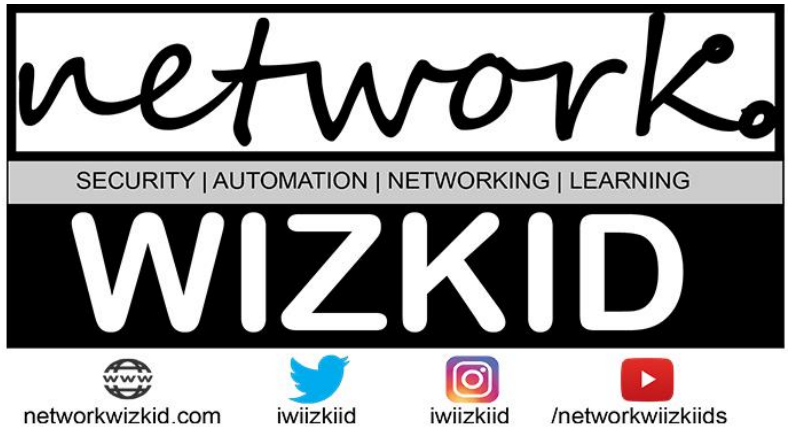
Duo Two-Factor Authentication for ASA/FTD Remote Access VPN's with Cisco ISE

Duo Lab Sessions with Kelvin

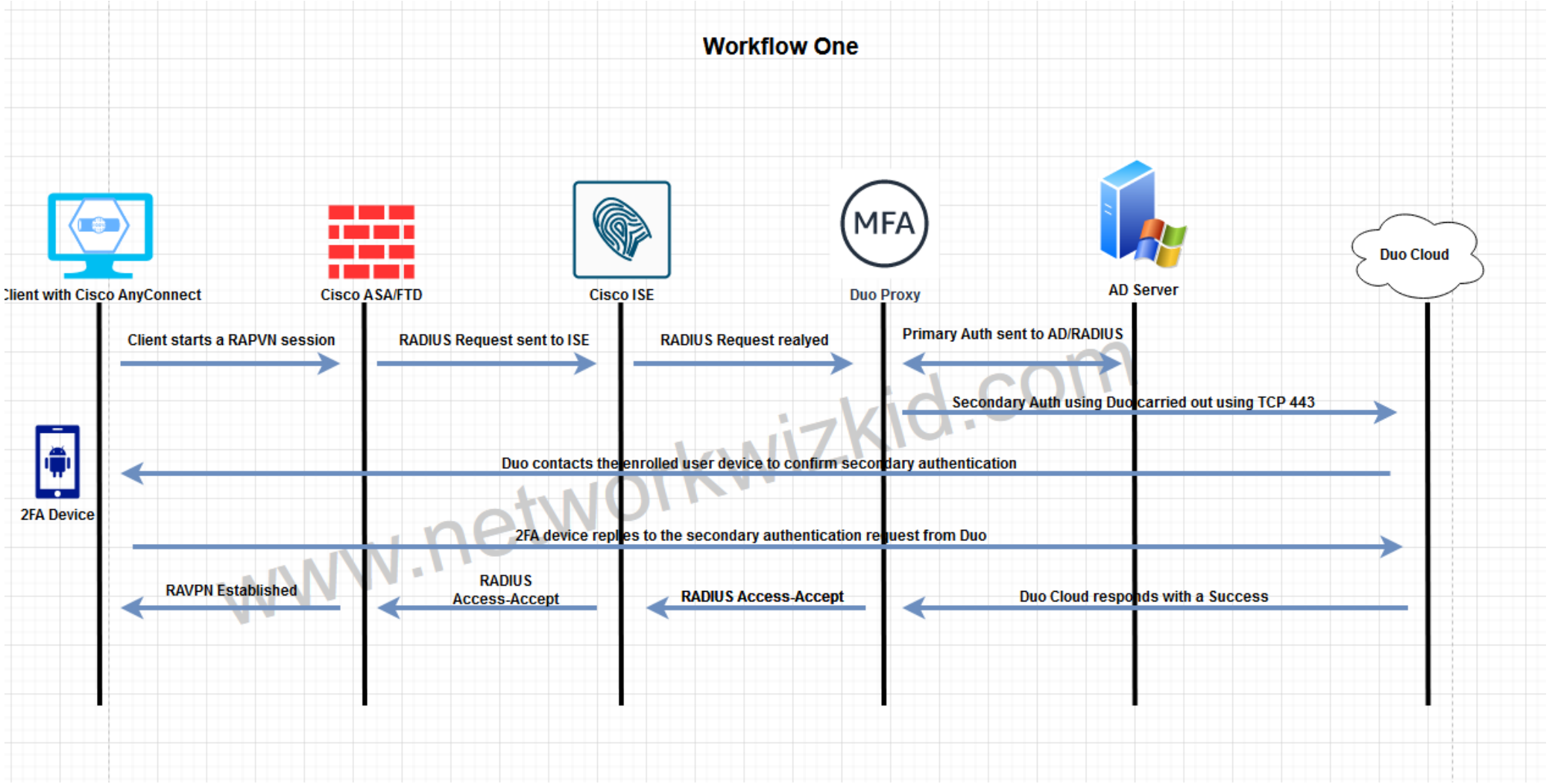
#NetworkWizkids



Considerations

- This setup can be achieved in a few different ways:
  - Client > ASA/FTD > ISE > Authentication Proxy > AD/RADIUS Server > Duo > Authentication Proxy > ISE > ASA/FTD > Client
  - Client > ASA/FTD > Authentication Proxy > ISE > AD Server > Duo > Authentication Proxy > ASA/FTD > Client
  - Client > ASA/FTD > ISE > AD Server >> ASA/FTD > Authentication Proxy > Duo > ASA/FTD > Client
  - LDAP also available and DAG **(Note: DAG going away)**

Workflow One



Workflow One Benefits

- Allows the use of profiling and posturing within ISE
- CoA still functions as normal
- Benefits existing environments where you want to bolt-on Duo 2FA
- DACL's, SGT's, VLANs and other RADIUS Attributes can still be used
- Unenrolled users can be prompted to enroll

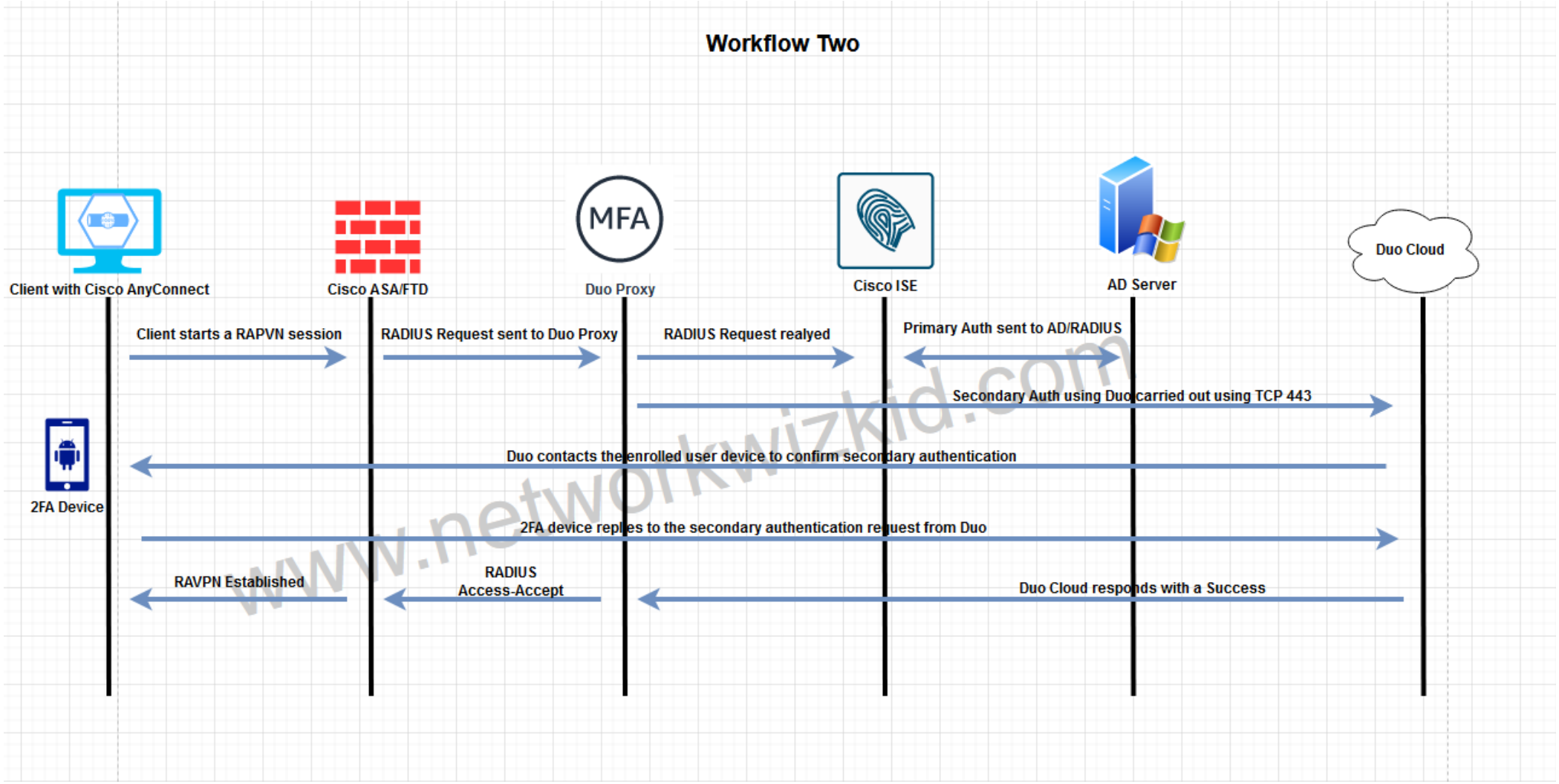
Workflow One Considerations

- Latency could be added depending on where Auth proxy and ISE are located
- MS-CHAP not supported by the auth proxy. Therefore, users won't be able to change their AD passwords through AnyConnect if/when they expire
- Worth designing for HA with ISE nodes and Auth proxies
- Look at failover capabilities if ISE fails or the Duo auth proxy fails

Workflow One Configuration Steps

1. Configure the ASA for RA VPN
2. Configure the Cisco RADIUS VPN application in the Duo Admin panel
3. Download, install and configure the authentication proxy
4. Configure Cisco ISE
    1. Add the ASA as a network device with the correct shared secret with the ASA
    2. Configure Duo as a RADIUS token external identity source. The shared secret needs to match the one configured in the auth proxy
    3. Create a RADIUS source sequence for Duo and AD source
    4. Create a policy set for RA VPN users
5. Test the new 2FA workflow

Workflow Two



Workflow Two Benefits

- Supports MSCHAP so users can change their passwords
- RADIUS attributes such as SGT's can be used
- As there is two separate auth flows, the only thing that needs to be added to ISE is the IP address and shared secret of the auth proxy
- Unrolled users will be promoted to enroll by HTTPS

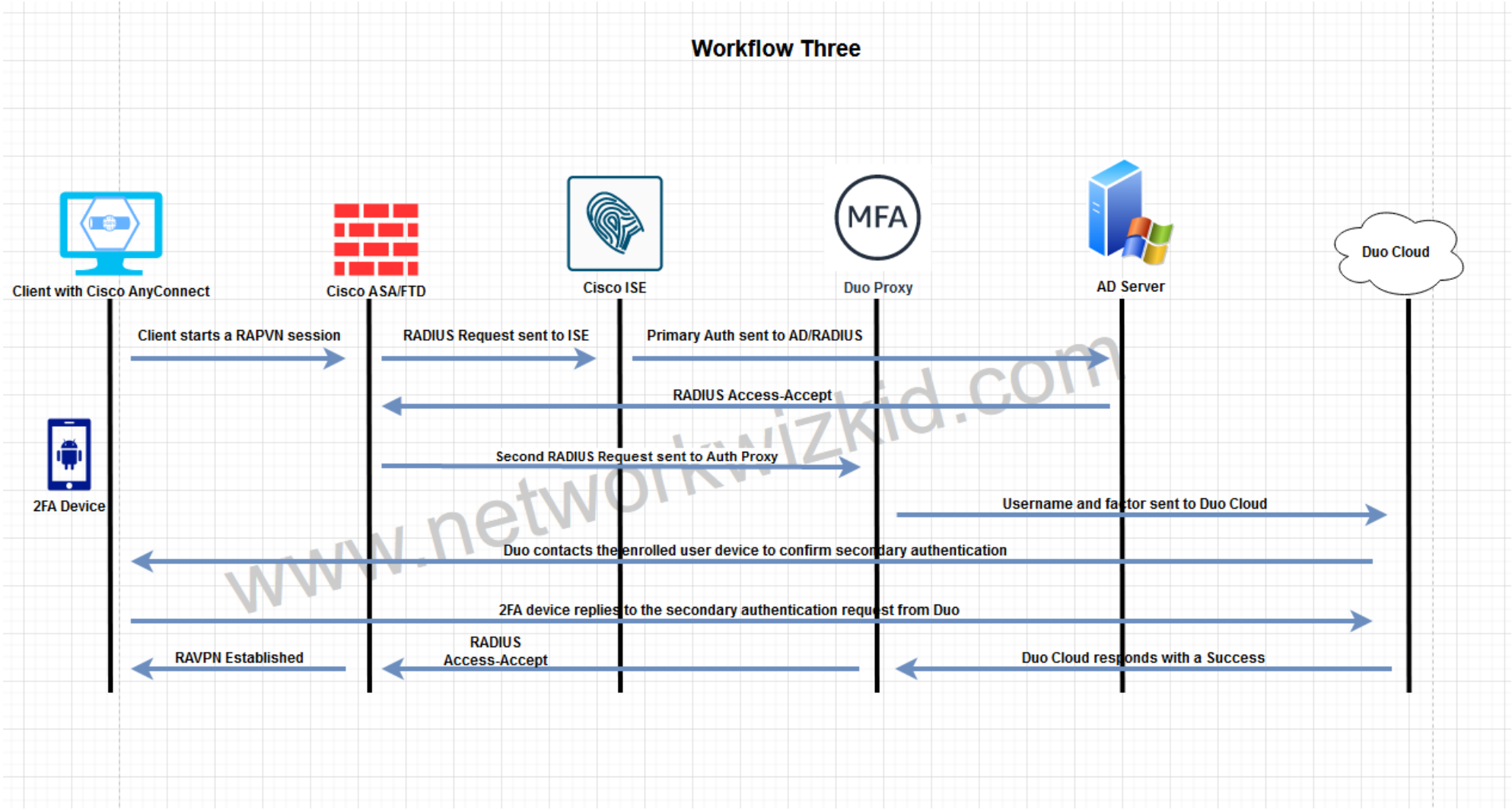
Workflow Two Considerations

- Firewall RADIUS configuration needs to change to point to the auth proxy
- Profiling and posturing on ISE won’t work as the auth proxy doesn’t support CoA
- DACL’s can’t be used
- Latency could still be an issue depending on location of devices
- HA and failover considerations still count with this workflow

Workflow Two Configuration Steps

1. Configure the ASA for RA VPN
2. Configure the Cisco RADIUS VPN application in the Duo Admin panel
3. Download, install and configure the authentication proxy
4. Configure Cisco ISE
    1. Add the auth proxy as a network device with the correct shared secret with the ASA
    2. Create a RADIUS source sequence for the AD source
    3. Create a policy set for RA VPN users
5. Test the new 2FA workflow

Workflow Three



Workflow Three Benefits

- No additional configuration required on ISE if already configured
- Only an additional authentication server needs to be added to the tunnel-group on the firewall (Auth proxy)
- RADIUS attributes supported (SGT’s, DACLs etc)
- Profiling and posturing is supported
- RADIUS requests are not chained as there are two separate authentication flows

Workflow Three Considerations

- MSCHAP is not possible as Password-Management cannot be separated for both auth flows
- No support for unenrolled users
- HA and failover considerations still count with this workflow

Workflow Three Configuration Steps

1. Configure the ASA for RA VPN
    1. Add ISE and Auth Proxy IP's as RADIUS servers
2. Configure the Cisco RADIUS VPN application in the Duo Admin panel
3. Download, install and configure the authentication proxy
4. Configure Cisco ISE
    1. Add the ASA as a network device with the correct shared secret with the ASA
    2. Create a RADIUS source sequence for the AD source
    3. Create a policy set for RA VPN users
5. Test the new 2FA workflow

Demonstration

Useful Links

- www.youtube.com/networkwiizkiids
- www.networkwizkid.com
- www.twitter.com/iwiizkiid
- https://community.cisco.com/t5/security-documents/duo-integration-options-for-cisco-anyconnect-vpn-with-asa-and/ta-p/4114832
- https://duo.com/docs/cisco