

Identity Source: Remote Access VPN

The following topics discuss how to perform user awareness and user control with Remote Access VPN:

- Remote access VPN identity sources, on page 1
- Configure Remote Access VPN for AD-authenticated users, on page 2
- Remote Access VPN for Microsoft Entra ID-authenticated users (Beta), on page 3
- Hybrid Entra ID and on-premises AD deployments, on page 5
- Troubleshooting guidelines for remote access VPN identity source, on page 6

Remote access VPN identity sources

A remote access VPN identity source authenticates a user before establishing secure remote connection to the network. It requires the user to provide credentials through a client to verify the identity.

Identity source configuration

Secure Client is the only client supported on endpoint devices for remote VPN connectivity to Firewall Threat Defense devices.

When you set up a secure VPN gateway as discussed in Configure a remote access VPN policy, you can set up an identity policy for those users and associate the identity policy with an access control policy, provided your users are in an Active Directory repository.

Note If you use remote access VPN with User Identity and RADIUS as the identity source, you must configure the required RADIUS Server Group (**Objects** > **AAA Server** > **RADIUS Server Group**). Configure a realm separately when the selected user-awareness or user-control workflow requires one.

The login information provided by a remote user is validated by an LDAP or AD realm or a RADIUS server group. These entities are integrated with the Secure Firewall Threat Defense secure gateway.

Note If users authenticate with remote access VPN using Active Directory as the authentication source, users must log in using their username; the format domain\username or username@domain fails. (Active Directory refers to this username as the logon name or sometimes as sAMAccountName.) For more information, see User Naming Attributes on MSDN.

If you use RADIUS to authenticate, users can log in with any of the preceding formats.

Once authenticated through a VPN connection, the remote user takes on a VPN identity. This VPN identity is used by identity policies on the Secure Firewall Threat Defense secure gateway to recognize and filter network traffic belonging to that remote user.

Identity policies are associated with access control policies, which determine who has access to network resources. It is in this way that a remote user blocked or allowed to access your network resources.

Related Topics

Secure Connections Overview
Remote access VPN
VPN basics
Configure a remote access VPN policy

Configure Remote Access VPN for AD-authenticated users

Configure remote access VPN for Active Directory-authenticated users. Manage VPN connections and apply identity-based policies to control user access and traffic filtering.

Remote access VPN user control allows you to implement identity-based policies that manage and monitor VPN user connections, providing enhanced security and access control for your network environment.

Before you begin

- Create a realm as discussed in Create an LDAP realm or an Active Directory realm and realm directory.
- To use authentication, authorization, and accounting (AAA), set up a RADIUS server group as discussed in Add a RADIUS server group.

Follow these steps to configure RA VPN for user control:

Procedure

Step 1 Log in to the Firewall Management Center.

Step 2 Click **Secure Connections** > **Remote Access VPN**.

Step 3 See Configure a remote access VPN policy.

Step 4 Specify users to control and other options using an identity policy as described in Create an identity policy.

Step 5 Associate the identity policy with an access control policy, which filters and optionally inspects traffic, as discussed in Associate prefilter, decryption, and identity policies with an access control.

Step 6 Deploy your identity and access control policies to managed devices as discussed in Deploy configuration changes.

What to do next

Monitor VPN user traffic .

Remote Access VPN for Microsoft Entra ID-authenticated users (Beta)

Microsoft Entra ID (formerly Azure AD) remote access virtual private network (RA VPN) support lets Secure Firewall use Microsoft Entra ID-authenticated VPN sessions for identity-aware access control. After a user signs in through Security Assertion Markup Language (SAML), the system enriches the session with realm and group information so Snort can enforce access control rules based on Entra ID users and groups.

Guidelines for configuring RA VPN Entra ID support

- Create an Azure SSO object for SAML authentication.
- Create an Azure AD realm using the same Azure tenant as your Azure SSO object.
- Enable Dynamic Attributes Connector when Cloud-Delivered Firewall Management Center prompts you during realm creation.
- You do not need to attach a separate identity policy for access control because identity is available when the VPN session is established and enriched.

Configure Entra ID Remote Access VPN support (Beta)

Set up remote access VPN identity to support Entra ID (formerly Azure AD)-authenticated users and groups.

This task allows you to leverage Entra ID for remote VPN user authentication and group mapping, enabling advanced access control policies.

Before you begin

Note Use the same Azure tenant for the Azure SSO object and the Azure AD realm. If these configurations do not match, users can authenticate successfully but do not receive the group data that is required for identity-based access control.

- The managed devices must run version 10.1 or later.
- Entra ID Remote Access VPN is not supported on clustered devices.

Procedure

Step 1 In Cloud-Delivered Firewall Management Center, register the Smart License.

Confirm that the target Firewall Threat Defense device is licensed for remote access VPN.

Step 2 Create the Azure SSO object with the Identity Provider (IdP) and service provider details that Azure AD requires. For information, refer to Add a Single Sign-On server.

Note the Entity ID identifier value.

Step 3 Configure or edit the remote access VPN connection profile to use SAML authentication, as discussed in Create a new Remote Access VPN Policy.

Note Use the Entity ID value (Azure SSO object) as the connection profile name so the profile matches Azure AD SAML configuration. This is essential for proper authentication of users.

Select the Azure SSO object as the authentication server for the connection profile.

Step 4 Create a SAML Azure AD realm as discussed in Create a Microsoft Azure AD (SAML) Realm

Step 5 Configure Access Control Rules: Open the access control policy and add or edit a rule as discussed in Create and edit access control rules.

On the **Users** tab, select the Azure AD users or groups that matches the rule.

Step 6 Deploy the configuration changes to the managed Firewall Threat Defense device.

What to do next

Verify the configuration as discussed in Verify the Microsoft Entra ID RA VPN configuration, on page 4

Verify the Microsoft Entra ID RA VPN configuration

After you have configured Microsoft Entra ID remote access VPN, verify that the configuration is successful.

To verify successful Microsoft Entra ID remote access VPN configuration, ensure the following criteria are met:

- The managed device successfully accepts connections from Secure Client, using Azure AD as the authenticator.
- The Task Manager in the Firewall Management Center UI confirms a successful user or group download.
- These views help you find key user and session details:
  - The user activity dashboard (**Events & Logs** > **Users** > **User Activity**) and VPN dashboard (**Insights & Reports** > **VPN Dashboards**) displays login, logoff, and event visibility across the session lifecycle.

- The active sessions view (**Events & Logs** > **Users** > **Active Sessions**) in Firewall Management Center displays the user, internal IP address, and realm data.

Hybrid Entra ID and on-premises AD deployments

The hybrid Entra ID and on-premises AD deployment model enables secure, flexible authentication and authorization for remote access users, provided the correct policy order and rule configuration are maintained.

In a hybrid deployment, remote access VPN users can authenticate with Microsoft Entra ID (formerly Azure AD). Cisco ISE authorizes the session and Firewall Management Center uses an on-premises Microsoft Active Directory realm for user identity and user-based access control. In this deployment model:

- Remote access VPN (RA VPN) is configured on Firewall Threat Defense
- Microsoft Entra ID or Azure is used as the SAML identity provider for VPN authentication
- Cisco ISE is used for session authorization
- Cisco ISE authorization policies may include both Microsoft Entra ID/Azure and on-premises AD rules or conditions
- Firewall Management Center uses the on-premises AD domain as the realm for user identity and user enforcement

Best practice: ISE authorization policy order for hybrid deployments

Beginning with Cisco ISE Release 3.4 Patch 4, when ISE evaluates an Entra ID identity source during authorization, it associates Entra ID attributes with the session. If Firewall Management Center uses an on-premises AD realm, the presence of Entra ID attributes may prevent correct user-to-IP mapping for RA VPN sessions. Identity-based access control rules that depend on user or group identity might not match as expected.

To prevent this issue:

Place ISE authorization rules that use the on-premises AD external identity source before rules that evaluate Entra ID or Azure conditions for the same users. This ensures that the session attributes published to FMC through pxGrid align with the configured on-premises AD realm.

After configuring the authorization policy order, verify that new RA VPN sessions create user mappings in Firewall Management Center and that user-based or group-based access control rules match as expected.



Note This behavior applies to Cisco ISE Release 3.4 Patch 4 and later. If user mappings stopped appearing after an ISE upgrade, review the ISE authorization policy order as described in this section.

Troubleshooting guidelines for remote access VPN identity source

For other related troubleshooting information, see Troubleshoot realms and user downloads and Troubleshoot user control.

If you experience issues with Remote Access VPN, check the connection between your Cloud-Delivered Firewall Management Center and a managed device. If the connection fails, all Remote Access VPN logins reported by the device cannot be identified during the downtime, unless the users were previously seen and downloaded to the Cloud-Delivered Firewall Management Center.

The unidentified users are logged as Unknown users on the Cloud-Delivered Firewall Management Center. After the downtime, the Unknown users are reidentified and processed according to the rules in your identity policy.

The host name of the managed device must be less than 15 characters for Kerberos authentication to succeed.

Active FTP sessions are displayed as the **Unknown** user in events. This is normal because, in active FTP, the server (not the client) initiates the connection and the FTP server should not have an associated user name. For more information about active FTP, see RFC 959

Not Observing Correct Settings for VPN Statistics

This task ensures that managed devices receive the correct health policy settings after modifying VPN statistics configurations.

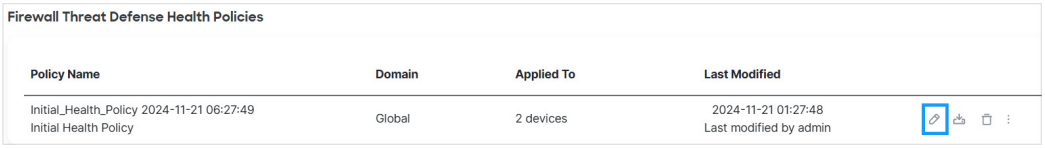
This task discusses steps you must take after either enabling or disabling the **VPN Statistics** setting in a health policy. Failure to perform this task means managed devices have a health policy with incorrect settings.

Procedure

Step 1 Log in to the Cloud-Delivered Firewall Management Center if you haven't already done so.

Step 2 Click **Troubleshooting** > **+ Show more** > **Health** > **Policies**.

Step 3 Under Firewall Threat Defense Health Policies, click **Edit** (✎) next to a policy to edit.



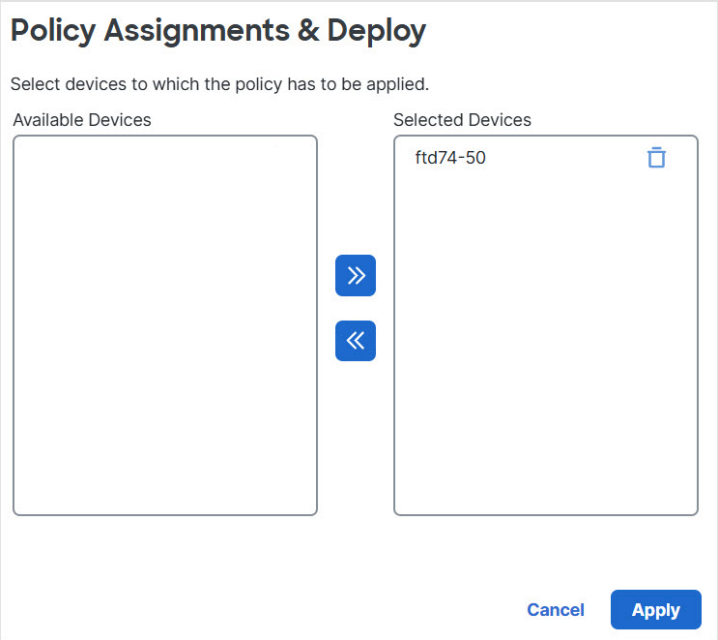
Step 4 On the **Health Modules** tab page, scroll down to locate **VPN Statistics**.

Step 5 Verify the VPN statistics setting is correct or change it if necessary.

Step 6 If you changed the setting, click **Save**, then click **Cancel** to return to the health policy.

Step 7 Under Firewall Threat Defense Health Policies, click **Deploy health policy** (⬆) to apply the policy.

Step 8 In the **Policy Assignments & Deploy** dialog box, move the devices to which to deploy the health policy to the **Selected Devices** field.



Step 9 Click **Apply**.
A message is displayed when the health policy is deployed.

Step 10 After the health policy has finished deploying, click **Policies** > **Security policies** > **Access Control** to edit an access control policy.

Step 11 Click **Edit** (✎) next to a policy to edit.

Step 12 Make a minor change to the policy, such as changing its name.

Step 13 Save the access control policy.

Step 14 Deploy configuration changes..