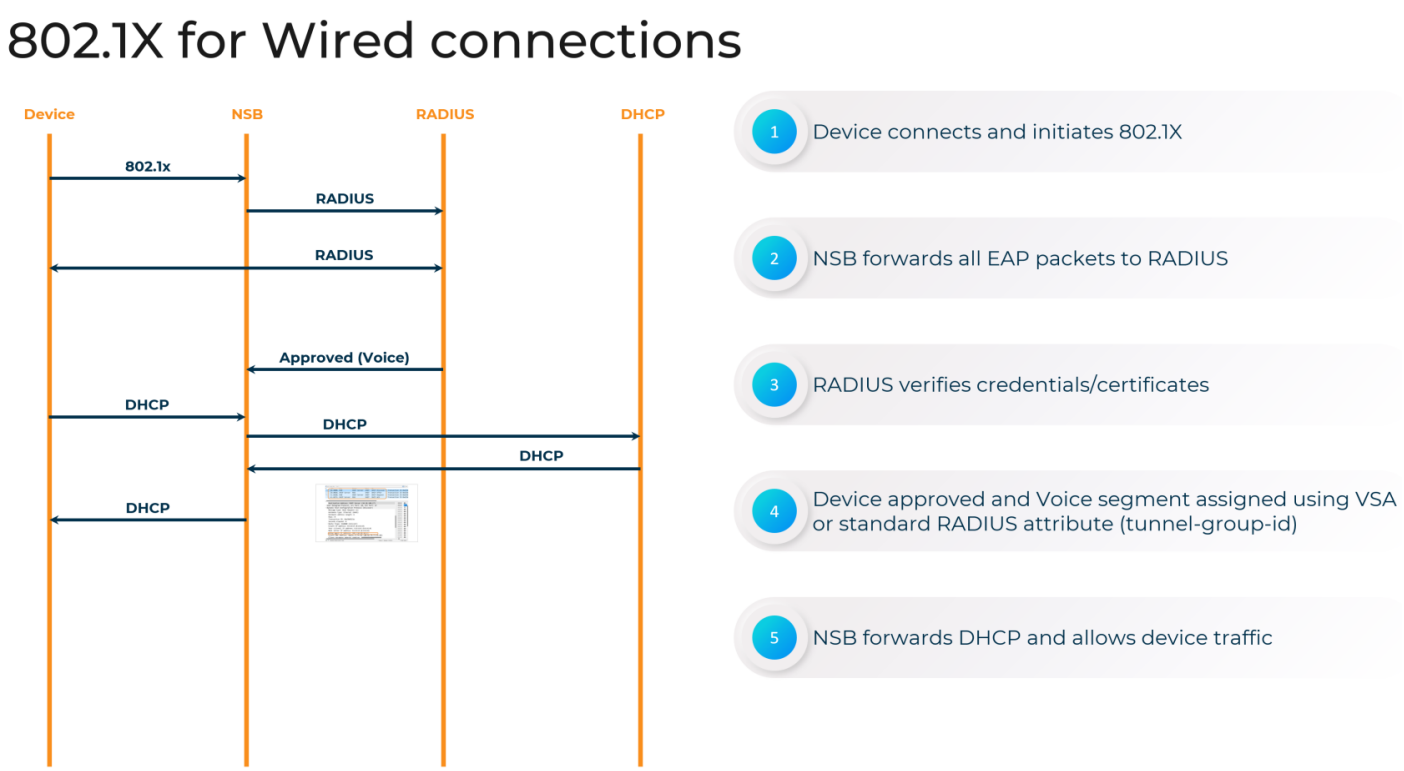
Zero Trust Access 802.1x

Overview

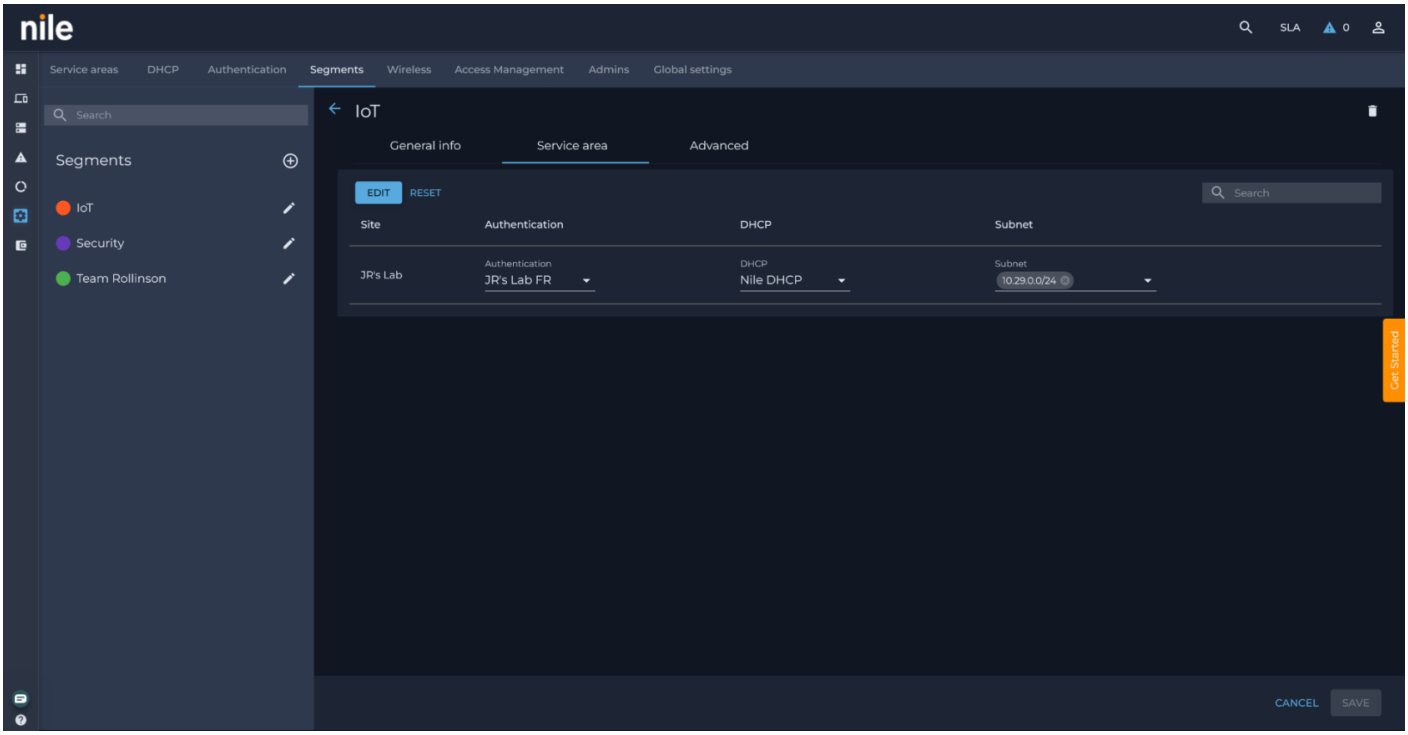
Nile's Campus Zero Trust approach to network security is essential in today's high risk environment. Nile's support for industry-standard 802.1X authentication enables you to enforce consistent access controls and policies across your wired and wireless campus networks, ensuring only authorized devices and users can connect.

By integrating with your existing RADIUS infrastructure, such as Active Directory, to authenticate clients The Nile Access Service ensures only authorized devices and users can access network resources. In the Campus Zero Trust architecture, devices are denied access by default, and can only access resources through one of the supporteed authentication methods, including 802.1x. This streamlines the onboarding process and ensures a seamless user experience, all while maintaining a strong security posture.



Configuring 802.1X Authentication on Nile
To set up 802.1X authentication on your campus zero trust network with Nile, follow these steps:

1. Configure RADIUS Servers
    - In the Nile Portal, navigate to "Settings>Authentication" tab and click "Add".
    - Enter the details for your RADIUS server, including the Name, port, shared secret, the Geo Scope which it supports, nad the IP address or FQDN. I
    - Click the "VERIFY HOSTS" button to confirm your settings. If everything passes, you can then save this server configuration.
2. Enable 802.1X on a Nile Segment
    - Go to Settings>Segements tab. section, click the pencil icon to edit your chosen segment.
    - In the segment details, navigate to the Service Area tab.
    - Select the RADIUS server you just configured in the Authentication dropdown.
    - Click SAVE to immediately enable 802.1x on that segment.



Supporting Non-802.1X Devices in a Campus Zero Trust Network

Nile understands that not every device on your network will support 802.1X. For these non-802.1X-capable clients, Nile offers MAC Authentication Bypass; learn more.

Shiv> I forgot about this. We need to upload the NIle dictionary file here. This file is uploaded in the RADIUS server and is used to send us back the segment name as a Vendor specific attribute.

Dynamic Segment Assignment with Nile Dictionary

The Nile Access Service supports dynamic segment assignment based on user and device attributes received from external RADIUS servers, such as Cisco Identity Services Engine (ISE) and Aruba ClearPass. To facilitate this, Nile provides a custom dictionary file that can be uploaded to the RADIUS servers.

When a user or device authenticates to the Nile Access Service using 802.1X, the RADIUS server can send the "netseg" attribute during the authentication process. This attribute informs the Nile Access Service which network segment the user or device should be assigned to.

Example Use Case: Single SSID for Teachers and Students

Shiv provided the following example use case:

- The SSID "Univ of Den" is used by both teachers and students.
- Teachers belong to the "teacher" segment, while students belong to the "student" segment.
- The RADIUS server is configured to send the "netseg" attribute during the 802.1X authentication process.
- The RADIUS server sends "netseg=teacher" when a teacher authenticates, and "netseg=student" when a student authenticates.
- The segment names sent by the RADIUS server must exactly match (case-sensitive) the segment names configured in the Nile Access Service.

Configuring Dynamic Segment Assignment

To configure dynamic segment assignment using the Nile dictionary file, follow these steps:

- **Obtain the Nile Dictionary File**: Contact Nile support or your account representative to obtain the Nile dictionary file. This file contains the necessary vendor-specific attributes (VSAs) used for dynamic segment assignment.
- **Upload the Nile Dictionary to the RADIUS Server**: Depending on the RADIUS server you're using (Cisco ISE or Aruba ClearPass), follow the instructions in the respective guides:
  - Integrating Cisco ISE with the Nile Access Service for Dynamic Segment Assignment
  - Integrating Aruba ClearPass with the Nile Access Service for Dynamic Segment Assignment
- **Configure the RADIUS Server to Send the "netseg" Attribute**: Ensure that your RADIUS server is set up to send the "netseg" attribute during the 802.1X authentication process. The attribute value should match the segment names configured in the Nile Access Service.

- **Configure Segments in the Nile Customer Portal**: In the "Settings" > "Segments" section of the Nile Customer Portal, create the necessary network segments that correspond to the "netseg" attribute values received from the RADIUS server (e.g., "teacher" and "student" segments).
- **Associate Segments with 802.1X Authentication**: When configuring 802.1X authentication in the "Settings" > "Segments" section, select the RADIUS server you've set up and enable dynamic segment assignment. The Nile Access Service will then automatically place users and devices in the appropriate network segments based on the "netseg" attribute received from the RADIUS server.

By leveraging dynamic segment assignment with the Nile-provided dictionary file, organizations can achieve a higher level of granular access control, ensuring that users and devices are consistently placed in the correct network segments based on their identity, device type, and location. This enhances the overall security of the campus zero trust network by reducing the risk of unauthorized access and lateral movement.

Unique Passphrase (UPSK) with SSO ~~External RADIUS~~

The Nile Access Service supports the integration of Unique Passphrase (UPSK) with external RADIUS servers, such as Cisco ISE and Aruba ClearPass. UPSK enhances the security of traditional pre-shared key (PSK) wireless networks by assigning a unique passphrase to each authenticated user, rather than a single shared key.

To configure UPSK with an external RADIUS server in the Nile Access Service, follow these steps:

- **Configure the SSO Provider**
  - ??
- **Create a UPSK-enabled SSID in the Nile Customer Portal**:
  - Navigate to the "Settings" > "Wireless" page in the Nile Customer Portal.
  - Select the "Personal" SSID type and enable the "Enable SSO" option.
  - Enter a pre-shared key and select the network segments accessible via this SSID.
- **Configure the RADIUS Integration in the Nile Customer Portal**:
  - Go to the "Settings" > "Authentication" page and add the external RADIUS server details, including the name, IP address or FQDN, port, and shared secret.
  - Verify the RADIUS server connection by clicking the "Verify Hosts" button.
  - In the "Segments" section, edit the segment associated with the UPSK-enabled SSID and select the RADIUS server you just configured.
- **Provide Users with the UPSK Registration Link**:
  - Instruct users to visit the my.nilesecure.com website or use the unique registration link provided in the Nile Customer Portal.
  - Users will be prompted to authenticate using your organization's identity provider (IdP), which should be integrated with the external RADIUS server.

    - After successful authentication, users can generate a unique passphrase for their device to connect to the UPSK-enabled SSID.

By integrating UPSK with an external RADIUS server, you can leverage your existing identity management infrastructure to provide secure wireless access, while still benefiting from the enhanced security and user-specific credentials offered by the Nile Access Service's UPSK feature.

Centralized Management and Visibility

Nile's cloud-managed architecture provides a simple path for 802.1X deployment. This includes the ability to:

- Easily onboard and manage primary, secondary and tertiary RADIUS servers for redundancy and segmentation
    - Shiv> We should point out how redundancy works
        - Its a primary, secondary, tertiary model. So only if primary faiils we send it to secondary and if secondary fails we send it to tertiary. I will find out what happens if primary comes online.
- Track authentication events and client activity across your wired and wireless networks
- Quickly troubleshoot connectivity issues with detailed logs and reporting

(Screenshot of the Nile Portal's 802.1X monitoring and reporting dashboard)

By leveraging Nile's 802.1X capabilities, you can establish a robust, campus zero trust network that securely connects all devices and users, regardless of their location or device type.

Contact us today to learn more about how Nile can help secure your campus environment.

Read Next

Single Sign-On (SSO)

Revision #9
Created 20 March 2024 18:20:59 by JR
Updated 28 March 2024 21:53:20 by JR