ılıılı
CISCO

The bridge to possible

Cisco ISE and Duo: Better Together

Peanut butter and jelly.

Batman and Robin.

What do these pairs have in common? By themselves, they're fine; but together they're amazing. You can also add Cisco® Identity Services Engines (ISE) and Cisco Duo to the list of partnerships that work better together.

Separately they're strong

Cisco ISE powers security resilience with the flexibility and choice required to tether Network Access Control (NAC) workloads to multiple clouds and maintain business continuity through uncertainty. Moving from managing infrastructure in a box to leveraging Infrastructure as Code (IaC) across hybrid deployments, teams gain an agile approach to accelerate the delivery of pervasive visibility and dynamic control in support of zero-trust architectures. What all this means is that Cisco ISE lowers risk, protects business integrity, and accelerates secure network access across the distributed network.

Cisco Duo is a modern authentication and access management solution that prevents unauthorized access and protects against breaches due to stolen credentials. With a range of user-friendly features such as Multi-Factor Authentication (MFA), Single Sign-On (SSO), Passwordless login, Device Trust, and more, Cisco Duo delivers strong security that frustrates attackers but not users. It's designed to be easy to use, administer, and deploy and to provide detailed and actionable visibility and controls. This combination makes Cisco Duo a smart choice to quickly build the foundation for a successful zero-trust security model.

But together they're even more powerful!

Taken solely, Cisco ISE and Duo are strong options for your network security, but when the two are used in conjunction, your security becomes so much stronger. How?

Cisco Duo and ISE offer tremendous visibility. You've heard the adage, "You can't fight what you can't see," right? Think of the software team as a spotlight that shines on your network. With these two solutions, you get deep visibility into the users, devices, and applications that run both on and off your network. It's not difficult to manage either, as the Cisco ISE and Duo give network admins the simple tools needed to keep their network data under lock and key.

Your security is enhanced via Zero Trust. When your network employs Zero Trust, it means that it doesn't trust any endpoint connected to it and provides end-to-end accounting, authentication, and authorization via threat visibility. In other words, "If it's connected, it's protected!".

In order for Zero Trust to carry out its primary function of end-to-end security, both Cisco Duo and ISE has their own job to do:

- **Before granting application access, Cisco ISE:**
  - Provides network admins with insight into users and devices—including IOT.
  - Secures network access.
  - Contains threats.

- **At the same time, Cisco Duo:**
  - Authenticates users.
  - Verifies devices.
  - Enables access.

To put it another way, Cisco ISE gets the information and then gives it to Duo, which then allows for this now-authorized device to connect to the network. It's a one-two punch that takes the guess work out of who or what should be on the network.

Peeking under the hood

We've talked a bit about how Cisco Duo and ISE protect your network, but let's dive into how this process actually works:

1. An endpoint requests access.

    - Cisco Duo identifies the endpoint and trust is established.

2. The endpoint is classified and profiled into groups.

    - Cisco ISE tags the endpoint.

    - Cisco ISE applies network policy to profiled groups based on least privilege. Least privilege means: the only information (apps, tools) that a person or device needs to access will only be available to that person or device. For example, an intern is not going to be able to review files and apps that the CEO works with.

3. The endpoint is authorized access based on least privilege.

    - At this point, Cisco Duo grants access.

    - Cisco ISE recognizes that network segmentation has been achieved.

The good news is that the network administrator isn't constantly monitoring their laptop, determining who gets access and who gets denied. It's done automatically—that's the job of Cisco ISE and Duo.

Now your network is ultimately safer, and since it's automatic, you'll have time to work on the projects that are desperately requiring your attention.

So if given a choice between Cisco ISE or Cisco Duo, choose both! With these two solutions working together, your network will be busting more bad guys than Batman and Robin.

Learn more:

- **Cisco Duo**

- **Cisco ISE**