Project Overview

The N.C. Department of Information Technology is updating the N.C. Identity Management (NCID) service through the Citizen Identity Project. This involves enhancing security, improving self-service and moving external user identities from the department's on-prem infrastructure to a modern cloud-based service. Additional details and timeline information can be found at: https://it.nc.gov/support/ncid/ncid-citizen-identity-project

HTTP Proxy Integration Overview

Currently when a user accesses an application URL which is configured as a protected resource on NCID's HTTP Proxy Server, the user is directed to a login page and the user credentials are validated against NCID eDirectory. Upon successful validation, the user is directed to the application page. At cutover, the configuration changes on NetIQ will perform authentication for internal users against NCID directory and external users against Simeio-Ping directory. Applications will need to work with Simeio such that Simeio Ping Federate is configured to protect application resources. After this, when a user accesses an application URL, the configuration changes on Simeio Ping Federate will perform authentication for internal users against NCID directory and external users against Simeio-Ping directory.

Definitions

- **Cutover:** At this point in time, all External identities would be migrated from NCID eDirectory to Simeio-Ping Directory in Production.
- **Co-existence phase:** This will be the phase when the new Simeio-hosted systems are available for external users' registration and self-service, but application integration with Simeio systems is not yet complete.
- **External user identities:** Individual user accounts and Business user accounts
- **Internal user identities:** State employee user accounts and Local Govt employee user accounts
- **NCID eDirectory:** It is a repository that currently stores internal and external user identities. After successful migration to Simeio, NCID eDirectory will act as the source of truth for all identity attributes associated with the internal user's profile.
- **NetIQ AM:** NetIQ Access Manager.
- **Ping Directory:** It is an LDAP repository that stores the external user identities. It will act as the source of truth for all identity attributes associated with the external user's profile.
- **Ping Federate:** It is a federation server that enables external user authentication and Single Sign-On for applications (**HTTP Proxy & SAML Apps**). It delegates authentication of internal users to **NetIQ AM** (1FA) and **Azure AD** (MFA).
- **Ping One:** It provides Multi-Factor Authentication (MFA) for external users.

Application User Impact after Cutover

1) For New User Registration for NCID Account and for Self-Service options (Forgot Username, Forgot Password, Unlock Account)
   - External Users (Individual Users and Business Users): They would go to https://myncid.nc.gov.
   - Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.
2) Application access flow: No change.

Application Admin Impact after Cutover

1) Role Assignment:
   - To manually assign a role to External users (Individual Users and Business Users): They would go to https://myncid.nc.gov.
   - To manually assign a role to Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.
   - To programmatically assign a role to External or Internal users through Web Service Integration: No change.

2) App Membership Report:
   - To view the report for External users (Individual Users and Business Users): They would go to https://myncid.nc.gov
   - To view the report for Internal Users (State Employee Users and Local Govt Employee Users): No change. They would continue to go to https://ncid.nc.gov.

Preparing for Cutover

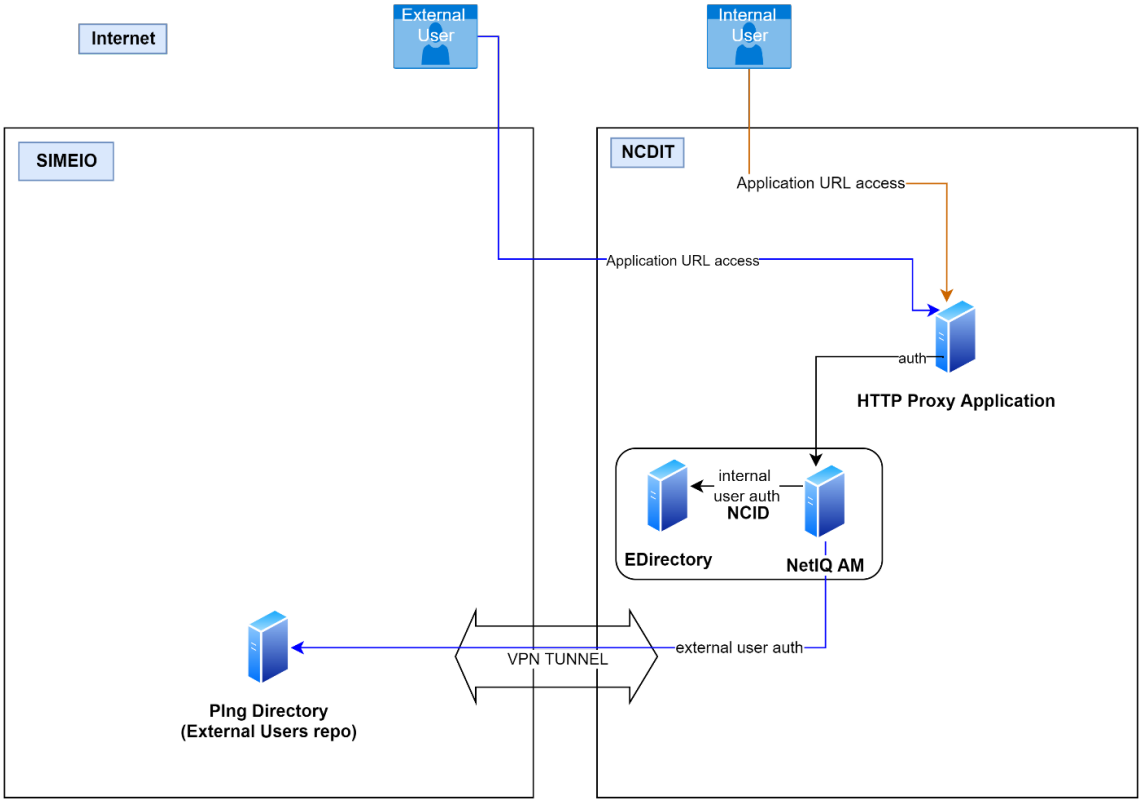
- **NCID Team** will ensure that at the time of cutover, config change is in place in NETIQ to handle multiple data stores. This will ensure that it can perform authentication for internal users against NCID directory and external users against Simeio-Ping directory.

- **Simeio Team** will ensure that at the time of cutover, config change is in place in Simeio Access Manager to handle multiple data stores. This will ensure that it can perform authentication for internal users against NCID directory (using NetIQ Access Manager and Azure) and external users against Simeio-Ping directory.

- **Application team** will ensure that right after cutover:
  - An existing external user (whose account was migrated from NCID to Simeio) can successfully access their application.
  - A new external user (who registered their NCID account in Simeio after cutover and was provided appropriate access to the application by the application admin) can successfully access their application.
  - If applicable, an internal user can successfully access their application.

At Cutover

At cutover, the application is still with NCID. Applications are still using the existing HTTP Proxy Solution.



HTTP based applications Co-existence

Preparing to Migrate applications to Simeio

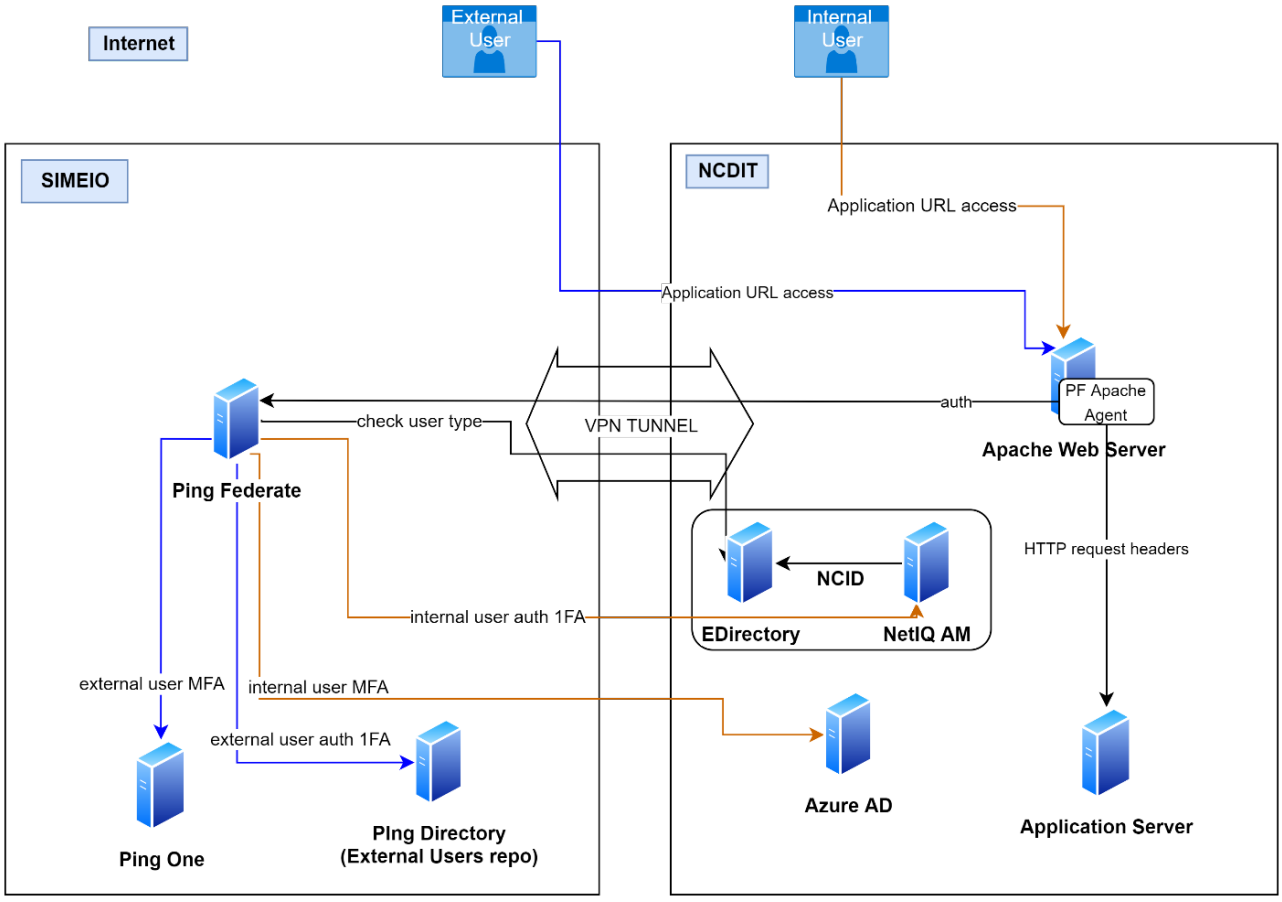
- **NCID Team** to build new HTTP Proxy servers for non-prod & prod environment.
- **Simeio Team** to work with NCID team to install Apache, agent, configure it with Simeio Ping Federate to protect resources. Work with the application team to do the required application specific configuration.
- **Application Team** will need to work with NCID & Simeio Team to provide the URLs, resources to protect, HTTP header variables required by the application. They will have to coordinate for the DNS cut over and perform functional testing as well.

After Application Migration

- **NCID Team** will disable the configuration on the old HTTP Proxy servers, after the application is migrated over to Simeio.

User Login Flow after Migration

- A user attempts to access a resource on the Apache server protected by the PingFederate Apache Agent.
  - The user is redirected to the PingFederate server for authentication if a session does not exist.
  - If the session already exists, the user is granted immediate access.
- PingFederate checks the user type
  - For internal users, the PingFederate server redirects the user's browser to NetIQ (1FA) or Azure AD (MFA) for authentication using the SAML protocol. The IdP partner authenticates the user and returns a SAML assertion. PingFederate validates the assertion and creates a session for the user including any configured attributes. PingFederate then redirects the browser, including the session, back to the Apache Agent.
  - For external users, the PingFederate authenticates the user against Ping Directory (1FA) or Ping One (MFA). PingFederate creates a session for the user including any configured attributes. PingFederate then redirects the browser, including the session, back to the Apache Agent.
- The Apache Agent verifies the session and grants access to the protected resource, as appropriate. The User ID and any attributes from the session are exposed to the resource as HTTP request headers or Apache environment variables.



HTTP-Proxy based applications - final state