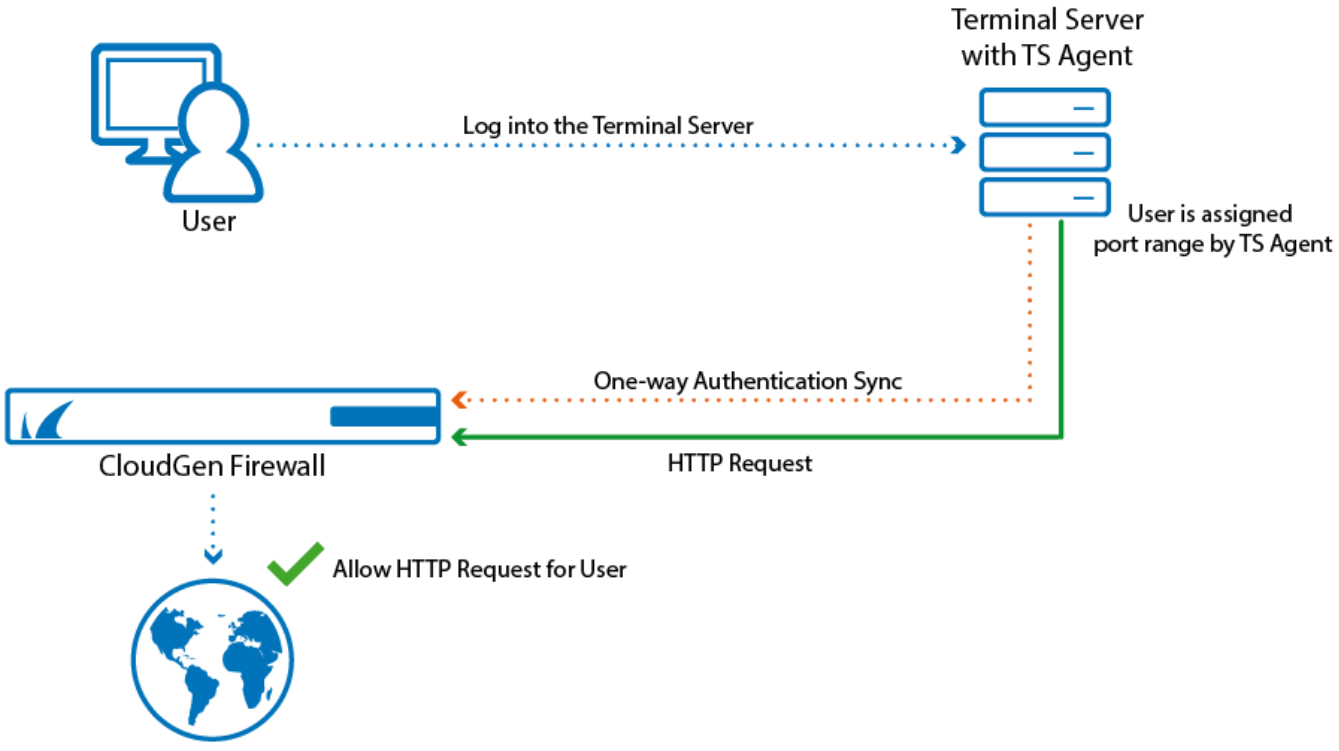
How to Configure TS Agent Authentication

https://campus.barracuda.com/doc/72516616/

The Barracuda TS Agent is the connector between various Barracuda Networks products and Microsoft Terminal Servers to transparently monitor user authentication. Because the source IP address for all users on the terminal server is the same, the Barracuda TS Agent assigns each user a specific port range and sends this mapping information to the firewall. The firewall can now check the source port of a TCP or UDP packet from the terminal server and, with the port-user information from the TS Agent, determine the username and group context. Connections with the Barracuda TS Agent are SSL encrypted. Mapping information for users is only sent after connections are established.
The Barracuda TS Agent also writes a debug log that helps you monitor your Terminal Server and identify possible problems. You can use SSL client certificates to authenticate the remote TS Agent on the Terminal Server, or, if no SSL certificates are configured, all incoming SSL connections from the server are allowed. TS Agent authentication with automatic port mapping does NOT work for SMB sessions on TCP port 445 and 139.



Before You Begin

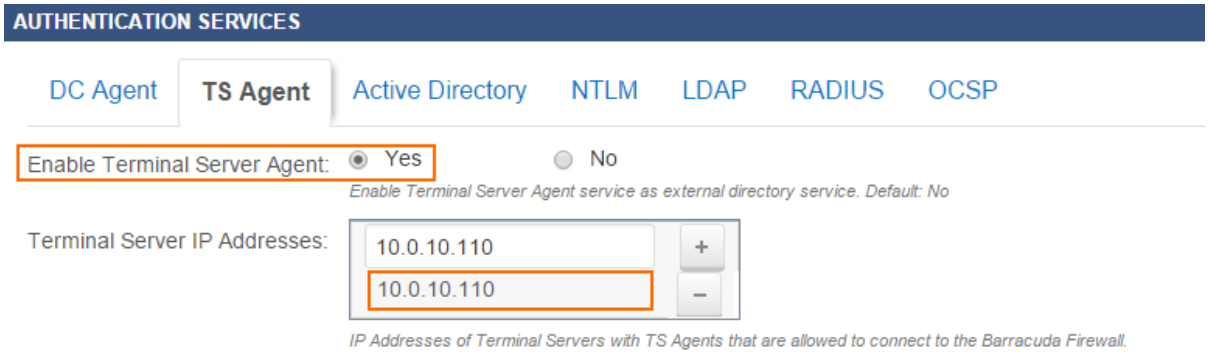
- Install the Barracuda TS Agent on the Microsoft Terminal Server(s). For instructions, see How to Set Up the Barracuda Terminal Server Agent.

- (Optional) Create SSL client certificates.

Configure TS Agent Authentication

On the CloudGen Firewall, enter the IP address of the Terminal Server running the Barracuda TS Agent. The TS Agent must be configured to allow connections to the management IP address of the firewall.

1. Go to **USERS > External Authentication**.
2. Click the **TS Agent** tab.
3. Set **Enable Terminal Server Agent** to **Yes**.
4. Enter the IP address for the Terminal Server running the TS Agent and click **+** .



The firewall will now receive authentication information from the TS Agent on the Microsoft Terminal Server.

Use Custom SSL Certificates

If you enable SSL, the connection between the firewall and the TS Agent is SSL encrypted. By uploading your own SSL certificates to the TS Agent and CloudGen Firewall, the connection will only be established if the SSL certificate is valid.

> If the TS Agent is configured to use SSL, an SSL-encrypted connection will be established, even if the **Use SSL** option is disabled on the firewall.

1. Go to **USERS > External Authentication**.
2. Click the **TS Agent** tab.
3. Click **Show Advanced Options**.
4. Enable **Use SSL**.

5. Enter the **Subject Alternative Name** of the SSL client certificate.
6. Upload the SSL client certificate. For information on how to create and manage certificates, see How to Use and Manage Certificates with the Certificate Manager.
7. Click **Save**.

The firewall will now use SSL and verify the SSL certificate when connecting to the TS Agent.

Figures

1. ts_agent-01.png
2. ts_ip_67.png