

Overview of Universal ZTNA Configuration

This section describes the universal ZTNA configuration workflow.

- Configuring Universal ZTNA Solutions, on page 1

Configuring Universal ZTNA Solutions

As an administrator, set up the infrastructure, configure policies, deploy those policies at the enforcement point, and monitor the solution to ensure it works as expected. This section provides a high-level overview of the universal ZTNA configuration process.

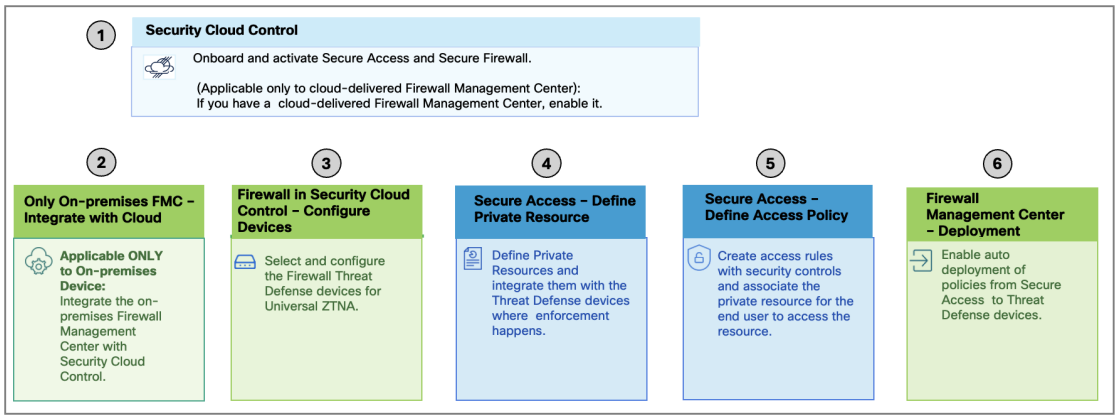
Summary

The configuration process involves the following key components and platforms:

- Security Cloud Control: Used for platform management, subscription claiming, and Firewall Management Center integration.
- Secure Access: Used for user management, trusted network configuration, and private resource definition.
- Firewall Management Center and Firewall Threat Defense, version 7.7.10 or later: Used for configuration deployment and policy enforcement.
- Secure Client: Used on remote user devices to enable zero trust access.

Workflow

Figure 1: Workflow to Set Up Universal ZTNA



These stages describe the configuration workflow for the universal ZTNA solution.

1. Onboard Security Cloud Control Firewall Management and Secure Access to the Security Cloud Control platform.
   - Claim a subscription and provision Secure Access and Security Cloud Control Firewall Management.
   - Configure user management in Secure Access manually or via an identity provider.
   - Configure trusted networks through Secure Access.
   - Update Secure Access with the CA certificate for the ZTNA user.
2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices.
   - Enable cloud-delivered Firewall Management Center or onboard an on-premises Firewall Management Center to Security Cloud Control.
   - Register smart licenses and specify routed interfaces, platform settings, and DNS for Firewall Threat Defense devices.
3. Configure the Threat Defense devices for universal ZTNA in Security Cloud Control.
   - Specify device FQDN, interfaces, and PKCS12 certificate.
   - Deploy changes.

     If your Firewall Management Center and Firewall Threat Defense devices run versions 7.7 and 10.0: After the changes are deployed, the devices reboot to reallocate system resources. Rebooting takes several minutes. If you deploy a High Availability (HA) pair of devices, both devices reboot simultaneously, interrupting traffic flow.

     If your Firewall Management Center and Firewall Threat Defense devices run versions10.1 and later: After the changes are deployed, the devices do *not* reboot.
4. Configure private resources in Secure Access.

   Private resources include applications, networks, or subnets your organization controls. They are not publicly accessible from outside your network.

Define private resources and specify connection information for the resources.

5. Create access policy rules and associate them with the private resources.

   Configure access rules to determine which users and devices can access the resource using the enabled connection methods.

6. Associate the private resources with the Threat Defense device.

   Verify that all configurations from Secure Access are synchronized with the Threat Defense devices.

7. Configure Secure Client for universal ZTNA.

   - Install Secure Client version 5.1.10 or later on remote user devices.
   - Enroll the user with Secure Access and enable zero trust access.

Result

After deployment, monitor logs and events on both the Secure Access and Firewall Management Center dashboards to analyze and troubleshoot issues.

For configuration details, refer to the Universal Zero Trust Access Configuration Guide and the Secure Client Administration Guide.