

Deployment of Universal ZTNA solution

Universal ZTNA provides a secure and controlled way to access applications based on zero trust principles. An administrator workflow includes setting up the infrastructure (onboarding Secure Access and Firewall to Security Cloud Control), configuring policies on Secure Access, deploying those policies to the enforcement point (Threat Defense devices), and monitoring the solution to ensure it is working as expected.

An administrator can deploy the universal ZTNA solution to achieve the following outcomes:

- Optimal path for traffic based on the user location
- Private inspection for sensitive applications

- Outcome 1: Optimal path for user traffic , on page 1
- Outcome 2: Private inspection for sensitive applications, on page 5
- Configuration workflow, on page 7
- Monitoring events, on page 19

Outcome 1: Optimal path for user traffic

Universal ZTNA uses the trusted network detection (TND) mechanism to detect whether a user is inside a trusted network (on-premises) or in an untrusted network (remote). Based on this location, universal ZTNA dynamically steers user traffic through the nearest enforcement point, ensuring security and optimal performance.

On-premises users: When a user logs in through the office network, user traffic is routed through the local Firewall (Threat Defense device), which acts as the enforcement point. This routing prevents unnecessary traffic through the cloud, avoiding latency and optimizing network performance.

Remote users: When a user is located outside a trusted network, user traffic is proxied through the cloud-based Secure Access service, which evaluates policies and proxies traffic securely in the cloud.

Trusted Network Detection

Trusted network detection (TND) identifies if a user or device is connected to a trusted internal network, such as a corporate LAN, or to an untrusted external network, such as public Wi-Fi. TND determines the network context of a user or device before granting access to applications or resources.

Secure Access enables you to define a trusted network based on specific criteria, such as DNS server addresses, DNS domains, and trusted servers. These trusted networks are included in TND profiles, which are then updated on the Secure Client.

When a user requests access to network resources, the Secure Client installed on the user's device detects the network context of the user. It includes this network information in the access request to Secure Access. Secure Access evaluates the TND data and determines how to route the user's access request:

- If the user is on a trusted network and the TND criteria match, the access request is routed through the on-premises firewall.
- If the TND criteria do not match, Secure Access identifies the user as being on an untrusted network and fulfills the access request through the cloud.

This hybrid approach ensures secure and optimized access to private network resources.

Sample Scenario

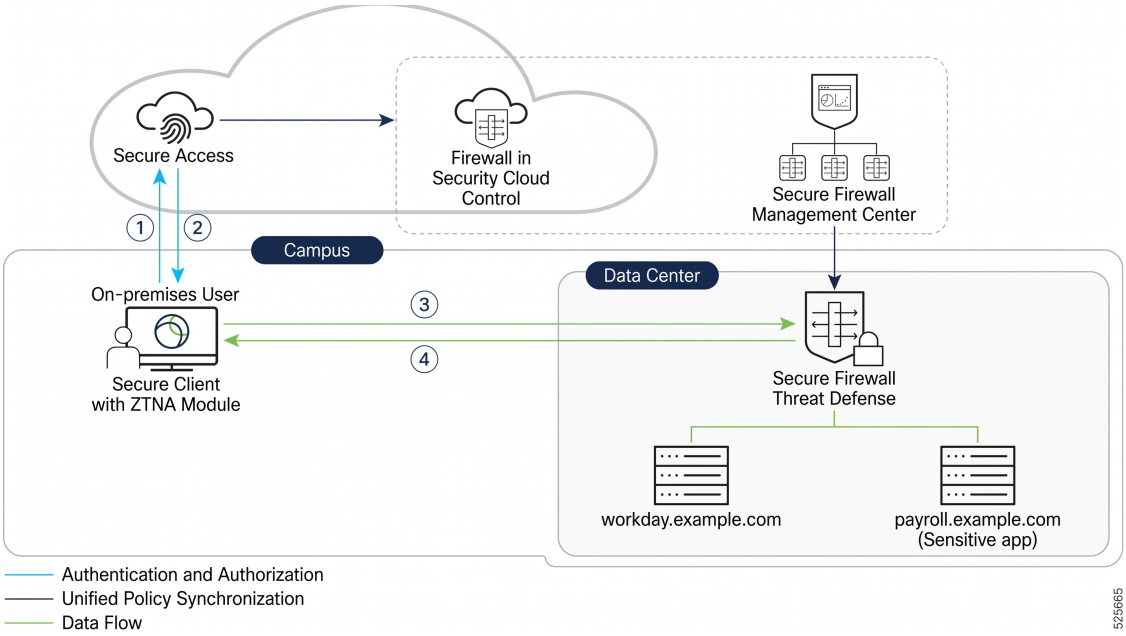
For example, Lee works from the office campus, and John works from home. When accessing HR resources such as https://workday.example.com, traffic is routed based on the user's location. For users who connect from office campus (example Lee), traffic is routed through the local Firewall (Threat Defense device)—avoiding unnecessary cloud traffic. For users who connect from outside the corporate network (example John), traffic is proxied through cloud-based Secure Access, which evaluates policies and ensures secure connectivity.

Data flow for an on-premises user

For a user operating within the private network, traffic to an internal resource is directed to the on-premises Threat Defense device, rather than being routed through the cloud.

In the sample scenario, Lee is working from the office campus and tries to access the internal resource workday.example.com through a browser.

Figure 1: Universal ZTNA Data Flow for On-Premises User



This sequence of events occurs when a user tries to access the internal resource, https://workday.example.com, from the office campus (trusted network):

- Secure Client Request: The secure client installed on Lee's laptop intercepts the connection and sends a connect request to Secure Access.
- Secure Access Policy Evaluation and Response: Secure Access evaluates the request based on the configured policies. These policies consider factors such as Lee's identity, device posture, and the application being requested. Since Lee is entitled to access this application, Secure Access authenticates Lee's credentials and authorizes the access request. It then sends a redirect message with a token as the response. Since Lee is within a trusted network, Secure Access redirects the Secure Client to the Threat Defense device.
- Secure Client Sends Access Request to Threat Defense: Secure Client sends a connect request to the Firewall Threat Defense device, providing the token and requesting access to workday.example.com.
- Firewall Threat Defense Validates and Enforces Security Profiles: Threat Defense device uses its configured DNS server to resolve the internal resource's FQDN to an IP address on the internal network. Threat Defense validates the token sent by Secure Client and responds with OK as the response. This establishes a connection between the Secure Client and the Threat Defense device. Threat Defense allows user access to https://workday.example.com and enforces security policies, such as IPS, file, and malware protection on the user traffic.

Data flow for a remote user

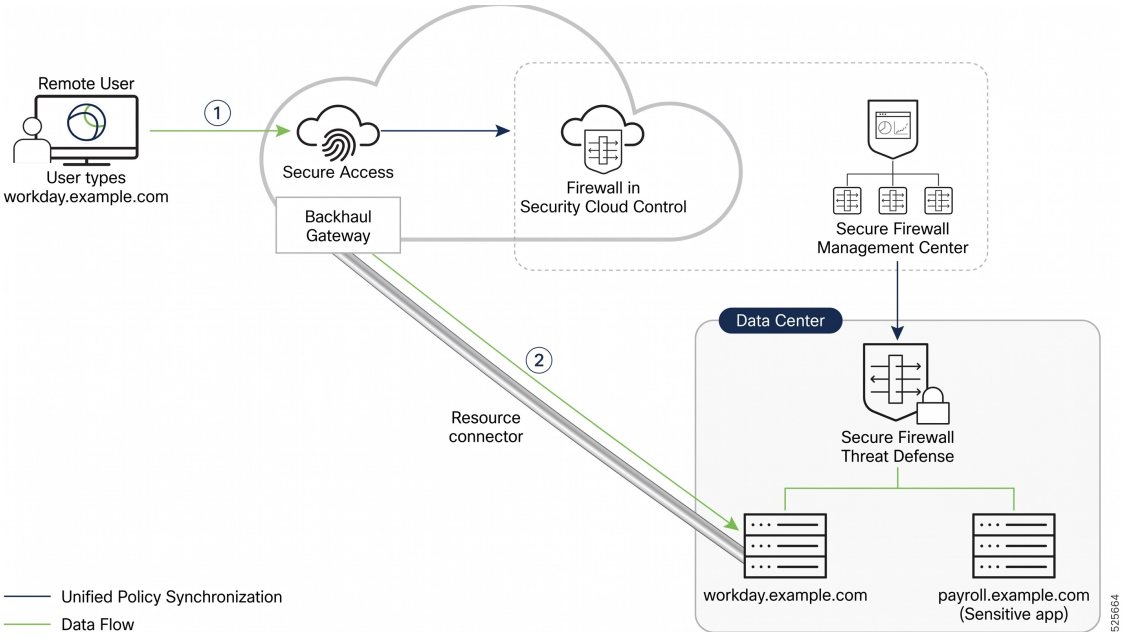
For a user operating from outside the private network, traffic to an internal private resource is directed through the cloud.

Summary

In the sample scenario, John is working from home and tries to access the internal resource workday.example.com through the browser.

Workflow

Figure 2: Universal ZTNA Data Flow for Remote User



This sequence of events occurs when John tries to access the internal resource (workday.example.com) from outside the office campus (untrusted network):

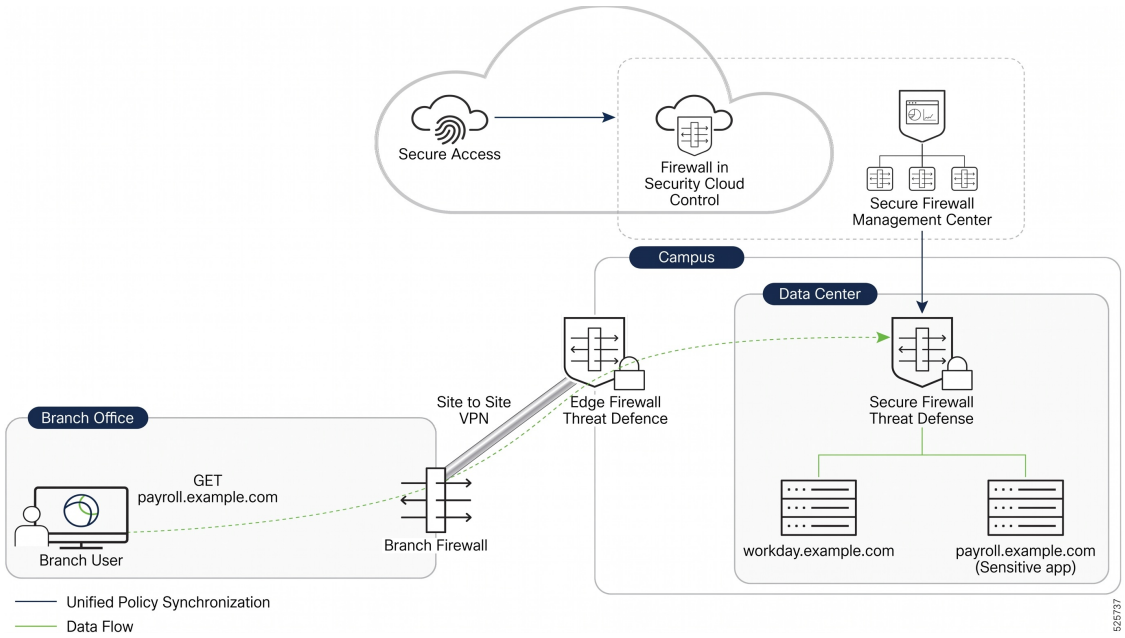
1. Secure Client intercepts the request: The Secure Client on John's system checks and finds that https://workday.example.com is a ZTNA-enabled application. It sends a connect request to Secure Access.
2. Secure Access Policy Evaluation and Response: Secure Access evaluates the policies and the user identity. Trusted Network Detection mechanism recognizes that the request has originated from an untrusted network. Secure Access Gateway establishes a connection to the Resource Connector, which then connects to workday.example.com residing on the private network.

Traffic from John's system to the private resource is routed through the Secure Access cloud.

Data flow for a branch user

In a typical enterprise network, multiple firewalls are deployed to enhance security and network segmentation. For example, a firewall at the Data Center protects private resources in a large enterprise. Branch offices are protected by branch firewalls and connect to the main campus through a site-to-site virtual private network (VPN).

Figure 3: Universal ZTNA Data Flow for a Branch User



Authentication and authorization for any universal ZTNA user occur in Secure Access. The Secure Client on the branch user's device obtains the authentication token from Secure Access and redirects the user to the Data Center firewall for access to private resources.

Data traffic from a branch user terminates at the edge firewall, which then establishes a connection with the Data Center firewall to forward the traffic.

Outcome 2: Private inspection for sensitive applications

Universal ZTNA enables private inspection of sensitive applications such as source code, and internal applications. It allows traffic destined for these applications to be inspected locally by the firewall instead of routing it through the cloud. This ensures that sensitive data remains within the trusted network perimeter and is subject to inspection policies, including Intrusion Prevention System (IPS) policies, file policies, and malware policies.

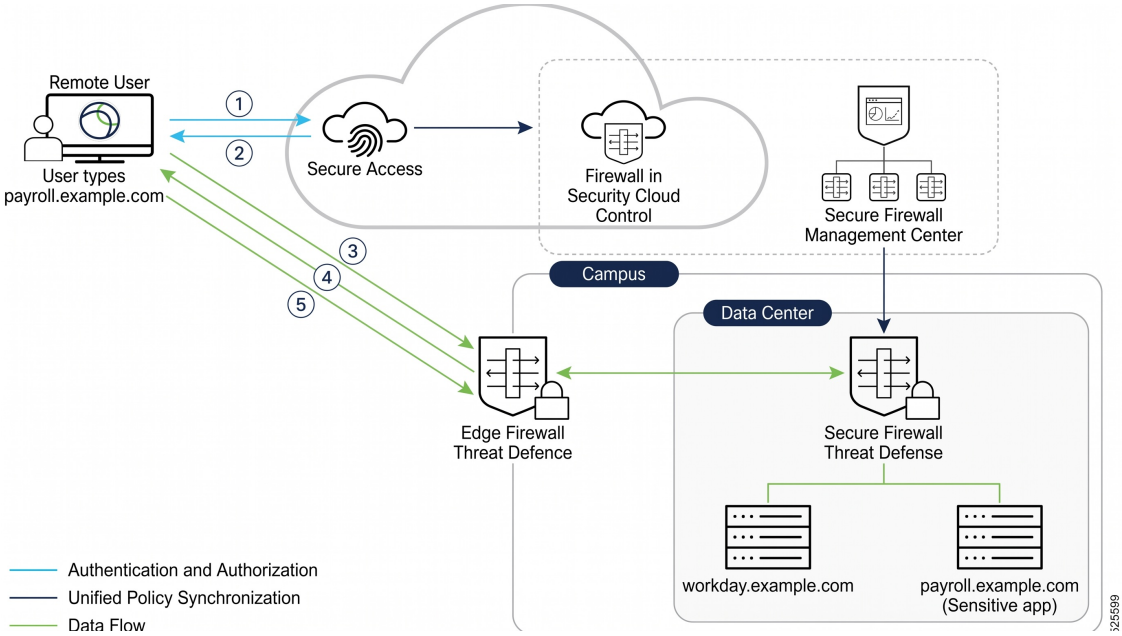
On-premises users and remote users: Traffic is routed through the local firewall (Threat Defense device), which acts as the enforcement point.

Data flow to a sensitive application from a remote user

This topic outlines the sequence of events that occur when a remote user attempts to access an internal resource from an untrusted network.

When a user operates from outside the private network, the local firewall directs user traffic to a sensitive resource. In this scenario, John works from home and tries to access the internal resource, payroll.example.com, through a browser.

Figure 4: Universal ZTNA Traffic Flow for Remote User



This is the sequence of events that happen when John tries to access the internal resource (payroll.example.com) from an untrusted network.

1. Secure Client request:

   The secure client installed on John's system intercepts the connection and sends a connect request to Secure Access.

2. Secure Access policy evaluation and response:

   Secure Access evaluates the request based on the configured policies. These policies consider factors like John's identity, device posture, and application being requested. Because John is an employee who is entitled to access payroll information, Secure Access authenticates John's credentials and authorizes the access request. It then sends a response with a token, redirecting Secure Client to the Threat Defense device.

3. Secure Client sends access request to Threat Defense device:

   Secure Client sends a connect request to the Firewall Threat Defense device, providing the token and requesting access to payroll.example.com.

4. Threat Defense device validates the request:

   The Threat Defense device uses its configured DNS server to resolve the internal resource’s FQDN to an IP address on the internal network. It validates the token sent by Secure Client and responds with "OK".

5. Threat Defense device enforces security policies:

   Threat Defense enforces the security policies, including IPS, file, and malware policies on the user traffic to payroll.example.com.

Configuration workflow

This reference provides the key steps to enable optimal path and private inspection for applications using Universal Zero Trust Access.

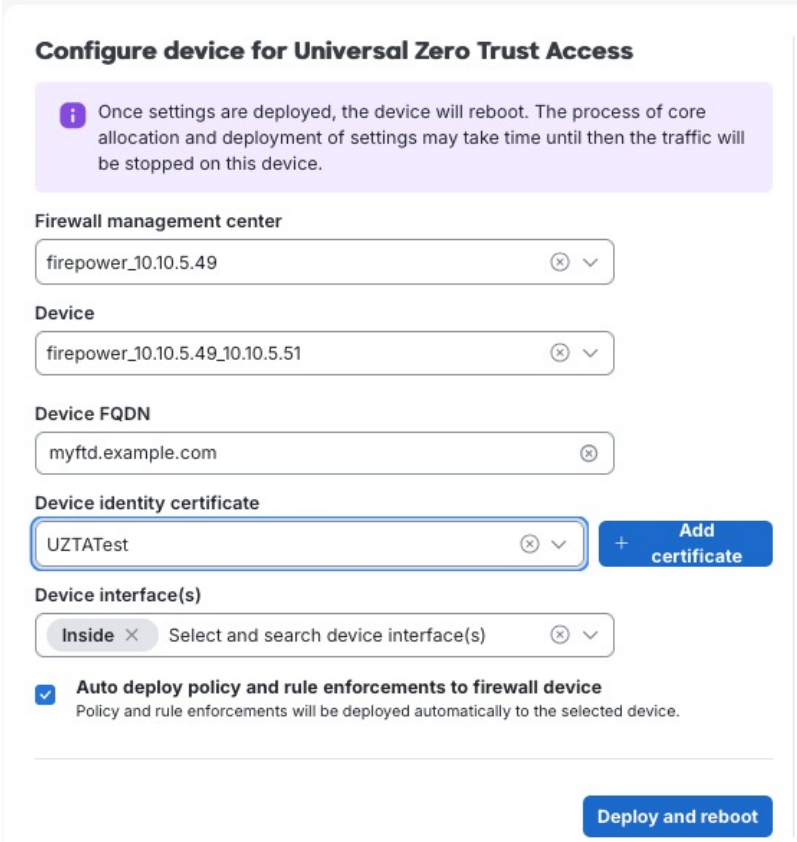
For detailed instructions, refer to the *Universal Zero Trust Network Access Configuration Guide*.

Note Unless specified otherwise, the term Firewall Management Center refers to both cloud-delivered and on-premises Firewall Management Center.

Table 1: Configuration Workflow Steps

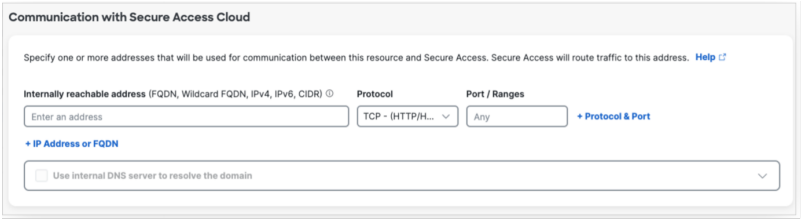
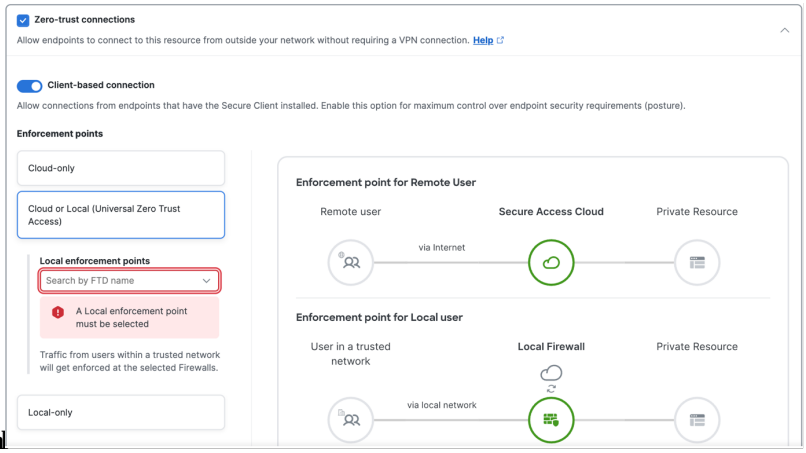
Configuration Task	Description
1. Onboard Secure Access and Firewall in Security Cloud Control	**1.** In a Security Cloud Control organization, claim a subscription to activate Secure Access and Security Cloud Control Firewall Management. **2.** Configure user management in Secure Access by setting up users and groups, either manually or by integrating with an identity provider. Enable the cloud-delivered Firewall Management Center if you have one. **3.** (This step applies only to Outcome 1: Optimal path for user traffic.) Configure one or more trusted networks through Secure Access. We recommend configuring a default trusted network. Secure Access automatically assigns a default trusted network to a universal ZTNA-enabled Firewall Threat Defense device. **4.** Update Secure Access with the CA certificate for the ZTNA user.
2. Prepare and set up Firewall Management Center and Firewall Threat Defense devices	**1.** Install the universal ZTNA build on the devices. Ensure that the Firewall Management Center has a smart license registered. **2.** Specify these configurations on the Management Center for the Firewall Threat Defense device: **a.** Routed interfaces to route the traffic **b.** Platform settings **c.** Domain Name Server (DNS) to resolve the IP address of the internal resources **3.** Onboard the on-premises Firewall Management Center to Security Cloud Control.

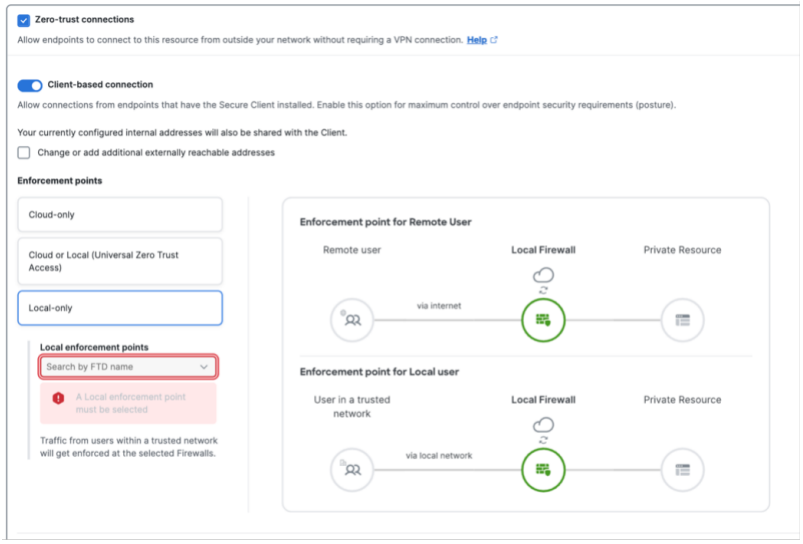
Configuration Task	Description
3. Configure the Threat Defense devices	

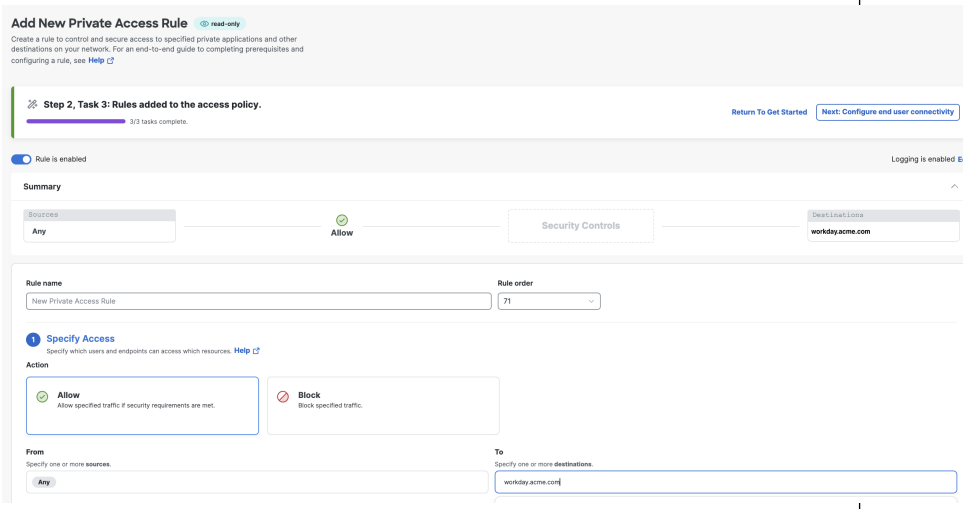
Configuration Task	Description
	1. Enable **universal zero trust network access settings** for the Firewall Threat Defense device (**Security Cloud Control** > **Security Devices** > **Firewall Threat Defense device**): **a.** Configure the device FQDN, inside interface, outside interface, and PKCS #12 certificate to enable universal ZTNA .  **b.** Deploy the changes. **Note** If your device operates version 7.7.10 or 10.0, it reboots so the system can reallocate resources for universal ZTNA components. During the reboot, traffic through this device is disrupted. If you deploy a High Availability pair of devices, both devices reboot simultaneously and traffic is disrupted. **c.** To see the events during the deployment process, click **Device Actions** > **Workflows** on the Security Devices page. After the changes are deployed, the device is connected to Secure Access. **2.** Check the availability of the Threat Defense device under Secure Access. **a.** Choose **Secure Access** > **Connect** > **Network Connections** . **b.** Click the **FTD** tab.

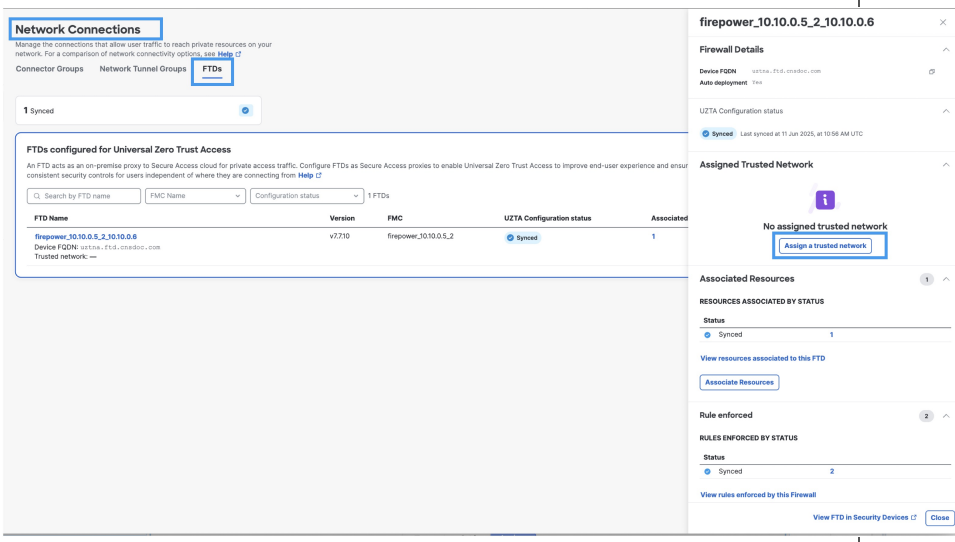
Configuration Task	Description
	Universal ZTNA -enabled devices are displayed. For more information, see "Configure Security Devices" in the *Universal Zero Trust Network Access Configuration Guide* .

Configuration Task	Description
4. Configure a private resource (payroll.example.com) on Secure Access	

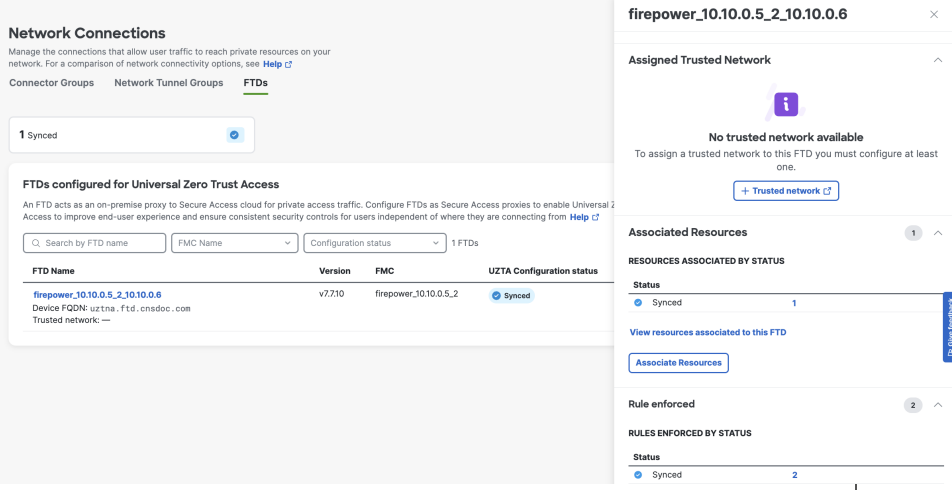
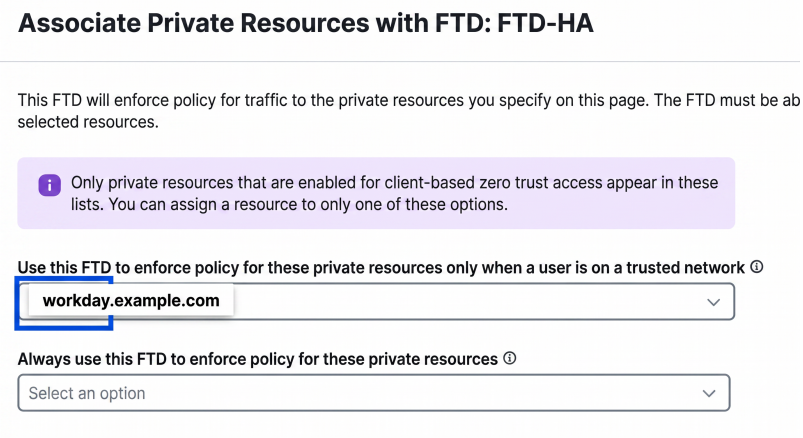
Configuration Task	Description
	In Security Cloud Control: **1.** Choose **Secure Access** > **Resources** > **Destinations** > **Private Resources** and click **+Add** . Specify the method Secure Access uses to communicate with the resource.  **2.** Specify how users can access this private resource: Under **Endpoint Connection Methods** , choose **Zero-trust connections** > **Client-based connection** . **3.** Specify the enforcement points. For Outcome 1: Optimal path for user traffic, select **Cloud or Local**  For Outcome 2: Private inspection for sensitive applications, select **Local only**.

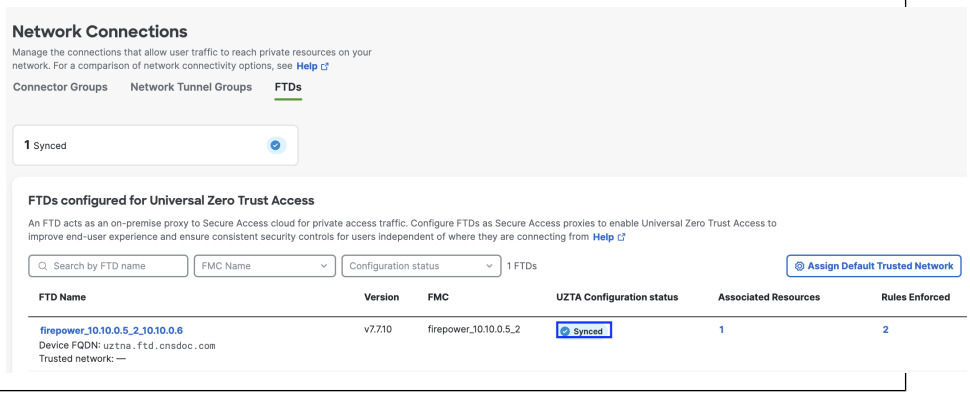
Configuration Task	Description
	 From the **Local enforcement points** drop-down list, select a device to enforce the policies. **4.** Save your configuration.

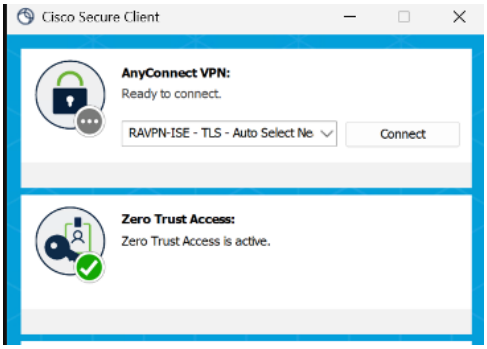
Configuration Task	Description
5. Create an Access Policy to allow users access to the private resource	In Security Cloud Control: **1.** Choose **Secure Access** > **Secure** > **Policy** > **Access Policy** > **Add Rule** > **Private Access** .  **2.** Specify the resources that an endpoint can access.  Next, follow the on-screen prompts to configure security such as Intrusion Prevention (IPS).

Configuration Task	Description
(Only for Outcome 1: Optimal path for user traffic) Verify that the Threat defense device is associated with a trusted network.	Assigning a trusted network to the device allows universal ZTNA to route user traffic to the correct Threat Defense device. Also, the device inspects and enforces security policies on traffic originating from or destined to that trusted network. This ensures that even trusted networks are continuously monitored for threats and policy compliance. Assign a trusted network to the Threat Defense device by completing these steps: **1.** Click **Assign a Trusted Network**.  **2.** From the **Trusted Networks** drop-down list, select a trusted network to map to the device. **3.** Click **Save**.

Configuration Task	Description
6. Associate the private resource to the Firewall Threat Defense Device	

Configuration Task	Description
	In Security Cloud Control: **1.** Choose **Secure Access** > **Connect** > **Network Connections** > **FTDs** . **2.** Click a device in the **FTD Name** column.  A slide-in pane displays details of the selected Firewall Threat Defense device. **3.** Under **Associated Resources**, click **Associate Resource**. **4.** In the **Associate Private Resources with FTD** window: (For Outcome 1: Optimal path for user traffic) Select the private resource from the **Use this FTD to enforce policy for private resources only when a user is in a trusted network** drop-down list.  (For Outcome 2: Private inspection of sensitive applications) Select the private resource from the **Always use this FTD to enforce policy for these private resources** drop-down list.

Configuration Task	Description
	This FTD will enforce policy for traffic to the private resources you specify on this page. The FTD must be able to reach all selected resources. Only private resources that are enabled for client-based zero trust access appear in these lists. To enable this option, associate at least one trusted network with this FTD Assign a trusted network **Use this FTD to enforce policy for these private resources only when a user is on a trusted network** Select an option **Always use this FTD to enforce policy for these private resources** payroll.example.com **5.** Click **Save**.
7. Wait for the UZTNA Configuration Status to display “Synced”	Secure Access policy and access configurations are automatically deployed to the Firewall Threat Defense device. Successful configuration synchronization displays a "Synced" status. 

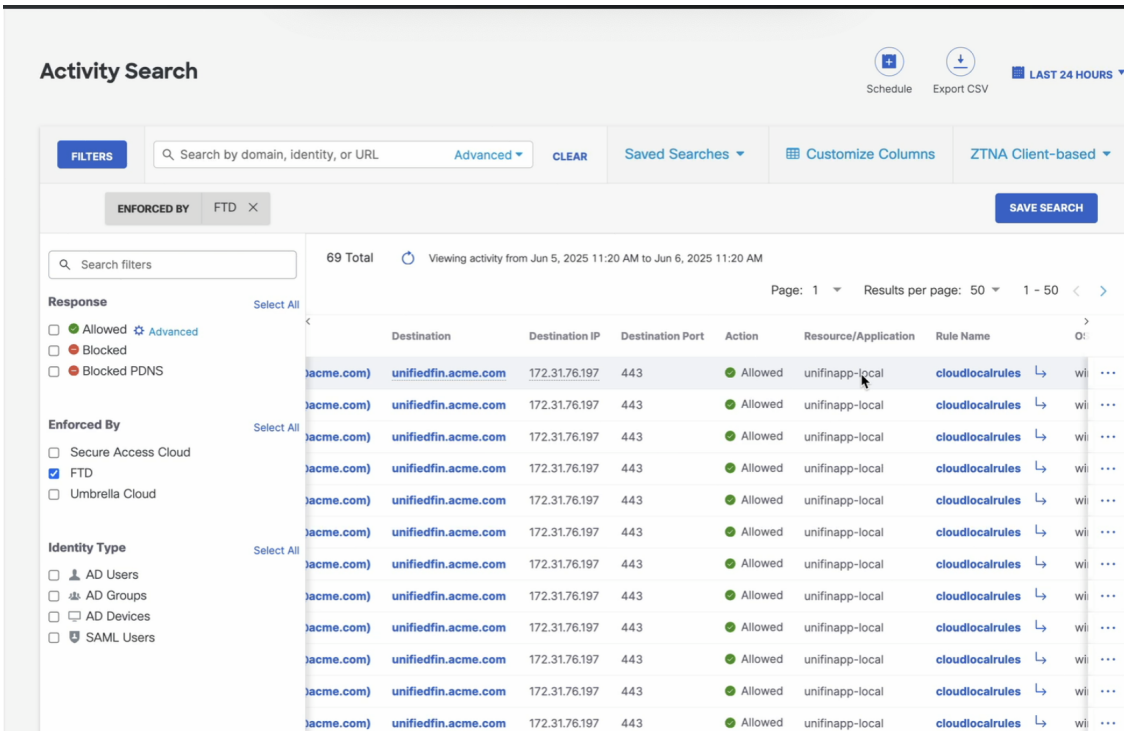
Configuration Task	Description
8. End User Device Configuration	1. Install Secure Client version 5.1.10 or later on the user devices. 2. Enroll the user with Secure Access using the device enrollment certificate 3. Enable Zero Trust Access in Secure Client.  For information on setting up Secure Client, refer to Secure Client Administration Guide .

Monitoring events

After you deploy universal ZTNA, you can monitor the access events in real time. Traffic to and from the private resources that traverses the Firewall Threat Defense is sent to Secure Access. Secure Access aggregates event logs from all access points and provides a centralized monitoring dashboard.

To see a log of the universal ZTNA activities, do these steps:

1. In Security Cloud Control, choose **Secure Access** > **Monitor** > **Activity Search**.
2. Click **All** under the **Filters** menu and select **ZTNA Client-based**.



3. Choose **FTD** to monitor the events and policies enforced by the Threat Defense device.