



Configure Secure Access

The final step in configuring universal ZTNA is to configure access policies, private resources, and the devices that are responsible for protecting the resources.

- [Configure Private Resources, on page 1](#)
- [Configure Universal ZTNA Access Policies, on page 2](#)
- [Trusted Network Detection, on page 4](#)
- [Associate Private Resources with Firewall Threat Defense, on page 8](#)

Configure Private Resources

Perform these steps to create the private resources in your organization.

Procedure

- Step 1** In Cisco Security Cloud Control, click **Products > Secure Access**.
The Secure Access product menu appears in the left navigation bar.
- Step 2** Click **Resources > Destinations > Private Resources**.
- Step 3** Click **+Add**.
- Step 4** Provide a meaningful name for the resource in the **Define a Private Resource** section.
- Step 5** To define how Secure Access can communicate with the resource, provide the network address or the fully qualified domain name (FQDN) of 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)	Protocol	Port / Ranges
<input type="text" value="Enter an address"/>	TCP - (HTTP/H...	Any

[+ IP Address or FQDN](#)

☐ Use internal DNS server to resolve the domain

Step 6 Under **Endpoint Connection Methods**, choose **Zero-trust connections** > **Client-based connections**. This selection allows endpoints with Secure Client to communicate with Secure Access.

Depending on how you want to enforce traffic flow, choose an appropriate enforcement point.

- Choose **Cloud or Local** to steer the traffic dynamically based on its origin.

If the user is in a trusted network, a local Firewall performs the traffic inspection. If the user is outside the trusted network, Secure Access (cloud) performs the traffic inspection.

- The enforcement point must be set to **Local only** for sensitive applications. This choice ensures that traffic inspection occurs only at the on-premises Firewall, regardless of the location of the user.

Choose a Threat Defense device from the **Local enforcement points** drop-down list. All devices that share the same FQDN as the selected device act as the enforcement points.

Step 7 Click **Save** to save the configuration.

Private resources are now added to the network.

For more information on managing private resources, refer to [Managing Private Resources](#) in the Secure Access documentation.

Configure Universal ZTNA Access Policies

Create a rule to control and secure the access to specified private resources.

An access rule consists of sources, destinations, endpoint profiles, and security controls. Sources specify the origin of the network traffic. Destinations specify the endpoint of the network traffic.

Endpoint profiles describe the requirements for a rule to match the traffic. For universal ZTNA, use the Client-based Zero Trust profile.

Procedure

- Step 1** In Cisco Security Cloud Control, click **Products > Secure Access**.
Secure Access product menu displays in the left navigation bar.
- Step 2** Click **Secure > Access Policy**.
- Step 3** Click **Add Rule** and choose **Private Access**.
- Step 4** Add a rule name and specify the order in which the rule must be executed.
- Step 5** Under **Specify Access**, specify one or more sources (users or devices) that can access a destination (private resource).
The **Summary** pane at the beginning of the page shows the rule that you have specified.

Add Allow-HR
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 [Edit](#)

Summary

Sources: ZTA Enrolled Device • Any ZTA Enrolled Device → **Allow** → Security Controls → Destinations: Any Private Resources

Rule name: Allow-HR Rule order: 2

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.
ZTA Enrolled Device • Any ZTA Enrolled Device

To
Specify one or more destinations.
Any

[+ AND](#)

- Step 6** (Optional) Under **Configure Security**:
- Define the Intrusion Prevention (IPS) method. Traffic is decrypted and inspected based on this IPS profile.
 - Define the security profile to protect the resources from malicious files.

Rule is enabled Logging is enabled [Edit](#)

Summary

Sources
 ZTA Enrolled Device
 Any ZTA Enrolled Device

Security Controls
 Security Profile: System Provided - Private Access
 IPS Profile is disabled for Global Settings

Destinations
 Any Private Resources

Rule name:
 Rule order:

☒ **Specify Access**
 Specify which users and endpoints can access which resources. [Help](#)

☒ **2 Configure Security**
 Configure security requirements that must be met before traffic is allowed. [Help](#)

Intrusion Prevention (IPS) [Rule Defaults](#)

Traffic that matches this rule will not be inspected by the intrusion prevention system. [Help](#)

☐ Disabled

Security Profile [Rule Defaults](#)

The following security settings will apply to traffic that matches this rule. [Help](#)

Security Profile: **System Provided - Private Access** | File Inspection: **Enabled** | File Type Blocking: **Disabled**

[Cancel](#)
[Back](#)
[Save](#)

Step 7 Save the configurations.

To understand more about private access policies in Secure Access, refer to [Get Started With Private Access Rules](#).

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.

By defining trusted networks, enabling TND, and integrating it with access policies, universal ZTNA enforces granular security controls. It ensures that access privileges are granted based not only on user identity but also on the security posture of the network connection.

To configure TND, add a trusted network and map it to a Threat Defense device.

Add a Trusted Network

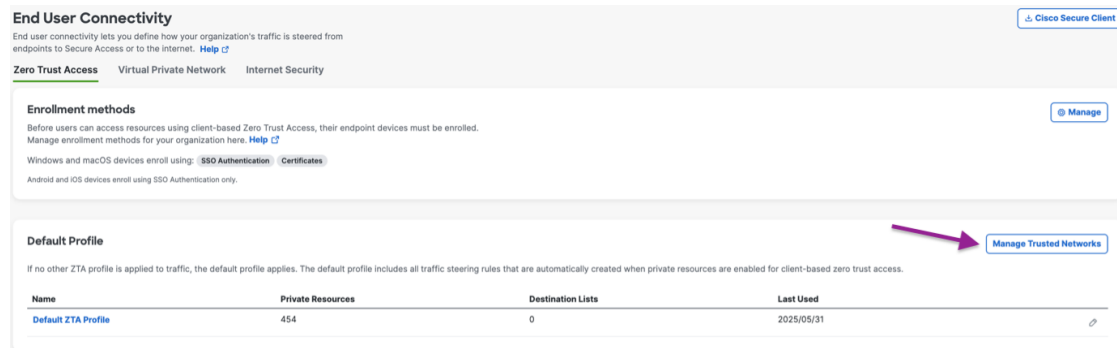
Define a trusted network by specifying a set of criteria such as DNS Servers, DNS Domains, and trusted servers. Secure Client uses these criteria to determine if an endpoint device is connected to the trusted network and routes the user's traffic accordingly.

Perform these steps to create a trusted network.

Before you begin

Procedure

- Step 1** In Cisco Security Cloud Control, click **Products > Secure Access**.
- The Secure Access product menu appears in the left navigation bar.
- Step 2** Click **Connect > End User Connectivity**.
- Step 3** Under the **Zero Trust Access** tab, click **Manage Trusted Networks**.



- Step 4** Click **+Add**.
- Step 5** On the **Add Trusted Networks** page, enter a name for the network. Then, define the criteria for the trusted network.

The screenshot shows the 'Add Trusted Networks' page. It has a 'Trusted Network Name' input field and a checkbox labeled 'Set as default Trusted Network for UZTA'. Below this, there's a section for 'Criterion' with a dropdown menu. The dropdown menu is open, showing 'Select one', 'DNS Servers', 'DNS Domains', and 'Trusted Servers'. A '+ Add Criterion' button is next to the dropdown.

(Optional) To set this network as the default trusted network, check the **Set as default Trusted Network for UZTA** check box.

You can choose one or more criteria for a trusted network.

- **DNS Servers:** Enter all DNS server addresses for the trusted network in the **DNS Servers** field, separated by commas. Secure Client treats a network as trusted if it matches any of these addresses.

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion DNS Servers ⓘ

DNS Servers

[+ Add Criterion](#)

- **DNS Domain:** Enter all DNS domain suffixes for the trusted network in the **DNS Domains** field, separated by commas. Secure Client treats a network as trusted if it matches any of these DNS domain suffixes.

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion DNS Domains ⓘ

DNS Domains

[+ Add Criterion](#)

- **Trusted Servers:** Enter a trusted server address in the **Trusted Servers** field. A DNS server that you specify in this profile must translate the domain name of the server to its IP address and provide a TLS certificate.

Multiple entries within each criterion are tested as OR: Any of the entered values can match.

Criterion

Trusted Servers

Trusted Servers ⓘ Certificate Hash ⓘ (optional)

1

[+ Add Trusted Server](#)

[+ Add Criterion](#)

(Optional) In the **Certificate Hash** field, enter the hash of the public key of this certificate.

(Optional) Click **+Add Trusted Server** to add up to 10 trusted servers.

Step 6

Click **Save**.

A trusted network is created.

What to do next

Assign this trusted network to a Threat Defense device.

Map a Trusted Network to a Threat Defense Device

If a default trusted network exists when a Threat Defense is added to the network, this default network is automatically mapped to the Threat Defense device.

If a default trusted network does not exist, map a trusted network to a device by performing the following steps.

Procedure

- Step 1** In Cisco Security Cloud Control, click **Products > Secure Access**.
The Secure Access product menu appears in the left navigation bar.
- Step 2** Click **Connect > Network Connections > FTD**.
- Step 3** Click the three dots (...) next to a Threat Defense device and select **Assign a Trusted Network** from the drop-down menu.

Network Connections read-only

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 2 FTDs [Edit Default Trusted Network](#) [Add FTD](#)

FTD Name	Version	FMC	UZTA Configuration status	Associated Resources	Rules Enforced	
sensor1_HA Device FQDN: www.cisco.com Trusted network: RK TND 07	v7.7.10	firepower.172.16.0.1	Synced	0	0	...

- View FTD Details
- Associate Resources
- Assign a Trusted Network
- View FTD in Security Devices

- Step 4** From the **Trusted Networks** drop-down list, select a trusted network to map to the device and click **Save**.

Map Trusted network to sensor1_HA

To allow this FTD to enforce policy for traffic originating on trusted networks, you must first associate the FTD with the applicable trusted networks. [Help](#)

Trusted Networks

RK TND 07 [+ Trusted network](#)

Cancel Save

The trusted network is now associated with the Threat Defense device.

Note

- If this Threat Defense device shares its fully qualified domain name (FQDN) with other devices, the trusted network is also mapped to those devices.
- A Threat Defense device can be associated with only one trusted network.

Associate Private Resources with Firewall Threat Defense

Before you begin

You must have created the private resources on Secure Access.

Procedure

Step 1 In Cisco Security Cloud Control, click **Products > Secure Access**.

Secure Access product menu displays in the left navigation bar.

Step 2 Click **Connect > Network Connections**.

Step 3 Click the **FTDs** tab.

The available Secure Firewall Threat Defense devices that are configured for universal zero trust network access are displayed.

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 Syncing

4 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 ...

Configuration status

5 FTDs

Edit Default Trusted Network

+ Add FTD

FTD Name	Version	FMC	UZTA Configuration status	Associated Resources	Rules Enforced
RKPMC-26May02_172.16.0.103 Device FQDN: www.rk92.aceme.com Trusted network: RKs TND 18	v7.7.10	RKPMC-26May02	Synced	7	5
RKPMC-26May02_172.16.0.101	v7.7.10	RKPMC-26May02	Synced	1	2

Ensure that the device is associated with a trusted network to enforce policies on traffic originating from the trusted network before proceeding to the next step.

After a Threat Defense device is onboarded, it is automatically associated with a default trusted network if one exists. Otherwise, you must [create a trusted network](#) and associate it with the Threat Defense device.

Step 4 Click the name of a Threat Defense device to configure.

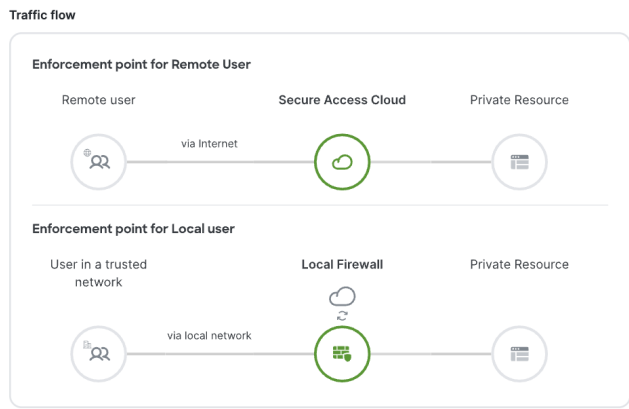
Step 5 In the right pane, click **Associate Resources**.

Note

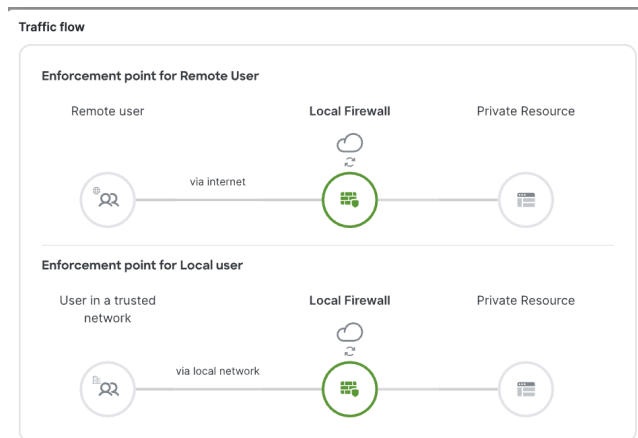
- Only those resources that are enabled for zero trust access may associate with a Threat Defense device.
- A Threat Defense device must reach the associated private resources.
- Resources associated with a Threat Defense device are shared with other devices with the same FQDN.

Step 6 In the **Associate Private Resources** dialog box, make the following selections to specify the access policy enforcement and traffic flow for a user:

- **Use Threat Defense device to enforce policy only for on-premises users:** From the **Use this FTD to enforce policy** drop-down list, select the private resources, which a user should be able to access only from an on-premises location.



- **Use Threat Defense device to enforce policy for both on-premises and remote users:** From the **Always use this FTD to enforce policy** drop-down list, select the private resources for which the selected Threat Defense device always enforces policy, regardless of whether the user is located on-premises or is remote.



The following figure shows an example of using a Threat Defense device to enforce access rules for the **vfdd-quic-app** for on-premises users and **vfdd-amazon-app** for all users, whether on-premises or remote.

Associate Private Resources with FTD: **vfdd-quic-app**

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.

i 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 ⓘ

vfdd-quic-app × Select an option ▼

Always use this FTD to enforce policy for these private resources ⓘ

vfdd-amazon-app × Select an option ▼

Cancel

Save

Step 7 Click **Save**.

The configurations are applied to the device, and the **UZTA Configuration status** column for the device displays **Synced**. The following figure shows an example.

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 Syncing

4 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](#).

5 FTDs
[Edit Default Trusted Network](#)
[+ Add FTD](#)

FTD Name	Version	FMC	UZTA Configuration status	Associated Resources	Rules Enforced	
RKPMC-26May02_172.16.0.103 Device FQDN: www.rk92.acme.com Trusted network: RKs TND 10	v7.7.10	RKPMC-26May02	Synced	7	5	...
RKPMC-26May02_172.16.0.101 Device FQDN: www.rk91.acme.com Trusted network: RKs TND 10	v7.7.10	RKPMC-26May02	Synced	1	2	...
RKPMC-26May02_172.16.0.102 Device FQDN: www.rk93.acme.com Trusted network: RKs TND 10	v7.7.10	RKPMC-26May02	Synced	1	2	...

Configuration status can also be:

- Syncing—updates to the Threat Defense device are ongoing.
- Out of sync—modifications to Secure Access configurations are pending update to the Threat Defense device.
- Failed to sync—configurations were not updated on the Threat Defense device.

To view a detailed and granular status for each resource and rule associated with a Threat Defense device, perform the actions outlined:

- Click the numeral in the **Associated Resources** column.

In the slide-in pane, under the **Associated Resources** section, click **View resources associated with this FTD**.

firepower_172.16.0.1_sensor1

Trusted network

Networks

RKs TND 10

(Default trusted network)

1 Trusted Servers

Edit assignment

+ Trusted network

Associated Resources

2

RESOURCES ASSOCIATED BY STATUS

Status

✓ Synced

2

View resources associated to this FTD

Associate Resources

The configuration status of each resource is displayed.

Resources associated with firepower_172.16.0.1_sensor1

The following resources will get enforced on firepower_172.16.0.1_sensor1 when users connect to it from the trusted network RKs TND 10

Q Search by resource name

✓ Synced

⊗

⌵

2 Resources

Associate Resources

Resource name

Status

RK-PrivateResource-4398

✓ Synced

RK-PrivateResource-4469

✓ Synced

Close

- b) Similarly, to check the configuration status of each rule that is enforced by the Threat Defense device, click the numeral in the **Rules Enforced** column.

In the slide-in pane, under the **Rules Enforced** section, click **View rules enforced by this Firewall**.

firepower_172.16.0.1_sensor1

[Edit assignment](#) [Trusted network](#)

Associated Resources 2

RESOURCES ASSOCIATED BY STATUS

Status
<input checked="" type="checkbox"/> Synced 2

[View resources associated to this FTD](#)

[Associate Resources](#)

Rule enforced 2

RULES ENFORCED BY STATUS

Status
<input checked="" type="checkbox"/> Synced 2

[View rules enforced by this Firewall](#)

The configuration status of each rule that is enforced is displayed.

Rules enforced on firepower_172.16.0.1_sensor1

The following rules are enforced on firepower_172.16.0.1_sensor1

☒ Synced 2 Rules

Rule name	Status
16June-AnytoAny	<input checked="" type="checkbox"/> Synced
For all private access -RK	<input checked="" type="checkbox"/> Synced

[Close](#)

Universal ZTNA is now set up for your clients to securely access the private resources in your network.
