Deployment of Universal ZTNA Solution

Universal ZTNA provides a secure and controlled way to access application based on zero trust principles. Aa discussed earlier, 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 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

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 ouside 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. They intend to access their HR resource, available at https://workday.acme.com.

You will learn how traffic flow is optimized for both Lee and John.

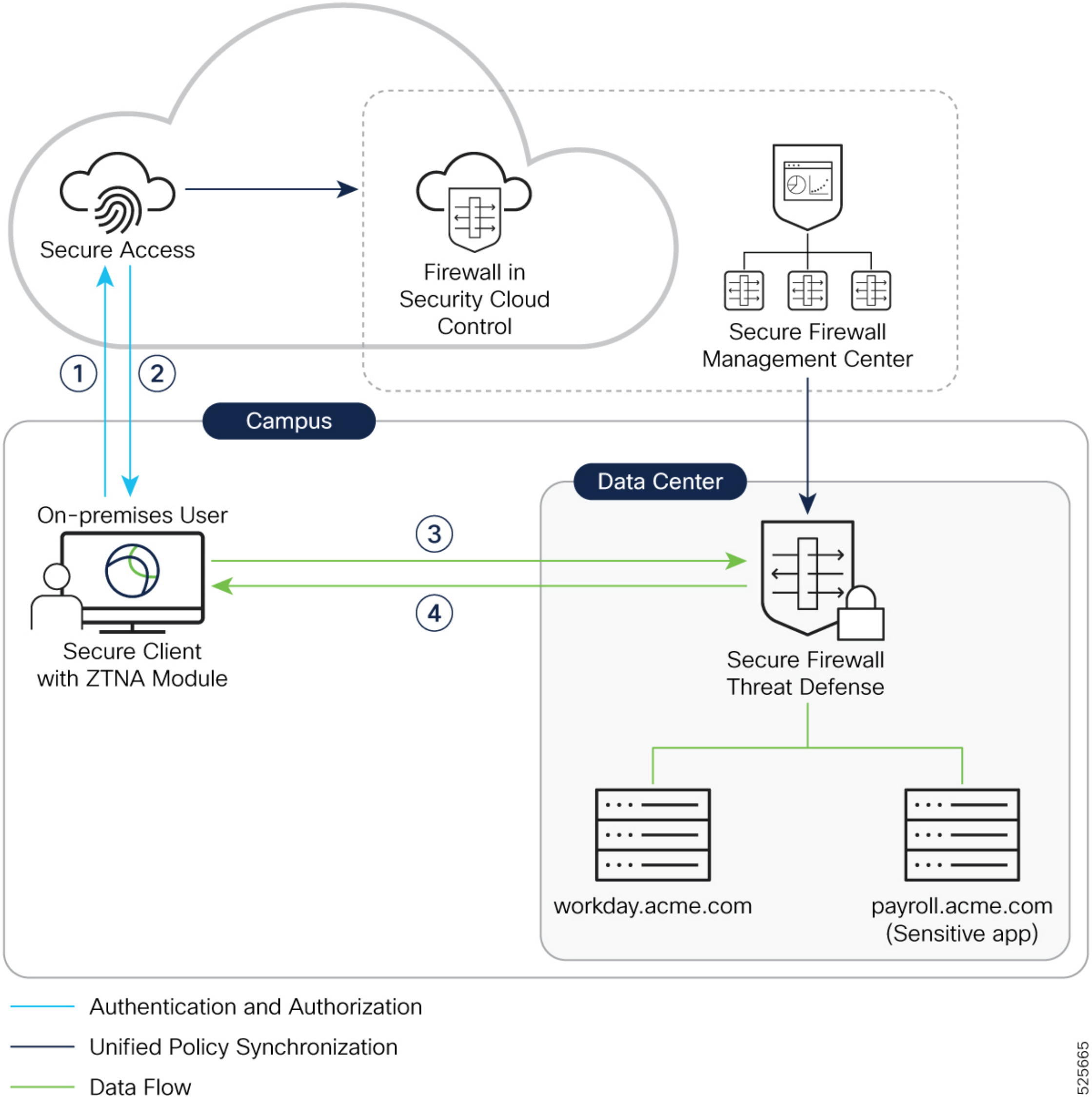
Data Flow for an On-Premises User

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.acme.com through a browser.

Workflow

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


Secure Access
Firewall in Security Cloud Control
Secure Firewall Management Center
1
2
Campus
Data Center
On-premises User
3
4
Secure Client with ZTNA Module
Secure Firewall Threat Defense
workday.acme.com
payroll.acme.com (Sensitive app)
Authentication and Authorization
Unified Policy Synchronization
Data Flow
525665

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

1. **Secure Client Request**: The secure client installed on Lee's laptop 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 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.

3. **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.acme.com.
4. **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.acme.com and enforces security policies, such as IPS, file, and malware protection on the user traffic.

Data Flow for a Remote User

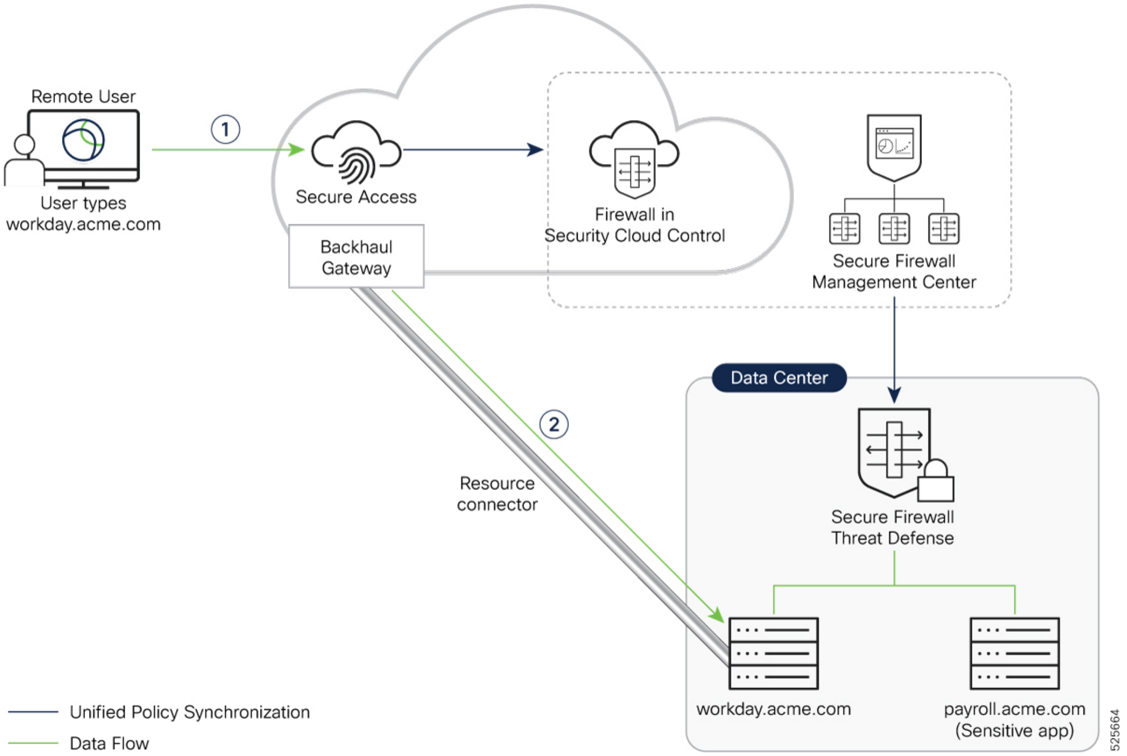
For a user operating from outside the private network, traffic to an internal private resource is directed through the cloud.

Summary

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

Workflow

Figure 2: Universal ZTNA Data Flow for Remote User



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

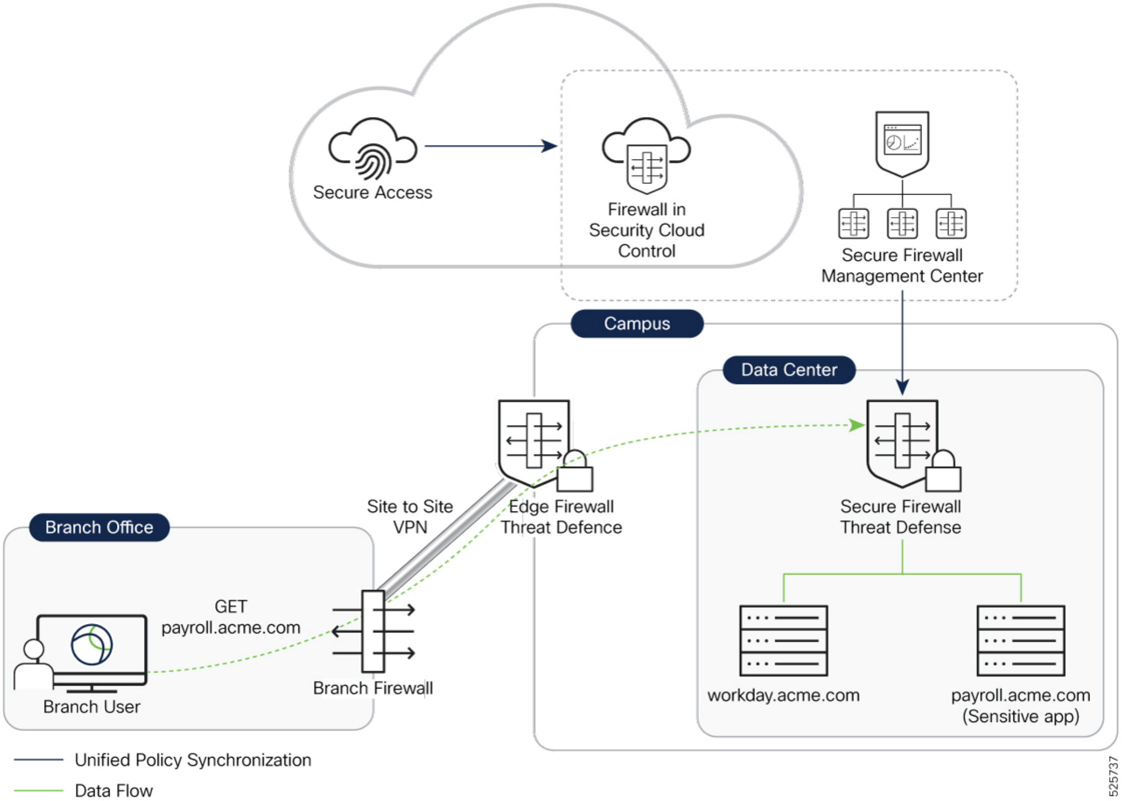
1. **Secure Client intercepts the request**: The Secure Client on John’s laptop checks and finds that https://workday.acme.com is a ZTNA-enabled application. It sends a connect request to Secure Access.
2. **Secure Access Policy Evaluation and Response**: Secure Access evaluates the policies and the 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.acme.com residing on the private network.

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

Data Flow for a Branch User

An enterprise network normally deploys multiple firewalls to enhance security and network segmentation. Consider one such scenario where the private resources in a large enterprise are protected by a firewall at the Data Center. The branch offices are protected by branch firewalls and connect to the main campus through site-to-site virtual private network (VPN).

Figure 3: Universal ZTNA Data Flow for a Branch User


Secure Access
Firewall in Security Cloud Control
Secure Firewall Management Center
Campus
Data Center
Site to Site VPN
Edge Firewall Threat Defence
Secure Firewall Threat Defense
Branch Office
GET payroll.acme.com
Branch Firewall
Branch User
workday.acme.com
payroll.acme.com (Sensitive app)
Unified Policy Synchronization
Data Flow
525737

As with any universal ZTNA user, authentication and authorization happen 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.

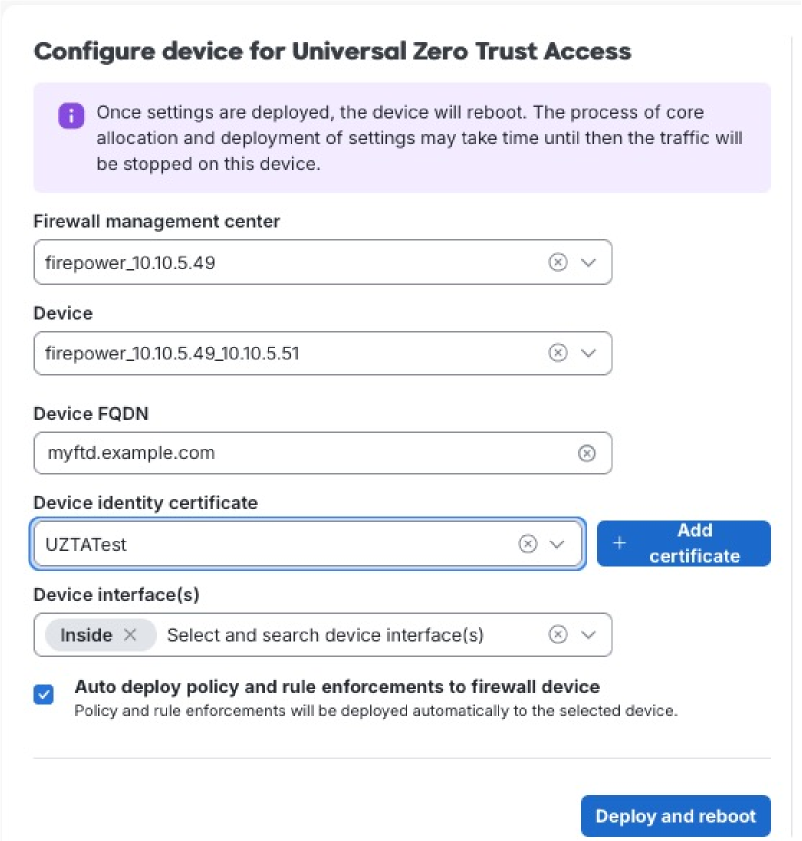
Configuration Workflow for Outcome 1

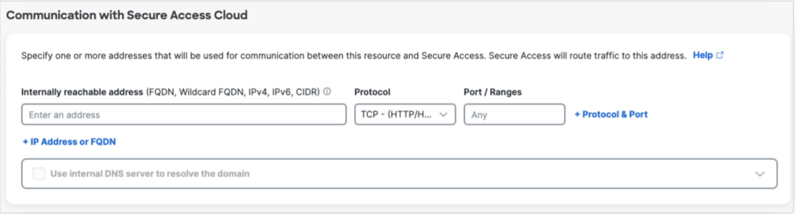
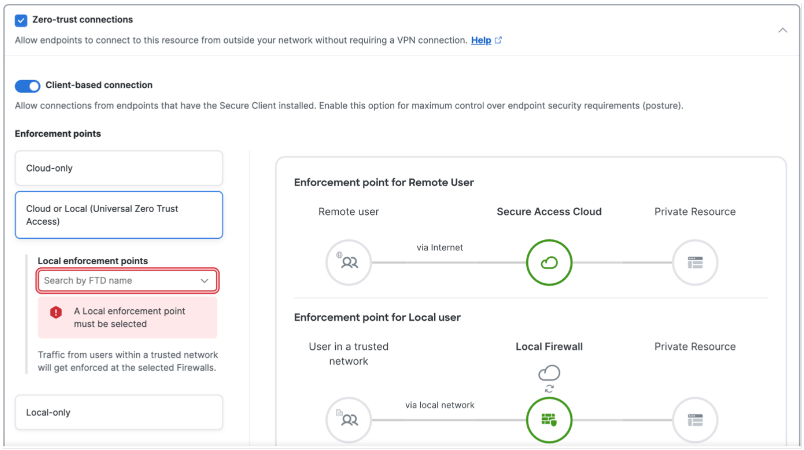
This table describes the key steps for enabling the optimal path for traffic. For detailed instructions, refer to the *Universal Zero Trust Access Configuration Guide*.

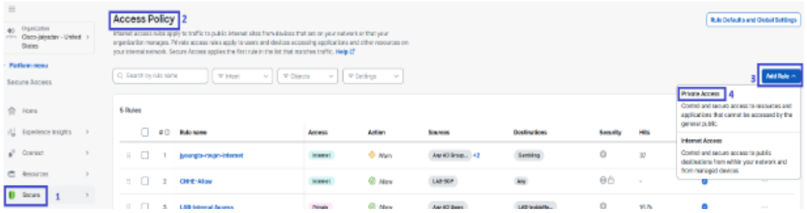
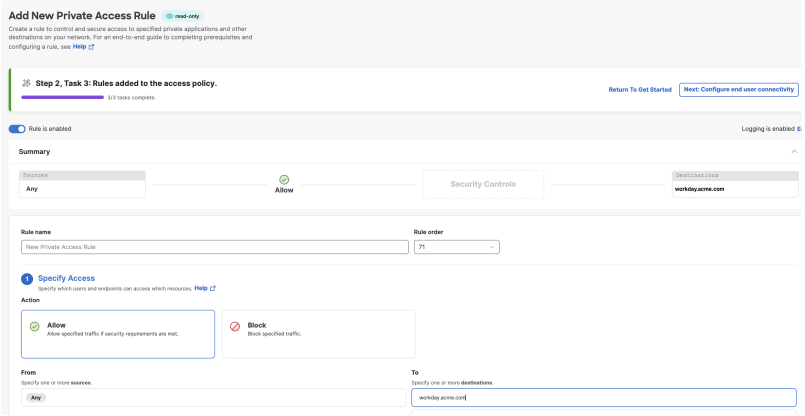
Note Unless specified otherwise, the term Firewall Management Center refers to both the cloud-delivered and on-premises Firewall Management Center.

Configuration Task	Description
1. Onboard Secure Access and Security Cloud Control Firewall Management to Security Cloud Control	**1.** In a Security Cloud Control organization, claim a subscription to activate Secure Access and Security Cloud Control Firewall Management. Enable the cloud-delivered Firewall Management Center if you have one. **2.** Configure user management in Secure Access: configure users and groups, either manually or integrate an identity provider. **3.** 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.  Configure device for Universal Zero Trust Access Once settings are deployed, the device will reboot. The process of core allocation and deployment of settings may take time until then the traffic will be stopped on this device. Firewall management center: firepower_10.10.5.49 Device: firepower_10.10.5.49_10.10.5.51 Device FQDN: myftd.example.com Device identity certificate: UZTATest Device interface(s): Inside ☑ Auto deploy policy and rule enforcements to firewall device Policy and rule enforcements will be deployed automatically to the selected device. + Add certificate Select and search device interface(s) Deploy and reboot b. Deploy the changes. c. The device reboots for the system to reallocate resources for universal ZTNA components. During the reboot, traffic through this device is disrupted. If a High Availability pair of devices are deployed, both the devices are rebooted simultaneously, causing a traffic disruption. To see the events during the deployment process, click **Device Actions** > **Workflows** on the Security Devices page. After the devices reboots, it is connects 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*.
4. Configure a private resource (workday.acme.com) on Secure Access	In **Security Cloud Control**: 1. Choose **Secure Access** > **Resources** > **Destinations** > **Private Resources** and click **+Add.** Specify the internally reachable addresses of the resource. Secure Access uses this address, which can be an FQDN or an IP address, to communicate with the resource. Communication with Secure Access Cloud Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. Help **Internally reachable address** (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR): Enter an address **Protocol**: TCP - (HTTP/H... **Port / Ranges**: Any + Protocol & Port + IP Address or FQDN □ Use internal DNS server to resolve the domain 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: Select **Cloud or Local**. ☑ Zero-trust connections Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. Help Client-based connection (on) Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture). Enforcement points Cloud-only Cloud or Local (Universal Zero Trust Access) Local enforcement points: Search by FTD name A Local enforcement point must be selected Traffic from users within a trusted network will get enforced at the selected Firewalls. Local-only Enforcement point for Remote User: Remote user — via Internet — Secure Access Cloud — Private Resource Enforcement point for Local user: User in a trusted network — via local network — Local Firewall — Private Resource From the **Local enforcement points** drop-down list, select a device to enforce the policies. 4. Save your configuration. For more information about creating a private resource, see "Configure Private Resource" in the *Universal Zero Trust Network Access Configuration Guide*.

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**.  Access Policy 2 Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help Rule Defaults and Global Settings Organization Platform menu Secure Access Home Experience Insights Connect Resources Secure 1 Search by rule name Filters Objects Settings 3 Add Rule Private Access 4 Control and secure access to resources and applications that cannot be accessed by the general public. Internet Access Control and secure access to public destinations from within your network and from managed devices. 5 Rules Rule name Access Action Sources Destinations Security Hits Internet Warn Allow Private 2. Specify the resources you created in the earlier steps. An endpoint can access these resources.  Add New Private Access Rule read-only Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see Help Step 2, Task 3: Rules added to the access policy. 3/3 tasks complete. Return To Get Started Next: Configure end user connectivity Rule is enabled Logging is enabled Summary Sources: Any Allow Security Controls Destinations: workday.acme.com Rule name: New Private Access Rule Rule order: 71 1 Specify Access Specify which users and endpoints can access which resources. Help Action Allow — Allow specified traffic if security requirements are met. Block — Block specified traffic. From Specify one or more **sources**. Any To Specify one or more **destinations**. workday.acme.com Next, follow the on-screen prompts to configure security such as Intrusion Prevention (IPS).

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

<table>
<tr><th>Configuration Task</th><th>Description</th></tr>
<tr><td></td><td>

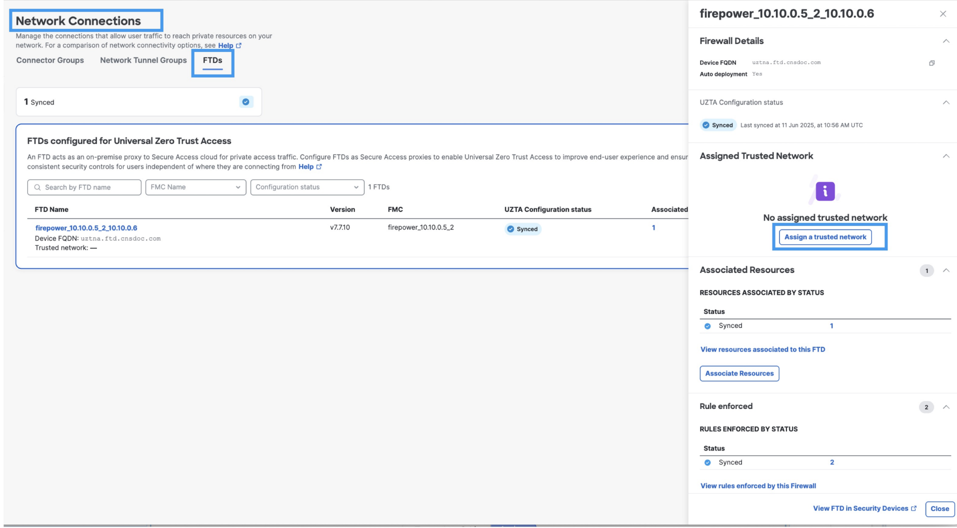
In **Security Cloud Control**:

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. 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.

   To assign a trusted network to the Threat Defense device, perform these steps:

   a. Click **Assign a Trusted Network**.

   Network Connections

   Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help

   FTDs configured for Universal Zero Trust Access

   An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve end-user experience and ensur consistent security controls for users independent of where they are connecting from Help

FTD Name	Version	FMC	UZTA Configuration status	Associated
firepower_10.10.0.5_2_10.10.0.6 Device FQDN: uztna.ftd.cnsdoc.com Trusted network: —	v7.7.10	firepower_10.10.0.5_2	Synced	1

   firepower_10.10.0.5_2_10.10.0.6

   Firewall Details

   Device FQDN uztna.ftd.cnsdoc.com
   Auto deployment Yes

   UZTA Configuration status

   Synced Last synced at 11 Jun 2025, at 10:56 AM UTC

   Assigned Trusted Network

   No assigned trusted network

   Associated Resources 1

   RESOURCES ASSOCIATED BY STATUS

Status	
Synced	1

   Rule enforced 2

   RULES ENFORCED BY STATUS

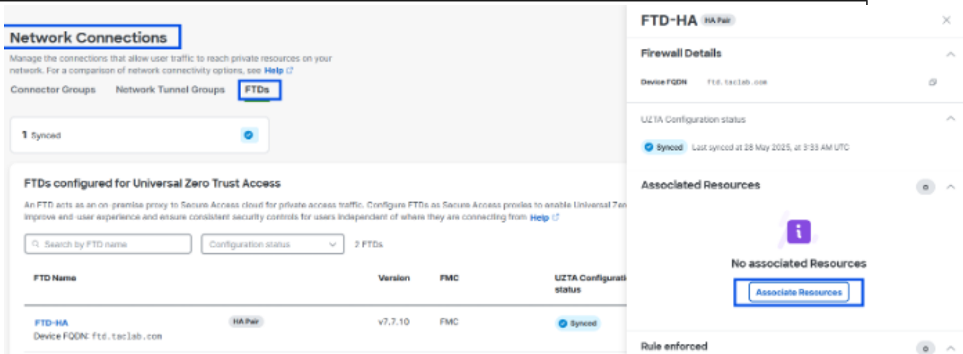
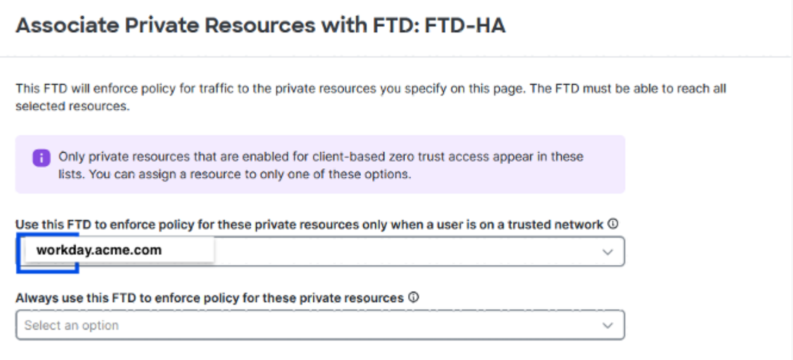
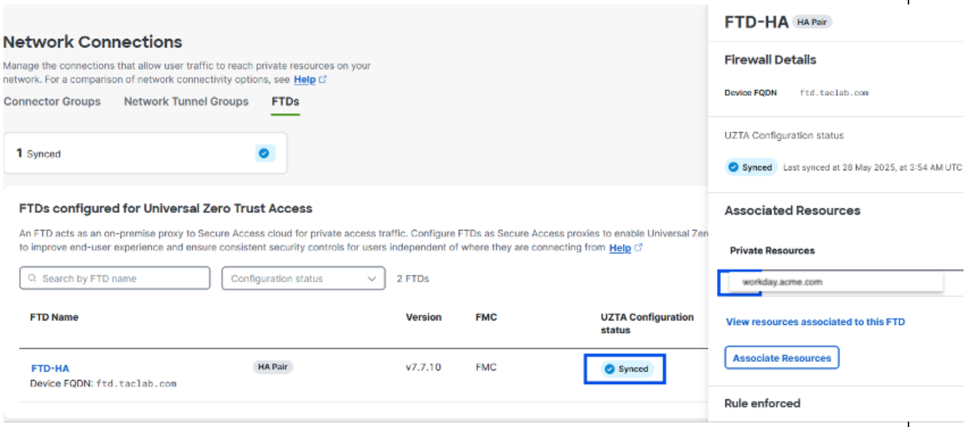
Status	
Synced	2

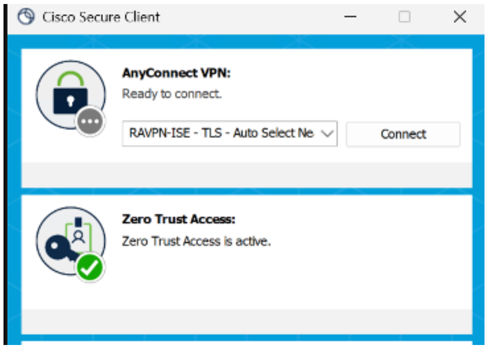
   View rules enforced by this Firewall
View FTD in Security Devices
Close

   b. From the **Trusted Networks** drop-down list, select a trusted network to map to the device.

   c. Click **Save**.
4. Under **Associated Resources**, click **Associate Resource**.

</td></tr>
</table>

Configuration Task	Description
	 Network Connections Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help Connector Groups Network Tunnel Groups FTDs 1 Synced FTDs configured for Universal Zero Trust Access An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zer improve end-user experience and ensure consistent security controls for users independent of where they are connecting from Help Search by FTD name Configuration status 2 FTDs FTD Name Version FMC UZTA Configurati status FTD-HA HA Pair v7.7.10 FMC Synced Device FQDN: ftd.taclab.com FTD-HA HA Pair Firewall Details Device FQDN ftd.taclab.com UZTA Configuration status Synced Last synced at 28 May 2025, at 3:33 AM UTC Associated Resources No associated Resources Associate Resources Rule enforced 5. In the **Associate Private Resources with FTD** window:  Associate Private Resources with FTD: FTD-HA 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. You can assign a resource to only one of these options. Use this FTD to enforce policy for these private resources only when a user is on a trusted network: workday.acme.com Always use this FTD to enforce policy for these private resources: Select an option 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. 6. 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.  Network Connections Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help Connector Groups Network Tunnel Groups FTDs 1 Synced FTDs configured for Universal Zero Trust Access An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zer to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from Help Search by FTD name Configuration status 2 FTDs FTD Name Version FMC UZTA Configuration status FTD-HA HA Pair v7.7.10 FMC Synced Device FQDN: ftd.taclab.com FTD-HA HA Pair Firewall Details Device FQDN ftd.taclab.com UZTA Configuration status Synced Last synced at 28 May 2025, at 3:54 AM UTC Associated Resources Private Resources workday.acme.com View resources associated to this FTD Associate Resources Rule enforced

Configuration Task	Description
8. End User Device Configuration	**1.** Install Secure Client version 5.1.10 or later on the user devices. Ensure that the client runs on a platform that supports Trusted Platform Module (TPM), such as Windows 11. **2.** Enroll the user with Secure Access using the device enrollment certificate. **3.** Enable the **Zero Trust Access** module in Secure Client.  Cisco Secure Client **AnyConnect VPN:** Ready to connect. RAVPN-ISE - TLS - Auto Select Ne **Zero Trust Access:** Zero Trust Access is active. For information on setting up Secure Client, see Secure Client Administration Guide.

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.

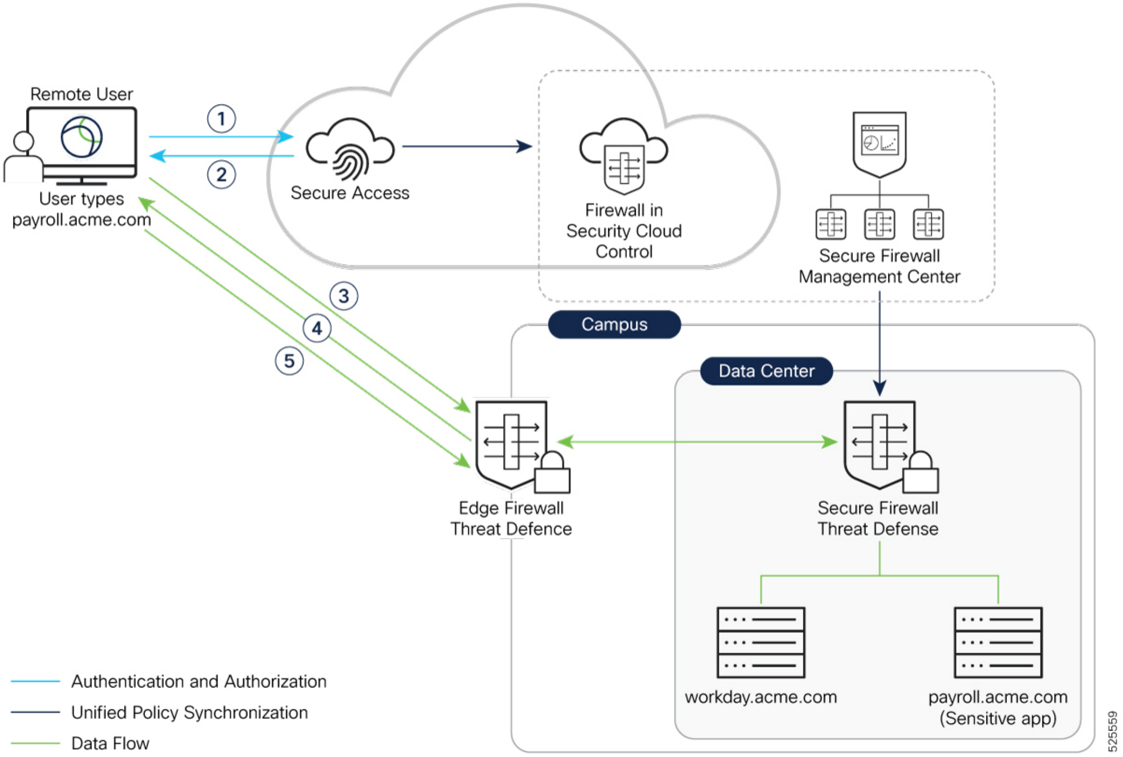
Data Flow to a Sensitive Application from a Remote User

For a user operating from outside the private network, the local firewall directs traffic to a sensitive private resource.

In the sample scenario, John is working from home and tries to access a sensitive internal resource, payroll.acme.com, through the browser.

Workflow

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.acme.com) from an untrusted network:

1. **Secure Client Request**: The secure client installed on John's laptop 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 his 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.acme.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 as the response.

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.acme.com.

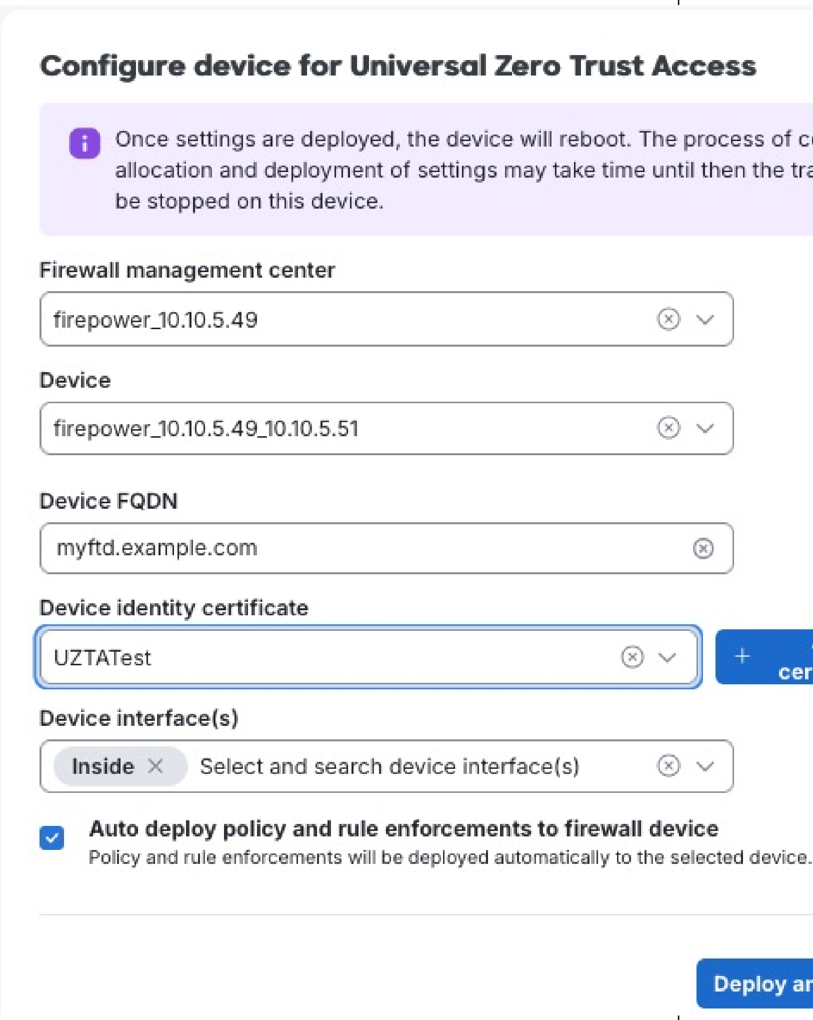
Configuration Workflow for Outcome 2

This table lists the key steps to enable private inspection for sensitive applications. For detailed configuration steps, refer to the *Universal Zero Trust Access Configuration Guide*.

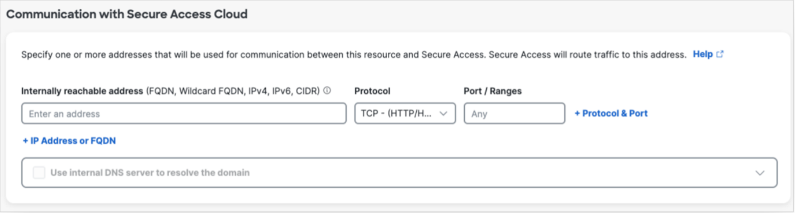
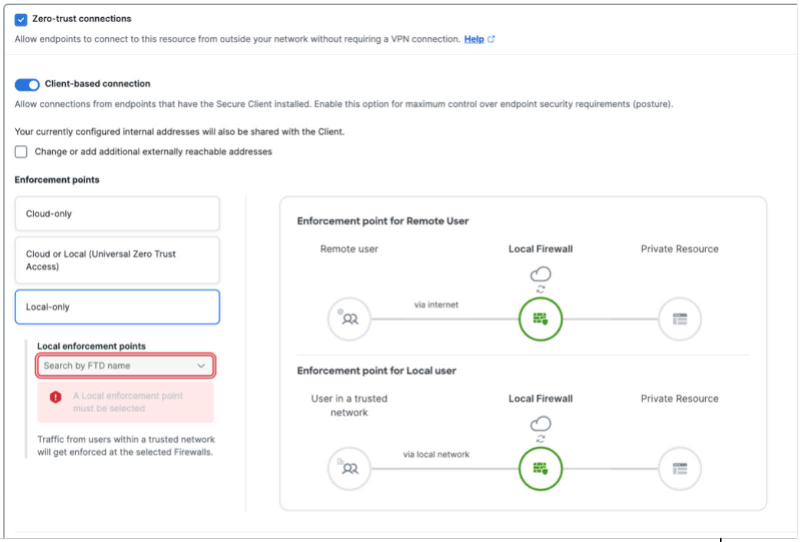
Note Unless specified otherwise, the term Firewall Management Center refers to both cloud-delivered and on-premises Firewall Management Center.

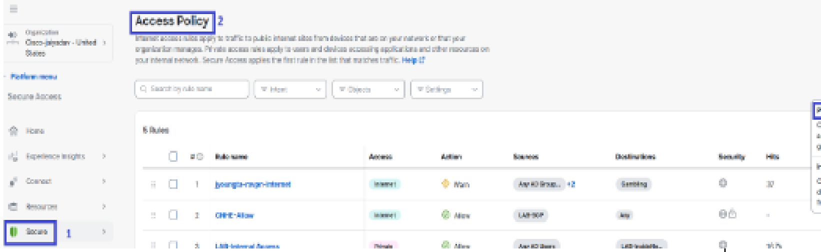
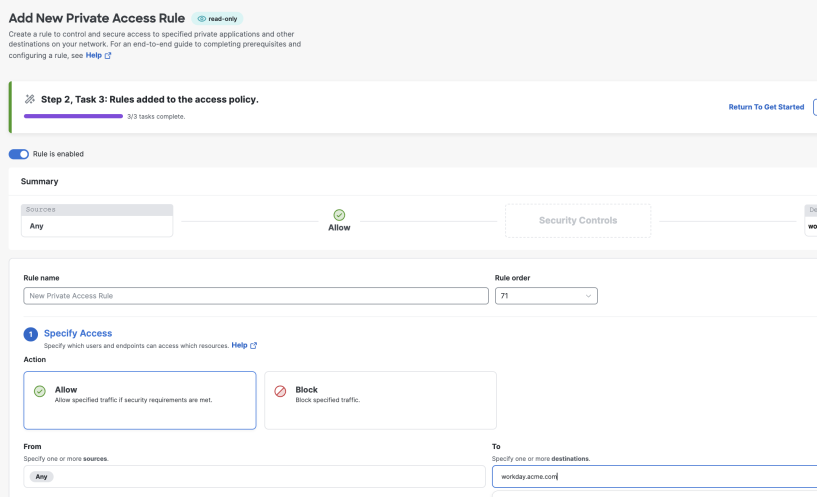
Configuration Task	Description
1. Onboard Secure Access and Firewall in Security Cloud Control	**1.** In a Security Cloud Control organization, claim a subscription to activate Secure Access and Security Cloud Control Firewall Management. **2.** Configure user management in Secure Access by setting up users and groups, either manually or by integrating with an identity provider. Enable the cloud-delivered Firewall Management Center if you have one. **3.** 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.

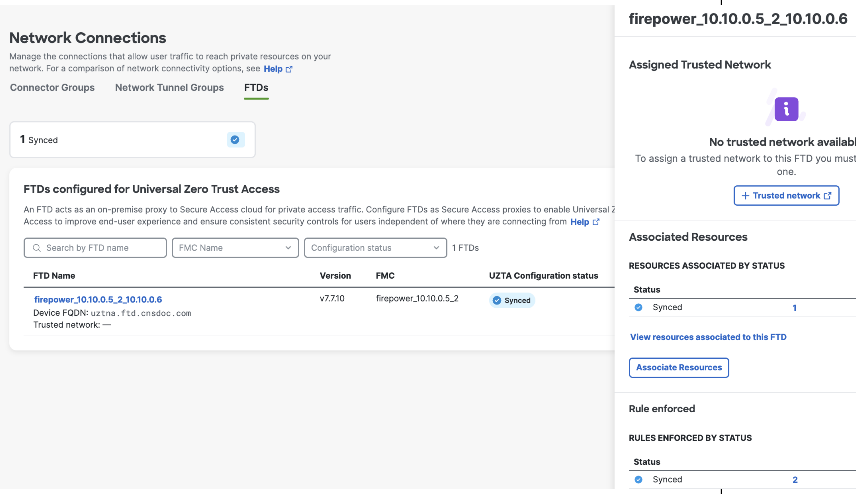
Configuration Task	Description
3. Configure the Threat Defense devices	

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.  Configure device for Universal Zero Trust Access Once settings are deployed, the device will reboot. The process of c allocation and deployment of settings may take time until then the tra be stopped on this device. Firewall management center: firepower_10.10.5.49 Device: firepower_10.10.5.49_10.10.5.51 Device FQDN: myftd.example.com Device identity certificate: UZTATest Device interface(s): Inside × ☑ Auto deploy policy and rule enforcements to firewall device Policy and rule enforcements will be deployed automatically to the selected device. b. Deploy the changes. c. The device reboots for the system to reallocate resources for universal ZTNA components. During the reboot, traffic through this device is disrupted. If a High Availability pair of devices are deployed, both the devices are rebooted simultaneously, causing a traffic disruption. To see the events during the deployment process, click **Device Actions** > **Workflows** on the Security Devices page. After the devices reboots, it is connected to Secure Access.

Configuration Task	Description
	2. Check the availability of the Threat Defense device under Secure Access. **a.** Choose **Secure Access** > **Connect** > **Network Connections** . **b.** Click the **FTD** tab. 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.acme.com) on Secure Access	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.  Communication with Secure Access Cloud Specify one or more addresses that will be used for communication between this resource and Secure Access. Secure Access will route traffic to this address. Help Internally reachable address (FQDN, Wildcard FQDN, IPv4, IPv6, CIDR): Enter an address Protocol: TCP - (HTTP/H... Port / Ranges: Any + Protocol & Port + IP Address or FQDN ☐ Use internal DNS server to resolve the domain **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: select **Local only**  ☑ Zero-trust connections Allow endpoints to connect to this resource from outside your network without requiring a VPN connection. Help ● Client-based connection Allow connections from endpoints that have the Secure Client installed. Enable this option for maximum control over endpoint security requirements (posture). Your currently configured internal addresses will also be shared with the Client. ☐ Change or add additional externally reachable addresses Enforcement points Cloud-only Cloud or Local (Universal Zero Trust Access) Local-only Local enforcement points: Search by FTD name A Local enforcement point must be selected Traffic from users within a trusted network will get enforced at the selected Firewalls. Enforcement point for Remote User Remote user Local Firewall Private Resource via internet Enforcement point for Local user User in a trusted network Local Firewall Private Resource via local network From the **Local enforcement points** drop-down list, select a device to enforce the policies. **4.** Save your configuration. With this configuration, traffic to the selected private resource is proxied through the selected Threat Defense device, regardless of the user location.

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**.  Access Policy 2 Secure Access Home Experience Insights Connect Resources Secure 1 Rule name Access Action Sources Destinations Security Hits 2. Specify the resources that an endpoint can access.  Add New Private Access Rule read-only Create a rule to control and secure access to specified private applications and other destinations on your network. For an end-to-end guide to completing prerequisites and configuring a rule, see Help Step 2, Task 3: Rules added to the access policy. 3/3 tasks complete. Return To Get Started Rule is enabled Summary Sources: Any Allow Security Controls Rule name: New Private Access Rule Rule order: 71 1 Specify Access Specify which users and endpoints can access which resources. Help Action ○ Allow — Allow specified traffic if security requirements are met. ○ Block — Block specified traffic. From Specify one or more **sources**. Any To Specify one or more **destinations**. workday.acme.com Next, follow the on-screen prompts to configure security such as Intrusion Prevention (IPS).

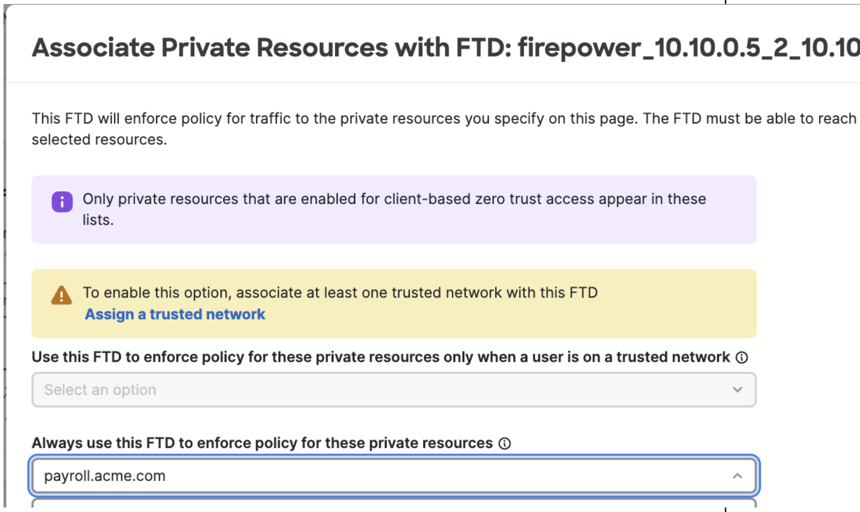
<table>
<tr><th>Configuration Task</th><th>Description</th></tr>
<tr><td><b>6. Associate the private resource to the Firewall Threat Defense Device</b></td><td>In <b>Security Cloud Control</b>:
1. Choose <b>Secure Access</b> > <b>Connect</b> > <b>Network Connections</b> > <b>FTDs</b>.
2. Click a device in the <b>FTDName</b> column.

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help

1 Synced
FTDs configured for Universal Zero Trust Access
An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Z Access to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from Help

1 FTDs
FTD Name / Version / FMC / UZTA Configuration status
firepower_10.10.0.5_2_10.10.0.6 / v7.7.10 / firepower_10.10.0.5_2 / Synced
Device FQDN: uztna.ftd.cnsdoc.com
Trusted network: —
firepower_10.10.0.5_2_10.10.0.6
Assigned Trusted Network
No trusted network availab
To assign a trusted network to this FTD you must one.

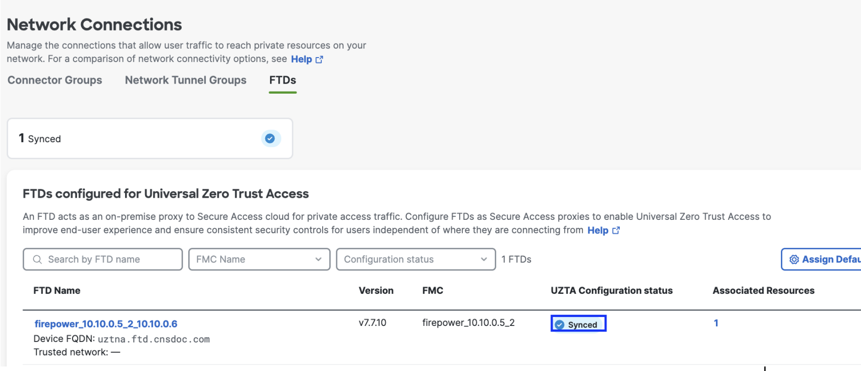
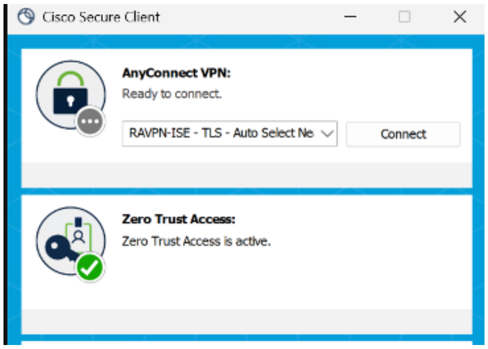
Associated Resources
RESOURCES ASSOCIATED BY STATUS
Status
Synced 1

View resources associated to this FTD
Associate Resources

Rule enforced
RULES ENFORCED BY STATUS
Status
Synced 2
A slide-in pane displays details of the selected Firewall Threat Defense device.
3. Under <b>Associated Resources</b>, click <b>Associate Resource</b>.
4. In the <b>Associate Private Resources with FTD</b> window:

Associate Private Resources with FTD: firepower_10.10.0.5_2_10.10
This FTD will enforce policy for traffic to the private resources you specify on this page. The FTD must be able to reach 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

Use this FTD to enforce policy for these private resources only when a user is on a trusted network

Always use this FTD to enforce policy for these private resources
payroll.acme.com
Select the private resource from the <b>Always use this FTD to enforce policy for these private resources</b> drop-down list.
5. Click <b>Save</b>.</td></tr>
</table>

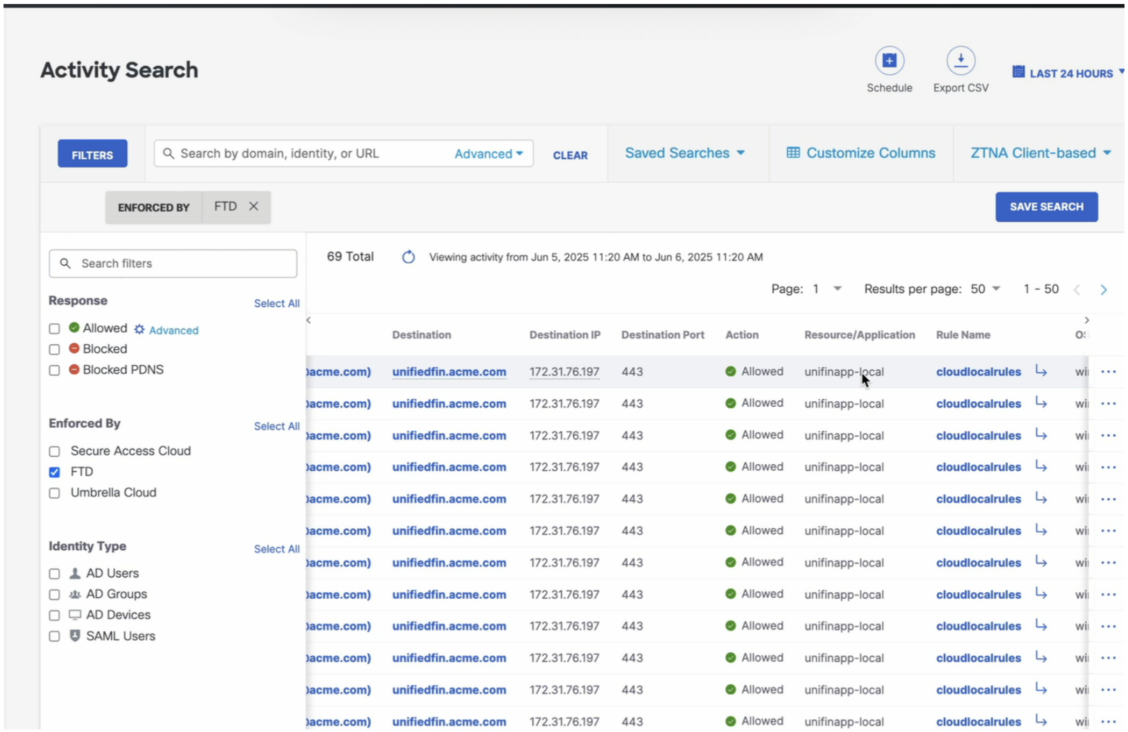
<table>
<tr><th>Configuration Task</th><th>Description</th></tr>
<tr><td><b>7. Wait for the UZTNA Configuration Status to display “Synced”.</b></td><td>Secure Access policy and access configurations are automatically deployed to the Firewall Threat Defense device. Successful configuration synchronization displays a "Synced" status.

Network Connections
Manage the connections that allow user traffic to reach private resources on your network. For a comparison of network connectivity options, see Help
Connector Groups | Network Tunnel Groups | FTDs
1 Synced
FTDs configured for Universal Zero Trust Access
An FTD acts as an on-premise proxy to Secure Access cloud for private access traffic. Configure FTDs as Secure Access proxies to enable Universal Zero Trust Access to improve end-user experience and ensure consistent security controls for users independent of where they are connecting from Help
Search by FTD name | FMC Name | Configuration status | 1 FTDs | Assign Defau
FTD Name | Version | FMC | UZTA Configuration status | Associated Resources
firepower_10.10.0.5_2_10.10.0.6
Device FQDN: uztna.ftd.cnsdoc.com
Trusted network: — | v7.7.10 | firepower_10.10.0.5_2 | Synced | 1</td></tr>
<tr><td><b>8. End User Device Configuration</b></td><td>
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.

Cisco Secure Client
AnyConnect VPN:
Ready to connect.
RAVPN-ISE - TLS - Auto Select Ne
Connect
Zero Trust Access:
Zero Trust Access is active.
For information on setting up Secure Client, refer to Secure Client Administration Guide.</td></tr>
</table>

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**.



Activity Search

ENFORCED BY FTD ×

Response
- ☐ Allowed
- ☐ Blocked
- ☐ Blocked PDNS

Enforced By
- ☐ Secure Access Cloud
- ☑ FTD
- ☐ Umbrella Cloud

Identity Type
- ☐ AD Users
- ☐ AD Groups
- ☐ AD Devices
- ☐ SAML Users

69 Total Viewing activity from Jun 5, 2025 11:20 AM to Jun 6, 2025 11:20 AM

Page: 1 Results per page: 50 1 - 50

	Destination	Destination IP	Destination Port	Action	Resource/Application	Rule Name	O
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
acme.com)	unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi

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