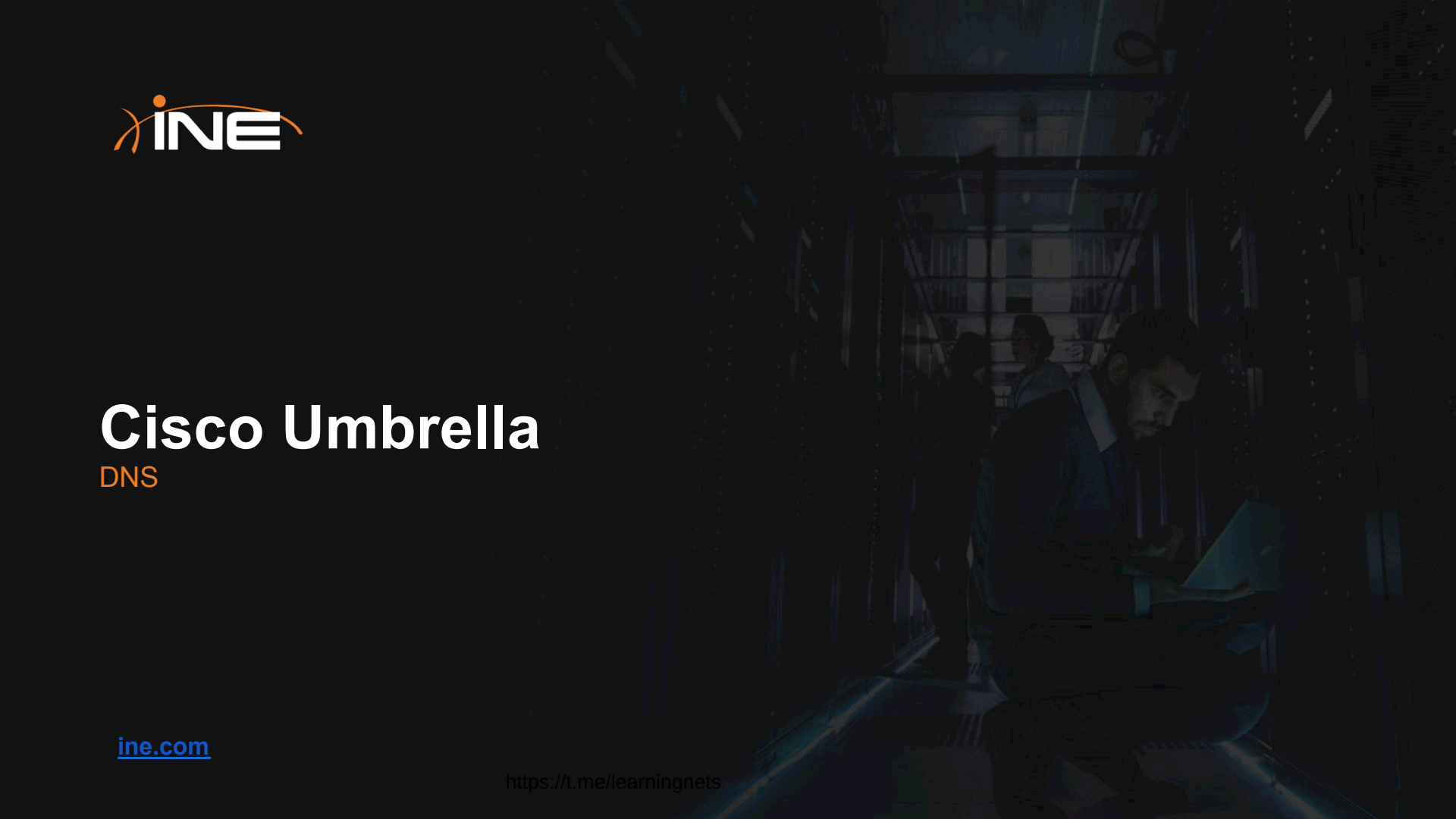


Cisco Umbrella

DNS

ine.com

Module Overview

- Protocol overview
- DNS structure, components & records

Domain Name System (DNS) Overview

- TCP/IP communication is established through logical (IP) addresses
  - Most people find them hard to remember (especially IPv6)

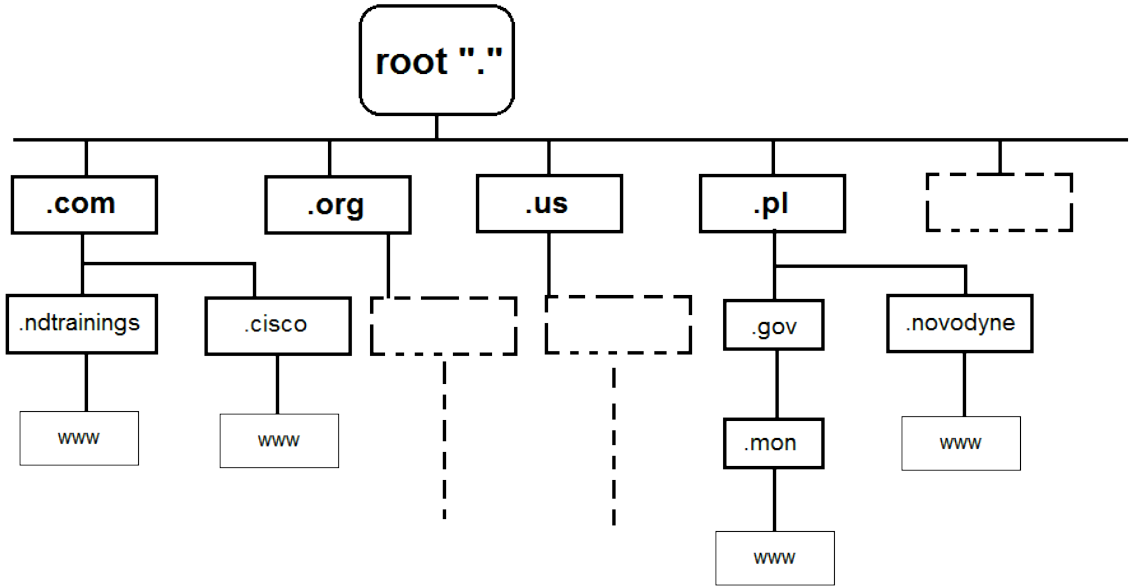
- DNS is an application-layer protocol created to allow to use names rather than addresses when referring to TCP/IP hosts or applications
  - IP addresses are still needed & will be provided by DNS through name resolution
    - For example, DNS knows that www.ndtrainings.com is actually 67.20.89.54

DNS Structure

- DNS names are organized into Domains
  - Domains are hierarchical
    - Root domain is represented as a dot „.”
    - All domains right below Root are known as Top Level Domains (TLDs)
      - .com, .org, .us, .pl, .edu, .gov & many more
    - All other domains are known as sub-domains
      - .ndtrainings.com, .cisco.com, .usa.gov

- Fully Qualified Domain Name (FQDN)
  - The complete and unique name of a DNS endpoint
    - A combination of hostname (DNS leaf) and its (sub)domain, e.g. www.ndtrainings.com

DNS Structure



DNS Components

- Resolver
  - Client DNS software (e.g. web browser) triggering Name Resolution
  - DNS Requests are generally sent for FQDN (UDP port 53)
    - E.g. what is an IP address corresponding to www.ndtrainings.com ?
- Domain Name Servers
  - Responsible for maintaining and providing DNS information to clients
    - DNS information is grouped into Zones & stored in Zone Files
    - Zones allow to separate DNS information from the domain
      - A given DNS server must only know (be authoritative for) information of its Zone(s)
      - It does not need to know the details of any of the subdomains

DNS Records

- Resource Record Types
  - Name Server (NS)
    - A list of authoritative DNS servers
  - Address (A)
    - FQDN to IP mapping
  - IPv6 Address (AAAA)
    - FQDN to IPv6 mapping
  - Pointer (PTR)
    - IP/IPv6 to FQDN mapping
  - Mail Exchange (MX)
    - A list of mail servers

Cisco Umbrella

Introduction to Umbrella

ine.com

Module Overview

- Overview
- Packages
- Access & documentation

Umbrella Overview

- Umbrella offers an advanced recursive DNS service
  - Secure
    - DNS inspection & much more
  - Cloud-based
    - Consolidates security services at one place despite of the recent "decentralized network" trend
  - Fast & highly resilient
    - Extensive BGP peerings
    - Anycast routing
  - Fully controllable
    - Single configuration/reporting dashboard
    - APIs

Umbrella Packages

- Packages determine product's functionality & features
  - Cisco Umbrella
    - DNS Security Essentials
    - DNS Security Advantage
  - Cisco Umbrella SIG
    - Secure Internet Gateway (SIG) Essentials

Access & Documentation

- Umbrella Dashboard
  - https://login.umbrella.com
- Umbrella Documentation
  - Cisco Umbrella
    - https://docs.umbrella.com/deployment-umbrella/docs
  - Cisco Umbrella SIG
    - https://docs.umbrella.com/deployment-umbrella/v1.0.6/docs/welcome-to-cisco-umbrella

Cisco Umbrella

Deploying Umbrella

ine.com

Module Overview

- Deployment options
- Basic configuration

Deployment Options

- DNS traffic can be redirected to Umbrella in several ways
  - On-network
    - Internal DHCP
      - Locations with no internal domain(s)
    - Internal DNS
      - Some endpoints may need to be configured manually
    - Umbrella Virtual Appliance
    - Network devices
  - Roaming & Mobile
    - Umbrella Roaming Client
    - AnyConnect Umbrella module
    - Cisco Security Connector (iOS agent)

Umbrella Virtual Appliance (VA)

- Lightweight virtual machine for VMware, AWS, Azure & more
  - Works as a conditional DNS forwarder
    - Receives all client DNS queries
      - Only public/external DNS queries go to Umbrella

- VA Advantages
  - Extended DNS (EDNS)
    - Device & Organization ID, client's IP
      - Enhanced visibility & granular policies (public IP address does not matter)
  - Easy AD integration
    - Adds user/group information
  - Encryption (DNSCrypt) & Authentication

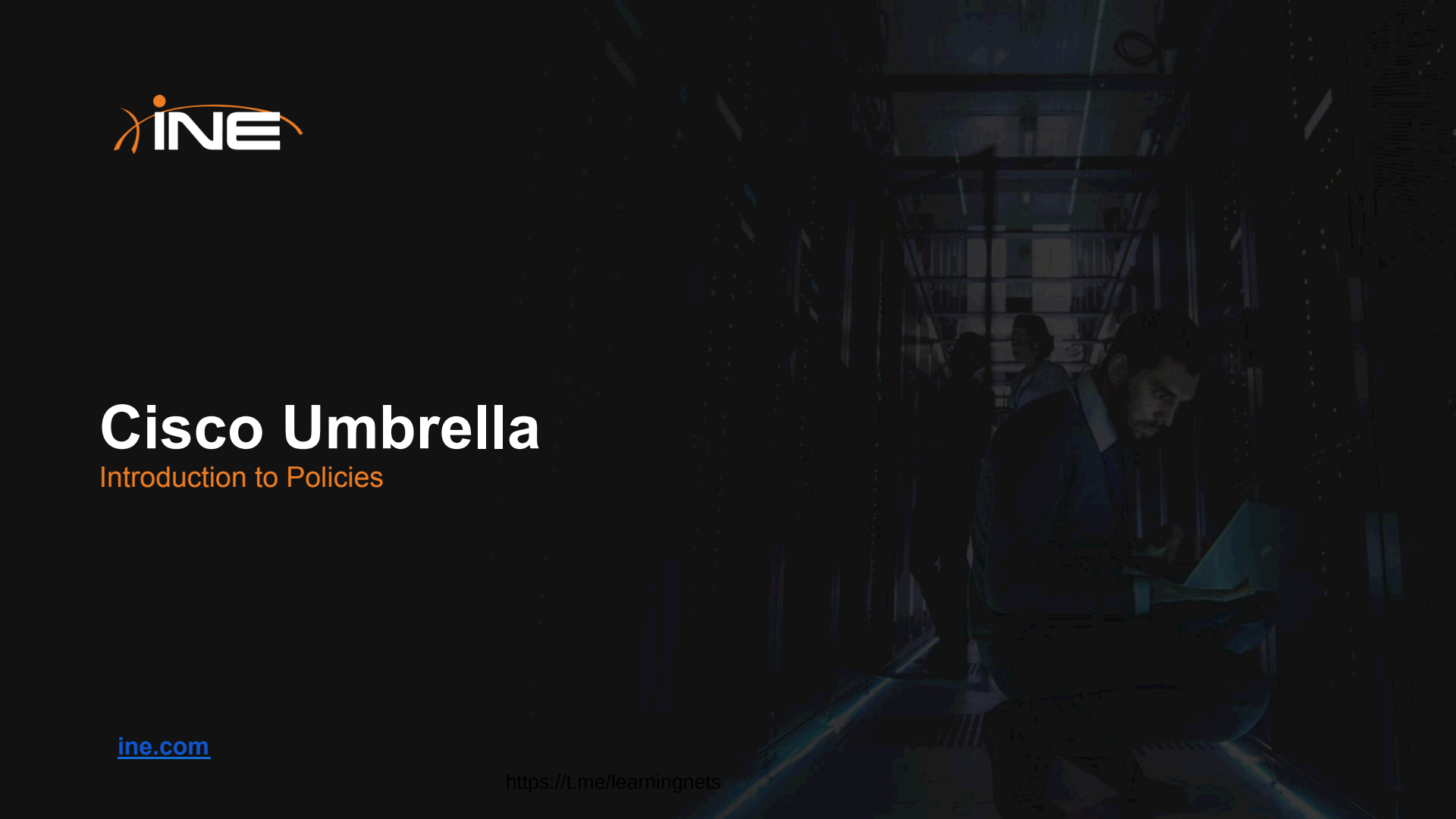
Hardware Integration

- Requires DNS traffic to go through the supported platform
  - ISR4k, ISR1100
  - WLC (8.4+)
  - ASA 5500-X & ASAv (9.10.1+)
  - Firepower 2100/4100/9300
  - Other
- Umbrella-integrated hardware uses EDNS to maintain the client's IP
  - DNSCrypt is also supported

Basic Configuration

- Register the organization
  - **Deployments -> Core Identities -> Networks**
    - A public IP (including dynamic IPv4)
      - Or a VA's/Network redirector's IP
  - Edit internal domains (**Domain Management**)

- Send non-local DNS traffic to the Umbrella Cloud
  - Modify DHCP/DNS server and/or endpoint settings
    - 208.67.222.222 & 208.67.220.220
    - 2620:119:35::35 & 2620:119:53::53
  - Test with http://welcome.umbrella.com
  - Optionally adjust your firewall rules (DNS)



Cisco Umbrella

Introduction to Policies

ine.com

Module Overview

+ Policies overview
+ Policy engines

Policies Overview

- Umbrella enforces security & access controls through Policies
  - A policy points to at least one identity
  - Policies are evaluated top-down
    - Only the first policy matching the identity gets executed
    - Default Policy is a catch-all (applies to all identities)

- Policy Engines
  - DNS Layer Security
  - Content Inspection
  - Application Inspection
  - File Analysis
  - Destination Lists

DNS Layer Security

- Umbrella separates “bad” DNS traffic to categories
  - Malware
  - Newly Seen Domains
  - Command Control Callbacks
  - Phishing Attacks
  - Dynamic DNS
  - Potentially Harmful Domains
  - DNS Tunneling VPN
  - Cryptomining

Content & Application Inspection

- Allows to block traffic sent to non-malware sites based on content or application category
  - Content Category Levels
    - High, Moderate, Low & Custom
  - Application Categories
    - Social Networking, Games, P2P & more

File Inspection

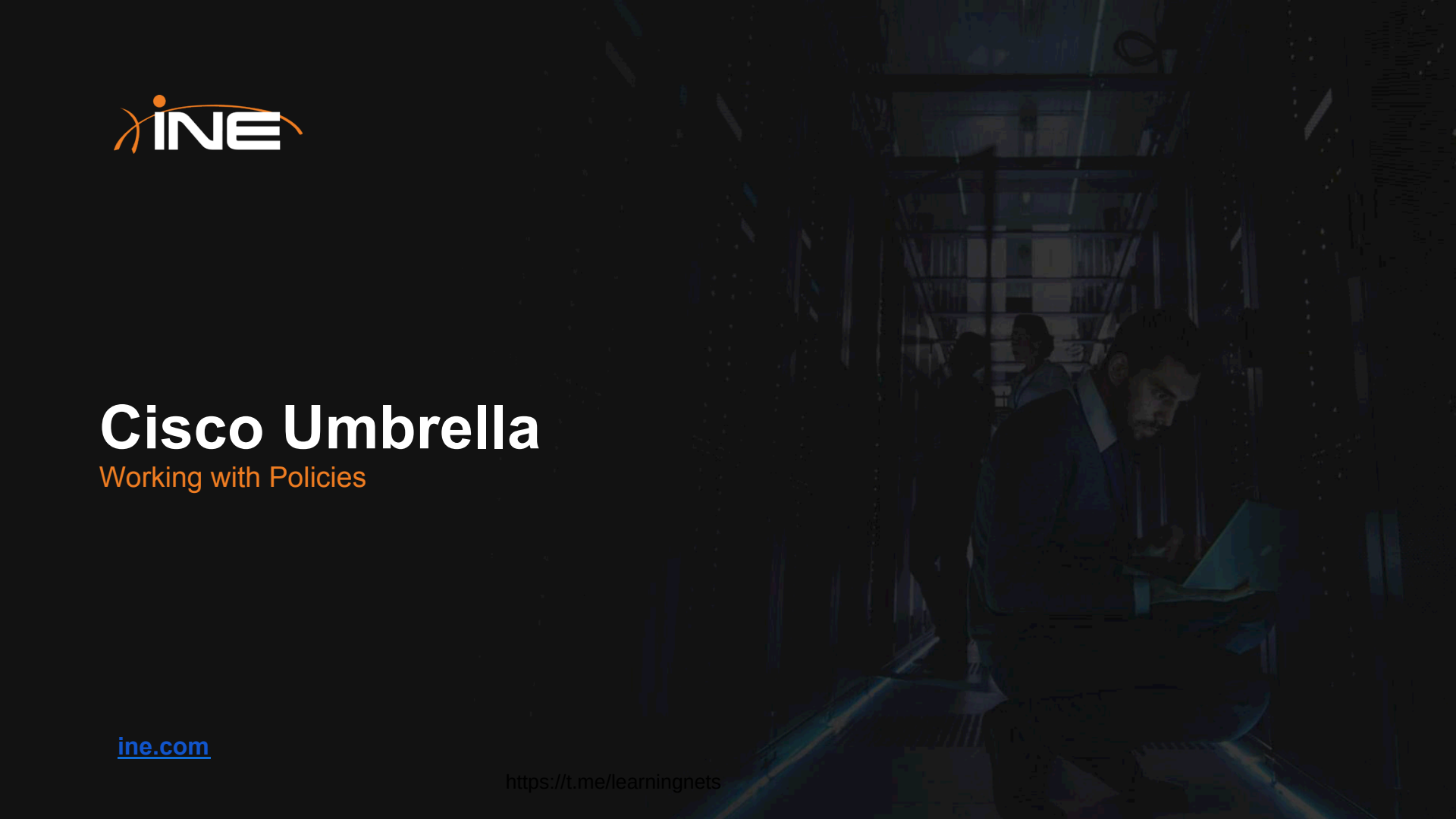
- Allows to scan files hosted on "risky" websites
  - Umbrella resolves a "risky" website to the IP of Intelligent Proxy
    - Intelligent Proxy must be enabled
  - The proxy passes the file to AMP & Anti-Virus engines for inspection
    - Only files deemed to be clean are returned to the user

- Using SSL Decryption enhances File Inspection
  - Certain websites won’t be proxied (and inspected) without it

Destination Lists

- Static exceptions for destinations to allow/block
  - IP addresses, URLs or FQDNs
  - Allow entries (whitelist) take precedence over block entries (blacklist) and security-related blocks
  - Default Global Lists (allow & block) apply to all policies and identities

- Certain services require multiple domains to be added to work
  - https://support.umbrella.com/hc/en-us/articles/115007472907-Block-Page-Bypass-or-Whitelist-Only-mode-Domains-to-Allow
  - Use Wireshark or Chrome's DNS Prefetch to fix other websites



Cisco Umbrella

Working with Policies

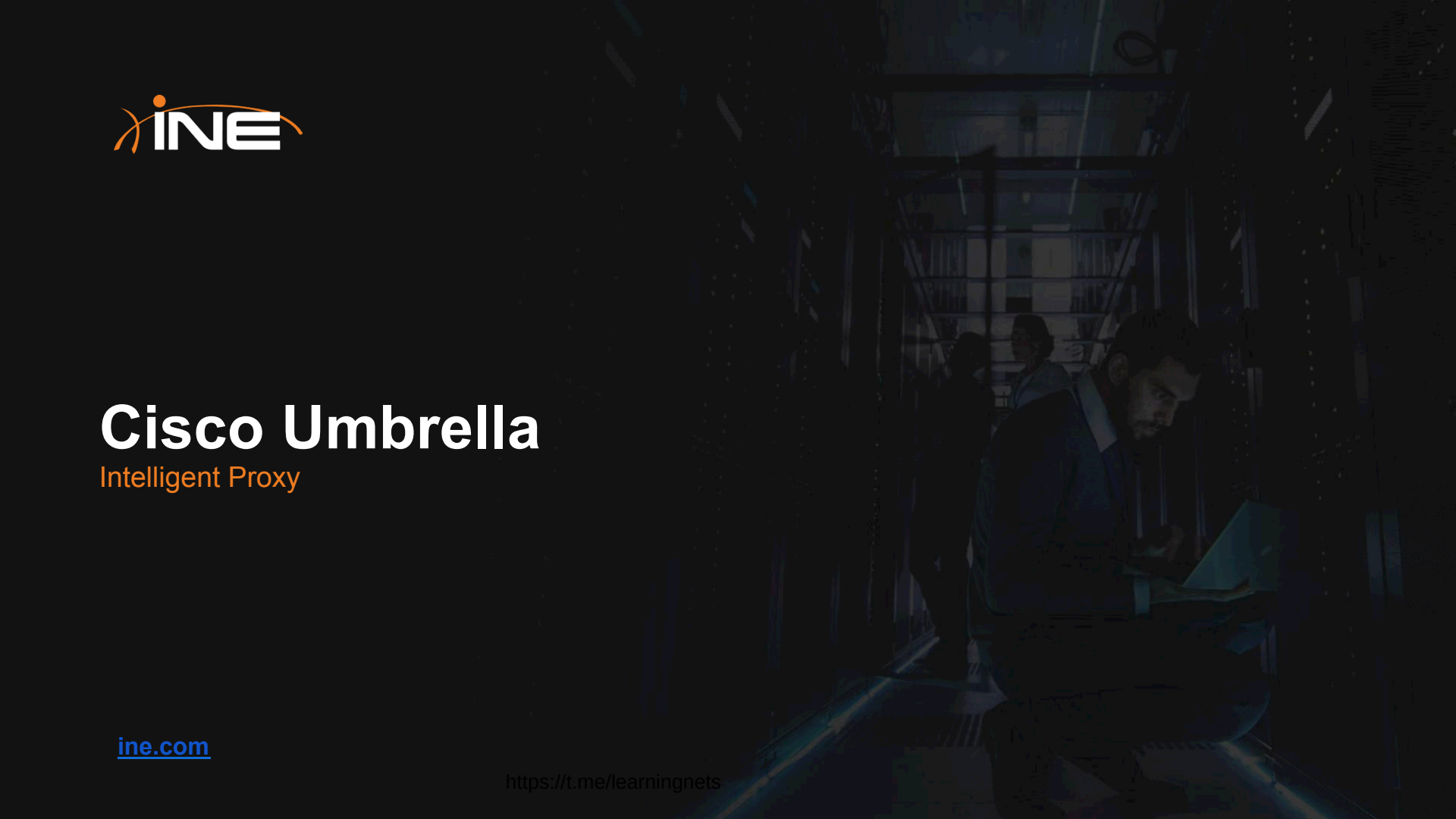
ine.com

Module Overview

+ Policy configuration & testing

Policy Configuration

- Create a new policy
  - **Policies -> Management -> All Policies**
    - Select at least one identity
    - Enable/disable policy engines
- HTTPS Block Pages require installation of the Cisco Root certificate
  - Per-device or through Group Policy (GPO)
    - Obtain certificate from your Umbrella account or via documentation
    - Install certificate to the “Trusted Root Certificate Authorities”
- Policy changes require up to ten minutes to take effect



Cisco Umbrella

Intelligent Proxy

ine.com

Module Overview

- Feature overview
- SSL Decryption
- Configuration

Intelligent Proxy Overview

- Extends DNS-layer protection to the session level
  - Allows for selective traffic interception (standard ports)
    - Gray/risky domains
      - Proxied website resolves to the IP address of the Intelligent Proxy
    - Traffic to known good/bad sites is handled at the DNS level
- Addresses important concerns related to traditional proxies
  - Scalability
    - Cloud-based service
  - Off-network protection
  - Speed & user experience
    - Selective proxying

SSL Decryption

- Recommended for Intelligent Proxy deployments
  - Works for proxy-intercepted traffic only
  - Allows to inspect HTTPS traffic
    - Certain domains my be bypassed through Selective Decryption
  - Improves behavior of other features
    - E.g. Custom URL Blocking or File Inspection
- SSL Decryption requires installation of the Cisco's Root certificate

Configuration

- Enable & tune Intelligent Proxy
  - **Policies > Management > All Policies**
    - **Advanced Settings**
  - Domain exceptions can be added via the Allow Lists
- Test
  - http://proxy.opendnstest.com