Control Users with Remote Access VPN

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

The Remote Access VPN Identity Source

Firepower Threat Defense provides secure gateway capabilities that support remote access SSL and IPsec-IKEv2 VPNs. The full tunnel client, AnyConnect Secure Mobility Client, provides secure SSL and IPsec-IKEv2 connections to the security gateway for remote users. AnyConnect is the only client supported on endpoint devices for remote VPN connectivity to Firepower Threat Defense devices.

When you set up a secure VPN gateway as discussed in Create a New 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.

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 Firepower Threat Defense secure gateway.

Note If users authenticate with RA 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 via a VPN connection, the remote user takes on a *VPN Identity*. This VPN Identity is used by *identity policies* on the Firepower 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 the remote user blocked or allowed to access your network resources.

Related Topics

VPN Overview for Firepower Threat Defense

Firepower Threat Defense Remote Access VPN Overview
VPN Basics
Remote Access VPN Features
Guidelines and Limitations for Remote Access VPNs
Create a New Remote Access VPN Policy

Configure RA VPN for User Control

Before you begin

- Create a realm as discussed in Create a Realm.
- To use authentication, authorization, and auditing (AAA), set up a RADIUS server group as discussed in RADIUS Server Groups.

Step 1 Log in to the Firepower Management Center.

Step 2 Click **Devices** > **VPN** > **Remote Access**.

Step 3 See Create a New Remote Access VPN Policy.

What to do next

- Specify users to control and other options using an identity policy as described in Create an Identity Policy.
- Associate the identity rule with an access control policy, which filters and optionally inspects traffic, as discussed in Associating Other Policies with Access Control.
- Deploy your identity and access control policies to managed devices as discussed in Deploy Configuration Changes.
- Monitor VPN user traffic as discussed in VPN Session and User Information.

Troubleshoot the Remote Access VPN Identity Source

- For other related troubleshooting information, see Troubleshoot Realms and User Downloads, Troubleshoot User Control, and VPN Troubleshooting for Firepower Threat Defense.
- If you experience issues with Remote Access VPN, check the connection between your Firepower 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 Firepower Management Center.

  The unidentified users are logged as Unknown users on the Firepower Management Center. After the downtime, the Unknown users are re identified 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.

History for RA VPN

Feature	Version	Details
Remote Access VPN	6.2.1	Feature introduced. RA VPN allows individual users to connect to a private business network from a remote location using a laptop or desktop computer connected to the internet, or an Android or Apple iOS mobile device. Remote users transfer data securely and confidentially using encryption techniques crucial for data being transferred over shared mediums and the Internet.