorization commands**
  - Console access is not authorized unless **aaa authorization console**

- Fallback Authorization works similar to Fallback Authentication

EXEC Authorization

- Controls access to the CLI Shell
  - Yes/No
  - Shell attributes
    - Privilege Level (**username privilege**)
    - CLI View (**username view**)
    - Autocommand (**username autocommand**)
- Works with RADIUS, TACACS+ and Local database

Command Authorization

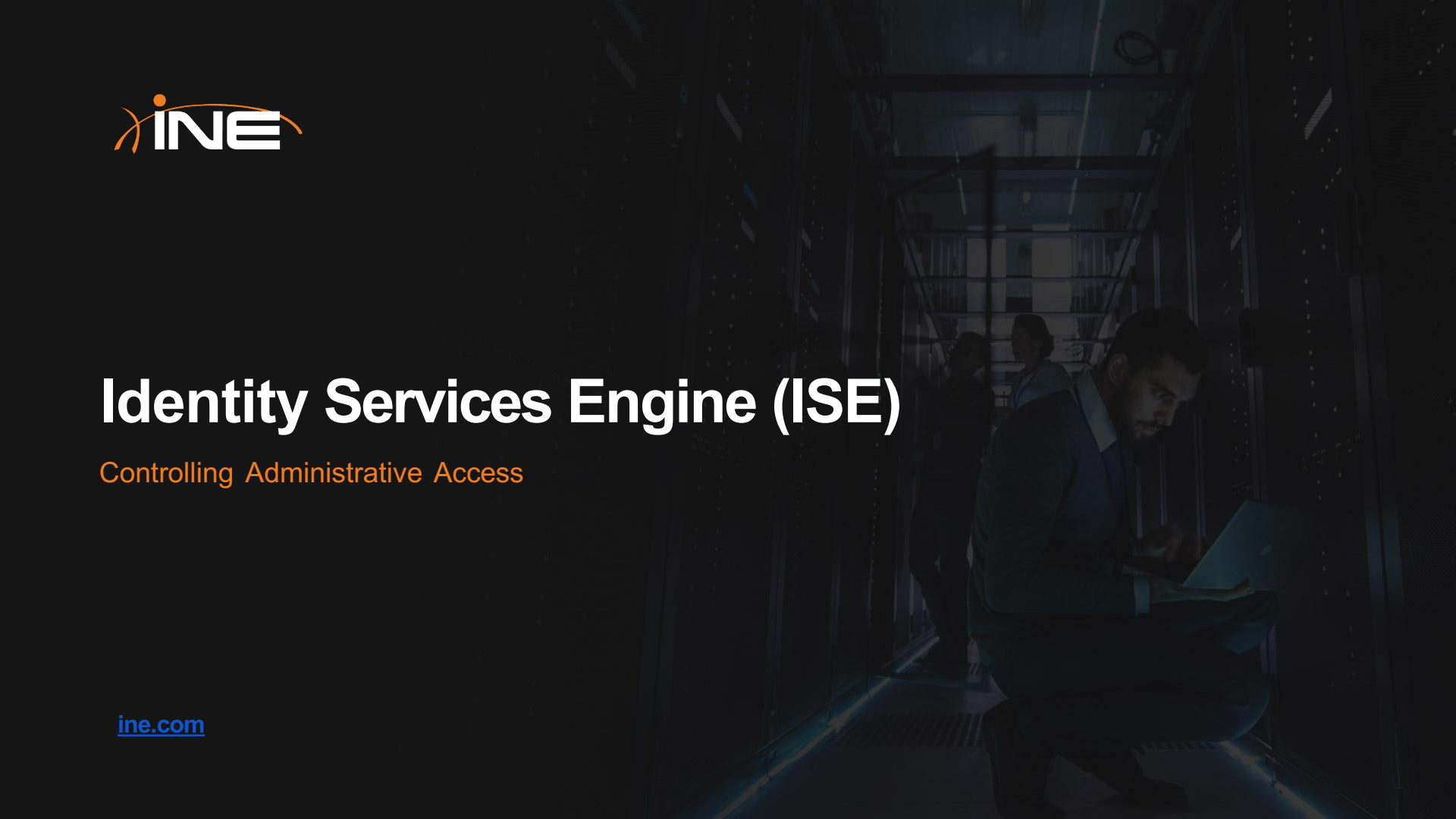
- Controls access to individual CLI commands
  - Yes/No
  - Only affects access to commands at a configured level
    - E.g. **aaa authorization commands 15 default group tacacs+**
  - Consider **aaa authorization config-commands**

- Works with TACACS+
  - Decouples authorization from authentication

Accounting

- A process of logging session activities
  - Common applications
    - EXEC/Shell (**exec**)
      - **start-stop** vs **stop-only**
      - To activate a custom list use **accounting exec**
    - Commands (**commands**)
      - To activate a custom list use **accounting commands**

- Works with RADIUS or TACACS+



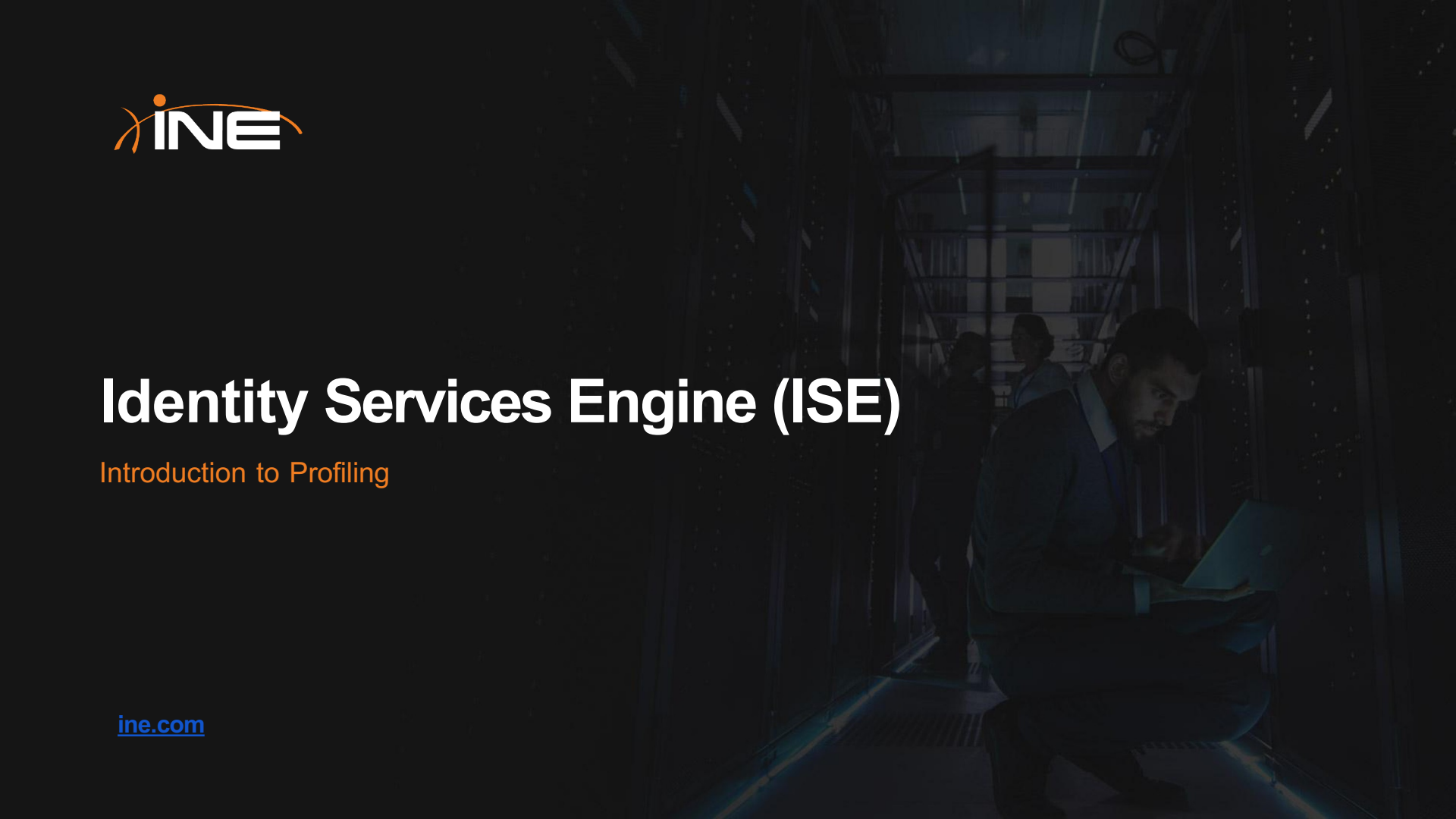
Identity Services Engine (ISE)

Controlling Administrative Access

ine.com

Module Overview

+ Configuration example



Identity Services Engine (ISE)

Introduction to Profiling

ine.com

Module Overview

+ Profiling overview

Profiling Overview

- ISE uses Profiling for endpoint detection & classification
  - Relies on Probes & Policies
    - Profiling Probes analyze received network traffic
      - Collect endpoint attributes
    - Profiling Policies
      - Analyze attributes to determine the endpoint's Profile
- Profiling information aids in building accurate Policies

The Process

- Profiling is ongoing & consists of several steps
  - Analysis of the received network traffic
    - RADIUS, SNMP, DHCP and more
  - Extraction of profiling data
    - Attributes
    - Addresses
      - MAC, IP or both
  - Endpoint database update
  - Evaluation of the attributes against Profiling Policies
    - Usually results in Profile assignment or update

Profiling Policies

- Profiling Policies are similar to IPS signatures
  - Consist of Rules
    - If *condition* then *action*
      - Actions : Increase Certainty Factor (CF), Network Scan, Exception
  - May be hierarchical

- Policy selection
  - Based on the highest total Certainty Factor (CF)
    - Rules with “Increase CF”
      - For the Child Policy to be selected its Parent must match as well
  - Ties are handled alphabetically

Profiling Policies

- Policy match aftermath
  - Profile assignment
    - If none Policy was matched, the endpoint gets profiled as “Unknown”
  - Identity Group assignment
    - Not very important since 1.2
      - May be useful for MAC address management (e.g. blacklisting)

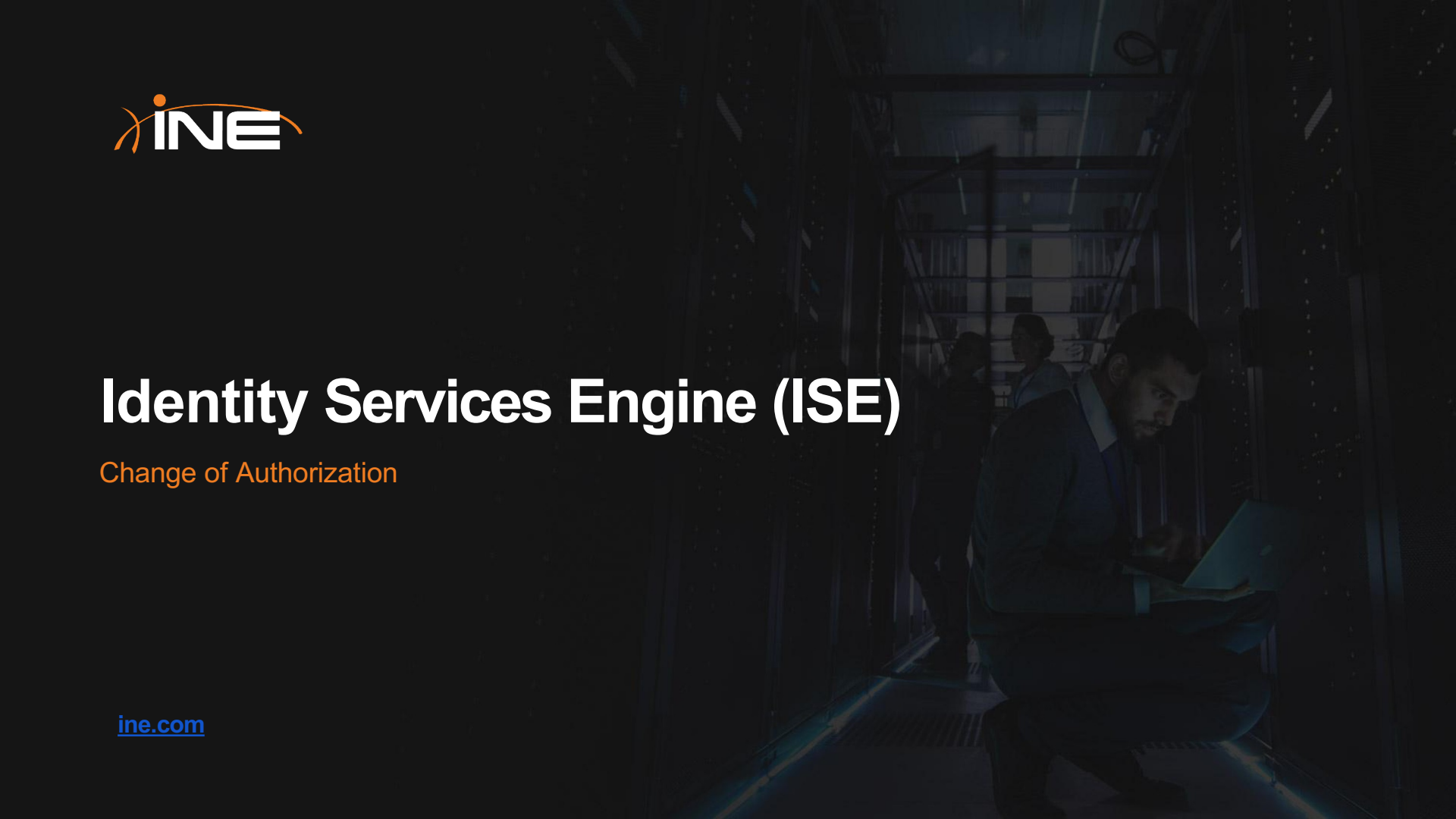
- Static Policy assignment disables Profiling for the endpoint
  - Manual
  - Exception action

Profiling Policies

- ISE comes with hundreds of Profiling Policies
  - New Policies can be downloaded through the Profiler Feed service
  - Custom Policies can be created
    - Tip : use high CF values

Logical Profiles

- A custom group of Profiling Policies
  - The Policies can be arbitrary
    - E.g. Cisco & non-Cisco IP Phones
  - Simplifies configuration of AuthZ Policies



Identity Services Engine (ISE)

Change of Authorization

ine.com

Module Overview

+ Feature overview
+ CoA & Profiling

Change of Authorization (CoA)

- Standards-based (RFC 3576) RADIUS improvement
  - Allows a RADIUS Server to send unsolicited messages to its clients (NADs)
  - Critical for Profiling, Posture, and more
    - E.g. new endpoint attributes may result in re-profiling & different AuthZ rule

- Configuration
  - Wired : **client** under **aaa server radius dynamic-author**
  - Wireless : **Support for CoA** under **Security -> RADIUS -> Authentication**

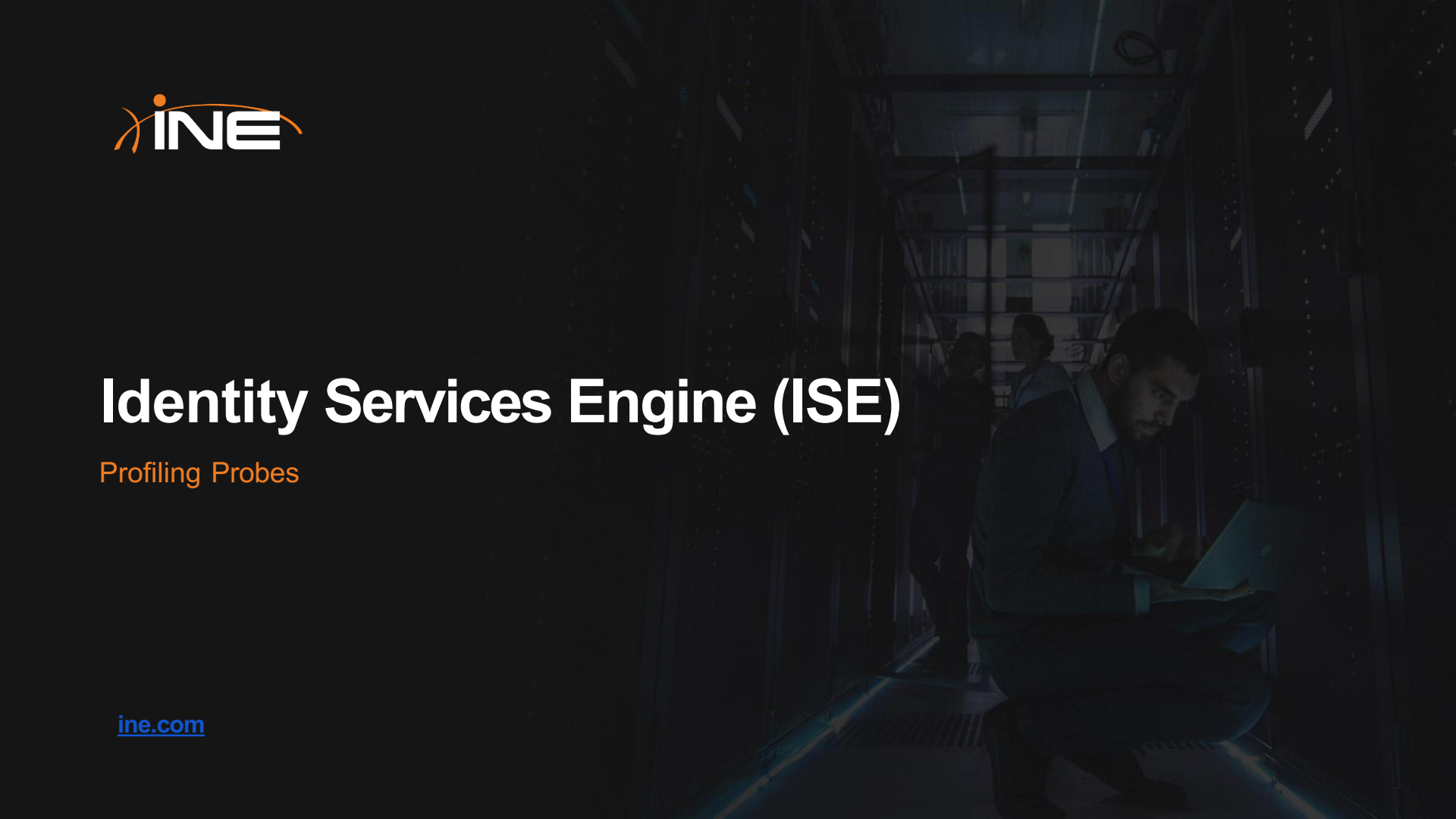
CoA & Profiling

- ISE Profiler issues CoA (if enabled) under certain events
  - Endpoint profiled for the first time
  - Endpoint deleted from the database, and more

- CoA Profiling settings
  - Global
    - Enable/disable CoA for Profiling
      - Off by default (“No CoA”)
  - Per-profile
    - Overrides the global CoA action in a given Policy
      - Requires CoA to be globally enabled

CoA & Profiling

- CoA Actions
  - Port Bounce
    - Simulates a link change (**shutdown**, **no shutdown**)
  - Reauth
    - New authentication with the same session ID
    - Also used instead of “Port Bounce” when 2+ MACs were detected on a port
- CoA can be disabled per Profiling Policy
  - No CoA
  - Exception action



Identity Services Engine (ISE)

Profiling Probes

ine.com

Module Overview

+ Feature overview
+ Probe details & configuration

Profiling Probes Overview

- Software collecting & analyzing network data for Profiling
  - Several Probes exist to collect different attributes
    - RADIUS, SNMP, HTTP, etc.
  - Most Probes are “passive”
    - Traffic must be delivered to ISE

- Probes are useful if the collected data can be bound to an endpoint
  - Full MAC-IP address bindings are always desirable
    - HTTP, DNS & NetFlow

RADIUS Probe

- Originally used to gather MAC & IP address information
  - Calling-Station-ID
    - MAC
  - Framed-IP-Address (Accounting packets)
    - IP
- RADIUS Probe is commonly deployed along with Device Sensor

Device Sensor

- Enables a switch/WLC to include additional profiling attributes inside of RADIUS Accounting packets
  - CDP, LLDP & DHCP
  - Recommended for scaling the deployment

- Configuration (switch)
  - Turn on RADIUS Accounting, Accounting VSAs, CDP/LLDP & DHCP Snooping
  - Enable with **device-sensor accounting** & **device-sensor notify all-changes**
  - Verify with **show device-sensor cache**

SNMP Probe

- Only recommended if Device Sensor is not supported
- TRAP
  - Sent by NAD to ISE on a link up/down event
  - Capable of collecting MAC address if MAC Notifications were enabled
- QUERY
  - Sent by ISE to NAD to fetch CDP/LLDP/ARP data
    - In response to SNMP TRAP or RADIUS Accounting packet
    - Periodically
    - During Network Scan (NMAP)

DHCP Probe

- Useful to capture IP-MAC address bindings & OS information
- DHCP (no SPAN)
  - Requires DHCP packets to be sent to ISE
    - Accomplished by using a Relay Agent (**ip helper-address**)
- DHCP SPAN
  - Might be hard to deploy and cause replication issues

HTTP Probe

- Main source of the OS information
  - HTTP Request (User Agent)

- HTTP (no SPAN)
  - Requires HTTP packets to be sent to ISE portals
    - Traffic will be profiled even if the Probe is disabled

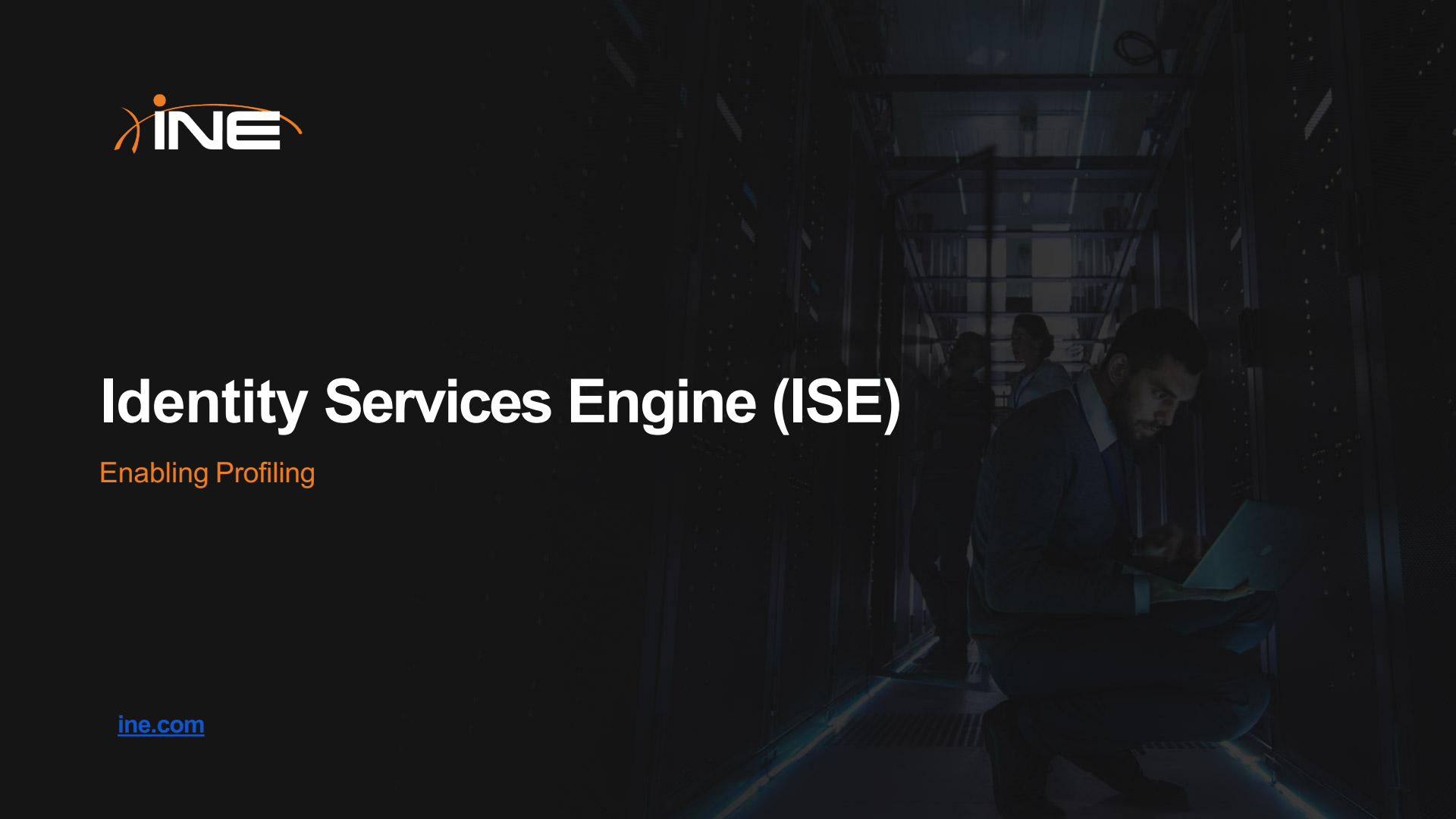
- HTTP SPAN
  - Commonly deployed in the Internet Edge
  - Might be too resource-intensive

Other Probes

- DNS
  - Acquires FQDN based on a reverse DNS lookup
- Active Directory
  - Extracts AD-related information (Windows systems)
- NetFlow
  - Profiles endpoints based on flow characteristics rather than attributes
  - NetFlow data may quickly oversubscribe a PSN
    - Only use Flexible NetFlow v9 along with a filtering solution (e.g. Stealthwatch)

Other Probes

- NMAP
  - “Active” mechanism communicating directly with an endpoint
    - TCP/UDP Port Scans including SNMP walk
  - Activation
    - Manual
      - IP host, subnet
    - Dynamic
      - Profiling Policy “Take Network Scan”
- Like HTTP & DNS requires ISE to already know the IP-MAC address binding



Identity Services Engine (ISE)

Enabling Profiling

ine.com

Module Overview

+ Configuration overview
+ Example

Profiling Configuration

- Enable the Profiling Engine
  - **Administration -> System -> Deployment -> General Settings -> Enable Profiling Service**
- Activate Probes
  - **Administration -> System -> Deployment -> Profiling Configuration**
- Configure Probe-related ISE & NAD settings
  - Most Probes require NADs to be added to Network Devices

Profiling Configuration

- RADIUS
  - Enabled by default
    - Configure NADs for Device Sensor if needed

- SNMP
  - TRAP
    - NAD : **snmp-server host** + **snmp-server enable traps**
  - QUERY
    - NAD : **snmp-server community** or according to v3
  - Configure SNMP settings on the NAD profile

Profiling Configuration

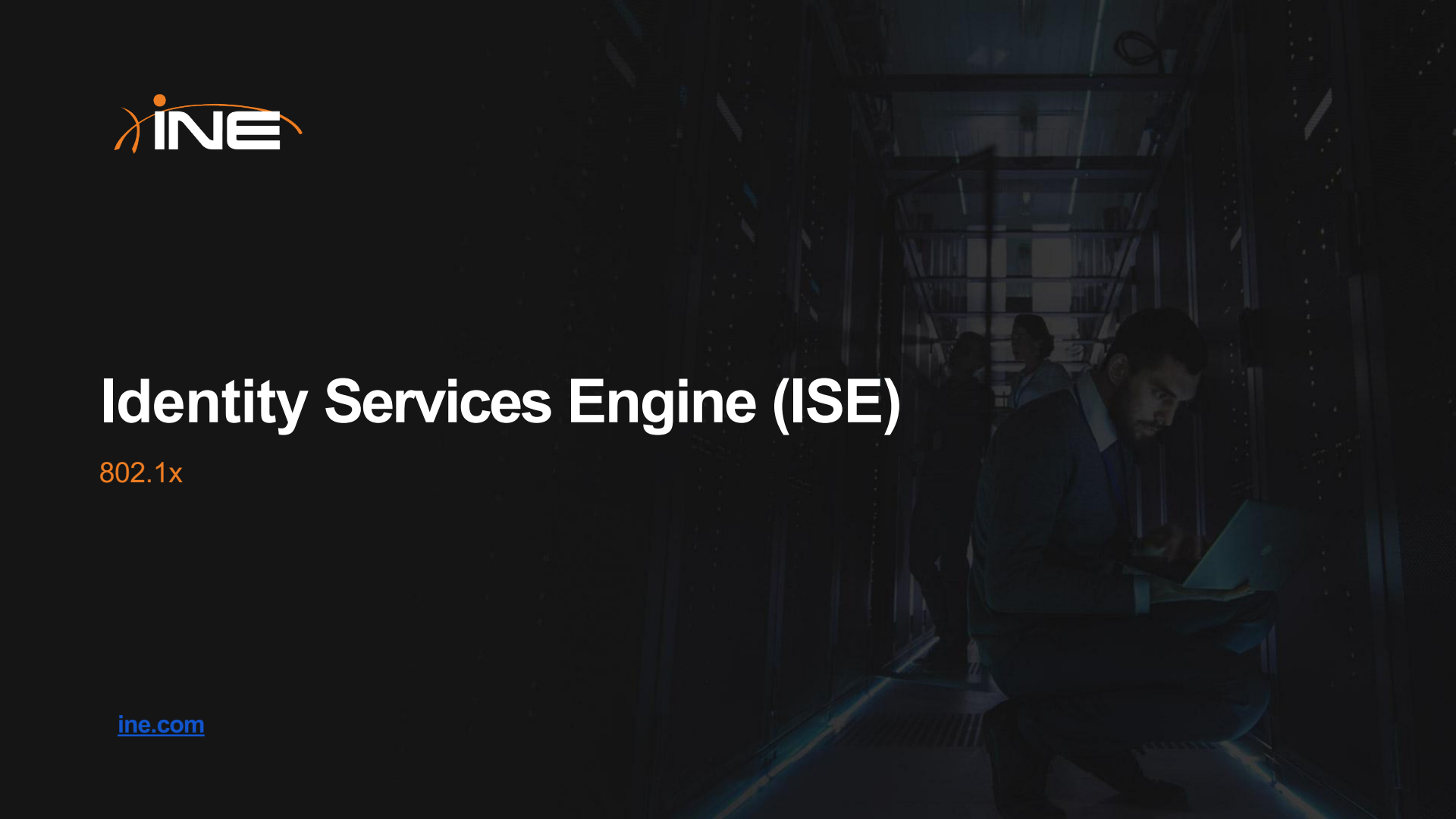
- DHCP
  - Copy DHCP Packets to ISE with a Relay (**ip helper-address**)
    - Tune with **no ip forward protocol udp**
    - DHCP Server won't forward local DHCP packets
  - For DHCP SPAN configure SPAN/RSPAN with ISE as a session destination
  - For wireless disable DHCP Proxy (**Controller -> Advanced -> DHCP**)
    - Still requires a "wired" Relay
- DNS
  - Configure DNS Server with entries for Reverse Lookups

Profiling Configuration

- HTTP
  - Configure an appropriate Web Portal
    - The Probe does not even have to be enabled
  - For HTTP SPAN configure SPAN/RSPAN with ISE as a session destination
- Active Directory
  - Configure your AD server
- NetFlow
  - Configure (Flexible) NetFlow v9 on NADs with ISE as an exporter

Profiling Configuration

- NMAP
  - Run a scan manually
    - Specify SNMP credentials under **Work Centers -> Profiler -> Settings**
    - **Work Centers -> Profiler -> Manual Scans**
      - Previously under Node's Profiling Configuration
  - Tune Profiling Policies if dynamic scans are needed



Identity Services Engine (ISE)

802.1x

ine.com

Module Overview

- Feature overview
- 802.1x components & process
- Related features

802.1x Overview

- L2 authentication standard (IEEE) for wired & wireless networks
  - Used for identity-based networking
  - Implemented through EAP (EAP over LAN “EAPOL”)
    - A framework for exchanging arbitrary authentication data

- 802.1x components
  - Supplicant
    - Client software
  - Authenticator
    - Policy enforcement (Switch/AP/WLC)
  - Authentication Server (RADIUS)

802.1x Authentication

- Authenticator drops non-EAPOL frames before/during AuthC
  - Cisco switches add exceptions for STP, CDP & LLDP

- The Process
  - Authentication process starts on reception of a EAP Request Identity frame
    - Sent on link up/w-less connection or upon reception of EAPOL START
  - Authenticator acts as a proxy between Supplicant & RADIUS server
    - EAP data is extracted & encapsulated using two RADIUS EAP-specific attributes
  - Authentication method is negotiated followed by authentication

802.1x Authentication

- Authentication results determine network access rights
  - Success (Access-Accept – EAP Success)
    - Allow access + return optional AuthZ data (dACL/VLAN)
  - Failure (Access-Reject - EAP Failure)
    - Wireless
      - No access
    - Wired
      - No access (reauthenticate after **dot1x timeout quiet-period**)
      - Next authentication method
      - Auth-Fail VLAN

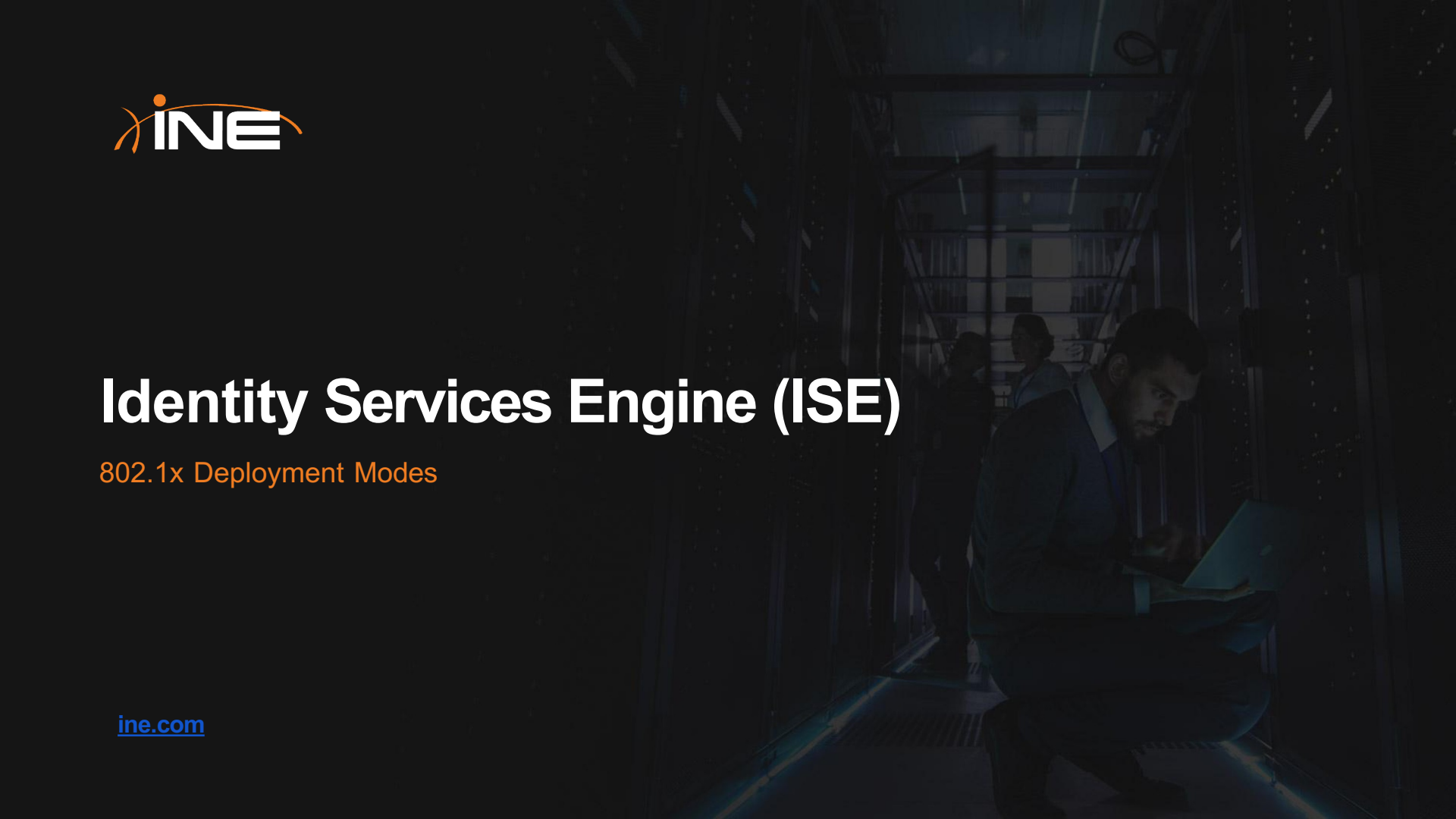
MAC Authentication Bypass (MAB)

- An alternative authentication method for 802.1x environments
  - Needed for non-Supplicant devices (IP cameras, printers, etc.)

- MAB Details
  - If enabled (**mab**), triggers after 802.1x times out (**dot1x timeout tx-period**)
    - In wireless for WLANs configured with MAC Filtering
  - Processed as “Host Lookup”
    - No password verification, authC based on presence of MAC address
    - Identified via RADIUS Service-Type 10 (Call-Check) & NAS-Port-Type
      - 15 (Ethernet)
      - 19 (Wireless)

Flexible Authentication

- Cisco's 802.1x enhancement for wired deployments
  - Single configuration that fits all 802.1x authentication scenarios
    - Authentication method list (ordered)
      - **authentication order [dot1x] [mab] [webauth]**
    - Failed authentication fallback
      - **authentication event fail action next-method**
    - Authentication method preference
      - **authentication priority [dot1x | mab] webauth**
- Not available for wireless 802.1x



Identity Services Engine (ISE)

802.1x Deployment Modes

ine.com

Module Overview

+ Monitor, Low-Impact & Closed Modes
+ ISE considerations

Deploying 802.1x

- In the past most of 802.1x deployments initially failed
  - Supplicant problems, ID store/switch/RADIUS misconfig, wrong MACs, etc.
- Cisco allows to deploy 802.1x in phases (“Modes”)
  1. Monitor
  2. Low Impact and/or Closed
- Wireless 802.1x is “binary” and cannot be phased
  - No Monitor or Low Impact Modes

Monitor Mode

- Enables 802.1x authentication but without affecting users/endpoints
  - Provides full visibility to the devices connecting to the network
  - Allows to address any authentication issues prior to moving to the next deployment

- Monitor Mode components
  - Flexible Authentication & MAB
  - Multi-Auth Port Mode
  - RADIUS Accounting (802.1x)
  - Open Authentication (**authentication open**)
  - Profiling

Low-Impact Mode

- Provides partial network access prior to authentication
  - Useful for Preboot Execution Environments (PXEs), diskless workstations, etc.
- Low-Impact Mode builds on top of the Monitor Mode
  - Open Authentication is still critical
  - Pre-Authentication ACL
    - DHCP & DNS
    - Microsoft ports for Machine Authentication (Kerberos, LDAP, etc.)
- Successful authentication extends the default policy

Closed Mode

- Works like original 802.1x
  - No data traffic is allowed before successful authentication
  - Perfect for VLAN-based segmentation
    - No IP address is assigned prior to authentication

- Changes from the Monitor Mode
  - Open Authentication must be disabled
  - VLANs must exist prior to assignment
    - Including WLC subinterfaces

Main Configuration Considerations (ISE)

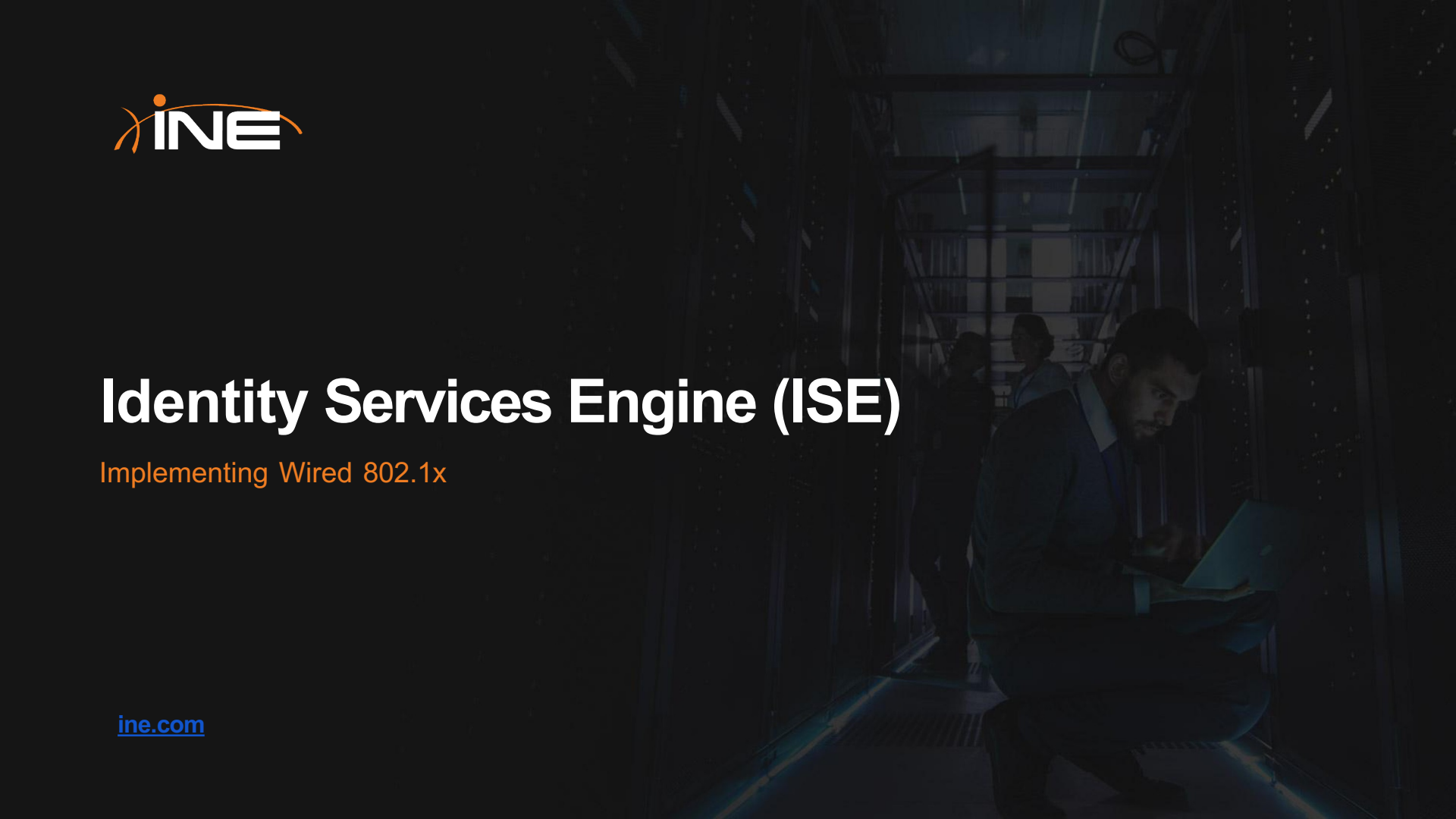
- Monitor Mode
  - Successful authentication for unknown endpoints (“Continue” action)
  - User/device specific authorization rules
    - No authorization profiles (e.g. dACL, VLAN)
      - Except for Voice Permission (IP Phones)

- Low-Impact Mode
  - Authorization rule tuning
    - Authorization profiles

Main Configuration Considerations (ISE)

- Closed Mode
  - Authentication rules for wireless MAB & 802.1x
  - Authorization rule tuning
    - Authorization profiles

- Using Network Device Groups (NDGs) may help in any deployment
  - One for each Mode
    - Separate Policy Sets



Identity Services Engine (ISE)

Implementing Wired 802.1x

ine.com

Module Overview

+ Configuration syntax
+ Example

802.1x Configuration

- Switch
  - Enable AAA (**aaa new-model**)
  - Define RADIUS server (**radius-server host** or **radius server** *name*)
  - Enable 802.1x globally (**dot1x system-auth-control**)
  - Configure 802.1x method list (**aaa authentication/accounting dot1x default**, **aaa authorization network default**)
  - Configure a switchport
    - Enable access mode (**switchport mode access**)
    - Activate 802.1x (**authentication port-control auto**)
    - Make it act as Authenticator (**dot1x pae authenticator**)

802.1x Configuration

- Port Settings (**authentication port-control**)
  - **force-authorized** (default)
  - **force-unauthorized**
  - **auto**

- Port Modes (**authentication host-mode**)
  - Controls a number & type of devices allowed to connect through a port
    - **single-host**
    - **multiple-host**
    - **multi-domain**
    - **multi-auth**

802.1x Configuration

- Port Violations (**authentication violation**)
  - Port-Security behavior applies to **single-host** & **multi-domain** modes
    - **shutdown** (default)
    - **restrict**
    - **protect**
    - **replace**

- MAC Move (**authentication mac-move permit**)
  - Allows to move already authenticated devices between the ports

802.1x Configuration (optional)

- Guest VLAN
  - Assigned to clients without Supplicant
    - Compatible with MAB (assigned if MAB fails)
    - Not supported on **multi-auth** ports
    - Enabled with **authentication event no-response action authorize vlan**

- Auth-Fail (Restricted) VLAN
  - Assigned to clients that failed 802.1x authentication
    - Not compatible with MAB or WebAuth
    - For **single-host** ports only
    - Enabled with **authentication event fail action authorize vlan**

802.1x Configuration (optional)

- Critical VLAN
  - Assigned to clients if AAA server is not reachable
    - Enabled with **authentication event server dead action authorize vlan**

- Other
  - RADIUS VSAs
    - **radius-server vsa send [authentication | accounting]**, **radius-server attribute**
  - CoA
  - Device Tracking
  - Pre-Authentication ACL

802.1x Configuration

- RADIUS Server
  - Add Network Devices
  - Configure Identity Stores & AuthC policy
  - Create authorization elements/profiles
  - Configure AuthZ policy

Identity Services Engine (ISE)

Implementing Wireless 802.1x

ine.com

Module Overview

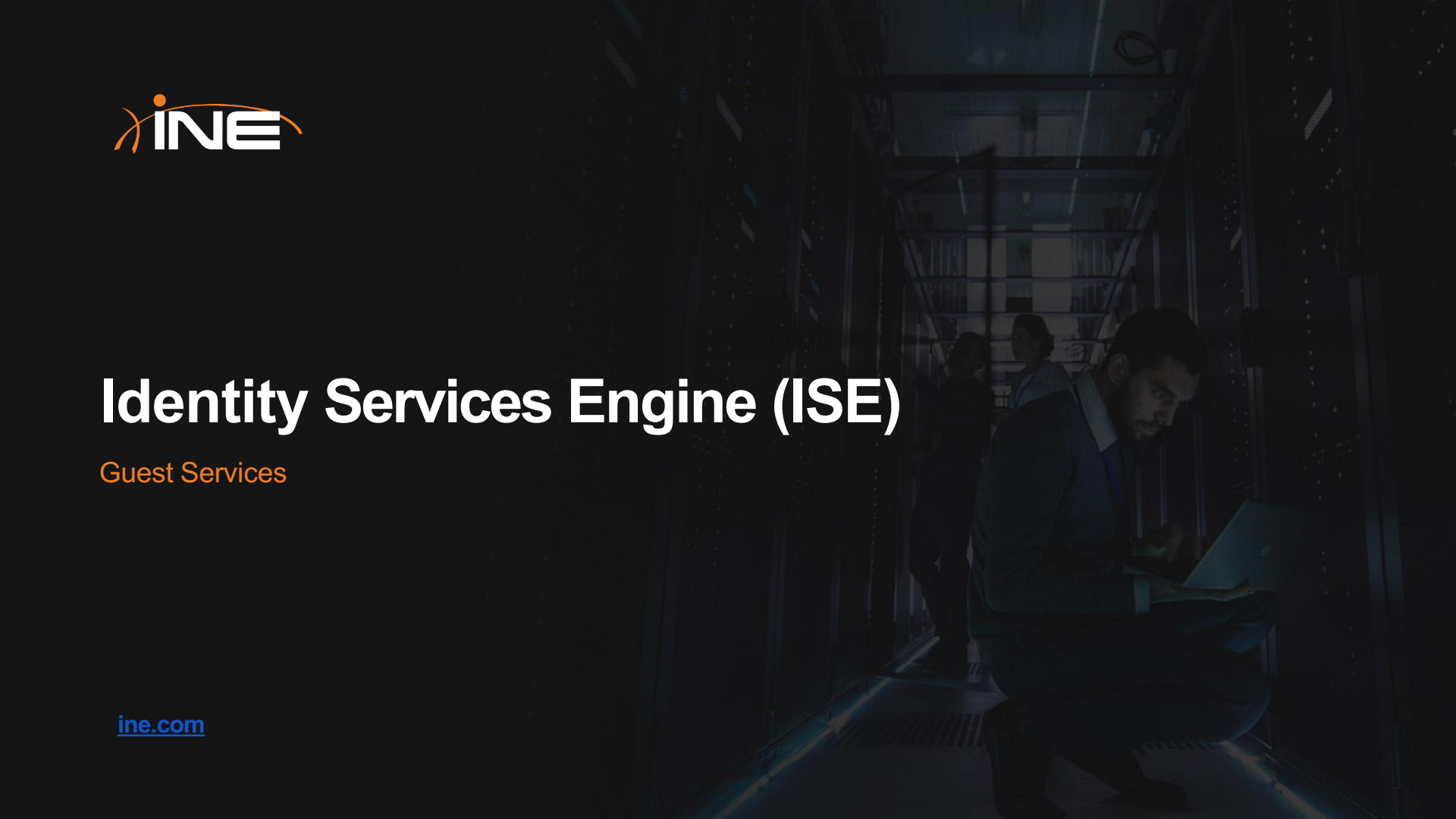
+ Configuration overview
+ Example

802.1x Configuration (Wireless)

- WLC
  - Add an interface & WLAN
  - Define RADIUS Server(s)
  - Secure WLAN
    - Authentication method
    - Advanced options
  - Create ACL(s) and additional interface(s) if needed

802.1x Configuration (Wireless)

- RADIUS Server
  - Add Network Devices
  - Configure Identity Stores & AuthC policy
  - Create authorization elements/profiles
  - Configure AuthZ policy



Identity Services Engine (ISE)

Guest Services

ine.com

Module Overview

+ Guest access
+ Central Web Authentication (CWA)

Guest Services Overview

- ISE provides a complete solution for guest users
  - Guest users are temporary and require limited network access
  - Deployed through a Local or Central Web Authentication (LWA/CWA)
    - CWA vs LWA
      - Centralized configuration
      - CoA support
      - AuthZ with dACLs & VLANs

- Guests can be authenticated or not
  - Authenticated guests require special accounts
    - Created by Sponsors or via self-registration

Default Guest Portals

- Sponsor
  - Grants access through sponsored accounts
- Self-registered
  - Allows access with accounts created by guests themselves (“self-register”)
- Hotspot
  - Provides non-authenticated guest access
- More than one portal can be configured & customized

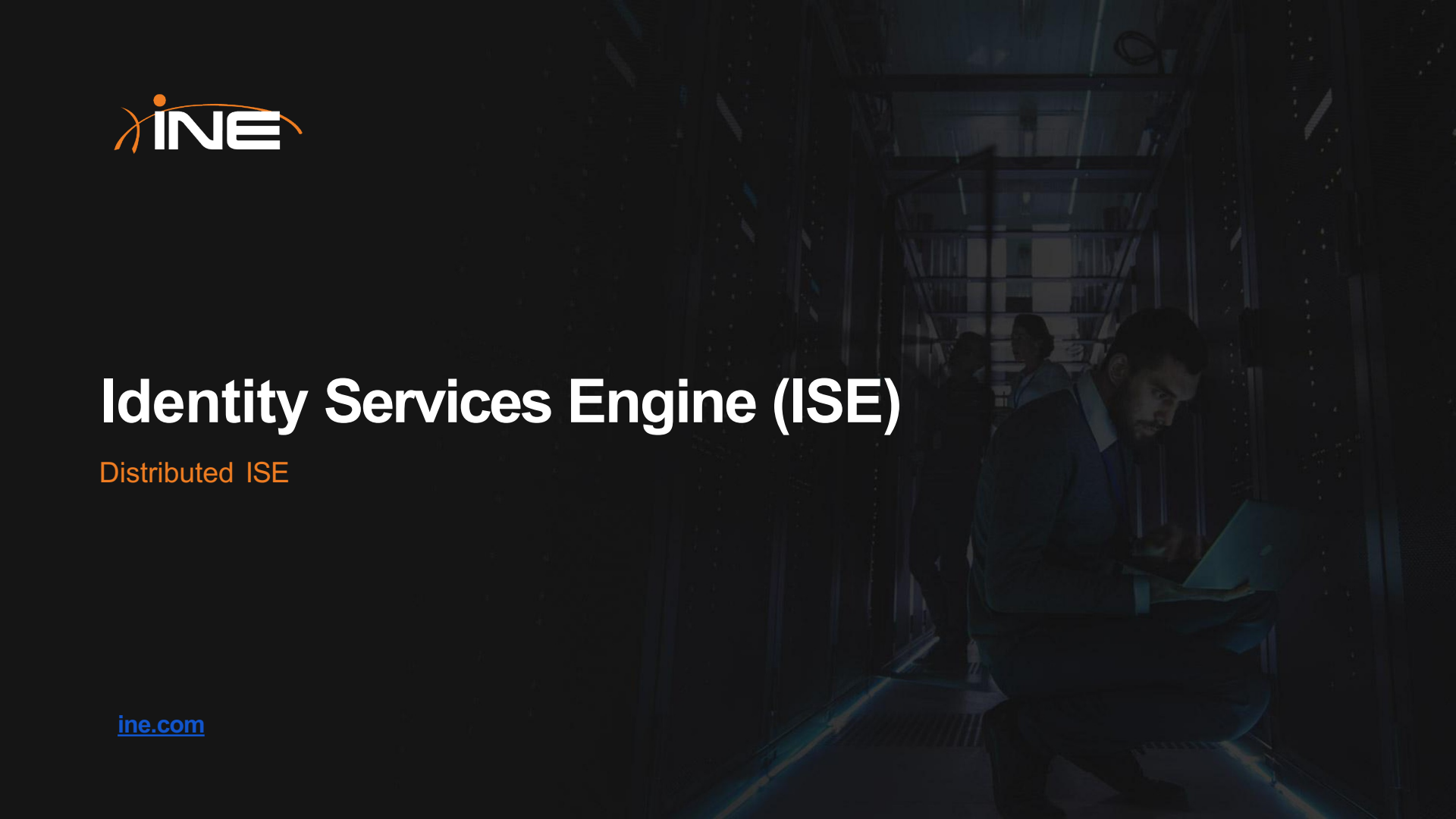
CWA Workflow

- Applies to wired & wireless deployments
  - User connects to a 802.1x/MAB port or open SSID with MAC Filtering on
  - Successful MAB Authentication triggers Authorization
    - Set “Continue” for “User Not Found” to account for unknown endpoints
  - A matching AuthZ rule (typically Default) returns a profile with CWA
    - Redirection ACL & Guest Portal URL
  - Authenticated host gets an IP (DHCP) & its web traffic reaches ISE portal
  - Successful web authentication (guest user/endpoint) triggers CoA
    - Re-Auth (authenticated guests) or Termination (non-authenticated guests)
      - Results in a hit in a different AuthZ policy rule

CWA Configuration Considerations

- Authorization Policy
  - Authenticated guest sessions can be matched through a special condition
    - **Network Access:UseCase Equals GuestFlow**
  - If automatic guest Device Registration is on, guest endpoint groups can be used
    - E.g. **GuestEndPoints**, **GuestType_Daily** or **GuestType_Weekly**
    - A must for Hotspot connections

- Redirection ACL
  - Switch “permit” & WLC “deny” ACL entries define traffic to redirect
  - DHCP, DNS & IP traffic to ISE servers should be never redirected
    - Also applies to all ISE traffic sent to the client



Identity Services Engine (ISE)

Distributed ISE

ine.com

Module Overview

- Terminology
- Deployment modes
- ISE Personas

Distributed ISE Overview

- ISE Terminology
  - Node
    - Single ISE instance
  - Persona
    - A role describing the main function of a Node
      - Service refers to individual features Persona provides

- Deployment Models
  - Standalone
  - Distributed
    - Redundancy & improved performance

ISE Personas

- Policy Administration Node (PAN)
  - Handles all system & policy related configuration (“mothership”)
  - Synchronizes databases of all other nodes
- Redundancy
  - Primary & Secondary PAN
    - Active/Standby
      - Standby unit (Secondary) is not used – it gets all config from the Active unit
  - Failover
    - Manual
    - Automatic
      - Health checks of the Primary PAN are made by an additional node

ISE Personas

- Policy Service Node (PSN)
  - Delivers all configured services (“workhorse”)
- Redundancy
  - Multiple PSNs
    - Since all PSNs have the same database, NADs can pick any of them
      - Sessions can be load-balanced with **radius-server load-balance**
    - Larger designs might be simplified by “hiding” PSNs behind one IP
      - Load Balancer
      - Anycast

Node Groups

- An optimization mechanism for PSN deployments
  - Improved convergence of services based on URL redirection
    - A failure of a group member triggers CoA on another node
      - Allows to reestablish all disconnected sessions through another PSN
  - Reduced replication
    - Less significant attributes can be shared directly instead of via PAN
- Works best for PSNs that are local (LAN) or behind a load balancer

ISE Personas

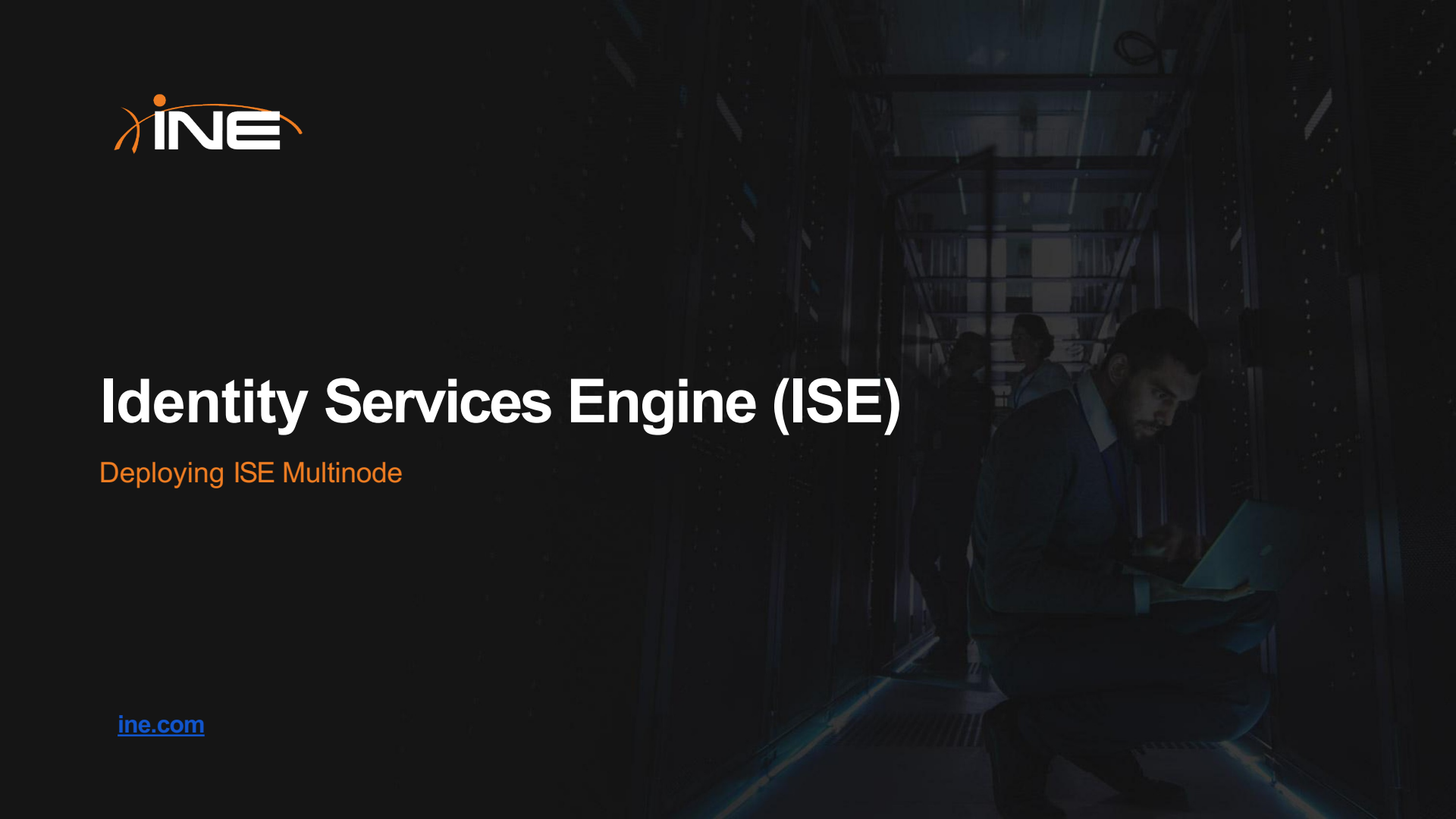
- Monitoring & Troubleshooting (MnT)
  - Enables ISE to function as a Log Collector
    - Stores logs from all other nodes – PAN & PSNs

- Redundancy
  - Primary & Secondary MnT
    - Active/Standby but logs from PAN & PSNs are sent to both units
      - Failover happens automatically but databases are not synced on node recovery

ISE Personas

- pxGrid
  - Shares context-sensitive data with other systems
    - NGFW, Stealthwatch, non-Cisco ISE partner systems (“ecosystems”)

- Redundancy
  - Primary & Secondary pxGrid
    - Active/Standby with automatic failover



Identity Services Engine (ISE)

Deploying ISE Multinode

ine.com

Module Overview

+ Before you start
+ Configuration

Before You Start

- Prerequisites
  - IP connectivity
  - DNS server
    - Forward & reverse entries for all nodes
  - Certificate setup
    - Primary PAN must be able to validate Admin cert of each Secondary node
      - Add appropriate CA certificate(s) under Certificate Trust List (CTL)
      - Self-signed certificates are not recommended but may be used
  - Time synchronization (NTP)
    - Certificates, Logs & Reports

Configuration

- Primary PAN
  - Designate one node as mothership
    - **Administration -> System -> Deployment**
      - MnT persona is also required but may be then disabled

- Registration
  - Register all other units (Secondary nodes) on the Primary PAN
    - **Administration -> System -> Deployment -> Register**
  - Successful registration results in config replication (Primary -> Secondary)
    - Configuration changes should be only done on the Primary PAN

Identity Services Engine (ISE)

Course Conclusion

ine.com

Course Conclusion

- ISE is a powerful next-generation security platform with much to offer
  - Centralized AAA (network access, administration)
  - Advanced Services (Profiling, Posture, BYOD, etc.)
- ISE policy enforcement capabilities allow for controlled & scalable 802.1x deployments
- Multi-node deployments provide redundancy & scalability

Thank You

EXPERTS AT MAKING YOU AN EXPERT