Cisco Duo Security-Multi-Factor Authentication

Course Objective:

Multi-factor authentication (MFA) is becoming the standard approach for securing enterprise systems. Companies large and small are embracing the technology due to its flexibility, affordability, and ease to implement.

The modern workforce is more mobile than ever before. Users and devices can connect from anywhere so companies must protect them everywhere. A zero trust security model establishes trust in users and devices through authentication and continuous monitoring of each access attempt, with custom security policies that protect every application.

What is a Zero Trust Approach?

Traditional security approaches assume that anything (devices, users, infrastructure, etc.) inside the corporate network can be trusted. The reality is that this assumption no longer holds true.

Now more than ever, employees and users have more control over the applications they use. Data and applications are no longer behind the firewall, and users can connect directly to work applications over the internet using personal owned devices.When approaching security design using the zero trust model, it's easiest to break adoption down into three pillars:

- **Workforce**
  Ensure only the right users and secure devices can access applications.
- **Workload**
  Secure all connections within your apps, across multi-cloud.
- **Workplace**
  Secure all user and device connections across your network, including IoT.

In Cisco We are Implementing Zero Trust for Workforce Using Duo Security. The massive demand to support remote work and adopt cloud environments amplifies the need for security in the workforce, so that's where many organizations begin their adoption of a zero trust security.

You will learn how to configure Duo Security fundamental elements in the Course

- How to Build Zero Trust Security for Workforce Using Duo
- Zero trust requires that a user be given access only to the applications they truly need to do their job and no more using protected Application
- Ensuring users and their devices are trustworthy at every access request, no matter where it comes from Using Trusted Devices
- How to Setup MFA for Different use case with Duo Security

Pre-requisite

- Basic knowledge about networking concepts
- Basic knowledge about IT and security protocols
- Basic knowledge about remote connectivity mechanisms like VPN
- Basic Knowledge on SAML and factor of Authentication.

Lab Setup

In order to do Different Scenario based Lab in this Course, User should have below setup available at their side

- Internet Access
- Computer (Laptop/Desktop) Running Any browser like Safari, Firefox, Chrome and Edge/IE
- Official or Personal Email Address to setup the Trial Account with Duo Security (Incase if you are Worried about Marketing Email then please Setup a Free Account on gmail or Yahoo)
- Smartphone (Android/IOS) to complete the Enrollment of Duo Security

Course Delivery and Duration

Delivery method can be Classroom and Online
Duration of Training: **5 Days**

Course Outline

1. **Multi-Factor Authentication Fundamentals**
   1.1 Factor of Authentication
   1.2 Types of 2FA?
   1.3 Supported Authentication Methods in Duo Security

2. **Duo Security MFA Implementation**
   2.1 Duo Security MFA Overview
   2.2 Licenses in Duo Security
   2.3 Features Supported by Duo Security
   2.4 Duo Prompt
   2.5 Duo Central
   2.6 Duo Access Gateway
   2.7 Duo Endpoint Self Enrollment

3. **Duo Security Admin Portal**
   3.1 Different Components of Duo Admin Portal
   3.2 First-Time Administrator Account Setup With Duo Security
   3.3 On-Boarding Users into Duo Security

3.4 Protected Application
3.5 Managing Administrator and Different Roles
3.6 Users Groups
3.7 Administrative Settings

4. **Duo Security Integration**
   4.1 Integration with Active Directory for Directory Sync
   4.2 Integration with Azure AD for Directory Sync
   4.3 Integration with Authentication Proxy Server
   4.4 Different Customization Options for authproxy.cfg

5. **Duo SSO Using SAML**
   5.1 What is SAML?
   5.2 Duo SSO-Cloud Hosted Using Active Directory
   5.3 Duo SSO-Cloud Hosted Using SAML iDP Provider
   5.4 Administrator Log-in Setup using SSO
   5.5 Duo Access Gateway
   5.6 DAG Running on Windows Server
   5.7 DAG Running on Linux Server
   5.8 DAG Launcher
   5.9 Bookmarks Link into DAG Launcher
   5.10 Best practice for DAG like HA, Backup and Restore

6. **Duo Access Features**
   6.1 Policy and Control
   6.2 Device Health
   6.3 Device Insight and Endpoint
   6.4 Trust Monitor

7. **Duo Trusted Endpoints**
   7.1 Trusted Endpoint Overview
   7.2 Trusted Endpoint with Duo Certificate Proxy
   7.3 Trusted Endpoint with Manual Enrollment
   7.4 Trusted Endpoint with MDM Like Cisco Meraki
   7.5 Trusted Endpoint with Cisco Secure Endpoint (Formerly Called as Cisco AMP)

8. **Common Use-Case | Remote Access VPN**
   8.1 Duo Network Gateway Overview
   8.2 Cisco ASA and Cisco FTD VPN Integration
   8.3 Palo Alto Firewall VPN Integration

9. **Common Use-Case | Microsoft**
   9.1 Microsoft RDP Integration
   9.2 Microsoft Office 365 Integration

10. **Common Use-Case | Web Application**
    10.1 WordPress Integration

10.2 Splunk Integration

11. Common Use-Case | Identity Provider

11.1 Integration with Radius Server like Identity Service Engine

12. Common Use-Case | Cloud Service Provider Using SAML

12.1 Integration with AWS

12.2 Integration with Cisco Umbrella

12.3 Integration with Zoom Meeting