

Zero Trust Network Access Overview

Zero Trust Network Access (ZTNA) secures internal resources by verifying user identity and device posture to grant least-privilege access. Organizations implement either browser-based Clientless ZTNA for web applications or agent-based Universal ZTNA for comprehensive, protocol-wide support using existing threat defense infrastructure.

- Zero Trust Access, on page 1
- History for zero trust network access, on page 16

Zero Trust Access

Zero Trust Access is based on Zero Trust Access principles. Zero Trust Access is a zero trust security model that eliminates implicit trust. The model grants the least privilege access after verifying the user, the context of the request, and after analyzing the risk if access is granted.

Zero Trust Access enables you to authenticate and authorize access to protected web-based resources and applications from inside (on-premises) or outside (remote) the network using an external Security Assertion Markup Language (SAML) identity provider (IdP) policy.

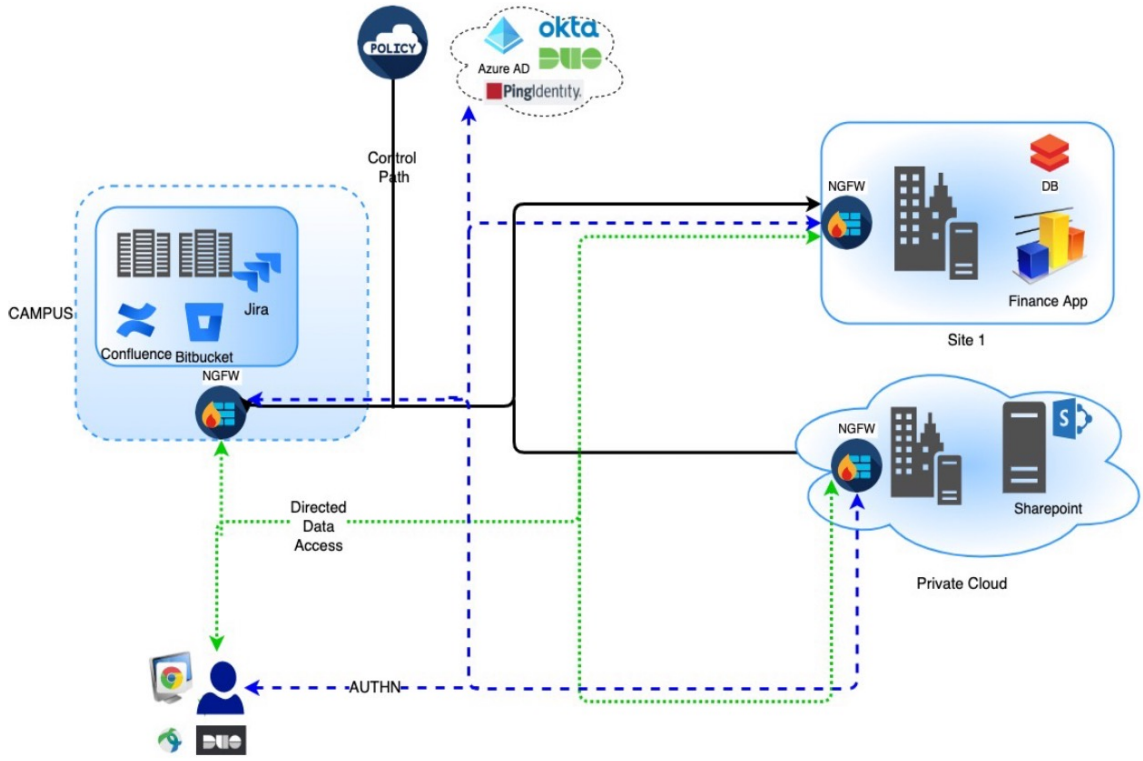
The features are:

- Supports multiple SAML-based identity providers such as Duo, Azure Active Directory (Azure AD), Okta, and other identity providers.
- Client applications such as Cisco Secure Client are not required on the endpoint (client devices) for secure access.
- Access and authentication is through the browser.
- Supports only TLS web applications.
- Client device posture is supported through agents such as Duo Health, using which the posture of the device can be evaluated against a policy in Duo, and access can be provided based on the same. The same functionality can be performed in conjunction with third-party identity providers that support posture evaluation with their agents such as Okta or PingID.
- Supports HTTP-Redirect SAML binding.
- Supports application groups that make it easier to enable zero trust access protection on a set of applications.
- Leverages threat defense intrusion and malware protection on zero trust application traffic.

You can use the Secure Firewall Management Center web interface to create a Zero Trust Application Policy that allows you to define private applications and assign threat policies to them. The policy is application specific where the administrator decides the inspection levels based on the threat perception for that application.

How Threat Defense Works with Zero Trust Access

Figure 1: Threat Defense Deployment



1. Using a browser, a remote or on-prem user sends a HTTPS request to connect to an application from an endpoint.
2. The HTTPS request is intercepted by the firewall that protects the application.
3. The firewall redirects the user to application's configured IdP for authentication.

Note In the figure, each firewall protects a set of web applications. The user can directly access the applications behind the firewall after authentication and authorization.

4. After the authentication and authorization process is complete, the firewall allows the user to access the application.

Zero trust network access

Zero Trust Network Access (ZTNA) provides secure, segmented application access by requiring explicit authorization for every connection. This approach reduces the attack surface and simplifies secure migrations without adding devices.

Key characteristics

ZTNA uses your existing Threat Defense deployment as an enforcement point for application access, enabling segmented and per-application authorization. ZTNA establishes individual tunnels for both remote and on-premises users.

ZTNA hides the network from users and ensures that they can only access applications for which they have been explicitly authorized. Authorization for one application does not provide implicit access to other applications, which significantly reduces the attack surface. In other words, every access to an application or a resource must be explicitly authorized.

You can adopt a more secure access model by adding zero trust access functionality to Threat Defense. This eliminates the need to install or manage additional devices in the network.

Components of a Clientless Zero Trust Network Access Configuration

A new configuration consists of a Zero Trust Application Policy, Application Group, and Applications.

- **Zero Trust Application Policy**— Consists of application groups, and grouped or ungrouped applications. Security Zones and Security Controls settings are associated at a global level for all the ungrouped applications and group of applications.

  A global port pool is assigned to the policy, by default. A unique port is automatically assigned from this pool to each private application that is configured.

  Zero Trust Application policy consists of application groups, and grouped or ungrouped applications.

- **Application Groups**—Consists of a logical group of applications that share SAML authentication settings and can optionally share Security Zones and Security Controls settings.

  Application Groups inherit the Security Zones and Security Controls settings from the global policy and can override the values.

  When an Application Group is created, the same SAML IdP configuration can be used for authenticating multiple applications. Applications that are part of an Application Group inherit the Application Group's SAML configuration. This eliminates the need to configure the SAML settings for each application. After the Application Group is created, new applications can be added to it without configuring the IdP for it.

  When an end user tries to access an Application that is part of group, the user is authenticated to the Application Group for the first time. When the user tries to access other applications that are part of the same Application Group, the user is provided access without being redirected again to the IdP for authentication. This prevents overloading the IdP with requests for application access and optimizes the usage of the IdP if a limit is enabled.

- **Applications**—There are two types:

  - **Ungrouped Applications**— Are standalone applications. SAML settings must be configured for every application. The applications inherit the Security Zones and Security Controls settings from the global policy and can be overridden by the application.

- **Grouped Applications**— Are multiple applications that are grouped under an Application Group. The SAML settings are inherited from the Application Group and cannot be overridden. However, the Security Zones and Security Controls settings can be overridden for each application.

The following certificates are required for the configuration:

- **Identity Certificate**—This certificate is used by Firewall Threat Defense to masquerade as the applications. Firewall Threat Defense behaves as a SAML Service Provider (SP). This certificate must be a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of the private applications. It is a common certificate for all applications protected by Firewall Threat Defense. Upload the public key from the same certificate to the identity provider (IDP), designating it as the SP certificate. The identity provider uses this certificate to verify the authentication request it receives. By default, Firewall Threat Defense signs the SAML authentication request before sending it to IDP. You cannot disable authentication request signing, and it is not configurable.
- **IdP Certificate**—The IdP provides a certificate for each defined Application or Application Group. This certificate must be configured so that Firewall Threat Defense can verify the IDP's signature on incoming SAML assertions.

Note IdP certificates are commonly included within the metadata file; otherwise, users are required to have the IdP certificate readily available during the configuration of applications.

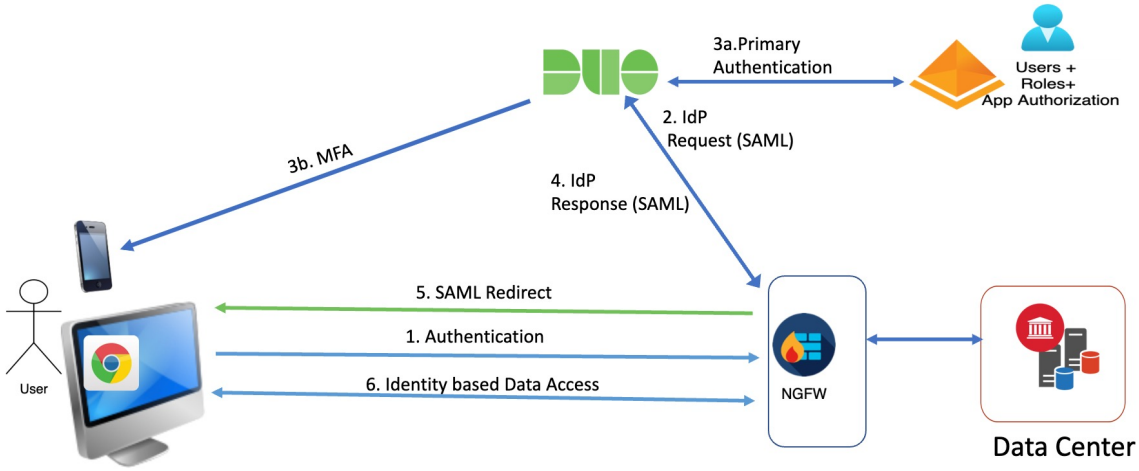
- **Application Certificate**—The encrypted traffic from user to the application is decrypted by Firewall Threat Defense using this certificate for the purpose of inspection.

Note This certificate is required to verify the cookies in the header to authorize connections, even if we are not conducting an IPS/Malware inspection.

Clientless Zero Trust Network Access Workflow

This figure depicts the Zero Trust Access workflow.

Figure 2: Clientless Zero Trust Network Access Workflow



The workflow is as follows:

1. User types the application URL in the browser.
   - If the HTTPS request is valid, the user is redirected to the mapped port (Step 6).
   - If the HTTPS request is invalid, the user is sent for authentication per application (Step 2).
2. The user is redirected to the configured identity provider (IdP).
3. **a.** The user is redirected to the configured primary authentication source.
   b. The user is challenged with the configured secondary multi-factor authentication, if any.
4. The IdP sends a SAML response to threat defense. The user ID and other necessary parameters are retrieved from the SAML response through the browser.
5. The user is redirected to the application.
6. The user is allowed access to the application after validation is successful.

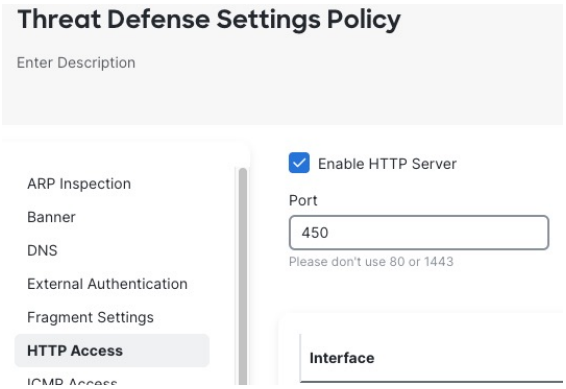
Limitations for Clientless Zero Trust Network Access

- Supports only TLS-enabled web applications. All traffic must be decrypted.
- Supports only SAML identity providers.
- IPv6 is not supported.

  NAT66, NAT64, and NAT46 scenarios are not supported.
- Clientless zero trust network access is available on Firewall Threat Defense only if Snort 3 is enabled.
- By default, the Firewall Threat Defense device uses port 443 for secure communications. Because this is the same port used by TLS-enabled applications likely to be configured for zero trust network access, you must change the device's HTTP server port.

Go to **Devices** > **Platform Settings**, then edit the Threat Defense Settings policy for the device, click **HTTP Access**, select the **Enable HTTP Server** check box, and enter a port other than 443 in the field. When you're finished, click **Save** in the upper right corner of the page.

The following figure shows an example.



- All hyperlinks in protected web applications must have a relative path and are not supported on individual mode clusters.
- Protected web applications running on a virtual host or behind internal load balancers must use the same external and internal URL.
- Not supported on applications with strict HTTP Host Header validation enabled.
- If the application server hosts multiple applications and serves content based on the Server Name Indication (SNI) header in the TLS Client Hello, the external URL of the zero trust application configuration must match the SNI of that specific application.

Prerequisites for Zero Trust Application Policy

Prerequisite Type	Description
Licensing	• Smart license account with export-controlled features • (Optional) IPS and Threat licenses—It is required if security controls are used.
Configurations	Create a wildcard or Subject Alternative Name (SAN) certificate that matches the FQDN of private applications. For more information, see Add certificate enrollment objects.
	Create a security zone through which access to private applications are regulated. For more information, see Create security zone and interface group objects.

Manage Zero Trust Application Policies

You can create, edit, and delete zero trust application policies.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Manage the zero trust access policies:

- Create—Click **New Policy**. See Create a Zero Trust Application Policy, on page 7
- Edit—Click **Edit** ( ). See Edit a Zero Trust Application Policy, on page 12
- Report—Click **Report** ( ).
- Delete—Click **Delete** ( ).

Step 3 Click **Save**.

What to do next

Ensure that there are no warnings before you deploy the configuration to threat defense. To deploy configuration changes, see Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create a Zero Trust Application Policy

This tasks configures a Zero Trust Application Policy.

Before you begin

Ensure that you complete all the prerequisites listed in Prerequisites for Zero Trust Application Policy, on page 6.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**.

Step 2 Click **Add Policy**.

Step 3 In the **General** section, enter the policy name in the **Name** field. The description field is optional.

Step 4 Enter a domain name in the **Domain Name** field.

Ensure that the domain name is added to the DNS. The domain name resolves to the Firewall Threat Defense gateway interface from where the application is accessed. The domain name is used to generate the ACS URL for all private applications in an Application Group.

Step 5 Choose an existing certificate from the **Identity Certificate** drop-down list.

Click the **Add** (+) icon to configure a certificate enrollment object. For more information, see Add certificate enrollment objects.

Step 6 Choose a security zone from the **Security Zones** drop-down list.

Click the **Add** (+) icon to add a new security zone.

To add security zones, see Create security zone and interface group objects.

Step 7 In the **Global Port Pool** section, a default port range is displayed. Modify, if required. Port values range from 1024 to 65535. A unique port from this pool is assigned to each private application.

Note This port range should avoid any conflicts with the existing NAT range.

Step 8 (Optional) In the **Security Controls** section, you can add an Intrusion or Malware and File policy:

- **Intrusion Policy**—Choose a default policy from the drop-down list or click the **Add** (+) icon to create a new custom intrusion policy. For more information, see Creating a Custom Snort 3 Intrusion Policy topic in the latest version of the Cisco Secure Firewall Management Center Snort 3 Configuration Guide.
- **Variable Set**—Choose a default variable set from the drop-down list or click the **Add** (+) icon to create a new variable set. For more information, see Create a variable set.

Note To use variable sets, you must have the Secure Firewall Threat Defense IPS license for your managed devices.

- **Malware and File Policy**—Choose an existing policy from the drop-down list. Click the **Add** (+) icon to create a new malware and file policy. For more information, see Manage file policies.

Step 9 Click **Save** to save the policy.

What to do next

1. Create an Application Group. See Create an Application Group, on page 9.
2. Create an Application. See Create an Application, on page 10.
3. Associate a Zero Trust Application Policy with a device. See Set Targeted Devices for Zero Trust Access Policy, on page 12
4. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create an Application Group

Before you begin

Create a Zero Trust Application Policy, on page 7

Procedure

Step 1 Click **Add Application Group**.

Step 2 In the **Application Group** section, type the name in the **Name** field and click **Next**.

Step 3 In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the values of the **Entity ID** and **Assertion Consumer Service (ACS) URL** fields or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.

Step 4 In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:

- **XML File Upload**—Choose a file or drag and drop the XML file.

  The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.

- **Manual Configuration**—Perform these steps:
  - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
  - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.
  - **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

    Click the **Add** (+) icon to configure a new certificate enrollment object. For more information, see Add a certificate enrollment.

- **Configure Later**—In the event you do not have the IdP metadata, you can configure it later.

Click **Next**.

Step 5 In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**.

The re-authentication interval allows you to provide a value that determines when a user must authenticate again.

Step 6 In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy. You can override these settings. Click **Next**.

Step 7 Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.

Step 8 Click **Save**.

The Application Group is created and is displayed on the Zero Trust Application page.

What to do next

1. Create an Application, on page 10.

2. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Create an Application

Use this task to create a Grouped or Ungrouped Application.

Before you begin

1. Create a Zero Trust Application Policy, on page 7.
2. Create an Application Group, on page 9 (required only for Grouped Applications).

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Choose the policy.

Step 3 Click **Add Application**.

Step 4 In the **Application Settings** section, complete the following fields.

- **Application Name**—Enter the application name.
- **External URL**—Enter the URL that is used by the user to access the application.
- **Application URL**—By default, the external URL is used as the Application URL. Uncheck the **Use External URL as Application URL** check box to specify a different URL.

  If Threat Defense uses an internal DNS, the Application URL must match an entry within that DNS to ensure it resolves to the application.

- **Application Certificate**—Choose the certificate for the private application. Click the **Add** (+) icon to configure an internal certificate object. For more information, see Add internal certificate objects.
- **IPv4 Source Translation**—Choose the source network for NAT from the list. Click **Add** (+) to create a network object. For more information, see Networks.

  This Network Object or Object Group is used to translate a public network source IPv4 address of an incoming request to a routable IPv4 address inside the corporate network.

Note Only object or object groups of type Host or Range are supported.

- **Application Group**—Choose the Application Group from the drop-down list. See Create an Application Group, on page 9.

Note This field is not applicable for an ungrouped application.

Step 5 Click **Next**.

Step 6 Depending on the type of application:

- For a Grouped Application, the **SAML Service Provider (SP) Metadata**, **SAML Identity Provider (IdP) Metadata** , and **Re-authentication Interval** are inherited from the Application Group and do not need to be configured by the user.
- For an Ungrouped Application, perform these steps:

  a. In the **SAML Service Provider (SP) Metadata** section, the data is dynamically generated. Copy the **Entity ID**, **Assertion Consumer Service (ACS) URL** of the IdP, or click **Download SP Metadata** to download this data in XML format for adding it to the IdP. Click **Next**.

  b. In the **SAML Identity Provider (IdP) Metadata** section, add the metadata using any one of the methods:

  - **XML File Upload**—Choose a file or drag and drop the XML file.

    The details of the **Entity ID**, **Single Sign-On URL**, and **IdP Certificate** are displayed.

  - **Manual Configuration**—Perform these steps:
    - **Entity ID**—Enter the URL that is defined in the SAML IdP to identify a service provider uniquely.
    - **Single Sign-On URL**—Enter the URL for signing into the SAML identity provider server.
    - **IdP Certificate**—Choose the certificate of the IdP enrolled in threat defense to verify the messages signed by the IdP.

      Click the **Add** (+) icon to configure a new certificate enrollment object. For more information, see Add a certificate enrollment.

  - **Configure Later**—If you do not have the IdP metadata, you can configure it later.

  Click **Next**.

  c. In the **Re-authentication Interval** section, enter the value in the **Timeout Interval** field and click **Next**. The reauthentication interval allows you to provide a value that determines when a user must authenticate again.

Step 7 In the **Security Zones and Security Controls** section, the security zones and threat settings are inherited from the parent policy or application group. You can override these settings. Click **Next**.

Step 8 Review the configuration summary. Click **Edit** to modify the details in any of the sections. Click **Finish**.

Step 9 Click **Save**.

The application is listed on the Zero Trust Application page and enabled by default.

What to do next

1. Set Targeted Devices for Zero Trust Access Policy, on page 12.
2. Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Set Targeted Devices for Zero Trust Access Policy

Each Zero Trust Application policy can target multiple devices; each device can have one deployed policy at a time.

Before you begin

1. Create a Zero Trust Application Policy, on page 7.
2. Create an Application Group, on page 9.
3. Create an Application, on page 10.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Choose the policy.

Step 3 Click **Targeted Devices**.

Step 4 Choose the devices where you want to deploy the policy using any one of the methods:

- Choose a device in the **Available Devices** list and click >> or the **Add** ( ) icon.
- To remove a device from the **Selected Devices** list, choose a device and click << or the **Delete** ( ) icon.

Step 5 Click **Apply** to save policy assignments.

Step 6 Click **Save** to save the policy.

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Edit a Zero Trust Application Policy

You can edit the settings of a Zero Trust Application Policy, Application Group, or Application.

Procedure

Step 1 Choose **Policies** > **Zero Trust Application**

Step 2 Click **Edit** ( ) next to the Zero Trust Application Policy you want to edit.

Step 3 Edit your Zero Trust Application Policy.

You can change the following settings or perform these actions:

- Name and Description—Click **Edit** ( ) next to the policy name, make your changes, and click **Apply**.

- To modify the policy settings:
  - Click **Settings**
  - Modify the settings as required.



Important Editing the domain name for the SAML ACS URL interrupts application access.

  - Click **Save**.

- To modify the Application Group settings:
  - Click **Applications**.
  - Click **Edit** (✎) next to the Application Group you want to edit.
  - In each section, click **Edit** to modify the settings, as required



Important Editing the Application Group name interrupts application access.

  - Click **Apply** after you modify the settings in a section.
  - Click **Finish**.
  - Click **Save**.

- To modify the Application settings:
  - Click **Applications**.
  - Click **Edit** (✎) next to the Application you want to edit.
  - In each section, click **Edit** to modify the settings, as required.



Important Editing the Application name interrupts application access.

  - Click **Apply** after you modify the settings in a section.
  - Click **Finish**.
  - Click **Save**.

- To enable, disable, or delete multiple Applications, choose the Applications, click the required bulk action, and click **Save**.



Note These actions are also available in the right-click menu.

  - To enable all Applications, click **Bulk Actions** > **Enable**.

- To disable all Applications, click **Bulk Actions** > **Disable**.
- To delete all Applications, click **Bulk Actions** > **Delete**.

- Click **Return to Zero Trust Application** to return to the policy page.

What to do next

Deploy configuration changes. See Deploy Configuration Changes in the Cisco Secure Firewall Management Center Administration Guide.

Monitor Zero Trust Sessions

Connection Events

After a Zero Trust Application Policy is deployed, new fields are available. To add the fields to the table view:

1. Choose **Analysis** > **Unified Events**.
2. Click the column picker ( ) icon and add these columns:
   - **Authentication Source**
   - **Zero Trust Application**
   - **Zero Trust Application Group**
   - **Zero Trust Application Policy**
3. Click **Apply**.

See the Connection and Security-Related Connection Events in the Secure Firewall Management Center Administration Guide for more information on the connection events.

Zero Trust Dashboard

The Zero Trust dashboard allows you to monitor real-time data from active zero trust sessions on the devices.

The Zero Trust dashboard provides a summary of the top zero trust applications and zero trust users that are managed by the management center. Choose **Overview** > **Dashboards heading** > **Dashboard**, and click the **Zero Trust** tab to access the dashboard.

The dashboard has the following widgets:

- Top Zero Trust Applications
- Top Zero Trust Users

CLI Commands

Log in to the device CLI and use the following commands:

CLI Command	Description
show running-config zero-trust	To view the running configuration for a zero trust configuration.
show zero-trust	To display the run-time zero trust statistics and session information.
show cluster zero-trust	To display the summary of zero trust statistics across nodes in a cluster.
clear zero-trust	To clear zero trust sessions and statistics.
show counters protocol zero_trust	To view the counters that are hit for zero trust flow.

Diagnostics Tool

The diagnostics tool facilitates the troubleshooting process by detecting possible issues with zero trust configurations. The diagnostics can be classified into two types:

- **Application-specific diagnostics** are used to detect issues such as:
  - DNS-related issues
  - Misconfigurations such as socket not open, and issues with classification and NAT rules.
  - Issues with deployment of zero trust policy or SSL rules
  - Issues with source NAT issues and exhaustion of PAT pool
- **General diagnostics** are used to detect issues such as:
  - Strong cipher license not enabled
  - Invalid application certificate
  - SAML-related issues
  - Home agent and cluster bulk sync issues

To run the diagnostic tool:

1. Click Diagnostics ( ) next to the zero trust application that you want to troubleshoot. The **Diagnostics** dialog box appears.
2. Choose the device from the **Select Device** drop-down list and click **Run**. A report is generated in the **Reports** tab after the diagnostic process is complete.
3. To view, copy, or download the logs, click the **Logs** tab.

History for zero trust network access

This reference provides the minimum Firewall Management Center and Threat Defense versions needed to support zero trust application policies and monitoring.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Zero trust access enhancements.	7.4.1	7.4.1 with Snort 3	Firewall Management Center now includes the following zero trust access enhancements: • You can configure source NAT for an application. The configured network object or object group translates the incoming request's public network source IP address to a routable IP address inside the application network. • You can troubleshoot the zero trust configuration issues using the diagnostics tool. New/modified screens: **Policies** > **Access Control** > **Zero Trust Application** New/modified CLI commands: **show running-config zero-trust**, **show zero-trust statistics**
Clientless zero-trust access.	7.4.0	7.4.0 with Snort 3	Zero Trust Access allows you to authenticate and authorize access to protected web based resources, applications, or data from inside (on-premises) or outside (remote) the network using an external SAML Identity Provider (IdP) policy. The configuration consists of a Zero Trust Application Policy (ZTAP), Application Group, and Applications. New/modified screens: • **Policies** > **Zero Trust Application** • **Analysis** > **Connections** > **Events** • **Overview** > **Dashboard** > **Zero Trust** New/modified CLI commands: • **show running-config zero-trust application** • **show running-config zero-trust application-group** • **show zero-trust sessions** • **show zero-trust statistics** • **show cluster zero-trust statistics** • **clear zero-trust sessions application** • **clear zero-trust sessions user** • **clear zero-trust statistics**