How to configure Client Authentication in R80.20

Rick Carlo
Security Engineer
November 29, 2018

Table of Contents:

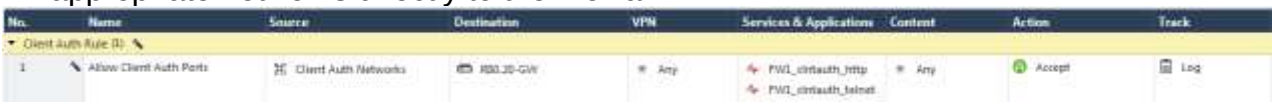
What is a Client Authentication?

Client Authentication permits multiple users and connections from the authorized IP address or host. Authorization is performed per machine, so client authentication is best enabled on single-user machines. For example, Client Authentication can be used to authorize FTP for a client machine to a specific server. With Client Authentication all users on this machine would now be authorized to use FTP to the same server. Users on other machines would not be able to use FTP. Client Authentication can be used on a number of connections for any service. Authentication can be set to valid for a time period. These authentication methods can also be used for unencrypted communication.

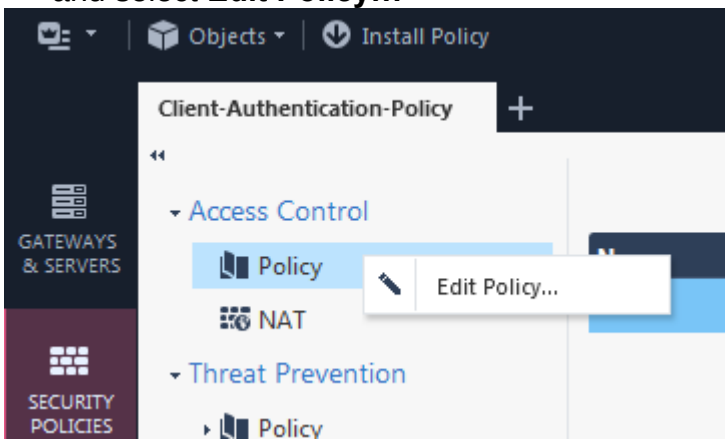
Client Authentication Policy Configuration:

1. Create appropriate objects for Client Authentication. These include the following:
    a. Network object or Network Group object to designate sources from which users will be connecting.
    b. User Group for the Client Authentication Users.
    c. User objects as needed. These should be added to the Client Authentication Users group object created above.

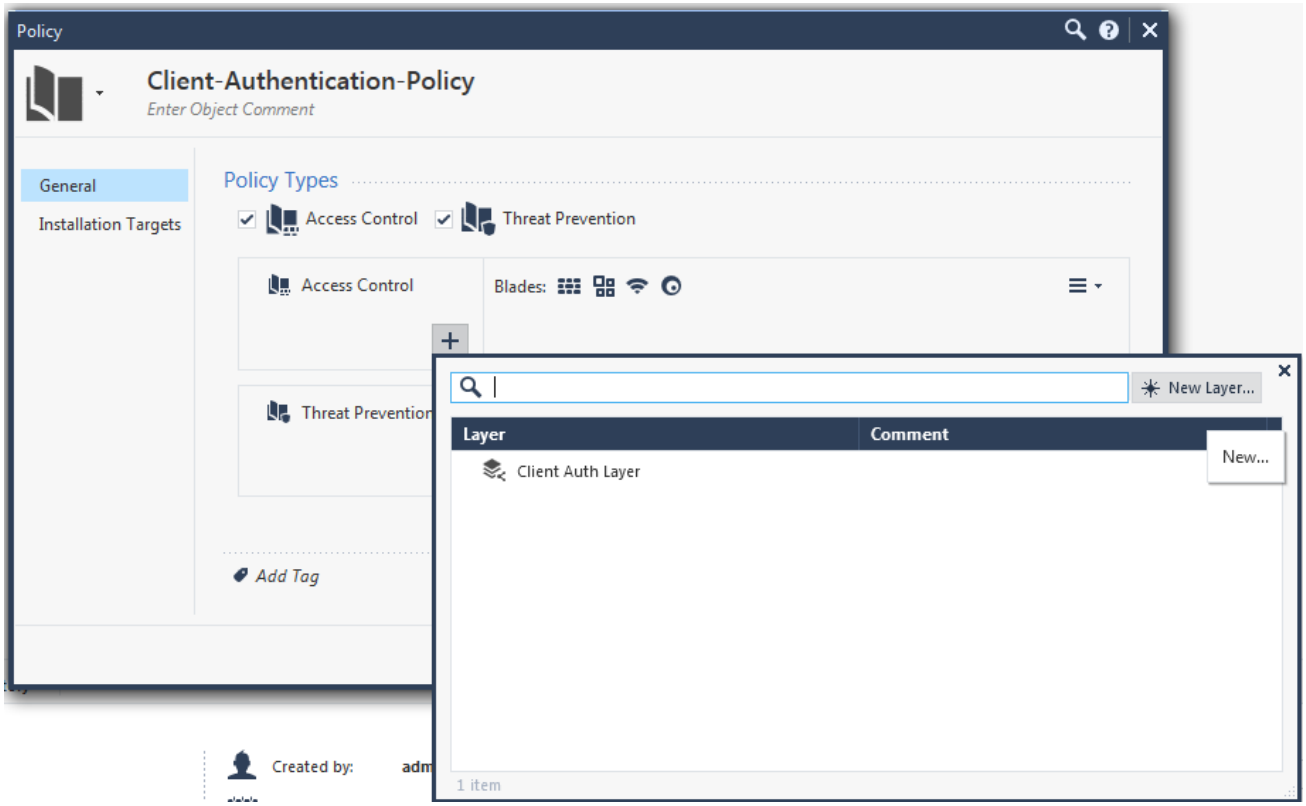
2. Add rule to allow Client Authentication associated ports to gateway.
    a. Above the standard Stealth Rule, add a new rule to the existing Firewall policy to allow the Client Authentication services (TCP 259 and TCP 900) from the appropriate networks directly to the firewall.



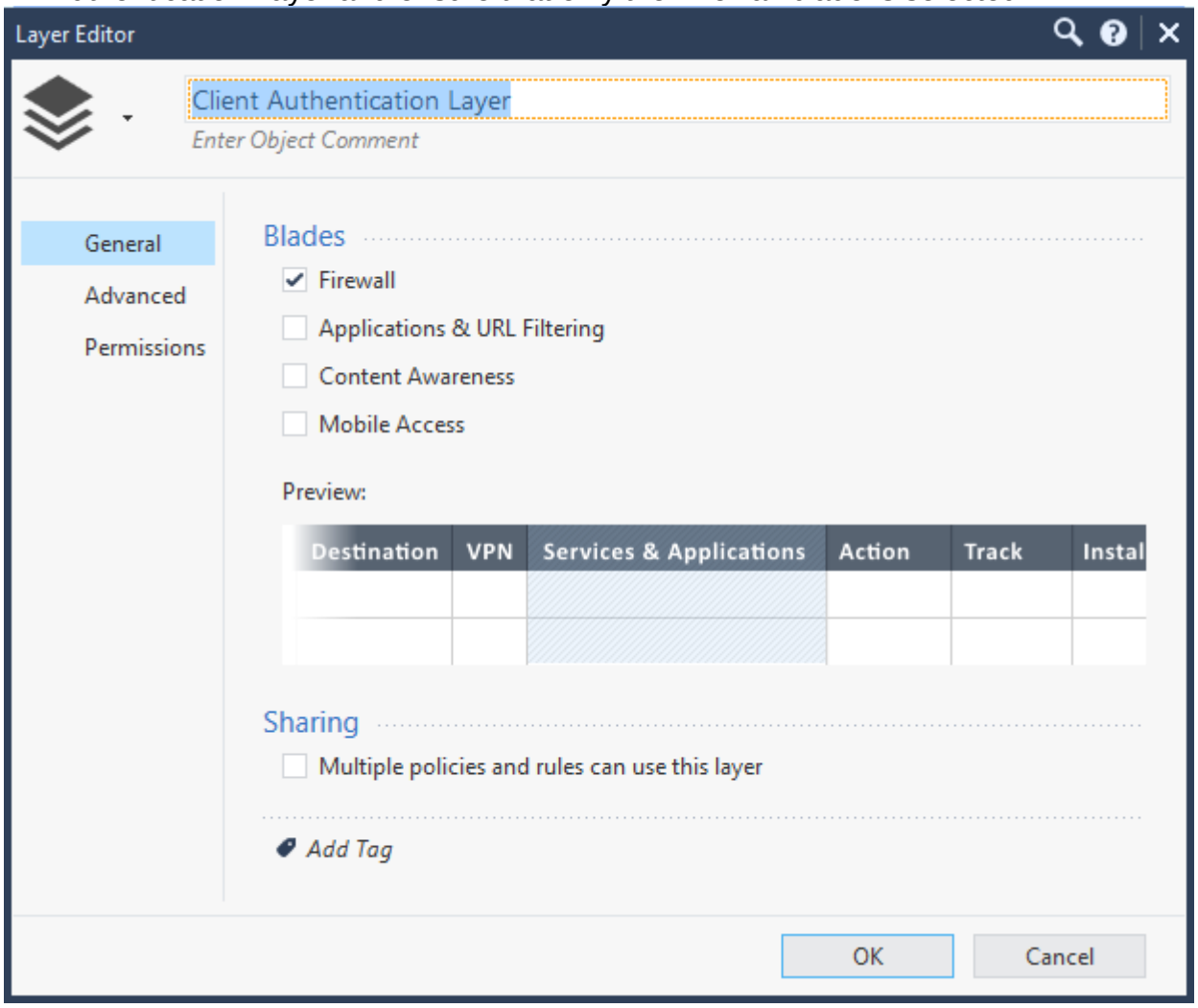
3. Add a new layer to your existing policy
    a. On the **Security Policies** page under **Access Control**, right-click on the policy and select **Edit Policy…**



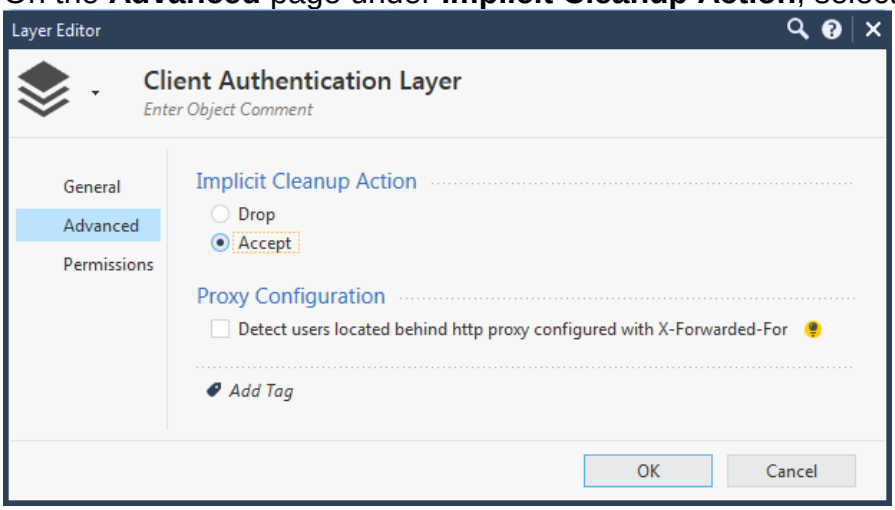
    b. Under **Access Control**, click the **+** sign and click the *** New Layer…** button.



c. In the **Layer Editor** window on the **General** page, enter a name for the Client Authentication Layer and ensure that only the Firewall blade is selected.

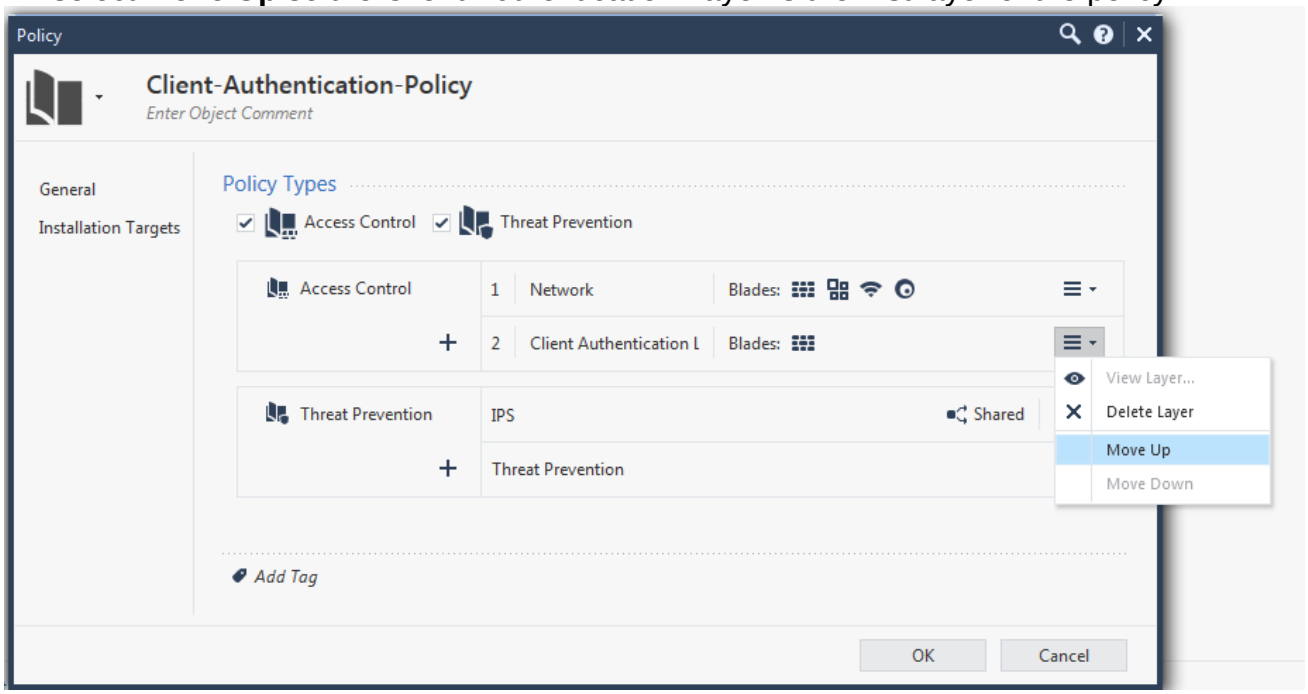


d. On the **Advanced** page under **Implicit Cleanup Action**, select **Accept**.



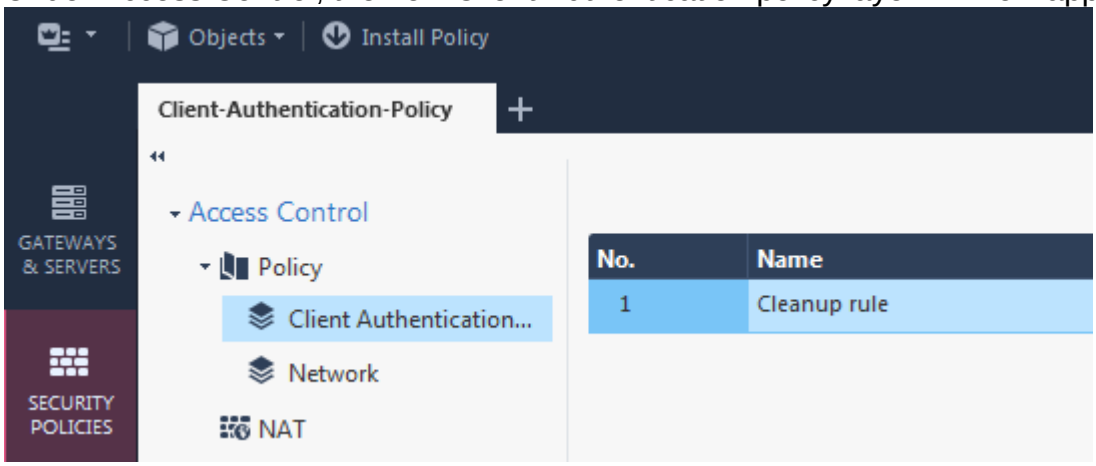
e. Click the **OK** button to close the **Layer Editor** window.

f. Click the drop-down menu icon next to the new layer just added to the policy and select **Move Up** so the Client Authentication Layer is the first layer of the policy.



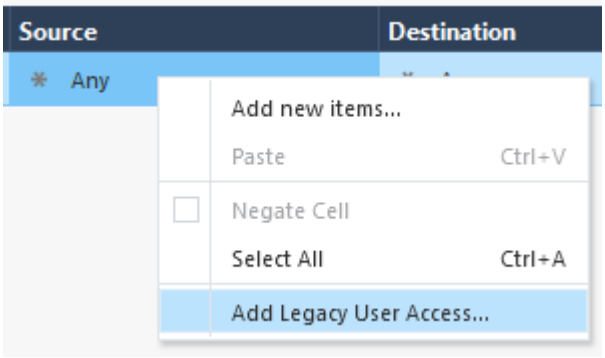
g. Click the **OK** button to close the Policy properties window.

Under Access Control, the new Client Authentication policy layer will now appear.

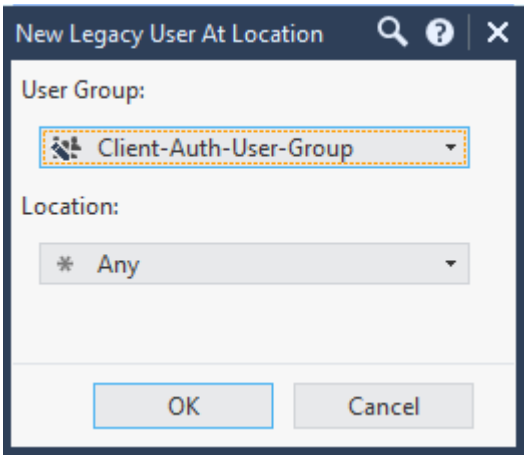


4. Add rules to allow the Client Authentication Users access over the specified ports and deny others.
   a. Within the Client Authentication Layer policy, add a new rule and provide an appropriate rule name.

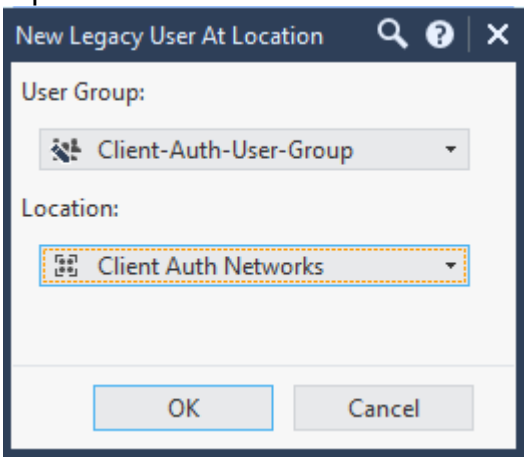
b. In the **Source** field, right-click and select **Add Legacy User Access…**



c. In the **User Group:** dropdown, select the Client Authentication User group created earlier.



d. In the **Location:** dropdown, select the network or network group object that represents the location from which Client Authentication is allowed.

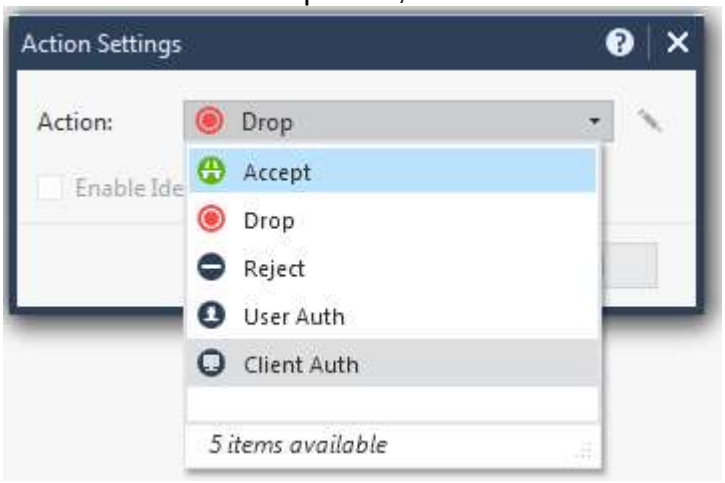


e. Set the appropriate destination server(s) or network(s).

f. In the **Services & Applications** field, select the services that Client Authenticated users are allowed to use through the gateway.

g. Right-click in the **Action** column and select **More…**

h. In the **Action**: dropdown, select **Client Auth** and click **OK**.



i. Set the appropriate logging level.

j. Add another rule to drop traffic from unauthenticated sources to the same servers over the same ports.

Rules should be similar to the following:

No.	Name	Source	Destination	Services & Applications	Action	Track
1	FTP Allow for Client Auth	Client-Auth-User-Group@Client Auth Networks	FTP Server	ftp	Client Auth	Log
2	FTP Block for Everyone Else	Client Auth Networks	FTP Server	ftp	Drop	Log

k. Remove any existing **Cleanup Rule** that may exist.

5. Within the Network Layer, add rule to allow access to the server(s) or network(s) over the ports used in the Client Authentication rules.

6. Publish and Install policy to gateway.

Client Authentication Policy Logic Explained:

In the above policy, we created an Ordered layer that is hit before the main firewall policy. The rules in this layer only pertain to the ports that are relevant for Client Auth access. Users can authenticate using Client Auth over TCP 259 or 900, ports which are now allowed to the firewall in the main policy. Authenticated users will hit the first rule of the Client Authentication Policy layer and move to the Main policy where that traffic needs to be accepted a second time before they can reach the server. Clients coming from the protected Client Authentication networks who do not successfully authenticate using Client Auth will be dropped by rule 2 of the Client Authentication Policy layer and not fall into the Main policy. Any other traffic that is not related to the Client Auth rules will be accepted at the end of the Client Authentication Policy layer and fall into the Main policy.

