

Universal Zero Trust Network Access

The following topics provide an overview of Universal Zero Trust Network Access (universal ZTNA), including the prerequisites, limitations, and workflow involved in configuring the universal ZTNA solution.

- Overview of Universal Zero Trust Network Access, on page 1
- Prerequisites for Universal Zero Trust Network Access, on page 2
- Limitations of Universal Zero Trust Network Access, on page 4
- Configuration Workflow for Universal ZTNA, on page 4

Overview of Universal Zero Trust Network Access

Universal Zero Trust Network Access (universal ZTNA) enables administrators to specifically allow access to internal network resources according to user identity including user trust and posture, without granting access to the entire network as with Remote Access VPN. Universal ZTNA is a client-based ZTNA solution that enables users to securely access internal resources and applications regardless of their location, whether remote or on-premises.

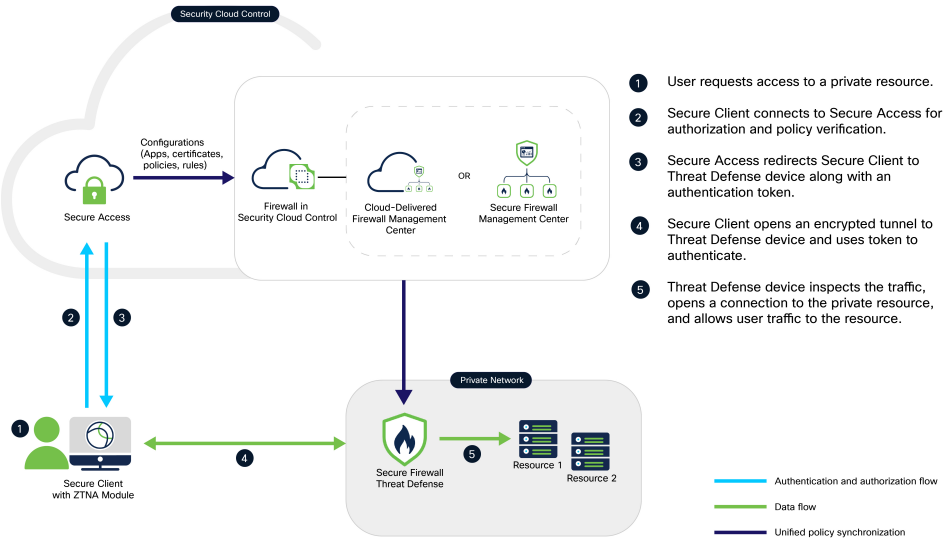
Because universal ZTNA does not assume that access granted to one application implicitly authorizes access to other applications, the network attack surface is reduced.

Universal ZTNA ensures least-privileged, per-application, per-user access with strong authentication, posture validation, and comprehensive traffic inspection. It secures applications effectively across hybrid environments.

Components of Universal ZTNA

A new configuration of universal ZTNA consists of Security Cloud Control Firewall Management (formerly called Cisco Defense Orchestrator), and Secure Access, both provisioned on the Security Cloud Control platform. Security Cloud Control Firewall Management manages the Firewall Threat Defense devices through the Secure Firewall Management Center.

Figure 1: Components of Universal ZTNA



- **Security Cloud Control Firewall Management**: Manages the configuration and deployment of universal ZTNA policies to the Firewall Threat Defense devices. The Threat Defense devices protect on-premises resources by enforcing universal ZTNA policies. Threat Defense inspects traffic and enforces intrusion prevention system (IPS), file, and malware policies on the traffic.
- **Secure Access**: Secure Access defines the access policies, posture, and security profiles for the user. It enforces the policies for user traffic through the cloud.
- **Security Cloud Control platform**: Security Cloud Control provides a unified secure management plane for both Secure Access and Firewall, simplifying the administration of universal ZTNA policies across them.
- **Secure Client**: The Secure Client is installed on the end user's device. It acts as the enforcement point that intercepts connection requests to protected internal resources, enabling secure, identity-based access.

Prerequisites for Universal Zero Trust Network Access

This topic discusses requirements and guidelines for Universal Zero Trust Network Access (universal ZTNA).

Licensing Requirements

- Secure Firewall Management Center requires a smart license account with export-controlled features. It does not function in evaluation mode for universal ZTNA.

  Secure Firewall Threat Defense devices require an IPS license if Intrusion policy is configured. If Malware policies are configured, the devices require IPS and Malware Defense licenses. For more information, refer to the "Licenses" section in the *Cisco Secure Firewall Management Center Administration Guide*.

- Secure Access requires a subscription of Cisco Secure Private Access Essentials or Advantage.

Device Requirements

- All Secure Firewall Management Center and Secure Firewall Threat Defense devices must be running Version 7.7.10 or later.
- All Secure Firewall Threat Defense devices must be configured for routed mode; transparent mode is not supported.
- In Security Cloud Control, when you are configuring universal zero trust access for a device, ensure that the Enrollment Type for the device identity certificate is an object that is created using the PKCS12 file format. No other certificate type is supported. If necessary, you can also create a new certificate object from Security Cloud Control, which supports the PKCS12 format. See Configure Security Devices.
- Configure the Domain Name System (DNS) to resolve Fully Qualified Domain Name (FQDN) of private resources. Use the Platform Settings menu on the Secure Firewall to configure the DNS. See Interface and Device Settings.
- High Availability (HA) devices *are* supported; they are displayed as one entity.
- Secure Client (with ZTNA module enabled) Version 5.1.10 and later is supported.

  The client must be running in a platform that supports Trusted Platform Module (TPM), such as Windows 11.

Guidelines on Certificate Types

- **User Device Identity Certificate**: Secure Client, which is zero trust access enabled, presents the user identity certificate during the Mutual Transport Layer Security (mTLS) session with Secure Access and Firewall Threat Defense to request access to private resources.
- **Firewall Threat Defense Device Certificate**: Threat Defense devices that are universal ZTNA-enabled use device certificates to establish secure mTLS connections with the Secure Client and Secure Access. Ensure that the device identity certificate is of type PKCS12.

  If you have already enrolled a manual certificate for the device, first export it to the PKCS12 format using the **Devices** > **Certificates** > **Export Certificate** menu on Firewall Management Center. Use the exported PKCS12 file to create a new PKCS12 certificate enrollment object.
- **Decryption Certificate**: (Optional) To decrypt the traffic that is sent to private resources, enable **Decryption** for the resources in Secure Access and provide the server certificate and key. We recommend that you use a certificate that is signed by a publicly recognized certificate authority (CA).

Supported Devices

Both on-premises Firewall Management Center and cloud-delivered Firewall Management Center can be configured to manage the devices.

Only devices that have 16 cores or more are supported. Such models of Secure Firewall Threat Defense are:

- 1150
- 3105, 3110, 3120, 3130, 3140
- 4115, 4125, 4145, 4112
- 4215, 4225, 4245

- FTDv

Limitations of Universal Zero Trust Network Access

- Universal ZTNA does not support IPv6.
- Universal ZTNA-enabled devices do not enforce policies for traffic over a site-to-site tunnel.
- Universal ZTNA does not support clustered devices.
- Universal ZTNA does not support devices in multi-instance mode.
- Universal ZTNA sessions do not support jumbo frames.
- Currently, universal ZTNA supports only the United States and Europe regions.
- Universal ZTNA supports only global VRF.
- Universal ZTNA does not support protocols such as FTP or TFP, where the data or secondary connection originates from a server.

  For example, an active FTP connection uses a persistent control connection for commands and creates temporary data connections for file transfers. Universal ZTNA does not support such data connections that originate from the server.

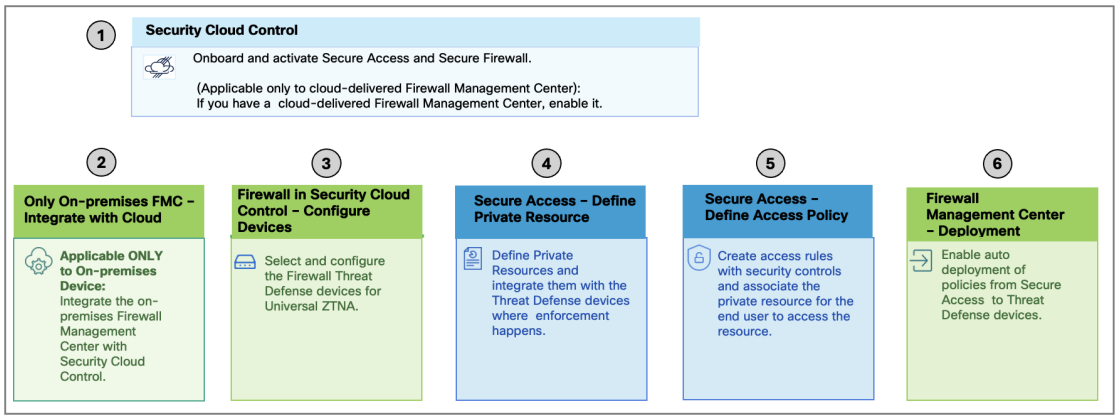
Configuration Workflow for Universal ZTNA

As an administrator, you set up the infrastructure, configure policies, deploy policies at the enforcement point, and monitor the solution to ensure it works as expected. These tasks can be classified by the product used:

- Configure Security Cloud Control Firewall Management, which includes setting up the Threat Defense devices with their Management Center.
- Configure Secure Access, which includes private resources, access policies, and network connections.

The steps described in the figure provide a high-level overview of the universal ZTNA configuration process. For detailed instructions, see the specific tasks.

Figure 2: Configuration Workflow for Universal ZTNA



Workflow

1. Onboard Secure Access and Security Cloud Control Firewall Management to the Security Cloud Control platform.

   See Onboard Applications in Security Cloud Control.

2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices to enable universal ZTNA.

   See Set Up Firewall Threat Defense Devices.

3. Configure the Firewall Threat Defense devices.

   Enable **universal zero trust network access settings** for the Firewall Threat Defense device and ensure that the Threat Defense device is visible in Secure Access.

   See Configure Security Devices.

4. Configure private resources.

   Private resources include applications, networks, or subnets that your organization controls.

   In Secure Access, configure private resources to specify the connection information for the resources.

   See Configure Private Resources.

5. Define the access policies for user traffic.

   In Secure Access, add private access rules to control access and enforce security for private resources in the organization. The access rules determine which users and devices can access the resource using the connection methods you have enabled.

   See Configure Universal ZTNA Access Policies.

6. Deploy the configurations to the Firewall Threat Defense Device.

   In Secure Access, associate the private resources to the Threat Defense device and ensure that all configurations are synchronized with the Threat Defense device.

   See Associate Private Resources to Threat Defense Device.

Note that after you provision the applications in Security Cloud Control (Step 1 and Step 2), you can use the **Secure Access** > **Workflows** > **Set up hybrid private access** workflow to continue with the universal ZTNA configuration process.