How to enable Domain Map in AsyncOS for Web Security Guide

In transparent mode, when the SNI (Server Name Indicator) is not present in Client Hello message, WSA sends its own client hello to the server to validate server certificate and domain name (per current design) even in pass-through custom category case. However, for the server who uses proprietary TLS, the TLS handshake would fail due to cipher incompatibility of WSA and server. Eventually, the entire request was dropped. Due to these issues the application like Skype, WhatsApp does not work when the transparent WSA proxy is present.

In skype meeting call case, even the skype request was matched the pass-through custom category, the connection fails. This is because the skype server is using propitiatory TLS cipher and which is not supported by WSA, hence the WSA's client hello for the certificate validation fails and eventually the entire connection get dropped.

While these are non-standard behaviour, there are some popular applications (like WhatsApp, Skype For Business) that follow this approach. For these, a WSA administrator may require traffic to be permitted as per organisation policies. To support such use-cases, the WSA currently has the "Proxy Bypass" feature. This allows such traffic to pass through the WSA without being "seen" by the proxy and hence, not subjected to any policies. However, the flip side of this approach is that there is literally "no trace" of this traffic having ever traversed the WSA, i.e., there are no access logs and reporting for this traffic.

To overcome these situations, we have introduced Domain Map feature starting in AsyncOS 11.8.

Introduction to Domain Map:

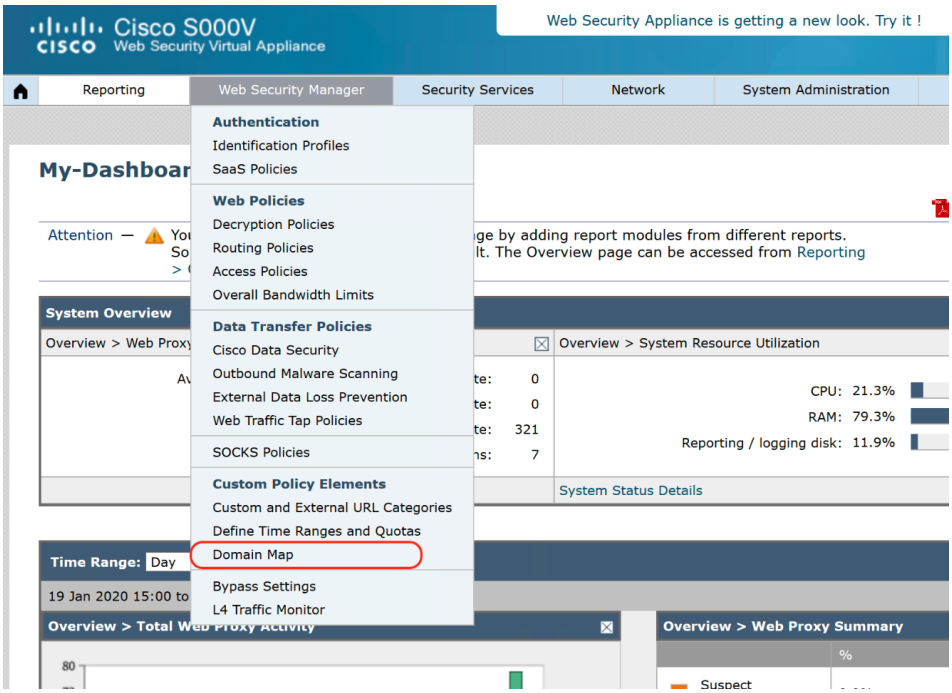
Starting in AsyncOS 11.8, you can configure the Web Security appliance so that transparent HTTPS requests from particular clients, or to particular destinations, bypass the HTTPS Proxy.

You can use passthrough for applications that require traffic to pass through the appliance, without undergoing any modification, or certificate checks of the destination servers.

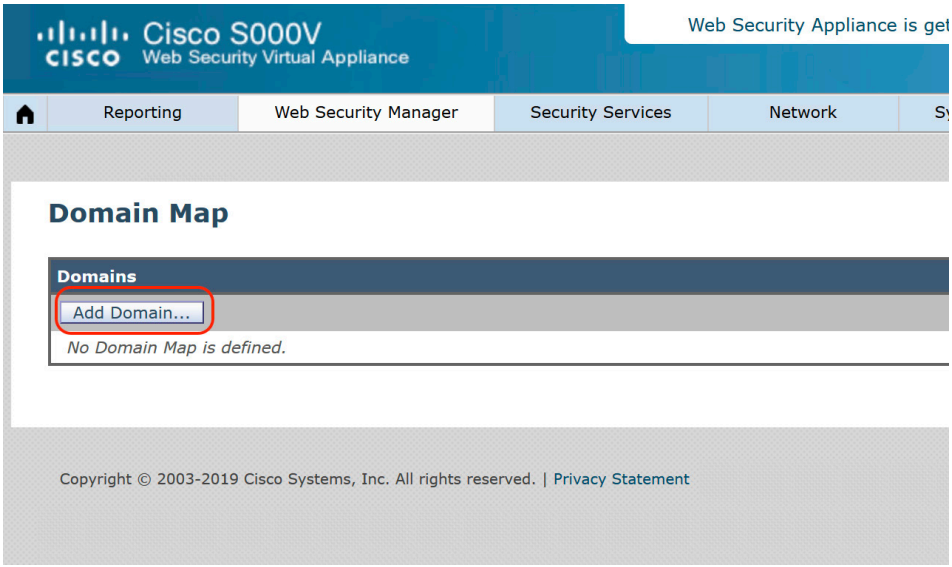
Configuration Steps:

Step 1. First enable the HTTPS proxy, you can follow Enable HTTPS Proxy.

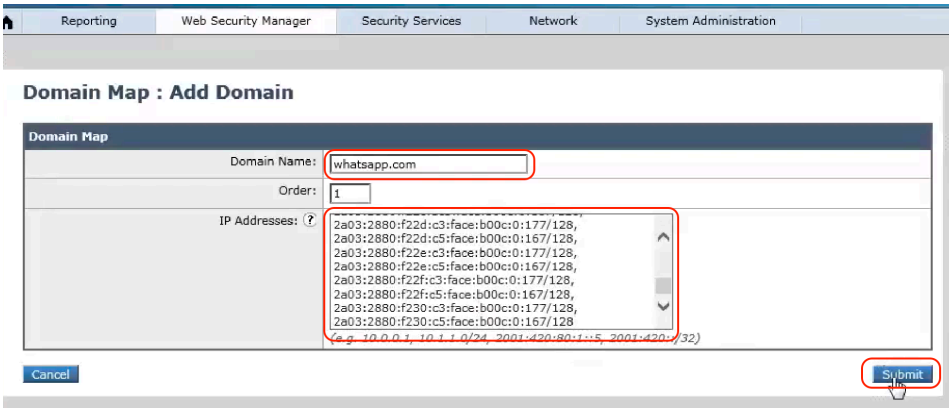
Step 2. Once you enable the HTTPS proxy, we have to create a mapping for each domain with corresponding IP addresses. Choose **Web Security Manager > Domain Map**



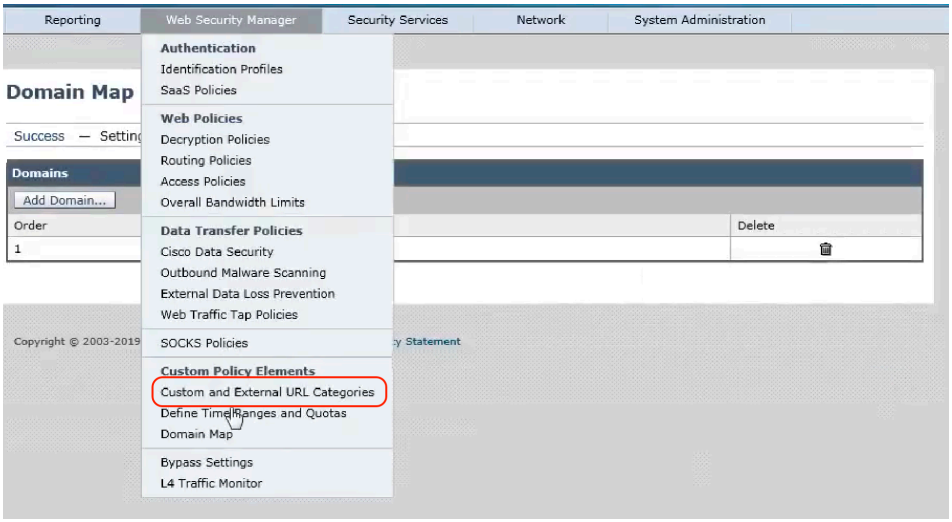
a. To create a Mapping, click **Add Domain**. To edit the existing Domain Map, click on the name of the Domain Map



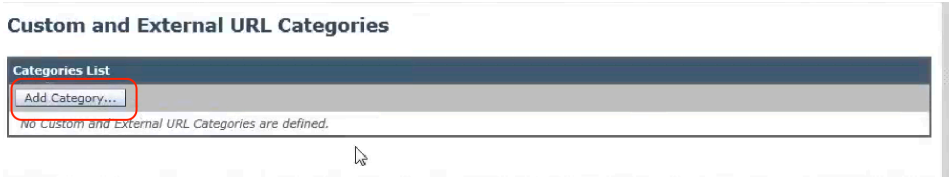
a. Enter the Domain Name or the destination server, you can also choose the order of the priority if there are existing domains specified, Enter the IP addresses and Click **Submit** button.



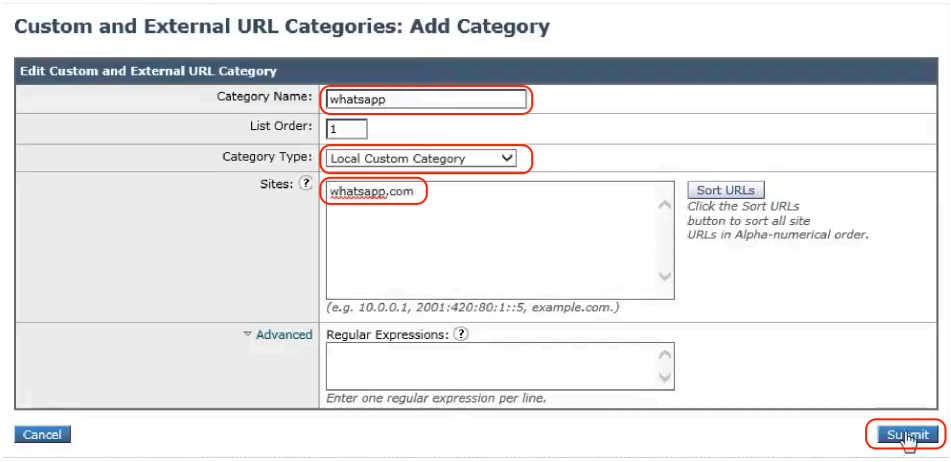
Step 3. After creating the Domain Map, we have to create a Custom URL Category, Choose **Web Security Manager**, and click **Custom and External URL Categories.**



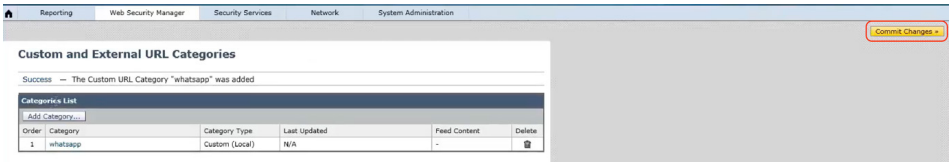
a. To add the category, click **Add Category**. To edit the existing URL Category, click on the name of the URL Category.



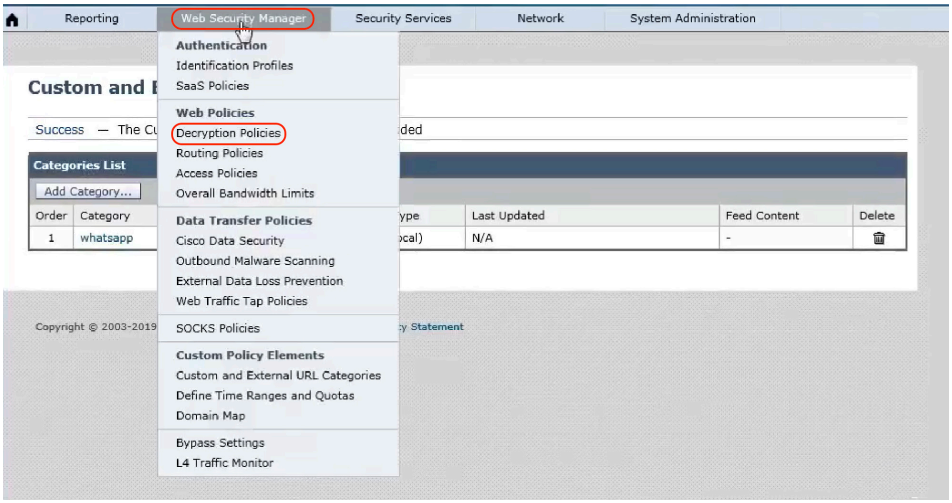
b. Provide the Category Name, this name appears when you configure URL filtering for policy groups. Specify the order of this category in the list of custom URL categories. Enter “1” for the first URL category in the list. The URL filtering engine evaluates a client request against the custom URL categories in the order specified, choose Local Custom Category. Additionally, under the Advanced section, you can enter regular expressions to specify additional sets of addresses. You can use regular expressions to specify multiple addresses that match the patterns you enter. Click on **Submit** button



c. Make sure you **Commit** the changes.

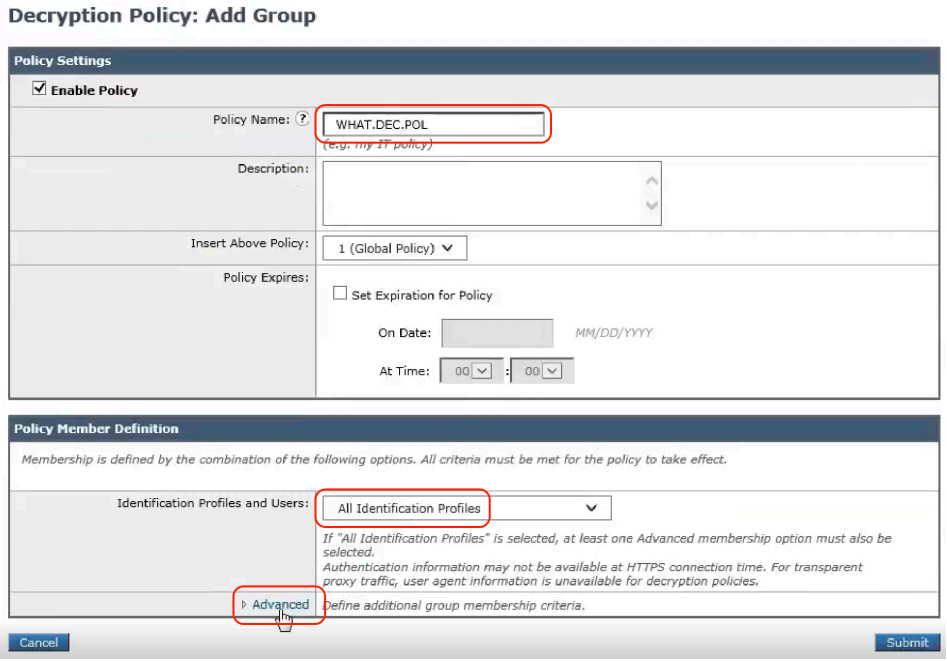


Step 4. To configure Decryption Policy, Choose **Web Security Manager**, click on **Decryption Policies**.

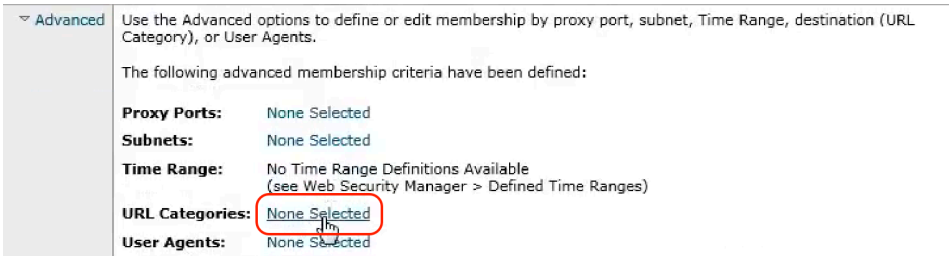


a. Click on Add Policy... to create a new decryption policy.

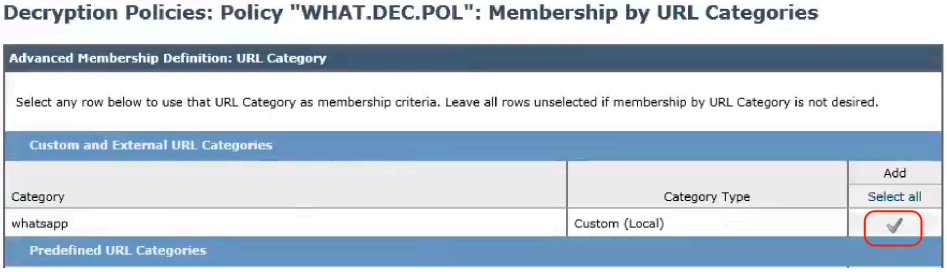
b. Enter the Policy name, set the order of the policy, choose the identification profile that you created for bypassing HTTPS traffic for specific applications.



c. Click on **Advanced** panel to expand the options, click the *link* for URL Categories.

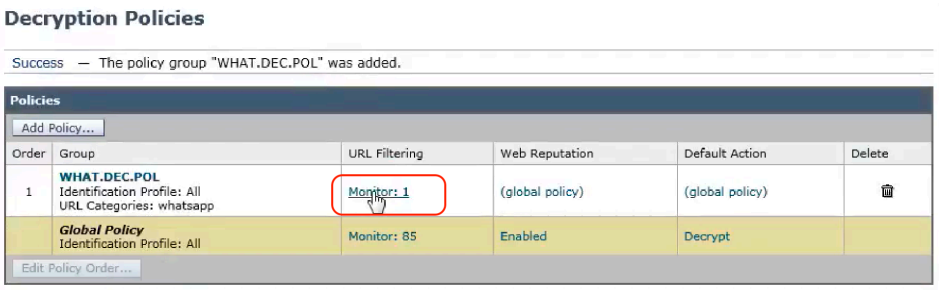


d. In the **Add** column for the respective custom URL Category, click to add the custom URL category created in step 3.

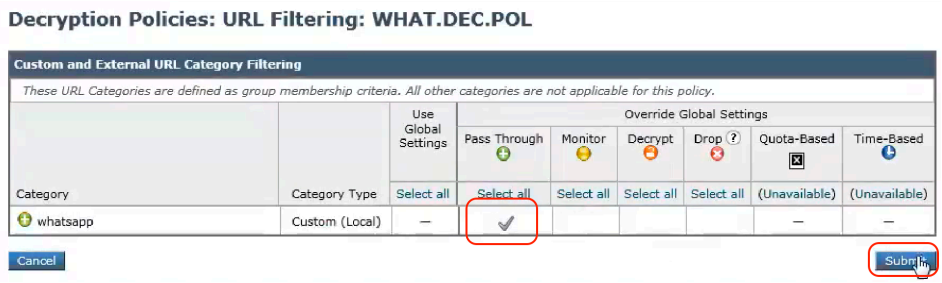


e. Click **Done**.

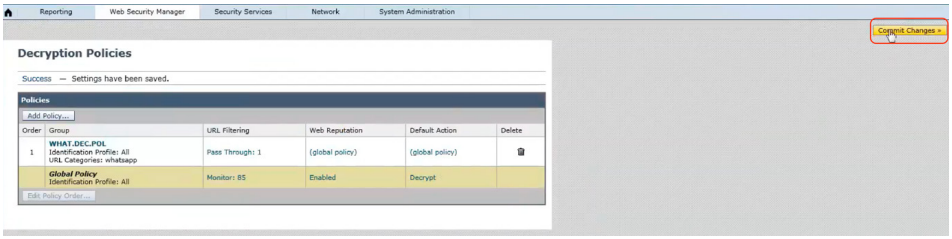
f. In the Decryption Policies page, click the link for **URL Filtering**.



g. Choose **Pass-Through** for the URL category and click on **Submit** button



h. Commit the changes.

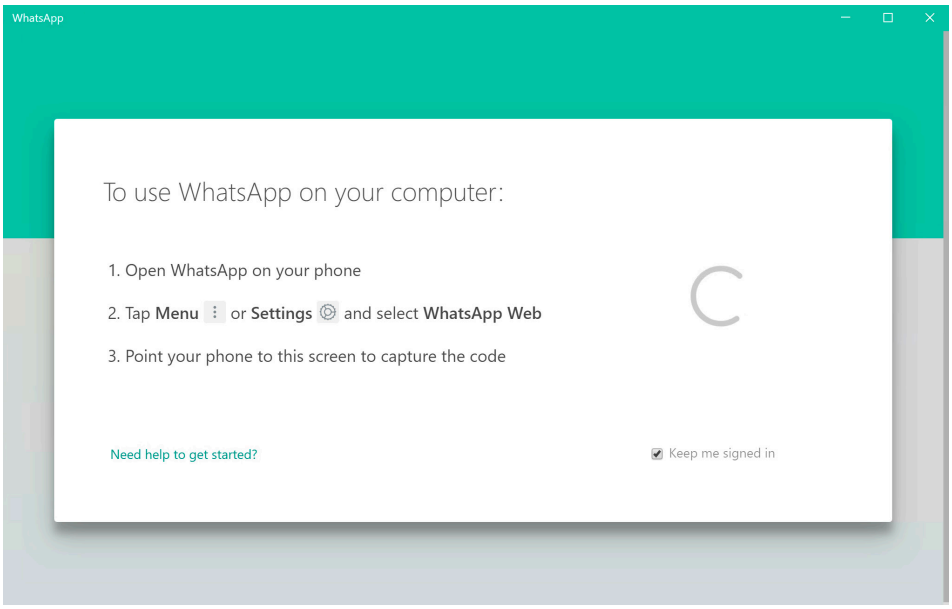


Use cases:

1. WhatsApp.com

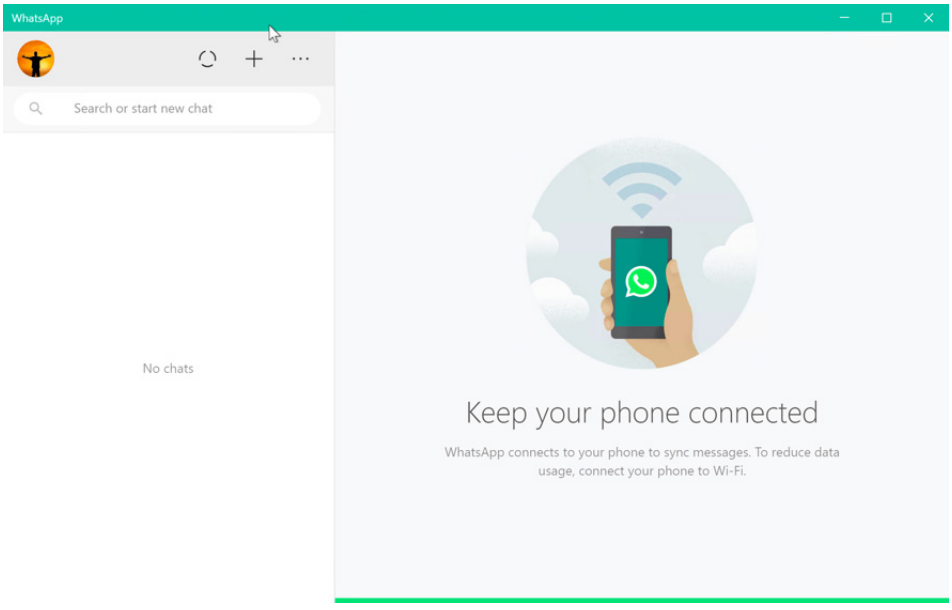
Here is the screenshot when WhatsApp is not connecting:

(it gets stuck on the loading window)



After configuring the Domain Map:

Users get the QR code to connect and it's connected:

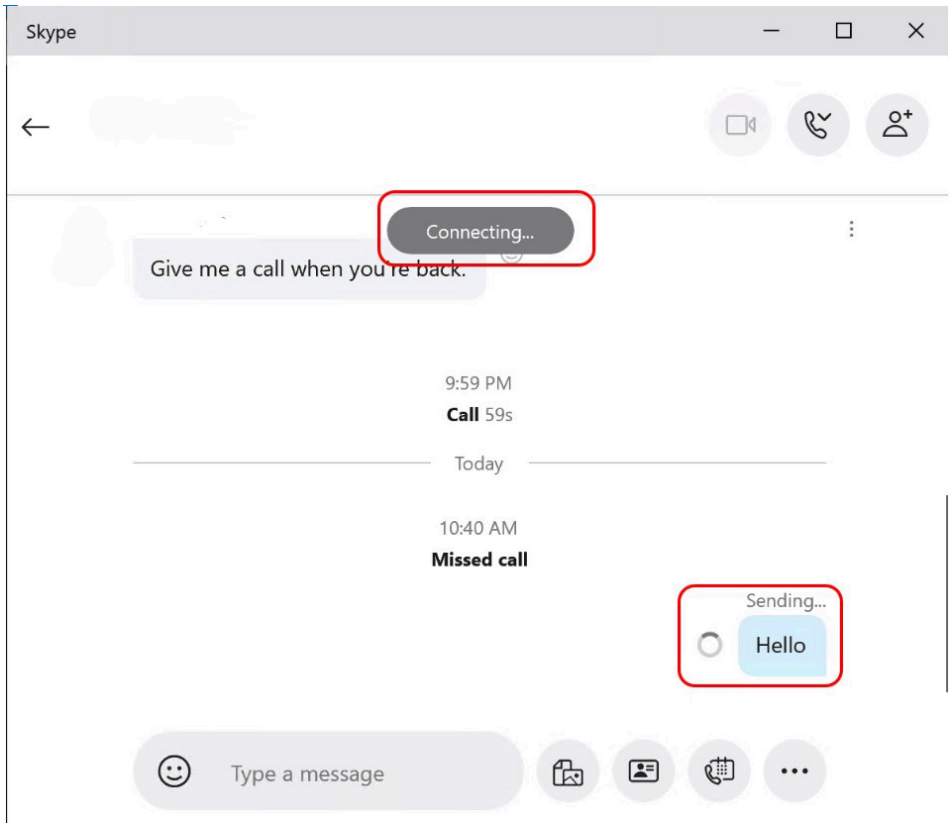


1579627402.437 1493 192.168.0.150 TCP_MISS/200 3064 TCP_CONNECT **157.240.192.52:443** - **DIRECT/157.240.192.52** - PASSTHRU_CUSTOMCAT_7-WHAT.DEC.POLI-idenPolicy-NONE-NONE-NONE-DefaultGroup-NONE <"**C_what**",-,-,"-",-,-,-,-,"-",-,-,"-",-,-,"-","-","-","-","-","-","-","-","-","-","-","-","-","-","-",16.42,0,-,"-","-","-",-,"-","-",-,-,"-","-","-",-,-,"-",-> -

2. Skype

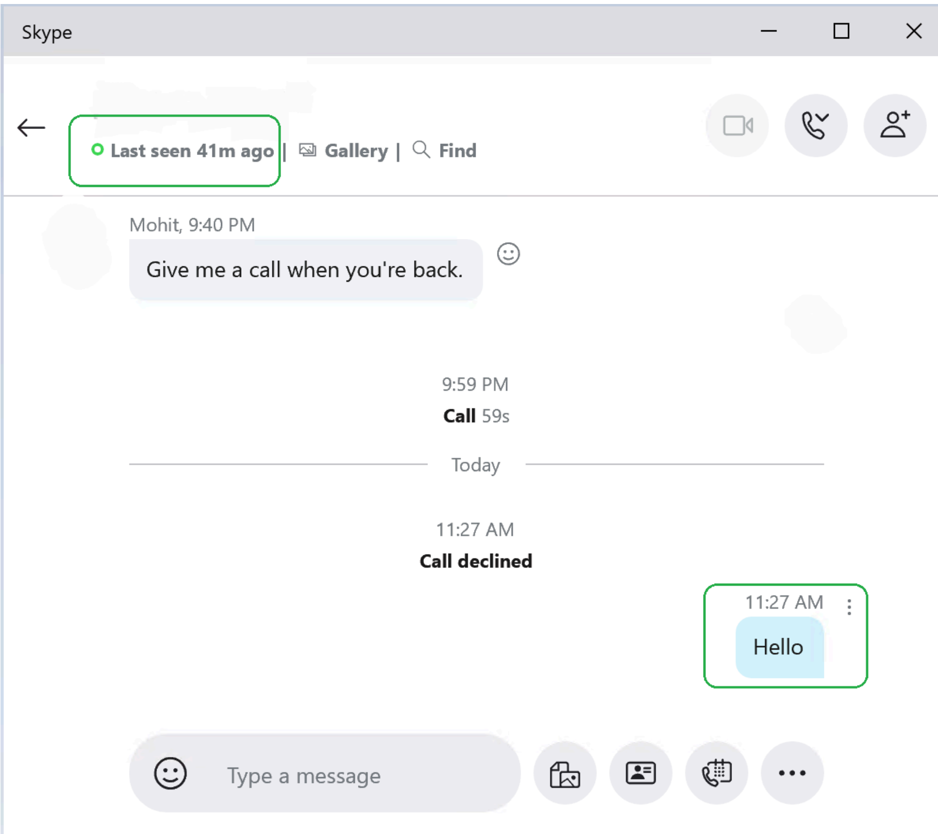
Before implementing Domain-map, Skype application is not connecting and messages are not going over:

1581570529.211 75000 192.168.0.150 TCP_MISS/504 0 TCP_CONNECT 52.179.209.218:443 MOHSONI\usertwo@AD DIRECT/options.skype.com - OTHER-NONE-IdenPolicy-NONE-NONE-NONE-DefaultGroup-NONE <"-",-,-,"-","-",-,-,-,-,"-","-",-,-,-,"-","-",-,-,"-","-","-",-,"-","-","-","-","-","-","-","-","-","-","-",0.00,0,-,"-","-","-",-,"-","-",-,-,"-","-","-",-> - -



After configuring Domain Map and action to Pass through for defined custom category, application is connected:

1581573559.770 121356 192.168.0.150 TCP_MISS/200 6774 TCP_CONNECT 52.179.209.218:443 "MOHSONI\usertwo@AD" DIRECT/options.skype.com - PASSTHRU_CUSTOMCAT_7-DecryptPoli-IdenPolicy-NONE-NONE-NONE-DefaultGroup-NONE <"C_skyp",-,-,"-","-",-,-,-,-,"-","-",-,-,-,"-","-",-,-,"-","-","-",-,"-","-","-","-","-","-","-","-","-","-","-",0.45,0,-,"-","-","-",-,"-","-",-,-,"-","-","-",-,-,"-",-> - skype.com



Logging:

You can use the **%(** format specifier to view access log information.

Here are the sample logs for your reference:

Once we implemented the domain map and added custom field in access logs “**%(**“ :

1579627734.509 77 192.168.0.150 TCP_MISS/200 3063 TCP_CONNECT 157.240.192.52:443 - DIRECT/157.240.192.52 - PASSTHRU_CUSTOMCAT_7-WHAT.DEC.POLI-idenPolicy-NONE-NONE-NONE-DefaultGroup-NONE <”C_what”,-,-,”-”,-,-,-,-,”-”,-,-,-,”-”,-,-,”-”,”-”,-,-,”-”,-,”-”,”-”,”-”,”-”,”-”,”-”,”-”,318.23,0,-,”-”,”-”,-,”-”,-,-,”-”,”-”,-,-,”-”,-> - **whatsapp.com**

Key Notes

- The Domain Map feature works in HTTPS Transparent mode.
- This feature does not work in Explicit mode and for HTTP traffic.
- Local Custom Category must be configured to allow the traffic using this feature.
- Enabling this feature will modify or assign the server name as per the server name configured in the Domain Map, even if SNI information is available.
- This feature does not block traffic based on the domain name if that traffic matches the Domain Map and corresponding custom category, decryption policy and passthrough action are configured.
- UDP traffic is not monitored. You must configure UDP traffic not to come to the WSA, instead, it should go directly through the firewall to the internet for applications like WhatsApp, Telegram etc.
- WhatsApp, Telegram and Skype work in Transparent mode. However, some apps like WhatsApp do not work in Explicit mode due to restrictions on the app.